



«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР–2009)»

VI САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 28-30 октября 2009 года

ТРУДЫ КОНФЕРЕНЦИИ

Санкт-Петербург

2010



VI САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

**«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
РЕГИОНОВ РОССИИ (ИБРР–2009)»**

Санкт-Петербург, 28-30 октября 2009 года

ТРУДЫ КОНФЕРЕНЦИИ

Санкт-Петербург

2010

Информационная безопасность регионов России (ИБРР-2009). VI Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009)». Санкт-Петербург, 28-30 октября 2009 г.: Труды конференции \ СПОИСУ. – СПб, 2010. – 226 с. ISBN 978-5-904031-95-4.

Сборник содержит труды VI Санкт-Петербургской Межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2009)», учредителями которой являются: 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.

Сборник охватывает широкий круг направлений: государственная политика обеспечения информационной безопасности регионов России, правовые аспекты информационной безопасности, безопасные информационные технологии, современные средства защиты информации, информационная безопасность телекоммуникационных сетей, подготовка и переподготовка 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, Л.Н. Федорченко

Публикуется в авторской редакции

Подписано в печать 30.12.2009. Формат 60х84 $\frac{1}{8}$. Бумага офсетная.
Печать – ризография. Усл. печ. л. 26,27. Тираж 500 экз. Заказ № 972

Отпечатано в ООО «Политехника-сервис»
191011, Санкт-Петербург, ул. Инженерная, 6

ISBN 978-5-904031-95-4

© Санкт-Петербургское Общество информатики,
вычислительной техники, систем связи и
управления (СПОИСУ), 2010 г.

© Авторы, 2010 г.



VI ST. PETERSBURG INTERREGIONAL CONFERENCE

**«INFORMATION SECURITY
OF RUSSIAN REGIONS (ISRR – 2009)»**

St. Petersburg, October 28-30, 2009

**PROCEEDINGS
OF THE CONFERENCE**

**St. Petersburg
2010**



УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ «ИБРР-2009»

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

СОУСТРОИТЕЛИ КОНФЕРЕНЦИИ «ИБРР-2009»

- Российский фонд фундаментальных исследований
- Государственный научный центр РФ - Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики
- ФГУП «Научно-исследовательский институт «Рубин»
- ФГУП «Научно-производственное объединение «Импульс»
- ФГУП «ЦентрИнформ»
- СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
- ЗАО «Ассоциация специалистов информационных систем»
- ЗАО «Метроком»
- ЗАО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
- ЗАО «Санкт-Петербургский Региональный Центр защиты информации»
- ЗАО «Эврика»
- ООО «Компания «Марвел»
- ООО «Компания «Radio Net»
- ОАО «Северо-Западный Телеком»
- Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
- Санкт-Петербургский государственный политехнический университет
- Санкт-Петербургский государственный университет водных коммуникаций
- Санкт-Петербургский государственный университет технологии и дизайна
- Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
- Санкт-Петербургский университет МВД России
- Санкт-Петербургский институт экономики и бизнеса
- 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 «ИБРР-2009»

Матвиенко Валентина Ивановна	Губернатор Санкт-Петербурга
Тюльпанов Вадим Альбертович	Председатель Законодательного собрания Санкт-Петербурга
Сердюков Валерий Павлович	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
Щеголев Игорь Олегович	Министр связи и массовых коммуникаций Российской Федерации
Фурсенко Андрей Александрович	Министр образования и науки Российской Федерации
Никандров Николай Дмитриевич	Президент Российской академии образования
Федоров Александр Вячеславович	Первый заместитель Министра юстиции Российской Федерации
Макаров Евгений Иванович	Помощник полномочного представителя Президента Российской Федерации в Северо-Западном федеральном округе

ПРЕЗИДИУМ КОНФЕРЕНЦИИ «ИБРР-2009»

Тихонов Валерий Владимирович	Вице-губернатор Санкт-Петербурга
Цивирко Евгений Геннадьевич	Председатель Комитета по информатизации и связи Санкт-Петербурга
Максимов Андрей Станиславович	Председатель Комитета по науке и высшей школе Санкт-Петербурга
Акулич Владимир Александрович	Генеральный директор ОАО «Северо-Западный Телеком»
Гусев Владимир Сергеевич	Вице-президент Международного Банка «Санкт-Петербург»
Петров Владимир Гавриилович	Заместитель руководителя Управления Федеральной службы технического и экспортного контроля России по Северо-Западному федеральному округу
Пешехонов Владимир Григорьевич	Генеральный директор ГНЦ РФ-ОАО «Концерн «ЦНИИ «Электроприбор»
Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга
Шульц Владимир Леопольдович	Заместитель президента Российской академии наук
Юсупов Рафаэль Мидхатович	Директор Санкт-Петербургского института информатики и автоматизации Российской академии наук

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2009»

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 Комитета по информатизации и связи Санкт-Петербурга
-------------------------------	---

Члены Организационного Комитета

Александров Анатолий Михайлович	Заместитель начальника Центра анализа и экспертизы ФГУП «Научно-производственное объединение «Импульс»
Бакурадзе Дмитрий Викторович	Ученый секретарь Санкт-петербургского института информатики и автоматизации Российской академии наук
Блажис Анатолий Константинович	Генеральный директор ЗАО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
Богданов Владимир Николаевич	Директор ФГУП «ЦентрИнформ»
Васильев Владимир Николаевич	Ректор Санкт-Петербургского государственного университета информационных технологий, механики и оптики
Вус Михаил Александрович	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Гирдин Сергей Алексеевич	Президент ООО «Компания «Марвел»
Гладков Геннадий Леонидович	Ректор Санкт-Петербургского государственного университета водных коммуникаций
Гоголь Александр Александрович	Ректор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
Григорьев Владимир Александрович	Генеральный директор Компании «Radio Net»
Гуца Анатолий Григорьевич	Главный специалист СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Жданов Сергей Николаевич	Заместитель генерального директора ЗАО «ВТБ-Девелопмент»
Демидов Александр Алексеевич	Первый заместитель председателя Комитета по работе с исполнительными органами государственной власти и взаимодействию с органами местного самоуправления Администрации Губернатора Санкт-Петербурга
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	Директор по специальным проектам ЗАО «Синтерра»
Жигадло Валентин Эдуардович	Профессор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
Заборовский Владимир Сергеевич	Заведующий кафедрой Санкт-Петербургского государственного политехнического университета
Зегжда Петр Дмитриевич	Директор Специализированного центра защиты информации, заведующий кафедрой информационной безопасности компьютерных систем Санкт-Петербургского государственного политехнического университета
Зубков Юрий Сергеевич	Советник первого заместителя председателя Комитета по градостроительству и архитектуре
Игумнов Владимир Вячеславович	Главный конструктор ФГУП «Научно-производственное объединение «Импульс»

Ипатов Олег Сергеевич	Заведующий кафедрой Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова
Исаев Борис Анатольевич	Директор СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Касаткин Виктор Викторович	Декан ФПК Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова
Котенко Денис Алексеевич	Генеральный директор ЗАО «Ассоциация специалистов информационных систем»
Кузичкин Александр Васильевич	Исполнительный директор Компании «Radio Net»
Кузьмин Юрий Григорьевич	Ученый секретарь Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления, начальник сектора Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова
Куренков Евгений Владимирович	Директор Санкт-Петербургского Научно-технического центра ФГУП «Научно-производственное предприятие «Гамма»
Марков Вячеслав Сергеевич	Ученый секретарь Объединенного научного совета Санкт-Петербургского Научного центра Российской академии наук
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»
Пашкевич Константин Эдуардович	И.О. генерального директора ЗАО «Метроком»
Романов Виктор Егорович	Президент Санкт-Петербургского государственного университета технологии и дизайна
Рунеев Анатолий Юрьевич	Генеральный директор ФГУП «Научно-исследовательский институт «Рубин»
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»
Федорченко Людмила Николаевна	Научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Цыулев Сергей Валентинович	Начальник сектора информационно-компьютерной безопасности 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-2009»

Председатель Программного Комитета

Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга
-------------------------	---

Заместители председателя Программного Комитета

Жигадло Валентин Эдуардович	Профессор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
Молдовян Александр Андреевич	Заместитель директора Санкт-Петербургского института информатики и автоматизации Российской академии наук по информационной безопасности

Члены Программного Комитета — руководители секций

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

Цивирко Е.Г.

Россия, Санкт-Петербург, Комитет по информатизации и связи Санкт-Петербурга ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ САНКТ-ПЕТЕРБУРГА

В Концепции национальной безопасности Российской Федерации информационная безопасность позиционируется как одно из приоритетных направлений деятельности по обеспечению безопасности российского общества. В современных условиях повышение эффективности деятельности в сфере государственного управления приобретает первостепенное значение как для органов государственной власти Российской Федерации в целом, так и для исполнительных органов государственной власти (ИОГВ) Санкт-Петербурга в частности. При этом следует отметить, что автоматизация деятельности органов государственной власти Санкт-Петербурга является одним из ключевых направлений повышения её эффективности.

Можно с уверенностью заявлять, что информация, представленная в электронном виде и накопленная за последние годы в различных автоматизированных информационных системах ИОГВ Санкт-Петербурга, стала критически важным ресурсом для города. По оценке специалистов практически все базы данных автоматизированных информационных систем ИОГВ Санкт-Петербурга содержат информацию, включающую: персональные данные жителей города, коммерческую тайну хозяйствующих субъектов, медицинскую тайну, сведения об усыновлении, служебную тайну ИОГВ Санкт-Петербурга и т.п.

Наряду с информацией ограниченного доступа, важным ресурсом является открытая информация о деятельности органов власти, для которой должна быть обеспечена одновременно и доступность, и защита от модификации. В связи с этим, особую проблему вызывает необходимость приведения информационных систем в соответствие с требованиями федеральных законов № 52-ФЗ «О персональных данных» и №8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» к 1 января 2010 года.

В Санкт-Петербурге разработаны и разрабатываются соответствующие нормативные, правовые акты и методические документы (распоряжения Губернатора и Администрации Санкт-Петербурга, постановления Правительства Санкт-Петербурга, руководства, положения, инструкции и др.) для организации работ по защите информации ограниченного доступа в соответствии с требованиями Закона РФ «О государственной тайне», Федеральных законов «Об информации, информационных технологиях и о защите информации», «О персональных данных», а также других законодательных актов и руководящих документов федеральных уполномоченных органов.

Основными факторами, определяющими необходимость повышенного внимания к вопросам защиты информации в органах государственной власти Санкт-Петербурга и на критически важных объектах, являются:

1. Приграничное расположение Санкт-Петербурга, близость государств – членов и потенциальных членов НАТО, а также наличие на территории Санкт-Петербурга значительного числа консульств, иностранных представительств и совместных предприятий со странами дальнего и ближнего зарубежья.

2. Санкт-Петербург является одним из главных российских центров сосредоточения предприятий военно-промышленного комплекса, наукоемких производств, научных организаций, занимающихся фундаментальными и прикладными проблемами, что вызывает повышенный интерес со стороны иностранных представительств различного уровня к информационным ресурсам этих объектов.

3. Широкое использование в Санкт-Петербурге межрегиональных и глобальных информационных систем, накапливающих и передающих большие объемы информации, уязвимость которых может привести к возникновению критических ситуаций, связанных с нарушениями режимов безопасности информации в системах управления экологически опасными производствами, транспортом, энергетикой, кредитно-финансовыми учреждениями и другими системами.

4. Рост преступлений, осуществляемых с использованием информационных технологий, которые связаны с несанкционированным доступом к пользовательской информации и с распространением вирусных программ.

5. Попытки криминальных структур использовать открытые телекоммуникационные сети и автоматизированные информационные системы для осуществления финансовых махинаций и мошенничества.

6. Использование в исполнительных органах государственной власти Санкт-Петербурга и в подведомственных им предприятиях, учреждениях и организациях незащищенной от утечки информации и не сертифицированных импортных технических и программных средств.

Все это обуславливает необходимость проведения мероприятий по обеспечению безопасности информации, которые в настоящее время стали неотъемлемой составной частью деятельности органов государственной власти, учреждений и организаций Санкт-Петербурга.

Несвоевременное принятие мер по защите информации может привести к значительному количеству негативных последствий финансового, социального и юридического характера.

На 2010 год определены следующие основные направления деятельности в области защиты информации:

1. Обеспечение эффективного управления системой защиты информации в ИОГВ Санкт-Петербурга.

2. Разработка и реализация организационно-технических мероприятий по защите информации в области:

3. Создание и развитие инфраструктурных и обеспечивающих систем

4. Организация и проведение контроля состояния защиты информации в ИОГВ Санкт-Петербурга.

5. Организация подготовки и переподготовки специалистов по защите информации в ИОГВ Санкт-Петербурга.

В ближайшей перспективе предполагается решить следующие задачи:

1. Продолжить формирование комплексной системы защиты информации в Санкт-Петербурге. Сформировать систему защиты персональных данных в исполнительных органах государственной власти Санкт-Петербурга, как подсистему комплексной системы защиты информации в Санкт-Петербурге.

2. Разработать план формирования системы защиты персональных данных в исполнительных органах государственной власти Санкт-Петербурга

3. Активизировать взаимодействие с Управлением ФСТЭК России по Северо-Западному федеральному округу, Управлением ФСБ России по Санкт-Петербургу и Ленинградской области и Управлением Роскомнадзора по Санкт-Петербургу и Ленинградской области по направлению оказания методической помощи операторам наиболее важных специальных информационных систем персональных данных.

В заключение хотелось бы отметить, что качественное практическое решение основных вопросов информационной безопасности в Санкт-Петербурге остро нуждается в четко проработанной нормативной базе федерального уровня.

Федоров А.В.

Россия, Москва, Министерство юстиции Российской Федерации

О ГАРМОНИЗАЦИИ И УНИФИКАЦИИ ЗАКОНОДАТЕЛЬСТВА О ГОСУДАРСТВЕННОЙ ТАЙНЕ В ГОСУДАРСТВАХ – УЧАСТНИКАХ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

После распада Советского Союза и образования Содружества Независимых Государств (СНГ) возникла потребность разработки механизма принятия согласованных решений на всем пространстве СНГ, обеспечивающих интересы государств – участников Содружества.

В частности, развитие сотрудничества государств – участников СНГ обусловило постановку вопроса о принятии решений в рамках Содружества по унификации и гармонизации национальных законодательств о защите сведений, составляющих государственную тайну, в целях выработки и реализации согласованной политики и совместных мер защиты таких сведений.

При этом в качестве механизма унификации и гармонизации национальных законодательств была предложена разработка модельных законов и рекомендаций.

Соответствующими полномочиями наделена Межпарламентская Ассамблея (МПА) СНГ [1], которой для обеспечения унификации и гармонизации национальных законодательств государств – участников Содружества, в частности, принимаются модельные законодательные акты (модельные кодексы и модельные законы) рекомендательного характера для формирования и осуществления согласованной законодательной деятельности государств – участников СНГ по вопросам, представляющим общий интерес, а также для приведения законодательства государств – участников Содружества в соответствие с международными договорами, как заключенными в рамках Содружества, так и иными.

В первые годы работы МПА СНГ вопросы защиты государственной тайны были учтены при разработке уголовно-правовых и уголовно-процессуальных модельных актов. В частности, они

нашли отражение в принятых в качестве рекомендательных законодательных актов модельном Уголовном [2] и модельном Уголовно-процессуальном [3] кодексах.

Следующим этапом унификации и гармонизации в этой сфере стало принятие модельного закона «О государственных секретах» [4]. Положения данного модельного закона уже стали предметом научного анализа [5].

В то же время само по себе принятие модельных законов проблему не решало. Требовалось принятие соответствующих нормативно-правовых решений на национальном уровне.

Таким образом, принятие МПА СНГ указанных модельных законов создало условия для дальнейшего совершенствования, унификации и гармонизации национальных законодательств, способствовало, с одной стороны, разработке необходимых национальных актов и повышению эффективности деятельности компетентных органов государств – участников Содружества по вопросам защиты государственной тайны, с другой стороны, – развитию экономического, военно-технического и ряда иных видов сотрудничества.

Тем не менее, не все прогрессивные новации модельных законов нашли отражение в национальных законах и по-прежнему обоснована постановка вопроса об их реализации при развитии национальных законодательств.

Применительно к Российской Федерации это актуально в части касающейся уголовно-процессуального законодательства. Так, изучение имеющихся проблемных вопросов, возникающих при осуществлении уголовно-процессуальной деятельности по делам, связанным с государственной тайной, показывает, что не все из них получили должное разрешение в Уголовно-процессуальном кодексе Российской Федерации и необходима более детальная регламентация охраны государственной тайны в уголовном процессе [6,7].

Для этого целесообразно использовать нашедшие отражение в Модельном уголовно-процессуальном кодексе для государств – участников СНГ положения, связанные с обеспечением защиты государственной тайны при осуществлении уголовно-процессуальной деятельности.

Указанный рекомендательный законодательный акт содержит специальную статью, названную «Охрана государственной тайны».

К сожалению, разработчики Уголовно-процессуального кодекса Российской Федерации [8,9] не восприняли нормы модельного законодательства, и принятый кодекс, повторяя и детализируя отраженные ранее в УПК РСФСР нормы, регламентирующие особый порядок производства следственных действий по делам, связанным с государственной тайной, не содержит специальной статьи или специального раздела, отражающих все особенности охраны государственной и иных видов тайн в уголовном процессе.

В этой связи с учетом имеющегося модельного законодательства государств – участников СНГ представляется обоснованным нашедшее отражение в юридической литературе предложение выделить в Уголовно-процессуальном кодексе Российской Федерации по аналогии с разделом XVII «Особенности производства по уголовным делам в отношении отдельных категорий лиц» самостоятельный раздел «Использование в уголовном процессе сведений, составляющих охраняемую законом тайну» [10], в котором предусмотреть основания и пределы получения в процессе доследственной проверки и производства по уголовному делу сведений, составляющих ту или иную охраняемую законом тайну, а также другие особенности производства по уголовным делам, связанным с государственной и иными видами тайн, и уголовно-процессуальные средства их защиты.

Кроме того, рассматривая модельное законодательство в качестве основы для унификации и гармонизации законодательств государств – участников СНГ, необходимо дальнейшее совершенствование и этой основы. В частности, в системе СНГ в настоящее время функционирует ряд международных организаций, деятельность которых требует получения сведений, относимых национальными законодательствами к государственной тайне (государственным секретам). Однако модельное законодательство (ст. 28 модельного закона «О государственных секретах») не предусматривает возможность передачи сведений, составляющих государственную тайну, международным организациям.

В то же время в российский Федеральный закон «О государственной тайне» (ст. 18) уже включены положения о передаче сведений, составляющих государственную тайну, другим государствам или международным организациям [11–17]. Возможность передачи международным организациям сведений, составляющих государственную тайну, также предусмотрена ст. 29 Закона Республики Таджикистан от 22 апреля 2003 г. №4 «О государственной тайне».

С учетом изложенного, а также учитывая дальнейшее развитие интеграционных процессов, представляется целесообразным рассмотреть вопрос о включении соответствующих положений и в модельное законодательство.

Следует также учитывать, что в документах СНГ в качестве механизма реализации унификации и гармонизации предлагается не только разработка модельных законов, но и рекомендаций Межпарламентской Ассамблеи СНГ. Таким образом, Межпарламентской Ассамблеей СНГ для обеспечения унификации национальных законодательств государств – участников

Содружества принимаются: 1) модельные законодательные акты (модельные кодексы и модельные законы) рекомендательного характера и 2) рекомендации (предложения) по сближению законодательств государств – участников СНГ, в том числе по приведению их в соответствие с положениями международных договоров, участниками которых являются государства – участники СНГ.

В имеющихся исследованиях, за редким исключением [18], упускается вопрос о роли рекомендаций для унификации законодательства как в рамках СНГ, так и в рамках другой, более эффективной международной организации – Организации Договора о коллективной безопасности (ОДКБ).

В качестве удачного примера использования такого механизма унификации можно привести Рекомендации по унификации и гармонизации законодательства государств – членов Организации Договора о коллективной безопасности в сфере борьбы с международным терроризмом, незаконным оборотом наркотических средств и психотропных веществ, согласованные Постановлением совместного заседания членов МПА СНГ – членов Организации Договора о коллективной безопасности и Комитета секретарей советов безопасности государств – членов ОДКБ от 16 апреля 2004 г.

Представляется целесообразным подготовить подобного рода рекомендации на основе анализа модельного закона «О государственных секретах» и соответствующих национальных законов государств – участников СНГ (Закона Республики Армения от 3 декабря 1996г. "О государственной и служебной тайне", Закона Республики Беларусь от 29 ноября 1994 г. №3410–XII «О государственных секретах», Закона Республики Казахстан от 15 марта 1999 г. №349–1 "О государственных секретах», Закона Кыргызской Республики от 14 апреля 1994 г. № 1476–XII «О защите государственных секретов», Закона Российской Федерации от 21 июля 1993 г. №5485–1 "О государственной тайне", Законов Республики Таджикистан от 10 мая 2002 г. №57 "О перечне сведений, составляющих государственную тайну" и от 22 апреля 2003 г. №4 «О государственной тайне», Закона Республики Узбекистан от 7 мая 1993 г. №848–XII «О защите государственных секретов» и др.).

Предметом анализа могли бы стать и двусторонние соглашения [19–24] о взаимной защите секретной информации с целью подготовки унифицированного многостороннего соглашения в указанной сфере.

СПИСОК ЛИТЕРАТУРЫ

1. Конвенция о Межпарламентской Ассамблее государств – участников Содружества Независимых Государств от 26 мая 1995 (ст. 4) // Вестник Межпарламентской Ассамблеи. 1995. №3 (10). С.224–234.
2. Информационный бюллетень МПА СНГ. 1996. №10. С.83; Приложение № 1 к «Информационному бюллетеню». 1996. №10. С.84–216.
3. Информационный бюллетень МПА СНГ. 1996. №10. С.83–84; Приложение №2 к «Информационному бюллетеню». 1996. №10. С.3–373.
4. Информационный бюллетень МПА СНГ. 2003. №31. С.230–261.
5. Верютин В.Н. Анализ основных положений Модельного закона СНГ «О государственных секретах» на основе общеправовых принципов // «Черные дыры» в Российском законодательстве. 2009. №6. С.51 – 54.
6. Государственная тайна и её защита в Российской Федерации / Под общ. ред. М.А. Вуса и А.В. Федорова. – СПб., 2007. С.30–333.
7. Федоров А.В. Тайноведческий уголовный процесс // От культа секретности к информационной культуре. – СПб., 2008. С.65–81.
8. Собрание законодательства Российской Федерации. 2001. №52 (Ч.I). Ст. 4921.
9. Собрание законодательства Российской Федерации. 2002. №22. Ст. 2027.
10. Смолькова И.В. Гласность и тайна в уголовном процессе // Законность. 1998. № 7. С. 42.
11. Собрание законодательства Российской Федерации. 1997. №41. Ст. 4673.
12. Собрание законодательства Российской Федерации. 2003. №27. Ст. 2700.
13. Собрание законодательства Российской Федерации. 2003. №46. Ст. 4449.
14. Собрание законодательства Российской Федерации. 2004. №27. Ст. 2711.
15. Собрание законодательства Российской Федерации. 2004. №35. Ст. 3607.
16. Собрание законодательства Российской Федерации. 2007. №49. Ст. 6055, 6079.
17. Собрание законодательства Российской Федерации. 2009. №49. Ст. 3617.
18. Вус М.А. Рекомендации по совершенствованию и гармонизации законодательства о защите государственной тайны для государств – членов Организации Договора о коллективной безопасности (ОДКБ). // Условия реализации прав граждан и организаций на основе информационных технологий. – М.: ИГ и П РАН, ИПО « У Никитских ворот», 2010. С.202–207.
19. Соглашение между Правительством Российской Федерации и Правительством Республики Армения о взаимной защите секретной информации (Ереван, 5 ноября 2002 г.).
20. Соглашение между Российской Федерацией и Республикой Беларусь о взаимном обеспечении защиты государственной тайны Российской Федерации и государственных секретов Республики Беларусь (Минск, 20 января 2003 г.).
21. Соглашение между Правительством Российской Федерации и Правительством Республики Казахстан о взаимной защите секретной информации (Уральск, 7 июля 2004 г.).
22. Соглашение между Правительством Российской Федерации и Правительством Киргизской Республики о взаимной защите секретной информации (Москва, 19 сентября 2003 г.).
23. Соглашение между Правительством Российской Федерации и Правительством Республики Таджикистан о взаимной защите секретной информации (Душанбе, 22 января 2003 г.).
24. Соглашением между Правительством Российской Федерации и Правительством Республики Узбекистан о взаимной защите секретной информации (от 31 октября 2003 г.).

Кононов А.А., Стилиславский А.Б., Цыгичко В.Н., Черешкин Д.С.

Россия, Москва, Институт системного анализа РАН

АВТОМАТИЗИРОВАННЫЙ КОМПЛЕКС СРЕДСТВ ОБЕСПЕЧЕНИЯ АНТИТЕРРОРИСТИЧЕСКОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ ТРАНСПОРТНОЙ СИСТЕМЫ

Аннотация

В статье описывается созданный коллективом разработчиков ИСА РАН аппаратно-программный комплекс «РискДетектор», реализующий в режиме диалога «ЭВМ – пользователь» основные процедуры обеспечения транспортной безопасности, определенные директивными документами. Идеология комплекса была разработана и опубликована ранее и предполагает, что система управления рисками нарушения транспортной безопасности строится на основе категорирования объектов транспортной инфраструктуры и транспортных средств путем оценки возможного ущерба при реализации угроз террористического воздействия.

1. Основные положения Концепции обеспечения транспортной безопасности

Использованная при создании аппаратно-программного комплекса (АПК) Концепция обеспечения безопасности объектов транспортной инфраструктуры и транспортных средств на основе категорирования была опубликована [1–3] и обсуждалась на двух международных Форумах по безопасности, кратко рассмотрим только ряд основных ее положений.

Для определения минимального объема финансовых средств, необходимых для создания и эксплуатации единой государственной системы обеспечения транспортной безопасности, и рационального распределения выделяемых средств, нужно определить требуемый уровень защиты опасных объектов транспорта (здесь и далее под объектами транспорта понимаются объекты транспортной инфраструктуры и транспортные средства) всех видов транспорта в зависимости от степени их опасности по потенциальному ущербу с учетом вероятности (степени риска) совершения на них террористической атаки и ее негативных политических последствий.

Эта задача решается на основе идентификации и категорирования объектов транспорта, что обеспечивает выделение объектов, требующих постоянного контроля за их безопасностью, и дифференциации требований к системам их антитеррористической и противокриминальной защиты. Другими словами, учитывая очень большое количество и, с одной стороны – разнообразие такого рода объектов, а, с другой – их функциональное единство (например, множество одинаковых по функциям, но различных по «мощности» аэропортов, вокзалов, морских и речных портов, транспортных средств и т.д.), необходимо провести их ранжирование (категорирование) по характерным признакам. Эта процедура позволяет выделить типовые объекты транспорта в каждой категории и далее формировать типовые требования и решения по обеспечению безопасности.

Требования к защите объектов транспорта должны обеспечивать минимально необходимые и достаточные уровни безопасности в соответствии с установленными категориями их потенциальной опасности, с учетом критериев оценки возможного ущерба интересам личности, общества и государства. Концепция предусматривает, что оценка эффективности имеющейся или создаваемой на объекте транспорта системы обеспечения транспортной безопасности выполняется на основе оценки рисков нарушения безопасности, возникающих при невыполнении или не полном выполнении комплекса директивных требований по защите всех уязвимостей объекта транспорта (оценка уязвимости). Соответственно, управление безопасностью объекта транспорта ориентировано на снижение рисков нарушения безопасности объекта, т.е. на выполнение всего комплекса директивных требований, соответствующего имеющейся категории объекта.

Система обеспечения транспортной безопасности на основе категорирования в соответствии со статьей 2 Федерального Закона «О транспортной безопасности» предполагает последовательное решение следующих задач:

- предварительный анализ текущего состояния уязвимости объекта;
- идентификацию и категорирование опасных объектов;
- индексацию всех типов опасных объектов и транспортных средств в соответствии с категорией и внутривидовой классификацией объекта;
- построение моделей угроз для каждого типа объектов транспорта;
- оценку допустимой стоимости системы обеспечения безопасности каждого типа объектов транспорта с учетом его индекса и величины потенциального ущерба;
- построение профилей защиты для каждого типа объектов транспорта в соответствии с их индексом, моделями угроз и допустимой стоимостью системы защиты;
- формирование требований для каждого типа объектов транспорта в соответствии с его индексом и профилем защиты;
- оценку уязвимости объектов транспорта в зависимости от степени выполнения на них требований по обеспечению безопасности;
- периодический контроль (мониторинг) выполнения требований по обеспечению безопасности на опасных объектах транспортной инфраструктуры;

– составление субъектом транспортной инфраструктуры плана повышения защищенности объекта по результатам мониторинга и на основании официального заключения по оценке уязвимости объекта, утверждение составленного плана в установленном порядке.

Перечисленные задачи решаются путем последовательной реализации специальных вычислительных процедур, состав которых приведен на рисунке 1.



Рис.1. Процедуры решения задач обеспечения безопасности

2. Практика применения АПК «РискДетектор» для решения задач обеспечения транспортной безопасности

Были разработаны и реализованы в АПК алгоритмы решения всех входящих в данную процедуру задач. На рисунке 2–4 показаны соответствующие алгоритмы. Эти алгоритмы реализуются АПК «РискДетектор», который представляет собой комбинацию двух самостоятельных взаимосвязанных составляющих – «РискДетектор-Анализ» и «РискДетектор-Контроль». Исходя из обозначений на рисунке 1, отметим, что комплекс «РискДетектор-Анализ» обеспечивает реализацию процедур 1А, 2А и 3А, образующих верхнюю ветвь проблемного поля. В большинстве случаев это задачи, решаемые на уровне руководства того вида транспорта, к которому принадлежит данный объект, а результаты полученных решений являются типовыми для всех аналогичных объектов.

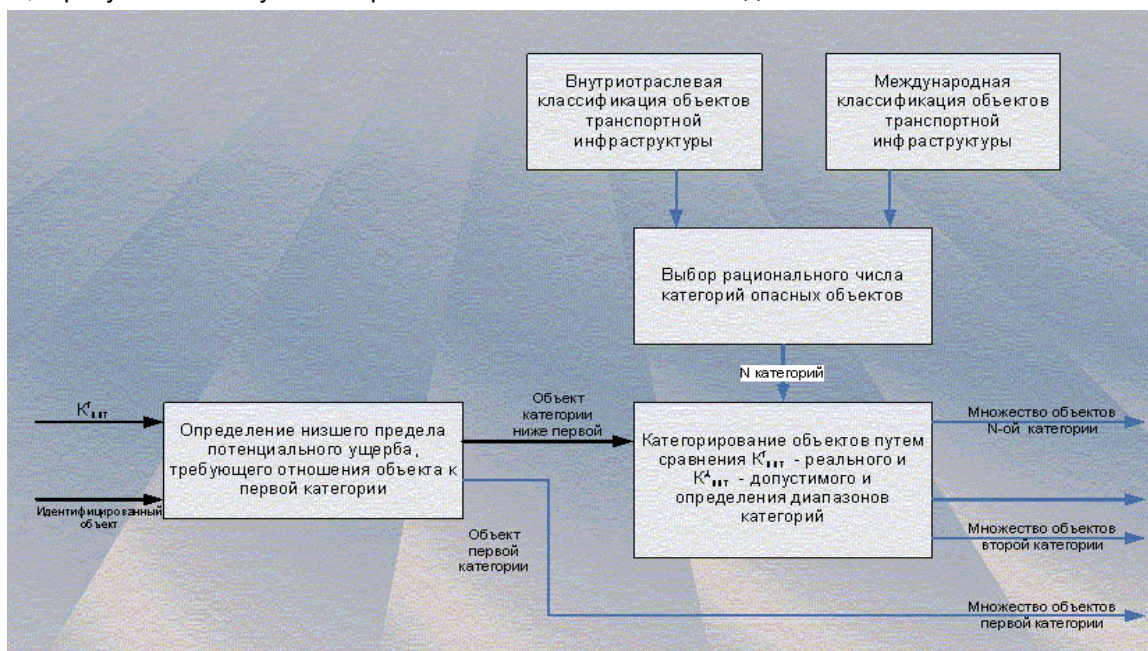


Рис.2. Структурный алгоритм выполнения процедуры «Категорирование»

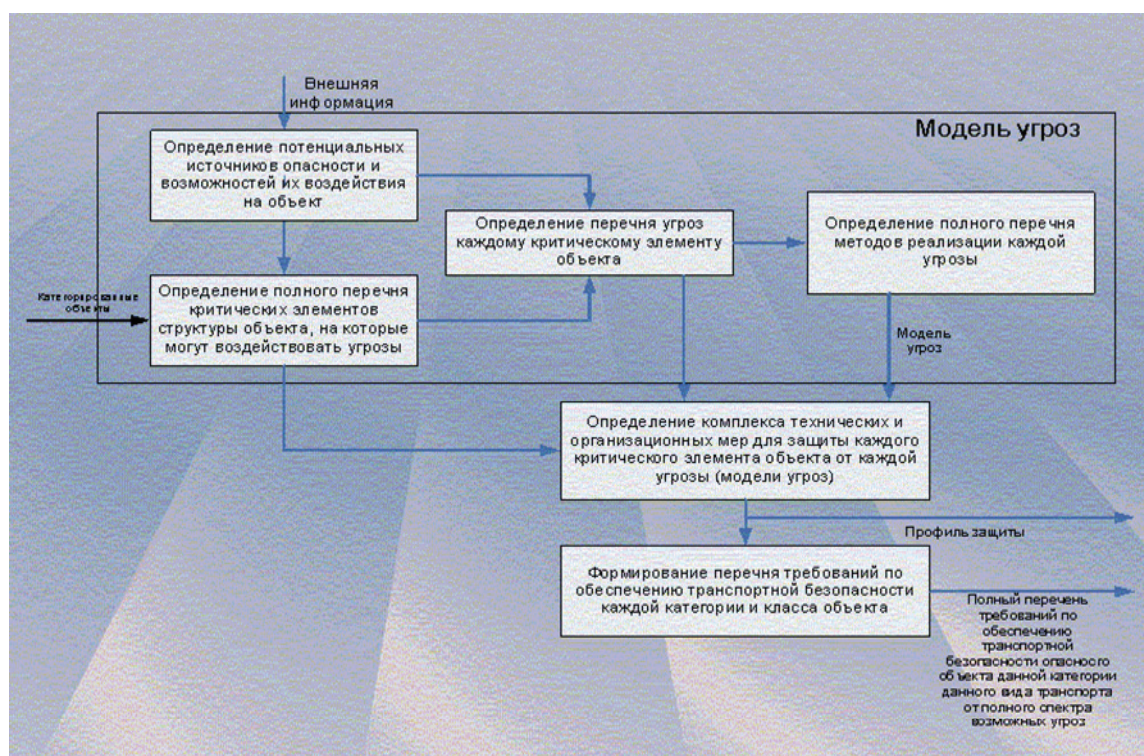


Рис.3. Структурный алгоритм выполнения процедуры «Построение профилей защиты объекта»



Рис.4. Операции, реализующие процедуру «Оценка уязвимости»

Эта «ветвь» комплекса обеспечивает решение таких задач, как:

- построение модели угроз и модели нарушителя;
- идентификация критически важных объектов (КВО) данного вида транспорта;
- идентификация критических точек и рисков реализации террористических актов по КВО данного типа;
- оценка уязвимостей КВО данного типа;
- категорирование объектов транспорта;
- определение стоимостных параметров мероприятий по обеспечению безопасности;
- анализ системы требований по обеспечению безопасности объектов транспорта;
- ведение реестра категорированных объектов транспорта.

Вторая часть комплекса – «РискДетектор-Контроль», решает задачи процедур 1К, 2К, 3К и 4К («нижняя ветвь» процедур на рисунке 1). Предполагается, что эта часть комплекса будет использоваться непосредственно на объекте для решения следующих задач:

- определение состава нормативных требований по обеспечению безопасности объекта i-ой категории и построение профилей защиты для критических точек объекта;
- контроль выполнения требований по обеспечению безопасности;
- выявление уязвимых мест и оценка уязвимости объекта;
- ведение досье по проблемам безопасности;
- формирование и ведение «Паспорта безопасности объекта»;
- разработка вариантов комплексов мер и средств защиты и выбор лучшего по критерию «эффективность – стоимость».

На рисунке 5 приведена схема АПК «РискДетектор» с выделением верхней и нижней «ветвей».



Представленные на рисунке 7 машинная форма и соответствующий результирующий документ показывают результаты решения задачи оценки уязвимостей объекта и лимитов затрат на их устранение.



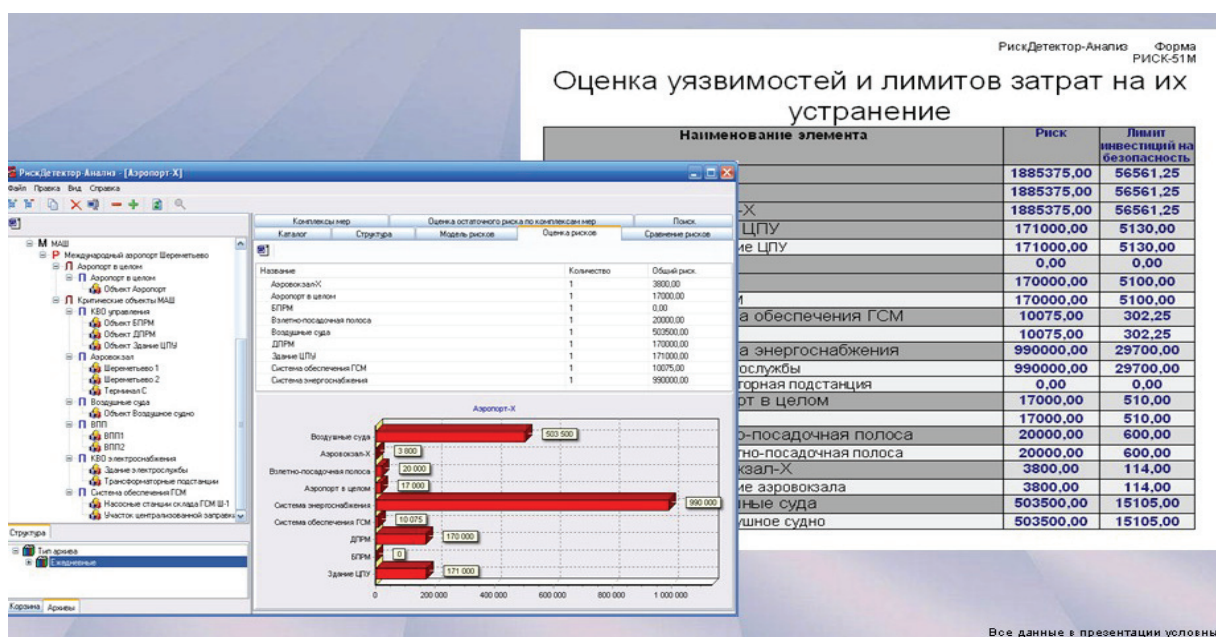


Рис. 7. Машинная и документальная форма «Оценка уязвимостей»

АПК «РискДетектор» в автоматизированном режиме на основе данных, характеризующих рассматриваемый объект (критические точки, модель угроз, классность объекта), рассчитывает категорию объекта. Результаты расчета показаны на рисунке 8.

Следующая важная задача, решаемая комплексом – это формирование, на основе анализа определенных ранее критических точек объекта и всей совокупности имеющихся нормативных требований по обеспечению безопасности объекта транспорта, профилей защиты объекта, т.е. наборов требований, выполнение которых обеспечивает защиту критических точек от всех возможных методов реализации угроз. На основании профилей защиты осуществляется, с учетом ограничений по стоимости защиты, выбор организационных мер и технических средств. Машинная и документальная формы выполнения этой задачи показаны на рисунке 9.

Важной задачей является доведение до всех исполнителей полученных профилей защиты объекта. При этом преследуется ряд целей. Во-первых, каждый исполнитель получает в концентрированном виде набор тех требований и средств, которые он должен выполнять на своем рабочем месте. Во-вторых, руководство службой безопасности имеет возможность конкретно требовать выполнение направленного исполнителю всего комплекса требований. Одновременно, руководство имеет возможность запросить от исполнителя отчет по выполнению требований, что далее используется для расчетов рисков реализации угроз на объекте, т.е. для оценки реальной уязвимости объекта.

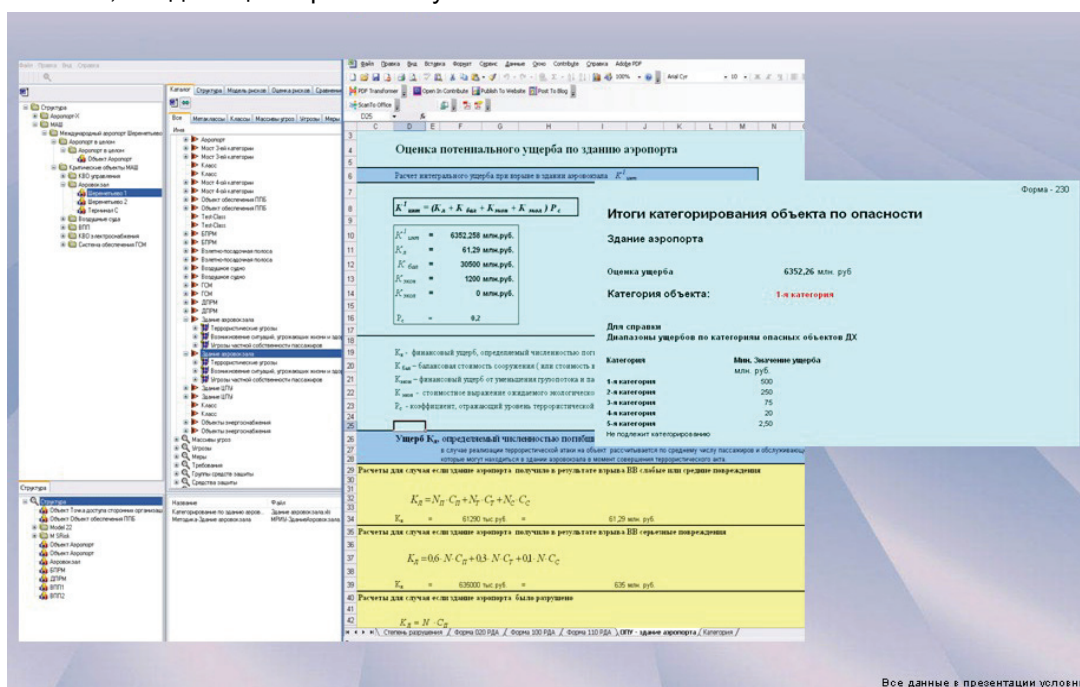


Рис. 8. Формы задачи «Определение категории объекта»

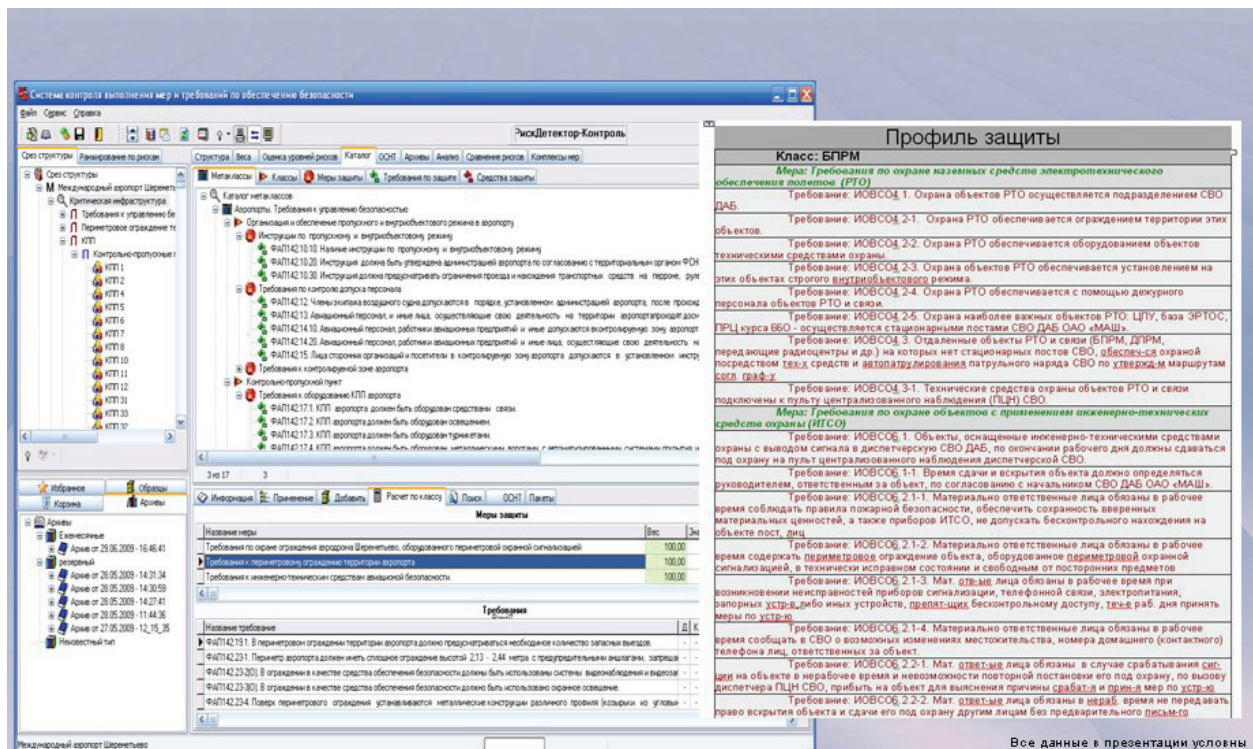


Рис. 9. Решение задачи «Построение профилей защиты»

На приведенной на рисунке 10 машинной форме показано решение задачи доведения до исполнителей требований и дана форма регистрации их ответов по выполнению требований.

Машинная форма, отображенная на рисунке 11, показывает результаты расчетов рисков реализации всей совокупности угроз по всем критическим точкам объекта и по объекту в целом. Основой для расчетов рисков служат отчеты исполнителей по выполнению ими профилей защиты.

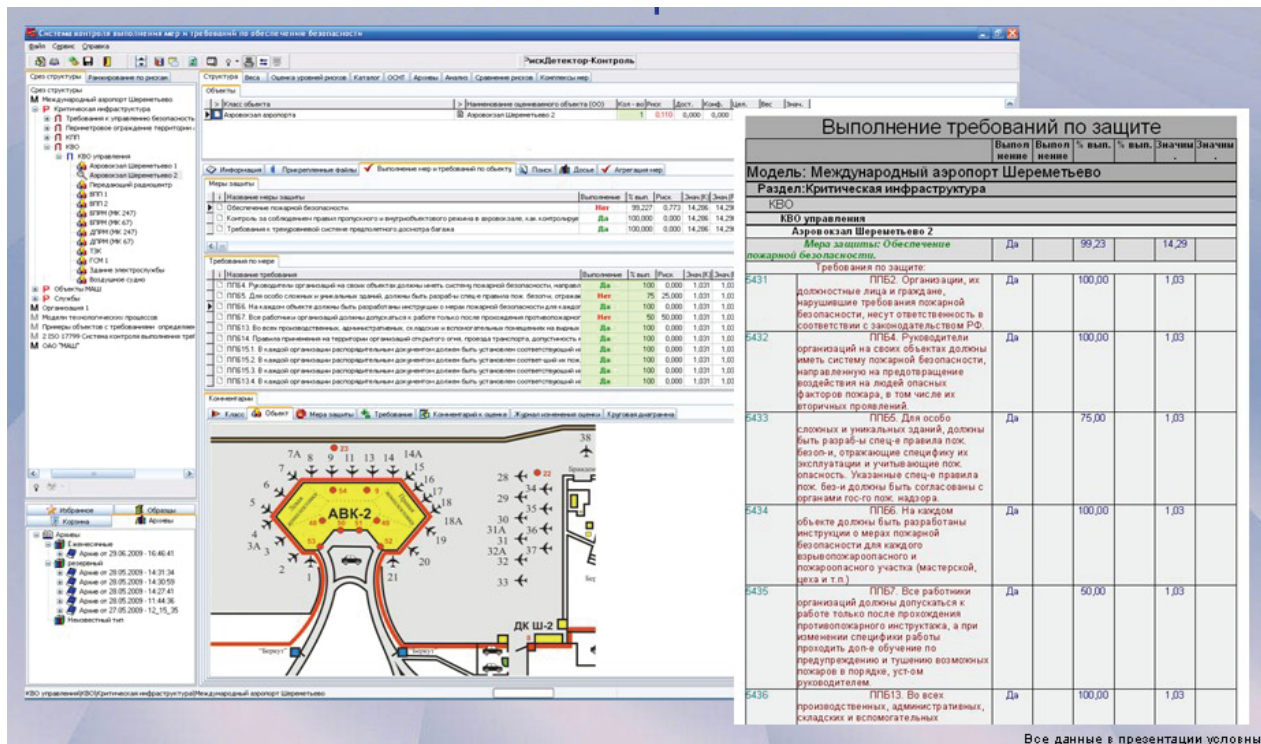


Рис. 10. Форма информирования исполнителей о требованиях по обеспечению безопасности

Из приведенного примера видно, что по некоторым критическим точкам риск реализации террористических угроз чрезмерно велик и требуется проведение мероприятий по повышению реального уровня выполнения профиля защиты.



Рис. 11. Расчет рисков реализации совокупности угроз

Использование комплекса «РискДетектор» позволяет обеспечить:

- систематический мониторинг состояния безопасности объекта;
- минимизацию средств на обеспечение защиты объекта;
- контроль работы соответствующих подразделений и выполнения необходимых работ.

Отличительной чертой комплекса является способность его быстрой адаптации для обеспечения любых видов безопасности – информационной, технико-технологической, кадровой, экологической и др. Такая способность подтверждается пятилетней эксплуатацией комплекса в ЦБ РФ для обеспечения информационной безопасности систем безличных расчетов. В настоящее время комплекс проходит апробацию в реальных условиях ОАО «Международный аэропорт Шереметьево».

СПИСОК ЛИТЕРАТУРЫ

1. Кононов А.А., Стиславский А.Б., Цыгичко В.Н. Управление рисками нарушения транспортной безопасности/ М., 2008, АС-Траст. – 210 с.
2. Черешкин Д.С., Цыгичко В.Н., Козлов Ю.П., Кононов А.А. Концепция категорирования потенциально опасных объектов национальной транспортной инфраструктуры // Проблемы управления рисками и безопасностью: Труды Института системного анализа Российской академии наук. Т. 31. – М.:Издательство ЛКИ, 2007.
3. Стиславский А.Б., Козлов Ю.П. Концепция реализации основных положений Закона о транспортной безопасности. // Терроризм и безопасность на транспорте: Материалы VII международной научно-практической конференции. – М.: РПА «АГПР», –2009. С.49–64.

Бачило И.Л.

Россия, Москва, Институт государства и права РАН

ПРОБЛЕМЫ РАЗВИТИЯ ИНФОРМАЦИОННОГО ЗАКОНОДАТЕЛЬСТВА

1. Информационное право и информационное законодательство в Российской Федерации

Осмысление проблем национальной безопасности в условиях, которые неизбежно определяются материальными, организационными изменениями в структуре общества, его экономики, социальной сферы под влиянием факторов глобализации, информатизации, под влиянием кризисных явлений, затрагивающих весь комплекс мироустройства, обязывает более строго оценить роль права и закона в системе обеспечения национальной безопасности. Проблемы современного законодательства органически включаются в систему и средств и объектов обеспечения национальной безопасности.

Законодательство призвано решать две задачи: обеспечивать правовое регулирование перестраивающихся общественных отношений, и вместе с тем, создавать безопасные условия развития самой системы законотворчества и законности с учетом трансформации институтов общества. Форумы и конференции по проблемам информационной безопасности подводят к пониманию этих проблем. В данном случае остановимся на некоторых сторонах развития и действенности информационного права и законодательства в Российской Федерации.

Развитие информационных технологий и сетевых систем коммуникаций, опирающееся на достижения кибернетики, обусловило такое продвижение информатики, как самостоятельной науки и производств, поддерживающих процессы информатизации общества, которое открыло новую эпоху в развитии земной цивилизации. Она получила название эпохи развития информационного общества. Изменения, происходящие в материальной, интеллектуальной, духовной культуре разных государств и их сообщества, соответствующих изменений в области права и практики правового регулирования поведения людей и организаций, изменения отношений субъектов разных уровней и форм. В структуре отраслей законодательства появились нормы, акты, посвященные информационным отношениям. В ряде государств формируются такие направления законодательства, которые называются киберправом, компьютерным правом, интернет-правом. В Российской Федерации стала формироваться отрасль информационного права еще в семидесятих годах прошлого столетия. К настоящему времени эта отрасль права получила легитимное признание как в системе высшего образования, так в системе науки, будучи представленной в ряде направлений соискательства и получения научной степени кандидата и доктора наук, в области законодательства.

Информационное право реализует себя в четырех формах, которые раскрывают его роль и значение. Это: доктринальное, научное развитие проблем средств, направлений их использования в процессах информатизации общества; развитие законодательства в данной области правовых отношений; учебная дисциплина в средних, высших и академических формах образования и повышения профессиональной подготовки специалистов, массового обучения граждан использования информационных технологий; наконец, как способ развития и воспитания правосознания. В целом, информационное право может быть определено как наука о предметах, принципах и методах правового регулирования деятельности и отношений в областях формирования и использования информационных ресурсов, технологий и коммуникаций и их сетей, организации управления процессами информатизации и обеспечения информационной безопасности граждан, государства и общества в целях удовлетворения их информационных потребностей и обеспечения развития общества.

В институте государства и права Российской академии наук проблематика информационного права развивается уже более тридцати пяти лет. Вначале это осуществлялось на базе научно-исследовательской группы в составе сектора административного права, а с 1999г. в рамках сектора информационного права. За последние десять лет в этом направлении реализуется большая работа. Ее формы включают работу теоретического семинара по проблемам информационного права, проводимого ежегодно Институтом государства и права РАН и систематическим выпуском материалов этого семинара; подготовкой кандидатов юридических наук по специальности 12.00.14., которая включает специализацию по информационному праву; выпуском нескольких изданий учебников по информационному праву [1–3]. К наиболее крупным коллективным работам можно отнести коллективные монографии [4], ряд персональных работ сотрудников сектора в форме монографий, большого количества научных статей; непосредственной педагогической работе, а также активном участии специалистов в конференциях, форумах международного, общероссийского и иного уровней.

Информационное право является самой молодой комплексной отраслью, которая имеет достаточно четко определенный предмет правового регулирования и комплексной является по методам регулирования отношений в своей сфере. Это отрасль как бы третьего уровня, ибо основана на таких классических отраслях как конституционное, административное, гражданское, уголовное право; является дочерней относительно административного права, но в силу специфики предмета – сохраняет значительную самостоятельность при комплексном использовании методов регулирования выше обозначенных отраслей права. Общая теория государства и права лежит в основе формирования принципов и институтов этой отрасли.

Функциональная роль информационного права проявляется в двух направлениях. Во-первых, через эту отрасль формируется и развивается информационное законодательство, регулирующее отношения в области ИКТ (информационно-коммуникационных технологий), охватывая такие исходные составляющие, базу и инфраструктуру информатизации как технологии, информационные ресурсы и сетевые коммуникации, а также все пути их применения в процессах информатизации и инноваций. Во вторых, выполняет роль выявления состояния информационного значения всей системы законодательства, выступает в роли катализатора развития современного права с учетом трансформации общественных отношений и общественных институтов в условиях информатизации.

2. Законодательство как регулятор отношений в информационной сфере Российской Федерации

Не прибегая к перечислению всех законодательных актов в области регулирования отношений, реализуемых в информационной сфере, отметим, что к настоящему времени это законодательство в составе федеральных законов, указов президента, постановлений Правительства РФ, законов субъектов РФ и иных нормативных правовых актов в этой области насчитывает несколько сот единиц. К настоящему времени сложились такие правовые институты в системе законодательства как: право на информацию, правовой режим информационных ресурсов и ИТ; регулирование деятельности СМИ

и иных средств массовых коммуникаций; правового регулирования использования разных категорий информации по доступу и защите; защита прав интеллектуальной собственности в информационной сфере; институт использования глобальных информационных систем, включая Интернет; институт правового мониторинга; институт обеспечения информационной безопасности и реализации правовой ответственности в информационных отношениях и др. Обзор состояния законодательства с учетом перечисленных правовых институтов показывает их далеко не равномерный системный, согласованный охват действующим законодательством. Преимущественное точечное нормативное регулирование даже и важных сторон в каждом из этих институтов свидетельствует об отсутствии общепринятой концепции и политики правового обеспечения сферы информационных отношений.

Такая ситуация создает определенные трудности как в самой законотворческой деятельности, так и в процессе правоприменения и исполнения действующего законодательства.

Принятие к исполнению таких методологически важных документов как Стратегия развития информационного общества, Стратегия национальной безопасности, стратегия информатизации судебной системы обязывают усилить внимание к гармонизации внутреннего для России информационного законодательства, всей нормативно-правовой системы в этой области. Попытки ускоренной ликвидации имеющихся пробелов в законодательстве и обеспечения более высокого уровня защиты информации, отечественного программного продукта, получить более высокую оценку в рейтингах оценки состояния информационного общества в масштабе всего информационного сообщества пока не дают очень заметных результатов. На этом фоне отдельные успехи в области правового регулирования информатизации, например в Ханты-Мансийском автономном округе – Югра, в Республике Татарстан, в Москве и других регионах, общую картину меняют мало. И в этой связи стоит вопрос, какие факторы мешают более успешно реализовать ФЦП «Электронная Россия» и программы, связанные с деятельностью Электронного правительства как основной институции и формы обновления работы органов государственной власти, деятельности организаций и жизни граждан в условиях информатизации.

В этой связи на первый уровень препятствий в получении реальных успехов в информатизации стоит отнести параллельность развития законодательства по трем направлениям. Это мало пересекающиеся и согласованные по целям направления правового регулирования в области:

1. Административной реформы.
2. Правового регулирования сферы информатики и отечественного производства «софта» и «харда» в сфере информационных технологий.
3. Регулирования использования информационных технологий, информационных ресурсов в процессах модернизации управления, производства, социальной сферы, государственных и муниципальных услуг, которое аккумулируется в области ФЦП «Электронная Россия» и деятельности электронного правительства (э-правительства).

Слабая работа в области комплексного и согласованного позитивного регулирования информационных процессов и отношений при стремлении каждого из названных направлений к самостоятельности, существенно влияет на состояние обеспечения безопасности всех ресурсов информатизации общества. Это прямым образом связано и с обеспечением безопасности прав и обязанностей субъектов в этой сфере, состоянием инновационных процессов на базе ИТ и рационального, полноценного и экономичного использования информационных ресурсов и коммуникаций. Каждое из названных направлений правового регулирования и реальных отношений развивается как бы само по себе. Сложно проследить связь, например, таких установок информационного права на внедрение электронного документа и применение электронной подписи в деятельности и взаимодействии между органами государственной власти и местного самоуправления, в отношениях этих органов с организациями и гражданами как по вертикали системы управления так и по горизонтальным каналам их взаимодействия. Очень заметен трафарет чисто отраслевого, а часто и корпоративного, подхода к развитию законодательства.

В целях установления более тесных контактов между специалистами информатики и информационных реальных процессов в ходе формирования информационного общества Институт государства и Права РАН заключил соглашение о научном сотрудничестве с Санкт-Петербургским институтом информатики и автоматизации РАН. Есть надежда в процессе этого сотрудничества сблизить терминологию, понятия и языки на которых разговаривают специалисты в области технологий и юристы.

Не менее сложно сближаются позиции информационного права и законодательства с областью позитивного регулирования институтов управления (администрации), административного права. Положения об органах исполнительной власти, регламенты по исполнению функций и государственных услуг только сейчас начинают отражать связь работы аппаратов управления с применением ИТ в этой сфере деятельности. И, естественно, в этом направлении еще предстоит большая работа. Если технологическая основа в части создания таких институций как ОГИЦ, МФЦ, удостоверяющие центры по ЭЦП, центры доступа к информации граждан и организаций, сайты в

Интернете находятся в готовности к их использованию, то готовность служащих аппаратов органов публичной власти еще только в начале марша.

Для примера напомним, что переустройство документации и документооборота с учетом перехода на электронную форму документации в системах управления в США была как бы первым шагом в системе программ по информатизации, то в России до сих пор этот вопрос остается в обозе и организационных мер и развития нормативной базы. Опыт Австрии, Германии и др. государств Европы свидетельствует о пристальном внимании к этой стороне обеспечения фундамента информатизации. Например, в Австрии, по словам исполнительного директора службы информатизации органов власти Австрии Карла Майрхофера, освоение работы с электронным документами обеспечивают 48 тысяч государственных служащих. И перевод государственных услуг в электронную форму осуществлялся на протяжении двадцати лет. И еще: по стандартам ЕС в настоящее время в электронной форме выполняются примерно двадцать государственных услуг.

Формат конференции позволяет остановиться на отдельных примерах подхода к позитивному правовому регулированию в области информатизации. В данном случае остановим внимание на проекте федерального закона (ФЗ) «Об общих принципах организации государственных (муниципальных) услуг и исполнения государственных (муниципальных) функций», который прошел первое чтение в Государственной думе в конце декабря 2009 г.

Ознакомление с процессом подготовки к переходу предоставления государственных и муниципальных услуг в электронную форму показывает, что пока нет четких представлений о том, как определяется содержание и определение таковой услуги, сколько их должно быть и каков порядок их реализации. Одни ведомства считают, что сегодня можно обеспечить около пятидесяти государственных и муниципальных услуг (Минсвязь России), другие – семьдесят (Минэкономразвития России), в целом же называется цифра пятьсот услуг.

Если попытаться проиллюстрировать общие проблемы формирования информационного законодательства на конкретном примере, то обнаруживаем, что проект названного закона затрагивает вопросы, которые касаются общей теории права, государственного управления и организации непосредственной деятельности по регулированию порядка осуществления государственных услуг на базе использования ИТ и всех средств информационного обеспечения.

Почему останавливаемся на этом проекте? Тема его – государственные услуги – является знаковой для решения многих проблем настоящего и предстоящего времени жизни общества. Выход из кризиса ставит вопросы социальности общества, государства на первый план. Основным актором жизни общества является человек, и создание нормальных условий для его разумной активности, развития его креативности и умения действовать во благо свое и общества в условиях информатизации становится определяющим для парадигмы социального развития в целом.

Проект закона об услугах затронул проблему соотношения социального государства и государства сервисного, патерналистского. Данной теме посвящаем отдельную публикацию. Однако этот вопрос получает отражение и в названии и в определении предмета правового регулирования взятого для рассмотрения закона.

Для любого закона, в том числе и для каждого в области регулирования информационных отношений первостепенное значение имеет его концепция и идеология решения определенной проблемы. Это требование соблюдается не всегда и не обеспечено в данном случае. В центре внимания исполнителей закона обязательно окажутся вопросы определения названия, предмета и цели правового регулирования. По всем этим параметрам нет полной ясности.

Название этого акта смешивает индивидуальный акт предоставления конкретной услуги физическому лицу или организации с выполнением функций государственного уровня управления, которые, как правило, реализуются в процессе принятия нормативных или общих правовых актов. Предоставление услуг – одна из важнейших функций государственных и муниципальных органов власти, но не покрывает всего диапазона их разнообразия. Поэтому вынесение в название проекта закона темы «исполнения государственных (муниципальных) функций» представляется неверным. В плане обеспечения социальности государства работают буквально все органы исполнительной власти, создавая материальную, производственную, финансовую инфраструктуру, необходимую для реализации прав и обязанностей граждан и получения соответствующих услуг от государства. Услуги реализуются на базе этих условий. От состояния обеспечения общих социальных задач государства зависит и область услуг для каждого. Нужны школы, больницы, садики, рабочие места, жилье и пр. для удовлетворения потребностей и их поддержки через услуги.

Сегодня важно создать взаимодействие функциональной и сервисной деятельности органов государственных и муниципальных на основе использования ИТ и коммуникаций современных. Однако, нерешенность проблем императивного включения ИТ и единых правил документирования с использованием цифровой подписи или иных форм идентификации документов в деятельность государственного аппарата управления, в муниципальные системы управления требует самостоятельного правового регулирования, которое неоправданно затягивается. Но связь общего и конкретного в данном случае со стороны законодательства в области информатизации не обеспечена. Нарушается связь материальных, технологических, информационных, управленческих и

правовых условий решения поставленной проблемы как путем перевода исполнения функций в электронную форму и на этой уже основе перевода услуг на новые технологии.

Второй вопрос. Закон должен четко определить предмет и цель регулирования. Проект не дает определения понятия государственной и муниципальной услуги. Цель закона также не имеет определения и весь его текст нацелен на регулирование процедур и условий, в том числе и платы за государственные услуги.

Проект не уделяет должного внимания специфике работы различных субъектов в области оказания услуг в электронной форме, в то время как сама область услуг не однородна и требует специализации в зависимости от состава их и средств обеспечения безопасности.

Имеем в виду систематизацию государственных и муниципальных услуг на такие категории как:

- информационные и информационно-консультативные.
- услуги правореализующие – позволяющие установить правила подтверждения прав и обязанностей граждан и организаций в электронной форме, например, в области регистрации жилья, земли, автомобилей и пр. Подтверждения и выдачи юридически значимых документов о полномочиях гражданина в той или иной области отношений.

- правоустанавливающие услуги, например, получение паспорта, свидетельств о рождении, смерти, заключение договора и т.п.

Если в настоящее время наиболее обеспечены информационные услуги на основе ФЗ о доступе к информации о деятельности государственных и муниципальных органов, создания и функционирования порталов, сайтов, иных средств массовой информации, то другие виды пока обеспечиваются отдельными операциями в электронной форме. Создание общегосударственного единого классификатора услуг и ведение реестров каждым органом, действующим в сфере услуг необходимо. И на этой основе возможно определение специализации отдельных органов в области оказания государственных услуг.

Еще одна проблема. Неурегулированным остается вопрос о порядке оформления электронных документов, по результату государственной услуги. Здесь не исключены конфликты, неполноценное решение проблемы заявителя, непризнание решения по услуге для дальнейших действий гражданина или организации в области реализации своих прав и обязанностей, которые потребуют обращения в суд, прокуратуру, в административные системы защиты прав и установления ответственности нерадивых исполнителей услуги или признания ее результата в электронной форме. Насколько обеспечена проблема юридической силы индивидуальных решений по услугам в электронной форме структур различных административных органов – это тоже специальный вопрос.

Более подробное рассмотрение проекта названного ФЗ обосновано специалистами ИГП РАН и представлено в Государственную думу. Подготовлены и публикации по данному вопросу в очередном сборнике материалов теоретического семинара Сектора информационного права, который выйдет в феврале 2010г.

Внимание к одному проекту ФЗ не означает, что все в порядке с другими уже принятыми или готовящимися проектами законов и иных нормативных актов в области информатизации. Напомним о множестве критических замечаний относительно ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ «О персональных данных», о поправках к ФЗ.

«Об электронной цифровой подписи», о выплеснутых проблемах информационных ресурсов из последнего законодательства по этой отрасли права.

Приводим эти примеры не для того, чтобы как-то принизить значение и состояние информационного законодательства. В этой отрасли права отражается ситуация трансформации феноменов времени и пространства, которое определяется сжатием в физическом измерении, но значительно усложняет решение проблем регулирования отношений в информационных средах и в информационном пространстве в целом. Отставание России по многим параметрам в освоении информационной и технологической культуры от наиболее развитых стран задает условия ускорения темпов продвижения по всем параметрам, в том числе и в правовом регулировании. Сжатые сроки при слабой гармонизации уже наработанного на фронте правового регулирования, с одной стороны, как бы и оправдывают спешку, но с другой – чреваты последствиями дисбаланса в общей системе правовой основы. Объективные условия отставания сознания и массового поведения субъектов в новых условиях понятны и неизбежны. Их надо преодолевать. Но огрехи в правовом регулировании усугубляют эту ситуацию еще и субъективными факторами. Например, установки «создать закон здесь и сейчас». Исполнителями могут быть и случайные структуры в силу несовершенства конкурсной основы, имеющие локальные цели и т.п. И это особый вопрос.

Поиск выхода из противоречивой и рассогласованной системы информационного законодательства приводит к обоснованию создания информационного кодекса, который бы соединил под единой концепцией все направления правового регулирования в этой достаточно чувствительной и молодой отрасли. Но делать это надо не только при тщательном разборе состояния и гармонизации всех направлений информационного регулирования в информационной проблематике, но и при учете эволюционных изменений в административных реформах, реализации

программ в экономической, социальной сфере, массовой информации и т.д. Отрасль сложная по предметам и комплексная по методам регулирования к этому обязывает.

3. Несколько замечаний по поводу роли информационного права как катализатора эволюции системы законодательства в целом

Что обуславливает постановку этого вопроса? Здесь два момента. Первый связан с общей функцией информативности и любой отрасли права и законодательства. Знание закона – условие его соблюдения, тем более, что не знание не освобождает от ответственности. Каждая отрасль законодательства представлена максимально в информационной правовой системе и доступна для любого пользователя.

Второй момент связан с выполнением специальной функции и развитием института правового мониторинга как одного из институтов информационного права. Этот институт призван отслеживать состояние и динамику всего законодательства в любых формах нормативного правового регулирования. Известно, что уже несколько лет эта деятельность организовывается Советом Федерации и что эта палата Российского парламента ежегодно представляет доклады о состоянии российского законодательства на основе использования результатов мониторинга законотворчества и правоприменения. Отметим, что Институт государства и права наряду с другими участниками анализа мониторинга принимает участие в подготовке некоторых разделов докладов Совета Федерации.

Именно это направление информационного права и законодательства формирует такие наблюдения и предложения, которые имеют значение для любой отрасли законодательства России и ставят достаточно сложные вопросы для общей теории права.

Нельзя утверждать, что отмеченные выше недостатки в развитии информационного законодательства не присутствуют и в других отраслях. Спешка и сжатие сроков подготовки проектов, корпоративность в определении целей и предмета правового регулирования подтверждается тем, что правовой мониторинг законодательства фиксирует нарастание числа законов о внесении изменений и дополнений в уже принятые законы, а порой принятые, но еще не введенные в действие.

Очень слаба связь науки и законотворческих инициатив и процессов. Стоит отметить, что почти ни в одном учебнике по праву и даже в литературе по теории права мало или совсем не уделяется исследованию состояния законодательства, как нормативной основы реализации права. В отраслях рассматриваются отдельные институты с привлечением конкретных законов, но общей оценки соответствия законодательства отрасли состоянию сферы ее применения, почти не случается.

В неразвитом состоянии остается институт экспертизы проектов законов и иных правовых нормативных актов с привлечением разных профилей экспертов. Наблюдаем увлечение темой коррупционности законодательства и нормотворчества в целом, но другие исходные позиции обеспечения качества закона остаются в тени. Они касаются и юридической техники и еще больше юридической технологии. Это подтверждается не точным определением названий, цели закона, его предмета, пренебрежением к определению субъектов, к которым закон обращен, к субъектам, ответственным за его реализацию, к однозначному пониманию общих для ряда отраслей и законов терминов, определению их правового статуса и других основных параметров нормативного акта.

Много лет Россия не может решиться принять ФЗ «О нормативно-правовых актах», в то время как особую остроту приобретает вопрос об официальном электронном опубликовании федеральных законов, законов субъектов Российской Федерации, актов муниципального уровня. Нет ясности и в законодательном регулировании различных форм собственности и различных сегментов интеллектуальной собственности, что тормозит и развитие экономики в целом и проблем защиты интересов и интеллектуальных прав создателей продуктов творческого труда в России. А это отражается и на отношениях в глобальном пространстве Интернета и всех форм международного сотрудничества по этим проблемам. Вопросы служения собственности в любой форме интересам общему благу пока остаются слабо выраженными в теоретическом плане, не говоря о законодательстве.

Все острее ставятся вопросы об отсталости административно-правового законодательства, которое не может быть сведено только к проблемам государственной службы (ее внутрисистемного устройства) и административной ответственности. Вопросы организации государственного управления потеряны в системе государственного регулирования в связи с прямолинейным пониманием «поменьше государства».

Обострение внимания на базе информационного права к вопросам толкования феномена «свобода» и торможение на позиции «свобода от», а не «для», о чем ясно говорит Председатель Конституционного суда России В.Д. Зорькин, также требует внимания многих отраслей законодательства. Перечень общих проблем для права и законодательства может быть продолжен. Но и этого достаточно для понимания резкого поворота законодательного регулирования и идеологии права к проблеме развития социальности общества, понимаемого не узко как «социальное обеспечение» или услуги, а как пробуждение каждого гражданина, каждой ассоциации граждан в области активного строительства жизни государства, отечества.

И последнее. Для современной теории права пора повернуть толкование роли государства и права от роли принуждения, наказания, боязни, осуждения и достаточно откровенно обоснованной либеральной идеологией экстрадиции этих институтов из социального бытия российского общества к обеспечению их роли в организации позитивного устройства социального управления, оказания поддержки, воспитания доверия к новой дисциплине всех видов администраций и каждого человека в современном и предстоящем периоде развития гражданского, информационного, демократического и правового общества. Именно к этому преобразованию толкают инновации на базе информационных технологий и все более развивающиеся институты гражданского общества.

Реализация такого более высокого обоснования и обеспечения исполнения закона, в частности и ФЗ об услугах, требует применения пакетного регулирования связанных проблем и снижения попыток заниматься выделенной как самостоятельной и независимой проблемы отдельного закона. Возвращаясь к области задач собственно информационного законодательства и теме услуг, подчеркнем, что правильно ее решить, можно только при наличии ФЗ «Об электронной подписи», ФЗ об электронном документообороте на единой методологической основе для всей страны и ее различных подсистем взаимодействия; а также подготовки и принятия ФЗ «О служебной информации и служебной тайне».

СПИСОК ЛИТЕРАТУРЫ

1. Бачило И.Л., Лопатин В.Н., М.А. Федотов. Информационное право. Учебник. Под редакцией академика РАН Б.Н. Топорнина. СПб.: Изд. «Юридический центр Пресс», 2001. 789 с.; Второе издание 2005.
2. Бачило И.Л. «Информационное право. Основы практической информатики». Учебное пособие. М. 2001. 325с. повторный выпуск 2003.
3. Бачило И.Л. Информационное право. Учебник для ВУЗов. Специальный курс. Юрайт. Высшее образование. М. 2009.
4. Информационные ресурсы развития Российской Федерации. Правовые проблемы. М.: Наука. 2003. 403с.; Кол. мон. «Информационное право. Актуальные проблемы теории и практики». М.: Юрайт. 2009. 530с.

Зегжда Д.П., Калинин М.О.

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

ТЕХНОЛОГИЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ СРЕД ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Современные требования к реализации безопасных систем обработки информации, применяемых в критических технологиях, подразумевают обеспечение доверия к информационной среде и контроля всех компонентов информационно-телекоммуникационной системы (ИТКС). Под доверенной средой понимается информационная среда, включающая совокупность защитных механизмов, которые обеспечивают обработку информации без нарушения политики безопасности. Для обеспечения доверенности среды недостаточно реализовать контроль доступа, необходим комплекс мер, обеспечивающих контроль целостности и подлинности компонентов защиты, стабильность конфигурационных параметров систем защиты и операционной среды, соблюдение ограничений политик безопасности. Поэтому в усиление традиционных средств разрабатываются и применяются инновационные решения и продукты: например, системы обнаружения и предотвращения вторжений, методы проактивной антивирусной защиты, системы анализа рисков, позволяющих реализовать активную информационную безопасность и, тем самым, сократить время реакции на киберугрозы и предпринять скорейшие меры, направленные на противодействие им. Сочетание традиционных и инновационных методик представляет собой современную технологию информационной безопасности в рамках любой ИТКС.

Свойство доверенности информационной среды плохо формализуемо, но стремление достичь его определяется двумя факторами:

1. Огромное количество уязвимостей в существующих операционных системах, что делает их свойства непредсказуемыми и создает предпосылки для разнообразных компьютерных атак.
2. Трудности сертификационных испытаний импортных систем даже при наличии исходных текстов, вызванные отсутствием абсолютно надежных методов анализа безопасности программного обеспечения, и тем, что объем кодов не позволяет использовать какую-либо из известных методологий верификации.

Для противодействия первому фактору создан ряд направлений: «доверенные» (trusted) версии известных систем (например, T-Solaris, T-Math, специальные версии Linux и Windows); контролирующие прослойки (например, пакеты RSAC, GRSecurity); изолирующие технологии (например, шлюз контроля доступа Astaro Security Gateway); делегирующие технологии (например, Multiple Independent Levels of Security). Перечисленные решения объединяет принцип обособления систем, заключающийся в фиксации состава операционной среды и в том числе средств защиты. Вариативность этих решений в сочетании с традиционными подходами и сохранение степени участия администраторов в регулировании операционных сред не только не обеспечивает защищенность систем, но и открывает для злоумышленников новые возможности по нарушению безопасности за

счет привнесения новых уязвимостей. Кроме того, усиление средств защиты систем и процесс их эксплуатации усложняют задачу динамического контроля защищенности: например, стандартный механизм контроля целостности путем контрольного суммирования в данном случае бесполезен, поскольку не учитывает свойство системности (совпадение сумм для каждого контролируемого компонента не может гарантировать цельность функционала безопасности относительно всей системы). Но при этом отказаться от контроля целостности среды невозможно, поскольку нарушения целостности делают бесполезным применение любых высококачественных систем защиты.

Второй фактор стимулирует создание разнообразных методов анализа безопасности ПО, которые, в конце концов, связаны с разработкой критериев наличия вредящего кода, что в общем случае является трудоемкой (NP-полной) задачей. В любом случае, среда с непредсказуемыми свойствами становится препятствием для достижения необходимой степени защищенности ИТКС, поскольку влияет на работу средств защиты и делает ее недоверенной по определению.

По мнению авторов, указанные трудности можно преодолеть, разработав метод мониторинга и управления состояниями вычислительной среды и средств защиты, расширив при этом определение понятия целостности. Цель данной работы — предложить математическую модель и структуру системы обеспечения защищенности ИТКС, т.е. достижения доверенности информационной среды путем фиксации, контроля и управления ее состояниями в пределах, определяемых требуемым функционалом и критериями безопасности.

