



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2011)

VII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 26-28 октября 2011 г.

ТРУДЫ КОНФЕРЕНЦИИ

Санкт-Петербург

2012



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2011)

VII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 26-28 октября 2011 г.

ТРУДЫ КОНФЕРЕНЦИИ

Санкт-Петербург

2012

УДК (002:681):338.98

И 74

И 74 **Информационная** безопасность регионов России (ИБРР-2011). VII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 26-28 октября 2011 г.: Труды конференции / СПОИСУ. – СПб., 2012. – 185 с.

ISBN 978-5-905687-97-6

Сборник охватывает широкий круг направлений: государственная политика обеспечения информационной безопасности регионов России; правовые аспекты информационной безопасности; безопасность информационных технологий; современные средства защиты информации; информационная безопасность телекоммуникационных сетей; информационная безопасность в критических инфраструктурах; информационная безопасность в гидрометеорологии; подготовка и переподготовка кадров в области обеспечения информационной безопасности, а также материалы круглого стола по проблемам подготовки и переподготовки кадров в области защиты персональных данных.

Предназначен для широкого круга руководителей и специалистов предприятий и организаций, органов государственной власти и управления, научных работников, преподавателей, аспирантов и студентов, занимающихся вопросами сохранения и развития единого защищенного информационного пространства России, обеспечения безопасности и эффективности использования региональных информационных ресурсов, защиты информации в региональных информационных и телекоммуникационных системах, подготовки и переподготовки кадров в области обеспечения информационной безопасности.

УДК (002:681):338.98

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

Публикуется в авторской редакции

Подписано в печать 10.09.2012. Формат 60х84 $\frac{1}{8}$. Бумага офсетная.
Печать – ризография. Усл. печ. л. 21,5. Тираж 300 экз. Заказ № 4531
Отпечатано в ООО «К-8»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-905687-97-6

© Санкт-Петербургское Общество информатики,
вычислительной техники, систем связи и
управления (СПОИСУ), 2012 г.

© Авторы, 2012 г.



INFORMATION SECURITY OF RUSSIAN REGIONS (ISRR-2011)

VII ST. PETERSBURG INTERREGIONAL CONFERENCE

St. Petersburg, October 26-28, 2011

PROCEEDINGS OF THE CONFERENCE

St. Petersburg

2012



УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ

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

СОУСТРОИТЕЛИ КОНФЕРЕНЦИИ

- Российский фонд фундаментальных исследований
- Государственный научный центр РФ - Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики
- ФГУП «Научно-исследовательский институт «Масштаб»
- ФГУП «Научно-исследовательский институт «Рубин»
- ФГУП «Научно-производственное объединение «Импульс»
- ФГУП «ЦентрИнформ»
- СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
- ОАО «Центр компьютерных разработок»
- ЗАО «Ассоциация специалистов информационных систем»
- ЗАО «Институт телекоммуникаций»
- ЗАО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
- ЗАО «РАМЭК-ВС»
- ЗАО «Санкт-Петербургский Региональный Центр защиты информации»
- ЗАО «Эврика»
- ЗАО «Метроком»
- ОАО «Северо-Западный Телеком»
- ООО «ИнТехСервис»
- ООО «Компания «Марвел»
- ООО «Лаборатория инфокоммуникационных сетей»
- ООО «Максима»
- ООО «НеоБИТ»
- Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
- Петербургский государственный университет путей сообщения
- Санкт-Петербургский государственный политехнический университет

- Санкт-Петербургский государственный университет аэрокосмического приборостроения
- Санкт-Петербургский государственный университет водных коммуникаций
- Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
- Санкт-Петербургский государственный университет технологии и дизайна
- Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
- Санкт-Петербургский институт экономики и бизнеса
- Санкт-Петербургский университет МВД России
- Смольный институт Российской академии образования
- Учебно-методическое объединение вузов России по университетскому политехническому образованию при Московском государственном техническом университете им. Н.Э. Баумана
- Партнерство для развития информационного общества на Северо-Западе России
- Северо-западное отделение Российской академии образования
- Санкт-Петербургская инженерная академия
- Санкт-Петербургское отделение Международной академии информатизации
- Санкт-Петербургское отделение Академии информатизации образования

КООРДИНАЦИОННЫЙ СОВЕТ КОНФЕРЕНЦИИ

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

ПРЕЗИДИУМ КОНФЕРЕНЦИИ

Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга
Юсупов Рафаэль Мидхатович	Директор Санкт-Петербургского института информатики и автоматизации Российской академии наук
Дивинский Игорь Борисович	Вице-губернатор Санкт-Петербурга - руководитель Администрации Губернатора Санкт-Петербурга
Селин Владимир Викторович	Директор ФСТЭК России
Громов Иван Александрович	Председатель Комитета по информатизации и связи Санкт-Петербурга
Васильев Владимир Николаевич	Председатель совета ректоров Санкт-Петербурга, ректор Санкт-Петербургского государственного университета информационных технологий, механики и оптики

Гусев Владимир Сергеевич	Директор департамента безопасности Международного Банка «Санкт-Петербург»
Кучерявый Михаил Михайлович	Руководитель Управления Федеральной службы технического и экспортного контроля по Северо-Западному федеральному округу
Лопота Виталий Александрович	Президент - генеральный конструктор Ракетно-космической корпорации «Энергия» им. С.П. Королева
Максимов Андрей Станиславович	Председатель Комитета по науке и высшей школе Санкт-Петербурга
Пешехонов Владимир Григорьевич	Генеральный директор ГНЦ «Центральный научно-исследовательский институт «Электроприбор»
Шульц Владимир Леопольдович	Заместитель президента Российской академии наук

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Председатель Организационного Комитета

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

Заместитель председателя Организационного Комитета

Майоров Владимир Владимирович	Начальник отдела информационной безопасности, противодействия техническим разведкам и развития системы защиты информации Комитета по информатизации и связи Санкт-Петербурга
-------------------------------	--

Члены Организационного Комитета

Александров Анатолий Михайлович	Заместитель начальника Центра анализа и экспертизы ФГУП «Научно-производственное объединение «Импульс»
Андропова Ольга Олеговна	Главный редактор газеты «Компьютер Информ»
Бакурадзе Дмитрий Викторович	Ученый секретарь Санкт-петербургского института информатики и автоматизации Российской академии наук
Барышников Сергей Олегович	Ректор Санкт-Петербургского государственного университета водных коммуникаций
Басков Дмитрий Вячеславович	Генеральный директор ООО «НеоБИТ»
Бачевский Сергей Викторович	Ректор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
Блажис Анатолий Константинович	Генеральный директор ЗАО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
Богданов Владимир Николаевич	Директор ФГУП «ЦентрИнформ»
Борисов Николай Валентинович	Директор Междисциплинарного центра Санкт-Петербургского государственного университета
Викторов Александр Дмитриевич	ректор Санкт-Петербургского государственного университета сервиса и экономики
Вус Михаил Александрович	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Гирдин Сергей Алексеевич	Президент ООО «Компания «Марвел»

Гоголь Александр Александрович	Советник ректора, заведующий кафедрой Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
Григорьев Владимир Александрович	Генеральный директор ООО «Лаборатория инфокоммуникационных сетей»
Гуца Анатолий Григорьевич	Главный специалист СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Давыдов Евгений Борисович	Главный конструктор ФГУП «Научно-исследовательский институт «Масштаб»
Демидов Алексей Вячеславович	Ректор Санкт-Петербургского государственного университета технологии и дизайна
Долгирев Валерий Алексеевич	Помощник директора Санкт-Петербургского института информатики и автоматизации Российской академии наук по защите информации
Дрожжин Владимир Васильевич	Начальник департамента разработки специальных программ ОАО «МегаФон»
Жданов Сергей Николаевич	Заместитель генерального директора ЗАО «ВТБ-Девелопмент»
Жигадло Валентин Эдуардович	Генеральный директор ООО «Максима»
Заборовский Владимир Сергеевич	Заведующий кафедрой телематики Санкт-Петербургского государственного политехнического университета
Захаров Юрий Никитич	Директор СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Зегжда Петр Дмитриевич	Директор Специализированного центра защиты информации, заведующий кафедрой информационной безопасности компьютерных систем Санкт-Петербургского государственного политехнического университета
Зубков Юрий Сергеевич	Действительный государственный советник Санкт-Петербурга 3 класса
Игумнов Владимир Вячеславович	Главный конструктор ФГУП «Научно-производственное объединение «Импульс»
Ипатов Олег Сергеевич	Заведующий кафедрой Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова
Искандеров Юрий Марсович	Заместитель директора Института проблем транспорта им. Н.С. Соломенко Российской академии наук
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, декан ФПК Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова
Кирсанов Игорь Петрович	Генеральный директор ЗАО «ВО «РЕСТЭК»
Ковалев Валерий Иванович	Ректор Петербургского государственного университета путей сообщения
Коршунов Сергей Валерьевич	Заместитель председателя Совета УМО вузов России, проректор по учебной работе Московского государственного технического университета им. Н.Э. Баумана
Кузичкин Александр Васильевич	Заместитель директора ФГУП «Научно-исследовательский институт телевидения»
Кузьмин Юрий Григорьевич	Ученый секретарь Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления

Марков Вячеслав Сергеевич	Ученый секретарь Объединенного научного совета Санкт-Петербургского Научного центра Российской академии наук
Михайлов Николай Семенович	Технический директор Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Михайлова Анна Сергеевна	Заместитель директора по связям с общественностью Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Молдовян Александр Андреевич	Заместитель директора Санкт-Петербургского института информатики и автоматизации Российской академии наук по информационной безопасности
Николаев Алексей Юрьевич	Генеральный директор ЗАО «Эврика»
Оводенко Анатолий Аркадьевич	Ректор Санкт-Петербургского государственного университета аэрокосмического приборостроения
Остапенко Александр Николаевич	Генеральный директор ЗАО «Лаборатория противодействия промышленному шпионажу»
Перепелица Сергей Николаевич	Генеральный директор ООО «ИнТехСервис»
Присяжнюк Сергей Прокофьевич	Генеральный директор ЗАО «Институт телекоммуникаций»
Рунеев Анатолий Юрьевич	Генеральный директор ФГУП «Научно-исследовательский институт «Рубин»
Солодьянников Александр Владимирович	Генеральный директор ЗАО «Ассоциация специалистов информационных систем»
Терещенко Павел Геннадьевич	Заместитель генерального директора ФГБУ «Президентская библиотека им. Б.Н. Ельцина»
Тихомиров Сергей Григорьевич	Генеральный директор ОАО «Центр компьютерных разработок»
Ткач Анатолий Федорович	Заместитель директора Санкт-Петербургского института информатики и автоматизации Российской академии наук
Устинов Игорь Анатольевич	Генеральный директор ФГУП «Научно-производственное объединение «Импульс»
Уткин Виктор Викторович	Директор Центра информационных технологий управления и электронных услуг Санкт-Петербургского государственного университета сервиса и экономики
Федорченко Людмила Николаевна	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Цыулев Сергей Валентинович	Начальник сектора информационно-компьютерной безопасности отдела информационной безопасности, противодействия техническим разведкам и развития системы защиты информации Комитета по информатизации и связи Санкт-Петербурга
Черешкин Дмитрий Семенович	Заведующий лабораторией Института системного анализа Российской академии наук
Эркин Анатолий Григорьевич	Генеральный директор ЗАО «Санкт-Петербургский Региональный Центр защиты информации»

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2011»

Председатель Программного Комитета

Советов Борис Яковлевич

Сопредседатель Научного совета по информатизации
Санкт-Петербурга

Заместители председателя Программного Комитета

Жигаadlo Валентин Эдуардович

Генеральный директор ООО «Максима»

Молдовян Александр Андреевич

Заместитель директора Санкт-Петербургского института
информатики и автоматизации Российской академии наук
по информационной безопасности

Исполнительный директор Конференции

Касаткин Виктор Викторович

Ученый секретарь Научного совета по информатизации
Санкт-Петербурга, декан ФПК Балтийского
государственного технического университета
«ВОЕНМЕХ» им. Д.Ф. Устинова

Ученый секретарь Конференции

Заболотский Вадим Петрович

Руководитель научно-исследовательской группы
Санкт-Петербургского института информатики и
автоматизации Российской академии наук

Информационное обеспечение Конференции

«Компьютер Информ»

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



ПЛЕНАРНЫЕ ДОКЛАДЫ

Александрова О.А.

Россия, Москва, Министерство юстиции Российской Федерации

О ПЕРСПЕКТИВАХ ИСПОЛЬЗОВАНИЯ МОДЕЛЬНЫХ ЗАКОНОДАТЕЛЬНЫХ АКТОВ МПА СНГ В ИНФОРМАЦИОННОЙ СФЕРЕ И ИХ АНТИКОРРУПЦИОННОЙ ЭКСПЕРТИЗЕ

Кто сегодня будет спорить с утверждением, что информация является главным фактором управления современным миром и основным ресурсом и инструментом власти? Справедливы слова: «кто владеет информацией, тот владеет миром». Государство может добиться стратегических преимуществ лишь тогда, когда оно обладает полноценными информационными возможностями. Безопасность нашей страны во многом зависит от эффективного функционирования информационной среды.

В связи с развитием глобального информационного общества вопросы обеспечения доступа к информации и одновременно защита информации от новых вызовов и угроз приобретают особую актуальность.

Сегодня принимается множество концептуальных и стратегических национальных и международных документов, правовых актов, направленных на обеспечение информационной безопасности личности, общества и государства. При этом особую важность приобретают анализ состояния правового регулирования, выявление правовых лакун и разработка предложений по совершенствованию законодательства в рассматриваемой сфере.

В современном обществе все с большей очевидностью проявляется взаимосвязь и взаимозависимость глобализации и роста информационно-коммуникационных технологий во всех сферах его жизни. В настоящее время информационные инновации, наряду с техническими и управленческими, значительно расширяют возможности управления государством, существенно повышают ценность информации как стратегического ресурса, и становятся важной составляющей модернизации экономики государства. Это связано также с формированием в России системных подходов к созданию инфраструктуры электронного правительства и оказания государственных услуг населению, что обуславливает особую актуальность обеспечения информационной безопасности.

Развитие информационных технологий позволяет выстраивать отношения государства и общества на принципиально новом уровне. Информационные технологии дают возможность гражданам не только получать информацию, но и взаимодействовать с государственными структурами, получать государственные услуги в электронном виде.

В настоящее время общество заинтересовано в прозрачности и открытости государственного управления. Широкий доступ к информации о государственных и муниципальных органах, к информации о деятельности судов позволяют обеспечить прозрачность их деятельности, что является важной составляющей для создания механизмов противодействия коррупции.

Динамичное развитие правоотношений в информационной сфере требует соответствующего правового регулирования, обеспечивающего возможность эффективного противодействия коррупционной деятельности в государстве и повышения уровня открытости и прозрачности информации в деятельности государственных органов.

Но процессы глобализации породили целый ряд проблем, решить которые государствам возможно только сообща, что, в свою очередь, требует развития сотрудничества государств, гармонизации их национальных законодательств, в том числе и в сфере информационной безопасности.

Межпарламентская Ассамблея государств-участников СНГ уделяет в своей деятельности огромное внимание вопросам, связанным со сближением и гармонизацией законодательств государств Содружества, которое обеспечивается принимаемыми МПА СНГ модельными законодательными актами и рекомендациями.

Согласно Положению о разработке модельных законодательных актов и рекомендаций МПА СНГ (далее – Положение), принятым МПА СНГ 14 апреля 2005 года и дополненным постановлением МПА СНГ от 25.11.2008 г. №31-21, под модельным законодательным актом Содружества Независимых Государств понимается акт рекомендательного характера, принятый МПА в установленном порядке в целях осуществления согласованной законодательной деятельности государств – членов СНГ по вопросам, представляющим общий интерес, а так же в целях приведения законодательства государств – участников Содружества в соответствие с международными договорами, заключенными в рамках СНГ, и иными многосторонними международными договорами,

участие в которых государств – участников Содружества является весьма желательным для достижения общих целей.

К модельным законодательным актам Содружества, согласно Положению, относятся Модельный кодекс и Модельный закон.

Положением также предусмотрено, что в необходимых случаях модельные законодательные акты могут иметь форму типовых положений, уставов, соглашений.

Схожую природу имеют рекомендации МПА СНГ. Это предложения, принятые МПА в установленном порядке с целью сближения законодательства государств – участников Содружества по вопросам общих интересов, приведения их законодательства в соответствие с положениями международных договоров, заключенными в рамках Содружества, и содействия синхронизации процедур их ратификации.

Необходимо отметить, что за годы существования МПА СНГ принято более 300 модельных законодательных актов, в том числе только в 2010 году – 17.

Модельные законодательные акты, разрабатываемые и принимаемые МПА СНГ, предлагаются национальным законодательным органам в качестве образца, оптимального варианта регулирования соответствующей сферы отношений, на основе которого может быть принят тот или иной правовой акт. При этом, однако, ни одно государство-участник СНГ не связано а priori обязательством использовать эту модель.

Вместе с тем, как показывает практика, модельные акты в информационной сфере активно используются парламентами для совершенствования законодательств государств-участников Содружества.

Принципиальное обстоятельство, которое должно быть учтено при сближении правовых систем государств-участников СНГ на основе модельных актов, состоит в том, что в этом случае осуществляется не унификация, т.е. создание единых правовых норм, которые бы действовали во всех государствах, использующих данные акты, а гармонизация права, – создание сходных (в той или иной степени) норм национального права.

Говоря о перспективах использования модельных законодательных актов в информационной сфере, необходимо отметить, что в МПА СНГ в ближайшее время завершится работа над модельным законом об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов. Но, принимая во внимание все возрастающие масштабы коррупции во всех сферах жизнедеятельности государств и общества, этого явно недостаточно.

Так, учитывая, что модельные законодательные акты МПА СНГ в информационной сфере берутся за основу принятия целого ряда национальных актов, целесообразно подвергать антикоррупционной экспертизе и сами модельные законодательные акты, в том числе и их проекты.

Можно пойти еще дальше, и предусмотреть в Положении о разработке модельных законодательных актов и рекомендаций МПА СНГ вместо правовой экспертизы, – комплексную, включающую в себя правовую, антикоррупционную, лингвистическую, юридико-техническую и др. виды экспертиз, что позволит значительно повысить качество принимаемых актов.

Необходимо так же и развитие системы мониторинга как самих модельных законодательных актов и рекомендаций МПА СНГ, так и практики их реализации, важной составляющей частью которого является антикоррупционный мониторинг.

Подводя предварительный итог, можно сказать, что предлагаемые меры по проведению антикоррупционной экспертизы и мониторинга законодательства и правоприменения особенно актуальны для быстро формирующихся сфер новых отраслей законодательства, к которым относятся и информационное законодательство.

В число принятых МПА СНГ актов, относящихся к этой сфере, входят:

- Рекомендательный законодательный акт «О принципах регулирования информационных отношений в государствах – участниках Межпарламентской Ассамблеи», принятый постановлением МПА СНГ от 23 мая 1993 г.;

- Модельный закон «О международном информационном обмене», принятый постановлением МПА СНГ от 26 марта 2002 г. № 19-7;

- Модельный Уголовный кодекс для государств – участников СНГ, принятый постановлением МПА СНГ от 17 февраля 1996 г., глава 30 которого включает такие преступления против информационной безопасности, как несанкционированный доступ к компьютерной информации (ст. 286), модификация компьютерной информации (ст. 287), компьютерный саботаж (ст. 288), неправомерное завладение компьютерной информацией (ст. 289), изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 290), разработка, использование и распространение вредоносных программ (ст. 291), нарушение правил эксплуатации компьютерной системы или сети (ст. 292);

- Модельный закон «О персональных данных», принятый постановлением МПА СНГ от 16 октября 1999 г. №14-19;

– Модельный закон «О трансграничном спутниковом телевизионном и радиовещании и международном спутниковом информационном обмене», принятый постановлением МПА СНГ от 15 июня 1998 г. №11-11;

– Модельный закон о праве на доступ к информации, принятый постановлением МПА СНГ от 17 апреля 2004 г. №23-14, и ряд других актов.

Анализ указанных актов выявил принципиальные недостатки: противоречивость, декларативность, наличие «белых пятен», неточность понятийного аппарата, широту дискреционных полномочий (отсутствие или неопределенность сроков, условий или оснований принятия решения, наличие дублирующих полномочий), выборочное изменение объема прав, юридико-лингвистическую неопределенность (употребление неустоявшихся, двусмысленных терминов и категорий оценочного характера) и т.д., а ведь модельные законодательные акты предлагаются за основу странам-участницам Содружества.

Это подтверждает необходимость проведения системной правовой и антикоррупционной экспертиз указанных актов и мониторинга практики их применения.

В настоящее время в МПА СНГ активно идет работа по разработке Рекомендаций МПА СНГ по совершенствованию и гармонизации национальных законодательств государств – участников СНГ в сфере обеспечения информационной безопасности.

На наш взгляд, указанные рекомендации должны не только базироваться на многочисленных международных актах, а также актах Российской Федерации и других государств-участников СНГ в области информационных отношений, но и обязательно учитывать анализ результатов антикоррупционных экспертиз уже принятых модельных законодательных актов и рекомендаций в информационной сфере, в том числе по результатам антикоррупционного мониторинга законодательства и правоприменения.

Почти 20-летний опыт работы Межпарламентской Ассамблеи государств – участников СНГ подтвердил востребованность и эффективность модельного правотворчества. Для участия в разработке проектов актов МПА СНГ приглашает наиболее квалифицированных специалистов, использует новейшие научные достижения и в результате можно сказать, что разрабатываемые МПА СНГ модельные акты работают на перспективу, отражая право завтрашнего дня.

Полагаем, что внедрение практики антикоррупционной экспертизы модельных законодательных актов и рекомендаций МПА СНГ в информационной сфере, а также мониторинга их применения, сделает их еще более совершенными и полезными для законотворческой деятельности государств – участников СНГ.

Жигадло В.Э., Терещенко П.Г., Рубинштейн Д.В.

Россия, Санкт-Петербург, ООО «Максима», ФГБУ «Президентская библиотеки имени Б.Н. Ельцина»,

Москва, ФГУП «ГлавНИВЦ» Управления делами Президента Российской Федерации

ПРОБЛЕМЫ СОЗДАНИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА ПРИМЕРЕ «ПРЕЗИДЕНТСКОЙ БИБЛИОТЕКИ ИМЕНИ Б.Н. ЕЛЬЦИНА».

ОРГАНИЗАЦИЯ УДАЛЕННОГО ДОСТУПА В ЧИТАЛЬНЫЙ ЗАЛ ЭЛЕКТРОННОЙ БИБЛИОТЕКИ

Вопросы удаленного доступа к корпоративным ресурсам через публичные сети в последнее время приобретают все большую популярность. Ключевым вопросом при этом, требующим своего решения, становится вопрос обеспечения безопасного удаленного доступа через публичные сети к непубличным корпоративным ресурсам.

Наглядным примером решения данной проблемы является организация удаленного доступа в читальный зал электронной библиотеки ФГБУ «Президентская библиотеки имени Б.Н. Ельцина».

Архитектура системы защиты информационной системы Президентской библиотеки (ИСПБ) функционально состоит из следующих компонент:

1. Аппаратно-программные комплексы обеспечения информационной безопасности информационных ресурсов ПБ в составе:

– Подсистемы межсетевого экранирования на основе:

- специализированных многофункциональных устройств Cisco Adaptive Security Appliance;
- модулей межсетевого экранирования FWSM для установки в шасси коммутаторов Cisco Catalyst 6500.

– Подсистемы криптографической защиты информационных потоков на основе:

- специализированного программного обеспечения Inter-PRO Server и Inter-PRO Client;
- АПКШ «Континент»;
- ПО удаленного защищенного доступа «Континент-АП».

– Подсистемы обнаружения и предотвращения атак на основе специализированных устройств Cisco IPS 4260;

– Подсистемы антивирусной защиты на основе ПО «Dr.Web Enterprise Suite»;

– Подсистемы защиты от НСД

- Подсистемы мониторинга и управления на основе:
 - программного обеспечения Positive Technologies X-Spider;
 - программного комплекса Cisco Security Manager;
 - программно-аппаратного комплекса Cisco MARS.

2. Аппаратно-программные средства обеспечения санкционированного удаленного доступа в электронный читальный зал ПБ на основе электронной цифровой подписи (ЭЦП).

Доступ к информационным ресурсам ПБ осуществляется через Интернет-портал и через внутренний интерфейс Электронного читального зала ПБ.

Интернет-портал является ключевой подсистемой Президентской библиотеки и предназначен для организации универсального доступа к информационным ресурсам Президентской библиотеки и предоставления единого инструментария доступа к сервисам системы. Он обеспечивает доступ к санкционированным, в рамках публичного доступа, ресурсам библиотеки в следующих режимах:

- публичный доступ,
- служебный доступ,
- межбиблиотечный доступ к электронному каталогу Президентской библиотеки из внешних библиотечных систем.

Система электронного читального зала предназначена для сервисного, оперативного и более полного удовлетворения запросов читателей через предоставление доступа ко всему объему информационных ресурсов Президентской библиотеки и осуществления информационно-библиографического обслуживания в следующих режимах:

- навигация и поиск,
- просмотр контента,
- регистрация и аутентификация,
- управление правами доступа,
- администрирование.

Структура доступа читателей к защищенным фондам ПБ приведена на рисунке 1.

Алгоритм организации работы системы удаленного доступа и подключения удаленных пользователей к электронному читальному залу ПБ показан на рисунке 2 и состоит из следующих шагов:

1. По заявке удаленного пользователя Удостоверяющий центр выпускает персональный сертификат удаленного пользователя.

2. Сертификат записывается на электронный ключ RuToken, который отправляется пользователю по почте.

3. Удаленный пользователь подключает электронный ключ к компьютеру (требуется установка драйвера RuToken, который свободно загружается с сайта ПБ).

4. Удаленный пользователь запускает программу терминального доступа (входит в поставку большинства современных клиентских операционных систем) и соединяется с терминальным сервером.

5. В процессе авторизации удаленный пользователь вводит ПИН-код электронного ключа RuToken.

6. Происходит сложная процедура двусторонней аутентификации между терминальным клиентом и сервером терминалов, основанная на сертификате пользователя. В результате сервер терминалов однозначно авторизует пользователя – владельца сертификата.

7. На терминальном сервере для данного конкретного пользователя создается виртуальный рабочий стол, на который загружается программа читального зала, работающая в режиме «киоска» (урезанный режим в целях обеспечения безопасности функционирования).

8. Программа загружает данные из Президентской библиотеки имени Б.Н. Ельцина по защищенному каналу передачи данных (технология VPN).

9. Виртуальный рабочий стол и приложение транслируются в программу терминального доступа и становятся доступны удаленному пользователю.

10. Программа терминального доступа транслирует управляющую информацию от удаленного пользователя в приложение читального зала Президентской библиотеки имени Б.Н. Ельцина.

После подтверждения подлинности посредством ЭЦП пользователь получает доступ к электронной библиотеке и ему предоставляется следующий набор услуг:

- подключение пользователя и организация его доступа к ресурсам основного хранилища ПБ;
- удаленный просмотр файлов цифрового контента ПБ с аутентификацией читателя с помощью его ЭЦП;
- предоставление по заказу читателя файлов цифрового контента ПБ подписанных ЭЦП ПБ на внешних носителях;
- предоставление по заказу читателя файлов цифрового контента ПБ подписанных ЭЦП ПБ по сети Интернет.

При этом каждая из услуг реализуется посредством определенного набора шагов.

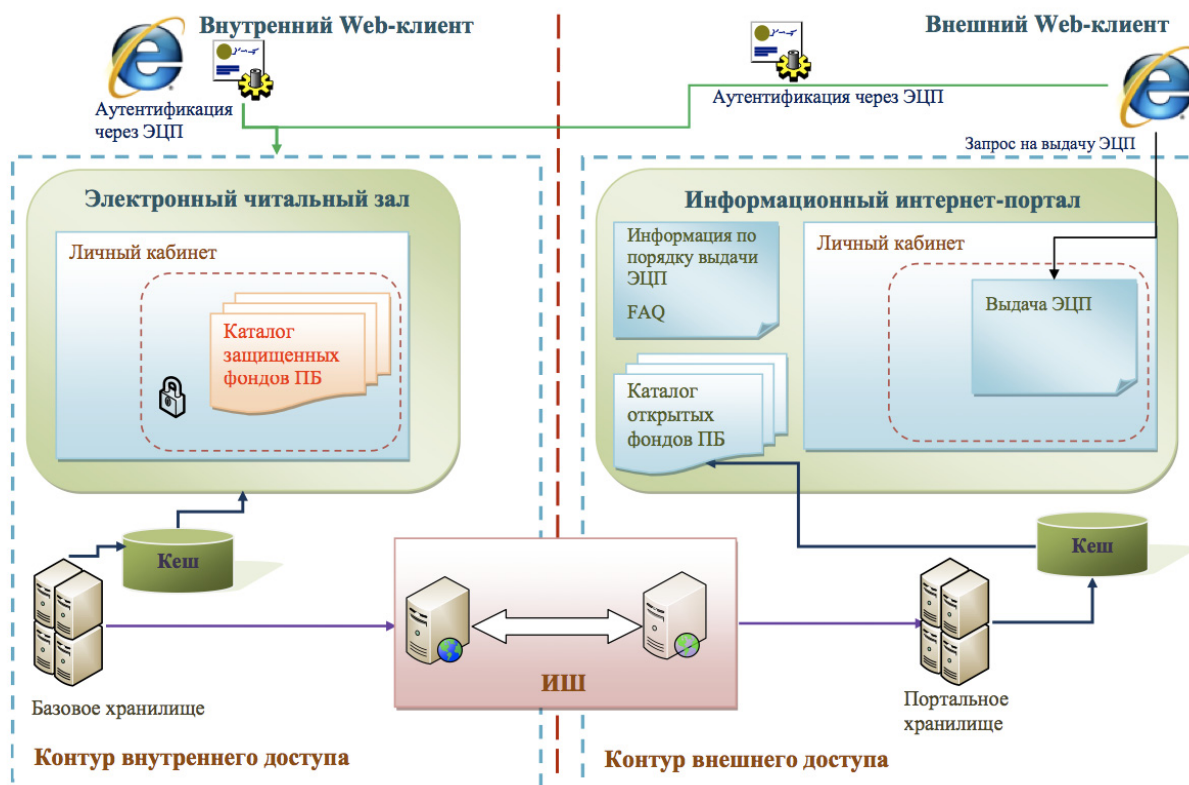


Рис. 1. Доступ читателей к защищенным фондам ПБ



Рис. 2. Алгоритм удаленного доступа

Процесс подключения пользователя включает:

- получение инструкции на Интернет портале ПБ по оказываемой услуге;
- формирование заявки читателем на оказание услуги;
- выполнение заявки читателя, подключение читателя к услуге и выдача читателю клиентского сертификата на носителе ru-Token.

Процесс просмотра цифрового контента включает:

- аутентификацию читателя по ЭЦП, определение прав читателя;
- создание запроса читателем на просмотр единиц хранения цифрового контента ПБ (запрос должен быть подписан ЭЦП);
- публикацию/адаптацию файлов единиц хранения;
- уведомление читателя о выполнении заказа;
- просмотр читателем цифрового контента.

Процесс загрузки цифрового контента включает:

- аутентификацию читателя по ЭЦП;
- создание запроса читателем на загрузку единиц хранения цифрового контента ПБ (запрос должен быть подписан ЭЦП);
- публикацию/адаптацию файлов единиц хранения (файлы должны иметь ЭПЦ ПБ);
- уведомление читателя о выполнении заказа;
- загрузку читателем файлов цифрового контента (пользователь ПБ должен подтвердить получение контента с помощью ЭЦП).

Процесс предоставления цифрового контента на внешних носителях включает:

- аутентификацию читателя по ЭЦП;
- создание запроса читателем на предоставление единиц хранения цифрового контента ПБ (запрос должен быть подписан ЭЦП);
- адаптацию файлов единиц хранения (файлы должны иметь ЭПЦ ПБ), оформление и доставка заказа;
- уведомление читателя о выполнении заказа;
- получение читателем заказа (пользователь ПБ должен подтвердить получение контента с помощью ЭЦП, либо обычной подписи).

Важной процедурой организации удаленного доступа является процедура изготовления ЭЦП, которая должна быть максимально простой и удобной в использовании конечным пользователем. Алгоритм изготовления ЭЦП для читателей ПБ представлен на рисунке 3.

Изготовление сертификата производится по распределенной схеме, не требующей приезда читателей в Удостоверяющий центр и состоит из следующих шагов.

1. Формирование запроса

Читатель пишет по электронной почте письмо в региональный филиал Президентской библиотеки им. Б.Н. Ельцина с запросом на приобретение сертификата ЭЦП и указанием своих реквизитов. При необходимости, читателем дополнительно заказывается лицензия на программное обеспечение «КриптоПро CSP» и ключевой носитель (eToken или Rutoken).

2. Выставление счета

В ответ на полученный запрос читателю высылается счет на оплату сертификата (включая стоимость лицензии и ключевого носителя, если они были заказаны).

А). Счет читателю выставляется Удостоверяющим Центром.

Б). Счет читателю выставляется региональным представительством Президентской библиотеки им. Б.Н. Ельцина, который выступает в роли агента между читателем и Удостоверяющим Центром.

В). Затраты на изготовление сертификата оплачиваются сторонней стороной.

3. Подготовительные работы

С сайта Удостоверяющего центра читателем скачивается и устанавливается программное обеспечение «КриптоПро CSP» и сертификаты удостоверяющего центра.

4. Запрос на регистрацию

Читатель обращается к Web-сайту Удостоверяющего центра, выбирает ссылку «Начать регистрацию» и создает запрос на регистрацию, заполняя предлагаемую форму. В процессе первичной регистрации формируется маркер временного доступа, включающий ID маркера и пароль. Маркер временного доступа необходимо сохранить для продолжения процедуры регистрации.

5. Оформление заявлений

С Web-сайта Удостоверяющего центра читателем скачиваются шаблоны «Заявления о присоединении к Регламенту Удостоверяющего центра» и «Заявления на регистрацию Пользователя в Удостоверяющем центре». Заполненные заявления с подписью читателя отправляются в региональное представительство Президентской библиотеки им. Б.Н. Ельцина (по электронной почте в отсканированном виде).

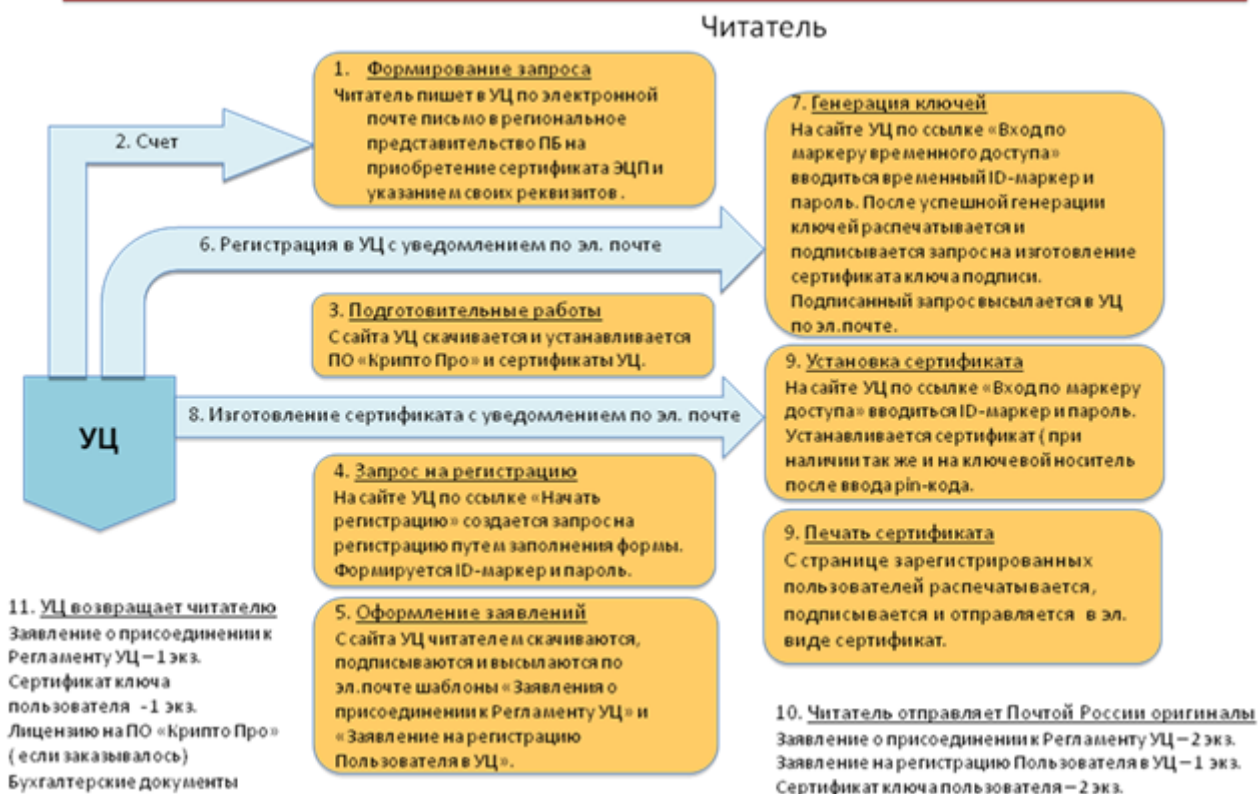


Рис. 3. Алгоритм изготовления ЭЦП для читателей ПБ

Таким образом, реализованные механизмы и аппаратно-программные средства удаленного доступа в электронный читальный зал ПБ на основе электронной цифровой подписи (ЭЦП) обеспечивают санкционирование доступа читателей к ресурсам ПБ через публичные сети с минимальными затратами на реализацию самой процедуры доступа.

Жигadlo В.Э., Терещенко П.Г., Рубинштейн Д.В.
Россия, Санкт-Петербург, ООО «Максима», ФГБУ «Президентская библиотеки имени Б.Н. Ельцина»,
Москва, ФГУП «ГлавНИВЦ» Управления делами Президента Российской Федерации
ЗАЩИЩЕННАЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА
«ПРЕЗИДЕНТСКОЙ БИБЛИОТЕКИ ИМЕНИ Б.Н. ЕЛЬЦИНА»

Информационно-телекоммуникационная система (ИТКС) Президентской библиотеки (ПБ) – это комплекс взаимосвязанных подсистем, взаимодополняющих и взаимно-обеспечивающих работу друг друга. Базовая архитектура комплекса библиотечных центров включает следующие библиотечные центры:

Основной библиотечный центр, который размещен в здании Синода, расположенном по адресу: Санкт Петербург, Площадь Декабристов, д.2;

Пилотная зона Президентской библиотеки, которая размещается в Российском Государственном Историческом Архиве (РГИА) по адресу: Санкт-Петербург, Заневский пр.,36;

Резервный библиотечный центр в Москве.

В Основном библиотечном центре решается весь комплекс задач по управлению деятельностью Президентской библиотеки, формированию и поддержке библиотечных фондов и электронного мультимедиа контента, обслуживанию читателей и посетителей Президентской библиотеки на территории библиотеки, предоставлению доступа потребителям информации к документам и электронному контенту через библиотечную сеть и Интернет. Пилотная зона Президентской библиотеки (Служебный библиотечный центр) предназначена для апробации основных технологических решений по автоматизации деятельности Президентской библиотеки на период подготовки и ввода в действие Основного библиотечного центра. Резервный библиотечный центр Президентской библиотеки рассматривается в первую очередь как хранилище страховой копии электронного фонда, формируемого в Основном библиотечном центре. В экстренных ситуациях (сбои, аварии и т.п.) резервный библиотечный центр должен взять на себя все основные функции по поддержанию электронного фонда Президентской библиотеки и обслуживанию потребителей информации, включая обеспечение удаленного доступа к информационным ресурсам и электронному

контенту. Помимо Основного, Резервного библиотечного центра и Пилотной зоны в системе ЭБП функционируют Региональные библиотечные центры.

Для реализации полнофункциональной системы защиты информации компоненты Информационной Системы Президентской библиотеки (ИСПБ) разделяются на функциональные модули и логические сегменты. Каждый из модулей реализует только установленную функциональность в рамках ИСПБ. Разделение на логические сегменты реализуется в соответствии с функциональностью сегментов и дает возможность контроля информационных потоков между сегментами. Архитектура системы защиты ИСПБ функционально состоит из следующих подсистем:

- подсистемы межсетевого экранирования на основе специализированных многофункциональных устройств Cisco Adaptive Security Appliance и модулей межсетевого экранирования FWSM для установки в шасси коммутаторов Cisco Catalyst 6500;

- подсистемы криптографической защиты информационных потоков на основе специализированного программного обеспечения (ПО) Inter-PRO Server и Inter-PRO Client, АПКШ «Континент» и ПО удаленного защищенного доступа «Континент-АП»;

- подсистемы обнаружения и предотвращения атак на основе специализированных устройств Cisco IPS 4260;

- подсистемы антивирусной защиты на основе ПО «Dr.Web Enterprise Suite»;

- подсистема защиты от несанкционированного доступа (НСД);

- подсистемы мониторинга и управления на основе программного обеспечения Positive Technologies X-Spider, программного комплекса Cisco Security Manager и программно-аппаратного комплекса Cisco MARS.

Согласно требованиям нормативных документов при построении системы защиты информации (СЗИ) ПБ были использованы только сертифицированные программно-технические средства, в том числе средства защиты информации, обеспечивающие ее целостность, доступность и криптографическую защищенность.

Логическая схема размещения перечисленных выше компонентов СЗИ представлена на рисунке 1.

Как показано на схеме (рисунок 1), ИСПБ разделяется на 2 основных логических сегмента сетей: сегмент внешних сетей и сегмент внутренних сетей. К внешним сетям относятся сегмент Внешних подключений и сегмент Портал. К внутренним сетям относятся Прикладные сегменты, Сегменты подключения пользователей, сегмент ЦОД и сегмент управления.

Сегмент внешних подключений реализует физическое и логическое подключения ИСПБ к сети Интернет, к выделенным частным сетям (ВЧС) «Технологическая» и «Президентская библиотека», созданным в целях обеспечения взаимодействия библиотечных центров, а также обеспечивает беспроводной доступ пользователей ПБ к ресурсам библиотеки. Межсетевые экраны этого сегмента контролируют потоки информации между подключенными сегментами сетей и реализованы в отказоустойчивой конфигурации.

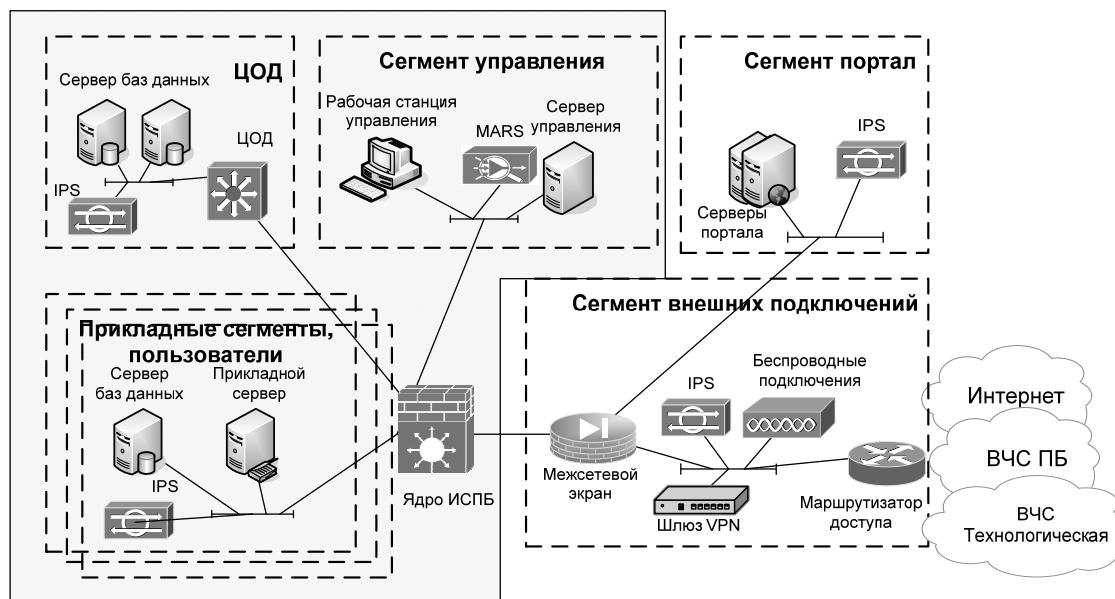


Рис. 1. Логическая схема построения системы защиты информации ИСПБ

Прикладные сегменты, а также сегмент ЦОД включают в себя прикладные серверы ИСПБ, разделенные по функциональному признаку.

Сегменты пользователей включают в себя сегменты подключения пользователей на уровне доступа к сети, объединяющие АРМ сотрудников ПБ, АРМ, устанавливаемые в читальном зале ПБ и другие АРМ, объединенные по логическому признаку.

В сегменте управления находятся: сетевые устройства и серверы, с помощью которых осуществляется мониторинг состояния ИСПБ и управление ее ресурсами и компонентами, рабочие станции сетевых и системных администраторов, рабочие станции администраторов информационной безопасности.

Логически и физически устройства каждого сегмента объединяются с помощью коммутаторов Cisco Catalyst. Помимо физической коммутации каналов, коммутаторы разделяют сегмент на логические сети с использованием технологии VLAN. Фильтрацию сетевого трафика, направленного к устройствам, серверам сегмента осуществляют межсетевые экраны коммутаторов ядра.

Подсистема межсетевого экранирования

Подсистема межсетевого экранирования ИСПБ предназначена для физического и логического сегментирования ИСПБ, реализации правил контроля доступа к ресурсам и сетевым узлам ИСПБ, их защиты от атак на сетевом и прикладном уровнях.

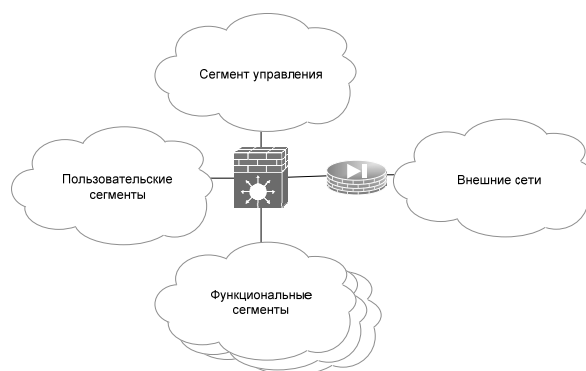


Рис. 2. Логическая схема построения подсистемы межсетевого экранирования

Подсистема межсетевого экранирования ИСПБ состоит из следующих компонент:

- специализированные многофункциональные устройства Cisco Adaptive Security Appliance – обеспечивающие межсетевое экранирование и фильтрацию сетевого трафика между сегментами сетей ИСПБ, и разделение сетей на физические и логические сегменты;

- модули межсетевого экранирования Cisco FWSM – устанавливаемые в шасси коммутаторов Cisco Catalyst 6500 и обеспечивающие межсетевое экранирование и фильтрацию сетевого трафика между сегментами сетей ИСПБ, и разделение сетей на физические и логические сегменты.

На подсистему межсетевого экранирования и фильтрации сетевого трафика возлагается выполнение следующих функций:

- разделение существующих сегментов физических сетей между собой и на логические сегменты в соответствии с их функциональностью;
- защита существующих ресурсов ИСПБ от сетевых атак с использованием фильтрации сетевого трафика;
- ограничение доступа к ресурсам ИСПБ с использованием межсетевого экранирования;
- реализация возможности «горячего» резервирования функций работы подсистемы («горячее» резервирование, cluster).

В подсистеме межсетевого экранирования реализуются возможности многоуровневой проверки информационных потоков.

Подсистема криптографической защиты информационных потоков

Подсистема криптографической защиты информационных потоков СЗИ ИСПБ предназначена для обеспечения контроля целостности и конфиденциальности данных системы при передаче информации через внешние сети передачи данных.

С точки зрения криптографической защиты всех субъектов, взаимодействующих с ресурсами ИСПБ можно разделить на три группы:

- внешние пользователи системы (Интернет-пользователи);
- пользователи ИСПБ (Администраторы, сотрудники);
- репликация БД (ВЧС «Технологическая»).

Взаимодействие каждой из перечисленных групп пользователей описывается различными регламентами, что приводит к возникновению различных требований к криптографической защите информации для каждой из групп.

Схема взаимодействия компонентов подсистемы криптографической защиты приведена на рисунке 3.

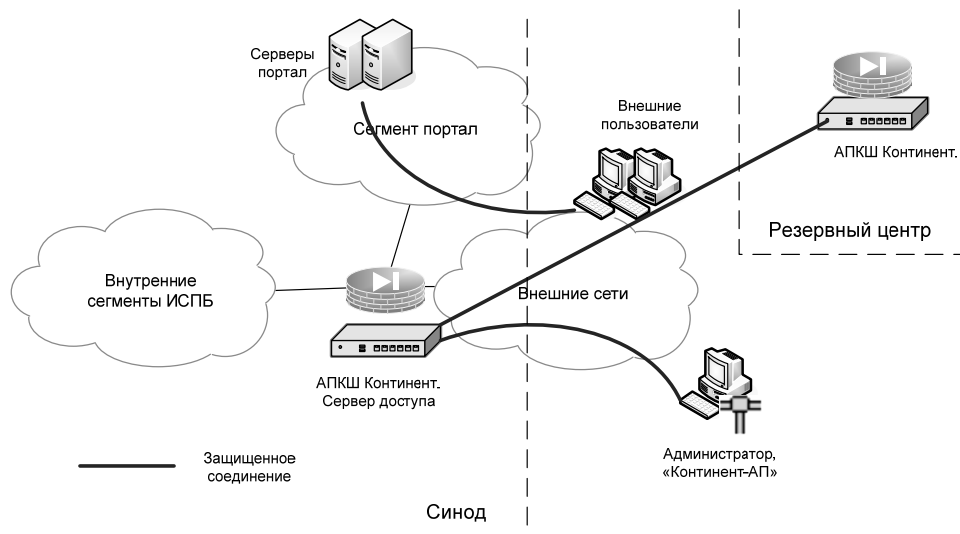


Рис. 3. Схема организации защищенных соединений

Внешние пользователи получают доступ к общедоступным ресурсам ИСПБ с использованием протокола HTTP. Потенциально в эту группу входят все пользователи глобальной информационной сети Интернет. Большая часть взаимодействий данной группы пользователей не требует применения криптографических средств защиты информации. В ситуациях, когда защита необходима, применяется протокол SSL/TLS (для доступа к ресурсам используется протокол HTTPS).

Обеспечение безопасности коммуникаций пользователей, производящих операции с ИСПБ регламентируются законами Российской Федерации, требующими использования сертифицированных средств защиты. Сетевые взаимодействия данной группы пользователей защищаются с использованием сертифицированного решения, реализующего SSL/TLS с поддержкой ГОСТ Р 34.10-2001, ГОСТ Р 34.10-94, ГОСТ Р 34.11-94, ГОСТ 28147-89.

При необходимости использования защищенного протокола HTTPS, программное обеспечение Сервера криптографической защиты на основе Inter-PRO Server и клиентское ПО Inter-PRO Client используются для построения защищенного канала связи между пользователями и приложениями ИСПБ. Указанное ПО реализует криптографические алгоритмы ГОСТ Р 34.10-2001, ГОСТ Р 34.10-94, ГОСТ Р 34.11-94, ГОСТ 28147-89. Программный комплекс Inter-Pro имеет сертификаты ФАПСИ СФ/114-0604, СФ/124-0605 от 21.04.2003 г. Таким образом, информационные потоки между пользователями и приложениями ИСПБ защищаются с использованием сертифицированных средств криптографической защиты.

Репликации БД между основным и резервным центрами ПБ осуществляется через ВЧС «ПБ Технологическая». Для обеспечения контроля целостности данных используется АПКШ «Континент». Основным назначением комплекса «Континент» является защита информации, передаваемой по каналам связи ВЧС, а также защита сегментов ВЧС от проникновения извне. Комплекс «Континент» обеспечивает: шифрование и имитозащиту данных, передаваемых по открытым каналам связи между защищенными сегментами сети, защиту внутренних сегментов сети от несанкционированного доступа извне, скрытие внутренней структуры защищаемых сегментов сети, централизованное управление защитой сети.

Комплекс «Континент» включает в свой состав следующие компоненты:

- криптографический шлюз «Континент»;
- центр управления сетью криптографических шлюзов;
- программа управления сетью криптографических шлюзов;
- агент управления сетью криптографических шлюзов.

Для осуществления безопасного удаленного доступа Администраторов и сотрудников ИСПБ через сеть Интернет используется ПО «Континент-АП».

В состав данного решения входят следующие компоненты:

- сервер доступа;
- программа управления сервером доступа;
- абонентский пункт;

Сервер доступа (СД) представляет собой специализированное ПО, входящее в состав криптошлюза (КШ), и используется для организации доступа удаленных пользователей к ресурсам защищаемых сетей. СД устанавливается на КШ, защищающий сегмент сети, к которому необходимо

организовать удаленный доступ. После запроса на соединение сервер доступа проводит идентификацию и аутентификацию удаленного пользователя. СД позволяет осуществить практически неограниченное количество одновременных сеансов связи с удаленными пользователями. Аутентификация пользователя при подключении к серверу доступа осуществляется с помощью открытых ключей. Схема реализована с применением сертификатов X.509. Управление сертификатами осуществляется при помощи встроенных средств программы управления сервером доступа. В качестве внешнего центра сертификации может быть использована инфраструктура открытых ключей на основе компоненты Microsoft Certification Authority со встроенным сертифицированным СКЗИ «КриптоПро CSP».

СКЗИ «Континент-АП» (абонентский пункт – АП) является специальным программным обеспечением, которое устанавливается на рабочих местах удаленных пользователей для организации их доступа к ресурсам защищаемой сети.

СКЗИ «Континент-АП» обеспечивает: установление защищенного соединения и обмен данными с СД, обоюдную аутентификацию с СД при установке защищенного соединения посредством технологии сертификатов открытых ключей, защищенное соединение с КШ, возможность фильтрации IP-пакетов во время установленного защищенного соединения с СД, необходимый функционал для работы с сертификатами открытых ключей по средством СКЗИ «КриптоПро CSP», поддержку криптопровайдера «КриптоПро CSP» версии 3.0, протоколирование подключений к СД в журнале соединений, возможность кэширования ключей, отображение и управление записями журнала соединений. СКЗИ «Континент-АП» работает под управлением ОС семейства MS Windows.

Подсистема обнаружения и предотвращения атак

Подсистема обнаружения и предотвращения атак ИСПБ предназначена для обеспечения обнаружения и предотвращения различного рода нарушений установленных политик информационной безопасности (ИБ) на уровне системных и прикладных приложений и в сетевом трафике ИСПБ. Компоненты подсистемы располагаются на ключевых точках контроля трафика во всех ключевых сегментах ИСПБ.

Подсистема обнаружения и предотвращения атак СИБ состоит из аппаратных комплексов Cisco IPS 4260, которые обеспечивают обнаружение и предотвращение атак на сетевом и прикладном уровнях и осуществляют как сигнатурный, так и поведенческий анализ воздействий.

На подсистему обнаружения и предотвращения атак возлагается выполнение следующих функций:

- осуществление мониторинга сетевого трафика ИСПБ с целью обнаружения признаков атак;
- предотвращение атак, направленных на ресурсы ИСПБ;
- проверки информационных потоков.

Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для защиты информации, хранимой и обрабатываемой на серверах и рабочих станциях, от вирусов и вредоносных программ (adware, spyware). Компоненты подсистема антивирусной защиты располагаются серверах и рабочих станциях.

Подсистема антивирусной защиты строится на базе ПО «Dr.Web Enterprise Suite» и включает в себя следующие компоненты:

- главный сервер антивирусной защиты Dr.Web, предназначенный для получения обновлений с серверов всемирной сети обновлений (BCO) Dr.Web, передачи обновлений на подчиненные серверы антивирусной защиты и получения от них информации об антивирусных событиях;
- подчиненные серверы антивирусной защиты Dr.Web, предназначенные для получения обновлений с главного сервера Dr.Web и передачи на него информации об антивирусных событиях на контролируемых ими рабочих станциях и серверах;
- APM администратора безопасности СЗИ, предназначенное для централизованного управления подсистемой антивирусной защиты с использованием консоли;
- защищаемые рабочие станции пользователей, объединенные в единую антивирусную сеть.

Компоненты подсистемы антивирусной защиты взаимодействуют между собой по сети по протоколу TCP/IP с использованием шифрования.

Логическая схема построения подсистемы антивирусной защиты показана на рисунке 4.

Подсистема мониторинга и управления

Подсистема управления и мониторинга ИСПБ предназначена для обеспечения следующих функций:

- защищенное управление компонентами ИБ и сетевым оборудованием ИСПБ;
- мониторинг состояния компонентов СЗИ ИСПБ;
- проверка защищенности сетевой инфраструктуры;
- анализ компонентов ИСПБ и настроек используемых сетевых сервисов, операционных систем и СУБД для выявления уязвимостей на программном уровне.

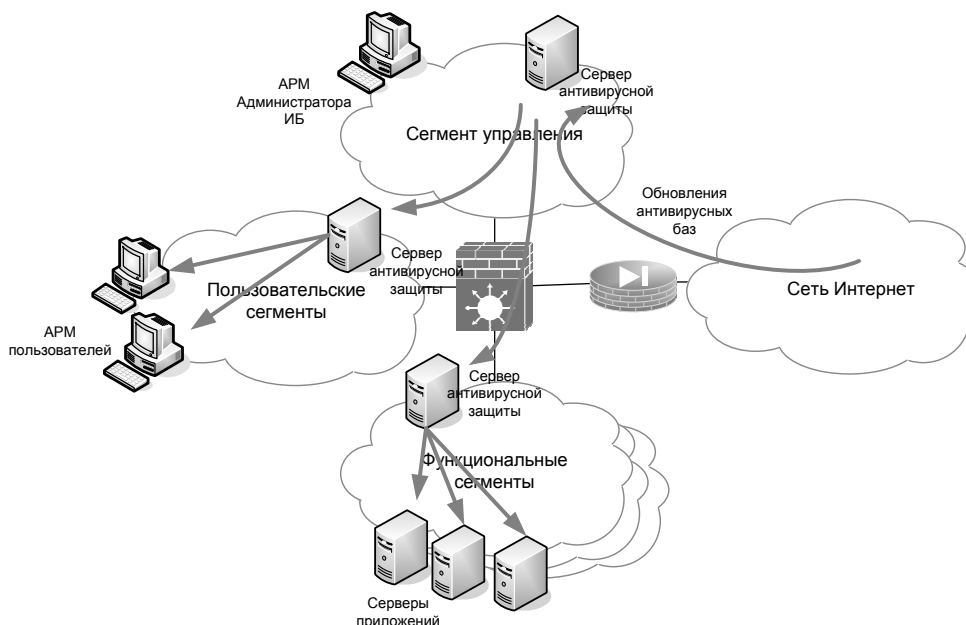


Рис. 4. Логическая схема построения подсистемы антивирусной защиты

Средства анализа защищенности обеспечивают периодическое сканирование узлов и сетевых ресурсов (служб) с целью поиска уязвимостей. Кроме того, сетевые средства анализа защищенности могут быть использованы для проведения периодической инвентаризации сетевых ресурсов.

Логическая схема построения подсистемы централизованного управления и мониторинга показана на рисунке 5.

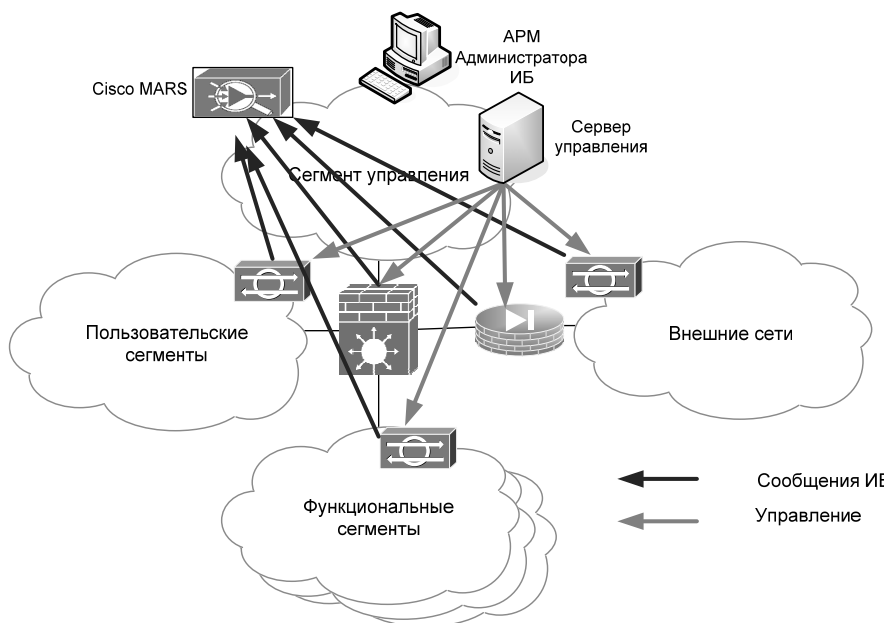


Рис. 5. Логическая схема построения подсистемы централизованного управления и мониторинга

Система централизованного управления Cisco Security Manager выполняет следующие функции:

- управление многофункциональными устройствами Cisco Adaptive Security Appliance, управление модулями Cisco IPS 4260;
- управление модулями межсетевого экранирования Cisco FWSM;
- создание, модификацию и применение политик обнаружения и предотвращения атак.

Программно-аппаратный комплекс Cisco MARS позволяет анализировать и коррелировать события безопасности получаемые из различных источников, таких как маршрутизаторы, коммутаторы, средства обнаружения вторжения, логи операционной системы и др.

Молдовян А.А., Молдовян Н.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ФУНКЦИОНАЛЬНОСТЬ, СТОЙКОСТЬ И БЕЗОПАСНОСТЬ КРИПТОГРАФИЧЕСКИХ МЕХАНИЗМОВ**

Введение

Криптографические механизмы играют важную роль в практике информационной безопасности, причем в электронных технологиях управления и обработки документов, связанных с сообщениями, имеющими юридическую значимость, также для решения задачи анонимности пользователей (технологии тайного электронного голосования и электронных денег) их роль уникальна. Многочисленные задачи, связанные с аутентификацией сообщения и его источника решаются с помощью протоколов электронной цифровой подписи (ЭЦП) различного типа, отличающихся по своей функциональности. Наиболее широко известны протоколы обычной индивидуальной подписи, групповой подписи, коллективной подписи, слепой ЭЦП и др. Схемы ЭЦП относятся к криптосистемам с открытым ключом, которые основаны на трудности некоторых вычислительных задач, которые в настоящее время считаются хорошо изученными, и предположении, что в обозримом будущем не будут найдены прорывные алгоритмы их решения. Сложность лучшего алгоритма взлома криптосистемы принимается за стойкость последней. Достаточно высокая стойкость является обязательным свойством криптосистем, применяемых на практике. При условии наличия такого свойства в различных приложениях становятся важными технологические свойства алгоритмов и протоколов, таких как требуемая функциональность, простота аппаратной реализации, производительность, размер параметров криптосистемы, например размер цифровой подписи, удостоверяющей подлинность электронного документа. Несмотря на широкое применение криптосистем с открытым ключом вопросы оценки стойкости, расширения функциональности и требуемых размеров параметров криптографических механизмов и получения требуемых технологических остается важной практической задачей. Это стимулирует поиск новых решений по разработке алгоритмов и протоколов известных типов, ориентированных на эффективную реализацию в конкретных технологических условиях. Разнообразие практических задач информационной безопасности, имеющих конкретную технологическую направленность, создают широкое поле для перспективных технических разработок прикладной криптографии. Другое перспективное направление развития криптографии связано с поиском новых трудных задач, которые могли бы быть положены в основу криптосистем с открытым ключом. Последнее направление существенно стимулируется ожиданием появления квантового компьютера. В квантовой модели вычислений наиболее широко используемые в криптографии трудные задачи – факторизации и дискретного логарифмирования в конечной коммутативной группе – могут быть решены за полиномиальное. Несмотря на то, что в последнее время высказываются сомнения в реалистичности проекта создания квантового вычислителя, в криптографической литературе достаточно много внимания уделено проблеме разработки примитивов «постквантовой» криптографии. Осуществляется поиск новых вычислительно трудных задач, которые имеют экспоненциальную (или хотя бы сверхполиномиальную сложность) и могут быть использованы для построения двухключевых криптосистем.

В настоящем сообщении рассматривается толкование понятий «безопасность криптосхемы» и «нулевое разглашение секрета» и связанная с этим разработка новых криптографических алгоритмов и протоколов. Также рассматривается построение криптографических протоколов с расширенной функциональностью.

1. Безопасность криптографических алгоритмов

Понятие стойкости характеризует важнейшее свойство криптографических схем выдерживать всевозможные атаки. Под стойкостью понимается трудоемкость лучшего известного алгоритма взлома криптосхемы. Однако вопрос о том, что в настоящее время известен лучший алгоритм решения базовой трудной задачи, остается открытым, несмотря на то, что как правило в качестве базовых трудных задач при построении криптосхем используются давно известные и хорошо изученные задачи. Основной проблемой оценки стойкости криптосхем является то, что трудно доказать, что в ближайшем будущем не будут найдены более эффективные алгоритмы взлома, чем лучший из известных в настоящее время алгоритмов взлома данной криптосистемы. Таким образом, стойкость отражает 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.

В основе наиболее известных и апробированных криптосхем лежат следующие две вычислительные проблемы: 1) задача факторизации (ЗФ) составного числа специального вида и 2) задача дискретного логарифмирования (ЗДЛ) в конечной алгебраической структуре (конечных простых или расширенных полях, конечных группах различного типа). Задача нахождения корней e – й степени ($e > 2$), возникающая в криптосистеме RSA, и задача извлечения квадратного корня, возникающая в криптосистеме Рабина, являются зависимыми от ЗФ, т. е. решение ЗФ легко приводит

к решению указанных задач извлечения корней по модулю. Сформулированная в общем виде ЗДЛ может быть разделена на частные типы, определяемые конкретной конечной алгебраической структурой, над которой задается ЗДЛ. Можно выделить такие варианты ЗДЛ: 1) ЗДЛ в простом конечном поле; 2) ЗДЛ в расширенном конечном поле; 3) ЗДЛ на эллиптической кривой, 4) ЗДЛ в конечных некоммутативных группах матриц, 5) ЗДЛ по многомерному основанию в нециклических группах и др. По принятым в настоящее время оценкам ЗДЛ в вариантах 1, 2 и 4 имеет субэкспоненциальную сложность и только в специальных случаях варианта 3 сложность ЗДЛ является экспоненциальной. При разработке криптосхемы выбираются размеры ее параметров такие, чтобы обеспечить требуемый уровень стойкости. В последнем случае считается, что криптосхема безопасна и допускается ее практическое использование. При этом в понятии безопасности криптосхем неявно включено ожидание того, что вероятность появления в обозримом будущем прорывных решений рассматриваемых вариантов ЗДЛ является пренебрежимо малой (например, создание практически действующего квантового компьютера означает появление прорывного решения сразу для двух трудных задач: ЗДЛ в циклической конечной группе и ЗФ). Количественная оценка порядка этой вероятности является весьма условной и трудно обосновываемой, но факт применения криптосхем основанных на ЗДЛ говорит о том, что общепринятым является предположение о достаточно малом значении такой вероятности. Появление прорывного алгоритма решения трудной задачи, положенной в основу криптосхемы, учитывает лобовую атаку на криптосхему, но возможны и другие способы атаки, поэтому в понятии безопасности должна учитываться вероятность появления прорывной атаки на криптосхему. Последняя зависит от вероятности появления прорывного способа решения трудной задачи, но эти две вероятности должны рассматриваться как различные. Только в частном случае доказуемо стойких двухключевых криптосхем (для которых дано формальное доказательство того, что любой алгоритм взлома криптосхемы полиномиально сводится к алгоритму решения трудной задачи, положенной в ее основу) эти вероятности совпадают.

Таким образом, понятие безопасности криптосхем с открытым ключом является векторным параметром, включающим стойкость и вероятность появления прорывных атак на криптосистему. Если бы можно было дать приемлемые оценки такой вероятности, то тогда безопасность можно было бы определить как отношение стойкости к указанной вероятности. Ввиду условности оценок рассматриваемой вероятности целесообразно рассматривать два указанных параметра безопасности в отдельности. Рассматриваемое толкование понятия безопасности имеет следующее значение для синтеза криптосхем с открытым ключом. Оно непосредственно указывает на способ повышения уровня безопасности путем синтеза таких криптосхем, взлом которых требует одновременного решения двух независимых (и более) трудных задач, которые являются хорошо апробированными. Так как оцениваемая вероятность достаточно низка (и не важно это есть значение 0,001 или 0,000001) для каждой из таких задач, то вероятность одновременного появления за заданный промежуток времени прорывных решений для каждой из используемых трудных задач является значительно меньшей величиной, поскольку она равна произведению достаточно малых значений.

Наибольший интерес в таком подходе представляет использование ЗДЛ в конечном простом поле и ЗФ. На основе трудности одновременного решения этих двух задач построены криптосхемы следующих типов:

- протоколы индивидуальной ЭЦП [1,2];
- протокол слепой ЭЦП [3];
- протокол коллективной ЭЦП [2,4];
- протокол открытого согласования секретного ключа [5];
- протокол с нулевым разглашением секрета [5];
- алгоритм открытого шифрования [5].

Для толкования этого термина следует учесть следующее. Имеется некоторая начальная утечка о секрете, связанная с тем, что выполнение процедуры аутентификации пользователя выполняется по его открытому ключу (ОК), с которым связан его личный секретный ключ (ЛСК). Нахождение ЛСК по ОК составляет вычислительно трудную задачу. Сам факт, что это возможно указывает, что информация о ЛСК присутствует в ОК, т.е. мы умышленно по построению протокола с нулевым разглашением допустили такую утечку. Поэтому нулевое разглашение секрета в ходе протокола следует понимать в том смысле, что к этой начальной утечке не добавляется никакой дополнительной утечки. Теперь надо дать толкование факту отсутствия дополнительной утечки. Его следует понимать в том смысле, что все значения, которые направляет доказывающий (пользователь, который подтверждает свою подлинность в ходе протокола) проверяющему, могут быть выработаны проверяющим самостоятельно. Такая интерпретация основывается на статистической неотличимости случайных пар значений, связанных между собой некоторым соотношением (а именно, соотношением, используемым для проверки правильности ответов доказывающего на вопросы проверяющего). Таким образом, доказуемая стойкость протоколов с нулевым разглашением связана с тем, что выполнение протокола никоим образом не упрощает задачи вычисления ЛСК по ОК.

В протоколах с нулевым разглашением используются вычислительно трудные задачи следующих типов: 1) задача дискретного логарифмирования в конечной циклической группе (или в конечном поле), 2) задача факторизации, 3) задача извлечения корней по модулю большого простого числа и некоторые другие. На основе используемой трудной задачи пользователями формируются пары значений, одно из которых служит в качестве долговременного ОК, а другое – ЛСК. В ходе выполнения протокола взаимодействуют два субъекта – проверяющий и доказывающий. При этом используется ОК доказывающего, который должен доказать, что он знает ЛСК. Обычно протоколы с нулевым разглашением включают многократное повторения трех типовых шагов: 1) генерация доказывающим разового случайного секретного ключа и вычисление по нему разового ОК (последнее значение называется фиксатором), который передается проверяющему; 2) генерация проверяющим нулевого ($e = 0$) или единичного ($e = 1$) запроса с вероятностью 0,5 и направление бита запроса e доказывающему; 3) доказывающий направляет ответ на запрос, который проверяется с использованием некоторого проверочного соотношения, зависящего от разового ОК, долговременного ОК и запроса e . Итеративный протокол, основанный на ЗФ, может быть модифицирован в трехпроходный протокол с нулевым разглашением, в котором на втором шаге используется случайный запрос, представляющий собой достаточно длинную битовую цепочку [7], а последний – преобразован в достаточно компактную схему ЭЦП [8]. Почти любой протокол с нулевым разглашением может быть преобразован в схему ЭЦП. Идея такого преобразования состоит в использовании фиксатора как рандомизирующего параметра ЭЦП R , а значение хэш-функции от подписываемого документа M с присоединенным к нему фиксатором – в качестве битовой h -битовой цепочки запроса, т.е. подписываемый документ и фиксатор служат источником запроса. При использовании стойкой хэш-функции данный запрос может рассматриваться как имеющий случайное значение. При этом потенциальный фальсификатор подписи не имеет возможности модифицировать значение фиксатора после получения запроса, так как это моментально приведет к изменению значения запроса. Владелец ОК может сформировать правильный ответ S для любого запроса. Пара значений (R, S) рассматривается как подпись к заданному документу M .

Например, при использовании итеративных протоколов с нулевым разглашением следует задать условия, при которых подписывающий (в этой роли теперь выступает доказывающий) должен формировать h различных разовых ОК до того момента, когда станет известной битовая цепочка запросов (если это не будет обеспечено, то тогда нарушитель сможет подделать ЭЦП). Это достигается заданием процедуры вычисления хэш-функции от подписываемого документа, к которому присоединяются h сформированных разовых открытых ключей. После того как значение хэш-функции вычислено, оно рассматривается как последовательность запросов проверяющего, причем последовательный номер бита запроса должен соответствовать последовательному номеру открытого ключа в порядке его присоединения к документу при вычислении значения хэш-функции. Поскольку подписывающий знает секретный ключ, соответствующий его ОК, он может вычислить правильный ответ на каждый запрос. Подпись представляет собой две последовательности значений: упорядоченное множество разовых ОК и упорядоченное множество ответов. Процедура проверки ЭЦП состоит в вычислении хэш-функции от подписанного документа с присоединенной к нему последовательностью разовых открытых ключей и проверки всех ответов на h запросов, заданных значением хэш-функции.

Рассмотренный пример показывает принципиальную возможность преобразования протокола с нулевым разглашением в схему ЭЦП, например протоколов, основанных на задаче скрытого дискретного логарифмирования [10], называемой также скрытой задачей поиска сопрягающего элемента [11]. Для практических приложений ЭЦП важным является технический вопрос о ее размере. Описанное преобразование итеративного протокола с нулевым разглашением приводит к схеме ЭЦП с весьма большим размером подписи. Для сокращения размера следует выбирать такие трудные задачи, которые позволяют реализовать протокол с нулевым разглашением всего за три шага. При разработке трехшаговых протоколов с нулевым разглашением, ориентированных на их преобразование в схему ЭЦП полезным является использование толкования понятия нулевого разглашения данного ранее. Такие построения схем ЭЦП представлены в статье [9].

2. Расширение функциональности протоколов цифровой подписи

Под функциональностью криптографических протоколов понимается набор присущих им свойств, обеспечивающих возможность их применения в рамках специфических сценариев процедуры аутентификации, т.е. возможность генерации и проверки подлинности ЭЦП при обеспечении некоторых дополнительных свойств, накладываемых особенностями решаемых практических задач. Потребности практики связаны с использованием протоколов ЭЦП, различных типов, которые предоставляют следующие возможности электронных технологий:

- тайное электронное голосование;
- электронные деньги;

- доказательство наличия знаний без их разглашения;
- защита материальных объектов от подделки;
- протоколы подтверждения подлинности субъектов и объектов.

Например, протоколы слепой ЭЦП лежат в основе технологий электронных денег и позволяют построить наиболее эффективные системы тайного электронного голосования. Практический интерес имеют также и протоколы групповой ЭЦП как подписи некоторого уполномоченного органа, формируемая штатными сотрудниками последнего. Другим интересным для практики типом криптосхем являются протоколы коллективной ЭЦП, обеспечивающие возможность формирования подписей фиксированного размера, принадлежащие произвольным совокупностям субъектов.

Объединение функций протоколов ЭЦП различных типов в единой криптосхеме повышает технологичность механизма аутентификации в ряде специальных случаев применения протоколов ЭЦП, заключающуюся в сокращении числа выполняемых процедур, связанных с механизмом аутентификации информации при решении специальных задач. Известны следующие типы схемы ЭЦП с расширенной функциональностью: протоколы коллективной ЭЦП, протоколы коллективной слепой ЭЦП, протоколы коллективной ЭЦП с восстановлением сообщения, основанные на трудности ЗФ. Представляет интерес разработка протоколов слепой ЭЦП с с восстановлением сообщения и протоколов коллективной ЭЦП над ЗДЛ. Использование ЗДЛ вместо ЗФ при построении протоколов с расширенной функциональностью представляет существенный интерес, поскольку это позволяет значительно сократить размер подписи и повысить быстродействие протоколов такого типа. В частности уменьшение длины ЭЦП имеет значение для совершенствования технологии криптографической защиты материальных документов от подделки, в которой цифровой эталонный образ бумаги, на которой изготовлен документ, ключевые слова документа и коллективная цифровая подпись печатаются на документе в виде машиночитаемой метки (использование коллективной ЭЦП, подтверждающей подлинность документа двумя и более уполномоченными органами, существенно снижает вероятность подделки документа с участием внутренних нарушителей).

Заключение

Многие из известных в настоящее время протоколов ЭЦП с расширенной функциональностью (протоколы коллективной, слепой коллективной и утверждаемой групповой подписи) используют стандартную инфраструктуру открытых ключей, что упрощает их практическое использование. Потребности практики в различных типах схем ЭЦП делает актуальным расширение функциональности официальных стандартов ЭЦП, что для ГОСТ Р 34.10–2001, СТБ 1176.2–99 и ДСТУ 4145–2002 может быть сделано с сохранением специфицированных процедур проверки подлинности ЭЦП.

Рассмотрение интегрального параметра безопасности двухключевых криптосхем, равного отношению стойкости к вероятности появления прорывной атаки, непосредственно показывает на возможность повышения уровня безопасности криптосистем с открытым ключом путем использования трудности одновременного решения двух независимых трудных задач. В частности в недавних публикациях [3,12,13] детально рассматривается вопрос синтеза протоколов слепой ЭЦП, взлом которых требует одновременного решения ЗФ и ЗДЛ.

СПИСОК ЛИТЕРАТУРЫ

1. Дернова Е.С., Молдовян Н.А. Синтез алгоритмов цифровой подписи на основе нескольких вычислительно трудных задач // Вопросы защиты информации. 2008. №1. С. 22–26.
2. Дернова Е.С. Механизмы аутентификации информации, основанные на двух вычислительно трудных задачах // Автореф. дисс. канд. тех. наук. СПб, 2009. –18 с.
3. 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.
4. 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.
5. Молдовян Д.Н., Кишмар Р.В., Васильев И.Н. Двухключевые криптосхемы на основе комбинирования задач факторизации и дискретного логарифмирования // Вопросы защиты информации. 2011. № 4.
6. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи.– Санкт-Петербург, БХВ–Петербург, 2010. – 304 с.
7. Дернова Е.С., Молдовян Д.Н., Молдовян Н.А. Криптографические протоколы. – СПб., Издательство СПбГЭТУ «ЛЭТИ», 2010. – 100 с.
8. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. – Санкт-Петербург, БХВ–Петербург, 2005. – 286 с.
9. 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
10. Moldovyan D.N., Moldovyan N.A. A New Hard Problem over Non-Commutative Finite Groups for Cryptographic Protocols // Springer Verlag LNCS. 2010. Vol. 6258. P. 183–194 / 5th Int. Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ANCS 2010 Proceedings. St.Petersburg, September 8–11, 2010.
11. Moldovyan D.N., Moldovyan N.A. Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms // Quasigroups and Related Systems. 2010. Vol. 18. P. 177–186.
12. Tahat N.M.F., Shatnawi S.M.A., Ismail E.S. New Partially Blind Signature Based on Factoring and Discrete Logarithms // Journal of Mathematics and Statistics. 2008. V. 4. N. 2. P. 124–129.
13. Taha N.M.F., Ismail E.S., Ahmad R.R. A New Blind Signature Scheme Based On Factoring and Discrete Logarithms // International Journal of Cryptology Research. 2009. V. 1. N. 1. P. 1–9.

Черешкин Д.С., Кононов А.А., Сичкарук А.В.

Россия, Москва, Институт системного анализа РАН

КОНЦЕПЦИЯ ОЦЕНКИ КРИТЕРИАЛЬНЫХ РИСКОВ В УПРАВЛЕНИИ БЕЗОПАСНОСТЬЮ БОЛЬШИХ РЕГИОНАЛЬНЫХ СИСТЕМ

Среди задач управления рисками в чрезвычайных ситуациях (ЧС) больших региональных систем (БРС), в виду масштаба и сложности такого рода систем, возникает задача контроля рисков для множества структур и объектов их образующих. На сегодняшний день решение именно этой задачи практически не было проработано в научном и теоретическом плане, что в значительной степени обуславливает то, что ответственность лиц, отвечающих за безопасность БРС, зачастую превышает их возможности контроля состояния безопасности БРС и что является одной из фундаментальных причин большинства техногенных катастроф, а так же большого числа жертв и высоких уровней материального ущерба, в том числе, при природных катастрофах. Приблизиться к решению этой и еще целого ряда взаимосвязанных задач управления рисками чрезвычайных ситуаций позволяет введение понятия, и методов оценки «критериальных рисков».

В связи с тем, что это новое понятие остановимся на его определении.

Пусть существует некоторая организационная (социально-экономическая) система.

Для того, чтобы не произошло ЧС, или чтобы ущерб и жертвы при неизбежной природной катастрофе были минимальны, система должна соответствовать некоторому идеальному множеству критериев, или, иными словами, в ней должно выполняться некоторое идеальное множество требований.

Риски ЧС, существующие из-за не полного выполнения идеального множества требований будем называть критериальными рисками.

В качестве причин существования критериальных рисков могут быть названы следующие две:

1. Заданная к исполнению система требований некорректна (отлична от идеальной):

- неполна;
- избыточна;
- требования некорректны;
- требования противоречивы;
- требования некорректно ранжированы.

2. Невыполнение корректных требований заданной к исполнению системы.

В качестве примера реализации критериальных рисков возникших из-за некорректной критериальной базы может быть приведен фрагмент из доклада В.Р.Болова, сотрудника Всероссийского центра мониторинга и прогнозирования чрезвычайных ситуаций природного и техногенного характера МЧС России (Центр «Антистихия»): «Низкий уровень информационного взаимодействия в области мониторинга и прогнозирования ЧС сказывается и на ведомственной нормативной базе. В ряде случаев ЧС, что называется, формируются в полном соответствии с инструкциями. Только один пример: ЗЕЯ. Аномалия осадков в районе Зейской ГЭС привела к затоплению ряда населенных пунктов, только потому, что решение о повышении сбросов воды с водохранилища принимается не на основе оценки складывающейся ситуации, а по достижению определенной отметки. В результате, когда назревает необходимость повысить сбросы, с тем чтобы избежать переполнения водохранилища, их уровень должен быть уже такой, что избежать ЧС уже не представляется возможным» [1].

В качестве примера формирования критериальных рисков из-за невыполнения требований можно привести случаи многочисленного нарушения требований в нефтегазовом комплексе, приведшие к авариям и ЧС [2]: при расследовании 118 аварий и несчастных случаев, зафиксировано 378 нарушений. При этом 24 раза зафиксированы нарушения актов законодательного характера; 170 раз – нарушения нормативных актов, принимаемых федеральными органами 184 раза – нарушения требований стандартов организаций и предприятий.

При использовании любой компьютеризированной системы для обеспечения ее безопасного функционирования также должно выполняться некоторое идеальное множество требований. Тем не менее, как правило, этого достичь не удастся, и потому что все это множество требований составляющих идеальное критериальное множество не всегда известно, и потому, что в реальной жизни многие даже известные требования не выполняются. Задача состоит в том, чтобы оценить риски из-за возможной недостаточной кибербезопасности АИС.

Современные подходы к созданию безопасных АИС [3–6] предполагают, что для того, чтобы на безопасность АИС можно было положиться должны быть построены модели угроз АИС, модели защиты, оценены риски нарушения безопасности. Эти методы позволяют снизить критериальные риски, связанные с неполнотой критериальной базы и приблизиться к получению такой системы требований, которые должны выполняться, для того, чтобы безопасности АИС можно было бы доверять. При этом требования предъявляются как к АИС в целом, так и каждой из ее структур, к отдельным компонентам, а так же к технологическим и бизнес процессам и точкам этих процессов (рисунок 1).

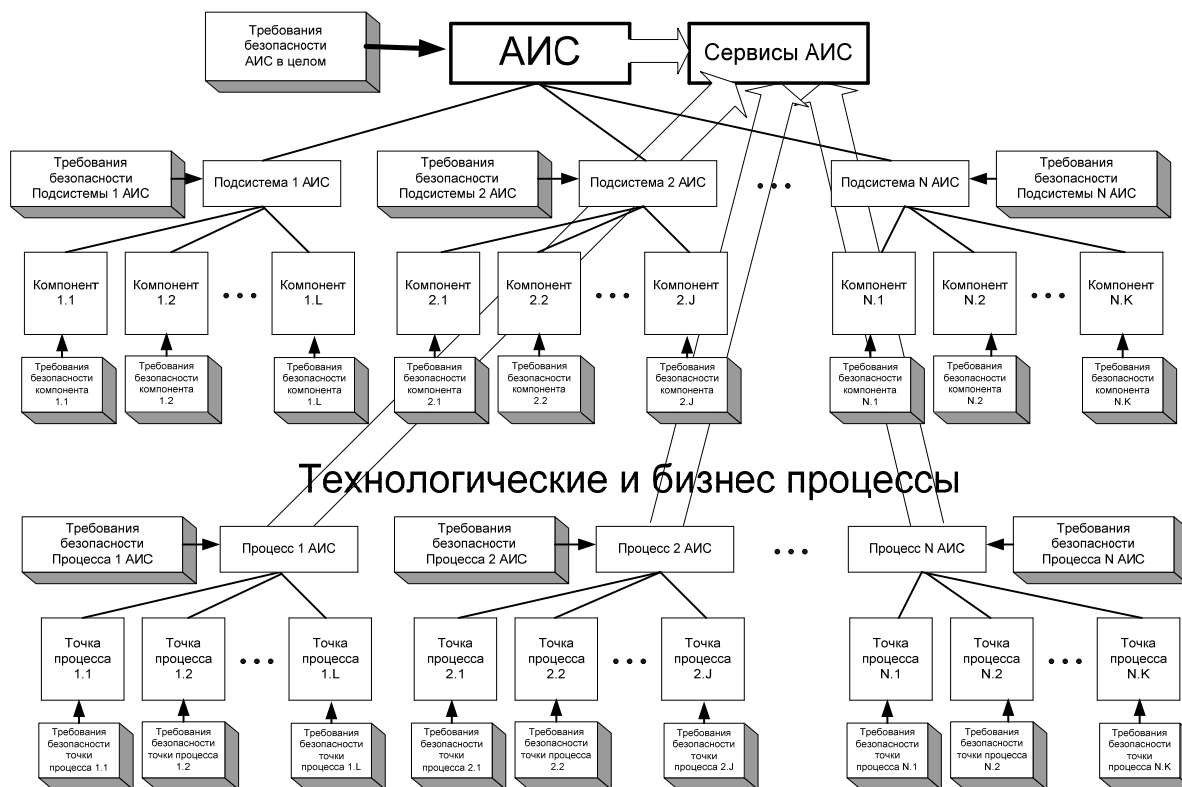


Рис. 1. Распределение требований безопасности по структурным составляющим, технологическим и бизнес процессам АИС

Применительно к проблемам безопасности АИС, принято использовать термин – «информационная безопасность». При выполнении системы требований информационной безопасности (ИБ) могут возникнуть следующие проблемы:

- исполнение всех возможных требований по обеспечению ИБ может быть невозможно из-за слишком высокой стоимости их реализации;
- требования по безопасности могут не выполняться из-за отсутствия достаточно эффективного контроля за выполнением требований, низкой дисциплины и низкого качества требований;
- требования могут не выполняться, поскольку они плохо усвоены исполнителями.

Во всех трех перечисленных случаях контроль за выполнением требований может дать большой положительный эффект.

Если часть требований не может быть реализована из-за недостатка средств на их реализацию, контроль должен позволить не упускать из вида существующие проблемы и решать их по мере появления средств на повышение ИБ, с учетом показателей важности решения указанных проблем. В тоже время контроль позволяет ориентироваться в обнаружении возможных проблемных мест.

При отсутствии эффективного контроля за выполнением требований, со стороны исполнителей могут проявляться тенденции оптимизировать свою работу за счет игнорирования требований по безопасности. Поэтому постоянный контроль за выполнением требований, помимо прочего, призван внушить исполнителям важность выполнения требований.

В системах, где организован всеобъемлющий контроль всех требований, как правило, помимо огромного числа инструкций, приказов, законодательных и подзаконных актов, в которых формулируются требования, составляются списки требований по подконтрольным структурам и процессам. Наличие такого рода списков позволяет как контролерам, так и исполнителям быстрее вникать во всю систему требований, быстрее ее осваивать и, соответственно, лучше их исполнять, а при необходимости сообщать о недостатках системы требований.

Очевидно, что эффективный контроль за выполнением, большого числа требований отнесенным к большому количеству компонентов, процессов и исполнителей невозможен без измеряемых характеристик и показателей, которые позволили бы судить о реальных уровнях выполнения требований по структурным подразделениям, по процессам обработки и хранения информации, выявлять наиболее проблемные («узкие») места и возможные источники наибольших проблем с обеспечением ИБ. Решить эту задачу на сегодняшний день позволяет только применение оценок критериальных рисков, когда оценку любых возможных потерь и любых показателей защиты можно свести к указанию уровня возможных или достигнутых степеней соответствия критериев по 100-балльной шкале (рисунок 2.).

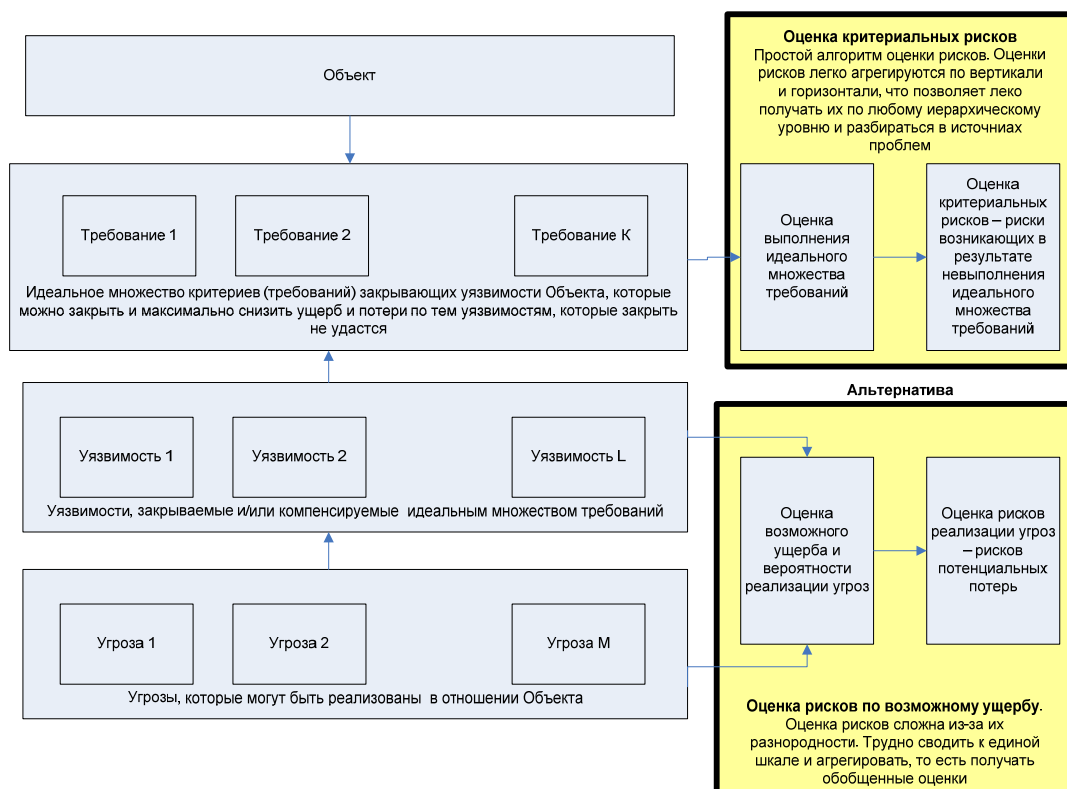


Рис. 2. Два альтернативных метода оценки рисков

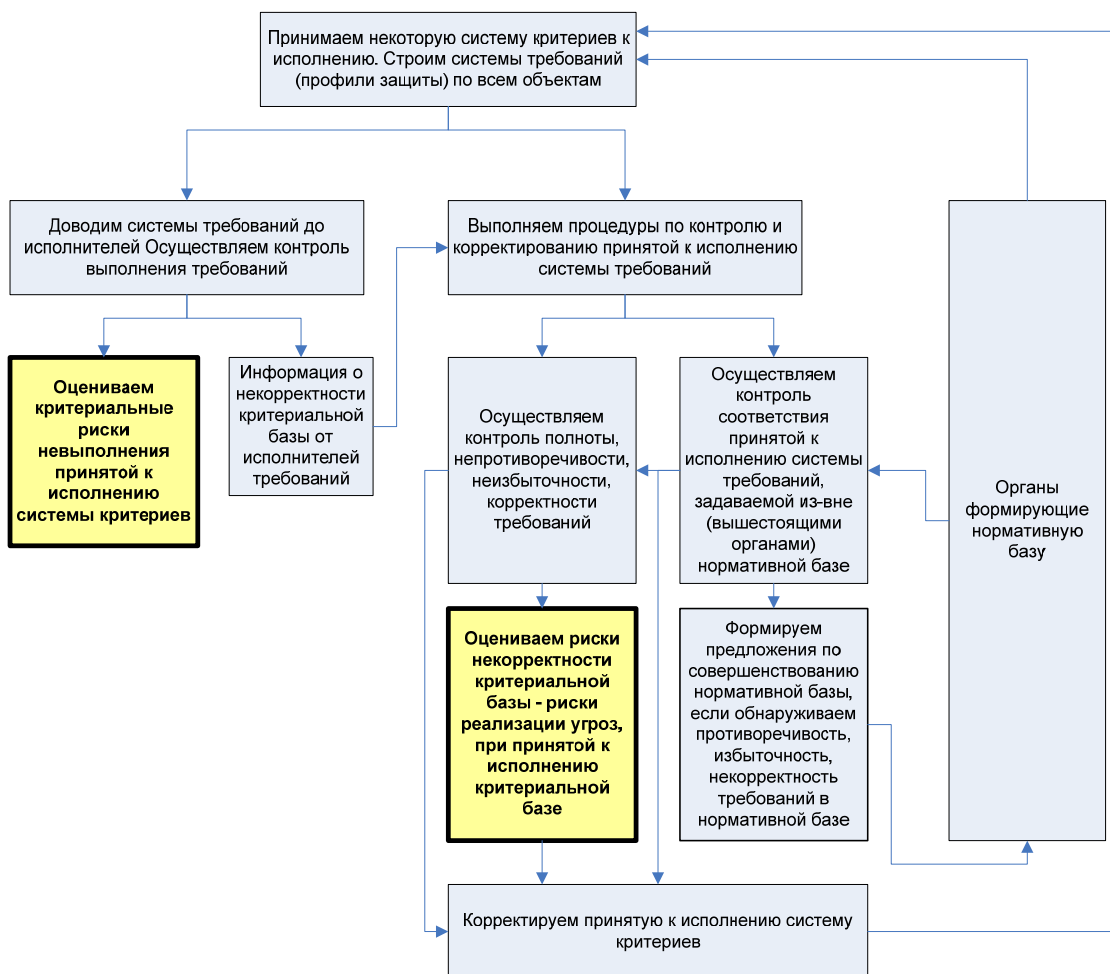


Рис. 3. Концепция оценки критериальных рисков в больших территориально-распределенных системах

На рисунке 3 проиллюстрирована концепция оценки критериальных рисков в больших региональных системах. Эта концепция предполагает наличие некоторых органов, формирующих

нормативную базу. Эта нормативная база используется для формирования критериальной системы – множества требований доводимых до исполнителей в виде профилей защиты. По результатам исполнения требований проводится оценка критериальных рисков, а так же осуществляются мероприятия по снижению рисков, связанных с некорректностью критериальной базы.

Таким образом, применение методологии оценки критериальных рисков позволяет помимо оценки рисков, контролировать качество всей нормативной базы и своевременно ставить задачи по ее корректировке, если в ней существуют недостатки, и таким образом принимать обоснованные решения по снижению всех возможных критериальных рисков.

СПИСОК ЛИТЕРАТУРЫ

1. В.Р. Болов. Основные проблемы повышения эффективности функционирования системы мониторинга и прогнозирования чрезвычайных ситуаций и пути их решения // Проблемы прогнозирования чрезвычайных ситуаций. VII научно-практическая конференция. 2-4 октября 2007 г. Доклады и выступления. – М: «МТП-инвест», 2008. Стр.15.
2. Анализ аварий и несчастных случаев в нефтегазовом комплексе России / Под ред. Б.Е. Прусенко, В.Ф. Мартынюк – ООО «Анализ опасностей», Москва, 2002–310с.
3. Кононов А.А., Поликарпов А.К. Обеспечение безопасности информации: задачи и решения» // Информационная безопасность –2005. – №5.
4. Кононов А.А., Поликарпов А.К. Обеспечение гарантированной защиты информации в компьютерных системах // Науч.-техн. информ. – Сер. 1. –2006. – №4. – С.42–43.
5. BS ISO/IEC 27001:2005 RU. Информационные технологии- Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования. Британский стандарт. –М. ООО «GlobalTrust Solutions», 2006 г.
6. ГОСТ Р ИСО/МЭК 15408. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – М. Госстандарт России, Москва. 2002 г.



ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ

Полончик О.Л.

Россия, Архангельск, Северный (Арктический) федеральный университет
имени М.В. Ломоносова

РАЗВИТИЕ СИСТЕМ ДЛЯ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В БЕЗОПАСНОМ УПРАВЛЕНИИ РЕГИОНОМ НА ОСНОВЕ ДАННЫХ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ

Задача повышения конкурентоспособности экономики является одной из наиболее актуальных для развития Архангельской области, занимающей огромную территорию.

Одним из направлений повышения эффективности управления регионом является использование данных космического зондирования земной поверхности. Это один из самых объективных способов получения достоверной информации практически в реальном масштабе времени. Использование данных космического мониторинга региона предоставит руководству региона возможность оперативного получения данных, необходимых для устойчивого управления.

Дистанционное зондирование Земли представляет собой современные технологии, включающие получение, и обработку данных космической съемки с целью их дальнейшего использования для решения различных научных и практических задач.

В настоящее время в САФУ создан центр космического мониторинга Арктики. Научное оборудование позволяет получать информацию с различных иностранных спутников в оптическом, инфракрасном и радиодиапазонах в режиме реального времени или близких к нему. Центр мониторинга уже вошёл в ряд систем университетского и прикладного характера России.

Эффективность использования полученной информации во многом определяется потребностями существующих и вновь создаваемых информационных систем, скоростью актуализации их баз данных, информационными технологиями обработки данных.

Анализ показывает, очевидное отставание нашей страны, это выражается в том, что новые системы будут созданы в ближайшие годы, а другие государства владеют этими технологиями уже в настоящее время.

В настоящее время место России на рынке коммерческой космонавтики не соответствует статусу космической державы. Обеспечивая 40% мировых запусков и 20% производства космических аппаратов, Россия имеет на рынке коммерческих космических услуг лишь 3%. Это при том, что 2010 году Россия провела больше 40% всех запусков космических ракет в мире — 31 из 74.

Однако в последние годы начата интенсивная разработка ряда новых отечественных систем ДЗЗ и изучения околоземного космического пространства. Созданы новые типы малых КА (*Канопус-В*, *Кондор-Э*, *Электро-Л*), позволяющих эффективно решать поставленные задачи. Налаживается их серийное производство и начаты лётные испытания. Технические характеристики соответствуют мировому уровню. Они послужат основой для создания новых космических систем. «К 2015 году планируем увеличить количество спутников дистанционного зондирования Земли с 5 до 20 космических аппаратов, навигационных спутников ГЛОНАСС - с 24 до 30, с 26 до 48 - спутников связи и системы КОСПАС-SARSAT», - пообещал глава Роскосмоса

В. Поповкин с думской трибуны.

Поэтому в настоящее время целесообразно использовать методы коммерческих структур, ориентированные на получение и обработку данных ДЗЗ с иностранных КА. Это позволит специалистам и учёным С(А)ФУ овладеть существующими технологиями тематической обработки пространственной информации, создавать новые, искать области эффективного применения получаемых данных.

Необходима тесная интеграция САФУ с ведущими научными космическими и производственными организациями региона, округа, России (Академия РАН РФ, ВКА им Можайского, Космодром «Плесецк», предприятия «Роскосмоса»). Это позволит САФУ овладеть новейшими отечественными разработками по тематической обработке информации, оперативно получать данные с новых отечественных систем, правильно определять потребности рынка по подготовке специалистов требуемого профиля и организовывать их подготовку.

Задача повышения конкурентоспособности экономики не может быть решена без усиления роли высшего профессионального образования. Инновационное образование предполагает обучение

в процессе создания новых знаний – за счет интеграции фундаментальной науки, непосредственно учебного процесса и производства.

Подготовка специалистов такого профиля планируется на базе Института информационных и космических технологий Северного (Арктического) Федерального Университета.

Использование данных технологий позволит проводить производственно-коммерческая деятельность по мониторингу территории региона и предоставление на коммерческих условиях информации для поддержки принятия управленческих решений хозяйствующим субъектам Архангельской области и соседним регионам.



ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Большакова Л.В., Примакин А.И.

Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ИНФОРМАЦИОННЫЙ ПОДХОД ДЛЯ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА

Современный этап развития экономики ставит перед отдельными экономическими субъектами ряд задач, связанных с выбором дальнейших действий по повышению своих доходов, уменьшению риска и затрат, сохранению своей экономической безопасности. Для успешного решения подобных задач может быть применен информационный подход исследования экономики и, в частности, теория принятия решений. С помощью методов этой теории могут быть получены способы оценки того или иного выбора действия, критерии надежности и безопасности этого действия, а также может быть сделан правильный прогноз относительно дальнейшего развития [1].

Однако довольно часто возникают ситуации, при которых невозможна полная математическая формализация проблемы, а значит выбор, обоснование и оценка последствий не могут быть произведены на основе точных расчетов. В этом случае применяют метод экспертных оценок, в котором точные математические методы дополняются рекомендациями специалистов-экспертов, что позволяет хотя бы частично восполнить недостающую информацию, проверить ее достоверность или оценить качественные признаки.

В настоящее время существует различная интерпретация понятия методов экспертных оценок. Некоторые специалисты под этими методами понимают различные формы проведения экспертного оценивания, а именно, методы Дельфы, мозгового штурма и т.д. [2]. Другие считают, что методы экспертных оценок – это различные способы получения экспертной информации, например, методы простого, последовательного или парного ранжирования [3]. Наконец, третьи связывают метод экспертных оценок с математико-статистической обработкой результатов [4].

Авторы настоящей статьи считают, что необходимо устранить эти разногласия и предлагают свое видение в решении вышеуказанной проблемы, свой алгоритм решения задач по обеспечению экономической безопасности хозяйствующего субъекта.

На наш взгляд существуют не методы, а метод экспертных оценок, определяемый как метод теории принятия решений, в котором используются рекомендации экспертов-специалистов. Метод экспертных оценок включает в себя комплекс организационных, логических, математико-статистических процедур и методов, направленных на подготовку и выбор рациональных решений.

Область применения метода достаточно широка. С помощью метода экспертных оценок могут быть решены следующие задачи:

- установление степени предпочтительности (ранга) того или иного показателя, например, расположение факторов в порядке уменьшения степени их влияния на экономическую безопасность предприятия;
- определение оценок экономических показателей, например, величины предполагаемых расходов для проведения какого-то мероприятия;
- определение оценки относительной важности показателей, объектов или критериев;
- нахождение альтернативных вариантов решения некоторой проблемы;
- определение наиболее вероятных интервалов времени свершения последовательности каких-то событий;
- решение задачи классификации, т.е. разбиение совокупности объектов на определенные группы по каким-то признакам.

Особенностями данного метода, которые отличают его от обычной экспертизы, являются научная обоснованность организации проведения экспертного исследования и применение математико-статистических методов при обработке и анализе полученной экспертной информации. Эти особенности определяют основные этапы метода экспертных оценок:

Этап 1. Формулировка проблемы, постановка задач.

Этап 2. Подготовка, организация и проведение экспертного оценивания.

Этап 3. Анализ и обработка экспертной информации.

Этап 4. Получение выводов, рекомендаций и прогнозов.

Для каждого из этапов существуют свои задачи, при решении которых могут применяться различные процедуры и методы, связанные с основной проблемой исследования.

Выполняемые на первом этапе формулировка проблемы (1.1), постановка целей и задач исследования имеют определяющее значение для метода экспертных оценок. Они, безусловно, связаны с потребностями практики и должны быть четко сформулированы руководителем данного исследования – лицом принимающим решение (ЛПР). Для помощи в проведении данного исследования ЛПР может сформировать рабочую группу специалистов-аналитиков (1.2), в задачи которых входит организация и проведение экспертизы, а также, в некоторых случаях, проведение обработки и анализ экспертной информации. При небольших исследованиях ЛПР может само организовать и провести экспертизу.

На втором этапе метода экспертных оценок решают вопросы, связанные с подготовкой, организацией и проведением экспертного оценивания. Необходимо отметить, что экспертное суждение не является решением проблемы, это лишь полезная информация, которая помогает сделать правильный вывод.

На втором этапе должны быть проведены следующие мероприятия:

2.1. Формирование экспертной группы.

2.2. Выбор формы проведения процедуры экспертного оценивания.

2.3. Составление задания для экспертов и определение вида информации, которая должна быть от них получена.

2.4. Проведение процедуры экспертного оценивания и сбор экспертной информации.

При формировании экспертной группы (2.1) необходимо определить оптимальную численность группы, получить правило оценки компетентности каждого эксперта и найти окончательный состав экспертной группы. Вопрос об оптимальном числе экспертов остается открытым, несмотря на то, что в некоторых работах предлагаются методы или формулы определения этого числа, но, как правило, без строгих обоснований [5].

В связи с этим особое внимание заслуживает задача определения компетентности экспертов. Для ее решения существует достаточно много методов, некоторые из которых дают очень неплохие результаты [6].

Параллельно с формированием экспертной группы должна быть определена форма проведения процедуры экспертного оценивания (2.2). При анализе этих процедур необходимо ответить на два вопроса:

1. Каков должен быть характер взаимодействия экспертов в процессе опроса?

2. Должна ли существовать в процедуре оценивания обратная связь, т.е. возможно ли информирование экспертов о предыдущих турах опроса?

В зависимости от ответа на эти вопросы существуют четыре вида возможных процедур экспертного оценивания:

1. Одноразовые процедуры без обратной связи.

2. Одноразовые процедуры с обратной связью.

3. Многократные процедуры с обратной связью.

4. Многократные процедуры без обратной связи.

При экспертном оценивании по процедуре первого вида предполагается проведение одноразового раздельного опроса экспертов. Процедура проста в организации и не требует больших затрат на проведение. Как правило, ее применяют только в тех случаях, когда имеется дефицит времени и нет достаточно средств. Примерами такой процедуры могут служить обычное анкетирование или интервью.

Второй вид процедур предусматривает возможность общения экспертов во время экспертного оценивания. Примером могут служить различные совещания и дискуссии, на которых можно свободно отстаивать свою точку зрения, не допускается лишь критиковать ответы других. Наиболее распространенным способом получения экспертной информации по второй процедуре является метод «мозгового штурма».

Дискуссии, которые проводятся в несколько четко выраженных туров, являются примером экспертного оценивания третьего вида. В ходе дискуссии эксперт может неоднократно высказывать свою точку зрения, менять ее.

Основным методом, в котором используется процедура четвертого вида, является метод Дельфы. Этот метод часто применяется для решения задач прогнозирования, для оценки вероятности наступления тех или иных возможных в будущем событий. Он состоит из нескольких последовательно осуществляемых туров, результатом которых является формирование группового мнения по рассматриваемой проблеме. В первом туре эксперты отвечают на поставленные вопросы. Во втором туре каждый эксперт знакомится с ответами всех остальных, но без указания авторов ответов. Кроме этого, эксперта знакомят с общим решением каждого тура. В результате чего каждый эксперт может поменять свое мнение или же аргументировать свой первоначальный ответ, если он существенно отличается от остальных.

От задач и целей экспертного оценивания зависят вопросы и задания для экспертов, а также виды получаемой от них информации (2.3). Вопросы и задания должны быть четкими, понятными эксперту, в них не должно быть никаких наводящих на какой-либо ответ данных.

При формировании своих оценок (2.4) эксперты могут использовать следующие способы измерения и сравнения объектов [7]:

- ранжирование;
- парное сравнение;
- непосредственная оценка;
- последовательное сравнение.

Перейдем к третьему этапу метода экспертных оценок – к анализу и обработке экспертной информации (3).

На этом этапе должны быть решены следующие задачи:

- 3.1. Анализ индивидуальных оценок каждого эксперта.
- 3.2. Анализ совокупности оценок всей группы экспертов.
- 3.3. Объединение экспертных оценок.

Каждый эксперт, даже достаточно компетентный, в силу различных причин, в том числе и случайного характера, может дать нелогичные или противоречивые ответы. Переход ко второй задаче (3.2) данного этапа невозможен, если доказана противоречивость оценок эксперта. В этом случае необходимо провести соответствующие мероприятия, а иногда даже исключить эти оценки из дальнейшего рассмотрения.

Решение второй задачи (3.2) предполагает анализ оценки всех экспертов на предмет их согласованности.

Анализ согласованности оценок экспертов может быть произведен путем вычисления числовой меры, характеризующей степень близости индивидуальных мнений. Оценки экспертов могут быть в виде рангов и в виде произвольных чисел, характеризующих степень значимости каждого фактора для решения исследуемой проблемы. Если экспертная информация представлена в виде рангов, то согласованность оценок экспертов можно проверить по значению коэффициента конкордации W [7].

Предположим теперь, что согласованность экспертов получена, тогда появляется задача объединения индивидуальных экспертных оценок в обобщенные групповые (3.3). В зависимости от целей экспертного оценивания, выбранного метода измерения и вида экспертной информации при обработке результатов возникает необходимость решения следующих основных задач:

3.3.1. Нахождение обобщенных рангов факторов на основе индивидуальных оценок экспертов, полученных после процедуры ранжирования.

3.3.2. Нахождение обобщенных рангов факторов на основе результатов парного сравнения факторов каждым экспертом.

3.3.3. Нахождение обобщенных относительных весов факторов на основе индивидуальных оценок экспертов.

3.3.4. Определение зависимостей между различными последовательностями рангов.

Решение первой задачи (3.3.1) зависит от способа ранжирования факторов и вида информации, полученной от экспертов. Если для группы экспертов ставилась задача произвести обычное ранжирование имеющихся факторов, то для получения окончательных обобщенных рангов факторов поступают следующим образом. Вначале находят для каждого фактора сумму рангов, полученных от всех экспертов. Фактор, имеющий наименьшую сумму получает окончательный ранг, равный 1, фактор, имеющий наименьшую сумму из оставшихся получает ранг, равный 2 и т.д.

При применении двухэтапного процесса ранжирования информация от каждого эксперта представляется в виде двух последовательностей рангов: рангов групп факторов и рангов самих факторов внутри группы. В этом случае, задача получения обобщенных рангов делится на две части. В первой части необходимо преобразовать полученную от экспертов информацию в обычную последовательность рангов факторов. Во второй части по преобразованной информации – найти обобщенные ранги.

Очевидно, что решение второй части в точности повторяет вышеописанную процедуру получения обобщенных рангов при обычном ранжировании. Поэтому главной является первая часть общей задачи, которая состоит в преобразовании, полученной от каждого эксперта информации. Для такого преобразования может быть предложено несколько способов.

По первому способу ранг каждого фактора полагается равным номеру его места в последовательности факторов, сформированной по правилу: вначале располагаются факторы первой группы (группы, имеющей ранг 1) в порядке увеличения их рангов, затем присоединяют соответствующим образом факторы второй группы и т.д. В итоге для каждого эксперта получают ранжирование всех имеющихся факторов.

Очевидное достоинство такого способа – легкость и простота. Однако это ранжирование является достаточно грубым и может не учитывать существенные моменты. Например, по мнению эксперта, какой-нибудь фактор второй группы может иметь более важное значение, чем какой-то из факторов первой группы, однако по предложенному способу он получит ранг меньший, чем любой из факторов первой группы.

Устранить подобный недостаток можно при применении другого способа преобразования экспертной информации – ранжирования по сумме оценок. Для получения рангов факторов

используют сравнение сумм двух оценок, а именно, ранга группы, к которой относится фактор и ранга самого фактора в группе. Полученное по этому способу ранжирование более объективно, так как учитывает степень различия в оценках мест групп и факторов внутри группы. Однако и здесь имеются недостатки, связанные, прежде всего, с тем, что число групп и число факторов в группах может не совпадать. Тогда приходится складывать величины, измеренные в разных масштабах. Для устранения этого недостатка может быть использован способ ранжирования по сравнимой шкале, в котором предполагается нахождение некоторого корректирующего коэффициента, при умножении на который можно определить оценки по сравнимой шкале.

При применении парного сравнения (3.3.2) от каждого эксперта получают таблицу парных сравнений. Наиболее простой вариант определения последовательности рангов для каждого эксперта состоит в следующем. Находят сумму элементов каждой строки таблицы. Ранги факторов определяются по степени уменьшения этих сумм, причем ранг, равный 1, получает тот фактор, который расположен в строке с наибольшей суммой элементов. После нахождения последовательности рангов факторов по таблице парных сравнений для каждого эксперта находят обобщенные ранги факторов по описанному выше способу.

Для нахождения обобщенных относительных весов факторов по индивидуальным оценкам экспертов (3.3.3) требуется проведение определенных расчетов. Вначале происходит нормирование всех оценок для каждого эксперта, т.е. рассчитывается относительная значимость каждого фактора в отдельности. В качестве обобщенной оценки фактора принимают среднюю арифметическую из нормированных оценок этого фактора, полученных от всех экспертов.

Важную роль при обработке и анализе экспертной информации играет задача установления зависимости между последовательностями рангов, полученных от двух экспертов или от двух групп экспертов (3.3.4).

Предположим, что решается задача упорядочения факторов по степени их влияния на какой-то объект. Группы экспертов выбираются из двух разных научных школ, т.е. фактически происходит две процедуры экспертного оценивания для экспертов из одной и другой школы.

В результате обработки экспертной информации получены две последовательности обобщенных рангов факторов, построенных на суждениях экспертов этих школ. Возникает вопрос: являются ли согласованными обобщенные мнения представителей двух направлений по рассматриваемому вопросу?

Для ответа могут быть использованы определенные коэффициенты, характеризующие степень ранговых зависимостей – коэффициенты Кендалла и Спирмена. Чаще всего зависимость между последовательностями рангов проверяется по критерию Спирмена. Для этого находят коэффициент ранговой корреляции ρ . Этот коэффициент изменяется от -1 до $+1$. Если величина коэффициента ρ близка к 1 , то можно говорить о высокой согласованности мнений двух школ, если к 0 , то согласованность мнений практически отсутствует. Если величина коэффициента близка к -1 , то мнения представителей школ противоположны, т.е. факторы, имеющие наибольшие ранги по оценкам представителей одной школы, будут иметь наиболее низкие у представителей другой школы и наоборот.

Обработка результатов экспертного оценивания представляет собой достаточно трудоемкий процесс, особенно при большом числе факторов или экспертов. Поэтому для такой работы целесообразно применение средств вычислительной техники [7].

После анализа и обработки экспертных данных переходят к последнему этапу метода экспертных оценок (4) – этапу, на котором формулируются выводы по рассматриваемой проблеме, принимаются какие-то решения, делаются возможные прогнозы.

Таким образом, предложенный в статье информационный подход позволяет не только сформулировать научно обоснованные выводы, принять соответствующие решения в сфере обеспечения экономической безопасности хозяйствующего субъекта, но и определить направления будущих исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Моудера Дж., Элмаграби С. Исследование операций. Модели и применения. В 2-х томах. Москва. Издательство «Мир», 1981.
2. Орлов, А. И. Теория принятия решений – Экзамен, 2005.
3. Громова, Н. М., Громова, Н. И. Основы экономического прогнозирования. Изд-во «Академия Естествознания», 2006.
4. Граб, В. П. Экспертная оценка показателей качества // Надежность и качество: Труды Международного симпозиума. Пенза: ПГТУ, 2005.
5. Домарев, В. В. Безопасность информационных технологий. Методология систем защиты информации. К.: Изд-во ТИД «ДС», 2001.
6. Панкова, Л. А., Петровский, А. М., Шнейдерман, Н. В. Организация экспертизы и анализ экспертной информации – М.: Наука, 1984.
7. Большакова, Л. В., Примакин, А. И. Метод экспертных оценок в решении задач обеспечения экономической безопасности хозяйствующего субъекта. Вестник Санкт-Петербургского университета МВД России. №1 (53). 2012. – С. 191-200.

Домбровская Л.А.

Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ОСНОВНЫЕ НАПРАВЛЕНИЯ, ПРИНЦИПЫ И УСЛОВИЯ ОРГАНИЗАЦИОННОЙ
ЗАЩИТЫ ИНФОРМАЦИИ

Для наиболее полного и глубокого анализа происходящих в сфере защиты конфиденциальной информации процессов, понимания сущности планируемых и проводимых в этих целях мероприятий прежде всего необходимо рассмотреть одно из важнейших направлений защиты конфиденциальной информации – организационную защиту информации [1].

Организационная защита информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации предприятия. От полноты и качества решения руководством предприятия и должностными лицами организационных задач зависит эффективность функционирования системы защиты информации в целом. Роль и место организационной защиты информации в общей системе мер, направленных на защиту конфиденциальной информации предприятия, определяются исключительной важностью принятия руководством своевременных и верных управленческих решений с учетом имеющихся в его распоряжении сил, средств, методов и способов защиты информации и на основе действующего нормативно-методического аппарата.

Прежде чем перейти к определению организационной защиты, ее направлений и условий, рассмотрим источники конфиденциальной информации и каналы ее утечки.

Основными источниками конфиденциальной информации являются:

- персонал предприятия, допущенный к конфиденциальной информации;
- носители конфиденциальной информации (документы, изделия);
- технические средства, предназначенные для хранения и обработки информации;
- средства коммуникации, используемые в целях передачи информации;
- передаваемые по каналам связи сообщения, содержащие конфиденциальную

информацию.

Способы обмена конфиденциальной информацией (например, между сотрудниками предприятия) могут носить как непосредственный (личный) характер, так и характер передачи формируемых на основе информации сообщений посредством технических средств и средств коммуникаций (различных средств и систем связи).

Из существующих способов обмена конфиденциальной информацией необходимо выделить организационные каналы передачи и обмена информацией:

- конфиденциальное делопроизводство (защищенный документооборот);
- совместные работы, выполняемые предприятием по направлениям его основной и иной деятельности;
- совещания (конференции), в ходе которых обсуждаются вопросы конфиденциального характера;
- рекламная и издательская (публикаторская) деятельность;
- различные мероприятия в области сотрудничества с иностранными государствами (их представителями и организациями), связанные с обменом информацией;
- научные исследования, деятельность диссертационных и иных советов учреждений и организаций;
- передача сведений о деятельности предприятия и данных о его сотрудниках в территориальные инспекторские и надзорные органы.

Организационные каналы передачи и обмена конфиденциальной информацией в ходе их функционирования могут быть подвергнуты негативному воздействию со стороны злоумышленников, направленному на получение этой информации. Данное воздействие, в свою очередь, может привести к возникновению каналов утечки конфиденциальной информации и потребовать от руководства предприятия, руководителей структурных подразделений и персонала принятия мер по защите конфиденциальной информации, направленных на недопущение ее утечки и несанкционированного распространения (утраты носителей конфиденциальной информации).

Для определения необходимых мер по защите информации, необходимо провести классификацию всех возможных каналов утечки информации в зависимости от направлений и специфики деятельности предприятия, видов конфиденциальной информации, особенностей функционирования системы защиты информации и иных факторов.

Организационные каналы утечки конфиденциальной информации, возникающие в процессе деятельности предприятия, можно подразделить следующим образом:

- по источникам угроз защищаемой информации (внешние и внутренние);
- по видам конфиденциальной информации или тайн (государственная, коммерческая, служебная или иная тайна; персональные данные сотрудников предприятия);

- по источникам конфиденциальной информации (персонал, носители информации, технические средства хранения и обработки информации, средства коммуникации, передаваемые или принимаемые сообщения и т.п.);

- по способам или средствам доступа к защищаемой информации (применение технических средств, непосредственная и целее направленная работа с персоналом предприятия, осуществление непосредственного доступа к информации, получение доступа к защищаемой информации агентурным путем);

- по характеру взаимодействия с партнерами (каналы утечки, возникающие в отсутствие взаимодействия, при осуществлении взаимодействия, в условиях конкурентной борьбы);

- по продолжительности или времени действия (каналы утечки постоянного, кратковременного, а также периодического или эпизодического действия);

- по направлениям деятельности предприятия (каналы утечки, возникающие в обычных условиях или при повседневной деятельности предприятия, при выполнении совместных работ, осуществлении международного сотрудничества, проведении совещаний, выезде персонала за границу, в ходе рекламной и публикаторской или издательской деятельности, при проведении научных исследований или командировании сотрудников предприятия);

- по причинам возникновения каналов утечки информации (действия злоумышленников, ошибки персонала, разглашение конфиденциальной информации, случайные обстоятельства).

Далее по тексту термин «защита информации» распространяется только на информацию, в установленном порядке отнесенную к конфиденциальной информации, если иное не оговорено особо.

- по каналам коммуникации, используемым для передачи, приема или обработки конфиденциальной информации (каналы утечки, возникающие при хранении, приеме-передаче, обработке или преобразовании информации, а также в канале связи, по которому передается информация);

- по месту возникновения каналов утечки информации (каналы утечки, возникающие за пределами территории предприятия или на территории предприятия – в служебных помещениях, на объектах информатизации, объектах связи и в других местах);

- по используемым способам и методам защиты информации (каналы утечки, возникающие при нарушении установленных требований по порядку отнесения информации к категории конфиденциальной, обращения с носителями информации, ограничения круга допускаемых к информации лиц, непосредственного доступа к информации персонала предприятия или командированных лиц, а также по причине нарушения требований пропускного или внутриобъектового режимов).

Задачи по исключению возможных каналов утечки конфиденциальной информации решаются как отдельными должностными лицами (персоналом), так и структурными подразделениями предприятия, создаваемыми и функционирующими по различным направлениям защиты информации. Успешное решение этих задач невозможно без применения совокупности средств и методов защиты информации.

Среди основных направлений защиты информации наряду с организационной выделяют правовую и инженерно-техническую защиту информации. Однако организационной защите информации среди этих направлений отводится особое место.

Организационная защита информации призвана посредством выбора конкретных сил и средств, в том числе правовых и инженерно-технических, реализовать на практике спланированные руководством предприятия меры по защите информации. Эти меры принимаются в зависимости от конкретной обстановки на предприятии, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к ее утечке.

Роль руководства предприятия в решении задач по защите информации трудно переоценить. Основными направлениями деятельности, осуществляемой руководителем предприятия в этой области, являются: планирование мероприятий по защите информации и персональный контроль за их выполнением, принятие решений о непосредственном доступе к конфиденциальной информации своих сотрудников и представителей других организаций, распределение обязанностей и задач между должностными лицами и структурными подразделениями, аналитическая работа и т.д. Цель принимаемых руководством предприятия и должностными лицами организационных мер – исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.

Система мер по защите информации в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые, в свою очередь, определяются состоянием устремленности разведок противника либо действиями конкурента на рынке товаров и услуг, направленными на овладение информацией, подлежащей защите. Это правило действует как на государственном уровне, так и на уровне конкретного предприятия.

В нормативной и научной литературе используются два примерно равнозначных определения организационной защиты информации.

Организационная защита информации – составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационная защита информации на предприятии – регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

Первое из приведенных определений в большей степени показывает сущность организационной защиты информации. Второе – раскрывает ее структуру на уровне предприятия. Вместе с тем оба определения подчеркивают важность нормативно-правового регулирования вопросов защиты информации наряду с комплексным подходом к использованию в этих целях имеющихся сил и средств.

Основные направления организационной защиты информации:

1. Организация допуска и доступа к конфиденциальной информации и документам.

2. Организация работы с носителями сведений.

3. Организация внутриобъектового и пропускного режимов и охраны.

4. Организация работы с персоналом.

5. Комплексное планирование мероприятий по защите информации.

6. Организация аналитической работы по предупреждению утечки конфиденциальной информации и контроля ее осуществления.

Построение системы организационной защиты информации должно базироваться на следующих принципах:

- принцип комплексного подхода – эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;

- принцип оперативности принятия управленческих решений (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации; данный принцип направлен, в том числе, и на упреждение предполагаемых угроз целостности конфиденциальной информации);

- принцип персональной ответственности – наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.

Среди основных условий организационной защиты информации можно выделить следующие:

- непрерывность всестороннего анализа функционирования системы защиты информации в целях принятия своевременных мер по повышению ее эффективности;

- неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.

При соблюдении перечисленных условий обеспечивается наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

СПИСОК ЛИТЕРАТУРЫ

1. Организационное обеспечение информационной безопасности: учебник для студ. высш. учеб. заведений / О.А. Романов, С.А. Бабин, С.Г. Жданов. – М.: Издательский центр «Академия», 2008. – 192 с.

Жарова А.К.

Россия, Москва, ФГБУН Институт государства и права РАН

ЭЛЕКТРОННЫЕ СПОСОБЫ РАЗРЕШЕНИЯ КОНФЛИКТОВ И ЭЛЕКТРОННЫЕ СУДЫ

В статье раскрываются понятия электронные суды и электронные способы осуществления правосудия, дается отличие данных процедур. Анализируется законодательство зарубежное и РФ, обеспечивающее возможность реализации судебного процесса электронным способом.

Ключевые слова: Электронный суд. Электронные способы осуществления правосудия. Видеоконференция. Электронный документ. Интернет. Законодательство.

В то время, как большинство отношений переходят в электронную среду, остается не решенным вопрос о том насколько применимы технологии для создания основы разрешения конфликтов. В качестве ответа на данный вопрос стали развиваться системы альтернативного разрешения конфликтов, споров. Изначально такие структуры зарождалась, как аналогичные существующим процессуальным формам реализации государственного правосудия, сейчас в некоторых странах это вид государственной процедуры разрешения конфликта в электронной среде.

В зарубежной литературе [8] такую процедуру называют виртуальные суды, в нашей, российской практике их называют электронные суды. Однако не только судебная власть применяет данную процедуру, но и негосударственные структуры также предлагают услуги по разрешению конфликтов в электронной среде и их число увеличивается. Хотя не так быстро, как это происходит за

рубежом. Такие услуги включают в себя различные процедуры, формируемые по усмотрению лиц, предоставляющих услуги.

Таким образом, мы видим, что в электронной среде в целях разрешения конфликтов одновременно сосуществуют как электронные процессуальные механизмы, так и электронные способы разрешения конфликта. В качестве электронной базы, формирующей среду реализации механизмов и формы электронного процесса разрешения конфликта, могут использоваться различные технологии – мобильная связь, интернет связь, но предпочтение отдается интернету.

Некоторые авторы, считают, что между электронным способом разрешения конфликтов и электронным судом можно поставить знак равенства. Необходимо разграничить эти два понятия, т.к. электронных способов существует великое множество, например, по видам используемых технологий, в то время как электронным судом является сам процесс осуществления правосудия в электронной среде и соответственно при этом может применяться любое количество электронных технологий.

В Российском законодательстве проблемы в применении электронных судов связаны с отсутствием соответствующего нормативного регулирования.

Примером электронного способа является способ подачи электронных документов в Верховный суд РФ по сети интернет. Так, с этой целью, разработано Положение [17] в соответствии с Федеральным законом от 22 декабря 2008 года №262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации», которое определяет правила подготовки и направления пользователями запросов в Верховный Суд в виде электронного документа, их регистрации и обработки в Верховном Суде, а также правила подготовки и отправки ответов на них в электронном виде.

Однако в том же Положении указано, что ответ на запрос, данный в электронном виде, не может быть представлен в качестве официального документа, подтверждающего или устанавливающего юридически значимый факт [10].

В настоящее время десять государств-участников предусмотрели возможность подачи заявления в электронном виде, это Австрия (используется «WebERV», основанное на интернет-технологиях электронное правосудие (web-based electronic justice)), Кипр, Чешская Республика, Германия, Эстония, Финляндия, Франция, Словения, Швеция и в Соединенном Королевстве – Англия и Уэльс. [13].

Международное сообщество рассматривает создание такой новой структуры – электронные суды как средство обеспечения доверия потребителей к Интернет-услугам. Электронные суды предлагают общественности открытую систему правосудия, обеспечивают быстрое разрешение конфликтов и состоят из электронной процессуальной системы разрешения споров. Электронная процессуальная система разрешения споров может включать в себя такие элементы, как: руководство процессом и судебным разбирательством; оборот судебных документов; доступ к судебной информации; судебные извещения; правовой поиск; внутренние судебные процедуры.

Развитие системы электронных судов обусловлен причинами объективного характера – необходимостью быстрого и экономичного разрешения огромного количества конфликтов, участники которых находятся за сотни и тысячи километров друг от друга.

Примером создания электронного суда является сайт Адвокатского образования Московской области (АОМО), на котором предоставляемая бесплатная услуга, создания «виртуального» суда в составе 1–3 реальных судей из числа членов АОМО [18].

Конечно, данную услугу нельзя приравнять к полноценной процессуальной системе разрешения споров, т.к. в настоящее время в нашем государстве не создана законодательная база для применения электронного суда. Однако эта услуга позволяет построить модель виртуального суда, результатом работы которого, является мотивированное и основанное на конкретных нормах действующего законодательства решение, которое позволит участникам процесса оценить перспективы реального судебного процесса, в данном случае по гражданско-правовым спорам.

Другим примером электронного суда в РФ, является электронный третейский суд ЮНЕТ, созданный в соответствии с ФЗ РФ «О третейских судах в Российской Федерации» [7].

Электронный Третейский Суд ЮНЕТ уполномочен разрешать экономические споры и другие дела, связанные с осуществлением предпринимательской и иной экономической деятельности, используя современные информационные и телекоммуникационные технологии.

Важнейшими преимуществами третейского разбирательства в режиме он-лайн являются оперативность принятия судебных решений и независимость третейских судей, гарантированные самой технологией электронного судопроизводства.

Решения Электронного Третейского Суда ЮНЕТ, принятые в соответствии с законом, подлежат принудительному исполнению наравне с решениями государственных арбитражных судов.

Другим примером, такого суда является постоянно действующий третейский суд при некоммерческом партнерстве «Объединенная Консалтинговая Палата», созданный в 2010 году [9] Третейский суд при Некоммерческом партнерстве «Объединенная Консалтинговая Палата» осуществляет свою деятельность на основании Конституции РФ, Федерального Закона РФ от

24.07.2002 №102-ФЗ «О Третейских судах в Российской Федерации», Закона РФ от 07.07.1993 № 5338-1 «О международном некоммерческом арбитраже», Положения о Третейском суде при Некоммерческом партнерстве «Объединенная Консалтинговая Палата».

В обеспечение процедуры рассмотрения споров третейским судом при некоммерческом партнерстве «Объединенная Консалтинговая Палата» в электронной среде была разработана система «Электронное правосудие», которая может применяться в двух вариантах: с участием сторон в слушании по делу и без участия сторон в слушании по делу.

Наличие в третейском соглашении указания на применение процедуры рассмотрения спора с применением системы «Электронное правосудие» не лишает истца возможности обратиться к обычной процедуре, о чем должно быть указано в исковом заявлении.

Согласно п. 1.4. Регламента данного третейского суда при некоммерческом партнерстве «Объединенная Консалтинговая Палата» суд применяет нормы Арбитражного Процессуального Кодекса Российской Федерации (АПК РФ) в части, касающегося общих положений и искового производства ко всем категориям дел.

На странице данной организации указано, что подача искового заявления осуществляется путем заполнения специальной формы, размещенной на странице.

В случае принятия материалов суд направляет сторонам Определение о принятии дела к производству посредством телеграфного уведомления, дополнительно, истцу Определение направляется посредством электронной почты отдельно сформированным файлом в формате pdf. Тот же способ используется при оставлении заявления без рассмотрения. Место разбирательства по делу может проходить в месте, определенном сторонами в третейском соглашении, но на территории России.

В 2002 году Европейская экономическая комиссия ООН (ЮНЕСЕ) организовала в Женеве первый Форум по вопросам разрешения споров в электронной среде. В этом мероприятии приняли участие представители следующих международных организаций: Организация экономического сотрудничества и развития, Международный союз электросвязи; Международная торговая палата; Всемирная Организация Интеллектуальной Собственности; Конференция ООН по торговле и развитию; Комиссия ООН по праву международной торговли, а также представители научного сообщества, торгово-промышленных палат и государственных структур со всего мира. Данное мероприятие проводится ежегодно.

Комиссия Европейских Сообществ в Зеленой книге по вопросам альтернативного разрешения гражданско-правовых и коммерческих споров, представленной 19 апреля 2002, определила в качестве стимула развития электронного правосудия – легкость в вовлечении в качестве сторон лиц, находящихся в разных государствах, что особенно актуально для коммерческих споров [4].

Применение системы электронного суда позволит выстроить более рационально и эффективно внутренние организационно-процессуальные отношения между судами и внутри судов, а также между судами, гражданами и организациями.

В России развивается система подачи документов в арбитражные суды Российской Федерации в электронном виде, конечно, эти действия не являются примером ведения суда в режиме онлайн, но в тоже время это механизмы, обеспечивающие организацию в дальнейшем таких судебных заседаний. Регламент подачи документов в арбитражные суды в электронном виде сформировался после вступления в силу Федерального закона «О внесении изменений в Арбитражный процессуальный кодекс Российской Федерации» от 27 июля 2010 года [23], но и до этого времени ст. 41 АПК РФ определялось, что лица, участвующие в деле вправе представлять в арбитражный суд документы в электронном виде, заполнять формы документов, размещенных на официальном сайте арбитражного суда в информационно-телекоммуникационной сети «Интернет», в порядке, установленном в пределах своих полномочий Высшим Арбитражным Судом Российской Федерации [24]. Введен временный порядок подачи документов в Арбитражные Суды РФ в электронном виде [25], разработанный в целях реализации положений АПК РФ. Представление документов иными способами, включая направление их по электронной почте, а равно представление документов, которые содержат сведения, составляющие государственную тайну, настоящим Порядком не регулируется.

С октября 2011 года в Высшем арбитражном суде доступна подача исковых заявлений, апелляционных, кассационных жалоб, заявлений о пересмотре судебных актов в порядке надзора, отзовов и иных заявлений и ходатайств, в том числе документов по делам о банкротстве, расширен список иных документов [22]. Высший Арбитражный Суд РФ к системе электронного правосудия относит обмен документами между арбитражными судами в электронном виде, получение информационных данных о движении дел в режиме реального времени, о судебных делах не только с помощью компьютера, но и с помощью мультимедийных смартфонов iPhone [19], а также доступ к другим функциям электронного документооборота. Но, однако, сама процедура судебного процесса в электронной среде пока не раскрывается.

Можно привести пример судебного решения по вопросу о соблюдении права на доступ к правосудию. Так, в данном деле обжаловался отказ судов в принятии исковых заявлений, поданных

компанией-заявителем в электронной форме [16]. Суть конфликта состояла в том, что в 2005 году заявитель – частная компания с ограниченной ответственностью, намеревалась подать свыше 70000 исков о взыскании задолженности. С учетом числа заинтересованных лиц компания-заявитель оформила иски в электронной форме и записала их на цифровой диск, который направила в компетентные районные суды с сопроводительным письмом. Однако суды отказались принимать исковые заявления со ссылкой на отсутствие оборудования для получения и обработки материалов, составленных и подписанных в электронной форме. Компания-заявитель подала на каждый отказ жалобы в Конституционный Суд, ссылаясь на право доступа к правосудию. Жалобы заявителя были отклонены как поданные по истечении установленного двухмесячного срока. Хотя установленный срок был соблюден в отношении частных жалоб, Конституционный суд посчитал, что течение соответствующего срока началось с момента, когда компания-заявитель узнала об отказе судов в принятии исковых заявлений в электронном виде.

Европейский Суд по данному делу определил, что компания-заявитель подала или намеревалась подать большое количество исков, затрагивающих десятки тысяч человек. В случае подачи в печатном виде исковые заявления и приложенные документы заняли бы свыше 40 миллионов страниц. При таких обстоятельствах выбор средств подачи исковых заявлений не может рассматриваться как процессуальное злоупотребление или ненадлежащий с иной точки зрения. Кроме того, с 2002 года национальное законодательство допускает подачу исковых заявлений в электронной форме, и компании-заявителю не могло быть поставлено в вину использование этой возможности. Отказ судов в принятии их исков создал несоразмерные ограничения права представить свои дела эффективным способом.

В порядке применения статьи 41 Конвенции о защите прав человека и основных свобод [14] Европейский Суд присудил выплатить компании-заявителю 10000 евро в счет компенсации причиненного материального ущерба и морального вреда.

Несмотря на положительные примеры, применения электронных способов в целях осуществления правосудия мы не можем утверждать, что эти способы и есть электронный суд, т.к. осуществлению судебной деятельности в сфере организации электронного суда требуется уточнение процессуального принципа устности и непосредственности, например, идентификации и установление личности лица.

Кроме того, для полноценной реализации процедуры электронного суда необходимо исключить следующие возможные информационные риски:

1. Изменение информации, в том числе и в процессе ее передачи, например, при транслировании суда способом видеоконференции.
2. Подтверждение подлинности полученных документов по каналам связи, как со стороны суда, так и со стороны пользователей таких услуг.
3. Беспрепятственный доступ к судебной информации, которую суды обязаны размещать.

На это указывал В.В. Ярков, так использование видеоконференции потребует коррекции законодательства в части принципа непосредственности. Например, присяга свидетеля с подписью в протоколе (ч. 4 ст. 56 АПК РФ) потребует изменения формы подписи. По иному необходимо подойти и к процедуре фиксации в протоколе отказа от иска или признания иска в судебном заседании, в котором одна из сторон или обе участвуют в режиме видеоконференции. В таком случае фиксация будет производиться с использованием видео- и аудиозаписи.

При этом следует иметь в виду, что электронный документ как компьютерная информация может быть представлен на нескольких уровнях: физическом (на материальном носителе и находящаяся в процессе взаимодействия с носителем); логическом; синтаксическом; семантическом; прагматическом [12].

В. В. Ярков также пишет, что при допросе свидетеля, находящегося за рубежом, в режиме видеоконференции потребуются пересмотр всей системы судебных поручений, в настоящее время основанной на письменной их форме согласно Гаагским конвенциям, многосторонним и двусторонним договорам о правовой помощи [26].

Обеспечение действия принципа диспозитивности также потребует пересмотра, потребуются иная проверка подлинности волеизъявления стороны. В частности, подача исков и совершение процессуальных действий через интернет, извещение сторон, другие отношения суда и участников процесса, если они будут проводиться с использованием информационных технологий, вызывают вопросы о сертификации электронной и проверке подлинности волеизъявления стороны, полученного через сеть [26].

Возможности использования технологий предоставляет и ст. 71 ГПК РФ, которая предусматривает в качестве письменных доказательств, в том числе документы и материалы, выполненные в форме цифровой, графической записи, в том числе полученные посредством факсимильной, электронной или другой связи либо иным позволяющим установить достоверность документа способом. Однако, ГПК в той же статье указывает, что письменные доказательства должны предоставляться в подлиннике или в форме надлежащим образом заверенной копии.

По мнению С.И. Семилетова, можно привести множество примеров реальных судебных процессов, когда при рассмотрении гражданских дел в процесс вовлекаются доказательства, полученные с использованием высоких технологий и технических средств, в частности: кассеты и ролики с аудио- и видеозаписями, дискеты, CD-диски, флэш-карты, жесткие диски и даже сами системные блоки компьютеров с записями файлов, сообщений в тех или иных форматах, записями баз данных, представляющих собой фактические данные текстовой, графической и фотографической, табличной, аудио- и видеодокументированной информации или их комбинации[20]. В связи с этим остается открытым вопрос о применимости доказательств «нетрадиционной формы» в процессуальной деятельности.

В. М. Елин приводит пример из законодательства США, в котором основными источниками американского права, регулирующими использование доказательств, полученных с помощью компьютера, служат принятые Федеральные правила уголовного процесса и Федеральные правила о доказательствах [1]. Кроме того, ряд положений содержится в USA Patriot Act, Federal Criminal Code Related to Computer Intrusions, многочисленных судебных прецедентах.

Федеральные правила о доказательствах не содержат непосредственного упоминания компьютерных доказательств. Однако комментарии и судебная практика позволяют утверждать, что Правила создавались с расчетом их применения к «нетрадиционным» доказательствам, к которым также относятся электронные документы.

Положения Федеральных правил о доказательствах [2] требуют предоставления информации в пригодном для использования виде. Во многих случаях таковой признается копия-распечатка содержимого файла на бумаге. Однако правило не содержит положений, запрещающих или ограничивающих использование иного формата.

Кроме того, есть пример указания Верховного Суда штата Висконсин о том, что правило подачи документов в электронном виде можно предоставлять только адвокатам или лиц, участвующих в деле и тогда можно разрешить проблему ответственного лица за распространение информации и ограничения доступа общественности при необходимости [11].

В РФ с 2002 году в Верховном Суде РФ эксплуатируется система технической фиксации судебных процессов «SRS-Femida», особенностью которой является не только качественная цифровая аудиозапись и возможность получения текстовых отчетов на компьютере, а действительно полная фиксация судебного процесса за счет получения фонограммы выступлений каждого участника и электронного протокола судебного заседания, в котором указываются все события судебного процесса и выступления участников, привязанные ко времени и непосредственно к фонограмме [21].

В зарубежной практике реализации электронного правосудия используется система видеоконференции со сторонами по делу. В РФ также имеются примеры применения видеоконференции, например, по сообщению пресс-центра Алтайского краевого суда, между Алтайским краевым судом и Свердловским областным судом был проведен сеанс видеоконференцсвязи с использованием системы ГАС «Правосудие». В Алтайский краевой суд был вызван свидетель из Бийска, который дал показания по уголовному делу, рассматриваемому Асбестовским городским судом Свердловской области. «Технические возможности позволили в режиме реального времени с соблюдением всех процессуальных норм провести допрос свидетеля. Видеоконференцсвязь прошла без сбоев и технических накладок» [6].

Положительным примером применения электронных средств, но не организации электронного суда является внедрение процедуры электронного обмена информацией Федеральным арбитражным судом Московского округа. Данная процедура введена в целях совершенствования процедуры документооборота и использования современных технологий при обмене информацией. В процессе применения данной процедуры можно получить информацию о времени и месте судебного заседания и о движении по делу, направить электронные копии судебных актов лицам, участвующим в деле и иным участникам арбитражного процесса.

Так, на сайте Федерального арбитражного суда Московского округа определено, что под электронным обменом подразумевается направление участнику арбитражного процесса судебных документов согласно нормам статей 121, 122 Арбитражного процессуального кодекса Российской Федерации по электронной почте, а также направление уведомлений участником арбитражного процесса о получении документов в суд. Электронный обмен между Федеральным арбитражным судом Московского округа и лицами, участвующими в деле или являющимися участниками арбитражного процесса осуществляется на основании Соглашения об электронном обмене, которое размещено на основной странице ФАС МО. Данное соглашение заполняется, подписывается и скрепляется печатью лицами, участвующими в деле и иными участниками арбитражного процесса и направляется в ФАС МО по почте сканированный текст подписанного соглашения с приложениями отправляется на адрес электронной почты суда, применяется и классический способ через канцелярию.

В Чешской республике также применяется процедура ведения электронного суда, например, приняты «Дополнительные процедуры для он-лайн арбитража» [5], которые содействуют арбитражному разбирательству с целью разрешения конфликтов, посредством сети интернет.

Однако для реализации данных правил необходима договоренность сторон о применении этих правил. В данном случае под он-лайн арбитражем понимается подача документов электронным способом, сама процедура разбирательства в режиме онлайн, а также вынесение арбитражного решения в режиме онлайн. Данный арбитражный суд является структурой Арбитражного суда при Экономической палате Чешской Республики и Аграрной палате Чешской Республики.

На сегодняшний день можно заключить, что информационно-коммуникационные технологии применяются не только в качестве средства коммуникации людей, но и как среда и средство осуществления различной деятельности юридическими лицами. Зарождается концепция электронного разрешения споров, целью которой является реализация принципов правосудия в электронной среде. Такую процедуру используют различные суды РФ. При этом вовлекаются в этот процесс не только они, но и все государственные структуры, так или иначе связанные с обеспечением и осуществлением правосудия. Однако на данное время все еще существуют проблемы, которые мешают реализации электронного суда.

Анализ методов реализации процесса электронного суда на территории РФ судами РФ позволяет говорить только об активном применении некоторых технологических моделей, например таких, как система электронного документооборота и в редких случаях применение видеоконференции по сети интернет. Таким образом, использование информационно-коммуникационных технологий на территории РФ в процедурах разрешения споров носит вспомогательный характер. В то время как в других странах уже активно реализуется модель ведения судебного процесса в электронной среде.

Таким образом, можно сделать вывод о необходимости внесения изменений в законодательство РФ. Можно также утверждать, что электронное разрешение конфликтов признается как международным сообществом, различными государствами, в том числе и РФ, как некоторая параллельная система, существующей государственной судебной системе. Однако, несмотря на указанные факторы, рассматриваемая форма разрешения конфликтов еще недостаточно исследована: не выработано единое понятие категории «электронное разрешение споров», нет однозначности в подходах к сущности данного явления, не существует даже единого терминологического обозначения.

Кроме того, для обеспечения применимости данной процедуры в РФ необходимо решить следующие вопросы, связанные с:

- обеспечением неприкосновенности частной жизни, конфиденциальности при проведении электронного суда;
- обеспечением справедливого и прозрачного судебного процесса;
- защитой подлинности и целостности электронных документов;
- обеспечением целостности процесса разрешения конфликтов;
- разрешением последствий цифрового неравенства;
- разрешением вопросов существующей компьютерной неграмотности;
- обеспечением качества проводимых процессов и процедуры электронного суда;
- мониторингом эффективности процессов;
- обеспечением достоверной оценки сторон, в настоящий момент существующая оценка традиционных доказательств поведения этому не способствует.

Таблица №1.

Применение электронных способов осуществления правосудия

		Реализация в РФ	Зарубежная практика
Электронные способы разрешения конфликтов	Способ подачи электронных документов	1. Положение о порядке направления, регистрации и обработки запросов, поступающих в ВС РФ. Приложение №4 к Порядку организации доступа к информации о деятельности Верховного Суда Российской Федерации, утвержденному приказом Председателя Верховного Суда Российской Федерации от 18 июня 2010 г. №10-П. определяет правила подготовки и направления пользователями запросов в Верховный Суд в виде электронного документа, их регистрации и обработки в Верховном Суде, а также правила подготовки и отправки ответов на них в электронном виде. 2. Федеральный закон «О внесении изменений в Арбитражный процессуальный кодекс Российской Федерации» от 27 июля 2010 г., и ст. 41 АПК РФ определяют, что лица, участвующие в деле вправе представлять в арбитражный суд документы в электронном виде, заполнять формы документов, размещенных на официальном сайте арбитражного суда в информационно-телекоммуникационной сети «Интернет», в порядке, установленном в пределах своих полномочий Высшим Арбитражным Судом Российской Федерации. 3. Временный порядок подачи документов в Арбитражные Суды РФ в электронном виде 4. С октября 2011 года в Высшем арбитражном суде доступна подача исковых заявления, апелляционных, кассационных	1. Десять государств-участников предусмотрели возможность подачи заявления в электронном виде, это Австрия (используется «WebERV», основанное на интернет-технологиях электронное правосудие (web-based electronic justice)), Кипр, Чешская Республика, Германия, Эстония, Финляндия, Франция, Словения, Швеция и в Соединенном Королевстве – Англия и Уэльс. 2. Суд штата Висконсин определил, что правило подачи документов в электронном виде можно предоставлять только адвокатам или лиц, участвующих в деле.

		Реализация в РФ	Зарубежная практика
		жалоб, заявлений о пересмотре судебных актов в порядке надзора, отзывов и иных заявлений и ходатайств, в том числе документов по делам о банкротстве, расширен список иных документов. 5. Возможности использования электронных технологий предоставляет и ст. 71 ГПК РФ, предусматривающая в качестве письменных доказательств, в том числе документы и материалы, выполненные в форме цифровой, графической записи, в том числе полученные посредством факсимильной, электронной или другой связи либо иным позволяющим установить достоверность документа способом. Однако, ГПК в той же статье указывает, что письменные доказательства должны предоставляться в подлиннике или в форме надлежащим образом заверенной копии. 6. Между Федеральным арбитражным судом Московского округа. Данная процедура введена в целях совершенствования процедуры документооборота и использования современных технологий при обмене информацией. В процессе применения данной процедуры можно получить информацию о времени и месте судебного заседания и о движении по делу, направить электронные копии судебных актов лицам, участвующим в деле и иным участникам арбитражного процесса.	
	Применение видео-конференции	1. Между Алтайским краевым судом и Свердловским областным судом был проведен сеанс видеоконференцсвязи с использованием системы ГАС «Правосудие». 2. С 2002 г. в Верховном Суде РФ эксплуатируется система технической фиксации судебных процессов «SRS-Femida», особенностью которой является не только качественная цифровая аудиозапись и возможность получения текстовых отчетов на компьютере, а действительно полная фиксация судебного процесса за счет получения фонограммы выступлений каждого участника и электронного протокола судебного заседания, в котором указываются все события судебного процесса и выступления участников, привязанные ко времени и непосредственно к фонограмме.	Судом штата Висконсин применяется видеоконференция. В Лондоне в судах с мая 2009 года, применяется система видеоконференции.
Электронный суд РФ	Электронная процессуальная система разрешения споров	1. Сайт Адвокатского образования Московской области (АОМО), на котором предоставляется бесплатная услуга, создания «виртуального» суда в составе 1–3 реальных судей из числа членов АОМО. 2. Электронный третейский суд ЮНЕТ, созданный в соответствии с ФЗ РФ «О третейских судах в Российской Федерации». Электронный Третейский Суд ЮНЕТ уполномочен разрешать экономические споры и другие дела, связанные с осуществлением предпринимательской и иной экономической деятельности, используя современные информационные и телекоммуникационные технологии. 3. Третейский суд при некоммерческом партнерстве «Объединенная Консалтинговая Палата», созданный в 2010 г.	В Чешской республике, приняты «Дополнительные процедуры для он-лайн арбитража». Под он-лайн арбитражем понимается подача документов электронным способом, процедура разбирательства в режиме онлайн, а также вынесение арбитражного решения в режиме онлайн. В ноябре 2000 г. Парижский центр посредничества и арбитража при содействии канадского ЭРС-провайдера eResolution создал сайт CyberCMAP для урегулирования в порядке посредничества и арбитража коммерческих споров. Но данный проект не получил своего развития, поскольку в него не поступило ни одного обращения.

СПИСОК ЛИТЕРАТУРЫ

1. Federal Criminal Code and Rules. Federal Rules of Criminal Procedure. West Group. St. Paul, Minn. 1997. P. 257, 342, 379. Federal Rules of Evidence for United States Courts and Magistrates // Federal Rules of Evidence, 2004 – 2005 Edition. Also including California Evidence Code (with selected comments), Uniform Rules of Evidence, Westlaw Electronic research guide, Report on caselaw divergence from FRE. West Group; 3d Bk & Map edition, 2004.
2. Federal Rules of Evidence. 34.
3. Virtual court' scheme backed by Ministry of Justice // <http://www.bbc.co.uk/news/uk-england-15910688>.
4. http://alanuzelac.from.hr/izborni/green_paper_eu.pdf
5. <http://en.soud.cz/rules/additional-procedures-for-on-line-arbitration-1st-june-2004>
6. <http://www.bankfax.ru/page.php?pg=55238>
7. <http://www.iunet.ru/>
8. <http://www.justice.qld.gov.au/justice-services/courts-and-tribunals/going-to-court/virtual-tour/magistrates-court-virtual-tour>
9. http://www.uc-c.ru/original_pdf/regulations.pdf
10. <http://www.supcourt.ru> // Верховный Суд РФ.
11. Zemlicka J. Milwaukee County moving toward digital document storage // Wisconsin Law Journal 27 Sept. 2011.
12. Дуленко В.А. О доказательной ценности компьютерной информации // Правовые вопросы связи, 2006, №2.

13. Исполнительное производство: традиции и реформы (под редакцией Р. Ван Рее и др.). – «Инфотропик Медиа», 2011 г.
14. Конвенция о защите прав человека и основных свобод. Рим, 4 ноября 1950 г. // Гарант.
15. Миронова С.Н. Использование возможностей сети Интернет при разрешении гражданско-правовых споров. – «Волтерс Клувер», 2010 г.
16. Постановление от 16 июня 2009 г. [вынесено IV Секцией] Компания «Лойер партнерс А.С.» против Словакии [Lawyer Partners A.S. v. Slovakia] (№54252/07 и другие) // Гарант.
17. Приложение №4 к Порядку организации доступа к информации о деятельности Верховного Суда Российской Федерации, утвержденному приказом Председателя Верховного Суда Российской Федерации от 18 июня 2010 г. №10-П. Положение о порядке направления, регистрации и обработки запросов, поступающих в ВС РФ // Гарант.
18. Сайт Адвокатские образования Московской области (АОМО) <http://www.aomo.ru/page/11>
19. Сайт Высшего Арбитражного Суда РФ, <http://www.arbitr.ru/e-justice/doc/29061.html>
20. Семилетов С.И. Использование электронных документов в качестве доказательств в судебном производстве // Гражданин и право, №1., 2007 г.
21. Соколов Ю.Н. Электронный протокол судебного заседания // Российская юстиция. 2010. №8.
22. Соловьев И. доклад на XI Форуме Государственные электронные услуги. 26 октября 2011 г., Москва.
23. ФЗ РФ О внесении изменений в Арбитражный процессуальный кодекс Российской Федерации №228-ФЗ от 27 июля 2010 г. // Гарант.
24. Абзац введен Федеральным законом от 27.07.2010 №228-ФЗ, в ред. Федерального закона от 11.07.2011 №200-ФЗ.
25. В ред. Федерального закона от 27.07.2010 №228-ФЗ «О внесении изменений в Арбитражный процессуальный кодекс Российской Федерации» // Гарант.
26. Ярков В.В. «Электронное правосудие //эж-ЮРИСТ», №41, октябрь 2006 г.

Золотенко В.А., Муханов Ю.В.

Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

**ФИЗИЧЕСКОЕ ВОСПИТАНИЕ КУРСАНТОВ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ МВД
РОССИИ В ОБЩЕЙ СИСТЕМЕ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ – ОСНОВА
БЕЗОПАСНОСТИ ОБЩЕСТВА**

Современный социальный заказ системе образования на качественную профессиональную подготовку работников правоохранительных органов, связанный со сложным и противоречивым характером процессов, происходящих в российском обществе, и усилением криминогенной обстановки, диктует необходимость разработки и внедрения такой модели подготовки курсантов образовательных учреждений МВД России, которая наряду с формированием профессиональных знаний, умений и навыков обеспечивала бы их психофизиологическую и физическую подготовленность к профессиональной деятельности для обеспечения эффективной защиты безопасности современного общества.

Деятельность сотрудника полиции протекает на фоне больших психических нагрузок. Она требует высокой профессиональной подготовленности и морально-волевых качеств. Возможность возникновения экстремальных ситуаций остро ставит вопрос о физической подготовленности каждого сотрудника полиции.

Общее содержание требований к физическому воспитанию курсантов образовательных учреждений МВД России и физической подготовке сотрудников ОВД на протяжении многих лет не изменяется, дифференцируется лишь в плане предназначения, особенностей и специфики прохождения службы [13].

Формирование адекватной системы подготовки кадров для органов внутренних дел России, требует выведение профессионального образования на качественно новый уровень. Между тем, современные преобразования, происходящие в государственной системе высшего образования, не затрагивают систему подготовки сотрудников полиции. Ведь известно, что неразрывность общества и полиции является основным постулатом государственного функционирования.

В соответствии со ст. 38 Федерального закона от 7 февраля 2011 г. №3-ФЗ «О полиции» граждане Российской Федерации, принятые на службу в полицию, проходят первоначальную подготовку в порядке, определяемом федеральным органом исполнительной власти в сфере внутренних дел [1].

Каждый сотрудник полиции обязан постоянно совершенствовать свое профессиональное мастерство и работать над повышением уровня своей нравственной, физической и правовой подготовленности. Данное условие детерминировано специфическими целями и задачами, стоящими перед полицией [8].

Специальное профессиональное обучение рядового и начальствующего состава осуществляется в центрах профессиональной подготовки, а также в образовательных учреждениях федерального органа исполнительной власти в сфере внутренних дел России при возможности создания учебной группы в установленном количестве, регламентирующим деятельность образовательного учреждения или центра профессиональной подготовки [9].

Среди основных проблем профессиональной подготовки кадров для органов внутренних дел можно выделить следующие: неопределенность целевых установок, квалификационных характеристик и требований к профессиональным и социальным качествам специалистов, текучесть кадров; гибель сотрудников, полная или временная потеря трудоспособности.

Анализ процесса физического воспитания в общей системе профессиональной подготовки сотрудников органов внутренних дел позволил выявить ряд существенных недостатков.

Во-первых, реформа профессионального образования, с одной стороны, и криминогенная обстановка в стране – с другой, предъявляют повышенные требования к профессиональной компетенции специалиста органов внутренних дел, а внедрение современных педагогических технологий идет крайне медленно.

Во-вторых, не имеют достаточного научного обоснования педагогическая, содержательная и организационная составляющая технологии обучения в рамках профессионально-прикладной физической подготовки. Наблюдается недостаток ведомственных учебных пособий, учебников по дисциплине «Физическая подготовка» как важного условия эффективности педагогических технологий. Социальная составляющая технологии физической подготовки сотрудников полиции нуждается в повышении профессиональной компетенции преподавательского состава в соответствии с современными требованиями педагогической деятельности.

В-третьих, начальный уровень физической подготовленности кандидатов на учебу и службу в органы внутренних дел является недостаточным ввиду низкой эффективности функционирования системы физического воспитания общеобразовательной школы, что накладывает дополнительную нагрузку на процесс физической подготовки в учебных заведениях и органах внутренних дел. Данные обстоятельства требуют поиска путей совершенствования системы профессиональной подготовки сотрудников полиции России [7].

Для осуществления непосредственно самого процесса обучения курсантов необходимо, прежде всего, ответить на вопрос: чему надо учить? На этот вопрос отвечает содержание образования, которое должно включать в себя систему научных знаний, практических умений и навыков, а также мировоззренческих и нравственных идей, которыми необходимо овладеть в процессе обучения.

В процессе исследования было установлено, что на процесс физического воспитания будущих специалистов воздействует ряд факторов. Это, прежде всего, состояние системы образования и научно-методического обеспечения учебного процесса в образовательном учреждении; требования к физической подготовленности курсантов; физическое развитие поступающих на службу [13].

Содержание физического воспитания курсантов должно опираться на научную теорию физического воспитания.

К ведущим научным основам физического воспитания курсантов относят: направленность на формирование разносторонне и гармонично развитой личности; построение образования на строго научной основе, раскрывающей сущность общественной жизни, способствующей формированию гражданско-патриотической позиции; системность и логичность (от простого к сложному); наличие взаимосвязи с родственными дисциплинами; отражение связи теории с практикой; соответствие возрастным и физиологическим возможностям; способствование профессиональной ориентации [9].

Перечисленные выше научные основы должны обеспечивать не только гармоничное развитие личности обучающегося, но и обуславливать необходимость обновления и совершенствования, как самого содержания физического воспитания, так и педагогического процесса.

Физическое воспитание курсантов в высших учебных заведениях организовано, и проводится согласно руководящим документам, в следующих формах: учебные физические занятия, утренняя физическая зарядка, физическая тренировка в процессе вне учебного времени. В современной теории физической культуры классифицируют две характерные формы построения занятия: урочное и неурочное [12].

Функция приоритетных знаний в области физической культуры, как считают специалисты в данной области, является основой интеллектуальных и психических новообразований личности обучающегося. Этот факт, в свою очередь, является основой активизации и мотивационной сферы личности, обеспечивающей двигательную активность, стремление к ведению здорового образа жизни и, как результат, – эффективную профессиональную деятельность при обеспечении общественной безопасности и профессиональный рост [4].

Анализ состояния физической подготовки сотрудников полиции показал, что, во-первых, сам процесс физической подготовки обучающихся направлен на решение общих задач учебно-воспитательного процесса в образовательном учреждении и на решение задач в оперативно-служебной подготовке. Формы занятий по физической подготовке направлены на поддержание высокого уровня умственной и физической работоспособности, а также развитие профессионально-значимых двигательных умений и навыков. Занятия по физической подготовке восполняют недостаток двигательной активности и физических нагрузок, возникающих у курсантов в образовательном учреждении и у сотрудников органов внутренних дел с гиподинамическим характером профессиональной деятельности.

Во-вторых, занятия по физической подготовке подразделяются на индивидуальную и служебно-прикладную (специализированную) физическую подготовку, которая характеризуется выраженной профессиональной направленностью. При этом прикладной аспект физической подготовки имеет тенденцию к увеличению как на уровнях профессионального образования, так и на этапах специализированного обучения. Необходимо обратить внимание и на влияние физической

подготовки на повышение уровня готовности курсантов в образовательных учреждениях МВД России к предстоящей профессиональной деятельности и реализации двигательного потенциала при выполнении оперативно-служебных задач, с целью обеспечения безопасности [10].

В силу нарастания данной тенденции назрела острая необходимость планомерного перехода от физического воспитания, ориентированного на обеспечение физического развития и физической подготовленности, к физкультурному образованию, связанному, прежде всего, с развитием способностей будущего специалиста к самостоятельной физкультурно-спортивной деятельности и общей культурой личности.

Таким образом, результаты проведенного анализа физического воспитания сотрудников МВД России и требований к их профессиональным качествам позволили определить следующее:

- учебные программы в образовательных учреждениях МВД России в большей степени ориентированы на решение задач обучения двигательным действиям и развития физических качеств, и, в гораздо меньшей степени, на решение задач воспитания потребностей в ценностях физической культуры для достижения жизненных и профессиональных целей;

- несогласованность нормативных требований для абитуриентов, курсантов (слушателей) и сотрудников полиции;

- установка программ на нормативы и показатели, а не на личные интересы и желания личности, в соответствии с их полом и уровнем физического развития;

- стабильность (даже косность) и единообразие форм и методов физического воспитания.

Сегодня на первый план в качестве основной цели физического воспитания выдвигается развитие физической культуры личности, содержащей в себе в значительной степени образовательный компонент, дающий возможность преемственного переключения от физического воспитания к физическому самовоспитанию, самосовершенствованию.

Юный возраст курсантов образовательных учреждений МВД России, возросший престиж профессии юриста, отсутствие жизненного опыта во многом определяют необходимость внедрения принципиально новых коррекционных педагогических технологий обучения, учитывающих несоответствие уровня развития психических и физических способностей поступающих в образовательные учреждения требованиям их будущей профессиональной деятельности. В этой связи немаловажным направлением по совершенствованию системы профессиональной подготовки специалистов для органов внутренних дел является оптимизация такого составляющего компонента, как отбор и комплектование образовательных учреждений с использованием средств физического воспитания с учетом специфики их будущей профессиональной деятельности. Данная проблема обусловлена тем, что уровень здоровья, физического развития и подготовленности выпускников общеобразовательных средних школ остается на низком уровне. Все это говорит о значимости процесса физического воспитания школьников и курсантов образовательных учреждений МВД России. Внедрение основных положений научных теорий, инновационных находок в профессиональном образовании специалистов для органов внутренних дел позволит более качественно применить имеющийся потенциал методов, приемов и средств физического воспитания в системе профессиональной подготовки специалистов, что напрямую скажется на безопасности нашего общества.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 7 февраля 2011. №3-ФЗ «О полиции». Принят Государственной Думой 28 января 2011 года.
2. Бальсевич В.К., Лубышева Л.И. Физическая культура: молодёжь и современности // Теория и практика физической культуры. – 2005. – №4.
3. Бовин Б.Г., Киселева Е.А., Калашников М.О. Профессионально-личностные качества сотрудников органов внутренних дел // Известия ГУК МВД РФ. – 2006. – №2. – С. 105-129.
4. Бондаренко К.К., Марченко В.З., Ковалева О.Н., Кривошей Н.Н. Актуальные проблемы физического воспитания в вузах на современном этапе // Организация и методика учебного процесса, физкультурно-оздоровительной и спортивной работы: материалы международной конференции. – М.: Изд-во МГУ, 2002. – 224 с.
5. Выдрин В.М. Неспециальное (непрофессиональное) физкультурное образование // Теория и практика физической культуры. – 1995. – №5.
6. Гейжан Н.Ф. Психолого-педагогические основы индивидуализации профессионального воспитания учащихся профессиональных учебных заведений: Дис. ... д-ра пед. наук. – СПб, 1995. – 251 с.
7. Иваницкий А.Т. Организационно-педагогическая система профессионального развития и саморазвития курсантов (слушателей) вузов МВД России: Дис. ... д-ра пед. наук. – СПб, 2000. – 184 с.
8. Комментарий к Федеральному закону «О полиции» / Под ред. В.М. Чибинёва. – Санкт-Петербург: «ОЦ «СоветникЪ», 2011. – 264 с.
9. Лубышева Л.И. Концепция физкультурного воспитания: методология развития и технология реализации // Физическая культура: воспитание, образование, тренировка. – 2006. – №1.
10. Фарфель В.С. Двигательные способности // Теория и практика физической культуры. – 2001. – №12.
11. Харламов И.Ф. Педагогика: Учебник. – Мн.: Университет, 2005. – 500 с.
12. Холодов Ж.К., Кузнецов В.С. Теория и методика физического воспитания и спорта: Учебное пособие. – М.: Академия, 2001. – 480 с.
13. Числов А.И. Профессионализм и деятельность сотрудников милиции: Научное издание. – СПб: СПб университет МВД России, 2001. – 176 с.

Парфенов Н.П.

Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛИЦЕЙСКИХ

Персональные данные – это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация) [1].

Полицейские также являются субъектами персональных данных, согласно той же статье 3 Федерального Закона «О персональных данных». По существующему положению, данный Федеральный закон должен был вступить в силу 1 января 2010 г. К сожалению, перед самым 2011 г. объявили, что в силу ряда причин вступление в силу этого закона откладывается еще на год.

26 июля 2011 г. президент РФ Дмитрий Медведев подписал поправки к закону «О персональных данных». Данные поправки ужесточают требования к обеспечению мер безопасности персональных данных. В частности, компаниям и индивидуальным предпринимателям необходимо использовать средства защиты персональных данных, которые прошли соответствующую сертификацию ФСБ.

Какие же необходимо применить меры, чтобы защитить персональные данные при вступлении вышеназванного закона?

В данной статье рассмотрим основные меры по обеспечению защиты персональных данных полицейских.

Ст. 19 Федерального закона «О персональных данных» обязывает все организации и предприятия принимать необходимые меры для защиты персональных данных своих работников от случайного доступа, уничтожения, изменения, блокирования, копирования, неправомерного распространения и от иных неправомерных действий.

Защита персональных данных полицейских имеет свои специфические особенности, и этому обстоятельству мне бы хотелось уделить особое внимание.

Полицейский является государственным служащим.

В соответствии с Конституцией РФ правовые и организационные основы государственной службы РФ определяются [2,3,4]: ФЗ от 27 мая 2003 г. №58-ФЗ «О системе государственной службы Российской Федерации», ФЗ от 27 июля 2004 г. №79-ФЗ «О государственной гражданской службе Российской Федерации», ФЗ от 28 марта 1998 г. №53-ФЗ «О воинской обязанности и военной службе». Система государственной службы включает в себя следующие виды государственной службы:

- государственная гражданская служба;
- военная служба.

Поддерживая постатейный комментарий к Федеральному закону от 27 июля 2006 г. №152-ФЗ «О персональных данных» М.И. Петрова мы также считаем, что при обработке, хранении и передаче персональных данных государственного служащего кадровая служба государственного органа обязана соблюдать следующие требования:

1. Обработка персональных данных государственного служащего проводится в целях обеспечения соблюдения Конституции РФ, федерального законодательства и иных нормативных правовых актов, содействия государственному служащему в прохождении государственной службы, обучении и должностном росте, обеспечения личной безопасности государственного служащего и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества, учета результатов исполнения им должностных обязанностей и обеспечения сохранности имущества государственного органа.

2. Персональные данные необходимо получать лично у государственного служащего. В случае возникновения необходимости получения персональных данных государственного служащего у третьей стороны следует известить об этом государственного служащего заранее, получить его письменное согласие и сообщить государственному служащему о целях, предполагаемых источниках и способах получения персональных данных.

3. Запрещается получать, обрабатывать и приобщать к личному делу государственного служащего не установленные федеральным законом и другими федеральными законами персональные данные об его политических, религиозных и иных убеждениях и частной жизни, о членстве в общественных объединениях, в том числе в профессиональных союзах.

4. При принятии решений, затрагивающих интересы государственного служащего, запрещается основываться на персональных данных государственного служащего, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей.

5. Защита персональных данных государственного служащего от неправомерного их использования или утраты обеспечивается за счет средств государственного органа в порядке, установленном настоящим Федеральным законом и другими федеральными законами.

6. Передача персональных данных государственного служащего третьей стороне не допускается без письменного согласия государственного служащего, за исключением случаев, установленных федеральным законом. Условия передачи персональных данных государственного служащего третьей стороне устанавливаются нормативными правовыми актами РФ.

Государственный служащий, виновный в нарушении норм, регулирующих получение, обработку и передачу персональных данных другого государственного служащего, несет ответственность в соответствии с настоящим Федеральным законом «О персональных данных» и федеральными законами, регулирующими соответствующие правоотношения в системе государственной службы.

В личное дело государственного служащего вносятся его персональные данные и иные сведения, связанные с поступлением на гражданскую службу, ее прохождением и увольнением с государственной службы и необходимые для обеспечения деятельности государственного органа.

Кроме того, в дополнение к вышесказанному, необходимо соблюдать следующие принципы обработки персональных данных:

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных осуществляется только для достижения конкретной, заранее определенной законной цели.

3. Нельзя объединять базы данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. При обработке персональных данных необходимо обеспечить точность персональных данных, их достаточность и актуальность по отношению к целям обработки персональных данных.

5. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

6. Обрабатываемые персональные данные должны быть уничтожены по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

В основном, специфические особенности защиты персональных данных обусловлены условиями прохождения службы сотрудниками полиции и вытекают из положений нижеперечисленных нормативно-правовых документов:

– Конституция РФ (Статья 23, 24).

– Трудовой кодекс РФ (Глава 14).

– Федеральный закон «О полиции».

– Федеральный закон №152-ФЗ «О персональных данных» от 27 июля 2006 г.

– 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.

– Положение «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждено постановлением Правительства Российской Федерации №687 от 15 сентября 2008 г.

– Приказ Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия №154 «Об утверждении Положения о ведении реестра операторов, осуществляющих обработку персональных данных» от 28 марта 2008 г.

– «Порядок проведения классификации информационных систем персональных данных», утверждён приказом ФСТЭК России, ФСБ России и Мининформсвязи России №55/86/20 от 13 февраля 2008 г.

– Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержден приказом Гостехкомиссии России №282 от 30 августа 2002 г. (ДСП).

– №128-ФЗ «О лицензировании отдельных видов деятельности» от 8 августа 2001 г.

– Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.

– «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных, вне информационных систем персональных данных», утверждены постановлением Правительства Российской Федерации №512 от 6 июля 2008 г.

– Приказ Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия №154 «Об утверждении Положения о ведении реестра операторов, осуществляющих обработку персональных данных» от 28 марта 2008 г.

– «Порядок проведения классификации информационных систем персональных данных», утверждён приказом ФСТЭК России, ФСБ России и Мининформсвязи России №55/86/20 от 13 февраля 2008 г.

- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержден приказом Гостехкомиссии России №282 от 30 августа 2002 г. (ДСП).
 - Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15 февраля 2008 г. (Пометка «для служебного пользования» снята Решением ФСТЭК России от 16 ноября 2009 г.).
 - Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК, 2008 г. (Пометка «для служебного пользования» снята Решением ФСТЭК России от 11 ноября 2009 г.).
 - Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных. ФСТЭК, 2008 г. (Пометка «для служебного пользования» снята Решением ФСТЭК России от 11 ноября 2009 г.).
 - Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации от 21 февраля 2008 г.
 - Типовые требования, по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных от 21 февраля 2008 г.
- Невыполнение требований вышеназванных документов может привести к конфликту с государственными органами, осуществляющими контроль и надзор в данной сфере деятельности, и привлечению организации или ее руководителя к административной или иным видам ответственности.
- Возможны также гражданские иски, принудительное приостановление или прекращение обработки персональных данных, при определенных условиях возможно приостановление деятельности или аннулирование лицензий.
- Согласно ст. 24 Федерального Закона «О персональных данных» на лиц, виновных в нарушении его требований, возлагается гражданская, уголовная, административная, дисциплинарная и иная предусмотренная законодательством Российской Федерации ответственность.
- На настоящий момент предусмотрена следующая административная ответственность для операторов персональных данных:
- за нарушение установленного законом порядка сбора, хранения, использования или распространения персональных данных: на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей (ст. 13.11 КоАП РФ);
 - за разглашение информации, доступ к которой ограничен федеральным законом, лицом, получившим к ней доступ в связи с исполнением служебных или профессиональных обязанностей: на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц – от четырех тысяч до пяти тысяч рублей (ст. 13.14 КоАП РФ);
 - за отказ в предоставлении, несвоевременное предоставление, предоставление неполной или заведомо недостоверной информации: гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина в размере от пятисот до одной тысячи рублей (ст. 5.39 КоАП РФ).
- Преступлениями, влекущими за собой уголовную ответственность, являются:
- незаконные сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации – наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев (ст. 137 УК РФ);
 - неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан – наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет (ст. 140 УК РФ);
 - неправомерный доступ к охраняемой законом компьютерной информации, содержащейся на машинном носителе, в электронно-вычислительной машине, системе ЭВМ или сети, если это деяние повлекло за собой уничтожение, блокировку, модификацию, либо копирование информации, нарушение работы ЭВМ, системы или сети – наказываются штрафом в размере до двухсот тысяч

рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет (ст. 272 УК РФ).

Таким образом, закон четко гласит, что лица, виновные в его нарушении, несут гражданскую, административную, уголовную ответственность, предусмотренную законами Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. ФЗ №152 «О персональных данных» от 27.07.2006 г.
2. ФЗ №58-ФЗ «О системе государственной службы Российской Федерации» от 27 мая 2003 г.
3. ФЗ №79-ФЗ «О государственной гражданской службе Российской Федерации» от 27 июля 2004 г.
4. ФЗ № 53-ФЗ «О воинской обязанности и военной службе» от 28 марта 1998 г.

Пономаренко А.В.

Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПУТИ ДОСТИЖЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБЩЕСТВА РОССИИ

Для достижения успешного развития России в современных условиях необходимо ориентироваться на адаптацию всех государственных структур, приоритетов, ценностей, институтов в соответствии с требованиями информационного общества.

Информатизация считается прорывом в будущее. На это пошли все развитые страны, придав информатизации высшие приоритеты, подчинив этой цели основные ресурсы и усилия. Информатизация превратилась в критерий оценки могущества и фактор выживания той или иной страны в борьбе за экономическое и политическое превосходство, стала важнейшим ориентиром для выработки внутренней и внешней стратегии государства.

Информатизация вступила в стадию индустриализации. Индустриализация получения и обработки информации означает создание и развитие крупного машинного производства в информационной сфере. В области развития информационной сферы человечество столкнулось с проблемами индустриализации получения и обработки информации, психологическими, экономическими, социальными правовыми, и др.

Эти проблемы порождены противоречиями между необходимостью современного использования во всех сферах человеческой деятельности больших объемов информации и невозможностью оперативно формировать такие объемы с помощью традиционных информационных средств, технологий и систем связи.

К психологическим проблемам следует отнести в первую очередь проблему готовности населения к переходу в информационное общество.

Экономические проблемы обусловлены переходом к экономике информационного общества.

Социальные проблемы связаны с коренным изменением образа жизни общества под воздействием информатизации.

Правовые проблемы возникают в связи с превращением информации в основные ресурсы развития общества. Возникают новые виды правонарушений, которые свойственны лишь информационной сфере.

Данные проблемы необходимо решать через воспитание и обучение новых специалистов, а также создания информационно-правового поля жизнедеятельности общества.

В настоящее время ощущается огромная нехватка специалистов способных разобраться на достаточно высоком профессиональном уровне в вышеперечисленных вопросах. В этих условиях необходимо особое внимание уделять подготовке юристов в совершенстве владеющих современными информационными технологиями. Данную проблему возможно решить при подготовке юристов с техническим уклоном, где существует солидная юридическая и информационно-компьютерная подготовка. Базовой дисциплиной должен стать курс правовой информатики, опирающийся на знания, полученные обучающимися по различным дисциплинам, читаемым в вузе.

В этой связи назрела необходимость создания фундаментального курса правовой информатики, обеспечивающего с правовых и логико-математических позиций развитие информатизации правовой системы России. В настоящее время рядом авторов предлагается видение решения данной проблемы.

В учебнике О.А. Гаврилова [1] «Курс правовой информатики» обобщается его многолетний опыт научно-исследовательской и практической работы в сфере правовой информатики и кибернетики. Важно отметить, что автор убедительно показывает на конкретных примерах роль и значение математической логики для формализации нормативных текстов. При этом учебник не перегружен избыточными профессиональными терминами и понятиями; программа курса изложена достаточно ясно и вполне доступно для студенческой аудитории. Одна из важных особенностей состоит в том, что автору курса правовой информатики удалось добиться плавного перехода в подаче материала от курса математики к юридическим дисциплинам.

Автор сделал попытку охватить весь круг проблем, включая некоторые частные вопросы. Обобщая понятия «информация», «информатизация», «правовая информация» он справедливо отмечает их возрастающую роль не только в действующем законодательстве, но и в общей теории права. При этом акцент делается на понятиях информационных правовых отношений и информационно-правовых норм. Кроме того, автор всесторонне анализирует концепцию информатизации правовой сферы России, к которой он относит наряду с компьютеризацией, деятельность СМИ, опубликование официальных текстов нормативно-правовых актов, деятельность юридических органов и учреждений по распространению правовой информации, обучение и переобучение кадров, развитие научных исследований. Вместе с тем учебнику присущ один существенный недостаток. Студентам, как известно, принято преподавать уже устоявшиеся формулировки истины, отработанные и признанные в большинстве теоретических работ. Между тем, автор произвольно ввел понятие федерального информационного права. Однако, как известно, дискуссии по поводу формирования новой отрасли права продолжаются и существуют несколько достаточно взвешенных подходов к определению единого информационно-правового пространства.

Учебник «Информационное право», подготовленный коллективом авторов под редакцией академика РАН Б.Н. Топорнина [2] систематизирует накопленный опыт преподавания в Санкт-Петербургском университете МВД РФ и др. вузах, охватывая все направления изучаемые в рамках информационного права, что позволит проводить подготовку специалистов в области разработки законодательной базы в сфере информатизации, контроля за информационными потоками и т.д.

Особо необходимо отметить, что через весь учебник проходит красной нитью мысль о том, что приоритетным направлением развития законодательства Российской Федерации должна стать проблема охраны прав человека в условиях формирования информационного общества.

В учебнике особое внимание уделено вопросам, недостаточно разработанным в законодательстве РФ: реализации права на информацию; формированию эффективной системы информирования общества и совершенствованию функционирования СМИ; совершенствованию законодательства в области предпринимательства, прежде всего в части новых видов деятельности, таких, как электронная торговля, работа, обучение; дальнейшей либерализации рынков информационных продуктов, технологий и услуг, развитию конкуренции; защите персональной тайны; охране интеллектуальной собственности; улучшению сетевого доступа к информационным ресурсам и защите информации в сетях передачи данных.

И.Л. Бачило [3] выдвигает идею гиперсистемного правового образования – информационно-компьютерного права, регулирующего сферу, в которой реализуется информационный процесс и происходит информационное обеспечение.

В.А. Копылов [4] отстаивает понятие информационного права как системы норм и отношений, возникающих в информационной сфере, хотя, в настоящее время речь следует вести о развитии информационно-электронного права, которое представляется совокупностью правовых норм и институтов, складывающихся по поводу использования информационно-электронных технологий хранения информации, а также развития и применения био- и психокомпьютерных систем.

Существуют и некоторые другие авторы, работающие в области указанной выше проблемы: Наумов В.Б., Снетков В.Н., Пономаренко А.В., Федотов М.А., Юсупов Р.М. [5,6,7,8].

Приведенный ряд авторов практически полностью исчерпывает список ученых работающих в данном направлении, что вызывает определенные трудности в преподавании дисциплины «Правовая информатика».

Зачастую курс правовой информатики преподается на втором курсе. Опыт показывает, что студенты не готовы к восприятию данного материала, в силу отсутствия знаний по многим отраслевым дисциплинам: уголовное право, криминалистика, административное право и некоторым другим. Место данной дисциплины на четвертом курсе.

В настоящее время многие авторы обращаются к теме «информационное право», существуют курсы лекций, учебные пособия в рамках которых охвачены все направления, изучаемые в области информационного права, что позволит проводить подготовку специалистов в области разработки законодательной базы в сфере информатизации, контроля за информационными потоками и т.д. При этом необходимо понимать, что потеря контроля за информационными потоками на государственном уровне по последствиям может сравниться с последствиями разрушения единой энергетической, транспортной и иных систем жизнеобеспечения государства.

Для перехода к информационному обществу наряду с подготовкой специалистов необходимо совершенствовать законодательную базу. К настоящему времени основные направления развития законодательства в информационной сфере определены, в основном соответствуют зарубежной практике правового регулирования информационных отношений и осуществляются в соответствии с международно-правовыми требованиями к обеспечению

свободы слова и иных прав и законных интересов граждан в области производства, хранения и распространения информации.

В России интенсивное использование зарубежных технологий опережает реакцию законодателя, которому требуется время для адекватной регламентации в законах и иных нормативно-правовых актах отношений, возникающих в рассматриваемой сфере. Кроме того, очень важно разумно учитывать опыт других государств, которые, значительно раньше приступив к освоению информационного пространства и в частности в борьбе с преступлениями в сфере высоких технологий, выработали систему эффективных правовых средств этой борьбы.

На современном этапе законодательные инициативы должны затрагивать два основных направления регулирования в информационной деятельности общества: информационное экономическое право (регулирует порядок осуществления в информационной сети электронной экономической деятельности: электронной торговли, интернет-банкинга, электронного консалтинга, электронного рекламинга, интернет-страхования и т.д.); информационное гуманитарное право (регулирует порядок осуществления в информационной сети электронной гуманитарной деятельности по обеспечению государством реализации информационных прав физических лиц, в том числе путем создания и функционирования систем электронного администрирования). Одним из направлений здесь является внедрение и развитие существующих более чем в 30 странах мира так называемых систем электронного правительства (управления). На необходимость принятия соответствующей концепции и развития системы электронного правительства уже неоднократно указывалось в работах различных авторов, ведущих специалистов по информационному праву и это возымело действие. К 2017 году поэтапно предполагается выдать всем дееспособным гражданам России пластиковую карту, с помощью которой можно будет совершить большинство уведомительных, регистрационных и платежных операций через инфоматы. В рамках этой системы реализация прав граждан на оказание им публичных услуг осуществляется органами государства с помощью глобальных компьютерных сетей. В частности, уже сейчас граждане получают возможность через специальные сайты государственных органов в сети Интернет получать доступ к соответствующей публичной информации о деятельности этих государственных органов, обращаться с жалобами и обращениями, направлять заявки на выдачу всевозможных справок, разрешений, оказание услуг социального характера.