Согласно ГОСТ Р ИСО 13335–1, целостность — свойство сохранения правильности и полноты информационных активов. Под активом в данном стандарте понимается «все, что имеет ценность для организации». Однако необходимость внесения новых компонентов и изменение конфигураций существующих вынуждает изменить это определение. В частности, по отраслевому стандарту Банка России, РИББС–1.0–2008, целостность — это свойство сохранять неизменность или обнаруживать факт изменения в информационных активах. Таким образом, определение целостности из статического превращается в динамическое, в котором не констатируется неизменность среды, а прогнозируются последствия ее изменения. По мнению авторов, эту тенденцию следует продолжить и расширить понятие целостности до фиксации допустимого диапазона варьирования среды, в котором сохраняются условия безопасности и необходимый функционал. Под термином «целостность» в данной статье понимается свойство постоянной взаимосогласованности параметров информационной среды (комплекса системного, прикладного программного обеспечения и средств защиты), что является необходимым условием безопасности ИТКС.

Решение задачи контроля целостности информационной среды в контексте безопасности ИТКС невозможно без учета разнообразия программного обеспечения с множеством функциональных свойств и настроек, предназначенного для обработки огромных объемов разнородной информации, поступающей из различных источников; гетерогенности ИТКС, в которых взаимодействуют различные операционные среды (например, MS Windows, UNIX/Linux); необходимости оперативной передачи информации между территориально удаленными подразделениями; необходимости учитывать изменения операционной среды ИТКС, связанные с ее обновлением, установкой функциональных дополнений; необходимости контроля, предупреждения и предотвращения нарушений информационной безопасности. Перечисленные факторы и анализ угроз целостности позволяет определить методы и средства контроля целостности ИТКС (рисунок 1).

Компоненты информационной среды ИТКС группируются в два класса: стабильные и изменяемые. К стабильным, долговременным, компонентам относятся функциональные модули, которые создавались при разработке системы. Их изменение требует дополнительного проектирования и связано с модификацией системы, повторными испытаниями, настройками и т.д. К изменяемым компонентам относятся модули, предназначенные для произвольного модифицирования или внедрения в систему, и этот процесс осуществляется автоматически или в результате деятельности администратора или пользователя. Применение криптографических методов обеспечения целостности позволяет решить проблему целостности стабильных компонентов. В то же время при эксплуатации ИТКС могут проявляться изменения, которые достаточно серьезно влияют на безопасность системы и стабильность ее функционирования, но для которых криптографические методы неприменимы:

- установка несовместимого ПО (например, двух криптобиблиотек, использующих разные версии API);
- обновление ПО, требующее перенастройки уже установленного (например, применение в системе пакета обновлений Service Pack);
- изменение пользовательского состава, приводящее к модификации рабочей среды и ее настроек (например, создание в системе нового профиля пользователя).

В этом случае для обеспечения целостности как свойства взаимосогласованности используемых компонентов с учетом взаимного влияния их параметров требует специальной технологии, которая и представлена в данной работе.



Рис. 1. Систематизация угроз целостности информационной среды ИТКС

Рассмотрим формальное представление проблемы контроля целостности. Состояние системы характеризуется совокупностью программных единиц, где — множество программных единиц, каждая из которых задана:

- типом $T_n \in T$, где T – множество типов программных единиц (например, ОС, пользовательское ПО, СЗИ), $n \in N$;

- множеством параметров $A^{T_n} = \{a_j^{T_n}\}$, где T_n – тип программной единицы, a_j – компоненты параметров, $i \in N$;

- множеством текущих значений параметров $V^{T_n, p_i} = \{v_k^{T_n, p_i}\}$, где $v_k^{T_n, p_i} = \text{var}(p_i, T_n, A^{T_n})$, $\forall k \in N$. Функция $\text{var}: P \times T \times A^T \rightarrow V^T$ ставит в соответствие программной единице $p_i \in P$ определенного типа $T_n \in T$, обладающей параметрами A^{T_n} , их значения V^{T_n} .

Для соблюдения целостности системы она должна удовлетворять:

- условиям безопасности в каждом системном состоянии;
- условиям взаимосогласованности в каждом безопасном системном состоянии.

Условия безопасности выполняются в системе, когда она постоянно обеспечивает безопасность в соответствии с заложенными в нее правилами безопасного поведения (т.е. в соответствии с моделью контроля и управления доступом) и соблюдает требования безопасности (ограничения политики безопасности, технические условия и правила эксплуатации).

Формально, в общем виде, система Σ представляет собой машину состояний: $\Sigma = \{S^\Sigma, tr, s_{init}^\Sigma, Q\}$, где S^Σ – множество системных состояний, $S^\Sigma = P \times T \times A^T \times V^T$, т.е. системное состояние образовано множеством программных компонентов P определенных типов T с соответствующим набором параметров A^T заданных значений V^T ; Q – множество запросов, обрабатываемых системой; tr – функция перехода из состояния в состояние, $tr: S^\Sigma \rightarrow S^\Sigma$, которая под действием запроса $q \in Q$ переводит систему из состояния s_x^Σ в следующее состояние $s_{x+1}^\Sigma = tr(q, s_x^\Sigma)$; s_{init}^Σ – начальное состояние системы. Состояние s^Σ достижимо в системе Σ тогда и только тогда, когда существует последовательность $\langle (q_0, s_0^\Sigma), \dots, (q_n, s_n^\Sigma) \rangle$, в которой $s_0^\Sigma = s_{init}^\Sigma$,

$s_n^\Sigma = s^\Sigma$, а $s_{x+1}^\Sigma = tr(q, s_x^\Sigma)$, $0 \leq x < n$. Для любой системы состояние s_{init}^Σ достижимо тривиальным способом.

Модель контроля и управления доступом M , реализованная в системе Σ , в общем случае, представляется как кортеж множеств $M = \{S, R\}$, где S — множество состояний модели (состояний безопасности), R — множество правил контроля и управления доступом, сформулированных в форме предикатов вида $r(q, s, s')$. Определим взаимнооднозначную функцию pr проекции состояний, $pr: S^\Sigma \rightarrow S$, которая определяет соответствие между системными состояниями и состояниями безопасности. Предикаты $r(q, s, s')$, которые определены на множествах запросов Q и состояний S , осуществляют проверку перехода системы из состояния s в состояние s' в результате запроса q , т.е. $s^{\Sigma_1} = tr(q, s^\Sigma)$, $s' = pr(s^{\Sigma_1})$, $s = pr(s^\Sigma)$, $s^{\Sigma_1} = pr^{-1}(s')$, $s^\Sigma = pr^{-1}(s)$ — срабатывание функции — разрешен правилами модели контроля и управления доступом.

Иными словами, переход системы из состояния $s^\Sigma \in S^\Sigma$ в следующее состояние $s^{\Sigma'} \in S^\Sigma$ по некоторому запросу $q \in Q$ разрешен тогда и только тогда, когда для этого запроса все предикаты $r(q, s, s')$, разрешающие переход, истинны, т.е. $\forall s^\Sigma, s^{\Sigma'} \in S^\Sigma, \exists s, s' \in S: s = pr(s^\Sigma), s' = pr(s^{\Sigma'})$, $\forall r \in R: r(q, s, s') = \text{"ИСТИНА"}$.

Свойство безопасности системы Σ может быть сформулировано как $\Delta = \{\Sigma, M, Cr\}$, где Cr — множество требований безопасности, представленных в виде критериев безопасности, которые сформулированы как предикаты вида $cr(s)$, определенных на множестве S и осуществляющих проверку безопасности состояния s . Состояние $s \in S$ является безопасным тогда и только тогда, когда для каждого критерия безопасности $c \in C$ истинны все предикаты $c(s)$, т.е.

$$\forall s^\Sigma \in S^\Sigma \quad \exists s \in S: s = pr(s^\Sigma), \forall c \in C: c(s) = \text{"ИСТИНА"}.$$

Таким образом, формально система Σ , реализующая модель контроля и управления доступом M , удовлетворяет условиям безопасности тогда и только тогда, когда:

система Σ реализует правила модели M :

$$\forall s^\Sigma, s^{\Sigma'} \in S^\Sigma \quad \exists s, s' \in S: s = pr(s^\Sigma), s' = pr(s^{\Sigma'}), \exists r \in R: r(q, s, s') = \text{"ИСТИНА"};$$

множество значений параметров безопасности заданного и любого достижимого из заданного системного состояния удовлетворяет применяемым к системе требованиям безопасности:

$$\forall s^\Sigma \in S^\Sigma \quad \exists s \in S: s = pr(s^\Sigma), \forall c \in C: c(s) = \text{"ИСТИНА"}.$$

Одновременное выполнение этих двух правил свидетельствует о безопасности системы в каждом ее достижимом состоянии и, следовательно, о безопасности ее параметров, которыми характеризуются ее состояния.

Для формализации взаимосогласованности параметров введем функцию отображения $ref: P \times T \times A^T \times V^T \rightarrow P \times T \times A^T \times V^T$, которая для перечня параметров $a^t \in A^T$,

проинициализированных значениями $v^{t,p} \in V^{t,p}$, заданной программной единицы $p \in P$ типа $t \in T$,

указывает перечень согласующихся с ними параметров $a^{t'} \in A^{t'}$, проинициализированных значениями $v^{t',p'} \in V^{t',p'}$

значениями программной единицы $p' \in P$ типа $t' \in T$. В общем случае, для данной функции ограничение $p \neq p'$ отсутствует, так как в сложных системах существует взаимовлияние параметров в рамках программной единицы (например, в настройках безопасности ОС влияние одних параметров может отменять действие других).

В общем случае, каждому значению параметров одной программной единицы может соответствовать не одно V^T , а множество значений (обозначим как $V^T \pm \Delta V^T_{\Leftarrow}$) другой программной единицы: $ref: P \times T \times A \times V^T \rightarrow P \times T \times A \times (V^T \pm \Delta V^T_{\Leftarrow})$.

Введем обратную функцию $ref^{-1} : P \times T \times A \times (V^T \pm \Delta V_{\Leftarrow}^T) \rightarrow P \times T \times A \times (V^T \pm \Delta V_{\Rightarrow}^T)$, определяющую область отображения $V^T \pm \Delta V_{\Rightarrow}^T$ для каждой точки, принадлежащей области $V^T \pm \Delta V_{\Leftarrow}^T$.

Существование областей $V^T \pm \Delta V_{\Leftarrow}^T$ и $V^T \pm \Delta V_{\Rightarrow}^T$ позволяет формально определить целостность системы через взаимосогласованность значений параметров ее программных компонентов. Для системы, состоящей из программных компонент P , область существования всех парных отношений, должна составлять непустое множество:

$$\begin{aligned} \forall p \in P, \forall t \in T \quad \exists a \in A' : \exists p' \in P, \exists t' \in T, \exists d_{\Rightarrow} = V^{p,t} \pm \Delta V_{\Rightarrow}^{p,t} \text{ и} \\ d_{\Leftarrow} = V^{p',t'} \pm \Delta V_{\Leftarrow}^{p',t'} : ref(p, t, a', d_{\Rightarrow}) = \langle p', t', a', d_{\Leftarrow} \rangle; \\ ref^{-1}(p', t', a', d_{\Leftarrow}) = \langle p, t, a', d' \rangle; d' \cap d_{\Rightarrow} \neq \emptyset. \end{aligned}$$

Пересечение всех парных областей, удовлетворяющих такому условию, образует пространство целостности. Мерой целостности является мощность пространства целостности.

При этом, любые парные отношения в пространстве целостности являются толерантными, т.е. удовлетворяют свойствам рефлексивности и симметричности. Следует напомнить, что если отношение рефлексивно и симметрично, то оно остаётся таким же и для операции объединения и пересечения отношений, но не всегда соблюдается для транзитивного замыкания отношений.

Указанное свойство показывает, что предложенная модель и мера целостности сохраняются при любой комбинации элементов вычислительной среды, для которых построено пространство целостности.

На рисунке 2 схематически изображен процесс установления и контроля целостности для среды состоящей из трех компонент: операционная система, прикладное программное обеспечение и средства защиты информации. Если исходное множество параметров состоит одного элемента, т.е. вся область взаимосоответствия проецируется в одну исходную точку, то система обладает устойчивой целостностью.

Если такое условие не выполняется, т.е. существует область обратного отражения, возможно два случая:

1. область обратного отображения попадает в множество параметров ОС, не соответствующим условиям безопасности (политика безопасности). Тогда система потенциально не целостна или несовместима;

2. область обратного отображения не выходит из требований безопасности. Тогда необходима рекурсивная проверка каждой точки из области обратного отображения в пространстве операционной системы на область в пространстве средств защиты информации и программного обеспечения для определения существования их пересечений. Когда область найдена, установлен гомоморфизм области для всех рассмотренных параметров, которые определяют область оперативной целостности системы в целом.

Продемонстрируем предлагаемую модель, используя аппарат теории ориентированных трехдольных графов. Элементы множеств X, Y, Z являются вершинами соответствующих долей графа. Стрелки соединяют только вершины различных долей графа. Стрелка из x в y означает, что элемент $x \in X$ может давать безопасное состояние системы только в сочетании с элементом $y \in Y$ (это необходимое, но не достаточное условие). Стрелка из y в x означает, что элемент $y \in Y$ может давать безопасное состояние системы только в сочетании с элементом $x \in X$ (это необходимое, но недостаточное условие). Аналогичная ситуация со стрелками между элементами множеств X и Z , Y и Z . Из вершины может выходить (в нее могут входить) 0, 1 или несколько стрелок.

Утверждение. Стрелка $x \rightarrow y$ существует тогда и только тогда, когда существует стрелка $y \rightarrow x$. Поэтому трехдольный граф может быть неориентированным.

Доказательство. Стрелка $x \rightarrow y$ означает, что состояние $(x, y, *)$ может быть безопасным, если существует соответствующий элемент $* \in Z$. Точно так же стрелка $y \rightarrow x$ означает, что состояние $(x, y, *)$ может быть безопасным, если существует соответствующий элемент $* \in Z$. Стрелка из x в y (и стрелка из y в x) отсутствует, если ни для одного $* \in Z$ состояние $(x, y, *)$ не может быть безопасным. Поэтому либо обе стрелки $x \rightarrow y$ и $y \rightarrow x$ существуют одновременно, либо ни одна из них не существует. Что и требовалось доказать.

Далее вместо стрелок в графе будем использовать ребра. Клика в трехдольном графе – это трехдольный подграф, в котором каждая вершина соответствующей доли связана со всеми вершинами двух других долей. Состояние $w = (x, y, z)$ безопасно, если оно – треугольник в трехдольном графе (или элементарная клика). Обратно, любой треугольник дает безопасное состояние. Множество всех треугольников трехдольного графа совпадает с множеством безопасных состояний системы. Представляет интерес описание безопасности системы не в точке, а в некоторой области так, чтобы некоторое изменение изначально безопасного состояния системы по любой координате оставалось бы безопасным. Аналогом такой области является клика трехдольного графа. Чем больше вершин в клике, тем сильнее может изменяться состояние системы, оставаясь безопасным. Однако задача поиска такой клики является трудоемкой, поэтому на практике она сводится к автоматизации процесса анализа параметров компонентов информационной среды ИТКС.

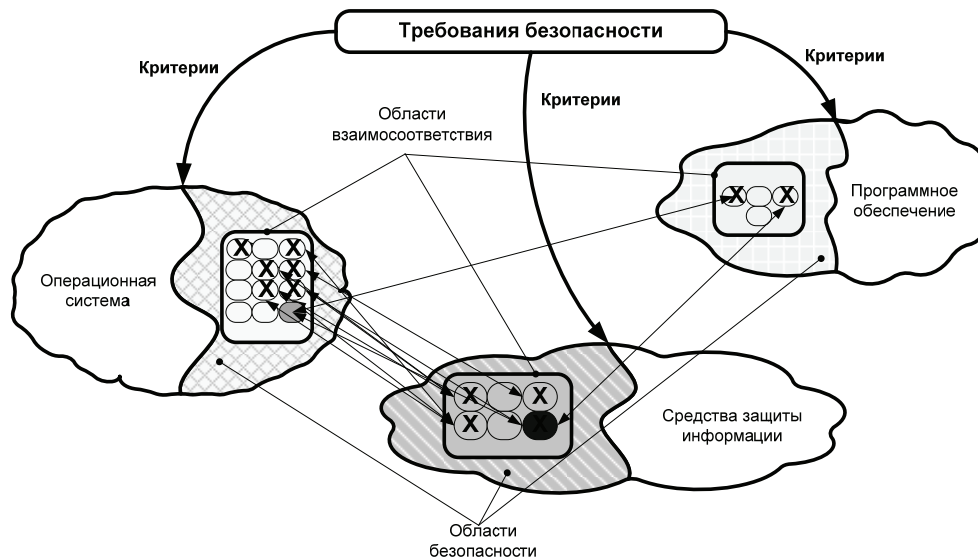


Рис. 2. Влияние параметров безопасности на целостность

Рассмотренная модель позволяет разработать технологию контроля целостности информационной среды ИТКС путем мониторинга и управления параметрами взаимосоответственности и реализовать ее в качестве программного средства. Предлагаемая технология включает следующие компоненты:

- логическую модель (позволяет установить «интеллектуальное» взаимосоответствие параметров среды на основе модели среды, ПО и правил их поведения);
- критериальный аппарат (позволяет задать отношения между требованиями функциональности, требованиями безопасности и текущим состоянием среды в виде критериев);
- механизм отклонений для изменяемых компонентов среды (учитывает изменения параметров безопасности в рамках допустимой области целостности, ограниченной критериями);
- механизм криптографического контроля целостности для стабильных компонентов среды;
- управление безопасностью и обеспечение динамической защищенности (реализует замкнутый цикл «управление–контроль–анализ–управление»).

Структура логической модели приведена на рисунке 3. Данная структура реализована в виде специального логического процессора.

Логическая модель среды ИТКС включает модель безопасности операционной среды (иерархия настроек безопасности ОС, факторы контроля и управления доступом) и модель функционирования и безопасности ПО и средств защиты (рабочие настройки, настройки безопасности, параметры совместимости). Критерий целостности состоит в проверке логических условий безопасности среды и логических условий функциональности среды. Область целостности определяется как множество состояний операционной среды, для которых выполняются критерии целостности.

Предлагаемая технология позволяет, используя средства динамического контроля состояния информационной среды ИТКС, построить систему управления безопасностью и обеспечение динамической целостностью в виде рисунка 4.

Программный комплекс «Декарт» реализует централизованное удаленное управление безопасностью и обеспечивает динамическую защищенность ИТКС путем настройки значений конфигурационных параметров штатных программных средств контроля доступа, входящих в состав операционных систем семейства Windows, фиксацию и автоматический анализ заданной системной конфигурации, выявление нарушений безопасности, вызванных допущенными при администрировании ошибками.

Принцип функционирования программного комплекса «Декарт» при настройке конфигурационных параметров заключается в формализации требований, предъявляемых к безопасности операционных систем семейства Windows, в виде набора необходимых параметров безопасности, и их установке в настраиваемой системе.



Рис. 3. Логическая модель контроля целостности

Наличие встроенных типовых шаблонов, учитывающих базовые рекомендации по безопасности Windows-систем, возможность автоматической настройки по «снимку» предварительно сконфигурированной системы, и наличие средства описания правил разграничения доступа корпоративной политики безопасности позволяют использовать программный комплекс «Декарт» в качестве инструмента реализации доверенной среды на базе механизмов Windows.

Программный комплекс «Декарт» реализует централизованное удаленное управление безопасностью и обеспечивает динамическую защищенность ИТКС путем настройки значений конфигурационных параметров штатных программных средств контроля доступа, входящих в состав операционных систем семейства Windows, фиксацию и автоматический анализ заданной системной конфигурации, выявление нарушений безопасности, вызванных допущенными при администрировании ошибками.

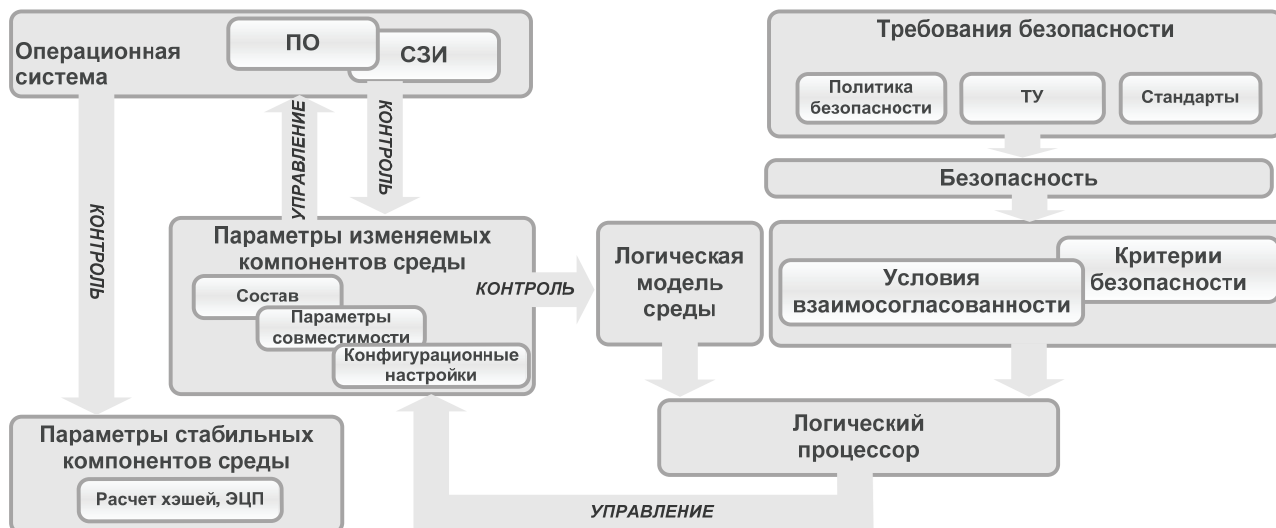


Рис. 4. Управление безопасностью и обеспечение динамической защищенности

Принцип функционирования программного комплекса «Декарт» при настройке конфигурационных параметров заключается в формализации требований, предъявляемых к безопасности операционных систем семейства Windows, в виде набора необходимых параметров безопасности, и их установке в настраиваемой системе. Наличие встроенных типовых шаблонов, учитывающих базовые рекомендации по безопасности Windows-систем, возможность автоматической настройки по «снимку» предварительно сконфигурированной системы, и наличие средства описания правил разграничения доступа корпоративной политики безопасности позволяют использовать

программный комплекс «Декарт» в качестве инструмента реализации доверенной среды на базе механизмов Windows.

В состав программного комплекса «Декарт» (рисунок 5) включены следующие компоненты:

- агент управления конфигурационными параметрами безопасности;
- редактор политик безопасности;
- процессор безопасности;
- менеджер отчетов;
- консоль управления программным комплексом;
- менеджер сетевого взаимодействия и безопасности программного комплекса.



Рис. 5. Модульная схема программного комплекса «Декарт»

Менеджер сетевого взаимодействия и безопасности программного комплекса обеспечивает установку/удаление агентов на компьютеры домена Active Directory, поддерживает сетевое взаимодействие с ними, реализует каталогизацию и безопасность сохраняемых файлов системных состояний безопасности, файлов проверяемых встроенных шаблонов безопасности и создаваемых описаний политик безопасности, отчетов с результатами работы и служебной информации программного комплекса «Декарт».

Описание произвольных политик безопасности создается в полуавтоматическом режиме. При помощи редактора политик безопасности эксперт может сгенерировать логическое описание правил путем задания условий безопасности системы.

Файлы зафиксированного системного состояния и условия безопасности, указанные в виде шаблона или политики безопасности, обрабатываются в процессоре безопасности. Он производит интерпретацию описаний, оценивает безопасность состояния системы в соответствии с указанными условиями безопасности. Пространство перебора конфигурационных параметров определяется моделью безопасности операционной системы Windows и ограничивается областью определения требований безопасности. В том случае, если процессор безопасности выявляет нарушение требований безопасности состояния системы, то программный комплекс «Декарт» позволяет в терминах исследуемой операционной системы продемонстрировать набор конфигурационных параметров, который приводит к нарушению. Менеджер отчетов формирует описания уязвимых состояний системы, проверенные условия безопасности, результаты настройки и анализа безопасности.

Программный комплекс «Декарт» активно развивается и вбирает в себя познания и опыт широкого круга специалистов. Это позволяет иметь решение, которое максимально отвечает реальным потребностям профессионалов в сфере информационной безопасности. Применение представленной технологии, помимо автоматизации мониторинга целостности и управления безопасностью, позволяет также оптимизировать администрирование и конфигурирование систем информационной безопасности, повысить эффективность эксплуатации инфраструктуры ИТКС, снизить персональные квалификационные требования и тем самым сократить ресурсные и финансовые издержки.

Молдовян А.А., Молдовян Н.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПЕРСПЕКТИВЫ РАЗВИТИЯ КРИПТОГРАФИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ**

Введение

Практика обеспечения безопасности информационных технологий тесно связана с широким применением криптографических протоколов и алгоритмов, предоставляющих гибкие и эффективные механизмы защиты информации, придания юридической значимости электронным документам и сообщениям, контроля их целостности и решения задачи неотслеживаемости (анонимности). Криптографическое обеспечение информационных технологий в настоящее время еще не достигло такого уровня, который можно было бы охарактеризовать как достижение соответствия практического и теоретического арсенала криптографии. В этом плане практика информационной безопасности имеет значительный резерв для своего совершенствования путем вовлечения в область практического использования незадействованных резервов арсенала современных криптографических алгоритмов и протоколов. В то же время практика приложения криптографических методов выдвигает перед прикладной криптографией задачу поиска новых примитивов, на основе которых можно обеспечить повышение производительности и снижение стоимости реализации алгоритмов шифрования, генерации и проверки электронной цифровой подписи (ЭЦП) при обеспечении требуемого уровня безопасности. 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 разработкой новых типов криптографических протоколов и 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. Такие результаты делают актуальным проблему разработки примитивов «постквантовой» криптографии, с которой связано направление поиска новых вычислительно трудных задач, которые имеют экспоненциальную (или хотя бы сверхполиномиальную сложность) в квантовой модели вычислений и могут быть использованы для построения двухключевых криптосистем.

Предваряя момент практической реализации квантового компьютера, в настоящее время предложены новые примитивы, перспективные в качестве базы «постквантовой криптографии». В этом направлении развития криптографии весьма привлекательным представляется использование бесконечных некоммутативных групп переплетения (Infinite Braid Groups) и трудной задачи нахождения сопрягающего элемента для двух заданных элементов некоммутативной группы (Conjugacy Search Problem) и некоторых других трудных задач. При этом данное направление имеет существенные перспективы стать конкурентоспособной ветвью современной прикладной криптографии, поскольку по текущим оценкам при заданном уровне стойкости оно обеспечивает разработку алгоритмов и протоколов криптографии с открытым ключом, обладающих существенно более высокой производительностью.

В настоящем сообщении рассматриваются перспективы криптографического обеспечения безопасности информационных технологий в плане более широкого внедрения результатов современной прикладной криптографии, разработки новых прикладных криптоалгоритмов и расширения арсенала современной криптографии путем разработки новых криптографических протоколов и поиска примитивов «постквантовой» криптографии. Поскольку расширение криптографического арсенала, применяемого в практических системах и средствах информационной безопасности, во многих приложениях тесно связано с вопросами стандартизации криптографических алгоритмов и протоколов, то предлагается также и рассмотрение перспектив расширения криптографических стандартов.

1. Современные блочные шифры

Первым широко применявшимся криптографическим стандартом явился американский стандарт блочного шифрования DES. Ему на смену пришел международный стандарт блочного шифрования AES –результат многолетней деятельности широкого круга ведущих криптографов всего мира. По оценкам специалистов ушедший в отставку стандарт заслуживает самых высоких похвал. Принципы, положенные в основу синтеза этого алгоритма блочного шифрования полностью себя оправдали. Признано, что за период его существования не было предложено методов криптоанализа, которые были бы более эффективными, чем простой перебор по пространству возможных значений секретного ключа. Только возросшая вычислительная мощность массово доступных компьютеров потребовала замены шифра DES. При этом единственной

криптографической проблемой признана малая длина секретного ключа. В переходный период от момента, когда стандартный вариант DES был признан недостаточным для обеспечения современного уровня стойкости, и до момента принятия нового стандарта AES был принят временный стандарт, известный как тройной DES (TripleDES, TDES или 3DES) и расширяющий функциональность первого стандарта блочного шифрования. Последнее опиралось на опыт многолетнего анализа исходного стандарта, благодаря чему, новый вариант стандарта DES не потребовал большого объема новых исследований по оценке его стойкости и мог быть принят в достаточно короткие сроки. Основным недостатком алгоритма 3DES является уменьшение производительности программной реализации в 3 раза и снижение эффективности аппаратной реализации по критерию отношения производительности к схемотехнической сложности примерно во столько же раз.

В заданных критериях проектирования алгоритма DES из технологических требований фигурировал критерий обеспечения достаточной скорости шифрования при сравнительно недорогой аппаратной реализации с учетом уровня микроэлектронной технологии 70х годов прошлого века. Программные реализации DES всегда отставали от практических потребностей практики защиты информации, поэтому при разработке нового стандарта AES в критерии разработки было включено требование эффективности, как аппаратной, так и программной реализации, причем на различных платформах. Таким образом, AES изначально разрабатывался как универсальный блочный шифр, поэтому он не мог обеспечить максимальной производительности при программной реализации и максимальной эффективности при аппаратной реализации. Новый стандарт прочно занял нишу криптосистем для универсальных применений. Однако области специализированных технологических применений блочных шифров требуют максимального увеличения скорости программ шифрования или максимального увеличения эффективности аппаратной реализации, поэтому остаются актуальными специализированные решения. Отсутствие стандартов на специализированные блочные шифры оставляет открытым вопрос расширения стандартов на блочные шифры и открывает перспективы по поиску новых решений по разработке специализированных алгоритмов блочного шифрования.

В России эта проблема усугубляется еще и тем, что в современных условиях стандарт блочного шифрования ГОСТ 2814789 едва ли находится среди лидеров как универсальный алгоритм блочного шифрования. Несмотря на существование большого числа хорошо апробированных универсальных блочных шифров и проверенных подходов к проектированию стойких алгоритмов, имеются существенные проблемы принятия новых стандартов блочного шифрования. Это связано в первую очередь с тем, что стойкость современных блочных шифров обосновывается экспертно, а появление формальным подходов к доказательству стойкости не предвидится. В процессе разработки нового стандарта следует предусмотреть все возможные атаки, причем даже те, которые представляются не актуальными в виду их технической неосуществимости. Следует показать, что все эти атаки имеют трудоемкость не ниже полного перебора по ключевому пространству. Для фиксированного набора формализованных атак это сделать было бы проще, однако решение вопроса о границах этого набора достаточно сложен. Иллюстрацией этой проблемы является недавно предложенные атаки на стандарт AES (см. <http://eprint.iacr.org/2009/374.pdf>), которые аналитикам позволяют говорить о взломе этого стандарта, хотя на практике не просматриваются реальные случаи, когда нарушитель мог бы их использовать и вычислить ключ AES. Тем не менее, если бы эти атаки были предложены на этапе анализа всех шифров, являвшихся кандидатами, а затем финалистами AES, то новым стандартом быстрее всего стал бы не Rijndael, а другой шифр (например, RC6 или Serpent).

Перспективы разработки эффективных аппаратноориентированных блочных шифров можно связать с подходом, базирующимся на использовании операций, управляемых данными (datadriven operations). В этом направлении первым перспективным предложением явилось использование управляемых битовых перестановок произвольного типа [1,2], реализуемых с помощью перестановочных сетей (ПС), ранее использовавшихся для реализации перестановок, зависящих от секретного ключа для придания гибкости алгоритму шифрования [3]. Последнее применение оказалось малоэффективным, что было показано в работе [4]. Идея реализации переменных перестановок с помощью ПС дала новый импульс к использованию этого примитива при разработке скоростных шифров. Исследование переменных перестановок как криптографического примитива выполнено в работе [5], а различные варианты скоростных аппаратных шифров на основе ПС предложены и исследованы в работах [6–9]. На основе ПС с симметричной топологией предложен новый тип криптографического примитива – переключаемые переменные битовые перестановки [9,10], которые реализуют две взаимно обратные управляемые перестановки в зависимости от бита режима операции и могут быть выполнены операционными блоками с достаточно низкой сложностью схемотехнической реализации.

Криптографическое применение ПС выдвинуло задачу разработки новых топологий ПС, реализующих перестановки различного порядка (порядок это максимальное число входных битов, которые могут быть переставлены на выходе в произвольные разряды) при минимальном

критическом пути комбинационной схемы, реализующей ПС. Для построения эффективных переключаемых ПС потребовалось построить симметричные топологии ПС различного порядка и размера входного блока данных. Решение этих вопросов предлагается в работах [9,10]. В частности показано, что для фиксированного значения порядка, реализуемого некоторой минимальной ПС с четным числом активных слоев, могут быть построены симметричные ПС, обладающие тем же значением порядка и числа активных слоев.

С целью повышения производительности программных реализаций шифров на основе переменных битовых перестановок в работе [11] предложена универсальная архитектура команды управляемой битовой перестановки, реализуемая на основе переключаемых ПС с симметричной топологией. Предложенная команда обеспечивает реализацию за один машинный такт как переменных битовых перестановок (например, перестановок, зависящих от преобразуемых данных), так и произвольных наперед заданных фиксированных перестановок. При этом в обоих случаях обеспечивается выполнение двух взаимно обратных перестановок за два последовательных машинных такта. Встраивание данной команды в стандартный набор элементарных операций микропроцессора требует минимальных аппаратных затрат, а ее наличие обеспечит резкое повышение производительности при программной реализации большого числа алгоритмов (криптографических и не криптографических), широко применяемых на практике. Это обстоятельство потенциально придает новые привлекательные возможности процессорам, повышая их конкурентоспособность, что дает основание ожидать практического внедрения предложенной команды в массово используемые микропроцессоры общего назначения.

В случае встраивания универсальной команды битовых перестановок открываются перспективы существенного повышения скорости шифрования, обеспечиваемой программно-ориентированными шифрами. Перспективным в этом направлении является подход, основанный на комбинировании следующих двух примитивов: 1) переключаемых переменных перестановок и 2) выборки подключей в зависимости от преобразуемых данных [12,13]. Также перспективно для построения скоростных программных шифров комбинирование операции переменной битовой перестановки с операциями сложения, вычитания и «поразрядного исключающего ИЛИ» (XOR).

Операция переключаемых переменных битовых перестановок весьма перспективна также и для встраивания в микроконтроллеры, ориентированные на решение специальных задач. Для криптографических контроллеров предложены также и упрощенные архитектуры, позволяющие минимизировать аппаратные затраты на команду управляемых перестановок за счет некоторого снижения функциональности универсальной команды битовых перестановок. В случае микроконтроллеров может оказаться целесообразной реализация различных вариантов переменных подстановочных операций в виде самостоятельной команды. Этот вариант реализуется с использованием, рассматриваемых ниже управляемых сетей.

Для дальнейшего повышения эффективности (по критерию отношения производительности к затрачиваемым схемотехническим ресурсам при обеспечении требуемого уровня безопасности) аппаратной реализации предложено использовать управляемые подстановочно-перестановочные сети (УППС), построенные по аналогии с ПС с использованием управляемых подстановок минимального размера (2×2) типа $F_{2/1}$ и $F_{2/2}$. Обоснование применения, критерии выбора и классификация элементов $F_{2/1}$, имеющих одноразрядный управляющий вход, приведены в работах [15]. Аналогичные вопросы для элементов $F_{2/2}$, имеющих двухразрядный управляющий вход, даны в работе [16]. Анализ стойкости и различных вариантов аппаратной реализации шифров на основе УППС показал, что применение этого примитива вместо ПС позволяет обеспечить дальнейшее повышение эффективности аппаратной реализации алгоритмов, основанных на переменных операциях. По аналогии с ПС для УППС введено понятие порядка. Показано, что все топологические решения, найденные для ПС могут быть использованы и для УППС, в том числе и решения, обеспечивающие построение переключаемых управляемых операций. Показано, что наиболее интересными для практики являются УППС со значением порядка $h = 1, 2, \dots, n/4, n$, где n разрядность входа УППС.

В настоящее время в ряде приложений используется «слабая» криптография, к которой могут быть отнесены следующие два типа криптоалгоритмов: 1) криптографические алгоритмы, использующие нормативно ограниченную длину секретного ключа (разрешенная криптография) и 2) ослабленные криптографические алгоритмы, используемые по технологическим причинам (например, в случае недостаточной производительности микропроцессоров, ограничивающей применение алгоритмов «сильной» криптографии). В первом случае имеет место тенденция увеличения разрешенной длины секретного ключа, а во втором – усиление алгоритмов и в перспективе переход к использованию «сильной» криптографии. Последняя тенденция связана с совершенствованием микроэлектронной технологии и элементной базы вычислительных и телекоммуникационных устройств, а также с разработкой более эффективных специализированных аппаратных решений, предоставляемых «сильной» криптографией.

Одной из проблем криптографического обеспечения информационных технологий является доверие пользователей к криптоалгоритмам и протоколам. Перспективное решение этой проблемы в области симметричных криптосистем связано с вопросами расширения функциональности набора криптографических стандартов и повышение уровня криптографических знаний среднего пользователя в области информационных технологий. В области криптосистем с открытым ключом доверие пользователей обеспечивается не только экспертными оценками, но и формальными доказательствами того, что стойкость криптосистемы не ниже сложности решения трудной задачи, положенной в основу криптосистемы. Абсолютным доверием пользуются безусловно стойкие криптосистемы, к которым можно отнести шифр с бесконечным равновероятным ключом и систему квантового распределения ключей. Однако технологическая значимость данных криптосистем достаточно ограничена, кроме того, их безусловная стойкость доказывалась для случая, когда вопросы аутентификации информации считаются решенными. В специальных приложениях безусловно стойкие криптосистемы представляют особый интерес, что стимулирует исследования в области квантовой криптографии.

2. Расширение арсенала криптографии с открытым ключом

Криптография с открытым ключом широко раздвинула границы криптографических приложений. В самом общем плане задачи решаемые криптографией можно отнести к следующим трем типам:

- обеспечение секретности,
- аутентификация электронной (цифровой) информации,
- обеспечение неотслеживаемости анонимности.

Симметричная криптография (криптосистемы с секретным ключом) рассматривают главным образом только первый тип задач. Вопросы аутентификации информации для одноключевой криптографии являются зависящими от задачи обеспечения секретности, кроме того, реализация на их основе систем электронной цифровой подписи (ЭЦП) требует вовлечения доверительного центра, что практически оставляет такие системы ЭЦП вне поля практического использования. Две последние задачи определяют в значительной степени лицо и содержание современной криптографии. Имеются достаточное число других частных задач, решаемых с привлечением двухключевых криптографических алгоритмов, однако они часто оказываются связанными с аутентификацией информации или обеспечением анонимности. Обеспечение секретности передаваемых сообщений также может быть реализовано с использованием криптоалгоритмов с открытым ключом. Более того, по аналогии с двухключевыми алгоритмами, обладающими свойством коммутативности (алгоритм RSA) могут быть построены алгоритмы коммутативного блочного шифрования, востребованные рядом практически значимых криптографических протоколов (бесключевое шифрование, игра в покер по телефону и др.).

Доверие пользователей к криптосистемам с открытым ключом основано на предположении о том, что используемые в них вычислительно трудные задачи имеют экспоненциальную, по крайней мере, сверхполиномиальную сложность. Причем эти задачи являются хорошо изученными, поэтому вероятность появления прорывных алгоритмов их решения, которые приведут к взлому криптосистем, в обозримое время является достаточно малой. Технический прогресс, приводящий к росту производительности вычислительной техники, может быть компенсирован сравнительно небольшим увеличением размера параметров криптоалгоритмов. Появление новых прорывных алгоритмов решения трудных задач может привести к необходимости отказа от использования некоторых криптоалгоритмов. Несмотря на малую вероятность таких событий для случая хорошо апробированных трудных задач, лежащих в основе алгоритмов двухключевой криптографии, перспективны разработки схем ЭЦП, основанных на двух трудных задачах различного типа, т.е. схем, взлом которых требует одновременного решения двух трудных задач. В таких схемах стойкость как число операций, которые необходимо выполнить для успешного осуществления лучшей известной атаки, не повышается, однако значительно повышается уровень безопасности как векторное понятие, включающее как стойкость, так и вероятность взлома за счет появления новых прорывных алгоритмов решения трудных задач. Данное направление отражено в работах [17,18], в которых рассматриваются подходы к построению алгоритмов ЭЦП, протоколов коллективной ЭЦП и слепой ЭЦП, основанных на двух трудных задачах.

Технологические применения выдвигают задачу разработки двухключевых криптосистем, обладающих сравнительно высокой производительностью при достаточно низкой сложности аппаратной реализации. В этом направлении существенное продвижение оказалось возможным за счет использования эллиптических кривых (ЭК) над конечным полем в качестве примитивов криптоалгоритмов с открытым ключом. Основные перспективы практического применения алгоритмов эллиптической криптографии связаны с тем фактом, что ЭК могут быть выбраны так, что задача дискретного логарифмирования на них будет иметь экспоненциальную сложность. В этом случае достигается снижение сложности процедур формирования и проверки ЭЦП при заданном уровне стойкости по сравнению со схемами ЭЦП, основанными на сложности дискретного логарифмирования в конечном поле. Кроме того, ЭК предоставляют возможность применения

новых подходов к разработке криптоалгоритмов, в частности на основе использования разрыва между сложностью вычислительной задачи Диффи-Хеллмана и сложностью задачи принятия решения Диффи-Хеллмана, которое имеет место для специальных случаев суперсингулярных ЭК. Последняя особенность специальных видов ЭК предоставляет специфические возможности построения цифровых подписей различного типа: обычные ЭЦП, схемы слепой подписи, протоколы агрегированной ЭЦП и другие протоколы мультиподписи.

Протоколы мультиподписи в настоящее время представляют в настоящее время достаточно развитую область криптографических протоколов. Однако перспективы практического использования можно связать главным образом с их частным видом, известным как протоколы коллективной подписи или схемы коллективной ЭЦП. В частности протоколы коллективной подписи наиболее простым способом решают проблему одновременного подписания контракта и проблеме одновременного подписания пакета контрактов (различные контракты подписываются различными группами пользователей) на расстоянии. Области применения коллективной ЭЦП достаточно многообразны. В частности они могут быть применены в системах электронного голосования, защиты документов от подделки, системах принятия коллективных решений удаленными пользователями и др. Видимо из известных протоколов мультиподписи коллективная ЭЦП имеет перспективы быть принятой в качестве стандарта. Другим практически важным типом криптографических протоколов является слепая подпись, представляющая интерес для решения задачи обеспечения неотслеживаемости (анонимности) в системах электронных денег и системах тайного электронного голосования. Этот тип протоколов также представляется целесообразным для стандартизации.

Поскольку разработка новых стандартов является трудоемким и долговременным мероприятием, то расширение функциональности криптографических стандартов, востребованное практикой, целесообразно реализовать на базе уже принятых стандартов, принимая в качестве основы уже имеющиеся рекомендованные процедуры формирования и проверки подлинности ЭЦП. В этом случае могут быть значительно сокращены сроки введения стандартов на новые криптографические протоколы. Изучение этого вопроса по отношению к стандартам ЭЦП России, Беларуси и Украины показало, что базовые процедуры этих стандартов в неизменном виде могут быть использованы в протоколах: 1) коллективной ЭЦП, 2) слепой ЭЦП и 3) слепой коллективной ЭЦП. Этот факт может быть использован для сокращения затрат на расширение криптографических стандартов в этих странах.

Сравнительно новым и перспективным для практического применения направлением в двухключевой криптографии является использование некоммутативных конечных групп в качестве криптографического примитива. С их применением связаны ожидания снижения сложности аппаратной реализации, повышения производительности криптоалгоритмов и протоколов и сохранения стойкости в случае появления квантового компьютера. Последнее связано с тем, что в синтезе криптосхем на основе некоммутативных групп может быть использована новая трудная задача, заключающаяся в нахождении сопрягающего элемента для двух заданных элементов группы. Ожидается, что данная задача сохранит экспоненциальную сложность и в случае квантовой модели вычислений. Зарубежными исследователями разрабатываются схемы ЭЦП, открытого распределения ключей и открытого шифрования с использованием бесконечных некоммутативных групп, известных как Braid Groups. Для криптографических построений представляют интерес также и конечные некоммутативные группы. Предварительные исследования показали, что последний случай также весьма интересен для реализации перспективных криптосхем. Для синтеза некоммутативных конечных групп различного типа может быть использован подход, ранее апробированный для построения коммутативных групп векторов [19,20]. Показано, что для некоторых некоммутативных групп (например, Braid Groups) имеется разрыв между сложностью вычисления сопрягающего элемента и сложностью задачи принятия решения о сопряженности двух заданных элементов. Этот разрыв может быть использован при построении схем ЭЦП [21]. Также представляет интерес использование сложности дискретного логарифмирования в циклической подгруппах некоммутативных групп. Реализация криптографических алгоритмов на основе циклических подгрупп простого порядка, содержащихся в нециклической конечной группе, мотивируется ожидаемой экспоненциальной сложностью используемой задачи дискретного логарифмирования. Для развития последнего подхода представляет интерес синтез некоммутативных конечных групп легко вычислимого порядка, который содержит достаточно большие простые делители. Некоммутативные конечные группы векторов в ряде случаев дают примеры таких групп, в связи с чем они представляются перспективным криптографическим примитивом.

По сравнению с другими структурами, используемыми в криптографии, некоммутативные группы являются относительно малоизученным объектом и только будущие исследования могут показать будут ли подтверждены ожидания, связанные с ними, включая экспоненциальную стойкость в квантовой модели вычислений.

СПИСОК ЛИТЕРАТУРЫ

1. Moldovyan A.A., Moldovyan N.A. A Cipher Based on DataDependent Permutations // Journal of Cryptology. 2002. Vol. 15. No 1. P. 61–72.
2. Moldovyan A.A. Fast Block Ciphers Based on Controlled Permutations // Computer Science Journal of Moldova. 2000, Vol. 8. No 3. P. 270–283.
3. Portz M. A. Generalized Description of DESbased and Benesbased Permutation generators // Advanced in Cryptology – AUSCRYPT'92 // Lecture Notes in Computer Science. SpringerVerlag. 1992. Vol. 718. P. 397–409.
4. Biryukov A. Methods of cryptanalysis. Research thesis, Israel institute of Technology, Haifa, 1999.
5. Moldovyan N.A., Moldovyan A.A., Goots N.D. Variable Bit Permutations: Linear Characteristics and Pure VBPBased Cipher // Computer Science Journal of Moldova. 2005. Vol. 13. No 1(37). P. 84–109.
6. Goots N.D., Moldovyan A.A., Moldovyan N.A. Fast encryption algorithm SPECTRH64 // Proceedings of the International workshop, Methods, Models, and Architectures for Network Security / Lect. Notes Comput. Sci., Berlin: SpringerVerlag. 2001. Vol. 2052. P. 275–286.
7. Moldovyan N.A. Fast DDPBased Ciphers: Design and Differential Analysis of CobraH64. // Computer Science Journal of Moldova. 2003. Vol. 11. No 3 (33). P. 292–315.
8. Sklavos N., Moldovyan N.A., Koufopavlou O. High Speed Networking Security: Design and Implementation of Two New DDPBased Ciphers // Mobile Networks and Applications. 2005. Vol. 10. P. 219–231.
9. Moldovyan N.A., Moldovyan A.A. DataDriven Block Ciphers for Fast Telecommunication Systems. – Auerbach Publications. Talor & Francis Group. New York, London. 2007 185 p.
10. Moldovyan N.A. On Cipher Design Based on Switchable Controlled Operations // Proceedings of the International workshop, Methods, Models, and Architectures for Network Security / Lect. Notes Comput. Sci., Berlin: SpringerVerlag. 2003. Vol. 2776. P. 316327.
11. Moldovyan A.A., Moldovyan N.A., Moldovyanu P.A. Architecture Types of the Bit Permutation Instruction for General Purpose Processors // Springer LNCS. 2007. Vol. XIV. P. 147159 / 3d Int. Workshop IF&GIS'07 Proc. St.Petersburg, May 2829, 2007.
12. Moldovyan N. A., Moldovyanu P. A., Summerville D. H.. On Software Implementation of Fast DDPBased Ciphers. // International Journal of Network Security. 2007. Vol. 4. No. 1. P. 81–89.
13. Moldovyan A.A., Moldovyan N.A. Software Encryption Algorithms for Transparent Protection Technology // Cryptologia. 1998. Vol. XXII. No 1. P. 56–68.
14. Moldovyan N.A., Moldovyan A.A. Flexible block ciphers with provably inequivalent cryptalgorithm modifications // Cryptologia, 1998. Vol. XXII. No 2. P. 134–140.
15. Moldovyan N.A., Moldovyan A.A., Ereemeev M.A. A class of datadependent operations // International Journal of Network Security. 2006. Vol. 2. No. 3. P. 187204 (<http://ijns.femto.com.tw>)
16. Молдовян Н. А., Молдовян А. А., Еремеев М. А. Криптография: от примитивов к синтезу алгоритмов СПб, БХВПетербург, 2004. 446 с.
17. Дернова Е.С., Молдовян Н.А. Синтез алгоритмов цифровой подписи на основе нескольких вычислительно трудных задач // Вопросы защиты информации. 2008. № 1. С. 22–26.
18. 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.
19. С.Е. Доронин, П.А. Молдовяну, В.Е. Синева. Векторные конечные поля: задание умножения векторов большой четной размерности // Вопросы защиты информации. 2008. № 4(83). С. 2–7.
20. Дернова Е.С., Костина А.А., Молдовян Н.А., Молдовяну П.А. Направления применения конечных векторных пространств в криптографии // Вопросы радиоэлектроники. Серия общетехническая. 2009. Выпуск 2. С. 164–174.
21. Ko K.H., Lee S.J., Cheon J.H., Han J.W., Kang Jusung, Park Ch. New public key cryptosystems using braid groups // Advances in cryptology – CRYPTO 2000 Proc. / SpringerVerlag LNCS. 2000. Vol. 1880. P. 166–183.

Вус М.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
О ГАРМОНИЗАЦИИ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО
ДОСТУПА В ГОСУДАРСТВАХ – УЧАСТНИКАХ МЕЖПАРЛАМЕНТСКОЙ АССАМБЛЕИ СНГ**

Введение

Целью сотрудничества государств – участников Содружества Независимых Государств (СНГ) в сфере обеспечения информационной безопасности является совместная защита интересов этих государств в информационной сфере. Защите подлежит информация ограниченного доступа. Под информацией ограниченного доступа понимается информация, доступ к которой ограничен законодательством государств – участников СНГ либо межгосударственными договорами. Защищаемыми свойствами информации ограниченного доступа являются ее целостность и конфиденциальность.

К угрозам информационной безопасности в Содружестве относят осуществление действий в интересах получения несанкционированного доступа к информации государств – участников СНГ. Несмотря на происходящие в мире изменения в экономической и политической сферах опасность шпионажа нисколько не перестала быть менее актуальной. Формы и методы работы спецслужб постоянно совершенствуются. Разведки предпочитают сегодня действовать под прикрытием коммерческих, общественных, научно-исследовательских и иных иностранных и международных организаций [1].

Акцентируем внимание на трех следующих аспектах гармонизации законодательства по защите информации ограниченного доступа в государствах – участниках межпарламентской ассамблеи СНГ.

1. Важное место в законодательствах государств СНГ об информационной безопасности занимает законодательство о государственной тайне (государственных секретах). Феномен государственных секретов (государственной тайны) – объективная реальность в сфере межгосударственных отношений. Посягательства на государственные тайны в развитых государствах рассматриваются как преступления против основ конституционного строя и безопасности государства. Все страны Европы, например, реализующие самостоятельную внешнюю политику, признают обоснованность защиты информации в режиме государственной тайны в области обороны.

Системы защиты государственных секретов в государствах, образовавшихся на пространствах бывшего СССР, объективно имеют общие корни, происходящие от системы защиты информации, ранее имевшей место в нашей общей стране. В системе обеспечения информационной безопасности государств – участников СНГ защита государственных секретов (государственной тайны) представляется одной из важнейших её составляющих, призванных обеспечить интересы национальной и коллективной безопасности, гарантии обороноспособности, а также сохранение приоритета новейших научных и технологических разработок в ряде отраслей экономики.

Законодательного определения государственной тайны, как известно, ни в Российской империи, ни в СССР не было. Активное законотворчество в информационной сфере, законодательная легитимация институтов тайн начали развиваться в ставших независимыми государствах лишь в начале 90-х годов прошлого века. В числе основных принципов правового регулирования информационных отношений, наряду с законодательным закреплением прав всех субъектов на свободный поиск, получение, использование и распространение информации, изначально было определено «установление правовых форм защиты информации и гарантий информационной безопасности» [2].

Закон о государственной тайне впервые был принят в Российской Федерации в 1993 году. В том же году был принят Закон «О защите государственных секретов» в Республике Узбекистан. В 1994 г. были приняты Закон Республики Беларусь «О государственных секретах», Закон Кыргызской Республики «О защите государственных секретов», Закон Республики Молдова «О государственной тайне» и Закон Украины «О государственной тайне». В 1996 г. были приняты первые Законы «О государственной тайне» в Республике Таджикистан и в Азербайджанской Республике, а также Закон Республики Армения «О государственной и служебной тайне». В 1999 г. был введен в действие Закон «О государственных секретах» в Республике Казахстан. В последующие годы в эти законодательные акты неоднократно вносились изменения. В Республике Беларусь, например, в настоящее время действует вторая редакция Закона «О государственных секретах» и проходит парламентскую экспертизу его третья версия.

Сегодня в законах всех государств – участников СНГ в той или иной мере определены перечни сведений, относимых к государственной тайне, что может рассматриваться как непосредственное закрепление принципа законности при построении системы правового регулирования защиты государственных тайн. Нашел свое закрепление в законодательных актах государств также и принцип обоснованности засекречивания сведений, что позволяет легализовать содержательную оценку относимости к государственной тайне конкретных сведений.

В рамках Содружества Независимых Государств в настоящее время существует ряд двусторонних межправительственных соглашений о защите секретной информации. В их числе соглашение о защите секретной информации между Российской Федерацией и Республикой Армения (2002); соглашение о взаимном обеспечении защиты государственной тайны Российской Федерации и государственных секретов Республики Беларусь (2003). Аналогичные соглашения подписаны между Российской Федерацией и Республикой Таджикистан, Российской Федерацией и Киргизской Республикой, между Российской Федерацией и Республикой Узбекистан (2003), Российской Федерацией и Республикой Казахстан (2004). Многостороннее соглашение о взаимном обеспечении сохранности секретной информации заключено государствами СНГ – участниками Договора о коллективной безопасности в 2004 году [3].

Хотя законодательства государств – участников СНГ и методологии защиты государственных секретов в этих государствах имеют общую предысторию и теоретическую базу, концептуальные подходы в ряде случаев являются оригинальными, отражающими результаты самостоятельного на протяжении почти двух десятилетий развития собственных правовых систем этих независимых государств. Вследствие этого в действующем сегодня законодательстве государств – участников СНГ существуют как отдельные концептуальные различия, так и различия в структуре элементов правового регулирования [4].

Вопросы унификации и гармонизации законодательства в сфере защиты государственной тайны нашли свое место в работе Межпарламентской Ассамблеи Государств – участников Содружества Независимых Государств (МПА СНГ). На первом этапе её работы эти вопросы были учтены при разработке уголовно-правовых и уголовно-процессуальных модельных законодательных актов. Так, вопросы защиты государственной тайны нашли отражение в принятых в 1996 г. в качестве рекомендательных законодательных актов модельном Уголовном и Уголовно-процессуальном кодексах [5].

Знаковым этапом международного сотрудничества стало принятие в 2003 году МПА СНГ Модельного закона «О государственных секретах». Закон «определяет правовые основы и единую систему защиты государственных секретов в интересах обеспечения национальной безопасности, регулирует общественные отношения, возникающие в связи с отнесением сведений к государственным секретам, их засекречиванием, распоряжением ими, защитой и рассекречиванием» [6]. Этот закон охватывает своим регулированием государственную и служебную тайну. Подчеркнем, также, что Модельный закон в первой своей статье дает определения применяемых в нем основных понятий.

Принятие Межпарламентской Ассамблеей государств – участников СНГ модельных законов и соглашений создало определенные условия для дальнейшего совершенствования, унификации и гармонизации национальных законодательств государств – участников, способствует развитию их экономического, научно-технического и военно-технического сотрудничества. Вместе с тем работа в этом направлении должна быть продолжена. Не все прогрессивные новации модельных законов нашли

отражение в национальных законах, и по-прежнему обоснована постановка вопроса об их реализации при развитии национальных законодательств. Применительно к Российской Федерации это актуально, например, в части касающейся уголовно-процессуального законодательства [7]. Специалисты-аналитики отмечают, например, что сегодня требуют совершенствования уголовное и уголовно-процессуальное законодательства. «Практика сталкивается, например, с серьезнейшей проблемой доказывания состава государственной измены, когда иностранным адресатом являются, например, экологическая организация, благотворительный фонд, средство массовой информации, коммерческая фирма» [8].

Развитие интеграционных процессов высветило и новые проблемы. Так в системе СНГ, например, в настоящее время функционирует ряд международных организаций, деятельность которых требует получения сведений, относимых национальными законодательствами к государственной тайне (государственным секретам). В то же время модельное законодательство (ст. 28 модельного закона «О государственных секретах») не предусматривает возможность передачи сведений, составляющих государственную тайну, международным организациям. Сегодня положения о передаче сведений составляющих государственную тайну другим государствам или международным организациям включены только в российский Федеральный закон «О государственной тайне» и новый, принятый в 2003 году Закон Республики Таджикистан «О государственной тайне».

2. Базовым различием для правового регулирования отношений в сфере оборота государственных секретов в государствах – членах ОДКБ сегодня представляется толкование основных понятий. Данный тезис можно проиллюстрировать, например, обратившись к сравнительному анализу ныне действующих базовых законов России и Беларуси.

Сегодня основы отношений в сфере защиты государственных секретов у этих двух государств – участников СНГ и членов Организации Договора о коллективной безопасности, а также государств-партнеров по Союзному государству, регламентируются Законом Российской Федерации «О государственной тайне» [9] и Законом Республики Беларусь «О государственных секретах» [10]. Различия видны уже в самом названии базовых законов. Российское законодательство использует единое неделимое понятие: «государственная тайна», в то время как в белорусском законодательстве о государственных секретах выделены две правовые категории: «государственная тайна» (таблица 1) и «служебная тайна». Отметим, что в действующем сегодня в Российской Федерации законодательстве нет закона о служебной тайне.

Таблица 1

Государственная тайна

Российская Федерация	Республика Беларусь
Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.	Государственные секреты, разглашение или утрата которых могут повлечь тяжкие последствия для национальной безопасности Республики Беларусь, а также создать угрозу безопасности граждан либо их конституционным правам и свободам.

Отметим, что вышеупомянутый Модельный закон МПА СНГ использует следующее определение понятия: «государственная тайна – сведения военного, экономического, политического и иного характера, разглашение или утрата которых носит или может нанести ущерб национальной безопасности государства». Такую же формулировку этого понятия содержит Закон Республики Казахстан «О государственных секретах».

Наибольшие различия, как представляется, имеют место в толковании таких понятий, как «допуск» и «доступ».

Таблица 2

Допуск

Российская Федерация	Республика Беларусь
Процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений.	Право на доступ к государственным секретам физического лица или на осуществление деятельности юридического лица с использованием сведений, составляющих государственные секреты, санкционированное в порядке, установленном актами законодательства Республики Беларусь.

Таблица 3

Доступ

Российская Федерация	Республика Беларусь
Санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну	Полномочие на ознакомление и (или) работу физического лица со сведениями, составляющими государственные секреты, предоставленное в порядке, установленном актами законодательства Республики Беларусь

Заметим, что данный модельный закон МПА СНГ использует следующие понятия:

- «допуск к государственным секретам – процедура оформления права граждан на доступ к сведениям, составляющим государственные секреты, а организаций – на проведение работ с использованием таких сведений»;

- «доступ к сведениям, составляющим государственные секреты – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственные секреты».

В связи с последним важно подчеркнуть, что понятийный аппарат модельного законодательства призван выполнять роль межнационального языка правового общения.

Можно также отметить, что существенные различия имеют место в действующем сегодня российском и белорусском законодательствах в подходах к правовому регулированию допуска к государственной тайне (государственным секретам) юридических лиц.

В Российской Федерации применяется лицензирование деятельности – по своей сути хозяйственная форма государственного регулирования. Лицензия выдается на основании результатов специальной экспертизы предприятия и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, «расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию» (статья 27 Закона РФ «О государственной тайне»). В Республике Беларусь используется разрешительная система – форма административного регулирования. Допуск юридических лиц к государственным секретам осуществляется на основе разрешения, выдаваемого по результатам проверки юридического лица и аттестации его руководителей, ответственных за защиту государственных секретов. Проверка осуществляется органами государственной безопасности в рамках их служебной деятельности и финансируется из бюджетных средств.

Отдельные различия в понятийном аппарате и подходах к правовому регулированию можно также обнаружить, обратившись к базовым законам других государств – участников СНГ. Все вышесказанное только подчеркивает необходимость актуализации внимания к вопросам совершенствования и гармонизации законодательства о защите государственной тайны в Межпарламентской Ассамблее государств – участников СНГ.

3. Важные социально-правовые аспекты. В легальной интерпретации тайна – это информация, доступ к которой ограничен. По своей природе тайна – не простое и противоречивое социально-правовое явление. Информация приобрела сегодня статус товара в международном и национальном обороте. При этом вопросы разрешения противоречий между правом на информацию и необходимыми его ограничениями в целях обеспечения баланса интересов субъектов информационных отношений становятся все более сложными и комплексными. Законодательное регулирование не может обойти сферу защиты государственной тайны, которая хотя и отражается на степени открытости государства перед обществом, но является важным и необходимым элементом обеспечения суверенитета и безопасности государства.

Академия ФСБ России, например, проводившая анализ расследовавшихся в период 1997–2002 гг. уголовных дел, предметом преступления в которых являлась государственная тайна, отмечает, что «два из трех преступных посягательств на государственную тайну инициировались иностранными специальными службами». В то же время исследователи отмечают, что по сравнению с советским периодом резко участились посягательства на сведения об оперативно-розыскной, контрразведывательной и разведывательной деятельности, в том числе со стороны преступных группировок и коммерческих структур [7].

Институт защиты государственной тайны привлекает внимание исследователей и общественности. В последние годы вышел в свет целый ряд открытых публикаций, в том числе монографий, предметом рассмотрения в которых являются различные аспекты защиты государственной тайны [11–12]. Среди увидевших свет публикаций есть и работы теоретического характера, в которых анализируется сам феномен «тайна», исследуется «тайноведческий процесс» [13–16].

Государственная тайна – это та часть информации, которая изъята из свободного оборота. Она ограничивает конституционные права граждан, интересы в научной, экономической и иных сферах и приводит к конфликту интересов, в котором приоритет отдается интересам безопасности государства. Имея своей целью обеспечение безопасности государства, государственная тайна не должна препятствовать развитию экономики, росту деловой и интеллектуальной активности граждан. В силу этого недопустим расширительный подход к определению её понятия и круга относимых к ней сведений. Критерии государственной тайны должны быть понятными и приемлемыми не только для государства, но и для гражданина и общества.

Проведенные в 2008 г. в Российской Федерации научно-практическая конференция «15 лет российскому Закону «О государственной тайне» и парламентские слушания «Законодательство о государственной тайне: вчера, сегодня, завтра» дали полезный материал для дальнейшего анализа и совершенствования действующего законодательства о защите государственной тайны. Материалы конференции и парламентских слушаний опубликованы и доступны для изучения [17–18].

Государственная тайна – это межотраслевой правовой институт. Поэтому правовое регулирование оборота государственной тайны должно быть комплексным, т.е. осуществляться нормами различных отраслей права. Аналитики отмечают, как «настоятельную потребность современного общества»,

необходимость разработки методик оценки ущерба от распространения сведений, составляющих государственную тайну, подчеркивая, что «дальнейшее превращение оборота государственной тайны в административно-правовой режим бесперспективно» [19].

Заключение

Развитие государств – участников Межпарламентской Ассамблеи СНГ протекает сегодня в русле глобальной общемировой тенденции формирования информационного общества. Процессы информационной глобализации и расширяющееся применение информационно-телекоммуникационных технологий во всех сферах жизнедеятельности общества проецируют новые риски и угрозы безопасности. Обостряющаяся при этом проблема информационной безопасности требует комплексных решений.

Работа по выработке рекомендаций по совершенствованию и гармонизации законодательства об информационной безопасности для государств СНГ требует осмысления современного состояния и систематизации понятийного аппарата (не в последнюю очередь в сфере защиты информации и защиты государственной тайны). Рассматривая модельное законодательство в качестве основы для унификации и гармонизации законодательств государств – участников, необходимо дальнейшее и его совершенствование.

В целях совершенствования механизмов правового регулирования складывающихся общественных отношений, а также унификации законодательства разных стран, целесообразно наладить сотрудничество в вопросах изучения наработанного в независимых государствах опыта и его взаимное заимствование.

В рамках совместной работы российскими и белорусскими коллегами, подготовлен глоссарий (словарь) базовых терминов, толкование которых закреплено юридически в законодательных актах государств ряда государств – участников СНГ [20]. Представляется, что такой материал будет полезен в повседневной работе руководителям всех уровней как справочное практическое пособие. При разработке нормативной основы, и особенно, в международных договорах и соглашениях принципиально важно грамотное толкование и использование терминов и понятий.

СПИСОК ЛИТЕРАТУРЫ

1. Государственная тайна и ее защита в Российской Федерации / Под ред. М.А. Вуса и А.В. Фёдорова. 3-е изд. СПб.: Изд-во «Юридический центр Пресс», 2007. С. 92–112.
2. Рекомендательный законодательный акт «О принципах регулирования информационных отношений в государствах – участниках МПА СНГ», статья 3 // Вестник Межпарламентской Ассамблеи, 1994. С. 24–29.
3. О ратификации соглашения о взаимном обеспечении сохранности секретной информации в рамках Организации Договора о коллективной безопасности. Закон Республики Беларусь от 04.05.2005 №6-з // Национальный реестр правовых актов Республики Беларусь, 13.05.2005, №73, 2/1103.
4. Макаров О.С. Сравнительно-правовой анализ закона Республики Беларусь «О государственных секретах» и закона Российской Федерации «О государственной тайне» // Условия реализации прав граждан и организаций на основе информационных технологий. М.: ИГП РАН, 2010. С. 180–189.
5. Информационный бюллетень МПА СНГ. 1996. №10. (С. 83–84); Приложения: №1 (С. 84–216); № 2 (С. 3–373).
6. Информационный бюллетень МПА СНГ. 2003. №31. (С. 230–261).
7. Фёдоров А.В. Гармонизация и унификация законодательства о государственной тайне в государствах – участниках сообщества независимых государств // Материалы конференции «Информационная безопасность регионов России (ИБРР–2009)». СПб.: СПОИСУ, 2009. С. 21–22.
8. Власов В.А. Совершенствование правового регулирования сведений, составляющих государственную тайну // В кн. «Организационно-правовые вопросы борьбы с терроризмом»; Центр исследований проблем безопасности РАН; Науч. совет при Совете Безопасности РФ. М.: Наука, 2006. С. 215–237.
9. Закон Российской Федерации «О государственной тайне» от 21.07.1993 №5485–1 (ред. от 01.12.2007 с изм. и доп.) // Собрание законодательства РФ, 13.10.1997, №41, стр. 8220–8235.
10. Закон Республики Беларусь «О государственных секретах» от 4.01. 2003 № 172–3 // Национальный реестр правовых актов Республики Беларусь. – 22.01.2003, №8.
11. Дьяков С.В. Преступления против основ конституционного строя и безопасности государства. СПб.: Изд-во «Юридический центр Пресс», 2009. – 267с.
12. Рябчук В.Н. Государственная измена и шпионаж. – СПб.: Изд-во «Юридический центр Пресс», 2007. – 1102с.
13. Рабкин В.А. Исторический генезис правового регулирования защиты государственной тайны в России // Информационное право. 2006, 4 (7). С. 7–11.
14. Ловцов Д.А. Концептуально-логическое моделирование юридического понятия «тайна» // Информационное право. 2009, 2(17). С. 12–14.
15. Верютин В.Н. Анализ основных положений Модельного закона СНГ «О государственных секретах» на основе общеправовых принципов // «Черные дыры» в Российском законодательстве. 2009. №6. С. 51–54.
16. Крюков С.В. Конституционные основы ограничения основных прав и свобод человека и гражданина в целях защиты государственной тайны // Автореф дисс. канд. ю.н. – М., ВШЭ, 2009. (<http://www.hse.ru/lingua/en/sci/diss/8875944/index.html>)
17. От культа секретности к информационной культуре (К 15-летию российского Закона «О государственной тайне»). – СПб.: ОНТЗ, 2006. – Вчера, сегодня, завтра. М.: Издание Государственной Думы, 2009. – 96с.
18. Законодательство о государственной тайне: вчера, сегодня, завтра. М.: Издание Государственной Думы, 2009. 96с.
19. В кн. «Организационно-правовые вопросы борьбы с терроризмом / [сост. В.Л. Шульц]; Центр исследований проблем безопасности РАН; Научн. Совет при Совете Безопасности РФ. – М.: Наука, 2008. – 240с.
20. Вус М.А., Макаров О.С. К вопросу об унификации законодательства стран ОДКБ в сфере оборота сведений, составляющих государственную тайну (государственные секреты) // «Управление защитой информации». – Минск–Москва, 2010.



ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ

Блашков В.И., Ермохин К.М.

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

ООО НПП «Аналитическая геофизика»

ФИЗИЧЕСКАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО ПОЛЯ И ЕГО ВЗАИМОДЕЙСТВИЯ С МАТЕРИЕЙ В СВЕТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧЕЛОВЕКА И ОБЩЕСТВА

Одной из разновидностей информационной деятельности человека является борьба в информационной сфере (между отдельными индивидами, организациями, государствами)

Ведение информационных войн предполагает наличие и использование определенных средств борьбы, то есть оружия. Информационное оружие, воздействующее непосредственно на человека, делится на два вида [1].

Информационно-психологическое оружие обращено на сознание человека и через него воздействует на поведение, убеждения, мотивы и потребности, нравственные установки, отношение к тому, что происходит в обществе. В качестве такого оружия могут использоваться все средства массовой информации, Интернет, публичные выступления, беседы, внушение, гипноз и т. п.

Энергоинформационное оружие воздействует на физиологию и психофизиологию человека, минуя его сознание. Человек не осознает факта воздействия, но в зависимости от его вида начинает ощущать либо бодрость, уверенность в себе, либо подавленность, тревогу, страх, агрессивность на фоне утраты способности контролировать свои действия.

В данной статье мы рассмотрим физическую модель информационного поля, которое может служить основой применения энергоинформационного способа воздействия на человека. Данная модель интересна также и с общей познавательной, и с философской точки зрения.

В научном сообществе существует множество концепций и определений информации как специфической философской субстанции, принципиально отличной от вещества и энергии. Не разрешен также спор о том, оставить за информацией общенаучный статус или рассматривать ее в качестве философской категории.

В качестве примера приведем классификацию, предложенную И.Б. Новиком и А.Ш. Абдуллаевым [2]. Всё множество трактовок понятия информации они сводят к трем подходам – субстанциальному, реляционному и релевантному:

1. Субстанциальный подход отождествляет информацию с материей, а именно, с её атрибутивным свойством – структурой. Наибольшее число исследователей информации – сторонников диалектического материализма – придерживается этого подхода.

2. Реляционный подход отождествляет информацию с некоей материально-духовной субстанцией как фундаментальной структурой бытия, в которой исчезают различия между субъективной и объективной реальностями. Данный подход имеет идеалистические черты.

3. При релевантном подходе информационные процессы непосредственно связываются с мыслительными и психическими процессами человека. Это наиболее узкий подход, антропный по своей сущности.

Целью данной статьи является попытка предложить объяснение природы носителей информации и способ ее существования в рамках материалистической концепции, которая близка к субстанциальному подходу. Для этого вводится в рассмотрение новое материальное поле, называемое нами информационным.

Представляется разумным начать с обсуждения имеющихся на данный момент некоторых определений самого понятия информации.

Можно упомянуть Библию, где говорится: «В начале было слово...». Хотя определение отсутствует, имеется указание на первичность информации по отношению к другим формам существования материи, ее основополагающую роль в зарождении и существовании вселенского бытия.

Краткий словарь иностранных слов [3] трактует информацию как осведомление, сообщение, осведомляющее о положении дел или чьей-либо деятельности, сведения о чём-либо.

Наиболее адекватным, близким к реальности, нам представляется определение информации в рамках физики: «Объекты материального мира находятся в состоянии непрерывного изменения, которое сопровождается обменом энергии. При этом изменение состояния одного объекта приводит к изменению состояния другого объекта. Это явление, вне зависимости от того, как, какие именно состояния и каких

именно объектов изменились, называется передачей сигнала (информации) от одного объекта другому. Изменение состояния объекта при передаче ему сигнала называется регистрацией сигнала» [4]. В рамках такого определения первичными по отношению к информации фактически объявляются материя и энергия.

Приведем высказывание автора книги «Дао физики» физика Фритьофа Капры [5]: «...теперь я чувствую себя гораздо увереннее, поскольку параллели с восточными мистическими учениями обнаруживаются не только в физике, но и в биологии, психологии и других науках. Изучая взаимосвязи между физикой и этими науками, я обнаружил, что понятия современной физики могут быть перенесены и в другие области посредством теории систем. Изучение понятия “системы” в биологии, медицине, психологии и общественных науках показало, что подход с позиций теории систем значительно усиливает параллели между современной физикой и восточным мистицизмом. Помимо этого, новая биология систем и новая психология систем обнаруживают другие совпадения с мистическими учениями, лежащие за пределами предмета изучения физики».

Из этой цитаты можно заключить, что, по мнению автора, мистические явления не должны отвергаться наукой, наука должна чувствовать себя неполноценной, пока она неспособна объяснить те явления, которые кажутся нам невероятными только из-за ограниченности нашего знания. Мистические же явления для человека в подавляющем большинстве сводятся к процессам передачи и восприятия информации. Возможно, мистические явления связаны с существованием непознанной пока субстанции – слабо энергетического информационного поля, как самостоятельной физической сущности.

Потребность решения вопроса о природе информации, с нашей точки зрения, наиболее четко была сформулирована в [6]: «Для характеристики реального мира ныне недостаточны фундаментальные понятия классической физики – материя, вещество, движение, энергия, пространство, время. Для полноты этой характеристики необходимо столь же фундаментальное и столь же всеобщее понятие информации. Нет материи без информации, нет и информации без ее материального носителя – вещества и энергии». Это высказывание во многом предвосхитило содержание данной статьи.

Отталкиваясь от этих определений и высказываний, попытаемся представить природу носителей информации на пути аналогии с другими фундаментальными понятиями. Для этого мы предлагаем обратиться к современной теории гравитации, поскольку именно к ней близка предлагаемая концепция информационного поля.

По преданию, после открытия закона всемирного тяготения, Исаак Ньютон, в ответ на вопрос о причине взаимного притяжения материальных тел, признал, что это пока тайна, покрытая мраком, а цель его исследований – познать законы мироздания. Совершенно ясно, что ответы на вопросы «Почему?» в науке получить намного сложнее, чем ответы на вопросы «Как?», но ученые неустанно пытаются это сделать.

Так, согласно теории В.Я. Бриля [7], причиной (источником) гравитации является всесторонний изотропный поток струнообразных частиц во Вселенной, а в книге С.А. Николаева [7] предложен и механизм зарождения этих частиц. На этом механизме следует остановиться подробнее, поскольку он приводит к нетрадиционному взгляду на гравитацию вообще и красное смещение в спектрах далеких галактик в частности, а также может подвести к универсальной трактовке информации, как практически самостоятельной сущности.

Излучаемые звездами фотоны в процессе движения в мировом эфире тормозятся, излучая при этом часть своей энергии в окружающее пространство в виде специальных частиц, названных “фотониками” [8] (аналогично электрон излучает энергию в тормозящем электрическом поле). Всестороннее давление этих частиц на материальные тела объясняет гравитацию как образование зоны тени между ними, в которую они и “затягиваются” в направлении друг к другу (гипотеза швейцарского физика Ж.Л. Лесажа, выдвинутая в 1782г.).

Таким образом, данная теория объясняет как явление гравитации, так и красное смещение излучения дальних галактик в процессе “старения” фотонов которые теряют часть своей энергии за счет торможения мировым эфиром. В реальном же существовании эфира не только не сомневался величайший физик – экспериментатор XX века Н. Тесла, но и использовал его энергию на практике.

После этих разъяснений представляется возможным сделать логический шаг дальше, к более мелким частицам – носителям информационного поля. Термин мелкая частица употребляется нами в смысле ее малого радиуса взаимодействия с веществом или эфиром. Если фотон в своем движении излучает фотоники, то что мешает им в свою очередь излучать часть своей энергии в процессе движения в эфире в виде еще более мелких частиц? Процесс такого переизлучения, очевидно, может быть многократным. Эти частицы, будучи еще более мелкими, чем фотоники, уже не должны подчиняться известным нам законам гравитации. Их предельная скорость движения может значительно превосходить скорость света, поскольку их радиус взаимодействия с частицами эфира много меньше, чем даже у нейтрино.

Принимая такую гипотезу, мы можем говорить о существовании всестороннего потока сверхмелких частиц, образующих вселенское информационное поле. В качестве доводов в пользу его существования можно предложить следующее.

1. Широко известное сейчас излучение Кирлиана, визуализируемое с помощью современных приборов, различает у человека семь “нематериальных” энергетических оболочек, что косвенно свидетельствует о существовании по крайней мере семи энергетических уровней (разновидностей частиц). Это излучение не исчезает одновременно с физической смертью человека, а продолжает свое существование и фиксируется достаточно длительное время.