Указанная система должна способствовать упрощению диалога между обществом и властью, повышать эффективность и адресность государственного и муниципального управления. Другим направлением выступает обеспечение государством информационных прав граждан, в том числе на свободный оборот незапрещенной (находящейся в открытом доступе) информации, ее сбор, обработку и распространение в электронной форме.

Необходимо также создание и совершенствование сетевого законодательства, регулирующего: сетевые безналичные расчеты для подготовки перехода к электронным деньгам, сетевое взаимодействие для дистанционного заключения договоров, сетевое разрешение споров в виртуальных процессах и многое другое.

Особо необходимо отметить, что приоритетным направлением развития законодательства Российской Федерации должна стать проблема охраны прав человека в условиях формирования информационного общества. Особое внимание необходимо уделять вопросам недостаточно разработанным в законодательстве РФ: реализации права на информацию; формированию эффективной системы информирования общества и совершенствованию функционирования СМИ; совершенствованию законодательства в области предпринимательства, прежде всего в части новых видов деятельности, таких, как электронная торговля, работа, обучение; дальнейшей либерализации рынков информационных продуктов, технологий и услуг, развитию конкуренции; защите персональной тайны; охране интеллектуальной собственности; улучшению сетевого доступа к информационным ресурсам и защите информации в сетях передачи данных.

И естественно, информация, превращаясь в основные ресурсы развития общества должна защищаться государством. С этой целью законодательство обязано стоять на страже интересов граждан, обеспечивать правовую защиту на всех уровнях взаимодействия в новых условиях жизнедеятельности информационного общества.

СПИСОК ЛИТЕРАТУРЫ

1. Гаврилов О.А. Курс правовой информатики: Учебник для вузов. М.: Норма, 2000.
2. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник / Под ред. Б.Н.Топорнина. СПб.: Юридический центр «Пресс», 2001.
3. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник. 2 – е изд. изм. и доп. М.: Юридический центр «Пресс», 2005.
4. Копылов В.А. Информационное право. Учебник. 2-е изд., перераб. и доп. М.: Юристъ, 2003.
5. Наумов В.Б. Книга Право и Интернет: очерки теории и практики. М.: Книжный дом «Университет», 2002.
6. Снетков В.Н., Пономаренко А.В. Власть в обществе и информационная политика. СПб.: Изд-во СПбГТУ, 2001.
7. Федотов М.А. Право массовой информации в Российской Федерации. М.: Международные отношения, 2002.
8. Юсупов Р.М., Заболотский В.П. Научно-методические основы информатизации. СПб.: Наука, 2000.

Примакин А.И.

**Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
О НЕКОТОРЫХ ОСОБЕННОСТЯХ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БАЗЕ САНКТ-ПЕТЕРБУРГСКОГО
УНИВЕРСИТЕТА МВД РОССИИ**

Анализ статистических данных о преступлениях, совершаемых в сфере компьютерной информации, показывает, что в России, начиная с 2000-х годов, наблюдалось ежегодное удвоение числа зарегистрированных преступлений: 2001 год – 3 тысячи, 2002 год – 6 тысяч, 2003 год – 12 тысяч. С 2004 года ежегодно регистрируется порядка 15 тысяч киберпреступлений. Причем, большая их часть совершается с использованием вредоносных компьютерных программ, а также специфических возможностей операционных систем, позволяющих получать удаленный доступ к информационным ресурсам пользователей.

Очевидно, что сегодня проблема защиты граждан, их прав и свобод от преступных посягательств с использованием новых информационных технологий стоит как никогда остро.

Начало активной работы по организации противодействия правонарушениям в сфере информационных технологий можно отнести к концу 90-х годов прошлого века. Впервые подразделение по борьбе с преступлениями в сфере высоких технологий в МВД России было создано в 1998 году. С января 2002 года начала свою работу линия «К» (борьба с киберпреступностью).

В 2008 году на территории России было возбуждено более 5,5 тысячи уголовных дел, связанных с незаконной деятельностью в сфере информационных технологий. Это более чем на 20% превышает уровень 2007 года. К примеру, только в январе-мае 2009 года ОВД еженедельно возбуждали от 50 до 100 уголовных дел. За шесть месяцев этого года было зарегистрировано 11333 преступления [1].

В 2006 году Санкт-Петербургским университетом МВД России получена лицензия на подготовку специалистов по специальности 090103.65 – организация и технология защиты информации. Первый набор слушателей на факультет заочного обучения был осуществлен в 2009 году, причем, отбирались на обучение действующие сотрудники ОВД, имеющие уже высшее образование, и в силу своих служебных обязанностей занимающиеся вопросами обеспечения информационной безопасности. Следующий набор слушателей на специальность 090103.65 в 2010 году происходил на базе среднего специального образования.

Опыт работы при подготовке специалистов в области информационной безопасности показал, нужно разработать такие методы учебно-воспитательной работы, где бы гармонично сочеталось обучение современным информационным технологиям с формированием высоких нравственных качеств для выработки иммунитета к совершению компьютерных преступлений. Далеко не каждый способен удовлетворить этим требованиям. Наиболее эффективны, с этой точки зрения, могут быть методы предварительного тестирования абитуриентов, поступающих на соответствующую специальность.

В качестве примера, можно привести профотбор, дистанционно проводимый на сервере Академии ФАПСИ (www.academ.fnnnet.ru) по четырем факторам [2]:

1 фактор – оценка мотивационных аспектов личности (тест «Мотивация») определение мотивов выбора профессии, устойчивость профессиональной направленности, ценностные ориентации и морально-нравственные установки;

2 фактор – оценка психологической устойчивости личности к противоправным деяниям – изучение «психологической наследственности»;

3 фактор – оценка познавательной активности кандидата «Творческий потенциал». Оценивается уровень развития познавательных способностей личности, определяющих не только успешность приобретения новых знаний, умений и навыков, но и способность к применению их в практической деятельности. Дополнительный анализ общеобразовательной подготовленности кандидата позволяет реально оценить его шансы на поступление в учебное заведение.

4 фактор – оценивает активность личности в достижении поставленной цели («Целеустремленность», «Готовность к риску»), умение объективно оценивать ситуацию и людей, умение вырабатывать оптимальную стратегию поведения.

Кафедра специальных информационных технологий и информационной безопасности Санкт-Петербургского университета МВД России предлагает, в рамках внедрения инновационных технологий в учебный процесс, работу, посвященную созданию компьютерной системы тестирования, инвариантной предметной области ее использования [3].

Разработанная программная оболочка предназначена для контроля знаний учащихся по различным учебным дисциплинам, преподаваемым в Санкт-Петербургском университете МВД России, однако, реализованные в работе принципы контроля знаний могут быть использованы и в любой другой предметной области.

Система может быть использована в таких случаях обучения и переобучения, когда требуется однозначная дифференцированная оценка знаний тестируемого для последующего принятия решения о направлении его текущей подготовки или об изменении дальнейших планов обучения.

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

В предлагаемой системе мониторинга знаний в полном объеме реализованы возможности классической формы тестирования, а также некоторые специфические функции, воплотившиеся в жизнь благодаря применению компьютера. Это такие функции как собственный бал или вес вопроса в тесте и введение для каждого вариантов ответов на вопрос шкалы степени уверенности в правильности выбранных альтернатив ответов.

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

Вторая специфическая функция позволяет учесть эмоциональное состояние тестируемого относительно правильности своего ответа, что достигается путем указания степени его уверенности. Таким образом, неуверенный неправильный ответ позитивнее скажется на результате чем одновременно уверенный и неправильный ответ. В то же время неуверенный правильный ответ даст худший результат, чем мог бы дать уверенный правильный ответ. Данная специфическая функция позволит тестируемому сформировать определенную тактику поведения во время прохождения теста и будет развивать в нем качества, необходимые для умелого лавирования и рационального использования твердо усвоенных знаний. Предложенная компьютерная система тестирования сотрудников ОВД позволяет практически реализовать преимущества применения новых информационных технологий (инновационных технологий) и систем модульного и дистанционно-модульного обучений.

Помимо вопросов связанных с тестированием, практика обучения слушателей позволила сформулировать ряд условий, реализация которых обеспечит качественную подготовку специалистов в области защиты информации.

1. Обеспечение тесной связи учебного процесса с научными исследованиями в области информационной безопасности.

Как известно, качество обучения во многом определяется глубиной соответствующих научных исследований. Чрезвычайная наукоемкость информационных технологий требует привлечения большого числа специалистов и мощного технического обеспечения. Исследования в области информационной безопасности до недавних пор проводились только в закрытых и военных вузах. Стремительное развитие информационных технологий стимулирует вузы к интенсивному накоплению собственного опыта, созданию своих научных школ.

Касаясь темы организации и проведения международных и межрегиональных форумов, хотелось бы отметить, что на базе Санкт-Петербургского университета МВД России в рамках конференций «Информационная безопасность регионов России» и «Региональная информатика» существует секция «Правовые аспекты информационной безопасности», в работе которой активное участие принимают курсанты и слушатели соответствующего профиля подготовки. Общение с ведущими специалистами в вопросах информационной безопасности играет исключительно полезную роль в формировании будущих сотрудников полиции. Так, 28–30 октября 2009 года в рамках VI Санкт-Петербургской межрегиональной конференции с особым интересом был заслушан и обсужден доклад «О праве в свете становления информационного общества» заведующей сектором Информационного права Института Государства и права РАН, доктора юридических наук, профессора, заслуженного юриста РФ Бачило Илларию Лаврентьевны. В итоговых документах конференции секция рекомендовала отразить:

- необходимость совершенствования нормативно-правового регулирования процессов развития информационного общества и обеспечения информационной безопасности;
- важность и актуальность разработки единого федерального глоссария терминов и определений (правовых дефиниций) в сфере информационной безопасности;
- усиление внимания к изучению возможных негативных последствий влияния «социально-вредной» информации;
- необходимость включения в образовательные стандарты нового поколения вопросы информационного права и информационной безопасности, включая институты тайн и конфиденциальности информации.

2. Материально-техническое обеспечение учебного процесса.

Дополнительные трудности при подготовке специалистов по защите информации возникают и из-за жесткости существующих требований к материально-техническому обеспечению учебного процесса. Практические и лабораторные занятия должны проводиться в специально оборудованных помещениях, с применением современной вычислительной техники. Для обеспечения занятий по циклу дисциплин специализации нужны специальные технические средства (закладные устройства, сканирующие радиоприемники, приборы ночного видения, портативные металлодетекторы и т.д.). Значительных затрат требует лицензионное программное обеспечение, расходные материалы, доступ в Интернет.

В связи с открытием и первым набором слушателей (июнь 2009 г.) по двум новым специальностям: 090103 – «Организация и технология защиты информации» и 230201 – «Информационные системы и технологии» возникла потребность обеспечить проведение на высоком и качественном уровне большого количества дисциплин технического профиля, которые так или иначе связаны с информационными технологиями.

К таким учебным дисциплинам относятся:

– «Информационная безопасность и применение информационных технологий в борьбе с преступностью»;

– «Средства и системы технического обеспечения обработки, и передачи информации»;

– «Организационная защита информации»;

– «Программно-аппаратная защита информации»;

– «Инженерно-техническая защита информации»;

– «Комплексная система защиты информации на предприятии»;

– «Применение информационных технологий в аналитической разведке»;

– «Компьютерные информационные системы»;

– «Надежность информационных систем»;

– «Специальные информационные технологии в правоохранительной деятельности» и другие.

Со стороны кафедр «Специальных информационных технологий» и «Информационной безопасности и математических методов» было предложено и включено в план развития учебно-материальной базы Санкт-Петербургского университета МВД России создание лаборатории «Технические средства разведки и защиты информации» с приобретением комплекса оборудования для проведения лабораторных практических работ [4].

1. Лабораторный комплекс «Сетевая безопасность».

Комплекс предназначен для проведения лабораторно-практических работ для учащихся высших, средних специальных и профессионально-технических учебных заведений с целью овладения механизмами защиты проводных и беспроводных компьютерных сетей.

Позволяет обеспечить проведение лабораторных работ по учебным дисциплинам:

– организационная защита информации;

– программно-аппаратная защита информации.

2. Лабораторный комплекс «Интеллектуальная система управления доступом к объектам» (ACS).

Лабораторный комплекс предназначен для проведения лабораторно-практических работ для учащихся высших, средних специальных и профессионально-технических учебных заведений с целью получения опыта и навыков в области работы с программно-аппаратным обеспечением распознавания биометрических данных (отпечатки пальцев, ладоней и образы лиц) и построения на его основе систем управления доступом к объектам.

Лабораторный комплекс позволяет обеспечить проведение лабораторных работ по учебным дисциплинам:

– комплексная система защиты информации на предприятии.

На основе данного комплекса можно провести комплекс лабораторных работ:

– управление сканером смарт-карт и электрозамком;

– управление сканером отпечатков пальцев и электрозамком;

– технологии распознавания образов;

– удаленное управление системой доступа с использованием сетей GSM;

– разработка комбинированной системы управления доступом.

С целью проведения практических занятий в рамках учебной дисциплины «Применение информационных технологий в аналитической разведке» предлагается доукомплектовать представленную выше лабораторию следующей аппаратурой:

– устройства активной защиты информации (генераторы шума для защиты от ПЭМИН, которые встраиваются в системный блок компьютера и обеспечивают маскировку ПЭМИН средств вычислительной техники путём формирования и излучения в окружающее пространство электромагнитного поля шума и наведения маскирующего сигнала в отходящие цепи и инженерные коммуникации);

- устройства виброакустической защиты (Генератор виброакустических помех для защиты помещений от аппаратуры съема речевых сигналов, использующей вибропреобразователи на стенах, потолках, окнах, воздухопроводах прослушиваемого помещений);
- поисковые приборы (Быстрое автоматическое обнаружение сигналов, излучаемых нелегальными радиопередатчиками и подавление каналов их приема);
- индикаторы поля (Обнаружение, распознавание и определение местонахождения различных источников радиоизлучения);
- подавление диктофонов.

Таким образом, наряду с изучением различных теоретических дисциплин, в процессе обучения в данной лаборатории, курсанты и слушатели получают представление о программном и аппаратном обеспечении средств защиты информации, основах построения компьютерных сетей и их защиты от внешних угроз; знакомятся с различными сетевыми технологиями глобальных и локальных вычислительных сетей; осваивают методы и средства сбора, обработки, хранения, накопления, передачи информации; учатся разбираться в различных способах разграничения прав доступа к информации и средствах её защиты.

3. Обеспечение учебного процесса педагогическими кадрами высшей квалификации.

Решение данной проблемы видится в организации краткосрочных курсов повышения квалификации, проведении семинаров и конференций по обмену опытом.

Таким образом, проблема совершенствования подготовки специалистов в области информационной безопасности (по специальности 090103.65 – организация и технология защиты информации) является многоплановой. Успешно решить её возможно только комплексно, на основе системного подхода.

СПИСОК ЛИТЕРАТУРЫ

1. Нурғалиева Р.Г. «Электронный патруль» – Российская газета №5021 от 16 октября 2009 г.
2. www.academ.fnnet.ru
3. 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.
4. Муравьев А.В., Примакин А.И., Селюгина С. В. Использование автоматизированных рабочих мест в деятельности органов и учреждений Министерства внутренних дел Российской Федерации. Вестник Санкт-Петербургского университета МВД России. №4 (52). 2011. – С. 95-99.



БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Атисков А.А., Воробьев В.И., Федорченко Л.Н.

Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
**ОНТОЛОГИЧЕСКИЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ СТАНДАРТОВ И ВОЗМОЖНОСТИ
ИХ ГАРМОНИЗАЦИИ**

Введение

Средства обеспечения безопасности компьютерных, сетевых и информационных ресурсов до сих пор не сбалансированы, малоэффективны и слабо интегрируются. Причина заключается, прежде всего, в том, что объект защиты представляет собой сложную многоуровневую нелинейную систему с большим числом степеней свободы. В немалой степени этому способствует отсутствие сбалансированных стандартов, регламентов, профилей и политик безопасности.

В частности, применение Российских (национальных) криптографических стандартов, например:

- ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;

- ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации; Процессы формирования и проверки электронной цифровой подписи»;

- ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования», делают невозможной сертификацию по «Общим критериям» (ISO/IEC 15408:2005 Information technology – Security techniques – Evaluation criteria for IT security).

1. Основные проблемы

Как показывает экспертный анализ, основанный на полуформальных моделях, тексты стандартов страдают противоречивостью и неполнотой, что проявляется в несогласованности трактовок таких базовых концептов стандартов в криптографии, как критерий выбора алгоритма, способ доказательства и проверки, угроза, уязвимость, актив, контрмера, агент угрозы, и т. д., неопределённости некоторых первичных понятий и вытекающей отсюда неполноте или несогласованности отдельных положений и рекомендаций.

Эти факты становятся наиболее заметны не только в национальных версиях стандарта, но и англоязычном оригинале. Так комитет JTC 1/SC 27/WG 2 включает в план работ следующие направления:

- улучшение применимости криптографических стандартов;
- активный пересмотр существующих криптографических стандартов;
- исключение слабых и противоречивых схем взаимодействия криптографических систем (алгоритмов);
- включение новых и более эффективных схем.

Таким образом, учитывая высокую значимость обеспечения информационно-коммуникационной безопасности, глобальный характер этой деятельности, криптографические стандарты нуждаются в гармонизации, прежде всего, семантической, как внутри национальных версий, так и в международном аспекте.

Ясно, что любая согласованная техническая политика требует определенности и однозначности понятийного аппарата. Без формализации и соответствующей автоматизации этого процесса получение конструктивного результата будет проблематично. Примером неудачной попытки гармонизации [1] является ГОСТ Р ИСО/МЭК 10116-93 «Информационная технология. Режимы работы для алгоритма n-разрядного блочного шифрования»; ISO/IEC 10116: 2006 «Modes of operation for an n-bit block cipher (3rd edition)».

С точки зрения практики гармонизация может вестись по нескольким направлениям.

В первую очередь – гармонизация внутри линейки Common Criteria, включающей в себя собственно Common Criteria (ISO 15408), национальные и международные криптографические стандарты, Общую методологию оценивания (ISO 18045) и Руководство по разработке профилей защиты и заданий по безопасности. Здесь важной является согласование в форме гармонизации и соответствия национальных стандартов к Common Criteria. Гораздо более актуальную и универсальную задачу представляет гармонизация Common Criteria с линейкой ISMS (ISO 27000).

Это семейство стандартов рассматривает вопросы ИБ, в первую очередь, с организационной точки зрения, в то время как семейство Common Criteria – с технологической. Поэтому

вышеперечисленные базовые понятия информационной безопасности имеют в этих двух семействах стандартов различное наполнение. Объективно различия полностью устранить нельзя (в силу объективно разного происхождения и назначения линеек), но максимально сблизить – можно и нужно. Решение подобных задач лежит в русле гармонизации на онтологическом уровне.

Вторым направлением является гармонизация между Common Criteria и линейкой стандартов ISMS. Содержание и интерпретация базовых концепций можно использовать вместе, и решение для этой и подобных задач является основной целью гармонизации на онтологическом уровне. На методологическом уровне, основная (онтологическая) гармонизация предоставляет необходимые инструменты для обработки нормативных рисков организации. Единственный способ избежать двойной работы и расходов является создание системы информационной безопасности, которые были бы приемлемы для требований обоих критериев.

На уровне нормативно-методических документов онтологическая гармонизация позволяет успешнее решать, например, задачи снижения нормативных рисков для организаций. Например, распространенной является ситуация (чаще всего – в финансовой сфере), когда организация вынуждена сертифицироваться и по ISMS (этого требуют, например, партнеры) и по Common Criteria (этого требуют органы государственных учреждений). Чтобы не делать двойную работу (и не нести двойные затраты), организации необходимо строить систему информационной безопасности, удовлетворяющую обоим семействам стандартов сразу. А без гармонизации стандартов на самом верхнем, концептуальном уровне это сложно делать. Гармонизация в широком смысле может трактоваться как стандартизация данных.

Нами предлагается для гармонизации использовать *онтологическое проектирование*, включающее построение таксономий терминов предметной области, предикативных отношений между терминами, грамматического вывода на основе трансляционной грамматики, учитывающей семантику концептов предметной области, а также средства интеграции онтологий, а именно встраивание (mapping), связывание (alignment) и объединение (merging). Целью является построение непротиворечивого формального описания или формальная унификация предметной области и построение прикладного программного обеспечения для поддержки унифицированной схемы данных. Процессом достижения цели будет построение терминологических таксономий, предикативных отношений, дескриптивных ограничений (ontological restrictions) для вывода новых типов данных и расширение множества правил вывода. Уточнение терминологии и отношений может (и скорее всего будет) происходить непосредственно в процессе разработки онтологий (серии онтологий), что возможно за счет гибкости онтологических описаний (атомарностью, где атомом является логическая тройка) и выгодно отличается их от описаний структур данных на основе реляционных таблиц.

На следующем уровне возникает задача согласования инструментальных средств поддержки внедрения стандартов в практических задачах. В настоящее время эти средства проектируются, разрабатываются и существуют независимо. Проектирование этих средств происходит, в основном, в UML или средствами, близкими к нему. Так или иначе проектировщикам приходится строить объектные модели стандартов, причем каждый проектировщик разрабатывает свою собственную. Согласованные объектные модели, построенные на основе онтологий, позволили бы согласовать также и системные проекты этих средств, имея целью в дальнейшем либо разработку некоего универсального программного обеспечения, либо хотя бы организацию между ними каких-то интерфейсов.

Однако для перспективных задач этого не достаточно. Как нам представляется, в дальнейшей работе необходимо использовать онтологическое моделирование, что позволит дать эффективное метаописание стандартов в виде формальной компьютерной модели (семантической сети), автоматизировать их смысловое сопоставление средствами семантического анализа, обеспечить программный механизм доступа к стандартам при использовании Web-технологий (XML, RDF, OWL, SPARQL) для их описания. В качестве метаописания стандартов могут быть также использованы средства, применяемые при описании алгоритмических языков высокого уровня типа Алгол-68, Simula-6 и др. – двухуровневые WW-грамматики, атрибутные КС-грамматики, диаграммы Вирта, синтаксические граф-схемы [2, 3]. Онтологии могут описываться такими мощными синтаксически ориентированными средствами, вопрос только насколько эффективно они используются.

Такие подходы с использованием метаописаний стандартов безопасности обеспечат условия их гармонизации на разных уровнях и направлениях.

Уже имеется определенный опыт семантического анализа понятийного аппарата стандартов Common Criteria и ISMS с применением средств полужормального моделирования, который позволяет говорить о полезности такого анализа: В частности, построены следующие модели [4, 5]:

- объектно-ориентированная модель общего контекста безопасности по Common Criteria;
- объектно-ориентированная модель угрозы по Common Criteria;
- объектно-ориентированная модель контекста угрозы по Common Criteria;
- полная функциональная модель оценки ИТ по Common Criteria и Общей методологии оценивания – ISO 18045;
- полная функциональная модель требований к СУИБ по стандарту ISO 27001;

- объектно-ориентированная модель требований к СУИБ по стандарту ISO 27001. и т.д.

Переход от текстов стандарта к формализованному онтологическому описанию состоит в определении онтологической тройки:

- множество концепций (терминов);
- множество отношений между концепциями;
- правила логического вывода в сети концепций и отношений (например, правило транзитивности, симметричности, антисимметричности, рефлексивности).

Процесс логического вывода удаётся разбить на два этапа, при этом первый этап (вывод схем правил и схем выводов) приводит к регулярным выражениям, что допускает эффективное использование специального инструментального средства, разработанного в СПИИРАН, упрощающего схемы правил и схемы выводов (например, удаление тупиковых и циклических выводов). Второй этап требует использования грамматик, содержащих контекстно-зависимые правила, которые также могут быть проанализированы.

Для онтологических описаний нами разрабатывается интерфейс автоматизированного экспорта-импорта с инструментами описания в стандарте UML.

Основные свойства нашей гибридной системы согласования могут быть определены следующим образом:

- модульность системы;
- независимость входного и выходного синтаксиса нотаций (с использованием JAXB (Java Architecture for XML Binding) может облегчить доступ к XML-документов из приложений, написанных на языке Java);
- абстрактное определение семантики нотаций посредством OWL-описания, которое определяется абстрактными правилами преобразования (в виде логической тройки);
- реализация того, что можно сделать, с помощью языка SPARQL.

Можно отметить, что реализация правила управляется пользователем, а система должна адаптироваться для ввода (например, для описания стандартов языка UML или IDEF). Таким образом, чтобы решить задачу трансформации, была задействована пирамида стандартов Semantic Web. Экспериментально проверено, что метод семантического анализа и преобразования метаданных подходит не только для текста, но и для любых других форматов данных (если они могут быть оформлены в стандарте RDF).

2. Гибридная технология трансформации диаграмм проектирования

Для трансформации IDEF0 диаграмм в диаграммы UML мы разработали новую технологию. Как было отмечено в [6] существующие подходы к трансформации модель-модель могут быть классифицированы на подходы прямой манипуляции, подходы на основе отношений, структурные подходы, графовые методы и гибридные подходы. Они имеют следующие особенности:

1. Прямая манипуляция – наиболее низкоуровневый подход. Он предлагает пользователю лишь небольшую поддержку или даже отсутствие таковой. В целом, вся работа должна быть проделана самим пользователем. В долгосрочной перспективе этот подход становится непрактичным.

2. Категория структурных трансформаций содержит прагматические подходы, которые созданы в контексте конкретных видов приложений (и поэтому наиболее подходят к ним), таких как создание EJB реализаций и схем баз данных из UML моделей. Эти подходы требуют строгой поддержки для трансформации моделей с множественностью связей вида 1:1 и 1:n (иногда n:1) между исходными и целевыми элементами. Также, в данном контексте приложения, обычно нет необходимости для итераций (и в особенных фиксированных точках) в расписании, а само расписание может быть определено на уровне системы. Неясным остается насколько хорошо эти подходы могут поддерживать другие виды приложений.

3. Подходы на основе трансформаций графов имеют объемную теоретическую базу в графовых трансформациях. Эти подходы являются мощными, декларативными, но при этом они же и самыми сложными. Сложность идет от неопределенности в расписании и стратегии применения, которые требуют аккуратного рассмотрения завершения процесса трансформации и порядка применения правил (включающих свойство «слияния»). Существует много теоретических работ и некоторый опыт с исследованием прототипов. Однако опыт практического применения данных подходов все еще ограничен. Это позволяет хорошо увидеть всю сложность применения данных подходов на практике.

4. Подходы на основе отношений соблюдают хороший баланс между гибкостью и декларативным выражением. Они обеспечивают гибкое расписание и хороший контроль над неопределенностью. Три из пяти текущих QVT моделей соответствуют данной категории (CDI, QVTP и частично AST+).

5. Гибридные подходы позволяют пользователям смешивать и сопоставлять различные концепции и парадигмы в зависимости от области применения. Практические подходы, скорее всего, имеют гибридный характер.

3. *Использованные термины*

IDEF0 – Function Modeling – методология функционального моделирования и графическая нотация, предназначенная для формализации и описания бизнес-процессов. Отличительной особенностью IDEF0 является её акцент на соподчинённость объектов. В IDEF0 рассматриваются логические отношения между работами, а не их временная последовательность (Workflow).

Стандарт IDEF0 представляет организацию как набор модулей, здесь существует правило – наиболее важная функция находится в верхнем левом углу, кроме того есть правило стороны: – стрелка входа приходит всегда в левую кромку активности, – стрелка управления – в верхнюю кромку, – стрелка механизма – нижняя кромка, – стрелка выхода – правая кромка.

UML (Unified Modeling Language) – язык графического описания для объектного моделирования в области разработки программного обеспечения. UML является языком широкого профиля, это открытый стандарт, использующий графические обозначения для создания абстрактной модели системы, называемой UML-моделью. UML был создан для определения, визуализации, проектирования и документирования, в основном, программных систем. UML не является языком программирования, но в средствах выполнения UML-моделей как интерпретируемого кода возможна кодогенерация.

Диаграмма классов (Static Structure diagram) – статическая структурная диаграмма, описывающая структуру системы, демонстрирующая классы системы, их атрибуты, методы и зависимости между классами.

SPARQL (SPARQL Protocol and RDF Query Language) – язык запросов к данным, представленным по модели RDF, а также протокол для передачи этих запросов и ответов на них. SPARQL является рекомендацией консорциума W3C и одной из технологий семантической паутины. Предоставление SPARQL-точек доступа (SPARQL-endpoint) является рекомендованной практикой при публикации данных во всемирной паутине.

OWL (Web Ontology Language) – язык описания онтологий для семантической паутины. Язык OWL позволяет описывать классы и отношения между ними, присущие веб-документам и приложениям. OWL основан на более ранних языках OIL и DAML+OIL и в настоящее время является рекомендованным консорциумом Всемирной паутины. В основе языка – представление действительности в модели данных «объект – свойство». OWL пригоден для описания не только веб-страниц, но и любых объектов действительности. Каждому элементу описания в этом языке (в том числе свойствам, связывающим объекты) ставится в соответствие URI.

4. *Примитивы, используемые при описании онтологий*

Для описания нотаций проектирования были использованы следующие примитивы:

- owl:Class – класс, определяющий группу экземпляров, которые связаны друг с другом посредством разделения общих свойств. Классы организуются в специальную иерархию при помощи отношения rdfs:subClassOf;

- owl:Thing – это класс, объединяющий в себе все экземпляры и являющийся суперклассом для всех других классов в OWL и, соответственно, описанной онтологии;

- rdfs:subClassOf – иерархии классов, формирующиеся посредством определения одного или нескольких отношений между ними, которые показывают, что один из них является подклассом другого класса;

- rdf:Property – свойство. При помощи свойств определяются специальные отношения между экземплярами или от экземпляров к значениям данных. В первом случае используется owl:ObjectProperty, во втором – owl:DatatypeProperty;

- owl:Restriction – определяет ограничение на использование свойства rdf:Property (при помощи отношения owl:onProperty) для экземпляра конкретного класса;

- owl:onProperty – отношение, определяющее свойство rdf:Property, для которого установлено ограничение owl:Restriction;

- rdfs:domain – отношение, связанное с rdf:Property, определяющее субъект (в логической тройке субъект–предикат–объект), а именно класс, для экземпляров которого только и может быть определено данное свойство;

- rdfs:range – в отличие от rdfs:domain определяет объект в логической тройке;

- owl:cardinality – вид ограничения. Показывает, как отношение связано с числом, описывающим точное количество элементов конкретного свойства owl:Property, которые должны быть определены для экземпляров конкретного класса owl:Class. В описанной онтологии в случаях использования ограничения owl:cardinality, оно всегда связано с числом «1», это означает, что связанное с ним свойство должно быть определено один раз;

- owl:minCardinality – вид ограничения. В отличие от owl:cardinality определяет минимально допустимое количество элементов конкретного свойства для конкретного класса.

Построение OWL-описания структуры диаграмм IDEF0 основывается на двух типах элементов (блоки и стрелки) и отношениях между ними. Стрелки могут иметь один из четырех типов (вход,

выход, управление и механизм), начинаться и заканчиваться либо на других блоках, либо на одной из сторон диаграммы (см. рисунок 1).

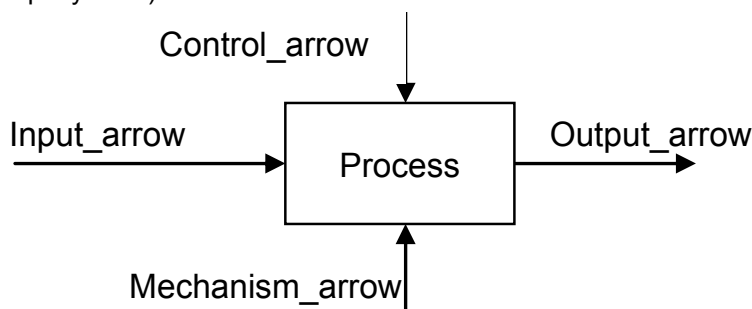


Рис. 1. Пример диаграммы IDEF0

Блоки также могут быть декомпозированы (то есть один блок внутри себя может содержать множество других). А стрелки могут сливаться и разъединяться. Описание стандарта IDEF0 позволяет построить его OWL-интерпретацию в среде Protégé.

В процессе разработки OWL-описания, объединяющего функциональный подход (диаграммы IDEF0) и объектно-ориентированный (диаграммы классов UML), были сформулированы [7, 8] следующие понятия: классы owl:Class и свойства owl:Property, включая owl:ObjectProperty и owl:DatatypeProperty. А также отношения:

- tf:Functional – owl:Class, наследниками которого являются все классы, описывающие метаданные диаграмм IDEF0.
- tf:ObjectOriented – в отличие от tf:Functional его наследниками являются классы, описывающие метаданные диаграмм классов UML.

Все понятия определены в пространстве имен (XML-namespace) `xmlns:tf="http://www.spiras.nw.ru/transform#"`.

5. OWL-описание нотации IDEF0

На рисунке 2 показаны элементы IDEF0-диаграмм, связанные с родительским классом tf:Functional посредством использования предопределенного в OWL отношения owl:subClassOf:

- tf:Arrow – класс, обозначающий «стрелку» в диаграммах IDEF0;
- tf:Block – класс, обозначающий «блок» в диаграммах IDEF0;
- tf:ArrowEnd – связь между конкретной «стрелкой» и «блоком». Связь имеет следующие разновидности:
- tf:Control, tf:Input, tf:Output, tf:Mechanism.

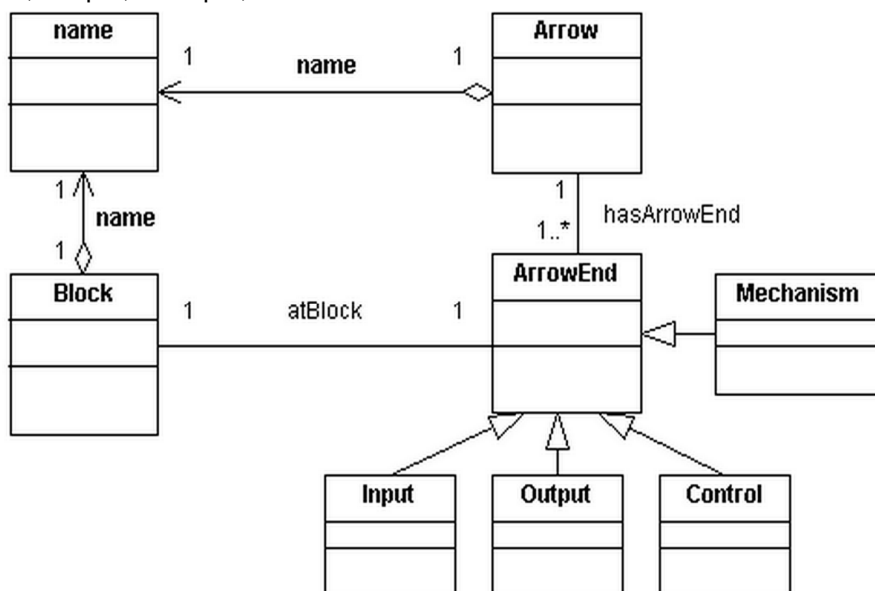


Рис. 2. Графическое представление OWL-описания нотации IDEF0

6. OWL-описание нотации UML диаграмм классов

Построение OWL-описания диаграмм классов UML (рис. 3) основывается на основных сущностях, которые используются при создании UML-диаграмм классов: класс, атрибут, метод, параметр метода, тип, связи (наследование, ассоциация, композиция, зависимость).

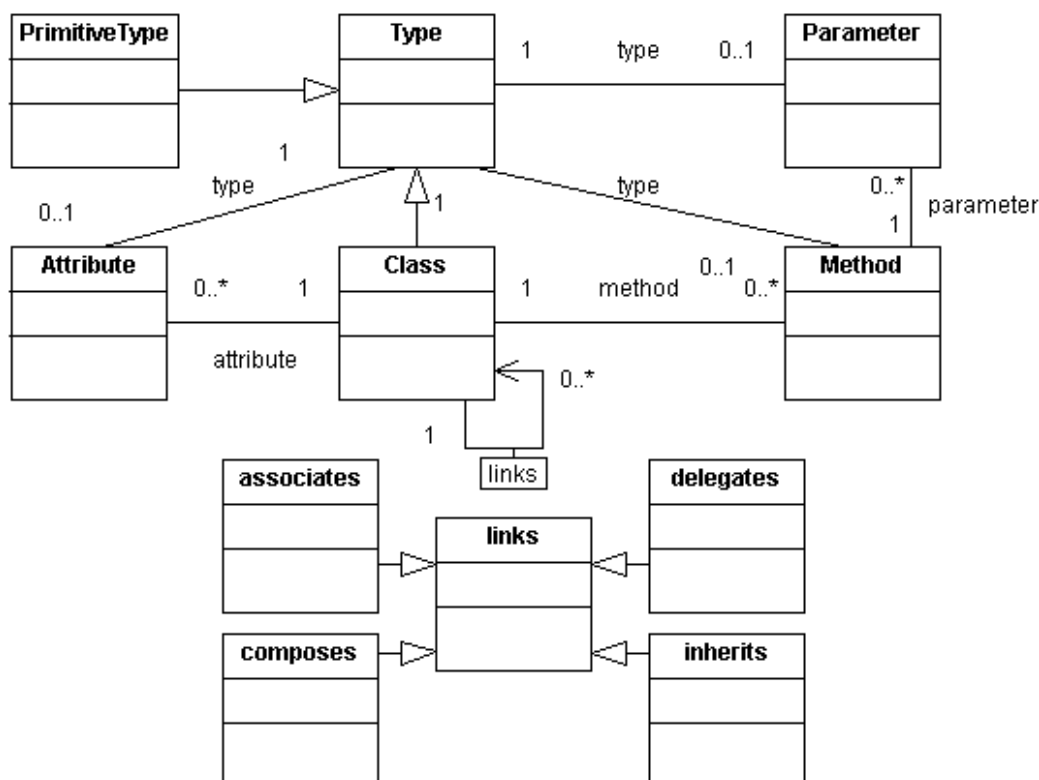


Рис. 3. Графическое представление OWL-описания нотации диаграмм классов UML

К элементам диаграмм UML (связанным с главным классом `tf:ObjectOriented`) относятся:

- `tf:Type` – класс, представляющий условное понятие «тип». Имеет разновидности (подклассы) `tf:Class` и `tf:PrimitiveType`;
- `tf:Attribute` – обозначает атрибут класса `tf:Class`;
- `tf:Method` – обозначает метод класса `tf:Class`;
- `tf:Parameter` – обозначает параметр метода `tf:Method`;
- Для связи введенных ранее понятий были определены следующие отношения `rdf:Property`:
- `tf:atBlock` – связывает `tf:ArrowEnd` и `tf:Block`. Определено ограничение `owl:Restriction`, согласно которому `tf:ArrowEnd` должен иметь ровно одно отношение `tf:atBlock`;
- `tf:hasArrowEnd` – связывает `tf:Arrow` и `tf:ArrowEnd`. Определено ограничение, согласно которому `tf:Arrow` должен иметь не менее одного отношения (свойства) `tf:hasArrowEnd`;
- `tf:type` – связывает `tf:Attribute`, а также `tf:Method` и `tf:Parameter` с `tf:Type`. Определено ограничение, согласно которому определенные выше субъекты логической тройки должны иметь ровно одно такое отношение;
- `tf:parameter` – связывает `tf:Method` и `tf:Parameter`;
- `tf:attribute` – связывает `tf:Class` и `tf:Attribute`;
- `tf:method` – связывает `tf:Class` и `tf:Method`;
- `tf:links` – связывает различные экземпляры `tf:Class`. Данное отношение имеет разновидности `tf:composes`, `tf:inherits`, `tf:delegates`, `tf:associates`.

7. OWL-описание правил трансформации

Для формального (в виде множества логических троек) описания правил были введены дополнительные понятия и отношения, а также использован ряд предопределенных понятия и отношений из языка RDF (Таблица 1).

Таблица 1

Использованные понятия и отношения из языка RDF

Выражение из RDF	Описание выражения
<code>rdf:Statement</code>	обозначает условие (представленное в виде логической тройки) правила
<code>rdf:parseType=«Collection»</code>	обозначает конечное объединение множества понятий
<code>rdf:subject</code>	связывает условие <code>rdf:Statement</code> с субъектом, входящим в состав логической тройки, которая описывает данное условие
<code>rdf:predicate</code>	связывает <code>rdf:Statement</code> с предикатом
<code>rdf:object</code>	связывает <code>rdf:Statement</code> с объектом

Для связывания OWL-описаний нотаций и OWL-описания правил трансформации были введены следующие понятия:

- `tf:Transform` – понятие, обозначающее правило;

- `tf:Object` – обозначает переменную, примененную в правиле.

А также отношения (свойства):

- `tf:functionalTemplate` – свойство правила `tf:Transform`, связывающее его с объединением множества условий `rdf:Statement`, которое описывает часть правила, относящуюся к диаграмме IDEF0. На менее формальном языке можно сказать, что данное свойство связывает правило с шаблоном (как множеством условий) из диаграммы IDEF0;

- `tf:objectOrientedTemplate` – в отличие от `tf:functionalTemplate` связывает правило с частью, относящейся к диаграмме классов UML.

При этом необходимо заметить, что правила нельзя трактовать как устойчивые и неизменяемые. Другими словами имеется возможность лишь определить возможную совокупность правил, позволяющую реализовать преобразование конкретной диаграммы.

Правила представляются в виде взаимосвязи двух множеств – множества трансформируемых элементов из диаграммы бизнес-процессов и множества элементов из диаграммы классов. Но для непротиворечивого определения был использован список логических троек (субъект–предикат–объект), причем этот список должен быть достаточно полным для однозначного определения нужного элемента при конкретной трансформации.

Рассмотрим пример правила преобразования: «все названия стрелок механизмов на диаграмме IDEF0 трансформируются в имена классов диаграммы классов UML». Вследствие ограниченных возможностей в ядре Protégé по описанию взаимосвязей между классами `owl:Class`, использовалась более абстрактная форма описания, а именно описание данного правила в виде множества логических троек. Такое представление можно интерпретировать как совокупность объектов, связи между которыми показаны на рисунке 4.

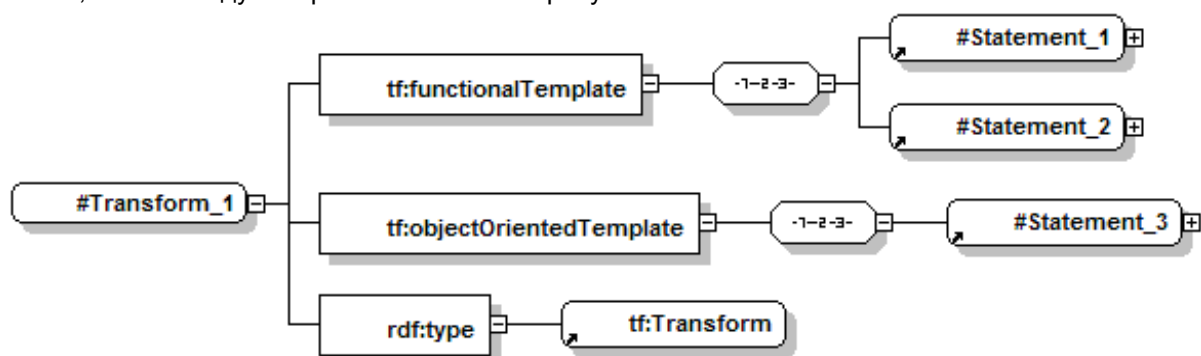


Рис. 4. Множество логических троек для примера правила трансформации
(где `Statement_1` раскрыт на рис.5, `Statement_2` – на рис. 6, а `Statement_3` – на рис. 7)

Здесь корневой элемент делится на три части (исходные данные `functionalTemplate`, целевые данные `objectOrientedTemplate`, и тип преобразования – трансформация)

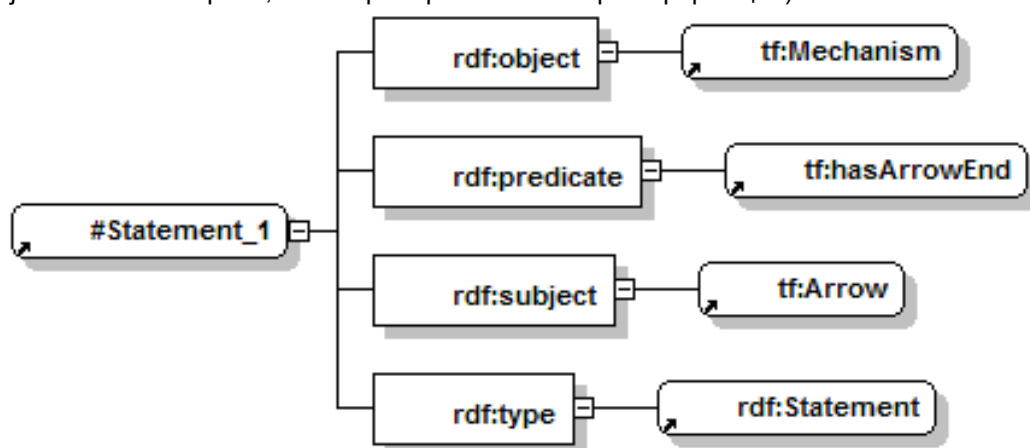


Рис. 5. Выражение для поиска «стрелки механизма»

На рисунке 5 показана первая логическая тройка в виде выражения, результатом выполнения которого является стрелка (`Arrow`), которая имеет тип (`hasArrowEnd`) механизм (`Mechanism`).

На рисунке 6 показана вторая логическая тройка в виде выражения, результатом выполнения которого является стрелка (`Arrow`), которая имеет имя (`name`), которую надо преобразовать в целевой объект (`object`).

На рисунке 7 показана третья логическая тройка в виде выражения, результатом выполнения которого является класс UML (`Class`), которая имеет имя (`name`), в которое преобразуется целевой объект (`object`).

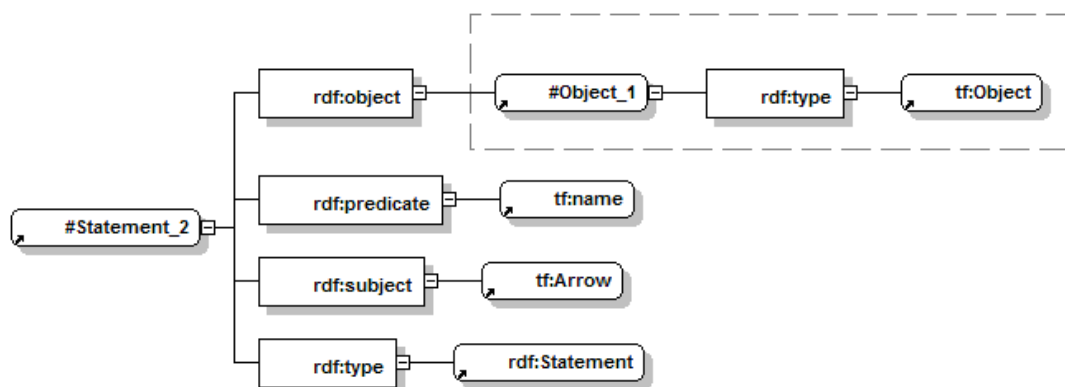


Рис. 6. Выражение для поиска «стрелки» с определенным именем

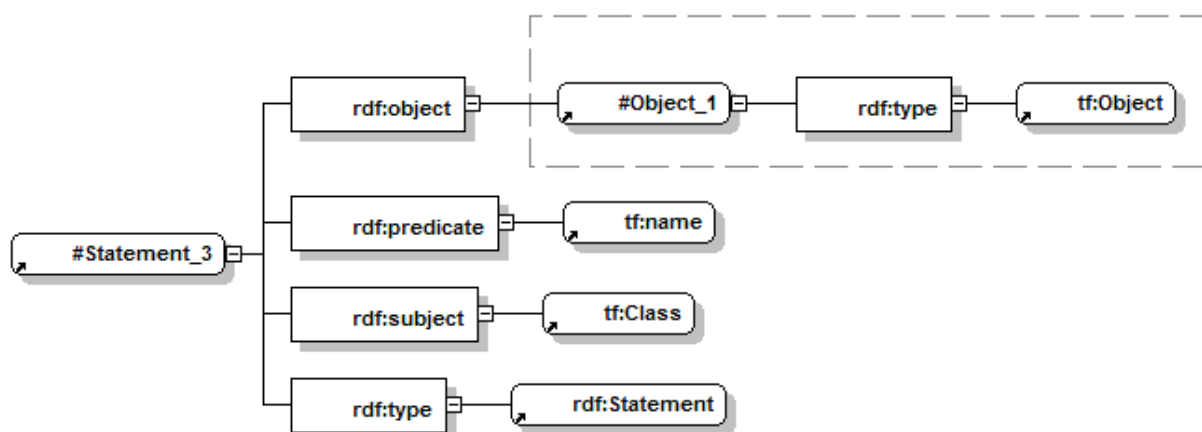


Рис. 7. Выражение для поиска «класса» с определенным именем

7. Алгоритм применения правил трансформации

1. Программная реализация использует следующий алгоритм (рисунок 8):
2. Ввести входной файл в программную модель RDF-данных исходной диаграммы.
3. Создать пустую программную модель RDF-данных выходной диаграммы.
4. Выполнить очередной SPARQL-запрос обрабатываемого правила.
5. Если не хватает данных в результате запроса, перейти к следующему запросу данного правила.
6. Если получен полный результат запроса, то подставить результат в соответствующий данному правилу шаблон RDF для выходной диаграммы, объединить результат с текущей программной моделью RDF-данных выходной диаграммы и перейти к следующему правилу.
7. Повторять пункты 3-5 до окончания обработки всех правил.(множество правил – конечное)
8. Записать программную модель RDF-данных выходной диаграммы в выходной файл.

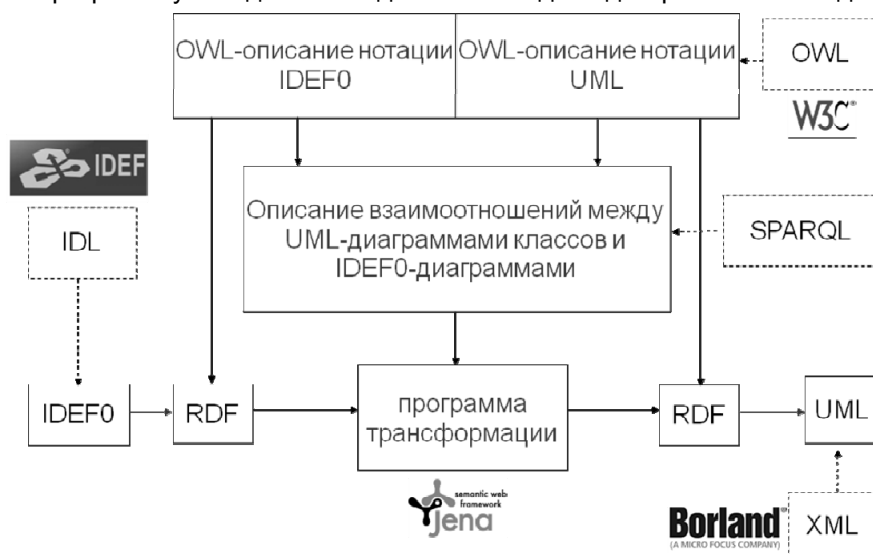


Рис. 8. Технология преобразования диаграмм IDEF0 в диаграммы классов UML

Рассмотрим формализацию на примере правила, состоящем из двух утверждений, в первом из которых говорится о том, что дуги механизмов являются объектами класса, а во втором, что блок – это метод для объектов класса. Сначала формализуем преобразование для первого утверждения. Так как задача преобразования сводится к трансформации одного RDF-формата данных (описывающего IDEF0-диаграмму) к другому (описывающему UML-диаграмму), используем стандартизованный язык запросов SPARQL [9] для извлечения данных из IDEF0-диаграммы. RDF-идентификаторы при преобразовании будут сохраняться. Предварительно определим XML-префикс, так как он будет использоваться во всех последующих формализмах:

PREFIX tf: <<http://www.spiras.nw.ru/transform#>>

Часть SPARQL-запроса, описывающего объект класса, выделим в отдельную константу, так как ее текст будет использоваться и в других запросах:

```
%class =  
?class a tf:Mechanism .  
_:class a tf:Arrow .  
_:class tf:hasArrowEnd ?class  
Запрос:  
SELECT ?class ?name  
WHERE {  
  %class .  
  _:class tf:name ?name  
}
```

Для приведения запроса к окончательному (стандартизованному) виду достаточно произвести в нем предварительную обработку с заменой константы *%class* ее значением и добавлением в него информации об используемом префиксе. Другая сторона преобразования состоит в генерации выходных RDF-данных для UML-диаграммы. Для простоты редактирования и восприятия правил построения выходных данных используем стандартную нотацию (основанную на примитивах языка SPARQL).

Следует отметить, что в этом случае мы использовали нескольких уровней, предложенных в рамках пирамиды стандартов Semantic Web [10], который является экспериментальным подтверждением предположения, что метод семантического поиска с использованием метаданных предназначен для анализа и преобразования, а не только данных, представленных в сети Интернет, но и для любых других данных, если она может быть оформлена для представления в стандарте RDF. Суть этого метода состоит в извлечении данных из их контекста или метаданных из исходного документа и формализация представления полученной информации в виде семантической сети и последующего формального поиска.

Библиотека моделей постоянно расширяется. Этого недостаточно, однако, для перспективных задач. Как мы видим, онтологическое моделирование необходимо в будущей работе, потому что это позволит эффективно создавать мета-описания стандартов с использованием формальной компьютерной модели (семантической сети), автоматизировать их онтологическое слияние и отображение с использованием семантических методов анализа, обеспечить общий доступ программного обеспечения к ним с помощью веб-технологий для их описания. Такой подход даст необходимые условия для согласования на различных уровнях и направлениях. Мы разрабатываем интерфейс, который обеспечит автоматизированный экспорт-импорт в UML инструменты для использования с онтологическим описанием.

8. Будущие направления исследований

В качестве основного направления будущих исследований предлагается для гармонизации использовать онтологическое проектирование, которое включает построение таксономий терминов предметной области, предикативных отношения между терминами, логический вывод на основе дескриптивной логики, а также средства интеграции онтологий, а именно встраивание (*mapping*), связывание (*alignment*) и объединение (*merging*). Для построения непротиворечивого формального описания или формальной унификации предметной области и построения прикладного программного обеспечения для поддержки унифицированной схемы данных предлагается применять аппарат регулярных грамматик. Процессом достижения цели будет построение терминологических таксономий, предикативных отношений, дескриптивных ограничений (*ontological restrictions*) для вывода новых типов данных и расширение множества правил вывода. Уточнение терминологии и отношений может происходить непосредственно в процессе разработки онтологий (серии онтологий). Все методики предполагается применять для проверки корректности использования крипто стандартов в области облачных вычислений.

Заключение

На определённом этапе гармонизации стандартов возникает задача согласования инструментальных средств поддержки внедрения стандартов в практические задачи. В настоящее время эти средства разрабатываются в СПИИРАН. Их проектирование происходит, в основном, в

UML или с помощью средств, близких к нему. В этом случае проектировщикам приходится строить объектные модели стандартов, причем каждый проектировщик разрабатывает свою собственную. Согласованные объектные модели, построенные на основе онтологий, позволили бы согласовывать также и системные проекты, нацеливаясь в дальнейшем либо на разработку некоего универсального программного обеспечения, либо на организацию между ними интерфейсов.

Однако для перспективных задач этого не достаточно. Как нам представляется, в дальнейшей работе необходимо использовать *онтологическое моделирование*, что позволит дать эффективное метаописание стандартов в виде формальной компьютерной модели (семантической сети), автоматизировать их смысловое сопоставление средствами семантического анализа, обеспечить программный механизм доступа к стандартам при использовании web-технологий (XML, RDF, OWL, SPARQL) для их описания. В качестве метаописания стандартов могут быть также использованы средства, применяемые при описании алгоритмических языков высокого уровня типа Алгол-68, Simula-6 и др. – двухуровневые WW-грамматики, атрибутные КС-грамматики, диаграммы Вирта, синтаксические граф-схемы и пр. Онтологии могут описываться такими мощными синтаксически ориентированными средствами, вопрос только насколько эффективно они используются.

Такие подходы с использованием метаописаний стандартов безопасности обеспечат условия их гармонизации на разных уровнях и направлениях.

СПИСОК ЛИТЕРАТУРЫ

1. Лунин А.. Взаимодействие государства и бизнеса в процессах стандартизации криптографических методов. Мир и безопасность № 1, 2008.
2. Федорченко Л.Н. Регуляризация контекстно-свободных грамматик. / LAP LAMBERT Academic Publishing GmbH & Co. KG Dudweiler Landstr. 99, 66123 Saarbrücken, Germany. 2011. С 180. ISBN: 978-3-8443-5360-0.
3. Федорченко Л.Н., Заболотский В.П. Лингвистический инструментарий в задачах обеспечения информационной безопасности. // Ежеквартальный журнал издательства СПбГПУ «Проблемы информационной безопасности. Компьютерные системы», № 1, 2009 г., С. 58–64, ISSN/Код НЭБ 2071–8217.
4. Любимов А.В. Инжиниринг стандартов информационной безопасности. // XI Санкт-Петербургская международная конференция "Региональная информатика-2008" (РИ-2008), Санкт-Петербург, 22-24 октября 2008г., Материалы конференции, Санкт-Петербург, 2008. С. 103 - 104
5. Любимов А.В., Суханов А.В. Полуформальные модели стандартов информационной безопасности // Вопросы защиты информации, №2 (81), 2008. С. 52 – 57.
6. Czarnecki K & Helsen S. (2003) Classification of Model Transformation Approaches. In Proceedings of the OOPSLA'03 Workshop on the Generative Techniques in the Context of Model-Driven Architecture. Anaheim, California, USA from http://www.swen.uwaterloo.ca/~kczarnec/ECE750T7/czarnecki_helsen.pdf.
7. Атисков А.Ю. Интеграция моделирования бизнес-процессов и объектно-ориентированного проектирования на основе гибридной технологии // Информационно-измерительные и управляющие системы. Вып. 4, т. 6. – М.: Радиотехника, 2008, С. 18-20.
8. Атисков А. Ю. Гибридная адаптивная технология проектирования бизнес-процессов / А.Ю. Атисков, С.В. Перминов // Труды СПИИРАН. Вып. 4. Под общ. ред. чл.-корр. РАН Р.М.Юсупова. — СПб.: Наука, 2007, С. 160-168.
9. SPARQL Query Language for RDF. W3C Recommendation 15 January 2008// from <http://www.w3.org/TR/rdf-sparql-query/>
10. Berners-Lee T. & Hendler J & Lassila O. (2001) The Semantic Web. A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities. Scientific American. No.5. 34–43.

Афанасьев С.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОНТОЛОГИЯ ТАКСОНОМИИ И БЕЗОПАСНОСТИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ**

Введение

Основное отличие облачных вычислений от распределенных и грид-вычислений в том, что в последних задается жесткая структура нахождения данных и сервисов, в то время как в облачных вычислениях структура не определена и может меняться. Для облачных вычислений необходим интернет-поиск данных и соответствующих сервисов. Существует ряд поисковых систем, которыми можно было бы воспользоваться, но при этом необходим ручной поиск и определение структуры выполнения системы вручную, а это требует много времени и жесткой структуры. Для облачных вычислений целесообразно использовать семантический поиск, который подразумевает онтологическое описание данных и сервисов, что при использовании языков онтологии (OWL/SWRL) позволит автоматически строить структуру облака и обеспечит релевантный поиск данных и сервисов. Кроме того, онтологическое описание данных и сервисов в облачных вычислениях позволяет существенно повысить безопасность вычислений в облаке.

Онтологическое описание данных и сервисов в облачных вычислениях

Вектор развития IT-сервисов явно указывает в сторону «облачных вычислений». Это заставляет задуматься о переходе к конкретным предложениям и реализациям SaaS-решений в различных сферах деятельности, т.е. «облака» имеют тенденцию быстрого расширения, объединения различных корпоративных облаков и т.д. Здесь и возникает проблема быстрого и релевантного поиска данных и сервисов [1]. Онтологическое описание позволит автоматически строить структуру и таксономию данных и сервисов в вычислительных облаках. Основными компонентами онтологии являются: «классы или понятия», «отношения», «функции», «аксиомы».

В соответствии с определением одного из классиков теории онтологического описания [2]) – это формально представленные на базе концептуализации знания. Формально онтологическое описание состоит из терминов, организованных в таксономию, их определений и атрибутов, а также связанных с ними аксиом и правил вывода; или База знаний, описывающая факты, которые предполагаются всегда истинными в рамках определенного общества на основе общепринятого смысла используемого словаря.

При разработке онтологического описания в облачных вычислениях необходимо, чтобы выполнялись следующие требования:

- ясность – онтология должна однозначно выражать значения терминов;
- непротиворечивость – онтологии должны быть непротиворечивы;
- расширяемость – необходимость учета расширения содержимого облака;
- минимизация онтологических соглашений;
- достаточность для решения требуемых задач.

Как правило, принято выделять следующие типы онтологий:

- онтология верхнего уровня (top-level ontology) – содержит универсальные знания, независимые от конкретных предметных областей, методов и задач;
- онтология предметной области (domain ontology) – определяет словарь конкретной области знаний;
- онтология метода (method ontology) – определяет понятия, связанные с определенным методом решения задач;
- онтология приложения (application ontology) – определяет термины конкретного приложения, связанные с онтологией конкретной предметной области и онтологией рассматриваемой задачи;
- мета-онтологии – определяют термины, используя специальные подходы (например, определение объекта через его части);
- онтологии проблемной области (domain-task ontologies) – описывают проблемную область с точки зрения решаемых задач.

В соответствии с требованиями и типами онтологического описания SaaS (Software as a Service) на рисунке 1 приведены три основных слоя (типа) онтологии и компонент программного обеспечения, которые требуют подробного онтологического описания в соответствии с вышеуказанными требованиями.

Метамодель безопасности вычислений в облаках

Относительно проблем безопасности существуют Руководства по безопасности, выработанные Облачным Союзом Безопасности (CSA), тем не менее, технический стандарт «облачных» вычислений находится все еще в его начальных стадиях разработки. Онтология показывает целостную перспективу операций безопасности и обеспечивает категории оперативной информации безопасности. Необходимо определить домены для операций безопасности, идентифицировать объекты, которые выполняют операции. На основе доменов и объектов идентифицируется информация безопасности, предоставленная объектами в каждом домене, и создается онтология оперативной информации безопасности [3].

Для безопасности в вычислительных облаках необходима сохранность информационной конфиденциальности, целостности, и доступности. Это также охватывает контроль, подлинность, и надежность информации. Операции по обеспечению безопасности основаны на трех доменах: управление активами ИТ, инцидентная обработка и накопление знаний.

Домен управления активами ИТ выполняет операции по обеспечению безопасности в каждом пользовательском устройстве, такие как установка, конфигурирование и управление активами ИТ. Актив ИТ включает и ресурсы потребителей и провайдеров; это включает не только собственные активы ИТ пользователей, но также и сетевую связь, «облачные» службы и оказанные услуги идентификационных данных внешними объектами для потребителя.

Инцидентный домен обработки обнаруживает и отвечает на эпизоды, встречающиеся в обществе пользователей и администраторов, следя за развитием компьютерных событий, отслеживая эпизоды из нескольких компьютерных событий и свойств атаки. Основываясь на отчете, исследуется инцидент так, чтобы это могло предотвратить атаки и принять контрмеры, обнаружить потенциальные угрозы.

Домен накопления знаний исследует безопасность и генерирует повторное использование знаний для других случаев.

В домене управления активами ИТ существует два объекта для его работы: Администратор и Провайдер инфраструктуры ИТ.

Администратор администрирует систему, обладая информацией о ее собственных активах ИТ. Провайдер инфраструктуры ИТ предоставляет каждому устройству инфраструктуру ИТ, которая включает сетевую связь, «облачные» службы, такие как программное обеспечение как сервис (SaaS), платформа как сервис (PaaS) и инфраструктура как сервис (IaaS), и идентификационные данные. Интернет-провайдер (ISP) и провайдер прикладных служб (ASP) являются его типичными экземплярами.

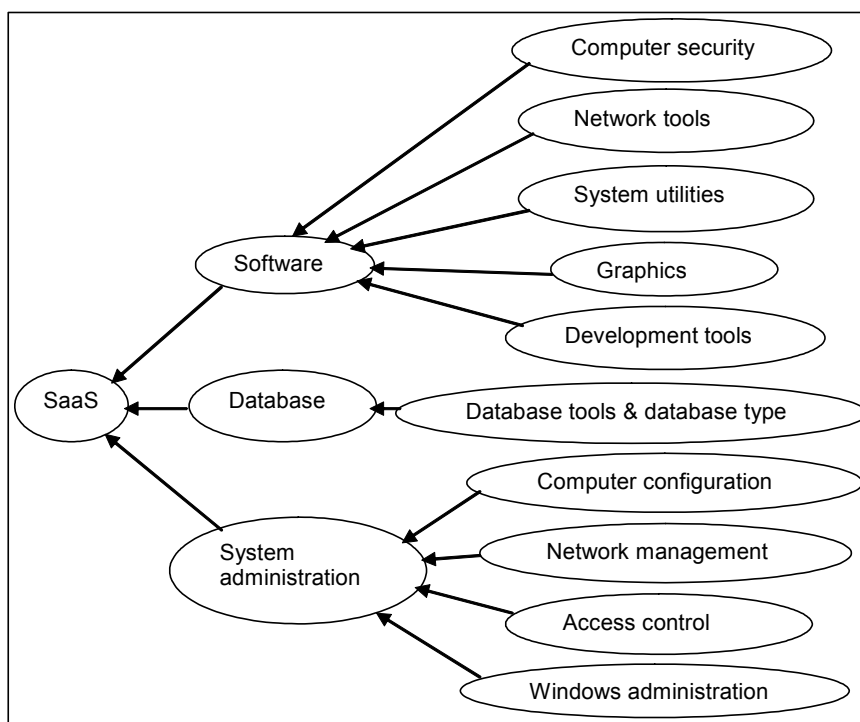


Рис. 1. Три основных слоя онтологического описания сервисов и данных

В инцидентном домене обработки существует два объекта: объект реагирования и координатор, Команда реагирования – объект, который контролирует и анализирует различные виды эпизодов, например, несанкционированный доступ, атаки DDoS и мошенничества с целью хищения личных данных, и накапливает инцидентную информацию. Основываясь на информации, это может реализовать контрмеры, например, регистрируя адреса Web-сайтов мошенничества.

В домене накопления знаний существует три объекта: исследователь-историк, сервис-провайдер и регистратор. Исследователь – объект, который исследует безопасность, извлекает знание от исследования и накапливает его. Сервис-провайдер – объект, который обладает информацией о продуктах и услугах, сервисах, их уязвимостях и конфигурационной информации. Регистратор – объект, который классифицирует, организует и накапливает знание о безопасности, обеспеченное исследователем и объектом сервиса так, чтобы знание могло повторно использоваться другим устройством.

Инцидентная база данных содержит информацию об инцидентах. Основной информацией в этой базе данных являются записи событий, инцидентные записи и записи атак. Запись события – запись компьютерных событий, которая включает информацию о пакетах, файлах и их транзакциях. Обычно, большинство записей обеспечивается компьютерами автоматически как компьютерные журналы; например журналы, такие как время и дата входа в систему. Инцидентная запись – запись эпизодов, обеспечивает описание эпизодов, таких как компьютерные состояния и их следствия. Инцидентная запись может записать ложные эпизоды.

База данных предупреждений является базой данных, которая содержит информацию о предупреждениях безопасности. Команда реагирования и Координатор манипулируют такой информацией. Эти предупреждения основаны на инцидентной базе данных и базе знаний риска.

Пользовательская база данных ресурса – база данных, которая накапливает информацию об активах внутренних устройств и содержит информацию, такую как список программного обеспечения и аппаратных средств, их конфигураций, состояния использования ресурсов, политики безопасности включая политику управления доступом, топологию интранет. Администратор использует эту информацию.

База данных ресурса провайдера – база данных, которая накапливает информацию об активах внешних отдельных устройствах. Провайдер инфраструктуры ИТ манипулирует такой информацией. Два основных компонента базы данных – внешняя сетевая информация и внешняя информация об «облачной» службе.

Внешняя информация об «облачной» службе включает спецификации службы, информацию о рабочей нагрузке и информацию о политике безопасности каждой «облачной» службы. Пользовательское устройство несет определенную информацию, такую как локальная конфигурация каждой «облачной» службы, которая хранится в пользовательской базе данных ресурса.

Объединив эти базы данных и базы знаний, получим метамодель безопасности для облачных вычислений, основанную на онтологическом подходе.

Заключение

Облачные вычисления – это способ обеспечения удобного и сетевого доступа к разделяемому пулу реконфигурируемых вычислительных ресурсов (например, сетям, серверам, устройствам памяти, приложениям и услугам), которые могут быть быстро подобраны и предоставлены с минимальными усилиями на менеджмент или взаимодействие с поставщиком услуг. Облачная модель должна обеспечивать высокую степень готовности и безопасности вычислительных ресурсов в облаке. Высокая готовность или доступность ресурсов (данных и сервисов) и безопасность вступает в некоторое противоречие. Разрешить эту проблему можно онтологическим описанием таксономии доступа к данным и сервисам (доступность) и онтологическим представлением безопасности вычислений в облаке, используя базы данных и базы знаний, в которых накапливается и анализируется доступность и риски безопасности вычислений в данном облаке. Здесь исследовалась релевантная таксономия данных и сервисов в облачных вычислениях и безопасность в части программного обеспечения как-сервис (SaaS), что требует дополнительных исследований, хотя онтологическое описание для PaaS и IaaS также необходимо полезно и для доступности/безопасности в облачных вычислениях.

СПИСОК ЛИТЕРАТУРЫ

1. Облачные сервисы. Под ред. Е. Гребнева – М.: CNews, 2011, 287с.
2. Gruberg T.R. Towards principals for the design of ontology's used for knowledge sharing. International Journal of Human – Computer Studies, 43(5–6):907–928, 1995.
3. Takahashi T. Ontological Approach toward Cyber security in Cloud Computing. Proceedings of Third International Conference on Security of Information and Networks (SIN2010), pp 100–109, 2010.

Блюм В.С., Заболотский В.П.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПАЦИЕНТОВ НА ОСНОВЕ
ПЕРВИЧНОЙ МЕДИЦИНСКОЙ ИНФОРМАЦИИ**

Введение

Каждый гражданин, обращаясь за услугой к системе здравоохранения, невольно приобретает новый статус, статус пациента. Этот статус порождает специфическое персональное информационное поле. Пациент вступает, если позволяет состояние, в откровенные диалоги, которые, как правило, не фиксируются, но их содержание защищено законом от разглашения. Про пациента и для него пишется множество различных документов: история болезни, назначения, рецепты и прочее, и прочее. Создаются графики жизненно важных переменных и таблицы различных параметров организма. Фиксируются разнообразные актуальные изображения, начиная от рентгенограмм и заканчивая томограммами. Возникновение и интенсивность заполнения этого информационного поля неразрывно связано с возникновением и интенсивностью лечебно-диагностического процесса, в рамках которого, собственно, и производится вся эта разнообразная персонализированная информация.

Российское здравоохранение в год производит более четырёх терабайтов первичной медицинской информации. Таков объём данных без учёта бухгалтерских, статистических и административных производных [1].

При этом информационная безопасность пациента имеет несколько противоречивых аспектов. С одной стороны, каждый пациент вправе рассчитывать на то, что не явные, временные или постоянные патологии его организма не будут сообщены третьим лицам без его согласия. С другой стороны, пациент рассчитывает на качественное и эффективное лечение, которое невозможно без полной, достоверной и доступной первичной медицинской информации (ПМИ) о текущем состоянии и всей предыстории. Полнота ПМИ складывается из необходимых и достаточных, по оценке лечащего врача, диагностических данных, собственно записей лечащего врача, а также зафиксированных суждений других привлечённых врачей, как в рамках текущего лечебно-диагностического процесса, так и на предыдущих этапах общения данного пациента с системой охраны здоровья. От полноты этой информации зависит принятие очередного лечебного решения, то есть здоровье и сама жизнь пациента. Не меньшее значение имеет достоверность ПМИ, поскольку из ложных посылок неизбежно следует ложное следствие. Поэтому обеспечение достоверности ПМИ – это одна из актуальных проблем современного здравоохранения. Наконец, доступность истории персональной ПМИ является необходимым условием обоснованных врачебных решений. Анализ анамнеза жизни и болезней пациента – аксиома врачебной практики. Всё выше сказанное указывает на то, что информационная безопасность пациента, а конечном итоге его жизнь и здоровье зависит от наличия и эффективного использования полной, достоверной и доступной ПМИ.

С информационной безопасностью пациента следует также связать проблему дефектов оказания медицинской помощи. На остроту этой проблемы неоднократно указано в документах Всемирной Организации Здравоохранения (ВОЗ) [2]. Статистический анализ, проведённый ВОЗ,

показал, что каждая десятая встреча пациента с системой здравоохранения связана с возникновением врачебной ошибки. Поскольку за плечом каждого врача невозможно поставить другого, более опытного и грамотного, то решение проблемы повышения безопасности пациента, в том числе, его информационной безопасности, следует искать в создании электронной системы полной, достоверной и доступной ПМИ и внедрении автоматизированных средств её обработки для раннего обнаружения врачебных ошибок.

Методам построения электронной системы полной, достоверной и доступной ПМИ и основных инструментов её анализа посвящена настоящая статья.

Состав и структура врачебных записей

Врачу приходится много писать. Особенно много из-за бюрократических требований. Талоны, расписки, отчёты – это то, что от чего средствами автоматизации необходимо избавить врача. Но есть записи, которые, напротив, надо помочь делать врачу. Вдумчивое отношение к пациенту невозможно без добротных описаний: состояния больного, предпринятых врачами действий, наблюдаемых результатов, сделанных оценок, полученных советов.

В таких текстах излагаются важные факты и ценные суждения, хронология и индивидуальность событий. Помимо того, что всё это не раз понадобится для осмысления, сама необходимость точного описания стимулирует и дисциплинирует врачебную мысль.

К такой работе врача с информацией надо относиться уважительно и квалифицированно. Недаром первые шаги студента в клинике начинаются с правил ведения истории болезни, с правильных описаний.

Сначала это самые общие правила, потом – свои требования в различных клинических разделах.

В результате жизнь вынуждает врача вырабатывать собственные стереотипы, основанные уже на личном опыте, на том, с чем он имеет дело чаще всего. К сожалению, это нередко означает шаг назад. Полнота и доброкачественность описаний попадают в зависимость от индивидуальности врача – его культуры, ответственности, квалификации. И, конечно, от обстоятельств работы. Главное обстоятельство известно: это занятость, нехватка времени.

Недостаток времени приводит к тому, что тексты потихоньку становятся облегчёнными и ущербными.

Но даже и такие тексты всё равно требуют немалых затрат. Следовательно, автоматизация составления документов должна помочь в решении двух проблем: обеспечить качество описаний и сэкономить врачу время.

Все описания в истории болезни можно разделить на 4 группы.

Первая группа записей – это записи, предопределённые в деталях: варьируются лишь количественные и качественные характеристики заранее указанных явлений и событий, только их врач и вводит от себя. Таковы протоколы хирургических вмешательств, описания функциональных исследований, официально регламентированные расписки пациентов («информированное согласие»), памятки пациентам. Странно было бы для всего этого не иметь электронных шаблонов и эффективных форм их заполнения. Сколько их потребуется? Теоретически – столько, сколько существует видов операций, исследований, памяток и расписок. На деле – существенно меньше, но жизнь постепенно побуждает продвигаться к максимуму. Разумеется, сначала требуются шаблоны самых обширных текстов и тех, которые используются часто. Затем придёт черёд остальных.

Вторая группа записей – описания рентгенологических и морфологических исследований, а также заключения консультантов различных специальностей. Это разнообразные и в немалой степени произвольные тексты. Шаблоны здесь уместны для наиболее частых вариантов, в частности, для описания нормы, для заключений при профилактических осмотрах, – для того, что в жизни, действительно, лишено существенной индивидуальности. А следом можно позаботиться и о шаблонах для описания типичных проявлений наиболее частых заболеваний.

Третья группа записей. Самые важные и самые трудоёмкие тексты – это первичное описание пациента (или – в поликлинике – первоначальное описание заболевания). Разнообразие здесь велико.

Но какими бы описания в истории болезни ни были, все они подчиняются изначально установленному в медицине порядку изложения.

Этот порядок – базовая структура текста. Его непеременные разделы: анамнез жизни, анамнез болезни, статус пациента, подробное описание поражённой системы органов и болезненных проявлений.

Роль шаблона, в данном случае, исполняет структура текста. А внутри каждого раздела существует своя структура, своя последовательность изложения, и её тоже надо предложить врачу в готовом виде.

Врач всегда описывает пациента по принципу «Коротко о влияющих факторах и полно о болезни». В этом и надо ему помочь.

«Коротко о влияющих факторах», но для всех врачей почти одинаково. Эта часть текста, будучи заготовленной заранее, – реальная техническая помощь врачу, а также интеллектуальная

поддержка, в которой содержится напоминание о том, чем надо поинтересоваться за пределами главной цели.

Но и «полно о болезни» – вовсе не абсолютно произвольный текст. Здесь каждая специальность диктует свои правила описаний. Они различны в разных областях медицины и даже в пределах одной специальности варьируются при разных заболеваниях, но это всегда правила, стереотипы. Следовательно, ничто не мешает эти стереотипы иметь в готовом виде заранее. В этом случае врачу останется только ответить на уже поставленные вопросы – внести конкретные количественные и качественные характеристики тех явлений, которые уже перечислены в шаблоне, либо убрать лишнее. И только в редких случаях дописать что-то совсем уж необычное и потому не предусмотренное.

В каждой специальности может быть ряд таких стереотипов: и десяток, и два, и три, но, при использовании программных инструментов, это не имеет значения. Всё однажды составленное можно сохранить, при необходимости пополнять и совершенствовать, а врачу подавать в нужный момент. Как помощь и как программу действий.

Четвёртая группа записей. Эта группа описаний включает дневниковые записи. Здесь фиксируются результаты наблюдения за состоянием и самочувствием больного. В процессе этого наблюдения врач фиксирует своё внимание на совершенно определённых явлениях, связанных с развитием болезни и лечением. Врач отмечает в дневниках не «всё на свете», а две группы явлений – ожидаемое и неожиданное.

Неожиданное проявляется в тех или иных изменениях общего состояния пациента, в его самочувствии, в его жалобах. Поэтому в дневниках всегда одинаковым образом упоминаются и то, и другое, и третье.

А ожидаемое – это динамика симптомов, связанных с болезнью и лечением. Эта информация всегда специфична для соответствующего раздела медицины и варианта лечения. Кардиолог, офтальмолог, уролог пишут разные дневники. Послеродовые и послеоперационные дневники не похожи на все прочие. В конкретных, узких рамках описываются только те явления, которые занимают именно этого специалиста в этих обстоятельствах. Но в пределах рамок эти явления и их описания одни и те же. Значит, можно и нужно иметь текстовые шаблоны для соответствующих «узких рамок». Сначала хотя бы для самых частых, а также для самых ответственных ситуаций.

Шаблон в таком понимании – не огрубление, не противопоставление индивидуальности.

Это не трафарет, а лекала, с помощью которых мастер отображает индивидуальность, соблюдая необходимые правила и пропорции. Ключ здесь – в достаточном наборе шаблонов, в их дифференциации, в том, чтобы они отражали если не весь спектр возможных клинических ситуаций, то хотя бы большую его часть. Когда это есть, врачи будут пользоваться шаблонами постоянно, а заодно – невольно – запоминать их повторяющееся содержание, усваивать его в качестве программы своих действий (а не только описаний).

Квалифицированно составленный текстовый шаблон – средство, вырабатывающее привычку, средство обучения. И с этой точки зрения на шаблоны надо посмотреть особенно внимательно.

Интегрированная история болезни

Осознание важности проблемы ведения электронной истории болезни (ЭИБ) произошло. Технологические возможности созрели. Государство выделило в 2012 году на создание федерального сервиса ведения интегральной электронной истории болезни более 180 миллионов рублей (см. соответствующий сайт госзакупок).

Деньги выделены. Цель, казалось бы, очевидна. Она состоит в том, чтобы реализовать облачную технологию, способную оказать реальную помощь каждому врачу, оснащённому компьютерной техникой и Интернетом для эффективного создания его электронных персональных медицинских записей (ЭПМЗ). А в результате, надёжно централизованно сохранять всю информационную историю каждого пациента. То есть обеспечить полноту персональной ПМИ для её оперативного использования.

Однако в рамках реализуемого проекта до сих пор не поставлена, а значит и не решается задача раннего обнаружения врачебных ошибок (дефектов оказания медицинской помощи) на основе анализа ПМИ. То есть, не закладываются основы решения проблемы информационной безопасности пациента.

Вновь создаваемая федеральная база интегрированных электронных историй болезни до настоящего времени не оценена по объёму потенциально сохраняемой информации и не предложен инструмент её анализа.

В наших публикациях [3,4] указывалось на необходимость разработки специализированной информационно-поисковой системы для организации оперативного доступа к ЭПМЗ в базе интегрированных электронных историй болезни. Главной особенностью указанной специализации ИПС является включение алгоритмов семантического анализа как отдельной ЭПМЗ, так и их последовательностей с целью выявления признаков врачебной ошибки (дефектов оказания медицинской помощи).

В предложенной технологии все тексты, цифры, графики и изображения о состоянии здоровья пациентов становятся доступны, во-первых, для автоматического формирования ответов на возникающие вопросы врача, во-вторых, для автоматического поиска и извлечения информации для алгоритмов анализа дефектов оказания медицинской помощи. Таким образом, базовой задачей над заданной системой данных становится задача информационного поиска.

В данной технологической схеме можно выделить два типа документов, для которых следует определить два типа задач информационного поиска:

1. Задача информационного поиска над множеством упорядоченных по времени и локализованных персонализированных данных пациента (записей) – документы гипертекстового файла персональной ЭИБ.

2. Задача информационного поиска над множеством документов – гипертекстовых файлов двух типов информационных источников (врачей, диагностических учреждений).

При этом следует учитывать высокую динамику внесения изменений в указанную систему данных [1].

Отметим ещё три принципиальных особенности приведенных выше коллекций документов.

Во-первых, это временная определённость каждого документа. Документ привязан к абсолютному времени, что оставляет возможность вычисления влияния на состояние пациента атмосферы и гелио-геофизических факторов. Кроме того, документ привязан к внутренней временной шкале пациента, что позволяет вычислять и учитывать возрастные особенности пациента.

Во-вторых, это семантическая определенность рассматриваемых коллекций. Для всех документов объектами номинации являются патологии человеческого организма и способы борьбы с ними.

В-третьих, это прагматическая определенность коллекций документов. Все документы носят целенаправленный характер: посвящены идентификации и нейтрализации вторжений в организм пациента.

Математическая модель поиска в базе электронной истории болезни

Рассмотрим общую постановку задачи информационного поиска на заданном множестве документов.

Пусть X – множество документов, Y – множество запросов.

Определим $\langle X, \sigma, P \rangle$ – вероятностное пространство, где σ – алгебра подмножеств X , P – вероятностная мера на σ .

Зададим бинарное отношение $\rho \in X \times Y$.

Тогда тип информационного поиска можно определить как четвёрку $S = \langle X, Y, \rho, \sigma, P \rangle$ (в нашем случае это $S_1 = \langle X_1, Y_1, \rho_1, \sigma_1, P_1 \rangle$ и $S_2 = \langle X_2, Y_2, \rho_2, \sigma_2, P_2 \rangle$).

Если $V \subseteq Y$ и $|V| < \infty$, то задачу информационного поиска типа S определим как $I = \langle X, V, \rho \rangle$ (для наших коллекций $I_1 = \langle X_1, V_1, \rho_1 \rangle$ и $I_2 = \langle X_2, V_2, \rho_2 \rangle$).

Таким образом, задача информационного поиска $I = \langle X, V, \rho \rangle$ состоит в том, чтобы для произвольного запроса перечислить те и только те записи $x \in X$, для которых $(x, y) \in \rho$.

Полнотекстовый поиск методом сканирования содержимого всех выше определенных и размещенных в сети документов возможен, но в разумное время невыполним. Необходимы алгоритмы, которые заранее сформируют для эффективного поиска полнотекстовый индекс – словарь, в котором перечислены все слова (термы) и указано, в каких документах они встречаются. Наличие индекса позволит осуществить поиск нужных слов и получить список документов, в которых они встречаются.

Помещение данных об очередном пациенте в полнотекстовый индекс можно рассматривать как аналог помещения реального пациента в стационар для интенсивного лечения. Отличие заключается в том, что для реального пациента надо считать число лейкоцитов в крови, а для ЭИБ пациента надо считать число, частоту и порядок слов в его гипертекстовом файле.

В качестве математической модели информационного поиска предлагается использовать матричную модель, как наиболее согласованную с теорией иммунокомпьютинга [5].

Пусть задано множество из n документов.

На его основе можно построить множество из m терминов, которые хоть раз встречались в каком-либо документе.

Введем матрицы сопряженности трех типов:

- D – «документ-документ»
- T – «термин-термин»
- C – «документ-термин»

Матрица сопряженности «документ-термин» размерностью $(n \times m)$ имеет вид:

$$C = \begin{array}{c|cccc} & t_1 & t_2 & \cdots & t_m \\ \hline d_1 & c_{11} & c_{12} & \cdots & c_{1m} \\ d_2 & c_{21} & c_{22} & \cdots & c_{2m} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ d_n & c_{n1} & c_{n2} & \cdots & c_{nm} \end{array}.$$

Элемент c_{ij} указывает на наличие j -го термина в i -м документе и вычисляется по методу TF-IDF для данной коллекции документов.

Матрица сопряженности «документ-документ» размерностью $(n \times n)$ имеет вид:

$$D = \begin{array}{c|cccc} & d_1 & d_2 & \cdots & d_n \\ \hline d_1 & d_{11} & d_{12} & \cdots & d_{1n} \\ d_2 & d_{21} & c_{22} & \cdots & d_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ d_n & d_{n1} & d_{n2} & \cdots & d_{nn} \end{array}.$$

Элемент d_{ij} указывает на наличие терминов содержащихся одновременно в j -м и i -м документах и равен количеству общих терминов в этих документах.

Матрица сопряженности «термин-термин» размерностью $(m \times m)$ имеет вид:

$$T = \begin{array}{c|cccc} & t_1 & t_2 & \cdots & t_m \\ \hline t_1 & t_{11} & t_{12} & \cdots & t_{1m} \\ t_2 & t_{21} & t_{22} & \cdots & t_{2m} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ t_m & t_{m1} & t_{m2} & \cdots & t_{mm} \end{array}.$$

Элемент t_{ij} указывает на наличие документов содержащих одновременно j -й и i -й термины и равен количеству таких документов.

Запрос пользователя можно представить в одном из двух видов:

1. n -мерный вектор-строка Q_i , i -я координата которого не равна нулю в том случае, если i -й документ включен в список документов, представляющих запрос;
2. m -мерный вектор-столбец Q_j , j -я координата которого не равна нулю в том случае, если j -й термин включен в список терминов, представляющих запрос.

Реакция системы на запрос пользователя Q вычисляется как:

$$A = C * Q.$$

Значение i -й координаты n -мерного вектора $A[a_i]$ при этом оказывается равным числу терминов запроса, оказавшихся в i -м документе.

Информационный поиск описывается в виде итерационного процесса:

$$\begin{aligned} A^{(0)} &= C * Q^{(0)}, \\ Q^{(1)} &= C^T * A^{(0)}, \\ A^{(1)} &= C * Q^{(1)}, \\ &\dots\dots\dots \\ A^{(t)} &= C * Q^{(t)}, \\ Q^{(t+1)} &= C^T * A^{(t)}. \end{aligned}$$

Элементы $Q^{(t)}$, для $t > 0$, рассматриваются как уточненные величины значимостей терминов в запросе.

Заметим, что

$$\begin{aligned} Q^{(t+1)} &= (C^T C)^t * Q^{(0)}, \\ A^{(t)} &= (C C^T) * A^{(0)}. \end{aligned}$$

Из теоремы Сильвестра при достаточно больших t можно получить приближение:

$$Q^{(t+1)} = \lambda_0 * Q^{(t)},$$

$$A^{(t+1)} = \lambda_0 * A^{(t)},$$

где λ_0 – собственное значение матрицы $C^T C$.

Если вектор $Q^{(0)}$ не учитывает фактор поисковой среды, то уже, начиная с $Q^{(1)}$, этот фактор учитывается. При больших значениях t вектор $Q^{(t)}$ выражает только свойства самой среды.

На первых тактах (при небольших t) итерационный процесс улучшает качество поиска, но при дальнейших итерациях качество поиска ухудшается, поскольку результаты перестают зависеть от запроса.

Чтобы преодолеть указанный недостаток скорректируем модель:

$$A^{(0)} = C * Q^{(0)},$$

$$Q^{(1)} = C^T * A^{(0)} + Q^{(0)},$$

$$A^{(1)} = C * Q^{(1)},$$

$$\dots\dots\dots$$

$$A^{(t)} = C * Q^{(t)},$$

$$Q^{(t+1)} = C^T * A^{(t)} + Q^{(0)}.$$

Можно показать, что при достаточно больших значениях t матрицы Q и A являются решением системы уравнений:

$$A = C * Q,$$

$$Q = C^T * A + Q^{(0)},$$

или в матричном виде:

$$\begin{pmatrix} A \\ Q \end{pmatrix} = \begin{pmatrix} 0 & C \\ C^T & 0 \end{pmatrix} \begin{pmatrix} A \\ Q \end{pmatrix} + \begin{pmatrix} 0 \\ Q^0 \end{pmatrix}.$$

Предложенная математическая модель применима для обоих типов задачи информационного поиска: как для поиска врачебной ошибки с помощью $I_1(S_1)$, так и для оценки преодоления эпидемического порога средствами $I_2(S_2)$.

Интересной математической задачей является исследование вложения $I_1(S_1)$ в $I_2(S_2)$.

Требования к оценке качества информационной безопасности пациента

Оценка качества результатов и эффективности информационной безопасности пациента должна производиться с помощью интегральных или частных показателей, позволяющих прямо или косвенно оценить результативность, ресурсоемкость, оперативность и эффективность процесса информатизации.

Показатели результативности должны позволять количественно или качественно оценивать [6]:

- уровень информированности врача и пациента, необходимый для обеспечения эффективного лечения;
- текущий уровень информированности врача и пациента, обеспечиваемый в ходе информатизации;
- объем и качество региональных и федерального информационного фонда здравоохранения, возможность использования российского и мирового информационных фондов здравоохранения;
- возможность доступа врача и пациента региона к региональным, российскому и мировому информационным фондам;
- степень развития и качество информационной инфраструктуры здравоохранения и ее элементов;
- степень подготовки врача и пациента региона к использованию информационных средств и технологий, включая уровень компьютерной грамотности и информационной культуры, а также готовность жителей региона к восприятию предоставляемой информации;
- степень удовлетворения и развитости информационных потребностей врача и пациента региона в ходе информатизации.

Показатели ресурсоемкости должны позволять оценивать затраты на информатизацию здравоохранения всех видов ресурсов, в том числе материальных, энергетических, информационных, людских и т.д., кроме временных. Стоимостная или натуральная форма показателей выбирается в зависимости от целей оценивания.

Оценка оперативности информатизации здравоохранения должна производиться с использованием показателей, позволяющих оценить временные затраты на информатизацию.

Выбор показателей результативности, ресурсоемкости и оперативности должен быть хорошо обоснован. На базе выбранных показателей формулируются критерии, позволяющие выработать суждения о качестве и эффективности информатизации по результатам контроля этого процесса.

Показатели эффективности должны позволять оценивать возможность достижения целей информатизации при реализации ее конкретных вариантов, сравнивать оцениваемые варианты и выбирать из них наиболее рациональные.

Показатели качества следует применять при оценке состояния и результатов информатизации, а показатели эффективности – при контроле хода информатизации.

Необходимо отметить, что использование только показателя экономической эффективности для оценки качества и эффективности информационной безопасности пациента не позволяет правильно оценить ход и результаты информатизации хотя бы потому, что не все составляющие показателей качества и эффективности могут быть корректно представлены в стоимостной форме.

Заключение

Проблема информационной безопасности пациента с позиции раннего обнаружения дефектов оказания медицинской помощи может решаться только на основе создания системы полной, достоверной и доступной первичной медицинской информации. А также на основе внедрения эффективных инструментов информационного поиска, включающих алгоритмы непрерывного анализа потока ПМИ. С этой целью все, без исключения, встречи пациента с врачом и соответствующие врачебные решения должны быть зафиксированы в сети в форме доступных для мониторинга документов. Результаты лабораторных исследований также должны быть обеспечены сетевым доступом. Более того, появление в сети указанных документов должно стать необходимым условием начала деятельности основных лицензируемых объектов системы здравоохранения: врачей и диагностических лабораторий.

Выполнение этих условий создаст реальную возможность для непрерывной работы поисковых роботов, формирующих индексные файлы поисковой машины и их оперативного анализа. Полученная таким образом интегрированная медицинская информация позволит эффективно отвечать почти на все вопросы к системе охраны здоровья, начиная от количества оказанных медицинских услуг и заканчивая оперативным вычислением врачебных ошибок.

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. Блюм В.С., Заболотский В.П. Подход к формированию единого информационного пространства здравоохранения. //Труды СПИИРАН / Под ред. чл.-корр. РАН Р.М.Юсупова. Вып.6, СПб., Наука, 2008. 248 с. С.112–129. ISBN 978-5-02-025350-6
3. 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
4. Блюм В.С., Заболотский В.П. Свободное программное обеспечение для здравоохранения //Труды СПИИРАН / Под ред. чл.-корр. РАН Р.М.Юсупова. Вып.8, СПб., Наука, 2009. 317 с. С.46–59. ISBN 978-5-02-025381-0
5. Tarakanov A. O., Skormin V. A., Sokolova S. P. Immunocomputing: Principles and Applications. New York.: Springer, 2003, 230 p.
6. Юсупов Р.М., Заболотский В.П. Научно-методологические основы информатизации. СПб, Наука, 2000, – 455 с.

Десницкий В.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
КОНФИГУРАЦИОННАЯ МОДЕЛЬ КОМБИНИРОВАННОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ СО ВСТРОЕННЫМИ УСТРОЙСТВАМИ**

Статья посвящена исследованию вопросов проектирования и анализа комбинированных механизмов защиты сложных телекоммуникационных систем со встроенными устройствами. В работе вводится понятие конфигурации устройства, которая представляет комбинацию компонентов защиты, развертываемых для поддержки безопасности устройства, а также предоставляемых им программных сервисов. Путем решения оптимизационной задачи с учетом функциональных и нефункциональных свойств отдельных компонентов защиты осуществляется поиск наиболее эффективных конфигураций.

Введение

Важнейшей задачей защиты информации является исследование вопросов безопасности систем, включающих встроенные устройства. Характерными особенностями таких систем являются автономность отдельных устройств, входящих в систему, ограничения, накладываемые на ресурсы устройств, и следующая из этого их слабая производительность [12,15]. Встроенные устройства предоставляют нарушителю широкий круг возможностей осуществлять различные виды атак, в частности, через прямое подключение к интерфейсам и элементам устройства [3,9]. Наличие значительных ограничений на ресурсы устройства влечет сложность применения традиционных

криптографических и других средств защиты, используемых для поддержки безопасности персональных компьютеров и серверных станций. Поэтому для реализации безопасных систем со встроенными устройствами требуется новые подходы к проектированию компонентов защиты информации, которые обеспечивали бы разумный компромисс между суммарной производительностью системы и ее защищенностью [1,13,18]. Для достижения такого компромисса в работе предлагается подход к конфигурированию защиты путем выбора наиболее эффективных комбинаций компонентов защиты, реализующих необходимые свойства безопасности.

Актуальность исследования вопросов конфигурирования обуславливается тенденцией к стремительному увеличению количества устройств, осуществляющих коммуникации в сети Интернет и управляющихся удаленно посредством беспроводных протоколов, что проявляется в развитии общей концепции и конкретных реализаций «Интернета вещей» («Internet of Things») [16]. Осуществляя коммуникации в потенциально опасном и неконтролируемом окружении, такие системы подвержены как универсальным, так и специализированным сетевым атакам [19]. Поэтому особенно важной становится задача построения эффективных механизмов защиты, направленных на противодействие атакам, выполняемым со стороны потенциального нарушителя [2,20].

В качестве ключевых проблем в области безопасности встроенных устройств в работах [13,19] выделяются проблемы безопасного хранения данных внутри устройства, идентификации пользователей, безопасного доступа к сети, устойчивости установленного программного обеспечения (ПО) к модификациям, безопасных сетевых соединений и другие. Вместе с тем, существующие механизмы защиты встроенных систем ориентированы главным образом на предоставление защиты против определенных видов угроз. В частности, в [4,14,19] предлагаются классификации нарушителей и угроз для встроенных систем, исходя из возможностей нарушителей, их компетенции, типа доступа к устройству, а также приводятся некоторые способы их предотвращения.

Возникновение некоторой угрозы влечет необходимость обеспечения определенного функционального свойства безопасности при помощи применения определенных защитных механизмов, которые позволят предотвратить эту угрозу. При этом комбинирование отдельных компонентов защиты с учетом лишь функциональных свойств защиты оказывается неэффективным в виду существенных ограничений на ресурсы устройств и невозможности развертывания полученных решений на практике. Подход, предлагаемый в настоящей работе, определяет способ комбинирования отдельных алгоритмов и решений, реализующих различные свойства защиты. Цель подхода состоит в достижении свойств защиты путем выбора наиболее эффективных комбинаций компонентов защиты с учетом нефункциональных свойств компонентов и ограничений устройства.

1. Постановка задачи

Под конфигурацией защиты понимается множество устанавливаемых на устройство компонентов защиты, каждый из которых реализует одну или несколько функций защиты. Конфигурирование является процессом, включающим поиск такой конфигурации, которая, во-первых, реализует все необходимые функциональные свойства защиты, во-вторых, удовлетворяет ограничениям, накладываемым устройством на объемы ресурсов, выделяемых для выполнения защитных функций, и, в-третьих, является оптимальной. Конфигурация, удовлетворяющая первым двум условиям, называется допустимой. Оптимальность понимается в соответствии с заданным критерием оптимальности, определяемым разработчиком системы. Любая, как допустимая, так и оптимальная конфигурация должна также удовлетворять ограничениям программно-аппаратной совместимости, как, например, определенные тип и версия операционной системы устройства. Процесс конфигурирования нацелен на решение следующих задач на стадии проектирования встроенных устройств: поиск допустимых конфигураций; поиск оптимальных конфигураций; проверка допустимости и оптимальности конфигурации.

Входными данными процесса конфигурирования являются: данные о функциональных свойствах защиты (например, применение безопасных коммуникационных протоколов для поддержки конфиденциальности передаваемых данных), которые требуется обеспечить для устройства, ограничения на значения нефункциональных свойств (например, объем расходуемой оперативной памяти), а также спецификации отдельных компонентов защиты. К выходным данным относится множество допустимых конфигураций защиты, а также набор оптимальных конфигураций. Несколько конфигураций могут быть рассматриваться в качестве оптимальных, если их множества функциональных свойств и нефункциональных требований совпадают, соответственно, или если применяемый критерий оптимальности приравнивает данные конфигурации согласно интегральным критериальным значениям.

Решаемая оптимизационная задача является в общем случае многокритериальной экстремальной задачей с заданным набором ограничений [8]. Ее математическая постановка формулируется с использованием теоретико-множественном представлении:

$$\begin{aligned} &opt_criterion(non_functional_properties(configuration)) \rightarrow \min \\ &Constr(functional_properties(configuration)) \end{aligned}$$

Constr(non _ functional _ properties (configuration))
Constr(platf _ compat _ properties (configuration)).

Постановка задачи включает определение критерия оптимальности на основе значений показателей нефункциональных свойств конфигурации, а также определение ограничений на функциональные, нефункциональные свойства и свойства программно-аппаратной совместимости. Формулируемая цель – найти экстремальное значение задачи, представляющее оптимальную конфигурацию, на которой достигается оптимум.

Примером может быть один из рассматриваемых ниже критериев оптимальности: минимизация показателя нефункционального свойства, определяющего объемы некоторого ресурса устройства; оптимальность на основе «цепочки свойств», при которой предыдущий критерий рассматривается последовательно для каждого из свойств; оптимальность на основе интегрального показателя ресурсов с учетом нефункциональных ограничений устройства; оптимальность на основе DEA-метода [17] и другие.

В частности, оптимальность на основе цепочки свойств предполагает процедуру поэтапного отбора конфигураций путем анализа некоторой заданной последовательности нефункциональных свойств, в порядке убывания их предпочтения. Оптимальность на основе интегрального показателя в работе рассматривается как выполнимость критерия минимизации отклонений значений свойств от заданных ограничений: $\min\{dev_i | i\}$, где параметр i задает номер рассматриваемого нефункционального свойства.

2. Архитектура механизма конфигурирования

Разработанный программный комплекс позволяет продемонстрировать предлагаемый подход к конфигурированию и представляет собой программное средство для конфигурирования защищенных распределенных систем со встроенными устройствами. В задачу механизма конфигурирования входит помощь разработчику устройства в принятии решений на стадии проектирования в контексте обеспечения безопасности и допустимого ресурсопотребления устройства. Программный комплекс реализует собственно функцию конфигурирования, которая по заданным ограничениям и множеству компонентов защиты, позволяет выявить оптимальные по выбранному критерию конфигурации, а также функции проверки оптимальности заданной конфигурации. Помимо этого, программный комплекс позволяет установить разработчику, какой ресурс является наиболее критичным по отношению к заданной конфигурации или же какими нефункциональными ограничениями должно обладать устройство должно, чтобы для его защиты можно было применить заданную конфигурацию.

Архитектура представляется при помощи серии диаграмм в нотации UML 2.0 [10] и включает статическую модель механизма конфигурирования, которая определяет его структурные элементы и связи между ними (рисунок 1). Применяются следующие элементы представления, согласуемые с принципами объектно-ориентированного проектирования и анализа: классы (сущности), их атрибуты и операции, ассоциации и их кратность, обобщения (наследование). На рисунке 1 показаны элементы модели, отвечающие за представление защищаемого устройства (ToE System, Func. requirement) и его свойств, включая функциональные требования защиты (RequiredResource, Non-functional property, SBB Requirements, Functional property Platform compatibility property), компонентов защиты (SBB, Configuration, Repository), представление критериев оптимальности (Optimization criterion) и функций конфигурирования, фильтрации и проверки допустимости конфигураций (Filter, Checker, Configurator).

Каждый компонент защиты представляется спецификацией (descriptive part) и реализацией (implementation_ref). Нефункциональные свойства характеризуются значением свойства (value) и типом значений (value_type). Критерий оптимальности задается на основе целевой функции (goal function), которую необходимо минимизировать. К основным функциям относятся функция фильтрации (filter), функции проверки (check) и конфигурирования (configure). Фильтрация позволяет отобрать те из компонентов защиты, находящиеся в хранилище компонентов (Repository), которые удовлетворяют программно-аппаратным ограничениям совместимости. Функция проверки оперирует конфигурациями в терминах функциональных и нефункциональных свойств и позволяет сформировать множество допустимых конфигураций. Функция конфигурирования является финальной функцией процесса и позволяет получить набор оптимальных конфигураций, которые отображаются разработчику (present, report).

Функция фильтрации реализует проверку программно-аппаратных свойств совместимости компонентов защиты. В качестве компонентов защиты рассматриваются программные, программно-аппаратные компоненты, а также «логические» компоненты, состоящие из нескольких связанных между собой компонентов и обеспечивающие одно или несколько функциональных свойств. Компоненты защиты представляются на основе описаний нефункциональных свойств ресурсов и требований с использованием их численных значений, функциональных свойств защиты и свойств программно-аппаратной совместимости. В качестве иллюстрации в табл. 1 приведен пример определения нефункционального свойства расходования ресурса оперативной памяти (в килобайтах) на выполнение функций защиты.

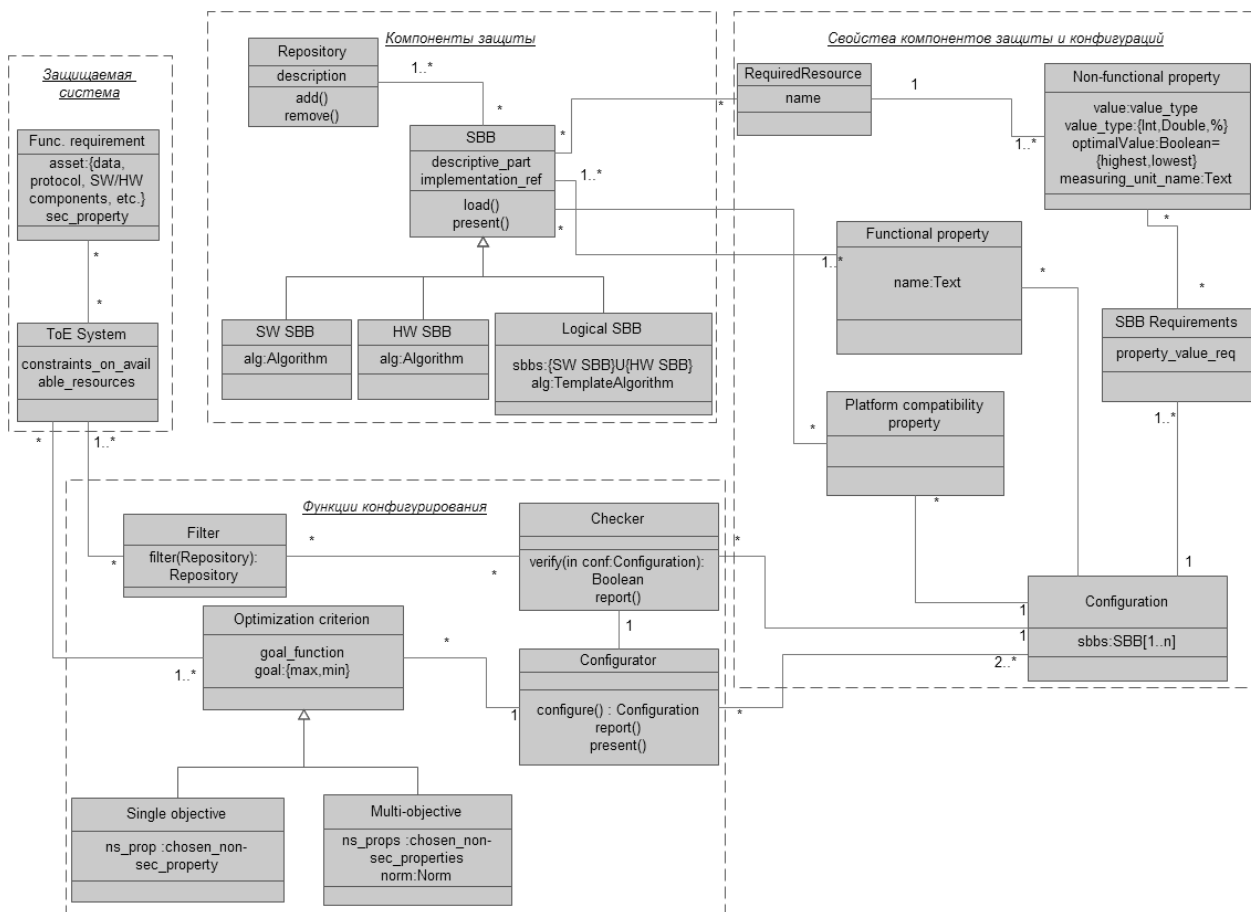


Рис. 1. Статическая модель механизма конфигурирования

На рисунке 2 приведен фрагмент «многооконного» пользовательского интерфейса программного комплекса конфигурирования. Показано главное окно механизма, где разработчику предоставляются информация о функциональных и нефункциональных свойствах компонентов защиты, информация о свойствах программно-аппаратной совместимости, критериях оптимизации, спецификация защищаемого устройства, а также функциями управления процессом конфигурирования.

Таблица 1

Пример описания нефункциональных свойств компонента защиты

Объект	Значение
Компонент защиты	«Компонент защиты 1»
Ресурс	«Оперативная память»
Нефункциональное свойство	«размер потребляемой памяти»
Границы значений	Промежуток 25–30
Тип значений	Тип Integer
Оптимальное значение	Наименьший
Единицы измерения	«Кб»

В качестве примера показаны параметры конфигурируемого устройства, в том числе свойства программно-аппаратной совместимости устройства – поддержка среды выполнения «JAVA 2», а также протоколов IPv4 и IPv6, и нефункциональные свойства защиты – объем расходуемой памяти, пропускная способность коммуникационного канала и значение стоимости компонента защиты (memory amount, Ethernet interface bandwidth, cost value). Показаны также функциональные свойства защиты – конфиденциальность данных, хранимых на устройстве, аутентичность сетевого канала, при помощи которого устройство осуществляет коммуникации (confidentiality of stored data, authenticity of customer, authenticity of communication channel) и аутентичность пользователя устройства. Результатами конфигурирования отображаются в разделе «результаты» (рисунок 4) и включают, во-первых, перечисление допустимых конфигураций (конфигурации {SBB-1,SBB-3}, {SBB-1,SBB-4}, {SBB-1,SBB-3,SBB-4}) и, во-вторых, перечисление оптимальных конфигураций ({SBB-1,SBB-3}, {SBB-1,SBB-4}) в соответствии с выбранным критерием оптимальности.

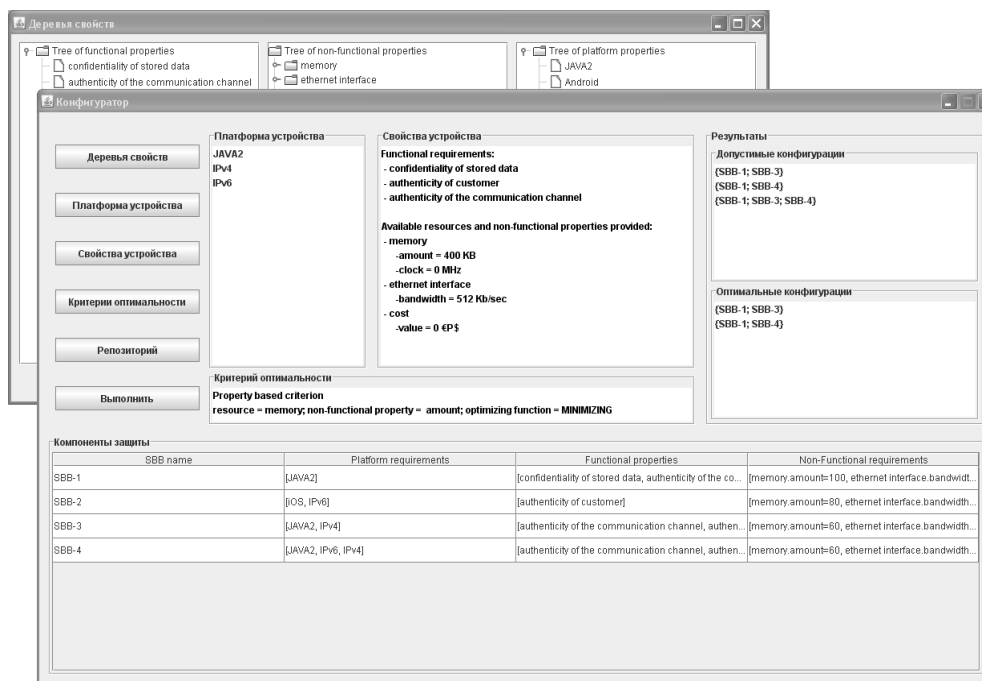


Рис. 2. Фрагмент пользовательского интерфейса программного комплекса конфигурирования

3. Пример применения

В качестве примера применения предложенного подхода к конфигурированию в работе рассматриваются элемент информационно-телекоммуникационной системы мобильной и быстро разворачиваемой коммуникационной сети поддержки и оперативного управления в чрезвычайных ситуациях, которая позволяет организовать совместную работу различных служб и задействованных устройств. Система разрабатывается компанией ASCOM (Швейцария) и относится к классу систем, характеризующихся динамически изменяемой топологией сети и отличающихся типами коммуникаций между ее отдельными узлами, а также заранее не фиксированным кругом функционирующих компонентов и задействованных устройств.

В частности, пример применения представляет коммуникационное мобильное устройство «смартфон», имеющее постоянную связь с сетью Интернет и управляющееся на основе мобильной операционной системы или виртуальной машины. На смартфон установлено прикладное программное обеспечение, которое реализует клиентскую сторону работы специализированного программного сервиса по предоставлению пользователю устройства функций получения и хранения конфиденциальных данных. В соответствии с предлагаемым подходом, для поддержки безопасности программы в нее встраивается комбинированный механизм защиты, который должен быть сконфигурирован. Для работы выделяются ресурсы устройства, которые расходуются как на выполнение целевых функций программы, так и на поддержку функций защиты. Коммуникации устройства базируются на использовании беспроводных каналов связи с удаленным сервером в рамках сетей типа 3G и 4G. Пользовательская информация может храниться как в рамках локальной памяти устройства, так и на сменных носителях информации miniSD.

Учитываются следующие угрозы безопасности устройства: несанкционированное получение данных в процессе их передачи на устройство по беспроводным каналам связи; несанкционированное копирование конфиденциальной информации на другие устройства; несанкционированный доступ к устройству и к функциям программы; неразрешенная модификация программы. В соответствии с данными угрозами возможны, в частности, следующие виды атак со стороны потенциального нарушителя: перехват и криптографический анализ трафика при обмене с удаленным сервером путем прослушивания беспроводных каналов связи; извлечение конфиденциальной информации; криптографический анализ данных, хранящихся локально, и извлечение содержимого; атаки «обратной разработки» (reverse engineering attacks) [5], исследование исполняемого кода и поиск уязвимостей.

При конфигурировании используются следующие типы компонентов защиты: протоколы безопасной передачи данных, обеспечивающие, в частности, конфиденциальность передаваемой информации; алгоритмы симметричного шифрования данных; методы удаленной аттестации; методы безопасного выполнения на основе шифрования [6], а также методы разделения кода [7]. В таблице 2 приведены значения рассматриваемых функциональных и нефункциональных свойств защиты, а также свойств совместимости программно-аппаратной платформы и компонента защиты. В зависимости от значений нефункциональных свойств, получаемых экспериментальным путем разработчиками компонентов защиты, и в зависимости от нефункциональных ограничений устройства, задаваемых при проектировании системы, различные конфигурации могут оказываться оптимальными.

Таблица 2

Примеры свойств компонентов защиты

Функциональные свойства защиты	Нефункциональные свойства	Свойства совместимости программно-аппаратной платформы
Применение безопасных коммуникационных протоколов для поддержки конфиденциальности передаваемых данных	Объем расходуемой оперативной памяти	Поддержка определенной ОС/виртуальной машины
Применение симметричного шифрования для поддержки конфиденциальности данных, сохраняемых на носителе	Величина пропускной способности сетевого интерфейса	Поддержка определенного сетевого коммуникационного протокола
Реализация функции защиты «удаленная аттестация»	Затраты на объемы данных, сохраняемых локально	
Реализация функции защиты «исполнение ПО с применением шифрования»		
Реализация функции защиты «разделение кода»		

Заключение

Разработана модель конфигурирования встроенных устройств, функционирующих в рамках сложных телекоммуникационных систем. Конфигурирование базируется на решении оптимизационной задачи и направлено на поддержку процесса защиты системы путем поиска и применения оптимальной конфигурации компонентов защиты для устройств, входящих в систему. Отличительной особенностью модели является построение комбинированной защиты на основе отдельных компонентов защиты с учетом как нефункциональных, так и функциональных свойств защиты компонентов. Нефункциональные свойства компонентов защиты позволяют задавать объемы ресурсов, которые должны обеспечиваться устройством для корректной работы функций защиты. Архитектура программного комплекса конфигурирования, предложенная в работе, раскрывает особенности механизма конфигурирования, который позволяет разработчику устройства на этапе проектирования системы получить наиболее эффективную конфигурацию защиты. Реализованный программный комплекс позволяет продемонстрировать важнейшие принципы конфигурирования на основе оптимизационной задачи, и его ограничением является использование целочисленных показателей для описания нефункциональных свойств. В дальнейшем планируется проведение экспериментов по получению численных значений для нефункциональных свойств на основе системы мобильной и быстро разворачиваемой коммуникационной сети поддержки и оперативного управления в чрезвычайных ситуациях и проведение экспериментов по оценке эффективности конфигурирования на основе сравнений результатов конфигурирования для различных критериев оптимальности.

Работа выполняется при финансовой поддержке Комитета по науке и высшей школе Правительства Санкт-Петербурга по результатам конкурсного отбора на предоставление субсидий молодым ученым, молодым кандидатам наук вузов и академических институтов, расположенных на территории Санкт-Петербурга.

СПИСОК ЛИТЕРАТУРЫ

1. Десницкий В.А., Котенко И.В., Чечулин А.А. Построение и тестирование безопасных встроенных систем // XII Санкт-Петербургская международная конференция «Региональная информатика» («РИ-2010»). Труды конференции. СПОИСУ: Санкт-Петербург. 2011. С.115-121.
2. Десницкий В.А., Чечулин А.А. Модели процесса построения безопасных встроенных систем // Системы высокой доступности, №2, 2011. С.97-101.
3. Котенко И.В., Десницкий В.А., Чечулин А.А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд, №3, 2011. С.68-75.
4. Abraham D.G., Dolan G.M., Double G.P., Stevens J.V. Transaction security system // IBM Systems Journal, No. 30, Issue 4, 1991. P.598-598.
5. Atallah M., Bryant E., Stytz M. A survey of Anti-Tamper Technologies // The Journal of Defence Software Engineering. No. 17, Vol.11, 2004. P.12-16.
6. Aucsmith D. Tamper-resistant software: An implementation // Information Hiding: First International Workshop: Proceedings, volume 1174 of Lecture Notes in Computer Science, Springer-Verlag, 1996. P.317-333.
7. Ceccato M., Preda M., Nagra J., Collberg C., Tonella P. Trading-off security and performance in barrier slicing for remote software entrusting // Journal of Automated Software Engineering, Springer. No 16, Vol.2, June 2009. P.235-261.
8. Cormen T.H., Leiserson C.E., Rivest R.L., Stein C. Introduction to Algorithms. The MIT Press, 2009.
9. Desnitsky V., Kotenko I., Chuchulin A. An abstract model for embedded systems and intruders // Proceedings of the Work in Progress Session held in connection with the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2011). Ayia Napa, Cyprus, February 2011. SEA-Publications. 2011. P.25-26.
10. Fowler M. UML Distilled: A Brief Guide to the Standard Object Modeling Language. Addison-Wesley Professional, 2003.
11. Gogniat G., Wolf T., Burleson W. Reconfigurable Security Primitive for Embedded Systems // Proceedings of System-on-Chip 2005 International Symposium, 2005. P.23-28.
12. Grand J. Practical Secure Hardware Design for Embedded Systems // Proceedings of the 2004 Embedded Systems Conference, San Francisco, California, CD-ROM, CMP Media, 2004.
13. Kocher P., Lee R., McGraw G., Ravi S. Security as a new dimension in embedded system design // DAC '04. Proceedings of the 41st Design Automation Conference. 2004. P.753-760.
14. Kommerling O., Kuhn M.G. Design principles for tamper-resistant smartcard processors // Proceedings of the USENIX Workshop on Smartcard Technology, 1999. P.9-20.

15. Koopman P. Embedded System Security // IEEE Computer, No. 37, Vol.7, July 2004. P.95-97.
16. Lee G.M., Kim J.Y. The Internet of Things – A problem statement // Information and Communication Technology Convergence (ICTC), 2010 International Conference on 17-19 Nov. 2010. P.517-518.
17. Mastotakis N. E., Caraus I., Tkachenko A. The DEA method in economical efficiency analysis (micro-level) // Proceeding MATH'07 of the 11th WSEAS International Conference on Applied Mathematics World Scientific and Engineering Academy and Society (WSEAS) Stevens Point, Wisconsin, USA, 2007. P.103-107.
18. Ovaska E., Balogh A., Campos S., Noguero A., Pataricza A., Tiensyrjä K. Model and Quality Driven Embedded Systems Engineering. Technical Research Centre of Finland, 2009.
19. Rae A.J., Wildman L.P. A Taxonomy of Attacks on Secure Devices. Department of Information Technology and Electrical Engineering, University of Queensland, Australia, 2003.
20. Ruiz J.F., Harjani R., Maña A., Desnitsky V., Kutenko I., Chechulin A. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components // The 20th Euromicro International Conference on Parallel, Distributed and Network-Based Computing (PDP2012). Munich, Germany, February 15-17, 2012.

Коноплев А.С.

Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

БЕЗОПАСНОЕ РАСПРЕДЕЛЕНИЕ ПОЛЬЗОВАТЕЛЬСКИХ ЗАПРОСОВ В ГРИД-СИСТЕМАХ

Введение

Грид-системы представляют собой разновидность информационно-телекоммуникационных систем распределенных вычислений, в которых компьютеры пользователей объединены в один вычислительный кластер, обеспечивающий совместное пользование его ресурсами. Одна из проблем обеспечения информационной безопасности в грид-системах – возможность несанкционированного доступа к вычислительным ресурсам и данным пользователей. Указанная проблема обусловлена особой природой таких систем, в основе которой лежит принцип совместного пользования инфраструктурой системы, реализуемый посредством механизма виртуальных организаций. Виртуальная организация (ВО) – динамическое сообщество пользователей, которые совместно используют ресурсы грид-системы в соответствии с решаемой задачей и согласованными между ними правилами. Каждый пользователь грид-системы может в любой момент времени состоять сразу в нескольких ВО. При этом динамика изменения состава ВО в грид-системах крайне высока.

Для разделения полномочий пользователей в грид-системах реализуются политики информационной безопасности, которыми регулируются правила доступа вида «субъект-объект-права доступа». Соблюдение правил политик информационной безопасности гарантируется посредством контроля и управления доступом пользователей к данным и ресурсам грид-систем. Гетерогенность грид-систем, наличие нескольких механизмов авторизации пользователей, а также отсутствие централизованного сервера безопасности затрудняют возможность реализации классических моделей контроля и управления доступом.

В работе [1] представлена логическая модель контроля и управления доступом в грид-системах, позволяющая задавать политики информационной безопасности с учетом различных механизмов авторизации пользователей при доступе к ресурсам. При этом грид-система представляется в виде множества состояний. Поскольку каждый пользователь грид-системы может в любой момент времени состоять сразу в нескольких ВО, недостаточно статического описания состояний безопасности грид-систем, т.к. необходимо моделировать динамическое распределение запросов пользователей. Кроме того, в указанной модели не учитываются предустановленные отношения доступа в хостовых средах.

1. Моделирование безопасности грид-систем

Автором предложен подход, позволяющий обеспечить защиту от несанкционированного доступа к ресурсам грид-систем на основе безопасного распределения запросов пользователей на предоставление ресурсов – в соответствии с требованиями политик информационной безопасности. Реализация данного подхода предусматривает описание предустановленных отношений в хостовых средах с учетом динамики состояний грид-систем с помощью математического аппарата цветных функциональных сетей Петри.

Узлы грид-системы (провайдеры ресурсов) представим в виде конечного непустого множества вершин $RP = \{rp_i\}$ сети Петри, задаваемой графом $c = (RP, T, *)$, где $T = \{t_i\}$ – множество переходов между вершинами графа c , $*$ – отношение между вершинами (дуги графа). Метками (маркерами) цветной сети Петри обозначим запросы пользователей грид-системы на предоставление определенного типа ресурса. Каждый переход между вершинами графа c представлен вероятностной функцией (например, временем нахождения метки в очереди).

В общем случае множество пользователей U и множество вершин RP могут не совпадать. Это объясняется тем, что на одном и том же узле грид-системы могут работать сразу несколько пользователей. С другой стороны, на некоторых узлах может не быть авторизовано ни одного пользователя, хотя вычислительные мощности данного узла могут быть включены в состав грид-системы. Для усреднения условимся, что каждой хостовой системе сопоставлен один пользователь грид-системы. Предположим, все пользовательские запросы проходят через провайдер ресурсов

RP_2 , а инициировать задачи могут пользователи U_1 и U_5 (рисунок 1). Причем указанные задачи всегда можно выполнить силами подключенных к RP_2 провайдеров ресурсов RP_3 и RP_4 .

Пусть t_{ij} – вероятность перехода маркера от одного узла грид-системы к другому. t_{11} , t_{12} – вероятности того, что для выполнения пользовательского задания потребуются вычислительные мощности узлов RP_3 и RP_4 , соответственно. t_{13} – вероятность того, что для выполнения указанного задания необходимы совместные вычислительные мощности двух хостовых систем. Такая ситуация возможна, например, когда для выполнения задания необходимо исполнение двух программ, каждая из которых установлена только на одной хостовой системе. t_{14} и t_{15} – вероятности того, что задача будет успешно отработана на соответствующей хостовой системе, и ее результат возвращен пользователям U_1 или U_5 .

В грид-системах всегда имеется несколько провайдеров ресурсов, соединенных друг с другом. Провайдеры ресурсов могут перераспределять задачи между собой (переходы t_{31} и t_{32}), что происходит в двух случаях:

1. На провайдере ресурсов достигнуто предельно допустимое количество активных запросов. В этом случае происходит балансировка нагрузки между провайдерами ресурсов.
2. Хостовые системы, подключенные к провайдеру ресурсов, не обладают нужным типом (или количеством) вычислительных ресурсов. В этом случае часть запросов передается подходящему провайдеру ресурсов.

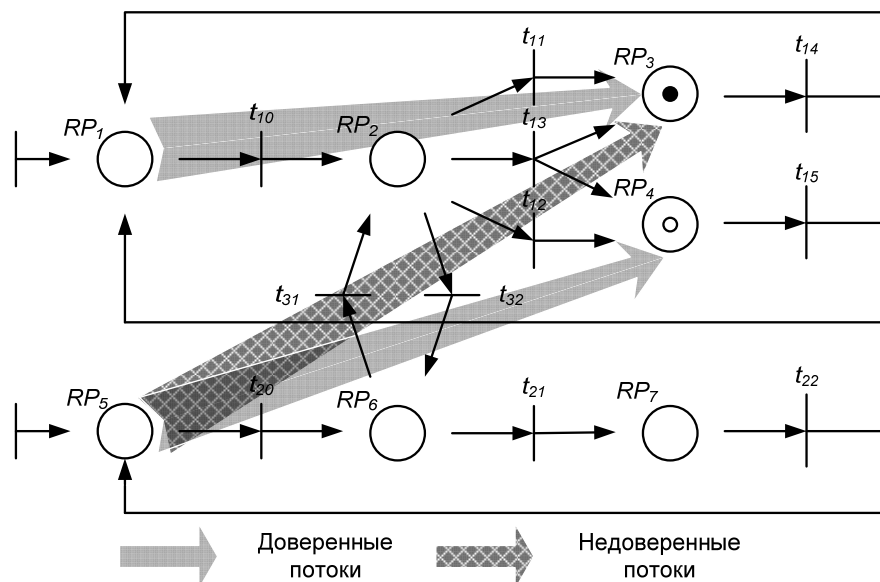


Рис. 1. Пример представления грид-системы с помощью сети Петри

Начальная маркировка сети Петри характеризуется вектором $\mu = (\mu(RP_1), \dots, \mu(RP_n))$, где n – число позиций сети Петри. Условимся, что для сети, изображенной на рисунке 1, начальная маркировка $\mu = (1, 0, 0, 0)$. Это означает, что в начальный момент времени в грид-систему поступает запрос на выполнение некоторого задания от пользователя U_1 . Пусть указанное задание представляет собой запрос к данным пользователя, которые расположены на хосте RP_3 . На рисунке 1 задание пользователя U_1 обозначено черным маркером. Далее в грид-системе появляется запрос на предоставление вычислительных ресурсов со стороны пользователя U_5 . Данный запрос обозначен полым маркером. Предположим, политика информационной безопасности в рассматриваемой грид-системе задана таким образом, чтобы ограничить доступ пользователя U_5 к данным пользователя U_1 . Тогда возможна ситуация, при которой вновь поступивший запрос (от пользователя U_5) также окажется на хосте RP_3 , где хранит свои данные пользователь U_1 . Следовательно, приложения, исполняющиеся на хосте RP_3 от имени пользователя U_5 (а значит, и сам пользователь U_5), получат доступ к закрытым данным. Таким образом, при распределении

заданий пользователей грид-системы необходимо учитывать предустановленные отношения доступа на хостовых системах.

2. Распределение заданий пользователей грид-системы

В построенной модели грид-системы функции переходов между вершинами графа определены вероятностно, что не позволяет учитывать ограничения, накладываемые требованиями политик информационной безопасности. Перейдем к функциональным сетям Петри, определив вид функции, действующей на множестве переходов $\{t_{ij}\}$ таким образом, чтобы при перемещении меток из одной вершины графа в другую выполнялась проверка соответствия заданным ограничениям. Введем множество ограничений SP , заданных в правилах политик информационной безопасности, а также множество предустановленных отношений R , т.е. множество запросов (меток сети Петри), которые в данный момент присутствуют в указанном узле грид-системы.

Согласно [2] пользователь $User$ имеет право пользования вычислительными ресурсами $CompAccessRight$ провайдера ресурсов $ResProv$ в данный момент времени $CurTime$, если пользователь и провайдер ресурсов доверяют друг другу (т.е. успешно прошли процедуру аутентификации) и на указанном хосте для пользователя $User$ определена учетная запись, от имени которой будут исполняться приложения, запускаемые данным пользователем:

$$\begin{aligned} &HasCompAccessRight(User, ResProv) \\ &= (IsTrustedByU(User, ResProv) \wedge \\ &IsTrustedByRP(ResProv, User) \wedge \\ &(MapUserToUID(ResProv, User) \neq \emptyset)). \end{aligned} \quad (1)$$

Множеством всех заданий в системе является множество J . Каждое задание характеризуется пользователем (множество U), который инициировал данную задачу, и одним из следующих типов (множество $ResourceType$): запрос вычислительных ресурсов или данных пользователя.

$$\begin{aligned} &JobToU: J \rightarrow U, \\ &GetJobType: J \rightarrow ResourceType, \\ &ResourceType = \{'CompRes', 'StorageRes'\}, \\ &IsCompJobType: J \rightarrow \{1, 0\}. \end{aligned}$$

Последняя функция возвращает 1 когда тип задания соответствует значению 'CompRes'. Каждый провайдер ресурсов также характеризуется совокупностью типов из множества $ResourceType$, определяющей какими ресурсами обладает данный узел грид-системы:

$$\begin{aligned} &GetRPTypes: RP \rightarrow ResourceType^k, \\ &k \in \{1, \dots, n\}, n = |ResourceType|. \end{aligned}$$

Кроме того, провайдер ресурсов характеризуется состоянием (множество $RPState$), показывающим, свободен ли он в данный момент:

$$GetRPState: RP \rightarrow \{'Avaliable', 'Busy'\}.$$

Поскольку мы считаем, что каждый пользователь грид-системы сопоставлен с некоторым хостом, введем функцию, позволяющую по имени пользователя определить его "домашний" хост:

$$GetUserHost: U \rightarrow RP.$$

Как было сказано выше, политика информационной безопасности в грид-системе представляет собой совокупность правил (ограничений), определяющих какой пользователь к какому хосту (или объекту ФС на хосте) может получить доступ. При этом тип запрашиваемого доступа однозначно соответствует одному из доступных типов ресурсов грид-системы. Тогда функция получения ограничений политики информационной безопасности (множество SP) грид-системы имеет следующий вид:

$$AllowedSPrights: \langle SP, U, RP \rangle \rightarrow ResourceType^k.$$

Множество предустановленных отношений доступа представляет собой совокупность записей о том, какой тип доступа, каким пользователем грид-системы и на каком провайдере ресурсов уже предоставлен:

$$\begin{aligned} &GetRelationsUsers: \langle R, RP \rangle \rightarrow U_{rp} \subset U, \\ &GetUserAccessType: \langle R, RP, U \rangle \rightarrow ResourceType. \end{aligned}$$

Попытка получения доступа к провайдеру ресурсов должна удовлетворять требованиям политики безопасности с учетом предустановленных отношений на указанном хосте:

$$\begin{aligned}
 &IsJobAllowed: \langle J, RP, SP, R \rangle \rightarrow \{0,1\} \\
 &IsJobAllowed: \langle Job, ResProv, SecPol, Relations \rangle \rightarrow IsRPAppr(Job, ResProv) \\
 &\wedge ((\forall User \in GetRelationsUsers(Relations, ResProv)) \\
 &TheSameAccess(User, ResProv, Job) \vee \\
 &IsAccessAllowedBySP(User, ResProv, Job, SecPol)).
 \end{aligned} \tag{2}$$

Первая часть функции проверяет, что запрашиваемый провайдер ресурсов свободен и имеет соответствующий тип:

$$\begin{aligned}
 &IsRPAppr: \langle J, RP \rangle \rightarrow \{0,1\} \\
 &IsRPAppr: \langle Job, ResProv \rangle \rightarrow (GetJobType(Job) \in GetRPTypes(ResProv)) \\
 &\wedge GetRPState(ResProv) = 'Avaliable'.
 \end{aligned}$$

Требования политики информационной безопасности не нарушаются, если запрашиваемый тип доступа совпадает с тем, что уже имеется на данном провайдере ресурсов:

$$\begin{aligned}
 &TheSameAccess: \langle U, RP, J \rangle \rightarrow \{0,1\} \\
 &TheSameAccess: \langle User, ResProv, Job \rangle \rightarrow GetUserAccessType(ResProv, User) \\
 &= GetJobType(Job).
 \end{aligned}$$

Если пользователю предоставлен тип доступа, отличный от того, что содержится в поступившем задании, необходимо убедиться, что политика безопасности не будет нарушена в случае предоставления запрашиваемого доступа:

$$\begin{aligned}
 &IsAccessAllowedBySP: \langle U, RP, J, SP \rangle \rightarrow \{0,1\} \\
 &IsAccessAllowedBySP: \langle User, ResProv, Job, SecPol \rangle \rightarrow (IsCompJobType(Job) \wedge \\
 &GetJobType(Job) \in AllowedSPRights(SecPol, JobToU(Job), GetUserHost(User))) \vee \\
 &(\neg IsCompJobType(Job) \wedge GetUserAccessType(ResProv, User) \in \\
 &AllowedSPRights(SecPol, User, GetUserHost(JobToU(Job)))).
 \end{aligned}$$

Перемещение задания пользователя с узла rp_i на узел rp_j означает выполнение достаточных условий для срабатывания перехода t_{ij} [2]. Введем оператор Ψ , который действует на множестве переходов $\{t_{ij}\}$:

$$\Psi: \langle J, RP, SP, R \rangle \rightarrow \{0,1\}. \tag{3}$$

Таким образом, в рамках безопасного распределения заданий пользователей оператор переходов (3) с учетом (1) и (2) имеет следующий вид:

$$\begin{aligned}
 &\Psi: \langle Job, ResProv, SecPol, Relations \rangle \rightarrow \\
 &HasCompAccessRights(JobToU(Job), ResProv) \wedge \\
 &IsJobAllowed(Job, ResProv, SecPol, Relations).
 \end{aligned}$$

Задачу поиска узлов, подходящих для выполнения пользовательских заданий, выполняет специальная служба грид-систем, функционирующая на провайдерах ресурсов. Следовательно, для решения рассмотренной задачи оператор Ψ должен быть интегрирован в ее состав. Таким образом, при выборе подходящего узла будет учитываться не только их доступность и тип ресурсов грид-системы, которыми располагает данный узел, но и требования политик информационной безопасности, разрешающих или запрещающих использование ресурсов на указанном узле пользователем, инициировавшим запрос. На рисунке 1 показано распределение заданий пользователей грид-системы с учетом оператора Ψ (сплошные стрелки) и без него (заштрихованные стрелки).

Заключение

Предложенный автором способ безопасного распределения пользовательских запросов в грид-системах, реализация указанного программного модуля и его интеграция в составе провайдеров ресурсов позволят обеспечить гарантированность защиты ресурсов грид-систем, автоматизировать процедуру анализа безопасности грид-систем, и тем самым обеспечить высокий уровень надежности

и безопасности грид-систем, используемых для построения доверенных информационно-телекоммуникационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Калинин, М.О. Верификация требований политик информационной безопасности в grid-системах / М.О. Калинин, Я.А. Марков. — Проблемы информационной безопасности. Компьютерные системы. — 2011. — 2. — 21 с.
2. Коноплев, А.С. Обеспечение высокой защищенности информационно-телекоммуникационных систем распределенных вычислений / А.С. Коноплев. — Сб. материалов Всероссийской научно-методической конференции «Фундаментальные исследования и инновации в национальных исследовательских университетах». — 2012. — 1. — 83 с.

Харинов М.В., Заболотский В.П.

Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПОДХОД К ПРОБЛЕМЕ СЕГМЕНТАЦИИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ ПОСРЕДСТВОМ
ОПТИМИЗАЦИИ ПОСЛЕДОВАТЕЛЬНОСТИ РАЗБИЕНИЙ

Введение

В современной обработке цифровых изображений одной из ключевых продолжает оставаться, так называемая, «проблема сегментации», которая в постановочной части сводится к формальному определению понятия сегментированного изображения. Определить сегментированное изображение, значит отличить, выделить его среди изображений, тем или иным способом разделенных на сегменты, не ссылаясь на конкретные алгоритмы разбиения изображения на сегменты, а также на неформализованное зрительное восприятие сегментов, занимаемых «объектами».

Требуемым условиям удовлетворяет определение сегментированного изображения как оптимального приближения. При этом каждому разбиению изображения сопоставляется некоторый функционал (вещественное число), и оптимальным разбиением считается разбиение, для которого значение функционала оказывается минимальным. Первыми подходами к сегментации на основе оптимизации являются метод Оцу (Н.Оцу, [1], P.-S Liao и др. [2]) и модель Мамфорда–Шаха (D. Mumford, J. Shah [3, 4], А.С. Бугаев, А.В. Хельвас [5]). Более поздним является популярный в настоящее время метод «разрезов графов» (Y. Boykov, V. Kolmogorov [6], Ю.В. Визильтер и др. [7]). В модели Мамфорда–Шаха и методе «разрезов графов» минимизируется функционал, который состоит из двух слагаемых, «компенсирующих» друг друга при изменении разбиения изображения. Смысл введения составного функционала состоит, прежде всего, в том, чтобы при определенных условиях получить алгоритмы точного решения задачи сегментации, которая сводится к нахождению оптимального разбиения изображения.

В статье развиваются вычисления в модели Мамфорда–Шаха, в которой приближения изображения получаются заполнением сегментов средними значениями яркости. В качестве функционала рассматривается «однокомпонентное» среднеквадратичное отклонение приближения от изображения [1, 2, 5], которое имеет тривиальный минимум при разбиении изображения на отдельные пиксели или связанные сегменты из одинаковых пикселей. Особенностью постановки проблемы сегментации является то, что сегментированное изображение определяется как оптимальное приближение при каждом значении числа сегментов от единицы до N , где N — число элементарных сегментов в изображении. В такой постановке пока не найдено точного решения задачи сегментации даже для случая разбиения изображения на два сегмента, а прямой перебор вариантов оказывается не эффективным уже для изображений размером 10×10 пикселей из-за недостаточного быстродействия современных компьютеров.

В задачах выделения объектов оказываются применимыми алгоритмы слияния сегментов, выработанные для минимизации оригинального функционала модели Мамфорда–Шаха [3, 4], которые упрощаются в случае редуцированного функционала [5]. Однако для вычисления последовательности оптимальных приближений слияние сегментов оказывается недостаточным, поскольку сегменты из различных оптимальных разбиений, в общем случае, могут перекрываться [8].

Для вычисления приближений, более близких к изображению по среднеквадратичному отклонению, слияние сегментов дополняется операцией коррекции границ, которая выполняется при условии сохранения при этом целостности сегмента. Поочередное выполнение операций слияния/коррекции сегментов позволяет для каждого числа сегментов улучшить визуальное качество приближений изображения и построить модель оптимального приближения изображения, в которой пиксели приближения разделяются на пиксели «площадок» и пиксели «соединений» шириной в один пиксель. Первые зрительно воспринимаются как «объекты», а вторые описывают близость объектов между собой. При этом с уменьшением числа сегментов каждый сегмент покрывает несколько объектов, что позволяет избежать «стирания» объектов, характерного для выполнения сегментации в алгоритмах обычного слияния сегментов.

Таким образом, в статье рассматривается версия модели Мамфорда–Шаха, в которой:

— сегментированное изображение определяется как оптимальное приближение для каждого числа сегментов;

— в дополнение к слиянию сегментов вводится операция их коррекции с сохранением целостности;

— предлагается модель сегментированного изображения, состоящее из «площадок» и «соединений» шириной в один пиксель.

Следует отметить, что инновации в области хранения, передачи, анализа и распознавания изображений применяются, прежде всего, в аппаратно-программных комплексах специального назначения. Поэтому развитие отечественных решений ключевых проблем обработки изображений, в частности, проблемы сегментации, имеет немаловажное значение для компенсации традиционного отставания аппаратных средств.

1. Примеры сегментации

Для решения проблемы вычисления оптимальных приближений изображения полезно представить примеры реального изображения, сегментированного с минимальной суммарной квадратичной ошибкой или минимальным среднеквадратичным отклонением $StdDev$ (рисунок 1).



Рис. 1. Оптимальное приближение изображения в двух градациях (в центре) и близкое к оптимальному приближение двумя связными сегментами (справа). Слева — исходное изображение «Лена»

На рисунке 1 показаны приближения изображения с минимальными значениями $StdDev$ в двух градациях яркости, а также парой связных сегментов. Над приближениями указаны анализируемые множества пикселей. Значения $StdDev$ выписаны под приближениями.

В центре рисунка 1 помещено оптимальное приближение стандартного изображения, полученное пороговым преобразованием по яркости, минимизирующим среднеквадратичное отклонение $StdDev$ приближения от изображения. Именно это представление изображения можно найти в электронных публикациях, описывающих метод Оцу [1]. Справа на рисунке 1 демонстрируется приближение стандартного изображения двумя связными сегментами, которое по значению $StdDev$ приближается к точной нижней границе и именуется, поэтому, приближением «близким к оптимальному».

Сравнивая приближения на рисунке 1, нетрудно заметить, что приближение изображения связными сегментами имеет выраженную структуру и состоит из «площадок» и «соединительных» элементов шириной в один пиксель, слабо влияющих на среднеквадратичное отклонение. При этом оптимальное приближение можно преобразовать в приближение, близкое к оптимальному, если некоторые «площадки» на нем стереть, а остальные соединить между собой посредством «соединительных» элементов.

Особенностью близкого к оптимальному приближения изображения связными сегментами рисунке 1 является то, что каждый сегмент покрывает несколько объектов, сливающихся между собой на некоторых участках. В расчетах по модели Мамфорда–Шаха посредством одного только слияния сегментов в результирующих приближениях выделяется меньшее количество объектов. Из-за пропущенных соединительных элементов часть объектов теряется, а среднеквадратичное отклонение возрастает. При этом выделение тех или иных объектов зависит от случайных причин, например, от исходного разбиения изображения на самостоятельные пиксели, или сегменты из одинаковых пикселей. На результат сегментации при малом числе сегментов могут влиять даже ошибки округления.

Таким образом, улучшение сегментации по среднеквадратичному отклонению интересно с точки зрения получения стабильной сегментации изображения в модели Мамфорда–Шаха, особенно при малом числе сегментов. При этом имеет смысл разделить задачу на вычисление «площадок» посредством оптимальных приближений изображения в различном числе градаций яркости и нахождение «соединительных» элементов, которые могут интерпретироваться буквально, как на рис. 1, или устанавливаться формально как «виртуальные».

2. Последовательность оптимальных приближений при каждом числе градаций яркости

В определенном смысле построить решение задачи вычисления всей последовательности оптимальных приближений при каждом числе $n = 1, 2, 3, \dots, N$ градаций яркости оказывается проще,

чем минимизировать среднеквадратичное отклонение для фиксированного числа градаций. Общая постановка задачи подсказывает логику итеративного построения требуемых приближений, отталкиваясь от тривиальных оптимальных приближений при единственной градации и максимальном числе градаций яркости ($n = 1$ и $n = N$).

При известном текущем приближении с минимальным среднеквадратичным отклонением, очередное приближение получается слиянием или разделением диапазонов яркости с последующей их коррекцией, которая выполняется при неизменном числе диапазонов n до тех пор, пока модифицируемое разбиение шкалы яркости на диапазоны не окажется устойчивым относительно реклассификации вложенных диапазонов пикселей. Затем выполняется очередное слияние, или разделение диапазонов яркости, при котором число диапазонов изменяется на единицу. При каждой реклассификации среднеквадратичное отклонение уменьшается. Процесс обработки посредством слияния/разделения диапазонов яркости по очереди с их коррекцией повторяется до получения последовательности устойчивых сегментированных приближений с минимальными значениями среднеквадратичного отклонения *StdDev*.

Как показывает эксперимент, большинство результирующих разбиений с минимальными значениями *StdDev* вычисляются на первом цикле обработке, а остальные незначительно уточняются на нескольких последующих циклах, что является признаком адекватной аппроксимации цифровых изображений ступенчатой функцией. В применяемом методе поиска оптимальных приближений процесс вычислений зависит от порядка анализа диапазонов яркости, тогда как результирующие приближения с минимальными значениями среднеквадратичного отклонения не должны от него зависеть. Неизменность результатов расчетов при модификации алгоритма вычислений за счет изменения порядка анализа диапазонов яркости контролировалась в качестве признака достижения минимально возможных значений *StdDev*.

Всего оптимальных приближений 216, так как в изображении «Лена» встречается 216 различных значений яркости. Оптимальные приближения характеризуются устойчивостью относительно реклассификации пикселей и инвариантны относительно линейного преобразования яркостей пикселей изображения, а также преобразования изображения в негатив. Характерно, что минимальные значения *StdDev* достигаются при неиерархической структуре приближений с перекрытиями диапазонов из различных разбиений.

3. Последовательность оптимальных приближений при каждом числе сегментов

Получение оптимальных приближений изображения связными сегментами является интересной вычислительной проблемой, хотя с формальной точки зрения последовательное приближение изображения связными сегментами принципиально не отличается от его приближения пикселями из различных диапазонов яркости. В процессе коррекции вместо неизменного числа градаций поддерживается неизменное число сегментов. Для этого коррекция выполняется посредством реклассификации пикселей из данного сегмента–донора в смежные сегменты–акцепторы при условии сохранения целостности сегмента–донора.

В отличие от программ генерации оптимальных разбиений при каждом числе градаций яркости, в разработанных программах аппроксимации изображения связными сегментами операция разделения сегментов не используется. Исходным приближением служит изображение, разделенное на пиксели. Приближения строятся посредством чередования слияния и коррекции сегментов изображения. При очередном слиянии сегментов в качестве исходных принимаются устойчивые приближения изображения, полученные в результате коррекции. При коррекции смежные сегменты обмениваются между собой пикселями, которые группируются в подмножества из условий максимального падения среднеквадратичного отклонения. Для получаемых устойчивых приближений гарантируется, что, если реклассификация любого пикселя не нарушает целостность сегмента–донора, то увеличивает или, по крайней мере, сохраняет среднеквадратичное отклонение приближения от изображения.

4. Сравнительный анализ последовательностей приближений изображения

Эксперименты показывают, что использование в модели Мамфорда–Шаха [3–5] дополнительной операции коррекции связных сегментов позволяет существенно улучшить результаты аппроксимации изображения по среднеквадратичному отклонению (рисунок 2).

Рисунок 2 описывает последовательное приближение изображения связными сегментами по различным алгоритмам, и иллюстрирует поведение среднеквадратичного отклонения *StdDev* при возрастании числа сегментов n от 1 до 1000, отложенном по оси абсцисс в логарифмическом масштабе. Графики на рисунке 2 представляют собой монотонные невозрастающие кривые, которые расходятся из точки максимального значения *StdDev* на оси ординат, описывающей приближение, составленное из пикселей со средней по изображению яркостью.

Пара ступенчатых кривых серого цвета получена в эвристических алгоритмах слияния сегментов, которые при малом числе сегментов вместо выделения объектов приводят к разрушению

изображения. На графиках неудачный выбор алгоритмов проявляется в наличии участков стабилизации среднеквадратичного отклонения, а на изображении при этом выделяются сегменты, отвечающие зрительно незначимым объектам [9].

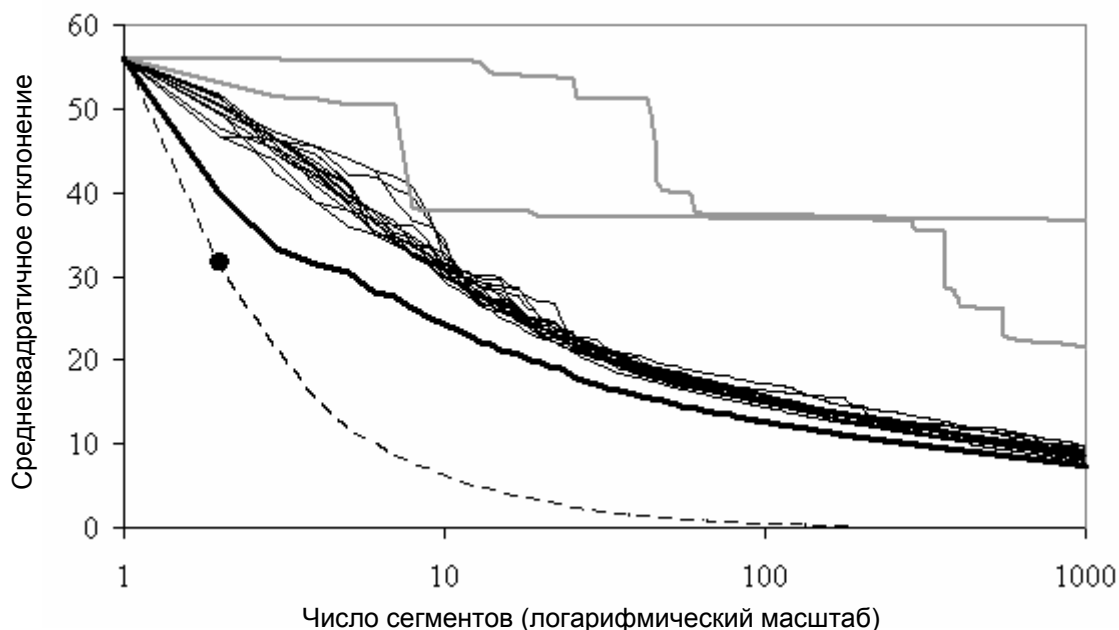


Рис. 2. Среднеквадратичное отклонение в зависимости от числа сегментов

Двадцать переплетающихся сплошных тонких кривых, сливающихся в полосу, описывают иерархические последовательности приближений, полученные в различных модификациях модели Мамфорда–Шаха [3–5, 9]. Одна из кривых отвечает версии FLSA (Full λ –Scheduled Algorithm) модели Мамфорда–Шаха [10], которая учитывает суммарную длину границ между сегментами и активно применяется на практике. Для применения модели Мамфорда–Шаха характерно, что с возрастанием числа сегментов наблюдается интенсивное падение *StdDev*, и, по сравнению с эвристическими алгоритмами, при малом числе сегментов лучше выделяются те или иные объекты. Однако в зависимости от изменчивых начальных условий и особенностей вычислений многие объекты оказываются пропущенными.

Жирная сплошная кривая описывает неиерархическую последовательность приближений изображения, полученную в алгоритме слияния сегментов по очереди с их коррекцией. На каждой итерации значение *StdDev* сначала увеличивается при слиянии очередной пары сегментов и уменьшении числа сегментов на 1, и затем уменьшается при неизменном числе сегментов. При этом вычисление последовательности приближений описывается некоторой зигзагообразной кривой, а обсуждаемая кривая является огибающей, проведенной через точки, отвечающие устойчивой сегментации изображения при каждом числе сегментов n . По сравнению с иерархическими приближениями, полученными посредством одного только слияния сегментов, приближения с перекрытиями сегментов из различных разбиений лучше аппроксимируют изображение по среднеквадратичному отклонению. На них проявляется большее количество объектов.

Плавная пунктирная кривая представляет собой зависимость значений среднеквадратичного отклонения *StdDev* от числа градаций яркости, которая получена для оптимальных приближений изображения. Указанные значения не зависят от геометрического перераспределения пикселей в изображении и с некоторым запасом ограничивают снизу предельные значения *StdDev*, достижимые при соответствующих значениях числа сегментов n .

Жирная точка на рисунке 2, расположенная несколько выше пунктирной кривой, отвечает близкому к оптимальному приближению изображения двумя связными сегментами с *StdDev* = 31,603, показанному на рисунке 1. По логике постановки задачи, жирная кривая, описывающая последовательность приближений изображения связными сегментами, должна проходить через обсуждаемую точку. Но она оказывается выше. Поэтому, хотя текущая программная реализация обеспечивает заметное улучшение приближений изображения по *StdDev*, возможности дальнейшего развития аппроксимации изображения устойчивыми приближениями с автоматическим формированием «площадок» и «соединительных» элементов, вероятно, пока не исчерпаны.

Следует заметить, что для описания несвязных объектов понятие сегмента можно трактовать в обобщенном смысле, ослабляя условие связности пикселей, например, допуская нарушение связности

сегмента–донора в процессе коррекции по алгоритму наращивания сегмента–акцептора. В предельном случае, связность пикселей можно игнорировать и строить приближение изображения так называемыми, «обобщенными» сегментами в виде множеств пикселей, для которых определено отношение соседства (или смежности), как для обычных связанных сегментов, но не обязательна связность пикселей. В этом случае, операция коррекции не выводит из множества «обобщенных» сегментов, и при обмене пикселями связность не контролируется.

Замещение связанных сегментов «обобщенными» сегментами в алгоритме слияния/коррекции на изображении «Лена» приводит к тому, что, сначала, при больших значениях числа обобщенных сегментов n и его снижении вплоть до нескольких десятков, значения $StdDev$ держатся в окрестности $StdDev = 1,5$. При этом формируются 216 множеств из пикселей одинаковой яркости, которые затем, при уменьшении числа n до тридцати обобщенных сегментов, образуют приближения со стабильно возрастающими значениями $StdDev$. Примечательно, что при числе обобщенных сегментов в пределах трех десятков получаются практически те же самые приближения стандартного изображения, что и в алгоритме гистограммной обработки. Обсуждаемый пример удачно иллюстрирует тезис об определении сегментированного изображения независимо от технологии его получения.

5. Аналитическое обобщение операции слияния сегментов

Очевидно, что операцию слияния произвольных множеств пикселей можно трактовать как частный случай реклассификации пикселей из одного множества в другое.

Пусть, для общности рассмотрения, пиксели характеризуются некоторым набором признаков и описываются векторами вещественных чисел. Компонентами векторов могут служить, например, значения яркости по цветовым компонентам, усредненные по сегментам некоторого начального разбиения изображения.

Рассмотрим реклассификацию k пикселей, исключаемых из множества 1 и включаемых в число пикселей множества 2. Тогда сопутствующее приращение ΔE квадратичной ошибки E выражается в виде:

$$\Delta E = \begin{cases} \Delta E_{merge}, & k = n_1, \\ \Delta E_{correct}, & k < n_1, \end{cases} \quad (1)$$

где n_1, n_2 — число пикселей в множествах 1 и 2, соответственно, а ΔE_{merge} и $\Delta E_{correct}$ имеют вид:

$$\Delta E_{merge} = \frac{\|I_1 - I_2\|^2}{\frac{1}{n_1} + \frac{1}{n_2}}, \quad \Delta E_{correct} = \frac{\|I - I_2\|^2}{\frac{1}{k} + \frac{1}{n_2}} - \frac{\|I - I_1\|^2}{\frac{1}{k} - \frac{1}{n_1}}, \quad (2)$$

где I — вектор средних значений признаков для реклассифицируемых k пикселей, I_1 и I_2 — вектора признаков, усредненные по множествам 1 и 2, соответственно, а знак $\| \cdot \|$ обозначает евклидову длину вектора.

ΔE_{merge} описывает приращение квадратичной ошибки при слиянии множеств пикселей посредством реклассификации всех пикселей из множества 1 в множество 2 и уменьшении числа множеств на 1. $\Delta E_{correct}$ описывает приращение квадратичной ошибки при реклассификации части пикселей из множества 1 в множество 2 и сохранении числа множеств пикселей.

Далее условимся разделять термины «слияние» и «реклассификация», употребляя последний только в узком смысле, для обозначения модификации классификации части пикселей.

Сегментация выполняется посредством итеративного слияния рассматриваемых множеств пикселей по очереди с коррекцией.

Следуя [5], слияние множеств 1 и 2 выполняется при минимальной величине приращения квадратичной ошибки ΔE_{merge} :

$$\Delta E_{merge} = \min. \quad (3)$$

Коррекция множеств выполняется посредством реклассификации пикселей из условия уменьшения квадратичной ошибки. Критерием коррекции является отрицательная величина приращения квадратичной ошибки $\Delta E_{correct}$:

$$\Delta E_{correct} < 0. \quad (4)$$

Элементарным преобразованием из (2) и (5) получаем условие коррекции, учитывающее только знак $\Delta E_{correct}$:

$$\|I - I_1\| > \alpha \cdot \|I - I_2\|. \quad (5)$$

где коэффициент $\alpha < 1$ описывает соотношение количеств пикселей в множествах и определяется в виде:

$$\alpha \equiv \sqrt{\frac{n_2(n_1 - k)}{n_1(n_2 + k)}}. \quad (6)$$

Из (5), (6) для реклассификации k одинаковых пикселей следует, что если среднеквадратичное отклонение снижается при реклассификации одного пикселя, то оно снижается и при реклассификации остальных пикселей, поскольку с ростом k коэффициент α уменьшается.

Применяя логическое отрицание к выражениям (4), (5), получаем условие устойчивости:

$$\Delta E_{correct} \geq 0 \Leftrightarrow \|I - I_1\| \leq \alpha \cdot \|I - I_2\|. \quad (7)$$

Разбиение пикселей изображения на множества считается устойчивым, если для всех рассматриваемых пар множеств реклассификация заданных подмножеств пикселей из одного множества в другое не приводит к уменьшению среднеквадратичного отклонения.

Очевидно, что оптимальное разбиение изображения является устойчивым, но устойчивое разбиение не обязательно оптимально. Ограничения на допустимые пары множеств 1 и 2, например, обменивающихся пикселями при сохранении связности, или рассмотрение одновременной реклассификации двух и более подмножеств пикселей приводит к различным вариантам программной реализации условия устойчивости (7).

Следует заметить, что метод k – средних [11–13], вообще говоря, приводит к неустойчивому разбиению пикселей с завышенным значением среднеквадратичного отклонения, поскольку в этом методе не учитывается коэффициент α (6).

Заключение

Таким образом, для оптимизации приближений по среднеквадратичному отклонению предложено дополнить слияние множеств пикселей в модели Мамфорда–Шаха операцией коррекции, описываемой выражениями (4)–(6). Для развития вычислений с сегментами изображения обобщено понятие связности множеств, к которым либо предъявляется, либо не предъявляется условие связности пикселей, относимых к одному множеству. В качестве формального признака оптимального разбиения установлено свойство (7) устойчивости сегментации относительно предусмотренных вариантов реклассификации пикселей.

Одним из перспективных направлений дальнейших исследований является применение формул (1)–(7) в контексте разработки и реализации метода кластеризации, альтернативного методу k –средних, который, вероятно, будет полезен для улучшения сегментации цветowych, а также многоспектральных изображений.

СПИСОК ЛИТЕРАТУРЫ

1. Otsu N. A Threshold Selection Method from Gray-Level Histograms // IEEE Transactions on systems, MAN, and CYBERNETICS, Vol. SMC-9, № 1, 1979. – pp. 62–66.
2. Ping-Sung Liao, Tse-Sheng Chen, Pau-Choo Chung. A Fast Algorithm for Multilevel Thresholding // J. Inf. Sci. Eng. Vol. 17 (5), 2001. – pp. 713–727.
3. Mumford D., Shah J. Boundary detection by minimizing functionals // Proc. IEEE Comput. Vision Patt. Recogn. Conf. – San Francisco, 1985. – P. 22–26.
4. Mumford D., Shah J. Optimal Approximations by Piecewise Smooth Functions and Associated Variational Problems // Communications on Pure and Applied Mathematics, Vol. XLII, No 4, 1989. – pp. 577–685.
5. 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.
6. Boykov Y. and Kolmogorov V. An Experimental Comparison of Min-Cut/Max-Flow Algorithms for Energy Minimization in Vision // IEEE Trans. Pattern Anal. Mach. Intell., 2004. Vol. 26, No.9, – P. 1124–1137.
7. Визильтер Ю.В., Желтов С.Ю., Князь В.А., Ходарев А.Н., Моржин А.В. Обработка и анализ цифровых изображений с примерами на LabVIEW IMAQ Vision. – М: ДМК Пресс, 2008 г., – 464 с.
8. Kharinov M.V. Merge-and-correct segmentation method // 8th Open German-Russian Workshop «Pattern Recognition and Image Understanding» OGRW-8–2011 / Proc. of the 8th Open German-Russian Workshop, – Nizhny Novgorod: Nizhny Novgorod Lobachevsky State University, November 21–26, 2011. – P. 123–126.
9. Kharinov M.V. Adaptive Dichotomous Image Segmentation Toolkit // Pattern Recogn. Image Anal.: Adv. Math. Theory Appl. 2012. Vol. 22(1), P. 228–235.
10. 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.
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. MacQueen J.B. Some Methods for classification and Analysis of Multivariate Observations // Proc. Fifth Berkeley Symp. Math. Stat. and Probab., Berkeley: University of California Press, Vol. 1, 1967. – P. 281–297.
13. Likas A, Vlassis N. and Verbeek J.J. The Global K-Means Clustering Algorithm // Pattern Recognition. Vol. 36, 2003. – P. 451–461.

Чечулин А.А., Котенко И.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АНАЛИЗ ПРОИСХОДЯЩИХ В РЕАЛЬНОЙ СЕТИ СОБЫТИЙ НА ОСНОВЕ
ИСПОЛЬЗОВАНИЯ СИСТЕМЫ МОДЕЛИРОВАНИЯ СЕТЕВЫХ АТАК**

Данная работа посвящена исследованию задачи учета сетевых событий, происходящих в реальном времени, в системах моделирования сетевых атак. Объектом исследования является процесс моделирования сетевых атак. В статье рассматриваются основные входные и выходные данные системы моделирования и информационные потоки внутри нее. Также в данной работе приведено описание разработанного прототипа системы моделирования.

Введение

Работа посвящена исследованию вопросов построения системы моделирования атак и оценки рисков (СМАОР), как части общей системы управления инцидентами и событиями (SIEM). Исследование проводится в рамках проекта Европейского сообщества MASSIF [1].

Основной задачей систем управления инцидентами и событиями является сбор и анализ событий, происходящих в контролируемой сети. В данной работе предлагается внедрить в существующие SIEM-системы дополнительную функциональность – подсистему моделирования атак, которая позволит расширить возможности и повысить точность выявления инцидентов, связанных с информационной безопасностью.

Поскольку результаты работы подсистемы моделирования атак часто не могут быть вычислены в реальном времени, их использование в процессах реального времени затруднено. Однако, построенные графы атак сохраняют актуальность достаточное время (до значительных изменений в политике безопасности или физической топологии сети). Благодаря этому в рамках общей системы анализа событий предлагается использовать построенные заранее графы атак. Эти графы атак могут применяться для решения двух основных типов задач – для предсказания последующих действий нарушителя и для анализа и выявления его прошлых действий, приведших систему к текущему состоянию.

Предсказание же последующих действий нарушителя производится на основе анализа следующих элементов: (1) моделей нарушителя, на основе которых были построены наиболее близкие к реальным графы атак; (2) использованных нарушителем видов атак и уязвимостей; (3) возможных целей, специфицированных в графах атак.

1. Анализ современной литературы

Во многих работах рассматриваются различные подходы к моделированию атак с учетом различных классов атак. В данном разделе будут кратко проанализировано текущее состояние исследований в следующих областях: (1) отображения сценариев атак; (2) злоумышленников; (3) спецификации платформ, уязвимостей, оценок уязвимостей, атак, конфигураций и возможных контрмер; (4) генерации графов атак.

В данном разделе из всего множества существующих работ проанализированы только основные, ввиду ограничений по объему тезиса.

В [2] предложена модель вторжений на основе раскрашенных сетей Петри. Каждая сигнатура вторжения выражается как шаблон, который отображает отношение между событиями и их контекстом. Обозначения начального и конечного состояний и пути между ними определяют набор последовательностей событий. Шаблоны вторжений имеют предшествующие условия и последующие действия, связанные с ними.

В [3] была разработана методика анализа перехода состояний для моделирования вторжений, основанных на хостах. Эта статья описывает компьютерное вторжение как последовательность действий, выполняемых атакующим для компрометации безопасности компьютерной системы. Атаки описываются с помощью диаграмм перехода состояний. Описание атаки имеет «безопасное» исходное состояние, ноль или больше переходных состояний, и (по крайней мере) одно «скомпрометированное» конечное состояние. Состояния характеризуются значениями утверждений, описывающих аспекты состояния безопасности (владение файлом, идентификация пользователя, авторизация пользователя).

Подход к моделированию вторжений в последовательной и параллельной формах был предложен в [4]. Эта статья предлагает алгоритм по преобразованию последовательного скрипта вторжения в набор параллельных скриптов, имитирующих вторжение.

Статья [5], описывающая систему обнаружения вторжений NetSTAT, предлагает формальные модели как сети, так и атак. Эти модели дают возможность определить, «какие сетевые события должны отслеживаться и где они могут отслеживаться». Подход NetSTAT расширяет методику анализа перехода состояний [2] для основанного на сети обнаружения вторжения, чтобы отображать сценарии атак в сетях.

В [6] была предложена простая модель сетевой безопасности «Причинно-следственная модель атаки и защиты информационной системы». Она состоит из модели сети, отображаемой узлами и связями, причинно-следственной модели, характеристических функций и псевдослучайного генератора

чисел. Тем не менее, отображение кибератак и защиты, основанное на причинно-следственной модели, очень упрощенное.

В [7] представлены наглядные модели сети и возможностей, целей и способа действий атакующего. Эти модели используются для определения устройств, которые будут скомпрометированы с наибольшей вероятностью. Для предсказания поведения атакующего используются экономические принципы (использующие компромисс «выгода – затраты»).

В [8–11] атаки описываются и моделируются в структурированной, основанной на деревьях форме.

В [8] представлена высокоуровневая концептуальная модель атак, основанная на намерениях нарушителя (стратегии атаки). Широкомасштабное распределенное обнаружение вторжения сравнивается с задачей военного управления. Статья определяет намерения вторжения как дерево целей. Конечная цель вторжения соответствует корневому узлу. Узлы нижних уровней отображают альтернативные или упорядоченные подцели в достижении верхнего узла/цели. Конечные узлы (листья) – подцели. Они могут подкрепляться событиями, сгенерированными в различных средах. Конструкции «ИЛИ», «И», и «Упорядоченное-И» используются для отображения временных последовательностей намерений вторжения.

Статья [9] также предлагает формальный подход для описания компьютерных атак. Этот подход называется «Деревья атак». В деревьях атак используются узлы «И» и «ИЛИ». Узлы ИЛИ – альтернативы. Узлы «И» отображают различные шаги на пути к одной цели. Работа, более детально рассматривающая так называемый основанный на «деревьях» подход, предложена в [10]. Эта статья описывает методы представления атак в форме деревьев атак.

Модель оценки жизнеспособности сетевых систем при воздействии сетевых инцидентов была представлена в [12]. Модель состоит из трех подмоделей. Первая отражает выполнение атак или инцидентов. Вторая определяет влияние атаки на систему в зависимости от типа атаки и завершенности системы защиты. Третья оценивает жизнеспособность системы.

Статья [13] предлагает методологию моделирования кибер-атак, основанную на схеме SES/MB (буквальный перевод структура системных сущностей, основанная на модели), формализме дискретного моделирования событий DEVS и объектно-ориентированного представления знаний на основе фреймов. Эта методология позволяет классифицировать угрозы, определять механизмы реализации атак и оценивать механизмы защиты.

В работе [14] описывается гибкая расширяемая модель компьютерных атак, язык для определения модели, и их использование в приложениях по безопасности, таких как анализ уязвимостей, обнаружение вторжений и генерация атак.

В [15] предлагается модель данных для системы обнаружения вторжений, называемую M2D2, которая использует четыре информационных типа: информация о характеристиках отслеживаемой информационной системы, информация об уязвимостях, информация о продуктах безопасности, используемых для проверки, и информация о наблюдаемых событиях.

В настоящей работе, были использованы подходы, описанные в публикациях из данного раздела. Новизна предложенного подхода, заключается в применении принципов моделирования атак для анализа событий, происходящих в реальном времени.

2. Общее описание подсистемы моделирования атак и оценки рисков

Предполагается, что общий подход к моделированию атак и оценке безопасности основывается на моделировании объекта защиты, поведения злоумышленника, генерации общего графа атак, вычислении различных показателей безопасности и предоставлении всеобъемлющих процедур анализа риска.

В качестве базиса для построения моделей (объекта защиты, злоумышленника, и т.д.) необходимо определить набор стандартов, на основе которых будут описываться элементы модели. Для этого предлагается использовать комплект взаимосвязанных MSM-стандартов [16] или других релевантных стандартов для представления информации, связанной с информационной безопасностью.

Указанные стандарты позволяют создать единое, обновляемое и согласованное хранилище данных, необходимое для построения и анализа сценариев атак (в виде графов или деревьев атак).

Общий Словарь Уязвимостей и Дефектов (CVE) [17] содержит список известных уязвимостей и дефектов информационной безопасности. Каждая уязвимость/дефект имеет уникальный идентификатор. Это позволяет осуществлять обмен данными между различными продуктами безопасности и дает возможность оценить защищенность продуктов и сервисов [17, 18]. Использование Национальной Базы Уязвимостей (NVD) [19], основанной на словаре CVE, основа моделирования атак по известным уязвимостям. Эти описания уязвимостей позволяют обнаружить все известные уязвимости, подходящие для систем с определенным аппаратным и программным обеспечением.

Общая Система Оценки Уязвимостей (CVSS) [20] – это открытая и стандартизованная система оценки уязвимостей для приоритизации уязвимостей. CVSS состоит из трех групп показателей: Базовые, Временные, и Конфигурационные [21]. Базовые показатели: Вектор Доступа (AV), Сложность Доступа (AC), Аутентификация (Au), Влияние на конфиденциальность (C), Влияние на целостность (I),

Влияние на доступность (A). Временные показатели: Возможность Использования (E), Уровень Исправления (RL), Степень Достоверности Отчета (RC). Контекстные показатели: Вероятность нанесения косвенного ущерба (CDP), Плотность целей (TD), Требования безопасности (CR, IR, AR). Для моделирования атак, используются базовые показатели. Другие группы показателей могут использоваться при анализе слабых мест сети и выборе контрмер.

Общее Перечисление Слабых Мест (CWE) [22] содержит унифицированный, измеримый набор слабых мест программного обеспечения. Это позволяет эффективно описывать, выбирать, обсуждать и использовать программные продукты безопасности и сервисы для поиска слабых мест в исходном коде и операционных системах. Также CWE дает лучшее понимание и управление слабыми местами программного обеспечения, связанными с архитектурой и дизайном [23]. Использование базы слабых мест может улучшить качество моделирования атак, основанных на уязвимостях нулевого дня.

Общее Перечисление Платформ (CPE) [24] дает унифицированный язык описания для компьютерных систем, платформ и пакетов. Он основан на универсальном синтаксе для Уникальных Идентификаторов Ресурсов (URI). CPE содержит: формальный формат имени, язык для описания сложных платформ, метод проверки имен против системы, и формат описания для связывания текста и проверки имени [25]. Использование словаря CPE позволяет избежать ошибок пользователя в установке исходных данных проверяемой сети. Также этот словарь позволяет искать подходящие для хоста уязвимости в базе NVD в процессе моделирования атак.

Так же в различных статьях описаны множество подходов для моделирования процесса атаки. Существуют следующие примеры основных широко известных таксономий атак: списки элементов атак; списки классов атак; классы результатов атак; практические списки типов атак; матрицы уязвимостей; таксономии дефектов безопасности или уязвимостей; таксономии вторжений, основанные на сигнатурах; таксономии инцидентов.

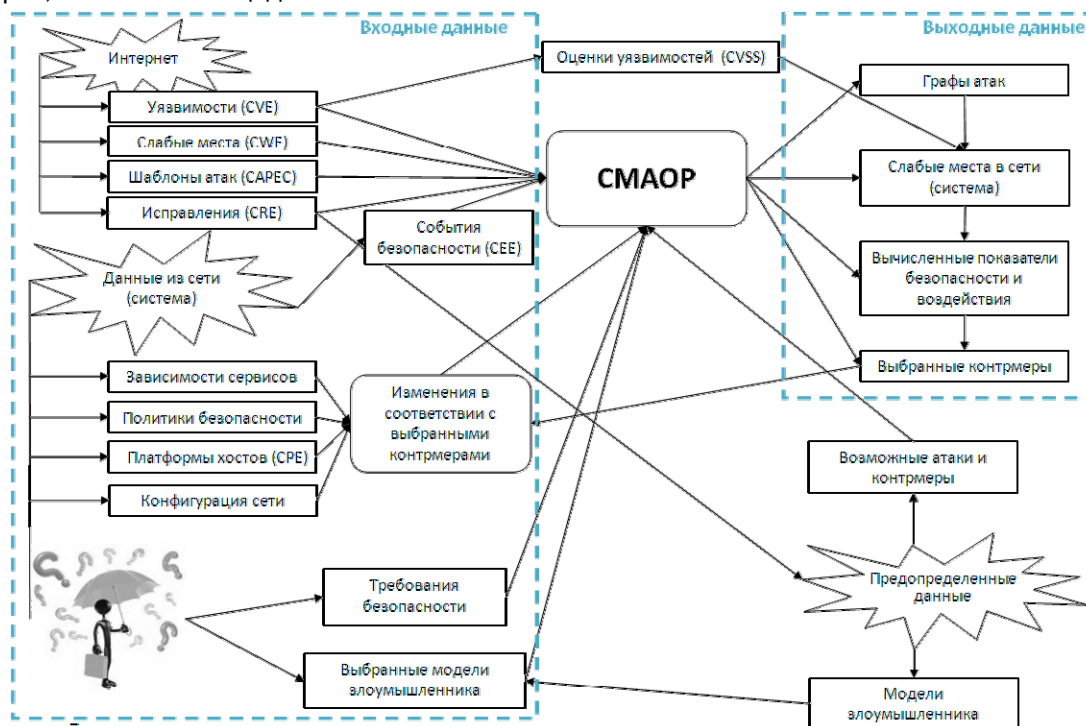


Рис.1. Основные потоки данных вне подсистемы моделирования

Общее Перечисление и Классификация Шаблонов Атак (CAPEC) [26, 27] описывает возможные последовательности действий злоумышленника. Описания шаблонов атак в CAPEC основаны на концепции проектных шаблонов, применяемых в деструктивном контексте, и анализе специфических примеров применения эксплоитов в реальном мире. Использование шаблонов атак позволяет применять последовательности известных уязвимостей и уязвимостей нулевого дня в одном атакующем действии. Это расширит возможности моделирования атак.

Общая архитектура СМАОР использующая все перечисленные стандарты описана на рисунке 1.

Примером таксономии событий является общий язык для описания инцидентов безопасности. Три основных понятия языка (инцидент, атака, и событие) определяются семью группами вспомогательных понятий (атакующие, продукты, уязвимости, действия, мишени, нелегитимные результаты, и цели). Атака определяется как «ряд преднамеренных шагов, предпринимаемых атакующим, чтобы достичь нелегитимного результата». Инцидент

определяется как «группа связанных атак, которые могут быть отличены от других атак, из-за различности атакующих, атак, целей, местоположений и времени» [28].

Типовой сценарий вторжения состоит из следующих этапов: (1) сбор информации; (2) поиск и использование уязвимостей; (3) использование скомпрометированного хоста. На первом этапе нарушитель пытается определить информацию об атакуемой сети, например, перечень функционирующих хостов, тип ОС и т.п.

Используя полученные данные, нарушитель выполняет атакующие действия (второй этап). Если на атакуемом хосте нарушителем получены дополнительные привилегии (локального пользователя или администратора), данный хост может послужить плацдармом для реализации атакующих действий, направленных на другие хосты сети.

Для разработки алгоритма формирования дерева атак уточним первый этап типового сценария вторжения, разделив его на два: (1-1) определение функционирующих хостов; (1-2) реализация сценариев (множества действий) разведки для каждого хоста, обнаруженного на первом этапе.

Второй и третий этапы уточним следующим образом: (2) второй этап заключается в реализации атакующих действий, использующих уязвимости программного и аппаратного обеспечения и общих действий пользователя; (3) третий этап включает в себя реализацию действий по перемещению нарушителя на успешно атакованный хост.

На базе данных этапов строится алгоритм формирования дерева атак.

Основные потоки данных внутри СМАОР изображены на рисунке 2.

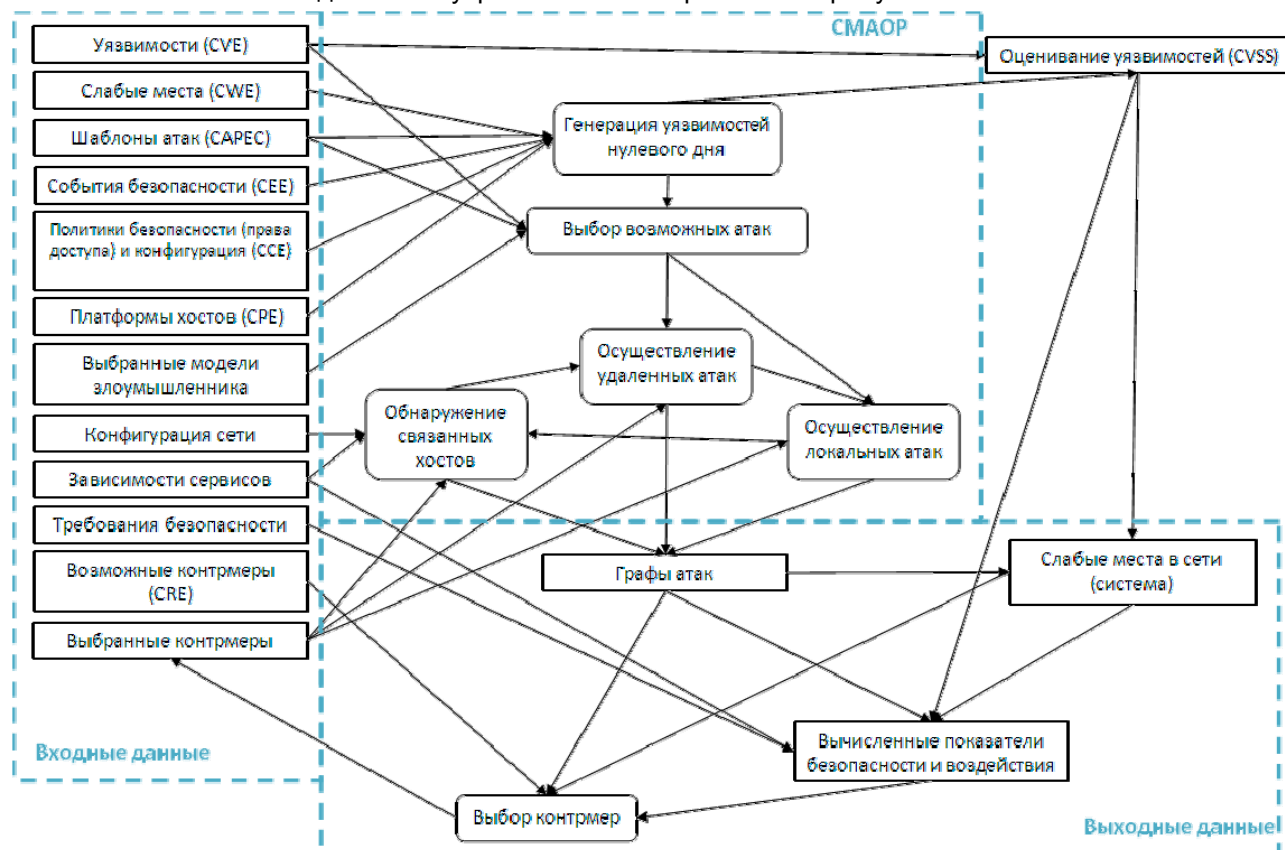


Рис.2. Основные потоки данных внутри подсистемы моделирования

3. Обнаружение вторжений на основе анализа событий происходящих в реальной сети

На рисунке 3 представлена общая архитектура использования графов атак для обнаружения атак, проводимых в реальной сети.

На основе модели сети и вероятностей реализации уязвимостей (определяемых в виде весовых коэффициентов) формируется граф атак. В реальной сети формируется сеть связанных сенсоров, которые позволяют обнаруживать отдельные атакующие действия. Система мониторинга позволяет построить общую картину событий происходящих в сети на основе собранной от сенсоров информации. Далее, общая система управления находит соответствия между графами атак и событиями в реальной сети. Таким образом, на основе анализа инцидентов с учетом данных полученных от подсистемы моделирования атак становится возможным делать выводы о том, что существует большая вероятность того, что инциденту «производится сканирование хоста С хостом В» предшествовал необнаруженный инцидент «хост В был атакован хостом А», и что последующим действием нарушителя будет «хост С подвергается атаке со стороны хоста В».

В настоящее время разработан программный прототип системы моделирования, который используется для различных сценариев, в том числе: критическая инфраструктура дамбы и корпоративная сети большого размера.

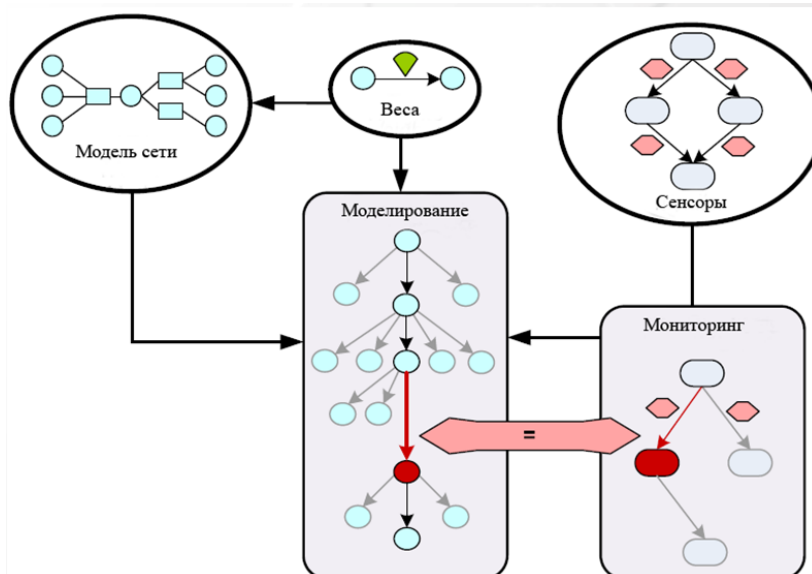


Рис.3. Архитектура системы анализа событий

Заключение

В настоящей работе предложен подход к использованию системы моделирования атак для повышения точности и оперативности обнаружения атак в общем потоке событий. Рассмотренные в статье задачи являются составными элементами общей системы управления инцидентами и событиями. Кроме того, предложенный подход позволяет после обнаружения атаки вычислить вероятные характеристики нарушителя (такие как, уровень знаний, технические возможности, цели, и т.д.), предсказать возможные направления развития атаки и возможные действия нарушителя, которые предшествовали проведению основной атаки (захват управления над сетевым оборудованием, кража паролей и т.д.). Так же, результатом работы системы моделирования атак могут быть следующие характеристики: (1) слабые места в топологии сети (хосты, через которые проходит наибольшее число графов атак); (2) выбранные контрмеры, позволяющие снизить вероятность максимального количества графов атак; (3) возможные последствия реализации контрмер, учитывающие зависимости сервисов.