2. Экстрасенсорное воздействие некоторых одаренных людей на других людей, животных, растения и предметы. Будучи узко направленным и обладая огромным дальностью действия, это воздействие не может быть объяснено электромагнитными полями, известными нам, но легко объясняется потоком сверхмелких частиц. Прямой аналогией этого является высокая проникающая способность коротковолновых рентгеновских лучей (мелких фотонов) и нейтрино – сверхмелких частиц.

3. И, наконец, сам процесс эволюции общественного сознания. Давно известно, что масса мозга человека и его мыслительные способности прямой зависимостью отнюдь не связаны. Более того, у многих крупных животных масса мозга больше, чем у человека, однако их творческие способности заведомо ниже. Решающим фактором в этом выступает степень извилистости поверхности мозга. Это напоминает структуру сложной электромагнитной антенны: чем больше различных и сложных контуров в ней, тем более широкополосной и одновременно избирательной она является. Напрашивается аналогия: мозг – специализированная антенна, работающая на сверхкоротких волнах – сверхмелких частицах.

Процесс обучения человека какому-либо делу с этой точки зрения является процессом обучения настраиваться на “нужную длину волны”. Это похоже на то, как опытный радист довольно быстро путем вращения ручек настройки находит нужный сигнал в радиозфире, в то время как неопытный может делать это долго, а подчас и безуспешно. Различным отраслям знания при этом соответствуют различные диапазоны излучения информационного поля.

Известно, что всякая антенна, работая на прием, является одновременно и супергетеродином, т.е. излучает на частоте приема. Это означает, что если кому-то удалось настроиться на новую волну (совершить открытие), то информационное поле вокруг него усиливается на этой частоте и те, кто находится рядом с ним, получают возможность также поймать эту частоту, хотя раньше не могли этого сделать. Таким образом, вокруг гениев-одиночек возникают научные школы, развивающие различные отрасли знания. Эти школы разрастаются за счет взаимного усиления и переизлучения информации, что приводит впоследствии к общечеловеческому знанию. Так было и с арифметикой, ныне доступной всем, а в древние века лишь избранным. Так было с аналитической геометрией – уделом профессоров в XIX веке, а сейчас ею владеет любой второкурсник. Перечисление может быть очень долгим.

Общение посредством информационного поля, является, вероятно, не только свойством человека, но и животных и растений, а, можно полагать, и косной материи. Обмен информацией происходит как в органическом, так и в неорганическом мире.

Любая реакция материального объекта на внешнее воздействие порождает ответный поток в информационном поле. А это означает, что все материальные объекты своим существованием поддерживают и усиливают информационное поле. В большей степени это присуще органическому миру, особенно – человеку. Смысл жизни в этом плане состоит в преумножении количества специфичной тонкой материи (генетической информации живого) во Вселенной путем активного взаимодействия (через переизлучение) с единым информационным полем. Это согласуется с выводом Гегеля о том, что Бог (Абсолют) создал Человека, чтобы через него, через его чувства и мысли глубже и всестороннее познать самое себя.

Таким образом, можно сформулировать философское определение информации как субстанции, соединяющей причину и следствие, в противоположность времени, их разделяющему. Носителем этой субстанции может являться излучение с более тонкой, чем у вещества и известных нам видов излучения, структурой. Информация так же материальна, как и вещество и, в частности, обладает энергией. Предложенная модель информационного поля может оказаться продуктивной в процессе изучения законов природы и общества.

Также, безусловно, она может иметь отношение к информационной безопасности отдельного человека, организаций, государства, поскольку описывает физический механизм передачи информации при помощи, не описанной ранее субстанции. В тоже время ряд фактов указывает на возможность существования подобной субстанции, а значит, предлагаемая модель информационного поля может иметь отношение к недостаточно изученным пока способам воздействия на поведение людей.

СПИСОК ЛИТЕРАТУРЫ

1. Петров В.П., Петров С.В. Информационная безопасность человека и общества. М.: ЭНАС, 2007. 334 с.
2. Новик И.Б., Абдуллаев А.Ш. Введение в информационный мир. М.: Наука, 1991. 228 с.
3. Новый краткий словарь иностранных слов. М.: Большая российская энциклопедия. 2005. 794 с.
4. Большая физическая энциклопедия. Т.2 М.: Советская энциклопедия. 1988, 704 с.
5. Фритьюф Капра, Дао Физики. М.: София. 2008. 416 с.
6. Берг А.И., Спиркин А.Г. Кибернетика и диалектико-материалистическая философия. Проблемы философии и методологии современного естествознания. М.: 1973. 251 с.
7. Брилль В.Я. Кинетическая теория гравитации и основы Единой теории материи. СПб.: Наука. 1995. 436 с.
8. Николаев С.А. Эволюционный круговорот материи во Вселенной. СПб.: Изд-во Политехнического университета, 2007. 301 с.

Воропаев Д.Б.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АНАЛИЗ МЕТОДОВ ФОРМИРОВАНИЯ СТОИМОСТИ ЭЛЕМЕНТОВ СЛОЖНЫХ
ВОЕННО-ТЕХНИЧЕСКИХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Введение

Под обеспечением информационной безопасности понимается целенаправленная деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на эту информацию. Информационная безопасность в настоящее время актуальна для подавляющего большинства предприятий, коммерческих организаций, и является одним из ключевых процессов обеспечения функционирования государственных учреждений, особенно учреждений государственного управления и силовых структур. С целью всесторонней защиты информационных ресурсов создаются комплексные технические системы по защите данных. Применительно к силовым структурам, здесь можно говорить о разработке военно-технических систем (ВТС) защиты информации. В общем случае, подобные ВТС защиты информации присутствуют в каждой системе вооружений, и решают ряд специальных задач. Постоянное совершенствование систем вооружений и военной техники требует развития технологий защиты информации, разработки новых образцов технологического оборудования защиты, совершенствования системы их управления. Проведение подобных разработок на современном этапе развития государства связано с разрешением ряда проблем, в том числе экономического характера. Одной из проблем является оценивание стоимости элементов перспективных систем защиты на этапе заключения контракта по их разработке. Точность оценивания стоимости элементов перспективных ВТС во многом определяется выбором метода расчета цены, поэтому настоящая статья посвящена обзору современных методов ценообразования и анализу их применимости для оценивания стоимости сложных военно-технических систем.

Элементы военно-технических систем (ВТС) являются специфической продукцией, самостоятельно создавать которую могут страны, имеющие высокий уровень развития науки и техники, а также способные вложить в исследования, разработку, испытания и производство значительные материальные ресурсы. Следовательно, стоимость элементов ВТС определяется их спецификой, которая складывается из следующих компонентов:

- сложность технологического процесса производства,
- особенность эксплуатации и технического обслуживания,
- необходимость наличия квалифицированных кадров для обслуживания и эксплуатации,
- значительные издержки на исследования и разработку.

Стоимость образца ВТС достаточно сложно прогнозировать на стадии заключения контракта, особенно в начале разработки перспективных образцов ВТС, не имеющих отечественных и зарубежных аналогов, в силу того, что стоимость таких образцов зависит от множества факторов, а облик перспективной ВТС, состав ее подсистем, тактико-технические характеристики (ТТХ) в процессе разработки могут значительно меняться. Это обуславливает разнообразие существующих методов ценообразования на образцы ВТС, потребность непрерывного совершенствования этих методов, а также существование системы мер государственного регулирования производственной сферы оборонного комплекса.

В высокоразвитых странах, разрабатывающих военно-техническую продукцию, существует достаточно жесткая система мер государственного регулирования в производственной сфере ВТС, а также в сфере военно-технического сотрудничества [10]. Государственное влияние на уровень цен в области производства элементов ВТС обусловлено характером взаимоотношений между государством и военно-промышленными компаниями. Государство вынуждено постоянно варьировать ценовой политикой с целью нахождения наиболее оптимального механизма ценообразования, который позволил бы совместить противоречивые тенденции – стремление государства к приобретению военно-технической продукции для национальных вооруженных сил при минимальных издержках и стремление подрядчиков получить максимальную прибыль.

Министерства обороны таких стран, таких как Великобритания, Франция, Германия, США используют в своей закупочной деятельности в основном два типа цен на военную продукцию. Первый тип представляет «фиксированные» цены, второй – цены «на основе компенсации издержек производства» [10]. При заключении контракта на производство ВТС определяется его цена, которая обычно отражает оценку издержек производства, условия, при которых заключается сделка, и обоснования, приводимые каждой из сторон, в данном случае заказчиком в лице министерства обороны и производителем. По существу, позиции сторон определяют верхний и нижний предел цены разрабатываемой системы. При обосновании цен достаточно широко применяются методы ценообразования, традиционно используемые в машиностроении, а также в торговле машинами и оборудованием [1,2]. При этом издержки производства являются основой, определяющей уровень цены на военно-техническую продукцию. В тоже время поставщики и производители ВТС, как

отечественные, так и зарубежные, учитывают и другие факторы, влияющие на стоимость ВТС. К таким факторам можно отнести следующие:

- новизна военно-технической продукции,
- объем заказа,
- тактико-технические характеристики системы в целом и составляющих ее элементов,
- подготовленность технического эксплуатирующего персонала,
- длительность периода эксплуатации,
- сопровождение системы в форме технического обслуживания, ремонтов, модернизаций, поставки запасных частей.

В российских организациях – производителях ВТС, разработаны и применяются на практике различные методики по определению цен на новые и модернизированные образцы ВТС.

В качестве основных методов, используемых в настоящее время в ценообразовании образцов ВТС, применяются затратные, параметрические методы, такие как расчет по удельным показателям, метод экспертных оценок (балловый), а также другие методы, также широко используемые при выполнении расчетов стоимости гражданской технической продукции.

Ниже рассмотрены основные, наиболее часто используемые методы ценообразования ВТС, представлена их сущность и краткие характеристики.

Классификация существующих методов ценообразования

Все существующие методы ценообразования технической продукции можно разделить на три основные группы:

- затратные,
- параметрические,
- рыночные.

При определении стоимости технической продукции выбор того или иного метода ценообразования обусловлен тем, на что в большей степени ориентируется производитель или продавец продукции: издержки производства, нормативы затрат на технико-экономические параметры продукции, конъюнктуру рынка, соответственно.

Военно-технические системы как товар обладают определенной спецификой, например, отсутствием четко выраженной рыночной дифференциации, наличием одного заказчика и ограниченного числа производителей военно-технической продукции, длительным сроком производства и эксплуатации ВТС. Поэтому использовать для определения их стоимости рыночные методы, например, такие как ориентацию на конкурентов, ориентацию на потребителя, или ориентацию на спрос, можно в лучшем случае при продаже элементов ВТС на внешнем рынке. Поэтому, в настоящей статье эту группу методов рассматривать не будем, а более подробно остановимся на затратных и параметрических методах. Что же касается рыночных методов ценообразования, то их подробный анализ и рамки применимости достаточно широко отражены в литературе [15]. На рисунке 1 представлена классификация существующих методов ценообразования.

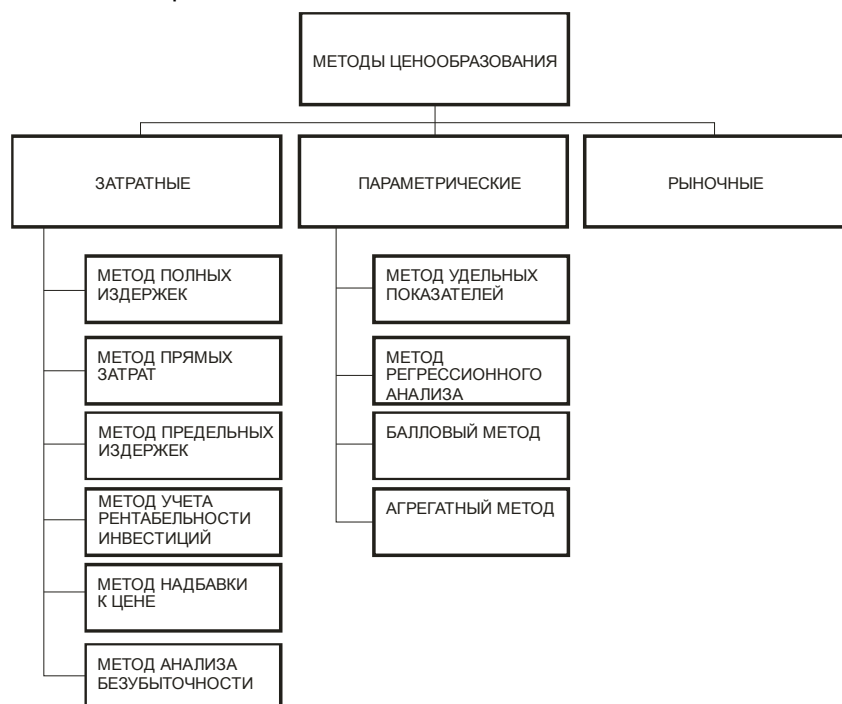


Рис. 1. Классификация методов ценообразования

Затратные методы ценообразования

Сущность затратных методов ценообразования заключается в расчете цены изделий ВТС путем суммирования издержек производства и некой определенной надбавки, которая составляет норму прибыли. Как показано на рисунке 1, к затратным методам относятся следующие:

- метод полных издержек,
- метод прямых затрат,
- метод предельных издержек,
- метод на основе анализа безубыточности,
- метод учета рентабельности инвестиций,
- метод надбавки к цене.

Метод полных издержек. Сущность метода, основанного на определении полных издержек (Full Cost Pricing, Target Pricing, Cost Plus Pricing) [4] состоит в суммировании совокупных издержек, постоянных и переменных, а также прибыли, которую производитель продукции планирует получить, и рассчитывается по формуле:

$$P = C_{\text{пер}} + C_{\text{пост}} + \Pi, \quad (1)$$

где P – цена продукции,

$C_{\text{пер}}$ – переменные издержки производства,

$C_{\text{пост}}$ – постоянные издержки производства,

Π – норма прибыли.

В том случае, если предприятие при расчете цены продукции отталкивается от определенного процента рентабельности производства, то расчет продажной цены производится по следующей формуле [5]:

$$P = (C_{\text{пер}} + C_{\text{пост}}) \times (1 + R/100), \quad (2)$$

где R – ожидаемая (нормативная) рентабельность.

Как показывает анализ литературы [5], любой метод отнесения на себестоимость продукции постоянных издержек (например, арендной платы), которые являются расходами по управлению предприятием, а не расходами для производства данного товара – условный, и он искажает подлинный вклад продукта в доход предприятия. В связи с этим на практике используются различные способы распределения постоянных затрат, например, такие как:

- пропорционально заработной плате персонала,
- пропорционально затратам на сырье и материалы,
- пропорционально переменным издержкам и др.

В зависимости от способа распределения постоянных затрат цена единицы продукции может существенно различаться [6], но является вполне обоснованной, и то, какую цену выберет предприятие зависит от специфики продукции или же от условий заключения контракта.

Методика расчета цен на основе полных издержек является одной из самых популярных среди большинства предприятий России, так как достаточно проста и удобна. Но вместе с тем, в случае ценообразования сложной военно-технической продукции данный метод обладает существенными недостатками:

Расчет полных издержек производства возможно провести для той продукции, которая уже выпущена, то есть метод работает «по факту». Соответственно, определить цену контракта по разработке перспективных образцов ВТС возможно только при наличии российских или зарубежных аналогов и при условии наличия достоверной информации об издержках их производства. Даже в случае наличия аналогичных образцов ВТС и достоверной информации об издержках производства, метод будет давать значительную погрешность оценки контрактной стоимости перспективного образца, что обуславливается постоянным изменением экономической ситуации в стране, инфляционными процессами, различными производственными факторами и др.

Метод не учитывает специфику военно-технической продукции, такую как необходимость хорошо обученного производственного и эксплуатирующего персонала военно-технической системы, возможную большую длительность периода производства и эксплуатации ВТС, необходимость расходов на испытания образцов, поддержание системы в боевой готовности, потребность в техобслуживании и модернизации и др.

При определении цены технической продукции гражданского потребления метод не позволяет принимать во внимание спрос на продукцию и конкуренцию на рынке, поэтому возможна ситуация, когда продукция при данной цене не будет пользоваться спросом.

При отнесении на себестоимость продукции постоянных издержек, сложно оценить долю прибыли от продажи конкретной продукции в общей прибыли предприятия.

Таким образом, метод полных издержек при ценообразовании сложной военно-технической продукции возможно использовать для определения цены типовых элементов ВТС, стоящих на

вооружении или перспективных образцов имеющих аналоги, максимально приближенные к по составу и технико-экономическим характеристикам. Что касается продукции гражданского использования, то данный метод успешно может быть применен на предприятиях с четко выраженной товарной дифференциацией для расчета цен традиционных товаров, а также для установления цен на совершенно новые товары, не имеющие рыночных конкурентов.

Метод прямых затрат. Сущность метода прямых затрат [7], или метода минимальных издержек, метода стоимостного изготовления (Conversion Cost Pricing), состоит в установлении цены путем добавления к переменным затратам определенной надбавки - прибыли. При этом постоянные расходы, такие как расходы предприятия в целом, не распределяются по отдельным видам продукции, а погашаются из разницы между суммой цен реализации и переменными затратами на производство продукции, так называемой «добавленной», или «маржинальной» разницы.

При правильном подходе переменные (прямые) издержки должны явиться тем пределом, ниже которого ни один производитель не будет оценивать свою продукцию. В любом случае истинная функция издержек заключается в установлении нижнего предела для первоначальной цены на продукт, в то время как ценность этого продукта для потребителя определяет высший предел установления цены на него.

Если в случае применения метода полных затрат расчет начинается с суммирования всех затрат, связанных с производством продукции, то в случае метода прямых затрат расчет стоимости продукции начинается с оценки потенциальной стоимости объема продаж по каждой предполагаемой цене. Подсчитывается сумма прямых переменных затрат, и определяется величина наценки («маржинальной» прибыли) на единицу продукции и весь объем прогнозируемых продаж по предполагаемой цене. Вычитая из полученных суммарных наценок постоянные расходы, определяют чистую прибыль реализации продукции.

Метод прямых затрат позволяет с учетом условий сбыта находить оптимальное сочетание объемов производства, цен реализации и расходов по производству продукции. Однако он может быть с уверенностью использован при установлении цен только тогда, когда имеются неиспользованные резервы производственных мощностей и когда все постоянные расходы возмещаются в ценах, установленных из текущего объема производства. Кроме того, при оценке стоимости сложной военно-технической продукции метод прямых затрат обладает такими же недостатками, как и метод полных издержек, и соответственно может использоваться в основном для расчета цен на продукцию гражданского использования.

Метод предельных издержек. Ценообразование продукции на основе метода предельных издержек [8] базируется на анализе себестоимости аналогично методам полных издержек и прямых затрат. Отличие его от рассмотренных выше методов заключается в том, что при предельном ценообразовании надбавка делается только к предельно высокой себестоимости производства каждой последующей единицы уже освоенного товара или услуги.

Этот метод оправдан только в том случае, если гарантированная продажа по несколько более высокой цене достаточна, чтобы покрыть накладные расходы. Основной аргумент предельного ценообразования состоит в следующем: как только достигнут уровень продаж, при котором можно покрыть все расходы, включая накладные, можно снизить цену на продукцию до того уровня, пока не будут покрыты все прямые расходы на производство единицы продукции. Любая цена, превышающая эту себестоимость, дает дополнительную прибыль, особенно если более низкая цена стимулирует повышение спроса на товар или услугу. Однако для установления цен на всю продукцию или весь объем услуг этот метод использован быть не может, так как постоянные расходы должны быть возвращены предприятию в общей выручке. Более того, недостатки данного метода при оценке стоимости сложной военно-технической продукции аналогичны недостатками рассмотренных выше методов.

Метод на основе анализа безубыточности. К методам ценообразования на основе издержек производства также относится расчет цен на основе анализа безубыточности и обеспечения целевой прибыли [9]. Сущность этого метода заключается в том, что предприятие стремится установить на свою продукцию цену на таком уровне, который обеспечивал бы ей получение желаемого объема прибыли. При расчете желаемой нормы прибыли определяется точка безубыточности, то есть объем продаж, который покроет все валовые издержки производства, по следующей формуле:

$$BSV = \frac{FC}{TR}, \quad (3)$$

где BSV – точка безубыточности,

FC – постоянные затраты,

TR – маржинальная прибыль.

Если предприятие выпускает широкую номенклатуру продукции, то используют расширенный вариант формулы для расчета точки безубыточности:

$$BSV = \frac{FC}{\sum_{i=1}^n (S_i \times TR)}, \quad (4)$$

где n – количество экземпляров различной продукции, производимой на предприятии,

S_i – процент объема продаж для каждого i -го экземпляра продукции в общем объеме продаж предприятия.

Анализ методов предельных издержек и расчета точки безубыточности показывает, что данные методы не применимы для оценки стоимости элементов сложных военно-технических систем, и в основном могут быть применены в ценообразовании продукции гражданского назначения.

Метод учета рентабельности инвестиций. Сущность этого метода заключается в оценке полных затрат при различных программах производства продукции и определении объема выпуска, реализация которого по определенной цене позволит окупить соответствующие капиталовложения. Подробное описание метода произведено в литературе [10], где также представлены примеры его использования.

Данный метод единственный из всех методов ценообразования, который учитывает расходы на оплату процентов по займам, используемым в производстве и реализации продукции. Этот метод успешно подходит при принятии решений о величине объема производства новой для предприятия продукции с известной рыночной ценой, а также для традиционно производимых изделий с устоявшимися ценами. Основной недостаток метода – использование процентных ставок, которые в условиях инфляции трудно прогнозируемы во времени. Данный метод отличается от метода полных издержек только наличием дополнительной составляющей цены продукции в виде процента по кредитам и займам, а цена продукции рассчитывается по формуле:

$$P = C_{\text{пер}} + C_{\text{пост}} + \delta_{\text{проц}} + \Pi, \quad (5)$$

где $\delta_{\text{проц}}$ – сумма процентов по кредитам и займам.

Методика расчета цен продукции с использованием данного метода, как в методе полных издержек, достаточно проста, но обладает теми же недостатками, и соответственно, для оценки стоимости сложной военно-технической продукции обладает аналогичными ограничениями.

Метод надбавки к цене. Сущность данного метода заключается в расчете цены продукции путем умножения себестоимости на повышающий коэффициент [11]. При этом цена продукции рассчитывается по формуле:

$$P_s = P_p (1 + m), \quad (6)$$

где P_s – цена продажи продукции,

P_p – цена приобретения продукции (себестоимость),

m – повышающий коэффициент, %.

Повышающий коэффициент может быть рассчитан несколькими способами. Первым способом вычисляется процент наценки на основе цены приобретения продукции по следующим формулам:

$$m_p = \frac{P_s - P_p}{P_p}; \quad (7)$$

$$m_p = \frac{M}{P_s - M}, \quad (8)$$

где m_p – коэффициент добавочной стоимости по отношению к цене приобретения,

M – маржинальная прибыль.

Вторым способом вычисляется процент наценки на основе цены реализации продукции по формулам:

$$m_s(\%) = \frac{P_s - P_p}{P_p}; \quad (9)$$

$$m_s(\%) = \frac{M}{P_p + M}, \quad (10)$$

где m_s – коэффициент добавочной стоимости по отношению к цене продажи.

Процент наценки на основе цены реализации легко пересчитывается в процент наценки на основе цены приобретения продукции. Возможна и обратная операция. Их взаимосвязь выражается формулами:

$$m_s = \frac{m_p}{(100\% + m_p)}; \quad (11)$$

$$m_p = \frac{m_s}{(100\% - m_s)}. \quad (12)$$

Выражение коэффициента повышения цены от цены продажи через коэффициент повышения цены от себестоимости называется восстановлением себестоимости. И наоборот, выражение коэффициента повышения цены от себестоимости через коэффициент повышения цены от цены продажи называется восстановлением цены продажи.

В том случае, если предприятие ведет политику снижения цены на свою продукцию, то коэффициент повышения цены от продажи будет различным при его подсчете до снижения цены и после ее снижения. Первый из них называется первоначальным, или исходным коэффициентом. Последний коэффициент называется реальным, так как показывает величину прибыли, которую можно получить в итоге, то есть в результате фактической сбытовой деятельности в связи с продажей продукции по сниженной цене. Он подсчитывается по формуле:

$$R_m = \frac{RECh}{NP}, \quad (13)$$

где R_m – реальный коэффициент повышения цены,

$RECh$ – сумма фактической надбавки к цене,

NP – выручка от реализации.

Первоначальный же коэффициент повышения цены подсчитывается по следующей формуле:

$$F_m = \frac{(RECh + D)}{(NP + D)}, \quad (14)$$

где F_m – первоначальный коэффициент повышения цены,

D – сумма снижения цены.

Так как данный метод базируется на сумме издержек по производству (приобретению) продукции, то его недостатки в случае оценки стоимости сложной военно-технической продукции аналогичны рассмотренным выше недостаткам других затратных методов.

Таким образом, проведенный анализ показал, что рассмотренные затратные методы ценообразования в большей степени могут удовлетворить производителей и продавцов новой или устоявшейся на рынке продукции гражданского назначения. Применять их для оценки и анализа стоимости образцов сложной военно-технической продукции, особенно с длительным сроком производства и эксплуатации, возможно в основном для восполнения запаса штатных образцов вооружений, или же для оценки стоимости перспективных образцов, имеющих аналоги, не значительно отличающиеся по составу и технико-экономическим характеристикам.

Параметрические методы ценообразования

Под параметрическими понимаются эмпирические методы, позволяющие решать вопросы ценообразования продукции на основании статистических зависимостей, существующих между ценами и параметрами изделий [12].

Основная концепция параметрических методов основана на том, военно-технические системы с одной стороны являются сложными изделиями с точки зрения разработки, производства и эксплуатации, а с другой стороны, в подавляющем большинстве случаев, состоят из одинаковых или однотипных узлов и устройств. Отличия изделий, предназначенных для выполнения разных функций, обычно касаются исполнительных, рабочих узлов и механизмов, в то время как двигатели, несущие конструкции, узлы автоматики и управления часто являются стандартными изделиями, цена каждого из которых может быть определена отдельно. В соответствии с этим используется прием разделения оцениваемого изделия на основные составляющие с последующим определением цены всего изделия как суммы цен составляющих узлов.

Подобным способом можно рассчитать, например, стоимость корабля. Его цена определится суммированием стоимости корпуса, машинного отделения, технологического оборудования и т.д.

Стоимость каждой из перечисленных составляющих определяется путем сопоставления с предлагаемыми на рынке аналогичными изделиями или их частями (с учетом различий в параметрах). Такой прием значительно расширяет возможности использования параметрических методов ценообразования.

К группе параметрических методов ценообразования можно отнести следующие:

- метод удельных показателей,
- метод регрессионного анализа,
- агрегатный метод,
- балловый метод.

Метод удельных показателей. Данный метод [13] используется в ценообразовании групп изделий, характеризующихся наличием одного основного параметра, величина которого в значительной степени определяет общий уровень цены изделия. При использовании метода удельных показателей первоначально рассчитывается удельная цена P' по формуле:

$$P' = \frac{P_b}{N_b}, \quad (15)$$

где P_b – цена базового (аналогичного) изделия,

N_b – величина параметра базового изделия.

Затем рассчитывается цена нового изделия P по формуле:

$$P = P' \times N, \quad (16)$$

где N – значение основного параметра нового изделия в соответствующих единицах измерения.

С использованием формул (15) и (16), можно рассчитывать уровень и соотношение цен для небольших параметрических групп изделий, имеющих простую конструкцию и характеризующихся одним параметром. В этом виде метод крайне несовершенен, поэтому на практике чаще используется связь какого-либо параметра изделия с его ценой, описываемая степенной формулой Берима:

$$\frac{P_1}{P_2} = \left(\frac{N_1}{N_2} \right)^n, \quad (17)$$

где P_1 – цена изделия, которую требуется определить,

P_2 – цена однотипного по функциональному назначению изделия, которая известна,

N_1 – величина главного параметра изделия, цену которого требуется определить,

N_2 – величина аналогичного главного параметра изделия, цена которого известна,

n – коэффициент торможения, показатель, учитывающий отставание цен на изделие от увеличения его параметров.

Из (17) можно получить формулу для расчета коэффициента торможения:

$$n = \frac{\lg(P_1 / P_2)}{\lg(N_1 / N_2)}. \quad (18)$$

Значение коэффициента торможения изменяется в зависимости от типа оборудования, его тактико-технических характеристик и ряда других факторов. В практической деятельности, как правило, пользуются готовыми таблицами коэффициентов торможения, полученных эмпирическим путем, которые публикуются в различных источниках, в том числе организациями-производителями данной продукции. Величина коэффициента колеблется в широком диапазоне, в пределах 0,2 – 0,91.

Популярность использования в ценообразовании формулы (17) обусловлена, прежде всего, ее простотой при достаточно высокой надежности.

Недостаток метода заключается в том, что по формуле (17) можно определять стоимость изделий с близкими значениями основных параметров, разброс которых не превышает 30%, в противном случае погрешность расчета цен изделий значительно повышается.

Агрегатный метод ценообразования. Сущность этого метода [14] заключается в суммировании цен отдельных конструктивных частей изделий, входящих в параметрический ряд, с добавлением стоимости оригинальных узлов, затрат на сборку и нормативной прибыли.

Этот метод применяется в тех случаях, когда новая продукция состоит из разных сочетаний основных конструктивных элементов (узлов, комплектующих изделий), цены которых известны, при этом совокупная цена продукции исчисляется как сумма цен отдельных конструктивных элементов или определяется путем суммирования (вычитания) цен добавляемых или сменяемых компонентов.

Метод регрессионного анализа. Этот метод [15] применяется для определения зависимости изменения цены от изменения технико-экономических параметров продукции, относящейся к данному ряду, построения и выравнивания ценностных соотношений, а цена изделия определяется по формуле:

$$P = f(X_1, X_2, \dots, X_n), \quad (19)$$

где X_1, X_2, X_n – параметры изделия.

Этот метод позволяет моделировать изменение цен в зависимости от их параметров, строго определять аналитическую форму связи и использовать рассчитанные уравнения регрессии для определения цен изделий, входящих в параметрический ряд. Метод регрессионного анализа является более точным, более совершенным среди других параметрических методов. Увязка цен с качеством достигается с помощью экономико-параметрических приемов и вычислительной техники.

Необходимым условием применения метода является тщательная аналитическая работа по формированию параметрического ряда, определению технических и экономических параметров, на основе которых он строится. Изделия отбираются в параметрический ряд по признакам однородности технических требований и однотипности технологии их изготовления. Однородность технических требований к изделиям предполагает наличие одних и тех же основных показателей качества, хотя технические требования к отдельным изделиям различаются. Для целей ценообразования важно выявить различия в пределах параметрического ряда, которые определяют разные эксплуатационные возможности, и, следовательно, связаны с удовлетворением конкретного спроса на каждое изделие.

Построение регрессионной модели зависимости изменения цены от технических параметров включает следующие этапы:

- определение классификационных параметрических групп изделий,
- отбор параметров, в наибольшей степени влияющих на цену изделия,
- выбор и обоснование формы связи изменения цены при изменении параметров,
- построение системы нормальных уравнений и расчет коэффициентов регрессии.

На первом этапе применения метода определяются классификационные группы изделий в виде параметрических рядов. Их формирование может производиться с помощью методов автоматической классификации [15], позволяющих из общей массы продукции выделять однородные группы по какому-либо классификационному признаку.

На втором этапе производится отбор технико-экономических параметров исходя из следующих основных требований:

- в состав отобранных параметров включаются параметры, зафиксированные в стандартах и технических условиях; помимо технических параметров (мощности, грузоподъемности, скорости и т.д.) используются показатели серийности продукции, коэффициенты сложности, унификации и др.;
- совокупность отобранных параметров должна достаточно полно характеризовать конструктивные, технологические и эксплуатационные свойства изделий, входящих в ряд, и иметь достаточно тесную корреляционную связь с ценой;
- параметры не должны быть взаимозависимы.

Для отбора технико-экономических параметров, существенно влияющих на цену, вычисляется матрица коэффициентов парной корреляции. По величине коэффициентов корреляции между параметрами можно судить о тесноте их связи. При этом близкая к нулю корреляция показывает незначительное влияние параметра на цену. Окончательный отбор технико-экономических параметров производится в процессе пошагового регрессионного анализа с использованием компьютерной техники и соответствующих стандартных программ.

В практике ценообразования обычно используется следующий набор функций:

- линейная

$$P = a_0 + a_1x_1 + \dots + a_nx_n, \quad (20)$$

- линейно-степенная

$$P = a_0 + a_1x_1 + \dots + a_nx_n + a_{n+1}x_1^2 + \dots + a_{n+n}x_1^2, \quad (21)$$

- обратный логарифм

$$P = a_0 + \frac{a_1}{\ln x_1} + \dots + \frac{a_n}{\ln x_n}, \quad (22)$$

- степенная

$$P = a_0x_1^{a_1}x_2^{a_2}\dots x_n^{a_n}, \quad (23)$$

- показательная

$$P = e^{(a_1 + a_1x_1 + \dots + a_nx_n)}, \quad (24)$$

- гиперболическая

$$P = a_0 + \frac{a_1}{x_1} + \frac{a_2}{x_2} + \dots + \frac{a_n}{x_n}, \quad (25)$$

где P – выравнивание цены,

$x_1, x_2, \dots, x_n$ – значение технико-экономических параметров изделий ряда,

$a_0, a_1, \dots, a_n$ – вычисляемые коэффициенты уравнения регрессии.

В практической работе по ценообразованию в зависимости от формы связи цен и технико-экономических параметров могут использоваться другие уравнения регрессии. Вид функции связи между ценой и совокупностью технико-экономических параметров может быть задан предварительно или выбран автоматически в процессе обработки ряда на ЭВМ. Теснота корреляционной связи между ценой и совокупностью параметров оценивается по величине множественного коэффициента корреляции. Близость этого коэффициента к единице говорит о тесной связи. По уравнению регрессии получают выровненные (расчётные) значения цен изделий данного параметрического ряда. Для оценки результатов выравнивания вычисляют относительные величины отклонений расчётных значений цен от фактических:

$$\Delta P = \frac{P_{\phi} - P_p}{P} 100, \quad (26)$$

где P_{ϕ} – фактические значения цены,

P_p – расчётная цена.

Величина ΔP не должна превышать 8 – 10 %. В случае значительных отклонений расчётных значений от фактических необходимо исследовать:

- правильность формирования параметрического ряда, так как в его составе могут оказаться изделия, по своим параметрам резко отличающиеся от других изделий ряда. Их надо исключить;
- правильность отбора технико-экономических параметров. Возможна совокупность параметров, слабо коррелированная с ценой. В этом случае необходимо продолжить поиск и отбор параметров.

Порядок и методика проведения регрессионного анализа, нахождения неизвестных параметров уравнения и экономическая оценка полученных результатов осуществляются в соответствии с требованиями математической статистики.

Балловый метод. Его сущность заключается в том, что на основе экспертных оценок значимости параметров изделий для потребителей каждому параметру присваивается определённое число баллов, суммирование которых даёт своего рода интегральную оценку технико-экономического уровня изделия [16]. Умножением суммы баллов по новому виду продукции на стоимостную оценку одного балла определяется общая ориентировочная оценка нового изделия. Цена на новое изделие рассчитывается по следующей формуле:

$$P_i = \sum_{i=1}^N (B_{ii} \alpha_i) P_{\phi\bar{a}}, \quad i = 1, 2, \dots, N, \quad (27)$$

где N – количество оцениваемых параметров,

P_i – расчётная цена нового изделия,

B_{ii} – балльная цена i -го параметра нового изделия,

α_i – удельный вес i -го параметра нового изделия,

$P_{\phi\bar{a}}$ – средняя оценка одного балла (стоимостной показатель).

Средняя оценка балла определяется по формуле:

$$P_{\phi\bar{a}} = \frac{P_{\bar{a}}}{\sum_{i=1}^N B_{\bar{a}i} \alpha_i}, \quad (28)$$

где $P_{\bar{a}}$ – цена базового изделия-эталона,

$B_{\bar{a}i}$ – балльная цена i -го параметра базового изделия-эталона.

С учетом формулы (28), получим выражение для расчета цены нового изделия:

$$P_i = P_{\bar{a}} \frac{\sum_{i=1}^N B_{ii} \alpha_i}{\sum_{i=1}^N B_{\bar{a}i} \alpha_i}. \quad (29)$$

Балловый метод успешно может применяться в ценообразовании сложных военно-технических систем для сравнительной оценки военно-технической продукции, в условиях ограниченной или полностью отсутствующей конъюнктуры рынка. Его реализация сводится к выравниванию цен на изделия с различным уровнем одних и тех же основных параметров в зависимости от суммы

присвоенных баллов. При этом необходимо иметь в виду, что увеличение или уменьшение затрат на создание продукции, при изменении технико-экономических и других характеристик изделий, не связано прямой пропорциональной зависимостью с балловыми оценками продукции. При балловом методе каждое изделие параметрического ряда сопоставляется с изделием – эталоном по показателям, зафиксированным в действующих стандартах, технических условиях, тактико-технических заданиях, и имеющих наиболее важное значение для заказчика военно-технической продукции.

Количество показателей, оцениваемых баллами, должно быть ограниченным и в то же время достаточно полно характеризовать потребительские свойства изделий. Ограничение числа оцениваемых показателей связано с тем, что при большом количестве показателей относительно меньший удельный вес занимает каждый из них и в результате снижается значимость каждого конкретного показателя.

По каждому конкретному техническому показателю устанавливаются его допустимые пределы. Они могут быть заданы различными методами: по данным стандартов и технических условий, по лучшим и худшим образцам, по оценке реально достижимого в ближайшей перспективе и по минимально обязательному в настоящее время. Соотношение пределов определяется для конкретных параметрических групп изделий. Если все показатели продукции, подвергающиеся балльной оценке, считаются равнозначными по удельному весу, то комплексный уровень качества каждого изделия ряда определяется путем простого сложения баллов, а цена – последующим умножением стоимости одного балла на сумму баллов. Если отобранные для оценки параметры не равнозначны для потребителя, то следует установить коэффициент весомости отдельных параметров. Оценки выставляются по каждому показателю качества, затем выводится среднеарифметическое значение по каждому показателю, который умножается на соответствующий коэффициент весомости. Полученные баллы суммируются. Средняя оценка балла исчисляется как частное от деления цены базового изделия-эталона на сумму его баллов.

Разновидностью баллового метода является метод на основе расчета цены безразличия, который также учитывает значимость технико-экономических параметров изделий [16] в определении их цены. Этот метод широко применяется в западных странах для определения цены продукции при условии существования изделий-конкурентов. Сущность этого метода заключается в расчете цены изделия исходя из цен изделий-конкурентов и цены эталонного изделия по следующей формуле:

$$P = P_k \left(1 + \frac{1 - E}{E} \right), \quad (30)$$

где P – цена изделия,

P_k – цена изделия-конкурента,

E – приведенный параметрический индекс.

Приведенный параметрический индекс рассчитывается по формуле:

$$E = \frac{E_k}{E_0}, \quad (31)$$

где E_k – сводный параметрический индекс изделия-конкурента,

E_0 – сводный параметрический индекс оцениваемого изделия.

Сводный параметрический индекс изделия-конкурента определяется как:

$$E_k = \frac{\sum_{j=1}^n B_j I_{jk}}{\sum_{j=1}^n B_j}, \quad (32)$$

а сводный параметрический индекс оцениваемого изделия по следующей формуле:

$$E_0 = \frac{\sum_{j=1}^n B_j I_{j0}}{\sum_{j=1}^n B_j}, \quad (33)$$

где B_j – весовые коэффициенты (значимость параметра);

I_{jk} – индивидуальный индекс j -го параметра изделия-конкурента, рассчитанный путем соотношения j -го параметра изделия-конкурента с j -м параметром эталонного изделия, условно принятого за идеальное;

I_{j0} – индивидуальный индекс j -го параметра оцениваемого изделия, рассчитанный путем соотношения j -го параметра оцениваемого изделия с j -м параметром изделия-образца;

j – вид параметра изделия;

n – количество параметров изделия, учитываемых при формировании цены.

Таким образом, рассмотренные параметрические методы ценообразования позволяют производить оценку стоимости элементов сложных военно-технических систем, могут успешно применяться и применяются в ценообразовании изделий военно-промышленного комплекса, поскольку учитывают не только затратную составляющую производства продукции, но и ценность параметров или характеристик изделий, важных для заказчика. С другой стороны, совокупность этих методов обладает рядом общих недостатков. Как правило, для оценки стоимости нового изделия требуется полная и достоверная информация о стоимости изделий-аналогов или изделий-конкурентов. При создании перспективных военно-технических систем, аналоги которых отсутствуют в природе, а потенциально достижимые тактико-технические характеристики на этапе проектирования системы могут быть не известны, данные методы применять затруднительно. Также затруднительно параметрические методы применять для оценки стоимости научно-исследовательских и опытно-конструкторских работ, которые являются неизменной частью процесса разработки элементов ВТС. Данные методы, как правило, громоздки, и требуют сложных расчетов с применением ЭВМ.

Заключение

Все рассмотренные в статье методы – затратные, параметрические, рыночные в настоящее время достаточно широко применяются на предприятиях промышленности в основном для оценки стоимости продукции гражданского назначения, с четко выраженной рыночной дифференциацией, имеющей короткий временной период производства и реализации. Что же касается ценообразования сложных военно-технических систем, то, как было сказано выше, такие системы обладают определенной спецификой, в силу которой применять в явном виде какой-либо из перечисленных методов возможно для отдельных узлов, агрегатов или изделий, составляющих ВТС. Для оценивания полной стоимости военно-технической системы должны быть разработаны комбинированные методы или применяться комплекс методов ценообразования. Военно-техническая система должна быть логически разделена на составные узлы или комплексы, и для каждого составного узла необходимо выбирать метод ценообразования, который позволит рассчитать его стоимость с минимальной погрешностью. Такой подход к ценообразованию ВТС в наибольшей степени позволит удовлетворить производителей и заказчиков оборонной продукции.

СПИСОК ЛИТЕРАТУРЫ

1. Голубков Е.П. Маркетинговые исследования: теория, методология и практика. – М.: Финпресс, 2000.
2. Котлер Ф. Маркетинг. Менеджмент. – СПб.: Питер Ком, 1999.
3. Липсиц И.В. Коммерческое ценообразование. – М.: БЕК, 2000.
4. Михайлова Е.А. Ценовые стратегии: современные мировые тенденции // Маркетинг в России и за рубежом, 1999, №5.
5. Ноздрева Р.Б. Основные методы ценообразования японских фирм // Маркетинг, 1995, № 1, – С. 64–73.
6. Ноздрева Р.Б. Основные методы ценообразования японских фирм // Маркетинг, 1995, № 2, – С. 40–57.
7. Попов Е.В. Теория маркетинга. – Екатеринбург: ИПК УГТУ, 2000.
8. Порошина Н. Новые аспекты ценообразования // Маркетинг, 1996, №6, – С. 50–55.
9. Родионова А.Н., Руднева Ю.Р., Пашин С.Т. Методы расчета цены на новый товар // Маркетинг в России и за рубежом, 2001, №2. С. 34–45.
10. Рыбас А.Л. Стратегический анализ мирового рынка вооружений и обеспечение национальной безопасности России. – М.: Русский биографический ин-т, 1999. 192 с.
11. Слепов В.А. Попов Б.В. Вопросы комплексного подхода к ценообразованию в новых экономических условиях. – М.: Система, 1994.
12. Солошенко М.В. Контрактно-ценовая политика в маркетинге: <http://www.marketing.spb.ru/read/kurs1/index.htm>.
13. Стоянова Е.С. Финансы маркетинга. – М.: Перспектива, 1994.
14. Цацулин А.Н. Ценообразование в маркетинге. – М.: Филин, 1997.
15. Ценообразование. – М.: Дека, 1994.
16. Цены и ценообразование / Под ред. В.Е. Есипова. – СПб.: Питер, 2000.

Воропаев Д.Б.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АНАЛИЗ СОВРЕМЕННЫХ ПРОБЛЕМ ЦЕНООБРАЗОВАНИЯ НА ЭЛЕМЕНТЫ
СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ СИЛОВЫХ СТРУКТУР**

Совершенствование системы информационной безопасности государства в настоящее время неразрывно связано с разработками и закупками отвечающих современным требованиям технических комплексов и средств, обеспечивающих выполнение мероприятий по защите специальной информации. Как правило, подобные технические комплексы уровня силовых структур являются сложными военно-техническими системами (ВТС), разработка (совершенствование) которых на

современном этапе экономического развития нашей страны связано с разрешением ряда проблем экономического характера. Одной из ключевых проблем является несовершенство методологии определения цен на подобную научно-техническую продукцию, заключающееся, с одной стороны, в трудности получения оценок стоимостей перспективных образцов ВТС, и с другой стороны, в большом расхождении прогнозных и реальных цен на перспективные образцы ВТС.

Анализ фундаментальных трудов в этой области, результаты которого представлены в ряде статей [1-5] показал, что в настоящее время разработано множество методов и методик ценообразования на военно-техническую продукцию, ориентированных на различные виды вооружений и обусловленных различными периодами социально-экономической эпохи государства. Например, во времена плановой экономики оценка стоимости подобной продукции основывалась главным образом на калькуляционном методе. При этом цены на типовые комплектующие и расходные материалы устанавливались централизованно и действовали на всей территории страны (в отдельных случаях применялись так называемые поясные надбавки), норма-часы на выполнение научно-исследовательских работ и изготовление комплектующих рассчитывались по утвержденным методикам, также в основном калькуляционным. Но даже тогда для проведения оценок необходимо было располагать большим количеством данных, начиная от стоимости сырья и материалов, используемых для разработки и производства образцов ВТС, и заканчивая затратами на изготовление и ремонт спецоснастки. Поэтому использовать калькуляционный метод на стадии программного планирования, при прогнозировании затрат, когда порой неизвестен даже облик изделия, который предполагается разрабатывать, практически не было возможности.

Для оценки стоимости научно-технической продукции применялись также межведомственные методики прогнозирования, базировавшиеся как на регрессионных зависимостях, так и на точечных оценках стоимости. Поскольку основной переменной здесь является временной параметр, важнейшим условием их использования была постоянная периодичность разработки образцов нового поколения. Из-за изменившейся финансово-экономической ситуации в России этот показатель в настоящее время не может быть взят за основу – слишком большими окажутся погрешности в расчетах. Математические же модели, которые применяются в такого же типа методиках, и в которых в качестве переменной выступают выходные значения параметров продукции, то есть тактико-технические характеристики (ТТХ), не могут быть использованы для оценки стоимости НИОКР по созданию образцов ВТС, не имеющих аналогов. Практическая ценность способа точечных оценок существенно снизилась вследствие того, что стоимости разработки отдельных подсистем перспективных образцов соответствовали уровню научно-технического прогресса 80-90-х годов, а это не отвечает современным требованиям.

За прошедшее десятилетие стоимость образцов научно-технической продукции резко возросла, изменилась и структура цены, что сделало проблематичным использование прежних устаревших методик. С переходом к рынку существовавшая ранее нормативная база утратила свое значение также из-за того, что процесс установления цен на закупаемые исполнителями НИОКР сырье и материалы практически вышел из-под контроля федеральных органов. Зарплата рабочих и служащих даже на одном предприятии резко дифференцирована, а на разных предприятиях напрямую зависит от имеющегося портфеля заказов, так что методический подход к ценообразованию образцов ВТС, базировавшийся на стабильных нормативах, потерял всякий смысл.

Устаревшее методическое обеспечение существенно осложнило работу военных представительств заказывающих органов Министерства обороны на предприятиях промышленности, задача которых, при неизменной много лет системе ценообразования состояла в аккуратном использовании всей нормативной и методической базы для объективной проверки рассчитанных плановыми органами предприятий стоимостей всех этапов НИОКР. В настоящее время заказывающие органы, не имея методического аппарата, адаптированного к современным условиям, зачастую руководствуются теми оценками, которые предлагают организации-разработчики, экспертными оценками или соображениями простого обеспечения выживания предприятий.

Проблема усугубилась тем, что условия формирования цен на научно-техническую продукцию военного и гражданского назначения по сути стали резко отличаться друг от друга – цена первой не может быть определена «на рынке» (на основе баланса спроса и предложения), по крайней мере на внутреннем, когда продавец и покупатель – явление массовое, и в ходе ежедневных торгов она устанавливается более-менее объективно. Поставщики военной научно-технической продукции вследствие все еще монополизированной системы создания вооружений и военной техники (ВВТ) и режимных ограничений малочисленны. Военные ведомства, чтобы сохранить ядро оборонно-промышленного комплекса, вынуждены сосредотачивать заказы на ограниченном количестве предприятий, что еще более сужает круг исполнителей НИОКР. Создавшееся положение способствует установлению диктата цен со стороны производителей научно-технической продукции, что, по мере выхода страны из кризиса и увеличения размера финансовых ресурсов, выделяемых на научно-исследовательские и опытно-конструкторские работы, должно быть исключено.

В последние годы принят ряд нормативно-правовых актов, предусматривающих размещение госзаказа на контрактной основе (особенно это касается военной научно-технической продукции),

преимущественно путем организации торгов (конкурсов). Выбор единственного поставщика допускается лишь в исключительных обстоятельствах, оговоренных этими актами. Но даже при проведении торгов и наличии нескольких потенциальных исполнителей оборонного заказа, заказчику все равно необходимо знать ожидаемый начальный уровень цены, ибо значительное его превышение приведет к неоправданному расходованию финансовых ресурсов, а значительное занижение – к нереализуемости заказа. Если у заказчика нет соответствующего методического аппарата, он не сможет проверить истинность цены, которую запросит исполнитель.

Совершенствованию методического аппарата в области ценообразования на образцы ВТС в настоящее время уделяется недостаточное внимание. В федеральных ведомствах разрабатываются методики, позволяющие прогнозировать и рассчитывать технико-экономические показатели образцов ВТС, но их качество не всегда отвечает современным потребностям практики, не редко в них отсутствуют координация и согласование (или хотя бы ознакомление) с организациями, представляющими интересы государственных заказчиков [1]. За последние годы в Министерстве обороны утверждены и используются на межвидовом уровне ряд практических методик по расчету цен на перспективные образцы вооружений и военной техники, например [6]. В этих методиках достаточно полно раскрыта проблематика ценообразования и расчет важнейших технико-экономических показателей НИОКР, но представленный в них методический аппарат в основном опирается на устаревший калькуляционный метод и на метод индексирования фактических цен. Выше показано, что калькуляционный метод не применим для оценки стоимости перспективных образцов ВТС, не имеющих аналогов. Что же касается метода индексирования фактических цен, то в [4] показано, что настоящее время этот метод широко применяется на практике, однако точность прогнозов оставляет желать лучшего. Во-первых, вследствие отсутствия информационной базы для определения цен закупок в текущем периоде. Хотя существующая нормативно-законодательная база предусматривает необходимость ведения реестров государственных и муниципальных контрактов, форма таких реестров утверждена Правительством РФ совсем недавно, тогда как до последнего времени статистика о ценах единицы продукции, закупаемой по государственному и муниципальному заказу, отсутствовала. Но и ведение реестров контрактов не гарантирует точности прогноза цен в плановом периоде, поскольку законодательство не обязывает заказчиков использовать данные этих реестров для обоснования стоимости заказа в плановом периоде. Во-вторых, фактором, определяющим качество прогнозов, получаемых путем индексации, является точность применяемых индексов инфляции. Однако применяемые на практике индексы этому требованию не отвечают, поскольку носят усредненный характер. Таким образом, решение задачи повышения точности прогнозирования цен перспективных образцов ВТС зависит от накопления достаточной информационной базы о текущих ценах его размещения и дифференциации применяемых дефляторов с учетом отраслевых и территориальных колебаний темпов роста цен. При рассмотрении вопроса о методах прогнозирования цен на военную продукцию также следует учитывать, что применение метода индексации невозможно по отношению к видам продукции, не имеющим аналогов в текущем периоде. Это относится, главным образом, к опытно-конструкторским разработкам и к закупке новых видов вооружения и военной техники, прогнозирование цен на которые невозможно без анализа затрат на исполнение каждого конкретного контракта.

Таким образом, существующие методики расчета стоимости выполнения отдельных операций и цен на комплектующие и расходные материалы, а также методики определения цены военной научно-технической продукции не позволяют удовлетворить в полной мере потребности заказывающих организаций.

Все вышесказанное обуславливает актуальность разработки методов и практических методик, позволяющих решить проблемные вопросы ценообразования на образцы ВТС. В основе этих методов должны лежать следующие принципы:

- системности, заключающийся в том, что процесс ценообразования рассматривается в неразрывной связи с общей экономической ситуацией в стране и учитывает основные факторы, влияющие на стоимость НИОКР,
- многовариантности, обеспечивающий возможность получения достоверных оценок при различном объеме исходных данных,
- иерархичности, при котором стоимости НИОКР представляется в виде совокупности стоимостей отдельных этапов работ, каждая из которых в свою очередь подразделяется на основные компоненты (прибыль, фонд заработной платы, накладные расходы, и др.),
- декомпозиции, предполагающий представление перспективного образца в виде множества основных подсистем, каждой из которых соответствует некоторый аналог.

В результате заказывающие организации должны быть обеспечены простым в использовании методическим аппаратом, который, опираясь на принципы многовариантности и упорядоченности по отношению к объему имеющихся исходных данных и уровню проработки перспективного образца ВТС, будет включать в себя совокупность способов оценки стоимости НИОКР в целом, или составляющих ее этапов, и в котором предусмотрена возможность оценки изменения стоимости работ при варьировании показателей финансово-хозяйственной деятельности организаций-

исполнителей (уровня прибыли, объемов прямых и накладных расходов, фонда оплаты труда и т.д.). Это позволит более точно учесть условия создания научно-технической продукции в различных организациях и выбрать ту из них, где ожидаемые затраты минимальны. Кроме того, при особой сложности заказа появляется возможность оценить степень увеличения стоимости работ, если повышется норма рентабельности.

В процессе совершенствования методологического аппарата ценообразования необходимо обеспечить максимальную результативность разрабатываемых методов и методик. Для этого целесообразно определить ряд следующих универсальных требований к разрабатываемым методам [2], независимых от прикладной области и не ориентированных на интересы конкретного федерального ведомства или государственного заказчика.

1. При прогнозировании контрактной цены должны учитываться лимитная и минимально допустимая цены. В рыночных условиях процесс формирования цены осуществляется непосредственно в ходе проведения конкурса или торговых переговоров между заказчиком и потенциальными исполнителями. При этом вторые стремятся (при прочих равных условиях) увеличить контрактную цену, а заказчик — ее уменьшить. Ясно, что увеличение цены рано или поздно поставит под сомнение целесообразность (возможность) создания рассматриваемого образца ВТС, так как либо найдется другой, позволяющий решить аналогичные задачи с меньшими затратами, либо у заказчика просто не окажется необходимых финансовых ресурсов. Поэтому определение верхнего, максимально допустимого размера цены (лимитной цены) является одной из важных задач в ценообразовании. Лимитная цена отражает такой ее уровень, превышение которого делает нецелесообразным с экономической точки зрения проведение НИОКР. В рамках реализации системного подхода для определения лимитной цены необходимо разработать специальное нормативно-методическое обеспечение, позволяющее связать контрактные цены на НИОКР и закупки ВТС с полными затратами заказчика на все стадии жизненного цикла и эффективностью применения образцов ВТС. Использование лимитной цены ставит заслон и на пути нерационального расходования финансовых ресурсов. С другой стороны, очевидно, что даже в условиях конкуренции цена на научно-техническую продукцию не может беспрестанно уменьшаться. Объективно существует некоторый порог, характеризующий минимальные финансовые ресурсы, которые необходимо затратить исполнителю на создание (поддержание) требуемой для выполнения заказа научно-технической и производственно-технологической базы. Поэтому наряду с лимитной ценой не менее важной задачей является определение минимально допустимой цены, обеспечивающей реализацию исполнителем заказа. Так как в общем случае может оказаться несколько потенциальных исполнителей заказа, у которых уровни развития научно-технической и производственно-технологической базы отличаются, то и различны цены создаваемой ими продукции.

Практическую важность разработки методического аппарата для определения минимально допустимой и лимитной цен можно проиллюстрировать на примере рассмотрения процесса создания образца ВТС, который начинается с проведения научно-исследовательских работ. Эти работы завершаются изготовлением опытного образца ВТС и комплексом испытаний, подтверждающих (или не подтверждающих) возможность и целесообразность реализации требований заказчика по значениям тактико-технических характеристик. Гипотетически может быть разработан образец ВТС, фактически достигнутые характеристики которого отличаются от определенных в тактико-техническом задании. По результатам проведения государственных испытаний принимается окончательное решение о целесообразности закупок образцов ВТС и их объемах, то есть решение о переходе к следующей стадии жизненного цикла — производству.

Принятие того или иного решения невозможно без оценки минимально допустимой и лимитной цен на серийные закупки образцов ВТС. Когда минимально допустимая цена выше лимитной, осуществление серийных закупок образцов ВТС нецелесообразно, даже если их разработка уже завершена.

2. При прогнозировании контрактной цены должны учитываться интересы заказчика и исполнителя, а также параметры «внешней среды», в которой осуществляется ее формирование. Как уже отмечалось, интересы заказчика и исполнителя при формировании контрактной цены могут не совпадать. В связи с этим контрактная цена на образцы ВТС военной направленности является своего рода компромиссом между покупателем и зачастую единственно возможным исполнителем заказа в отличие от равновесной цены в гражданском секторе экономики, где имеется, как правило, множество потребителей и несколько (отечественных и зарубежных) производителей продукции. Значение такой компромиссной цены может находиться только в некоторой допустимой области, границами которой выступают лимитная и минимально допустимая цены. Поэтому если область допустимых значений (ОДЗ) контрактной цены представляет собой непустое множество, то имеет смысл говорить о возможности ее соответствия интересам и заказчика, и исполнителя. Проблема же обоснования особенно актуальна в том случае, когда эта ОДЗ представляет собой интервал значительной протяженности.

С точки зрения учета интересов заказчика и потенциального исполнителя граничные точки интервала допустимых значений (при условии, что он не пуст) представляют собой крайние случаи:

левая граница (минимально допустимая цена) учитывает в максимальной степени интересы заказчика и в минимальной – исполнителя, а правая (лимитная цена) – наоборот. Все остальные варианты являются промежуточными и по своей сути могут рассматриваться как компромиссные.

Таким образом, методический аппарат оценки ожидаемого значения контрактной цены должен отражать реально складывающуюся готовность каждой из договаривающихся сторон идти на уступки.

Основными параметрами «внешней среды», существенно влияющими на размер цены, являются экономические нормативы и, при условии присутствия на рынке разных потенциальных исполнителей заказа, конкуренция, способствующая сдерживанию роста цен на создание научно-технической продукции и приближающая контрактную цену к левой границе ОДЗ. И это приближение может оказаться тем значительнее, чем привлекательней является заказ для организаций-исполнителей. Отсутствие же конкурентной среды, наоборот, способствует росту цены продукции и приближению ожидаемой контрактной цены к правой границе ОДЗ. Ввиду этого следует отметить, что одним из направлений совершенствования методологического аппарата в области ценообразования сложных ВТС, является анализ конкурентной среды и определение степени привлекательности заказа для исполнителя.

3. Разрабатываемый методический аппарат при определении контрактной цены должен учитывать экономическую целесообразность создания образцов ВТС. Ограничиться лишь оценкой потребных финансовых ресурсов на создание ВТС можно только тогда, когда объем имеющихся в распоряжении заказчика денежных средств превышает потребности. В этом случае могут реализовываться самые амбициозные планы, что, например, имело место во времена существования СССР и было связано с гонкой вооружений. А мизерные объемы финансовых ресурсов, которые в последние годы выделялись (и, по-видимому, в ближайшее время будут выделяться) на развитие ВТС, требуют максимальной экономии денежных средств. Однако такая экономия не должна быть беспредельной, так как это может привести к невыполнению заказа. Финансирование создания ВТС должно быть оправдано и с военно-экономической точки зрения, для чего необходимо учитывать затраты на всем жизненном цикле конкретного образца.

Следовательно, при формировании прогнозной оценки ожидаемой контрактной цены в процессе ведения торговых переговоров (конкурсов) и заключения контрактов на НИОКР и серийные закупки систем вооружений, необходимо руководствоваться следующими положениями:

- контрактная цена должна быть достаточна, по крайней мере, для покрытия всех экономически оправданных издержек исполнителя, т.е. обеспечивала бы реализуемость заказа,
- контрактная цена должна как можно ближе находиться к левой границе ОДЗ (минимально допустимой цене), обеспечивая максимальную рациональность расходования финансовых ресурсов.

Но заданные тактико-технические характеристики в общем случае могут быть такими, что минимально допустимая цена при указанном их уровне будет выше лимитной цены. В этом случае ОДЗ контрактной цены – пустое множество. Тогда возникает задача определения таких параметров, которые позволят лимитной цене превысить уровень минимально допустимой цены, т.е. обеспечить военно-экономическую целесообразность создания образцов ВТС. Для ее решения должно быть разработано соответствующее методическое обеспечение, составной частью которого является методика формирования контрактной цены.

Особое внимание при определении контрактной цены следует уделить степени ее жесткости. Решение данного вопроса в большей степени лежит в области создания и совершенствования нормативно-законодательной базы заключения договоров (контрактов) и ведения торгов. Проблема здесь заключается в том, что в условиях инфляции и труднопрогнозируемого роста цен на сырье и комплектующие, с увеличением срока контракта риски исполнителя возрастают. При отсутствии легальной возможности корректировки цены долгосрочных контрактов по объективным основаниям эти повышенные риски будут закладываться исполнителями в цену контракта и оплачиваться бюджетом в любом случае – независимо от того, реализовались ли они в действительности или нет. Это приведет к удорожанию долгосрочных контрактов, размещаемых на торгах. Что касается долгосрочных контрактов, размещаемых у единственного исполнителя, то в условиях прямого ценового регулирования и фиксированной цены – при существенном увеличении «входящих» затрат их исполнение может оказаться под угрозой.

4. При прогнозировании ожидаемой контрактной цены необходимо учитывать потребные объемы финансирования всех стадий жизненного цикла образца ВТС в неразрывной связи со временем. В процессе военно-экономических исследований возможна ситуация, когда создание образца ВТС может оказаться нецелесообразным, если поставленные перед ним цели могут достигаться существующими средствами или их модификациями с меньшими затратами. В таком случае время начала разработки перспективного образца целесообразно отодвигать на более поздний срок с пересмотром требований к его тактико-техническим характеристикам при условии, что лимитная цена будет превышать минимально допустимую.

Влияние фактора времени обуславливает необходимость учета совокупных затрат заказчика на всем жизненном цикле образца ВТС, так называемых полных затрат. При определении полных затрат необходимо знать количество образцов ВТС, требуемых для достижения заданного эффекта от их

применения, а также стоимостные и временные показатели, характеризующие расходы организации-заказчика на всех стадиях жизненного цикла каждого образца (полные предстоящие затраты по всей совокупности планируемых к закупке образцов зависят от времени начала разработки перспективного средства, так как эффект от применения единичных образцов ВТС может меняться во времени. Это связано с совершенствованием средств воздействия (противодействия) вероятного противника, социально-экономической обстановкой внутри страны, военно-политической и экономической ситуацией в мире).

5. При разработке методического аппарата в области ценообразования должны использоваться стоимостные показатели, приведенные к условиям бездефицитного нормативного финансирования. Разработка нового методического аппарата, как правило, базируется на анализе реальных данных о затратах по завершённым НИОКР и закупаемым (ранее приобретенным) образцам ВТС. Статистические данные о фактических затратах можно разделить на совокупности, соответствующие макроэкономическим и социально-экономическим условиям создания ВТС (таблица 1) и их сочетанию, то есть вся имеющаяся в настоящее время статистика о стоимостных показателях отвечает различным условиям, в силу чего использованию существующего статистического материала в интересах разработки новых методик должна предшествовать его предварительная корректировка, направленная на приведение их к условиям бездефицитного нормативного финансирования. Только после этого они могут быть использованы для получения обоснованных прогнозных оценок и совершенствования методического аппарата. При необходимости можно перейти к любым другим условиям финансирования, используя соответствующую экономико-математическую модель.

Таблица 1

Условия создания ВТС

Макроэкономические	Социально-экономические
Финансирование огромного количества НИОКР и осуществление масштабных закупок образцов ВТС (до 1991 года)	Организации промышленности практически не испытывали недостатка в ресурсах, и действовала централизованная система назначения цен на продукцию как военного, так и гражданского назначения
Глубокий экономический кризис после распада СССР и постепенное его преодоление	Непрерывное проведение реформ, направленных на изменение экономических отношений; преобразование организационно-правовых форм и форм собственности оборонных предприятий. Это привело в ряде случаев к увеличению сроков выполнения НИОКР и удорожанию научно-технической и серийной продукции военного назначения

Таким образом, представленный в настоящей статье анализ проблемных вопросов ценообразования на продукцию военного назначения позволил определить пути решения назревших проблем – дальнейшее совершенствование методологии ценообразования, заключающееся в разработке методов и методик расчета контрактных цен, совершенствование законодательной базы договорных (контрактных) отношений. А лежащие в основе разрабатываемых методов ценообразования принципы, и комплексное выполнение требований к разрабатываемым методам позволят обеспечить адекватность оценок договорных (контрактных) цен, что в конечном итоге обусловит реализуемость перспективных НИОКР, и удовлетворит в полной мере потребности заказывающих организаций и организаций – исполнителей.

СПИСОК ЛИТЕРАТУРЫ

1. Буренок В.М., Лавринов Г.А., Подольский А.Г. Оценка стоимости военной научно-технической продукции // Военная мысль, 2007, №12. С. 25–29.
2. Лавринов Г.А., Подольский А.Г. Нормативно-методическое обеспечение ценообразования на продукцию военного назначения // Военная мысль, 2004, №12. С. 58–65.
3. Золотарева А.Б. Проблемы размещения государственного оборонного заказа // Финансы, 2007, №8. С. 20–24.
4. Золотарева А.Б. Проблемы ценообразования на продукцию военного назначения // Экономическая политика, 2008, №4. С. 178–188.
5. Сорокин В.А. Развитие методологии ценообразования как ключевая задача в повышении оснащенности Вооруженных Сил РФ вооружением, военной и специальной техникой // Вооружение и экономика, 2008, №2. С. 19–32.
6. Приказ Федеральной службы по тарифам от 18 апреля 2008 г. №118. //Методические рекомендации по расчету цен на вооружение и военную технику, которые не имеют российских аналогов и производство которых осуществляется единственным производителем.

Дудкина О.К., Копыльцов А.В.

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

СОЗДАНИЕ ГОРОДСКОГО МОНИТОРИНГОВОГО ЦЕНТРА ЭКСТРЕМАЛЬНЫХ СИТУАЦИЙ

Постановление Правительства Российской Федерации «Об утверждении перечня экстренных оперативных служб, вызов которых круглосуточно и бесплатно обязан обеспечить оператор связи пользователю услугами связи, и о назначении единого номера «112» в качестве единого номера вызова экстренных оперативных служб. Правительством Санкт-Петербурга с января 2007 года проводятся

работы по созданию Городского мониторингового центра Санкт-Петербурга (ГМЦ), Он представляет собой государственное учреждение, осуществляющее учет, анализ и обработку сообщений об экстренных событиях и нештатных ситуациях, возникающих в черте города. А также отслеживание оперативной обстановки на городских объектах и в местах проведения массовых мероприятий, формирование доступных механизмов для оперативной передачи информации от населения Санкт-Петербурга по экстренным ситуациям в компетентные учреждения и ведомства, а также обеспечивающего координацию действий оперативных и диспетчерских служб города в рамках обработки данных по экстренным ситуациям [1].

С этой целью, на базе ГМЦ Санкт-Петербурга, выполнены следующие мероприятия:

- разработана и согласована всеми заинтересованными ведомствами, схема автоматизированного приема, учета и обработки экстренных вызовов на территории Санкт-Петербурга единой городской службой;
- создана единая коммуникационная структура города, позволяющая решать вопросы, связанные с приемом экстренных вызовов, их обработки и реагирования;
- разработан и внедрен в опытную эксплуатацию программно-технологический комплекс Центра обработки экстренных вызовов и обращений граждан на двух территориально-распределенных, взаимно резервирующих площадках, позволяющих одновременно осуществлять прием 60 операторам;
- разработаны и утверждены регламенты информационного взаимодействия ГМЦ Санкт-Петербурга с ведомственными дежурно-диспетчерскими службами;
- на основе утвержденных административных регламентов разработана и принята в опытную эксплуатацию система информационного взаимодействия ГМЦ Санкт-Петербурга и дежурной части ГУВД по Санкт-Петербургу и Ленинградской области, обеспечивающая прием, регистрацию и дальнейшую обработку поступающих экстренных вызовов и электронных сообщений;
- на основе утвержденных административных регламентов начата опытная эксплуатация системы информационного взаимодействия ГМЦ Санкт-Петербурга и ГУ «Центр управления силами ФПС по Санкт-Петербургу»;
- обеспечена интеграция автоматизированной информационной системы ГМЦ Санкт-Петербурга с городской системой видеонаблюдения и системой мониторинга стационарных и мобильных городских объектов, что позволило обеспечить комплексный подход к мониторингу оперативной обстановки в городской черте;
- осуществлена необходимая штатная реорганизация учреждения, произведен дополнительный набор и обучение операторов дежурных смен, выполнена полная модернизация аппаратно-программного комплекса и материально-технической базы ГМЦ.

Городской мониторинговый центр Санкт-Петербурга является основным структурным элементом системы обеспечения безопасности жизнедеятельности Санкт-Петербурга. ГМЦ обеспечивает эксплуатацию основных подсистем АИС ОБЖ, в том числе:

1. Локальный узел систем мониторинга подвижных и стационарных объектов – интегрирующий узел различных мониторинговых систем, отслеживающих состояние объектов городской инфраструктуры, в т.ч. охранные и пожарные сигнализации, системы экстренного вызова милиции.
2. Главный центр видеонаблюдения.
3. Мониторинг оперативной обстановки – интегрирующий узел дежурных служб 01, 02, 03, 004, формирующий ленту происшествий, зарегистрированных данными службами, а также процесс отработки каждого происшествия.
4. Автоматизированная информационная система ГМЦ – Call-центр позволяющий осуществлять прием экстренных обращений граждан, обработку их, интеграцию с АИС ведомств при передаче данных, обращений по системе электронной связи [3].

В настоящее время завершаются работы по интеграции нового программно-технологического комплекса ГМЦ с информационными системами организаций жилищно-коммунального хозяйства и предприятий инженерно-энергетического комплекса города, а также по обеспечению интеграции с городской геоинформационной системой. Помимо этого прорабатываются вопросы взаимодействия ГМЦ Санкт-Петербурга с городской станцией скорой медицинской помощи.

В настоящий момент прием экстренных вызовов в ГМЦ осуществляется по телефонному номеру «004». Операторами обрабатываются следующие виды вызовов (всего в среднем 42000 в месяц, в период начала отопительного сезона более 80000):

- обращения жителей по вопросам, относящимся к сфере ЖКХ и инженерно-энергетического комплекса;
- сообщения о дорожно-транспортных происшествиях;
- сообщения об угоне автотранспорта;
- предоставление справки об эвакуированном автотранспорте;
- сигналы противопожарных сигнализаций, установленных на стационарных городских объектах;

- сигналы охранных сигнализаций, установленных на стационарных городских объектах;
- любые экстренные вызовы, поступающие от иностранных граждан [2].

В марте 2008 года рабочая группа Департамента оперативного управления МЧС России посетила ГМЦ и подтвердила возможность создания на его базе Службы «112» Санкт-Петербурга.

Согласно Минкомсвязи РФ развертывание Единой дежурно-диспетчерской службы «112» в Санкт-Петербурге на базе Городского мониторингового центра не противоречит положениям проекта «Концепция создания системы обеспечения вызова экстренных оперативных служб через единый номер «112» на базе единых дежурно-диспетчерских служб муниципальных образований» (письмо исходящий №П13-1145 от 28.03.08 года).

Таким образом, в настоящий момент в Санкт-Петербурге выполнены основные этапы реализации федеральной концепции:

- проведено предпроектное обследование территории субъекта;
- завершены проектные работы по созданию единой дежурно-диспетчерской службы;
- разработана нормативно-правовая база функционирования системы на территории города;
- выполнены работы по приспособлению производственных помещений и строительству соответствующей инфраструктуры;
- разработан и внедрен в опытную эксплуатацию программно-технологический комплекс системы;
- произведен набор и обучение кадрового состава.

Созданный на базе ГМЦ Санкт-Петербурга рабочий прототип Единой дежурно-диспетчерской по обработке экстренных вызовов, удовлетворяющая требованиям федеральной Концепции Системы-112, одобренной Правительством Российской Федерации 27 декабря 2007 года.

19 июля 2008 года представители Комитета по информатизации и связи Санкт-Петербурга и ГМЦ приняли участие в совещании в Министерстве связи и массовых коммуникаций Российской Федерации по вопросу создания в Санкт-Петербурге системы вызова экстренных служб через единый номер «112». По итогам совещания создана совместная рабочая группа при Федеральном агентстве связи (далее – Россвязь), в состав которой включены специалисты Комитета и ГМЦ. В соответствии с решением совещания данная рабочая комиссия должна разработать проект схемы связи, обеспечивающей прохождение вызовов по номеру «112» к единой дежурной службе ГМЦ, а также технические требования к операторам связи для внедрения Службы «112» в пилотной зоне Кронштадтского района.

Экстренные вызовы граждан будут приниматься уже по единому телефонному номеру «112», а номера «01», «02», «03», «04», «004» будут упразднены (федеральная Концепция предполагает их замену на «101», «102», «103», «104» в резервных целях).

В рамках развития Концепции создания и развития Автоматизированной информационной системы обеспечения безопасности жизнедеятельности Санкт-Петербурга продолжаются работы по совершенствованию и развитию систем интегрированных с АИС ГМЦ:

1. Автоматизированная система дежурной части ГУВД по Санкт-Петербургу и Ленинградской области предназначена для автоматической регистрации и автоматизированного документирования, принимаемых по телефонным каналам голосовых сообщений в интерактивном режиме с минимальным отвлечением диспетчеров с последующей автоматической передачей непосредственному исполнителю;

2. Автоматизированная информационная ЕДДС ГУ «Центр управления силами ФПС по г. Санкт-Петербургу» предназначена для автоматизированного решения оперативной задачи ГУ «ЦУС ФПС по Санкт-Петербургу» при возникновении пожаров, аварий, стихийных бедствий и других чрезвычайных ситуаций, накопления информации о предпринятых действиях, ее последующего анализа [1].

В 2006 году в Центральном районе Санкт-Петербурга развернут первый пусковой комплекс городской системы видеонаблюдения. Установлено 86 телекамер системы, 16 пунктов экстренной связи типа «Гражданин-Милиция», поставлены под охрану 183 укрепленных чердачных помещений домов по Невскому проспекту. В 2007 году произведена установка 555 камер видеонаблюдения, 23 пунктов экстренной связи, а также постановка под охрану 250 чердачных помещений и подвалов в рамках работ второго пускового комплекса системы в Петроградском районе Санкт-Петербурга. В 2008 году в рамках утвержденной адресной программы проводятся работы по внедрению городской системы видеонаблюдения в Василеостровском районе. Предполагается установка 580 камер видеонаблюдения, 57 пунктов экстренной связи, постановка под охрану около 600 чердаков и подвалов.

В рамках городской системы мониторинга стационарных и подвижных объектов с использованием автоматических охранных и пожарных сигнализаций, систем экстренного вызова милиции и систем контроля доступа осуществляется контроль состояния систем безопасности на городских социальных объектах.

Достиженные результаты

1. С апреля 2007 года СПб ГУ «Городской мониторинговый центр» осуществляет круглосуточный мониторинг оперативной обстановки в центральных районах Санкт-Петербурга, а также в местах проведения массовых мероприятий. Поступающие в режиме реального времени вызовы, сообщения, аудио- и видеопоследовательности обрабатываются и анализируются операторами дежурной смены: информация, представляющая оперативный интерес, архивируется на электронные носители с целью дальнейшей передачи в заинтересованные ведомства и структуры. Указанная информация, получаемая в рамках эксплуатации АИС ОБЖ Санкт-Петербурга, может быть использована в оперативно-служебной деятельности.

2. Созданные видеоматериалы направлены в адрес соответствующих структур и ведомств, в т.ч. Ситуационный центр Санкт-Петербурга, РУВД административных районов Санкт-Петербурга, УГИБДД по Санкт-Петербургу и Ленинградской области, ССБ УФСКН по Санкт-Петербургу и Ленинградской области, Прокуратуру Санкт-Петербурга. Подготовлены видеоматериалы, позволяющие провести анализ работы карманников у станций метро и др. Дополнительно подготовлены видеоматериалы по состоянию системы безопасности дорожного движения в центральных районах города: «Организация парковки автотранспорта», «Дорожно-транспортные происшествия с участием маршрутных автобусов», «Организация движения гужевого транспорта» и др.

3. Дополнительно специалистами ГУ «ГМЦ» проведены мероприятия по комплексному мониторингу оперативной обстановки в дни организации праздничных общественно-политических мероприятий на территории Санкт-Петербурга (всего 107 мероприятий), в т.ч.:

- 08.06.2007–11.06.2007 Международный Экономический форум;
- 09.06.2007 Марш несогласных;
- 23.06.2007–24.06.2007 Общегородской праздник «Алые паруса»;
- 05.07.2007 концерт Э.Джона на Дворцовой площади;
- 16.07.2007 флэш-моб «Праздник поцелуев»;
- 02.08.2007 день ВДВ;
- 22.08.2007 день Государственного флага;
- 08.09.2007 Марш несогласных;
- 23.09.2007 Международный атлетический пробег;
- 07.10.2007 Митинг «Молодой Гвардии»;
- 11.10.2007 Митинг против ввоза радиоактивных отходов;
- 04.11.2007 День народного единства;
- 25.11.2007 Марш несогласных;
- 23.12.2007 Несанкционированный митинг на Пионерской площади;
- 27.01.2008 Мероприятия в связи с годовщиной прорыва Блокады;
- 23.02.2008 Несанкционированный митинг «Русский марш»;
- 03.03.2008 Марш несогласных;
- 08.03.2008 Футбольный матч «Зенит»–«Олимпик», подходы к стадиону;
- 16.03.2008 Футбольный матч «Зенит»–«Спартак», подходы к стадиону;
- 25.03.2008 Несанкционированное шествие антифашистов;
- 10.04.2008 Футбольный матч «Зенит»–«Байер», подходы к стадиону;
- 01.05.2008 Санкционированные (несанкционированные) мероприятия, посвященные Международному дню трудящихся;
- 01.05.2008 Футбольный матч «Зенит»–«Бавария», подходы к стадиону, гуляния болельщиков «Зенита» на улицах города.