В настоящее время продолжаются теоретические исследования способов построения графов атак, учитывающих существующие уязвимости и уязвимостей нулевого дня, политики безопасности, зависимости сервисов и т.д., и осуществляется разработка программного прототипа подсистемы моделирования атак. В дальнейшей работе планируется: (1) расширить функциональность прототипа, добавив в него анализ атак нулевого дня и связей сервисов; (2) расширить список метрик безопасности для уточнения оценки уровня защищенности сети; (3) уточнить модель нарушителя; (4) ускорить работу прототипа, за счет оптимизации процесса построения графов атак.

Данная работа проводится в лаборатории проблем компьютерной безопасности СПИИРАН. Работа выполняется при финансовой поддержке РФФИ (проект №10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект №3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

СПИСОК ЛИТЕРАТУРЫ

1. MASSIF Project. <http://www.massif-project.eu/>
2. Kumar S., Spafford E.H. An Application of Pattern Matching in Intrusion Detection // Technical Report CSDTR 94 013. The COAST Project. Department of Computer Sciences. Purdue University. West Lafayette, 1994.
3. Iglun K., Kemmerer R.A., Porras P.A. State Transition Analysis: A Rule-Based Intrusion Detection System // IEEE Transactions on Software Engineering, 21(3), 1995.
4. Chung M., Mukherjee B., Olsson R. Simulating concurrent intrusions for testing intrusion detection systems // Proceedings of the 1995 National Information Security Conference, 1995. P. 173–183.
5. Kemmerer R.A., Vigna G. NetSTAT: A network-based intrusion detection approach // Proceedings of the 14th Annual Computer Security Applications Conference, Scottsdale, Arizona, 1998.
6. F.Cohen. Simulating Cyber Attacks, Defenses, and Consequences // IEEE Symposium on Security and Privacy, Berkeley, CA. 1999.
7. Yuill J., Wu F., Settle J., Gong F., Forno R., Huang M., Asbery J. Intrusion-detection for incident-response, using a military battlefield-intelligence process // Computer Networks, No.34, 2000.
8. Huang M.-Y., Wicks T.M. A Large-scale Distributed Intrusion Detection Framework Based on Attack Strategy Analysis // First International Workshop on the Recent Advances in Intrusion Detection, Raid'98, Louvain-la-Neuve, Belgium, 1998.

9. Schneier B. Attack Trees // Dr. Dobbs's Journal, Vol.12, 1999.
10. Moore A.P., Ellison R.J., Linger R.C. Attack Modeling for Information Security and Survivability // Technical Note CMU/SEI-2001-TN-001. Survivable Systems, 2001.
11. Dawkins J., Campbell C., Hale J. Modeling network attacks: Extending the attack tree paradigm // Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection, Johns Hopkins University, 2002.
12. Moitra S.D., Konda S.L. A Simulation Model for Managing Survivability of Networked Information Systems // Technical Report CMU/SEI-2000-TR-020 ESC-TR-2000-020, 2000.
13. Chi S.-D., Park J.S., Jung K.-C., Lee J.-S. Network Security Modeling and Cyber Attack Simulation Methodology // Lecture Notes in Computer Science, Vol.2119, 2001.
14. Templeton S.J., Levitt K. A Requires/Provides Model for Computer Attack // Proceedings of the New Security Paradigms Workshop, 2000.
15. Morin B., Me L., Debar H., Ducasse M. M2d2: A formal data model for ids alert correlation // Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2002. Vol. 1516. P.115–137.
16. Making Security Measurable. <http://measurablesecurity.mitre.org/index.html>.
17. Common Vulnerabilities and Exposures. <http://cve.mitre.org/>
18. Christey S. Unforgivable Vulnerabilities, 2007.
19. National Vulnerability Database. <http://nvd.nist.gov/>
20. Common Vulnerability Scoring System. <http://www.first.org/cvss/>
21. Mell P., Scarfone K., Romanosky S. Common vulnerability scoring system // IEEE Security & Privacy Magazine, Vol.4, No.6, 2006. P.85–89.
22. Common Weakness Enumeration. <http://cwe.mitre.org/>
23. Christey T.S., Harris C. Introduction to Vulnerability, 2009.
24. Common Platform Enumeration. <http://cpe.mitre.org/>
25. Buttner A., Ziring N. Common Platform Enumeration (CPE) — Specification, Version 2.2, 2009.
26. Common Attack Pattern Enumeration and Classification. <http://capec.mitre.org/>
27. Barnum S., Sethi A. Attack Patterns as a Knowledge Resource for Building Secure Software, 2007.
28. Howard J.D., Longstaff T.A. A Common Language for Computer Security Incidents. SANDIA REPORT, SAND98-8667, 1998.



СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Баракин В.Н.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
СИСТЕМНЫЙ АНАЛИЗ СОВРЕМЕННОЙ КОНЦЕПЦИИ КАТАСТРОФОУСТОЙЧИВОСТИ
И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Рассмотрим сам термин «катастрофоустойчивость» (КУ). Для этой задачи необходимо сравнить КУ с отказоустойчивостью (ОУ). До сих пор ни теоретиками, ни практиками в области создания автоматизированной информационной системы (АИС) эти термины точно не определены.

Чтобы избежать останова АИС в результате сбоев в работе деталей оборудования или программного обеспечения (ПО), применяют дублированные компоненты. Набор дублированного оборудования позволяет АИС продолжить в полном объеме обеспечивать выполнение возложенных функций во время однократных сбоев. Такие АИС следует называть отказоустойчивыми, то есть нечувствительными к однократным отказам своих компонентов. При определенных условиях отказоустойчивые АИС способны продолжать работу и при многократных сбоях, если из строя выходят разные, не связанные между собой, узлы АИС. Вероятность наступления таких событий крайне мала, и в документации на отказоустойчивую АИС она не учитывается и не описывается.

Таким образом, в процессе проектирования АИС в отказоустойчивом исполнении исследуется возможность появления неисправности элементов (подсистем) АИС в результате однократных отказов отдельного оборудования и его комплектующих, то есть нарушения изнутри АИС. Предметом исследования АИС в катастрофоустойчивом исполнении (КАИС) является изучение влияния на работу АИС внешних факторов, приводящих к многократным, лавинообразным, крупномасштабным сбоям и, как следствие, – к останову целых подсистем, функциональных комплексов или всей АИС. Примерами возможных причин сбоев являются [2,11]:

- отсутствие электроэнергии в здании, районе или городе;
- пожары, наводнения или иные стихийные бедствия;
- коммунальные аварии;
- ошибки обслуживающего персонала;
- прекращение деятельности компаний-поставщиков услуг связи;
- их комбинации.

КУ, в отличие от ОУ, – более широкое понятие, охватывающее также и персонал, и регламенты, и финансовые средства. КУ следует определять как свойство АИС сохранять, реализовывать свои возможности, а также за заданное время восстанавливать работоспособное состояние при масштабных разрушающих воздействиях на большинство или все компоненты АИС.

Отказоустойчивые, а тем более катастрофоустойчивые, АИС, как правило, не дешевые. Рассчитать, тем более «прикинуть в уме», чем обернется та или иная авария на производстве довольно трудно. Каковы последствия простоя бухгалтера в течение одного дня? Каковы последствия простоя в течение одного часа системы поддержки банковских карт или целого аэропорта? События декабря 2010 года в Подмоскovie, когда «ледяной» дождь, шедший в течение нескольких часов, нарушил нормальную работу всех московских аэропортов на несколько дней и стоил карьеры ряду сотрудников из высшего руководства авиационных компаний, показывают, что крупные аварии всегда:

- неожиданные;
- не вовремя;
- совпадают с рядом других отвлекающих факторов;
- выходят за пределы технических проблем;
- имеют последствия, ощущаемые после устранения технических причин, приведших к аварии.

За последние 10 лет различными техническими комитетами, входящими в систему стандартизации РФ, разработан целый ряд стандартов, фиксирующих методы исследования и управления рисками и надежностью технологических систем. Эти стандарты играют важную роль в определении проблемы оценки надежности систем и постановке задачи повышения надежности. Особенно стоит выделить работы [6,7,10], где менеджмент риска и менеджмент надежности определяются как части общего менеджмента организации и предъявляются требования к высшему руководству компаний.

Один из руководителей IBM Том Глиб сказал: «Если вы сами активно не атакуете риски, то потом они будут активно атаковать вас» [12]. Самое серьезное, из-за чего наступают большие финансовые потери при катастрофических авариях, – это растерянность. В период аварии сотрудники не могут выполнять свои обязанности, обсуживающий персонал не способен быстро наладить работу АИС, а руководство не умеет в таких условиях управлять процессом.

Для эксплуатации КАИС в первую очередь необходимо иметь:

- обученный персонал;
- корректную документацию;
- отлаженные и протестированные процессы;
- утвержденную стратегию с указанием периодической оценки рисков.

К сожалению, крайне малое количество компаний обладает всеми четырьмя перечисленными элементами, чтобы а) осознать необходимость, б) правильно выбрать меры защиты и в) эффективно эксплуатировать собственные КАИС. Возникает следующая задача – как запланировать затраты на КУ и как оценить эффективность внедрения КАИС [1].

К сожалению, публичных методик для подобных расчетов нет. Ими обладают только несколько компаний, специализирующихся на исследованиях в области информационных технологий (Gartner, Tolly Group, Forrester Research), и ряд компаний, производящих инструменты для обеспечения КУ (Symantec, EMC, Hewlett-Packard, IBM). Зачастую, эти методики не содержат должной доли объективности, так как компания-разработчик методики в первую очередь стремится подтвердить ценность собственных продуктов, относящихся к обеспечению ОУ и КУ. В меньшей мере это присуще методикам исследовательских компаний, но их работа не редко оплачивается теми же производителями, что также подвергает сомнению их объективность.

Методика расчета эффективности внедрения КАИС должна основываться на сравнении преимуществ и недостатков, полученных в результате внедрения и эксплуатации такой АИС. При этом среди условий, приводящих к положительному экономическому эффекту, необходимо выделить:

- уменьшение стоимости ремонта АИС (части АИС);
- снижение степени последствий отказа АИС (части АИС);
- определение дополнительных выгод в связи с более надежным функционированием АИС;
- влияние более надежной работы АИС на маркетинговые стратегии предприятия;
- упрощение процесса принятия управленческих решений в тактическом и стратегическом горизонтах в связи со снижением количества рисков и вероятности их наступления;
- возможное изменение условий контрактов на поставку товаров (услуг, выполнение работ), а среди условий, приводящих к отрицательному экономическому эффекту, такие как:
- стоимость изготовления КАИС;
- затраты на эксплуатацию КАИС;
- возникновение вторичного риска: возможные отказы узлов КАИС, обеспечивающих КУ;
- высокий остаточный риск;
- низкая надежность срабатывания средств обеспечения КУ;
- малая вероятность наступления риска, для устранения которого АИС строилась в катастрофоустойчивом исполнении;
- слабое влияние простоя КАИС на деятельность предприятия.

В любом случае оценка необходимости внедрения КАИС должна начинаться с выявления рисков, способных повлиять на штатное функционирование АИС. Идентификация риска представляет собой главнейшую задачу, так как тем самым определяется, от чего должна защищаться КАИС, а, следовательно, ограничиваются методы защиты.

Любые способы идентификации рисков (например, [8]) являются субъективными и в значительной степени зависят от состава и опыта группы специалистов по оценке рисков. Так или иначе, количественная оценка риска должна быть ниже стоимости мер по модификации риска, а эффективность мер должна зависеть от того, насколько оценка остаточного риска отличается от оценки первоначального риска. Здесь следует подчеркнуть, что при количественной оценке риска необходимо учитывать влияние законодательных и отраслевых требований, социально-экономических аспектов, озабоченность причастных сторон, приоритеты [4].

Ни одна из мер защиты КАИС от стихийных бедствий не может дать полной гарантии функционирования КАИС при любых условиях. Меры защиты позволяют в какой-то степени снизить влияние риска на КАИС. Положения некоторых стандартов предлагают остаточный риск страховать [8], но не определяют какие-либо признаки, по которым можно четко определить, в каких случаях страховать остаточные риски.

Некоторые стандарты [3,5] содержат довольно подробное описание различных методов оценки надежности технических систем. Но ни один из представленных способов не подходит при исследовании влияния внешних воздействий: стихийных бедствий, массовых аварий, ошибок персонала, приводящих к множественным отказам нескольких компонентов АИС. В указанных источниках, и это явно отмечено в [5], нет критериев для установления потребности в анализе рисков, то есть определения типа анализа риска, необходимого для данной ситуации.

Наиболее эффективным для оценки влияний окружающей среды видится анализ дерева неисправностей. Дерево неисправностей схоже по форме и правилам чтения с диаграммой Исикавы (так называемым «рыбьим скелетом»). Вершиной дерева является состояние КАИС, а ветви и лепестки дерева — это события, приводящие (последовательно или параллельно) к неисправному состоянию КАИС. Корректно составленное дерево неисправностей может служить основой для оценки остаточных рисков КАИС и входной информацией для разработки договора страхования. Дерево неисправностей можно составлять по-разному для различных вершин. Одним из вариантов вершины дерева может быть нежелательное состояние КАИС, при котором значительно снижены показатели ее эффективности.

Анализ видов и последствий отказов (failure mode and effects analysis, FMEA) и анализ видов, последствий и критичности отказов (failure mode, effects and criticality analysis, FMECA) [9] представляют собой интересные модели, определяющие числовое значение рисков и различных состояний КАИС, соответствующих различным неисправностям. FMEA и FMECA отличаются от других методов тем, что предлагают попытку ранжировать риски по определенным критериям. Конечно, показатели можно создать другие, в зависимости от типа КАИС и контекста ее использования. Риски должны быть классифицированы по тяжести последствий, по вероятности появления, по природе возникновения. Снижать уровень вероятности (возможности) выхода из строя КАИС из-за наступления катастрофического события, наделяя КАИС более сложными механизмами функционирования (реконфигурации) и восстановления, необходимо до тех пор, пока класс самых критичных рисков или комбинация критичности и возможности появления риска, будет пустым, то есть рисков такого класса не будет.

Еще одна важная отличительная особенность FMEA и FMECA – учет времени появления и возможности рискованного события. Таким образом, можно учитывать износ оборудования или периоды пиковых нагрузок.

К сожалению, в [9] при описании метода анализа только упоминаются ситуации, при которых одна общая причина оказывает влияние на неисправность нескольких компонентов КАИС одновременно. Несмотря на это упоминание, методы FMEA и FMECA нельзя причислить к методам анализа типовых сценариев возникновения и развития нештатных ситуаций.

Каждый выявленный риск, каким бы методом он ни был определен, необходимо оценить. Оценка риска состоит в определении:

- что может выйти из строя (идентификации опасности);
- с какой вероятностью это может произойти (анализ частоты);
- каковы последствия этого события (анализ последствий) [5].

Идентифицированные опасности можно классифицировать по четырем основным категориям:

- природные опасности (стихийные бедствия);
- технические опасности (отказы оборудования, аварии на технических объектах);
- социальные опасности (войны, диверсии, эпидемии);
- опасности, связанные с укладом жизни (злоупотребления, невнимательность, саботаж) [5].

а также следует учитывать комбинированные опасности.

Не нужно забывать, что неотъемлемыми компонентами любых систем являются персонал и финансовые ресурсы [7], которые тоже должны быть надежными. Это означает, что для случаев неожиданной болезни, увольнения, отгулов на предприятии есть сотрудники, способные заменить отсутствующих специалистов. Кроме того, на предприятии должен быть всегда определенный фонд, состоящий из финансовых ресурсов, которые можно экстренно потратить на неожиданные нужды важных КАИС. Последнее может стать очередным требованием при страховании рисков выхода из строя КАИС.

Все современные исследования КУ можно условно разделить на два типа: маркетинговые и сугубо технико-технологические. Первые задаются целью разъяснить высшему руководству предприятий, что инвестиции в КАИС – это в первую очередь инвестиции в защиту бизнеса. Вторые исследуют предмет исключительно с технической или технологической стороны, зачастую упоминая КУ лишь в свете информационной безопасности. Ни одни, ни другие авторы не предлагают механизм, пользуясь которым, лицо, принимающее решение о внедрении АИС, может утверждать: внедряем систему с такой-то степенью КУ.

Еще тяжелее обстоит дело с подтверждением эффективности внедрения. Дело в том, что любые технологии, обеспечивающие КАИС, работают только тогда, когда происходят те события, ради которых эти технологии внедрялись. Основным показателем эффективности КУ – снижение чувствительности АИС к авариям. Но если нет самих аварий, не всегда можно проверить с требуемой степенью достоверности эффективность защиты от них.

Если в течение одного года в системе не было ни одной аварии, это несомненно успокаивает и обслуживающий персонал, который начинает халатно относиться к своим обязанностям, и руководство, которое перестает финансировать систему должным образом. Предположим, что каждая система по своим целевым характеристикам, заложенным при проектировании, допускает одну аварию в течение пяти лет. Это значит, что каждый безаварийный год работы системы

увеличивает вероятность выхода из строя системы в течение будущего года. То есть каждый безаварийный год наоборот должен стимулировать обслуживающий персонал и руководство к более пристальному вниманию к системе.

Пристальное внимание к КАИС выражается в следующем:

- аргументированная необходимость КУ;
- периодическая проверка расчета необходимости КУ;
- периодические тесты работоспособности средств КУ;
- комплексный подход в проведении тестов: вовлечение не только обслуживающего персонала, но и обычных пользователей;
- периодическое обучение персонала действиям в период аварий;
- постоянное обновление организационно-распорядительной документации, регламентирующей действия персонала в период аварии;
- учет организационных сбоев в информационных, материальных и финансовых потоках, задействованных в КАИС.

Последнее утверждение предполагает более широкий взгляд на собственную деятельность предприятия, а именно – с учетом своего ближайшего окружения. Например, налаженный производственный процесс в качестве точки входа информации предусматривает получение данных от смежных организаций. В паспорте КАИС, автоматизирующей этот производственный процесс, указано, что средства КУ способны избежать останова КАИС после наводнений и землетрясений в городе N. Но смежные организации не имеют подобных средств, и их АИС подвержены тем же рискам природных катаклизмов в городе N. Получается, что, обеспечив должный уровень КУ, предприятие не сможет гарантировать непрерывность своей деятельности из-за отсутствия соответствующего обеспечения в смежных организациях. Все инвестиции в КУ окажутся бессмысленными.

Таким образом, кроме обеспечения безопасности собственной деятельности, предприятие должно быть уверено в безопасной деятельности компаний, входящих в его ближайшее окружение. Иначе риск останова производственных процессов сохраняется на прежнем уровне. Об этом явно говорит требование ГОСТ Р 51901.2—2005: «Организация должна гарантировать, что закупленная продукция и продукция субподрядчика соответствуют критериям надежности» [6]; а ГОСТ Р 51901.3—2007 вводит понятие управления цепочкой поставки [7]. Оценить внутреннюю организацию стороннего предприятия зачастую невозможно, поэтому необходим какой-то внешний регулятор, позволяющий сертифицировать предприятия на КУ ведения бизнеса, сродни структуре сертификации процессов менеджмента качества по ГОСТ Р ИСО 9001.

Целесообразно разработать определенные критерии, согласно которым оценивать необходимость КАИС так, как это делается для защиты конфиденциальных и/или персональных данных. Предпосылок для появления новых регламентирующих процедур достаточное количество. Об этом скажет любой системный интегратор, занятый в сфере информационной безопасности. Несмотря на большое количество стандартов, принятых в России за последнее десятилетие, – стандартов удачных и современных, – ФСТЭК продолжает оценивать качество систем информационной безопасности по документам 1992 года. За 20 лет, прошедших с тех пор, информационные технологии совершили несколько рывков вперед, появились совершенно другие подходы в создании и защите АИС. Точно так же не стоят на месте и события, которые способны привести к потере или несанкционированному доступу к данным.

Таким образом, сложилась парадоксальная ситуация, когда предприятия видят реальные риски информационной безопасности, а для успешного получения аттестата ФСТЭК вынуждены применять другой, устаревший подход к защите данных. В первую очередь это касается самого предмета защиты. Руководящие документы ФСТЭК требуют защиты данных, тогда как защита самих АИС, их надежность остаются не регламентируемыми.

Отсутствие требований к КУ государственных АИС – серьезное упущение. Аттестат АИС, выдаваемый государственными регулирующими органами, должен подтверждать не только безопасность доступа к данным, но и устойчивость функционирования самой АИС. Ныне действующие нормы в области информационной безопасности не только не содержат требований к надежности, но в них полностью отсутствует механизм определения необходимости и достаточности предъявляемых требований к АИС. Существующая классификация АИС по обрабатываемым в них данным давно утратила актуальность. Кроме того, она нисколько не учитывает контекст АИС, в котором могут быть актуальными другие угрозы, а следовательно, и защита должна быть иной. Можно, например, разбить АИС на части по типу компонентов: ПО, оборудование, персонал, процедуры и применять методы планирования надежности (КУ) для каждой части АИС в отдельности.

Причинами использования этих методов могут быть:

- повышение котировок акций компании;
- дополнительное конкурентное преимущество;
- престиж на рынке;
- принадлежность «привилегированной части» предприятий.

Последнее утверждение дает компании определенный билет на вхождение в круг «особых» предприятий, ведение дел с которыми отвечает современным требованиям информационной безопасности. Информационная безопасность в целом и КУ процессов в частности должны перестать быть уделом гордости системных администраторов и директоров по ИТ, а стать обыденными вещами, так же как за последние десять лет сайт компании в Интернете превратился из забавной игрушки программистов в неотъемлемую часть визитной карточки предприятия. Комиссии по приемке и последующему периодическому тестированию должны содержать представителей смежных организаций, а результаты работы таких комиссий должны быть публичными.

Существует еще одна предпосылка для научного обоснования необходимости КАИС: страхование рисков. Окружающая среда любого предприятия накладывает разнообразные ограничения на деятельность. Все такие ограничения описываются вероятностными характеристиками и в экономической теории называются рисками. У любого риска есть два важных параметра: величина и степень влияния. Вероятность наступления катастрофы, способной вывести из строя всю АИС целиком – это тоже риск, причем с максимальной степенью влияния, а любой риск – это предмет для деятельности страховых компаний. То есть от длительного простоя по вине массовой аварии можно застраховаться. Страховые выплаты, конечно, в какой-то степени покроют возможные потери, но не вернут утраченный имидж. Тем не менее, расчет выплат, равно как и расчет страховых платежей, напрямую зависит от применения моделей, позволяющих оценить:

- необходимость КУ,
- эффективность КУ.

Итак, заинтересованность в подобных моделях могут проявить:

- крупные коммерческие организации – для объективного снижения риска возможных финансовых и нефинансовых потерь;
- средние и мелкие коммерческие организации – для объективной оценки величины вложений в устранение риска потери бизнеса целиком;
- налогоплательщики – для снижения расходов по устранению последствий катастроф в бюджетных (федеральных, региональных, муниципальных) организациях;
- страховые компании – для разработки новых собственных продуктов;
- финансовые институты – для использования дополнительного параметра оценки бизнеса;
- учреждения, регулирующие деятельность в подотчетных областях, – для использования нового метода регулирования;
- отраслевые и межотраслевые объединения, профсоюзы, цеха – для определения признака принадлежности предприятия к такому объединению.

Кроме математических моделей, совершенно необходимы методы, алгоритмы, методы манипулирования моделями, а также ПО для моделирования средств КУ – что-то наподобие ситуационных центров, только для КАИС. Такое ПО должно обладать возможностями визуального построения архитектуры проектируемой КАИС и возможностями анализа данной архитектуры. ПО должно выявлять и оценивать риски КАИС, а также предлагать варианты по их снижению или устранению.

При всей простоте и очевидной необходимости ПО для моделирования катастрофоустойчивых решений, такое ПО до сих пор не разработано, хотя имитационное моделирование упоминается в ГОСТ Р 51901.5—2005. Вот некоторые задачи, которые целесообразно возложить на такое ПО:

- насколько надежны могут быть компоненты КАИС при заданной степени надежности КАИС;
- какова должна быть кратность дублирования компонентов КАИС для достижения общей заданной надежности КАИС.

Все модели анализа надежности, упомянутые в статье, имеют строгое ограничение: при увеличении количества компонентов АИС сложность и количество расчетов растут экспоненциально. Это еще один аргумент в пользу появления специализированного ПО, осуществляющего расчеты надежности КАИС.

Данное исследование выполнялось при финансовой поддержке Программы фундаментальных исследований Отделения нанотехнологий и информационных технологий РАН (ОНИТ), проект 2.11.

СПИСОК ЛИТЕРАТУРЫ

1. Бабков В. Катастрофоустойчивая защита – какой ценой? [Электронный ресурс] / Business Continuity // Компания—Новости—Публикации. — URL: <http://www.business-continuity.com.au/ru/company/news/details/smid/1025/ArticleID/63/reftab/467.aspx>
2. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]: [курс лекций] / Интернет-ун-т информ. технологий. — URL: <http://www.intuit.ru/department/security/secbasics/1/>
3. ГОСТ Р 51891—2008. Менеджмент риска. Структурная схема надежности и булевы методы [Электронный ресурс] // База нормативной документации. — 49 с. — URL: <http://www.complexdoc.ru>
4. ГОСТ Р 51897—2002. Менеджмент риска. Термины и определения [Электронный ресурс] // База нормативной документации. — 18 с. — URL: <http://www.complexdoc.ru>
5. ГОСТ Р 51901.1—2002. Менеджмент риска. Анализ риска технологических систем [Электронный ресурс] // База нормативной документации. — 40 с. — URL: <http://www.complexdoc.ru>
6. ГОСТ Р 51901.2—2005. Менеджмент риска. Системы менеджмента надежности [Электронный ресурс] // База нормативной документации. — 90 с. — URL: <http://www.complexdoc.ru>

7. ГОСТ Р 51901.3—2007. Менеджмент риска. Руководство по менеджменту надежности [Электронный ресурс] // База нормативной документации. — 95 с. — URL: <http://www.complexdoc.ru>
8. ГОСТ Р 51901.4—2005. Менеджмент риска. Руководство по применению при проектировании [Электронный ресурс] // База нормативной документации. — 22 с. — URL: <http://www.complexdoc.ru>
9. ГОСТ Р 51901.12—2007. Менеджмент риска. Метод анализа видов и последствий отказов [Электронный ресурс] // База нормативной документации. — 61 с. — URL: <http://www.complexdoc.ru>
10. ГОСТ Р 52806—2007. Менеджмент рисков проектов. Общие положения [Электронный ресурс] // База нормативной документации. — 26 с. — URL: <http://www.complexdoc.ru>
11. Информационная безопасность [Электронный ресурс] = Security / Разраб. А.А. Дубаков. — URL: <http://portal.tpu.ru:7777/SHARED/a/AAD/work/Tab/8-2007.ppt>
12. Программное обеспечение IBM Rational. Методология и инструментальные средства разработки программных систем. [Текст] // Обзор продуктов и решений. 2006 / IBM Corporation. — [б. м.]: [б. и.], 2006. — 90 с.

Березин А.Н., Биричевский А.Р., Молдовян Н.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОСОБЕННОСТИ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФИМИРОВАНИЯ ПО СОСТАВНОМУ МОДУЛЮ
КАК КРИПТОГРАФИЧЕСКОГО ПРИМИТИВА**

Введение

Вычислительная трудность задачи дискретного логарифмирования (ЗДЛ) широко используется для синтеза криптосхем с открытым ключом. Эта задача определяется над конечными циклическими группами, например над мультипликативной группой колец классов вычетов по модулю n . В частном случае n равно 1024-битовому простому числу p или составному числу n , равному произведению 512-битовых сильных простых чисел q и r . В современной криптографии важнейшие практически используемые алгоритмы электронной цифровой подписи (ЭЦП) основаны на ЗДЛ на эллиптической кривой (ЭК), заданной над конечными полями. Известны общие методы дискретного логарифмирования, которые абстрагируются от конкретного вида групповой операции и вида элементов группы. Эти методы имеют экспоненциальную трудоемкость. Наибольшую трудоемкость данные методы имеют в случае, когда порядок группы является простым числом. Трудоемкость общих методов решения ЗДЛ (метод Полларда, метод больших и малых шагов) определяется наибольшим простым делителем порядка группы. При правильном выборе ЭК для задачи логарифмирования на кривой известны только общие методы, поэтому на практике могут применяться криптосхемы на основе ЭК, порядок которых равен от 160 бит до 512 бит. Для решения ЗДЛ в конечном простом поле известны специальные методы решения, имеющие субэкспоненциальную сложность (метод вычисления индексов). Сравнительно мало публикаций посвящено синтезу криптосхем над ЗДЛ по трудно разложимому модулю $n = rq$. Известно, что ЗДЛ по модулю n имеет одинаковый порядок с суммарной трудностью задачи факторизации (ЗФ) числа n , ЗДЛ по модулю q и ЗДЛ по модулю r [1]. Лучший известный алгоритм факторизации числа n имеет субэкспоненциальную сложность и при одинаковом размере чисел p и n трудоемкость ЗФ и трудоемкость ЗДЛ по модулю p имеют одинаковый порядок. Трудоемкость ЗДЛ по модулю q и ЗДЛ по модулю r на многие порядки меньше трудоемкости ЗФ числа n , поскольку размер простых чисел q и r в два раза меньше размера n . Таким образом, реализация криптосхем над ЗДЛ по модулю n не дает выигрыша в стойкости, что предопределило сравнительно малый интерес к построению алгоритмов с использованием трудности этой задачи.

В настоящей работе дается обоснование возможности построения алгоритмов и протоколов с открытым ключом, основанных на трудности ЗДЛ по модулю n и обеспечивающих более высокий уровень безопасности.

1. Особенности задачи дискретного логарифмирования по составному модулю

Задача факторизации и ЗДЛ по простому модулю являются независимыми, тогда как ЗФ составного числа n и ЗДЛ по модулю n связаны между собой, а именно алгоритм решения последней имеет трудоемкость не ниже трудоемкости факторизации n (см. с. 114 в книге [1]), поскольку алгоритм решения ЗДЛ по модулю n при случайно выбранном основании α может быть полиномиально модифицирован в алгоритм факторизации числа n (трудоемкость получаемого таким образом алгоритма полиномиально выражается через трудоемкость ЗДЛ по модулю n). Действительно, для пусть заданного значения y , принадлежащего циклической подгруппе, генерируемой степенями числа α , известен алгоритм вычисления числа x , такого, что выполняются условия $y = \alpha^x \bmod n$, $x < n$. Этот алгоритм может быть использован для факторизации n следующим образом.

Сгенерируем случайное число $X > n(X - n < n)$, вычислим значение $y = \alpha^X \bmod n$, а затем с помощью рассматриваемого алгоритма – значение x , такое, что $y = \alpha^x \bmod n$. Очевидно, что

порядок ω числа α делит разность $X - x: \omega | X - x$. Последнее означает, что значение ω может быть найдено как один из делителей числа $X - x$. Если простые числа q и r (делители числа n) не генерируются специальным образом, то число с вероятностью близкой к 1 можно будет достаточно легко факторизовать, т.е. найти все его простые делители d_i , среди которых будут содержаться и все простые делители порядка ω . Выбирая делитель d_i достаточно большого размера с достаточно большой вероятностью этот делитель будет делить либо $q-1$, либо $r-1$, но не будет одновременно делить $q-1$ и $r-1$. Пусть $\omega | q-1$. Тогда число $\beta = \alpha^{(X-x)/d_i} \bmod n$ легко вычисляется и имеет порядок по модулю q , равный d_i , т.е. $\beta^{d_i} \equiv 1 \bmod q$. Также имеет место соотношение $\beta^{d_i} \equiv 1 \bmod n \Rightarrow \beta^{d_i} \equiv 1 \bmod r$. Поскольку d_i не является порядком числа β по модулю r , то $\beta \equiv 1 \bmod r \Rightarrow r | \beta - 1$. Последнее соотношение показывает, что число n может быть факторизовано путем вычисления наибольшего общего делителя чисел n и $\beta - 1$. Таким образом, эффективный алгоритм решения ЗДЛ по модулю n модифицируется в эффективный алгоритм факторизации числа n . Однако это не касается частных специальных случаев, когда 1) функция Эйлера от числа n содержит два больших простых множителя и 2) числа $q-1$ и $r-1$ содержат одинаковый простой множитель γ , имеющий достаточно большой размер (160 бит и более), а число α имеет порядок по модулю n , равный γ . В первом случае делители числа n имеют вид $q = N_q q' + 1$ и $r = N_r r' + 1$, где q' и r' – простые числа, размером не менее 512 бит; N_q и N_r – достаточно большие четные числа. В качестве α берется число, порядок которого равен $\omega = q'r'$. Решение ЗДЛ по модулю n позволит вычислить значение ω , однако найти его делители ω является 3Ф, имеющей субэкспоненциальную сложность. Таким образом, для факторизации n после решения ЗДЛ снова требуется решить 3Ф, но уже по отношению к числу ω меньшего размера. Однако выбранные размеры делителей ω таковы, что разложить ω на множители является практически невыполнимой задачей при использовании лучшего известного алгоритма факторизации. Требование выбора в качестве N_q и N_r достаточно больших четных чисел связано с тем, чтобы сделать практически невыполнимым нахождение значения функции Эйлера $\varphi(n) = N_q N_r q' r'$ путем подбора возможных значений N_q и N_r при известном значении $\omega = q'r'$. Является ли число $\lambda = N_q N_r q' r'$ значением $\varphi(n)$, можно легко проверить возведением случайных чисел R в степень λ по модулю n , т.е. проверяя выполнимость условия $R^\lambda \bmod n = 1$. По значению $\varphi(n)$ легко вычисляются делители числа n (см. с.142 в [2]). При размере чисел N_q и N_r , равном 64 бит и более нахождение значения $\varphi(n)$ по описанному способу вычислительно невыполнимо.

Во втором случае делители числа n имеют вид $q = N_q \gamma + 1$ и $r = N_r \gamma + 1$, где γ – простое число, размером не менее 160 бит. В качестве α берется число, порядок которого равен $\omega = \gamma$ и для которого выполняются соотношения $\alpha \bmod q \neq 1$ и $\alpha \bmod r \neq 1$. Решение ЗДЛ по модулю n позволит вычислить значение γ , однако это недостаточно для нахождения делителей числа n , поскольку $\text{НОД}(\alpha^i - 1, n) = 1$ для всех значений $i \in \{1, 2, \dots, \gamma - 1\}$.

Рассмотренные варианты ЗДЛ по модулю n фактически являются частными случаями общей ЗДЛ, формулируемой следующим образом. Даны два числа α и β , имеющие по модулю n порядок, равный значению обобщенной функции Эйлера $L(n)$. При этом числа α и β относятся к разным циклическим подгруппам мультипликативной группы кольца вычетов по модулю n . Для произвольного заданного числа y , такого, что $\text{НОД}(y, n) = 1$, требуется найти пару чисел x и w ,

удовлетворяющих выражению $y = \alpha^x \beta^w \bmod n$. Этот вариант ЗДЛ можно назвать ЗДЛ по двумерному основанию. Общая ЗДЛ по модулю n сводится к решению ЗФ, ЗДЛ по простому модулю q и ЗДЛ по простому модулю r . Также можно показать, что эффективный алгоритм нахождения логарифма по двумерному основанию может быть модифицирован в эффективный алгоритм факторизации модуля n .

2. Построение криптосхем

Построение криптосхем с использованием трудности ЗДЛ по трудно разложимому модулю n может быть выполнено по аналогии с известными криптосхемами, основанными на трудности ЗДЛ по простому модулю. Однако следует учесть особенности, рассмотренные в предыдущем разделе. Также следует учесть то, что при выборе составного модуля длиной 1024 бит ЗДЛ будет практически сводиться к ЗФ модуля, поскольку ЗДЛ по простому модулю длиной 512 бит сравнительно легко решается. Поэтому для того, чтобы ЗДЛ по модулю n была независимой от ЗФ требуется использовать значение n , содержащее, по крайней мере, один простой делитель q такого размера, что ЗДЛ по модулю q была практически невыполнимой. В этом случае для взлома криптосистем, основанных на трудности ЗДЛ модулю n найти прорывное решение ЗФ будет недостаточным.

Из сказанного вытекает следующий подход к синтезу криптосхем с 80-битовой стойкостью, который состоит в реализации известных типов криптосхем с открытым ключом, основанных на сложности ЗДЛ, над конечным кольцом вычетов по составному модулю $n = rq$, где размер числа r равен 1024 бит, а размер числа q – 512 бит. При таком подходе существенно используется принципиальное отличие ЗДЛ по составному модулю от ЗФ и ЗДЛ по простому модулю. Известные криптосхемы, основанные на основе ЗДЛ по простому модулю, используются как аналоги, по которым строятся криптосхемы, использующие трудность ЗДЛ по модулю n размером 1536 бит. Последняя задача принципиально отличается от ЗДЛ по простому модулю. Для решения ЗДЛ по составному модулю могут быть использованы общие методы дискретного логарифмирования [1,3], имеющие субэкспоненциальную сложность, и метод сведения к ЗДЛ по простому модулю (имеющий экспоненциальную сложность) путем факторизации составного модуля и использования китайской теоремы об остатках [1,3]. Однако в последнем методе требуется вычислить дискретный логарифм по простым модулям r и q . Это показывает, что появление прорывного метода решения ЗФ или ЗДЛ по простому модулю не приведет к взлому криптосистемы, основанной на ЗДЛ по модулю n , один из простых делителей которого имеет длину 1024 бит.

Действительно, если будут найдены прорывные решения ЗФ, то ЗДЛ по составному модулю n потребует решения ЗДЛ по простым модулям q и r . Так как размер числа r в два раза больше размера q , то основной вклад в трудоемкость дискретного логарифмирования в рассматриваемом случае будет вносить ЗДЛ по простому модулю r . При 1024-битовом размере числа r трудоемкость ЗДЛ по модулю r равна 280 операций модульного умножения. Это обеспечит 80-битовую стойкость криптосхем, основанных на трудности ЗДЛ по модулю n даже в случае появления прорывных алгоритмов факторизации. Если будут найдены прорывные решения ЗДЛ по простому модулю, то эти методы смогут быть применены для взлома предлагаемых криптосхем только после решения ЗФ модуля n . Таким образом для взлома предлагаемых криптосхем потребуется решить как ЗФ, так и ЗДЛ по большому простому модулю r , следовательно они обладают существенно более высоким уровнем безопасности в смысле существенного снижения (на многие порядки) вероятности их взлома за счет появления прорывных атак.

3. Особенности криптосхем на основе сложности дискретного логарифмирования по составному модулю

Модуль n и связанные с ним параметры криптосхем могут быть выработаны некоторым доверительным центром, который уничтожит делители q и r после выработки значения n . В этом случае может быть построен более широкий ряд криптосхем различного типа, основанных на трудности одновременного решения ЗФ и ЗДЛ по простому модулю. Однако процедура замены значения модуля (при появлении такой необходимости) в значительной степени теряет гибкость. Последний недостаток устраняется при использовании значения модуля n и связанных с ним параметров в качестве открытого ключа. В обоих случаях появляется дополнительная возможность синтеза схем обычной и слепой ЭЦП над конечными группами с многомерной циклическостью [4,5].

В криптосхемах, основанных на трудности ЗДЛ по модулю n , в сравнении с их соответствующими аналогами имеет место увеличение временной сложности вычислительных процедур примерно в 2,25 раза, если в исходных схемах не выбираются значения простых модулей со специальной структурой их двоичного представления. В случае, если в исходных схемах

используются простые модули со специальной структурой, то имеет место увеличение сложности в десятки раз. Это связано с тем, что значение составного модуля не может быть выбрано таким, чтобы устранить операцию арифметического деления при выполнении операции модульного умножения. Однако в сравнении со схемами [6–8], основанными на трудности одновременного решения 3Ф и ЗДЛ, в предлагаемых схемах имеет место некоторое снижение сложности используемых вычислительных процедур. При этом в случае протоколов электронной цифровой подписи (ЭЦП) имеет место значительное сокращение размера подписи при заданном уровне стойкости.

Технические вопросы, связанные с особыми требованиями к модулю n , используемому в предлагаемых криптосхемах, рассматривались ранее в книгах [2,11] при описании ряда алгоритмов ЭЦП, основанных на сложности 3Ф. Рассмотрим алгоритм 240-битовой ЭЦП, основанный на ЗДЛ по модулю n . Открытый ключ представляет собой набор значений $(n, \alpha, \beta, \gamma, y)$, где элемент y вычисляется по формуле:

$$y = \alpha^x \beta^w \bmod n,$$

где α, β – числа, имеющие порядок, равный 80-битовому простому числу γ , и принадлежащие разным циклическим подгруппам. Секретным ключом является набор чисел (r, q, x, w) , где x и w – случайные 80-битовые числа ($x < \gamma$, $w < \gamma$); простые числа q и r являются секретными значениями и имеют следующую структуру: $r = N_r \gamma^2 + 1$ и $q = N_q \gamma^2 + 1$, где N_r и N_q – два больших четных числа. Процедура генерации ЭЦП включает следующие шаги:

1. Сгенерировать случайные числа $k < \gamma$ и $t < \gamma$ и вычислить значение $R = \alpha^k \beta^t \bmod n$.
2. Используя некоторую специфицированную 160-битовую хэш-функцию F_H , вычислить значение $F_H(M)$, где M – документ, который требуется подписать. Представить значение $F_H(M)$ в виде конкатенации двух 80-битовых чисел: $F_H(M) = H_1 \parallel H_2$.
3. Вычислить первый 80-битовый элемент ЭЦП $E = F_H(M, R) \bmod \gamma$.
4. Вычислить второй 80-битовый элемент ЭЦП $S = \frac{k + xE}{H_1} \bmod \gamma$.
5. Вычислить третий 80-битовый элемент ЭЦП $U = \frac{t + wE}{H_2} \bmod \gamma$.

В результате выполнения данной процедуры генерируется 240-битовая ЭЦП в виде тройки 80-битовых чисел (E, S, U) . Процедура генерации ЭЦП включает следующие шаги:

1. Вычислить значение $F_H(M) = H_1 \parallel H_2$.
2. Вычислить значения $\tilde{R} = y^{-E} \alpha^{SH_1} \beta^{UH_2} \bmod n$ и $\tilde{E} = F_H(M, \tilde{R}) \bmod \gamma$.
3. Сравнить значения $\tilde{E}$ и E . Если $\tilde{E} = E$, то ЭЦП признается подлинной.

На основе данной схемы ЭЦП в работе [14] разработан протокол 240-битовой слепой подписи. По аналогии с протоколами коллективной ЭЦП, основанными на трудности ЗДЛ по простому модулю, описанная схема ЭЦП может быть использована для разработки протоколов 240-битовой коллективной подписи.

Заключение

Принципиальное отличие ЗДЛ по простому от ЗДЛ по трудно разложимому модулю дает обоснование целесообразности синтеза криптосхем различного типа, основанных на ЗДЛ второго типа. Такие криптосхемы могут быть отнесены к схемам, взлом которых требует одновременного решения двух независимых вычислительно трудных задач – 3Ф и ЗДЛ по простому модулю. При этом для протоколов ЭЦП, относящихся к криптосхемам последнего типа, 80-битовая стойкость достигается при длине подписи, равной 320 и даже 240 бит, что существенно меньше размера подписи для известных схем ЭЦП, основанных на 3Ф (криптосистема Рабина, RSA), а также для схем ЭЦП, основанных на двух трудных задачах [7,12,13].

Работа выполнена в рамках ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009-2013 гг. (контракт № П635).

СПИСОК ЛИТЕРАТУРЫ

1. Menezes A. J., Vanstone S.A. Handbook of Applied Cryptography. – CRC Press, 1996. – 750p.
2. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. – Санкт-Петербург, БХВ–Петербург, 2005. – 286с.
3. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. – Санкт-Петербург, БХВ–Петербург, 2010. – 304 с.

4. Молдовян Н.А. Алгоритмы аутентификации информации в АСУ на основе структур в конечных векторных пространствах // Автоматика и телемеханика. 2008. №12. С.163–177
5. Молдовян Н.А. Аутентификация информации в АСУ на основе конечных групп с многомерной цикличностью // Автоматика и телемеханика. 2009. №8. С.177–190.
6. Молдовяну П.А., Молдовян Д.Н., Морозова Е.В., Пилькевич С.В. Повышение производительности процедур коммутативного шифрования // Вопросы защиты информации. 2009. №4. С.24–31.
7. Дернова Е.С., Молдовян Н.А. Синтез алгоритмов цифровой подписи на основе нескольких вычислительно трудных задач // Вопросы защиты информации. 2008. №1. С.22–26.
8. 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.
9. 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.
10. Moldovyan A.A., Moldovyan D.N., Gortinskaya L.V. Cryptoschemes based on new signature formation mechanism // Computer Science Journal of Moldova. 2006. Vol.14. No 3(42). P.397–411.
11. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. – Санкт-Петербург, БХВ–Петербург, 2007. –298 с.
12. Tahat N.M.F., Shatnawi S.M.A., Ismail E.S. New Partially Blind Signature Based on Factoring and Discrete Logarithms. Journal of Mathematics and Statistics 4 (2): 124–129, 2008.
13. Tahat N.M.F., Ismail E.S., Ahmad R.R. A New Blind Signature Scheme Based on Factoring and Discrete Logarithms. International Journal of Cryptology Research 1 (1): 1–9 (2009).
14. Молдовян Д.Н., Васильев И.Н., Краснова А.И. Схема слепой 240-битовой подписи // Информационно-управляющие системы. 2011. № 2. С. 49–53.

Головко В.А., Киричек Р.В., Ларионов С.М., Чванов В.П.

Россия, Санкт-Петербург, ФГУП «ЦентрИнформ»

ЗАЩИТА ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОТ ПРЕДНАМЕРЕННЫХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЙ

Актуальность электромагнитной угрозы для объектов информатизации

Одной из характерных тенденций нового века стало стремительное развитие и совершенствование систем информационной инфраструктуры (ИИ). Применяемые меры и средства информационной безопасности направлены на защиту этих систем с использованием программно-аппаратных средств. При этом не учитывается появившаяся в последние годы возможность проведения кибератак с использованием генераторов сверхкоротких электромагнитных импульсов. Особенностью таких генераторов является сравнительно малые габариты, низкая потребляемая мощность, формирование воздействующих импульсов, соизмеримых с длительностью рабочих сигналов электронной аппаратуры и сетей передачи данных. В результате воздействия происходит искажение исходной последовательности символов на физическом уровне модели ISO/OSI. Следует отметить, что эта угроза прямо указана в ГОСТ Р 51275-2007 «Защита информации. Объекты информатизации. Факторы, воздействующие на информацию. Общие положения».

Угроза преднамеренного электромагнитного воздействия (ПД ЭМВ) становится все более опасной в связи с нарастающей информатизацией общества, особенно в передовых промышленно развитых странах и регионах, для нормального функционирования которых насущно необходима информационная инфраструктура, включающая АСУ технологическими процессами, системами и средствами безопасности, мониторинга оперативной обстановки и кризисного реагирования, управления системами жизнеобеспечения, связи и телекоммуникаций, транспортом, банковской инфраструктурой и пр. Необходимо обратить самое пристальное внимание на то, что сопоставимой с последствиями прямых террористических актов по катастрофичности последствий может стать значительно менее энергоемкое электромагнитное нападение криминальных групп непосредственно на комплекс критически важных узлов информационной инфраструктуры региона.

Разработаны и быстро совершенствуются мобильные и портативные генераторы – источники сверхкоротких (сверхширокополосных) электромагнитных импульсов. К настоящему времени достигнуты следующие примерные значения параметров генераторов:

- мощность в импульсе до 10 МВт;
- длительность импульса от 0,2 до 10 нс;
- частота повторения до 10 кГц.

Такие генераторы в состоянии сформировать на расстояниях до 100 м критические уровни электромагнитного воздействия, вызывающие сбои и отказы в работе элементов ИИ, следствием чего явится уничтожение, блокирование или искажение информации. Компактность генераторов позволяет злоумышленникам за достаточно короткое время воздействовать на десятки критически важных объектов информатизации региона и обеспечить эффект воздействия на ИИ региона, сопоставимый по масштабам с воздействием электромагнитного импульса ядерного взрыва. Это, в свою очередь, может вызвать катастрофические последствия для систем связи и управления, энергетики, транспорта, банковской, финансовой и т.д.

Организационно и технически такая атака, очевидно, значительно проще, чем проведение любого другого криминального нападения, как в плане сравнительной простоты, дешевизны и доступности технических устройств для ее реализации, так и в плане возможностей скрытной подготовки. Важной особенностью такого способа электромагнитной атаки является то, что

идентифицировать факт атаки и выявить его источник (источники) на сегодняшний день практически невозможно. Кроме того в действующем законодательстве отсутствует нормативная база, предусматривающая уголовную и административную ответственность за проведение электромагнитных атак.

Все вышеизложенное является сильным аргументом в пользу безотлагательного создания государственной системы организационных и технических мер по защите информационной инфраструктуры России от возможных электромагнитных атак криминальных элементов.

Испытания на устойчивость технических средств безопасности к преднамеренным электромагнитным воздействиям

Принадлежность технических средств безопасности (ТСБ) к одной из разновидностей автоматизированных систем (согласно положениям ГОСТ 34.003-90) очевидна. Не вызывает также сомнений и требование по их устойчивости к внешним воздействиям, что достигается исполнением ТСБ в защищённом виде. Таким образом, ТСБ следует рассматривать как автоматизированные системы в защищённом исполнении (АСЗИ), на которые распространяются требования соответствующих нормативных документов, в том числе, ГОСТ Р 52863-07.

ТСБ являются интегрированными высокоинтеллектуальными информационными системами. Оснащение ими потенциально опасных и критически важных объектов производится в обязательном порядке согласно нормативным требованиям, определяемым документами федерального и ведомственного уровней. Бесперебойности функционирования ТСБ уделяется особое внимание, для чего в составе предъявляемых к ним требований фигурируют устойчивость к внешним воздействующим факторам, обеспечение электромагнитной совместимости, требование надёжности и т.п. Для предотвращения преднамеренного вывода оборудования ТСБ из строя задаются требования по обеспечению автоматизированного контроля их работоспособности, а также по изготовлению отдельных элементов ТСБ в антивандальном исполнении. Помимо этого, для режимных объектов предусматривается обеспечение защиты информации о структуре и тактике применения ТСБ.

Однако совокупность перечисленных требований, при всём своём разнообразии и полноте, не обеспечивает сохранение работоспособности ТСБ при преднамеренном электромагнитном воздействии (ПД ЭМВ). Именно этот фактор может эффективно использоваться злоумышленниками для подавления ТСБ при совершении противоправных действий. Для использования ТСБ по назначению в условиях возможного ПД ЭМВ необходимо знать уровни устойчивости оборудования ТСБ к деструктивным электромагнитным воздействиям. Эта задача может быть решена путём проведения целевых испытаний ТСБ согласно ГОСТ Р 52863-2007 [2].

Краткий обзор ГОСТ Р 52863-2007

Национальный стандарт Российской Федерации ГОСТ Р 52863-2007 разработан рядом организаций, занимающихся вопросами защиты информации, автоматизированных систем и объектов информатизации во главе с Санкт-Петербургским филиалом ФГУП «НТЦ «Атлас» (ныне ФГУП «ЦентрИнформ»). Этот стандарт устанавливает общие требования к испытаниям АСЗИ на устойчивость к ПД ЭМВ.

ГОСТ Р 52863-2007 является целевым стандартом. Его появление обусловлено общими стандартами ГОСТ Р 50922-2006 и ГОСТ Р 51274-2006, в которых даны определения угрозы ПД ЭМВ и сформулированы факторы его воздействия на информацию.

Необходимость разработки такого стандарта обуславливалась:

- принятием решения Федеральной службой технического и экспортного контроля РФ о построении целевой нормативной базы по защите от деструктивных электромагнитных воздействий;
- основополагающей ролью испытаний АСЗИ на устойчивость к ПД ЭМВ в процессе построения защиты от данной угрозы;
- потребностью в структурированном общедоступном представлении базовой информации по физическим характеристикам воздействий и их источникам, являющейся основой для адекватного проведения таких испытаний;
- согласованностью с направлениями разработки международных стандартов.

Основой для разработки стандарта ГОСТ Р 52863-2007 явились данные о параметрах ПД ЭМВ, полученные путём теоретических и экспериментальных исследований, а также результаты проведения компьютерного моделирования механизмов их воздействий на типовые элементы АСЗИ. При этом принималось во внимание то обстоятельство, что в период действия документа могут появиться новые, более полные и конкретные результаты исследований в его предметной области, которые будет необходимо учитывать при проведении испытаний. Кроме того, при написании стандарта предполагалось, что в числе его потенциальных пользователей будут не только заказчики и производители АСЗИ, но и широкий круг специалистов в области обеспечения безопасности информации и объектов. Поэтому, помимо конкретных данных, касающихся непосредственно испытаний АСЗИ, в документе содержатся сведения, дающие общее представление об угрозе и последствиях её реализации.

Структурно ГОСТ Р 52863-2007 состоит из шести основных разделов и шести приложений.

Наименование разделов:

1. Область применения.
2. Нормативные ссылки.
3. Определения и сокращения.
4. Требования устойчивости к преднамеренным силовым электромагнитным воздействиям.
5. Степени жёсткости испытаний.
6. Требования к испытаниям автоматизированных систем в защищённом исполнении.

Наименование приложений:

- А. Качественные признаки классификации условий эксплуатации АСЗИ.
- Б. Требования к основным характеристикам имитаторов ПД ЭМВ.
- В. Основные характеристики устройств связи/развязки имитаторов ПД ЭМВ.
- Г. Порядок проведения испытаний.
- Д. Схемы испытаний при ПД ЭМВ.
- Е. Критерии оценки.

Требования устойчивости АСЗИ к ПД ЭМВ в стандарте отнесены к разряду технических требований по защите информации, приведённых в действующих нормативных документах. Они имеют комплексный вид, и для их удовлетворения автоматизированная система (АС) может быть выполнена в защищённом исполнении с применением технических средств и (или) проведением организационных мероприятий. Помимо самих АС, требования устойчивости распространяются на их техническое обеспечение, на здания (помещения) или объекты, на которых устанавливаются АСЗИ, на программное обеспечение АСЗИ и на средства защиты информации и контроля защиты информации.

Требования устойчивости должны определяться:

- исходя из конкретных условий эксплуатации АСЗИ;
- на основе анализа модели воздействия;
- по результатам предварительных расчетно-экспериментальных оценок устойчивости АСЗИ и составных частей АСЗИ к ПД ЭМВ.

Степени жёсткости испытаний устанавливаются с целью последующей дифференциации испытательных воздействий. В стандарте они градуируются по четырём уровням в зависимости от класса условий эксплуатации АСЗИ и типа/характеристик элементов инфраструктуры, на которые непосредственно осуществляется воздействие.

Требования к испытаниям автоматизированных систем в защищённом исполнении включают общие положения, требования к объекту испытаний, испытательному оборудованию, порядку и условиям проведения испытаний, методам испытаний, результатам испытаний.

Особенности испытаний ТСБ на устойчивость к преднамеренным силовым электромагнитным воздействиям

ГОСТ Р 52863-07 устанавливает общие требования к испытаниям АСЗИ на устойчивость к ПД ЭМВ. Их уточнение и детализация должны производиться для АСЗИ конкретного предназначения с учётом особенностей их построения и функционирования.

Применительно к ТСБ такими особенностями являются:

- наличие встроенной функции контроля работоспособности, позволяющей информировать о выводе из строя оборудования в том числе, с помощью ПД ЭМВ и принимать адекватные компенсационные меры;
- многоуровневая архитектура и пространственная распределённость элементов ТСБ различных уровней при размещении на объекте;
- эшелонированное построение ТСБ.

Первый фактор требует при проведении испытаний на устойчивость выявлять те деструктивные последствия, которые не имеют явных демаскирующих признаков нападения и не фиксируются средствами контроля работоспособности ТСБ.

Примерный перечень последствий ПД ЭМВ приведён в таблице 1.

Таблица 1

Нарушения функционирования основных компонент ТСБ в результате ПД ЭМВ

№ п/п	Компоненты ТСБ	Виды нарушения функционирования
1	Охранно-пожарная сигнализация: – датчики; – оборудование сбора и обработки информации.	Отсутствие срабатывания при возникновении тревожных ситуаций, ложные срабатывания. Зависание оборудования, перезагрузка внутреннего ПО.
2	Система контроля управления доступом: – устройства считывания; – сетевые, узловые, управляющие контроллеры.	Блокировка оборудования, ввод вредоносной информации. Зависание оборудования. Разблокирование входа, блокирование выхода.
3	Система телевизионного наблюдения: – видеокамеры; – оборудование сбора и обработки информации.	Искажение строчной и кадровой развертки, «застывший кадр». Нарушение функции детектора движения. Зависание оборудования, перезагрузка внутреннего ПО.
4	Средства обнаружения ЯМ, ВВ.	Отсутствие срабатывания при попытках проноса/привоа.
5	Металлообнаружители.	Отсутствие срабатывания при попытках проноса/привоа.

6	АРМ интегрированной системы безопасности.	«Зависание» оборудования, перезагрузка ПО.
7	Автоматическая система пожаротушения.	Несанкционированный запуск.

Второй фактор позволяет сформировать адекватные для разных элементов ТСБ модели воздействия.

Среди видов ПД ЭМВ наиболее вероятным представляется воздействие электромагнитным полем. Это обусловлено тем, что цепи электропитания и проводные линии связи ТСБ, также являющиеся каналами возможных воздействий, как правило, имеют повышенную степень защиты.

Уровень воздействия зависит от возможности доставки конкретного источника ПД ЭМВ в точку применения. На рисунке 1 иллюстрируются варианты ПД ЭМВ на элементы ТСБ.

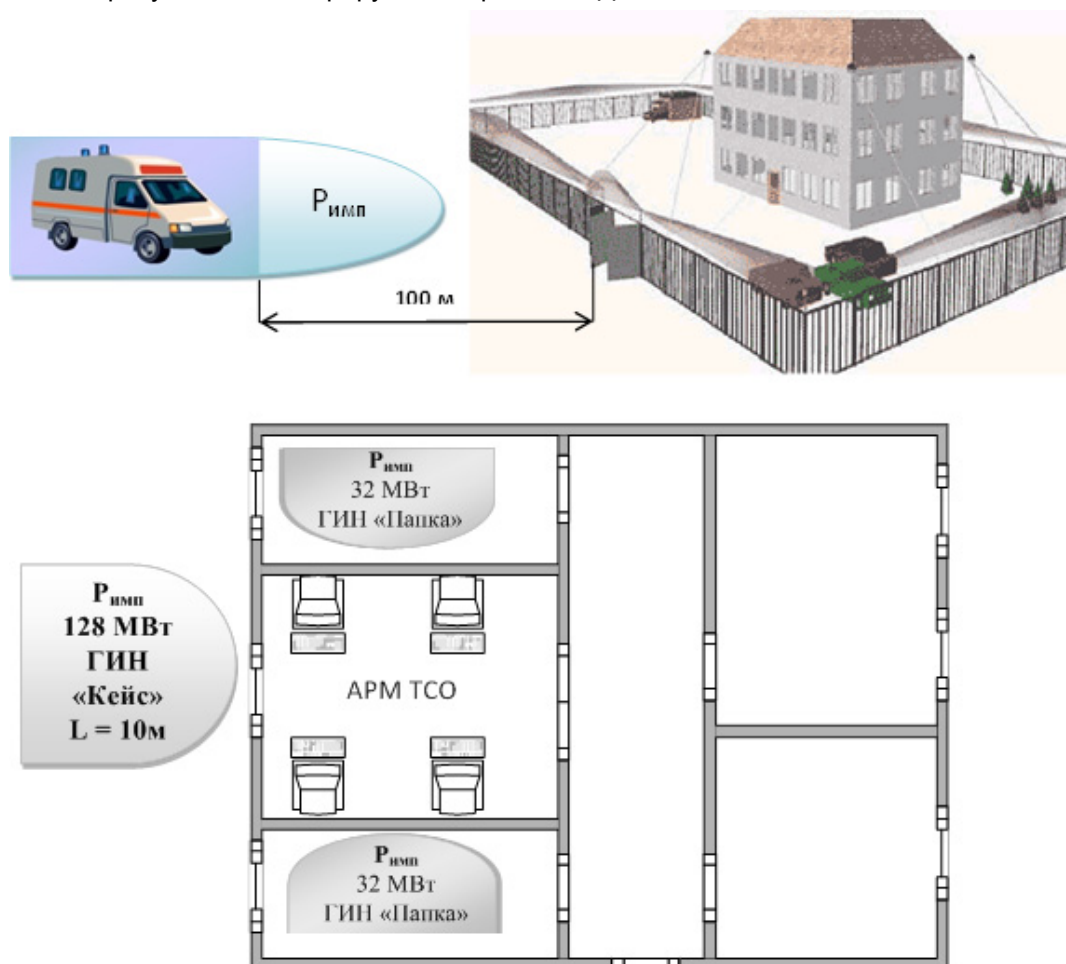


Рис. 1. Варианты ПД ЭМВ

При проведении испытаний ТСБ с целью определения уровней устойчивости к ПД ЭМВ как наиболее полного типа испытаний должны воспроизводиться все виды воздействий ПД ЭМВ, предусмотренные ГОСТ Р 52863-07. Результаты испытаний целесообразно группировать в форме таблицы, содержащей столбцы с названиями:

- № п/п.
- Компонент ТСБ.
- Вид воздействия.
- Вид нарушения функционирования.
- Уровень устойчивости, кВ/м.

Полученные результаты испытаний типовых изделий могут быть включены в их формуляры в виде дополнений.

Понятно, что проведение испытаний элементов ТСБ на устойчивость к ПД ЭМВ повлечёт за собой дополнительные затраты. Однако наличие в формулярах на изделия значений реальных уровней устойчивости к данной угрозе будет способствовать их приоритетному выбору заказчиком при оборудовании объектов техническими средствами безопасности.

Организация и содержание работ по защите автоматизированных систем от преднамеренных деструктивных электромагнитных и электрических воздействий

Проблеме защиты от ПД ЭМВ уделяется важное внимание со стороны зарубежных и отечественных организаций.

На международном уровне Комиссией EURSI в 1997 г. в составе Комитета по ЭМИ образован подкомитет по электромагнитному терроризму. Помимо этого, данная проблема выделена Международной электротехнической комиссией как самостоятельное направление в области электромагнитной совместимости образованием специального подкомитета 77С. Основным направлением международной деятельности является разработка целевых стандартов по обеспечению устойчивости гражданских объектов к действию мощных ЭМИ.

В России силами организаций научного и прикладного профиля ведутся работы по выявлению и изучению деструктивных эффектов, вызываемых ПД ЭМВ, по разработке способов и средств защиты от них информационных систем и по созданию нормативной базы по защите в виде системы целевых стандартов РФ (рисунок 2). При этом предполагается, что работы по защите от ПД ЭМВ должны вестись как на ведомственном/отраслевом, так и на региональном уровнях.

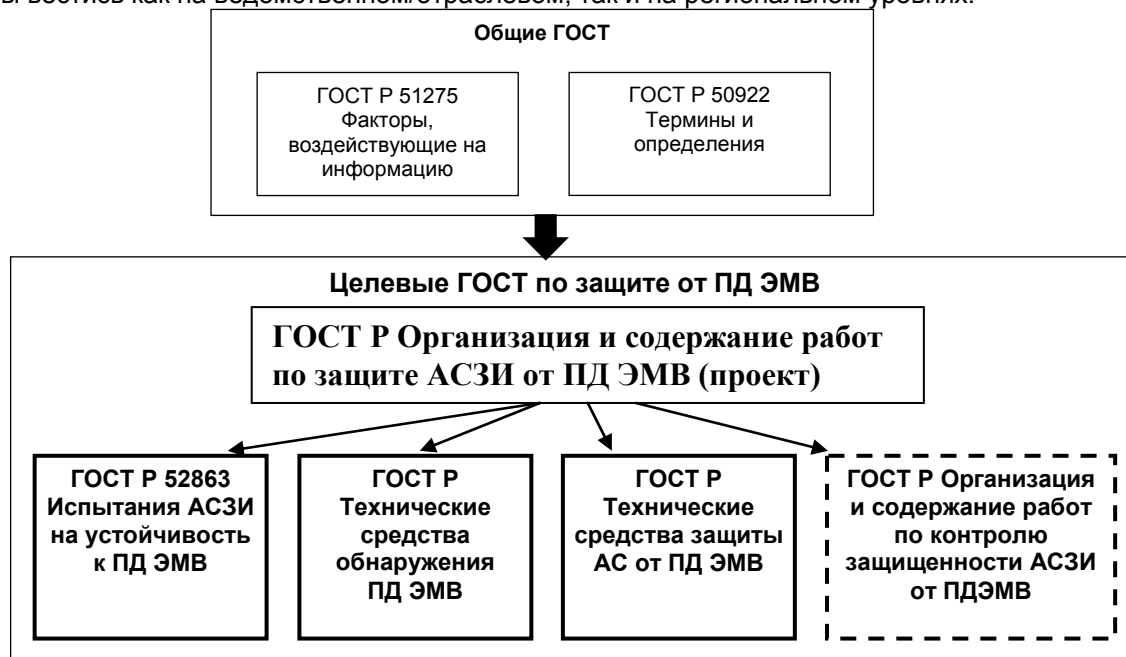


Рис. 2. Система целевых стандартов РФ по защите от ПД ЭМВ

На рисунке 3 представлен примерный перечень сфер применения средств информатизации региона, которые могут быть подвержены электромагнитному нападению, и его возможные последствия.

Их соизмеримость по масштабам с последствиями прямых террористических атак выдвигает проблему защиты этих средств от такого нападения в разряд первоочередных. К особенностям региональной информационной инфраструктуры, которые следует учитывать при построении её защиты от ПД ЭМВ, относятся:

- возможность как совместного местонахождения нескольких разнопрофильных объектов информатизации в пределах одного здания/комплекса (например, администрации региона), так и их обособленное размещение;
- нахождение в регионе объектов информатизации разной ведомственной/территориальной подчинённости;
- нахождение в регионе объектов информатизации разных категорий опасности/важности;
- функциональное взаимодействие ряда объектов, вследствие которого ПД ЭМВ может привести к эффекту «домино»;
- различие режимов функционирования средств информатизации и связанный с этим изменяющийся во времени уровень их уязвимости;
- замкнутость средств информатизации на существующую в регионе информационно-коммуникационную сеть и систему электропитания;
- специфика построения комплексной системы безопасности региона, включающей систему оповещения и реагирования и т.д.

Эти особенности, а также другие факторы, отражающие специфику выполнения работ по защите автоматизированных систем (АС) от ПД ЭМВ, учтены при разработке проекта ГОСТ Р «Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных деструктивных электромагнитных и электрических воздействий. Общие положения». В данном документе, выполняющем системообразующую функцию, определяются и устанавливаются:

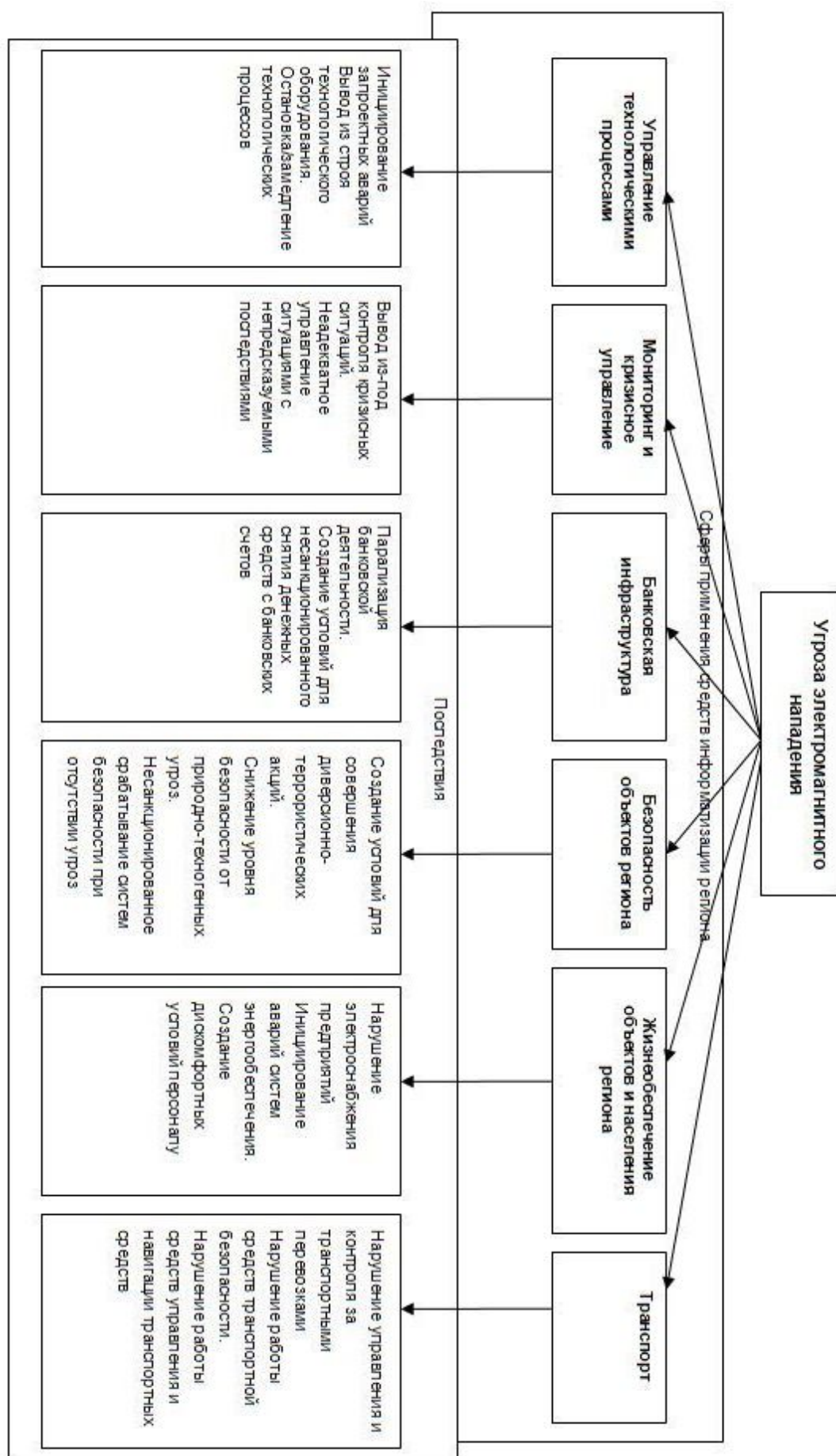


Рис. 3. Угрозы ПД ЭМВ региональным средствам информатизации и их последствия

- роль и место работ по защите АС от ПД ЭМВ во взаимодействии с работами по построению комплексной системы безопасности;
- структурные компоненты защиты (помещение, системы обеспечения, АС, средства обнаружения и защиты, организационные меры), рисунок 4;
- дифференцированный подход к защите (с учётом соотношения затрат и предотвращаемого ущерба);
- этапы и содержание работ по защите;
- исполнители работ по защите (организация/учреждение-пользователь АС, специализированная, проектная, строительно-монтажная, экспертная организации, поставщики технических средств (ТС), контрольно-надзорный орган);
- функции, возлагаемые на исполнителей работ по защите;
- ответственность за обеспечение требований по защите при эксплуатации АС.

При разработке стандарта принималось во внимание, что ПД ЭМВ сочетает в себе признаки как угроз информационной безопасности, так и совершения несанкционированных действий силовыми методами. Поэтому структура документа и стиль изложения материала ориентированы на достаточно широкий круг его потенциальных пользователей в области комплексной безопасности информации и объектов.

Согласно положениям стандарта, работы по защите выполняются:

- при создании АС в защищённом от ПД ЭМВ исполнении (см. таблицу 2);
- при эксплуатации АС в составе объектов ИИ (см. таблицу 3).

Таблица 2.

Виды, содержание и исполнители работ по созданию АС в защищённом от ПД ЭМВ исполнении

№ п/п	Виды работ	Содержание работ	Исполнители
1	Разработка Концепции защиты информации в АС от ПД ЭМВ	Обследование и тестирование АС в составе ОИ Построение модели угроз Формирование требований по защите Формирование проектных решений защиты Оценка эффективности защиты	Специализированная организация Заказчик (организация-пользователь АСЗИ) Экспертная организация
2	Реализация проектных решений защиты	Разработка ТЗ на проектирование Проектные работы Монтаж, пуск и наладка АС в защищённом от ПД ЭМВ исполнении	Проектная организация Поставщики АС, ТС обнаружения ПД ЭМВ и защиты от них Строительно-монтажная организация Организация-пользователь АСЗИ Экспертная организация Контрольно-надзорный орган ведомства
3	Ввод в действие АС в защищённом исполнении (АСЗИ)	Опытная эксплуатация АСЗИ в составе ОИ Приёмочные испытания АСЗИ в составе ОИ Аттестация АСЗИ в составе ОИ	Организация-пользователь АСЗИ Комиссия

Таблица 3.

Виды, содержание и исполнители работ по защите АС от ПД ЭМВ при их эксплуатации в составе ИИ

№ п/п	Виды работ	Содержание работ	Исполнители
1	Использование по назначению ТС обнаружения ПД ЭМВ и защиты от них	Мониторинг э/м обстановки Снижение/блокирование ПД ЭМВ Перевод АСЗИ в безопасный режим	Организация-пользователь АСЗИ
2	Выполнение целевых организационно-технических мероприятий	Предупреждение, пресечение ЭМА, локализация и ликвидация последствий	Организация-пользователь АСЗИ
3	Техническая эксплуатация ТС обнаружения ПД ЭМВ и защиты от них	Контроль исходного состояния и функционирования ТС Техническое обслуживание ТС Ремонт ТС	Организация-пользователь АСЗИ Поставщики ТС
4	Контроль защищённости АСЗИ в составе ОИ	Проверка функциональных свойств ТС обнаружения и защиты Проверка функциональных свойств защитных компонент и уровня защиты	Организация-пользователь АСЗИ Специализированная организация Контрольно-надзорный орган ведомства

По каждому виду работ в стандарте достаточно развёрнуто изложены их содержание, организация и порядок выполнения, формы отчётности.

В приложениях стандарта приведены:

- состав информации, определяемой при обследовании и тестировании АС в составе объекта информатизации;
- форма сводной таблицы угроз ПД ЭМВ;

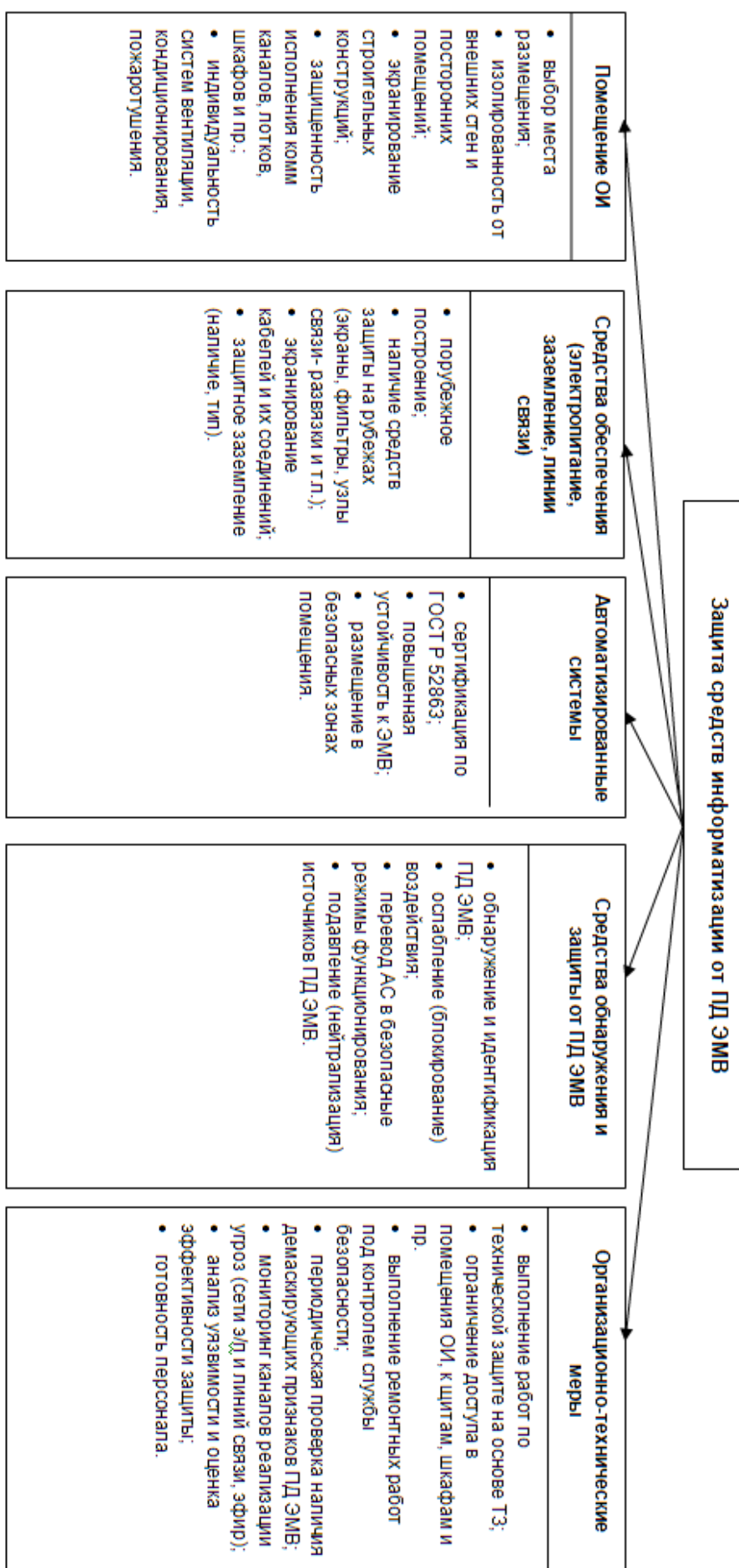


Рис. 4. Структурные компоненты защиты от ПД ЭМВ

- типовая форма раздела формуляра (технического паспорта) АСЗИ в составе объекта информатизации по защите от ПД ЭМВ;
- типовая методика категорирования АС по степени их важности (потенциальной опасности).
- типовые формы разрабатываемых документов и некоторые информационные данные, необходимые для проведения работ.

Являясь документом федерального уровня, стандарт содержит, главным образом, общие положения в части организации и содержания работ по защите АС от ПД ЭМВ. Их развитие и конкретизация на региональном уровне должны производиться в виде соответствующих комплектов документов, таких как:

- обобщённая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (КСИИ) региона;
- специальные требования и рекомендации по защите КСИИ региона от ПД ЭМВ;
- методические рекомендации по категорированию КСИИ региона и оценки их защищённости от ПД ЭМВ;
- методические рекомендации по контролю защищённости КСИИ региона от ПД ЭМВ;
- распорядительная, плановая и учётная документация по защите КСИИ от ПД ЭМВ.

Организационно работы по защите региональной информационной инфраструктуры могут проводиться как в индивидуальном порядке, так и в составе комплексной программы «Безопасный регион».

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищённом исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования.
2. В. Богданов, М. Жуковский, С. Ларионов, В. Чванов. Электромагнитная угроза: от мифа к реальности. БДИ №3(89), 2010.

Молдовян А.А., Морозова Е.В., Рыжков А.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
КОММУТАТИВНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ С УЧЕТОМ ТРУДНОСТИ РЕШЕНИЯ
ЗАДАЧИ ФАКТОРИЗАЦИИ**

Введение

Алгоритмы коммутативного шифрования применяются для решения ряда специфических задач информационных технологий, таких как построение протоколов бесключевого шифрования [1], электронной жеребьевки и игры в покер по телефону [2]. Широко известен алгоритм коммутативного шифрования Полига-Хеллмана [3], основанный на трудности задачи дискретного логарифмирования (ЗДЛ) в простом конечном поле. Для повышения производительности процедур коммутативного шифрования в работе [4] предложена реализация алгоритма Полига-Хеллмана над конечным расширенным полем, заданным в явной векторной форме. Повышение скорости шифрования достигается за счет сравнительно низкой сложности операции умножения и возможности ее эффективного распараллеливания в полях указанного типа. С целью повышения уровня безопасности коммутативной функции шифрования представляет интерес разработка алгоритма, взлом которого требует одновременного решения двух независимых трудных задач, в частности ЗДЛ в конечном поле и задачи факторизации (ЗФ).

В настоящем сообщении решается задача синтеза алгоритма коммутативного шифрования, основанного на трудности одновременного решения ЗДЛ в конечном поле и ЗФ.

1. Особенности использования задачи факторизации в коммутативных шифрах

Обычно предлагается, что входное сообщение, предназначенное для шифрования, не должно иметь ограничений, кроме как ограничений на длину шифруемых блоков или на максимально допустимое значение при его интерпретации как двоичного числа. Это связано с тем, что в реальных ситуациях может понадобиться выполнять шифрование самых различных сообщений, в том числе и случайных битовых строк. Данное требование трудно реализовать при разработке коммутативных шифров с использованием эллиптических кривых (ЭК), заданных над конечными полями. Причиной этому является то, что координаты точек ЭК должны удовлетворять некоторому уравнению третьей степени, а значит не все пары значений соответствуют точкам ЭК. Синтез алгоритмов коммутативного шифрования с использованием вычислений на ЭК требует решения задачи кодирования сообщений точками ЭК. Подходы к решению данной задачи неочевидны.

Проблемы имеются также и в случаях построения алгоритмов коммутативного шифрования с использованием вычислений по трудно разложимому модулю n , представляющему собой произведение двух больших простых чисел [5] q и r ($n = qr$). Эти проблемы обусловлены тем, что значение модуля не может использоваться в качестве секретного ключа или его части, поскольку вычисление по различным модулям не обладает свойством коммутативности. Это означает, что значение трудно разложимого на множители модуля должно быть общим системным

параметром алгоритма, т.е. должно быть известным всем пользователям. Поскольку предполагается, что стойкость алгоритма основывается на трудности 3Ф, то значение n должно вырабатываться некоторым доверительным центром, который уничтожит случайно сгенерированные им простые числа q и r после вычисления числа $n = qr$. Поскольку значения q и r являются для пользователей недоступными, то для них является вычислительно невозможным вычисление функции Эйлера $\varphi(n) = (q-1)(r-1)$ от числа n , что позволило бы вычислить пару значений e и d , таких, что $ed = 1 \bmod \varphi(n)$. Наличие такой пары значений позволило бы выполнять коммутативное шифрование. Однако предоставление пользователю значения функции Эйлера от модуля (например, значение $\varphi(n)$ могло бы быть вычислено доверительным центром) позволит им легко факторизовать модуль методом, описанным в [1].

Если возложить функцию генерации пар секретных ключей (e, d) на доверительный центр, то два различных пользователя могут раскрыть друг другу свои секретные значения, что позволит им вычислить значения q и r , т.е. взломать такую систему коммутативного шифрования. Способ реализации такой атаки описан, например, в книге [1]. Требуется найти механизм, использующий известные параметры, зависящие от множителей числа n , известность которых не упрощает задачи его факторизации. В качестве данного механизма можно использовать схему [6,7] формирования числа α , порядок которого по модулю n равен достаточно большому простому числу γ (размером не менее 160 бит), удовлетворяющему следующим условиям делимости: $\gamma | q-1$ и $\gamma | r-1$. Эти условия сохраняют высокую трудность 3Ф модуля n при известных значениях α и γ . В работе [7] описана процедура генерации значений n , α и γ , удовлетворяющих указанным условиям.

Механизм коммутативного шифрования работает следующим образом для всех сообщений, значения которых выражаются числами $\alpha^i \bmod n$, где $i = 1, 2, \dots, \gamma$. Используя известное значение γ , каждый пользователь генерирует случайное значение $e < \gamma$ и вычисляет значение $d = e^{-1} \bmod \gamma$. Пара значений e и d составляет ключ зашифрования и расшифрования, соответственно. Шифрование при этом обладает свойством коммутативности. Однако эти процедуры корректно работают только по отношению к сообщениям, которые представимы в виде $\alpha^i \bmod n$. Количество сообщений данного вида достаточно велико, однако среди них нет таких сообщений, которые может потребоваться зашифровать, т.е. возникла такая же проблема как и в случае синтеза коммутативных шифров с использованием вычислений на эллиптической кривой. Рассмотрим варианты решения данной проблемы.

В частных случаях приложений коммутативных шифров требуется зашифровывать конечное число заранее известных сообщений (например, в протоколе игры в покер по телефону). В этих случаях можно закодировать известные сообщения значениями вида $\alpha^i \bmod p$. Однако для шифрования произвольных сообщений рассмотренная схема неприменима непосредственно. Для того, чтобы с помощью предлагаемого механизма можно было бы выполнить коммутативное шифрование требуется использовать дополнительный механизм (расщепление сообщений), который описан далее. При этом предполагается, что значения n , α и γ генерируются некоторым доверительным центром.

2. Механизм расщепления сообщений

Число значений вида $\alpha^i \bmod n$ равно $\gamma \geq 2^{160}$. Количество этих значений практически нельзя перебрать, поэтому их можно использовать в качестве ключа шифрования. Пусть требуется зашифровать сообщение $M < n$. Сгенерируем случайное число $k < \gamma$ и вычислим значение $K = \alpha^k \bmod n$. Зашифруем сообщение M путем сложения со значением K по модулю n , т.е. по формуле $C = M + K \bmod n$. Сообщение M можно восстановить из пары значений (C, K) т.е. M можно расщепить на два значения C и K , причем C – число произвольного вида, а K принадлежит следующему множеству значений $\{\alpha^1 \bmod n, \alpha^2 \bmod n, \dots, \alpha^\gamma \bmod n\}$. После расщепления сообщения M его зашифрование (расшифрование) можно выполнить как зашифрование (расшифрование) значения K . Последнее можно выполнить путем возведения K в степень e по модулю n , т.е. по формуле $S = K^e \bmod n$. Расшифрование выполняется как возведение криптограммы S' в степень d по модулю n , т.е. по формуле $S'^d \bmod n = K$. Значение C , по которому можно восстановить сообщение M , не подвергается какому-либо преобразованию в процессе шифрования. Получаем следующую схему коммутативного шифрования:

1. Первичное шифрование сообщения M выполняется как расщепление $M : M = (C, K)$ и шифрование значения $K : S = K^e \bmod n$. На выходе первичной процедуры шифрования имеем пару значений (C, S) .

2. Последующие шаги зашифрования/расшифрования выполняются как шифрование значения S .

3. 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 $M = C - K \bmod n$.

Данная схема коммутативного шифрования основана на трудности 3Ф и трудности ЗДЛ по составному модулю n и позволяет выполнить шифрование сообщений $M < n$ произвольного вида. Последнее достигается за счет применения механизма расщепления шифруемого сообщения – представления сообщения в виде пары других сообщений, одно из которых представляет собой число вида $\alpha^i \bmod n$ при некотором значении $i \in \{1, 2, \dots, \gamma\}$.

3. Алгоритм коммутативного шифрования, взлом которого требует одновременного решения двух независимых трудных задач

Нетрудно заметить, что алгоритм Полига-Хеллмана может быть естественным образом встроен в описанный ранее алгоритм коммутативного шифрования при использовании в первом простого числа $p > n$. Это реализуется путем одновременного шифрования обоих значений, представляющих сообщение M в расщепленном виде. Для этого каждый пользователь выбирает две пары ключей (e_1, d_1) и (e_2, d_2) , удовлетворяющих условиям $e_1 d_1 = 1 \bmod \gamma$ и $e_2 d_2 = 1 \bmod p-1$. Шифрование первого значения в паре расщепления выполняется по первой паре подключей как возведение в степень e_1 (зашифрование) или d_1 (расшифрование) по модулю p . Шифрование второго значения в паре расщепления выполняется по второй паре подключей как возведение в степень e_2 (зашифрование) или d_2 (расшифрование) по модулю n . Получаем следующую схему коммутативного шифрования:

1. Первичное зашифрование сообщения M выполняется как расщепление $M : M = (C, K)$, зашифрование K по формуле $S = K^{e_2} \bmod n$ и зашифрование C по формуле $C^* = C^{e_1} \bmod p$. На выходе первичной процедуры шифрования имеем пару значений (C^*, S) .

2. Последующие шаги зашифрования/расшифрования выполняются как шифрование значения S путем выполнения операции возведения в степень по модулю n и шифрование значения C^* путем выполнения операции возведения в степень по модулю p .

3. Завершающий шаг расшифрования выполняется как расшифрование значения S , приводящее к восстановлению значения K , расшифрование значения C^* , приводящее к восстановлению значения C , и вычисление значения M по формуле $M = C - K \bmod n$.

Нетрудно видеть, что взлом данного алгоритма коммутативного шифрования требует одновременного решения 3Ф и ЗДЛ в конечном простом поле. Шифрование второго элемента пары расщепления осуществляется как возведение в секретную степень по модулю n , поэтому можно говорить не о 3Ф, а о ЗДЛ по трудно разложимому модулю n . Однако последняя задача принципиально отличается от ЗДЛ по простому модулю. Кроме того, алгоритм решения ЗДЛ модулю n может быть использован для факторизации значения модуля n . Алгоритм решения 3Ф сводит ЗДЛ по трудно разложимому модулю n к ЗДЛ по простому модулю. Это показывает существенную связь 3Ф и ЗДЛ по модулю n .

Заключение

Разработаны алгоритмы коммутативного шифрования, основанные на трудности 3Ф в том числе алгоритм, стойкость которого основана на трудности одновременного решения 3Ф и ЗДЛ. Существенным конструктивным элементом синтезированных алгоритмов является механизм расщепления исходного сообщения. Применяя предложенный механизм расщепления легко разработать алгоритмы коммутативного шифрования, основанные на трудности ЗДЛ на ЭК. Коммутативные алгоритмы шифрования на основе ЭК представляют значительный практический интерес, поскольку они могут обеспечить существенное повышение производительности. Однако это представляет задачу самостоятельного исследования по расширению типов криптосхем, реализуемых на основе трудности ЗДЛ на ЭК [8,9].

Алгоритмы шифрования, включающие в себя механизм расщепления сообщения, могут быть отнесены к классу вероятностных шифров. Их недостатком является то, что размер шифртекста

превышает размер исходного сообщения. В случае рассмотренных алгоритмов коммутативного шифрования размер криптограммы примерно в два раза больше размера сообщения. Однако за счет этого обеспечивается возможность использования трудности 3Ф, а также на основе трудности одновременного решения 3Ф и 3ДЛ в конечном поле, за счет чего может быть существенно повышен уровень безопасности алгоритма коммутативного шифрования.

СПИСОК ЛИТЕРАТУРЫ

1. Молдовян А.А., Молдовян Н.А. Введение в криптосистемы с открытым ключом. – Санкт-Петербург, БХВ–Петербург, 2005. – 286с.
2. Дернава Е.С., Молдовян Н.А., Молдовян Д.Н. Криптографические протоколы. – СПб., Изд. СПбГЭТУ, 2010. – 100с.
3. Hellman M.E., Pohlig S.C. Exponentiation Cryptographic Apparatus and Method // U.S. Patent # 4,424,414. 3 Jan. 1984.
4. Молдовяну П.А., Молдовян Д.Н., Морозова Е.В., Пилькевич С.В. Повышение производительности процедур коммутативного шифрования // Вопросы защиты информации. 2009. №4. С.24–31.
5. Menezes A. J., Vanstone S.A. Handbook of Applied Cryptography. – CRC Press, 1996. – 750p.
6. Молдовян Н.А. практикум по криптосистемам с открытым ключом. – Санкт-Петербург, БХВ–Петербург, 2007. – 298с.
7. Moldovyan A.A., Moldovyan D.N., Gortinskaya L.V. Cryptoschemes based on new signature formation mechanism // Computer Science Journal of Moldova. 2006. Vol.14. №3(42). P.397–411.
8. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. – М., КомКнига, 2006. – 320с.
9. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. М., КомКнига, 2006. – 274 с.

Никифоров В.В., Шкиртиль В.И.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ЗАЩИТА ЦЕЛОСТНОСТИ ЛОКАЛЬНЫХ ДАННЫХ В РАСПРЕДЕЛЕННЫХ РЕАГИРУЮЩИХ СИСТЕМАХ**

Проблема обеспечения целостности информационных ресурсов, стоит в ряду ключевых проблем логической корректности программных приложений для систем реального времени (СРВ) [1]. Защита информационных ресурсов, доступных различным задачам (разделяемых информационных ресурсов), обеспечивается использованием специальных синхронизирующих механизмов (например, мьютексов). Локальные статические информационные ресурсы конкретной задачи недоступны другим задачам, но при периодической активизации задачи могут использоваться однотипными заданиями (экземплярами этой задачи), порождаемыми в результате каждой такой активизации. Необходимость защиты целостности статических информационных ресурсов возникает в том случае, если интервалы существования однотипных заданий могут пересекаться. Подобные пересечения возможны, если время отклика задачи (максимально возможная длина интервала существования соответствующих ей заданий) превышает продолжительность периода ее активизации. В таком случае защита целостности статических информационных ресурсов может быть обеспечена использованием тех же синхронизирующих механизмов, которые используются для защиты разделяемых глобальных информационных ресурсов [2-5]. Однако, для большинства задач СРВ время отклика не превышает периода, для таких задач угроза нарушения целостности локальных ресурсов отсутствует и в этом случае использование синхронизирующих механизмов защиты означало бы ненужные затраты памяти и процессорного времени. Это обстоятельство является одной из причин, вызывающих актуальность разработки методов, обеспечивающих оценку величины времени отклика задач для многозадачных программных приложений и в частности для программных приложений СРВ.

Авторами разработаны методы оценки времени отклика задач в распределенных программных приложениях, представляемых вычислительными моделями, отвечающими ряду ограничений. Особенностью вычислительных моделей программных приложений для распределенных систем является наличие отношений предшествования между задачами, размещаемыми в различных узлах. В общем случае отношения предшествования для задач, вовлекаемых в реакцию СРВ на определенный тип внешних событий, представляются ориентированным графом без контуров. Большинство практических систем отвечает более строгому ограничению — графы предшествования имеют вид цепочек. Еще более глубокое ограничение — две соседние задачи в цепочке принадлежат различным узлам системы. Тогда каждая дуга графа предшествования соответствует сообщению, посылаемому из одного узла системы в другой узел. Время отклика всей последовательности задач, соответствующих цепочке, на внешнее событие получается суммированием продолжительностей исполнения каждой из задач и продолжительностей передачи каждого из сообщений. Проблема оценки времени отклика сводится к оценке величины каждого из слагаемых этой суммы. Время исполнения отдельной задачи цепочки зависит от состава задач, претендующих на процессорное время в этом узле и используемой дисциплины планирования. Расчет этого времени выполняется с использованием методов, разработанных для однопроцессорных систем с учетом задержек регистрации некорневых задач цепочки. Разработан подход, обеспечивающий использование тех же методов для оценки времени передачи пакетов сообщений и элементарных сообщений в локальных коммуникационных сетях со встроенными механизмами арбитража (например, с интерфейсами типа CAN).

Коммуникационная система как исполнительный ресурс. В распределенных СРВ прикладные программы рассредоточены по узлам, соединяемым коммуникационными каналами (рисунок 1).

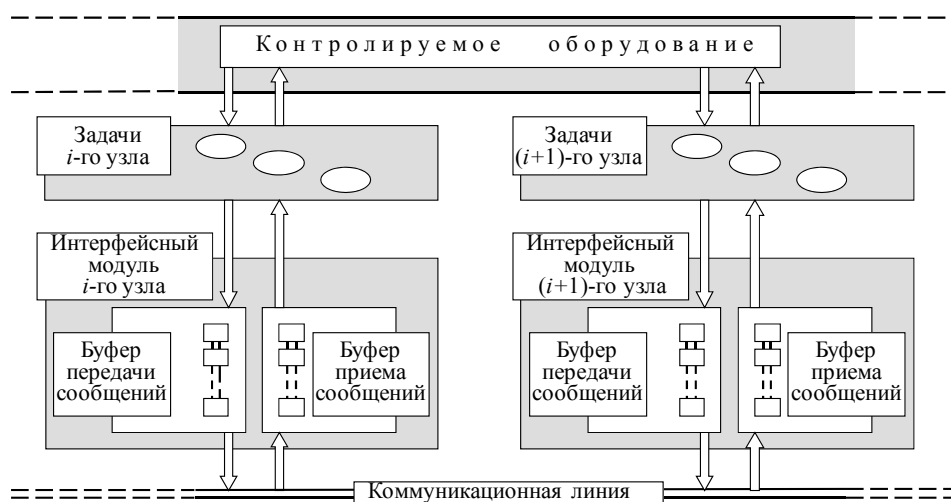


Рис. 1. Связи узлов распределенной СРВ между собой и с внешним (контролируемым) оборудованием

Коммуникационная линия является аппаратным ресурсом, динамически разделяемым сообщениями. Сообщения генерируются в узлах распределенной системы и поступают в интерфейсные блоки, обеспечивающие их передачу по коммуникационной линии. Очередность использования коммуникационной линии готовыми к передаче сообщениями определяется принятым для данной коммуникационной системы протоколом. В случае использования коммуникационных линий с CAN-интерфейсом каждому типу передаваемых сообщений статически присваиваются фиксированные значения приоритетов. Порожденное в одном из узлов сети с CAN интерфейсом низкоприоритетное сообщение ожидает момента, когда линия окажется свободной от передачи более приоритетных сообщений. Таким образом, время доставки сообщения по сети с CAN интерфейсом зависит не только от быстродействия образующей сеть аппаратуры и от длины самого сообщения, но и от загруженности сети более приоритетными сообщениями. То есть, имеет место интерференция передаваемых по сети сообщений, аналогичная интерференции задач многозадачного приложения, исполняемого одним процессором.

Аналогия между заданиями, разделяющими ресурс процессора и сообщениями, разделяющими ресурс коммуникационной линии, оказывается достаточно глубокой. Различные аспекты этой аналогии представлены в таблице 1 [6].

Таблица 1

Две разновидности исполнительных ресурсов

Системные объекты и события	Целевая функция исполнительного ресурса	
	Обработка данных	Передача данных
Исполнительный ресурс	Процессор, ядро многоядерного процессора	Интерфейсные модули с коммуникационной линией
Статический объект – класс динамических объектов	Задача τ_i	m_i – тип сообщений
Динамический (исполняемый) объект	Задание $\tau_i^{(j)}$	Конкретное сообщение $m_i^{(j)}$
Начало интервала существования объекта	Порождение задания $\tau_i^{(j)}$	Поступление $m_i^{(j)}$ в интерфейсный блок
Старт исполнения целевой функции	Начало исполнения задания $\tau_i^{(j)}$	Начало передачи сообщения $m_i^{(j)}$ по каналу
Конец интервала существования объекта	Задание $\tau_i^{(j)}$ выполнено	Сообщение $m_i^{(j)}$ передано

При определенных условиях методы анализа, разработанные для оценки выполнимости задач в однопроцессорных СРВ, могут быть использованы для оценки своевременности доставки сообщений между узлами распределенных систем. Эти результаты могут быть использованы для оценки продолжительности выполнения цепочек задач, обеспечивающих реакцию СРВ, на внешние события. Рассмотрение ведется на примере СРВ, использующих локальные коммуникационные сети с интерфейсом CAN (Controller Area Network).

Основные особенности CAN-интерфейса. Локальные сети на основе коммуникационного интерфейса CAN широко используются в автомобилях, системах автоматизации технологических процессов, медицинской аппаратуре и других системах реального времени [7,8].

При использовании локальной сети, оснащенной CAN-интерфейсом, элементарные сообщения, передаваемые в однопроводную коммуникационную линию, разделяются интервалами пассивного состояния линии (логический ноль). Формат стандартного сообщения в упрощенном виде представлен на рисунке 2. Сообщение начинается стартовым фреймом, за которым следуют информационные поля и стоповый фрейм.

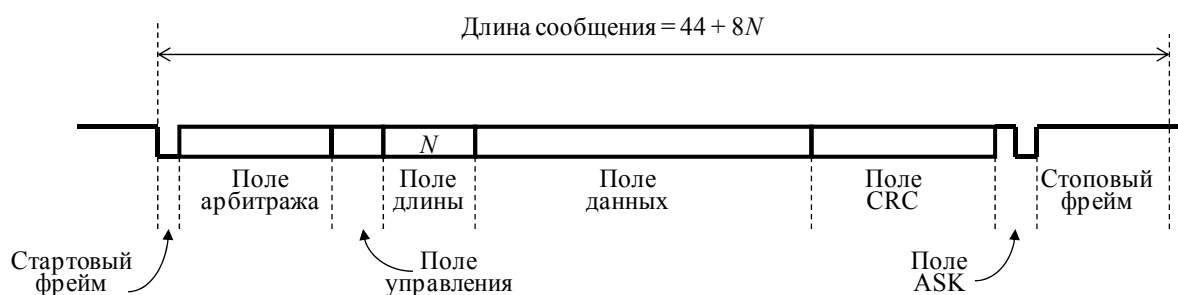


Рис. 2. Структура стандартного сообщения сетей с CAN интерфейсом

Узлы сети могут начинать передачу сообщения только тогда, когда линия находится в пассивном состоянии. При появлении в линии стартового фрейма все узлы синхронизируются его фронтом. Может оказаться, что два и более узла одновременно генерировали стартовый фрейм – возникает конфликт по запросу на использование коммуникационной линии. Этот конфликт должен быть устранен в ходе формирования поля арбитража.

Поле арбитража длиной 11 бит имеет двойное назначение. Во-первых, код, размещаемый в поле арбитража, идентифицирует тип передаваемого сообщения. Во-вторых, значение этого кода определяет приоритет сообщения: нулевой код соответствует наиболее приоритетным сообщениям; чем больше значение двоичного числа, размещаемого в поле арбитража, тем ниже приоритет передаваемого сообщения. Типы передаваемых сообщений распределены между узлами сети, так что если два узла сети одновременно начали передавать сообщения, то это сообщения различных типов.

Пассивное состояние коммуникационной линии соответствует символу 1 (рецессивный бит), активное состояние – символу 0 (доминантный бит). В рамках поля арбитража несколько узлов могут попытаться начать передачу очередного сообщения. Каждый передающий узел контролирует состояние коммуникационной линии в ходе передачи каждого бита. Если все они передают рецессивный бит, линия находится в пассивном состоянии. Узел, передающий пассивный бит, прекращает попытку передачи сообщения, если он обнаруживает, что существует конкурирующий узел, который в этот момент передает активный бит (линия находится в активном состоянии). К моменту, когда завершается передача битов поля арбитража только один узел продолжает передачу. Таким образом, в ходе дальнейшей передачи наиболее приоритетного сообщения предотвращается одновременная передача сообщений, генерируемых другими узлами.

Четырехбитный код поля длины задает число байт (до 8), размещаемых в поле данных. Само поле данных содержит информацию, доставка которой является целью передачи сообщения, остальные поля играют служебную роль. Поэтому байты, размещаемые в поле данных, уместно называть целевыми данными. За полями длины, данных и контрольной суммы следует поле ASK – поле подтверждения приема. Это означает, что принимающий узел сети, обнаружив адресованное ему сообщение, помечает его как принятое в рамках формата самого передаваемого сообщения, а не в последующих сообщениях. Такое решение повышает оперативность обмена данными.

Порядок доставки сообщений через сеть иллюстрируется на рисунке 2. Отдельный узел сети содержит ряд прикладных задач, которые генерируют сообщения, адресуемые либо соседним задачам, либо задачам, содержащимся в других узлах. В последнем случае сгенерированное сообщение направляется в интерфейсный блок и размещается в его буфере. В буфере интерфейсного блока сообщения упорядочиваются по приоритетам. В момент, когда линия переходит в пассивное состояние, интерфейсный блок пытается передать самое приоритетное из сообщений, находящихся в его буфере. Эта попытка окажется удачной, если одновременно интерфейсный блок какого-то другого узла не пытается передать более приоритетное сообщение.

Оценка времени доставки пакетов сообщений. Ключевым обстоятельством, определяющим полноту аналогии, отражаемой в таблице 1, является тот факт, что для коммуникационных систем с CAN-интерфейсом порядок учета приоритетов сообщений, поступивших в интерфейсные блоки, в точности соответствует порядку учета приоритетов заданий, порождаемых универсальным процессором. Характер конкуренции (между поступившими в интерфейсные блоки сообщениями) за предоставление ресурса коммуникационной линии в точности повторяет характер конкуренции (между порожденными заданиями) за предоставление ресурса процессора. Интерференция сообщений, приводящая к увеличению времени их доставки в точности соответствует интерференции заданий с теми же значениями модельных параметров. Поэтому вычислительные модели и методы, используемые для оценки времени отклика задач с фиксированными приоритетами могут использоваться для оценки времени доставки сообщений в сетях с CAN-интерфейсом [9].

В ряду вычислительных моделей, используемых для оценки времени отклика задач с фиксированными приоритетами, отметим модели, позволяющие учитывать задержку регистрации заданий, возникающих в результате активизации задач и взаимное блокирование задач, разделяющих глобальные информационные ресурсы. Такие модели содержат параметры:

- период T_i активизации задачи τ_i (минимальный интервал времени между активизациями задачи τ_i),
- фактор веса C_i (максимальный объем процессорного времени, требуемого для выполнения отдельного задания типа τ_i),
- фактор приоритета I_i (суммарная продолжительность интервалов времени, в рамках которых задача ожидает момента освобождения процессора, занятого выполнением экземпляров более приоритетных задач),
- фактор блокирования B_i (максимальная продолжительность интервала времени блокирования, в течение которого высокоприоритетная задача ожидает момента освобождения ресурсов, занимаемых менее приоритетными задачами),
- фактор дребезга J_i (максимально возможная задержка регистрации заданий типа τ_i).

Для вычислительных моделей с такими параметрами время отклика R_i задачи τ_i определяется как сумма

$$R_i = C_i + J_i + I_i + B_i, \quad (1)$$

где значение фактора приоритета определяется равенством

$$I_i = \sum_{\text{prio}(\tau_i) < \text{prio}(\tau_k)} C_k \left\lceil \frac{R_i + J_k - J_i}{T_k} \right\rceil \quad (2)$$

(символ $\lceil x \rceil$ означает целое число, ближайшее сверху к числу x), выражение $\text{prio}(\tau_i) < \text{prio}(\tau_k)$ означает, что приоритет задачи τ_k выше, чем приоритет задачи τ_i .

Аналогично определяется продолжительность интервала времени доставки пакетов сообщений. Каждый из типов сообщений m_i характеризуется модельными параметрами $C(m_i)$ и $T(m_i)$. Величина параметра задает ограничение на частоту поступления сообщений типа m_i в интерфейсные блоки коммуникационной системы: моменты времени поступления сообщений и разделены интервалами времени, длина которых не меньше $T(m_i)$. Величина $C(m_i)$ определяет максимально возможную длину сообщений типа m_i . Для сообщений с низшим приоритетом значение фактора блокирования $B(m_i)$ по определению равно нулю. Для остальных сообщений $B(m_i)$ равно максимальной продолжительности передачи коммуникационной линией отдельного элементарного сообщения. Параметр $J(m_i)$ определяет максимально возможную вариацию продолжительности интервала времени между моментом порождения прикладной задачи, генерирующей сообщения типа m_i и моментом поступления этого сообщения в интерфейсный модуль коммуникационной системы.

Условимся индексировать типы сообщений в порядке понижения их приоритетов: сообщения типа имеют наивысший приоритет, с увеличением значений индекса приоритет сообщений снижается. Время доставки сообщения $m_i^{(j)}$ определяется как разность $\tau_i^{(j)} = t_{\text{end}}(m_i^{(j)}) - t_{\text{arr}}(m_i^{(j)})$, где $t_{\text{arr}}(m_i^{(j)})$ – момент поступления $m_i^{(j)}$ в интерфейсный блок передающего узла, $t_{\text{end}}(m_i^{(j)})$ – момент времени поступления $m_i^{(j)}$ в интерфейсный блок принимающего узла. Величина $R(m_i)$ максимально возможного времени доставки сообщений типа m_i (при любых допустимых сценариях поступления сообщений в коммуникационную систему) определяется, подобно величине времени отклика заданий:

$$R(m_i) = C(m_i) + B(m_i) + J(m_i) + \sum_{\text{prio}(m_i) < \text{prio}(m_k)} C(m_k) \left\lceil \frac{R(m_i) + J(m_k) - J(m_i)}{T(m_k)} \right\rceil. \quad (3)$$

Локальные и распределенные задачи. Формула (3) дает оценку максимальной продолжительности интервала времени между двумя событиями – завершением формирования сообщения прикладной задачей на передающем узле и готовностью коммуникационной системе предоставить переданное сообщение прикладной задаче на приемном узле. Оба эти события являются внутрисистемными событиями распределенного программного приложения. Но требования к функционированию СРВ состоят в корректной и своевременной реакции на внешние события, представляемые информационными посылками от контролируемого оборудования (рисунок 1).

Реакция СРВ (реакция программного приложения СРВ) выражается формированием информационных посылок направляемых внешнему оборудованию. В этом смысле СРВ относится к классу реагирующих систем. Формулы (1 – 2) ориентированы на такую обработку внешних событий, в которой задействован единственный узел системы. На этом узле выполняются следующие действия:

- регистрируется внешнее событие (информационная посылка со стороны контролируемого оборудования), требующее реакции со стороны программного приложения,
- активизируется и исполняется задача, реагирующая на это событие, причем в ходе своего исполнения задаче не требуется взаимодействие с другими узлами системы,
- перед своим завершением задача формирует информационную посылку, реакцию системы на обрабатываемое внешнее событие,
- интерфейсный блок узла, выполнившего задачу, посылает сформированную информационную посылку на контролируемое оборудование.

Подобные задачи являются локальными прикладными задачами программного приложения. Обрабатываемые локальными задачами внешние события не требуют привлечения других узлов системы. В этом случае максимальная длина интервала времени между регистрацией внешнего события и реакцией программной системы на это событие в виде информационной посылки на контролируемое оборудование (время отклика системы на внешнее событие) оценивается по формулам (1–2). В общем же случае, когда реакция на внешнее событие требует участия двух и более узлов, при оценке времени отклика на внешнее событие необходимо учитывать продолжительность исполнения компонент программного приложения, размещаемых в различных узлах системы, и продолжительность передачи сообщений, направляемых этими компонентами через коммуникационную подсистему. Для такой оценки требуется построение соответствующей вычислительной модели распределенного программного приложения.

Простейшая модель такого рода ориентирована на системы, в которых обработка каждого внешнего события состоит в исполнении цепочки Ψ_i фрагментов программного приложения, отвечающего следующим условиям:

- каждый фрагмент $s_{i,k}$ цепочки Ψ_i является задачей τ_x (последовательной программой, замкнутой по передачам управления), реализуемой j -м узлом распределенной системы,
- соседние фрагменты $s_{i,k}$ и $s_{i,k+1}$ цепочки Ψ_i принадлежат различным узлам системы,
- завершение фрагмента $s_{i,k}$ сопровождается передачей сообщения $s_{i,k} \rightarrow s_{i,k+1}$,
- завершение передачи сообщения $s_{i,k} \rightarrow s_{i,k+1}$ является системным событием, порождающим экземпляр той задачи, которая соответствует фрагменту $s_{i,k}$.

Вариации продолжительности исполнения фрагментов цепочки Ψ_i приводят к сдвигам моментов порождения задач $s_{i,k}$ и генерации сообщений $s_{i,k} \rightarrow s_{i,k+1}$, следующих за такими фрагментами. Подобные сдвиги влияют на значения максимально возможной продолжительности исполнения фрагментов менее приоритетных цепочек Ψ_i , ($i < j$) аналогично тому, как фактор дребезга задачи τ_i влияет на время отклика менее приоритетных задач τ_j в однопроцессорных системах. Назовем такое влияние фактором сдвига.

Фактор сдвига $S(s_{i,k})$ для задачи $s_{i,k}$ определяется выражением

$$S(s_{i,k}) = R(\dots, s_{i,k}) - R_{\min}(\dots, s_{i,k}),$$

где $R(\dots, s_{i,k})$ — максимальная продолжительность интервала исполнения фрагмента цепочки Ψ_i , предшествующего исполнению задачи $s_{i,k}$. Величина $R_{\min}(\dots, s_{i,k})$ — минимальная продолжительность интервала исполнения этого фрагмента цепочки Ψ_i .

Эффект сдвига следует учитывать и при оценке продолжительности передачи сообщений. Фактор сдвига $S(s_{i,k} \rightarrow s_{i,k+1})$ сообщений типа $s_{i,k} \rightarrow s_{i,k+1}$ определяется выражением

$$S(s_{i,k} \rightarrow s_{i,k+1}) = R(\dots, s_{i,k} \rightarrow) - R_{\min}(\dots, s_{i,k} \rightarrow),$$

где $R(\dots, s_{i,k} \rightarrow)$ — максимальная продолжительность исполнения фрагмента цепочки Ψ_i , предшествующего передаче сообщения $s_{i,k} \rightarrow s_{i,k+1}$;

$R_{\min}(\dots, s_{i,k} \rightarrow)$ — минимальная продолжительность исполнения этого фрагмента цепочки Ψ_i .

Время отклика $R(\Psi_i)$ всей цепочки задач Ψ_i равно сумме:

$$R(\Psi_j) = \sum_{1 \leq i \leq l_j} R(s_{j,i}) + \sum_{1 \leq i \leq l_j - 1} R(s_{j,i} \rightarrow s_{j,i+1}),$$

где $R(s_{j,i})$ — время отклика задачи $s_{j,i}$, $R(s_{j,i} \rightarrow s_{j,i+1})$ аналогичная характеристика сообщений типа $s_{i,k} \rightarrow s_{i,k+1}$.

Для цепочки Ψ_1 время отклика отдельной задачи $s_{1,i}$ и отдельного сообщения выражается равенствами

$$R(s_{1,i}) = C(s_{1,i}) + B(s_{1,i}); R(s_{1,i} \rightarrow s_{1,i+1}) = L(s_{1,i} \rightarrow s_{1,i+1}) + t_{\max_m}.$$

Здесь $C(s_{1,i})$ и $L(s_{1,i+1} \rightarrow s_{1,i+1})$ соответственно фактор веса для задачи $s_{1,i}$ и фактор сообщения $s_{1,i} \rightarrow s_{1,i+1}$ (объем вычислений в секундах, требуемых для выполнения задачи $s_{1,i}$ и длина сообщения $s_{1,i} \rightarrow s_{1,i+1}$ в секундах). Фактор блокирования $B(s_{1,i})$ задачи $s_{1,i}$ соответствует максимально возможной продолжительности ожидания задачей $s_{1,i}$ момента освобождения информационных ресурсов, контролируемых процессором P ($s_{1,i} \in P$). Фактор блокирования $t_{\max_m}$ любого сообщения $s_{i,k} \rightarrow s_{i,k+1}$, равен продолжительности передачи максимально длинного элементарного сообщения по каналу сети.

В случае низкоприоритетных цепочек Ψ_j , ($j \geq 2$) в выражениях для времени отклика задач и сообщений появляются дополнительные слагаемые — факторы приоритета задач $I(s_{j,i})$ и факторы приоритета сообщений $I(s_{j,i} \rightarrow s_{j,i+1})$:

$$R(s_{j,i}) = C(s_{j,i}) + B(s_{j,i}) + I(s_{j,i}),$$

$$R(s_{j,i} \rightarrow s_{j,i+1}) = L(s_{j,i} \rightarrow s_{j,i+1}) + B(s_{j,i} \rightarrow s_{j,i+1}) + I(s_{j,i} \rightarrow s_{j,i+1}).$$

Здесь фактор приоритета $I(s_{j,i})$ для задач отражает максимально возможную суммарную продолжительность интервалов времени, в течение которых задача $s_{j,i} \in P$ ожидает момента предоставления ей процессора P , занятого исполнением более приоритетных задач. Аналогично фактор $I(s_{1,i} \rightarrow s_{1,i+1})$ — максимальная суммарная продолжительность интервалов ожидания сообщением $s_{1,i} \rightarrow s_{1,i+1}$ освобождения коммуникационной подсистемы занятой передачей более приоритетных сообщений.

Минимальные значения $R_{\min}(s_{i,k})$ и $R_{\min}(s_{i,k} \rightarrow s_{i,k+1})$ продолжительности исполнения задач и передачи сообщений достигаются при отсутствии факторов блокирования и приоритета:

$$R_{\min}(s_{i,k}) = C(s_{i,k}), \quad R_{\min}(s_{i,k} \rightarrow s_{i,k+1}) = L(s_{i,k} \rightarrow s_{i,k+1}).$$

Фактор приоритета $I(s_{j,i})$ для задачи $s_{j,i}$ соответствует времени ожидания задачей $s_{j,i}$ момента освобождения требуемого ей процессора в рамках критического для $s_{j,i}$ сценария внешних событий. Критический сценарий неизвестен, не ясно, существует ли такой сценарий, при котором каждая из вытесняющих $s_{j,i}$ задач τ_x активизируется в рамках интервала существования задания типа $s_{j,i}$ максимально возможное для τ_x число раз. Поэтому в рамках общей вычислительной модели можно определить лишь оценку сверху $I^*(s_{j,i})$ для величины $I(s_{j,i})$.

$$I(s_{j,i}) \leq I^*(s_{j,i}) = \sum_{\text{prio}(\tau_x) > \text{prio}(s_{j,i})} C(\tau_x) \left[\frac{R^*(s_{j,i}) + S^*(\tau_x)}{T(\tau_x)} \right],$$

где суммирование ведется по всем более приоритетным, чем $s_{j,i}$, задачам $\tau_x \in P$. Период $T(\tau_x)$ каждой из этих задач τ_x равен периоду $T(\Psi)$ всей цепочки Ψ , в состав которой входит задача τ_x , но каждая из таких τ_x отличается своим значением сдвига $S(\tau_x)$. В правой части

выражения для $I^*(s_{j,i})$ приведены оценки сверху для времени отклика $R(s_{j,i})$ и фактора сдвига $S(s_{j,i})$ поскольку сами эти значения зависят от факторов приоритета, оцениваемых приближенно.

Оценка фактора приоритета для сообщений представляется выражением

$$I^*(s_{j,i} \rightarrow s_{j,i+1}) = \sum_{x < j} \sum_{1 < y < l_x - 1} L(s_{x,y} \rightarrow s_{x,y+1}) \left[\frac{R^*(s_{j,i} \rightarrow s_{j,i+1}) + S^*(s_{x,y} \rightarrow s_{x,y+1})}{T_x} \right].$$

Оценка времени отклика задач цепочки Ψ_j требует предварительного вычисления оценки $S^*(\tau_x)$ фактора сдвига для задач из всех более приоритетных цепочек. Аналогично, оценка времени отклика сообщений из цепочки Ψ_j требует предварительного вычисления оценки $S^*(s_{x,y} \rightarrow s_{x,y+1})$ фактора сдвига для всех сообщений из более приоритетных цепочек.

При вычислении оценок $S^*(s_{j,k} \rightarrow s_{j,k+1})$ сдвига сообщений учитывается фактор блокирования и оценка фактора приоритета $I^*(s_{j,i})$:

$$S^*(s_{j,k} \rightarrow s_{j,k+1}) = S^*(s_{j,k}) + B(s_{j,k}) + I^*(s_{j,k}).$$

Сдвиги корневых задач $s_{j,1}$ любой цепочки Ψ_j равны нулю. При вычислении оценок $S^*(s_{1,k})$ сдвига некорневых задач учитывается вклад $t_{\max_m}$ вариации продолжительности блокирования сообщений, принимаемых задачей $s_{1,k}$, и оценка фактора приоритета $I^*(s_{j,k-1} \rightarrow s_{j,k})$ возникающей в ходе передачи принимаемого задачей $s_{j,k}$ сообщения:

$$S^*(s_{j,k}) = S^*(s_{j,k-1} \rightarrow s_{j,k}) + t_{\max_m} + I^*(s_{j,k-1} \rightarrow s_{j,k}).$$

Для вычисления значений фактора сдвига сообщений $S^*(s_{j,k} \rightarrow s_{j,k+1})$ требуется учесть значения сдвига задач, входящих в состав более приоритетных (по отношению к Ψ_j) цепочек. К моменту вычисления $S^*(s_{j,k} \rightarrow s_{j,k+1})$ все необходимые оценки сдвигов для элементов более приоритетных цепочек будут уже вычислены, поскольку производные параметры модели определяются последовательно — сначала для Ψ_2 , затем для Ψ_3 и так далее. Аналогично при вычислениях значений фактора сдвига задач $S^*(s_{j,k})$ требуется учесть уже вычисленные значения сдвигов сообщений, генерируемых при исполнении более приоритетных (по отношению к Ψ_j) цепочек.

Закключение. В распределенных системах нарушение целостности локальных данных возможно при интерференции однотипных цепочек задач с пересекающимися интервалами существования. Для исключения такой интерференции программные приложения реального времени следует строить таким образом, чтобы время отклика задач не превосходило величины периода их активизации. Приведенные выше методы позволяют выполнить оценку времени отклика для цепочек задач, составляющих программное приложение для распределенной СРВ.

СПИСОК ЛИТЕРАТУРЫ

1. Никифоров В.В., Шкиртиль В.И. Защита целостности данных в программных приложениях реального времени. // Труды VI Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» (ИБРР-2009). СПб: СПОИСУ, 2010. С.152–156
2. Никифоров В.В., Павлов В.А. Операционные системы реального времени для встроенных программных комплексов. // Программные продукты и системы, №4, 1999.
3. Никифоров В.В., Павлов В.А. Динамическое разделение ресурсов задачами с состояниями ожидания. // Материалы всероссийской конференции «Теория и практика системной динамики» – Апатиты, 2004. С.129–139.
4. Никифоров В.В., Шкиртиль В.И. Оценка времени отклика задач в системах реального времени с многоядерными процессорами. // Известия ВУЗов, Приборостроение, №12, 2008. С.40–45.
5. Никифоров В.В., Скорлышев Д.Ю., Шкиртиль В.И. Моделирование защиты целостности данных в системах реального времени. // Материалы конференции «Информационная безопасность регионов России» (ИБРР-2009). СПб: СПОИСУ, 2009. С.69/.
6. Никифоров В.В., Шкиртиль В.И. Своевременность доставки пакетов сообщений в распределенных системах реального времени. // Информационно-измерительные и управляющие системы, №11, 2010/ С.58-65.
7. Никифоров В.В. Разработка программных средств для встроенных систем. // СПб.: СПбГЭТУ, 2000, 74с.
8. Введение в CAN 2.0B интерфейс. ООО Микро-Чип, Москва, 2001. www.microchip.ru.
9. Никифоров В.В., Шкиртиль В.И. Оценка времени доставки сообщений в распределенных системах реального времени. // Известия ВУЗов, Приборостроение, №7, 2010/ С.33–39.

Рыжков А.В., Молдовян А.А., Березин А.Н.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ШИФРЫ С ВЕРОЯТНОСТНЫМ КОДИРОВАНИЕМ СООБЩЕНИЙ ТОЧКАМИ ЭЛЛИПТИЧЕСКОЙ
КРИВОЙ**

Введение

Алгоритмы коммутативного шифрования (АКШ) применяются в ряде специальных криптографических протоколов. Для построения АКШ используется трудность задачи дискретного логарифмирования (ЗДЛ) в конечных полях [1-3], имеющей субэкспоненциальную сложность. При таком подходе каждое сообщение, кроме сообщения, представляющего нулевую битовую цепочку, интерпретируется ненулевым элементом поля. Однако для задания высокой стойкости АКШ требуется использовать поля, порядок которых выражается простым числом или степенью простого числа размером не менее 1024 бит, что существенно ограничивает производительность АКШ. При этом увеличение быстродействия АКШ путем выбора в качестве модуля простого числа p специального вида связано также и со следующим ограничением. В разложении числа $p-1$ будут содержаться делители сравнительно малого размера, которые определяют наличие «слабых» значений сообщения, зашифрование которых даст возможность потенциальному нарушителю вычислить часть секретного ключа. Кроме того, во многих случаях применений АКШ выполняется шифрование сообщений сравнительно малого размера, но в зашифрованном виде они имеют размер, равный размеру числа p .

Использование вычислений на эллиптической кривой (ЭК) с целью выполнения процедур шифрования представляет интерес в связи с тем, что при правильном выборе ЭК обеспечивается экспоненциальная стойкость [4,5], что позволяет существенно уменьшить размер чисел, над которыми выполняются операции умножения по модулю, за счет чего повышается производительность алгоритмов шифрования. При этом выбор простого модуля, имеющего специальный вид, позволяет уменьшить сложность вычислений без того, чтобы это влияло на появление «слабых» сообщений, а размер зашифрованного сообщения небольшой длины может быть равен 160–256 бит.

При шифровании обычно предполагается, что любое сообщение, размер которого не превосходит некоторое заданное значение, может быть корректно зашифровано и расшифровано, т.е. на входные значения АКШ не накладывается ограничений. При использовании ЭК для синтеза АКШ возможны следующие два подхода: 1) для шифрования выбираются сообщения, которые могут быть интерпретированы как точки используемой ЭК; 2) размер сообщений задается на h бит меньше, чем размер порядка конечного поля, над которым задана ЭК.

Первый подход может быть применен в протоколах, в которых пространство шифруемых сообщений ограничено (например, в протоколах честной игры в покер по телефону) и имеется возможность табличной кодировки шифруемых сообщений точками ЭК. Во втором варианте сообщение дополняется случайными битами (размещение которых заранее оговаривается) таким образом, что получаемые значения являются абсциссами точек ЭК. Задаваемые таким образом точки шифруются с помощью АКШ. Выбор в качестве используемой кривой идеальной ЭК, которая содержит простое число точек, полностью устраняет «слабые» сообщения.

В настоящей работе рассматривается второй подход к построению АКШ с использованием эллиптических кривых (ЭК), заданных над конечными полями, который является универсальным, т.е. не накладывает ограничений на шифруемые сообщения.

1. Вероятностное кодирование сообщений точками эллиптической кривой

Во втором подходе обеспечивается практическая возможность корректного преобразования любого сообщения. Входное сообщение интерпретируется как часть абсциссы точки ЭК, к которой справа (или слева) присоединяются h случайных битов. Полученное значение принимается за абсциссу и проверяется существование точки ЭК с данным значением абсциссы. Если такой точки на используемой ЭК не существует, присоединяются новые случайные h битов и проверка повторяется. Если такая точка M существует, то вычисляется ее ордината. Точка M шифруется путем умножения ее на число e , которое является ключом зашифрования. Полученная точка C может быть корректно расшифрована по формуле $M = dC$, где d – значение, обратное числу e по модулю, равному порядку ЭК. Стойкость к атакам на основе известного исходного сообщения определяется трудностью задачи дискретного логарифмирования на ЭК, которая состоит в нахождении значения d при известных значениях точек M и C . Указанная задача не может быть решена за обозримое время при соответствующем выборе ЭК и размере координат точек, равном 160 бит и более.

Сообщение извлекается из расшифрованной точки путем удаления из значения ее абсциссы правых h битов. Таким образом, второй подход состоит в вероятностном кодировании шифруемых

сообщений точками ЭК. Точка ЭК задается парой чисел – абсциссой x и ординатой y , однако ордината определяется значением абсциссы, т.е. при заданном значении x ордината задается уравнением ЭК, причем имеются два значения ординаты, отличающиеся знаком. Имеются две симметричные точки ЭК для каждого значения абсциссы. Чтобы устранить эту неопределенность при задании точки значением абсциссы можно к абсциссе присоединить дополнительный бит b и оговорить правило, пользуясь которым можно однозначно установить, какая из этих двух точек задается. Пусть ЭК задана над простым полем характеристики p и в ходе вычислений получена точка C с координатами (x_c, y_c) . Эту точку можно задать как $(x_c, 1)$, если $y_c > p - y_c$, или как $(x_c, 0)$, если $y_c < p - y_c$. Таким образом, зашифрованное сообщение, представляющее собой некоторую точку ЭК, имеет размер на $h+1$ бит больше размера исходного сообщения. Относительное увеличение размера зависит от выбираемого значения h и размера координат ЭК. Величина h выбирается из условия малой вероятности того, что сообщение со случайным значением не может быть закодировано точкой ЭК. Указанная вероятность равна 2^{-h} . Пусть допустима вероятность, не превышающая 0,00001. Тогда можно выбрать значение $h=15$ бит, при котором относительное увеличение размера закодированного сообщения не превышает 10% при размере абсциссы, равном $|x|=160$ бит, и уменьшается с ростом $|x|$.

Для построения АКШ с использованием вероятностного кодирования представляет интерес использование ЭК, порядок которых является простым числом (идеальных ЭК) или равен простому числу, умноженному на достаточно малое натуральное число. В этом случае можно пренебречь вероятностью получения шифруемых точек малого порядка, что могло бы позволить потенциальному нарушителю вычислить часть секретного ключа. В случае вероятностного кодирования сообщений точками ЭК можно устранить возможность шифрования точек, которые имеют сравнительно малое значение порядка, однако это требует выполнения специальных процедур для определения порядка точек, кодирующих сообщение. Применение данных процедур приведет к существенному снижению скорости шифрования, поэтому предпочтительным является использование идеальных ЭК.

2. Сравнение с алгоритмом шифрования Эль-Гамала

В предыдущем разделе рассмотрен АКШ, использующий вычисления на ЭК. Он может быть применен также и для решения стандартной задачи защиты передаваемых сообщений от несанкционированного чтения, которая обычно решается с использованием алгоритмов шифрования, не обладающих свойством коммутативности. В таком применении описанный АКШ используется как обычный симметричный шифр, а пара ключей d и e должна быть известной отправителю сообщения и получателю. Шифрование на ЭК может быть выполнено также и по алгоритму Эль-Гамала. Для таких применений представляет интерес сравнение АКШ с алгоритмом Эль-Гамала [6], реализованном с использованием вычислений на ЭК [5]. Пусть специфицирована ЭК простого порядка q и точка G , имеющая порядок q . Владельцу открытого ключа $Q = sG$, можно послать зашифрованное сообщение m воспользовавшись следующим алгоритмом:

1. Сгенерировать случайное число k и вычислить точку $R = kG$ (разовый открытый ключ отправителя).
2. Вычислить точку $Z = kQ = (x_z, y_z)$ (разовый общий секретный ключ).
3. Зашифровать сообщение m по формуле $t = x_z m \bmod q$.
4. Отправить криптограмму (t, R) получателю.

Чтобы сократить размер криптограммы точку R можно отправить в виде ее абсциссы с присоединенным значением бита b , по которому однозначно идентифицируется точка R . Это приводит к увеличению времени расшифрования криптограммы, поскольку для восстановления ординаты точки R потребуется выполнить операцию извлечения квадратного корня в поле, над которым задана ЭК, однако относительное снижение скорости расшифрования невелико (около 10%). Описанный алгоритм является вероятностным. Случайное значение, определяющее ход шифрования генерируется на первом шаге. При экономичной записи точки R размер криптограмм примерно в два раза превышает размер исходного сообщения. Для зашифрования (расшифрования) сообщения требуется выполнить в среднем $1,5|q|(|q| - \text{битовый размер значения } q)$ операций сложения точек ЭК, примерно столько же таких операций требуется выполнить и в случае описанного ранее АКШ.

Алгоритм Эль-Гамала по своему содержанию представляет собой гибридную криптосхему, в которой распределение ключей осуществляется с использованием схемы открытого согласования общего секретного ключа Диффи-Хеллмана, а симметричное шифрование – путем умножения

сообщения на разовый ключ шифрования x_z . Процедура расшифрования криптограммы (t, R) выполняется получателем следующим образом:

1. Вычислить разовый общий секретный ключ – точку $Z = sR = (x_z, y_z)$, где x_z – разовый ключ симметричного шифрования.

2. Вычислить обратное значение $w = x_z^{-1} \bmod q$.

3. Расшифровать шифртекст t : $m = tw \bmod q$.

Очевидно, что никто, кроме владельца открытого ключа Q не может расшифровать криптограмму и получить доступ к сообщению m . Однако послать зашифрованное может любой пользователь, в том числе и потенциальный нарушитель. Это означает, что при применении алгоритма Эль-Гамала аутентификацию источника сообщения, если это требуется, следует выполнять с использованием дополнительных механизмов, обеспечивающих проверку подлинности отправителя. При применении АКШ для передачи секретного сообщения по открытому каналу в соответствии с протоколом бесключевого шифрования [3] имеет место аналогичная ситуация – участники сеанса секретной связи должны удостовериться в подлинности друг друга, что делает такое применение АКШ непрактичным. При этом в последнем случае требуется выполнение двухсторонней аутентификации пользователей, тогда как в случае алгоритма открытого шифрования Эль-Гамала требуется односторонняя аутентификация, т.е. только проверка подлинности отправителя. Если описанный АКШ используется как симметричный шифр, когда отправитель и получатель владеют одинаковыми ключами, то тогда аутентификация отправителя выполняется одновременно с расшифрованием сообщения, если оно избыточно. Если исходное сообщение имеет случайное значение, то могут использоваться коды аутентификации сообщения – контрольные суммы от сообщения, которые вычисляются по секретному ключу и направляются вместе с зашифрованным сообщением получателю.

С целью обеспечения возможности аутентификации отправителя сообщения непосредственно в процессе выполнения расшифрования к исходному случайному сообщению может вноситься заранее специфицированная битовая строка. При размере этой битовой строки, равном 16 бит и более, обеспечивается достаточно малая вероятность принять ложное сообщение за подлинное. Для повышения производительности АКШ с использованием ЭК, заданных над полем $GF(p)$, могут использоваться простые числа вида $p = 2^k \pm \mu_g 2^g \pm \mu_h 2^h \pm 1$, где $0 < g < k$; $0 < h < g$; $\mu_g \in \{0,1\}$; $\mu_h \in \{0,1\}$. Использование простых чисел данного вида позволяет выполнить операцию умножения в поле $GF(p)$ без выполнения операции арифметического деления, которая является наиболее трудоемкой при выполнении умножения по модулю p , что позволяет существенно повысить скорость шифрования по сравнению со случаем использования простых чисел произвольного вида.

Заключение

Построение АКШ с использованием вычислений на ЭК обеспечивается механизмом вероятностного кодирования шифруемых сообщений точками ЭК. Такие АКШ обладают значительно более высокой производительностью по сравнению с другими известными коммутативными шифрами [1,7]. Выбирая для построения АКШ данного вида идеальные ЭК обеспечивается отсутствие слабых сообщений, поскольку все точки, которые кодируют исходные сообщения, имеют одно и то же значение простого порядка, равное числу точек на ЭК. Сообщение, имеющее значение нуль, зашифровывается также безопасно как и все остальные сообщения. Увеличение размера зашифрованного сообщения на 10% не накладывает каких-либо существенных ограничений для практического использования АКШ с вероятностным кодированием сообщений точками ЭК.

Работа выполнена в рамках ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009-2013 гг. (контракт № П635).

СПИСОК ЛИТЕРАТУРЫ

1. Hellman M.E., Pohlig S.C. Exponentiation Cryptographic Apparatus and Method // U.S. Patent # 4,424,414. 3 Jan. 1984.
2. Молдован Н.А. Теоретический минимум и алгоритмы цифровой подписи. – Санкт-Петербург, БХВ-Петербург, 2010. – 304 с.
3. Молдован Н.А., Молдован А.А. Введение в криптосистемы с открытым ключом. – Санкт-Петербург, БХВ-Петербург, 2005. – 286 с.
4. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. – М., КомКнига, 2006. – 320 с.
5. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. М., КомКнига, 2006. – 274 с.
6. Menezes A.J., Vanstone S.A. Handbook of Applied Cryptography. – CRC Press, 1996. – 750 p.
7. Молдовану П.А., Молдован Д.Н., Морозова Е.В., Пилькевич С.В. Повышение производительности процедур коммутативного шифрования // Вопросы защиты информации. 2009. №4. С.24–31.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Устинов И.А., Игумнов В.В.

Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Информационная безопасность (ИБ) - 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 ИБ и предъявляют особые требования к надежности функционирования информационных систем в соответствии с характером и важностью решаемых задач. Критические инфраструктуры (КИ) 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.

ИБ относится к числу важнейших характеристик КИ. Это относится как к ИБ в целом, так и к безопасности информации в частности. При этом ведущая роль в обеспечении ИБ принадлежит ключевой информационно-управляющей системе данной критической инфраструктуры (КСКИ).

Решение этой фундаментальной проблемы и ее контроль проходит на всех этапах жизненного цикла создания информационно-управляющих систем для КИ - от проектирования, изготовления, испытаний, эксплуатации и до утилизации. Меры, принимаемые для ее решения, должны быть сопоставимы с размером возможного ущерба от деструктивных воздействий на КИ.

Технические требования к КСКИ определяются классом решаемых ими задач и задаются соответствующими тактико-техническими заданиями (ТТЗ) Государственных Заказчиков. Отсюда определяются основные требования к алгоритмам функционирования системы, требования к выбору и применению электронной компонентной базы (ЭКБ), схемно-конструкторским решениям, программному обеспечению (ПО), системе защиты процессов и процедур обработки информации и защиты самих объектов системы, к защите каналов связи, подавлению побочных электромагнитных излучений, алгоритмам диагностики и контроля звеньев, технологии отработки и проведения всего комплекса испытаний с максимальным подтверждением заданных требований в условиях стендовой базы предприятия и т. д.

В ФГУП НПО «Импульс» сформирована особая отечественная научно-техническая школа в области создания больших информационных систем. Научные рекомендации этой школы определили технологию создания защищенных КСКИ. Полученные на этой технологии решения позволяют выполнить основные требования к проектируемым системам. Это – практически абсолютная надежность систем, сохранение работоспособности систем при частичных отказах (отказоустойчивость), гарантированная защита информации от различных воздействий, уникальные вероятностно-временные характеристики передачи данных, способность к развитию (открытость), высокие эксплуатационные характеристики систем. 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 Генерального Заказчика (МО РФ).

КСКИ в зависимости от уровня решаемых задач условно можно разделить на два основных класса – информационно-управляющие системы (ИУС) и командные системы управления (КСУ).

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 ИБ. Не последняя роль здесь принадлежит правильному выбору ЭКБ.

ИУС чаще всего построены в основном на применении импортных аппаратных, программных и технологических решений и, обеспечивают функционирование в мирное время и в начальный период ухудшения военно-политической обстановки. КСУ требуют высокого уровня технологической независимости и ИБ, 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 КСКИ – элементной базе, она должна быть сугубо отечественная и российского производства.

Применение импортной ЭКБ и импортного ПО не гарантирует необходимый уровень информационной защиты из-за возможного наличия в ней различных «закладок» (в ЭРИ), «троянских коней» (в ПО) и т. д. Наличие этих вредоносных вставок, приводит к блокированию выполнения системой основных функций, в случае перевода ее в режим применения, неприемлемый для эвентуального противника, и соответственно делает данную КСКИ беззащитной в конфликтных ситуациях.

Гарантированное противостояние угрозам и обеспечение требуемого уровня ИБ возможно надежно обеспечить применением доверительных отечественных программно-аппаратных платформ (ПАП) при создании систем, ее составных частей и комплексов средств автоматизации (КСА). Проблемам обеспечения кибер-безопасности в информационных системах и создания доверительных отечественных ПАП были посвящены в этом году два заседания НТС ВПК при правительстве РФ, что подчеркивает их важность и актуальность на современном этапе.

Свойство доверительности означает однозначное соответствие работы КСКИ 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 недеklarированных возможностей в конечный продукт.

Понятие доверительности сложилось в ФГУП НПО «Импульс» в процессе создания КСКИ на протяжении 50-летней напряженной инженерной деятельности объединения, юбилей которой мы будем отмечать в этом году 26 декабря. Доверительность не является новым свойством для систем разработки нашего объединения, так как они проектируются на отечественной радиационно-стойкой ЭКБ и на ПО собственной разработки, на базе доверительных операционных систем.

Необходимо отметить, что постоянно растущая сложность и объемы задач управления требует интенсивного развития отечественной ЭКБ, ее максимального быстродействия, максимальных объемов памяти, сверхмалых габаритов и энергопотребления. Однако не достаточно ограничиваться только вопросами создания отечественной ЭКБ, необходимо проводить работы и по совершенствованию технологий проектирования.

Необходимо подчеркнуть, что проведение определенных мероприятий по технической защите информации и реализация организационных мер также позволяют решать задачу повышения уровня ИБ. Так большое влияние на качество создаваемых систем имеет уровень развития стендовой базы настройки и отработки создаваемых КСА, который позволяет полностью решить все вопросы противодействия иностранным техническим разведкам (ИТР) и провести максимальную проверку всех заданных функций на систему в соответствии с ТТЗ Генерального Заказчика.

Наличие в составе научно-производственного объединения крупного опытного завода и стендового комплекса позволяет без задержек проводить изготовление и отработку новейших образцов создаваемой техники и запускать в серийное производство изделия по тщательно отработанной конструкторской документации, а в дальнейшем на этапе эксплуатации осуществлять авторское сопровождение созданных систем.

Важное значение для обеспечения необходимого уровня работы системы имеет качество контроля состояния звеньев систем и процессов функционирования. На всех этапах создания и эксплуатации изделий функционирует эффективная система контроля качества создаваемой продукции.

Сложнейшие изделия, выпускаемые ФГУП НПО «Импульс», невозможно создать в одиночку. Решающую роль здесь играют кооперация предприятий промышленности (соисполнители работ) и умение организовать с ними работу. ФГУП НПО «Импульс» накопило богатый опыт работы с обширной кооперацией по созданию КСКИ.

На всех жизненных этапах разработки, изготовления, эксплуатации создаваемых систем определяющая роль принадлежит квалифицированным кадрам и их технологической поддержке. Источником достижений объединения является его коллектив высококвалифицированных специалистов в области системотехники, схемотехники, телекоммуникаций, конструирования, микроэлектроники, программного обеспечения, защиты информации и других разделов информатики.

Понимая значимость создания защищенных КСКИ, опыт нашего объединения в вопросах создания таких систем «под ключ», в 2010 году на базе ФГУП НПО «Импульс» была создана секция №6 «Информационные технологии в критических инфраструктурах». Секция успешно работает уже второй год.

Александров А.М.

Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»

РАЗЛОЖЕНИЕ ИНТЕГРАЛЬНЫХ ТРЕБОВАНИЙ ПО ВЕРОЯТНОСТЯМ ЛОЖНЫХ СИГНАЛОВ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Рассматривается некоторая критическая инфраструктура (КИ), содержащая n объектов. Состояние объектов контролируется по совокупности параметров. Результаты этого контроля образуют случайный поток, который поступает для обработки в центр КИ. Поступившие в момент времени t сигналы, от i -го объекта могут нести как истинную информацию о некотором событии, которое произошло на объекте в момент времени t (вероятность этого $p_i(t)$), так и ложную информацию (вероятность этого $q_i(t)$) может не поступить никакой новой информации (вероятность этого $r_i(t)$).

Очевидно, $p_i(t) + q_i(t) + r_i(t) = 1$

Центр КИ обрабатывает поступающую информацию по соответствующему правилу.

Например, если для решения некоторой задачи требуется истинная информация от всех объектов, вероятность этого, есть:

$$\prod_{i=1}^n p_i(t)$$

Если хотя бы от одного объекта поступит ложная информация, то центр КИ выдаст ложное решение задачи. Интегральная вероятность ложного решения есть:

$$Q(n,t) = \prod_{i=1}^n [p_i(t) + q_i(t)] - \prod_{i=1}^n p_i(t). \quad (1)$$

Вероятность Q , определяется формулой (1) и является условной вероятностью, так как не учитывает вероятность распределения моментов времени t_i .

В дальнейшем будем рассматривать условную вероятность однородных объектов $p_i(t_i) = \dots$, $p_n(t_n) = p$, $q_i(t_i) = \dots$, $q_n(t_n) = q$. Поэтому из (1) получается:

$$Q(n) = (p+q)^n - p^n \quad (2)$$

Исследуем некоторые свойства функции $Q(n)$. В частности, при каких условиях:

$$Q(n+k) < Q(n), \quad k \geq 1 \quad (3)$$

Введем обозначение $\delta = q/p$.

Опуская промежуточные выкладки, получим, что неравенство (3) выполняется если:

$$q^k < \delta^k \frac{(1+\delta)^n - 1}{(1+\delta)^{n+k} - 1} \quad (4)$$

Для иллюстраций этих результатов построим таблицу значений вероятности $Q(n)$ для $q=0,1$ и различных значений n и p .

Таблица 1

Вероятность интегрального ложного сигнала

$n \backslash p$	1	2	3	4	5	6	7
0,3	0,1	0,050	0,037	—	—	—	—
0,4	0,1	0,090	0,061	—	—	—	—
0,5	0,1	0,110	0,089	0,057	—	—	—
0,6	0,1	0,130	0,127	0,111	0,090	—	—
0,7	0,1	0,150	0,169	0,170	0,160	0,141	0,117

Из таблицы непосредственно видно, что интегральная вероятность $Q(n)$ может принимать наибольшее значение по n . Это значение можно ориентировочно найти, если в формуле (2) считать n непрерывной величиной, а вероятность Q непрерывной функции:

$$Q(x) = (p+q)^x - p^x \quad (5)$$

Применив известные правила поиска максимума, и решив уравнение $Q'(x)=0$, найдем соотношение для получения искомого x :

$$\left(\frac{p+q}{q}\right)^x = \frac{\ln p}{\ln(p+q)} \quad (6)$$

Таблица 2

Значения x , n , при которых $Q=\max_1 [q=0,1]$

p	0,4	0,5	0,6	0,7	0,8
x	1,25	1,65	2,19	3,58	6,57
n	1	2	2÷3	3÷4	6

Некоторые выводы:

1. Значение интегральной вероятности ложного сигнала $Q(n)$ в общем случае не является монотонной функцией и может иметь максимум, зависящий от соотношения индивидуальных вероятностей истинных и ложных сигналов.

2. Грубой оценкой экстремальных значений ёмкости n критической инфраструктуры может служить решение дифференциального уравнения $Q'(x)$.

3. Изложенный способ разложения интегральной вероятности при обработке сигналов по логической схеме «И», может быть использован для других логических схем, например для схемы «ИЛИ» и др.

Антонов А.А., Ридигер В.К., Федотов А.А., Филиппов А.С.

**Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
ИСПОЛЬЗОВАНИЕ ВЫСОКОУРОВНЕВЫХ СРЕДСТВ ПРОЕКТИРОВАНИЯ ДЛЯ
РАЗРАБОТКИ СНК НА БАЗЕ БМК 5516БЦ1Т1-002 В КРИТИЧЕСКИХ СИСТЕМАХ**

Введение. В настоящее время в России активно развивается навигационная система ГЛОНАСС. Согласно программе модернизации системы ГЛОНАСС, действующей до 2020 года, на 2013-2014 годы намечен запуск усовершенствованного спутника КА «Глонасс-К2» для проведения летно-конструкторских испытаний. Одним из усовершенствований будет применение более точного хронометра. Задача разработки хронометра возложена на ОАО «РИРВ». Для повышения скорости и качества разработки ОАО «РИРВ» привлекло к разработке ЗАО «МК ИМКО» и каф. КСПТ ФТК СПбГПУ. Авторы статьи приняли участие в разработке системы на кристалле (СНК) «ТАИМ-ИМКО» — специализированной ИС на базе радиационно-стойкого БМК 5516БЦ1Т1-002 фирмы ОАО «Ангстрем».

1. Описание разрабатываемой СНК

1.1. Назначение и состав разрабатываемой системы

Разрабатываемая СНК является системой для бортового синхронизирующего устройства спутников ГЛОНАСС. Функции разрабатываемой СНК:

- Синтез частоты для квантового стандарта частоты на рубидиевой газовой ячейке — формирование частоты подмешивания;
- Формирование сетки частот и шкалы времени;
- Передача данных внешней телеметрии.

Под частотой подмешивания понимается частота f , избирательно поглощаемая рубидиевой газовой ячейкой 87Rb . Эта частота используется для подстройки кварцевого генератора (5 МГц). Точность выходной частоты при этом не ниже 10^{-11} [2].

Получаемая с кварцевого генератора частота поступает на вход сетки частот, формирующей набор служебных частот, а также частоту 1 Гц для шкалы времени, которая является источником точного времени.

Разрабатываемая ИС состоит из двух независимых блоков:

- Синтезатор синусоидального сигнала управляемой частоты;
- Блок БСУ.

Разработка синтезатор синусоидального сигнала управляемой частоты (далее генератор синуса) велась непосредственно авторами статьи. Разработку блока БСУ осуществлял специалист ОАО «РИРВ», а авторы статьи проводили его корректировку и тестирование. В связи с этим в данной статье вопросы разработки блока БСУ практически не затрагиваются.

1.2. Синтезатор синусоидального сигнала управляемой частоты

Синтез сигналов управляемой частоты имеет широкое применение в вычислительной технике. Под термином «синтезатор частоты» понимают электронное устройство, способное из опорной частоты получать на выходе требуемую частоту или набор частот, согласно управляющим сигналам [6]. Наиболее простым и популярным методом синтеза сигналов на данный момент является прямой цифровой синтез. Структурная схема синтезатора приведена на рис. 1.

На рис. 1 приведена типовая структура DDS-синтезатора. Частота формируемого сигнала определяется входом аккумулятора фазы. Аккумулятор фазы — это накапливающий сумматор, формирующий код аргумента x функции $\sin(x)$. Аргумент подается на адресный вход ПЗУ, содержащей значения функции, соответствующие подаваемому адресу.

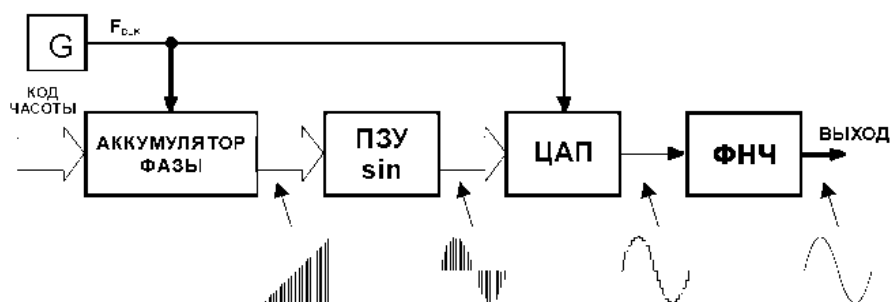


Рис. 1. Структурная схема синтезатора сигнала методом DDS

Цифро-аналоговый преобразователь (ЦАП) преобразует цифровое значение синуса в аналоговый сигнал, а фильтр нижних частот (ФНЧ) делает выходной сигнал гладким.

Наиболее популярна реализация функции $\sin(x)$ на ПЗУ, однако также возможна реализация в виде логической функции (ЛФ). Выходная частота синтезатора вычисляется по формуле 1, где f_{in} – опорная частота, D – код частоты, N – разрядность аккумулятора фазы.

$$f_{out} = \frac{f_{in} \cdot D}{2^N} \quad (1)$$

К разрабатываемому генератору синуса предъявлены следующие основные требования:

- 1) Максимальная опорная тактовая частота не ниже 40 МГц;
- 2) Точность выходной частоты не ниже 10^{-9} ;
- 3) Для обеспечения заданной точности, разрядность аккумулятора фазы должна составлять 40 разрядов.
- 4) Генератор синуса должен осуществлять переключение между двумя выходными частотами с одной из заданных частот модуляции, а также формировать частоты модуляции и другие служебные частоты на выходе;
- 5) Загрузка кода частоты должна осуществляться как последовательным, так и параллельным кодом.

Анализ и выполнение этих и других требований рассмотрены в п.п. 2.2.

1.3. Этапы разработки. Элементная база

В связи с высокой ценой ошибки при проектировании БМК 5516БЦ1Т1 принято решение разделить проектирование на два этапа:

- 1) проектирование на нестойком аналоге 1592ХМ1Т-021 [3],
- 2) переход к БМК 5516БЦ1Т1-002 [4].

Оба БМК разработаны компанией ОАО «Ангстрем». В первый этап также входит прототипирование разрабатываемой СнК на ПЛИС, что позволяет исключить функциональные ошибки при проектировании. Прототипирование на ПЛИС, однако, не позволяет осуществить проверку временных характеристик схемы. Это объясняет необходимость применения БМК 1592ХМ1Т, временные характеристики которого совпадают с временными характеристиками БМК 5516БЦ1Т1. Обе БИС БМК 100000 четырех-транзисторных логических ячеек; максимальная частота тактирования – 50 МГц; напряжение питания: 4,5..5,5 В. БМК 5516БЦ1Т1 выполнена по технологии кремний на сапфире (КНС), что обеспечивает ее высокую стойкость к внешним воздействующим факторам (ВВФ) по ГОСТ РВ20.39.414.2-98.

Показатели 1592ХМ1Т по стойкости к ядерным воздействиям существенно ниже, чем у 5516БЦ1Т1, особенно по фактору 7.И8, который является наиболее критичным в рамках данной разработки: сбои в схеме формирования точного времени недопустимы. Это стало причиной выбора 5516БЦ1Т1 в качестве целевой элементной базы. 5516БЦ1Т1 является полным функционально-библиотечным аналогом 1592ХМ1Т, это обеспечит возможность быстрого и безошибочного портирования СнК «ТАЙМ-ИМКО» на целевой кристалл, после отработки на относительно дешевом БМК 1592ХМ1Т.

2. Разработка СнК «ТАЙМ-ИМКО». Основные этапы

2.1. Разработка маршрута проектирования. Согласование с ОАО «Ангстрем»

Основной идеей при выполнении данной работы было внедрение нового маршрута проектирования, позволяющего ускорить процесс проектирования и снизить риск ошибок, привносимых в процессе проектирования. При этом основным требованием является возможность поддержки разработанного маршрута фирмой-изготовителем БМК, т.е. ОАО «Ангстрем».

Разработка БМК 1592ХМ1Т (также и 5516БЦ1Т1) поддержана средой разработки фирмы Cadence в отличие от других, более старых разработок ОАО «Ангстрем». Это существенно упрощает задачу разработчика, поскольку в этом случае нет необходимости в схемном вводе проекта. Проект можно вводить на языках VHDL/Verilog HDL. Кроме того ангстремовская среда разработки

поддерживает наиболее распространенные форматы временных диаграмм, что упрощает процесс моделирования и формирования тестов. В данном маршруте проектирования не применяется устаревший САПР «Невод». В результате разработан маршрут проектирования для генератора синуса (рис. 2).

Основной особенностью разработанных маршрутов проектирования является проведение верификации на всех этапах разработки, позволяющей не допустить привнесения ошибок на каком-либо этапе.

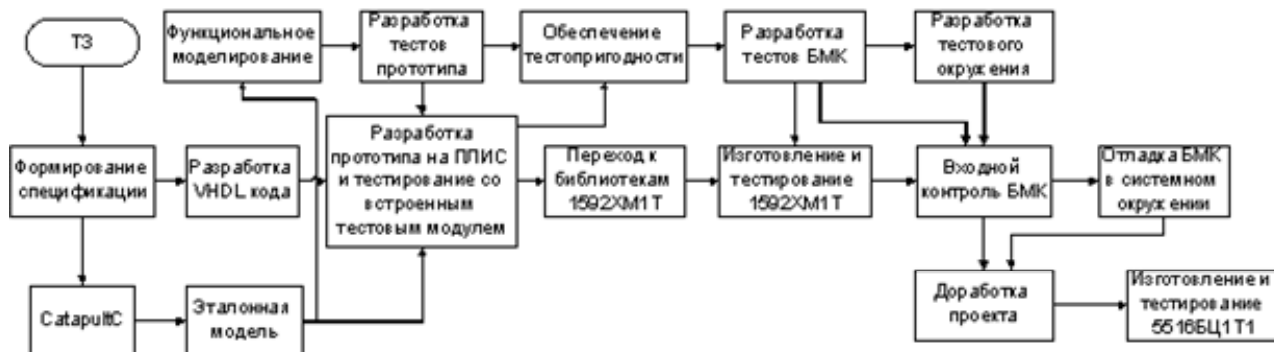


Рис. 2. Разработанный маршрут проектирования генератора синуса

Первым этапом после получения технического задания (ТЗ) на генератор синуса от ОАО «РИРВ» является формирование спецификации. Спецификацию на генератор синуса удобно задавать на языке программирования высокого уровня (ЯВУ), например С, с использованием стандартных библиотек. Такую спецификацию можно довольно легко перевести в синтезируемое HDL-описание с использованием высокоуровневых средств проектирования и верификации класса SystemC. В работе применялся язык CatapultC, в результате чего получено синтезируемое описание, соответствующее спецификации по своей функциональности, однако непригодное для реализации в целевой элементной базе. Полученное описание используется как эталонная модель (ЭМ) при тестировании (см. рис 2). Подробнее об ЭМ на CatapultC в п.2.3.

2.2. Разработка VHDL-описания генератора синуса. Прототипирование на ПЛИС

Разработка велась в САПР Altera Quartus II 9.0. ОАО «Ангстрем» имеет положительный опыт изготовления БМК из проектов, заданных в среде Quartus II. Кроме того прототипирование велось на ПЛИС EP2K8F256 и EP3K5E144, фирмы Altera, для которых Quartus II является основной средой разработки. В результате: описание для БМК без проблем «легло» в ПЛИС. Результаты тестирования прототипа совпали с результатами моделирования и результатами тестирования ЭМ на CatapultC. В дальнейшем прототип генератора синуса на ПЛИС будет использоваться в качестве эталонной модели при тестировании БМК.

Структурная схема генератора синуса (блок Sin_Generator) представлена на рис. 3.

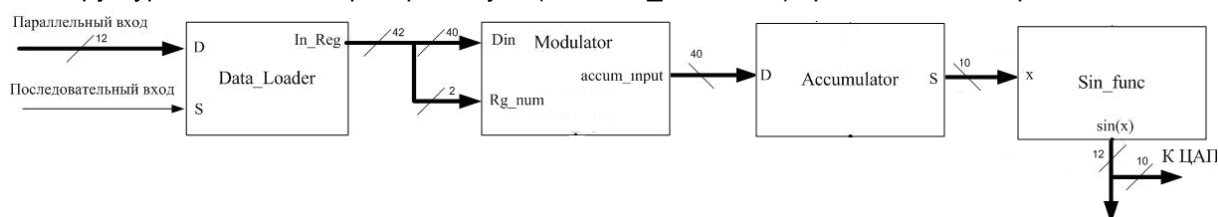


Рис. 3. Структурная схема блока Sin_Generator

Блок Data_Loader осуществляет загрузку кода частоты как в последовательном режиме (42 разряда) так и в параллельном (12 разрядов). Полученный код частоты попадает в блок модуляции (Modulator), где записывается в один из двух регистров, выходы которых коммутируются с частотой модуляции (15, 30 или 78 Гц) на вход 40-разрядного аккумулятора фазы (Accumulator). Аккумулятор фазы – накапливающий сумматор, формирующий аргумент функции Sin(x), который поступает на устройство Sin_func, реализующее функцию Sin(x) с помощью ЛФ. На выходе этого блока формируется 12-разрядный цифровой код синуса, который далее поступает на ЦАП (10 старших разрядов). Большая разрядность аккумулятора фазы, а также возможность модуляции, обеспечивают высокую точность выходной частоты.

Наиболее сложным блоком генератора синуса является аккумулятор фазы — это 40-разрядный накапливающий сумматор, работающий на частоте 40 МГц. Для обеспечения заданной производительности был разработан блок Accumulator со специфической архитектурой. Блок Accumulator представляет собой 10-ступенчатый конвейер, разбивающий суммирование 40-разрядных слов на суммирование 10 групп по 4 разряда. Он состоит из простейших 4-разрядных

сумматоров и цепочек конвейеризирующих регистров. Суммирование 4-разрядных групп осуществляется с последовательным переносом, между группами реализован управляющий перенос. Суммирование каждой 4-разрядной группы дублируется, сумма вычисляется как для единичного переноса в младший разряд группы, так и для нулевого. Сигнал переноса, полученный при суммировании в предыдущей группе разрядов, является управляющим для мультиплексора, коммутирующего обе суммы на выход. Такой подход позволяет значительно ускорить процесс суммирования. Время срабатывания одноразрядного сумматора из библиотеки AGA12C 1592XMx составляет ~2 нс [5]. Это означает, что время срабатывания четырехразрядного сумматора составит не менее 8 нс, но и скорее всего не более 10 нс. При работе на частоте 40 МГц ($T = 25$ нс) такого времени срабатывания достаточно для корректной работы устройства. В связи с применением 10-ступенчатого конвейера, для обеспечения заданной тактовой частоты 40 МГц, задержка появления первого слова на выходе блока Accumulator составляет 10 тактов.

Функция синуса реализована в виде ЛФ в связи с тем, что встроенное в кристалл ПЗУ ресурсоемко и не отвечает требованиям быстродействия, а применение внешнего ПЗУ недопустимо.

2.3. Применение языка CatapultC для верификации генератора синуса

Спецификация проектируемой системы является первичным и главным источником информации для разработчика конечных модулей системы. Современный подход предполагает задание подобных спецификаций, в том числе и на ЯВУ класса C и C++, что позволяет реализовывать систему программно, а с привлечением современных компиляторов и аппаратно [1]. Одним из путей оптимизации процесса перехода от высокоуровневой спецификации на ЯВУ к аппаратной реализации на заданной элементной базе является использование C-подобных языков для проектирования аппаратных средств. Такие языки являются подмножествами SystemC — языка проектирования и верификации моделей системного уровня. Используемый в данной работе язык CatapultC [7,8,9] фирмы Mentor Graphics является одним из самых популярных SystemC-подобных языков, так как поддержан необходимыми инструментальными средствами (среда разработки CatapultC Synthesis).

CatapultC имеет одно существенное преимущество по сравнению с другими SystemC-подобными языками проектирования цифровых устройств: код на CatapultC, описывающий проектируемое устройство не отличается значительным образом от стандартного C-кода, используемого в чисто программных реализациях алгоритма, с помощью которого ведется проектирование устройства [7,8,9].

Тем не менее, есть один существенный фактор, затормаживающий бурное развитие SystemC-подобных языков: достаточно сложные устройства, заданные на CatapultC, скорее всего, будут уступать по быстродействию и аппаратным затратам аналогичным устройствам заданным на VHDL или Verilog HDL. Синтезируемое из кода на CatapultC RTL-описание очень сложно для человеческого восприятия, поскольку оно синтезировано в автоматическом режиме. В связи с этим ручная корректировка получаемого RTL-описания с целью оптимизации крайне затруднена и практически невозможна. Компания Mentor Graphics – разработчик языка CatapultC и среды CatapultC Synthesis не предполагает ручную доводку описания на уровне RTL.

Указанный выше фактор ограничивает использование SystemC-подобных языков при синтезе цифровых устройств, в которых необходима высокая производительность или низкие аппаратные затраты. По той же причине ограничено использование SystemC-подобных языков при проектировании высоконадежных цифровых устройств. Особенно актуальна эта проблема для отечественной электронной промышленности. Невысокая логическая емкость отечественных ИС по сравнению западными аналогами делает необходимой значительную минимизацию аппаратных затрат, что не позволяет на данный момент применять языки класса SystemC в маршруте проектирования. Другой причиной, не позволяющей применять языки класса SystemC в маршруте проектирования отечественных цифровых устройств, являются высокие требования к их надежности. Кроме того, изменение маршрута проектирования на уровне промышленности всей страны — процесс сложный и длительный, требующий большой технической и административной работы.

Несмотря на ограниченность применения языков класса SystemC непосредственно для синтеза цифровых устройств, есть возможность их альтернативного применения в маршруте проектирования любых цифровых устройств. Так как описание на таких языках полностью соответствует функционально-логической спецификации на устройство, их можно использовать для формирования ЭМ [1], используемой при тестировании разрабатываемого устройства. В данной работе реализована ЭМ генератора синуса на языке CatapultC. Она была успешно синтезирована и использована для тестирования прототипа на ПЛИС. После того, как прототип на ПЛИС прошел тест, он был взят за эталон и использовался для тестирования БМК.

2.4. Доработка проекта под требования ОАО «Ангстрем». Изготовление БМК 1592XM1T-021

После того, как проект был передан в ОАО «Ангстрем» и там был проведен его анализ, потребовались некоторые доработки проекта:

1. Комбинаторная цепочка, синтезированная разработчиками ОАО «Ангстрем» по выданному им исходному описанию на VHDL, реализующая функцию $\sin(x)$, оказалась слишком длинной и не давала гарантированного срабатывания на частоте 40 МГц. В связи с этим пришлось конвейеризировать функцию синуса.

2. Потребовалась доработка тестов в соответствии с требованиями системы тестирования ОАО «Ангстрем»:

- 1) формирование единого теста для обеих частей проекта,
- 2) увязывание тактовых частот тестирования,
- 3) расширение тестов для обеспечения заданного тестового покрытия БМК.

3. Согласование разводки выводов в корпусе 4236.208

После проведения доработок были изготовлены опытные образцы БМК 1592XM1T-021. Сформированные тесты обеспечили тестовое покрытие 96%.

3. Исследование разработанной СнК

3.1. *Формирование окружения для тестирования и отладки. Тестирование в системном окружении*

Генератор синуса и БСУ — логически независимые блоки, поэтому тестируются отдельно. Формированием системного окружения для тестирования блока БСУ занимается ОАО «РИРВ». Для генератора синуса на базе ПЛИС EP1S10F780 разработан тестовый стенд, формирующий управляющие сигналы и код частоты. Кроме того в ПЛИС расположен прототип разработанный и верифицированный ранее. Результаты работы БМК и прототипа можно наблюдать в реальном времени в программном логическом анализаторе SignalTap II на рис. 4.

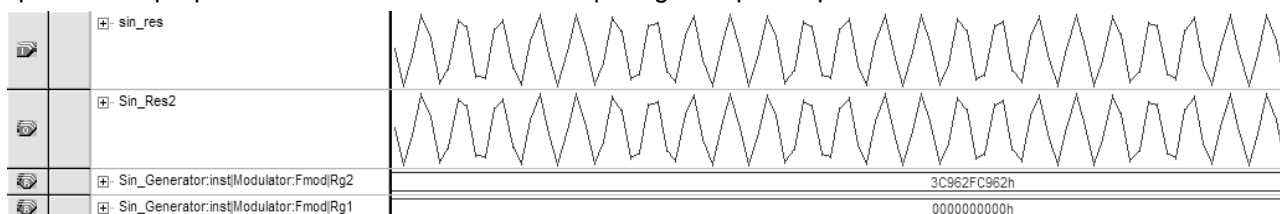


Рис.4. Временная диаграмма работы генератора синуса в SignalTap II

На рис. 4 верхний сигнал соответствует цифровому выходу синуса БМК, а нижний — цифровому выходу прототипа на ПЛИС. Как видно из рисунка, они полностью совпадают. Форма сигнала не гладкая потому, что схема работает на предельных выходных частотах: синус строится по 3-4 отсчетам. Это наиболее тяжелый для схемы режим, который нуждался в проверке в первую очередь. Частота близка к требуемой. Более точно определить ее соответствие можно будет с использованием высокоточного частотомера и спектроанализатора.

Применение такого метода тестирования и отладки позволило быстро убедиться в работоспособности БМК, а также выявить ошибки в печатной плате, на которую был установлен тестируемый БМК.

Кроме того была разработана и изготовлена специализированная плата «Монитор», также реализованная на базе ПЛИС (EP3C5E144). Она может выступать в роли монитора сигналов, проходящих между БМК и его окружением, а также в роли самого БМК для проверки корректности работы системного окружения.

3.2. Анализ результатов тестирования. Доработка проекта. Переход к БМК 5516БЦ1Т1-002

Результаты тестирования БМК 1592XM1T подтвердили полное соответствие спецификации, однако они обнаружили ошибки, допущенные при формировании ТЗ, а также при переходе от ТЗ к спецификации, т.е. ошибки, допущенные на тех этапах проектирования, которые невозможно автоматизировать. Это еще раз подтверждает необходимость автоматизации всех, этапов проектирования, которые возможно автоматизировать с целью минимизации воздействия человеческого фактора, а также демонстрирует работоспособность предложенного маршрута проектирования.

По результатам тестирования было сформировано ТЗ на доработку. Доработки не затрагивают ядра генератора синуса, а касаются лишь вопросов загрузки кода частоты и выдачи служебных частот. На данный момент доработки выполнены, доработанный проект передан в ОАО «Ангстрем» для реализации на БМК 5516БЦ1Т1-002.

Закключение. В данной работе успешно применен новый для отечественных БМК маршрут проектирования, отличающийся высокой скоростью реализации и защищенностью от ошибок. Его основная особенность — осуществление верификации на всех этапах проектирования, а также максимальная автоматизация всех этапов проектирования с целью исключения человеческого фактора. Он полностью адаптирован для современного отечественного производства. При успешной реализации БМК 5516БЦ1Т1-002 разработанный маршрут проектирования может быть рекомендован как базовый при проектировании относительно сложных СнК на отечественной элементной базе. Так

как БМК 5516БЦ1Т1 является новой разработкой и находится в стадии ОКР, работоспособный и эффективный маршрут проектирования под эту микросхему будет нести в себе научную новизну и практическую ценность.

СПИСОК ЛИТЕРАТУРЫ

1. Антонов А. А. Методика построения встраиваемых средств тестирования высоконадежных цифровых устройств с использованием высокоуровневых спецификаций // Экстремальная робототехника. Труды XXI Международной научно-технической конференции. СПб., 2010. С. 448–458.
2. Григорьянц В. В., Жаботинский М. Е., Золин В. Ф., Квантовые стандарты частоты, М., 1968.
3. Микросхемы интегральные на основе БМК 1592ХМ1Т. Технические условия. АЕЯР.431250.263ТУ, 2003.
4. Микросхемы интегральные на основе БМК 5516БЦ1Т, 5516БЦ1Т1. Технические условия. АЕЯР.431260.385ТУ, 2009.
5. Семейство матричных кристаллов 1592ХМх. Библиотека стандартных элементов АГА12С, ОАО «Ангстрем», 2004.
6. Ридико Л. DDS: Прямой цифровой синтез частоты // Компоненты и технологии. №7. 2001. С. 50-54.
7. Catapult C Synthesis. Automated Verification Extension. User's and Reference Manual: Release 2004b. Mentor Graphics Corporation. 2004. http://www.megratec.ru/data/files_db/7338/Catapult_Verification.pdf.
8. Designing High-Performance DSP Hardware Using Catapult C Synthesis and the Altera Accelerated Libraries. Altera Corporation; Mentor Graphics Corporation. 2007. <http://www.altera.com/literature/wp/wp-01039.pdf>.
9. Takach A. An Overview and Demonstration of Catapult C. [Видеоматериал]. <http://www.mentor.com/player/2007/catapultc/>. Проверено 14.06.2010.

Великовская С.А.

Россия, Москва, Московский государственный университет технологий

и управления им. К.Г. Разумовского,

Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»

ГОРОДСКОЙ ИНТЕРНЕТ ДНЕВНИК

Современный мир постоянно меняется, меняется и отношение к школьному образованию. Сегодня говорят о реальной необходимости перехода школы к Электронному журналу, Электронному дневнику школьника.

Электронный журнал это периодическое рецензируемое издание, электронный аналог печатного журнала, доступный для просмотра на компьютере. Распространяется через Интернет или на любых носителях информации (магнитных, оптических).

Электронный дневник это система, позволяющая перевести большую часть оперативной информации, используемой в образовательном процессе, в электронный вид с последующей доставкой до участников системы (родители, обучающиеся, педагогические работники) посредством сети Интернет и на различные устройства (стационарный компьютер, мобильный телефон, интернет-планшет и т.п.).

Использование электронного журнала и электронного дневника это не дань моде. Однако это требует нового образа мышления, ломки привычных, выработанных десятилетиями навыков работы. Связано это с тем, что Электронный журнал и Электронный дневник – это не просто копия бумажного журнала и дневника, это уже информационная среда, в которую включены учителя, администрация, обучающиеся, родители учеников. Введение Электронного журнала и Электронного дневника открывает переход классической школы в Электронную школу.

Вовлечение ребенка, педагогов и родителей в образовательный процесс через новые информационные технологии направлено на повышение качества образования, обеспечение соответствия его содержания актуальным потребностям развития российского общества.

В муниципальной системе образования городов России Электронный Журнал и Электронный Дневник чаще всего реализованы в форме программного комплекса АСИОУ+ГИД (автоматизированная система информационного обеспечения управления + городской интернет-дневник).

Возможности программного комплекса АСИОУ+ГИД:

- для родителей: просмотр расписания, тем уроков, домашних заданий, объявлений, новостей любой другой информации, выложенной для всеобщего ознакомления; просмотр отметок своих детей с указанием типа произведенного контроля знаний и комментариями учителя; общение с учителем, администрацией, другими родителями, обучающимися;

- для обучающихся: просмотр расписания, тем уроков, домашних заданий, объявлений, новостей и любой другой информации, выложенной для всеобщего ознакомления; просмотр своих отметок с указанием типа произведенного контроля знаний и комментариями учителя; размещение в «Личном кабинете» своих материалов; общение с учителем, директором, другими обучающимися;

- для учителей: ввод отметок с указанием типа произведенного контроля знаний и по желанию, снабжение их комментариями; размещение домашних заданий и тем уроков просмотр расписания, тем уроков, домашних заданий, объявлений, новостей и любой другой информации, выложенной для всеобщего ознакомления размещение в «Личном кабинете» своих материалов; общение с учениками, их родителями, администрацией школы, другими учителями; тестирование обучающихся по различным тестам с автоматической обработкой закрытых вопросов;

- для администрации: просмотр всей информации по школе, за исключением личной переписки статистика активности пользователей интернет-дневника по школе; просмотр динамики

успеваемости обучающихся по классам/ по школе; получение результатов обработки успеваемости в табличных и графических формах; возможность массовой рассылки сообщений по всем участникам зарегистрированных по школе в Интернет-дневнике; общение с учениками, их родителями, учителями; проведение опросов обучающихся, родителей, педагогов по различным основаниям с автоматической обработкой закрытых вопросов.

Данный комплекс позволяет не только формировать банк данных обучающихся и учителей, их достижений и всевозможных показателей степени обученности и качества знаний, но и проводить аналитическую обработку информации. Программный комплекс позволяет осуществлять выборку данных, как по конкретному ребенку, так и по их различным объединениям (классам, группам) и тем самым оперативно получать полную и достоверную информацию о состоянии и динамике образовательного процесса.

Система позволяет автоматически рассчитывать и использовать обобщенные показатели успеваемости, степени обученности, качество знаний, получать статистику отметок (по классам, параллелям, ученикам, предметам, преподавателям, отчетным периодам) для формирования таблиц и диаграмм.

Такой интегрированный банк данных позволяет решать задачи оценки качества образования, осуществлять мониторинг образовательной деятельности, проводить объективный анализ состояния образовательного процесса в школе, получать достоверную информацию о полученном уровне образования и, что самое главное, о результатах учебной деятельности каждого участника образовательного процесса.

Проблема не в том, в каком виде эта информация представлена: в бумажном или электронном, а в том, каким образом она рассчитывается и сколько времени тратит администратор на расчеты. При использовании АСИОУ все вычислительные операции автоматизированы и возможность ошибок практически исключена.

Для того чтобы внедрить Региональный интернет – дневник существует алгоритм:

Электронный журнал – это новая система учета успеваемости для школ и других образовательных учреждений. Это прекрасный инструмент для администрации и учителей, который облегчает их каждодневную бумажную рутину, а также удобный помощник для родителей, чтобы контролировать успехи своего ребенка в учебе и быть на связи со школой.

Главная задача, решаемая Электронным классным журналом, – это своевременное информирование родителей по вопросам успеваемости и посещаемости их детей.

Таким образом, использование Электронного журнала классным руководителем ориентировано на решение одной из проблем школы – информативность.

В планах развития программного комплекса АСИОУ+ГИД — создание общего информационного поля образовательных учреждений с участием органов управления образованием, методических центров и других уполномоченных организаций. Специалисты самых разных уровней смогут получать сводную отчетность, анализировать статистику и более эффективно управлять качеством образования.

Конечно, существуют проблемы введения Электронного журнала в школе. Учителю-предметнику приходится выполнять двойную работу, заполняя бумажный и электронный журналы. Некоторые учителя пока ещё настороженно относятся к нововведению, многие боятся дополнительных трудностей. Но те из учителей, кто овладел компьютерными навыками, уже понимают, что есть масса возможностей сэкономить время на бумажной работе, ведь многие отчеты здесь генерируются автоматически.

В настоящее время техническое оснащение кабинетов недостаточно для масштабной планомерной работы. Но в школах создаются компьютерные классы, где подключен Интернет, постепенно возможности расширяются. Не будет ли поздно начинать осваивать Электронные журналы, когда система заработает в полную силу?

Не вызывает сомнения, что вскоре Электронный журнал придет в каждую школу. И это неудивительно. Помимо курса на модернизацию образования (в том числе и в отношении использования информационных технологий в школе), озвученного президентом, есть ряд неоспоримых преимуществ Электронного журнала перед своим бумажным прототипом.

Доступ к данным системы регулируется согласно полномочиям пользователей. Информация предоставляется администрации, учителям, родителям и ученикам в строгом соответствии с их правами.

Информация, поступающая в Электронный журнал, передается в Электронный дневник на сайт Регионального Интернет Дневника (РИД). Доступ к данным системы регулируется согласно полномочиям пользователей. Информация предоставляется администрации, учителям, родителям и ученикам в строгом соответствии с их правами.

Всегда актуальная информация об изменениях расписания, заменах, любых значимых событиях в школе доступна всем пользователям. Вместе со скоростью, с которой информация становится доступна, здесь заключено еще одно заметное преимущество для администрации школы: при работе со многими журналами больше не требуется выстраивать порядок работы с разными

классами, так как всегда наглядно видно, в какой части журналы уже заполнены, а кроме этого, можно контролировать работу учителей.

Таким образом, Электронный журнал обеспечивает открытость информационного пространства, стимулирование новых отношений между всеми участниками учебно-воспитательного процесса.

Электронный дневник школьника формируется автоматически на сайте «Региональный Интернет Дневник»: выгрузка данных из АСИОУ в РИД происходит под административным паролем и не требует дополнительного заполнения Электронного дневника ни классными руководителями, ни учителями – предметниками.

Электронный дневник представляет собой систему для взаимодействия школьников, их родителей, учителей и администрации школы посредством Интернета. С помощью Электронных дневников родители отслеживают успеваемость ребенка: расписание занятий, домашнее задание, оценки, посещение уроков. Школьники всегда имеют под рукой расписание и домашнее задание, а также возможность посмотреть статистику и рейтинги своих оценок по неделям, месяцам или четвертям.

Электронный дневник дисциплинирует обучающихся: уменьшаются пропуски по неуважительным причинам, ученики, которые отсутствовали по болезни, могут без проблем узнать домашнее задание. Учителя получили удобный и быстрый способ общения с родителями.

Чем же может привлечь Электронный дневник родителей:

1. Электронный дневник – это открытая электронная версия школьного журнала с явными преимуществами: в отличие от его бумажного аналога доступен в любой момент времени и предоставляет больше информации в наглядной и понятной форме: выписки всех оценок, точные данные о посещаемости уроков, возможность цветового кодирования информации.

2. Дневник ребенка является для них доступным через сеть Интернет в любое удобное для них время: дома или на работе, с компьютера, ноутбука, сотового телефона.

3. Электронный дневник помогает родителям проверять ребенка – отговорки вроде того, что дневники сданы на проверку, теперь не пройдут.

4. Из вкладки «Сообщения» родители имеют возможность прочитать запись в Электронном дневнике обучающегося, которую может оставить классный руководитель.

5. Расписавшись за одну неделю в дневнике, родители, как правило, не возвращаются к предыдущей, а в случае с Электронным дневником все оценки с начала четверти никуда не пропадают, а только ведется последующее наполнение, все пропуски отмечены, объявления сделаны. Таким образом, и родители, и ученики могут следить за накопляемостью оценок.

6. Информация в Электронном дневнике защищена от взлома. Родителям и обучающимся, желающим воспользоваться данным сервисом, классными руководителями выдается уникальные логин и пароль, который не подлежит разглашению. Благодаря паролю родители имеют доступ только к собственным данным, оценки других детей для них недоступны.

Таким образом, внедрение Электронных дневников позволяет школьникам стать более ответственными и открытыми перед родителями. Родители могут наладить эффективное взаимодействие с образовательным учреждением. В конечном итоге благодаря Электронному дневнику повышается успеваемость и посещаемость школьников, что, несомненно, повышает престиж школы.

Этот комплекс использует персональные данные, поэтому требуется защита персональных данных. Выделение категории персональные данные из более общей категории частная жизнь связано, прежде всего, с распространением автоматизированных систем обработки и хранения информации, в первую очередь компьютерных баз данных, к которым возможен несанкционированный доступ.

Именно эти системы, по сути, сделавшие революцию в вопросах структурирования, хранения и поиска необходимых данных, создали предпосылки для возникновения проблемы защиты сведений персонального характера – персональных данных с целью защиты прав и свобод граждан.

Технические меры защиты информации предполагают использование программно-аппаратных средств защиты информации.

При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов предприятия.

Технические средства защиты информации делятся на два основных класса:

– средства защиты информации от несанкционированного доступа (НСД): системы разграничения доступа к информации; антивирусная защита; межсетевые экраны; средства блокировки устройств ввода-вывода информации, криптографические средства и т.п.

– средства защиты информации от утечки по техническим каналам: использование экранированных кабелей; установка высокочастотных фильтров на линии связи; установка активных систем шумления и т.д.

Организационные меры по защите персональных данных включают в себя разработку организационно-распорядительных документов, которые регламентируют весь процесс получения, обработки, хранения, передачи и защиты персональных данных.

Перечень мероприятий по защите персональных данных:

- определение круга лиц, допущенных к обработке персональных данных;
- организация доступа в помещения, где осуществляется обработка ПДн;
- разработка должностных инструкций по работе с персональными данными;
- установление персональной ответственности за нарушения правил обработки ПДн;
- определение продолжительности хранения ПДн и т.д.

Реализация организационных мер защиты информации осуществляется с учетом категорий персональных данных – чем выше категория, тем выше требования их защиты.

Виноградов А.А.

**Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
ДОВЕРИТЕЛЬНАЯ ПРОГРАММНО-АППАРАТНАЯ ПЛАТФОРМА АСУ
КРИТИЧЕСКИХ ИНФРАСТРУКТУР**

Сетецентрическая концепция ведения военных действий и стратегического противостояния, активно внедряемая государствами НАТО, выдвигает ряд новых угроз, требующих адекватного парирования в информационных системах критических инфраструктур.

Целью первого парализующего и сокрушительного удара становятся не военные объекты и непосредственно оружие, а информационные ресурсы стратегических систем государственного и военного управления.

В современных условиях на первый план выходит доверительность работы АСУ. Свойство доверительности означает:

- Кибер-устойчивость (парирование информационных атак и других угроз, порождаемых сетецентрическим противостоянием);
- Функциональная полнота заложенных алгоритмов для решения задач применения системы по основному назначению;
- Полное соответствие работы системы заложенным в неё алгоритмам и функциям;
- Предсказуемость поведения системы в соответствии с ТЗ на полном наборе внешних и внутренних дестабилизирующих факторов (эффективное парирование угроз).