Развитие системы в 2008-2009 годы

2008 год. Проведены работы в рамках третьего пускового комплекса городской системы видеонаблюдения, дальнейшее развитие системы экстренной связи и оборудование охранной сигнализацией чердаков и подвалов домов в Василеостровском районе. Текущее состояние работ – разработана адресная программа размещения камер видеонаблюдения, пунктов экстренной связи и постановки на охрану подвалов и чердаков жилых домов. Проводится проектирование системы на основе ранее разработанной адресной программы.

В рамках развития центра обработки экстренных вызовов проводилась интеграция единого центра обработки экстренных вызовов с диспетчерской службой Городской станции скорой медицинской помощи (Служба «03»), дежурными службами СПб ГУП «ТЭК» и СПб ГУП «Водоканал», с диспетчерскими службами обработки экстренных вызовов операторов сотовой связи на территории Санкт-Петербурга. Указанные мероприятия позволят уже в текущем году создать на территории субъекта Российской Федерации первый полностью функциональный работающий прототип единой дежурно-диспетчерской службы спасения «112» [2].

2009 год. Проведены работы в рамках четвертого пускового комплекса городской системы видеонаблюдения, дальнейшее развитие системы экстренной связи и оборудование охранной сигнализацией чердаков и подвалов домов в Центральном районе.

В рамках развития центра обработки экстренных вызовов проводилась интеграция с геоинформационной системой для обеспечения комплексного мониторинга ситуаций, связанных с экстренными событиями, а также интеграция со справочными и дежурными службами отраслевых органов исполнительной власти Санкт-Петербурга.

Планы развития ГМЦ на 2010 год

Планируется проведение работ в рамках пятого пускового комплекса городской системы видеонаблюдения, дальнейшее развитие системы экстренной связи и оборудование охранной сигнализацией чердаков и подвалов домов в Адмиралтейском районе.

В рамках развития центра обработки экстренных вызовов планируется организация информационного взаимодействия со Службой экстренных вызовов Ленинградской области, автоматизация мониторинга и контроля выполнения административных процессов в рамках деятельности электронного правительства города, а также дальнейшее расширение масштабов внедрения системы.

СПИСОК ЛИТЕРАТУРЫ

1. Постановление Правительства Российской Федерации от 31.12.2004 № 894 «Об утверждении перечня экстренных оперативных служб, вызов которых круглосуточно и бесплатно обязан обеспечить оператор связи пользователю услугами связи, и о назначении единого номера вызова экстренных оперативных служб»

2. Устав ГМЦ (Распоряжение губернатора Санкт-Петербурга от 01.02.2005 № 3-рп).

3. Организация Городского мониторингового центра и центра обработки вызовов «Служба 112» на базе ГУ. «Центр». [Сайт Администрации СПб [Электронный ресурс] URL: http://www.gov.spb.ru/gov/admin/otrasl/c_information/centre112 (дата обращения: 25.03.2010)

Колин К.К.

Россия, Москва, Институт проблем информатики РАН

КАЧЕСТВО ЖИЗНИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИИ

Аннотация. Актуальные проблемы повышения качества жизни населения России рассматриваются в контексте процесса развития в нашей стране информационного общества и обеспечения информационной безопасности. Показано, что становление информационного общества может и должно стать важным фактором в решении многих социально-экономических проблем, напрямую связанных с качеством жизни населения.

Введение. В Стратегии национальной безопасности Российской Федерации на период до 2020 года, которая утверждена Указом Президента России 13 мая 2009 года [1], качество жизни населения рассматривается как один из важнейших факторов обеспечения национальной безопасности страны. Однако в современных условиях глобализации и информатизации общества представления людей о качестве жизни быстро изменяются. В какой мере развитие информационного общества в России может стать фактором повышения качества жизни ее населения? Что необходимо сделать сегодня, в условиях глобального финансово-экономического кризиса, для того, чтобы более эффективно использовать для повышения качества жизни населения те новые возможности, которые создает научно-технический прогресс в сфере информационных и коммуникационных технологий? Анализ этих вопросов и является основной целью данной работы.

1. Новые представления о качестве жизни в информационном обществе. В 2007 году в России издана монография известного американского специалиста в области изучения глобальных проблем развития цивилизации Элвина Тоффлера «Революционное богатство» [2]. В ней показано, что на современном этапе развития научно-технологической революции традиционные представления о качестве жизни у многих миллионов людей существенным образом изменяются. Качество жизни современного человека становится во все большей степени зависимым от уровня потребления им информационных продуктов и услуг, а также от их доступности и качества. Мобильная телефония, персональные компьютеры с выходом в сеть Интернет, многоканальное цифровое телевидение, бортовые автомобильные навигационные спутниковые системы – все это уже неотъемлемые атрибуты современного человека, без которых его повседневная жизнь и профессиональная деятельность становятся неполноценными.

В последние годы средства информатики и новые информационные технологии быстро совершенствуются и, что очень важно, становятся доступными для все более широких слоев населения. Они позволяют людям экономить затраты времени на решение многих повседневных и производственных проблем, создают новые возможности для практической реализации человеком своих гражданских прав и свобод.

Весьма характерно, что уже сегодня, как в развитых, так и во многих развивающихся странах, все большее количество информационных услуг оказывается населению бесплатно, а затраты по их обеспечению принимают на себя муниципальные, региональные и государственные бюджеты.

Таким образом, качество жизни современного человека все больше определяется способностью общества предоставлять ему необходимые информационные продукты и услуги, т.е. информационным качеством самого общества. Именно поэтому в последние годы и появились такие новые понятия, как информационная бедность и информационное неравенство. Причем, эти понятия используются не только по отношению к отдельным людям, но также и для характеристики целых стран и регионов мира.

По мнению Э.Тоффлера, в информационном обществе будут совсем другие, отличные от традиционных, представления о структуре личного, корпоративного и национального богатства. Так, например, если ранее основными компонентами личного богатства считались, главным образом, материальные ценности и денежные средства, которые давали людям возможности не только удовлетворять насущные потребности, но также и осуществлять свои желания и планы деятельности, то в ближайшем будущем дело будет обстоять совершенно иначе. Ведь уже сегодня многие потребности и желания человека связаны с возможностью использования им современных информационных ресурсов и технологий, средств связи и телекоммуникации. Весь наш образ жизни становится в последние годы все более информационным по своему содержанию, и нет никакого сомнения в том, что эта важная тенденция развития цивилизации сохранится и в будущем.

2. Развитие информационного общества в России как социально-экономическая проблема.

В феврале 2008 года в области информационного развития нашей страны произошло важное событие – утверждена Стратегия развития информационного общества в Российской Федерации на период до 2015 года [3]. Этот документ имеет не только концептуальный, но также и прикладной характер, так как он содержит конкретные значения основных индикаторов развития информационного общества, которые должны быть достигнуты в нашей стране уже в 2010 и 2015 годах, соответственно.

В настоящее время по темпам развития процесса формирования информационного общества Россия существенно уступает не только передовым странам Запада, но также и таким развивающимся странам, как Китай, Индия и Малайзия. Причем, это отставание в последние годы не сокращалось, а продолжало нарастать. Так, например, в международном рейтинге сетевого развития, который был опубликован к началу проведения международного экономического форума в Лондоне в марте 2009 года, Россия заняла 74-е место среди 170 стран мира. При этом еще год назад она занимала в этом рейтинге 72-е место.

Главные причины этого отставания эксперты видят в недостаточной развитости информационной инфраструктуры нашей страны, а также в неравномерности информационного развития ее регионов. Называют и еще две причины: снижение эффективности системы административного управления в России после ее реформирования, проведенного в 2004 году, а также недостаточный уровень информатизации сферы образования. И действительно, начиная с 2004 года, информатизация образования уже не рассматривается в России в качестве приоритетного направления модернизации системы образования.

Удивление российских ученых вызвало также и предложение Минобрнауки РФ исключить развитие ИКТ-технологий (информационно-коммуникационных технологий) из формирующегося в настоящее время нового Перечня приоритетных направлений развития научно-технического прогресса в России на ближайшие годы. Российская академия наук представила по этому поводу аргументированные возражения.

Приведенные факты свидетельствуют о том, что актуальность и социально-экономическая значимость проблемы формирования информационного общества в России многими нашими чиновниками сегодня явно недооценивается. И это несмотря на то, что и Президент России Д.А. Медведев, и Председатель Правительства РФ В.В. Путин в своих выступлениях неоднократно подчеркивали стратегическую важность информационного развития нашей страны и необходимость ее полноправного вступления в уже формирующееся глобальное информационное общество.

К сожалению, несмотря на то, что Совет по развитию информационного общества в России возглавил лично Президент РФ Д.А. Медведев, а указанная выше Стратегия развития информационного общества была утверждена еще в феврале 2008 года, комплексный план действий по реализации основных положений этой Стратегии до сих пор не утвержден Правительством РФ, так как он находится в стадии согласования с различными министерствами и ведомствами. Кроме того, как показывает анализ содержания программ информатизации российских регионов [4], эти программы, как правило, не нацелены на решение крупных социально-экономических проблем, а содержат, в основном, второстепенные мероприятия частного характера.

Таким образом, развитие информационного общества в России является сегодня не столько инструментально-технологической сколько информационно-психологической проблемой, для решения которой необходимо изменить общественное сознание и, в первую очередь, ментальность наших федеральных и региональных чиновников. Они должны, наконец, понять, что формированию информационного общества сегодня нет альтернативы, что это магистральное направление развития цивилизации в 21-м веке, по которому уже идут все развитые и многие развивающиеся страны мира. Ведь именно благодаря приоритетному информационному развитию в последние годы добились

весьма впечатляющих экономических успехов такие страны, как Финляндия, Норвегия, Швеция, которые по величине ВВП на душу населения вошли в первую десятку стран мира [5].

3. Социальная значимость информационного развития страны в условиях современного финансово-экономического кризиса. В условиях глобального финансово-экономического кризиса, который сегодня охватил практически все страны мира, в том числе и Россию, социальное значение информационного развития общества существенным образом возрастает. Кризис обострил такие проблемы, как занятость населения и переподготовка специалистов с целью получения ими новых профессий и специальностей, которые являются сегодня более востребованными на рынке труда. По данным Всемирного банка, многие страны мира (Австралия, Ирландия, Сингапур, Франция, Южная Корея и Япония) увеличивают свои вложения в развитие широкополосного доступа к сети Интернет, рассматривая это как важную антикризисную меру в национальной экономике.

В условиях России, с ее колоссальной по протяженности территорией, указанные выше проблемы могут быть эффективно решены лишь на основе существенно более широкого использования методов открытого образования и дистанционного обучения на базе современных ИКТ. К сожалению, и то, и другое требует в России более энергичного развития, а также правовой и финансовой поддержки, как на федеральном, так и на региональном уровне.

Информационное развитие страны и проблема занятости населения. По данным официальной статистики, количество безработных в России уже превысило 2,1 млн. человек и продолжает расти. Это серьезная социальная проблема, над решением которой сейчас работают органы государственной власти в центре и на местах, а также руководители структур бизнеса. Однако, возможности новых информационных технологий при этом практически не используются. А ведь такие возможности есть и их использование может дать весьма существенный социально-экономический эффект достаточно быстро. Прежде всего, здесь следовало бы подумать об увеличении занятости в информационной сфере общества, развитие которой является для современной России исключительно важной и актуальной проблемой.

По оценкам экспертов, уровень обеспеченности необходимыми кадрами отечественной отрасли ИКТ сегодня не превышает 40% [6]. А ведь мы уже строим информационное общество! Наиболее дефицитными сегодня являются разработчики программного обеспечения, системные интеграторы, руководители проектов информатизации различных сфер деятельности, и, конечно же, преподаватели информатики для ВУЗов, общеобразовательных школ и колледжей. Поэтому подготовка специалистов современного уровня квалификации по указанным направлениям является важнейшей задачей системы образования, которая должна быть соответствующим образом перестроена.

Помимо социального эффекта повышения занятости населения, решение этой задачи даст в будущем и весьма существенный экономический эффект. В качестве примера здесь можно привести опыт Индии, которая сегодня занимает второе (после США) место на мировом рынке программного обеспечения. Доля Индии на этом рынке составляет 20%, в то время как России принадлежит всего около 1%. Этот результат был достигнут благодаря реализации в Индии национальной программы создания крупных центров так называемого «оффшорного программирования». Сегодня в Индии существуют 13 таких центров, в которых занято около 500 тысяч человек. Их основной продукцией являются компоненты программных систем, которые разрабатываются индийскими специалистами по заданиям американских и канадских компаний. По имеющимся прогнозам, объем таких разработок к 2010 году может достигнуть 100 млрд. долларов, что составит почти четвертую часть всего индийского экспорта.

Развитие в Индии индустрии программного обеспечения потребовало создания и соответствующей технической и кадровой поддержки. Для этих целей в стране были созданы два крупных сборочных завода компьютерной техники, принадлежащие известным американским компаниям. Кроме того, ряд крупных индийских фирм осуществили перепрофилирование своей деятельности в направлении разработки программного обеспечения. В этой области даже появились первые индийские миллиардеры.

При активной поддержке государства в Индии создана сеть специализированных учебных заведений, которая осуществляет подготовку специалистов для индийских ИКТ-технопарков. Зарплата программиста в этих технопарках составляет 15–17 долларов в час, что для индийских условий является вполне достойным уровнем оплаты труда.

Индийский опыт развития ИКТ-технопарков и современной России. В какой же мере описанный выше индийский опыт может быть использован в современной России? По инициативе В.В. Путина попытки его использования уже предприняты, но гордиться здесь нам пока еще нечем. Решение о создании в России первых четырех специализированных ИКТ-технопарков было принято Президентом России В.В. Путиным еще в 2004 году после его посещения одного из аналогичных индийских технопарков в штате Бангалор. Сегодня реализуется государственная программа создания таких технопарков в г. Сарове Нижегородской области, Санкт-Петербурге, Новосибирске и г. Дубне Московской области. Планируемые сроки ввода в действие технопарков — 2010–2011 гг. Наиболее

крупный из них создается в Дубне. В нем будет работать около 10 тыс. программистов, для которых уже строится городок на 30 тыс. жителей.

Таким образом, можно ожидать, что в результате реализации данной программы российская отрасль ИКТ получит 20–30 тыс. современных специалистов, что, конечно же, хорошо, но кадровых проблем этой отрасли в целом далеко не решает. Здесь нужны совсем другие масштабы, да и несколько иной подход к решению проблемы. В России нужно создать не 4–7 ИКТ-технопарков, как это осуществляется сегодня, а 40–50 крупных специализированных ИКТ-технопарков для того, чтобы иметь собственную высокоэффективную отрасль ИКТ, занять достойное место на мировом рынке программного обеспечения и снизить зависимость страны от его зарубежных производителей, которая представляет сегодня одну из угроз для национальной безопасности.

Кроме того, представляется целесообразным сформировать и осуществить федеральную целевую программу создания ИКТ-технопарков среднего уровня при крупных университетах. В них должна осуществляться разработка отечественных программных средств и информационных продуктов для сферы образования, науки, культуры, соответствующей отрасли экономики, а также социальной сферы. Сегодня же во всех этих сферах доминируют зарубежные продукты, которые приходится закупать и адаптировать к российским условиям. Думается, что создание 200–300 таких технопарков с численностью специалистов порядка 200–500 человек в каждом могло бы существенным образом изменить ситуацию в России, как в области информатизации образования, так и в области подготовки специалистов для развития информационного общества.

4. Информационное общество и проблема занятости инвалидов, пенсионеров и женщин с детьми. По данным социологических исследований, в России сегодня насчитывается более 9 млн. инвалидов, многие из которых имеют ограниченную мобильность, но вполне могли бы работать на дому. Современные информационные технологии предоставляют для этого хорошие возможности, которые пока еще очень мало используются. Персональный компьютер с выходом в сеть Интернет, лазерный принтер и, возможно, сканер – вот и весь тот минимальный набор средств информатики, который может дать работу нескольким миллионам наших инвалидов. Для многих из них это единственная возможность почувствовать себя полезными для общества и заработать необходимые средства для своего существования. К сожалению, наши социальные службы этой возможности не видят и никаких действий для ее практического использования не предпринимают. И здесь мы вновь сталкиваемся с проблемой ментальности наших чиновников, сознание которых находится еще на уровне прошлого века.

Развитие системы «информационного надомничества» могло бы дать работу не только инвалидам, но также и пенсионерам, которые, по мере своих возможностей, могли бы участвовать в трудовой деятельности. Для многих из них это не только дополнительный заработок, но также и весьма важный морально-психологический фактор. Ведь многие пенсионеры имеют большой производственный, научный и педагогический опыт, который они могли бы передавать молодому поколению, повышая таким образом интеллектуальный уровень российского общества.

Информационное надомничество является перспективным занятием и для тех женщин, которые вынуждены прервать свою трудовую деятельность в связи с беременностью или же необходимостью воспитывать дома маленьких детей. Их квалификация, знания и опыт также могли бы использоваться более эффективно по сравнению с тем, как это имеет место сегодня.

5. Доступ в Интернет как национальная проблема России. Для практической реализации тех новых возможностей, которые создаются в информационном обществе для повышения уровня занятости населения, в стране должна быть создана современная информационная инфраструктура. Прежде всего, здесь необходимо решить проблему широкополосного доступа пользователей к сети Интернет на всей территории России. Сегодня такой доступ обеспечивается только в крупных городах, да и то его стоимость является еще слишком высокой для массового пользователя.

Кардинальное решение этой проблемы видится на пути развития системы космической связи и создания новых технологий широкополосного доступа в Интернет с использованием возможностей уже существующих проводных радиотрансляционных сетей и сетей электроснабжения производственных и жилых помещений. Экспериментальные разработки таких технологий уже существуют, нужно лишь решить организационно-технические проблемы их промышленной разработки и массового внедрения в практику. Дело это непростое, но, с инженерной точки зрения, вполне осуществимое в течение нескольких ближайших лет. Затраты на создание и внедрение таких технологий многократно окупятся, так как социально-экономический эффект от их использования будет колоссальным. Именно тогда и можно будет говорить о создании в России информационного общества.

6. Московский социально-технологический проект «Социальная розетка» – новый шаг на пути повышения качества жизни населения России. Важный социально-психологический эффект глобальной информатизации общества связан с повышением качества жизни, которое обусловлено более широкими возможностями практического осуществления человеком своих прав и свобод, и которое, в первую очередь, предполагает свободный доступ человека к необходимой ему информации. Именно поэтому во многих странах существуют программы государственной поддержки

систем и технологий обеспечения доступа населения к национальным и мировым информационным ресурсам. Так, например, в США уже более 10 лет действуют меры государственной поддержки процесса подключения пользователей к сети Интернет. Для оказания этих услуг населению установлены налоговые льготы, а подключение пользователей из малообеспеченных слоев населения дотируется государством.

Этот опыт обязательно нужно использовать и в России, и первые шаги в этом направлении уже делаются. Так, например, на состоявшейся недавно в Москве выставке «Связь–Экспокомм–2009» Президенту России Д.А. Медведеву был представлен новый социально-технологический проект «Социальная розетка», который получил его одобрение. Инициатором этого проекта является ФГУП «Московская городская радиотрансляционная сеть», которое уже приступило к его реализации с 1 июля 2009г. Постановление московского правительства по этому поводу было подписано в мае 2009 г.

Суть проекта состоит в том, чтобы в каждой московской квартире появилось специальное устройство, названное социальной розеткой, которое будет обеспечивать москвичам следующие информационные возможности:

- бесплатное подключение к сети Интернет на минимальной скорости;
- 8 основных каналов телевидения;
- 3 канала проводного радиовещания с последующим увеличением их числа до 9;
- оповещение населения о различного рода чрезвычайных ситуациях;
- прямую связь с городскими экстренными службами (так называемая «тревожная кнопка»).

Принципиальная технологическая особенность этого проекта состоит в том, что для его реализации используются средства уже существующей городской радиотрансляционной сети, которая создавалась с учетом требований военного времени и поэтому является энергонезависимой и имеет многократное резервирование по оборудованию. Поэтому она может функционировать даже при аварийных перерывах в электроснабжении.

Предполагается, что установка «социальных розеток» в московских квартирах будет производиться, главным образом, за счет средств городского бюджета, а пользование ею будет стоить столько же, сколько сегодня жители платят за обычную радиоточку. Московское правительство планирует установить социальные розетки во всех квартирах вновь строящихся жилых домов, а также в домах, в которых проводится капитальный ремонт. Что же касается других квартир, то они также будут бесплатно для их владельцев оснащаться «социальными розетками» по заявлениям москвичей. С этой целью в настоящее время вносятся необходимые изменения в городское законодательство, а ФГУП МГРС ведет переговоры с провайдерами сети Интернет о том, чтобы они предоставляли всем жителям Москвы бесплатный доступ в эту сеть на минимальной скорости. При необходимости скорость информационного обмена может быть повышена на основе отдельного договора пользователя с провайдером.

Таким образом, проблема «социального доступа» в сеть Интернет может быть решена в Москве уже в самые ближайшие годы. Это хороший пример для других городов России, где аналогичные проекты также могут быть реализованы при соответствующей поддержке муниципальных и региональных органов власти. Социально-экономическую значимость этих проектов для современной России трудно переоценить и поэтому они заслуживают особого внимания и поддержки также и на федеральном уровне.

7. Развитие информационного общества в России и проблемы образования. Известно, что в современном мире две трети валового продукта производится за счет интеллектуального труда, Поэтому качество общества в той или иной стране, а, следовательно, и качество жизни каждого ее гражданина напрямую зависит от способности данного общества к интеллектуальному труду и производству высококачественных продуктов и услуг. А это, в свою очередь, определяется качеством существующей в данной стране системы образования. К сожалению, исследования показывают, что традиционное для России высокое качество образования в последние годы неуклонно снижается.

Так, например, по данным Минобрнауки РФ, в 2008 году четвертая часть выпускников российских общеобразовательных школ показала неудовлетворительные знания по математике, что стало поводом для рассмотрения в данном министерстве вопроса об отмене выпускного экзамена по математике вообще. Против этой идеи категорически выступил Союз ректоров ВУЗов России, который сегодня возглавляет ректор МГУ им. М.В. Ломоносова академик В.А. Садовничий. Ведь изучение математики необходимо каждому человеку для развития системы логического мышления. Тем не менее, выпускной экзамен по истории в российских школах уже отменен, а знания русского языка и литературы у наших школьников, по оценкам специалистов, оставляют желать много лучшего.

Таким образом, знания подавляющей части молодого поколения российских граждан по базовым предметам, которые формируют фундамент образованности человека (филология, история, математика), являются сегодня неудовлетворительными. И это наносит ущерб качеству российского общества, представляет собой прямую угрозу для национальной безопасности нашей страны. Именно такая оценка содержится в тексте Стратегии национальной безопасности Российской Федерации до 2020 года [1].

Крупным недостатком современной системы образования в России является также и то, что ее содержание еще не нацелено на подготовку человека к жизни и профессиональной деятельности в условиях информационного общества [8]. Причем, речь здесь идет не о том, что необходимое количество специалистов для профессиональной деятельности в информационной сфере нашего общества еще не готовится. Это, конечно, очень серьезный недостаток, но все же не главный. Более важным, по нашему мнению, является то, что современная система образования не ориентирована на формирование новой информационной культуры личности и общества. А ведь эта культура должна быть адекватной той новой информационной реальности, которая уже сегодня окружает каждого человека, изменяет весь его образ жизни, многие ценности, привычные стереотипы поведения.

Исследования показывают [9], что особенно острой эта проблема является для системы педагогического образования, где проблемы развития информационного общества сегодня на должном уровне практически не изучаются. Поэтому для того, чтобы хоть как-то изменить современную ситуацию к лучшему, нам нужно, прежде всего, изменить содержание педагогического образования. С этой целью в 2008 году группой специалистов РАН, РАО, Сибирского федерального университета и ряда других научных и образовательных учреждений России были разработаны предложения по составу и содержанию комплекса магистерских программ нового поколения для модернизации системы высшего педагогического образования. В состав этих программ было предложено включить ряд принципиально новых учебных курсов, направленных на изучение наиболее актуальных проблем развития информационного общества и формирование у магистров современно научного мировоззрения.

Изучение этих курсов будущими преподавателями и руководителями образовательных учреждений, а также научными работниками сферы образования сегодня крайне необходимо для повышения качества педагогического образования и его адекватности тем новым требованиям, которые предъявляет информационное общество. Ведь новая школа России, формирование которой Президент РФ Д.А. Медведев в своем первом Послании к Федеральному Собранию РФ объявил одним из важнейших государственных приоритетов нашей страны, это не только современные здания и оборудование. Это, прежде всего, новое содержание образования, адекватное современным требованиям. И обеспечить его смогут лишь те педагогические и научные кадры системы образования, которые сами предварительно получают соответствующую подготовку.

По инициативе Института проблем информатики РАН и Сибирского федерального университета в настоящее время сформирована сетевая структура, состоящая из ряда научных и образовательных организаций России, которая способна разработать комплексный инновационный проект модернизации системы магистерской подготовки в педагогическом образовании с учетом новых требований информационного общества, а также подготовить для этих целей необходимые учебно-методические материалы, базовые программы и учебные пособия.

Аналогичные проекты необходимо осуществить и по другим направлениям развития российского образования для того, чтобы сделать его содержание адекватным Стратегии развития информационного общества в России.

Заключение. Повышение качества жизни населения является сегодня одной из важнейших задач стратегии социально-экономического развития России и обеспечения ее национальной безопасности. Решение этой задачи самым тесным образом связано с реализацией Стратегии развития информационного общества в России на период до 2015 года, которая должна осуществляться опережающими темпами.

В условиях современного глобального финансово-экономического кризиса информатизация общества должна стать действенным фактором для решения проблем занятости населения, подготовки и переподготовки кадров, повышения конкурентоспособности России на мировом рынке, а также для решения многих других проблем, непосредственно связанных с повышением качества жизни населения.

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента РФ от 13 мая 2009 г. № 537.
2. Тоффлер Э. Революционное богатство. – М.: АСТ: АСТ МОСКВА: ПРОФИЗДАТ, 2008. – 569 с.
3. Стратегия развития информационного общества в России на период до 2015 года. Утверждена Президентом РФ 14 февраля 2008 г.
4. Анализ развития и использования ИКТ в субъектах Российской Федерации. Аналитический доклад. – М.: Институт развития информационного общества, 2008.
5. «Группа восьми» в цифрах. 2006. Стат. Сб./Росстат. – М.: 2006. – 123 с.
6. Колин К.К. Интеллектуальные ресурсы человека в информационном обществе. // Труд и социальные отношения, №5, 2008. – С. 63–67.
7. Колин К.К. Информационные технологии как импульс к развитию национальной экономики. // Человек и труд, №4, 2006. – С. 74–77.
8. Соколов И.А., Колин К.К. Новый этап информатизации общества и проблемы образования. // Информатика и ее применения. Том 1, вып. 2. 2008. – С. 34–43.
9. Колин К.К. Инновационное развитие в информационном обществе и качество образования. // Открытое образование, №3(74), 2009. – С. 63–72.

Сальников М.А., Копыльцов А.В.

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

ПЕРСПЕКТИВЫ РАЗВИТИЯ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ В РОССИИ

Эффективность комплексной защиты безопасности государств Европы и Азии в начале XXI века была ознаменована снижением. Эта тенденция не могла не затронуть и Российскую Федерацию. Поэтому Правительства Российской Федерации постепенно расширило деятельность и финансирование в данной области. Так, в 2009–2011 годах Правительством Российской Федерации выделяются следующие направления развития Комплексных систем безопасности (КСБ):

1. Создание Общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей (далее ОКСИОН) в Российской Федерации.

Целью построения ОКСИОН является повышение эффективности Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций посредством подготовки и своевременного информирования населения по действиям в чрезвычайных ситуациях природного и техногенного характера, при совершении террористических актов, трансляции материалов профилактической направленности, а также получение оперативной информации с мест массового пребывания людей [1]. В настоящее время развернуты и функционируют на территории Российской Федерации 25 информационных центров.

2. Создание в 2009–2011 годах пилотных зон ОКСИОН в метрополитенах Москвы и Санкт-Петербурга, создание КАСИП АЗМ.

В рамках «Межведомственной комплексной программы мероприятий по совершенствованию антитеррористической защищенности метрополитенов России, утвержденной Распоряжением Правительства Российской Федерации от 27.05.2005 №682, создана комплексная автоматизированная система информационной поддержки антитеррористической защищенности метрополитена (КАСИП АЗМ) [2]. В целях дальнейшего развития предлагается интегрировать вышеуказанную систему КАСИП АЗМ в систему ОКСИОН. К 2010 году планируется подготовка презентации о взаимодействии служб ГУ МЧС России по Санкт-Петербургу, ГУВД по Санкт-Петербургу и Ленинградской области и Петербургского метрополитена по отработке сигнала «Радиационная опасность» со станции метрополитена «Чкаловская».

3. Комплексная система безопасности городов (АПК «Безопасный город»).

АПК «Безопасный город» – система, направленная на решение проблем профилактики. Она способна осуществлять реагирование не только на криминальные, в том числе и террористические угрозы. Но и обеспечивать предупреждение техногенных аварий, экологических катастроф, нарушения устойчивого функционирования органов управления и особо важных или опасных объектов. С этой целью предлагается создать централизованно управляемую комплексную систему обеспечения безопасности Санкт-Петербурга на основе созданных уже элементов обеспечения безопасности в рамках субъектов и федеральных программ. Предполагается учитывать опыт разработки и работы с:

- автоматизированной системой обеспечения безопасности жизнедеятельности Санкт-Петербурга (АИС ОБЖ),
- аппаратно-программными комплексами систем обеспечения общественной безопасности городов Российской Федерации (АПК «Безопасный город»),
- Общероссийской комплексной системой информирования и оповещения населения (ОКСИОН),
- системой обеспечения вызова экстренных оперативных служб («Система – 112»),
- комплексной системой обеспечения безопасности объектов социальной инфраструктуры (КСОБ),
- комплексной автоматизированной системой информационной поддержки антитеррористической защищенности метрополитена (КАСИП АЗМ).

В дальнейшем данная комплексная система позволит обеспечить единый подход к развитию и эксплуатации систем безопасности в масштабе субъекта и может быть использована как типовая модель при развертывании в других регионах Российской Федерации [2].

Если по предыдущим трем направлениям существует достаточно много статей, откуда можно почерпнуть достаточно полную информацию, то следующий пункт не подлежал широкой огласке хотя бы в силу технической сложности реализации и отсутствия специалистов в данной области.

4. В отдельное направление развития КСБ выделяется развитие и внедрение систем видеонаблюдения на базе вышеописанных направлений как одно из наиболее перспективных.

Анализ опыта использования систем видеонаблюдения в борьбе с преступностью за рубежом показывает, что такие системы вполне эффективны и рентабельны. В настоящее время в Австрии используется для видеонаблюдения 160000 камер. Большая часть камер находится в частном ведомстве, например, банков, казино и почтовых отделений. Соответствующими органами применяется только 1200 камер. Камеры не только выполняют функцию наблюдения, но и способствуют повышению

чувства безопасности населения. В Великобритании с 80-х годов видеонаблюдение очень широко распространено.

Большинство жалоб, направленных в Европейский суд по правам человека, составляют жалобы из Великобритании. Основной причиной жалоб было, как правило, отсутствие правовой основы для проведения такого наблюдения или неправомерное вмешательство в области охраны частного сектора, которое привело к нарушению права, гарантированного конституцией. В Австрии в законе об охранной полиции и в Уголовно-процессуальном кодексе установлены нормы, позволяющие проводить наблюдение с помощью передачи изображения. Основное внимание на заседании уделялось аспекту охранной полиции. Главной задачей охранной полиции является предотвращение потенциальной опасности. Для выполнения этой задачи согласно закону об охранной полиции 1993 года полиции даны полномочия на использование видео- и аудиотехники в целях осуществления открытого и скрытого наблюдения [4].

Открытое видеонаблюдение с помощью видеотехники разрешено только в том случае, если не устанавливаются данные о личности преступника или подозреваемого. Открытое видеонаблюдение разрешается также для обеспечения охраны людей и вещей. Охрана государственных учреждений и международных организаций всегда связана с риском, который оправдывает применение видеотехники в частном секторе. Кроме того, наблюдение разрешается в общественных местах для предотвращения опасных нападения, а также для оказания поддержки службе надзора и патрульной службе. Использование записывающих устройств допустимо при установлении данных о личности, если – как на футбольных матчах и демонстрациях – следует опасаться нападений, представляющих собой угрозу жизни и здоровью.

Органам государственной безопасности не разрешено проводить наблюдение и запись в общественных местах, например, на вокзалах и в аэропортах, даже в случае возможных опасных нападений. Однако, в проекте дополнения к закону об охранной полиции предусматривается применение устройств для передачи изображения и записи звука для проведения наблюдения в особо опасных местах (зоны интенсивной преступности). При этом на заседании также шла речь о том, что наблюдение играет значительную роль в области предупреждения преступности. Потенциальные преступники, зная об использовании видеокамер, отказываются от намерения совершить преступление.

В Великобритании применяются также камеры, которые составляют цифровой профиль. Это должно повысить эффективность борьбы с преступностью. В Ирландии при определении биометрических признаков используют систему «Face it». С помощью этой системы полученные данные можно сопоставлять с данными банка. Однако, при этом существует большой процент погрешностей. Техника несовершенна.

В США после 11 сентября 2001 года перешли к интенсивному видеонаблюдению. В Германии наблюдение на вокзалах осуществляется федеральной пограничной охраной. Видеозаписи могут просматривать только служащие пограничной охраны, так как средства программирования находятся только в распоряжении сотрудников федеральной пограничной охраны. Полученные данные могут передаваться в случае необходимости полиции земель. Такие методы наблюдения целесообразно применять при проведении массовых мероприятий в целях своевременного выявления опасности или для наблюдения в районе вокзала за лицами, вызывающими подозрение (воры-карманники). Наблюдение может осуществлять также управление железной дороги, производить записи может только федеральная пограничная охрана [4].

В 2003 и 2004 годах с помощью видеонаблюдения полицией было выявлено на вокзалах 268 преступлений и обнаружено 165 подозреваемых в совершении преступлений. Применение видеокамер очень эффективно в борьбе с уличной преступностью и, особенно, в «зонах интенсивной преступности». Это относится, прежде всего, к нелегальной торговле наркотиками в общественных местах. В случае «ликвидации» зоны интенсивной преступности видеонаблюдение прекращается. Важным элементом является взаимодействие полиции с гражданами и сотрудничество полиции с соответствующими органами власти, задачей которых является обеспечение общественной безопасности. При этом речь идет о мерах, которые способствуют повышению чувства безопасности населения и не ограничивают личную свободу. По поводу методов наблюдения в Штутгарте было опрошено 84% населения, 60% опрошенных высказались за применение видеонаблюдения во всех районах города. Оптические приборы наблюдения могут использоваться одновременно в разных местах. При этом применяются переносные устройства, которые размещаются в контейнере и могут легко транспортироваться на грузовом автомобиле. Эти приборы с успехом применяются на платформах метро и на перронах городской железной дороги.

Вопрос эффективности прямого видеонаблюдения в России и необходимость освещения данного вопроса вытекает из анализа практики работы подразделений ОВО. Число камер, приходящихся на одного оператора, чаще всего определяется техническими возможностями системы теленаблюдения или материальными возможностями заказчика оборудования. Такой подход к решению данной проблемы в корне неверен. К тому же, анализ результатов записей с камер видеонаблюдения показывает и отрицательные моменты в организации работы видеосистем, а именно:

1. Крайне низкое качество изображения;

2. Малые размеры объекта наблюдения (люди, совершающие преступление);
3. Наличие постоянного перемещения людей в переходах.

Можно предположить, что на оператора наблюдения приходится не одна, а несколько камер наблюдения (скорее всего 8, или 16, а может быть и более).

При таких исходных данных любой оператор даст высокую вероятность пропуска объекта наблюдения (события преступления).

Различные исследования возможностей оператора видеонаблюдения носят противоречивый характер, поскольку на результат исследования влияют:

1. Психофизиологические особенности человека (его утомляемость, невнимательность, тип нервной системы, пол и т.д.)
2. Мотивация при работе (оператор РЛС или пункта наблюдения РВСН имеет большую мотивацию по сравнению с оператором, наблюдающим за подъездом в жилом доме).
3. Наличие или отсутствие личных проблем в жизни оператора;
4. Уровень зарплаты оператора и т.д.

Однако, все исследователи едины во мнении, что пропуск объекта наблюдения человеком возможен при любом даже самом благоприятном случае.

Кроме того, выводя на один монитор изображения от нескольких камер, мы уменьшаем разрешение системы теленаблюдения. Если использовать стандартное разрешение монитора 1280x1024 пикселя (960x768 ТВ-линий), то для 4 камер получим соответственно разрешение 240x192 ТВ-линий, что уже мало для полноценного наблюдения.

Для наблюдения оператором изображения от телекамер необходимо использовать монитор с размером по диагонали не менее 17 дюймов, желательно для наблюдения полноэкранного видео использовать мониторы с размером по диагонали в 20–21 дюйм.

Угол поля зрения камеры напрямую влияет на вероятность обнаружения объекта, стремление получить широкое поле наблюдения всегда приводит к уменьшению вероятности обнаружения объекта.

Следует ли из выше сказанного, что видеонаблюдение крайне неэффективно? Конечно нет! Здесь мы говорим только о проблемах прямого видеонаблюдения. Система охранного телевидения (СОТ) наиболее информативная система охраны, по сравнению с другими охранными системами. Она предназначена не столько для прямого видеонаблюдения, сколько для решения других важных для безопасности задач, например для видеорегистрации событий с целью их последующего анализа [4].

Анализ видеоизображения преступления происходит чаще всего после его совершения. Поэтому к качеству видеозаписи должны предъявляться достаточно высокие требования.

Таким образом, можно сделать выводы:

1. Количество камер, используемых для непосредственного наблюдения из расчета на одного оператора должно быть минимальным и не превышать 1–4 штуки. Допускается увеличение количество ТВ – камер, из расчета на одного оператора более 4 штук, но тогда с оператора должна сниматься задача непрерывного наблюдения. Допустим, оператор реагирует только на срабатывание видеодетектора движения, или эпизодически наблюдает за движением автомобилей (за автомобильными пробками в час пик), но если движение происходит непрерывно, например, на многолюдной улице, то нагрузка на оператора должна быть не более 4 ТВ-камер.
2. Эффективность прямого наблюдения крайне низка, поэтому при проектировании СОТ разумно подходить к необходимости непрерывного наблюдения оператором обстановки на охраняемой территории. Наверное, непрерывное наблюдение оператором заднего двора здания необязательно.
3. При работе оператора с СОТ необходимо два монитора. Один монитор необходим для наблюдения изображения от нескольких камер (не более 4 штук). Второй монитор необходим для вывода изображения от выбранной оператором камеры вручную или по срабатыванию датчика движения или иного охранного устройства для детального анализа оператором изображения.
4. Кроме того, не изучена в должной степени проблема защиты информации и возможности перехвата сигнала с видеокамер сторонними лицами при использовании глобальных систем видеонаблюдения в рамках КСБ. Эта проблема занимает отдельное место в списке актуальных проблем Комплексных Систем Безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ № 428/432/321 от от 31.05.2005 г. «О порядке размещения современных технических средств массовой информации в местах массового пребывания людей в целях подготовки населения в области гражданской обороны, защиты от чрезвычайных ситуаций, обеспечения пожарной безопасности и охраны общественного порядка, а также своевременного оповещения и оперативного информирования граждан о чрезвычайных ситуациях и угрозе граждан о чрезвычайных ситуациях и угрозе террористических акций»
2. Общероссийская комплексная система информирования и оповещения населения [Электронный ресурс] URL: <http://gu-okision.ru/oxion/> (дата обращения: 25.03.2010)
3. ОКСИОН – Общероссийская комплексная система информирования и оповещения населения в местах массового пребывания. [Электронный ресурс] URL: <http://www.mchsr.ru/oksion/> (дата обращения: 25.03.2010)
4. Сайт VOCORD Россия [Электронный ресурс] URL: <http://www.vocord.ru/> (дата обращения: 25.03.2010)



ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Абламейко М.С., Абламейко С.В.

Белоруссия, Минск, Белорусский государственный университет

ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ОТ КИБЕРАТАК: МЕЖДУНАРОДНЫЕ АКТЫ

С момента распространения первых вирусов начались направленные кибератаки компьютерных систем с целью завладения информацией и денежными средствами. Каждый день осуществляется около двадцати тысяч компьютерных атак. Ежегодно доходы от киберпреступности составляют порядка пяти миллиардов долларов США, а на обеспечение безопасности от таких угроз в мире расходуется триллион долларов. Примером массированного нападения на правительственные и коммерческие сайты произошло в июле 2009 года в Южной Корее – там были взломаны интернет-порталы администрации президента, министерства обороны, парламента, а также ряда банков. В настоящее время с целью защиты компьютерных систем от внешнего воздействия необходимо выработать международно-правовые механизмы.

Одним из основополагающим документом, регулирующим правовое взаимодействие стран, является Хартия ООН. Многие государства стараются применить данный документ для правовой оценки кибернападений. Основной структурой Организации Объединенных Наций, работающей в сфере информационных технологий, является Международный Союз Телекоммуникаций (International Telecommunication Union). Международный Союз Телекоммуникаций в мае 2007 года принял Глобальную Повестку по Кибербезопасности (Global Cybersecurity Agenda). Она является большим комплексом международных мероприятий, объединяющая всех желающих для достижения общих целей по киберстабильности. Затем была создана группа высококвалифицированных экспертов (High-Level Experts Group), включающая около 100 самых известных ученых из разных стран мира. Развивая данное направление, Международный Союз Телекоммуникаций в 2009 году выступил с инициативой создать международный Протокол против киберугроз (Protocol Against Cyber-Threats – ПАСТ). Совет Европы в 2001 году принял Конвенцию о киберпреступности, которая предлагает различные способы для совместной правовой работы стран по оценке кибератак и мер по их отражению. Данная Конвенция вступила в силу 1 июля 2004 года и является единственным имеющим обязательную силу международным инструментом в этой области. Россия, в свою очередь, в 1998 году представила Резолюцию ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» («Developments in the field of information and telecommunications in the context of international security»), определив основные понятия неавторизованных вторжений в компьютерные сети, и предложив международные принципы защиты от кибернападений. В 1999 году Резолюция включила военные угрозы, проистекающие от информационных и телекоммуникационных технологий. Эти резолюции регулярно одобряются Генеральной Ассамблеей ООН, а США регулярно голосуют против них.

Итак, ни Хартия ООН, ни Договор НАТО, ни какой либо другой международный документ не предусматривал кибернападений на компьютерные сети и не может напрямую быть использован применительно к появившемуся новым вызовам 21-го века. Очевидно, что настала чрезвычайная необходимость для разработки новых правовых механизмов защиты от массированных кибератак. В докладе анализируются существующие правовые механизмы и предлагаются пути их совершенствования и развития.

Алексеев А.А.

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

О СТИМУЛИРОВАНИИ ТРУДОВОЙ ДЕЯТЕЛЬНОСТИ ПЕРСОНАЛА, ОБЕСПЕЧИВАЮЩЕГО ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Вопросы стимулирования трудовой деятельности на современном этапе развития нашего государства очень актуальны. Это обусловлено и теми реформами, которые проводятся в различных сферах экономики России, и проблемами, связанными с мировым финансовым кризисом. Отметим, что одной из важнейших задач успешного реформирования экономики является создание заинтересованного отношения граждан в улучшении результатов своей деятельности, преумножения общественного достояния.

Как известно, система стимулирования труда представляет собой совокупность взаимосвязанных и взаимодополняющих стимулов, воздействие которых стимулирует деятельность

сотрудника для достижения поставленных целей. Стимулы подразделяют на материальные и нематериальные, причем материальные могут быть денежными и не денежными.

Например, материальное стимулирование персонала органов внутренних дел Российской Федерации состоит из таких элементов как оклад по занимаемой должности, оклад по специальному званию, процентные надбавки за выслугу лет, за ученую степень, ученое звание, сложность, напряженность и специальный режим службы, надбавка за классность и т.д.

Несмотря на широкий спектр перечисленных денежных надбавок, большим мотивационным потенциалом для сотрудника органов внутренних дел они не становятся. Во-первых, размер этих надбавок очень низкий, а во-вторых, подавляющая их часть ни как не отражается на размере пенсионного обеспечения сотрудника, к которому он стремится в перспективе.

Хотите повысить заинтересованность сотрудников в работе? Самый верный способ — деньги. Но в связи с кризисом многие работодатели не могут, как это было раньше, стимулировать своих сотрудников с помощью премий. И тут на помощь приходит нематериальное поощрение.

Как показали исследования, больше всего сотрудники организаций, учреждений независимо от форм собственности ценят такой способ поощрения, как дополнительный выходной или незначительное сокращение рабочего дня (36%). Чуть менее популярные методы нематериального поощрения – гибкий график работы и хорошие бытовые условия в рабочем кабинете (офисе) (29%). Формула, которую знает практически каждый работодатель: «Лучше не знать где находится работник, но знать чем он занимается, чем знать, где он находится, но не знать чем он занимается».

Почти каждый пятый участник исследования (19%) был бы рад публичной благодарности за хорошую работу из уст руководителя. Для 16% респондентов очень важна помощь в личных делах (рецензия на диплом, помощь устроить ребёнка в детский сад и т.п.). В свою очередь 14% респондентов не отказались бы от возможности работать дома. А вот конкурсы и соревнования, красивое название должности и фотография на доске почёта вызывают у респондентов гораздо меньше энтузиазма (7%, 3% и 5% соответственно).

При этом, опрос также показал, что большинство современных россиян не против внедрения практики трудовых соревнований в своих организациях. В целом принять участие в подобном соревновании готовы 75% респондентов. Однако далеко не все из них стали бы перевыполнять производственный план за идею: около половины участников опроса (45%) сообщили, что включатся в трудовое соревнование только в случае материального стимулирования. Респонденты предложили массу вариантов поощрения, которое они бы хотели получить от руководства за переработку: «Премия, 100% оклада»; «Повышение оклада»; «Бонус в размере 15% от проекта»; «Бонус в виде абонеента в бассейн или спортклуб»; «Материальная премия либо отгулы в удобное для меня время».

По мнению 7% опрошенных, неплохой мотивацией могут стать карьерный рост, человеческое отношение к сотрудникам, корпоративный отдых, беспроцентная ссуда, своевременная оплата труда или же возможность учиться за счёт организации.

Каждый десятый респондент (10%) не смог ответить на поставленный вопрос. Большинство из них считают, что самое большое благо – это грамотный руководитель, который знает, что лучше для коллектива.

Исходя из высказанного, можно четко определить и понять какие приоритеты в стимулировании труда ставят для себя современные работники различных организаций, учреждений, в том числе в полной мере их (эти приоритеты) можно отнести и к сотрудникам органов внутренних дел.

Применение материальных стимулов должно соответствовать следующим принципам:

- системы материального стимулирования должны быть просты и понятны каждому сотруднику;
- эти системы должны быть гибкими, дающими возможность сразу же поощрять каждый положительный результат служебной деятельности;
- поощрение работников важно организовать по критериям, которые воспринимаются каждым как правильные;
- размеры поощрений должны быть экономически и психологически обоснованы (больше и реже, чаще и меньше);
- система поощрений должна формировать у сотрудников ощущение справедливости материальных вознаграждений;
- эта система должна способствовать повышению заинтересованности сотрудников в улучшении не только индивидуальной работы, но и работы в коллективе;
- в этой системе сотрудники должны видеть четкую взаимосвязь между результатами своей работы и деятельности коллектива организации.

Неадекватная система мотивации влечет за собой недоверие к руководству и ощущение несправедливости порядков, установившихся в организации, и как результат – либо низкие показатели в работе, либо текучесть кадров. При этом мало кому приходит в голову разобраться, в чем причины угасания энтузиазма и низкой производительности труда, и выяснить, а как именно

мотивировать сотрудников. Наиболее типичной ошибкой руководителей становится попытка бороться не с причинами, порождающими низкую отдачу сотрудников, а с их последствиями.

Например, низкая служебная и исполнительская дисциплина сотрудников может являться следствием плохого морально-психологического климата в коллективе, плохих условий труда, низкого качества управления и т.д. В ряде случаев руководители стремятся повышать уровень дисциплины лишь за счет ужесточения требований к исполнителям и введения наказаний для нарушителей. Такой односторонний подход, когда не устраняются причины, порождающие проблему, естественно, не может дать положительного результата в долгосрочной перспективе, а иногда вместо улучшения положения дел даже ухудшает ситуацию.

Таким образом, только правильное сочетание материальных и моральных стимулов трудовой деятельности персонала, умелое и своевременное их применение с учетом индивидуальных особенностей конкретной личности будет способствовать улучшению профессиональной деятельности каждого конкретного работника, созданию здорового морально-психологического климата в коллективе и, как результат, успешному решению задач, стоящих перед правоохранительной службой в целом и перед подразделениями информационной безопасности, в частности.

Вус М.А., Кондратьев В.В., Заболотский В.П., Старков А.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
Санкт-Петербургский государственный университет информационных технологий, механики и оптики
О СОВЕРШЕНСТВОВАНИИ ЗАКОНОДАТЕЛЬСТВА ГОСУДАРСТВ – УЧАСТНИКОВ СНГ
В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Введение

Развитие государств – участников Содружества Независимых Государств (СНГ) происходит сегодня в русле глобальной общемировой тенденции формирования информационного общества. Процессы информационной глобализации и расширяющееся применение информационно-телекоммуникационных технологий во всех сферах жизнедеятельности общества создают новые риски и угрозы безопасности. Обостряющаяся при этом проблема информационной безопасности требует комплексных решений.

Проблематика информационной безопасности имеет свои специфические особенности. С одной стороны, бурное развитие и расширение информационной сферы сопровождается расширением применяемой, связанной с этой сферой терминологии, которая фактически является междисциплинарной. С другой стороны, лексика сферы информационной безопасности, как и вообще любой контекст безопасности, должна быть теснейшим образом связана с юриспруденцией и правом.

Главная цель обеспечения информационной безопасности – защита законных прав и интересов граждан, общества и государства. Чисто технических средств для этого явно недостаточно, необходимы и правовые средства. Реализация же защиты правовыми методами может быть эффективна только при закреплении в законодательных актах (в том числе на международном уровне) правового толкования базовых терминов. На основе этих терминов, используемых в общественном обороте, только и может строиться разрешение правовыми методами различных ситуаций, связанных с защитой прав и интересов субъектов общественных отношений.

Межпарламентская Ассамблея государств – участников Содружества Независимых Государств (МПА СНГ), обеспечивая сотрудничество парламентов, осуществляет важную интеграционную роль в регулировании взаимоотношений государств. Развитию и укреплению межгосударственных партнерских взаимоотношений в современных динамичных политических и экономических условиях призвано служить разрабатываемое модельное законодательство, понятийный аппарат которого фактически выполняет роль межнационального языка правового общения. Статьи модельных законов, содержащие толкование понятий, стали неотъемлемой принадлежностью практически каждого принимаемого МПА СНГ правового акта.

Правовые дефиниции модельного законодательства должны аккумулировать в себе мировой опыт социальной практики. При этом они же должны включать в себя такое содержание и иметь тот объем, которые приемлемы для регулирования в каждом из государств Содружества, не препятствуют осуществлению и развитию международных взаимоотношений. В силу этого понятийный аппарат модельных актов может и должен стать важнейшим инструментом в процессе сближения национальных законодательств СНГ и международного права. Правовые понятия модельного законодательства призваны служить основополагающими ориентирами законодательной и правоприменительной практики в странах СНГ.

Целью сотрудничества государств – участников Содружества Независимых Государств (СНГ) в сфере обеспечения информационной безопасности является совместная защита интересов этих государств в информационной сфере. Для достижения этой цели необходимо, в первую очередь, обеспечить защиту информации ограниченного доступа.

Под информацией ограниченного доступа понимается информация, доступ к которой ограничен законодательством государств – участников СНГ либо межгосударственными договорами.

Сравнительный анализ национальных законодательств

Одной из важнейших составляющих в системе обеспечения информационной безопасности государств Содружества, призванной обеспечить интересы их национальной и коллективной безопасности, гарантии обороноспособности, сохранение приоритета новейших научных и технологических разработок в ряде отраслей экономики представляется защита государственных секретов (государственной тайны). В рамках Содружества Независимых Государств в настоящее время существует ряд двусторонних межправительственных соглашений о защите секретной информации.

Вопросы унификации и гармонизации законодательства в сфере защиты государственной тайны нашли свое место в работе Межпарламентской Ассамблеи Государств – участников Содружества Независимых Государств (МПА СНГ). Важным этапом международного сотрудничества явилось принятие МПА СНГ в 2003 году Модельного закона «О государственных секретах». Этот закон охватывает своим регулированием государственную и служебную тайну и в первой своей статье приводит определения применяемых в нем основных понятий.

Исходя из того, что правовые понятия модельного законодательства призваны служить основополагающими ориентирами законодательной и правоприменительной практики в странах СНГ, рассмотрим, как они отражены в национальном законодательстве. Возьмем для примера три базовых понятия законодательства о государственной тайне: «государственная тайна», «государственные секреты» и «служебная тайна».

Таблица 1

Правовая дефиниция «Государственная тайна»

№	Государство, законодательный акт	Определение (трактровка) используемого понятия
1.	Модельный Закон МПА СНГ «О государственных секретах»	Сведения военного, экономического, политического и иного характера, разглашение или утрата которых наносит или может нанести ущерб национальной безопасности государства.
2.	Закон Российской Федерации "О государственной тайне"	Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
3.	Закон Республики Армения "О государственной и служебной тайне"	Государственной тайной являются те сведения в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной, оперативно-разведывательной области деятельности, которые охраняются государством, и распространение которых может привести к тяжелым последствиям для безопасности Республики Армения.
4.	Закон Азербайджанской Республики «О государственной тайне»	Защищаемые государством сведения, связанные с военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельностью, и распространение которых может нанести ущерб безопасности Азербайджанской Республики.
5.	Закон Республики Беларусь "О государственных секретах"	Государственные секреты, разглашение или утрата которых могут повлечь тяжкие последствия для национальной безопасности Республики Беларусь, а также создать угрозу безопасности граждан либо их конституционным правам и свободам.
6.	Закон Республики Казахстан "О государственных секретах"	Сведения военного, экономического, политического и иного характера, разглашение или утрата которых наносит или может нанести ущерб национальной безопасности Республики Казахстан.
7.	Закон Кыргызской Республики "О защите государственных секретов Кыргызской Республики"	К государственной тайне относится информация, разглашение которой может повлечь тяжкие последствия для обороноспособности, безопасности, экономических и политических интересов Кыргызской Республики.
8.	Закон Республики Молдова "О государственной тайне"	Защищаемые государством сведения в области его военной, экономической, научно-технической, внешнеполитической, разведывательной, контрольно-разведывательной и оперативно-розыскной деятельности, распространение, разглашение, утрата, похищение либо разрушение <...> которых может нанести существенный ущерб безопасности Республики Молдова.
9.	Закон Республики Таджикистан "О государственной тайне"	Защищаемые государством сведения в области обороны, экономики, внешних отношений, государственной безопасности и охраны правопорядка, распространение которых может нанести ущерб безопасности Республики Таджикистан; государственная тайна является собственностью Республики Таджикистан.
10.	Закон Республики Узбекистан "О защите государственных секретов"	Государственную тайну составляют сведения, разглашение которых может оказать отрицательное воздействие на качественное состояние военно-экономического потенциала республики или повлечь другие тяжкие последствия для обороноспособности, государственной безопасности, экономических и политических интересов Республики Узбекистан.

Как видим, даже в определении основополагающего понятия «государственная тайна» в законах суверенных государств есть некоторые различия. Все государства в качестве квалифицирующего признака государственной тайны используют ущерб (тяжкие последствия) для

своей безопасности, которым чревато распространение (разглашение) таких сведений (информации). Наряду с этим только в законах Российской Федерации, Республики Армения, Азербайджанской Республики, Республики Молдова и Республики Таджикистан в качестве квалифицирующего признака предусмотрена охрана (защита) государством таких сведений.

Таблица 2

Правовая дефиниция «ГОСУДАРСТВЕННЫЕ СЕКРЕТЫ»

№	Государство, законодательный акт	Определение (трактовка) используемого понятия
1.	Модельный Закон МПА СНГ «О государственных секретах»	Защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права.
2.	Закон Республики Беларусь "О государственных секретах"	Защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права.
3.	Закон Республики Казахстан "О государственных секретах"	Защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права.
4.	Закон Кыргызской Республики "О защите государственных секретов Кыргызской Республики"	Информация, хранящаяся и перемещаемая любыми видами носителей, затрагивающая обороноспособность, безопасность, экономические и политические интересы Кыргызской Республики, подконтрольная государству и ограничиваемая специальными перечнями и правилами, разработанными на основе и во исполнение Конституции Кыргызской Республики.
5.	Закон Республики Узбекистан "О защите государственных секретов"	Государственными секретами Республики Узбекистан являются особой важности, совершенно секретные и секретные военные, политические, экономические, научно-технические и иные сведения, охраняемые государством и ограничиваемые специальными перечнями.

Понятие «государственные секреты» является собирательным, и оно используется правовыми системами не всех государств – участников СНГ. В качестве квалифицирующего признака государственных секретов в законах предусмотрены защита государством таких сведений (информации), ограничение их специальными перечнями, а также названа цель ограничения распространения этих сведений.

Таблица 3

Правовая дефиниция «СЛУЖЕБНАЯ ТАЙНА»

№	Государство, законодательный акт	Определение (трактовка) используемого понятия
1.	Модельный Закон МПА СНГ «О государственных секретах»	Сведения о сферах деятельности государственных органов, доступ к которым ограничивается служебной необходимостью и разглашение или утрата которых может нанести ущерб государственным органам или государству.
2.	Закон Республики Армения "О государственной и служебной тайне"	Служебной тайной являются те сведения в областях, предусмотренных первой частью данной статьи, которые охраняются государством, и распространение которых может принести иной вред безопасности Республики Армения. Такие сведения, как правило, содержат факты, составляющие часть государственной тайны, однако сами по себе не раскрывают государственную тайну.
3.	Закон Республики Беларусь "О государственных секретах"	Государственные секреты, разглашение или утрата которых могут причинить существенный вред национальной безопасности Республики Беларусь, а также конституционным правам и свободам граждан. Сведения, составляющие служебную тайну, имеют характер отдельных данных, входящих в состав сведений, составляющих государственную тайну и не раскрывающих ее в целом.
4.	Закон Республики Казахстан "О государственных секретах"	Сведения, имеющие характер отдельных данных, которые могут входить в состав государственной тайны, разглашение или утрата которых может нанести ущерб национальным интересам государства, интересам государственных органов и организаций Республики Казахстан.
5.	Закон Кыргызской Республики "О защите государственных секретов Кыргызской Республики"	К служебной тайне относится информация, разглашение которой может оказать отрицательное воздействие на обороноспособность, безопасность, экономические и политические интересы Кыргызской Республики. Такая информация имеет характер отдельных сведений, относящихся к государственной или военной тайне, и не раскрывает их полностью.
6.	Закон Республики Узбекистан "О защите государственных секретов"	Служебную тайну составляют сведения в области науки, техники, производства и управления, разглашение которых может нанести ущерб интересам Республики Узбекистан.

Приведенные выше определения из базовых законов ряда государств – участников СНГ трактуют понятие служебной тайны как пограничное с тайной государственной. В законах же Российской Федерации, Азербайджанской Республики, Республики Молдова и Республики Таджикистан нормативно-правового определения понятия «служебная тайна» нет.

Заключение

Из приведенных примеров видно, что даже в такой области, правовое регулирование которой имеет общие традиции, происходящие от системы защиты информации, ранее имевшей место в нашей общей стране, в государствах МПА СНГ существуют отдельные расхождения в нормативных трактовках базовых понятий.

Принимая во внимание исключительную важность грамотного толкования и использования терминов и понятий, при разработке рекомендаций для государств – участников Содружества Независимых Государств по совершенствованию законодательства в области информационной безопасности, первым шагом на пути гармонизации такого законодательства представляется составление возможно более полного словаря-справочника понятий и определений используемых в национальных законодательствах государств – участников СНГ в информационной сфере.

При подготовке доклада использованы тексты нормативных документов:

1. Модельный Закон «О государственных секретах», принятый на двадцать первом пленарном заседании МПА СНГ (Постановление № 21-10 от 16 июня 2003 года);
2. Закон Российской Федерации "О государственной тайне" от 21.07.1993 № 5485-1 в редакции Федерального закона от 06.10.1997 N 131-ФЗ (с изм. и дополнениями);
3. Закон Республики Армения от 3 декабря 1996 года "О государственной и служебной тайне";
4. Закон Республики Беларусь от 29 ноября 1994 года 3410-XII "О государственных секретах";
5. Закон Республики Казахстан от 15 марта 1999 года 349-1 "О государственных секретах";
6. Закон Кыргызской Республики от 14 апреля 1994 года 1477-XII "О защите государственных секретов Кыргызской Республики";
7. Закон Республики Таджикистан от 22 апреля 2003 года "О государственной тайне";
8. Закон Республики Узбекистан от 7 мая 1993 года 848-XII "О защите государственных секретов".

Домбровская Л.А.

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

УТЕЧКА ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

В результате деятельности спецслужб по добыванию защищаемой информации им иногда удается получать несанкционированный доступ к секретной и конфиденциальной информации соперника и завладеть ею. Тем самым этот соперник (собственник или владелец информации) утрачивает монополию на владение и использование охраняемой им информации, и лишается, следовательно, всех преимуществ и выгод, вытекающих из этого.

Утрата собственником (владельцем) защищаемой информации ее монопольного использования расценивается обычно как утечка этой информации.

Иногда под утечкой информации понимается ее несанкционированное разглашение, выход ее за пределы круга лиц, которым эта информация была доверена. Однако одного этого признака недостаточно, чтобы считать факт утечки защищаемой информации состоявшимся. Основным признаком утечки информации все-таки должен считаться факт завладения защищаемой информацией субъектом, от которого информация защищается. Весь смысл затеваемой организации защиты информации состоит в предотвращении несанкционированного завладения защищаемой информацией именно определенными субъектами — это могут быть конкуренты, соперники, действительный или потенциальный противник. Информация защищается и от посторонних лиц, но лишь потому, что появление защищаемой информации в среде, не регламентированной режимными рамками, увеличивает вероятность завладения этой информацией теми лицами, от которых она защищается.

В процессе деятельности предприятия по защите информации может складываться ситуация, когда защищаемая информация выходит за пределы охраняемой специальными режимами сферы обращения, утрачивается контроль за ее обращением и распространением. Какие же последствия могут наступить для собственника секретной и конфиденциальной информации?

1. Защищаемая информация может попасть в руки противника или конкурента, от которого она охранялась. Тем самым ставится под угрозу возможность достижения системой, засекретившей информацию, поставленных целей. Собственнику этой информации наносится политический, материальный или моральный ущерб. Ему могут потребоваться дополнительные меры, в том числе экономического порядка, для ликвидации негативных последствий, наступивших в результате завладения соперником засекреченной информацией.

2. Защищаемая информация, хотя и вышла из-под контроля системы, в рамках которой она должна была обращаться, но к конкуренту не попала. Однако это обстоятельство не снимает угрозы

того, что эта информация может попасть к противнику. Какова вероятность того, что эта информация может стать достоянием соперника?

На основе логических оценок практики защиты информации можно высказать следующие версии:

а) защищаемая информация уже не охраняется и сопернику не составит труда «подобрать» эту бесхозную информацию и использовать в своих целях. Или же она может попасть в руки лиц, которые могут попытаться извлечь из владения этой информацией какие-то выгоды, например, продать ее конкуренту, шантажировать собственника информации или лицо, ответственное за ее хранение и т.д.;

б) несмотря на кажущуюся легкость получения соперником этой защищаемой информации, на самом деле может быть и не так. Конкурент может просто не знать, что какая-то защищаемая информация вышла из владения ее собственника и не будет пытаться заполучить ее. Соперник же по-прежнему будет пытаться получить информацию не из случайного источника, а там, где она постоянно находится, т.к. вероятность получения ее там гораздо выше;

в) защищаемая информация, вышедшая из-под контроля ее собственника, вообще может не интересовать соперника, и, следовательно, никак не может оказать влияние на достижение системой стоящих перед ней задач.

Исходя из сказанного, можно сделать вывод, что утечка защищаемой информации — это несанкционированное, неправомерное завладение соперником этой информацией и получение тем самым возможности использования этой информации в своих, в ущерб интересам собственника (владельца) информации целях. Наряду с утечкой информации следует параллельно рассматривать и различать такие понятия, как разглашение защищаемой информации, ее раскрытие и распространение.

Разглашение защищаемой информации — это несанкционированное ознакомление с этой информацией лиц, не имеющих законного доступа к ней, лицом, которому эти сведения были доверены или стали известны по службе или работе.

Разглашение может быть совершено: среди своих коллег, не имеющих доступа к данной информации; среди близких знакомых и родственников; среди других лиц. Разглашение информации, безусловно, создает реальную угрозу завладения такой информацией соперником. Но, тем не менее — это пока еще не утечка. Разглашение утечкой может не стать вообще.

Раскрытие защищаемой информации — это опубликование ее в средствах массовой информации, использование ее в выступлениях на публичных конференциях или симпозиумах, в том числе и международных, собственником или владельцем этой информации, или лицами, которым эта информация была доведена или стала известна по работе. В данном случае секретная и конфиденциальная информация становится достоянием неопределенно широкого круга лиц, утрачивает свою секретность, а, следовательно, ценность и потребительную стоимость как защищаемая информация.

Под распространением следует, по нашему мнению, понимать открытое использование этих сведений.

Каждый из приведенных видов выхода защищаемой информации из владения собственника может повлечь для него различные последствия.

Рассмотрим факторы, при наличии которых может произойти утечка информации.

1. Наличие противника, которого интересует данная секретная или конфиденциальная информация. Готовность его принимать меры, нести затраты на добывание этой информации, в том числе путем преодоления режимных мер, путем вербовки агентуры, создания или приобретения в этих целях технических устройств, специально приспособленных для добывания интересующей его и защищаемой от него информации. Если нет соперника, которого интересует данная информация, то вопрос должен стоять о том, что такую информацию нет смысла защищать.

2. Наличие носителей, содержащих интересующую соперника информацию. Носители секретной и конфиденциальной информации охраняются собственником информации. Конкуренты, преодолевая защитные меры, создают себе возможности получить несанкционированный доступ к этим носителям и превратить их тем самым в свои источники информации.

3. Наличие определенных причин и условий, создающих предпосылки и возможности для получения соперником несанкционированного доступа к защищаемой и интересующей его информации.

При организации защиты засекреченной информации постоянно обращается внимание на необходимость защиты носителей секретной и конфиденциальной информации, т.к. такая информация неотрывна от них, она не может существовать помимо носителя. И только получая доступ к носителю, соперник может добыть интересующую (и защищаемую собственником) информацию. Можно сделать вывод, что основная цель защиты информации сводится, в конечном счете, к тому, чтобы не позволить сопернику получить доступ к охраняемому носителю информации.

Однако в деятельности по защите информации постоянно возникают ситуации, когда на носители информации не «повесишь замок», не закроешь их в сейф, особенно в процессе их использования, а также когда ими являются люди, различного рода излучения, служащие

«продуктом» деятельности технических систем, каналов связи, излучением слаботочных приборов и т.д. Поэтому все эти носители являются потенциальными источниками утечки информации. К ним-то и стремится получить доступ соперник, прокладывая пути к интересующей его информации.

При рассмотрении причин утечки защищаемой информации следует проследить причинно-следственные связи и условия, при наличии которых причины начинают действовать. Причинность всех явлений в мире отражает всеобщую необходимую связь между предметами и явлениями. Все явления, события, процессы в природе, обществе и мышлении вызываются или обуславливаются другими явлениями, событиями, процессами, то есть более или менее определенными причинами'.

Если произошла утечка защищаемой информации, то, следовательно, этому есть определенные причины, т.е. совершились какие-то события, которые по времени предшествовали утечке и явились ее причиной, они «породили» эту утечку информации.

Таким образом, причины утечки защищаемой информации это те факторы и явления, которые складываются в процессе научно-производственной, управленческой или иной деятельности предприятия и его деятельности по защите информации, и которые создают предпосылки к утечке защищаемой информации.

Выделяют обычно две основные группы причин утечки информации:

1. Принятие недостаточных мер защиты информации:

- несовершенство нормативных актов, регламентирующих проблемы защиты информации, даже буквальное выполнение которых не гарантирует защищенность информации;
- недостаточность наличных сил и средств для перекрытия всех возможных каналов утечки информации.

2. Нарушения лицами, допущенными к работе с защищаемой информацией, правил защиты, что создает возможность и облегчает несанкционированный доступ к защищаемой информации.

Однако причины начинают действовать и наступают определенные последствия (в рассматриваемом случае — утечка информации) тогда, когда этому способствуют и соответствующие условия.

Условия, способствующие или создающие возможность утечки информации можно разделить на внутренние и внешние. Такая классификация является несколько условной. Внутренние условия в свою очередь можно разделить на субъективные и объективные. К субъективным условиям относятся:

- незнание конкретными исполнителями нормативных актов по вопросам защиты информации;
- слабая воспитательно-профилактическая работа в коллективе;
- недостаточное внимание со стороны руководителей к вопросам обеспечения режима секретности;
- слабый контроль за состоянием системы сохранения секретов;
- принятие руководителями решений по различным вопросам без учета требований режима секретности и конфиденциальности.

К объективным условиям относятся:

- несовершенство (или отсутствие) нормативных актов, регламентирующих правила защиты информации по отдельным вопросам;
- несовершенство Перечня сведений, подлежащих засекречиванию;
- текучесть кадров из режимных подразделений;
- несоответствие помещений требованиям, необходимым для ведения работ с секретными и конфиденциальными документами и изделиями и др.

К внешним условиям относятся:

- обширные связи предприятия со смежниками и поставщиками;
- частое участие сотрудников предприятия, осведомленных в секретной информации, в различных конференциях, симпозиумах и др.

Условия в совокупности тех элементов, которые создают предпосылки и возможности утечки информации, играют роль катализатора в процессе образования канала утечки защищаемой информации.

Канал утечки защищаемой информации — это социотехническое явление, отражающее и характеризующее противостояние, скрытую борьбу, соперничество двух и более субъектов (юридических или физических лиц). Если выигрывает защитник (собственник) защищаемой информации, тогда канала утечки информации не будет и соперник не сумеет получить несанкционированный доступ к носителям защищаемой информации.

Если же победа окажется на стороне конкурента, охотящегося за защищаемой информацией, прилагающего при этом усилия, затрачивающего силы и средства, чтобы получить несанкционированный доступ к носителям интересующей его секретной или конфиденциальной информации, превращая эти носители в источники информации, — канал утечки информации состоялся. Каналы утечки информации носят вероятностный характер.

Таким образом, канал утечки информации — это не техническое явление, устройство или система, а социальное, или учитывая, что социум у нас в настоящее время весьма технизирован, — социально-техническое явление.

В зависимости от используемых соперником сил и средств для получения несанкционированного доступа к носителям защищаемой информации различают каналы агентурные, технические, легальные, иные. Агентурные каналы утечки информации — это использование противником тайных агентов для получения несанкционированного доступа к носителям защищаемой информации. Технические каналы утечки информации — совокупность технических средств разведки, демаскирующих признаков объекта защиты и сигналов, несущих информацию об этих признаках. Легальные каналы утечки информации это использование соперником открытых источников информации (литературы, периодических изданий и т.п.), обратный инжиниринг, выведывание под благовидным предлогом информации у лиц, располагающих интересующей соперника информацией и других возможностей.

Иные каналы утечки информации — выдача конкуренту добровольно защищаемой информации лицами, имеющими доступ к такой информации по работе, экспортные поставки секретной продукции за рубеж и т.п.

Таким образом, устранение возможных каналов утечки секретной информации является одной из важнейших задач в комплексной системе защиты информации на предприятии.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ ISO/IEC 17799-2005 раздел «12.5.4. Утечка информации».
2. Петренко С. А., Курбатов В. А. Политики информационной безопасности. — М.: Компания АйТи, 2006.
3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. — М.: ДМК Пресс, 2008.

Журавков И.А.

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

ПОЛИГРАФ КАК СРЕДСТВО ПОЛУЧЕНИЯ ИНФОРМАЦИИ НА СТАДИИ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ

На современном этапе развития науки и техники высокие технологии, применяемые при производстве допроса, доказывают свою эффективность. Одним из наиболее известных средств инструментальной диагностики психоэмоциональных состояний, является полиграф («детектор лжи», lie-detector). В Российской Федерации полиграф широко применяется органами ФСБ и МВД как в ходе оперативно-следственных мероприятий, так и при работе с кадрами.

Первым государственным судебно-экспертным учреждением, где была освоена новая форма использования специальных знаний в целях оказания содействия правоохранным органам, помощи государственным и негосударственным учреждениям, а также гражданам стала Саратовская лаборатория судебной экспертизы Министерства юстиции РФ, в которой опросы с использованием полиграфа регулярно проводятся с 1998 года. Уголовные дела из числа направленных в суд, в ходе расследования которых использовался полиграф, успешно проходят стадию судебного разбирательства.

Правом проведения исследований с использованием полиграфа в ОВД обладают специально подготовленные сотрудники оперативно-технических и оперативных подразделений, прошедшие соответствующую подготовку и имеющие допуск к работе с полиграфными устройствами. Порядок их подготовки, получения ими допуска (свидетельства) на право работы с полиграфными устройствами регламентируется соответствующей инструкцией, утвержденной Приказом МВД РФ №353 от 12 сентября 1995 года.

Девятого февраля 1995 года МВД России издало квалификационные требования к специалистам, использующим полиграф при опросе граждан, и программу подготовки специалистов по работе с полиграфными устройствами при опросе граждан. В них определен перечень основных требований к квалификации, объему и уровню знаний и навыков, которыми должен обладать сотрудник оперативного или оперативно-технического подразделения для получения допуска к самостоятельной работе.

Известна уголовно-процессуальная модель использования полиграфа при допросе, предложенная В.И. Комиссаровым [1]. Суть ее состоит в «объединении» отдельных положений УПК РФ, касающихся проведения допроса, и инструкции о порядке использования полиграфа при опросе граждан. При этом допрос с использованием полиграфа должен проводиться только при наличии письменного согласия допрашиваемого, с привлечением специалиста соответствующей квалификации, в присутствии иных лиц (защитника, законного представителя и т.д.), если это предусмотрено законом и т.д. Программа тестирования (то есть использованные вопросники) и расшифрованная специалистом полиграмма прилагаются к протоколу допроса.

Э.У. Бабаева дополняет «модель» В.И. Комиссарова важными, с ее точки зрения, деталями, касающимися преимущественно организационно-тактических аспектов проведения допроса. В частности, предлагается проводить дополнительную подготовку специалистов-полиграфологов для

получения права проведения допросов (а не опросов) с использованием полиграфа. Соответствующая подготовка предполагается и для следователей. Расшифровка же полиграммы должна быть не приложением к протоколу допроса, а его полноценной частью [2].

Не стоит забывать, что окончательная юридическая оценка результатов тестирования производится не оператором полиграфа и уж тем более не самим прибором, а инициатором проведения опроса (то есть оперативным работником, следователем, прокурором или судом) с учетом имеющихся материалов уголовного дела и данных оперативно-розыскного характера.

Главным в эффективности применения полиграфа при раскрытии и расследовании преступлений является не технические особенности прибора, а качество подготовки специалистов.

Анализ существующих мнений приводит к выводу, что в условиях действующего уголовно-процессуального законодательства говорить о допросе с использованием полиграфа можно лишь в форме гипотетического суждения. Фактически речь идет уже не о допросе, а о совершенно новом следственном действии, в котором проявляется ряд новых существенных черт: изменяется порядок получения показаний (при допросе на полиграфе допрашиваемый должен давать лишь односложные ответы «Да» или «Нет»); роль специалиста в ведении следственного действия значительно возрастает, в то время как роль следователя, по сути, низводится к простому наблюдению и т.д. Эти и иные обстоятельства не позволяют «вписать» допрос с использованием полиграфа в рамки процессуальной формы традиционного допроса (ст. ст. 164, 173, 174, 187 – 191 УПК РФ) и требуют внесения значительных изменений в действующее уголовно-процессуальное законодательство.

Подытоживая сказанное, полагаем, что в российском уголовном процессе уже существуют возможности для проведения проверок с использованием полиграфа в двух формах: непроцессуальной (в форме ставшего уже традиционным опросом с использованием полиграфа как разновидности оперативно-розыскного мероприятия) и процессуальной (в форме судебной экспертизы).

Непроцессуальная форма применения полиграфа распространена достаточно широко. Результаты опроса с использованием полиграфа не являются доказательствами и используются как ориентирующая информация. В то же время они могут быть приобщены к уголовному делу: во-первых, путем допроса в качестве свидетеля специалиста, проводившего исследование; во-вторых, путем приобщения документа о результатах исследования к уголовному делу в порядке ст. 84 УПК РФ.

В настоящее время применение полиграфа в рамках экспертных исследований не носят массовый характер. Причины подобного положения заключаются не столько в правовой регламентации (отсутствие прямого законодательного регулирования применения полиграфа в уголовном процессе), сколько в характере психологического «барьера», обусловленного новизной метода, трудностями в плане отношения и доверия к нему и результатам его использования. В перспективе, с накоплением опыта положительных результатов и реальной помощи в раскрытии и расследовании преступлений востребованность метода, безусловно, возрастет.

СПИСОК ЛИТЕРАТУРЫ

1. Комиссаров В.И. Использование полиграфа в борьбе с преступностью // Законность. 1995. № 11. С. 47.
2. Бабаева Э.У. Предупреждение изменения показаний подследственным и свидетелем на предварительном расследовании. М.: Экзамен, 2001. С. 50–52.

Никишкин А.В., Оськин Ф.Ф.

**Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ СИСТЕМЫ ФУНКЦИОНИРОВАНИЯ
ПОДРАЗДЕЛЕНИЙ ГОСУДАРСТВЕННОЙ ИНСПЕКЦИИ БЕЗОПАСНОСТИ
ДОРОЖНОГО ДВИЖЕНИЯ ГОРРАЙОРГАНОВ ВНУТРЕННИХ ДЕЛ**

В последнее время в Российской Федерации наметился серьезный рост количества автомобильного транспорта. Всё это стало следствием развития экономики нашей страны, повышения общего благосостояния населения. Увеличение количества связей требует всё большего использования транспорта, как средства быстрого и надёжного межсубъектного взаимодействия в различных сферах: политической, социальной, экономической и других. Однако подобное увеличение количества транспорта, «имеет и негативные стороны», так как «существенными отрицательными последствиями автомобилизации является резкое повышение аварийности на автомобильном транспорте» [1].

Всё это является следствием объективных и субъективных факторов. Объективные факторы возникают в результате функционирования дорожных служб (например, низкое качество дорожного полотна, посторонние предметы на проезжей части дорог), действий водителей и пешеходов, вызванных низкой правовой культурой, а порой и правовым нигилизмом. Такого рода факторы являются результатом комплексных проблем, а потому требуют именно системного решения разнообразных государственных органов, а также и населения. Субъективные факторы носят конкретный характер и возникают именно по причине существования различных проблем в рамках

государственных органов, непосредственно отвечающих за безопасность дорожного движения, а именно в рамках Государственной инспекции безопасности дорожного движения.

Эти субъективные факторы целесообразно рассматривать с двух позиций. С одной стороны, их возникновение неразрывно связано с несоответствием модели ГИБДД, существующей в настоящий момент, с требованиями современности. Подразделения Государственной инспекции безопасности дорожного движения во многом продолжают функционировать с применением тех методов и средств, которые использовались в советское время. Излишняя бюрократизация, опора на использование огромного количества документов в деятельности ГИБДД, резко снижает оперативность и готовность этих подразделений к решению тех проблем, которые возникают на дорогах России в настоящее время. С другой стороны ГИБДД, как и многие другие органы государственной власти поразили проблемы коррупции, мздоимства [2].

Таким образом, проблема современной самоидентификации Государственной инспекции безопасности дорожного движения, тесно связана с несоответствием функционального компонента по форме и содержанию в деятельности ГИБДД. В то время, когда с формальной стороны инспекция функционирует не по рыночной, а по «советской» схеме, не задействует позитивные рыночные методы и средства, используемые в различных коммерческих организациях, с содержательной стороны такие «теневые» рыночные механизмы имеют место, что усугубляет проблемы развития Государственной инспекции безопасности дорожного движения в Российской Федерации. На это указывается во многих современных изданиях, «необходимо отказываться от старых, изживших себя методов управления государственной системой обеспечения безопасности дорожного движения, требуется проводить разработки в организационно-правовых направлениях её совершенствования в условиях построения правового государства и перехода страны к рыночной экономике» [1].

Важнейшим компонентом самоидентификации Государственной инспекции в области обеспечения безопасности дорожного движения, является определение целей и задач. В данной статье рассматривать этот аспект мы будем на примере подразделений ГИБДД горрайорганов внутренних дел.

Произошедшие кардинальные изменения в нашей стране, а именно реорганизация существующей ранее структуры Государственной автомобильной инспекции в Государственную инспекцию безопасности дорожного движения, привели к расширению объема задач данного подразделения Министерства внутренних дел, изменению их содержания, так административный надзор становится одним из способов обеспечения законности в управлении и наряду с контролем охватывает практически все сферы жизни общества. Особенно данные изменения заметны на примере горрайорганов внутренних дел и их структурных элементов – отделов (отделений) ГИБДД.

Подразделения ГИБДД горрайорганов внутренних дел, «самое многочисленное звено системы ГИБДД МВД России, являющейся составной частью государственной системы обеспечения безопасности дорожного движения, осуществляющей специальные контрольные, надзорные и разрешительные функции в сфере обеспечения безопасности дорожного движения, на территории того или иного муниципального образования (города, района, иного населённого пункта)» [3].

Прежде всего, подразделения ГИБДД являются, с точки зрения теории государства и права, органами исполнительной власти. В пределах своей компетенции данные органы имеют необходимую для их нормального функционирования оперативную самостоятельность, а их специализированные задачи закрепляются в соответствующих нормативно-правовых актах. По своему уровневому положению подразделения ГИБДД горрайорганов внутренних дел принадлежат к местным органам, деятельность которых ограничивается рамками одной или нескольких административно-территориальных единиц (района, города, муниципального образования и т.п.).

Профессор А.В. Поляков указывает, что «орган государства – это часть государственного аппарата, образуемая в установленном порядке, наделённая властными полномочиями и действующая в пределах установленной компетенции», а исполнительные органы (в том числе и подразделения ГИБДД) «выступают как непосредственные исполнители требований, содержащихся в государственных правовых актах», кроме того, «они осуществляют распорядительную деятельность, которая выражается в обеспечении выполнения сформулированных в государственных актах требований, всеми субъектами права» [4].

Определяющим в уяснении оперативной самостоятельности, а так же в рассмотрении правового статуса таких подразделений, является очерчивание основных направлений их деятельности – функций. Что такое функция? Словарь Ожегова даёт нам четыре определения этого слова, из которого внимания заслуживают только два. Во-первых, функция – это «работа, производимая органом, организмом, роль, значение чего-нибудь». Во-вторых, функция – это «обязанность, круг деятельности». Таким образом, в первом случае речь идёт о деятельности (то есть о том, что происходит на самом деле – материальной стороне), а во втором – о предписанной, необходимой (то есть, о формальной стороне). Опираясь на эти два определения, можно сделать вывод, что функция – определённое направление деятельности органа, которое предписано

определенными нормативными актами или вышестоящими органами и должностными лицами. Теоретик права М.Н. Марченко указывает, что «термин – функция, имеет в отечественной и зарубежной литературе далеко не одинаковое значение». Так, «в философском и общесоциологическом плане он рассматривается как:

- внешнее проявление свойств какого-либо объекта, в данной системе отношений»;
- совокупность обычных и специфических действий отдельных лиц и органов, обусловленных их природой или необходимостью выживания;
- наличие у отдельного лица или группы лиц, специфических обязанностей, выполнение которых им предписывается в процессы выполнения ими служебной деятельности (функции врача, полисмена и т.д.).

В последнем случае функция воспринимается как служебная, профессиональная или любая иная потребность или обязанность действовать в соответствии с существующими правовыми и моральными установками и «в соответствующей манере» [5].

В данной статье функции рассматриваются как «основные направления деятельности, предписанные определёнными нормативными правовыми актами». Когда речь идёт о подразделениях ГИБДД горрайорганов внутренних дел, то «краеугольным камнем» является Типовое положение об Отделе (отделении) Государственной инспекции безопасности дорожного движения Управления (отдела) внутренних дел района, города, округа, района в городе, утверждённое Приказом МВД России от 28 сентября 1998 года № 618 в целях обеспечения реализации единой государственной политики в области безопасности дорожного движения, совершенствования правовых основ организации деятельности Государственной инспекции безопасности дорожного движения Министерства внутренних дел Российской Федерации.

Так, именно основные задачи, указанные в разделе II Типового положения, и определяют основные функции подразделений ГИБДД горрайорганов внутренних дел.

Непосредственно сами функции указаны в разделе III Типового положения. Таким образом, в ходе реализации своих функций Отдел (отделение) ГИБДД горрайоргана внутренних дел:

- контролирует в рамках полномочий Государственной инспекции, соблюдение требований нормативных правовых актов в области обеспечения безопасности дорожного движения;
- согласовывает разрешения органов местного самоуправления на распространение наружной рекламы на территории городских и сельских поселений, в полосе отвода и придорожной зоне автомобильных дорог, за пределами указанных поселений, контролирует её размещение, а также размещение рекламы на автотранспортных средствах;
- принимает квалификационные экзамены на получение права управления автотранспортными средствами, трамваями и троллейбусами, выдаёт водительские удостоверения, а также другие документы, необходимые для допуска граждан к управлению автотранспортными средствами;
- регистрирует и ведёт учёт автотранспортных средств и прицепов к ним, осуществляет выдачу государственных регистрационных знаков, регистрационных и других документов на зарегистрированные транспортные средства и прицепы к ним, необходимые для допуска к участию в дорожном движении;
- организует и проводит в установленном порядке государственный технический осмотр автотранспортных средств и прицепов к ним;
- изучает условия дорожного движения, принимает меры к их совершенствованию. Регулирует дорожное движение, в том числе с использованием технических средств и автоматизированных систем, организует движение транспортных средств и пешеходов в местах проведения массовых мероприятий, а также ремонтно-строительных, аварийно-спасательных и других работ;
- участвует в мероприятиях по охране общественного порядка и обеспечению общественной безопасности, пресечении и раскрытии преступлений и иных противоправных проявлений, связанных с использованием автотранспортных средств;
- организует и проводит в порядке, определённом МВД России, мероприятия по розыску угнанных и похищенных автотранспортных средств, а также автотранспортных средств участников дорожного движения, скрывшихся с мест дорожно-транспортных происшествий;
- осуществляет в соответствии с законодательством Российской Федерации дознания по делам о преступлениях, против безопасности дорожного движения и преступлениях, связанных с эксплуатацией транспортных средств, а также производством по делам об административных правонарушениях в области безопасности дорожного движения;
- осуществляет неотложные действия на местах дорожно-транспортных происшествий, в том числе по эвакуации людей и оказанию им доврачебной медицинской помощи, а также содействует транспортировке повреждённых транспортных средств и охране имущества, оставшегося без присмотра;

- ведёт учёт бланков водительских удостоверений, государственных регистрационных знаков транспортных средств, справок-счетов и другой специальной продукции, необходимой для допуска граждан к управлению транспортными средствами и транспортных средств к участию в дорожном движении;
- согласовывает в установленном порядке проекты организации дорожного движения в городах и на автомобильных дорогах;
- сопровождает в установленном порядке транспортные средства;
- участвует в установленном порядке в работе градостроительных и технических советов, комиссий по приёмке в эксплуатацию дорог, дорожных сооружений, железнодорожных переездов, линий городского электрического транспорта;
- рассматривает заявки и выдаёт заключения на открытие маршрутов регулярного движения общественного транспорта;
- проводит работу по разъяснению требований нормативных правовых актов по вопросам безопасности дорожного движения с использованием средств массовой информации, проводит в этих целях смотры, конкурсы, соревнования. Содействует органам местного самоуправления в обучении граждан правилам безопасного поведения на дороге;
- разрабатывает предложения по повышению безопасности дорожного движения, вносит их в установленном порядке в органы местного самоуправления, юридическим лицам и в иные организации, способствует их реализации;
- осуществляет совместно с органами местного самоуправления, юридическими лицами и иными организациями мероприятия по профилактике детского дорожно-транспортного травматизма;
- разрабатывает проекты правовых актов УВД, ОВД по вопросам, отнесённым к компетенции Государственной инспекции, участвует в разработке проектов правовых актов соответствующего органа местного самоуправления по вопросам обеспечения безопасности дорожного движения;
- осуществляет сбор и обобщение информации о состоянии безопасности дорожного движения, а также деятельности подразделений Государственной инспекции на территории соответствующего района, города, округа, района в городе, ведёт в установленном порядке государственный учёт показателей состояния безопасности дорожного движения;
- анализирует причины и условия, способствующие совершению дорожно-транспортных происшествий, нарушений правил дорожного движения и иных противоправных действий, влекущих угрозу безопасности дорожного движения, принимает меры по их устранению;
- выдаёт в установленном порядке разрешения на оборудование транспортных средств, специальными световыми и звуковыми сигналами;
- рассматривает жалобы и заявления по вопросам деятельности Государственной инспекции;
- осуществляет взаимодействие с другими подразделениями органов внутренних дел, органами местного самоуправления, военной автомобильной инспекцией, юридическими лицами и иными организациями по вопросам, отнесённым к компетенции Государственной инспекции [6].

Сказанное позволяет сделать вывод, что в настоящее время деятельность подразделений ГИБДД горрайорганов внутренних дел не в полной мере удовлетворяет работе, по решению возложенных на неё задач и функций по обеспечению безопасности дорожного движения. Такое положение обусловлено многими факторами: и это недостаточно конкретное нормативно-правовое закрепление основных задач, возлагаемых на ГИБДД и не в полном объёме организованное регулирование функций этих органов, что не позволяет им эффективно воздействовать на участников дорожного движения [3]. И именно от определения места подразделений ГИБДД горрайорганов внутренних дел в обеспечении безопасности дорожного движения, выявления и корректировки их функций, и будет зависеть повышение безопасности дорожного движения на дорогах нашей страны в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Никишкин А.В. Безопасность дорожного движения – главная задача государства // Психология обеспечения правопорядка и безопасности; Материалы международной научно-практической конференции. Санкт-Петербург, 21–23 мая 2008 г. / Сост.: Пряхина М.В., Корчмарюк В. А., Андреева И.А, Статный В.М. СПб.: Изд-во СПб ун-та МВД России, 2008. С. 241.
2. Организация деятельности Государственной инспекции безопасности дорожного движения МВД России. Альбом схем: Учебное наглядное пособие / МВД России СПбУ; Сост.: Е.В. Болотина и др. Под ред. В.П. Сальникова. СПб., 2004. 96 с.
3. Никишкин А.В. Отделы ГИБДД горрайорганов внутренних дел, пути совершенствования их деятельности // Психология обеспечения правопорядка и безопасности; Материалы международной научно-практической конференции. Санкт-Петербург, 21–23 мая 2008 г. / Сост.: Пряхина М.В., Корчмарюк В.А., Андреева И.А, Статный В.М. СПб.: Изд-во СПб ун-та МВД России, 2008. С. 239.
4. Поляков А.В. Общая теория права. Курс лекций. СПб.: Издательство «Юридический центр Пресс», 2001. С. 378–379.
5. Марченко М.Н. Теория государства и права: Учебник. 2-е изд., перераб. и доп. М.: ТК Велби, Изд-во проспект, 2006. С. 327.
6. Газизов Ф.А. Задачи и основные направления деятельности Государственной инспекции безопасности дорожного движения в современных условиях: Лекция / МВД России, ВПГК. Домодедово, 2001. 38 с.

Ороева О.Д.

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

СОСТОЯНИЕ НОРМАТИВНОГО ПРАВОВОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПРАВ И СВОБОД ЧЕЛОВЕКА И ГРАЖДАНИНА, РЕАЛИЗУЕМЫХ В ИНФОРМАЦИОННОЙ СФЕРЕ

Информационная безопасность Российской Федерации – это состояние защищенности интересов Российской Федерации в информационной сфере. Информационная сфера представляет собой совокупность субъектов информационной сферы, информации, информационной инфраструктуры, системы сбора, формирования, обработки, распространения и использования информации, а также системы регулирования возникающих при этом общественных отношений. Интересы Российской Федерации в информационной сфере определяются, прежде всего, исходя из следующего: информационная сфера играет ключевую роль в реализации многих конституционных прав и свобод граждан, в обеспечении возможности самореализации личности, духовном обновлении, политической и социальной стабильности общества, обеспечении функционирования государства и становится все более важным фактором развития экономики Российской Федерации и мировой экономики в целом; жизнедеятельность человеческого общества во все большей степени зависит от информационной сферы, которая, в связи с этим, все активнее используется отдельными государствами, международными, террористическими и преступными группами для оказания "силового" давления на государственную политику тех или иных стран. Интересы Российской Федерации в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа. Обеспечение интересов Российской Федерации в информационной сфере предполагает достижение следующих трех целей:

- соблюдение конституционных прав и свобод граждан в области духовной жизни и информационной деятельности, обеспечение духовного возрождения России;
- развитие отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Защита интересов Российской Федерации в информационной сфере от угроз внешнего и внутреннего характера составляет основное содержание деятельности по обеспечению информационной безопасности Российской Федерации. Угрозы конституционным правам и свободам граждан в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России проявляются в виде: недостаточной разработанности нормативной базы, определяющей порядок реализации правовых норм, регулирующих отношения в информационной сфере; создания монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем; противодействия, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на охрану личной и семейной тайны, тайны переписки, телефонных переговоров и иных сообщений; нерационального, чрезмерного закрытия общественно необходимой информации; противоправного применения специальных средств воздействия на индивидуальное, групповое и общественное сознание; неисполнения органами государственной власти, организациями и гражданами требований законодательства Российской Федерации, регулирующего отношения в информационной сфере; неправомерных ограничений доступа граждан к открытым государственным информационным ресурсам органов государственной власти, к архивным материалам и другой социально значимой информации; дезорганизации и разрушения системы накопления и сохранения культурных ценностей, включая архивы; нарушений конституционных прав человека и гражданина на свободу массовой информации, а также недостаточного нормативного правового регулирования отношений в области реализации конституционных ограничений этой свободы; вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиления зависимости духовной жизни страны, экономической и политической сфер общественной жизни России от зарубежных информационных структур; пропаганды образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих нормам, принятым в российском обществе; снижения уровня образованности граждан, существенно осложняющего подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных; манипулирования информацией (дезинформация, сокрытие или искажение информации).

Основными источниками права в области обеспечения гарантий прав и свобод человека и гражданина являются Конституция Российской Федерации, Европейская конвенция о защите прав и

основных свобод, "Всеобщая декларация прав человека", другие международные нормативные правовые акты, признанные Российской Федерацией и регулирующие отношения в рассматриваемой области, решения Конституционного Суда Российской Федерации, Уголовный кодекс Российской Федерации, Гражданский кодекс Российской Федерации, Кодекс РФ об административных правонарушениях, Закон Российской Федерации "О средствах массовой информации", Федеральный закон "Об информации, информатизации и защите информации", Закон Российской Федерации "О государственной тайне", Федеральный конституционный закон "Об уполномоченном по правам человека в Российской Федерации", некоторые другие федеральные законы и подзаконные нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

Зафиксированные в данных нормативных правовых актах правовые нормы обеспечения гарантий прав и свобод человека и гражданина в целом оказывают положительное влияние на состояние защищенности интересов Российской Федерации в этой области.

К числу основных недостатков нормативного правового обеспечения защиты прав и свобод человека и гражданина в информационной сфере следует отнести: неопределенность правовых механизмов обеспечения доступа к открытой информации органов государственной власти и органов местного самоуправления, что создает условия для ущемления прав и свобод человека и гражданина, включая право на информацию о состоянии окружающей среды, фактах и обстоятельствах, представляющих угрозу для жизни и здоровья людей; отсутствие правовых норм, устанавливающих ответственность за ограничение или нарушение права на доступ к открытой информации; отсутствие правового регулирования общественных отношений в области сбора и использования персональных данных, механизмов их внесудебной защиты, реализации права на личную и семейную тайны, неприкосновенность частной жизни, защиту своей чести и доброго имени, тайну переписки, телефонных переговоров, телеграфных и иных сообщений; недостаточную согласованность и полноту правовых норм, регулирующих установление режимов ограничения доступа к информации, обязанностей субъектов правоотношений по защите информации с ограниченным доступом, ответственности за нарушения установленных режимов ограничения доступа к информации; неурегулированность прав государства на объекты интеллектуальной собственности, полученные в результате выполнения работ, полностью или частично финансируемых за счет средств государственного бюджета, а также недостаточное правовое регулирование общественных отношений в области охраны таких объектов интеллектуальной собственности, как ноу-хау, изобретения, составляющие государственную или служебную тайны, фирменные наименования; недостаточное развитие правового регулирования отношений, связанных с ограничением распространения массовой информации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства; отсутствие правового регулирования распространения информации, предназначенной для неограниченного круга потребителей, в открытых информационно-телекоммуникационных сетях.

На основании вышеизложенного, для оказания положительного влияния на состояние защищенности интересов Российской Федерации в области обеспечения гарантий прав и свобод человека и гражданина, необходимо совершенствование системы международных договоров и нормативных правовых актов международных организаций, участником которых является Российская Федерация, по направлениям:

- организация взаимодействия правоохранительных органов различных государств в области предупреждения, выявления и пресечения преступлений в сфере информационных технологий;
- защита законных интересов человека и гражданина, связанных с безопасностью информационного обмена, обеспечением неприкосновенности частной жизни, личной и семейной тайны, тайны сообщений в глобальных информационно-телекоммуникационных системах.

А также, необходимо совершенствование российского законодательства по направлениям:

- установление унифицированного перечня оснований для ограничения права на доступ к информации, перечня видов информации с ограниченным доступом и механизмов реализации этих ограничений, принципов и организационных механизмов доступа к открытой информации органов государственной власти, органов местного самоуправления, общественных организаций и хозяйствующих субъектов;
- регулирование общественных отношений в области сбора, хранения и использования (распространения) персональных данных, защиты личной и семейной тайны, неприкосновенности частной жизни;
- внесение изменений и дополнений в законодательство Российской Федерации, регуливающее общественные отношения в области обеспечения конституционных прав и свобод человека и гражданина, реализуемых в информационной сфере, в целях конкретизации механизмов наступления ответственности за нарушение содержащихся в них правовых норм, устранения имеющихся противоречий;

- усиление правовой охраны объектов интеллектуальной собственности, в том числе ноу-хау, изобретений, составляющих служебную и государственную тайну, фирменных наименований, а также закрепление права государства на объекты интеллектуальной собственности;
- конкретизация правовых механизмов недопущения пропаганды или агитации, возбуждающих социальную, расовую, национальную и религиозную ненависть и вражду; создание государственной системы контроля за оборотом специальных технических средств негласного получения информации;
- определение порядка использования государственных информационных ресурсов, включая ресурсы музеев, библиотек и архивных фондов, а также создание правового механизма предотвращения и пресечения их неправомерного использования; регулирование общественных отношений, связанных с распространением массовой информации по каналам радио- и телевидения, включая предотвращение монополизации деятельности в области массовой информации.

Осипов Я.В.

Россия, Архангельск, Следственное управление при УВД по Архангельской области
КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ ДИАГНОСТИКИ ЛЖИ

Бурное развитие в последнее десятилетие компьютерных технологий и микроэлектроники вызвало создание нового класса приборов для диагностики лжи – **компьютерных полиграфов**. Появление мощных персональных мультимедийных компьютеров и использование операционной системы MS Windows для создания программного обеспечения делает полиграфы универсальным и доступным инструментом для исследовательских целей. Использование стандарта IBM PC PENTIUM позволяет пользователю, имея базовую комплектацию таких приборов, самостоятельно дополнять и обновлять ее новейшими разработками в области вычислительной техники и программного обеспечения. В существующем виде полиграф представляет собой точный прибор, достоверно отражающий психофизиологическое состояние организма испытуемого. Развитие новых областей науки и техники (в частности автоматизации, кибернетики и искусственного интеллекта, космической медицины и пр.) открыло широкие перспективы для совершенствования полиграфа. Стало возможным принципиально изменить технику «снятия» информации, используя метод бесконтактных датчиков.

Под бесконтактными датчиками понимают такие, действие которых испытуемым не ощущается или даже сам факт существования которых для испытуемого остается неизвестным.

В психофизиологических экспериментах различают три группы таких датчиков:

- датчики, вмонтированные в предметы одежды (халат, комбинезон, головной убор, пояс) либо такие предметы, как часы, компас;
- датчики, вмонтированные в орудия труда (пишущий прибор, рукоятка управления механизмом или аппаратом, тетрадь для записей и др.);
- датчики, вмонтированные в элементы бытового оборудования (кресло, кровать, стул) [2, с. 343].

Датчики с успехом используются для контроля за состоянием космонавтов в условиях полета, при изучении реакций испытуемых в процессе их профессионального отбора и т. п.

Полиграф – прибор для объективной регистрации психофизиологических реакций, сопровождающих изменения в нервной системе, которые возникают во время любого психического акта или состояния. В то время, когда протекает психический процесс, происходит множество явлений, которые можно зарегистрировать с помощью специальных датчиков и приборов. Психический процесс сопровождается сложной комбинацией электромагнитных и биохимических реакций. Некоторые реакции имеют генерализованный характер, охватывают самые различные системы организма, отчетливо и однозначно интерпретируются. В качестве примера можно привести ориентировочные и оборонительные рефлексy, стрессовые и эмоциональные реакции. Другие реакции имеют локальный характер и регистрируются в специфических областях мозга. Например, восприятие зрительной или слуховой информации отражается только в динамике суммарной активности мозга и регистрируется с помощью метода вызванных потенциалов.

Современный компьютерный полиграф представляет собой переносной персональный компьютер с сенсорным блоком и датчиками съема информации. Сенсорный блок предназначен для снятия сигналов с датчиков, регистрирующих информацию о физиологических процессах, усиления и фильтрации этих сигналов, преобразования их в цифровой код и передачи его на персональный компьютер. Для регистрации физиологических данных используются датчики верхнего (грудного) и нижнего (брюшного) дыхания, сердечно-сосудистой активности: пульса, ПГ, АД и датчики электрокожной проводимости (сопротивление кожи, КГР) [4, с. 56].

Одновременный контроль указанных физиологических процессов в ходе психофизиологического исследования является строго обязательным: согласно существующим международным стандартам, исключение из контроля хотя бы одного из этих процессов делает

процедуру проверки на полиграфе невалидной. Остальные датчики, включаемые в комплектность разных моделей полиграфов, несут вспомогательную функцию:

- датчики тремора используются для фиксации двигательной активности обследуемого;
- голосовой датчик (микрофон) используется для точной фиксации моментов вопроса – ответа и для записи фонограммы опроса.

Программа обеспечивает формирование в редакторе Word текстовых файлов тестов, результатов компьютерного тестирования, результатов балльной и метрической оценки. На принтере происходит отображение графиков физиологических показателей, зарегистрированных реактограмм.

Главная идея, лежащая в основе работы детектора лжи заключается в том, что человеческое подсознание от природы «запрограммировано» выдавать правдивую информацию, сколь нелицеприятной она бы ни была. Когда человек пытается солгать, возникает стресс, который находит свое отражение во всех физиологических реакциях человека. Исходя из определения, детектор лжи предназначается для непрерывного считывания и фиксации таких физиологических процессов человека, результаты записи могут быть отражены полиграммой.

Система по выявлению противодействия используется с компьютерным полиграфом для обнаружения попыток физического и умственного противодействий обследуемого в течение полиграфной проверки. Программное обеспечение служит для записи форм голосовых волн произведенных обследуемым и полиграфологом. Эти формы волн затем анализируются программным обеспечением для того, чтобы помочь полиграфологу установить результат проверки на детекторе лжи. На рисунке 1 отображены графики получения основных данных, снимаемых во время тестирования [2, с. 346].



грудное дыхание



брюшное дыхание



кожно-гальваническая реакция



сердечно-сосудистая активность



тремор



Голос

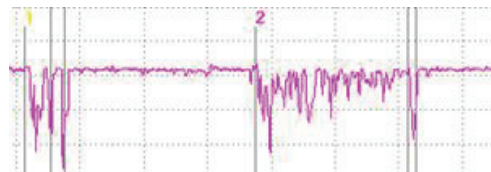
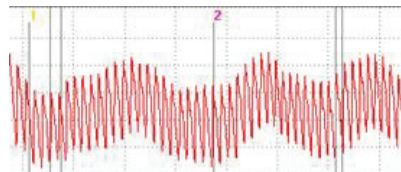
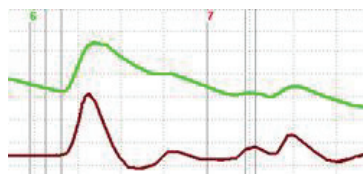
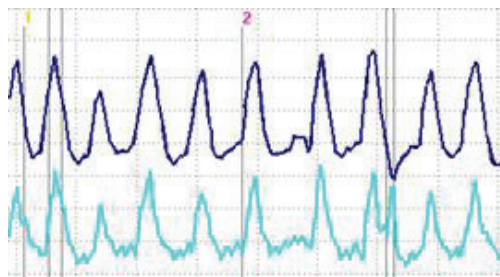


Рис. 1. Датчики и графики физиологических показателей тестирования

Сканер отпечатков пальцев для компьютерных полиграфов позволяет полиграфологу проводить запись отпечатков пальцев обследуемого лица, проходящего проверку на детекторе лжи. Этот сканер функционирует с персональными компьютерами и ноутбуками.

При выборе конфигурации мультимедийного компьютера следует обратить внимание на следующие характеристики. Корпус системного блока должен иметь достаточно места для его расширения дополнительными платами. Для одновременной регистрации полисомнограммы и видеоизображения необходим большой объем жесткого диска и оперативной памяти. Для создания архива – записывающий CD-ROM или магнитооптическое устройство памяти. Для создания локальной сети и подключения к Интернету требуются соответствующие платы.

Для визуализации и анализа данных обычно используют большой монитор с высоким разрешением, а для анализа видеоизображения иногда используют дополнительный монитор. При наличии усилителя не требующего сетевого питания, возможна работа в полевых условиях с использованием компьютера типа note-book с батарейным питанием. Использование для полиграфа мультимедийного компьютера позволяет пользователю самостоятельно комплектовать прибор новейшими разработками в области вычислительной техники по доступным ценам. Например, для стимуляции и анализа деятельности испытуемых возможно подключение дополнительных мониторов, звуковых карт, динамиков, микрофонов, джостиков и других специализированных периферических устройств.

Для оценки изменений кровоснабжения отдельных участков поверхности лица, прежде всего в области глаз, используются тепловизоры. Изменения в кровоснабжении лица не всегда бывают очевидными. Главная цель использования тепловизоров – обнаружение кратковременных изменений кровотока, обусловленных активностью симпатической нервной системы. Очевидным преимуществом использования тепловизоров в детекции лжи является возможность их использования скрытно от обследуемого лица, поскольку они предназначены для дистанционной регистрации теплового излучения изучаемых объектов. Однако серьезным недостатком данного подхода является необходимость специальных преобразований термоизображений для получения сведений о происходящих изменениях температуры. Зарегистрированные тепловизором сигналы должны подвергаться серьезной компьютерной обработке, прежде чем можно будет их интерпретировать.

В Институте полиграфа Министерства обороны США (Department of Defense Polygraph Institute – DoDPI) в 2002 году было проведено исследование в формате так называемого «мнимого преступления» (mock crime), в ходе которого часть испытуемых-добровольцев «наносили удар ножом» манекену и затем «грабили» его, а другая часть была только проинформирована о «преступлении». В ходе последующего допроса по результатам термографического исследования удалось правильно определить 83% как «причастных к преступлению», так и «непричастных» испытуемых. В другом исследовании, проведенном в том же году, тепловизор использовался в качестве дополнительного канала информации в процессе проведения обследования на полиграфе. Полученные данные в целом показали, что в качестве независимого метода термография обладает меньшей точностью, чем полиграф, тогда как их совместное использование повышало эффективность диагностики лжи. Пока еще не разработана теория, которая обосновывала бы применение тепловизоров для целей детекции лжи. Высказывается мнение о ведущей роли ориентировочного рефлекса в изменении кровоснабжения и микроциркуляции крови в процессе лжи. Так, ранее Е. Соколовым было показано, что уменьшение кровотока в области лба при воздействии угрожающих стимулов является компонентом оборонительной реакции. Реакция же на новые стимулы, наоборот, сопровождается увеличением кровоснабжения в области лба, что может быть связано с механизмами ориентировочного рефлекса, направленными на улучшение восприятия. Оба эти явления могут быть положены в основу объяснения изменения температуры кожи лица, сопровождающие ложные высказывания.

Измерение зрачковой реакции не является современным изобретением в психофизиологии. Известно, что расширение зрачка происходит в результате стимуляции симпатической нервной системы или снижения активности парасимпатической нервной системы, то есть имеет в своей основе те же механизмы, которые лежат в основе психофизиологической детекции лжи. Оценка зрачковой реакции используется в целом ряде прикладных направлений, таких как отвыкание от героина, оценка уровня умственной нагрузки или исследование различных аспектов памяти.

Первые попытки использования зрачковой реакции в детекции лжи были предприняты в начале 40-х годов прошлого века. Эти ранние исследования показали, что в процессе лжи действительно наблюдаются изменения размера зрачка. В частности, было показано, что зрачковая реакция возникает при ответах на все вопросы, относящиеся к преступлению, однако она более выражена при ложных ответах на них. Всем известны крылатые выражения «глаза – зеркало души», «глаза не лгут». Некоторые люди владеют способностью определять ложь по глазам, а в настоящее время появилась техническая возможность автоматизировать этот процесс. Анализ движений глаз – популярное направление исследований в современной науке. Мнения специалистов, изучающих процессы зрения, единодушно сходятся на том, что глаза – это вынесенный вперед мозг, т.е. глаза непосредственно отражают мыслительные процессы, которые происходят в мозгу.

Анализ движения глаз ведется в двух направлениях:

- первое – анализ движения в зависимости от предложенных визуальных стимулов (например, рекламных плакатов), доказано, что движения глаз при восприятии привлекательных и не очень образов отличаются друг от друга;

- второе – анализ движения в зависимости от внутренних мыслительных процессов вне зависимости от того, куда смотрит человек.

Допустим, когда человек задумается, его взор устремлен внутрь себя, и он не видит, что происходит вокруг. Так же экспериментально подтверждено, что возможно измерение мыслительных процессов (например, принятие трудного решения) и психологического состояния (тревоги) человека по характеру движения глаз.

Большинство из нас считает, что характер движений глаз – плавный. Однако при внимательном изучении мы убеждаемся в том, что глаза совершают так называемые саккадические движения. Эти движения представляют собой смену остановок (фиксаций) и скачков глаз. Восприятие информации происходит только в момент фиксаций. На них при восприятии приходится основное время – 92–94 процента, остальное время занимают скачки – перемещения взгляда с одного участка визуального образа к другому. При этом глаза действуют подобно кинокамере. Они как бы снимают неподвижные кадры, а затем проецируют их на экран (в мозг). Впечатление непрерывности создается за счет особенности глаз сохранять видимое изображение на сетчатке глаза. Длительность фиксации складывается из времени, необходимого для восприятия участка образа, и времени, требующегося для его осмысления как части целого.

Движения глаз человек обычно не осознает. Одна из причин этого – отсутствие так называемой осознаваемой, произвольно управляемой обратной связи, посредством которой в мозг передавались бы сообщения о микродвижениях глаз. Человек узнает о направлении своего взгляда лишь по положению наблюдаемых объектов и под влиянием некоторых других факторов, например поворота или наклона головы. Тем не менее, произвольные движения глаз играют большую роль в зрительном восприятии. Не случайно исследователи, оценивая комплекс процессов, происходящих в зрительной системе человека, отмечают: «Мы часто не знаем, что видим, пока не узнаем, на что мы смотрим». При взгляде на определенный объект глаз совершает по его контуру регулярные скачки с частотой 2 – 5 раз в секунду.

Длительность фиксаций во многом зависит от сложности деятельности. При этом имеется ввиду внешний план деятельности, связанный с информационным поиском и восприятием визуальной информации. Кроме фиксаций, которые предполагают неподвижность взгляда и, соответственно, глаз относительно некоторого внешнего объекта, существуют медленные, дрейфовые движения глаз, приводящие к смещению взгляда по объекту.

Раскрытие более сложных психических процессов происходит в случае, который можно обозначить, как «отстройка от ситуации», «мысленное представление», «внутренний взор», «внутреннее зрение», который характеризуют мыслительную деятельность на внутреннем плане. При этом всем известно явление, когда в случае глубокой задумчивости человек «смотрит, но не видит», т.е. глаз фиксирует какой-то объект, но человек его не замечает.

Таким образом, глаза являются непосредственным отражением мыслительных процессов. На особенности движения глаз не влияют ни эмоциональное состояние человека, ни его психофизиологические реакции. Анализ движения глаз является прямым информационным каналом получения сведений о мыслительных операциях выполняемых человеком. Прежде чем солгать, человек должен совершить определенную мысленную работу, при этом он переключается с внешнего плана деятельности на внутренний, что совершенно четко проявляется в изменении характера движения глаз.

Использование современных аппаратно-программных комплексов дает возможность непосредственно во время конкретной ситуации (собеседование с кандидатом на работу, деловые переговоры) получать информацию об искренности собеседника, также возможно осуществление анализа ранее сделанных видеозаписей.

Рассмотрим схему работы такого комплекса на примере ведения деловых переговоров. Скрытая высокоскоростная мегапиксельная видеокамера осуществляет видеосъемку лица собеседника. Видеопоток поступает в компьютер, далее специальное программное обеспечение производит его оцифровку и распознает на нем расположение глаз и их перемещение, затем программа по особому алгоритму определяет особенности траектории движения глаз, и если она будет свидетельствовать о лжи, то программа подаст специальный сигнал. Представляется, что данная технология обладает определенными преимуществами: во-первых, детекция лжи производится скрытно и дистанционно, во-вторых, это происходит непосредственно в момент развития ситуации и, в-третьих, роль «человеческого фактора» самого специалиста сведена к нулю.

Вызванные потенциалы (ВП) мозга – это попытки использования изменения биоэлектрической активности головного мозга в ответ на действие различных стимулов. Основываясь на результатах изучения с помощью ВП мозговых процессов, сопряженных с ложью, ученые предложили несколько противоречащих друг другу теорий. Одни считают, что процесс лжи сопряжен с изменением в

активности механизмов внимания, другие – с изменением нагрузки на механизмы памяти, или разрешением конфликта, возникающего между процессами восприятия и памяти [3, с. 12]. Изменение внимания заключается, прежде всего, в его переключении на факторы возможной угрозы. Например, громкий шум привлекает наше внимание потому, что он может представлять угрозу. Аналогично вопросы, на которые человек собирается солгать, привлекают его повышенное внимание, поскольку связаны с угрозой возможного разоблачения лжи.

Нагрузка на память определяется тем, какой объем информации индивид может держать под контролем и анализировать одновременно. Человек, говорящий правду, не испытывает необходимости поддерживать в активном состоянии большой объем информации, находящейся в памяти, тогда как человек, говорящий ложь, вынужден постоянно контролировать как содержание и качество своих ложных высказываний, так и содержание действительного состояния вещей. Произнесение лжи всегда является гораздо более сложной деятельностью, чем произнесение правды.

Исследования показали, что в процессе лжи наибольшие изменения наблюдаются в таких компонентах ВП, как Р3b, Р3а и N4 [5, с. 12]. Наиболее часто упоминается компонент Р3b, который оказывается информативным в экспериментальной схеме, направленной на выявление «скрываемой информации» с использованием стимулов, предъявляемых в случайном порядке («CIT/Oddball paradigm»). В рамках этой схемы редко встречающийся стимул случайным образом предъявляется в последовательности более знакомых стимулов. Например, высокочастотный звук, время от времени предъявляемый в большой серии низкочастотных звуков, будет привлекать внимание, благодаря своему отличию от общего фона, и вызывать появление компонента Р3b.

Подобные «случайные» стимулы приводят к появлению на электроэнцефалограмме волны с положительным пиком в интервале 300–650 миллисекунд от момента предъявления стимула. Максимальную амплитуду этот пик имеет в теменной области головного мозга, а минимальные – в лобной. Использование данной экспериментальной схемы для выявления скрываемой информации предполагает одновременное предъявление низко вероятных стимулов, отражающих конкретные знания виновного, и высоко вероятных стимулов, не имеющих отношения к содержанию преступления. Соответственно, характеризующиеся низкой вероятностью стимулы с элементами знания виновного вызывают более выраженный компонент Р3, чем фоновые стимулы с более высокой вероятностью предъявления. Хотя исследователи, изучающие ВП в рамках описанной экспериментальной схемы, и не определяют их точно как Р3b, данные по их пространственно-временным характеристикам позволяют утверждать, что это все-таки не что иное, как самые настоящие позитивные компоненты Р3b [там же].

Эффективность описанной выше экспериментальной схемы была продемонстрирована как для зрительных, так и для звуковых стимулов. Во всех случаях компонент Р3 с высокой точностью и надежностью указывал на наличие скрываемой информации. Однако проблема заключается в том, что волна Р3b оказывается связанной со многими видами высших корковых функций, включая оценку значимости стимула, перераспределение внимания и переработку информации перед ее перемещением из кратковременной в долговременную память.

Сказать точно, какой из перечисленных процессов непосредственно связан с ложью, трудно, и положительные результаты, получаемые с помощью описанного выше теста выявления скрываемой информации, только усложняют ситуацию, поскольку этот тест фактически зондирует память испытуемого, а измеряемый компонент Р3 скорее отражает реакцию узнавания, а не процессы, связанные с ложью. Цель метода – обнаруживать в памяти следы преступления.

Не все исследования связи биоэлектрической активности мозга и лжи используют схему выявления скрываемой информации. Однако развитие иных направлений упирается в отсутствие ясного понимания того, что же в действительности происходит в мозге во время лжи. Две основные теории – изменения фокуса внимания и нагрузки на память – предполагают разные направления изменения компонента Р3b. В частности, согласно первой из них амплитуда пика волны должна возрастать, а согласно второй – уменьшаться. Оба этих явления могут быть получены в эксперименте путем манипулирования условиями его проведения. Поэтому для установления связи ВП и лжи необходимо исследовать другие характеристики биоэлектрической активности мозга.

Подобно компоненту Р3b, волну Р3а можно получить в схеме эксперимента со случайным предъявлением при введении третьей категории стимулов – низко вероятностный /новый. Волна Р3а возникает также при переключении внимания, переходе от выполнения сложной задачи к более простой и при резком общем возбуждении мозга. При этом понятие Р3а относится к комплексу ранних компонентов волны Р3, наблюдающихся через 250–350 секунд после предъявления стимула.

В отличие от позитивных волн Р3b и Р3а, последний из используемых в исследованиях компонент N4 является чувствительным к появлению семантической рассогласованности. Некоторые исследователи утверждают, что при лжи имеет место рассогласованность между внутренней правдой и внешним ложным ответом. Компонент N4 представляет собой отрицательную волну с латентным временем около 400 миллисекунд и максимальной амплитудой в височной и лобной областях мозга. Он вызывается стимулом, который не согласуется с предшествующим контекстом и несет

ограниченную лингвистическую информацию. Считается, что N4 чувствителен к аномалиям в семантической структуре высказываний и сбоям в кратковременной памяти.

Исследования, проведенные в лаборатории А.Б. Пелевина, показали, что комбинация компонентов P3a, P3b, N4 и более поздней позитивной волны одновременно наблюдаются в процессе лжи. Ранний положительный компонент P3a в основном локализуется в области предцентральной извилины, в которой расположены мозговые механизмы внимания. Компонент P3b связан с активностью нескольких областей мозга, имеющих отношение к процессу принятию решения. Поздний отрицательный компонент N4 преимущественно связан с нижней лобной извилиной и отвечает за комплексную согласованность ответа с памятью и семантическим планом высказывания. Наконец, самая поздняя положительная волна возникает в височной и предцентральной извилинах и может быть связана с повторным и окончательным анализом содержания ответа.

Компьютерная томография (КТ) – использование ядерного магнитного резонанса. Когда человек выполняет те или иные когнитивные операции (арифметический счет, чтение или произнесение лжи), у него активируются различные отделы мозга. Повышение активности нейронов сопровождается усилением их метаболизма и увеличением локального кровоснабжения. Для регистрации изменения кровоснабжения различных областей мозга можно использовать технологию ядерного магнитного резонанса.

В типичном эксперименте испытуемый, расположенный в трубе томографа, выполняет определенные когнитивные задачи. Вначале делается общее изображение мозга, так как каждая томограмма неповторима так же, как неповторим мозг каждого индивида, отличающийся формой, размером и метаболизмом. Затем через короткие интервалы времени делаются последовательные снимки низкого разрешения. Часть из них делаются в процессе выполнения когнитивной задачи, а часть – в состоянии, используемом для контроля. Например, одни изображения можно получать в периоды, когда человек лжет, а другие тогда, когда он говорит правду. После этого два комплекта снимков сравниваются между собой для выявления зон активации в мозге. Исследования показали, что во время лжи усиливается активность в нижней и боковой областях лобной коры, отвечающей за особо сложные процессы переработки информации [1, с. 23]. Ложь сопровождается также повышением активности в предцентральной, средней и верхней коре лобных долей, а также в средней височной извилине.

Компьютерная томография стала родоначальницей ряда других еще более совершенных методов исследования: томографии с использованием эффекта ядерного магнитного резонанса (ЯМР-томография), позитронной эмиссионной томографии (ПЭТ), функционального магнитного резонанса (фМР). Эти методы относятся к наиболее перспективным способам неинвазивного совмещенного изучения структуры, метаболизма и кровотока мозга. При ЯМР-томографии получение изображения основано на определении в мозговом веществе распределения плотности ядер водорода (протонов) и на регистрации некоторых их характеристик при помощи мощных электромагнитов, расположенных вокруг тела человека. Полученные посредством ЯМР-томографии изображения дают информацию об изучаемых структурах головного мозга не только анатомического, но и физикохимического характера. Помимо этого, преимущество ядерно-магнитного резонанса заключается в отсутствии ионизирующего излучения; в возможности многоплоскостного исследования, осуществляемого исключительно электронными средствами; в большей разрешающей способности. Другими словами, с помощью этого метода можно получить четкие изображения "срезов" мозга в различных плоскостях.

Позитронно-эмиссионная трансаксиальная томография (ПЭТ-сканеры) сочетает возможности КТ и радиоизотопной диагностики. В ней используются ультракороткоживущие позитронизлучающие изотопы («красители»), входящие в состав естественных метаболитов мозга, которые вводятся в организм человека через дыхательные пути или внутривенно [1, с. 25]. Активным участкам мозга нужен большой приток крови, поэтому в рабочих зонах мозга скапливается больше радиоактивного «красителя». Излучения этого «красителя» преобразуют в изображения на дисплее. С помощью ПЭТ измеряют региональный мозговой кровоток и метаболизм глюкозы или кислорода в отдельных участках головного мозга. ПЭТ позволяет осуществлять прижизненное картирование на «срезах» мозга регионального обмена веществ и кровотока.

В настоящее время разрабатываются новые технологии для изучения и измерения происходящих в мозге процессов, основанные, в частности, на сочетании метода ЯМР с измерением мозгового метаболизма при помощи позитронной эмиссии. Эти технологии получили название метода функционального магнитного резонанса (фМР).

Таким образом, в настоящее время исследуется возможность использования нескольких современных технологий в целях выявления лжи: обсуждаются потенциальные возможности таких методов, как анализ вызванных потенциалов мозга, изображений, полученных методом ядерного магнитного резонанса, измерение стресса в голосе, термография (дистанционное определение температуры поверхности кожи), динамическое измерение диаметра зрачка глаза. Развитие детекции лжи в будущем зависит от того, насколько новые технологии будут согласовываться с современной

практикой использования полиграфа в этих целях, а также от глубины теоретической и методической проработки новых направлений. Важно отметить, что наше понимание и теоретические представления о процессе лжи становятся все более сложными, так же, как и методы, которые применяются для ее выявления. И хотя на сегодняшний день опрос с использованием полиграфа является самым точным методом выявления лжи, однако продолжается изучение возможностей других современных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Александров Ю.И. Психофизиология: Учебник для вузов. 2-е изд., М.: 2001.
2. Данилова Н.Н. Психофизиология. М.: Аспект Пресс, 2003.
3. Компьютерные технологии в медицине / под ред. К.Л. Ипатова. М.: Аспект, 2000.
4. Муркин В.И. Информатика и информационные технологии. М: Эксмо, 2007.
5. Пеленицын А.Б. Детекция лжи. // Полиграф. 2008. №2.

Потапов Ю.А.

**Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
РЕАЛИЗАЦИЯ МЕЖДУНАРОДНО-ПРАВОВЫХ АКТОВ О СВОБОДЕ ИНФОРМАЦИИ
В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Принятая в 1948 году Всеобщая декларация прав человека устанавливает право на свободу информации. Статья 19 этой декларации гласит: «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ». Важная роль в получении и распространении информации принадлежит СМИ.

Международный пакт о гражданских и политических правах, вступивший в силу 23 марта 1976 года, в части 2 статьи 19 закрепляет: «Каждый человек имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору».

Статья 10 Европейской Конвенции о защите прав человека и основных свобод от 4 ноября 1950 года гласит:

1. Каждый человек имеет право на свободу выражения своего мнения. Это право включает свободу придерживаться своего мнения, получать и распространять информацию и идеи без вмешательства со стороны государственных органов и независимо от государственных границ. Эта статья не препятствует государствам вводить лицензирование радиовещательных, телевизионных или кинематографических предприятий.

2. Осуществление этих свобод, налагающее обязанности и ответственность, может быть сопряжено с формальностями, условиями, ограничениями или штрафными санкциями, предусмотренными законом и необходимыми в демократическом обществе в интересах государственной безопасности, территориальной целостности или общественного спокойствия, в целях предотвращения беспорядков и преступности, защиты здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия.

Также существует целый ряд решений Парламентской Ассамблеи Совета Европы (ПАСЕ), касающихся конкретного воплощения свободы массовой информации. Прежде всего следует указать резолюцию 428 (1970 г.), посвященную принятию Декларации о средствах массовой информации и правах человека. Здесь перечисляются принципы, которые следует соблюдать для того, чтобы СМИ могли выполнять свои функции в интересах общественности и среди них:

- свобода выражения мнений должна распространяться на СМИ;
- свобода выражения мнений в СМИ должна включать свободу искать, получать, передавать, публиковать и распространять информацию и идеи;
- власти обязаны в разумных пределах предоставлять информацию по вопросам, представляющим интерес для общественности, а СМИ обязаны сообщать полную и исчерпывающую информацию о государственных делах;
- независимость СМИ от государственного контроля должна быть записана в законе; любое ущемление независимости допустимо только на основании решения суда, но не органов исполнительной власти;
- не должно быть ни прямой, ни косвенной цензуры печати или содержания телерадиопрограмм; ограничения могут налагаться лишь в пределах, разрешенных статьей 10 Европейской конвенции о правах человека;
- внутренняя организация СМИ должна гарантировать свободу ответственных редакторов выражать свое мнение, их независимость должна быть защищена;
- независимость СМИ должна быть защищена от угрозы со стороны монополий;

– ни частные предприятия, ни финансовые группы не должны иметь права на монополию в области СМИ и не следует разрешать образование монополии, подконтрольной правительству;

– необходимо принять специальные меры для обеспечения свободы иностранных журналистов, включая статус, обязанности, привилегии и защиту от произвольной депортации, что предполагает соответствующую обязанность иностранных журналистов точно освещать события.

Конституция Российской Федерации гарантирует каждому свободу мысли и слова, право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Эти права закреплены в части 1 и части 4 статьи 29, а часть 5 этой же статьи гарантирует свободу массовой информации и запрещает цензуру.

В соответствии со статьей 5 Закона РФ «О средствах массовой информации» законодательство Российской Федерации о средствах массовой информации состоит из данного Закона и издаваемых в соответствии с ним иных нормативных правовых актов Российской Федерации. Если межгосударственным договором, заключенным Российской Федерацией, предусмотрены иные правила, чем установленные Законом о СМИ, то применяются правила межгосударственного договора.

Взаимодействие органов внутренних дел со средствами массовой информации регулируется следующими федеральными законами: «О средствах массовой информации», «О государственной тайне», «О милиции»; «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации», «Об информации, информационных технологиях и защите информации», «О рекламе», «Об экономической поддержке районных (городских) газет», «О связи», «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации», «Об оперативно-розыскной деятельности», «О противодействии терроризму», «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов», а также Гражданским и Уголовным кодексами Российской Федерации, Кодексом Российской Федерации об административных правонарушениях и др.

Наиболее значимыми ведомственными нормативными актами являются следующие:

1. Приказ МВД России от 1 декабря 2005 года №985 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в органах внутренних дел Российской Федерации заявлений, сообщений и иной информации о происшествиях».

2. Приказ МВД России от 10 апреля 2006 года №246 «Об информационно-пропагандистской работе».

3. Приказ МВД России от 12 октября 2007 года №888 «Вопросы организации деятельности подразделений информации и общественных связей органов внутренних дел российской федерации».

4. Приказ МВД России от 30 декабря 2007 года №1246 «О повышении эффективности изучения общественного мнения об уровне безопасности личности и деятельности органов внутренних дел Российской Федерации на основе использования вневедомственных источников социологической информации».

5. Приказ МВД России от 13 сентября 2001 г. №812 «Об Общественном совете при Министерстве внутренних дел Российской Федерации».

6. Приказ МВД России от 5 декабря 2005 года №992 «Об Информационном совете Министерства внутренних дел Российской Федерации».

7. Приказ МВД России от 01 января 2009 года №1 «Об утверждении Концепции совершенствования взаимодействия подразделений системы Министерства внутренних дел Российской Федерации со средствами массовой информации и общественными объединениями на 2009-2014 годы».

Провозглашенные Конституцией Российской Федерации свобода слова и свобода массовой информации возводят на новый уровень взаимоотношения прессы и органов внутренних дел. Недостоверность, неполнота и искаженность информации возникают из-за недоступности источников информации, а повсеместно созданные пресс-службы, по оценкам экспертов, «превратились в непреодолимые барьеры и выдают лишь ту информацию, в которой заинтересована данная структура». Создание и функционирование аппаратов органов внутренних дел по связям со средствами массовой информации и общественностью - явление вполне закономерное и отвечающее требованиям времени, объективным тенденциям развития нашего государства и органов внутренних дел на современном этапе.

Годы реформ изменили не только российское общество, но и средства массовой информации. Телевидение, радио и пресса превратились в независимые социальные институты и во многом стали выступать в качестве «четвертой власти». Перемены коснулись и органов внутренних дел. Обеспечение социального порядка, законности, общественной стабильности объективно повысило в жизни общества роль права и тех людей, которые реализуют правоприменительную деятельность. А это настоятельно требовало хорошо организованного и объективного освещения в средствах массовой информации правоохранительной деятельности. Поэтому поиск эффективной концепции,

позволяющей поддерживать баланс двустороннего информационного взаимодействия между органами внутренних дел и средствами массовой информации никогда не прекращался.

В настоящее время пресс-службы функционируют во всех главных управлениях МВД России по федеральным округам, созданы управления (отделы, отделения) информации и общественных связей МВД, ГУВД, УВД по субъекту Российской Федерации, отделения (группы) информации и общественных связей УВДТ, ОВДРО, штаба горрайлинооргана внутренних дел. Они занимают важное место в организации пропаганды оперативно-служебной деятельности органов внутренних дел и создании положительного имиджа МВД России.

СПИСОК ЛИТЕРАТУРЫ

1. Взаимодействие средств массовой информации и правоохранительных органов: материалы научно-практической конференции. – СПб., 2001.
2. Основы взаимодействия органов внутренних дел со средствами массовой информации и общественными объединениями: Учебное пособие. – СПб., 2001.

Примакин А.И., Мельник И.А., Щапков Д.А.

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

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ СВЯЗИ НА ПРИМЕРЕ ТЕЛЕФОНИИ

Одними из основных источников угроз информационной безопасности являются деятельность иностранных разведывательных и специальных служб, преступных сообществ, организаций, групп, формирований и противозаконная деятельность отдельных лиц, направленная на сбор или хищение ценной информации, закрытой для доступа посторонних лиц. Причем в последние годы приоритет в данной сфере деятельности смещается в экономическую область.

При сборе разведывательной информации на территории России широко используются портативные технические средства разведки. Поэтому в последние годы защите информации от утечки по техническим каналам связи уделяется все большее внимание.

Основными направлениями защиты информации от утечки по техническим каналам связи являются:

- предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также за счет электроакустических преобразований;
- выявление внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);
- предотвращение перехвата с помощью технических средств речевой информации из помещений и объектов [1].

Информация может быть представлена в различной форме и на различных физических носителях. Основными формами информации, представляющими интерес с точки зрения защиты, являются:

- документальная;
- акустическая (речевая);
- телекоммуникационная и т.п.

Документальная информация содержится в графическом или буквенно-цифровом виде на бумаге, а также в электронном виде на магнитных и других носителях. Особенность документальной информации в том, что она содержит сведения, подлежащие защите.

В сжатом виде речевая информация возникает в ходе ведения в помещениях разговоров, а также при работе систем звукоусиления и звуковоспроизведения. Носителем речевой информации являются акустические колебания (механические колебания частиц упругой среды, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины). Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 200...300 Гц до 4...6 кГц.

Телекоммуникационная информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче. Носителем информации при ее обработке техническими средствами и передаче по проводным каналам связи является электрический ток, а при передаче по радио и оптическому каналам.

Скрытие информации предусматривает такие изменения структуры и энергии носителей, при которых злоумышленник не может непосредственно или с помощью технических средств выделить информацию с качеством, достаточным для использования ее в собственных интересах.

Различают информационное и энергетическое скрывание. Информационное скрывание достигается изменением или созданием ложного информационного портрета семантического сообщения, физического объекта или сигнала.

Информационным портретом можно назвать совокупность элементов и связей между ними, отображающих смысл сообщения (речевого или данных), признаки объекта или сигнала. Элементами

дискретного семантического сообщения, например, являются буквы, цифры или другие знаки, а связи между ними определяют их последовательность. Информационными портретами объектов наблюдения, сигналов и веществ являются их эталонные признаковые структуры.

Возможны следующие способы изменения информационного портрета:

- удаление части элементов и связей, образующих информационный узел (наиболее информативную часть) портрета;
- изменение части элементов информационного портрета при сохранении неизменности связей между оставшимися элементами;
- удаление или изменение связей между элементами информационного портрета при сохранении их количества.

Изменение информационного портрета объекта вызывает изменение изображения его внешнего вида (видовых демаскирующих признаков), характеристик излучаемых им полей или электрических сигналов (признаков сигналов), структуры и свойств веществ. Эти изменения направлены на сближение признаков структур объекта и окружающего его фона, в результате чего снижается контрастность изображения объекта по отношению к фону и ухудшаются возможности его обнаружения и распознавания.

Но при изменении информационного портрета информация не воспринимается не только злоумышленником, но и ее санкционированным получателем. Следовательно, для санкционированного получателя информационный портрет должен быть восстановлен путем дополнительной передачи ему удаленных элементов и связей или алгоритма (ключа) этих изменений [2].

Что же касается защиты телефонных линий как каналов утечки информации необходимо учитывать следующее:

- телефонные аппараты (даже при положенной трубке) могут быть использованы для перехвата акустической речевой информации из помещений, в которых они установлены, то есть для подслушивания разговоров в этих помещениях;
- телефонные линии, проходящие через помещения, могут использоваться в качестве источников питания акустических закладок, установленных в этих помещениях, а также для передачи перехваченной информации;
- возможен перехват (подслушивание) телефонных разговоров путем гальванического или через индукционный датчик подключения к телефонной линии закладок (телефонных ретрансляторов), диктофонов и других средств несанкционированного съема информации.

Телефонный аппарат имеет несколько элементов, способных преобразовывать акустические колебания в электрические сигналы (микрофонный эффект). К ним относятся звонковая цепь, телефонный и, конечно, микрофонный капсули. За счет электроакустических преобразований в этих элементах возникают информационные (опасные) сигналы. При положенной трубке телефонный и микрофонный капсули гальванически отключены от телефонной линии и при подключении к ней специальных высокочувствительных низкочастотных усилителей возможен перехват опасных сигналов, возникающих в элементах только звонковой цепи.

При использовании для съема информации метода «высокочастотного навязывания», несмотря на гальваническое отключение микрофона от телефонной линии, сигнал навязывания благодаря высокой частоте проходит в микрофонную цепь и модулируется по амплитуде информационным сигналом. Следовательно, в телефонном аппарате необходимо защищать как звонковую цепь, так и цепь микрофона.

Для недопущения несанкционированного использования телефонной линии (ТЛ) применяются следующие технические способы (ТС):

- применение пассивных ТС защиты: сигнализаторов подключения, обрыва линии, счетчиков времени разговора, в т.ч. по межгороду;
- применение активных ТС защиты: устройства защиты от параллельного подключения, блокираторы выхода на межгород, устройства кодирования доступа к телефонной линии, устройства активного маскирования информации и др.

Контроль состояния телефонной линии и обнаружение атак осуществляется посредством применения аппаратуры контроля линий связи:

- индикаторных устройств;
- анализаторов проводных линий и кабельных локаторов (рефлектометров и устройств, использующих принципы нелинейной локации);
- универсальных комплексов контроля.

Для проведения углубленных исследований телефонных линий на предмет обнаружения несанкционированных подключений подслушивающих устройств используется более серьезная аппаратура, эффективная работа с которой доступна только специалистам. Это – анализаторы телефонных линий и кабельные локаторы. При использовании стандартных анализаторов

телефонных линий можно эффективно обнаруживать наличие радиозакладных устройств с непосредственным подключением телефонной линии.

Активные методы защиты информации от утечки по электроакустическому каналу предусматривают линейное зашумление телефонных линий. Шумовой сигнал подается в линию в режиме, когда телефонный аппарат не используется (трубка положена). При снятии трубки телефонного аппарата подача в линию шумового сигнала прекращается.

К основным методам активной защиты относятся:

- подача во время разговора в телефонную линию синфазного маскирующего низкочастотного сигнала (метод синфазной низкочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного сигнала звукового диапазона (метод высокочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного ультразвукового сигнала (метод ультразвуковой маскирующей помехи);
- поднятие напряжения в телефонной линии во время разговора (метод повышения напряжения);
- подача во время разговора в линию напряжения, компенсирующего постоянную составляющую телефонного сигнала (метод «обнуления»);
- подача в линию при положенной телефонной трубке маскирующего низкочастотного сигнала (метод низкочастотной маскирующей помехи);
- подача в линию при приеме сообщений маскирующего низкочастотного (речевого диапазона) с известным спектром (компенсационный метод);
- подача в телефонную линию высоковольтных импульсов (метод «выжигания») [3].

Многообразие возможных ситуаций определяет многообразие мер и способов защиты телефонных разговоров. Очевидно, что обеспечить безопасность телефонного канала связи очень сложно и дорого. Экономически выгоднее воспользоваться устройствами, позволяющими закрыть сообщения, передаваемые по телефонным каналам, или применять организационные меры, обеспечивающие конфиденциальность переговоров. Простейшими и в то же время крайне важными мерами борьбы с подслушиванием телефонных переговоров являются мероприятия по обеспечению строгой дисциплины ведения телефонных переговоров. Внешней телефонной связью должен пользоваться ограниченный круг лиц. Никакие частные переговоры из выделенных помещений не допускаются. Наименования организаций, учреждений, должностных лиц, фамилии и другие сведения не должны употребляться в ходе переговоров. Запрещается передача по телефону распоряжений, отчетов, сведений о составе, состоянии и деятельности организаций и предприятий. При переговорах всегда нужно помнить, что злоумышленник «не дремлет». К организационным мерам защиты можно отнести планирование прокладки телефонных линий в зданиях и помещениях таким путем, чтобы было удобно их контролировать и трудно использовать возможности подслушивания. Прокладку телефонных линий следует проводить с уменьшением возможного параллельного пробега и перекрещивания друг с другом.

Весьма эффективной мерой противодействия подслушиванию переговоров является использование для ведения конфиденциального общения маскираторов речи или скремблеров. На сегодня техника шифрования речевых сигналов достаточно развита и появилась на рынке в виде удобных переносных или стационарных аппаратов, надежно шифрующих речевой сигнал до его подачи в телефонную линию. Скремблер – это автономное или встроенное устройство для засекречивания речевой информации, передаваемой по каналам проводной и радиосвязи. Выбор той или иной модели скремблера зависит от его конкретного применения и характеристик канала связи. Модели скремблеров, предлагающиеся на отечественном рынке, различаются назначением, конструктивным исполнением и возможностями, а также стойкостью засекречивания, порядком ввода ключа, качеством восстановленной речи, способом электропитания, конструкцией (встроенный или автономный) и другими характеристиками [4].

Предотвращение несанкционированного доступа к конфиденциальной информации, циркулирующей в телефонных каналах связи государственного и военного управления, к информации национальных и международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью и международным терроризмом, а также в банковских, государственных, коммерческих и социальных сетях является важной задачей обеспечения безопасности глобальной информации.

СПИСОК ЛИТЕРАТУРЫ

1. Хорев А.А. Способы и средства защиты информации. М.: МО РФ, 2000. 316с.
2. Устинов, Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий/ Г.Н. Устинов. М.: Радио и связь, 2003. 342с.
3. Барсуков В.С. Безопасность: технологии, средства, услуги. / В.С. Барсуков. М. 2001. 496 с.
4. Ярочкин В.И. Информационная безопасность.: Учебник для студентов вузов. М.: Академический Проект. Гаудеамус, 3-е изд. 2005. 544с.

Черепанова Ю.Е.

**Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
К ВОПРОСУ О ТЕРМИНЕ «ЗАЩИТА ИНФОРМАЦИИ»**

Принято считать информацию объектом регулирования специальной отрасли права – информационного права. Вместе с тем, в некоторых случаях информация становится также объектом административно-правового регулирования. Это происходит, когда:

1. Информация в соответствии с Конституцией РФ и федеральным законодательством подлежит обязательной защите;
2. Одним из участников информационного правоотношения является орган государственной власти;
3. В отношении документированной информации вводится административно-правовой режим;
4. Открытая информация циркулирует в государственных информационных системах;
5. Информация является информацией ограниченного доступа.
6. Рассматривая информацию как объект административно-правового регулирования, нельзя не остановиться на широко используемом термине «защита информации». В настоящее время, под защитой информации принято понимать «принятие правовых, организационных и технических мер, направленных на:
7. Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
8. Соблюдение конфиденциальности информации ограниченного доступа;
9. Реализацию права на доступ к информации».

Вместе с тем, согласно мнению И.Л. Бачило, «широко употребляемое выражение «защита информации» не имеет однозначной трактовки. В прямом понимании – это недопущение какого-либо воздействия на информацию, которую некто должен сохранить в определенном состоянии. Но данная цель подвергается вполне понятному противодействию на основании реализации всеобщего принципа свободы и доступности информации в процессе реализации права на информацию, в процессе обеспечения гласности деятельности различных институтов общества» [1].

В.И. Ярочкин с позиций системного подхода предъявляет к защите информации требования быть непрерывной, плановой, целенаправленной, конкретной, активной, надежной, универсальной и комплексной [2], и далее подразделяет защиту информации на правовую защиту, организационную защиту и инженерно-техническую защиту, делая вывод о том, что правовые меры обеспечения безопасности и защиты информации являются основой порядка деятельности и поведения сотрудников всех уровней и степени их ответственности за нарушения установленных норм и правил работы по обеспечению сохранности коммерческих секретов.

Кроме того, в ряде международных соглашений Российской Федерации можно также встретить термин «защита информации». Под ним в этих документах подразумевается:

- деятельность, направленная на предотвращение утечки конфиденциальной информации, несанкционированных и непреднамеренных воздействий на конфиденциальную информацию;
- комплекс административных, организационных и технических мероприятий по ограничению доступа к информации и ее носителям в целях обеспечения ее сохранности и недоступности третьим сторонам, предусмотренный законодательством РФ.

Два последние определения, на наш взгляд, неоправданно сужают понятие защита информации, предполагая необходимость такой защиты только для информации ограниченного доступа, или конфиденциальной информации. Однако данный подход противоречит мнению о том, что защиты от искажения, модификации и уничтожения требует в том числе открытая информация, которая может быть использована последующими поколениями с помощью еще неизвестных нам способов и в ещё не сформулированных в настоящее время научных, образовательных и иных инновационных целях.

Лапина М.А., Ревин А.Г., Лапин В.И. [3] предлагают следующее определение защиты информации – «защищенность информации от внешних воздействий (попыток неправомерного копирования, распространения, модификации (изменения смысла) либо уничтожения)» [3]. Указанное определение, на наш взгляд, также нельзя назвать удачным, поскольку определять термин защита однокоренным защищенность не означает прояснять сущность понятия, хотя достоинством приведенного определения следует признать перечисление возможных воздействий, которые могут посягать не только на конфиденциальность, но также на целостность и доступность информации.

Родичев Ю.А. [4] предлагает использовать следующее определение:

защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [4].

Достаточно полное определение исследуемого понятия приводит в своей работе А.А. Шиверский. Под защитой информации он понимает «комплекс мероприятий, проводимых

собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих её распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и её носителям» [5]. Однако данное определение также нельзя признать идеальным, поскольку А.А. Шиверский возлагает необходимость осуществления мероприятий по защите информации исключительно на собственника информации, искусственно лишая хранителя или производителя информации возможности предпринимать меры по её защите. Кроме того, исходя из указанного определения следует, что А.А. Шиверский также считает необходимым защищать лишь информацию ограниченного доступа или засекреченную информацию, что, на основании вышеизложенных диссертантом доводов никак нельзя признать верным.

В свою очередь, толковый словарь «Бизнес и право» правовой системы «Гарант» под данным понятием подразумевает «все средства и функции, обеспечивающие доступность, конфиденциальность или целостность информации или связи, исключая средства и функции, предохраняющие от неисправностей. Она включает криптографию, криптоанализ, защиту от собственного излучения и защиту компьютера» [6].

Анализируя приведенные определения, автор считает необходимым предложить собственное определение защиты информации, которое, на наш взгляд, наиболее полно отражает суть данного понятия.

Защита информации – это комплекс правовых, организационных инженерно-технических и программных мер, направленных на обеспечение её доступности, целостности, а также в определяемых Конституцией или федеральными законами случаях конфиденциальности, осуществляемых владельцем информации или иным, уполномоченным на то действующим законодательством, субъектом.

СПИСОК ЛИТЕРАТУРЫ

1. Бачило И.Л. Информационное право: Основы практической информатики. Учебное пособие. М., 2001. С. 253.
2. Ярочкин В.И. Информационная безопасность. М., 2006. С. 9-10.
3. Лапина М.А., Ревин А.Г., Лапин В.И. Информационное право. М., 2004. С. 55.
4. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты. СПб., 2008. С. 17.
5. Шиверский А.А. Защита информации: проблемы теории и практики. М., 1996. С. 59.
6. Правовая система Гарант. Официальный сайт – www.garant.ru



БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Асанович В.Я., Зеленцов В.А., Соколов Б.В., Цивирко Е.Г.

Беларуссия, Минск, Белорусский государственный экономический университет

Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,

Комитет по информатизации и связи Санкт-Петербурга

МЕТОДОЛОГИЧЕСКИЕ И МЕТОДИЧЕСКИЕ ОСНОВЫ КОМПЛЕКСНОГО ПЛАНИРОВАНИЯ РАЗВИТИЯ КАТАСТРОФОУСТОЙЧИВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Анализ существующих и прогнозируемых кризисных и чрезвычайных ситуаций, повсеместно возникающих в настоящее время в различных предметных областях, (особенно после известных событий 11 сентября 2001 года в США, а также веерных отключений систем электроснабжения в США, Европе, РФ и т.п.) показывает, что они перестают быть отраслевыми, а перерастают в аварии и катастрофы, имеющие уже системный (межотраслевой) характер, когда, например, из-за аварии, произошедшей в 2006 году в Москве на одной из трансформаторных подстанций РАО ЕЭС РФ, произошло лавинообразное отключение электрических сетей жилищно-коммунального хозяйства города, электрических сетей больниц и государственных учреждений, в том числе и МО, и, как следствие возникновение вторичных аварий и нештатных ситуаций (загрязнение устья Московского водохранилища, остановку всех видов электротранспорта мегаполиса и т.п.). В этих условиях исследовать и решать задачи повышения катастрофоустойчивости как бизнес-процессов, так информационных систем (ИС), обеспечивающих их выполнение, необходимо уже в рамках междисциплинарного подхода, интерпретируя их как задачи управления структурной динамикой (УСД) указанными процессами и системами [1–4].

Особую опасность для современных автоматизированных и информационных систем (АС и ИС) представляют причины, которые приводят к возникновению кризисных ситуаций, аварий и катастроф, имеющих природно-экологическую, технико-производственную или антропогенно-социальную природу. При этом спектр угроз экономической, физической и информационной безопасности, а также перечень уязвимостей аппаратно-программной и информационной инфраструктур ИС постоянно растет.

Так, например, к числу таких угроз могут быть отнесены следующие угрозы [1–4]: отказы аппаратных средств; разрушение блоков питания или элементов телекоммуникационной инфраструктуры компании; сбои приложений и баз данных; ошибки, связанные с человеческим фактором; вирусы, черви, «троянские кони» и т.д.; атаки злоумышленников; террористические акты либо ведение военных действий; пожары; наводнения, удары молнией и другие стихийные бедствия; веерные отключения систем жизненного обеспечения (электросети, сети водоснабжения и газоснабжения и т.п.).

Таким образом, в реальной жизни возможны ситуации, когда указанные угрозы являются комбинированными и приводят к лавинообразному возникновению и развитию негативных событий, приводящих в конечном итоге к катастрофическим последствиям. В этих условиях обеспечение непрерывности бизнес-процессов (БП) и повышение катастрофоустойчивости соответствующих производственных систем, входящих в состав бизнес-систем (БС) является одним из важнейших стратегических направлений развития экономики. Это обусловлено необходимостью сохранять устойчивость и стабильность функционирования интегрированных ИС в различных условиях неблагоприятного воздействия внешних и внутренних факторов техногенного и/или природного характера. При этом под катастрофоустойчивостью ИС следует понимать способность компьютерного комплекса, состоящего из нескольких систем, сохранить критически важные данные и продолжить выполнять свои функции после массового (возможно, целенаправленного) уничтожения его компонентов в результате различных катаклизмов как природного характера, так и инспирированных человеком. Необходимо подчеркнуть разницу между понятием «отказоустойчивость» и «катастрофоустойчивость» [1,3]. В понятии «отказоустойчивость» акцент делается на восстановление работоспособности после единичных, случайных, не связанных между собой отказов компонентов. Технология отработки таких отказов предполагает, как правило, что в работу вводятся резервные компоненты каждой подсистемы либо оставшиеся компоненты многократно дублированной подсистемы перераспределяют между собой работу независимо от того, что происходит в это время в других подсистемах.

В понятии «катастрофоустойчивость» главное — сохранение данных и продолжение работы (обеспечение непрерывности выполнения бизнес-процессов) в условиях массовых и, возможно, последовательных отказов систем и связанных между собой подсистем. В качестве основного показателя в этом случае используется показатель доступности катастрофоустойчивой информационной системы (КАИС), который характеризует степень возможности получения требуемых данных и осуществления взаимодействия с заданными приложениями в приемлемые сроки и с необходимым уровнем производительности. В данном контексте составляющими показателя доступности КАИС являются показатели надежности аппаратно-программных средств КАИС, а также показатель производительности данной системы, представляющей собой отношение времени отклика информационной системы к ее пропускной способности. Приведенному ранее определению катастрофоустойчивости точно соответствует англоязычный термин «Disaster Tolerance» (DT), однако в общем случае термин «Disaster Recovery» (DR) (дословно — «восстановление после катастрофы») можно также переводить как «катастрофоустойчивость». Первое отличие DR от DT состоит в том, что DR концентрирует внимание на сохранности данных (при строго контролируемых потерях, если они неизбежны), а средства для продолжения полноценной работы во многих случаях предполагаются внешними по отношению к собственно катастрофоустойчивой части комплекса. Технология отработки отказов в этом случае требует учета взаимосвязанности подсистем и способности систем специфически реагировать на каждый вариант последовательности развития событий (так называемый сценарий катастрофы) с целью обеспечения максимально возможной сохранности защищаемых данных.

Второе отличие кроется в распределении возможностей отказов по подсистемам. В отказоустойчивых системах предполагается (хотя в большинстве случаев и неявно), что каналы связи между активными компонентами (например, медные или оптические кабели) гораздо надежнее самих активных компонентов, поскольку протяженность этих каналов ограничена и вероятность их повреждения в большинстве случаев относительно невелика. В территориально распределенных катастрофоустойчивых системах возможность потери связи для каждого отдельного канала сравнима с вероятностью выхода из строя одного из активных компонентов. Это обстоятельство требует уделять повышенное внимание каналам связи и проблеме восстановления работоспособности после потери связи при проектировании и эксплуатации катастрофоустойчивой системы, причем сценарии отработки отказов и настройка всегда пишутся «по месту» — с учетом конкретных требований, как к комплексу в целом, так и к каждой площадке, принимая во внимание различные вероятности ожидаемых катастрофических событий. Потому просто «растянутая» в пространстве традиционная отказоустойчивая система без принятия дополнительных мер все же не может быть по-настоящему катастрофоустойчивой и в большинстве случаев не способна автоматически восстановить полную функциональность.

Следует подчеркнуть, что создание КАИС ведется из предположения, что катастрофа в отличие от отказа (события возможного, прогнозируемого, вероятного) — это событие возможное, но невероятное, либо вероятность которого мала и не может быть обоснованно оценена в процессе проектирования. В противном случае речь шла бы не о катастрофе, а об условиях функционирования [1–3]. Тогда основные элементы и подсистемы КАИС должны были бы создаваться исходя, например, из требований отказоустойчивого функционирования в условиях воздействия огнем, в водной или химической агрессивной среде, в условиях поражения оружием (различных типов). Понятно, что стоимость таких систем была бы существенно выше по сравнению с ИС, ориентированными на нормальное функционирование. Таким образом, в реальности, как составные элементы, так и в целом КАИС не гарантируют в полном объеме выполнение всех целевых, обеспечивающих и вспомогательных задач в условиях возникновения нерасчетных нештатных ситуаций, аварий и катастроф. Вместе с тем, необходимо отметить, что в оборонной сфере и сфере государственной безопасности как в нашей стране, так и за рубежом во второй половине XX века были сделаны отдельные катастрофоустойчивые системы, которые были ориентированы на функционирование в особо сложных условиях, вызванных последствиями ракетно-ядерной войны. Для этого в рамках соответствующих автоматизированных систем управления войсками и оружием создавались основные, дублирующие и резервные контуры управления, системы запасных и резервных мобильных пунктов управления, на которых в случае уничтожения основных командных пунктов можно было продолжать решать задачи управления. Таким образом, свойство катастрофоустойчивости ИС целенаправленно формируется (возникает) в этом случае в процессе ее функционирования и характеризуется соответствующей системой показателей. В частности может быть предложен следующий перечень основных показателей качества функционирования КАИС: показатели доступности КАИС (суммарное время простоев ИС по любым причинам), показатели, оценивающие риски возникновения и развития аварий и катастроф, показатели, оценивающие последствия аварий и катастроф для конкретных бизнес-процессов (продолжительность, масштаб и объем ущерба), показатели, оценивающие общие затраты времени и полноту выполненных операций, связанных с восстановлением работоспособности КАИС, показатели, оценивающие, капитальные и эксплуатационные затраты на обеспечение требуемого уровня

катастрофоустойчивости, затраты других видов ресурсов, показатели, оценивающие, степень критичности операций, выполняемых в КИС, значимость ресурсов и информации, используемой для обеспечения требуемого уровня катастрофоустойчивости.