Функциональные задачи, условия и порядок применения стратегических систем государственного и военного управления существенно отличаются друг от друга, что неизбежно отражается на технической политике по созданию систем и по обеспечению парирования угроз.

Подавляющее большинство глобальных информационно-управляющих систем критических инфраструктур России построено на импортных программно-аппаратных решениях. Современные импортные информационные технологии (ИТ) – это инструмент, который является обоюдоострым. Импортные ИТ содержат встроенную избыточность, необходимую для выполнения работы системы по основному назначению, однако эта избыточность позволяет получать дополнительную информацию и вести стороннюю деятельность, в том числе и враждебного характера. Типичный пример – мобильные телефонные сети. Платные услуги мобильной связи демонстрируют возможность эксплуатации технологической избыточности ИТ:

- Позиционирование абонента, не нужное для передачи речи, – проводится и продаётся как информация о месте нахождения ребёнка;

- Тотальное архивирование цифровой информации, не нужное для передачи речи, проводится и часто используется в коммерческих интересах, следственных действиях, и т.д.

Вводится и эксплуатируется также наложенная избыточность – будильник срабатывает и включает выключенный Вами мобильник, то есть в телефоне реализуется не тот режим, который вы задали. Выключения на самом деле не произошло! Хотя для вас демонстрируется вид гашения всех индикаторов и прекращения реакции на кнопки.

Соответственно более сложные информационные системы имеют гораздо больше ресурсов встроенной технологической избыточности для реализации не декларированных возможностей и поддержки информационных атак, которые и лежат в основе реализации концепции информационной разведки и стратегии влияния при сетецентрическом противостоянии.

Свойство доверительности распространяется не только на сами системы, но и на технологии их проектирования, изготовления, испытаний.

В системах требуется особо обратить внимание на такие составляющие свойства доверительности, как кибер-устойчивость, информационная безопасность, отказобезопасность, устойчивость систем к не выявленным при проектировании инженерным ошибкам.

Кибер-устойчивость систем на импортных решениях обычно обеспечивается методами упреждающего выявления действий вредоносных программ до наступления катастрофических последствий с дальнейшим их блокированием. Учитывая, что защита против новых вирусов

реализуется только после их выявления, не следует предполагать, что в реальном конфликте противник будет применять старые методы атак и системы будут «знать» о необходимых методах противодействия. На этапе мирного времени и в условиях начального периода ведения военных действий, когда еще не наступили последствия от применения противником кибер-ударов по информационным ресурсам систем можно рассматривать выстраивание системного противостояния кибер-атакам, однако из-за технологического отставания следует предполагать высокую вероятность последующего вывода из строя систем, совместимых по системе команд с технологиями кибер-вторжения. В условиях дополнительной деградации от применения высокоточного оружия прекращение функционирования систем на импортных решениях неизбежно наступит на начальных этапах военного конфликта.

По мнению ФГУП «НПО «Импульс» надёжная кибер-устойчивость систем, от которых требуется работа в чрезвычайных условиях, может быть достигнута только при их невосприимчивости к методам и технологиям кибер-вторжений, что возможно реализовать только на программно-аппаратной платформе, программно не совместимой с технологиями вторжения и доступной для тотального технологического контроля на не декларированные возможности. Для глобальных систем, построенных на импортных решениях с высокой производительностью и большими информационными ресурсами хорошее решение даёт виртуализация вычислительной среды, позволяющая построить виртуальные ресурсы не на стандартных, а на специализированных программных решениях. Методы воздействия, направленные против уязвимой физической платформы, не воспринимаются на виртуальном уровне как коды вредоносных программ и оказываются не эффективными. Виртуализация вычислительной среды позволяет также сократить количество уязвимых точек физического вхождения и обеспечить тотальный организационно-технический и информационный контроль над их использованием.

Отказобезопасность – это свойство систем не допускать возникновения катастрофических последствий от проявления любых неисправностей и искажений информации. Отказобезопасность в системах разработки ФГУП «НПО «Импульс» закладывается и обеспечивается на всех стадиях их создания.

Инженерные ошибки становятся постоянно присутствующим фактором, так как существенно повысилась алгоритмическая насыщенность систем, сложность программного обеспечения и степень интеграции аппаратных платформ. Абсолютно всё ошибки выявить и устранить на этапах отладки и испытаний становится невозможным. Даже в массовых высоко интегрированных программных продуктах и аппаратных платформах мировых разработчиков и производителей постоянно обнаруживаются не выявленные на этапах отладки ошибки в микросхемах и в программном обеспечении. Для борьбы с не выявленными ошибками важнейшим свойством систем становится контролируемость целостности вычислительных процессов и массивов данных по ходу их выполнения со своевременным принятием парирующих мер. Контролируемость должна обеспечиваться на всех уровнях функционирования систем, начиная от ЭРИ и заканчивая системными алгоритмами.

Свойство доверительности должно обеспечиваться как в самих системах, так и в технологиях их создания, исключающих утечку проектной информации, минимизирующих инженерные ошибки и исключающих внедрение не декларированных возможностей в конечный продукт. Общепринятым является мнение о том, что достаточно закупить и установить на предприятии современный САПР, чтобы качественно повысить уровень проектирования. На самом деле САПР – это только инструмент. Очень важно правильно поставить процесс проектирования и обучить этому процессу специалистов. Каждый САПР требует создания стандарта предприятия по его применению.

Важнейшим аспектом является моделирование в САПР. Это сложный процесс, который требует разработки моделей объекта в целом и его составных частей, начиная с ЭРИ. Лицензионные САПР рассчитаны на дополнительную закупку библиотек информационных моделей, но только для импортных компонентов. Требуется дополнительная разработка отечественных моделей. Применение моделирования не сокращает сроков выпуска КД, а наоборот требует дополнительных интеллектуальных и временных затрат на стадии разработки КД. Эффективность от внедрения процессов проектирования на современных САПР, экономия средств и сокращение сроков работ достигается на стадиях автономной и комплексной отработки реально изготовленной аппаратуры, благодаря существенному сокращению объема требуемых доработок аппаратуры и программного обеспечения.

Важнейшей стадией отработки доверительности систем является тестирование и верификация программно-аппаратной платформы, функционального программного обеспечения и системы в целом. На эти работы в полном объеме, включая проверку алгоритмов негативного управления по парированию сбоев, отказов и других угроз, требуется время и усилия, которые категорически надо планировать и эффективно использовать в целях проверки и подтверждения доверительности работы создаваемых систем.

Понятие доверительности сложилось в НПО «Импульс» в процессе создания информационно-управляющих систем на протяжении 50-летней напряженной инженерной деятельности.

Доверительность не является новым свойством для систем разработки нашего предприятия, так как они проектируются на отечественной радиационно-стойкой ЭКБ и на программном обеспечении на базе доверительных операционных систем собственной разработки.

Доверительность системы закладывается, отрабатывается и проверяется на всех уровнях проектирования:

1. Функциональность и встроенный контроль ЭРИ.
2. Схемные решения на уровне электронных модулей.
3. Горячее и холодное резервирование на уровне вычислительных структур.
4. Алгоритмические решения на уровне системных протоколов и функционального программного обеспечения.
5. Конструкционная надёжность.
6. Производственно-технологическая надёжность.
7. Эксплуатационная надёжность.

НПО «Импульс» на протяжении своей деятельности на разных этапах развития отечественной промышленности вынуждено было заниматься созданием необходимой ЭКБ, технологий и самих систем, которые по определению уже в первых поколениях носили доверительный характер.

Подавляющее большинство созданных стратегических глобальных систем в России построены на импортных аппаратно-программных платформах, которые настойчиво предлагаются по дешёвым ценам иностранными государствами и заняли на сегодня практически всё информационное пространство страны.

В условиях, когда неоднократно подтверждалась возможность блокирования военных управляющих систем и систем связи со стороны противника в ходе локальных военных конфликтов, требуется понимать, что такие же методы информационных блокировок и организации утечки информации реализованы в информационных ресурсах импортных систем, развернутых на территории России.

Адекватное парирование новых угроз обеспечивается надёжно только при условии применения доверительных отечественных программно-аппаратных платформ.

На переднем плане остаётся также надёжность, радиационная стойкость, устойчивость к внешним воздействующим факторам систем специального назначения.

Доверительные технологии должны также давать возможность просматривать и совершенствовать алгоритмы негативного управления при деградации компонентов платформы, а также автоматического восстановления конфигурации при устранении неисправностей. Важнейшим является вопрос живучести систем и реализации встроенного и наложенного аппаратного, программно-аппаратного и программного контроля в платформах.

Только комплексный подход к обеспечению действительной доверительности отечественных программно-аппаратных платформ обеспечивает позволяет создавать высоконадёжные технические средства и системы специального назначения.

Нужно говорить о целостной государственной технологической политике по созданию доверительной отечественной программно-аппаратной платформы с целевым финансированием. Доверительная платформа м.б. сделана только на доверительных технологиях.

Государственная технологическая политика должна охватывать весь комплекс работ, которые необходимо возобновить или поставить заново территории страны, чтобы обеспечить действительную технологическую независимость систем управления критическими инфраструктурами.

Совершенно не достаточно ограничиваться только вопросом создания отечественной ЭКБ, хотя это одна из ключевых задач.

Государственная технологическая политика должна включать в себя следующие направления работ:

- Технологии моделирования возможных возмущений от воздействующих факторов, выработки, оптимизации и верификации на моделях требований к системам и к ЭКБ в зависимости от условий их применения;
- Интегрированные доверительные технологии проектирования систем специального назначения, их программных и аппаратных средств;
- Доверительные технологии проектирования специализированной ЭКБ;
- Независимые технологии изготовления специализированной ЭКБ, материалов и конструкций для компонентов систем специального назначения;
- Технологии автономной и комплексной отладки систем специального назначения;
- Технологии испытаний специализированных систем в привязке к стойкости к воздействующим факторам и к требуемому функционалу основной работы с учётом алгоритмов негативного управления, предельных и разрушающих испытаний.

Технологии моделирования возмущений должны включать в себя виртуальные компьютерные методы, создание современных моделирующих установок реальных воздействующих факторов. В

результате должны быть разработаны требования по стойкости к воздействующим факторам для разных видов платформы в зависимости от условий их применения.

Не менее важным является этап системного проектирования, по результатам которого разрабатываются функциональные требования к различным видам платформ в зависимости от предметной области применения.

В результате появляется система требований к ЭРИ, материалам, конструкции, к функционированию платформ для каждого вида применения.

Центральным обычно становится вопрос оптимизации соотношения стойкости платформы к условиям применения и ее вычислительной мощности. Хочется иметь всегда максимальную вычислительную мощность, однако на практике мощность процессора и мощность готовой платформы существенно отличаются между собой. Основная задача технологий проектирования аппаратных и особенно программных средств концентрируется вокруг максимального использования всех возможностей аппаратуры, программного обеспечения, конструкции для достижения максимальной вычислительной мощности создаваемой платформы в целом при обеспечении требований по стойкости к воздействующим факторам.

Технологии проведения испытаний должны включать в себя значительно большую моделирующую составляющую для выявления проблем на ранних стадиях создания систем и для сокращения затрат на натурные испытания.

Отдельного внимания требует также вопрос создания эквивалентных технологий испытаний для условий применения, моделирование или создание которых затруднено (термо-вакуумные испытания).

Таким образом, в современных условиях сетецентрического противостояния реализация доверительности информационных систем критических инфраструктур становится важнейшим требованием по обеспечению работоспособности при наличии информационных и физических дестабилизирующих факторов.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 19176 - 80. Системы управления техническими средствами корабля. Термины и определения.
2. Черкесов Г.Н. О системном анализе безопасности. – Безопасность жизнедеятельности, 2004, № 1.
3. Черкесов Г.Н. Методы и модели оценки живучести сложных систем. – М.: Знание, 1987.
4. Половко А.М., Гуров С.В. Основы теории надежности. Глава 13. Надежность и риск. – СПб: БХВ-Петербург, 2006.
5. ГОСТ 27.310-95. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения.
6. ГОСТ ЕН 1070-2003. Межгосударственный стандарт. Безопасность оборудования. Термины и определения. – Минск: Изд-во стандартов, 2003. – 23 с.
7. ГОСТ ИСО/ТО 12100-1-2001. Межгосударственный стандарт. Безопасность оборудования. Основные понятия, общие принципы конструирования. Часть 1. Основные термины, методика. – Минск: Изд-во стандартов, 2001. – 17 с.
8. Авиженис А. Отказоустойчивость – свойство, обеспечивающее постоянную работоспособность цифровых систем. Пер. с англ. – Труды ИИЭР, 1978, т. 66, № 10, с. 5-25.
9. Avizienis A. Design of fault-tolerant computers. – AFIPS Conf. Proc., 1967, FJCC, v. 31, p. 733-744.
10. Рябинин И.А. Надежность и безопасность структурно-сложных систем. – СПб: изд-во СПбГУ, 2007.
11. Надежность систем энергетики: Терминология. Сборник рекомендуемых терминов. – Вып.95. – М.: Наука, 1980. – 42 с.
12. Словарь по кибернетике. Под ред. В.М. Глушкова. – Киев: Главная ред. Укр. сов. энциклопедии, 1979.
13. Справочник по безопасности космических полетов//Береговой Г.Т. и др. М.: Машиностроение, 1989, 336 с.
14. Бахметьев А.М., Самойлов О.Б., Уснин Г.В. Методы оценки и обеспечения безопасности ЯЭУ. М.: Энергоатомиздат, 1988, 136 с.
15. Супаков Н.К. Безопасность эксплуатации ракетного оружия. М.: Изд. МО, 1972, 220 с.
16. Майоров А.В., Москатов Г.К., Шибанов Г.П. Безопасность функционирования автоматизированных объектов. М.: Машиностроение, 1988, 262 с.

Волкова А.В.

Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» СИНТЕЗ ОПТИМАЛЬНОГО МАНИПУЛЯЦИОННОГО КОДА ДЛЯ СИГНАЛЬНО-КОВОДНОЙ КОНСТРУКЦИИ НА ОСНОВЕ ТРЁХМЕРНОЙ СИМПЛЕКС-РЕШЁТКИ

Настоящая работа посвящена нахождению оптимального манипуляционного кода для сигнально-кодовой конструкции на основе трёхмерной симплекс-решётки для модема КВ-радиосвязи. Предполагается, что оптимальный манипуляционный код поможет повысить помехоустойчивость сигнала. В заключение работы будут представлены сравнительные характеристики, полученные в результате моделирования.

Благодаря преимуществам КВ радиосвязи, среди которых можно выделить возможность организации связи на расстоянии до нескольких тысяч километров при относительно небольшой мощности передатчиков (1 кВт), её применяют для передачи команд звеньям управления. Однако в связи с особенностями КВ канала, рассматриваемый тип радиосвязи подвергается ряду помех, связанных с многолучевостью и состоянием ионосферы. Таким образом, требуется повысить помехоустойчивость применяемых сигналов. Это, в свою очередь, приводит к снижению частотной эффективности или же уменьшению скорости передачи.

К системам КВ радиосвязи могут применять требования относительно внедрения структуры ISDN. Но существующие виды модуляции КВ модемов позволяют передавать не более 4800 бит/с.

Такая скорость не является достаточной для организации сервисов, соответствующих более высоким уровням модели OSI. Таким образом, возникает задача увеличения скорости при сохранении помехоустойчивости и частотной эффективности.

Одним из факторов, определяющих реально достижимое значение скорости передачи, являются применяемые виды модуляции и кодирования сигналов. Как известно, при применении обычных видов модуляции улучшение скорости передачи при заданной допустимой помехоустойчивости приводит к снижению спектральной и энергетической эффективности. Следовательно, поставленная задача увеличения скорости передачи при сохранении помехоустойчивости и полосы является актуальной.

Одним из способов решения поставленной задачи является повышение качества функционирования модемов. На рисунке 1 приведена блок-схема модемов на передающей и приёмной стороне. С точки зрения нашей задачи модулятор выполняет две функции:

1. Формирует набор сигналов с определёнными параметрами (т.е. задаёт положение всех возможных сигнальных точек на фазовой плоскости) (фактически, вид модуляции: ОФМ, КАМ и т. д.);
2. Сопоставляет каждой такой точке скаляр (т. е. кортеж бит).

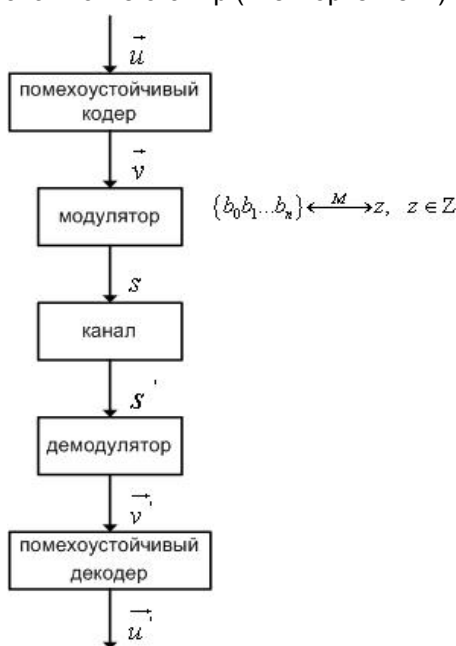


Рис.1. Блок-схема модема

Таким образом, повышение качества работы модулятора можно проводить по двум направлениям: выбор оптимального расположения точек созвездия и способ сопоставления каждой такой точке скаляра.

При применении обычных видов модуляции улучшение скорости передачи при заданной допустимой помехоустойчивости приводит к снижению спектральной и энергетической эффективности. В работе [1] был предложен новый принцип формирования набора сигналов. Такие сигналы получили название сигнально-кодовой конструкции на основе трёхмерной симплекс-решётки. В работе [2] было показано, что данная сигнальная конструкция обладает лучшей помехозащищённостью при заданной полосе и скорости по сравнению с сигналами обычных видов модуляции. Следующим возможным способом повышения помехоустойчивости сигнала является оптимизация манипуляционного кода с точки зрения минимизации расстояния по Хэммингу между соседними точками созвездия. Настоящая работа посвящена оптимизации манипуляционного кода, приводящей к улучшению помехозащищённости сигнала.

Манипуляционное кодирование — сопоставление картежу бит физического сигнала. В случае если имеет место канал с белым гауссовым шумом, наиболее вероятные ошибочные сигналы — ближайшие к переданному сигналу. Под оптимальным манипуляционным кодом в настоящей работе подразумевается код, дающий наименьшую вероятность ошибки при заданной энергии и полосе.

В случае отсутствия помехоустойчивого кодирования оптимальным манипуляционным кодом считается код Грея. Т. е. такой код, при котором «соседним» сигналам соответствуют кортежи бит, имеющие наименьшее расстояние по Хэммингу. Однако, в случае применения кодов, исправляющих ошибки, такой манипуляционный код не является оптимальным. Задачу можно сформулировать так: в случае, если искажение физического сигнала приводит к неисправляемой ошибке, то неверно декодированное информационное слово должно иметь наименьшее расстояние по Хэммингу от переданного информационного слова:

$$P_{erik} \uparrow \Rightarrow h_{ik} \uparrow$$

На рисунке 2 проиллюстрирован принцип разработанного манипуляционного кода. Данный метод манипуляции синтезировался для амплитудной модуляции и помехоустойчивого кода Хэмминга (7, 4). Алгоритм разработки метода манипуляции состоит из трёх этапов:

1. Нахождения кодовых слов для всех возможных информационных слов.
2. Сопоставление им сигнала с амплитудой, равномерно распределённой по множеству возможных значений, так чтобы расстояние по Хэммингу между соседними кортежами не превосходило единицы;
3. Оставшиеся свободные физические сигналы соответствуют кодовым словам, в которых произошли ошибки; так, для каждого из 2^k кодовых слов можно поставить в соответствие по $2^{n-k} - 1$ искажённых кодовых слов, где произошла однократная ошибка; следовательно, на сигнальной прямой вокруг неискажённых кодовых слов расставляются кодовые слова, где произошли однократные ошибки, соответственно.

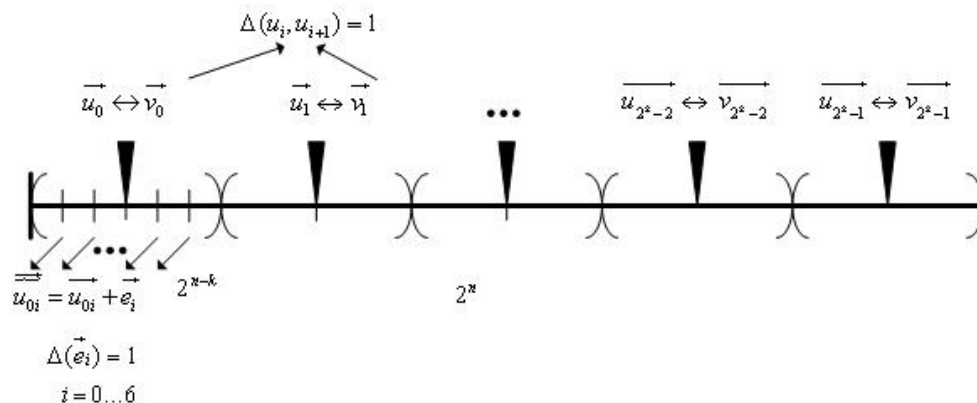


Рис. 2. Принцип формирования оптимального манипуляционного код

При синтезе оптимального манипуляционного кода было принято во внимание, что в условиях канала БГШ с наибольшей вероятностью искажается сигнал с соседними амплитудами. Таким образом, при данном методе манипуляционного кодирования наиболее вероятные искажения приводят к однократным ошибкам. Т. е. искажения находятся в области исправления ошибок. Если же ошибка приводит к области неисправляемых ошибок, то в результате декодирования получаем информационное слово, отличающее на один бит. Эта особенность предложенного манипуляционного кодирования даёт возможность предположить, что помехоустойчивость такого сигнала улучшится. Т.е. при заданном отношении сигнал/шум, то средняя вероятность ошибки (СВО) уменьшится.

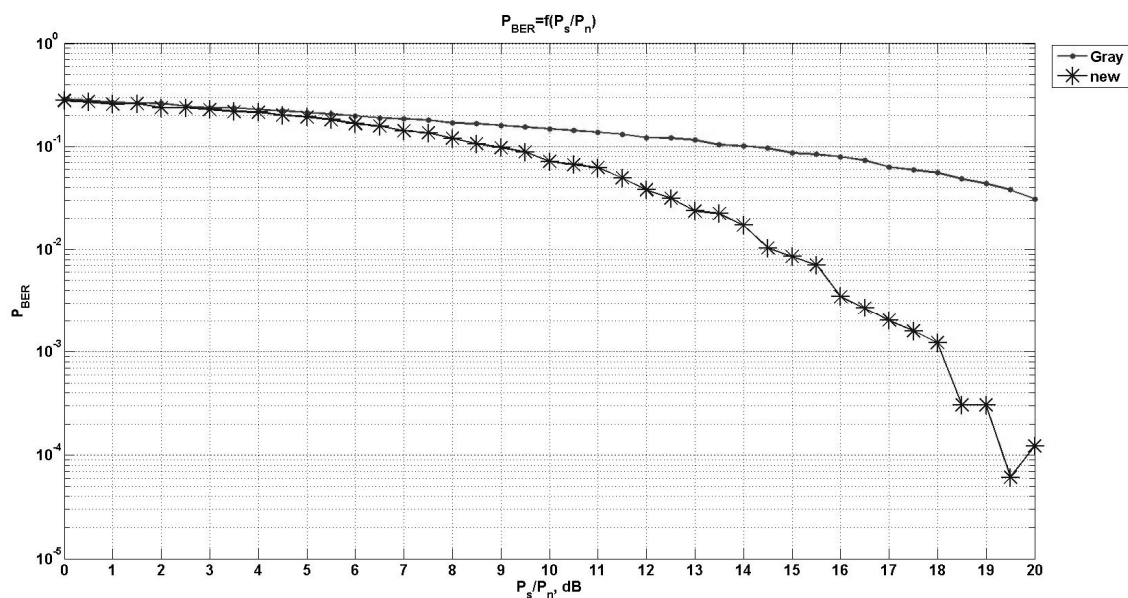


Рис.3. Зависимость вероятности ошибки от отношения сигнал-шум для амплитудной модуляции при использовании манипуляции кодом Грея ("Gray") и синтезированного оптимального модуляционного кода ("new")

Для проверки данного предположения была построена модель в среде MatLab. На рисунке 3 приведена зависимость вероятности ошибки на бит от отношения сигнал/шум для предложенного метода манипуляции сигнала и для манипуляции кодом Грея.

СПИСОК ЛИТЕРАТУРЫ

1. Путилин А.Н., Волкова А.В. Сигнально-кодовая конструкция на основе трёхмерной симплекс-решётки // 12-я Международная конференция «Цифровая обработка сигналов и её применение» («DSPА-2010»). М, 2010.
2. Волкова А.В. Анализ сигнально-кодовых конструкций, применяемых в модемах систем с псевдослучайной перестройкой рабочей частоты и предложения по их улучшению // Интегрированные автоматизированные системы управления: сборник докладов научно-технической конференции. Ульяновск, 2011.

Гук И.И., Путилин А.Н., Сиротинин И.В., Хвостунов Ю.С.

Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»

АДАПТИВНАЯ СИСТЕМА ДЕКАМЕТРОВОЙ РАДИОСВЯЗИ С ПОЛНОДИАПАЗОННОЙ ПЕРЕСТРОЙКОЙ РАБОЧЕЙ ЧАСТОТЫ И ПРЕДВАРИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ ТРАССОВЫХ ИСПЫТАНИЙ ЕЁ ФРАГМЕНТА

Адаптивная система коротковолновой радиосвязи с полнодиапазонной псевдослучайной перестройкой рабочей частоты (АСДР ППРЧ) предназначена для создания симплексных, полудуплексных и дуплексных каналов радиосвязи декаметрового диапазона на дальности до 300 км в движении и до 3000 км между стационарными пунктами связи со скоростями работы абонента от 2400 до 19 200 бит/с.

1. Принципы АСДР ППРЧ

Для каждой отдельной сети:

- выделяется пул рабочих частот (N рабочих частот);
- назначается n ($n < N$) начальных рабочих частот;
- назначается ключ закона перестройки рабочей частоты;
- устанавливается время t работы на одной рабочей частоте.

Для каждого абонента отдельной сети:

- назначается двухбайтный сетевой адрес;
- назначается одна из ортогональных строк частотно-временной матрицы рабочих частот.

При вводе абонента в сеть через радиоканал осуществляется начальная синхронизация переключения начальных рабочих частот (сетевая синхронизация). В дальнейшем в течение 1 – 1,5 месяцев абонент готов к обмену информацией из состояния радиомолчания без предварительного этапа зондирования канала связи и установления синхронизации. Если с течение этого времени в сети состоялся обмен информацией, то для всех абонентов сети время готовности продлевается на 1 – 1,5 месяца.

Адресная передача («точка» - «точка», «точка» - «многоточка») ведется пакетами длительностью 53 мс на каждой из n начальных рабочих частот.

Принимающая радиостанция в процессе обмена информацией без снижения пропускной способности подтверждает передающей успешный прием по каждой используемой рабочей частоте. В случае отсутствия приема на данной рабочей частоте принимающая радиостанция дает команду передающей радиостанции на замену на резервную рабочую частоту из общего набора.

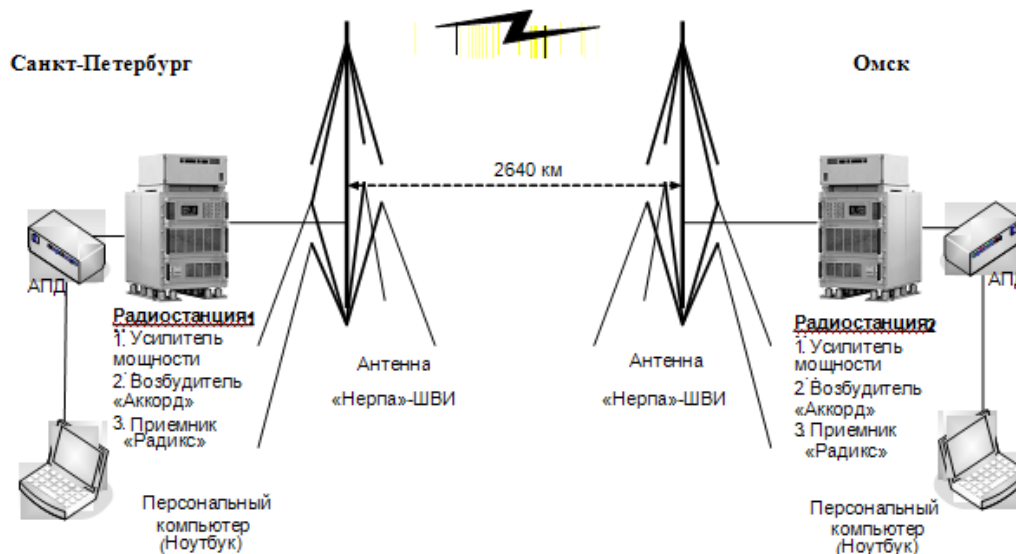


Рис.1. Схема трассовых испытаний

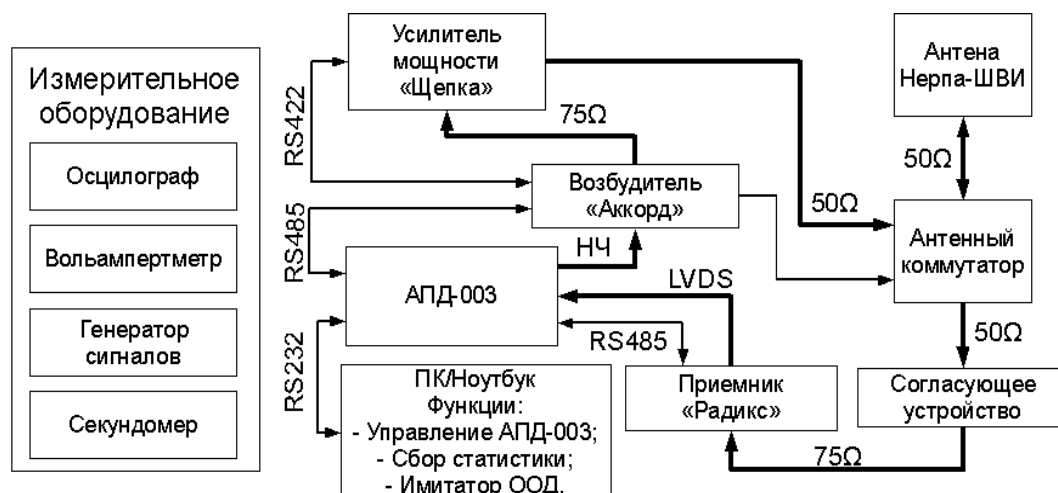
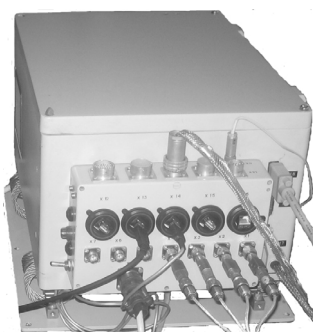


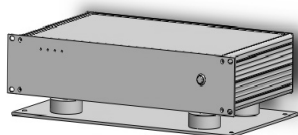
Рис.2. Состав оборудования

2. Характеристика аппаратуры



- Диапазон рабочих частот, МГц 1.5...30,
- Количество каналов приема 2,
- Полоса пропускания приемного канала, КГц 3.1; 4.5; 9.0,
- Динамический диапазон по основному каналу приема, дБ, не менее 124,
- Чувствительность, мкВ, не более 0.7,
- Избирательность по соседнему каналу на отстройке 5 КГц дБ, не менее 95,
- Количество значимых разрядов цифрового выхода LVDS (динамический диапазон 127дБ) 22,
- Время перестройки рабочей частоты, мс не более 0.1,
- Температурная нестабильность частоты опорного генератора, не более $\pm 2 \cdot 10^{-8}$.

Рис.3. Приёмник



- Диапазон рабочих частот изделия, МГц 1,5-30,
- Полоса пропускания приемного канала, КГц 3.1; 4.5; 9.0,
- Напряжение сигнала на входе НЧ, мВ 50 $\pm$ 5,
- Напряжение сигнала на ВЧ-выходе, мВ 3000 $\pm$ 450,
- Отношение сигнал/шум на ВЧ-выходе в полосе частот 3,1 КГц, при отстройках ± 10 %, не более, дБ минус 120,
- Время перестройки рабочей частоты не более, мс 0.1,
- Относительное отклонение частоты настройки от номинального значения, не более $\pm 2 \cdot 10^{-8}$.

Рис. 4. Возбудитель



- Диапазон рабочих частот, МГц 1,5-30,
- Пиковая выходная мощность при работе на согласованную нагрузку (50 Ом), Вт 1000 (+259; минус 205), 35%,
- КПД, в режиме полной мощности, не менее 35%,
- Время готовности изделия к работе из выключенного состояния после подачи на него электропитания, с, не более 6,
- Время перестройки рабочей частоты, не более, мс 3,0,
- Относительный уровень гармонических составляющих, в выходном сигнале не превышает, дБ:
 - на частотах до 3F минус 55,
 - на частотах от 4F до 8F минус 70
 - (F – частота настройки изделия),
- Относительный уровень шума на выходе, измеренный относительно номинальной мощности при отстройке на ± 10 % от основной частоты изделия, дБ/Гц, не более 170.

Рис.5. Усилитель мощности



- Рабочий диапазон частот, МГц 3,0 - 30,0,
- КСВН, не более:
 - в диапазоне частот от 3 до 4,99 МГц 3,5,
 - в диапазоне частот от 4,99 до 30 МГц 2,
- Диаграмма направленности в горизонтальной плоскости круговая,
- Входное сопротивление, Ом 50,
- Подводимая мощность, кВт 1,2,
- Габаритные размеры изделия в рабочем состоянии не более:
 - радиус без противовесов, м 9,5,
 - радиус с противовесами, м 15,
 - высота, м 15.

Рис.6. Широкополосная антенна



- Скорость передачи информации оконечного оборудования данных (ООД) по декаметровому радиоканалу с полосой пропускания:
 - 3,1 КГц, бит/с 2400 – 7200,
 - 4,5 КГц, бит/с 2400 – 9600,
 - 9,0 КГц, бит/с 2400 – 19 200,
- Длительность работы на одной рабочей частоте в режиме псевдослучайной перестройки рабочей частоты, мс 53,3,
- Вид модуляции ООФМ, ДОФМ, ТОФМ, КАМ, 1,5- 30,
- Диапазон перестройки рабочей частоты, МГц 1,5- 30,
- Период псевдослучайной последовательности перестройки рабочей частоты $2^{128}-1$,
- Количество рабочих частот, используемых в пакете перестройки 32,
- Время замены забракованной рабочей частоты в пакете перестройки на резервную рабочую частоту без перерыва обмена информации ООД (режим адаптации), с 5,1-54,
- Диапазон адаптации по скорости, бит/с 2400 – 19 200,
- Количество выделенных резервных рабочих частот 96,
- Интерфейс управления радиосредствами RS-485.

Рис.7 Аппаратура передачи данных

3. Предварительные результаты трассовых испытаний фрагмента системы

Трассовые испытания фрагмента системы проходили в период с 10.08.2011 г. по 06.09. 2011г. Работа велась круглосуточно с перерывами.

Оконечное оборудование данных (ноутбук) формировало файловую последовательность, которая поступала в аппаратуру передачи данных. Пройдя через канал связи, последовательность сравнивалась в приемной части оконечного оборудования данных (ООД), где и формировался поток

ошибок. ООД обрабатывало полученный поток и формировало по анализу состояния АПД для каждого сеанса связи статистические данные:

- текущая скорость работы;
- текущий режим работы модулятора;
- время поиска максимального количества рабочих частот удовлетворительного качества;
- процент времени с удовлетворительным качеством приема (вероятность ошибки на бит меньше 10⁻³ – 10⁻⁵);
- текущее количество рабочих частот удовлетворительного качества (из 32-х используемых в пакете перестройки);
- соотношение сигнал/шум для каждой рабочей частоты (на которой были сеансы связи или ведется работа в настоящий момент времени);
- средняя вероятность ошибки на бит на рабочих частотах удовлетворительного качества;
- частота использования каждой рабочей частоты удовлетворительного качества.

Таблица

Предварительные результаты трассовых испытаний фрагмента системы

№ п.п.	Параметр	Оценка параметра
1.	текущая скорость работы, Кбит/с	2,4 ÷ 19,2
2.	текущий режим работы модулятора	ООФМ, ДОФМ, ТОФМ, КАМ
3.	процент времени с удовлетворительным качеством приема	60 ÷ 100
4.	текущее количество рабочих частот удовлетворительного качества (из 32-х используемых в пакете перестройки)	40 ÷ 100
5.	соотношение сигнал/шум для каждой рабочей частоты, дБ	< 0 ÷ 26
6.	средняя вероятность ошибки на бит на рабочих частотах удовлетворительного качества	< (10 ⁻³ ÷ 10 ⁻⁵)
7.	частота использования каждой рабочей частоты удовлетворительного качества, %	< 1 ÷ 3,1

В результате трассовых испытаний АСДР ППРЧ доказана высокая эффективность предложенной системы адаптивной декаметровой радиосвязи с использованием ППРЧ. Подтверждена возможность использования декаметровой радиосвязи в системах автоматизированного управления.

Ефимов Е.А.

**Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПРИ ЗАСЕКРЕЧИВАНИИ**

Информационная безопасность обеспечивается применением аппаратуры засекречивания для информационных потоков, выходящих за пределы охраняемых зон.

Применяются два вида засекречивания – линейное и блочное.

Линейное засекречивание производится кодированием потоков информации, передаваемых по каналам связи. Для линейного засекречивания применяется покупная аппаратура засекречивания, которая кодирует информацию, выходящую из модемов, и декодирует информацию, входящую в модемы. Для предотвращения выхода высокочастотных составляющих, подлежащих засекречиванию информационных потоков, питание схем обработки этих потоков проводится через специальные фильтры, подавляющие высокочастотные составляющие сигналов.

Секретная информация передается в аппаратуру линейного засекречивания по специальному стыку с сигналом ограниченного спектра. Незасекреченная и засекреченная информация передается в аппаратуру через отдельные экранированные кабели.

До передачи засекреченной информации в каналы связи в некоторых случаях используются специальные фильтры, подавляющие высокочастотные составляющие незасекреченного сигнала, которые могут проникнуть на выходы и на входы передатчиков из-за паразитных связей.

Частоты срезов и глубина подавления этих фильтров зависит от скорости передачи и спектров сигналов во время обработки, подлежащих засекречиванию.

Кроме линейного засекречивания используется блочное засекречивание блоков информации отдельными приборами засекречивания.

В стыках аппаратуры блочного засекречивания и аппаратуры помехоустойчивого кодирования используются фильтры высокочастотного подавления спектров засекречиваемых сигналов для предотвращения попадания составляющих засекречиваемых сигналов на входы аппаратуры передачи данных.

Частоты срезов этих фильтров определяются скоростью передачи информации и спектрами засекречиваемых сигналов.

Далее приведены характеристики фильтров, использованных в цепях питания и информационных цепях.

1. *Фильтр помехоподавляющий ФП-009 ИМНЕ.468822.009* предназначен для снижения радиопомех по стыку с интерфейсом М-2 со скоростью передачи 1 Мб/сек.

Частота среза 4МГц.

Вносимое затухание цепей в диапазоне частот 10-1000 МГц:

- 40 дБ в диапазоне частот 10-20 МГц включительно;
- 60 дБ в диапазоне частот 20-40 МГц включительно;
- 40 дБ в диапазоне частот 40-80 МГц включительно;
- 60 дБ в диапазоне частот 80-1000 МГц включительно.

2. *Фильтр помехоподавляющий ФП-010 ИМНЕ.468822.010* предназначен для снижения уровней р/п в цепях первичного питания – двухпроводной сети постоянного тока, изолированной от корпуса, номинальным напряжением 28,5В. Вносимое затухание в полосе задерживания от 150 kHz до 100 MHz не менее 80dB.

3. *Фильтр помехоподавляющий ФП-012 ИМНЕ.468822.012* предназначен для подавления радиопомех в цепях сопряжения аппаратуры с каналами телеграфных сетей по стыку С1-ТГ.

Частота среза на уровне 3dB – 2 kHz.

Вносимое затухание в полосе задерживания от 100 kHz до 1000 MHz не менее 70 dB.

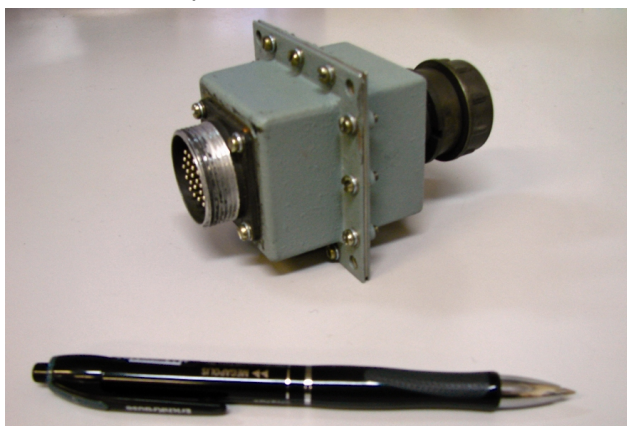


Рис. 4

Фильтр ФП-009 для подавления высокочастотных помех в канале «Манчестер-2», работающего со скоростью 1 Мбит/сек.

Иванов В.И.

**Россия, Санкт-Петербург, «Региональный Центр Защиты Информации «ФОРТ»
МЕТОДЫ ОБРАБОТКИ И АНАЛИЗА ДАННЫХ ПРИ АДАПТИВНОМ УПРАВЛЕНИИ
ИНЦИДЕНТАМИ В ГЕТЕРОГЕННЫХ СЕТЯХ СВЯЗИ**

В условиях динамического изменения ресурса информационных систем особое значение по реагированию на инциденты в гетерогенных сетях связи приобретают задачи комплексной обработки и анализа данных о событиях многоуровневой информационной безопасности по универсальным правилам, критериям, процедурам, методам и технологиям их реализации в реальном масштабе времени.

Анализ рынка систем обнаружения вторжений показывает, что заданные в них функции автоматического управления инцидентами в условиях непредвиденного воздействия внешних и/или внутренних угроз, имеющих многообразную природу происхождения, различные форматы представления, а также временные, пространственные и масштабные характеристики, не позволяет простыми методами смены алгоритмов функционирования и подбора оптимальных состояний, поддерживать заданную степень защищенности гетерогенных сетей связи.

Кроме того, следует учитывать, что общая оценка угроз информационной безопасности в этих сетях, определяется согласованными возможностями средств, как правило, автоматизированной регистрации учетных систем в контуре текущей (оперативной) обработки данных и экспертными возможностями аналитических систем в контуре комплексного анализа данных об инцидентах.

Основными причинами, вызывающими проблему адаптивного управления событиями информационной безопасности являются функциональные различия исполнительных систем текущей (оперативной) и комплексной обработки инцидентов, ограниченные вычислительные возможности, прежде всего средств комплексной обработки и анализа данных, распределенная неоднородная инфраструктура гетерогенной сети связи, трудность интеграции приложений, обрабатывающих и предоставляющих информацию о событиях в единую информационную систему.

Пытаясь решить проблему организации адаптивного управления инцидентами, специалисты по безопасности информационных сетей вынуждены отдавать приоритет построению многоуровневой системы обработки и анализа данных на основе создания периметров безопасности. При этом корреляционным, сигнатурным и инвариантным методам решения задач на всех уровнях

(прикладного программного обеспечения, системы управления базами данных, операционной системы, сети) предшествуют процедуры нормализации, фильтрации, классификации, агрегации, корреляции и приоритезации данных о событиях информационной безопасности по административно установленным критериям, правилам и метрикам.

Построенные таким образом по принципу «воронки» (рисунок 1), средства мониторинга, аудита и анализа данных об инцидентах оставляют вне поля обработки события с функциями принадлежности нечетких множеств, истинное значение которых было не определено, либо преднамеренно подвергнуто сомнению.

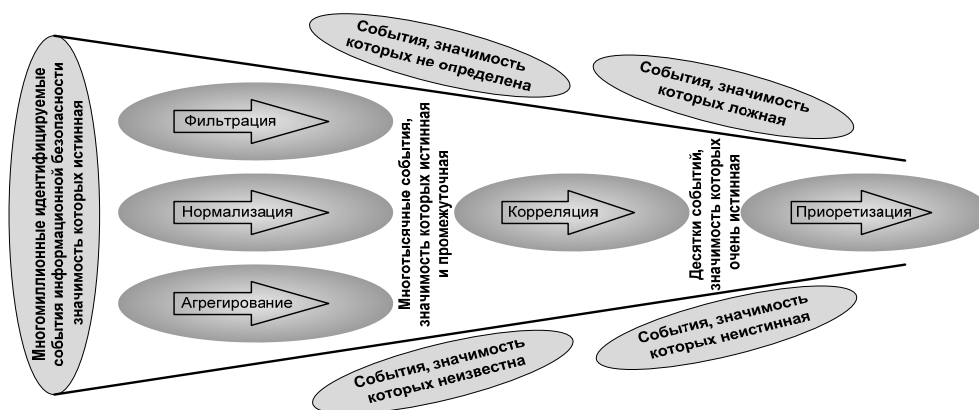


Рис.1. Принцип мониторинга событий информационной безопасности

В конечном результате при существующих методах обработки и анализа данных об инцидентах качество оценивания событий теряет полноценную совокупность своих характеристик и сводится чаще всего к количественной оценке угроз безопасности по пятибалльной шкале (незначительная, не существенная, умеренная, серьезная, критическая), а механизмы безопасности сети настраиваются на регистрацию только видимых явных угроз.

Такой подход в условиях интеграции межведомственных информационных систем значительно усложняет задачу адаптивного управления инцидентами и создает проблему идентификации многомерных событий и ошибок первого, второго рода.

В качестве оценочной шкалы нечеткого множества событий информационной безопасности (табл. 1) могут быть положены принципы построения матрицы суждений по методу Саати Т.Л. [1,2], когда система регистрации событий в гетерогенной сети связи настроена на идентификацию по показателям сравнения истинности события. При этом предлагается следующая градация оценочных суждений значения событий информационной безопасности:

- а) «Истинный», «Очень истинный» - показатель оценки «Норма» (события безопасности идентифицированы);
- б) «Неистинный», «Ложный», «Неопределено», «Неизвестно» - показатель оценки «Субнормальные»;
- в) «Промежуточные» - показатель оценки «Имеющие точки перехода».

Таблица 1

Шкала оценки нечеткого множества событий информационной безопасности

Сравнительные показатели оценки значений событийной модели	
Числовая оценка S_{in}	Качественная оценка ранга r_i , ранга r_n
1	Одинаковая значимость. Значения имеют одинаковый ранг, не влияют на выбор и/или поглощаются без усиления значимости
3	Слабое преимущество. Преимущество одного ранга перед другим малоубедительно
5	Сильное преимущество. Преимущество одного ранга перед другим весомо
7	Очевидное преимущество. Имеются убедительные свидетельства в пользу значения одного ранга.
9	Абсолютное преимущество. Имеются свидетельства в пользу одного ранга перед другим с наибольшей мерой убедительности
∅	Значимость не определена. Истинность значения ранга не определена в точке измерения.
[0,1]	Значимость неизвестна. Истинность значения ранга неизвестна в интервале [0,1].
2, 4, 6, 8	Промежуточные значения. Точки перехода нечеткого множества данных модели. Преимущество одного ранга перед другим имеет компромисс.

Такой подход к оценке событий информационной безопасности позволяет моделировать информационную обстановку для разнородных источников событий и средств (систем) их регистрации. Организационные аспекты предлагаемой модели показаны на рисунке 2.

Очевидно, что организующим элементом всестороннего взаимодействия средств (систем) текущей и комплексной обработки данных о событиях является создание интеграционной среды, построенной на платформе промежуточного программного обеспечения Middleware service и ориентированной на технологию объединения и совместного использования удаленных вычислительных, информационных ресурсов в системе безопасности гетерогенной сети связи. Взаимодействие в этой среде организуется по правилам, описываемым информационной, функциональной, динамической и экспертной моделями, которые являются составными частями обобщенной модели обработки и анализа данных о событиях информационной безопасности.

В основу предлагаемого метода, в отличие от применяемых методов оптимизации и минимизации вычислений, положена концепция организации виртуальной системы текущей обработки и комплексного анализа данных о событиях информационной безопасности, что в свою очередь позволяет моделировать полную событийную обстановку, устанавливать возможный замысел нарушителя, сценарии и трассы вторжения в систему, а также строить долгосрочные прогностические модели безопасности.

Задачами моделируемой интеграционной системы является эффективное распределение имеющихся вычислительных, сетевых и информационных ресурсов безопасности, ресурсов хранения данных о событиях, а также их координация в зависимости от состава и масштаба виртуальной модели, временных факторов реализации текущих и комплексных задач и целей, условий конфиденциальности и наличия, требуемых программных, программно-аппаратных, аппаратных компонентов сервисно-ориентированной архитектуры, которая способна выполнять функции как автоматической, автоматизированной, так и ручной обработки и анализа данных. При этом в структурном слое текущей обработки данных будет преобладать автоматизированная типовая модель оценки событий и противодействия угрозам, а в слое комплексной обработки и анализа данных – гибридные схемы.

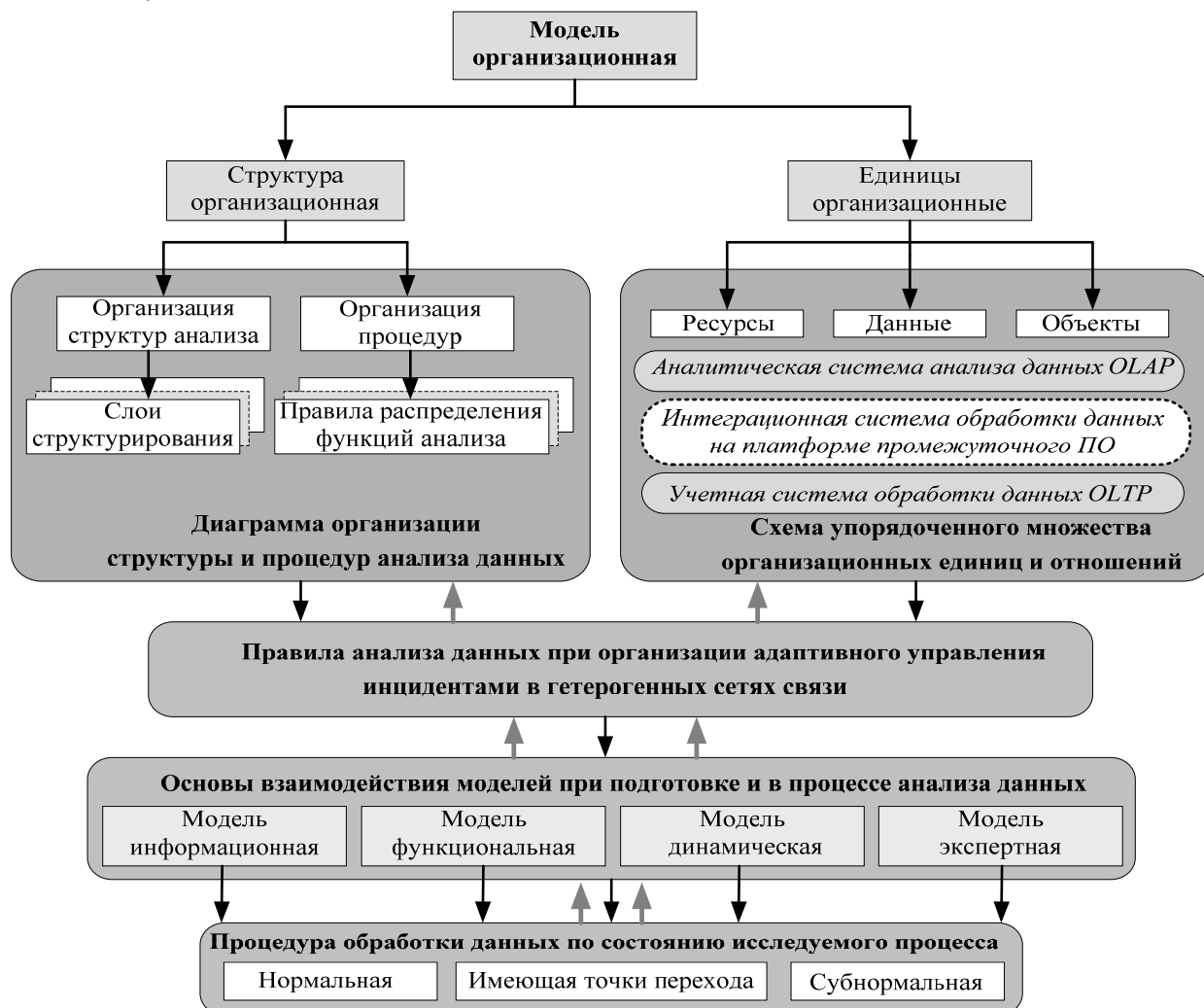


Рис.2. Модель организации системы обработки и анализа данных об инцидентах

Вариант алгоритма обработки и анализа данных об инцидентах в гетерогенной сети связи представлен на рисунке 3.

Создание интеграционной среды на платформе промежуточного программного обеспечения позволяет повысить эффективность и качество управления инцидентами, задает общий постоянный алгоритм функционирования системы безопасности, при котором локальные средства ведут текущую обработку событий, блокируют идентифицируемые угрозы, а затем по трассам событий передают полученные данные в интеграционную среду, ресурсы которой, при участии в ней системы комплексного анализа, позволяют в реальном масштабе времени исследовать многообразие сложных угроз и осуществлять обновление механизмов противодействия.

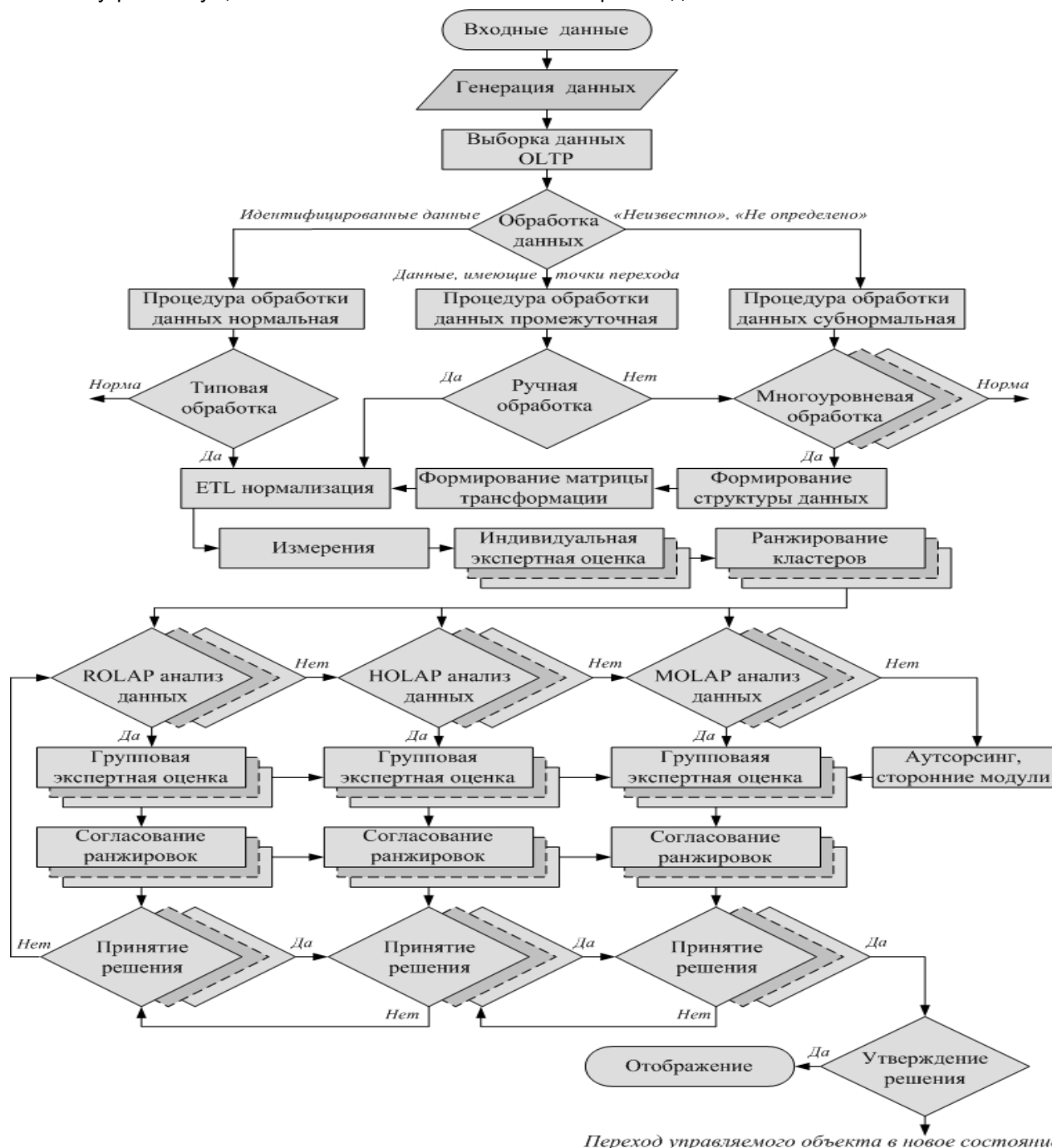


Рис. 3. Алгоритм организации процесса обработки и анализа данных (вариант)

СПИСОК ЛИТЕРАТУРЫ

1. Шумский А.А. Системный анализ в защите информации: Учебное пособие – М.: Гелиос АРВ, 2005, 224 с.
2. Корченко А.Г. Построение систем защиты информации на нечетких множествах: Теория и практические решения – К.: «МК-Пресс», 2006, 320 с.
3. Саати Т.Л. Принятие решений. Метод анализа иерархий: Перевод с английского – М.: Радио и связь, 1993, 320 с.
4. Антимонов С.Г. Мониторинг событий информационной безопасности и защита персональных данных: www.DialogNauka.ru
5. Демичев А.П. Введение в грид-технологии: Препринт НИИЯФ МГУ, 2007, 11/832.

Копыльцов А.А., Нечитайленко Р.А.

Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

**ОБЕСПЕЧЕНИЕ ПОРОГОВОЙ БЕЗОПАСНОСТИ ОБРАБОТКИ
СЛАБО ФОРМАЛИЗОВАННОЙ ИНФОРМАЦИИ ПРИ РАСПРЕДЕЛЕННОМ
УПРАВЛЕНИИ С ЦЕЛЮ ПРИНЯТИЯ РЕШЕНИЙ**

Проблема сбора, хранения, передачи слабо формализованной информации, и на основе ее обработки - принятия решения, актуальна как никогда ранее, из-за бурного развития геоинформационных систем. Эта проблема имеет как теоретический, так и практический интерес (Журкин И.Г., Шайтура С.В., Орлов А.И., Петровский А.Б.). Одной из важных практических задач является задача обеспечения безопасности при передаче и обработке информации, с целью принятия решений при распределенном управлении. Важной временной характеристикой обеспечения безопасности является интервал времени, в течение которого собирается, передается и обрабатывается информация, перед принятием решения. Учитываются два важных аспекта подготовленности информации к абстрагированию: к назначенному времени обработки и достаточной полноте с надлежащей предварительной обработкой. Стратегическая подготовленность информации в психологии управления уравновешена и решена как «Квадрат Наполеона» (Теплов Б.М. Ум полководца. М: Наука, 1980), и в значительной степени опирается на интуитивные формы управления.

В связи с разнородностью принимаемых решений и различной степенью формализованности управленческой информации предполагается подход, допускающий единые формы обработки информации с широкими границами формализации, структурирования и связности. Одновременно учитывается сложившиеся формы предпочтения представления информации для различных предметных областей в военном деле, в бизнесе, в промышленности и науки.

Интенсивное развитие средств вычислительной техники, открыло возможность сочетать средства от интуитивных подходов и строгих алгоритмов и математических моделей, а в связи с развитием быстродействующих суперкомпьютеров и кластеров, оказалось возможным реализовать эти алгоритмические подходы и модели в реальном масштабе времени. Далее рассматривается разработанный алгоритм обработки слабо формализованной информации, состоящий из 7 шагов.

1. Информация поступает в модуль «Классификация», где, с помощью разработанных алгоритмов, осуществляется классификация поступающей информации на классы $K_1, \dots, K_N$. Параметры этих алгоритмов изменяются в процессе работы системы, т.е. это самообучающаяся система. На начальном этапе работы системы можно использовать либо обучающую выборку, либо случайным образом сгенерированное распределение поступающей информации между классами.

2. Информация, поступившая в каждый из классов, подвергается своей, присущей данному классу, свертке (алгоритму обработки информации). В итоге получается информация, обработанная специальным образом, присущим данному классу. В алгоритме используется понятие свертки f , суть которой состоит в следующем. Пусть N - достаточно большое число. Согласно исследованиям по методам и модели оценивания качества программного обеспечения. (Воробьев В.И., Копыльцов А.В., Пальчун Б.П., Юсупов Р.М.), можно взять некоторую выборку показателей с $N \geq 20$.

$P_1=0, P_2=1/N, P_3=2/N, \dots, P_{n+1}=1$, где P -

- весовые коэффициенты в формуле для расчета величины i -го показателя n -1-го порядка, представляющей собой взвешенную сумму K_j ($j=1, \dots, S_i$) и K_j принадлежит промежутку $[0,1]$ - нормированных числовых значений показателей n -го порядка, определяющих i -й показатель n -1-го порядка, S_j - число показателей n -го порядка, определяющих i -й показатель n -1-го порядка, f_i - формируется пакет условий, соотносящих номер показателя и степень его важности. Условие «показатель с номером m примерно такой же или чуть важнее показателя с номером n » означает, что P_m больше или равно P_n . Условие «показатель с номером m важнее показателя с номером n » означает, что P_m больше P_n . Условие «показатель с номером m существенно важнее показателя с номером n » означает, что существует, по крайней мере один P_q , такой что P_m больше P_q и P_q больше P_n .

Величины f_i определяются для всех $i = 1, \dots, F$ с учетом введенных отношений порядка между показателями (примерно такой же или чуть важнее, важнее, существенно важнее) и условий нормировки для P_j .

Поскольку S_i меньше $N+1$, то для каждого i количество f_i больше 1, т.е. для каждого показателя n -1 -го порядка получаем несколько значений f_i . Можно определить среднее значение f_i (которое равно f), дисперсию и среднеквадратичное отклонение. Процедура получения f называется сверткой.

3. После свертки осуществляется оценивание достоверности и безопасности обработанной информации в каждом классе, путем сравнения ее с ранее полученной информацией (предполагается, что есть хранилище ранее полученной информации). Если информация недостоверна или небезопасна (достоверность и безопасность ее ниже некоторых, заранее заданных для каждого класса уровней), то осуществляется возврат в начало алгоритма: информация подвергается повторной классификации и помещается в другой класс.

4. Установление связей между вновь полученной информацией в каждом классе и ранее полученной информацией, находящейся в хранилище. Если количество связей меньше некоторой, заранее заданной величины, специфичной для каждого класса, то осуществляется переход в п.1, в котором информация подвергается повторной классификации и помещается в другой класс.

5. Оценивание вероятности, с которой можно доверять полученной информации в каждом классе – устанавливается требуемый порог безопасности для этого класса. Если вероятность меньше некоторой, заранее заданной величины, специфичной для каждого класса, то осуществляется повторная классификация, возврат в начало алгоритма для отнесения к другому классу.

6. Поддержка принятия решений в каждом классе: генерируются рекомендации для каждого класса (что и когда нужно делать, если получена такая информация).

7. Сбор сгенерированных решений, синхронный по назначенному времени и назначенной полноте в заданном формате из всех классов. Анализ сгенерированных решений в классах и генерация на их основе новой совокупности решений в поддержку принятия решения. Вывод рекомендаций (что и когда нужно делать). Окончательное решение (выбрать какое-то решение из рекомендованных, или принять свое собственное решение) принимает человек.

Предлагаемый алгоритм можно использовать, как оболочку специфичны технических решений с рекомендуемыми инструментальными средствами в различных областях и условиях применения. Представляется интересным и обоснованным использование алгоритма в гибридных системах принятия решения и экспертного оценивания, предназначенных для широкого круга организационных задач, обладающих количественными и качественными данными. Вживление алгоритма в среду отлаженных технологических решений позволяет продуктивно использовать растущую производительность современных компьютеров и включается в распределенные коммуникационные системы принятия как автономных, так и взаимосвязанных решений, с соблюдением устанавливаемых порогов безопасности обрабатываемой информации.

Мартьянов А.Г.

**Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ**

Информационная безопасность предприятия включает в себя большой спектр различных направлений:

- это и современные средства защиты информации;
- информационная безопасность телекоммуникационных сетей;
- подготовка и переподготовка кадров в области обеспечения информационной безопасности;
- безопасные информационные технологии.



Рис. 1

Но в современном мире вопросы информационной безопасности необходимо представлять в более широком спектре. Представим себе на минуту, что все наши средства и системы,

разработанные и изготовленные по суперсовременным технологиям, остались без электрической энергии. Или часть лабораторий с уникальным оборудованием оказалась залита водой из-за прорыва сетей водоснабжения, или еще хуже – произошел большой пожар. Поэтому необходимо включать в понятие «информационная безопасность предприятия» и такие направления как:

- энергетическая безопасность и эффективность (развитие энергетической составляющей, включающей в себя, в том числе и аварийные источники электроэнергии – дизельные электростанции, аккумуляторы);
- все мероприятия по линии МЧС (пожарная безопасность, защита от стихийных бедствий, наводнений, чрезвычайных ситуаций);
- создание современных систем охраны и видеонаблюдения;
- кадровая политика в области инженерной безопасности.

Большое значение в этом имеет своевременное, качественное и в необходимых количествах обеспечение предприятия энергетическими ресурсами. Особое значение этот факт имеет в наши дни с целью безусловного выполнения требований Федерального закона № 261-ФЗ от 23.11.2009 г. «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации».

С этой целью на предприятии разработана и утверждена Генеральным директором «Программа в области энергосбережения и повышения энергетической эффективности ФГУП «НПО «Импульс».

Выполняется много мероприятий, основными из которых являются:

- полное оснащение предприятия приборами учета электрической энергии (смонтирована автоматизированная информационно-измерительная система коммерческого учета электроэнергии), воды и тепловой энергии (завершен монтаж и проводятся испытания узла учета тепла);
- предприятие является членом Саморегулируемой организации «Некоммерческое партнерство «Экспертиза энергоэффективности»;
- проведение постоянного анализа работы энергоемких систем, переход на менее энергоемкие или локальные системы (внедрена система плавного пуска двигателя вентсистемы, система канального кондиционирования, система поддержания температурного режима в помещениях стенда Главного конструктора и т.д.);
- проведение закупок современного, имеющего высокую энергетическую эффективность оборудования;
- ежегодный комплекс работ по обеспечению нормальных условий работы в зимний период;
- введение в эксплуатацию системы аварийного энергоснабжения с использованием дизель-генератора;
- другие мероприятия.

Заключен договор и проводятся работы по испытаниям высоковольтных электроустановок предприятия, реконструкции релейной защиты, ремонту кабельных линий, что позволяет обеспечить бесперебойную работу электрических сетей предприятия, повысит их надежность.

Проводится большой объем работ по модернизации лифтового оборудования.

Большое значение для нормальной работы современного станочного парка имеет обеспечение их качественным сжатым воздухом. С этой целью на предприятии сделаны две локальные системы сжатого воздуха, заключен договор на приобретение и монтаж мощного осушителя для улучшения качества сжатого воздуха.

Проведен комплекс работ и введены в эксплуатацию системы контроля доступа на центральной проходной, на стендах Главного конструктора, в отделе кадров; система видеонаблюдения. В результате полученного опыта эксплуатации в план техперевооружения предприятия внесен вопрос по улучшению характеристик и модернизации данных систем.

Проводится большой объем работ по улучшению условий труда, в том числе:

- аттестация рабочих мест;
- медицинский осмотр сотрудников предприятия;
- улучшение санитарно-бытовых условий (душевые, раздевалки, кондиционирование воздуха);
- ремонт помещений и освещения;
- другие мероприятия.

Для обеспечения безопасности выполнения работ ежегодно проводится обучение главного энергетика и его заместителей, электрогазосварщиков, инженеров лифтового хозяйства, с последующей сдачей экзаменов и получением удостоверений, проводится обучение специалистов в области энергоэффективности, охраны труда, экологической безопасности и др.

Учитывая различный характер работ, проводимый на предприятии, наличие пожароопасных помещений огромное значение имеет выполнение требований пожарной безопасности.

С целью выполнения требований Федерального закона № 123-ФЗ от 22.07.2008 г. «Технический регламент о требованиях пожарной безопасности» на предприятии разработана и зарегистрирована в отделе Государственного пожарного надзора ГУ «СУ ФПС № 50 МЧС России» «Декларация пожарной

безопасности» и выполнен расчет уровня обеспечения пожарной безопасности работников предприятия.

Для достижения требуемого, согласно Федерального закона, уровня обеспечения пожарной безопасности работников предприятия необходимо выполнить целый комплекс мероприятий. Учитывая большой объем финансирования, необходимый для реализации, реальность сроков выполнения работ, разработана и утверждена в мае 2010 года «Целевая программа по обеспечению противопожарной защиты ФГУП «НПО «Импульс» на период с 2010 по 2014 г.г.». В основном мероприятия, запланированные этой «Целевой программой...», в 2010-2011 г.г. выполнены.



Рис. 2

За два года удалось реализовать много мероприятий, основными из которых являются:

- разработаны проекты автоматической пожарной сигнализации (АПС) и системы оповещения и управления эвакуацией (СОУЭ) по основным корпусам;
- в высотном сооружении произведен монтаж системы подпора воздуха в лифтовых шахтах, системы дымоудаления, выполнена молниезащита корпуса, произведен ремонт и введена в эксплуатацию сплинкерная система пожаротушения, смонтирована автоматическая пожарная сигнализация и система оповещения и управления эвакуацией;
- завершаются работы по монтажу и вводу в строй АПС и СОУЭ в основных корпусах;
- разработаны «План-схемы эвакуации людей на случай пожара» во всех корпусах предприятия;
- закуплены и установлены необходимое количество огнетушителей и пожарных рукавов;
- проводится работа по оборудованию пожароопасных и наиболее значимых помещений современными и безопасными для людей установками автоматического пожаротушения (аэрозольное и порошковое пожаротушение);
- заменены более 1000 светильников, эксплуатирующихся без колпаков и рассеивателей;
- установлено необходимое количество противопожарных дверей в различных помещениях предприятия;
- более 200 человек прошли обучение по пожарно-техническому минимуму;
- ежегодно проводятся 4 противопожарные тренировки (две в составе самостоятельных структурных подразделений и две – объектовые);
- другие мероприятия.

Руководство предприятия делает все, чтобы в полном объеме реализовать «Целевую программу...», что позволит достигнуть требуемый уровень обеспечения пожарной безопасности людей (работников) предприятия.

После монтажа и ввода в эксплуатацию во всех корпусах системы оповещения и управления эвакуацией на ее основе будет реализована объектовая система оповещения по сигналам отдела по гражданской обороне и чрезвычайным ситуациям.

Без реализации этих направлений, модернизации инженерных сетей и оборудования невозможно обеспечить информационную безопасность предприятия.

Поэтому одна из крупных составляющих информационной безопасности предприятия – поддержание, совершенствование и развитие инженерной инфраструктуры предприятия, слаженная и четкая работа всех служб главного инженера.

Приходько М.А.

Россия, Москва, Московский государственный горный университет

МУЛЬТИАГЕНТНЫЕ ТЕХНОЛОГИИ В СИСТЕМАХ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

В наше время системы дистанционного обучения зачастую представляют собой большие территориально распределенные комплексы, неоднородные как по составу технических средств, так и используемому программному обеспечению. Задача исследования и моделирования таких систем традиционными методами становится все более трудной, и требует новых подходов для своего решения. Одним из таких подходов является динамично развивающаяся теория мультиагентных систем, позволяющая описать любую большую систему в виде множества интеллектуальных агентов различных видов, взаимодействующих между собой. Подобное описание помимо своей естественности имеет и другие преимущества: возможность описания и моделирования крупномасштабных динамических организаций компонент и групп компонент, возможность оценки свойств групп компонент, предсказания глобальных свойств системы в целом и ее поведения, и многие другие.

Одним из важнейших информационных процессов систем дистанционного обучения является воспроизводство информации, формирование, управление и контроль над информационными потоками, приводящими к перераспределению информации и, в том числе, ее выводу за пределы системы (конечным пользователям). Зачастую процесс перераспределения и доступа к информации, предоставляемой системой, регламентируется рядом правил, в том числе ограничивающих его на платной основе. Это приводит к необходимости создания различных механизмов контроля и ограничения доступа, а также ставит перед проблемой обнаружения нарушений введенных ограничений.

Наиболее распространенным базовым механизмом разграничения доступа является регистрация и последующая аутентификация пользователя в системе. Для незарегистрированных пользователей доступ ограничивается единообразно, а для зарегистрированных – согласно данных их профиля.

Вместе с тем, даже при наличии большого числа ограничений нередко наблюдается эффект несанкционированной «утечки информации», когда пользователь системы, пользуясь регламентированными возможностями и способами получения информации, в конечном итоге получает информацию, доступ к которой для него должен быть ограничен. Проиллюстрируем это явление на примере тестирования.

Представим себе пользователя системы дистанционного обучения, проходящего пробные тесты по некоторому предмету. Пусть общая база вопросов по предмету содержит 500 вопросов, а для пробного теста из общей базы случайным образом отбираются 10 вопросов. В качестве образовательного элемента в конце пробного теста пользователю отображается подробная расшифровка тестирования, содержащая информацию о правильных ответах на вопросы, в которых были допущены ошибки.

Предполагается, что пользователь системы будет использовать пробные тестирования с целью проверки своих знаний, однако существует способ эксплуатации данной функции системы, позволяющий узнать правильный ответ на любой заранее известный вопрос. Для этого достаточно пройти большое число тестов, которое позволит сформировать список всех правильных ответов на вопросы теста. Таким образом, используя регламентированную возможность проверить свои знания, пользователь системы получает доступ к правильным ответам на вопросы по предмету, обладать которыми он, в общем случае, не должен.

Анализ описанной проблемы раскрытия формулировок правильных ответов на вопросы тестирования [2] показывает, что эффективное противодействие несанкционированной утечке информации возможно только при создании многоуровневой интеллектуальной системы фильтрации информации и ограничения прав доступа к ней. В частности, в АСИКЗ «Аргус-М» были реализованы следующие ограничительные механизмы:

- механизм защиты от раскрытия точных формулировок правильных ответов;
- механизм защиты от раскрытия информации о правильности/неправильности варианта ответа;
- механизм защиты от раскрытия набора ответов, гарантирующих определенную оценку;

- механизм защиты от возможного изменения варианта ответа для вопроса, на который ответ уже был дан;
- механизм защиты от нерегламентированной навигации по системе во время прохождения аттестации;
- механизм защиты результатов контроля знаний от попыток несанкционированного изменения без использования системы (т. е. от «взлома» данных системы злоумышленником извне).

Вместе с тем опыт эксплуатации автоматизированной обучающей системы «Аргус-М» [3] убеждает, что традиционных средств противодействия несанкционированной утечке информации в инфокоммуникационных системах недостаточно. Любая возможность получить санкционированный доступ к информации потенциально является источником возникновения ее несанкционированной утечки. А с учетом масштабов современных систем дистанционного обучения само обнаружение утечки информации становится более сложной и важной задачей, чем ее блокирование. Поэтому налицо потребность в разработке новых систем контроля над информационными потоками, призванных не только ограничить доступ к тем или иным данным, но и обнаружить изменения в информационных потоках и появление несанкционированных утечек.

Базисом создания таких систем контроля над информационными потоками инфокоммуникационных систем могут стать мультиагентные системы, построенные на основе интеллектуальных агентов, анализирующих в режиме реального времени информационные потоки. Причем первостепенной задачей данных агентов должно быть не ограничение доступа к информации, а выявление возникновения несанкционированных утечек информации.

Как видно из примера, возникновение таких утечек обусловлено гораздо большим упорядочиванием некоторых действий пользователя, которые в общем случае носят случайный характер. Поэтому критерием выявления несанкционированных утечек информации могут стать энтропийные характеристики системы, описывающие, например, неупорядоченность действий пользователя или функционирования определенных фрагментов инфокоммуникационной системы. Сигналом к активации дополнительных ограничений или блокированию подозрительной активности является снижение энтропии выбранных характеристик, говорящее о росте упорядоченности опасных действий.

Успешное функционирование подобной системы зависит от двух основных факторов. Во-первых, необходимо правильно построить модель мультиагентной системы, разместив интеллектуальные агенты соответствующих типов во всех ключевых узлах инфокоммуникационной системы, участвующих в обработке информации, утечку которой необходимо предотвратить. Во-вторых, необходимо правильно выбрать характеристики системы, энтропия которых будет использоваться как индикатор несанкционированной утечки информации.

Сама же система должна решать три основные задачи:

- обнаружение возникновения несанкционированной утечки информации;
- выявление причины и адресата несанкционированной утечки информации;
- блокирование нежелательной деятельности с целью предотвращения утечки информации.

Особо обратим внимание, что подобная система не просто состоит из большого числа однотипных агентов, а включает в себя большое число интеллектуальных агентов разных типов, соответствующих разным уровням абстракции (обработки) защищаемой информации. Это позволяет контролировать информацию на всех уровнях, которые могут стать источником утечки, а также использовать большое число различных энтропийных характеристик, повышающих надежность системы защиты. Кроме того, разнотипность агентов и используемых «сигнальных» характеристик затрудняет адаптацию опасных процессов с целью маскировки несанкционированной утечки информации регламентированными действиями. Проиллюстрируем это на ранее рассмотренном примере тестирования.

Информация о правильности выбранного ответа, а также правильном варианте ответа, предоставляется пользователю АСИКЗ «Аргус-М» в нескольких случаях:

- в подробной расшифровке результатов тестирования;
- в сводной таблице результатов тестирования на странице тестирования;
- в сводной таблице результатов тестирования на странице пользователя.

Также информация о возможных вариантах ответа предоставляется пользователю непосредственно в момент прохождения теста. Таким образом, налицо необходимость создания трехуровневой системы, состоящей из интеллектуальных агентов трех типов, собирающих и анализирующих информацию об активности пользователя на уровне прохождения теста, просмотра сводных результатов и просмотра подробной расшифровки результатов.

Данные интеллектуальные агенты должны уметь общаться друг с другом для обмена информацией об активности пользователя. Они также должны уметь анализировать активность многих пользователей с целью выявления корреляций в их действиях следующих типов:

- один человек под видом нескольких пользователей инициирует несанкционированную утечку информации;

– группа пользователей скоординированными действиями инициирует несанкционированную утечку информации.

Наличие нескольких разнотипных агентов усложняет задачу маскировки утечки информации регламентированной деятельностью, т.к. снижение активности пользователя на одном из уровней ведет к повышению активности на другом с целью добычи необходимой информации. А это, в свою очередь, позволяет варьировать качества интеллектуальных агентов, повышая в целом чувствительность системы.

Сформулированная проблема несанкционированной утечки информации открывает новую увлекательную область применения мультиагентных систем в современных системах дистанционного обучения. Требования к мультиагентным системам обнаружения и предотвращения несанкционированных утечек информации закладывают базис их создания, одновременно подсказывая направление развития, заключающееся в поиске и формализации энтропийных характеристик систем дистанционного обучения, которые могут служить индикаторами несанкционированных утечек информации. А область интерактивного тестирования предлагает поле для практической реализации и отработки решений по созданию такой системы.

СПИСОК ЛИТЕРАТУРЫ

1. Приходько М. А. Требования к системам интерактивного контроля знаний в традиционных учебных заведениях (вузах) на примере АСИКЗ «Аргус-М». Международная научно-методическая конференция «Информатизация образования-2009». Июнь 2009. Материалы конференции.

2. Приходько М. А. Автоматизированная обучающая система «Аргус-М» - первый свободный веб-сервис дистанционного обучения. Пятый международный научный конгресс "Роль бизнеса в трансформации российского общества". Март 2010. Сборник тезисов доклада.

Расторгуев В.Я., Виноградов А.А.

**Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
УСИЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРИТИЧЕСКИХ СИСТЕМАХ
НЕПРЕРЫВНОГО ФУНКЦИОНИРОВАНИЯ ПУТЕМ ВИРТУАЛИЗАЦИИ ЭЛЕМЕНТОВ
ИХ СИСТЕМ УПРАВЛЕНИЯ**

Термин «виртуализация», использованный в названии доклада, требует пояснения ввиду многозначности. В самом общем определении под глаголом «виртуализировать» понимают действие, состоящее в том, чтобы взять нечто, имеющее одну форму, и заставить его казаться имеющим другую форму.

При таком определении близким родственником (а м.б. даже синонимом) виртуализации может показаться на первый взгляд термин «моделирование», намного опередивший по времени появления термин виртуализация. Однако между этими понятиями есть различия.

Моделирование применяют для построения идеализированного образа (модели) некоторого объекта с основной целью удешевления получения прогнозов поведения объекта и сокращения таким образом рисков потери работоспособности объекта в результате экспериментов с ним. Модель всегда связана с моделируемым объектом принципом подобия, является средством исследования моделируемого объекта и не становится самостоятельным объектом эксплуатации.

Виртуализация допускает построение новой производной формы представления для некоторой первичной формы с необязательным использованием принципа подобия. Эта новая форма далее иногда становится самостоятельным объектом со своей историей эволюции, часто отличающейся от истории эволюции первичной формы. Для подтверждения этого достаточно вспомнить, например, кажущийся парадоксальным термин «виртуальная реальность».

Назовем общие направления виртуализации, используемые в компьютерной инженерии. Здесь виртуализировать такой объект, как компьютер, означает заставить компьютер казаться сразу несколькими компьютерами, фрагментом компьютерной сети или же компьютером совершенно иного типа (архитектуры). Виртуализацией м.б. названа также ситуация, когда несколько компьютеров представляются как один отдельный компьютер. Обычно результат этого действия называют серверным кластером.

Отметим отдельно также и то, что виртуализация дается не бесплатно, а иногда требует заметных «накладных» расходов, снижающих производительность Виртуальных Процессоров (ВП) на 2-3 порядка относительно производительности Физических Процессоров (ФП), на которых они развернуты.

На идеях интернета и виртуализации элементов глобальных компьютерных сетей специалистами таких мировых фирм-разработчиков виртуальных сред, как, например: VMWare, Xen, Parallel, Cisco, Citrix и т.д. построена современная и перспективная концепция «облачных» сервисов и вычислений. Использование этой концепции обеспечивает клиентам непрерывно и надежно функционирующую вычислительно-информационную среду, обладающую уникальными характеристиками в части мобильности точек базирования сервисов на ВП, ВП на ФП и, как следствие, их надежности и живучести. Разумеется, это оказывается возможным при одновременном введении мер противодействия жестким условиям эксплуатации ФП в Центрах

Обработки Данных (ЦОД), которые из-за своей жесткости представляют угрозу для работоспособности как ФП, так и ЦОД.

Назовем некоторые полезные следствия использования идей виртуализации, на основе которых оказывается возможным в вычислительных сетях:

- Произвести консолидацию различных сервисов, задействовав целиком ФП, и, балансируя при необходимости виртуальные сервисы между ФП, поднять КПД используемого оборудования при одновременном сокращении энергопотребления.

- Перемещать при необходимости ВП с ФП на ФП без их остановки, увеличивая доступность сервисов для конечных пользователей.

- Не привязывая сервисы, размещенные на ВП, к конкретному ФП, свободно перемещать их между ФП с целью технического обслуживания освобождаемых ФП без остановки вычислений. При этом в одном вычислительном пуле оказывается возможно совмещать вычислительное оборудование разных производителей.

- Seriously упростить обслуживание гостевых Операционных Систем (ОС) внутри ВП, т.к. при этом исчезает необходимость физических манипуляций с ФП и появляется еще один уровень удаленного контроля над сервисами со стороны администраторов.

- Значительно сократить количество проблем, связанных с неисправностью ФП и дефектами драйверов его отдельных устройств. Дело в том, что в относительно консервативной виртуальной среде ОС работают со специальными драйверами виртуальной периферии, предоставляемыми квалифицированными разработчиками виртуальной среды. Эти драйверы, как правило, лучше написаны, отлажены, протестированы и апробированы. На время устранения неисправности ФП ОС с активными приложениями м.б. перемещена вместе с ВП на исправный ФП. Современные технологии позволяют делать это автоматически и относительно быстро.

Из сказанного следует, что идея виртуализации вычислительного оборудования может в перспективе стать основой увеличения информационной безопасности в информационных системах продолжительного и непрерывного функционирования и, что особенно ценно, в Системах Управления Критическими Системами Непрерывного Функционирования (СУ КСНФ) за счет практически полного устранения угроз физического и морального старения оборудования из-за эффектов:

- отсутствия отказов ВП, т.к. ВП принципиально физически не стареет,

- устранения морального старения ВП, т.к. темп морального старения ВП никак не связан с темпом морального старения ФП. Это позволяет, если необходимо, исключить моральное старение ФП путем своевременной его модернизации, одновременно законсервировать на долгое время среду выполнения ответственных критических приложений (ВП, гостевую ОС, собственно приложений и т.д.), и, проведя их глубокую отработку, тестирование и опытную апробацию в законсервированной виртуальной среде, обеспечить, таким образом, безопасную эксплуатацию этих приложений.

Однако, следует признать то, что в настоящее время виртуализация практически не используется в СУ КСНФ и этому, по нашему мнению, способствуют, как минимум, три причины:

- «новизна» метода виртуализации для сообщества разработчиков различных СУ КСНФ,

- необходимость наличия запаса производительности ФП в 2-3 порядка из-за больших накладных расходов на поддержку ВП, часто отсутствующего в ФП из состава СУ КСНФ,

- преимущественное использование в СУ КСНФ специализированных процессоров двойного назначения с уникальной архитектурой, в некоммерческом отечественном исполнении, устойчивых к жестким условиям эксплуатации (термическим, механическим, электромагнитным, радиационным и т.д. воздействиям), но, к сожалению, не обладающих достаточной для эффективной виртуализации производительностью и оперативной памятью. Эти процессоры сегодня, как правило, находятся вне зоны коммерческих интересов мировых фирм-разработчиков программных средств виртуализации.

Первая причина имеет временный характер и, очевидно, м.б. устранена. Влияние второй причины в последние годы заметно сокращается за счет освоения отечественными фирмами новых производительных элементных баз и появлении на рынке специализированной вычислительной техники двойного назначения с рабочей частотой ~100-1000 МГц. По поводу возможности устранения третьей причины, путем привлечения внимания мировых фирм-разработчиков виртуальных сред к учету особенностей вычислительной техники двойного назначения, применяемой в СУ КСНФ у нас есть сильные сомнения в успехе из-за узости рынка специализированной вычислительной техники двойного назначения в сравнении с коммерческой. Поэтому поиск способа виртуализации элементов СУ КСНФ, работающих без прямой опоры на решения мировых фирм-разработчиков виртуальных сред, является актуальной задачей, возможные подходы к решению которой представлены ниже.

Любой из многочисленных способов виртуализации, достаточно полный перечень которых приведен, например, в [1, 2], предполагает такую модель вычислительного процесса, в которой приложение работает в многоуровневой операционной среде, образованной несколькими ОС,

развернутыми на ФП (см. рис. 1). Работа приложения состоит в последовательной (в соответствии с алгоритмом приложения) выдаче запросов либо ФП (команды ФП), либо какой-нибудь ОС (запрос на системное действие). На рис. 1 пунктиром выделены условно-возможные запросы ограниченного применения. Если алгоритмы приложений с номерами от 1 до М, размещены на М экземплярах ВП, то на каждом из ВП м.б. создана своя операционная среда, а рис. 1, соответственно м.б. мысленно рекурсивно расширен, если приложение само является ОС или программно реализует логику ВП некоторой физической или абстрактной архитектуры. Рассматривая подробнее рис. 1 увидим, что:

- каждое приложение выполняется в своем стеке операционных систем, в основном выдает системные запросы к операционной системе, находящейся на вершине своего стека и ограниченно может (если это не запрещено особо) выдавать системные запросы к любой из операционных систем своего стека. Кроме того, разумеется, возможна прямая выдача команд для ФП;
- стеки операционных систем различных приложений могут иметь различный состав уровней и глубину.

В качестве типового решения для построения среды виртуализации, состоящей из нескольких ВП, на отдельном ФП и для последующего развертывания на каждом из ВП своей собственной и независимой от остальных (если это необходимо) системы вычислений достаточно воспользоваться операционной средой из двух уровней, изображенной на рис. 2. Очевидно, что эта двухуровневая операционная среда является частным случаем многоуровневой операционной среды, приведенной на рис. 1. Точнее говоря, она м.б. получена поэтапно путем:

- Выбора относительно функционально-мощной первичной мультисреды (обычно мультизадачной или мультипроцессовой ОС), в роли которой часто используют Linux или Windows, хотя здесь могут быть и другие варианты.
- Выбора наиболее подходящей для последующих этапов и поддерживаемой в первичной мультисреде единицы многозадачности (задача, процесс, поток и т.д.).
- Построения на основе выбранной единицы многозадачности некоторого ВП путем создания отдельного приложения-эмулятора ВП, программно реализующего логику работы архитектуры либо некоторого физического (intel-x86, mips, arm, sparc и т.д.), либо абстрактного (java-ВП, shell-ВП, linux-ВП, windows-ВП и т.д.) процессора.
- Циклического развертывания на каждом из ВП_к вторичной мультисреды_к для к из диапазона $0 < k < m+1$.