Итак, устойчивость к катастрофам требует не только сохранности критически важных данных, но и обеспечения непрерывного (или прерываемого на некоторое время) функционирования ИС, а в случае невозможности реализации такого режима, в рамках КАИС должно быть обеспечено в максимально короткие сроки восстановление ее работоспособности. В этих условиях эффективность применения КАИС целесообразно оценивать не только показателем доступности, но и показателями функциональной устойчивости. Попутно можно отметить, что при отсутствии катастроф концепция обеспечения доступности к данным будет ориентирована на поиск технологий, обеспечивающих минимизацию потерь от плановых простоев [1–4].

Исходя из вышеизложенного, свойство катастрофоустойчивости ИС формируется на основе целенаправленной организационно-технической, модельно-алгоритмической, информационно-правовой и другой деятельности людей, направленной на непрерывное сохранение, реализацию и восстановление присущих (заложенных на этапе проектирования) ИС возможностей в условиях массового (возможно, целенаправленного) уничтожения ее компонентов в результате различных катаклизмов как природного характера, так и инспирированных человеком.

В целом, решая на современном этапе задачи создания и применения комплексных систем защиты информации (СЗИ), необходимо их, во-первых, рассматривать в более общем контексте задач структурно-функционального синтеза катастрофоустойчивых автоматизированных и информационных систем (КАИС) и, во-вторых, при решении указанных задач в качестве основных показателей, оценивающих результативность применения СЗИ, следует использовать показатели, характеризующие эффективность реализации целевых процессов (в сфере экономики — бизнес-процессов), и показатели, характеризующие функциональную устойчивость указанных процессов.

В этих условиях исследовать и решать проблемы повышения катастрофоустойчивости как конкретных прикладных процессов (бизнес-процессов), так и информационной систем (ИС), обеспечивающих их выполнение, необходимо уже в рамках междисциплинарного подхода, интерпретируя соответствующие задачи как задачи управления структурной динамикой (УСД) указанными процессами и системами [5].

Главная особенность задачи планирования развития ИС состоит в том, что переход от «старой» (не являющейся катастрофоустойчивой) ИС к «новой» (модернизированной, катастрофоустойчивой) ИС не может быть проведен мгновенно. Это, на практике, приводит к тому, что на достаточно длительном интервале времени (периоде модернизации ИС) происходит совместная эксплуатация элементов и подсистем «старой» и «новой» ИС. Так, например, создание и ввод в эксплуатацию дублирующих и резервных ИС, располагающихся на значительном расстоянии от основной ИС, предполагает поэтапный ввод элементов и подсистем соответствующих комплексов автоматизации. Однако, в этих условиях, показатели качества и эффективности бизнес-процессов, поддерживаемых данными ИС, не должны ухудшаться. Таким образом, всякое изменение и развитие той или иной подсистемы (структуры) ИС объективно осуществляется одновременно с решением оперативных (текущих) задач, стоящих перед соответствующей бизнес-системой (БС). Поэтому и возникает необходимость совместной постановки задач комплексного планирования модернизации и функционирования ИС. При этом само планирование должно осуществляться комплексно и затрагивать все основные элементы и подсистемы существующей и создаваемой ИС [2–4]. Совместное решение задач комплексного планирования модернизации и функционирования ИС предполагает: построение соответствующего полимодельного комплекса, описывающего все основные аспекты исследуемых процессов; разработку комбинированных методов, алгоритмов и методик многокритериального полимодельного синтеза программ управления модернизацией и функционированием существующей и внедряемой ИС.

В ходе проведенных исследований были предложены следующие основные фазы и этапы решения задачи комплексного планирования модернизации и функционирования (задачи выбора оптимальных программ управления структурной динамикой КАИС. *На первой фазе* должно осуществляться формирование (генерирование) допустимых вариантов многоструктурных макросостояний КАИС или, говоря другими словами, должен проводиться структурно-функциональный синтез нового облика модернизируемой ИС, соответствующего складывающейся (прогнозируемой) обстановке. В указанной ситуации задачи, решаемые *на данной фазе*, сводятся к задачам структурно-функционального синтеза КАИС.

На второй фазе проводится выбор конкретного варианта многоструктурного макросостояния КАИС с одновременным синтезом (построением) адаптивных планов (программ) управления переходом КАИС из текущего в требуемое (выбранное) макросостояние. При этом рассматриваемые планы должны обеспечивать такое эволюционное развитие КАИС, при котором наряду с реализацией программ перехода из соответствующих макросостояний предусматривается одновременно и реализация программ устойчивого управления КАИС в промежуточных макросостояниях. *На данной фазе* приходится решать целую совокупность частных задач многоуровневой и многоэтапной

оптимизации. Обобщенный алгоритм решения данных задач должен включать следующие этапы (шаги) [5].

Шаг 1. В интерактивном режиме осуществляется автоматизированная подготовка, контроль, анализ и ввод всей исходной информации, необходимой для решения задачи управления структурной динамикой КАИС.

Шаг 2. Планирование проведения комплексного моделирования процессов адаптивного управления функционированием и развитием КАИС в текущей и прогнозируемой обстановке, планирование проведения вычислительных экспериментов в имитационной системе (ИмС), определение состава и структуры моделей, методов и алгоритмов решения частных задач моделирования, расчет времени, необходимого для решения указанных задач.

Шаг 3. Генерирование, на основе проведения комплексного моделирования, допустимых вариантов функционирования КАИС в исходном, промежуточных и требуемых многоструктурных макросостояниях, вывод результатов моделирования ЛПР, предварительный интерактивный структурно-функциональный анализ указанных результатов моделирования; формирование классов эквивалентных многоструктурных макросостояний КАИС.

Шаг 4. Автоматизированный ввод допустимых вариантов функционирования КАИС, проверка корректности заданной системы ограничений, окончательный выбор необходимого уровня агрегирования при описании моделей УСД КАИС, вычислительной схемы и плана вычислительных экспериментов по поиску оптимальных программ УСД КАИС.

Шаг 5. Поиск оптимальных программ управления структурной динамикой КАИС, при которых обеспечивался переход из заданного в синтезируемое многоструктурное макросостояние КАИС, устойчивое управление функционированием КАИС в промежуточных многоструктурных макросостояниях.

Шаг 6. Имитация условий реализации оптимального плана управления переходом КАИС из текущего в требуемое (выбранное) макросостояние при наличии возмущающих воздействий и с учетом различных вариантов их компенсации на основе методов и алгоритмов оперативного управления.

Шаг 7. Структурная и параметрическая адаптация плана, СПМО и информационного обеспечения ИмС к возможным (прогнозируемым на имитационных моделях) состояниям объекта управления (ОУ), управляющей подсистемы (УП), внешней среды. В ходе указанной адаптации, кроме того, вводится необходимый уровень структурной избыточности КАИС, обеспечивающий на этапе реализации плана компенсацию не предусмотренных в плане возмущающих воздействий.

После проведения требуемого числа вычислительных экспериментов осуществляется оценивание устойчивости сформированного адаптивного плана УСД КАИС.

Шаг 8. Вывод полученных результатов комплексного адаптивного планирования применения КАИС, их интерпретация и коррекция ЛПР.

Одно из главных достоинств предлагаемого метода поиска оптимальных программ УСД КАИС состоит в том, что в ходе формирования вектора программных управлений в финальный момент времени, наряду с оптимальным планом, одновременно получаем и то искомое многоструктурное макросостояние, находясь в котором КАИС сможет выполнять поставленные перед ней задачи в складывающейся (прогнозируемой) обстановке с требуемой степенью устойчивости.

В настоящее время разработаны комбинированные методы и алгоритмы решения задач выбора оптимальных программ УСД КАИС в централизованном и децентрализованном режимах ее функционирования. В качестве базового комбинированного метода предложено использовать сочетание метода ветвей и границ и метода последовательных приближений. Теоретическое обоснование данного метода основано на доказанной теореме о свойствах релаксированной задачи выбора оптимальной программы УСД КАИС. Особенности реализации предлагаемого комбинированного метода исследованы при решении различных прикладных задач [5–7].

При исследовании различных классов задач УСД КАИС были предложены алгоритмы параметрической и структурной адаптации соответствующих моделей, основанные на методах нечеткой кластеризации и анализа иерархий, методах аналитико-имитационного моделирования. Кроме того, для проверки конструктивности использования предлагаемого подхода к решению рассматриваемых задач осуществлялась разработка прототипа программного обеспечения процессов поиска оптимальных вариантов управления структурной динамикой КАИС различного целевого назначения [5–7].

Работоспособность программного комплекса была проверена на примере решения задач планирования модернизации и функционирования центра управления полетами навигационными космическими аппаратами (ЦУП НКА). Разработаны и исследованы несколько прототипов программ реализующих решения перечисленных задач. В докладе приводятся результаты исследования устойчивости планов совместного функционирования основного и дублирующего ЦУП НКА при различных сценариях воздействия внешней среды. Для описания моделей планирования в разработанном программном комплексе используется широко распространенный сегодня язык XML. Применение XML позволяет в одном файле хранить как исходные данные модели (процессы,

ресурсы и их характеристики), так результаты выполнения алгоритма построения оптимального плана, а также обеспечивает простоту сопряжения с другими программными комплексами, с помощью которых решаются задачи оптимального распределения ресурсов, отображения полученных результатов, интерактивного взаимодействия с лицом, принимающим решения.

Исследования по рассматриваемой тематике проводились при финансовой поддержке РФФИ (гранты 09–07–00066, 10–07–00311, 09–07–11004 ано, 10–08–90027 Бел_а), ОНИТ РАН (проект №2.3).

СПИСОК ЛИТЕРАТУРЫ

1. Беленков В.Г., Будзко В.И., Сеницын И.Н. Катастрофоустойчивость корпоративных информационных систем. Часть 1. М.: ИПИ РАН, 2002.
2. Белов П.Г. Системный анализ и моделирование опасных процессов в техносфере: учеб. пособие для студентов высш. учеб. заведений. М.: Издательский центр «Академия», 2003.
3. Будзко В.И., Беленков В.Г., Кейер П.А. К выбору варианта построения катастрофоустойчивых информационно-телекоммуникационных систем // Системы и средства информатики, 2003. вып 13. М.: Наука, с. 16–40.
4. Юсупов Р.М. Наука и национальная безопасность. М.: Наука, 2006. 290 с.
5. Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. М.: Наука, 2006. 410 с.
6. Калинин Б.Н., Соколов Б.В. Многомодельный подход к описанию процессов управления космическими средствами // Теория и системы управления. 1995. №1. С. 56–61.
7. Соколов Б.В., Юсупов Р.М. Комплексное моделирование функционирования автоматизированной системы управления космическими аппаратами. // Проблемы управления и информатики. 2002. №5. С. 103–117.

Афанасьев С.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО КОДА НА СТАДИИ РАЗРАБОТКИ**

Введение

С целью повышения качества и сокращения расходов на разработку и сопровождение в жизненный цикл разработки программного обеспечения (ПО) целесообразно интегрировать средства анализа программного кода и его уязвимостей. Особую важность приобретает усиление безопасности ПО на этапе разработки, начиная с возможно более ранней стадии.

По прогнозам к 2011 году по крайней мере 80% коммерческого ПО будет содержать открытый программный код. Поскольку поставщики ПО вставляют в свои продукты программные компоненты из открытых источников, внутренние разработчики также с большой вероятностью будут использовать их в своих разработках. Следовательно, вопросы, касающиеся архитектуры, качества, безопасности и уязвимости открытого кода приобретают все большее значение. По оценкам компании Palamida Inc. (Сан-Франциско) [1], поставщика технологий аудита ПО и прикладных решений по обеспечению безопасности открытого кода, около 70% открытого кода уязвимо и подвержено другим угрозам безопасности.

Анализаторы кода

Существует ряд анализаторов программного кода такие как Palamida, Ounce, WebGain, Sniff+ и другие [2]. Технология Palamida's сканирует код, проверяет его происхождение и сравнивает его с содержащимися в базе данных многочисленными программными компонентами с целью оценить и обеспечить определенный уровень его защищенности. Palamida идентифицирует известные уязвимости уже использующегося ПО. Аналогично функционируют и другие анализаторы, т.е. анализируется конечный продукт, что в ряде случаев требует возврата к начальным этапам разработки.

Одним из существенных препятствий по внедрению тестирования безопасности в жизненный цикл является разрыв между разработкой ПО и обеспечением его безопасности. Поскольку, этими двумя проблемами занимаются, как правило, разные люди или рабочие группы, синергетический эффект присущ процессу в целом в очень незначительной степени. В то время как разработчики фокусируют внимание на функциональности и выполнении графика разработки приложения, персонал, ответственный за безопасность приступает к устранению уязвимостей и осуществлению контроля безопасности только после завершения разработки приложений и их внедрения. Для эффективного устранения уязвимостей, возникающих в процессе разработки, между этими двумя группами должно быть установлено сотрудничество, так чтобы процессы разработки и обеспечения безопасности шли параллельно, и, соответственно, осуществлялось поэтапное интегрирование средств безопасности в жизненный цикл ПО.

В свете вышесказанного автоматизированный анализ кода признан наиболее эффективным методом тестирования защищенности ПО на ранних стадиях жизненного цикла, поскольку он позволяет оценить любую часть кода до завершения разработки всего приложения. Наилучшие из этих технологий обнаруживают каждую уязвимость с точностью до конкретной строки кода и предоставляют подробную информацию, касающуюся типа обнаруженного недостатка, степени его критичности и способа его исправления. Проникающее тестирование также является важным элементом безопасности ПО, но представляет наибольшую ценность на более поздних стадиях

жизненного цикла и используется для анализа завершеного приложения с функциональным интерфейсом.

Важность контроля ошибок на этапах анализа требований и проектирования спецификаций обуславливается возможностью их автоматического обнаружения на ранних этапах жизненного цикла (ЖЦ). CASE обеспечивает автоматическую верификацию и контроль проекта на полноту и состоятельность на ранних этапах ЖЦ, что влияет на успех разработки в целом. В подтверждение этого можно привести следующие статистические данные, основанные на отчетах фирмы TRW [5] по анализу 5 крупных проектов:

- при традиционной организации работ ошибки проектирования и кодирования составляют, соответственно, 64% и 32% от общего числа ошибок;
- ошибки проектирования в 100 раз труднее обнаружить на этапе сопровождения ПО, чем на этапах анализа требований и проектирования спецификаций.

В CASE диаграммы и верификаторы способны осуществлять следующие типы контроля:

1). Контроль синтаксиса диаграмм и типов их элементов. Обычно такой контроль осуществляется при вводе и редактировании элементов диаграмм. Примеры контролируемых ситуаций:

- по синтаксису: любой функциональный элемент диаграммы должен иметь по крайней мере один входной и один выходной поток; два элемента данных не могут быть непосредственно связаны;
- по типам: функциональный элемент должен всегда использоваться для представления процедурной компоненты; поток данных всегда должен быть представлен компонентой данных.

2). Контроль полноты и состоятельности диаграмм: все элементы диаграмм должны быть идентифицированы и отражены в репозитории. Например, для DFD контролируются неименованные или несвязанные потоки данных, процессы и хранилища данных; источники и стоки данных (внешние сущности) вне контекстной диаграммы; хранилища данных на контекстной диаграмме и т.п. При анализе словаря данных необходимо выявлять циклические определения, эквивалентные определения, неопределенные объекты.

3). Контроль декомпозиции функций включает оценку качества на основе различных метрик ПО и частичный семантический контроль.

4). Сквозной контроль диаграмм одного или различных типов на предмет их состоятельности по уровням – вертикальное и горизонтальное балансирование диаграмм.

При вертикальном балансировании (диаграммы одного типа) выявляются несбалансированные потоки данных между детализируемой и детализирующей диаграммами. Горизонтальное балансирование определяет некорректности между DFD, ERD, STD, словарями данных и мини спецификациями процессов. Так при балансировании DFD-ERD контролируется соответствие каждого хранилища данных на DFD сущности или отношению на ERD. Контроль DFD-STD осуществляется по следующим правилам: каждый управляющий процесс на DFD детализируется спецификацией управления STD, и наоборот, каждой STD должен соответствовать управляющий процесс; каждое условие (действие) в STD должно соответствовать входному (выходному) управляющему потоку на DFD, и наоборот, каждому управляющему потоку в зависимости от его направленности должно соответствовать условие/действие на STD.

Мини спецификации DFD-словаря данных следует проверять по следующим правилам:

- каждый поток и хранилище данных должны быть определены в словаре данных (контроль неопределенных значений), и наоборот, каждое определение в словаре должно быть отражено на диаграмме, в мини спецификации или другом определении (контроль неиспользуемых значений);
- каждый процесс на DFD должен детализироваться с помощью DFD или мини спецификации (но не тем и другим одновременно), и наоборот, каждая мини спецификация должна соответствовать единственному процессу;
- ссылки к данным в мини спецификациях должны соответствовать объектам на диаграммах и в словаре данных;
- по возможности должна контролироваться семантика мини спецификации: например, если входные и/или выходные потоки связаны с хранилищем данных, то это должно быть отражено в мини спецификации (операторами READ, GET, WRITE, PUT и т.п.).

Количественная оценка качества программного обеспечения

Сравнивать качество программных продуктов, руководствуясь интуитивными соображениями, не слишком удобно, поэтому целесообразность применения количественных методов оценки качества (метрик) очевидна. Дитер Ромбах (Dieter Rombach), сотрудник американской организации Software Engineering Laboratory (SEL), в 1991 г. на парижской конференции по вопросам компьютерных вычислений Euromantics заявил: "Мы больше не должны задаваться вопросом, нужны ли компьютерные метрики. Проблема заключается в том, как их строить". Подобный подход исповедует и Международная организация по стандартизации – ISO (стандарт ISO 9000–3). История программных метрик насчитывает четверть века, а началась она с того момента, когда стоимость коммерческих продуктов стала расти и потребовались научные методы создания стандартов и

анализа процессов разработки ПО [3, 4]. Программирование из искусства постепенно превращалось в инженерную дисциплину.

Введение строгих количественных метрик в программирование должно было способствовать решению ряда практических задач:

- предсказывать вероятное число ошибок в системе с самого начала проектирования;
- на основе анализа фазы проектирования системы предсказывать уровень сложности последующего сопровождения;
- на основе анализа исходного кода программ прогнозировать уровень сложности процессов тестирования и процент остающихся ошибок;
- по оценкам сложности фазы проектирования системы определять конечный размер кода;
- определять корреляцию отдельных характеристик программного кода с качеством готовой системы;
- контролировать стадии развития проекта;
- анализировать явные и скрытые дефекты;
- на основе экспериментального сравнения выявлять лучшие методы и технологии.

При использовании объектно-ориентированного программирования активно используется унифицированный язык моделирования (UML). Существует ряд CASE-систем (Computer Aided Software Engineering), которые опираются на этот язык при проектировании, моделировании даже автоматизированной генерации кода. Наиболее популярны из таких систем Rational Rose (фирмы Rational) и Together (фирм TogetherSoft и Borland). Причем в систему Together включена возможность анализа проектируемой и разрабатываемой программной системы с помощью метрик и аудита на каждом этапе разработки. Более того, система имеет открытый интерфейс, что позволяет встраивать более мощные анализаторы генерируемого кода, в частности используется анализатор Sniff+.

Ценность метрик заключается в их применении к программам. В то время как существует множество рекомендаций относительно того, как интерпретировать метрики, не имеется достаточного количества статистических данных, доказывающих, что значение 8 для одной метрики вдвойне сложнее или вдвойне «хуже», чем 4. Поэтому предлагаются рекомендации по интерпретации, основанные на сравнении значений, чтобы определить, чем они отличаются от других модулей кода. Это не индикация «вредности», а индикатор различия, который должен быть исследован. Таблица 1 представляет пример желательных значений метрик.

Таблица 1

Рекомендации по интерпретации метрик

Метрика	Желательное значение
Циклическая сложность	Низкое
Строки кода/Выполнимые операторы	Низкое
Процент комментария	~ 20 – 30 %
Взвешенные методы на класс	Низкое
Отклик для класса	Низкое
Недостаток единства методов	Низкое
Единство методов	Высокое
Связь между объектами	Низкое
Глубина наследования	Низкое (связь)
Число потомков	Низкое (связь)

Однако, как показано в двух последних метриках, имеется связь между многими метриками. Большая глубина дерева наследования увеличит сложность поддержки, но также увеличит возможность повторного использования. Высокое число потомков увеличит усилия, затрачиваемые на тестирование, но попутно также увеличит степень эффективности повторного использования. Изменение размера какой-либо метрики может влиять на тестирование, понимаемость, возможность поддержки, усилия, затрачиваемые на разработку и повторное использование.

СПИСОК ЛИТЕРАТУРЫ

1. Корпорации Palamida. 2010. URL: <http://www.palamida.com/solutions/open-source-vulnerability-testing.html>. (дата обращения 05.05.2010)
2. Rational Unified Process, ver. 2002.05.00.25, Rational Software Corporation.
3. www-142.ibm.com/software/products/us/en/category/rational?pgel=lnav (дата обращения 05.05.2010).
4. Booch G, Object Oriented Analysis and Design with Applications, The Benjamin/Cummings Publishing Company, Inc., 1994, P. 431.
5. Jacobson I, Object Oriented Software Engineering. A Use Case Driven Approach, Addison-Wesley Publishing Company. 1993. P. 382.
6. IEEE Computer Society, 1990, <http://tcse.org/> (дата обращения 05.05.2010).

Блюм В.С., Заболотский В.П.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПАЦИЕНТОВ КАК КОМПОНЕНТА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА**

Введение

В ежегодном докладе ВОЗ (Всемирная организация здравоохранения) о состоянии здравоохранения в мире (2008 г.) отмечено: «Безопасность – основополагающий принцип лечения пациентов и критический компонент системы управления качеством. Для повышения безопасности необходимы всеобъемлющие и комплексные усилия на уровне системы в целом. Они должны охватывать практически все медицинские профили и всех участников системы, а для этого требуется комплексный, многосторонний подход к выявлению и управлению реальными и потенциальными рисками, угрожающими безопасности пациентов, как при оказании им отдельных медицинских услуг, так и в плане необходимости поиска общих долгосрочных решений, направленных на совершенствование системы в целом.» [8].

Проблемы информированной безопасности пациентов и оперативного обнаружения врачебных ошибок без сомнения относятся к сфере информационной безопасности государства. Ущерб, который наносят некачественные медицинские услуги, исчисляется сотнями тысяч человеческих жизней (точной цифры российская медицинская статистика не предоставляет).

В промышленно развитых странах приблизительно один пациент из десяти страдает от вреда, нанесенного неблагоприятными явлениями, возникшими в ходе лечения и которых можно было бы избежать [1]: только в США такие осложнения являются причиной более 98 тысяч смертных случаев ежегодно для пациентов, проходящих лечение в стационарах [2].

По оценкам ВОЗ [8] около 20% врачебных ошибок связано с неполнотой данных или невозможностью оперативного получения необходимой информации.

Решение указанных проблем лежит на пути создания единого информационного пространства здравоохранения, в основу которого должна быть положена система полной, достоверной и доступной первичной медицинской информации. При этом задача состоит в том, чтобы определить источники первичной медицинской информации, трезво оценить объём и интенсивность её производства и, на основе полученных данных, предложить эффективную технологию сбора, хранения и использования этих данных для повышения уровня безопасности пациентов.

Анализ многочисленных историй болезни указывает на то, что в отечественном здравоохранении имеется два основных класса источников первичной медицинской информации (информации о состоянии здоровья пациентов). Такими источниками являются, во-первых, множество действующих дипломированных врачей и, во-вторых, множество лицензированных диагностических лабораторий (ДЛ). Именно эти и только эти деятели системы охраны здоровья допущены государством для оценки состояния здоровья пациентов. Только они имеют право и обязаны фиксировать данные (писать тексты, строить графики, фиксировать изображения) о здоровье граждан своей страны, а также предлагать и записывать схемы их лечения.

1. Оценка объёма и интенсивности первичной медицинской информации

Для оценки информационного потока необходимо ввести ряд определений и зафиксировать численный состав источников первичной медицинской информации.

Медицинские услуги - это деятельность системы здравоохранения, непосредственно удовлетворяющая личные потребности членов общества, потребности разного рода предприятий, объединений, организаций, общественные потребности или потребности общества в целом в охране здоровья, которые не имеют материально-вещественной формы воплощения [9].

Первичными медицинскими услугами назовём услуги, которые оказывают пациентам дипломированные врачи и лицензированные диагностические лаборатории.

Под первичной медицинской информацией будем понимать только те данные, которые возникают в результате предоставления медицинской услуги пациенту со стороны врача или диагностической лаборатории.

Определение 1. Реализацией информационной медицинской услуги (РИМУ) будем называть документ, который формируется в результате проведения конкретного сеанса взаимодействия врача или диагностической лаборатории с пациентом и не может быть изменен без проведения повторного сеанса.

Каждая встреча пациента с врачом или контакт пациента с ДЛ приводит к возникновению документа (текста, графика, изображения), синтаксис которого имеет следующий вид:

<РИМУ ВРАЧА>::=<время сеанса>< идентификатор ВРАЧА>
<идентификатор ПАЦИЕНТА>< документ ВРАЧА> (1)

или

<РИМУ ДЛ>::=<время сеанса>< идентификатор ДЛ>
<идентификатор ПАЦИЕНТА>< документ ДЛ> (2)

Предположим, что каждый из работающих по специальности (дипломированных, лицензированных, сертифицированных, аттестованных) врачей имеет свой уникальный идентификатор. А полный перечень идентификаторов представлен в государственном реестре врачей. Этот реестр необходим для проверки права конкретного врача предоставлять соответствующие информационные медицинские услуги пациенту. Такую же контрольную функцию должен выполнять и государственный реестр работающих (лицензированных) диагностических медицинских лабораторий, в котором зафиксирован полный перечень соответствующих уникальных идентификаторов.

Пусть n – число идентификаторов в реестре врачей, а m – число идентификаторов в реестре диагностических лабораторий (ДЛ).

Построим неубывающую функцию $I_{nm}(t)$, значением которой будет количество информации, накопленное указанными источниками системы здравоохранения от начала отсчёта до момента t .

Пусть результат каждой информационной медицинской услуги записывается на цифровой компакт-диск (CD-диск). Выберем такой тип диска, объём которого достаточен для записи самого большого из возможных медицинских информационных массивов.

Каждый акт взаимодействия пациента с врачом или ДЛ будем связывать с возникновением CD-диска, на котором записана информация о состоянии здоровья пациента, выявленная и зафиксированная врачом или ДЛ в конкретном сеансе обслуживания.

Предположим, что материализованная таким образом информационная медицинская услуга без промедления складывается в определенном месте в две стопки CD-дисков: CD врачей и CD диагностических лабораторий (рисунок 1).



Рис. 1. Коллекции CD первичной медицинской информации

Оценим размеры «информационных» коллекций и объём сохранённой в них в течение года информации.

Согласно официальной статистике в России в течение года регистрируется около 200 млн. заболеваний [3].

Если принять, что в процессе обслуживания каждого заболевания врачи пишут только две страницы текста о состоянии больного (результаты общего осмотра, анамнез, диагноз, назначения) и несколько параметров измерений (температура, давление и т.п.), что в сумме составит около 5 кбайт новой информации, то за год минимальный объём новых данных о состоянии здоровья нации составит около 1000 Гбайт. При этом, если предположить, что для обслуживания одного заболевания пациент только два раза встречается с врачом (чтобы открыть и закрыть больничный лист), то число дисков, созданных врачами, составит 400 млн. штук – столб размером 480 км (высота CD – 1,2 мм).

С другой стороны, в России работает около 700 тыс. врачей [4]. Не имея достоверной информации о количестве диагностических лабораторий (ДЛ), примем, что их число соответствует числу лечебно-профилактических учреждений (ЛПУ), т.е. около 20 тыс.

Положим, что в течение рабочего дня врач обслуживает 10 пациентов, а ДЛ обслуживает 20 пациентов. Пусть в результате каждой встречи с пациентом врач пишет одну страницу текста объёмом 2 кбайт, а ДЛ генерирует массив данных размером 50 кбайт. Тогда в течение года врачами будет написан текст объёмом 3500 Гбайт (1750 млн. штук CD – столб размером 2100 км), а ДЛ сгенерируют файл объёмом 5000 Гбайт (100 млн. штук CD – столб размером 120 км).

Итогом наших построений стало создание двух базовых информационных коллекций здравоохранения – полного набора первичных медицинских данных о нездоровье нации. Этот набор соответствует современному уровню развития системы охраны здоровья и является единственным источником информации такого рода. Благодаря выбранному способу нормировки (размещение данных об одной медицинской услуге на CD стандартного размера) мы можем не только посчитать количество оказанных медицинских услуг, но и измерить объём накопленной информации как в традиционных битах, так и в условных «метрах».

Таким образом, врачи создают в год от одного до трёх с половиной терабайтов текстов о состоянии здоровья своих пациентов, то есть не менее 200 тысяч томов по 500 страниц каждый. А диагностические лаборатории в течение года производят информацию, издание которой потребует не менее 20 тысяч иллюстрированных томов объёмом 500 страниц каждый.

В результате первого шага проведённого анализа собраны две коллекции ранжированных по времени создания документов вида (1) и (2), сумма которых, по нашему мнению, обладает свойством полноты. Можно утверждать, что не существует иной первичной медицинской информации о состоянии здоровья нации, кроме собранной в указанных двух коллекциях документов, суммарная величина которой определяется значением функции $I_{nm}(t)$ на заданном интервале времени.

Справедливости ради, следует указать на неоднородность каждого из выделенных классов источников медицинской информации, что, тем не менее, не должно препятствовать процессу создания государственных реестров действующих врачей и диагностических лабораторий – объектов повышенной опасности для здоровья граждан.

2. О разнообразии источников первичной медицинской информации

Что можно сказать о разнообразии врачей-писателей? Согласно приказа Минздравсоцразвития России от 11.03.2008 г. №112н «О номенклатуре специальностей специалистов с высшим и послевузовским медицинским и фармацевтическим образованием в сфере здравоохранения Российской Федерации» – это лица, закончившие ВУЗ по специальностям, представленным в таблице 1.

Таблица 1

Классы медицинских специальностей, получаемых в ВУЗе

№ п/п	Специальность, полученная в вузе
1	Лечебное дело
2	Педиатрия
3	Медико-профилактическое дело
4	Стоматология
5	Фармация
6	Сестринское дело
7	Медицинская биохимия
8	Медицинская биофизика
9	Медицинская кибернетика

В результате дополнительного обучения в интернатуре и (или) ординатуре врач получает одну из основных специальностей, представленных в таблице 2.

Таблица 2

Основные врачебные специализации

№ п/п	Основная специальность	№ п/п	Основная специальность
1	Акушерство и гинекология	21	Терапия
2	Анестезиология и реаниматология	22	Травматология и ортопедия
3	Дерматовенерология	23	Фтизиатрия
4	Детская хирургия	24	Хирургия
5	Генетика	25	Эндокринология
6	Инфекционные болезни	26	Клиническая лабораторная диагностика
7	Клиническая лабораторная диагностика	27	Общая гигиена
8	Неврология	28	Социальная гигиена и организация госсанэпидслужбы
9	Неонатология	29	Эпидемиология
10	Общая врачебная практика (семейная медицина)	30	Стоматология общей практики
11	Онкология	31	Клиническая лабораторная диагностика
12	Организация здравоохранения и общественное здоровье	32	Управление и экономика фармации
13	Оториноларингология	33	Фармацевтическая технология
14	Офтальмология	34	Фармацевтическая химия и фармакогнозия
15	Патологическая анатомия	35	Управление сестринской деятельностью
16	Педиатрия	36	Генетика
17	Психиатрия	37	Клиническая лабораторная диагностика
18	Рентгенология	38	Судебно-медицинская экспертиза
19	Скорая медицинская помощь	39	Клиническая лабораторная диагностика
20	Судебно-медицинская экспертиза	40	Рентгенология

Можно насчитать 140 наименований врачебных специализаций, определённых нормами российского медицинского образования. Например, врач с основной специальностью «педиатрия» может приобрести одну из двадцати двух квалификационных специализаций.

Несмотря на отмеченное разнообразие специализаций, общим свойством врачебной деятельности является то, что каждый врач обязан фиксировать свои наблюдения и решения в форме текстов. Объем писательской работы поглощает до 50% рабочего времени врача.

Одной из основных трудностей на пути к обработке врачебных текстов является чрезвычайно большая размерность пространства понятий, используемых в современной медицине. По оценкам экспертов оно содержит более двух миллионов понятий и терминов. Для сравнения, издание Оксфордского словаря английского языка содержит 615 тысяч слов, а в Большом толковом словаре русского языка – 135 тысяч слов.

Разнообразие методов диагностических исследований пациентов не многим меньше разнообразия врачебных специальностей. Более того, число методов объективного контроля быстро увеличивается, что обусловлено высокими темпами научно-технического прогресса.

Современный объем лабораторных исследований в рамках оказания амбулаторно-поликлинической помощи характеризуется следующим разнообразием:

- биохимические исследования;
- гематологические исследования;
- общеклинические (неинвазивные) методы исследования;
- иммунологические исследования;
- паразитологические исследования;
- цитологические исследования;
- токсикологические исследования;
- химико-токсикологические исследования;
- бактериология.

Разнообразие типов цифровых медицинских данных, для хранения, визуализации и обмена которыми используется формат стандарта DICOM (Digital Imaging and Communication in Medicine) представлено в таблице 3. В данном стандарте в понятия информационных объектов введены не только изображения и графические данные, но также и протоколы и описания исследований; определены формы взаимодействия и способы описания этих объектов в компьютерных сетях.

Таблица 3

Типы визуальных результатов медицинских исследований

№ п/п	Типы медицинских изображений	№ п/п	Типы медицинских изображений
1	Ангиография	21	Рентгеноскопия
2	Ангиокардиография	22	Электрорентгенография
3	Аудиометрия	23	Флюорография
4	Биопсия	24	Томография
5	Бронхоскопия	25	Реография
6	Векторкардиография	26	Реогаптография
7	Гистеросальпингография	27	Реокардиография
8	Катетеризация сердца	28	Реопульмонография
9	Кольпоскопия	29	Реоэнцефалография
10	Лапароскопия	30	Термография
11	Мониторное наблюдение	31	Томография компьютерная
12	Определение глазного давления	32	Ультразвуковая диагностика
13	Пункция	33	Урография
14	Радиоизотопная диагностика	34	Фонокардиография
15	Радиография	35	Холеграфия
16	Радиометрия	36	Электрокардиография
17	Сканирование и сцинтиграфия	37	Электрэнцефалография
18	Определение радиоактивности биологических проб	38	Эндоскопические методы обследования
19	Радиоизотопное исследование в пробирке	39	Ядерный магнитный резонанс
20	Рентгенодиагностика		

И в этом случае, общим свойством диагностических исследований является то, что их обязательной составляющей являются текстовые данные, которые сопровождают графики или изображения.

Разнообразие врачебных специализаций, а также методов и результатов лабораторных исследований, не может быть препятствием к формированию единого информационного пространства первичных медицинских документов, которое должно быть полным и достоверным. Очевидно, что изъятие любого документа (рис.1) может привести к фатальной врачебной ошибке.

3. Полная и достоверная система первичных медицинских документов

На втором шаге мысленного эксперимента выполним копирование ранее созданных CD врачей и ДЛ. Из этих копий создадим ещё один многокилометровый ранжированный по времени столб данных, которые станут собственностью пациентов – CD пациентов (рис. 2).

Мотивом для двукратного увеличения объёма хранимой информации является наше стремление исключить всякую фальсификацию, которая может стоить жизни пациенту. Достоверными будем считать только те CD пациентов, для которых существует точная оригинальная копия.

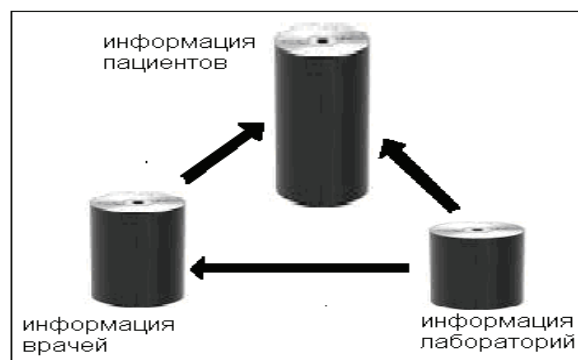


Рис. 2. Система полной и достоверной первичной медицинской информации

Пусть k – число идентификаторов различных пациентов, обслуженных на заданном интервале времени. Тогда функция $I_{nmk}(t)$ количества достоверной информации имеет вид:

$$I_{nmk}(t) = 2I_{nm}(t).$$

После того, как указанные три набора данных сформированы, над ними могут быть определены для любого заданного интервала времени функции $N(t)$ – число различных идентификаторов врачей и $M(t)$ – число различных идентификаторов диагностических лабораторий (ДЛ). Для вновь организованного набора данных пациентов, определим функцию $K(t)$ – число различных идентификаторов пациентов. Функция $K(t)$ вычисляется методом последовательного перебора CD пациентов для заданного интервала времени. Чтобы не возникало коллизий при формировании столба CD пациентов и расчете функции $K(t)$, позаботимся об однозначной идентификации пациентов, полагая, что идентификатор пациента соответствует номеру его полиса ОМС из единого всероссийского реестра.

Полная и достоверная система медицинских данных является воплощением идеи академика РАМН и РАН Андрея Ивановича Воробьева о том, что лечащий врач не может быть простым регистратором заключений лабораторий и диагностических служб; ему необходим весь объем первичной медицинской информации – и рентгеновские снимки, и фотографии гистологических препаратов и т.д.

4. Персонализированная система первичных медицинских документов

На этом шаге эксперимента проведём сортировку каждого из трёх столбов CD по соответствующему ключевому параметру: идентификатор врачей – для CD врачей, идентификатор ДЛ – для CD ДЛ, идентификатор пациентов – для CD пациентов. В результате получим три класса персонализированных коллекций медицинских документов: коллекции врачей, ДЛ и пациентов (рис. 3).

Отметим, что процедура сортировки не должна нарушать ранжирования документов по времени внутри каждой персональной коллекции.

Пусть $\{V_1, V_2, \dots, V_n\}$ – коллекция документов, сформированных врачами, где V_i , $i \in [1(1)n]$ – идентификатор врача (например, номер действующей лицензии), который может использоваться в качестве основы адреса сетевого ресурса для доступа к этим данным, а также для формирования гиперссылок к ресурсам, в которых хранятся данные обслуженных пациентов.

Обозначим как $\{L_1, L_2, \dots, L_m\}$ – коллекцию документов, сформированную диагностическими лабораториями. Эта коллекция имеет аналогичную структуру аналогичную структуре коллекции врачебных данных и ту же смысловую нагрузку.

Коллекция документов $\{P_1, P_2, \dots, P_k\}$ сформирована для пациентов, где P_i , $i \in [1(1)k]$ – это идентификатор пациента (например, номер его полиса ОМС), который может быть использован для автоматического формирования (вычисления) имени соответствующего сетевого ресурса. Коллекция с именами документов P_i – это ни что иное, как медицинские карты пациентов. Коллекция представлена, в данном случае, в виде стопки ранжированных по времени CD-дисков, каждый из которых имеет гиперссылку к оригинальному документу врача (рис. 4). Гиперссылки строго упорядочены по времени. В этом ряду, очевидно, первым является документ о рождении пациента, а заключительным станет документ, в котором врач фиксирует смерть пациента.

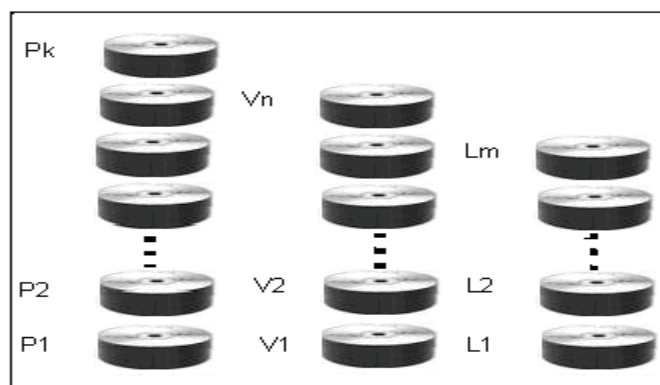


Рис. 3. Три класса персонифицированных коллекций медицинских документов

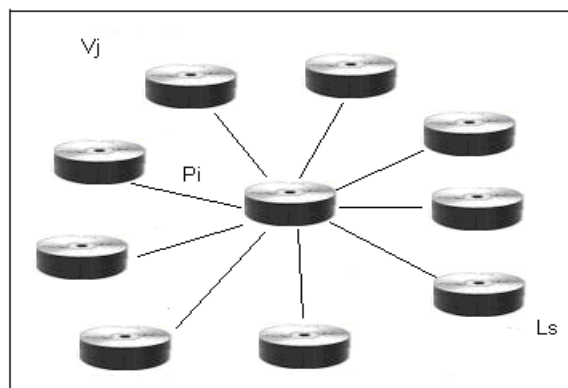


Рис. 4. Фрагмент сетевого распределения медицинских данных пациента

Следует отметить, что коллекция документов $\{V_1, V_2, \dots, V_n\}$ – это ни что иное, как собрание историй врачевания каждого допущенного к этой работе доктора, записная книжка врача. Документ врача V_i – это тот объект, который является предтечей современных историй болезни и к которому сегодня можно адресовать слова Н.И.Пирогова: “Усовершенствования во врачебном искусстве можно добиться только путем изучения ошибок, допущенных у постели больного” [10].

5. Формирование индекса здравоохранения

В докладе Всемирной организации здравоохранения отмечено, что около 20% врачебных ошибок связано с неполнотой данных или невозможностью оперативного получения необходимой информации.

Предыдущие шаги мысленного эксперимента были посвящены формированию полной и достоверной системы медицинской информации. Теперь мы можем отказаться от измерения информации в «метрах», выделить для каждой коллекции $\{V_1, V_2, \dots, V_n\}$, $\{L_1, L_2, \dots, L_m\}$ и $\{P_1, P_2, \dots, P_k\}$ документов, $n + m + k$ – персональных сетевых ресурсов в распределённой сети и заняться разработкой способа оперативного получения необходимых данных.

Для оперативного доступа к информации необходима специализированная поисковая машина, в основе которой лежит постоянно корректируемый поисковый индекс здравоохранения.

Индексом здравоохранения будем называть матрицу, которая ставит в соответствие полному перечню используемых в современном здравоохранении терминов содержащие их документы.

Предлагаемая структура поискового индекса близка к классической, которая описана в литературе [6,7]. В его основе лежат инверсные списки вхождений слов, которые используются для поиска релевантных документов, а также прямые индексы термов для формирования фрагментов, возвращаемых пользователю.

При формировании индекса здравоохранения надо учитывать две особенности системы данных: во-первых, каждая запись в рассматриваемых коллекциях документов содержит три обязательных атрибута: время события, идентификатор пациента и идентификатор источника информации, во-вторых, в пространстве документов всегда присутствует копия любой записи.

Индекс формируется специальной программой – сетевым роботом («пауком»). Паук не копирует страницы сайтов в индекс поисковой машины, а сохраняет информацию о структуре каждого документа сайта – например, какие слова встречаются в документе и в каком порядке, адреса гиперссылок страницы сайта, размер документа в килобайтах, дата его создания и многое другое.

Обмен данными между процессорами поиска характеризуется параметрами вычислительной среды, к которой подключены соответствующие серверы, и не могут быть изменены в рамках

конкретной технической реализации. Из этого факта следует необходимость решения следующих двух проблем:

1. Проектирование топологии подключения серверов поисковой системы, в которой минимальны риски конфликтов между информационными потоками.

2. Минимизация количества передаваемых данных в условиях запросов термов.

Попутно необходимо решить достаточно много мелких, неприятных, но необходимых, задач «очистки документов»: ликвидация переноса слов и фиксация таблиц, проверка алфавита и словосочетаний, проверка структуры, форматирование текста, ликвидация лишних пустых строк и строк разметки и т.п.

Построение предметного индекса на однородной коллекции документов это, по существу, процедура семантического сжатия информации.

На первом этапе выполняется последовательно несколько известных алгоритмов семантического сжатия индекса слов коллекции, полученного после стандартной операции индексирования, а именно:

- извлечение стоп-слов (наречий, союзов, предлогов и т.д.),
- учёт статистических закономерностей текстов (ранговые распределения как системное свойство текстов),
- морфологическая коррекция терминов и коррекция по частям речи,
- определение словосочетаний в полученном наборе терминов.

Структуры данных должны быть выбраны так, чтобы они допускали подключение таких параметров оценки терминов, как позиционное взвешивание и взвешивание по инверсной частоте.

На втором этапе вычисляются соотношения терминов в виде статистических данных, определяются семантические связи между терминами и выполняется усечение словаря терминов. Критерием усечения является малое число связей термина с другими терминами. Результатом второго этапа является минимизированный словарь связанных терминов, по существу представляющий предметный индекс коллекции медицинских документов.

Следует отметить, что борьба за оперативный доступ к медицинской информации имеет свою цену – объём базы данных индекса имеет тот же порядок, что и исходный объём хранимых данных.

Обозначим $I_{nmk}^i(t)$ – функция количества полной, достоверной и индексированной информации на заданном интервале времени. Тогда $I_{nmk}^i(t) \approx 3I_{nm}(t)$.

Таким образом, определена система полной и достоверной первичной медицинских информации, к которой гарантирован оперативный доступ с помощью индекса здравоохранения.

Заключение

Показана возможность построения единого информационного пространства здравоохранения, которое опирается на систему очевидных информационных источников, с известным объёмом и динамикой производимой ими медицинской информации.

Важной задачей в формировании информационного пространства здравоохранения является создание и мониторинг реестров действующих врачей и диагностических лабораторий, как объектов повышенной опасности для жизни граждан.

Первоочередными объектами информатизации здравоохранения должны стать карты (истории) врача и диагностических лабораторий, которые являются единственными (безальтернативными) источниками полной первичной медицинской информации. Дисциплинируя работу информационных источников, государством может быть решена проблема формирования и автоматизированного контроля истории болезни пациентов, которая станет простой технической задачей.

Поисковый индекс первичной медицинской информации – это индекс нездоровья нации (индекс здравоохранения), с помощью которого может быть оперативно получен релевантный ответ на любой запрос, касающийся информации о встречах пациентов с системой здравоохранения.

Решение проблемы создания системы полной, достоверной и доступной первичной медицинской информации должно рассматриваться как необходимое условие информационной безопасности пациентов, то есть всех граждан государства.

СПИСОК ЛИТЕРАТУРЫ

1. Shiffman J. Has donor prioritization of HIV/AIDS displaced aid for other health issues? *Health Policy and Planning*, 2008, 23:95–100.
2. Kohn LT, Corrigan JM, Donaldson MS, eds. *To err is human: building a safer health system*. Washington DC, National Academy Press, Committee on Quality of Care in America, Institute of Medicine, 1999.
3. Официальная медицинская статистика. [Электронный ресурс]. — Режим доступа: http://www.mzrd.ru/?f=np_about_pro
4. Медицинская статистика. [Электронный ресурс]. — Режим доступа: <http://www.medlinks.ru/article.php?sid=30795>
5. Peierls R. Model-Making in Physics. — *Contemp. Phys.*, January/February 1980, v. 21, pp. 3–17; Перевод: *Пайерлс Р.*, Построение физических моделей, УФН, 1983, №6.
6. G. Salton, C. Buckley. Term-weighting approaches in automatic text retrieval. // *Information Processing and Management: an International Journal*, Volume 24, Issue 5. P. 513 – 523, 1988.

7. S. Brin, L. Page. The Anatomy of a Large-Scale Hypertextual Web Search Engine. // In Computer Networks and ISDN Systems, Volume 30, number 1–7, pages 107–117, 1998.
8. Официальный сайт Всемирной организации здравоохранения. [Электронный ресурс]. — Режим доступа: <http://www.who.int/ru/>
9. Мировая экономика: учеб. / Л.С. Падалкина, В.В. Клочков, С.В. Тарасова [и др.]; под ред. И.П. Николаевой. М.: Проспект, 2009. — 240 с.
10. Сочинения Н. И. Пирогова в двух томах. СПб. 1887 (изд. 2-е, СПб., 1900).

Гарбук С.В., Завируха В.К., Комаров А.А.

Россия, Санкт-Петербург, Арктический и антарктический научно-исследовательский институт, Москва, ЗАО «Научно-технический центр «Станкоинформзащита»

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА КРИТИЧЕСКИ ВАЖНЫХ ТЕХНОЛОГИЧЕСКИХ ОБЪЕКТАХ

Современный, пятый [1], период развития информационной индустрии, наступивший после 2000 года, характеризуется глобальной информатизацией, виртуализацией и интеграцией знаний, переходом к информационному обществу, электронному государству, электронному бизнесу и т.д. Особенно велика значимость информационных технологий в развитии так называемых технологических объектов, т.е. объектов, предназначенных для реализации некоторых технологических процессов или их совокупности [2]. Подобные объекты функционируют в сферах энергетики, промышленности и транспорта, социально-экономического обеспечения и здравоохранения, поддерживают сектора связи и телекоммуникаций, государственного управления и обороны страны, предупреждения и ликвидации последствий чрезвычайных ситуаций. Учитывая критическую важность технологических объектов для обеспечения нормального функционирования отдельных отраслей экономики и поддержания обороноспособности страны, проблема обеспечения информационной безопасности на технологических объектах является одной из ключевых, в том числе на региональном уровне.

Актуализация этой проблемы на современном этапе технологического развития и реформирования экономики страны обуславливается следующими факторами:

- возрастание ущерба (экономического, военно-политического, экологического и др.) от аварий и сбоев на критически важных технологических объектах (КВТО), связанное с усилением зависимости экономики и обороноспособности современного государства от КВТО, увеличением их энергонасыщенности и экологической опасности;
- повышение уровня автоматизации технологических объектов и, соответственно, их доступности и уязвимости для средств информационно-технологического воздействия;
- агрегирование ключевых технологических инфраструктур, вызванное хозяйственно-экономическими процессами на этапе глобализации экономики, и, как следствие, рост числа критических уязвимых точек в КВТО;
- опережающее совершенствование средств информационно-технологического воздействия, происходящее на фоне общего развития информационной индустрии.

В частности, за минувшие годы по данным Центра хранения данных об инцидентах информационной безопасности на промышленных объектах (The Repository of Industrial Security Incident, RISI) [3] и британского Центра защиты национальных инфраструктур (CPNI, Centre for the Protection of National Infrastructure) [4] было зафиксировано свыше 100 случаев реализации угроз информационной безопасности КВТО, среди которых:

- проникновение хакеров в сеть индийского ядерного исследовательского центра в BARC (1 июля 2002 года);
- заражение червём Slammer энергетической станции Davis-Besse (США, штат Огайо, 15 января 2003 года);
- нарушение воздушного сообщения на юге Великобритании, включая аэропорт Хитроу, зафиксированное британской Национальной организацией управления воздушным движением (12 сентября 2008 года);
- приостановка движения поездов на всей территории Израиля, вызванная серьезными сбоями в АСУ на железной дороге (24 мая 2009 года).

Базовой ИТ-компонентой технологических объектов, определяющей уровень информационной безопасности КВТО, являются автоматизированные системы управления технологическими процессами (АСУ ТП), представляющие собой комплекс программно-технических средств, предназначенных для автоматизации функций управления технологическим оборудованием и реализуемым на нём технологическим процессом, а также для автоматизации информационных и вспомогательных функций. АСУ ТП состоит из единой системы управления, включающую один или несколько пультов управления, средства обработки и архивирования информации о ходе контролируемых процессов, а также типовые элементы автоматики: телеметрические датчики, контроллеры и исполнительные устройства.

Для реализации АСУ ТП в настоящее время широко используются системы сбора данных и диспетчеризации (Supervisory Control and Data Acquisition, SCADA-системы) и распределенные системы управления (Distributed Control System, DCS). В состав SCADA входят диспетчерский пункт управления (Master Terminal Unit, MTU), удаленные терминалы (Remote Terminal Unit, RTU) для сбора информации и управления объектами автоматизации и коммуникационная система (Communication System, CS). SCADA-системы создаются как универсальные продукты, базирующиеся на технологии открытых систем, подлежащие адаптации к конкретному технологическому объекту на этапе инсталляции. В то же время, DCS изначально являются «частнофирменным» решением, уникальным для каждой отдельной АСУ ТП.

Особенностями современных АСУ ТП как объектов обеспечения информационной безопасности являются:

- преобладание операционных систем реального времени, принципиальная невозможность применения в АСУ ТП механизмов обеспечения безопасности, нарушающих режим реального времени обработки информации;
- применение пакетных телеметрических каналов и компьютерных радиосетей для передачи данных на протяженных объектах (линии электропередач, трубопроводы, транспортные магистрали и т.п.);
- интеграция с производственными вычислительными сетями (Business Area Network, BAN), использование промышленных протоколов передачи данных;
- использование в КВТО значительного количества АСУ ТП импортной разработки, для которых условием поставки является обслуживание фирмой-поставщиком на этапах гарантийного и послегарантийного обслуживания. Если в АСУ ТП циркулирует информация ограниченного доступа, то при допуске стороннего обслуживающего персонала возникают определенные сложности, связанные с необходимостью удаления остаточной информации в системе. В частности, особую актуальность эта проблема приобретает в автоматизированных системах, включающих оборудование с числовым программным управлением.

Учитывая, что критически важные технологические объекты могут иметь различные формы собственности (государственная, частная, смешанная) основными источниками угроз информационной безопасности этих объектов (в порядке убывания вероятности реализации угроз) являются:

- представители неформальных Интернет-сообществ («хакеры»), не имеющие рациональных мотивов;
- террористические организации;
- недобросовестные конкуренты;
- негативно настроенные инсайдеры;
- специальные службы иностранных государств.

При этом особое значение придается обеспечению целостности и доступности информации, обрабатываемой в АСУ ТП. Требования по конфиденциальности циркулирующей информации, в отличие от традиционных задач обеспечения информационной безопасности, может не предъявляться вовсе.

Анализ последствий воздействия на КВТО целесообразно проводить в соответствии с рекомендациями Координационного центра реагирования на компьютерные угрозы (Computer Emergency Response Team, CERT) [5]. Применительно к АСУ ТП список угроз и атак в порядке убывания их важности может быть представлен следующим образом:

- угрозы физической безопасности людей;
- атаки на уровне суперпользователя или системном уровне на любую административную информационную систему или часть инфраструктуры магистральной сети;
- атаки на уровне суперпользователя или системном уровне на любую машину, предоставляющую крупный сервис, многопользовательский или специализированный;
- компрометация установок программного обеспечения, особенно тех, что используются администраторами и приложениями, работающими с информацией ограниченного доступа;
- атака на доступность сервисов, перечисленных в предыдущем пункте;
- любое из перечисленных выше нападений, направленных на другие информационные подсистемы АСУ ТП;
- масштабные атаки любого типа, например, перехват пакетов, атаки на пароли;
- угрозы, причинение беспокойства и другие противоправные действия, направленные на отдельных пользователей.

Учитывая, что в соответствии с [6] считается, что АСУ ТП реализовывает управляющие, информационные и вспомогательные функции, для оценки угроз информационной безопасности необходимо учитывать, на какую из функций оказывается деструктивное воздействие, причем функции выше перечислены в порядке убывания их важности. Так, наиболее значимые управляющие функции включают получение информации о состоянии технологического объекта управления,

оценку информации, выбор управляющих воздействий и их реализацию. Под информационными функциями понимают получение информации, обработку и её передачу персоналу АСУ ТП или вовне системы о состоянии технологического объекта управления или окружающей среды. Наименее критичные вспомогательные функции заключаются в сборе и обработке данных о состоянии АСУ ТП и либо предоставление этой информации персоналу системы, либо осуществление управляющих воздействий на соответствующие технические и (или) программные средства АСУ ТП.

На сегодняшний день число производителей и номенклатура SCADA-систем весьма ограничены. В таблице 1 в качестве примера приведены наименования основных разработчиков и производителей SCADA для систем электроэнергетики. Несмотря на это, вопросы формализации требований информационной безопасности и создания унифицированных средств анализа защищенности АСУ ТП находятся в начальной стадии проработки. Объясняется это тем, что, несмотря на относительно небольшое количество различных SCADA, инсталляция каждой из этих систем сопровождается глубокой адаптацией к определенному технологическому объекту. В результате конкретные реализации даже однотипных SCADA могут существенно различаться, вследствие чего различаются и подходы к обеспечению информационной безопасности соответствующих АСУ ТП. В целом, логика развития SCADA и DCS-систем такова, что грань между ними стирается: первые обретают дополнительную функциональность, а вторые – универсальность. Исключение составляют особо критические функции DCS в нефтехимических приложениях.

Таблица 1

Основные разработчики и производители SCADA для систем электроэнергетики

Компания	Сайт
Schneider electric	www.schneider-electric.com
ABB Group	www.abb.com
GE (GE Energy)	www.ge.com , www.gepower.com
Siemens	www.siemens.ru
KEMA	www.kema.com
Toshiba	www.toshiba.com
COOPER Power Systems	www.cooperpowereas.com
BPL Global	www.bplglobal.net
CD Nova Ltd.	www.cdnova.com
HARRIS Corporation	http://www.harris.com

При создании унифицированных средств анализа защищенности АСУ ТП необходимо учитывать, что типовые протоколы каналов связи элементов SCADA включают в себя промышленные протоколы (Modbus, DNP3, IEC 61850, Control Information Protocol, DeviceNet, Profibus, SC1801), протоколы коммутируемого сеансового доступа (PPP/SLIP), стеки протоколов беспроводных радиоканалов связи (IEEE 802.11, IEEE 802.16, IEEE 802.20) и протоколы сотовых сетей GSM/GPRS [7]. Для дублирования линий связи устройства могут подключаться к нескольким сетям, например к выделенной линии и резервному радиоканалу.

Подобное разнообразие используемых протоколов приводит к появлению новых векторов информационных атак, которые могут быть использованы злоумышленниками:

- «fuzzing» и эксплуатация уязвимостей протокола IEC61850;
- выявление переполнений буфера в серверах OPC;
- сетевая разведка и подавление безопасности OSCP по доступным каналам общего доступа;
- обнаружение общедоступных ресурсов DDE;
- прослушивание на предмет служебной информации с устройств, подключённых по протоколам Modbus/DNP3/Profibus/Profinet, модификация данных эфира;
- способы закрепления в среде системного программного обеспечения встраиваемых систем («embedded»);
- атаки на отказ в обслуживании по модулям телеметрии и их службам.

Игнорирование перечисленных особенностей SCADA приводит к недостоверным результатам сигнатурного и эвристического анализа, выполненного с использованием стандартных существующих сканнеров безопасности, средств активной и пассивной сетевой разведки. Более подробно технические аспекты обеспечения информационной безопасности систем SCADA изложены в [7].

Таким образом, проблема обеспечения информационной безопасности критически важных технологических объектов заключается в создании специализированных аппаратно-программных и методических средств анализа защищенности АСУ ТП, реализованных на основе SCADA и DCS, выработки и реализации требований и рекомендаций по повышению уровня защищенности этих систем [8].

СПИСОК ЛИТЕРАТУРЫ

1. История информатики и философия информационной реальности: Учеб. пособие для вузов/Под ред. чл.-корр. РАН Р.М.Юсупова, проф. В.П.Котенко. – М.: Академический проспект, 2007. – 429 с.
2. Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организации противодействия /О.О.Андреев и др. Под ред. В.А.Васенина. – М.: МЦНМО, 2008. 398 с.
3. The Repository of Industrial Security Incidents URL: <http://securityincidents.org>
4. CPNI URL: <http://cpni.gov.uk>
5. CERT URL: <http://www.cert.org/>
6. ГОСТ 34.003-90. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
7. Gordon Clarke. Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems (IDC Technology (Paperback)). USA, 2004. 400 с.
8. Гарбук С.В., Комаров А.А. Особенности обеспечения информационной безопасности систем SCADA URL: http://itdefence.ru/content/articles/scada_security_ruscrypto_2010/.

Десницкий В.А., Котенко И.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
РАЗРАБОТКА И АНАЛИЗ ПРОТОКОЛА УДАЛЕННОГО ДОВЕРИЯ**

В работе рассматривается механизм защиты программ от злонамеренных изменений, построенный на основе принципа «удаленного доверия» (remote entrusting principle) [3]. Основное внимание уделяется вопросам разработки и анализа одного из важнейших элементов механизма защиты, а именно специализированного протокола обмена сообщениями. Данный протокол предназначен для передачи данных между доверенным сервером [3] и защищаемой клиентской программой, необходимых для работы защитного механизма, и называется «entrusting-протокол». В работе рассматриваются модели нарушителя, имеющего цель скомпрометировать работу протокола, и тем самым осуществить вмешательство в работу клиентской программы. Формируются основные требования к протоколу, соблюдение которых необходимо для построения надежного, устойчивого к вмешательствам протокола. Предлагаются различные реализации протокола удаленного доверия, на основе существующих сетевых протоколов, а также интеграция с протоколами, способными его усилить или придать ему какие-либо дополнительные качества. В работе предлагается общий подход к оцениванию временных затрат на выполнение атак на протокол удаленного доверия, а также рассматривается возможность применимости методов автоматического синтеза протоколов к задаче построения протокола удаленного доверия.

1. Введение

Одной из актуальных и важных проблем в области информационной безопасности является защита программного обеспечения от злонамеренных изменений («взлома»). В настоящее время не существует полностью надежных и универсальных решений этой проблемы.

Целью разрабатываемого механизма защиты программного обеспечения на основе удаленного доверия является обнаружение несанкционированных модификаций клиентской программы, функционирующей в потенциально враждебном окружении. Данный механизм предусматривает включение в модель защиты требующей защиты клиентской программы, выполняющейся в рамках ненадежного окружения, а также доверенного сервера, располагающегося на защищенном хосте. Предполагается также непрерывное сетевое соединение между клиентом и сервером. Важнейшим принципом является реализация программного модуля, отправляемого сервером клиенту во время выполнения, с возможностью его последующего обновления в заданные моменты времени. Основными элементами данного модуля являются монитор и генератор тегов. В функцию монитора входит постоянное осуществление определенного набора проверок клиентского приложения во время выполнения, в том числе проверок состояния программы, ее кода, обрабатываемых данных. В свою очередь, генератор тегов ответственен за непрерывное формирование определенного вида тегов, содержащих результаты проверок и некоторые дополнительные данные, которые должны отправляться доверенному серверу.

Доверенный сервер анализирует полученную информацию, после чего принимает решение о том, было ли совершено вмешательство в работу клиентской программы. Доверенный сервер считает программу некорректной, если он обнаруживает, что хотя бы одна из выполненных проверок закончилась с отрицательным результатом. В такой ситуации сервер прекращает предоставление данному клиенту любых сервисов и программных обновлений.

Разработка и дальнейший анализ специализированного протокола обмена сообщениями (протокола удаленного доверия), как составной части механизма защиты [3], является важной задачей, требующей отдельного рассмотрения. Протокол удаленного доверия предназначен для защищенного обмена сообщениями между клиентской программой и доверенным сервером, и в частности для доставки кода мобильного модуля и данных, содержащих результаты выполненных проверок. Создание корректно спроектированного протокола удаленного доверия является сложной задачей, так как протокол может содержать большое количество трудно обнаружимых изъянов, которые могут привести к нарушению правильного функционирования механизма защиты.

В контексте решения общей задачи защиты программ необходимость разработки специализированного entrusting-протокола связана с тем, что данная задача требует специфического набора требований, предъявляемых к безопасности разрабатываемого протокола, в то время, как ни один из существующих сетевых протоколов в полной мере все эти требования не обеспечивает. Более того, в процессе дальнейшего развития и усовершенствования протокола удаленного доверия к нему могут предъявляться новые требования, что не должно ограничиваться рамками выбранного сетевого протокола. Поэтому, целью исследования является скорее создание некоторой модели данного протокола, представляемой в виде набора требований, для реализации которых в зависимости от существующих условий могут выбираться различные базовые сетевые и криптографические протоколы.

Среди существующих работ, посвященных построению и анализу протоколов безопасности, наибольшее внимание уделено изучению протоколов аутентификации [8]. В то же время задача построения entrusting-протокола, рассматриваемая в настоящей работе, предполагает возможность интеграции протокола удаленного доверия с различными другими протоколами и средствами, позволяющими придать протоколу некоторые дополнительные качества. В частности, интеграция «Time-stamp» протокола на основе сертификатов открытых ключей [6], способного обеспечить поддержку меток времени, в entrusting-протокол способна обеспечить поддержку контроля над временем доставки сообщений. Методы автоматического синтеза протоколов [5,10,11] пока еще не предоставляют готовые, окончательные решения, корректность и адекватность которых можно было бы гарантировать полностью, и являются в настоящее время объектом активных исследований, тем не менее, эти методы представляют большой интерес для нашего исследования.

2. Типы атак и модели нарушителя

Рассмотрим три основных типа атак на протокол удаленного доверия:

- прослушивание коммуникационных каналов, по которым осуществляется передача данных. Атака такого вида сама по себе не представляет угрозы для корректного функционирования entrusting-протокола, однако проведение данной атаки может являться необходимым условием выполнения других видов атак;

- злонамеренное изменение (не только передаваемых, но и обрабатываемых в рамках соответствующего клиентского компонента) данных. В случае, когда модификации подвергаются отправляемые клиенту данные (код мобильного модуля), целью такой атаки (подмены модуля) является желание повлиять на программу извне с целью изменения ее поведения в соответствии с ожиданиями злоумышленника. Основной же целью такой атаки является намеренное искажение данных о текущем состоянии клиентской программы, которую получает и затем анализирует доверенный сервер;

- DOS-атака – атака с целью сделать невозможным или затруднить корректное функционирование механизма защиты на основе удаленного доверия. Осуществление таких атак возможно даже в том случае, когда обе стороны протокола удаленного доверия являются легитимными. В такой ситуации DOS-атаку совершает некая третья сущность, желающая повлиять на работу протокола или исследовать его. Вообще же, защита от DOS-атак представляет собой отдельное направление исследований и выходит за рамки настоящей работы.

Для построения и последующего анализа entrusting-протокола необходимо определить модель нарушителя [4], который пытается вмешаться в процесс работы протокола. Такие вмешательства могут происходить как на каких-либо промежуточных узлах между доверенным сервером и клиентом, так и в пределах клиентской программы и ее окружения.

Рассмотрим две модели нарушителя, характеризующие возможные действия злоумышленника по компрометации протокола удаленного доверия. Первая модель позволяет описывать и анализировать возможные атаки типа “man-in-the-end” (“человек на конце”), тогда как вторая ориентирована на атаки “man-in-the-middle” (“человек посередине”). На практике злоумышленник может комбинировать атаки обоих видов, получая, таким образом, атаки, которые более эффективны и удобны для реализации.

В случае атаки типа «man-at-the-end» на протокол предполагается, что злонамеренным вмешательством подвергается специальный программный компонент, который реализует клиентскую сторону entrusting-протокола, и который находится в пределах мобильного модуля. Злонамеренное изменение данного компонента entrusting-протокола осуществляется атакующим с целью модификации правил работы протокола, и, в частности, правил формирования исходящего клиентского трафика. Действия нарушителя можно представить в виде действий некоторого агента, находящегося в пределах клиентской машины и пытающегося осуществлять воздействия на защищаемую программу и, в том числе, на мобильный модуль (см. рисунок 1). В случае если entrusting-протокол является достаточно стойким, то изменения подобного вида могут быть обнаружены доверенным сервером опосредованно (как обнаружение какой-либо несогласованности в протоколе или при обнаружении отклонения значений полученных данных от некоего ожидаемого набора значений).

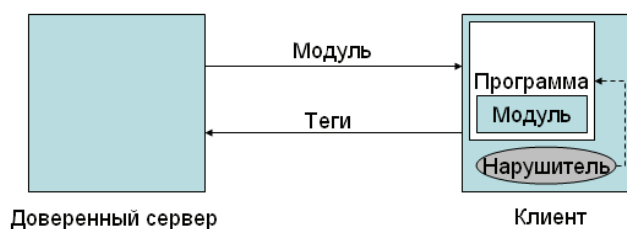


Рис.1. Область действий нарушителя при реализации man-in-the-end атаки

Стоит также учитывать, что уязвимости подобного рода могут вытекать не только из-за недостаточной стойкости непосредственно entrusting-протокола, но также из-за каких-либо недостатков соответствующих протоколов более низкого уровня (на которых базируется entrusting-протокол, и используемых в рамках конкретных реализаций протокола). Иначе говоря, такая атака может заключаться в поиске соответствующих уязвимостей сетевых протоколов, на базе которых строится entrusting-протокол, с целью сделать entrusting-протокол менее стойким. Это может быть возможность принудительного использования заведомо слабых криптографических примитивов. Например, использование шифров и хэш-функций, которые не являются стойкими и надежными. В частности, нарушитель может модифицировать соответствующий программный компонент клиента так, чтобы значительно упростить криптоанализ применяемого в протоколе шифра или нахождение коллизии используемой хэш-функции. В целом представляется, что выполнение каких-либо злонамеренных действий на протокол для атакующего предпочтительнее осуществлять в рамках атак man-in-the-middle, так как таким образом эти действия являются менее обнаружимыми сервером (так как действия посередине не могут быть обнаружены верификатором).

Также частным случаем (рассмотренной выше атаки) может быть атака, которая представляет собой прослушивание каких-либо данных, например секретных ключей, которые в явном виде не передаются по сети, но формируются и используются в рамках соответствующего программного компонента, ответственного за функционирование entrusting-протокола на клиенте. В качестве примера такой атаки можно отметить перехват общего, разделяемого секретного ключа, формируемого по протоколу Диффи-Хеллмана (Diffie-Hellman).

Рассмотренные выше злонамеренные воздействия могут осуществляться при помощи разнообразных программных инструментов, таких как отладчики бинарного кода, дамперы и пр.

В рамках модели, ориентированной на атаки man-in-the-end, возможной атакой на entrusting-протокол может быть также атака, осуществляющая прослушивание сетевого интерфейса (клиентской машины), используемого для работы протокола, с целью анализа приходящего и исходящего трафика, а также атака, выполняющая модификацию этого трафика. Функционально данная атака является аналогичной атаке типа man-in-the-middle, которая будет рассматриваться далее.

Атаки типа man-in-the-middle предполагают прослушивание или захват сетевого трафика на пути его следования между клиентом и доверенным сервером. В качестве субъекта атаки, совершающего злонамеренные действия, может выступать как непосредственно конечный пользователь клиентской программы, пытающийся вмешаться в сеанс протокола, так и некоторая третья сторона (рисунок.2). К наиболее важным относится первый случай. В такой ситуации конечной целью нарушителя является вмешательство в работу программы со стороны запускающего ее злонамеренного клиента. Во втором случае третья сторона способна лишь нарушить корректное выполнение entrusting-протокола без изменения состояния программы клиента. Примерами атак man-in-the-middle могут быть прослушивание канала посредством анализатора сетевого трафика подключения, который может использоваться как основа для атак на мобильный модуль, и изменение исходящего трафика с целью введения в заблуждение сервера о текущем состоянии клиентской программы.

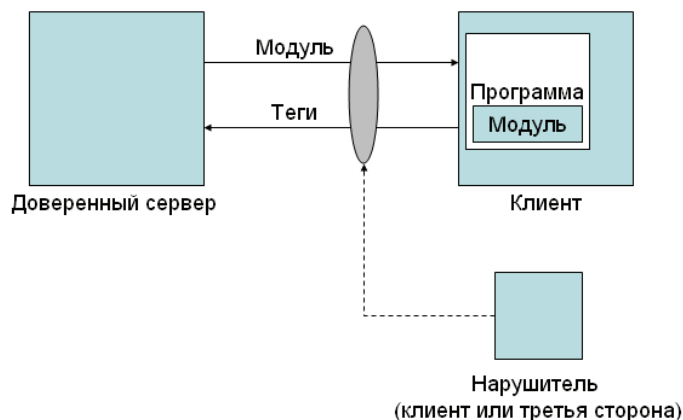


Рис.2. Область действий нарушителя при реализации атаки "man-in-the-middle"

Выделение двух рассмотренных моделей обуславливается необходимостью точного описания возможностей и целей потенциального нарушителя в контексте entrusting-протокола.

Отметим, что в соответствии с поставленной нарушителем целью, одну и ту же атаку можно реализовать несколькими способами, например, как атаку man-in-the-middle или как комбинацию атак man-in-the-middle и man-in-the-end. Поэтому в соответствии с различными условиями, разные реализации атак могут оказываться для нарушителя предпочтительными в различных ситуациях. К таким условиям можно отнести:

- сложность обнаружения атаки доверенным сервером (в частности, временная сложность или же объем необходимых для этого ресурсов);
- сложность выполнения атак нарушителем на клиентской стороне или посередине (в частности, временная сложность, либо объем задействованных ресурсов нарушителя);
- возможности автоматизации атаки или объем задействованного интеллектуального (человеческого) ресурса для выполнения атаки и требуемой технической квалификации нарушителя для осуществления атаки.

По временной сложности атака man-in-the-end может оказаться наиболее предпочтительной для злоумышленника, тогда как по сложности обнаружения доверенным сервером более выигрышной может быть комбинация атак man-in-the-middle и man-in-the-end.

3. Требования к протоколу удаленного доверия

Основными требованиями к entrusting-протоколу, реализация которых позволяет утверждать о его приемлемости для целей исследований, являются обеспечение аутентификации сторон протокола, обмена аутентифицированными ключами, конфиденциальности передаваемых данных, аутентификации данных, устойчивости к потере сообщений и своевременности доставки данных.

Хотя эти требования в достаточной степени освещены в имеющейся литературе, рассмотрим их кратко с учетом следующей специфики entrusting-протокола.

1. Аутентификация сторон протокола. Данное требование предполагает, что каждая сторона протокола должна быть уверена в аутентичности противоположной стороны. Это требование направлено на противодействие ситуациям, при которых нарушитель выдает себя за одну из законных сторон протокола. Аутентификацию сторон имеет смысл реализовывать посредством применения одного из существующих протоколов аутентификации сущности.

2. Согласование криптографических ключей. Для того чтобы entrusting-протокол был способен функционировать безопасным образом, необходимы определенные криптографические ключи, которые должны быть заранее согласованы между участниками. Необходимо использовать способ согласования, при котором согласование ключа происходит без передачи ключа по незащищенной сети. В то же время при таком типе согласования ключей протокол может быть подвержен атаке типа man-in-the-middle, когда некая третья сущность (нарушитель) может подменить одну из сторон, участвующих в протоколе. Поэтому для предотвращения таких атак требуется предварительная аутентификация. Подобные ключи могут использоваться сторонами протокола для реализации других требований, например обеспечения конфиденциальности передаваемых данных, а также их аутентификации.

3. Конфиденциальность передаваемых данных. Данное требование обеспечивает невозможность раскрытия передаваемых данных участнику протокола, которому они не предназначались. Имея общий секретный ключ, разделенный между законными сторонами протокола, и используя соответствующие алгоритмы, например, 3DES, AES или другие современные шифры, доверенный сервер и клиент способны передавать данные в соответствии с этим требованием.

4. Аутентификация передаваемых данных. Для того, чтобы нарушитель не мог изменить сообщение или подменить его другим, необходимо обеспечить аутентичность сообщений. Для этого к каждому сообщению прикрепляется код аутентификации сообщения (MAC, Message Authentication Code) [1], который вычисляется отправителем на основе оригинального сообщения, в результате чего законный получатель способен повторить процедуру вычисления MAC и сопоставить ее результат с полученным значением. Для того, чтобы нарушитель не мог подменить MAC-значение, процедура его получения должна основываться на знании секретного ключа, который своевременно должен безопасным образом быть согласован между доверенным сервером и клиентом. В частности, алгоритм создания MAC может основываться на использовании хэш-функций, зависящих от секретного ключа. Заметим, что аутентичность данных гарантирует также и их целостность, другими словами, обеспечивается защита не только от умышленных модификаций, но и от непреднамеренных действий.

5. Устойчивость к потере сообщений. Entrusting-протокол должен корректно передавать информацию, несмотря на возможные потери пакетов данных.

Важность данного требования заключается в том, что в случае его невыполнения могут возникать ситуации, при которых один из тегов, отправленных доверенному серверу, может быть потерян, в результате чего сервер получает некорректные данные о текущем состоянии клиента и

тем самым считает его подвергшимся несанкционированным модификациям.

В частности, данное требование может быть сформулировано, как необходимость гарантированной и своевременной передачи информации между клиентом и сервером при потере не более одного пакета за сеанс их взаимодействия или его определенную часть. В такой формулировке предполагается, что в случае потери одного пакета entrusting-протокол будет способен продолжать свою работу без необходимости повторной пересылки потерянного пакета. Для обеспечения данного требования могут использоваться различные алгоритмы, основанные на принципе избыточности данных, как например коды Хемминга, а также на основе избыточности коммуникационных каналов, например повтор потерянного пакета в случае необходимости или же заранее установленная параллельная передача данных несколькими путями.

Данное требование может быть выполнено, например, на основе подхода "Rollback Recovery", предполагающего использование двух стратегий. В соответствии со стратегией "Check-point based" состояние протокола периодически сохраняется на обеих сторонах обмена, и в случае потери пакета данных протокол способен вернуться к сохраненному состоянию. В соответствии со стратегией Log-based на обеих сторонах обмена ведется журнал сообщений, который предоставляет возможность отмены и повторной передачи сообщений.

6. Своевременность доставки данных. При помощи entrusting-протокола передаваемые данные должны доставляться получателю не позже, чем в определенные моменты времени. Таким образом, данное требование предполагает осуществление контроля за временем доставки сообщений, как на стороне доверенного сервера, так и на клиенте.

Помимо рассмотренных выше требований, определяющих защитные свойства, которыми должен обладать entrusting-протокол для того, чтобы быть надежным, следует также учитывать возможные архитектурные требования на протокол. Под архитектурными понимаются требования, касающиеся структуры разрабатываемого протокола и его архитектурных свойств. Стоит отметить, что в отличие от представленных выше общих требований к безопасности протокола, архитектурные требования зависят от конкретной реализации протокола и окружения, в которой он функционирует, и могут существенно изменяться в зависимости от конкретных пользовательских предпочтений владельцев программ, желающих их защитить посредством механизма удаленного доверия.

4. Построение протокола удаленного доверия

Одной из целей исследования является создание общей методики, определяющей процесс построения требуемого entrusting-протокола как элемента механизма защиты программ. В общем случае в соответствии с многообразием архитектурных, а также защитных требований могут быть реализованы entrusting-протоколы, отличающиеся друг от друга, как своими свойствами, так и особенностями реализации. Так, например, все множество entrusting-протоколов можно разделить на две категории: те из них, которые предполагают обязательную идентификацию программ (как различных копий), запускаемых конечными пользователями, и те, для которых все конечные пользователи и соответствующие им программы между сеансами их взаимодействия с доверенным сервером являются анонимными. Таким образом, отличие двух описанных выше ситуаций характеризуется необходимостью применения соответствующих методов аутентификации. Также стоит отметить, что необходимость аутентификации конечных пользователей может накладывать некоторые ограничения и требования на защищаемую программу в процессе ее написания. К примеру, парольная аутентификация конечных пользователей [8] потребует от программы реализации соответствующего программного интерфейса, ответственного за ввод пользователем и обработку секретных ключей.

Предлагаемая в настоящей работе *общая методика построения entrusting-протокола* заключается в следующем.

Вначале определяются protocol goals and assumptions. В соответствии с целью задачи формулируются необходимые защитные требования, должное выполнение которых позволяет обезопасить протокол от возможных атак на него со стороны потенциального злоумышленника.

После чего происходит формирование архитектурных требований, отражающих, как условия и ограничения среды функционирования протокола, так и соответствующие пользовательские предпочтения относительно структуры целевого протокола и, в частности, компонентов и блоков, из которых он состоит.

Далее проводится синтез и анализ создаваемого протокола ("синтез через анализ"). Синтез состоит в составлении (конструировании) протокола на основе композиции отдельных низкоуровневых блоков (коммуникационные и криптографические примитивы), исходя из сформированных требований. При этом правила построения протокола выводятся из высокоуровневой спецификации, определяющей защитные и архитектурные требования. Анализ протокола включает его верификацию посредством средств формального доказательства [2,7], анализ защищенности передаваемых пакетов данных и всего протокола в целом и анализ временной сложности атак на протокол, необходимый для поддержки механизма замещения общего подхода удаленного доверия [3].

Завершающая фаза методики предполагает возможную обратную связь (feedback), в соответствии с которой данные, полученные в результате анализа, применяются для коррекции требований к протоколу.

В целом, методика построения протокола удаленного доверия представляет процедуру, которая получает на вход требования к протоколу и выдает в качестве результата готовый протокол, реализующий необходимые бизнес процессы (функциональности) и обеспечивающий должный уровень их защиты. В общем случае данная методика является человеко-машинной (автоматизированной). Вопросом дальнейшего изучения является исследование возможностей автоматизации ее отдельных фаз.

При реализации entrusting-протокола часть из представленных выше требований может быть реализована на основе существующих сетевых протоколов, таких как IPSec или SSL/TLS.

В общем случае для более удобного моделирования и последующего анализа entrusting-протокола предлагается использовать модель “абстрактных коммуникационных каналов (abstract communication channels)” [9]. В соответствии с данной концепцией, протокол представляется как последовательность вложенных друг в друга каналов, каждый из которых реализует одно из требований безопасности. Данная модель удобна как при моделировании протокола, так и на стадии его анализа. В частности на основе модели абстрактных каналов можно проводить анализ разрабатываемого протокола на предмет определения требуемого порядка реализации требований к безопасности, а также начальный анализ сложности выполнения атак на предмет выявления требований, реализации которых злоумышленнику потребуется преодолеть для выполнения определенной атаки. В результате каждое из требований может либо быть реализовано напрямую разработчиком entrusting-протокола, либо полагаться на один (или несколько) из существующих сетевых протоколов.

На рисунке 3 показана упрощенная общая схема выполнения предлагаемого entrusting-протокола. На первой стадии происходит аутентификация сторон. Далее применяются протоколы согласования криптографических ключей, которые используются для открытия безопасного канала для обмена сообщениями между клиентом и сервером. После этого обе стороны обмена сообщениями способны передавать друг другу данные, гарантируя, в частности, их конфиденциальность и аутентичность. На финальной стадии работы протокола происходит закрытие безопасного канала (завершение соединения, а также уничтожение криптографических ключей с целью сделать невозможным их получение и дальнейшее использование нарушителем).

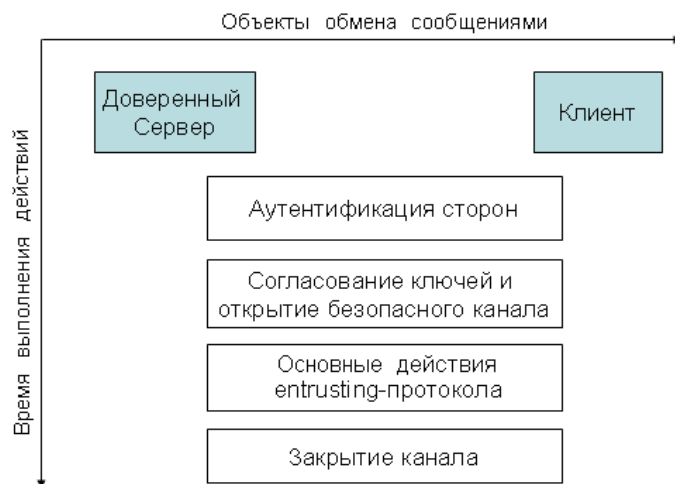


Рис.3. Схема выполнения entrusting-протокола

При практической реализации entrusting-протокол будет реализовываться при помощи существующих сетевых протоколов. В то же время на концептуальном уровне, для конструирования entrusting-протокола и его дальнейшей верификации удобно построить спецификацию, отвечающую всем перечисленным выше требованиям.

В работе предлагаются различные подходы к реализации entrusting-протокола, базирующиеся, в том числе, на основе различных комбинаций существующих сетевых протоколов.

Приведем ниже три варианта реализации прототипа entrusting-протокола (рисунок 4).

Entrusting-протокол может строиться непосредственно на основе протокола TCP/IP (или UDP), который не имеет встроенных средств защиты. Данный прототип протокола удобен в теоретическом плане, так как включает действия по обеспечению всех предъявляемых к нему требований, что дает возможность провести всесторонний анализ для оценивания общей стойкости. Более того, предлагаемый entrusting-протокол становится относительно независимым с точки зрения реализации, и поэтому, по сравнению с другими вариантами прототипа, является более адаптируемым (переносимым) к другим сетевым протоколам, на основе которых будет возможна его реализация.

Два других прототипа основываются на использовании существующих сетевых протоколов (IPSec, SSL/TLS), способных обеспечить часть требований безопасности, а также на применении каких-либо других протоколов, которые позволяют реализовать оставшиеся требования.

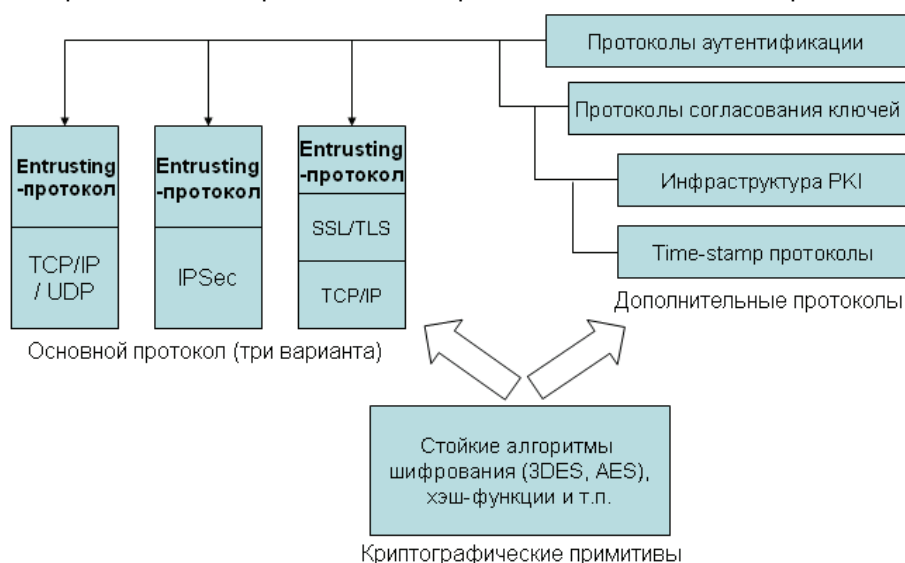


Рис.4. Реализации entrusting-протокола

Предлагается дополнительно применять протоколы, обеспечивающие требование аутентификации сторон, протоколы, обеспечивающие согласование/обмен криптографическими ключами (а также согласование используемых криптографических примитивов), необходимыми для работы entrusting-протокола.

5. Подход к оцениванию временной сложности атак на протокол удаленного доверия

Охарактеризуем кратко действия, которые необходимо осуществить для оценивания временной сложности атак на протокол. Требование получения таких оценок связано в первую очередь с необходимостью определения разумного периода обновления мобильного модуля для реализации принципа динамического замещения в рамках всего механизма защиты.

Итак, для оценивания атаки необходимо определить действия, из которых она состоит, а также все задействованные криптографические алгоритмы. Далее требуется найти формальные оценки стойкости этих криптографических алгоритмов (сложность нахождения коллизии хэш-функции, сложность применяемого крипто анализа и т.п.).

Помимо принятия во внимание оценивания сложности соответствующих действий атакующего, выполняемых автоматически посредством специальных программных инструментов, следует также учитывать человеческий фактор, вовлеченный в процесс выполнения атаки на практике. Такие интеллектуальные действия включают определенные действия, выполняемые атакующим вручную, например обратная разработка программы (reverse engineering), включая деобфускацию или поиск определенных конструкций в программном коде, которые удовлетворяют определенным условиям. По-видимому, единственным практически реализуемым способом получения подобного рода оценок сложности атаки является их исследование эмпирическим способом.

Возможным и разумным для практики решением задачи оценивания сложности атак будет использование формальных оценок стойкости соответствующих криптографических алгоритмов и средств, что будет давать некоторую минимально ожидаемую оценку сложности.

6. Интеграция протокола удаленного доверия с протоколами безопасности

При построении entrusting-протокола могут использоваться некоторые другие средства и протоколы безопасности с целью усиления определенных или обеспечения некоторых дополнительных свойств entrusting-протокола.

В случае интеграции, предполагающей последовательное выполнение действий двух или нескольких протоколов, взаимодействие происходит таким образом, что результаты работы сеанса одного протокола являются входными данными для другого. Интеграция данного типа является достаточно "слабой". Поэтому при реализации entrusting-протокола с использованием интеграции такого вида не предполагается каких-либо трудностей, связанных со взаимной несовместимостью составляющих ее протоколов или с появлением возможных уязвимостей, позволяющих злоумышленнику успешно атаковать протокол.

В случае более сложной интеграции, при которой происходит "вложение" одного протокола в другой требуется более сложный анализ их взаимодействия, в частности, требуется обоснование корректности полученной комбинации, даже если доказано, что каждый протокол в отдельности работает должным образом и лишен уязвимостей. Интеграция каждого конкретного протокола с

entrusting-протоколом будет иметь индивидуальные особенности и требует отдельного глубокого рассмотрения.

Одним из примеров протокола, который может быть интегрирован в entrusting-протокол, является Time-Stamp Protocol (TSP), основанный на использовании PKI (Public Key Infrastructure) и X.509 сертификатов [6]. Time-stamp представляет собой утверждение о том (доказательство того), что определенные данные были созданы не позднее определенного момента времени и не были модифицированы впоследствии. Работа TSP заключается в следующем: клиент, которому требуется связать свои данные с определенным моментом времени направляет запрос специально выделенной доверенной сущности (Time Stamping Authority, TSA), которая ответственна за time-stamp сертификацию. Такой клиентский запрос содержит хэш-значение рассматриваемых данных, а также некоторую другую информацию. В свою очередь TSA получает клиентский запрос, обрабатывает его и возвращает клиенту пару, то же значение хэш-функции и информацию о текущем моменте времени, подписанную секретным PKI-ключом TSA, то есть выдает time-stamp сертификат, соответствующий интересующим клиента данным. Соответственно, для проверки корректности сертифицированных по времени данных необходимо проверить валидность time-stamp сертификата, а также повторить соответствующую процедуру вычисления хэш-значения и сравнить оба хэша.

Возможным применением TSP является сертификация по времени entrusting tags, отправляемых клиентом доверенному серверу. В частности, возможным применением является ситуация, когда TSA реализуется аппаратно, в рамках специализированного hardware-модуля, располагающегося на стороне клиента и реализующего TSA-функциональность.

7. Методы автоматического синтеза протоколов

Рассмотрим парадигму в области построения протоколов безопасности, в соответствии с которой, участники договариваются и на лету формируют протокол в соответствии с их потребностями, то есть осуществляется автоматический синтез протоколов. Когда участники имеют желание осуществить взаимодействие, они не выбирают определенный протокол из фиксированного списка известных, а скорее синтезируют новый протокол, специально сделанный с учетом их текущих требований к безопасности и их окружения. Такие протоколы являются само конфигурирующимися, так как априори специфицируются только предположения об участниках (principal assumptions) и цели протокола. Изменения в окружении участников могут привести к тому, что стороны должны будут заново договориться и сгенерировать новый протокол (survivable-протокол).

Такие протоколы в потенциале способны даже преодолевать некоторые компрометации безопасности механизма. Так, компрометация ключа или изменение отношения доверия (trust) между участниками могли бы приводить к синтезу нового протокола, способного преодолеть последствия произошедшего события. Наиболее известным и перспективным подходом к реализации автоматических генераторов протоколов является подход, основанный на использовании BAN belief-логик, подробное описание которого представлено в работах [5,10,11].

В рамках традиционной методики построения, на начальной стадии протокол конструируется эвристически, после чего он проходит стадию формальной верификации на предмет наличия уязвимостей, и, соответственно, возможных атак, которые имеют цель скомпрометировать процесс его выполнения. В случае обнаружения таких атак проводится коррекция протокола, после чего он повторно проходит верификацию и т.д. Наконец, когда на некоторой итерации никакие новые атаки не будут выявлены, протокол считается корректным. Тем не менее, существующие средства формальной верификации не гарантируют полное обнаружение всех возможных уязвимостей, а скорее представляют собой лишь необходимую, но не достаточную процедуру, позволяющую обосновать корректности протокола. В случае же построения протокола с использованием методов автоматического синтеза, полученный протокол является correct-by-construction, что снимает необходимость проведения большого количества итераций проверки. Вместе с тем следует заметить, что на практике нет гарантий, что построенный таким образом протокол, будет в действительности полностью корректным. Помимо корректности заданной belief-аксиоматики, важно непротиворечивое и правильное формулирование в рамках данной аксиоматики требуемых целей, связанных с безопасностью, и предположений (assumptions) об участниках протокола и среде, в которой происходит коммуникация.

В контексте задачи создания entrusting-протокола методика его построения обретает следующие особенности. При помощи методов автоматического синтеза entrusting-протоколу могут быть приданы новые, имеющие отношение к безопасности, свойства, посредством задания дополнительных целей и предположений. Такие новые свойства могли бы быть связаны, как с приданием каких-либо дополнительных качеств непосредственно протоколу, для усиления его стойкости к вмешательствам, так и с целью поддержки каких-либо методик защиты клиентской программы, функционирующие части которой развернуты, как на клиентской стороне, так и на сервере и должны работать, взаимодействуя между собой.

Определенный интерес также представляет возможность применения методов автоматической генерации протоколов для введения некоторой вариативности (variance) в entrusting-протокол – возможности получения нескольких вариантов entrusting-протокола, имеющих одинаковую функциональность, но несколько отличающихся друг от друга. Подобная вариативность протокола, то

есть, по сути, динамическое изменение правил работы протокола, будет способствовать повышению его устойчивости к вмешательствам, требуя со стороны потенциального злоумышленника затрачивать дополнительное время на взлом каждой новой версии протокола. Так, в предложенной в [10,11] методике автоматического синтеза на финальной стадии вырабатывается несколько валидных протоколов-кандидатов, каждый из которых полностью соответствует лежащей в основе belief-логике. В [10] авторы предлагают производить выбор наиболее подходящего кандидата на роль протокола на основе проверки каких-либо дополнительных специализированных свойств (ad-hoc properties). Таким образом, заложенная в данном методе возможность получения набора валидных протоколов могла бы быть использована нами для реализации динамической модифицируемости протокола, делая его тем самым более устойчивым ко вмешательствам.

В настоящее время направление по разработке методов автоматического синтеза протоколов на основе belief-логик является интенсивно развивающимся. В то же время к основным недостаткам можно отнести отсутствие полноценной доказательной базы, подтверждающей корректность создаваемых протоколов. Также в настоящее время ощущается явный недостаток программных средств и инструментов, реализующие эти методы и готовых к применению.

Заключение

Предложен подход к разработке специализированного протокола обмена сообщениями entrusting-протокола. Проведен анализ протокола, в частности рассмотрены основные типы атак и модели злоумышленника, определены основные требования к entrusting-протоколу, дано представление об используемой методике синтеза и анализа протокола, затронуты некоторые аспекты реализации entrusting-протокола.

В дальнейшем планируется проведение углубленного анализа entrusting-протокола, в том числе его верификации на основе методов формального доказательства. Предполагается также проведение подробного анализа временной сложности атак, результаты которого могут быть использованы для усиления механизма защиты, основанного на удаленной аутентификации в целом. Планируется, также, продолжение работы по исследованию применимости методов автоматического синтеза протоколов к рассматриваемой задаче

Работа выполнена при финансовой поддержке РФФИ (проект №07–01–00547), программы фундаментальных исследований ОИТВС РАН (контракт №3.2/03), Фонда содействия отечественной науке и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST (контракт № 021186–2).

СПИСОК ЛИТЕРАТУРЫ

1. Bellare M., Canetti R., Krawczyk H. Keying hash functions for message authentication // Advances in Cryptology – CRYPTO '96, Lecture Notes in Computer Science, vol. 1109, Springer-Verlag, 1996, P.1–15.
2. Boichut Y., Hearn P.-C., Kouchnarenko O. Automatic Verification of Security Protocols Using Approximations // INRIA Research Report, October 2005.
3. Ceccato M., Ofek Y., Tonella P. «Remote entrusting by run-time software authentication» // SOFSEM 2008 – Conference on Current Trends in Theory and Practice of Computer Science, Tatras, Slovakia, January, 2008.
4. Cederquist J., Dashti M.T. An intruder model for verifying liveness in security protocols // Proceedings of the fourth ACM workshop on Formal methods in security, P.23–32, November 03–03, 2006, Alexandria, Virginia, USA.
5. Chen H. A Search-Based Framework for Security Protocol Synthesis // Submitted for the degree of Doctor of Philosophy. The University of York, Department of Computer Science. April 2007.
6. Ellison C., Schneier B. Ten Risks of PKI: What you're not being told about public key infrastructure // Computer Security Journal, Vol.16, No.1, 2000.
7. Khan A.S., Mukund M., Suresh S.P. Generic verification of security protocols // Proceedings of SPIN 2005, LNCS, Vol.3639, 2005.
8. Lampson B., Abadi M., Burrows M., Wobber E., Authentication in distributed systems: theory and practice // ACM Transactions on Computer Systems (TOCS), v.10 n.4, P.265–310, Nov. 1992.
9. Plasto D. Automated analysis of industrial scale security protocols // MSc Thesis, Bond University, Faculty of Information Technology. 2004.
10. Zhou H., Foley S. Fast Automatic Synthesis of Security Protocols using Backward Search // In Proceedings of the 2003 ACM Workshop on Formal Methods in Security Engineering (FMSE'03), P. 1–10, Washington DC, October 2003.
11. Zhou H., Foley S. A collaborative approach to autonomic security protocols // Proceedings of the 2004 workshop on New security paradigms, September 20–23, 2004, Nova Scotia, Canada.

Колодин М.Ю., Федорченко Л.Н.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МЕТАТЕХНОЛОГИИ В СИСТЕМАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Введение

Принципы, заложенные в стандартах обеспечения информационной безопасности и, в частности, в стандарте ISO 15408 (Common Criteria for Information Technology Security Evaluation, Common Criteria в зарубежной терминологии) [1], ставят перед разработчиками программного обеспечения (ПО) новые задачи автоматизации проектирования надёжного и конкурентного ПО с широким использованием формальных методов, среди которых особое место принадлежит применению метатехнологий при разработке разнообразного программного обеспечения.

Понятие «метатехнология» многозначно. Основное значение этого термина можно сформулировать как «многоуровневые технологические системы, системы с порождением новых систем с заданными свойствами на основе существующих, специально сконструированных для выполнения определённой функции». Составляющая «мета» соответствует понятиям «над» и «между». В общем случае количество уровней систем может быть произвольным и системы могут быть динамическими, выполняющими порождение новых систем в процессе своего функционирования. Таким образом, в процессе разработки ПО осуществляется получение многоуровневых систем, причём каждый следующий уровень генерируется из предыдущего и на каждом уровне достигается определённый промежуточный результат. На последнем уровне получаем целевой результат. Если каждый из уровней включает в себя язык (как спецификацию для получения следующего метауровня), то процесс разработки можно рассматривать как последовательность трансляций в определённой вычислительной среде.

С точки зрения информационной безопасности основными факторами, способствующими применению метатехнологий, являются понижение сложности получаемых систем и, соответственно, повышение их надёжности, повышение технологичности процессов разработки и использования программного обеспечения, а также снижение зависимости отечественной области информационных технологий от зарубежных составляющих, особенно в закрытых и критических областях (в т.ч. в военных, государственных, управляющих приложениях, для средств связи и т.п.), а также в образовательной, научной, медицинской и общекультурной областях.

1. Пример метатехнологии

Наиболее известным примером метатехнологии является технология производства языковых процессоров с применением различных классов грамматик. Чаще всего для этой цели используются контекстно-свободные и автоматные грамматики. В более развитых технологиях применяются модификации этих классов грамматик, такие как контекстно-свободные грамматики в регулярной форме (КСР-грамматики), атрибутные или аффиксные грамматики, обогащённые контекстной информацией.

КСР-грамматики (с регулярными выражениями в правых частях правил) [15–18] реализованы в системе Бета-Форт [23,24], в системе SYNTAX [19], в системе эквивалентных преобразований и регуляризации трансляционных грамматик SynGT [18]. Особенностью системы SynGT является автоматизированное применение разнообразных эквивалентных преобразований синтаксических конструкций реализуемого языка с последующей регуляризацией грамматики, описывающей данный язык. Под регуляризацией грамматики понимают процесс применения цепочки базисных преобразований исходной КС-грамматики G в новую КС-грамматику G_1 в регулярной форме (КСР-грамматику), причём такую, что из нее исключаются подстановками несамовставленные нетерминалы. Если все нетерминалы КС-грамматики G являются несамовставленными, то их можно исключить из правых частей правил. Определяющие правила для этих нетерминалов исключаются также. В этом случае грамматика G преобразуется в грамматику G_1 с одним правилом, правая часть которого является сложным по композиции операций регулярным выражением над терминалами и контекстными символами (семантиками). Значением этого регулярного выражения является регулярный язык $L = L(G_1) = L(G)$. Напомним, что вывод в КСР-грамматике заменяется вычислением значений соответствующих регулярных выражений.

При регуляризации грамматики правые части её правил по-прежнему являются регулярными выражениями над объединённым алфавитом грамматики, а синтезированный МП-преобразователь может вырождаться в конечноавтоматный.

Регуляризация грамматики является частью полного цикла реализации языка, который состоит из цикла пользователя, и полуавтоматического цикла разработчика (реализатора). Разработка реализации языка (выбор модели языка, модели синтаксического разбора и других моделей реализации) производится человеком, трансляция и машинная обработка входных текстов программ происходит автоматически.

1.1 Синтаксическая модель языка

Модель языка — это способ его описания. С помощью модели можно описывать бесконечно много конкретных языков. Синтаксическая модель предполагает четыре аспекта языка: лексику, синтаксис, семантику и прагматику.

Лексика определяет представление основных символов языка (терминальных символов грамматики) при помощи знаков входного устройства компьютера. Обычно лексика задается стандартом языка в виде перечня допустимых знаков для каждого терминала грамматики. Один терминал может иметь несколько разных вариантов конкретного представления. Иногда терминал представляется одной литерой, например, символ «открыть» может быть представлен литерой '(', или несколькими литерами, как, например, 'begin', или символ присвоить в виде цепочки литер ':='.

Задача лексического анализа – отображение цепочек литер конкретного представления текста программы в последовательность терминальных символов (основных символов языка).

Синтаксис определяет представление основных конструкций языка посредством терминальных символов. Обычно он описывается при помощи КС-грамматики, правила которой определяют одно или несколько альтернативных порождений для каждого нетерминала грамматики. Начальный нетерминал порождает конструкцию языка, называемую программой. Синтаксис определяет, из каких других подконструкций состоит данная конструкция (в первую очередь программа), если она не элементарна. Не все нетерминалы порождают конструкции, а только те, для которых определена семантика. Вспомогательные нетерминалы могут вводиться реализатором искусственно в процессе выполнения эквивалентных преобразований. Никакой терминальный символ или цепочка терминальных символов не имеют смысла сами по себе. Терминальная цепочка имеет смысл только в качестве терминального порождения некоторого понятия (нетерминала), которому смысл приписывается соответствующими правилами семантики. Под смыслом терминальной цепочки понимается некоторая последовательность действий по исполнению конструкции, представленной данной цепочкой, некоторой виртуальной или реальной машиной. Определение конструкционной структуры программы – задача бесконтекстного синтаксического анализа.

1.2. Преобразование КС-грамматик

Из теории известно, что проблема эквивалентности двух КС-языков, задаваемых различными КС-грамматиками, в общем случае неразрешима. Однако, часто удается преобразовать грамматику к требуемому виду для того или иного детерминированного разбора, не "испортив" описываемый ею язык.

1.3. Базовые преобразования

Метод подготовки исходной грамматики с целью её регуляризации предполагает использование следующих базисных эквивалентных преобразований над регулярными выражениями и КСР-правилами.

- подстановка вместо нетерминала его порождения;
- удаление вхождения лево(право)рекурсивного нетерминала в правой части правила;
- объединение общих префиксов в графе для нетерминала;
- удаление повторяющихся альтернатив для нетерминала;
- удаление крайних рекурсий для самовложенных нетерминалов;
- свёртка регулярного подвыражения в новый нетерминал и создание нового правила в грамматике;

- удаление лишних правил.

1.4. Основные процедуры системы генерации языкового процессора

1. GramCoding – свёртка лексем, кодирование КСР-грамматики.
2. GraphSynth – по кодированной КСР-грамматике строит соответствующую ей синтаксическую граф-схему.

3. AutomatSynth – ядро программной системы. Синтез состояний магазинного автомата из синтаксической граф-схемы, полученной от GraphSynth. Выходом является список состояний автомата.

4. AutomatConstruct – получает на вход список состояний автомата и строит представление магазинного автомата, пригодное для быстрого анализа предложений языка: переходная функция отображается в матрицу, которая содержит либо значение функции, либо ссылку на поля, содержащие составные значения функции.

5. Minimization – минимизирует размеры матрицы состояний, сокращает число элементарных состояний автомата.

6. Synchro – выполняет некоторые базисные эквивалентные преобразования в зависимости от аварийной диагностики на выходе процедуры AutomatSynth. В дальнейшем эта процедура преобразовалась в отдельный программный комплекс SynGT (Syntax Graph Transformations), выполняющий кроме базисных преобразований и другие, более глобальные преобразования, на множестве всех правил грамматики.

1.5. Этап предварительной подготовки грамматики

Предварительная обработка исходной грамматики использует те же технологические приёмы (верхний уровень метатехнологии), которые применяются в данной технологии для реализации языка программирования. Каждая КСР-грамматика рассматривается как текстовое слово в некотором метаязыке, который также можно описать с помощью некоторой мета-грамматики. Как оказалось, этот метаязык регулярен, а значит может быть проанализирован конечным автоматом. На этом свойстве КСР-грамматик основано построение верификатора грамматики в системе SynGT. Таким образом, верификация входной грамматики осуществляется конечным автоматом, синтез которого выполняется по той же методике, что и синтез магазинного процессора для исходной грамматики.

Ниже на рисунках 1–3 будет продемонстрирована схема преобразования этой мета-грамматики.

Этап предварительной подготовки входной грамматики анализируемого языка включает две операции:

1. Синтаксический контроль правильности записи грамматики – это верификация грамматики;
2. Преобразование грамматики с целью её приведения.

В результате выполнения этого этапа получаем следующее:

- корректную запись регулярных выражений: правильная скобочная структура, контроль всех операций в регулярных выражениях на бинарность (явное присутствие пустого операнда) и наличие конечного символа (конца правила);
- все входящие нетерминалы имеют определяющее их правило;
- правила, не порождающие предложения входного языка, удаляются (т.е. исключаются непродуктивные нетерминальные символы).

Таким образом, из исходной грамматики получаем приведенную КСР-грамматику.

Для построения конечно-автоматного верификатора исходная грамматика преобразуется в некоторую грамматику с учётом определённых соглашений.

1.6. Основные соглашения

Считается, что для каждого нетерминала имеется единственное определяющее его правило. В противном случае, два правила, определяющих данный нетерминал, можно заменить эквивалентным выражением, применив операцию объединения к регулярным выражениям в правых частях обоих правил. Начальным символом грамматики считается нетерминал в левой части первого правила.

Произведём переобозначения и вводим бинарную операцию обобщённой итерации, а именно:

- операцию объединения – точкой с запятой,
- операцию произведения или конкатенации – запятой,
- операцию обобщённой итерации – решёткой (знак #),
- терминальные символы – строчными буквами,
- нетерминалы – прописными буквами,
- перед семантиками ставим специальный знак (\$),
- используются как круглые, так и квадратные скобки,
- квадратные скобки обозначают возможное объединение с пустым словом.

Получаем текстовое представление КСР-грамматик с обобщёнными регулярными выражениями.

Неформально грамматика задается с учетом следующих соглашений.

- Словами КСР-грамматики будем называть терминалы, нетерминалы и семантики, присутствующие в регулярных выражениях правил в качестве операндов.
- Слова в грамматике представляются любой последовательностью букв, цифр, надчеркиваний и подчеркиваний.
- Терминалы – слова, заключенные в кавычки (' ').
- Семантики – слова с предшествующим символом \$ и последующей литерой, подчеркиванием или надчеркиванием.
- Длина слова ограничена 20 символами, включая кавычки и символ \$. Допустимы комментарии, начинающиеся символами "//". Верхний и нижний регистры клавиатуры неразличимы.
- Разделителями слов являются операции регулярных выражений (";", ",", "#", "!") и круглые или квадратные скобки, определяющие порядок выполнения заданных операций.
- Внутри слова возможны пробелы.
- Все операции должны быть явно бинарными, т.е. запрещен пропуск пустого операнда ("@") при любых бинарных операциях там, где он подразумевается.
- Признаком конца грамматики является слово "EOGram!".

Последовательное преобразование КСР-грамматики в форме Бэкуса-Наура в форму КСР-грамматики с регулярными выражениями в правых частях правил показано на рисунках 1–3.

G:

```

<КСР-грамматика>::=<КСР-правило>'EOGram!'|
                    <КСР-правило><КСР-грамматика>.
<КСР-правило>::=<нетерминал>':'<регулярное выражение>.
<регулярное выражение>::= <произведение>|
                    регулярное выражение ';' <произведение>.
<произведение>::=<итерация>|<произведение>'<итерация>.
<итерация>::=<терм>|<итерация>#<терм>.
<терм>::=<терминал>|<нетерминал>|<семантика>|@|
                    '('<регулярное выражение>')'|<регулярное выражение>']'.
<терминал>::='t'|'t'...'t'.
<нетерминал>::='n'|'n'...'n'.
<семантика>::='s'|'s'...'s'.

```

Рис.1. Представление произвольной КСР-грамматики в БНФ

Используя следующие сокращения: G – КСР-грамматика, R – КСР-правило, A – регулярное выражение, P–произведение, #–итерация, T–терм, t–терминал, n–нетерминал, s–семантика, получим спецификацию произвольной КСР-грамматики в виде КСР-грамматики G' с обобщёнными регулярными выражениями в правых частях правил (см. рисунок 2):

```
G':
G:R#@,','EOGram!'.
R:n,','A,','.
A:P#,'.
P:l#,'.
l:T##'.
T:t;n;ln;s;@,('A,');[A,']'.
```

Рис.2. Представление произвольной КСР-грамматики в виде КСР-грамматики

В грамматике G' терминальный алфавит– {',' ':' ';' '#' '!' '@ '(' ')' '[' ']' 'EOGram!' }+{t}+{n}+{s}, нетерминальный алфавит–{G,R,A,P,l,T}.

После применения эквивалентного преобразования (подстановки вместо нетерминальных символов их порождений), получим эквивалентную грамматику G'' (см. рисунок 3).

```
G''
G:(n,','A,')#@,'EOGram!'.
A:(t;n;ln;s;@,('A,');[A,'])###,##,.'.
```

Рис.3. Исходная грамматика G после применения эквивалентных преобразований

Конечный автомат, верифицирующий произвольные КСР-грамматики представлен матрицей переходных состояний в таблице 1. 0 –стартовое состояние, конечное состояние –6.

Таблица 1

Матрица состояний конечного автомата

Код лексемы	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Лексема/ Состояние	EOGram	:	(	)	.	!	[	]	;	,	#	@	n	t	s
0													1		
1		2													
2			2			3	2					4	4	4	4
3													4		
4				4	5			4	2	2	2				
5	6												1		

2. Обзор современных метатехнологий

Рассмотрим известные направления применений метатехнологий на примерах других работ (независимо от того, считают ли сами авторы свои работы таковыми и пользуются ли они терминами «метасистемы» и «метатехнологии» в своих работах).

Исторически наиболее известными являются работы Д. Кнута и ван Вейнгаардена. Д. Кнут применил метаподход при создании издательской системы TeX. Его концепция “*iterate programming*” («грамотное программирование», 1981) позволяла получать программу и документацию из единого кода, причём включала специальную технологию программирования [3]; Д. Кнут указывал, что без неё он не смог бы создать более большой и сложный продукт; технология описывалась как позволяющая «сделать программы более надёжными, более переносимыми, более легко сопровождаемыми, возможно, более легко разрабатываемыми, нежели это выполняется при работе только на языке высокого уровня». Двухуровневая грамматика А. ван Вейнгаардена (1968) позволила в формальном виде описать контекстные условия, которые при описании языка в расширенной форме Бэкуса-Наура (РБНФ) приходилось передавать словесно [5-6]; эта грамматика предоставляет способ определения потенциально бесконечных грамматик через конечное число правил.

Интересны и практически полезны работы на основе шитого кода. Прежде всего, это язык форт (Forth, С. Н. Moore, около 1970 [4], в т. ч. реализация BetaForth (С. Н. Баранов [5, 7])), основанные на нём и близкие ему технологии Комфорт (В. П. Котляров [6]) и иные, а также появившийся уже в новом тысячелетии язык Factor (2003, С. Пестов [8]). Эти системы позволяют на основе крайне малого ядра (от нескольких байтов машинного кода) получить саморасширяемые системы общего или специального назначения (посредством «раскрутки»), специализированные языки путём доопределения и переопределения слов базовой системы (например, таким образом были получены трансляторы языков Lisp, Prolog, Оссам, и многих других). Factor продолжает при этом линию «конкатенативных» языков, к каковым авторы относят и языки Forth, Joy, PostScript, Cat в противовес «аппликативным» языкам C, Python, Java, C, C++, Haskell и большинству прочих языков. Все эти

расширяемые системы изначально реализуются как интерпретаторы, но, как правило, позволяют выполнять отчуждение получаемого программного кода, целевую компиляцию или сохранение образа системы для последующего использования и наращивания.

Перспективны и грамматики, и трансляторы для языков типа SDF (1989–2007, Syntax Definition Formalism [2]). Этот формализм предназначен для «высокоуровневых описаний грамматик для языков программирования, прикладных языков, доменно-специфичных языков, форматов данных и прочих компьютерных формальных языков». Результатом его применения являются как синтаксическое описание языка, так и построение программы анализатора (parser) для него. Несмотря на то, что в примерах, сопровождающих эти работы, как правило, рассматриваются устаревшие языки типа Кобола, сами подходы по-прежнему имеют будущее. В основе этих работ лежит подход GLT (Generic Language Technology, 2002+), развивающий известную технологию ASF+SDF (Syntax Definition Formalism + Algebraic Specification Formalism, 1996).

Отметим общие тенденции в развитии языков программирования, в т. ч. в C++ и Java: от структурного программирования был совершён переход к объектно-ориентированному, а в нём — к средствам повышения технологичности работы: стандартные библиотеки на основе шаблонов, декораторов и т. п. Попутно шло и продолжается до сих пор создание языков как расширений уже существующих. Так, например, Симула (версий 1 и 67 [9]) включает в себя язык Алгол-60, но дополняет его своими предметно-ориентированными конструкциями, поскольку язык предназначен для выполнения работ по имитационному моделированию; некоторые другие языки и системы имитационного моделирования пошли по тому же пути, но основывались на расширении Фортрана и т. п. Дополнение языков пакетами используется в Tcl/Tk [10]: интерфейсный пакет Tk на основе Tcl заметно дополняет его синтаксис, причём эта возможность заложена в базовой системе; библиотека jQuery [11] выполнена на JavaScript'e; весьма новый язык Hancock (предназначен для обработки больших объёмов относительно однородных данных, разработан фирмой AT&T Labs [12]) — на C++. Таким образом, видно, что подход популярен и, соответственно, требует поддержки соответствующими технологиями и инструментарием.

Хорошо видно современное продолжение этих традиций — системы MPS для построения DSL (Domain Specific Languages), разработки Google/IBM. Доклад К. Соломатова (фирма JetBrains, 2010 [13]), представленный на конференции «Tech Days, Sun&Oracle» в Санкт-Петербурге в апреле 2010 г. — система «доменно»-ориентированного расширения языка (DSL) и системы программирования Java, на основе построения схем расширений языка с получением как транслятора, так и интегрированной среды разработки (MPS) для требуемого расширения языка, причём реализуются все основные требования, предъявляемые к подобным системам: форматирование и автодополнение кода, подсветка синтаксических конструкций, согласованное переименование (реинжиниринг), выдача справочной информации и т. п.; на данном этапе выполняются работы только на языке Java, но нет принципиальных ограничений, которые не позволили бы вести работу на других хорошо грамматически специфицированных языках высокого уровня, например, на C++. Можно поспорить с утверждением автора доклада о том, что классические текстовые способы спецификаций не соответствуют современным требованиям, а для реализации новых языков нужны диаграммы на основе графов; напротив, согласованное использование различных (формально-строгих текстовых и визуально-привлекательных графических) средств может помочь пользователям-разработчикам языков и систем поддержки разработки программных систем на них получить качественный результат надёжнее, технологичнее, быстрее и нагляднее, в то время как для автоматического получения требуемых программных и сопровождающих компонент системы подходит только классический текстовый вариант.

В организационно-технологическом плане важны также проект построения семейства компиляторов для группы языков программирования GNU, а также свободное и открытое программное обеспечение (СОПО, FOSS). Проект GNU объединяет тысячи разработчиков программ по всему миру и позволяет им согласованно выполнять разработки от малого до сверхбольшого размера и сложности путём согласования требований и предоставления удобных сетевого и пакетного инструментария в сочетании с общеизвестными правилами и, фактически, технологиями взаимодействия сотрудников различного типа. Открытое и, особенно, свободное программное обеспечение, реализуя 4 известные свободы, сформулированные Р. Столманом [14], включающие свободу установки, использования и удаления программ, их адаптации и модификации, а также распространения как исходного, так и производного продукта, подразумевают доступ к исходному коду программ для их развития следующими поколениями разработчиков; таким образом, осуществляется создание новых систем на основе существующих, а соответствующие технологии поощряют именно такое развитие (единые компиляторы и утилиты, системы согласованной разработки кода и версионирования, документирования и т. п.).

Заключение

На сегодняшний день построен, теоретически и экспериментально обоснован вариант метатехнологии построения трансляторов языков программирования на основе КСР-грамматик [15–19, 24, 25, 27]. Видно, что развитие систем формализации и преобразования языков (в частности,

трансляции) идёт по пути повышения технологичности, универсальности, переносимости, надёжности и безопасности, что достигается в т.ч. повышением уровня описания, применением метаописаний языков и систем, создания полноценных метатехнологий программирования. Авторы доклада последовательно применяют данный подход в своих работах.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 15408 – 2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», Госстандарт России – М., 2002.
2. A. Van Wijngaarden et al.: "Report on the algorithmic language ALGOL 68" *Numerische Mathematik* 14, pp. 79–218 (1969) Springer-Verlag Berlin.
3. Revised report on the algorithmic language Algol 68// *ACTA Informatica* 5 pp.1–236, (1974). In Russian "Пересмотренное сообщение о языке ALGOL 68".
4. Cornelis H.A.Koster "Affix grammars" в книге: *Algol 68 implementation/* Noth-Holland. 1971.
5. D.E.Knuth "Semantics of context-free languages" *Mathematical system theory* pp. 127–145. 1968 (2). Correction in *Mathematical system theory* 1075. (5)/1
6. H.F.Ledgard "Production system or can we do better than BNF?" *CACM* 1974/2, pp.94–102.
7. V.H.Williams "Static semantics features of Algol 60, and BASIC". *The Computer Journal*. Vol. 21. No. 3. pp. 234–242.
8. M.Griffiths "Relationship between definition and implementation of language". //Advanced courses on software engineering. *Lecture Notes in Economics and Math Syst.* Springer-Verlag 1973.
9. G.V.Bochmann "Semantic evaluation from left to right". *CACM* 1976/2 pp. 55–62.
10. Dick Grune "Two Level grammars are more expressive than Type 0 grammars or are they?", Dept. of Mathematics and Computer Science Vrije Universiteit, De Boelelaan 1081, HV Amsterdam. dick@cs.vu.nl
11. M.Sintzoff, "Existence of a van Wijngaarden syntax for every recursively enumerable set", *Annales de la Societe Scientifique de Bruxelles* 81(II), pp.115–118 (1967).
12. A. van Wijngaarden, "The generative power of two-level grammars", pp 9–16 in *Automata, Languages and Programming: Lecture Notes in Computer Science* #14, ed. J. Loecks, Springer-Verlag, Berlin (1974).
13. Dick Grune and Ceriel Jacobs "Parsing Techniques. A Practical Guide", Ellis Horwood, Chichester, England (1990), p.322.
14. Cornelis H.A.Koster, et all. *CDL3 manual* \http://www.cs.ru.nl/~kees/vbcourse/ivbstuff/cdl3.pdf
15. Федорченко Л.Н Извлечение крайней рекурсии из КСР-грамматики в системе SynGT, Труды СПИИРАН, вып.1, т. 1. — СПб: СПИИРАН, 2002, с.350–359
16. Федорченко Л.Н. О регуляризации контекстно-свободных грамматик. *Изв. вузов. Приборостроение*, 2006. Т.49, №11, с.50–54.
17. Федорченко Л.Н. , Мартыненко Б.К. Эквивалентные преобразования КСР-грамматик в регулярной форме в практике построения языковых процессоров. Часть первая. Определение и распознавание КСР-языков посредством синтаксических граф-схем. - Ленинград, АН СССР, Ленинградский Научно-исследовательский Вычислительный Центр, 1983г.
18. Федорченко Л.Н. Регуляризация контекстно-свободных грамматик на основе эквивалентных преобразований синтаксических граф-схем. Дисс... канд. тех. наук по специальности 05.13.11, СПИИРАН, 2009. 160 с.
19. Мартыненко Б.К. Синтаксически управляемая обработка данных. СПб, СПбГУ, 1997. 362 с.
20. Пересмотренное сообщение об Алголе 68. Ред. А. ван Вейнгаарден. Пер. с англ. — М., Мир, 1979. 533 с.
21. Introduction to Generic Language Technology. M. van der Brand, P. Klint, J. Vinju. — CWI, UvA, TUE, 2007.
22. Donald Knuth. "Literate Programming (1984)" in *Literate Programming*. CSLI, 1992, pg. 99.
23. Moore C. H. FORTH: A New Way to Program a Mimi-Computer. *Astr. And Astrophys. Suppl.* 1974. Vol.5. P. 497–511.
24. Баранов С.Н. Перенос и реализация больших пакетов компьютерной алгебры на базе форт-технологии. Дисс... доктора физ.-матем.наук по специальности 05.13.16 – применение вычислительной техники, математического моделирования и математических методов в научных исследованиях Л: ЛИИАН, 1990, 156 с.
25. Баранов С. Н., Ноздронов Н. Р. Язык Форт и его реализации. — Л.: Машиностроение, Ленингр. Отделение, 1988. 157 с.
26. Котляров В. П. CASE-технология и возможности современных CASE-средств в поддержке этапов проектирования программного продукта. // *Системная информатика*. Новосибирск, ВО «Наука», Сибирская издательская фирма, 1995. Вып. 4: Методы теоретического и системного программирования. С. 272–303.
27. Баранов С.Н., Колодин М.Ю. Феномен Форта. // *Системная информатика*. Новосибирск, ВО «Наука», Сибирская издательская фирма, 1995. Вып. 4: Методы теоретического и системного программирования. С. 193–291.
28. Сайт разработки языка Factor. URL: <http://factorcode.org>. — 2003.
29. Андрианов А. Н., Бычков С. П., Хорошилов А. И. Программирование на языке симула–67. — М.: Наука, гл. ред. Физ.-мат. Лит., 1985. 288 с.
30. Уэлш Б. Б., Джонс К., Хоббс Дж. Практическое программирование на Tcl и Tk. — М.: Изд. Дом «Вильямс», 2004. 1136 с.
31. Бибо Б., Кац И. jQuery. Подробное руководство по продвинутому JavaScript. — СПб: Символ-Плюс, 2009. 384 с.
32. K.Fisher, K.Hogstedt, A.Rogers, and F.Smith. *Hancock Manual*. — AT&T, 2009.
33. Solomatonov K. *Extending Java And Developing DSLs With Open Source Language Workbench JetBrains MPS*. — Sun&Oracle Tech Days, St.Petersburg, 2010.
34. URL: http://ru.wikipedia.org/wiki/Свободное_программное_обеспечение.
35. Колодин М. Ю. Мета-преобразования систем документов с гипертекстовой разметкой. // Труды СПИИРАН, вып.3, т.1.— СПб: СПИИРАН, 2006.
36. Колодин М. Ю. Практика и перспективы многоуровневых гипертекстов. // VIII Республиканская открытая научная конференция "Современные проблемы информатизации". – Воронеж, 2002–2003.

Копыльцов А.В., Сорокин И.В.

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

ЭНТРОПИЙНЫЙ АНАЛИЗ ФАЙЛОВ ДЛЯ ВЫЯВЛЕНИЯ И КЛАССИФИКАЦИИ ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Исследования, направленные на разработку алгоритмов анализа исполняемых файлов, актуальны в антивирусной индустрии, поскольку позволяют выявлять различные типы вредоносного программного обеспечения. Одним из таких типов являются программы-упаковщики, выступающие в

роли защиты от антивирусов. В них используются различные методы (обфускация, антидампинг, антиэмуляция и др.) для противодействия обнаружению скрытого вредоносного кода. В работах [3,5,9] при классификации вредоносных программ применяется метод N-грамм. Используя частоту появления последовательностей байт в файле как некую характеристику исполняемого файла можно применять различные методы классификации, такие как: метод ближайшего соседа, байесовский подход, метод опорных векторов и т.д. Особенно следует выделить работу [7], в которой также используются N-граммы. В этой работе данный метод используется не только для классификации исполняемых файлов как вредоносных, так и нормальных, но и для определения упакованности (или неупакованности) программ. Также в [7] применяются методы извлечения данных (data mining). По аналогии с работой [8], авторы выбирают некоторые наборы признаков исполняемого файла (например: количество секций, размер импорта и т.п.), на основе которых строят модель классификации. Важной деталью этой работы является то, что авторы используют комбинированный подход при разработке системы классификации [6]. Однако в опубликованных ранее работах недостаточно учитывается энтропийная структура упакованных файлов. Поэтому предлагается подход, позволяющий задать меру близости между файлами на основе анализа их энтропийной структуры, с целью дальнейшей классификации вредоносного программного обеспечения.

Постановка задачи

Представленный подход основывается на работе [4], где авторы исследуют особенности сжатия различных программ-упаковщиков. Для этого рассматриваемый файл, представленный в виде последовательности байтов, разбивается на блоки и для каждого такого блока вычисляется энтропия. Таким образом, файл представляется в виде массива векторов, компонентами которого являются порядковый номер блока и его энтропия. В качестве функции расстояния между двумя наборами векторов авторы рассмотрели евклидово расстояние и косинус угла между ними. Учитывая то, что на различных по длине файлах результат применения выбранных функций неудовлетворительный, авторы используют дополнительные эвристические методы. В частности, предлагают рассматривать не все блоки файла, а, например, только несколько блоков с начала или конца файла. Для решения этой проблемы наш подход, основывается на применении методов сегментации и обработки строк.

Описание модели

Первоначально исходный файл, с использованием метода скользящего окна, представляется в виде массива векторов $(\vec{x}_i, \vec{y}_i)_{i=1}^M$, где M - количество всех окон (рисунок 1). Для подсчета энтропии в каждом окне используется формула

$$y_i = -\sum_{j=1}^n p(j) \log_2 p(j), \quad (1)$$

где $p(j)$ – частота появления j -го байта в i -м окне, n – количество различных байтов в окне.

Затем ставится задача о выделении областей различных по своей структуре. Для решения подобной задачи сегментации необходимо использовать модели, являющиеся гибридными моделями регрессии и группирования: отдельные элементы исходных данных должны быть объединены в группы, для каждой из которых строится собственная регрессионная модель.

В качестве исходных данных выступает набор пар векторов $(\vec{x}_i, \vec{y}_i)_{i=1}^M$. Причем не допускается произвольное группирование элементов данных $(\vec{x}_i, \vec{y}_i)$. Тогда задачу сегментации можно сформулировать следующим образом. Пусть есть набор измерений $(\vec{x}_i, \vec{y}_i)_{i=1}^M$, где $\vec{x}_i \in X = N$ и $\vec{y}_i \in Y = R$. Необходимо сформировать области $G_1, \dots, G_k \subset X$ и для каждого набора пар $\{(\vec{x}_i, \vec{y}_i) : \vec{x}_i \in G_k\}$ построить собственную регрессионную модель $g_k(\vec{x}, \vec{w}_k) : G_k \rightarrow Y$.

Для определения критерия качества модели сегментации был использован теоретико-информационный подход, в рамках которого применялся принцип минимальной длины описания (MDL).

На основе этого принципа формула для описания файла представляется в виде:

$$L = \sum_k MDL((\vec{x}_i, \vec{y}_i) : \vec{x}_i \in G_k) + MDL(\delta G), \quad (2)$$

где первая сумма – длина описания регрессионной модели для точек, попавших в область G_k , а вторая сумма – длина описания границы, образованной каждой областью G_k . Остановимся более подробно на каждом слагаемом в этой формуле.

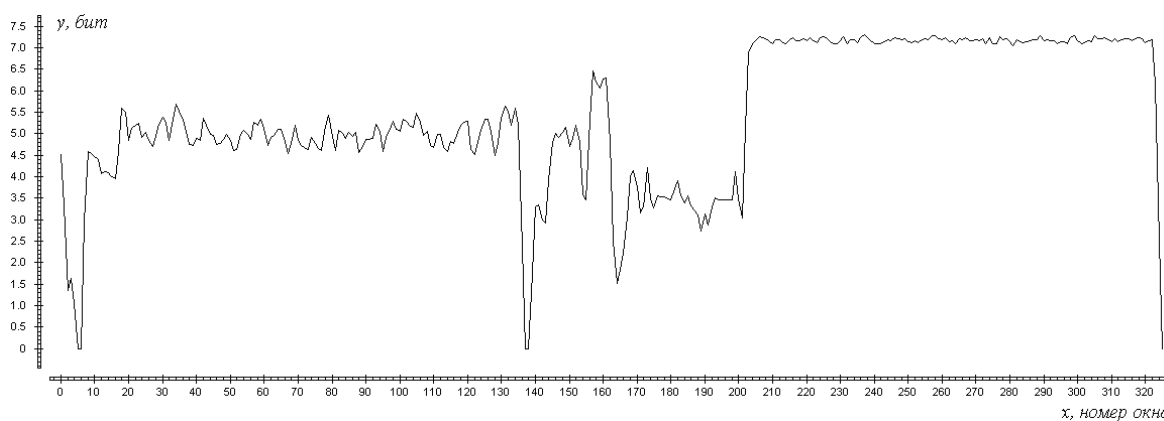


Рис. 1. График энтропии файла. По оси абсцисс – порядковый номер окна, по оси ординат – уровень энтропии в окне

Длина описания регрессионной модели определяет качество регрессионной модели в определенной области. Мы рассматривали линейную регрессионную модель вида:

$$\vec{Y} = \hat{X}\vec{w} + \vec{R},$$

где $\vec{w}$ – n неизвестных коэффициентов регрессии, $\vec{R}$ – вектор невязок. Для упрощения расчетов была выбрана аппроксимация полиномом первой степени, а для определения коэффициентов регрессии использован метод наименьших квадратов. Таким образом, в рамках теоретико-информационного подхода был выбран весьма простой критерий, позволяющий судить о сложности регрессионной модели:

$$MDL = L_r + L_p = M \log_2 \sigma[\vec{r}_i] + \frac{n}{2} \log_2 M, \quad (3)$$

где L_r – длина описания невязок, L_p – длина описания параметрической части модели, M – количество окон в G_i области, $\sigma[\vec{r}_i]$ – среднеквадратичное отклонение невязок в G_i области, n – количество коэффициентов регрессии ($n = 2$).

Вторая сумма из общей формулы (2) может быть проинтерпретирована как критерий качества группирования. Этот критерий определяется сложностью границы образованной областями G_k . Для ее формирования из каждой области мы выбрали три точки: две крайние и одну среднюю. К получившейся границе применили тот же самый критерий (3), что и для обычной области.

В итоге, для нахождения последовательности областей G_k , мы использовали следующий алгоритм группирования:

1. Объединение областей, не превышающих определенный минимум энтропии.
2. Объединение области, количество окон в которой меньше трех, с одной из своих соседней. Из двух соседних выбирается та, у которой уровень энтропии более близок. Это сделано для того, чтобы была возможность оценить сложность каждой области по формуле (3).
3. Последовательное объединение областей граничащих друг с другом, если это объединение приводит к уменьшению целевой функции (2). Причем, каждый раз шаг начинать с области, объединение которой дает наилучший результат.

Основной задачей стоящей перед нами была возможность сравнивать файлы. Описанный выше алгоритм позволяет представить файл в виде последовательности областей состоящих из сгруппированных окон. Каждую такую область будем рассматривать как некий символ, который описывается двумя характеристиками: размер – количество окон, энтропия – среднее значение энтропии окон. Последовательность таких символов будем называть строкой. Благодаря такому подходу можно применить различные методы и алгоритмы вычислений на строках [2].

В качестве функции расстояния d нами было выбрано расстояние преобразования. Оно определяется как минимальное количество операций удаления, вставки и подстановки, необходимых для преобразования одной строки в другую. Перечислим некоторые свойства операции редактирования, выполняемых на одиночных символах a, b .

1. Вставка (замена пустой строки ε на символ a): $d(\varepsilon, a) > 0$.
2. Удаление (замена символа на пустую строку ε): $d(b, \varepsilon) > 0$.
3. Подстановка (замена символа a на символ b): $d(a, b) > 0 \Leftrightarrow a \neq b$.

Таким образом, расстояние между двумя отдельными символами будем рассматривать как стоимость выполнения соответствующих операций редактирования. Учитывая то, что каждый символ описывается двумя характеристиками (s – количество блоков и e – уровень энтропии), определим функцию стоимости следующим образом:

$$d(a, b) = \sqrt{|e_a - e_b|} + \log|1 + s_a - s_b| + \sqrt{|e_a - e_b|} (|s_a - s_b|^2 \delta), (4)$$

где δ – параметр, определяющий значимость разницы в размерах двух областей.

Тогда, расстояние между двумя строками зададим как минимальную стоимость преобразования символов одной строки в символы другой, используя алгоритм динамического программирования. Это означает, что входные строки x_1 и x_2 , длиной n_1 и n_2 соответственно, сравниваются слева направо. Для этого введем двумерный массив стоимостей $c_{i,j}$, определяющий стоимость преобразования подстроки длиной i символов из первой строки x_1 в подстроку длиной j символов из второй строки x_2 , причем $i \in 0, \dots, n_1$ и $j \in 0, \dots, n_2$. Значения для этого массива определим следующим образом:

– $c_{0,0} = 0$ – стоимость преобразования пустой строки в пустую строку;

– $c_{i,0} = \sum_{1 \leq a \leq i} d(a, \varepsilon)$ – стоимость удаления первых i символов строки x_1 таким образом, чтобы сформировать пустую строку;

– $c_{0,j} = \sum_{1 \leq b \leq j} d(\varepsilon, b)$ – стоимость вставки первых j символов строки x_2 в пустую строку;

– $c_{i,j} = \min \{ c_{i-1,j} + d(i, \varepsilon), c_{i,j-1} + d(\varepsilon, j), c_{i-1,j-1} + d(i, j) \}$ – рекурсивное определение

стоимости преобразования соответствующих подстрок.

В итоге, используя массив стоимостей и схему рекурсии для его вычисления, минимальная стоимость преобразования одной строки в другую определяется последним элементом массива $c_{n_1 n_2}$.

Результаты и их обсуждение

В качестве примера рассмотрим сравнение двух файлов, взятых из коллекции антивирусной компании Dr.Web. Оба файла представляют собой вредоносные программы типа Trojan.Fakealert, защищенные с использованием одного и того же упаковщика. Размер первого файла составляет 347136 байт, а второго – 186368 байт. Разница почти вдвое позволит проверить эффективность, как алгоритма сегментации, так и функции расстояния.

Во-первых, построим графики упакованности обоих файлов. В качестве размера окна было взято 256 байт, а его смещение 128 байт. На рисунках 2 и 3 представлены первый и второй файл соответственно.

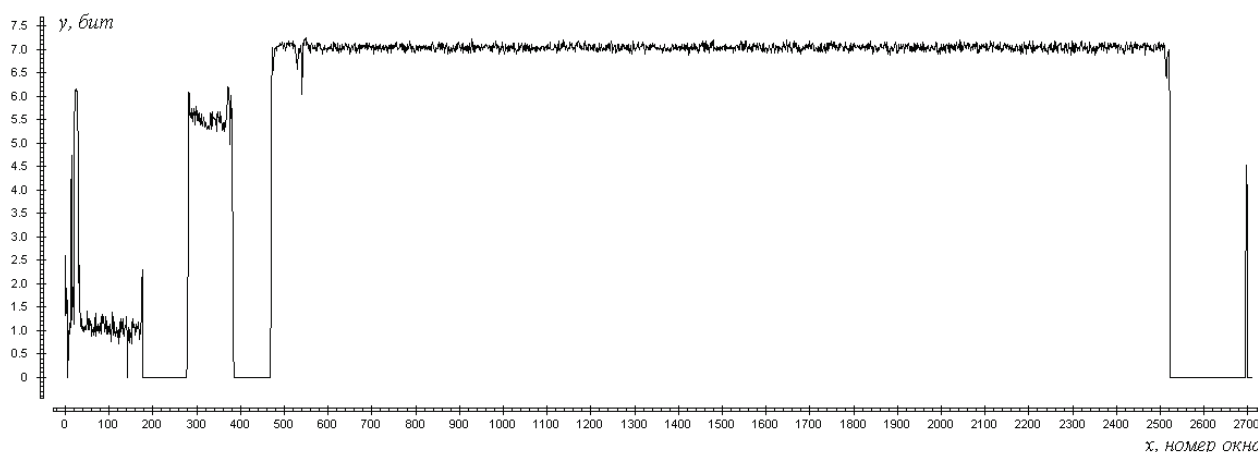


Рис. 2. График энтропии первого файла. По оси абсцисс – порядковый номер окна, по оси ординат – уровень энтропии в окне

Затем, применим алгоритм сегментации. В таблице 1 представлены характеристики сформированных областей. Так, для каждого файла было выявлено 14 областей. Как можно увидеть, структурные различия между файлами незначительны. В первом файле выявлена 5-я область, которой нет во втором файле, а во втором файле присутствует 3-я область, отсутствующий в первом файле.

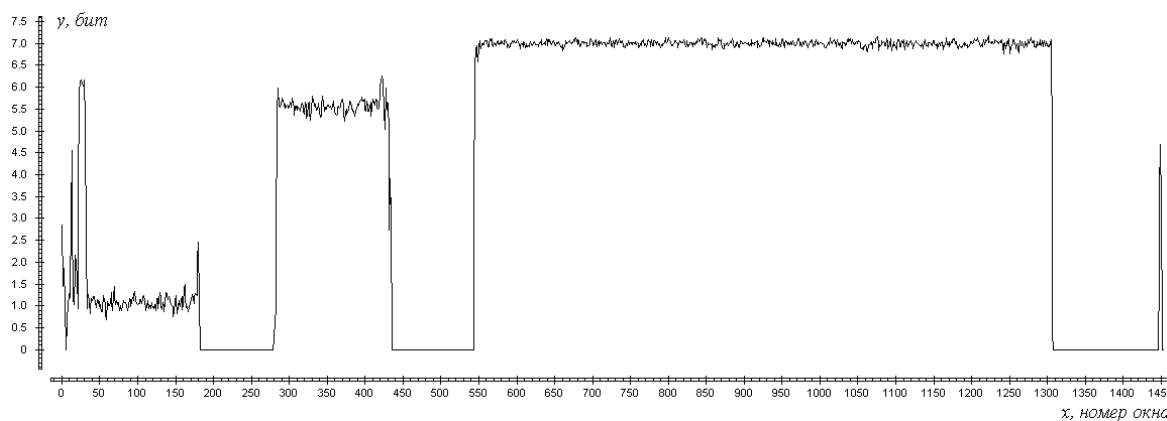


Рис. 3. График энтропии второго файла. По оси абсцисс – порядковый номер окна, по оси ординат – уровень энтропии в окне

Таблица 1

Сформированные области двух файлов, соответственно первого и второго файла
(выделенные строки обозначают недостающие области)

№	Количество окон	Энтропия (бит)	Коэффициент W_1	№	Количество окон	Энтропия (бит)	Коэффициент W_1
1	5	1.7188	-0.18	1	5	1.7557	-0.32
2	8	0.7485	0.17	2	7	0.7579	0.24
3	8	2.7545	-0.30	3	3	3.5282	-0.09
4	9	5.8261	-0.05	4	7	1.5329	0.03
5	3	2.1553	0.17	5	10	5.4801	0.10
6	144	1.0757	0.00	6	149	1.0975	0.00
7	105	0.0746	0.00	7	103	0.0644	0.00
8	95	5.5270	0.00	8	148	5.5696	0.00
9	7	4.9655	-0.44	9	3	3.2358	0.16
10	87	0.0317	0.00	10	110	0.0281	0.00
11	2051	7.0327	0.00	11	762	6.9932	0.00
12	174	0.0183	0.00	12	141	0.0152	0.00
13	3	3.9395	0.06	13	3	3.8785	-0.19
14	11	0.1012	-0.05	14	3	0.1200	-0.18

Таблица 2

Массив стоимостей сравнения двух файлов. По вертикали – первый файл, по горизонтали – второй
(выделенные ячейки обозначают стоимости выполненных операций редактирования)

№	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	0.01	0.02	0.02	0.07	0.79	1.11	2.92	2.93	3.28	20.8	21.27	21.28	21.28	0
1	0.01	0	0.01	0.02	0.07	0.76	1.08	2.89	2.89	3.24	20.76	21.24	21.24	21.25	0.01
2	0.01	0.01	0	0.01	0.05	0.76	1.09	2.89	2.89	3.24	20.76	21.23	21.24	21.24	0.01
3	0.04	0.03	0.03	0.04	0.02	0.73	1.06	1.74	1.75	2.1	19.05	19.52	19.53	19.53	0.04
4	0.04	0.04	0.03	0.03	0.02	0.74	1.06	1.75	1.75	2.09	19.05	19.53	19.53	19.53	0.04
5	0.41	0.37	0.37	0.39	0.38	0.02	0.34	2.11	2.11	1.86	19.38	19.18	19.18	19.18	0.41
6	0.59	0.54	0.55	0.56	0.56	0.2	0.02	1.83	1.83	2.03	19.56	19.35	19.36	19.36	0.59
7	1.13	1.09	1.1	1.11	0.67	0.74	0.57	0.05	0.06	0.41	7.34	7.82	7.82	7.83	1.13
8	1.14	1.1	1.09	1.11	0.68	0.76	0.58	0.06	0.06	0.41	7.36	7.83	7.82	7.82	1.14
9	1.28	1.24	1.23	1.25	0.82	0.85	0.72	0.2	0.2	0.07	7.49	7.39	7.39	7.4	1.28
10	33.11	33.06	33.06	33.07	32.65	32.67	32.54	11.33	11.33	11.68	0.38	0.86	0.86	0.86	33.11
11	33.44	33.39	33.39	33.4	32.98	32.79	32.68	11.66	11.66	11.34	0.71	0.39	0.4	0.4	33.44
12	33.44	33.4	33.39	33.41	32.98	32.79	32.68	11.66	11.66	11.34	0.72	0.39	0.39	0.39	33.44
13	33.45	33.41	33.4	33.4	32.99	32.8	32.69	11.67	11.67	11.35	0.73	0.4	0.4	0.39	33.45
14	0	0.01	0.02	0.02	0.07	0.79	1.11	2.92	2.93	3.28	20.8	21.27	21.28	21.28	0.39

Сравнив сформированные последовательности областей, получим массив стоимостей $c_{i,j}$, представленный в таблице 2. Второй столбец в этой таблице обозначает стоимости операций удаления соответствующих областей из первого файла. Соответственно, вторая строка таблицы обозначает стоимости операций вставки символов из второго файла. Значения ячеек с индексами (2,3) и (4,4) обозначают стоимости операций удаления дополнительных областей. Также следует обратить внимание на ячейку с индексами (10,10) – это стоимость операции преобразования самых больших участков рассматриваемых файлов. Окончательная стоимость преобразования первой последовательности во вторую приблизительно составляет 0.39. Если учитывать, что стоимость создания первой последовательности составляет 33.45, а стоимость удаления второй 21.28, то схожесть рассматриваемых файлов 99.29%.

Заключение

Представленное решение позволяет сравнивать файлы по их энтропии. При этом учитывается структура файла, т.е. расположение в нем характерных участков, благодаря чему появляется возможность адекватно сравнивать файлы разной длины. Таким образом, данный подход может быть применен для выявления различных вредоносных программ, упакованных специализированными программами-упаковщиками.

СПИСОК ЛИТЕРАТУРЫ

1. Потапов А.С. Распознавание образов и машинное восприятие: Общий подход на основе принципа минимальной длины описания. СПб.: Политехника, 2007 – 548с.
2. Смит Б. Методы и алгоритмы вычисления на строках.: Пер. с англ. – М.: ООО «И.Д. Вильямс», 2006. – 496с.
3. Abou-Assaleh T., Cercone N., Keşelj V., Sweidan R. Detection of New Malicious Code Using N-grams Signatures. In Proceedings of the Second Annual Conference on Privacy, Security and Trust (PST'04), Fredericton, New Brunswick, Canada, 2004.
4. Ebringer R., Li Sun, Boztas S. A fast randomness test that preserves local detail. Virus bulletin conference. October 2008.
5. Kolter J. Z., Maloof M. A. Learning to detect malicious executables in the wild. In Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 470–478, New York, 2004.
6. Kuncheva L. I. Combining Pattern Classifiers: Methods and Algorithms. Wiley-Interscience, 2004.
7. Perdisci R., Lanzi A., Lee W. "McBoost : Boosting Scalability in Malware Collection and Analysis Using Statistical Classification of Executables". Annual Computer Security Applications Conference, ACSAC 2008.
8. Schultz M. G., Eskin E., Zadok E., Stolfo S. J. Datamining methods for detection of new malicious executables. In IEEE Symposium on Security and Privacy, 2001.
9. Santos I., Penya Y. K., Devesa J. D., Bringas P. G. N-grams-based File Signatures for Malware Detection. ICEIS 2009 – Proceedings of the 11th International Conference on Enterprise Information Systems, Volume AIDSS, Milan, Italy, May 6–10, 2009.

Любимов А.В.

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

СОГЛАСОВАНИЕ ПОЛУФОРМАЛЬНЫХ МОДЕЛЕЙ ПРИ ИНЖИНИРИНГЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Методика интегрального инжиниринга информационной безопасности

В работе [1] было представлено общее описание методики интегрального инжиниринга стандартов информационной безопасности (ИБ) как подхода к решению целого ряда задач ИБ, основанного на построении и использовании систем полуформальных и формальных моделей семейств стандартов предметной области. В соответствии с этим подходом из семейств стандартов ИБ извлекаются их методологии, каждая методология представляется в виде системы согласованных моделей (обратный инжиниринг), которые затем модифицируются с различными целями (внутренний инжиниринг) и используются для создания и преобразования объектов, процессов, систем и документов ИБ (прямой инжиниринг).

Были предложены состав и структура интегральной модели семейства стандартов, в соответствии с которой интегральная система моделей методологии каждого семейства представляет собой совокупность функциональных (IDEF0, DFD), информационных (ER, IDEF1X), объектных (UML Class diagrams), процессных (UML Activity Diagrams) и онтологических (IDEF5, OWL) моделей, определенным образом согласованных между собой. Были рассмотрены варианты последовательности разработки интегральных систем, описаны уровни и виды интегрального инжиниринга и перечислены области и конкретные задачи ИБ, где применение интегрального инжиниринга наиболее эффективно. В качестве полезного инструмента для решения прикладных задач была представлена библиотека моделей стандартов ИБ, приведены необходимые спецификации моделей, описано текущее состояние библиотеки и перспективы ее развития и пополнения.

В настоящей работе общие положения, изложенные в [1], развиваются и углубляются, в частности – более детально рассматриваются методы внутреннего и прямого инжиниринга, объекты и операции инжиниринга, описываются общие логические схемы применения операций в конкретных приложениях.

Объектами интегрального инжиниринга могут выступать как сущности предметной области (domain entities), так и модели из интегральных систем для семейств стандартов. Сущностями предметной области, над которыми выполняются операции интегрального инжиниринга, могут служить: международные, национальные и низкоуровневые (отраслевые, ведомственные, корпоративные) стандарты; нормативно-методическая документация (НМД) по информационной безопасности (рекомендации, методики, руководства, руководящие документы, регламенты, профили, технические отчеты различного уровня); программное обеспечение (ПО) поддержки стандартов и его внешние или проектные спецификации; системы и средства защиты информации как организационного, так и технического уровня; и т. д.

2. Операции инжиниринга

Независимо от вида и уровня, инжиниринг включает в себя стандартный набор операций, который представлен на рисунке 1 в виде UML диаграммы.

Любая из представленных здесь операций инжиниринга может применяться как к моделям (компонентам интегральных систем), так и к любым сущностям предметной области. Операции над сущностями предметной области могут выполняться (и в настоящее время часто выполняются) и без

построения моделей. Основная инновация, предлагаемая интегральным инжинирингом, состоит в том, чтобы выполнять эти действия системно, по единой методике, на основе построенных и модифицированных моделей, включив само построение и модификацию моделей (обратный и внутренний инжиниринг) в общую последовательность работ как необходимые этапы. При таком подходе операции, которые необходимо выполнить над сущностями предметной области при решении конкретной прикладной задачи, естественным образом порождают (индуцируют) аналогичные операции над моделями этих сущностей. Пример такого порождения для операции согласования приведен на рисунке 2 в виде UML диаграммы.

Действия, связанные с согласованием (coordination) моделей, являются ключевой группой операций внутреннего инжиниринга и включают в себя:

- расширение (expansion);
- гармонизацию (harmonization);
- обобщение (generalization).

Все эти операции в качестве составной части предполагают сравнение моделей (models comparision).

Расширение (expansion) моделей имеет целью их взаимное дополнение (reciprocal supplement). При его выполнении некоторые концепты, отсутствующие в одной модели, переносятся в нее из другой и связываются с уже существующими.

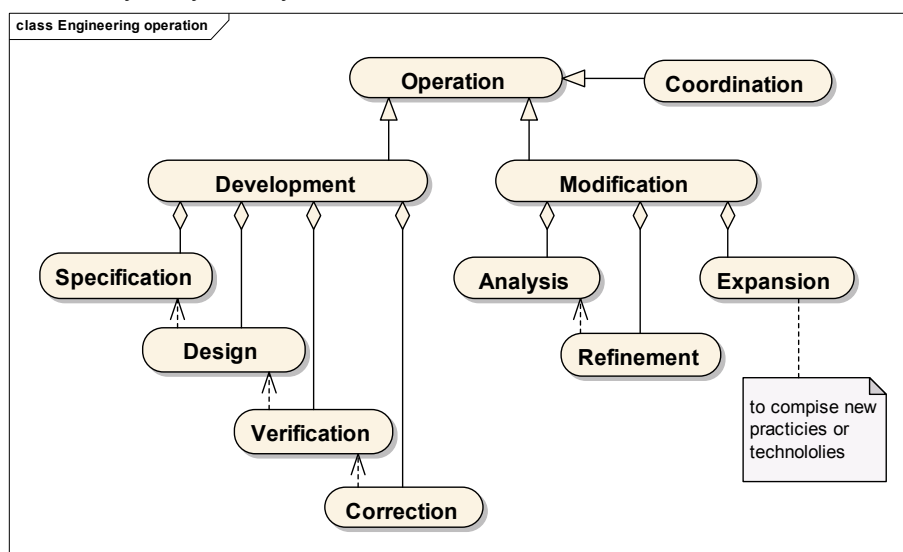


Рис. 1. Диаграмма Engineering operation

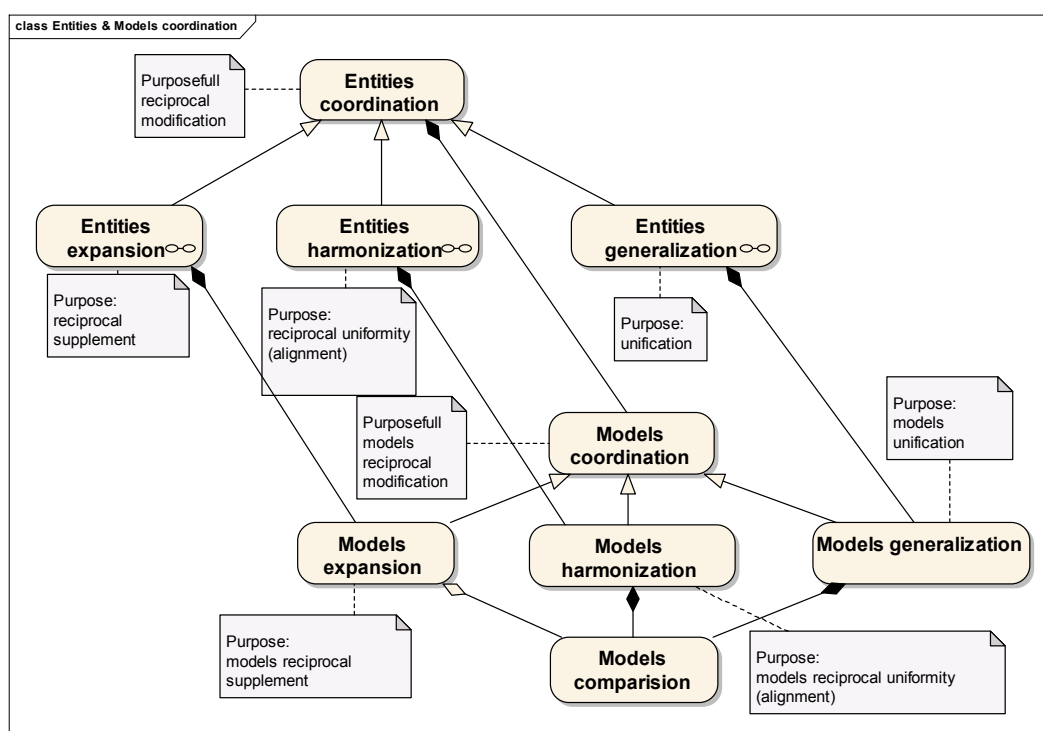


Рис. 2. Диаграмма Entities & Models coordination

Примечание. Под концептом (concept) понимается определенное понятие, идея, концепция, выраженная в модели посредством набора элементов (классов, атрибутов, методов, процессов, ресурсов) и связей (links) между ними.

При взаимном расширении моделей новые (относительно совокупности обеих расширяемых моделей) элементы практически не образуются, модификация существующих выполняется в незначительной степени.

Гармонизация (harmonization) моделей имеет целью их взаимное приведение к однородному виду (uniformity), в зарубежной терминологии – выравнивание (alignment). При ее выполнении близкие по смыслу концепты в обеих моделях преобразуются таким образом, чтобы иметь *по возможности* одинаковое содержимое, структуру и окружение (контекст). При гармонизации моделей новые элементы также практически не образуются, хотя модификация уже существующих может быть значительной.

Обобщение (generalization) моделей имеет целью их объединение (unification), частичное (как правило) или полное (редко). При его выполнении для близких по смыслу концептов в обеих моделях строится новый концепт, для которого объединяемые являются частными случаями. При обобщении моделей образуется известное число новых элементов, но изменения в исходных моделях минимальны по сравнению с расширением и гармонизацией. Во многих случаях новые элементы, образующие обобщенную модель (generalized model), можно хранить отдельно, оставив исходные модели практически без изменений, но иногда удобнее добавить их в обе исходные модели, например – в виде отдельного пакета. Совокупность исходных моделей и обобщенной модели представляет собой объединенную модель (unified model). Обобщение моделей, как правило, выполняется в тех случаях, когда их гармонизация по каким-либо причинам невозможна или нецелесообразна. При использовании интегрального инжиниринга в приложениях операция обобщения моделей является основным инструментом построения гибридных сущностей предметной области: стандартов, систем и средств защиты информации, программного обеспечения поддержки и так далее.