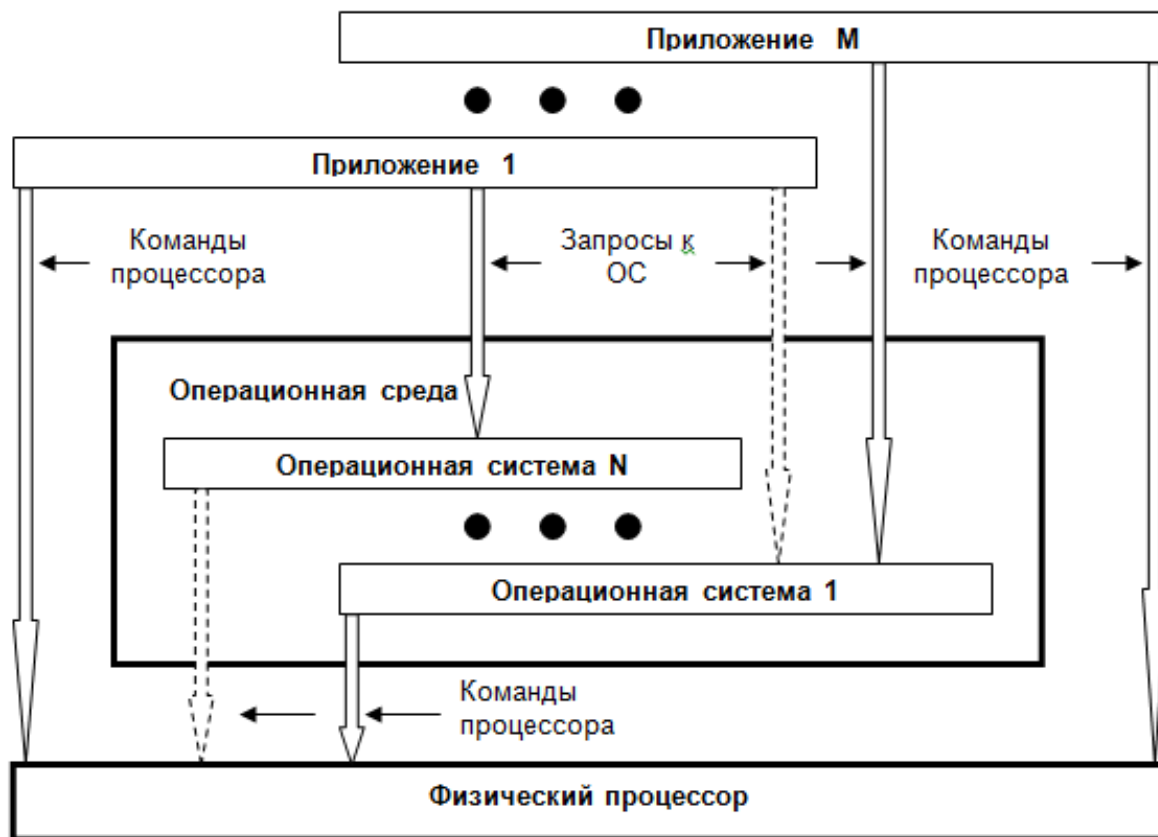


Рис. 1. Состав многоуровневой операционной среды. Общий случай

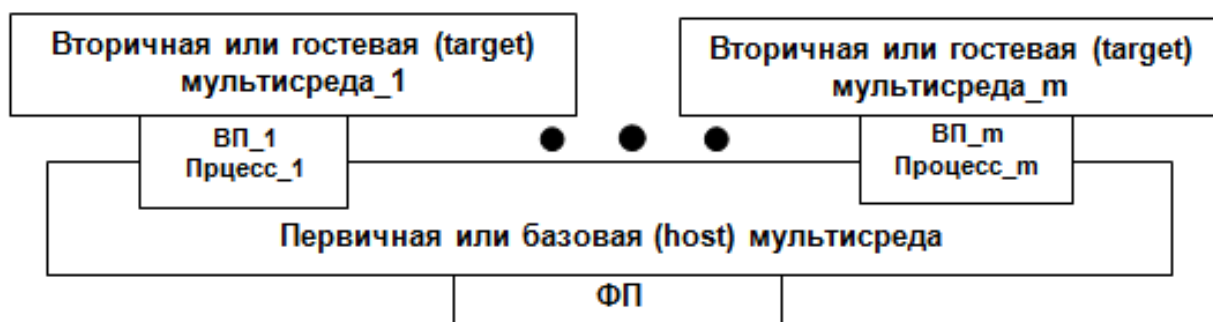


Рис. 2. Типовой состав операционной среды для построения системы из нескольких ВП

На практике этапы 1-3 выполняются фирмами-разработчиками виртуальных сред с включением полученных результатов в продаваемые ими пакеты средств виртуализации и только этап 4 выполняется покупателями-пользователями. В подавляющем числе случаев при выполнении этапа 3 фирмы-разработчики виртуальных сред предпочитают использовать архитектуры некоторых физических, а не абстрактных процессоров, если не считать особый случай с java-ВП. Более того, из всех принципиально-возможных архитектур физических процессоров, видимо, по коммерческим соображениям эти фирмы выбирают только архитектуру intel-x86 (как наиболее распространенную), игнорируя, например, RISC-архитектуры двойного назначения (mips, arm и т.д.), часто используемые именно в СУ КСНФ, что препятствует проникновению идей виртуализации в СУ КСНФ. Устранить это препятствие теоретически можно, выполнив все этапы с 1 по 4 самостоятельно, не прибегая к услугам фирм-разработчиков виртуальных сред, и выполняя этап 3 одним из двух способов:

- построением ВП, эмулирующего ФП, с необходимой физической архитектурой,
- использованием ВП с абстрактной архитектурой адекватной одновременно как первичной, так и вторичной мультисредам (например: linux-ВП, windows-ВП и т.д.).

Первый способ практически нереализуем, т.к. для получения качественного результата требует недостижимо высокой в среде программистов-прикладников квалификации, которой обладают только профессиональные системные программисты-разработчики виртуальных сред вообще и ВП в частности. Второй способ м.б. применен как указано выше при выполнении двух условий:

- вхождении ВП с выбранной абстрактной архитектурой в список ВП, поддерживаемых в первичной мультисреде,
- возможности размещения необходимой вторичной мультисреды на ВП с выбранной абстрактной архитектурой.

Первое условие может быть автоматически выполнено в случае правильного выбора функционально-мощной первичной мультисреды.

Второй условие требует наличия у вторичной мультисреды свойства мобильности, т.е. способности параметрической адаптации к ВП выбранной архитектуры, выполняемой методом портирования. Можно говорить, что и это условие тоже, как правило, автоматически выполняется, если учесть то, что в СУ КСНФ в качестве вторичной мультисреды часто используют специализированные мобильные операционные системы двойного назначения, например: VxWorks, RTEMS и т.п.

На рис. 3 приведен пример двухуровневой операционной среды, демонстрирующий один из возможных способов самостоятельного построения виртуальной среды, состоящей из:

- первичной мультисреды – ОС Linux, формирующей набор из N экземпляров linux_ВП, каждый из которых, будучи linux-процессом, одновременно является логическим процессором последовательного действия, работающим квази-параллельно и независимо от других linux_ВП и представляющим собой по сути процессор Фон Неймана с системой команд с повышенной семантикой, образованной из объединения команд ФП и набора системных вызовов ядра ОС Linux,
- вторичной мультисреды – ОС RTEMS, портированной в части пакета сопряжения с аппаратурой (т.е. Board Support Package) на программно-аппаратную платформу, формирующую linux_ВП, которая в свою очередь состоит из ФП и ОС Linux.

В заключение отметим, что, с нашей точки зрения, несмотря на низкую степень проникновения идей виртуализации в область СУ КСНФ в настоящее время, рост этой степени в будущем неизбежен после снятия ресурсных аппаратных ограничений ввиду тех очевидных достоинств и перспективности самой идеи виртуализации, которые указаны выше.

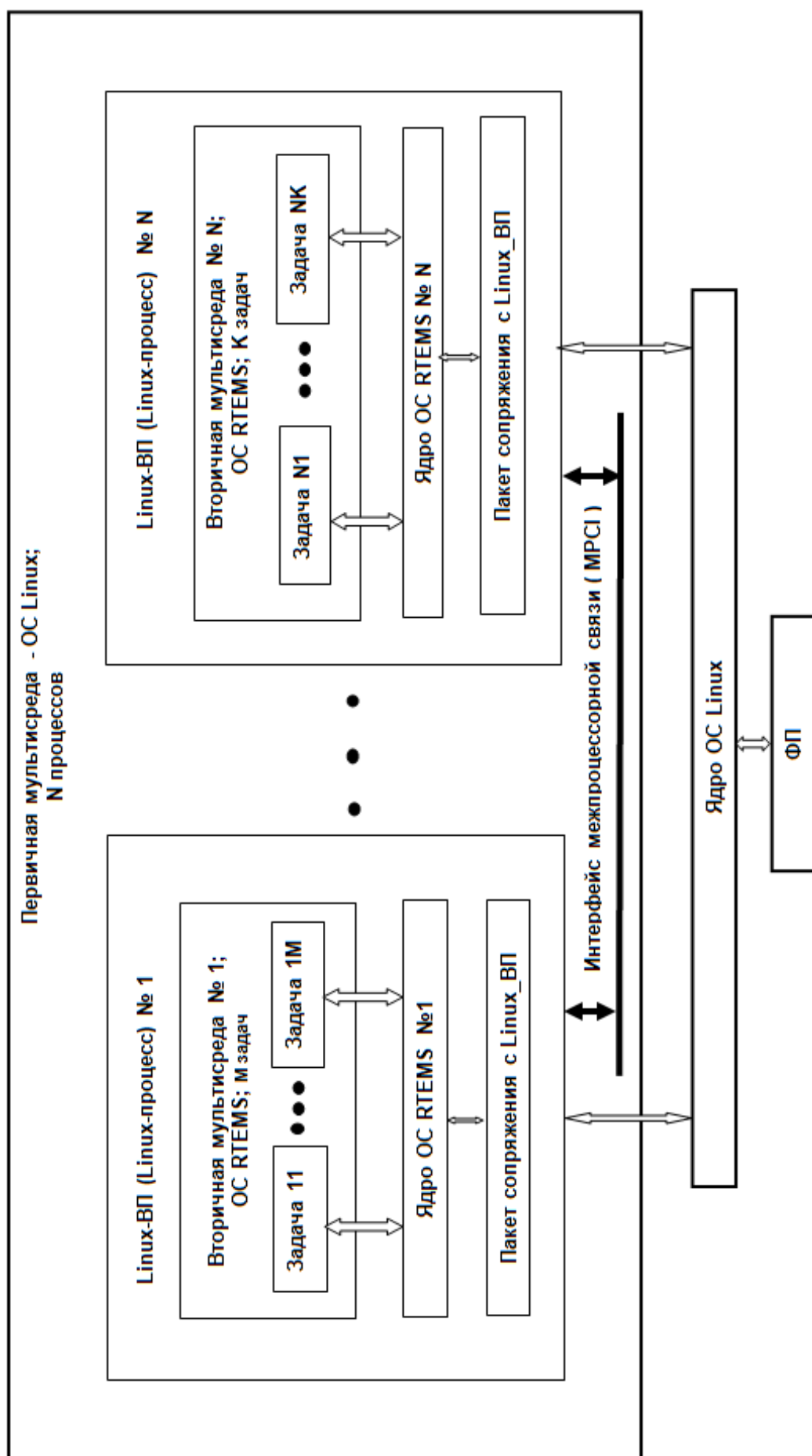


Рис. 3. Пример двухуровневой операционной среды, состоящей из ОС Linux и ОС RTEMS

СПИСОК ЛИТЕРАТУРЫ

1. M. Tim Jones. Virtual Linux. An overview of virtualization methods, architectures, and implementations: http://www.ibm.com/developerworks/linux/library/l-linuxvirt/index.html?S_TACT=105AGX99&S_CMP=CP.
2. Тормасов А. Виртуализация операционных систем. Электронный журнал «Открытые системы» № 1, 2002 г.

Тимохин А.П., Бочкарёв В.В.

Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»

**МЕТОДЫ ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ
КОНСТРУКЦИИ АППАРАТУРЫ ДЛЯ СИСТЕМ АВТОМАТИЗИРОВАННОГО
УПРАВЛЕНИЯ И ДВОЙНОГО НАЗНАЧЕНИЯ**

Конструктивно составные части аппаратуры представляют собой унифицированные базовые несущие конструкции (БНК) трех уровней разукрупнения. Координационные размеры уровней разукрупнения выбраны согласно ГОСТ Р 51623-2000 «Конструкции базовые несущие РЭС. Система построения и координационные размеры».

Аппаратура предусматривает поузловое экранирование электрических и магнитных полей. Экранирующие корпуса стоек и приборов аппаратуры представляют собой замкнутые объемы со съемными крышками.

1. Конструкция прибора

Корпус прибора изготовлен из алюминиевого сплава литьем (с последующим фрезерованием) или фрезерованием. Верхнее и нижнее основание выполнены в виде радиаторов с ребрами для отвода тепла от модулей.

Соединение боковых стенок, верхнего и нижнего оснований производится с применением токопроводящего клея НТК ОСТ 107.460007.004-91 для обеспечения электрического контакта частей корпуса.

Боковые стенки корпуса прибора имеют съемные крышки для свободного доступа к соединителям модуля питания (МПН), фильтра питания и монтажной части входных (выходных) соединителей прибора. После настройки прибора крышки устанавливаются на токопроводящую эмаль ХС-928 и герметизируются по контуру герметиком УП-5-201 ТУ6-05-246-80.

Толщина корпуса прибора выбрана и достаточна для защиты информации, содержащейся в аппаратуре, от воздействия внешних воздействующих факторов (ВВФ) в соответствии с условиями эксплуатации.

Сзади (со стороны пайки объединительной платы) корпус прибора закрыт корпусом МПН, который устанавливается на фланец прибора. Уплотнение для обеспечения герметичности и экранирования происходит с помощью электропроводного резинового шнура.

На лицевой панели прибора устанавливаются внешние соединители типа СНЦ127 АШДК.434410.082ТУ.

Площадь поверхности для установки соединителей 280×100 мм.

Фланцы внешних соединителей расположены снаружи и имеют гальванический контакт с корпусом прибора.

На лицевой панели прибора устанавливается съемная пломбируемая крышка, закрывающая доступ к модулям. Для обеспечения герметичности и экранирования крышка устанавливается через резиновый электропроводный шнур.

2. Конструкция стойки

Основой конструктивного построения стойки являются приборные шкафы, которые после установки в них каркасов блочных и проведения монтажа преобразуются в аппаратные стройки.

Шкаф представляет собой конструкцию с переменным количеством этажей, в которых размещаются каркасы блочные (КБ).

Основной модификацией шкафа (стойки) является конструкция, в которой на пяти этажах размещается 5 каркасов блочных.

Шкаф представляет собой штампованный сварной каркас, в котором размещаются элементы конструкции для установки и крепления необходимого количества КБ.

К нижней и верхней части шкафа болтами крепятся верхние и нижние основания. В верхнем основании расположена коробка распределительная (КР) с выходными соединителями и воздухопроводные окна для подключения стойки к системе вентиляции.

В нижнем и верхнем основаниях размещаются заборные окна системы охлаждения и устройство регулировки (заслонки) системы вентиляции стойки.

Вентиляционные окна закрыты сеткой с размером ячейки 3×3 мм. Сетка покрыта электропроводным покрытием.

Спереди шкафа предусмотрена экранированная металлическая дверь, закрывающая в рабочем состоянии устанавливаемые в стойку КБ с модулями.

Дверь шкафа оснащена концевым выключателем, который при открывании выдает сигнал в систему диспетчеризации.

Двери, съемные крышки стоек, закрывающие аппаратуру содержащую информацию, имеют места пломбирования заводом-изготовителем и службой эксплуатации, ограничивающих доступ к составным частям аппаратуры посторонним лицам.

Материал, из которого изготовлены верхнее, нижнее основание и шкаф стойки – сталь, толщиной 1,5 мм. Толщина стали достаточна для защиты информации содержащейся в аппаратуре стойки от воздействия ВВФ в соответствии с условиями эксплуатации.

Материалы из которых изготовлены стойки выбраны в соответствии с «Перечнем материалов и покрытий разрешенных к применению в аппаратуре изделий разрабатываемых НПО «Импульс». Аппаратура стойки, содержащая информацию защищена от воздействия пожара и взрывов.

Конструктивные решения принятые при проектировании аппаратуры обеспечивают экранирование корпуса стойки с целью обеспечения информационной безопасности.

Черкесов Г.Н.

**Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
ОЦЕНКА ЖИВУЧЕСТИ И ОТКАЗОБЕЗОПАСНОСТИ МАЖОРИРОВАННОЙ ПАМЯТИ
С КЛАСТЕРНОЙ СТРУКТУРОЙ**

Введение. Для повышения надежности и достоверности функционирования оперативной памяти в системах связи, системах управления, бортовых вычислительных системах самолетов, судов, космических аппаратов и других объектов с высокими требованиями к отказобезопасности применяют резервирование типа параллельного мажорирования по схеме «два из трех». При кластерной структуре памяти возможно мажорирование на уровне одного кластера.

Таким образом, структурно память может быть представлена как последовательное соединение мажорированных групп из трех кластеров. При этом процедура голосования может быть проведена как в процессоре, так и в специализированных мажорирующих элементах (МЭ). В необслуживаемых вычислителях возможно накопление отказов отдельных кластеров, возникающих вследствие естественных процессов или в результате внешнего воздействия (например, потоков космических частиц), без потери работоспособности системы. В связи с этим возникает вопрос о том, каков риск потери работоспособности памяти при заданном числе отказавших элементов (кластеров). Это зависит от распределения отказавших элементов по полю памяти.

Мерой риска могут быть условные вероятностные показатели при известном числе пораженных кластеров во всем поле памяти. Они являются показателями живучести (отказоустойчивости). С учетом однородности структуры памяти они могут быть определены с помощью комбинаторных методов. Представляют интерес показатели уровня деградации структуры, такие как вероятность неработоспособности некоторого числа групп при условии неисправности заданного количества структурных элементов (кластеров); вероятность потери работоспособности не более заданного количества групп.

Для обеспечения отказобезопасности и живучести могут использоваться следующие методы: процедуры периодической принудительной регенерации, регулирование размера кластеров, использование резервных кластерных групп, помехоустойчивое кодирование с коррекцией ошибок. При увеличении числа резервных групп вероятность можно сколь угодно близко приблизить к единице. Поэтому важно решить задачу о таком значении числа резервных групп кластеров, который обеспечит практически гарантированный уровень вероятности сохранения важной для системы информации (программ и данных). Достоинство этих показателей состоит в том, что этот уровень гарантируется при любых показателях надежности элементов памяти. Иначе говоря, для принятия решения об уровне резервирования в памяти вообще не надо знать статистики отказов памяти. Если источником поражения кластеров являются внутренние причины, приводящие к отказам ячеек памяти в кластерах или искажению информации в оперативной памяти вследствие сбоев, то необходимо оценивать показатели отказобезопасности [1], учитывающие потоки отказов и сбоев.

При достаточно высокой интенсивности поражения кластеров и (или) длительной эксплуатации изделий в условиях невозможности восстановления деградированной структуры обеспечение высоких показателей надежности и отказобезопасности достигается с помощью определённого сочетания различных методов структурного, информационного и функционального резервирования.

В процессе проектирования резервированной памяти уже на ранних стадиях надо установить приемлемые параметры системы памяти: число групп, размеры кластера, объем резервной части емкости памяти, а также оценить эффект от применения гибкой адресации, помехоустойчивого кодирования и возможности перезагрузки файлов в работоспособную часть памяти. При использовании схем мажорирования важно определить порог голосования в схеме « m из n ». Для оптимального выбора параметров требуется количественное обоснование с помощью количественных критериев.

При назначенном ресурсе эксплуатации возникает проблема оценки фактического состояния деградированной структуры с целью принятия решения по критерию приемлемого риска о продлении или сокращении срока эксплуатации. Эти вопросы излагаются в основной части доклада.

1. Постановка задачи и показатели живучести и отказобезопасности

Рассматривается оперативная память, состоящая из трех комплектов (линеек) кластеров, трех магистралей (М) и трех полноразрядных мажорирующих элементов (МЭ). Чтение осуществляется с трёх комплектов одновременно и синхронно по запросу процессора или другого смежного устройства. Запись осуществляется по требованию процессора или других смежных устройств, а также по требованию системы восстановления для повышения достоверности и защиты от сбоев. С целью упорядочения анализа будем различать четыре основных режима функционирования: режим чтения (РЧ); режим записи (РЗ); режим диагностирования (РД); режим повышения достоверности (РПД).

Режим РД используется для установления комплекта, данные которого отличаются от данных двух других комплектов. Режим РПД включается либо по сигналу РД, либо по инициативе контроллера периодически. В первом случае делается попытка устранить ошибку, если она произошла вследствие сбоя. При многократной неудаче делается вывод, что в кластере произошел устойчивый отказ и кластер вносится в регистр ошибок. Во втором случае реализуется профилактическая мера по устранению сбойных ошибок. Она состоит из последовательных действий: чтение – запись – чтение. Если при первом чтении есть одно несовпадение, то далее следует запись и чтение. Далее как в первом случае. В режиме записи может три ситуации: в три комплекта записывается одна и та же информация (три МЭ исправны и есть совпадение не менее двух входных данных); запись не производится из-за отсутствия двух одинаковых данных; запись производится только в два комплекта (один МЭ не исправен).

Обнаружение отказов осуществляется: в кластерах памяти путем использования режимов РД и РПД; в контроллерах памяти с помощью встроенных средств аппаратного контроля и режимов РД и РПД; в МЭ путем сравнения выходов МЭ: при работоспособных МЭ их выходы должны совпадать. Повышение достоверности осуществляется путем мажорирования; путем исправления сбойных ошибок в кластерах в режиме РПД; путем применения корректирующих кодов (например, кодов Хэмминга).

Для расчета показателей надёжности, отказоустойчивости (живучести) и достоверности необходимо знать следующие исходные данные: количество кластеров в памяти; количество БИС в одном кластере; состояние работоспособности каждого кластера (в каждом из трех комплектов); интенсивность отказов одного БИС памяти; интенсивность отказов контроллера и мажоритарного элемента; интенсивность сбоев в памяти; нормативная длительность функционирования.

Для анализа живучести и отказобезопасности и последующего выбора параметров системы памяти необходимо найти расчетные формулы для трех групп показателей. Условные показатели живучести:

– вероятность $Q^*(i)nmk$ того, что в системе из n последовательно соединённых мажорированных групп при условии неисправности k элементов будет неработоспособно ровно m групп, причём в i группах из m будут поражены все три элемента, а $m-i$ группах – только два элемента;

– вероятность Q^*nmk того, что в системе из n последовательно соединённых групп будет неработоспособно ровно m групп при условии неисправности k элементов, очевидно, что:

$$Q_{nmk}^* = \sum_{i=0}^m Q_{nmk}^{*(i)}, \quad (1)$$

вероятность Q_{nmk} того, что при условии неисправности k элементов в системе будет неработоспособно не более m групп; очевидно, что

$$Q_{nmk} = \sum_{j=0}^m Q_{njm}^* = \sum_{j=0}^m \sum_{i=0}^m Q_{njm}^{*(i)}. \quad (2)$$

Показатели надёжности при нулевой начальной деградации: вероятность $P_{nmk}^{*(i)}(t)$ того, что в момент времени t в системе из n групп будет неработоспособно ровно m групп при наличии k неисправных элементов. Причём в i группах из m поражены все три элемента. Известно, что в начальный момент времени все $3n$ элементов структуры памяти (кластеров) работоспособны. Безусловная вероятность связана с условной вероятностью соотношением:

$$P_{nmk}^{*(i)}(t) = Q_{nmk}^{*(i)} P_k(t), \quad (3)$$

где $P_k(t) = P(X(t)=k)$ – вероятность того, что за время t будут поражены по тем или иным причинам ровно k элементов; иначе можно определить вероятность (3) как вероятность достижения к моменту t уровня деградации (n, m, k, i) ;

– вероятность $P^*nmk(t)$ того, что в момент времени t будут поражены m групп из n при наличии ровно k неисправных элементов и при условии, что в начальный момент все $3n$ элементов памяти работоспособны; очевидно, что

$$P_{nmk}^*(t) = \sum_{i=0}^m P_{nmk}^{*(i)}(t) = \sum_{i=0}^m Q_{nmk}^{*(i)} P_k(t) = Q_{nmk}^* P_k(t), \quad (4)$$

– вероятность $P^*nm(t)$ того, что в момент t в памяти будут неработоспособны ровно m групп при условии работоспособности всех $3n$ элементов в начальный момент времени; очевидно, что

$$P_{nm}^*(t) = \sum_{k=0}^{n+2m} P_{nmk}^*(t) = \sum_{k=0}^{n+2m} \sum_{i=0}^m P_{nmk}^{*(i)}(t), \quad (5)$$

– вероятность $P_{nm}(t)$ того, что в момент t в памяти будут работоспособны не менее $n-m$ групп при условии работоспособности всех элементов в начальный момент времени.

Из определений показателей следует, что:

$$P_{nm}(t) = \sum_{j=0}^m P_{nj}^*(t) = \sum_{j=0}^m \sum_{k=0}^{n+2m} \sum_{i=0}^m P_{nj}^{*(i)}(t), m = 0 \dots n. \quad (6)$$

При необходимости с помощью (6) для различных m можно рассчитать среднюю наработку до отказа системы:

$$\bar{T}_{c,nm} = \int_0^{\infty} P_{nm}(t) dt, m = 0 \dots n. \quad (7)$$

Если минимальный рабочий объем памяти задан и требует работоспособности не менее n_0 групп, то объем памяти $m=n-n_0$ групп можно считать резервным и предназначенным для обеспечения заданного уровня вероятности безотказной работы

$$P_c(t, n_0, m) = P_{n_0+m, m}(t, n_0, m), \quad (8)$$

или средней наработки до отказа:

$$\bar{T}_c(n_0, m) = \int_0^{\infty} P_c(t) dt. \quad (9)$$

Гамма - процентный ресурс безотказности $T_\gamma(n_0, m)$ определяется как интервал времени, в течение которого вероятность безотказной работы будет не менее γ , то есть $T_\gamma(n_0, m)$ является решением уравнения:

$$P_c(T_\gamma, n_0, m) = \gamma, m \geq 0. \quad (10)$$

Если требования к надежности содержат нормативное значение T_γ^0 , то в соответствии с (10) подбирают такое значение m , чтобы:

$$T_\gamma(n_0, m) \geq T_\gamma^0. \quad (11)$$

Аналогично вводятся показатели надежности при ненулевой деградации (пост-деградации). Назначение этой группы показателей состоит в том, чтобы давать прогноз показателей надежности изделия на время t эксплуатации, следующего за интервалом t_0 с начала эксплуатации. При этом надо иметь в виду, что расчёт показателей надежности в интервале (t_0, t_0+t) может быть проведен и до начала эксплуатации как условные показатели надежности:

– вероятность безотказной работы:

$$P_c(t_0, t) = P_c(t_0 + t) / P_c(t_0), \quad (12)$$

– средняя наработка до отказа:

$$\bar{T}_c(t_0) = \int_0^{\infty} P_c(t_0, t) dt, \quad (13)$$

– гамма-процентный ресурс безотказности $T_\gamma(t_0)$ как решение уравнения:

$$P_c(t_0, T_\gamma(t_0)) = \gamma. \quad (14)$$

В реальной ситуации по истечении времени t_0 фактический уровень деградации характеризуется вектором (n, m, k, i) . При таком начальном уровне деградации можно рассчитать показатели надежности в течение последующей эксплуатации и сравнить их с (12) – (14).

Для этого вводятся следующие показатели надежности:

– вероятность $P^{*(i)}_{nmk, m+r}(t)$ того, что за время t уровень деградации достигнет величины $m+r$ (увеличится на r число неработоспособных групп) при начальном уровне деградации (n, m, k, i) ;

– вероятность $P^{*}_{nmk, m+r}(t)$ того, что за время t уровень деградации достигнет величины $m+r$ при начальном уровне деградации (n, m, k) ; эта вероятность рассчитывается в том случае, если при диагностировании не удастся установить i , и связана с предыдущей вероятностью соотношением:

$$P^{*}_{nmk, m+r}(t) = \sum_{i=0}^m \frac{Q_{nmk}^{*(i)}}{Q_{nmk}^*} P^{*(i)}_{nmk, m+r}(t), \quad (15)$$

вероятность $P^{(i)}_{nmk, m+r}(t)$ того, что за время t число дополнительно отказавших групп будет не более r при начальном уровне деградации (n, m, k, i) ; очевидно, что

$$P^{(i)}_{nmk, m+r}(t) = \sum_{j=0}^r P^{*(i)}_{nmk, m+j}(t), \quad (16)$$

вероятность $P_{nmk, m+r}(t)$ того, что за время t число дополнительно отказавших групп будет не более r при начальном уровне деградации (n, m, k) ; она связана с ранее введенными вероятностями соотношением

$$P_{nmk, m+r}(t) = \sum_{j=0}^r P_{nmk, m+j}^*(t) = \sum_{j=0}^r \sum_{i=0}^m \frac{Q_{nmk}^{*(i)}}{Q_{nmk}^*} P_{nmk, m+j}^{*(i)}(t) = \sum_{i=0}^m \frac{Q_{nmk}^{*(i)}}{Q_{nmk}^*} P_{nmk, m+r}^{(i)}(t). \quad (17)$$

В частности, $P_{nmk, m}(t)$ есть вероятность сохранения начального уровня деградации, а $P_{nmk, n}(t)$ вероятность потери всей памяти. С помощью (16) – (17) и (13) – (14) могут быть найдены ещё два показателя надёжности, а затем определено то значение r , при котором выполняется условие (11).

2. Результаты анализа

Вероятность потери m групп из n , в том числе i групп с тремя отказавшими элементами, определяется по формуле:

$$Q_{nmk}^{*(i)} = \frac{C_n^m}{C_{3n}^k} C_m^i (C_3^2)^{m-i} C_{n-m}^{k-2m-i} (C_3^1)^{k-2m-i} = \frac{C_n^m}{C_{3n}^k} C_m^i C_{n-m}^{k-2m-i} 3^{k-m-2i}, \quad (18)$$

для $0 \leq m \leq n-1$, $0 \leq i \leq m$ и $i+2m \leq k \leq m+n+i$. Вероятность потери ровно m групп:

$$Q_{nmk}^{(i)} = \frac{C_n^m}{C_{3n}^k} \sum_{i=0}^m C_m^i C_{n-m}^{k-2m-i} 3^{k-2m-i}, \quad 2m \leq k \leq n+2m, 0 \leq m \leq n-1. \quad (19)$$

Условная вероятность потери не более m групп определяется по формуле (2). Далее надо использовать формулы (3) – (11) для расчета показателей надежности и отказобезопасности при нулевой начальной деградации и формулы (12) – (17) при расчете показателей пост-деградации.

Анализируя зависимость вероятности потери m групп из n при k отказавших кластеров, можно определить наиболее вероятное значение числа отказавших кластеров k_0 , при котором не исправны m групп. Оказывается, что это число во много раз превосходит минимальное число $k_{\min} = 2m$, которое достаточно для вывода из строя m групп. Для $m = 1$ отношение $\delta = k_0 / k_{\min} = 7$ при $n = 64$ и $\delta = 10$ при $n = 128$. Для $m = 2$: $\delta = 5$ и 7 соответственно, а для $m = 3$: $\delta = 4,25$ и $5,83$ соответственно. Доля отказавших кластеров (из k), которые оказались в работоспособных группах, снизив в них избыточность, но не вызвав отказа группы, значительна. При различных m и n она колеблется в пределах от 50 до 90%. С увеличением n эта доля растет. Этот феномен очень важен для правильной оценки возможности изделия успешно выполнять свои функции в будущем. При относительно малом m создается видимость благополучия, поскольку отказавших групп не много, но надежность памяти низкая. При фиксированном k существует наиболее вероятное число m_0 отказавших групп. Оно значительно меньше максимально возможного $m_{\max} = [k/2]$. Например, при $n = 64$, $k = 19$: $m_0 = 2$, $m_{\max} = 9$; при $n = 128$, $k = 19$: $m_0 = 1$, $m_{\max} = 9$; при $n = 128$, $k = 34$: $m_0 = 3$, $m_{\max} = 17$.

Рассчитывая значения вероятности, можно найти такое максимальное значение числа отказавших кластеров, при котором вероятность отказа не более m групп остается на уровне не менее заданного значения p . Результаты оценки показывают, что весьма много отказавших кластеров расположено в работоспособных группах. Так при $n = 64$, $m = 2$, вероятность потери не более двух групп будет не менее 0,9. При этом возможны отказы 16 кластеров, из которых только 4-6 кластеров находятся в отказавших группах, а остальные 10-12 (что составляет 63-75%) находятся в работоспособных группах. При $n = 128$ еще большая доля отказавших кластеров (73-82 %) находится в работоспособных группах.

3. Классификация и вероятностные характеристики уровней деградации

Все уровни деградации могут быть разделены на две категории: докритические и критические. Чтобы дать определения этих понятий, введем следующие величины: T – заданное полное время функционирования, t_0 – промежуточное время, для которого проводится классификация уровней деградации, $t = T - t_0$ – предстоящее время эксплуатации, ε_0 – вектор параметров, характеризующий уровень деградации в момент t_0 , $P_c(t_0, t)$ – вероятность безотказной работы, определяемая по формуле (12), $P_c(\varepsilon_0, t)$ – вероятность безотказной работы, определяемая по формуле (17).

Уровень деградации будет докритическим, если при заданных ε_0 , t_0 и t имеет место неравенство:

$$P_c(t_0, t) \leq P_c(\varepsilon_0, t). \quad (20)$$

Уровень деградации будем называть первым критическим, если:

$$P_c(t_0, t) > P_c(\varepsilon_0, t), \quad (21)$$

и в изделии в полном объеме сохраняются все функции при надлежащем качестве.

Уровень деградации будем называть вторым критическим, если требуется переход от штатного режима функционирования к аварийному с возможной потерей одной из функций либо со снижением качества функционирования: снижение достоверности, снижение производительности и др.

Введем теперь понятия критических моментов времени и критических областей. Представим неравенство (20) в виде:

$$P_c(t_0, T - t_0) / P_c(\varepsilon_0, T - t_0) = b(t_0, T, \varepsilon_0) \leq 1, \quad (22)$$

и попытаемся найти значение t_0^* , при котором имеет место равенство. Здесь возможны три случая:

1. Решения, принадлежащего интервалу $(0, T)$, нет и для любых $t_0 < T$ выполняется неравенство.

$$P_c(t_0, T - t_0) < P_c(\varepsilon_0, T - t_0).$$

Это значит, что уровень деградации ε_0 является всегда докритическим.

2. Есть решение $t_0^* < T$. Тогда при $t_0 < t_0^*$ будет выполняться неравенство (21), а для $t_0^* \leq t_0 \leq T$ выполняется неравенство (20). Это значит, что при $t_0 < t_0^*$ уровень деградации ε_0 является критическим, а при $t_0^* \leq t_0 \leq T$ докритическим.

Область значений $[0, t_0^*)$, будем называть критической областью, t_0^* – границей критической области, а любую точку критической области – критической точкой (критическим моментом времени).

3. Решения, принадлежащего интервалу $(0, T)$, нет и для любых $t_0 < T$ выполняется неравенство (21). Тогда весь интервал $(0, T)$ является критической областью, а момент T – границей критической области.

Знание критической области для каждого уровня деградации ε_0 полезно в том смысле, что если уровень ε_0 достигается «слишком рано», то он становится критическим, но не навсегда. Если он сохраняется в течение некоторого времени до момента t_0^* , то после t_0^* уровень ε_0 перестает быть критическим и становится докритическим. Если происходит ещё один отказ и уровень деградации изменяется, то важно знать, в какой области находится момент отказа. Если он находится в докритической области, то выполняются требования по надежности и эта ситуация не вызывает озабоченности. Если же он находится в критической области, то это сигнал тревоги, требующий, возможно, дополнительных мероприятий.

Желательно иметь такую траекторию деградации изделия, чтобы ни одна её точка не попадала в критическую область. Прогнозировать поведение изделия в течение T и оценивать моменты отказов с точки зрения попадания их в критическую область можно с помощью имитационного моделирования [2].

Заключение. Анализ показателей живучести и отказобезопасности резервированной памяти позволяет уже на ранних стадиях проектирования установить приемлемые параметры системы памяти: число групп, размеры кластера, объем резервной части емкости памяти, а также оценить эффект от применения гибкой адресации, помехоустойчивого кодирования и возможности перезагрузки файлов в работоспособную часть памяти.

СПИСОК ЛИТЕРАТУРЫ

- 1 Черкесов Г.Н., Виноградов А.А. Отказобезопасность как важное свойство ответственных технических систем. // XII Санкт-Петербургская Международная конференция «Региональная информатика («РИ-2010»)). Труды конференции. СПб, 2010.
- 2 Черкесов Г.Н. Об одном способе обоснования решений о продлении сроков эксплуатации резервированной системы. – М. Надежность, 2002, №1, с.33 – 43.

Чистяков И.В., Орлов Д.Р.

Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
МЕТОДЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА
УСТРОЙСТВАХ ХРАНЕНИЯ

Современный подход к разработке безопасных информационных технологий требует обеспечения безопасности информации не только при ее передаче по каналам и сетям связи, но и при хранении на запоминающих устройствах различного типа.

Устройства хранения как среда безопасности имеют ряд особенностей, в том числе:

- длительный срок хранения информации с возможностью ее частичной модификации;
- возможность произвольного доступа к записям;
- отсутствие on-line взаимодействия между субъектами при работе с разделяемыми ресурсами,
- способ организации хранения

и ряд других, которые должны быть учтены при разработке системы криптографической защиты.

При этом необходимо минимизировать увеличения времени доступа и требуемый объем дополнительной памяти.

Основными сервисами, обеспечиваемыми криптографическими механизмами для устройств хранения, являются:

- конфиденциальность,
- контроль целостности,
- защита от навязывания устаревших (неактуальных) версий,
- криптографическое разграничение доступа к совместно используемым ресурсам.

Механизмы и сервисы безопасности хранения могут быть размещены на разных уровнях стека протоколов: на уровне записи или на более высоком уровне, например, на уровне файловой системы.

Конфиденциальность обеспечивается путем шифрования.

Размещение шифрования на уровне записи обеспечивает максимальную «прозрачность» для приложений (файловая система, база данных и другие). Наиболее подходящим для этого уровня представляется режим шифрования для блок-ориентированных устройств хранения [1], адаптированный к стандарту шифрования РФ. Указанный режим обладает следующими свойствами:

- длина шифртекста равна длине открытого текста;
- не требует хранения дополнительной информации;
- каждый блок шифруется независимо;
- преобразование шифрования зависит от положения шифртекста на устройстве хранения (от номера сектора и номера блока в секторе);
- изменение любого бита открытого текста «рандомизирует» соответствующий блок шифртекста.

Для контроля целостности записи, учитывая свойства режима шифрования [1], можно использовать функцию хэширования или некриптографическую контрольную сумму.

Для контроля целостности объектов с произвольным доступом к записям целесообразно использовать функцию хэширования с древовидной структурой.

При реализации криптографического разграничения доступа к защищенным разделяемым ресурсам возникает проблема хранения и распространения большого числа криптографических ключей.

Сложность данной проблемы может быть уменьшена, если полномочия субъектов могут быть представлены как иерархическая структура.

Тогда множество субъектов разбивается на непересекающиеся классы безопасности, отличающиеся полномочиями по доступу к ресурсам. При этом подчиненные могут иметь более одного начальника. Упорядоченные таким образом классы безопасности можно рассматривать как частично упорядоченное множество.

Каждому классу безопасности назначается свой ключ для шифрования принадлежащих ему файлов. Пользователи старших классов должны иметь возможность доступа к информационным ресурсам всех своих подчиненных.

Для доступа к файлам подчиненных классов субъект должен иметь ключи всех подчиненных классов или, с целью сокращения числа хранимых ключей, должен уметь строить (выводить) ключи этих классов. При этом субъекты подчиненных классов не должны иметь возможность вывести ключ старших классов безопасности.

Поэтому основой криптографического разграничения доступа в иерархических системах является схема назначения и вывода ключей (СНБК) [2].

Математическая модель СНБК включает две основные процедуры.

1. Процедура назначения реквизитов доступа (выполняется центром назначения реквизитов доступа).

2. Процедура вывода реквизитов доступа (выполняется субъектом при доступе к информации субъекта подчиненного класса безопасности).

Этот же механизм может быть использован при уменьшении пиковых нагрузок при смене криптографических ключей.

Проблема заключается в том, что при смене ключа шифрования необходимо перешифровать все информационные ресурсы, зашифрованные на этом ключе. Перешифрование может быть растянуто во времени, если положить, что информационный ресурс перешифровывается только при его модификации [3].

Тогда авторизованный субъект при чтении, модификации и записи информации должен иметь два ключа: сменяемый ключ расшифрования и новый ключ засшифрования.

Однако при использовании механизма СНБК субъекту достаточно обладать только одним новым ключом зашифрования, а ключ расшифрования может быть получен с помощью процедура вывода реквизитов доступа.

Для защиты от навязывания неактуальных версий файла используется механизм нумерации версий. Однако в больших многопользовательских системах использование данного подхода встречает трудности, обусловленные необходимостью организации отдельного нумератора версий для каждого файла и on-line взаимодействия между субъектами.

Для преодоления этого в [4] предложено использовать один централизованный защищенный монотонный счетчик, на базе которого строятся виртуальные нумераторы версий. Однако так организованные нумераторы являются возрастающими, но недетерминированными.

Поэтому для проверки файла необходим специальный журнал, в котором фиксируются номера версий всех файлов в порядке их получения. Данный журнал ведется в незащищенной области, а его записи заверены цифровой подписью увязаны между собой.

При контроле версии файла по указанному журналу проверяется, что данный номер версии является последним для данного файла. При этом не требуется on-line взаимодействия между пользователями

Таким образом, применение криптографических методов для защиты информации на устройствах хранения требует адаптации известных протоколов.

СПИСОК ЛИТЕРАТУРЫ

1. IEEE P 1619 Standart for cryptographic protection of data on block-oriented storage devices.
2. Crampton d P. On key assignment for hierarchical access control // IEEE Computer Security Foundations Workshop (CSFW'06), 2006.
3. Fu K, Kamara S., and Kohno T. Key regression: Enabling efficient key distirbution for secure distributed storage. // ISOC Network and Distributed System Security Symposium (NDSS 2006), 2006.
4. van Dijk and al. Offline untrusted storage with immdiate detection of forking and replay attacks // STC 2007.

Штогрин И.Р.

Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»

ОБЕСПЕЧЕНИЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ЭТАПЕ СТЕНДОВОЙ ОТРАБОТКИ ИЗДЕЛИЙ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ СИСТЕМ

Обеспечение безопасности информации в критических информационно-управляющих системах имеет главенствующее значение для их устойчивости к разного рода воздействиям.

На этапе разработки и отработки изделий и систем в целом, процесс обеспечения безопасности информации включает:

- определение требований по безопасности информации и выработку технических решений по порядку их реализации;
- реализацию требований по безопасности информации в конструкторской документации и технологиях проектирования;
- обеспечение требований нормативно-технической документации по безопасности при отработке и испытаниях;
- подтверждение реализации заданных требований по безопасности в процессе испытаний изделий и систем в целом.

В данной статье рассматриваются принимаемые меры по обеспечению безопасности информации на этапе отработки изделий на комплексных стендах «ФГУП НПО «Импульс».

Комплексный стенд представляет собой совокупность технических средств (технологическое оборудование) для настройки составных частей изделия и обеспечения их совместной отработки, разработки и отработки программного обеспечения, отработки алгоритмов функционирования изделия и взаимодействия со смежными системами, испытаний изделий.

Таким образом, привлекаемое для настройки и отработки изделия технологическое оборудование напрямую влияет на уровень создаваемой в изделии системы безопасности информации, и в то же время может при определенных условиях стать источником угрозы для нее.

Алгоритм отработки изделия (рис.1, 2) предполагает, что на начальных этапах комплексной отработки изделий технические решения по обеспечению безопасности информации в большинстве не внедрены, или не проведена оценка их эффективности, т.е изделия не защищены собственной системой безопасности информации от вторжения извне, в т.ч. посредством технологического оборудования.

Поэтому на данных этапах защиту информации в изделиях возможно обеспечить в основном только мерами, предусмотренными в нормативно-технической документации, ограничивающими доступ к информации, и обеспечивающими сохранение информации и которые подразделены на технические и организационные.

Среди основных технических и организационных мер защиты информации на этапе стендовой отработки необходимо отметить:

- размещение объектов и технологического оборудования для разработки в экранированном помещении, обеспечивающем защиту от утечек информации, в том числе по цепям электроснабжения, телефонным линиям связи и местным компьютерным сетям;
- применение технологической аппаратуры (ПЭВМ), прошедшей соответствующие проверки и имеющей предписание на эксплуатацию, исключение использования съемных носителей информации;
- применение в технологической аппаратуре (ПЭВМ) в т.ч. при разработке ПО сертифицированного ПО;
- исключение прямого выхода соединения локальной компьютерной сети с внешними сетями;
- ограничение и контроль допуска сотрудников в помещения с использованием автоматизированной системы контроля допуска и системы видеонаблюдения;
- многоуровневый контроль за перемещением и хранением всех видов носителей информации.

Обеспечение реализации указанных мер на практике осуществляется соответствующим графиком проверки уровня экранирования помещений, периодическим обновлением списков допущенных, совершенствованием системы допуска и документирования посещения.

Многолетний опыт по созданию информационно управляющих систем для обеспечения управления в критических условиях подтверждает, что применение и выполнение выше указанных в

докладе мер позволяет обеспечить выполнение всех требований по обеспечению безопасности информации на этапе стендовой отработки.

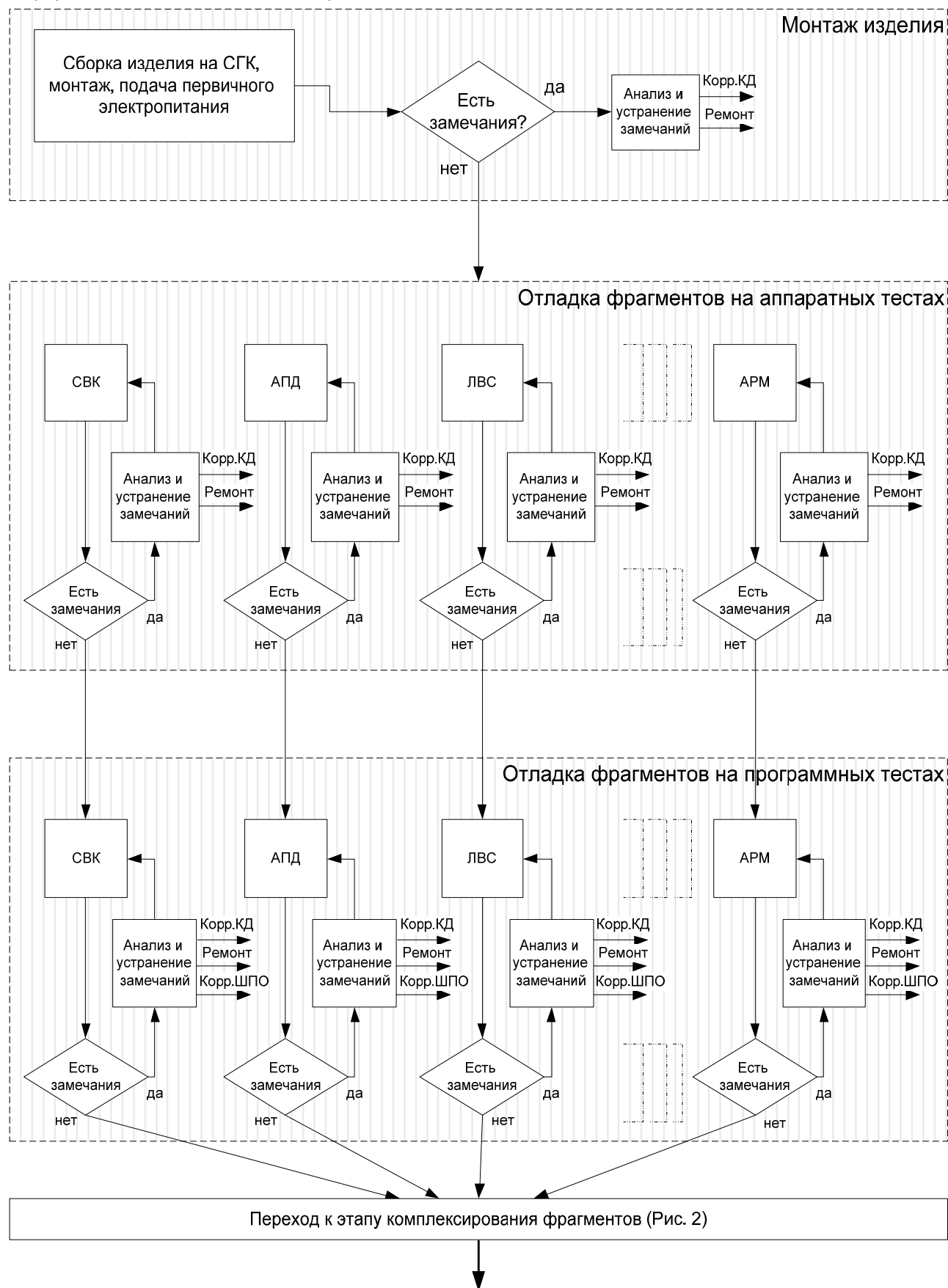


Рис.2

Рис.1. Начало алгоритма комплексной отладки изделия на СГК

Переход от этапа отладки на аппаратных тестах (Рис.1)

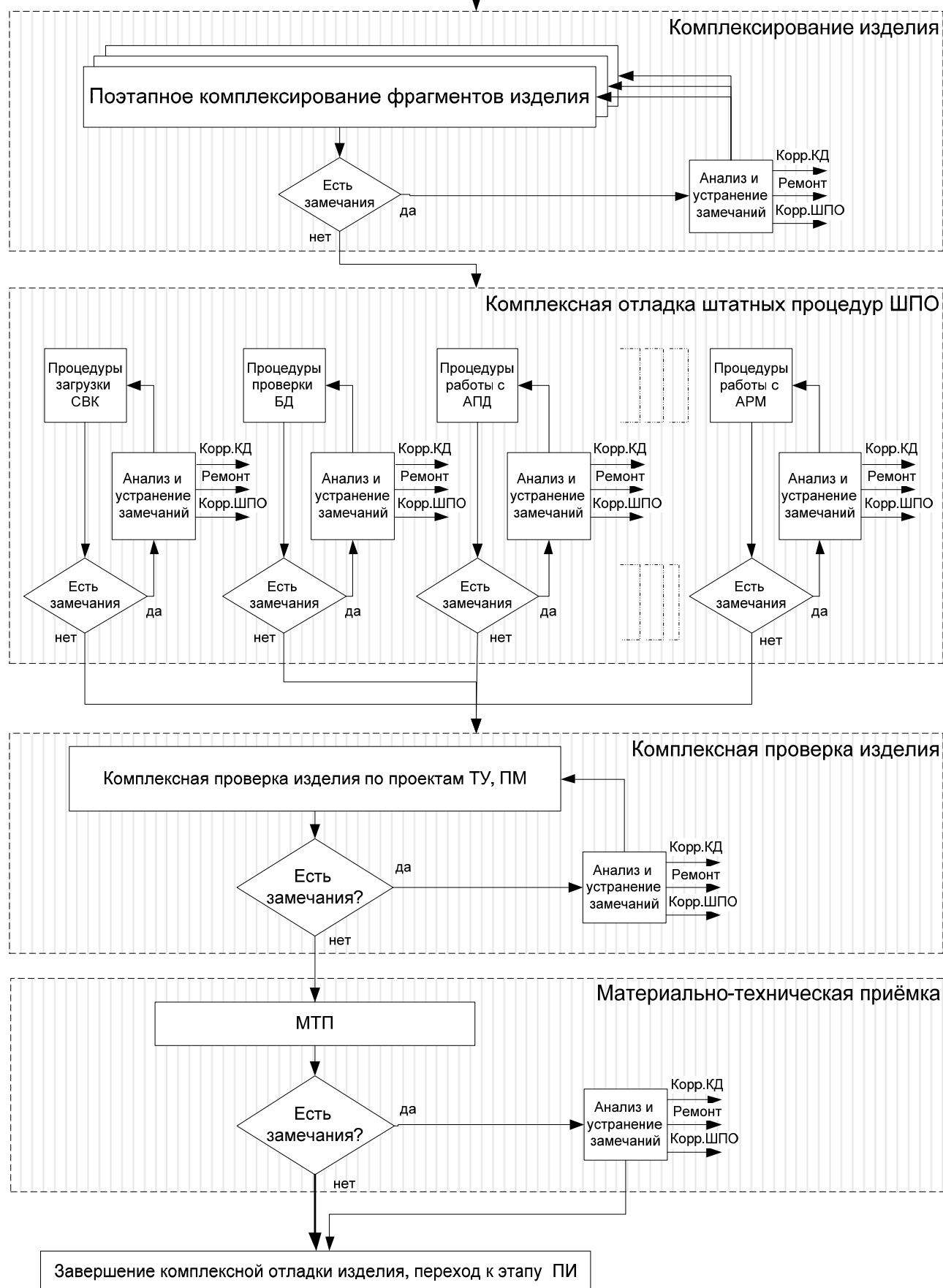


Рис.2. Окончание алгоритма комплексной отладки изделия на СГК

Щёткин И.Е.

**Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»,
Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
ИНВЕСТИЦИОННО-ИННОВАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ ПРЕДПРИЯТИЯ КРИТИЧЕСКОЙ
ИНФРАСТРУКТУРЫ В ЦЕЛЯХ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Исторически сложившаяся система генерации и обмена информацией во внутренней и внешней средах предприятий оборонного комплекса позволила сформировать основные принципы и методы защиты информационных ресурсов. С появлением и широким применением вычислительной техники резко увеличились объемы информации и методы ее передачи, хранения, доступа. Изменились и требования к защите информационных ресурсов и методологический подход к организации информационный безопасности предприятия.

Вопрос обеспечения информационной безопасности остается актуальным и сложным аспектом реализации бизнес идеи предприятий. Технологии передачи информационных ресурсов современного мира постоянно совершенствуются и находятся в конкурентной борьбе, в связи с этим растет сложность осуществления необходимой защищенности информационной среды.

Универсальных методов защиты не существует, все зависит от индивидуальных особенностей рассматриваемой системы, а учет всех особенностей трудно подогнать под какую либо формализацию. Поэтому информационная безопасность чаще всего рассматривается как совокупность неформальных рекомендаций по построению систем защиты информации в той или иной системе с ее конкретными особенностями.

Глобальность вопроса защиты информации и информационная безопасность как предмет анализа и принятия решений за счет наличия универсальных принципов своего построения превратилось в отдельное направление, которое подвергается самому тщательному анализу в современном быстроразвивающемся и постоянно изменяющемся мире.

Для предприятий России из сферы оборонно-промышленного комплекса (ОПК) информационная безопасность является обязательным аспектом деятельности. Уже работают механизмы, который и сегодня позволяют обеспечивать необходимый уровень защиты государственной и коммерческой тайны, но внедрение современных автоматизированных систем создает необходимость дополнительно развивать структуру и основные подходы и методы.

Информационные потоки, которые создают конкурентоспособность предприятия на рынке товаров и услуг, задают новые требования и предпосылки модернизационных и инновационных внедрений в уже сложившиеся системы. Инновационные подходы в производстве, создании единых информационных пространств, внедрение безбумажного документооборота формируют задания к осуществлению безопасности особенно в критической инфраструктуре, где несанкционированное использование информационных ресурсов может привести к необратимым последствиям, как для предприятия, так и для всей страны.

Основой новых решений становятся автоматизированные системы (АС). Автоматизированные системы обработки информации являются конкурентным преимуществом каждой компании их индивидуальность, защищенность, адаптивность позволяют выходить на рынок быстрее, а продукция становится более качественной, репутация предприятия и спрос на товар повышается.

Под элементами автоматизированных систем следует понимать: средства вычислительной техники, программное обеспечение, каналы связи, информация на различных носителях, пользователи системы, серверные реализации обмена и хранения информации.

Анализ нормативной документации и опыта работы структур по защите информации показывает: основные принципы информационной безопасности заключаются в том, что система способна противостоять дестабилизирующему воздействию как внешней, так и внутренней среды и функционирование системы не создает угроз для внутренней и внешней среды, а направления обеспечения защиты информации сводятся к разделению всех угроз по пунктам общей классификации, которым соответствуют определенные методы и средства.

Методы обеспечения информационной безопасности достаточно разнообразны, но классификация в общем виде может быть представлена, как показано на рисунке 1.

Классификация показывает достаточно широкий спектр задач и возможных путей решения проблем защиты, а индивидуальность каждой реальной ситуации и задачи задает широкое поле для получения результатов и внедрения новых методов и средств.

В связи с большим вниманием к этой теме и необходимостью совершенствования с целью осуществления безопасности и конкурентоспособности, как отдельного предприятия, так и государства в целом необходимым условием развития является инвестирование в инфраструктуру информационной защиты и обучение людей современным методам и технологиям.

Развитие инвестиционно-инновационной среды для реализации новых проектов и модернизации уже существующей структуры с учетом ширины спектра возможных методов и большого числа современных решений по обмену и хранению информационных ресурсов заключается в наработке и использованию законодательных, нормативных и регламентирующих

документов, созданию технических средств и методов защиты, которые позволяют получать конечный продукт удовлетворяющий потребностям заказчика и находящийся в рамках регламентирующих ограничений. При реализации данных задач при формировании инновационных продуктов внедрения необходимо учитывать фактор быстроменяющейся информационной среды.

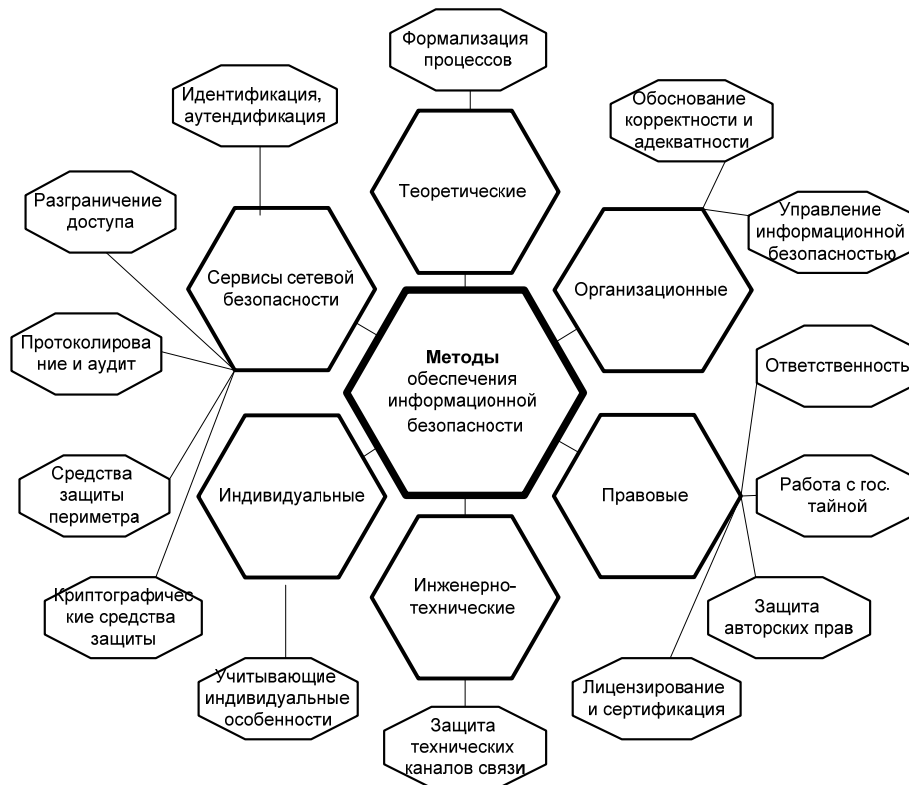


Рис.1. Методы и средства обеспечения защиты информации

Совершенствование методов инвестиционно-инновационной деятельности предприятия в части информационной безопасности – это затратная, сложная, но необходимая мера поддержания конкурентоспособности. С одной стороны недофинансирование данного направления может привести к отсталости методов и необеспеченности персонала для осуществления работ, с другой стороны каждая организация ограничена финансовыми и трудовыми ресурсами, а высокая рискованность осуществления проектов в данной сфере является ключевым фактором при принятии решений по инновационным разработкам. Одной из основных особенностей является скорость изменения и внедрения инноваций в сферу по всему миру, что делает обязательным учет тенденций и необходимость мониторинга и постоянное проведение обучения по данному направлению.

Инвестиционно-инновационная деятельность предприятия в целях повышения уровня информационной безопасности в критических инфраструктурах заключается в поиске новых решений и оптимизации уже существующих на рынке или собственных разработок, проведение научно-исследовательских и опытно-конструкторских работ, выход на рынок с новым товаром, преодоление конкурентных барьеров, создание систем для собственного применения не имеющих аналогов и обеспечивающих защиту информации и синтеза выгодных подходов к финансированию проектов за счет привлечения инвестиций разного вида. Данный вид деятельности является связующим звеном инноваций и источников их финансирования. Инвестиционные проекты в сферу новых технологий и производств, генерацию нового знания являются высокорискованными капиталовложениями. Данный вид инвестирования относится к венчурному и основным его признаком считается высокий риск и неопределенность конечного результата.

Внедрение новых и перспективных систем защиты являются одним из основных движущих рычагов дальнейшего развития сферы информационной безопасности. В данной сфере инновации являются залогом успеха выхода на рынок. Для осуществления данных целей необходимо для каждого предприятия рассмотреть и учесть ряд факторов, предопределяющих судьбу нововведений.

Среди основных факторов необходимо учитывать:

- необходим выход на рынок или нет;
- существует персонал способный взяться за данный вид деятельности;
- соответствие инновациям предприятия, восприимчивость предприятия к инновациям;
- экономически обоснованную систему отбора инновационных идей и проектов;
- эффективные методы управления инновационными проектами и контроль за их реализацией;

– индивидуальную и коллективную ответственность за реализацию проектов в данной сфере.

Формирование инвестиционных потоков и пунктов инвестиционного плана развития необходимо начинать с установления основных критериев в соответствии с деятельностью предприятия по инновационному менеджменту. Инновационный менеджмент – это область управленческих решений, связанная с реализацией инновационных решений и сфера сопряжения с другими отраслями менеджмента. Для осуществления инновационного менеджмента на уже функционирующем предприятии необходимо иметь платформу (задел) на котором можно строить новое направление. К такому заделу относится совокупный процесс функционирования предприятия в отрасли, а именно его позиции и наработки по планированию, организации работ, контролю, мотивации работников. Анализ данной платформы позволяет сделать вывод о какого рода инновациям может идти речь при построении инновационного менеджмента предприятия. Следующим этапом в построении идет уже процесс совершенствования инвестиционно-инновационной среды.

При реализации инновационных проектов необходимо опираться на основные принципы инновационного менеджмента:

- инновации являются решающим условием выживания предприятия на рынке товаров и услуг;
- ресурсы на НИР и ОКР оправданы лишь в той мере, в которой они приводят к поставленным результатам;
- успех инновации в постоянном мониторинге и анализе мира инноваций и совершенствование методов и схем их инвестирования.

Инвестиционная деятельность предприятия является неотъемлемой составляющей продвижения инновационных решений. Далеко не каждая идея и решение может получить реализацию даже при высоких показателях эффективности проектов и большинство таких решений требуют от предприятий привлечения капитала со стороны, когда собственные средства не могут покрыть рисованные шаги. Именно поэтому тесное взаимодействие инвестиционной и инновационной деятельности предприятия позволяет выводить идею на поверхность.

Параллельно с зарождением инновационной идеи встает вопрос поиска и формирования плана по источникам финансирования. Он соответствует этапам жизненного цикла инновационных решений. Проработка множества возможных источников позволяет сделать вывод о наличии основных базовых, к которым могут быть сведены большинство из возможных. Анализ источников финансирования инноваций для ОПК можно представить в виде таблицы 1.

Таблица 1

Источники финансирования этапов инновационного процесса

№	Название	Проводимая работа	Финансирование
1	Поисковые НИР	Выдвижение научно-технических идей, проведение экспериментов	Государственные программы, и государственные субсидии
2	Прикладные НИР	Проведение прикладных работ по выбранному направлению	Государственное целевое финансирование (для государственных научно-технических программ на конкурсной основе), промышленные предприятия, венчурные фирмы, «бизнес-ангелы»
3	Опытно-конструкторские и проектно-конструкторские работы (ОКР и ПКР)	Разработка аванпроектов, эскизно-технических проектов, РКД, изготовление и испытание образцов	Источники финансирования прикладных НИР и собственные средства предприятия
4	Коммерциализация нововведения	Запуск производства, выход на рынок и далее по жизненному циклу товара	Необходимость большого потока инвестиций для производственных мощностей. Венчурное инвестирование, в связи с рискованностью инновации на рынке

Определение этапов инновационного менеджмента и вида инвестирования позволяют сделать анализ и уделить внимание каждому пункту плана финансирования. Основное поступление средств на первых этапах инвестиционных вложений направляется в рамках государственных программ и венчурных компаний. Каждый из двух источников требует тщательной предварительной проработки. Инвестор в каждом из этих случаев анализирует показатели компании перспективность проектов при переходе на конечном этапе к финансированию из собственных средств предприятия. Венчурное финансирование инноваций опирается на авторитет фирмы и прибыльность итогового результата с учетом высоких рисков данного вида вложения средств.

Одной из основных особенностей вложения инвестиций в сферу обеспечения безопасности информации заключается в том, что получаемый результат формируется как взаимосвязанный технический и интеллектуальный продукт и для него вступают в силу законы поведения участника рынка интеллектуальной сферы. А в современных условиях конкурентной борьбы вторая отличительная особенность сферы информационной безопасности заключается в высоком риске. Именно поэтому данный вид инвестирования осваивают венчурные фирмы, которые

специализируются непосредственно на данном виде инвестиционных проектов, особенно на первоначальном уровне.

Применительно к сфере информационной безопасности в критической инфраструктуре основные элементы подхода сохраняются, но специфичность деятельности и ее особая важность ставит новые обязательные задачи для выполнения и учета в реализации. Специфичность данной сферы заключается в значительных последствиях неправильной реализации проектов. Несанкционированный доступ к информационным ресурсам атомной, оборонной и других видов деятельности государства может привести к большим жертвам среди населения и разворачиванием военных действий, экономической блокадой государства. Поэтому сложная задача осуществления информационной безопасности получает еще значительную прибавку ответственности и становится еще более сложной для осуществления, но государство не в силах уйти от этого – эта важная и необходимая задача, как на отдельном предприятии, так и на уровне государства в целом.

Финансирование работ по этапам реализации проекта распределяется неравномерно, так финансирование работ связанных с освоением масштабного производства нового продукта и последующем совершенствованием технологии в 6-8 раз больше, чем расходы на исследования и разработки, а на этот период реализации проекта основными источниками инвестиций на предприятиях являются собственные средства, аккумулируемые на специальных фондах и заемные средства, в основном банковские кредиты. Проработка детального плана, компьютерное моделирование, просчет основных рисков и финансовых потоков являются конкурентным преимуществом и современным обязательным средством для достижения результата.

Оценка результатов инновационной деятельности предприятия в рамках осуществления информационной безопасности и просчет рисков может производиться путем сравнения показателей факторного анализа, индексного метода, SWOT-анализа, функционально-стоимостного анализа и других видов информации по результатам деятельности предприятия за рассматриваемый период. Сравнительный анализ позволяет определить отклонение от плановых показателей, выявить резервы, установить причины отклонений. Особенности сравниваемых методов в таблице 2.

Таблица 2

Система методов подлежащих сравнительному анализу

№	Название	Описание
1	Факторный анализ	Установление влияния факторов на функцию (производительность труда, полезный эффект изделия и др.)
2	Индексный метод	При невозможности измерения отдельных элементов используются относительные показатели для оценки плановых, а также определение динамики процессов, выявление относительных и абсолютных отклонений.
3	SWOT-анализ	Комплексная процедура стратегического анализа окружающей среды и ресурсного потенциала предприятия указывая сильные, слабые стороны и угрозы.
4	Функционально-стоимостной анализ	Учет степени значимости выполняемых изделием функций с целью повышения полезного эффекта на единицу затрат

Системный подход к информационной безопасности предприятия заключается в обобщении и классификации множества факторов, ресурсов и методов в целях унификации способов защиты, постоянное отслеживание современных инновационных методов для оперативного реагирования и коррекции (модернизации) существующих алгоритмов и решений, сформированных на базе прошлого опыта. Регулярное планирование источников финансирования и формирования инвестиционных потоков в сферу, применение АС и программных продуктов для обработки информации и просчета инвестиционных проектов, что стало обязательным условием конкурентоспособности на рынке инновационных решений при условиях венчурного инвестирования. Изложенные подходы должны учитывать особенности венчурного инвестирования в критическую инфраструктуру, где в большинстве случаев невозможно использовать иностранный капитал и привлекать частные инвестиции, а основные условия формирует государство как заказчик проектов. В тоже время появление патентов и закрепление авторских прав за разработками позволяет рассчитывать на долгосрочное финансирование новых проектов в данной сфере.

Инвестирование инновационных проектов в области информационной безопасности и защиты информационных ресурсов предприятий является приоритетной и актуальной задачей для государства и руководителей предприятий. Огромное значение информационной безопасности обусловлено ее прямым влиянием на конкурентоспособность фирм и безопасность государства. При оптимизации процесса финансирования и построения плана с учетом рисков, а также своевременных управленческих решений данная сфера деятельности способна не только обеспечивать безопасность информационного обмена, но и являться источником получения прибыли для предприятия на рынке технических и интеллектуальных услуг.

СПИСОК ЛИТЕРАТУРЫ

1. Гурунян Т.В. Управление инвестиционно-инновационной деятельностью. – СибАГС, 2010.
2. Десянин П.Н. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000.
3. Корт С.С. Теоретические основы защиты информации. – М.: Гелиос АРВ, 2004.
4. Цирлов В.Л. Основы информационной безопасности. – Ростов н/Д: Феникс, 2008.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГИДРОМЕТЕОРОЛОГИИ

Александрова Л.В., Ткаченко Н.Н.

Россия, Санкт-Петербург, Российский государственный гидрометеорологический Университет
ЗАЩИТА ГЕОИНФОРМАЦИОННЫХ СИСТЕМ И ГИДРОМЕТЕОРОЛОГИЧЕСКИХ БАЗ ДАННЫХ

Ценность гидрометеорологической информации, будь то метеорологические прогнозы обеспечения авиации и судов, прогноз ледовой обстановки в Арктике или вовремя предсказанное наводнение, представляет значительную государственную и общественную ценность. Геопространственное моделирование является одним из перспективных направлений, развиваемых в Российском государственном гидрометеорологическом университете. Особую актуальность оно приобретает в связи со строительством «Северного потока», а также вводом в эксплуатацию новых портовых и нефтеналивных сооружений. Мониторинг, выявление и ликвидация возможных техногенных катастроф неосуществимы без развития инновационных технологий в области геоинформатики и организации геоинформационных систем (ГИС). Подобные системы позволяют проводить комплексный анализ состояния вод, в который входят: оперативное наблюдение за течениями, волнами, изменениями в морфологической структуре прибрежной зоны, качеством воды и переносом загрязнений, а также возможностью выявления антропогенных катастроф и подводного терроризма. Для создания и развития геоинформационной системы района Балтийского моря необходимо использовать гидрометеорологические данные из различных источников (рисунок 1). Это могут быть:

- изображения земной поверхности, полученные со спутников;
- данные численного моделирования;
- данные полевых наблюдений;
- архивные данные и т.д.



Рис. 1. Система сбора, хранения и анализа данных

Выходные данные подобной геоинформационной системы могут быть как гражданского назначения (прогноз ледовой обстановки, штормовые предупреждения и пр.), так и для служебного пользования.

Точность и эффективность работы ГИС [1] зависит от качества входящей информации, иными словами должны быть предусмотрены средства и методы защиты передаваемой гидрометеорологической информации. Организации, составляющие прогнозы должны быть уверены в том, что информация доходит до потребителей без искажений (как случайных, так и искусственно внесенных). Для этих целей можно организовывать выделенные шифрованные каналы [2,3]:

- использование VPN-технологии (PPTP, PPPoE, IPSec, L2TP, OpenVPN);

- использование продвинутых методов аутентификации vpn-клиентов, в т.ч. с использованием системы сертификатов, с серверами их проверки;
- проверка целостности данных (алгоритмы хеширования md5 и SHA-1);
- использование алгоритмов шифрования, например 3DES (длина ключа 168 бит, эффективная криптостойкость 112 бит), CAST128 (128 бит), Blowfish (до 448 бит), Twofish (до 256 бит), AES (до 256 бит), ГОСТ 28147-89 (256 бит).

Также необходимо учитывать, что максимально возможная длина ключа не определяет реальную надёжность шифрования. Так, например, 128-битному надёжному ключу шифрования соответствует 98-символьный пароль. Если выбранный пароль не превысит 6-ти символов, то итоговая надёжность будет соответствовать 32-разрядному ключу шифрования (и это несмотря на то, что сам криптопродукт по-прежнему поддерживает ключи длиной 256 бит).

В некоторых случаях, государство должно иметь возможность закрывать отдельные гидрометеорологические данные и прогнозы. Для этих целей должны быть использованы новейшие методы защиты информации такие как: организация выделенных каналов для обмена информацией с использованием шифрования высокой степени криптографической стойкости, использование СУБД и клиент-серверных систем для хранения и доступа к информации, позволяющих гибко настраивать права доступа локальных и удалённых пользователей и групп пользователей к данным и любым локальным устройствам, что обеспечивает существенное снижение риска утечек как через устройства, подключаемые к внешним портам (USB, LPT, COM, IrDA, PCMCIA, IEEE 1394 и т.д.), так и через внутренние устройства (сетевые карты, модемы, Bluetooth, Wi-Fi, CD/DVD-дисководы и т.д.). В Oracle, например, имеются два типа объектов – пользователи и роли. Роли это группы пользователей с одинаковыми правами. С помощью ролей, удобно управлять доступом, выделять разрешения или запрет целой группе пользователей. Одна роль может входить в другую, то есть наследовать ее права доступа. Таким образом, можно создать иерархическую структуру прав:

- аудит безопасности;
- безопасность учетных записей;
- безопасность данных (ограничить запросы UPDATE и DELETE).

Установка активного и пассивного сетевого оборудования в банке данных, позволяющего на физическом уровне управлять использованием сети – ограничивать нежелательный трафик внутри сети и попытки несанкционированного доступа извне. Использование IDS (intrusion detection system) и IPS (intrusion prevention system) для обнаружения и предотвращения атак, которые обошли Firewall, и оповещения администратора сети, который, в свою очередь, предпримет дальнейшие шаги по предотвращению атаки [4]. По способам определения вредоносного трафика IDS системы подразделяются на: signature-based (сигнатурного метода), anomaly-based (метода аномалий) и policy-based (метода, основанного на политике). Соответствие образца известной атаке называется сигнатурой, определение атаки или вторжения иногда называют «сигнатурным определением». Метод аномалий состоит в определении ненормального (необычного) поведения на хосте или в сети. Детекторы аномалий предполагают, что атаки отличаются от «нормальной» (законной) деятельности и могут, следовательно, быть определены системой, которая умеет отслеживать эти отличия. Метод, основанный на политике (policy-based) заключается в написании правил сетевой безопасности. В терминах распределения доступа, например, какие сети могут взаимодействовать друг с другом и какие протоколы при этом могут использоваться.

Также предполагается использование гибридного контент-анализа, позволяющего анализировать все данные, передаваемые за пределы локальной сети организации банка данных, и позволяет предотвращать утечки определенной информации по сетевым каналам в том числе через электронную почту, социальные сети, интернет-мессенджеры и т.д. и детального аудита доступа к данным как таковым и системе хранения и передачи данных в целом [5]. Подобный аудит ещё на ранней стадии обнаруживает подозрительную активность, что позволяет дополнительно сократить риски утечки данных. Различные технологии обнаружения утечек по-разному эффективны для различных категорий информации. Ключевым разделением здесь является новизна конфиденциальной информации и её изменяемость со временем. Такой аудит предполагает использование специальных программ, нацеленных на сбор и анализ текстовой информации. Он может включать, к примеру, следующие части:

- детектор объектов на базе регулярных выражений (детектор счетов, номеров паспортов, особых групп данных и т.п.).
- защиту статических данных на базе цифровых отпечатков (реактивная защита).
- защиту новых и динамических данных на базе контентного анализа (проактивная защита).

Как пример эффективного внедрения устойчивых информационных технологий в поддержание работы центра сбора и хранения данных, можно рассмотреть хранилище центра ЕСИМО в г. Обнинске (рис. 2) [6]. В настоящий момент инфраструктура центрального узла ЕСИМО включает в себя четыре сервера баз данных (два основных DBServ, RealTime), хранилище данных – DBGlobal и резервный сервер БД Standby с управляющим сервером резервирования GridControl, сервер

приложений портала ЕСИМО APServ, сервер интеграции – SI, сервер «Поставщик данных» – DP, отладочный комплекс APTest сервера приложений JBOSS.

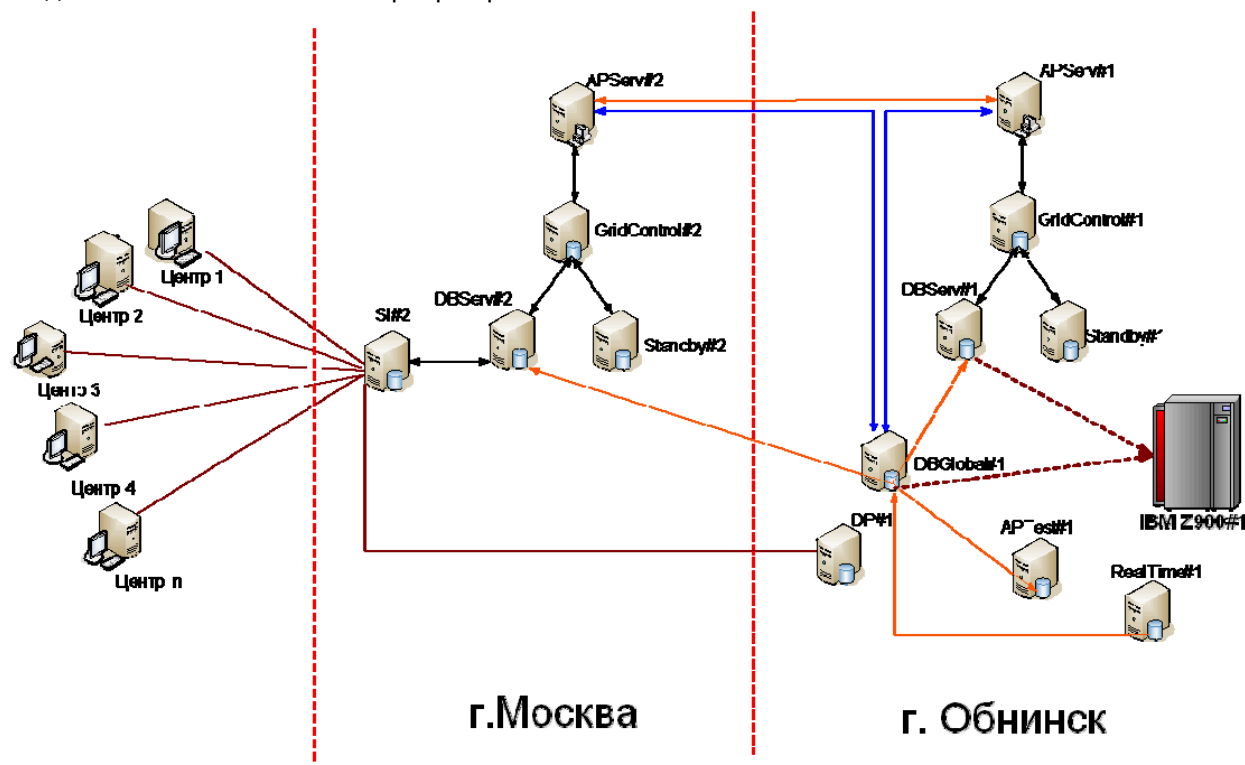


Рис. 2. Построение хранилища данных центра ЕСИМО на основе Oracle на базе ГУ «ВНИИГМИ-МЦД» Обнинск [6]

СПИСОК ЛИТЕРАТУРЫ

1. Бабенко Л.К., Макаревич О.Б., Журкин И.Г., Басан А.С. Защита данных геоинформационных систем. – Гелиос, 2010, 336с.
2. <http://www.securelist.com>
3. http://onlamp.com/pub/a/bsd/2002/12/12/FreeBSD_Basics.html
4. Марат Давлетханов. Обзор StoneGate Intrusion Prevention System. <http://www.anti-malware.ru>
5. Брачевский С.М., Д.В. Ландэ. Современные информационные потоки: актуальная проблематика. – НТИ. Сер.1.– №11.–2005.–С.21–33 [С.23]
6. Axel Buecke, Kent Browne, Louis Foss, Jaco Jacobs, Vladimir Jeremic, Carsten Lorenz, Craig Stabler, Joris Van Herzele. IBM Security Solutions Architecture for Network, Server and Endpoint. - IBM Redbooks, 2011, 510pp.
7. А.А. Федорцов. Построение хранилища данных центра ЕСИМО на основе инструментов Oracle. – Труды ГУ «ВНИИГМИ-МЦД», вып. 174, 2010.

ОГЛАВЛЕНИЕ

ПЛЕНАРНЫЕ ДОКЛАДЫ	11
Александрова О.А. Россия, Москва, Министерство юстиции Российской Федерации О ПЕРСПЕКТИВАХ ИСПОЛЬЗОВАНИЯ МОДЕЛЬНЫХ ЗАКОНОДАТЕЛЬНЫХ АКТОВ МПА СНГ В ИНФОРМАЦИОННОЙ СФЕРЕ И ИХ АНТИКОРРУПЦИОННОЙ ЭКСПЕРТИЗЕ	
	11
Жигадло В.Э., Терещенко П.Г., Рубинштейн Д.В. Россия, Санкт-Петербург, ООО «Максима», ФГБУ «Президентская библиотеки имени Б.Н. Ельцина», Москва, ФГУП «ГлавНИВЦ» Управления делами Президента Российской Федерации ПРОБЛЕМЫ СОЗДАНИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА ПРИМЕРЕ «ПРЕЗИДЕНТСКОЙ БИБЛИОТЕКИ ИМЕНИ Б.Н. ЕЛЬЦИНА». ОРГАНИЗАЦИЯ УДАЛЕННОГО ДОСТУПА В ЧИТАЛЬНЫЙ ЗАЛ ЭЛЕКТРОННОЙ БИБЛИОТЕКИ	
	13
Жигадло В.Э., Терещенко П.Г., Рубинштейн Д.В. Россия, Санкт-Петербург, ООО «Максима», ФГБУ «Президентская библиотеки имени Б.Н. Ельцина», Москва, ФГУП «ГлавНИВЦ» Управления делами Президента Российской Федерации ЗАЩИЩЕННАЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА «ПРЕЗИДЕНТСКОЙ БИБЛИОТЕКИ ИМЕНИ Б.Н. ЕЛЬЦИНА»	
	17
Молдовян А.А., Молдовян Н.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ФУНКЦИОНАЛЬНОСТЬ, СТОЙКОСТЬ И БЕЗОПАСНОСТЬ КРИПТОГРАФИЧЕСКИХ МЕХАНИЗМОВ	
	23
Черешкин Д.С., Кононов А.А., Сичкарук А.В. Россия, Москва, Институт системного анализа РАН КОНЦЕПЦИЯ ОЦЕНКИ КРИТЕРИАЛЬНЫХ РИСКОВ В УПРАВЛЕНИИ БЕЗОПАСНОСТЬЮ БОЛЬШИХ РЕГИОНАЛЬНЫХ СИСТЕМ	
	27
ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ	31
Полончик О.Л. Россия, Архангельск, Северный (Арктический) федеральный университет имени М.В. Ломоносова РАЗВИТИЯ СИСТЕМ ДЛЯ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В БЕЗОПАСНОМ УПРАВЛЕНИИ РЕГИОНОМ НА ОСНОВЕ ДАННЫХ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ	
	31
ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	33
Большакова Л.В., Примакин А.И. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ИНФОРМАЦИОННЫЙ ПОДХОД ДЛЯ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА	
	33
Домбровская Л.А. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ОСНОВНЫЕ НАПРАВЛЕНИЯ, ПРИНЦИПЫ И УСЛОВИЯ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ИНФОРМАЦИИ	
	37
Жарова А.К. Россия, Москва, ФГБУН Институт государства и права РАН ЭЛЕКТРОННЫЕ СПОСОБЫ РАЗРЕШЕНИЯ КОНФЛИКТОВ И ЭЛЕКТРОННЫЕ СУДЫ	
	39
Золотенко В.А., Муханов Ю.В. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ФИЗИЧЕСКОЕ ВОСПИТАНИЕ КУРСАНТОВ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ МВД РОССИИ В ОБЩЕЙ СИСТЕМЕ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ – ОСНОВА БЕЗОПАСНОСТИ ОБЩЕСТВА	
	46

Парфенов Н.П. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛИЦЕЙСКИХ.....	49
Пономаренко А.В. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ПУТИ ДОСТИЖЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБЩЕСТВА РОССИИ.....	52
Примакин А.И. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России О НЕКОТОРЫХ ОСОБЕННОСТЯХ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БАЗЕ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ	55
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.....	59
Атисков А.А., Воробьев В.И., Федорченко Л.Н. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ОНТОЛОГИЧЕСКИЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ СТАНДАРТОВ И ВОЗМОЖНОСТИ ИХ ГАРМОНИЗАЦИИ.....	59
Афанасьев С.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ОНТОЛОГИЯ ТАКСОНОМИИ И БЕЗОПАСНОСТИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ	68
Блюм В.С., Заболотский В.П. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПАЦИЕНТОВ НА ОСНОВЕ ПЕРВИЧНОЙ МЕДИЦИНСКОЙ ИНФОРМАЦИИ	71
Десницкий В.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН КОНФИГУРАЦИОННАЯ МОДЕЛЬ КОМБИНИРОВАННОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ СО ВСТРОЕННЫМИ УСТРОЙСТВАМИ	77
Коноплев А.С. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет БЕЗОПАСНОЕ РАСПРЕДЕЛЕНИЕ ПОЛЬЗОВАТЕЛЬСКИХ ЗАПРОСОВ В ГРИД-СИСТЕМАХ.....	83
Харинов М.В., Заболотский В.П. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ПОДХОД К ПРОБЛЕМЕ СЕГМЕНТАЦИИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ ПОСРЕДСТВОМ ОПТИМИЗАЦИИ ПОСЛЕДОВАТЕЛЬНОСТИ РАЗБИЕНИЙ	87
Чечулин А.А., Котенко И.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН АНАЛИЗ ПРОИСХОДЯЩИХ В РЕАЛЬНОЙ СЕТИ СОБЫТИЙ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ МОДЕЛИРОВАНИЯ СЕТЕВЫХ АТАК.....	93
СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ	99
Баракин В.Н. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН СИСТЕМНЫЙ АНАЛИЗ СОВРЕМЕННОЙ КОНЦЕПЦИИ КАТАСТРОФООУСТОЙЧИВОСТИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	99
Березин А.Н., Биричевский А.Р., Молдовян Н.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ОСОБЕННОСТИ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФИМИРОВАНИЯ ПО СОСТАВНОМУ МОДУЛЮ КАК КРИПТОГРАФИЧЕСКОГО ПРИМИТИВА	104

Головки В.А., Киричек Р.В., Ларионов С.М., Чванов В.П. Россия, Санкт-Петербург, ФГУП «ЦентрИнформ» ЗАЩИТА ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОТ ПРЕДНАМЕРЕННЫХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЙ.....	108
Молдовян А.А., Морозова Е.В., Рыжков А.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» КОММУТАТИВНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ С УЧЕТОМ ТРУДНОСТИ РЕШЕНИЯ ЗАДАЧИ ФАКТОРИЗАЦИИ.....	116
Никифоров В.В., Шкиртиль В.И. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ЗАЩИТА ЦЕЛОСТНОСТИ ЛОКАЛЬНЫХ ДАННЫХ В РАСПРЕДЕЛЕННЫХ РЕАГИРУЮЩИХ СИСТЕМАХ.....	119
Рыжков А.В., Молдовян А.А., Березин А.Н. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ШИФРЫ С ВЕРОЯТНОСТНЫМ КОДИРОВАНИЕМ СООБЩЕНИЙ ТОЧКАМИ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ.....	126
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ.....	129
Устинов И.А., Игумнов В.В. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ.....	129
Александров А.М. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» РАЗЛОЖЕНИЕ ИНТЕГРАЛЬНЫХ ТРЕБОВАНИЙ ПО ВЕРОЯТНОСТЯМ ЛОЖНЫХ СИГНАЛОВ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ.....	131
Антонов А.А., Ридигер В.К., Федотов А.А., Филиппов А.С. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» ИСПОЛЬЗОВАНИЕ ВЫСОКОУРОВНЕВЫХ СРЕДСТВ ПРОЕКТИРОВАНИЯ ДЛЯ РАЗРАБОТКИ СНК НА БАЗЕ БМК 5516БЦ1Т1-002 В КРИТИЧЕСКИХ СИСТЕМАХ.....	132
Великовская С.А. Россия, Москва, Московский государственный университет технологий и управления им. К.Г. Разумовского, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» ГОРОДСКОЙ ИНТЕРНЕТ ДНЕВНИК.....	137
Виноградов А.А. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» ДОВЕРИТЕЛЬНАЯ ПРОГРАММНО-АППАРАТНАЯ ПЛАТФОРМА АСУ КРИТИЧЕСКИХ ИНФРАСТРУКТУР.....	140
Волкова А.В. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» СИНТЕЗ ОПТИМАЛЬНОГО МАНИПУЛЯЦИОННОГО КОДА ДЛЯ СИГНАЛЬНО-КОВОДНОЙ КОНСТРУКЦИИ НА ОСНОВЕ ТРЁХМЕРНОЙ СИМПЛЕКС-РЕШЁТКИ.....	143
Гук И.И., Путилин А.Н., Сиротинин И.В., Хвостунов Ю.С. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» АДАПТИВНАЯ СИСТЕМА ДЕКАМЕТРОВОЙ РАДИОСВЯЗИ С ПОЛНОДИАПАЗОННОЙ ПЕРЕСТРОЙКОЙ РАБОЧЕЙ ЧАСТОТЫ И ПРЕДВАРИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ ТРАССОВЫХ ИСПЫТАНИЙ ЕЁ ФРАГМЕНТА.....	146
Ефимов Е.А. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПРИ ЗАСЕКРЕЧИВАНИИ.....	149

Иванов В.И. Россия, Санкт-Петербург, «Региональный Центр Защиты Информации «ФОРТ» МЕТОДЫ ОБРАБОТКИ И АНАЛИЗА ДАННЫХ ПРИ АДАПТИВНОМ УПРАВЛЕНИИ ИНЦИДЕНТАМИ В ГЕТЕРОГЕННЫХ СЕТЯХ СВЯЗИ	150
Копыльцов А.А., Нечитайленко Р.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» ОБЕСПЕЧЕНИЕ ПОРОГОВОЙ БЕЗОПАСНОСТИ ОБРАБОТКИ СЛАБО ФОРМАЛИЗОВАННОЙ ИНФОРМАЦИИ ПРИ РАСПРЕДЕЛЕННОМ УПРАВЛЕНИИ С ЦЕЛЬЮ ПРИНЯТИЯ РЕШЕНИЙ	154
Мартьянов А.Г. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ	155
Приходько М.А. Россия, Москва, Московский государственный горный университет МУЛЬТИАГЕНТНЫЕ ТЕХНОЛОГИИ В СИСТЕМАХ ДИСТАНЦИОННОГО ОБУЧЕНИЯ.....	158
Расторгуев В.Я., Виноградов А.А. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» УСИЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРИТИЧЕСКИХ СИСТЕМАХ НЕПРЕРЫВНОГО ФУНКЦИОНИРОВАНИЯ ПУТЕМ ВИРТУАЛИЗАЦИИ ЭЛЕМЕНТОВ ИХ СИСТЕМ УПРАВЛЕНИЯ.....	160
Тимохин А.П., Бочкарёв В.В. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» МЕТОДЫ ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ КОНСТРУКЦИИ АППАРАТУРЫ ДЛЯ СИСТЕМ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ И ДВОЙНОГО НАЗНАЧЕНИЯ	165
Черкесов Г.Н. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» ОЦЕНКА ЖИВУЧЕСТИ И ОТКАЗОБЕЗОПАСНОСТИ МАЖОРИРОВАННОЙ ПАМЯТИ С КЛАСТЕРНОЙ СТРУКТУРОЙ.....	166
Чистяков И.В., Орлов Д.Р. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» МЕТОДЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА УСТРОЙСТВАХ ХРАНЕНИЯ.....	170
Штогрин И.Р. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс» ОБЕСПЕЧЕНИЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ЭТАПЕ СТЕНДОВОЙ ОТРАБОТКИ ИЗДЕЛИЙ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ СИСТЕМ	172
Щёткин И.Е. Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс», Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова ИНВЕСТИЦИОННО-ИННОВАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ ПРЕДПРИЯТИЯ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ В ЦЕЛЯХ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	175
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГИДРОМЕТЕОРОЛОГИИ.....	179
Александрова Л.В., Ткаченко Н.Н. Россия, Санкт-Петербург, Российский государственный гидрометеорологический Университет ЗАЩИТА ГЕОИНФОРМАЦИОННЫХ СИСТЕМ И ГИДРОМЕТЕОРОЛОГИЧЕСКИХ БАЗ ДАННЫХ	179
ОГЛАВЛЕНИЕ.....	182