3. Приложения интегрального инжиниринга: общие методы (логические схемы)

Методы (логические схемы) применения операций интегрального инжиниринга весьма гибки, разнообразны и существенным образом зависят от области и конкретной задачи приложения. Ниже приводятся общие схемы операций инжиниринга, апробированные или планируемые к апробации в двух практических задачах согласования сущностей предметной области.

3.1 Анализ и улучшение международных стандартов

Каждый международный стандарт является обобщением разнообразного опыта многих организаций, полученного в разное время, в разных странах и с использованием различных подходов и методов. Несмотря на тщательную подготовку и последующую регулярную ревизию, он неизбежно содержит недочеты, выражающиеся, в частности, в неполноте или несогласованности отдельных определений, положений и рекомендаций. Эти и им подобные недочеты естественным образом выявляются как при объектном, так и при процессном анализе стандарта и явно проявляются в моделях. В соответствии с подходом интегрального инжиниринга устранение недочетов (уточнение и совершенствование) сначала производится на моделях путем дополнения, согласования и корректировки их элементов и связей, в результате чего получается скорректированная система моделей. По скорректированным таким образом моделям вырабатываются предложения по внесению изменений в стандарт. Логическая схема соответствующих операций инжиниринга представлена на рисунке 3 – UML диаграмма Standard analysis & refinement.

Конкретный пример применения метода интегрального инжиниринга в задаче анализа и коррекции словаря методологии семейства стандартов систем управления информационной безопасностью (СУИБ) приведен в работе [2].

Подобным же образом модели методологии стандарта при необходимости могут использоваться для его развития, в частности – для корректного расширения его предметной области (например – для учета новых практик или технологий).

3.2 Согласование стандартов информационной безопасности

Операция согласования применяется в первую очередь к стандартам ИБ, для которых она имеет особую актуальность, поскольку все другие сущности предметной области в той или иной степени на них основаны.

По мере возрастания значимости задач защиты информации, растет и количество стандартов, которые трактуют проблему обеспечения информационной безопасности с самых разных точек зрения. Например, семейство стандартов СУИБ – с организационной, семейство Общих Критериев (ОК) – с технологической, семейства ITIL и COBIT – с точки зрения корпоративного пользователя и т. д. (диверсификация подходов к обеспечению ИБ).

В силу различия целей, подходов и точек зрения даже такие базовые понятия ИБ, как Актив, Угроза, Уязвимость, Контрмера и т. д. имеют в этих семействах различное наполнение, структуру и

контекст. Объективно эти различия полностью устранить нельзя, но максимально сблизить концепты – возможно, а иногда и необходимо.

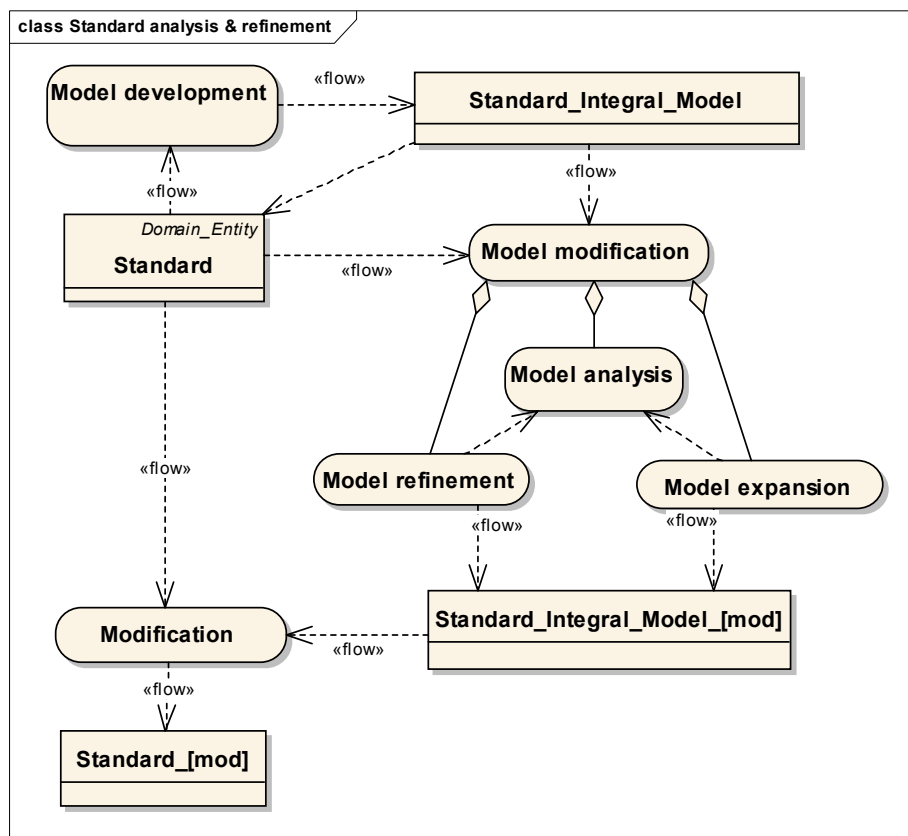


Рис. 3. Диаграмма Standard analysis & refinement

Как и в случае совершенствования стандартов, корректное и эффективное решение этой задачи может быть получено с использованием систем моделей стандартов. При этом возможны два подхода:

- непосредственное изменение стандартов путем их взаимного расширения или гармонизации;
- обобщение стандартов путем создания надстройки (метаметодологии) в виде метамодели, элементами которой являются метапонятия и их связи, по которой затем создается метастандарт.

Примечание. Метапонятие – такое обобщение двух или более понятий стандартов, при котором исходные понятия в каждом из стандартов являются частными случаями метапонятия.

При согласовании стандартов используются операции расширения, гармонизации и обобщения, содержание которых изложено выше в разделе "Операции внутреннего инжиниринга" применительно к моделям. В применении к сущностям предметной области принципиальных отличий нет.

В рамках первого подхода (взаимное изменение) выполняются операции гармонизации (схема представлена на рисунке 4 – UML диаграмма Entities harmonization) и расширения (проводится по аналогичной схеме). В рамках второго подхода выполняется операция обобщения, схема которой представлена на рисунке 5 – UML диаграмма Entities generalization.

Первый из упомянутых подходов обычно является менее затратным, но второй дает, как правило, более эффективный результат. Имеется также возможность комбинации обоих подходов в зависимости от конкретной задачи.

Набор кандидатов для согласования не ограничивается лишь стандартами ИБ. Для некоторых из них весьма актуальным оказывается согласование и с прилегающими стандартами, не относящимися непосредственно к ИБ. Например, для стандартов СУИБ это стандарты СМК (семейство ISO 9000), ITIL и COBIT, для Общих Критериев – стандарты ЖЦ ПО и и так далее.

Подход, связанный с обобщением и объединением (построением метамодели), является основным инструментом при построении гибридных сущностей предметной области – стандартов, СЗИ, ПО и т. д. Но особую важность он приобретает при создании низкоуровневых стандартов ИБ или конкретных СЗИ организаций. При его использовании выбирается набор семейств для создания гибрида, строятся (или выбираются из библиотеки) модели семейств той или иной степени полноты, далее строится объединенная (гибридная) модель, по которой затем создается текст гибридного стандарта (см. диаграмму Entities generalization – рисунок 5).

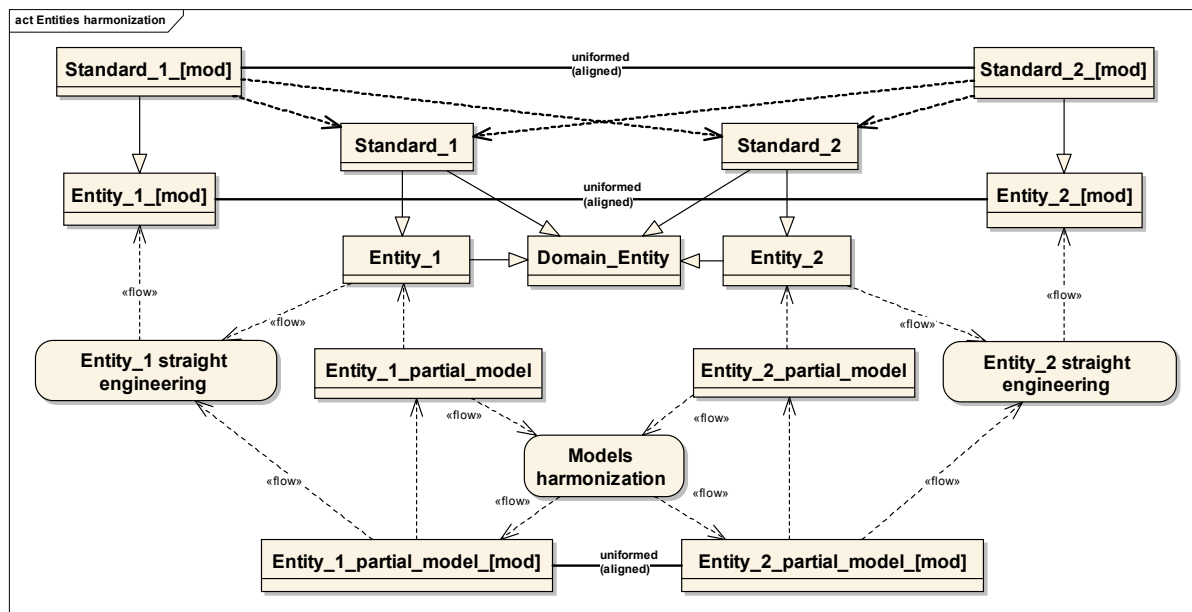


Рис. 4. Диаграмма Entities harmonization

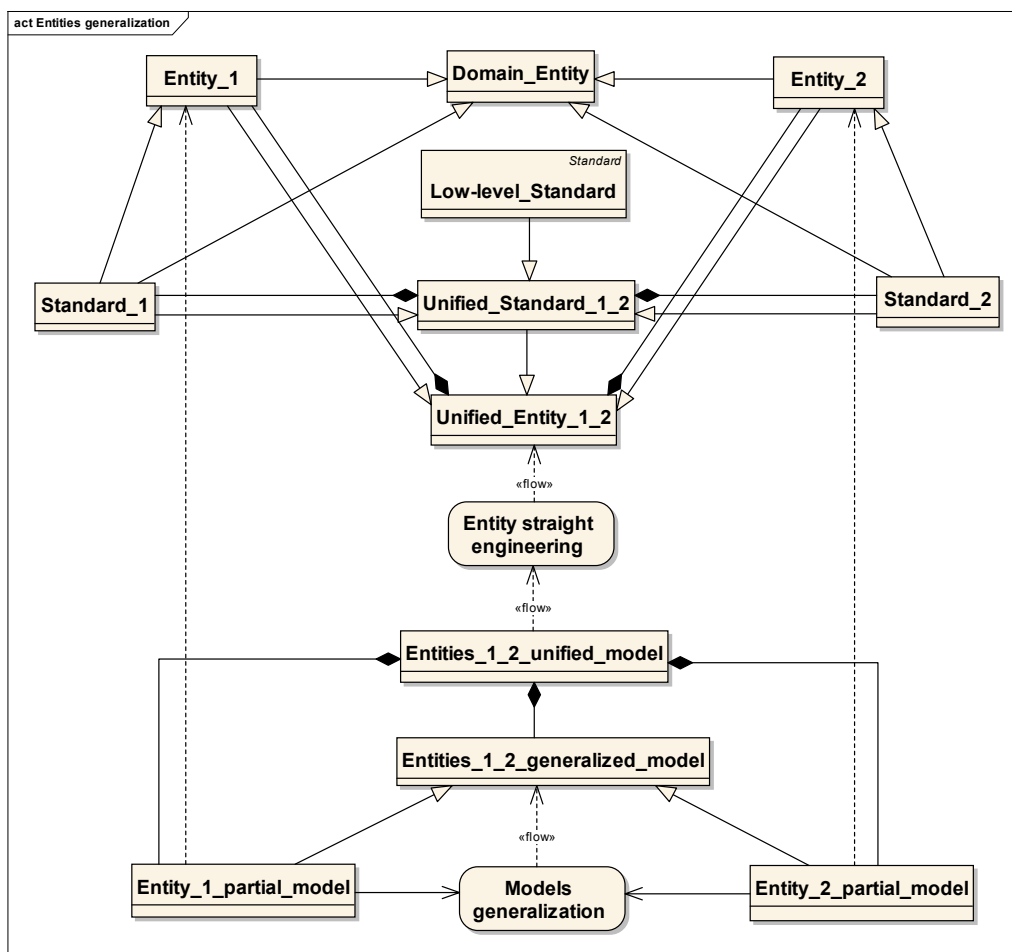


Рис. 5. Диаграмма Entities generalization

Для организаций и фирм, которые в силу специфики своей деятельности сталкиваются с серьезными нормативными рисками (необходимость учитывать требования нескольких семейств стандартов ИБ, как при организации процесса ИБ, так и при построении СЗИ) этот подход является средством их существенного снижения.

Комбинацию двух изложенных подходов (т. е. всех трех основных операций инжиниринга) можно использовать и для согласования семейств стандартов более высокого уровня, например – международных и национальных. Эта задача особенно актуальна в России, которая по различным причинам не принимала участия в разработке ныне действующих международных стандартов.

Сохранение наработанного за десятилетия самостоятельного развития опыта и концепций и включение их в контекст международных методологий на уровне национальных стандартов представляется совершенно необходимым. Указанная проблема активно обсуждается уже несколько лет [3], [4], но практических рекомендаций по ней немного, они носят эпизодический характер и не систематизированы. Представленная в данной и в предыдущих работах методика дает надежную и эффективную базу для решения подобных задач.

СПИСОК ЛИТЕРАТУРЫ

1. Любимов А. В., Суханов А. В. Полуформальные модели стандартов информационной безопасности // Вопросы защиты информации. – 2008. №2 (81). С. 52–57.
2. Черемушкин Д. В. Корректировка стандартов семейства ISO/IEC 27000 на основе объектной модели словаря. // Сборник трудов конференции молодых ученых, Выпуск 6. Информационные технологии / Главный редактор д.т.н., проф. В.Л. Ткалич. СПб. : СПбГУ ИТМО, 2009. – С. 43–48.
3. Кобзарь М., Сидак А. Стандартизация безопасности ИТ // Мир Связи. 2003. – №3. С. 36–40.
4. Калайда И. А., Трубачев А.П. Современное состояние и направления совершенствования нормативной базы в области ИТ-безопасности. // Information Security / Информационная безопасность. – 2004. №3. – С. 20–26.

Нестеров М.Ф., Кондратьев В.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ТАКТИКА НАРАЩИВАНИЯ СИЛ И СРЕДСТВ АУТСОРСИНГА ДЛЯ ПОВЫШЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА КОММЕРЧЕСКОМ ПРЕДПРИЯТИИ**

Система защиты государственной тайны на предприятиях военно-промышленного комплекса может служить источником опыта для коммерческих предприятий, сталкивающихся в настоящее время с тенденцией повышения конкуренции и приобретения ею самой жесткой формы – недобросовестной конкурентной борьбы [1]. Однако современные формы коммерческого сотрудничества, например, аутсорсинг, в настоящее время для и эффективного повышения уровня информационной безопасности на предприятиях практически не используются. Обычно всё сотрудничество сводится к отдельным работам (спецпроверки, специсследования, аттестация и экспертизы), выполняемые на коммерческой основе предприятиями, имеющими соответствующую лицензионную базу на отдельные виды деятельности, связанные с гостайной [2,3]. Тем не менее, при использовании достаточно типовой тактики, можно успешно использовать привлекаемые на основе аутсорсинга (аутстаффинга) ресурсы для защиты, как коммерческой тайны, так и других видов информации ограниченного доступа. Все услуги, включая аутсорсинг, оказываются за соответствующую оплату на основе договоров, заключаемых в простой письменной форме, что накладывает жесткие условия на формулирование предметов договоров, определение сроков оказываемых услуг и форм «оказания» и «принятия» услуг для таких договоров. Исходя из этих факторов, можно сформулировать следующую последовательность задач для аутсорсинга [9]:

- устранение замечаний по результатам проведенного аудита и выполнение плана первоочередных и неотложных мероприятий, согласованного с аудитором. Начало процесса внедрения методик ITIL (IT Infrastructure Library), ISO 17799, CobiT, BS 7799–2, ISO 9001;
- налаживание информационно-аналитической работы на предприятии заказчика;
- проведение внутреннего служебного расследования по некоторым критичным инцидентам.

Выявление инсайдера;

- выход на «проактивные» методы работ для обеспечения экономической и информационной безопасности предприятия.

Решение перечисленных задач, как правило, связано с существенными ограничениями: сохранение существующей структуры и кадрового состава службы безопасности (СБ) заказчика и максимальное выполнение работ её силами, что обусловлено доверием сотрудникам СБ со стороны заказчика и их невысокой «стоимостью» для заказчика в данном случае [7].

Основным побуждающим фактором к заключению таких договоров со стороны заказчика являются либо неожиданные результаты проверок со стороны контролирующих органов, либо выявление проведения успешных информационных атак на информационные ресурсы заказчика. Сам факт начала мероприятий по экстренному повышению уровня информационной безопасности (ИБ) на предприятии заказчика должен скрываться, так как является демаскирующим фактором при защите информации ограниченного доступа. Очевидно, что аутсорсинг для целей ИБ используется как временная экстренная мера. Поэтому все планирование деятельности аутсорсингового предприятия должно быть направлено как на максимально быстрое наращивание сил и средств СБ заказчика, так и на обеспечение достаточного уровня ИБ после окончания договора аутсорсинга с исполнителем.

Все мероприятия по ИБ должны проводиться под контролем и при непосредственном участии СБ заказчика. С учетом этого, на одном из первых этапов сотрудничества должна быть проведена объективная оценка возможностей кадрового и технического обеспечения СБ заказчика и «боевое сколачивание» с силами исполнителя. В некоторых случаях бывает, что источник проблем для заказчика – его собственная СБ. Руководители предприятий всегда могут «восстановить

управляемость» своей собственной СБ, однако в исключительно редких случаях такого не происходит, и прогноз эффективности любого сотрудничества с таким предприятием неблагоприятен. Поэтому оценка прогноза результатов сотрудничества должна проводиться непрерывно для того, чтобы либо своевременно корректировать мероприятия по ИБ, ориентируясь на нужды заказчика, либо своевременно расторгать (завершать) договор аутсорсинга на оказание услуг по ИБ, если заказчик ожидает недостижимых в существующих условиях результатов или в своих действиях выходит за рамки законодательства РФ. Таким образом, можно разделить весь процесс повышения боеготовности СБ заказчика на ряд этапов [5]:

1. Разработка легенды прикрытия проводимых мероприятий, мер по скрытию цели, содержания и методов проводимых работ. Планирование и выполнение мероприятий по дезинформации. Оформление оснований/полномочий для проведения совместных работ на территории заказчика.

2. Создание службы ИБ, её «сколачивание» с СБ как режимной службы, контроль и постоянное повышение её готовности. Этап пассивной работы.

3. Предварительное обследование кадрового состава СБ, информационно-аналитической группы (ИАГ), отдела кадров (ОК), канцелярии/архива/секретариата. Оценка эффективности группового взаимодействия. В случае необходимости переподготовка некоторых специалистов для наращивания кадрового потенциала этих служб.

4. Экспресс-проверка на угрозы ИБ, включая IT-угрозы (для обеспечения ИБ во время проводимых мероприятий). Контроль ключевых процедур и документов. Разработка модели нарушителя и поля угроз.

5. Внедрение системной информационно-аналитической работы в интересах СБ (плановость, законность, целенаправленность). Тактическое и операционное руководство ИАД. Обучение методам и тактике аналитической работы. Нарботка типовых решений, приемов и документов.

6. Разворачивание пункта технического контроля, ситуационного центра, технических средств и баз данных для информационно-аналитической работы. Доработка необходимой нормативно-методической документации. Если необходимо – меры по технической защите объектов информатизации, лицензирование, аудиты и аттестационные испытания («правовые меры по защите информации»).

7. Создание эффективной системы предупреждения и обнаружения «информационных атак» и вторжений (IDS/IPC, HoneyNet, систем логирования, резервных копий), планов восстановления работоспособности и средств противоаварийного управления.

8. Разработка планов, программ и проведение учений, «командно-штабных игр». Разбор результатов, корректировка планов/сроков.

9. Внедрение результатов информационно-аналитической работы в процесс принятия решений на стратегическом уровне.

10. Этап налаживания взаимодействия с СБ предприятий-партнеров, правоохранительными органами, предприятиями – поставщиками баз данных/знаний для ИАГ.

11. Этап разворачивания внутренней структуры уполномоченных СБ (администраторов безопасности), организация структуры доверенных лиц. Проведение полноценных тестов – имитаций несанкционированного доступа и вторжений (PEN-тестов). Анализ осведомленности и контроль лояльности сотрудников, проверка способности хранить доверенную тайну по морально-волевым качествам, возможность выполнять требования, предъявляемым к психофизиологическим качествам сотрудников. Повышение осведомленности сотрудников в вопросах ИБ и передача опыта по противодействию мошенничеству и методам недобросовестной конкуренции.

12. Этап активных мероприятий по противодействию недобросовестной конкуренции, мошенничеству и попыткам получения НСД со стороны нарушителя (организованной группы нарушителей, имеющей соответствующую структуру и управление). Анализ осведомленности сторонних лиц (организаций), оценка их возможностей и прогноз их намерений. «Атакующие» и превентивные мероприятия в рамках правового поля [6].

13. Заключительный этап – окончание сотрудничества заказчика и исполнителя, демонстрация возможностей СБ заказчика как управляемого и боеготового подразделения, переговоры об условиях и сроках продолжения сотрудничества.

В данной статье не рассматривается вопрос о том, как оценивать заказчику способность исполнителя реализовать цели заказчика. Даже на уровне терминологии в области защиты информации в настоящее время нет единства и однозначности. Фактически в Российской Федерации имеется три различных набора традиций, стандартов и подходов к реализации информационной безопасности:

- принятые в деятельности защиты государственной тайны РФ;
- заимствованные из других стран, в которых информационная безопасность «коммерциализировалась» значительно раньше или откуда идет основной поток импорта технических средств и используемых при их эксплуатации методик;

– адаптированные из других видов деятельности, например, из оперативно-розыскной деятельности министерства внутренних дел.

Однако каждый из подходов имеет свой понятийный аппарат и, к сожалению, эти подходы не «совместимы» даже на этом уровне. Таким образом, крайне важным остается вопрос о применимости и соответствии стандартов по защите государственной тайны, стандартам защиты коммерческой тайны и информации ограниченного доступа – как в области применения, так и на уровне понятийного аппарата. В советское время международные стандарты в учреждениях, работающих с гостайной, не применялись, применялись Единая Система Программной Документации (ЕСПД), многочисленные ГОСТы, ОСТы, СТП, ТЮ, другие технические и социотехнические нормы, включая РД Гостехкомиссии 1992–1996 годов. Однако их время объективно «подходит к концу» [4].

Современные стандарты часто еще называют лучшими практиками (best practice). Их количество de facto непрерывно увеличивается, а сами они и Стандарты образуют иерархическую систему. По состоянию на конец 2008 года, такая система насчитывала несколько десятков стандартов, применение которых комплексно обеспечивает безопасность и качество функционирования комплексных систем на всех этапах их жизненного цикла. Высокоуровневые стандарты часто называют процессными, процедурными или тактическими, т.к. они описывают процессы, процедуры. К числу данных стандартов относятся такие, как:

- управление информационными системами – CobiT, BS 15000, Microsoft Operations Framework (MOF) и ITIL (IT Infrastructure Library);
- управление проектами – PRINCE2 и the PMBOK;
- управление безопасностью – PCI DSS, ISO 13335, ISO 13569 (банковские и финансовые услуги), ISO 17799/BS 7799–2 (локализованные), IT Baseline Protection Manual (Германия);
- множество стандартов National Institute of Standards and Technology – NIST Handbook (SP800–12, USA), CobiT Security Baseline, ENV12924 (Медицинская информатика) и the Information Security Forum Standard of Good Practice;
- управление качеством – ISO 9001, EFQM и Baldrige National Q–Plan;
- IT Governance – COBIT, IT Governance Implementation Guide, COSO Internal Control-Integrated Framework и COSO Enterprise Risk Management-Integrated Framework, и недавно разработанный Австралийский стандарт AS 8015–2005 (корпоративное управление информационными и коммуникационными технологиями);
- BCP (планирование непрерывности бизнеса) – British Standards Institution PAS–56;
- аудит ИС – COBIT и ISO 19011 и другие.

Наибольшее и универсальное распространение в России из процессных стандартов получили стандарты ISO 17799, ITIL, COBIT, ISO 9001, BS 7799–2 и их сочетания и «адаптации». Кроме большого числа процессных стандартов, имеется еще большее число эксплуатационных, технических стандартов. Международная Организация по Стандартизации (ISO), Европейский Институт Стандартов Телекоммуникаций и Национальный Институт Стандартов и Технологии (NIST) издали стандарты по таким вопросам, как шифрование (FIPS 197), критерии (технические) оценки безопасности ИТ (ISO 15408), планирование непрерывности бизнеса (FIPS 87), использование паролей (FIPS 112) и др. Стандарты информационной безопасности, качества и управления в обязательном порядке учитываются при проведении сертификации и аудита. Использование стандартов увеличивает ценность продуктов, создаваемых информационными технологиями, но нет таких стандартов, которые охватывали бы все аспекты управления информационной безопасностью.

Принципы эволюционного развития естественных систем, которые необходимо учитывать при наращивании сил при обеспечении ИБ [13]:

1. Принцип поэтапного развития, определяющий, что переход к новым, более совершенным системам нельзя осуществить однократно, он происходит последовательно по этапам.
2. Принцип наследования и изменчивости свойств, означающий, что в своем развитии система, с одной стороны, наследует большую часть свойств систем-прототипов, находящихся на предыдущих этапах развития, а с другой – что всегда существует вероятность изменения, или мутации, того или иного свойства.
3. Принцип адаптивности поведения, определяющий, что система не должна быть пассивной, должна обладать способностью приспосабливаться к изменениям окружающей обстановки.
4. Принцип саморегулируемого управления, означающий, что система должна быть способна распознавать либо классифицировать состояния собственного функционирования и внешней среды и принимать адекватные этим состояниям решения.

Первые два принципа являются принципами *эволюционного построения* технических систем, последние два – принципами *эволюционного функционирования* этих систем.

Анализ особенностей обеспечения ИБ в условиях информационного конфликта как особой формы конфликта с пассивным поведением одной из сторон и использование известных моделей поведения участников конфликтов позволили выдвинуть следующие гипотезы о поведении системы и нарушителя в условиях информационного конфликта:

1. Имеются стратегии концентрации и распределения элементов системы ИБ и существует возможность и необходимость их реализации на основе структурного синтеза и рациональной реконфигурации системы ИБ;

2. Существуют стратегии упреждения и затягивания информационных воздействий нарушителя, а также возможность и необходимость их реализации на основе параметрической адаптации системы ИБ;

3. Существует компромисс между достоверностью обнаружения попыток и фактов НСД и своевременностью реализации стратегии управления системой ИБ и имеется возможность его нахождения на основе реализации саморегулируемого управления функционированием системы ИБ.

Физический смысл выдвинутых утверждений показан на примере влияния стратегий поведения системы ИБ и нарушителя на вероятность обеспечения ИБ, определяемую выражением

$$P_{\text{оз}}(T) = \int_0^T f_{\text{оз}}(\tau) \left[1 - \int_0^{\tau} f_{\text{пз}}(x) dx \right] d\tau, \quad (1)$$

где $f_{\text{оз}}(\tau)$ и $f_{\text{пз}}(x)$ – плотности распределения вероятностей обеспечения и преодоления защиты от НСД за время τ и x соответственно.

На примере нормального закона распределения вероятностей обеспечения и преодоления системы ИБ показано, что изменение параметров распределения приводит к изменению целевого показателя, а варианты максимизации отражают возможность и необходимость структурной оптимизации, параметрической адаптации и саморегуляции системы ИБ.

Концептуальная модель реализации воздействий нарушителя включает: систему классификации информационных атак; модель зависимости «мощности» множества информационных атак от уровня информированности нарушителя; принципы реализации воздействий нарушителя на защищаемые информационные ресурсы; граф состояний и переходов системы воздействий нарушителя (СВН) в процессе информационного конфликта; множество характеристик СВН, потенциально доступных для наблюдения. В целом концептуальная модель отражает основную закономерность процесса воздействий – при начальном защищенном состоянии информационных ресурсов НСД не может быть реализован мгновенно, а является многоэтапным итерационным процессом, при котором последовательное наблюдение во времени значений признаков СВН позволяет идентифицировать и оценить тип воздействия.

Концептуальная модель функционирования системы ИБ в соответствии с эволюционным подходом [6] представлена в виде динамической модели (рисунок 1).



Рис. 1. Динамическое представление процесса функционирования системы ИБ

Формальное представление процесса функционирования системы ИБ задается выражением:

$$\vec{y}(t) = F[\vec{x}^t, \vec{w}_G^t, \vec{u}^t, \vec{q}^t, \vec{r}^t], \quad (2)$$

где

$\vec{x}^t$ – вектор характеристик потока входных воздействий, представляющих собой совокупность запросов пользователей на предоставление информационных ресурсов;

$\vec{w}_G^t$ – вектор характеристик потока воздействий нарушителя, являющихся результатом конфликтного взаимодействия системы ИБ и СВН;

$\vec{u}^t$ – вектор характеристик потока управляющих воздействий, представляющих собой поток команд управления разграничением доступа, поступающий от системы ИБ;

$\vec{q}^t$ – вектор внутренних параметров СЗИ;

$\vec{r}^t$ – вектор характеристик защищаемых ресурсов, отражающий порядок предоставления доступа и требования по их защите от НСД;

$\vec{y}^t$ – вектор контролируемых параметров ИТКС, характеризующий защищенность информации от НСД;

F – функционал, определяющий порядок преобразования перечисленных векторов в $\vec{y}^t$.

Анализ взаимодействия элементов динамической модели позволил сформировать функциональную структуру системы ИБ как эволюционной системы, представленную на рисунке 2.

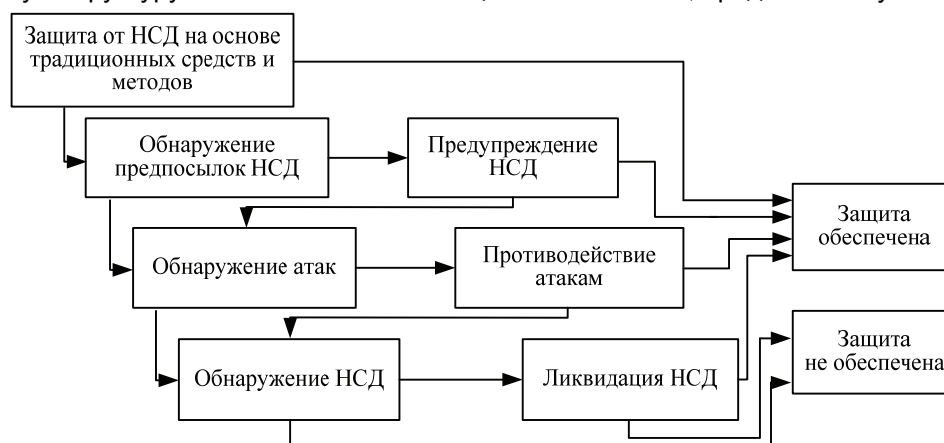


Рис. 2. Функциональная структура традиционной системы ИБ

С учетом условной зависимости результатов реализации каждой функции вероятность обеспечения защиты от НСД будет зависеть от вероятности противодействия на каждом из рубежей и в общем случае будет выше, чем в традиционном случае. Функциональная структура процесса разграничения доступа в свою очередь определяет множество показателей, которые могут быть использованы для оценки эффективности этого процесса. В качестве основного показателя эффективности разграничения доступа предложено использование вероятности обеспечения защиты информации от НСД на заданном интервале функционирования системы ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Вус М.А., Гусев В.С., Рябчук В.Н. Об информационной культуре и информационной безопасности // Материалы V-й Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2007)» – СПб: Изд-во СПИИРАН, 2007. С. 137.
2. Вус М.А., Молдовян А.А., Котенко В.П. Актуальные проблемы информационной реальности // «Информатизация и связь», М. № 1, 2007. С. 4–14.
3. Государственная тайна и ее защита в Российской Федерации: Учебное пособие / Под общ. ред. М.А. Вуса и А.В. Федорова. 3-е изд., испр. и доп. – СПб.: Изд-во Р. Асланова «Юридический центр Пресс», 2007. 47 п.л.
4. Гужва Д.Ю. Разработка функциональной структуры инфотелекоммуникационной системы военного вуза // Материалы НПК «Современные условия вооруженной борьбы и подготовка кадров ВМФ». Санкт-Петербург, 2008. (0,5 п.л.).
5. Дербин Е.А., Крылов Г.О. и др. Информационные операции современности. Учебное пособие / Военная академия Генерального штаба ВС РФ, М. 2004.
6. Концептуальные основы региональной информационной политики. / Под общ. ред. чл.-корр. РАН Р. М. Юсупова. СПб.: Изд-во «Анатолия», 2006. 84 с.
7. Крылов Г.О. и другие. Интегральная оценка методом главных компонент качества подготовки специалистов юридического профиля // Труды профессорско-преподавательского состава Военного Университета. ВУМО, М.: ВУМО, 2000 – 0,6/0,3 п.л.
8. Крылов Г.О., Н.И. Турко. Основы информационной безопасности государства на современном этапе М.: ВАГШ, 2000 – 0,3/0,2 п.л.;

9. Любимов А. В. Структурное моделирование угрозы ИТ в контексте методологии общих критериев // Труды 10-й международной научно-технической конференции «Теория и технология программирования и защиты информации» – СПб: Изд-во СПбГУ ИТМО, 2006. С. 36–39.
10. Молдовян А.А., Долгирев Д.В., Гусев В.С., Вус М.А. Информатика. Введение в информационную безопасность. СПб.: «Юридический Центр Пресс», 2004. 204 с.
11. От культа секретности к информационной культуре (К 15-летию российского закона «О государственной тайне»). Сборник материалов и документов / Составитель М.А. Вус. СПб : СПбОНТЗ. «Полиграф экспресс», 2008. 120 с.
12. Шумский А. А., Шелупанов А. А. Системный анализ в защите информации: Учебное пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности.— М.: Гелиос АРВ, 2005. — 224 с.
13. Юсупов Р.М., Заболотский В.П. Научно-методологические основы информатизации. СПб.: Наука, 2000. 455с.

Никифоров В.В., Шкиртиль В.И.

Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ЗАЩИТА ЦЕЛОСТНОСТИ ДАННЫХ В ПРОГРАММНЫХ ПРИЛОЖЕНИЯХ РЕАЛЬНОГО ВРЕМЕНИ

Программное обеспечение компьютерных комплексов, предназначенных для управления сложным автоматизированным оборудованием, относится к особому классу программных систем – системам реального времени (СРВ). Особые проблемы защиты данных в таких системах возникают ввиду специфики, связанной с условиями их взаимодействия с внешними процессами, в первую очередь с процессами, реализуемыми внешним автоматизированным оборудованием.

Принцип структурного соответствия. Определяющее свойство программных приложений реального времени состоит в том, что они работают «в структуре времени, определяемой ходом внешних процессов». Такое соответствие между ходом исполнения программных компонент СРВ и ходом внешних процессов обусловлено наличием более или менее жесткие временных рамок для информационных обменов с внешними процессами.

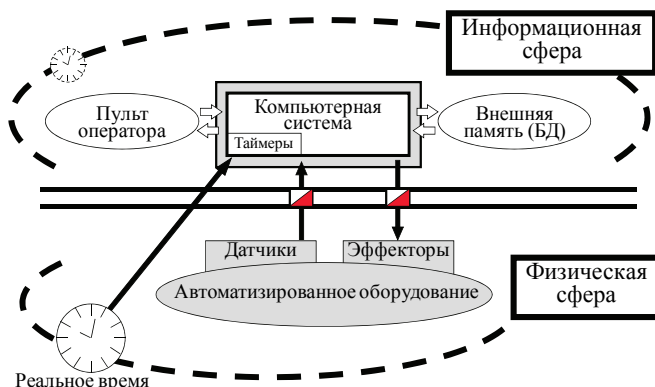


Рис. 1. Взаимосвязи программного приложения с внешними процессами

Внешние объекты СРВ разбиваются на две сферы – информационную и физическую (рисунок 1). Источниками данных, поступающих в СРВ от объектов информационной сферы, являются сугубо информационные процессы. Приемниками данных, поступающих от компьютерной системы (КС) объектам информационной сферы, также являются сугубо информационные процессы. Темпы развития внешних информационных процессов могут накладывать требования реального времени на характер выполнения функций СРВ. Однако, во многих случаях эти темпы могут быть адаптированы к возможностям самой СРВ. Процессы в физической сфере адаптировать сложнее. Объектами физической сферы являются, в конечном счете, силовые процессы, темп развития которых в большинстве случаев предопределен. Потому предопределенными являются и требования реального времени, накладываемые на функции программных приложений, обеспечивающие взаимодействие КС с этими силовыми процессами.

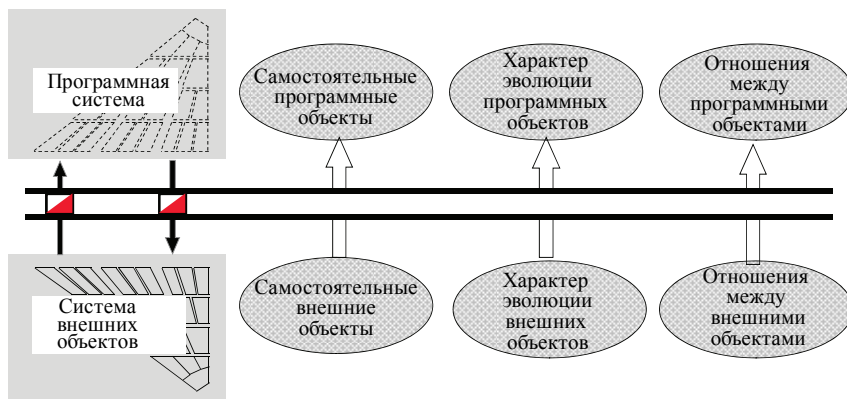


Рис. 2. Основные аспекты принципа структурного соответствия

Требование соответствия между «структурой времени», отражающей ход внешних процессов и «структурой времени» исполнения программных компонент является одним из проявлений общего требования к архитектуре рационально построенной СРВ – требования соблюдения принципа структурного соответствия. В самом общем виде этот принцип формулируется так: для рационально построенной СРВ структура комплекса программных объектов должна представлять собой преломленное отражение структуры множества внешних объектов (рисунок 2) [1].

Для СРВ характерно широкое разнообразие автоматизируемых узлов и агрегатов, разнообразие их взаимосвязей, различий в темпах их функционирования. В связи с этим программные приложения реального времени строят в виде множества относительно самостоятельных, но взаимосвязанных программных компонент. Такие компоненты программных приложений реального времени называют задачами.

Задачи и задания. Основными объектами, рассматриваемыми при анализе структурной организации программных приложений реального времени и анализе хода функционирования таких приложений, являются задачи и задания.

Прикладная задача τ_i представляет собой внутренне замкнутую (по передачам управления) компоненту программного приложения. Для каждой задачи определяется ее корневая программа — последовательный алгоритм исполнения этой задачи. Алгоритм, реализуемый корневой программой задачи, строится с использованием тех же средств и принципов, которые используются при построении последовательных вычислительных процедур, то есть, состоит из последовательности операторов с ветвлениями и циклами, с вызовами процедур, допускающих несколько уровней вложенности. Определяющее различие между корневой программой задачи и вычислительной процедурой состоит в способах активизации и завершения исполнения.

Вычислительные процедуры активизируются операторами вызова из других программ. В этом смысле вход в вычислительную процедуру открыт для активизации операторами вызова, являющимися разновидностями операторов передачи управления. Оператор завершения вычислительной процедуры возвращает управление в точку вызова, то есть, он тоже является разновидностью оператора передачи управления.

Принципиально отличным способом осуществляются действия по активизации и завершению исполнения корневой процедуры задачи (для удобства будем называть эти действия активизацией и завершением исполнения самой задачи). Исполнение задачи активизируется либо специальными аппаратными средствами по сигналам от периферийных блоков КС (механизмами системы прерываний), либо механизмами операционной системы вследствие регистрации соответствующего системного события, предписывающего активизацию исполнения задачи. В первом случае задача относится к разряду аппаратно контролируемых задач (к разряду обработчиков прерываний). Во втором случае задача относится к разряду программно контролируемых задач (контролируется операционной системой).

Задачи обеих разновидностей (как аппаратно контролируемые, так и программно контролируемые) являются статическими программными объектами (они неизменны в ходе функционирования системы). Под заданием $\tau_i^{(j)}$ понимается динамический объект — ход однократного исполнения задачи τ_i . Объект $\tau_i^{(j)}$ порождается в момент очередной, j -й активизации задачи τ_i . В момент $t_{\text{arr}}(\tau_i^{(j)})$ порождения задания $\tau_i^{(j)}$ начинается интервал его существования. В рамках интервала существования $\tau_i^{(j)}$ осуществляется исполнение корневой программы τ_i и всех прямо или косвенно вызываемых из нее процедур. Интервал существования задания $\tau_i^{(j)}$ завершается в момент $t_{\text{end}}(\tau_i^{(j)})$ выхода из корневой программы τ_i . На частоту порождения однотипных заданий накладывается ограничение $t_{\text{arr}}(\tau_i^{(j+1)}) - t_{\text{arr}}(\tau_i^{(j)}) \geq T_i$. Системные события «порождение $\tau_i^{(j)}$ » и «завершение $\tau_i^{(j)}$ » размещаются на краях интервала существования задания $\tau_i^{(j)}$, их уместно называть граничными системными событиями интервала существования задания $\tau_i^{(j)}$.

Длина $r_i^{(j)} = t_{\text{end}}(\tau_i^{(j)}) - t_{\text{arr}}(\tau_i^{(j)})$ интервала существования $\tau_i^{(j)}$ называется временем отклика задания. В рамках интервала своего существования задание является действующим. Временем отклика R_i задачи τ_i называется максимально возможное время отклика для однотипных заданий

$$R_i = \max \{j \geq 1 \mid t_{\text{end}}(\tau_i^{(j)}) - t_{\text{arr}}(\tau_i^{(j)})\}.$$

В конкретный момент времени задание считается активным, если оно либо готово к использованию ресурса процессора и ждет предоставления этого ресурса, либо уже исполняется процессором (является текущим заданием).

Задание перестает быть активным, если оно переходит в состояние *ожидания* какого-либо системного события, генерируемого другими действующими заданиями. Переходы в такие состояния ожидания характерны для тесно взаимодействующих заданий. Задачи, при исполнении которых попадание в такие состояния ожидания невозможно, называют *независимыми* задачами.

Отношение между задачей τ_i и заданием $\tau_i^{(j)}$ аналогично отношению между типом переменной (например, типом `int`) и конкретной переменной этого типа (например, переменной `int x`), между классом объектов и экземплярами этого класса. То есть, различные задания, соответствующие одной и той же задаче уместно называть однотипными заданиями, два задания, соответствующие различным задачам – разнотипными заданиями.

Источники нарушения целостности глобальных данных. В момент порождения задания $\tau_i^{(j)}$ выделяется область памяти, предназначенная для хранения данных, формируемых и используемых только в рамках $\tau_i^{(j)}$ – эти данные составляют локальный контекст $\tau_i^{(j)}$. Каждое задание имеет свой локальный контекст, недоступный другим заданиям. Данные, доступные различным заданиям, составляют глобальный контекст системы. Коды задач, составляющих программное приложение, содержат операторы доступа как к локальной, так и к глобальной памяти (к локальному и к глобальному контекстам). Путем построения операторов доступа к элементам глобального контекста формируются межзадачные связи. Взаимодействие заданий обеспечивается за счет использования этих межзадачных связей.

Если два задания с пересекающимися интервалами существования имеют доступ к одним и тем же элементам глобального контекста, то возникает проблема поддержания целостности этих элементов глобального контекста. Существуют две разновидности потенциальных источников нарушения целостности глобальных данных: а) интерференция однотипных заданий и б) интерференция разнотипных заданий. Вариант порядка возникновения системных событий, при котором возможны обе разновидности нарушения целостности, приведен на рисунке 3, где в моменты времени t_1, t_2, t_4, t_5 порождаются, соответственно, задания $\tau_1^{(1)}, \tau_2^{(1)}, \tau_1^{(2)}, \tau_2^{(2)}$, в моменты времени t_3, t_6 завершаются задания $\tau_2^{(1)}, \tau_1^{(1)}$.



Рис. 3. Пересечения интервалов существования однотипных и разнотипных заданий.

Потенциальная возможность интерференции однотипных заданий возникает в том случае, если $t_{\text{end}}(\tau_i^{(j)}) > t_{\text{arr}}(\tau_i^{(j+1)})$, т.е., задание $\tau_i^{(j+1)}$ порождается раньше, чем завершается задание $\tau_i^{(j)}$. На рисунке 3 однотипные задания $\tau_1^{(1)}$ и $\tau_1^{(2)}$ сосуществуют в интервале (t_4, t_6) . Один из подходов, исключающих возможность источников нарушения целостности глобальных данных типа а) состоит в обеспечении таких условий функционирования СРВ, при которых интервалы существования однотипных заданий гарантированно не пересекаются, то есть, для всех задач выполняется неравенство $T_i \geq R_i$. Чтобы обеспечить выполнение этих условий, необходимо располагать соответствующими методами анализа возможных вариантов порядка следования системных событий. В случае системы независимых задач со статическими приоритетами такой метод состоит в решении рекуррентного уравнения для определения значения R_i времени отклика каждой из задач [2]:

$$R_i = C_i + \sum_{\text{prio}(\tau_k) \geq \text{prio}(\tau_i)} \lceil R_i / T_k \rceil, \quad (1)$$

где $\lceil x \rceil$ – целое число, ближайшее сверху к x ;

$\text{prio}(\tau_i)$ – приоритет задачи τ_i ;

C_i – максимальный объем процессорного времени, требующегося для выполнения задачи τ_i .

Защита критических интервалов кода задач. Критическим интервалом называют такой фрагмент кода задачи, который содержит группу связанных операций над конкретным глобальным информационным ресурсом (например, структурой данных в глобальной памяти). Задача может содержать несколько критических интервалов – как однотипных (реализующих доступ к одному и тому же ресурсу), так и разнотипных (реализующих доступ к различным ресурсам). Два разнотипных

критических интервала одной и той же задачи могут быть либо независимыми (не пересекающимися) либо вложенными (один интервал полностью размещен внутри другого), либо сцепленными (см. рисунок 4).

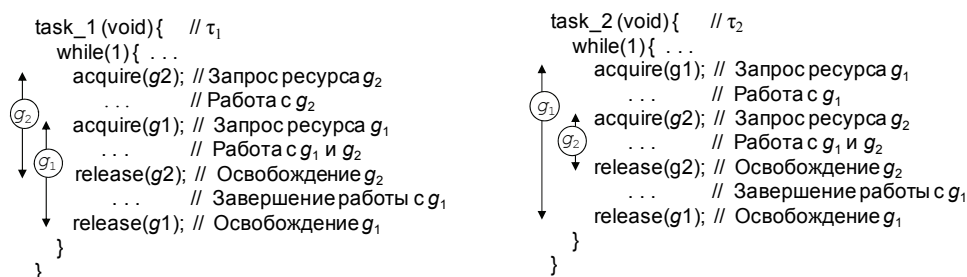


Рис. 4. Взаимосвязанные задачи со сцепленными и вложенными критическими интервалами

С целью защиты целостности глобальных данных, модифицируемых в рамках критического интервала для каждого ресурса g , формируется специальный синхронизирующий элемент мьютекс, в котором фиксируются системные события по запросу, предоставлению, освобождению ресурса g действующими заданиями.

Механизм контроля доступа к критическим интервалам предполагает, что в начале критического интервала выполняется операция запрос ресурса, в конце критического интервала выполняется операция освобождение ресурса.

Если в момент запроса ресурса g этот ресурс свободен, то он предоставляется запросившему его заданию. Мьютекс, соответствующий ресурсу g , переводится в состояние «занят». Задание, которому предоставлен ресурс, приступает к исполнению операций критического интервала по этому ресурсу. На выходе из критического интервала выполняется операция освобождения ресурса, мьютекс переводится в состояние «свободен». Если в момент запроса ресурса g запрашиваемый ресурс занят, то запросившее ресурс задание, поступает в очередь заданий, ожидающих предоставления ресурса g .

В системах с мьютексами наряду с граничными системными событиями происходят внутренние системные события заданий – события, возникающие при исполнении операций «запрос ресурса», «освобождение ресурса». Внутренние системные события происходят также при использовании других синхронизирующих механизмов (семафоры, очереди сообщений и др.).

При наличии в кодах задач операторов, исполнение которых генерирует внутренние системные события заданий, становится актуальным рассмотрение порядка следования таких операторов в теле задачи. Каждая из задач на рисунке 4 имеет критический интервал по ресурсу g_1 и критический интервал по ресурсу g_2 . Отметим топологические различия в размещении критических интервалов в задачах τ_1 и τ_2 . В задаче τ_1 критические интервалы по ресурсам g_1 и g_2 сцеплены, в задаче τ_2 критический интервал по ресурсу g_1 вложен в критический интервал по ресурсу g_2 . Анализ показывает, что при наличии вложенных или сцепленных интервалов по совместно используемым ресурсам может возникнуть взаимное блокирование действующих заданий.

На рисунке 5 приведен фрагмент модели программного приложения реального времени, содержащий две задачи τ_1 и τ_2 , а также два разделяемых ресурса g_1 и g_2 . Для представления схемы взаимодействия используется графический формализм маршрутной сети [3]. Каждая задача изображается в виде маршрута (на рисунке 5 – жирные овальные линии), разделенного на фрагменты переходами (переходы соответствуют операторам доступа к разделяемым ресурсам). Движущиеся по маршрутам треугольники (курсоры) соответствуют действующим заданиям. Размещение треугольника на своем маршруте указывает тот фрагмент задачи, который в рассматриваемый момент времени является для задания текущим. Разделяемые ресурсы представляются позициями, аналогичными позициям сетей Петри [4]. Отсутствие метки в позиции означает, что в рассматриваемый момент времени ресурс занят, наличие метки в позиции означает, что ресурс свободен.

Код каждой из задач τ_1 и τ_2 на рисунке 5 состоит из четырех фрагментов. Для задачи τ_1 в рамках ее фрагмента f_1 нет операторов доступа к разделяемым системным ресурсам; в рамках фрагментов f_2 и f_3 содержатся операторы доступа к ресурсу g_2 ; в рамках фрагментов f_3 и f_4 содержатся операторы доступа к ресурсу g_1 . Код задачи τ_2 имеет аналогичную топологию.

Под системным состоянием задания понимается текущее отношение задания к системным ресурсам. Согласно такому определению пространство системных состояний заданий типа τ_1 состоит из четырех элементов, каждому из четырех фрагментов f_1, f_2, f_3, f_4 кода задачи τ_1 соответствует отдельный элемент пространства системных состояний задания.

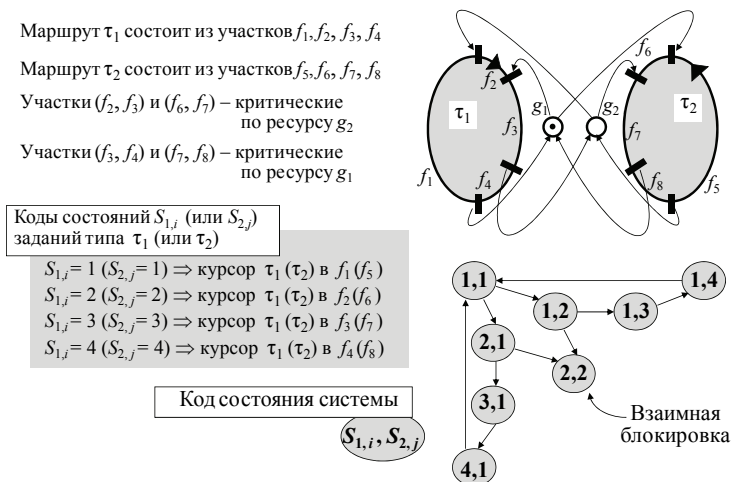


Рис. 5. Пространство состояний взаимодействующих заданий

Пространством состояний системы является произведение пространств системных состояний действующих заданий. Для двух заданий на рисунке 5 все пространство состояний системы содержит 16 элементов. В правом нижнем углу на рисунке 5 приведены 8 достижимых элементов пространства системных состояний двухзадачного комплекса. Механизм охраны одновременного доступа заданий типа τ_1 и τ_2 к критическим интервалам предотвращает достижимость элементов [3,2], [4,2], [4,3] (охрана g_1), элементов [2,3], [2,4], [3,4] (охрана g_2), и элемента [3,3] (охрана g_1 и g_2). Элемент [4,4] также недостижим, но не потому, что соответствует однотипным критическим интервалам, а потому, что попасть в него можно было только двумя способами – либо через запрещенный элемент [4,3], либо через запрещенный элемент [3,4].

Система может неопределенно долго работать в рамках циклов [1,1]–[2,1]–[3,1]–[4,1] и [1,1]–[1,2]–[1,3]–[1,4]. Но при попадании в состояние [2,2] происходит взаимное блокирование действующих заданий типа τ_1 и τ_2 : задание типа τ_1 ждет, когда освободится ресурс g_1 , а им владеет задание типа τ_2 , которое в свою очередь ждет, когда освободится ресурс g_2 , занятый заданием типа τ_1 .

Из приведенного примера видно следующее:

1. Оснащение системы взаимосвязанных задач механизмами защиты от одновременного доступа к однотипным критическим интервалам еще не обеспечивает корректной работы системы – возникает возможность взаимного блокирования заданий.

2. Необходимость ожидать момента освобождения занятого ресурса приводит к усложнению проблемы оценки значения R_i времени отклика каждой из задач – формула (1) в такой ситуации становится недействительной.

3. Для проверки корректности программных приложений реального времени с взаимодействующими задачами необходимо располагать не только данными о внешних параметрах задач (таких, как частота активизации, требуемый объем процессорного времени, приоритеты), но и данные о внутренней структуре задач (такие, как размещение и длина критических интервалов по доступу к разделяемым ресурсам).

Протоколы доступа к ресурсам. Эффективным подходом к решению проблемы взаимного блокирования является использование специальных протоколов доступа к критическим интервалам, охраняемым мьютексами, в частности, протоколом пороговых приоритетов (ППП) [5]. Согласно ППП с каждым ресурсом (другими словами, с каждым мьютексом) связывается параметр, называемый пороговым приоритетом ресурса. Пороговый приоритет ресурса (мьютекса) равен высшему уровню статического приоритета задачи, которая может занять ресурс. Заданию разрешается занять ресурс в том случае, когда уровень его статического приоритета выше, чем пороговые приоритеты всех ресурсов, уже занятых в настоящее время другими заданиями.

Таким образом, задание, занявшее ресурс, может блокировать исполнение более приоритетных заданий. В этих условиях для оценки значения R_i времени отклика задачи необходимо

учесть фактор блокирования – максимально возможную продолжительность B_i ожидания заданием типа τ_i момента освобождения ресурса, занятого менее приоритетным заданием:

$$R_i = C_i + B_i + \sum_{\text{prio}(\tau_k) \geq \text{prio}(\tau_i)} \lceil R_i / T_k \rceil \quad (2)$$

Для построения метода оценки фактора блокирования B_i ключевую роль играет утверждение: составное блокирование невозможно. Это означает, что каждое задание типа τ_i может быть заблокировано лишь единожды одним из менее приоритетных действующих заданий. Следовательно, для задачи τ_i нужно найти наихудший вариант блокирования – тот вариант, который приводит к максимально возможному времени ожидания освобождения требуемого ресурса. Рассмотрим шаги по поиску наихудшего варианта для известного примера с пятью обедающими философами [4].

Первым шагом поиска наихудшего варианта блокирования является построение таблицы доступа задач к системным ресурсам. В случае примера с пятью философами эта таблица имеет следующий вид:

Таблица 1

Доступ к ресурсам для примера с пятью философами

Задачи	Ресурсы				
	g_1	g_2	g_3	g_4	g_5
τ_1	$C_1(g_1)$	$C_1(g_2)$	0	0	0
τ_2	0	$C_2(g_2)$	$C_2(g_3)$	0	0
τ_3	0	0	$C_3(g_3)$	$C_3(g_4)$	0
τ_4	0	0	0	$C_4(g_4)$	$C_4(g_5)$
τ_5	$C_5(g_1)$	0	0	0	$C_5(g_5)$

Задачи τ_i в таблице доступа к ресурсам упорядочены по значениям приоритетов: наиболее приоритетной является задача τ_1 , наименее приоритетной – задача τ_5 . Значение $C_i(g_j)$ указывает объем процессорного времени, требуемого для самого длинного критического интервала задачи τ_i по доступу к ресурсу g_j .

Следующие шаги — отбор актуальных ресурсов и определение вариантов блокирования выполняются отдельно для каждой из задач. Таблица актуальных ресурсов получается из таблицы доступа к ресурсам исключением неактуальных для τ_i столбцов. Неактуальным для τ_i столбцом является каждый k -й столбец, в котором $C_j(g_k) = 0$ при любом $j \leq i$. Для задачи τ_3 из таблицы 1 неактуальным является 5-й столбец.

Таблица вариантов блокирования доступа задачи τ_i получается из таблицы ее актуальных ресурсов удалением i -й строки и всех строк выше нее. Для задачи τ_3 из таблицы 1 варианты блокирования содержатся в клетках, обведенных жирным прямоугольником. Таким образом, для приведенного в таблице 1 примера фактор блокирования для задачи τ_3 определяется равенством

$$B_3 = \max \{C_4(g_4), C_5(g_1)\}. \quad (3)$$

Задачи со сцепленными критическими интервалами. В примере с пятью философами структура каждой задачи аналогична структуре задач на рисунке 5: каждая из пяти задач содержит по два сцепленных критических интервала, причем эти критические интервалы сцеплены в связку.

При оценке фактора блокирования для задач τ_1 , τ_2 , τ_3 такая топологическая особенность блокирующих задач не влияет на корректность изложенного способа определения величины фактора блокирования: формула (3) для оценки значения B_i дает верный результат. Действительно, для задач τ_1 , τ_2 , τ_3 ненулевые значения $C_i(g_i)$ содержатся в разных строках таблицы вариантов блокирования (сцепленные с актуальными критическими интервалами блокирующих задач, остаются за рамками таблицы актуальных ресурсов). Для задачи τ_4 ситуация принципиально иная: оба критических интервала задачи τ_5 по ресурсам g_1 и g_5 актуальны для задачи τ_4 . К тому же, эти

критические интервалы в задаче τ_5 являются сцепленными. А это означает, что в результате запроса ресурса g_5 заданию $\tau_4^{(j)}$, возможно, придется ожидать, пока задание $\tau_4^{(j)}$ пройдет всю связку двух сцепленных интервалов. Это означает, что для задачи τ_4 расчет фактора блокирования по формуле, аналогичной (3), даст заниженный результат. В действительности $B_4 = C_5(g_5, g_1)$, где $C_5(g_5, g_1)$ – длина связки критических интервалов задачи τ_5 по ресурсам g_1 и g_5 .

Заключение. В системах с независимыми задачами нарушение целостности глобальных данных возможно при интерференции однотипных заданий с пересекающимися интервалами существования. Для исключения такой интерференции программные приложения реального времени строят таким образом, чтобы время отклика задач не превосходило величины периода их активизации. Величина времени отклика определяется решением уравнения (1).

В системах со взаимозависимыми задачами во избежание интерференции разнотипных заданий, разделяющих общие ресурсы, контроль доступа к критическим интервалам осуществляется путем реализации протокола пороговых приоритетов. При этом подход к предотвращению интерференции однотипных заданий, основанный на оценке времени отклика задач, дополняется оценкой фактора блокирования доступа к критическим интервалам из-за захвата разделяемых ресурсов низкоприоритетными заданиями. Как показано в представленной работе, корректная оценка величины фактора блокирования может потребовать учета внутренней структуры взаимосвязанных прикладных задач, учета структуры связок критических интервалов по доступу к разделяемым ресурсам.

СПИСОК ЛИТЕРАТУРЫ

1. Давиденко К.Я. Технология программирования АСУТП. Проектирование систем реального времени, параллельных и распределенных приложений. М.: Энергоатомиздат. 1985. 183 с.
2. Гома Х. UML. Проектирование систем реального времени, параллельных и распределенных приложений. М.: ДМК Пресс. 2002. 739 с.
3. Никифоров В.В. Представление структуры сигнальных связей алгоритмических процессов в гибких производственных системах. // Интегрированные производственные комплексы Л.: Машиностроение. 1987. С. 42–46.
4. Питерсон Дж. Теория сетей Петри и моделирование систем. М.: Мир, 1984. 263 с.
5. Данилов М.В. Методы планирования выполнения задач в системах реального времени. // Программные продукты и системы. 2001. №4. С.28–35.

Орлов К.М.

Россия, Санкт-Петербург, 4 филиал ВУНЦ ВМФ «Военно-морская академия» ФОРМИРОВАНИЕ СИСТЕМЫ ОЦЕНКИ КАЧЕСТВА ВИЗУАЛИЗАЦИИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Одну из важнейших задач в современных автоматизированных системах управления, в том числе в защищенном исполнении (АСЗИ), выполняют подсистемы визуализации и обработки информации (ПВОИ). Они обеспечивают эффективность интерфейса «человек-машина», возможность принимать своевременные управленческие решения при выполнении поставленных задач в заданные сроки. По существу ПВОИ взаимодействует с каждым элементом АСЗИ и на каждом этапе жизненного цикла – от поступления информации до выдачи результатов решения, как представлено на рисунке 1.



Рис. 1. Роль и место ПВОИ в автоматизированных системах управления

Задача построения эффективных систем управления различного назначения, максимально реализующих возможности современных информационных технологий, является традиционной и всегда актуальной. Пожалуй, в первую очередь это относится к ПВОИ, обеспечивающей информационную, аналитическую и интеллектуальную поддержку действий оператора в процессе оценки обстановки (наиболее «интеллектуально ёмкого» и сложного этапа аналитического обеспечения систем управления), а также в процессах выработки вариантов действий и непосредственного принятия решений.

В современных условиях, когда роль информации становится все более важной, вполне естественен тот факт, что изображение превращается в её преобладающий носитель. Вместе с тем, вопросы защиты визуальной информации, как наиболее системной и значимой (информативной, ценной), отдалённо практически не рассматриваются.

В общем случае, в современных ПВОИ (как, например, показано на рисунке 2) многомерные данные представляются в виде объединённых схем и таблиц. Это позволяет при визуальном анализе данных оператором сформировать адекватный образ (информационную модель) внешней обстановки (ситуации).

Основу подобного представления информации составляет обобщённая визуализация внешней и внутренней обстановки на соответствующей картооснове в двухмерном представлении данных. При этом преследуется, как правило, цель создания максимально полного отображения имеемых данных, которые могут повлиять на принимаемое оператором решение.

Более актуальным в этой связи представляется отображать данные на основе так называемого многомерного изображения, как показано на рисунке 3, т.е. одновременно в «нескольких ракурсах» («срезах»):

- традиционный – вид сверху (планшетный вариант, приведён в левом нижнем углу рисунка);
- в разрезе – по вертикальной плоскости сбоку и фронтально (правый верхний угол рисунка);
- объёмный – вид типа «3D-графического отображения», представляющего собой «объединение» (безызыточное, объёмное) предыдущих видов (правый нижний угол рисунка).

Приведённый вариант реализует так называемый метод многомерной комплексной визуализации и обработки информации (МКВОИ). Среди его особенностей – использование 3D-графического отображения обстановки (интегрированной информации), использование цветового канала отображения данных, например, для отображения прогнозных оценок по условиям функционирования, дальностям взаимного обнаружения целей, использование специальных символьных форм и другие.

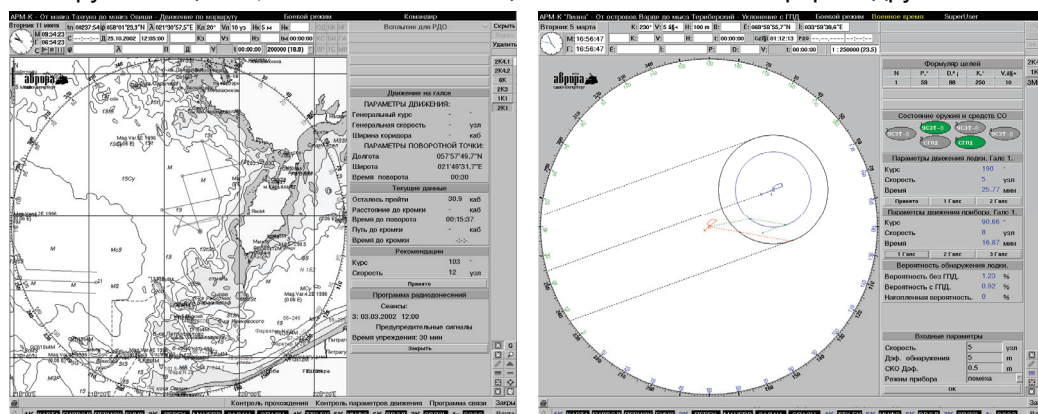


Рис. 2. Типовые варианты отображения информации в АСЗИ

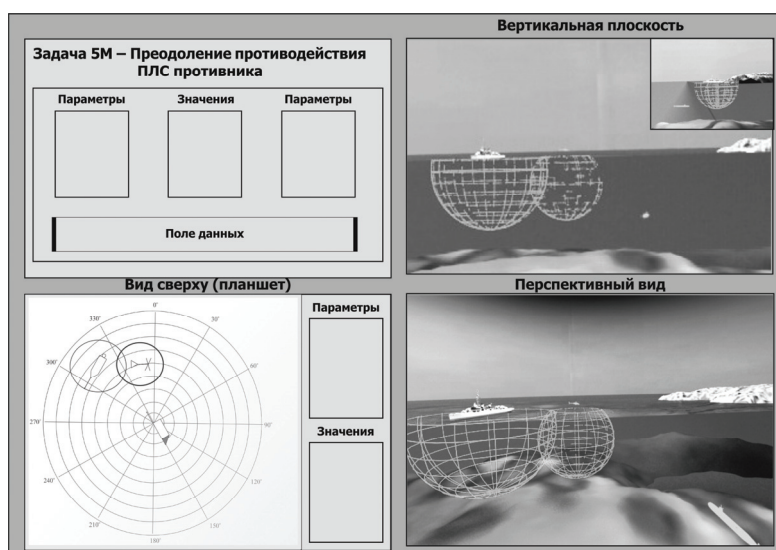


Рис. 3. Вариант представления информации по методу МКВОИ

Возможности автоматизированной комплексной визуальной обработки и многомерного отображения информации, можно утверждать, являются одним из резервов повышения эффективности АСЗИ за счёт, с одной стороны, минимизации избыточности и повышения тем самым ценности отображаемых данных, а, с другой стороны, за счёт «ускоренного» формирования информационной модели обстановки (см. рисунке 1) с учётом «объёмного видения» оператора.

В этих условиях актуальной исследовательской задачей является обоснование путей совершенствования структур и алгоритмов функционирования ПВОИ АСЗИ, для чего, в первую очередь, необходимо сформировать систему показателей оценки качества и эффективности процессов визуализации информации в АСЗИ.

Анализ ряда источников, включая [1–8], показал, что описание и сравнение различных методов, структур и алгоритмов ПВОИ АСЗИ можно встретить далеко не часто. Причина этому – отсутствие устоявшейся и «убедительной» системы критериев оценивания ПВОИ АСЗИ.

Как правило, под эффективностью подсистемы визуализации и обработки информации АСЗИ понимают главную, основную характеристику качества, полезности системы (ПВОИ). Традиционно формулировка показателей эффективности АСЗИ, в том числе её ПВОИ, является достаточно сложной теоретической и практической задачей, связанной с выбором и формулировкой одного, единственного, основного показателя эффективности ПВОИ АСЗИ.

Это обстоятельство приводит к тому, что на практике широко используют не один обобщенный, а множество частных показателей эффективности. С одной стороны, использование совокупности показателей эффективности с достаточной для практических задач проектирования полнотой и точностью должно позволить произвести обобщённую оценку эффективности АСЗИ.

С другой стороны, задача синтеза наиболее предпочтительных вариантов построения ПВОИ (выбора архитектуры, состава, параметров), а тем более оптимизации ПВОИ АСЗИ не только, как правило, не решаются, но и даже по существу не ставятся.

Как следствие, имеет место практика, когда на мониторе оператора «выгружается» столько информации, что её «обычный человек» даже теоретически обработать не в состоянии. Например:

1. В БИУС «Требование-М» [8] число пультов командного состава корабля – 10 (в БИУС «Сигма-Э» их 25) при числе одновременно обрабатываемых целей – 256, числе решаемых задач – 112. Проблема своевременности, достоверности, устойчивости, скрытности (включая вопросы защищённости данных) и непрерывности управления с максимизацией ценности визуализируемых данных, тем самым, очевидна.

2. Центральный пост охранного видеонаблюдения ОАО «Кировский завод». Число пультов наблюдения (операторов) – 8, на каждом мультиэкране – 32 видеосцены. Режим использования – автоматизированный (с использованием детекторов активности видеосцен), непрерывно, круглосуточно. И это при эргономических требованиях непрерывности работы операторов автоматизированных рабочих мест (АРМ) – не более (4...6) часов. Вместе с тем, реальное число используемых операторов – не превышает 4, чего явно не достаточно.

3. Аналогичная, но более напряжённая ситуация с системой видеонаблюдения имеет место на дорогах г. Москва (система действует с 2003 г.). Операторов – 48. Известные видеодетекторы (детекторы активности) алгоритмически далеко ещё не совершенны. Наличие и актуальность проблем и задач МКВОИ – налицо!

Известен ряд общих требований к частным показателям эффективности сложных систем типа ПВОИ АСЗИ, где показатель эффективности должен быть «измеряем», т.е. должна существовать возможность установления зависимости показателя от параметров подсистемы.

Наконец, система показателей эффективности ПВОИ АСЗИ должна отражать, с одной стороны, эффективность системы более высокого уровня, а с другой – способность ПВОИ АСЗИ осуществлять решение задач по обработке информации с требуемым качеством в заданном диапазоне условий применения рассматриваемой подсистемы.

Таким образом, анализ подсистем и средств визуализации информации [1–8] позволяет сделать следующие выводы:

1. Вопросы оценки и обоснования требований к ПВОИ, как функциональной подсистемы АСЗИ, до настоящего времени практически не рассматривались с позиций информационной эффективности. Вместе с тем, понятно, что эти вопросы всегда были в зоне внимания разработчиков.

2. Наиболее разработанными являются методы эргономической оценки алфавитно-цифровых дисплеев и информационных табло. На базе этих методов выполнены работы Варе В.И., Венды В.Ф., Зинченко В.П. и Мунипова В.М., Смолярова А.М., Костюка В.П. и Ходакова В.Е. и многих других. Однако, они ориентированы на исследование функционирования систем отображения информации в системах управления технологическими процессами, применительно к автоматизированному управлению и не могут без доработок использоваться при оценке эффективности ПВОИ АСЗИ.

3. Известные методы и методики оценки комплексов и отдельных систем отображения информации (методы оценки информационной емкости, качества отображения информации, точности ПВОИ, технической надежности, производительности ПВОИ, гибкости ПВОИ, технологичности, стоимости, эксплуатационных возможностей и др.), как правило, не связаны между

собой единым методическим аппаратом, не учитывают специфики и не позволяют производить комплексную оценку ПВОИ.

4. Качество функционирования ПВОИ при этом оценивается, как правило, по частным критериям и техническим показателям системы, характеризующим сами устройства отображения (мониторы, их визуально-оптические параметры), а также сами вычислительные средства и аппаратуру подсистемы связи АСЗИ.

5. Развитие методов оценивания качества и эффективности сложных организационно-технических комплексов в АСЗИ по-новому ставит задачу комплексного квалиметрического (количественного измерения качества) анализа возможностей АСЗИ.

6. Ещё более актуальна оценка потенциально-достижимых и ожидаемых (при эксплуатации – реальных) результатов целенаправленного использования каждой подсистемы и АСЗИ в целом с учётом степени соответствия этих результатов главным целям (по предназначению) функционирования АС.

7. Наконец, техническое регулирование требует выполнения оценок валидации на полном множестве входных ситуаций и состояний системы, включая типовые и нетиповые (нештатные) ситуации, учёта воздействия множества внешних и внутренних факторов (инсайдеров и т.п.).

Для комплексной оценки качества визуализации и обработки информации в АСЗИ с учётом вопросов восприятия оператором разнородной информации, специфики взаимодействия оператора и АСЗИ предлагается использовать систему критериев и показателей качества ПВОИ АСЗИ, представленную на рисунке 4.

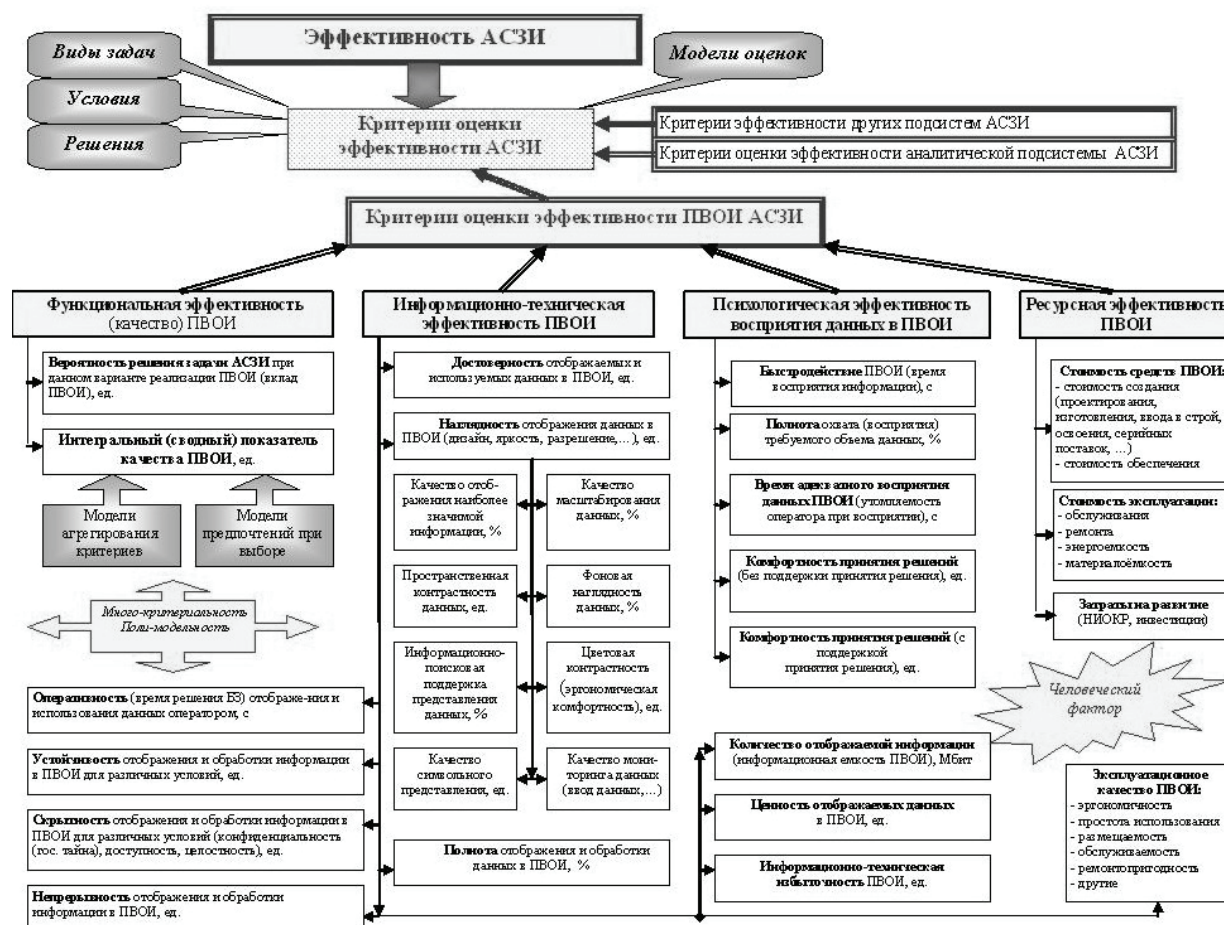


Рис. 4. Система критериев оценки качества ПВОИ АСЗИ

С учётом ряда выполненных оценок, по мнению автора, предлагаемая система критериев позволяет перейти к квалиметрическому анализу действующих и разрабатываемых АСЗИ, обоснованию требований и оптимизации параметров перспективных средств и систем визуализации АСЗИ с учётом специфики информационных преобразований, психо-физиологических особенностей операторов и даже ряда важных аспектов человеческого фактора.

Предлагаемый подход позволяет количественно обосновывать требования к качеству ПВОИ АСЗИ и, следовательно, аргументировано решать многовариантные задачи синтеза и оптимизации проектных решений сложных комплексов и систем при возрастании объёма собираемых, распределяемых, обрабатываемых и отображаемых данных.

Восприятие разнородной информации оператором АСЗИ в процессе функционирования системы «оператор – подсистема отображения информации» имеет ряд важных особенностей, которые также могут учитываться при использовании представленного подхода.

СПИСОК ЛИТЕРАТУРЫ

1. Автоматизация управления и связь в ВМФ / Под общ. ред. Кононова Ю.М. СПб.: Элмор, 1998. 288 с.
2. Глезер В.Д., Цуккерман И.И. Информация и зрение. Москва–Ленинград, Изд-во Академии наук СССР, 1961. 181 с.
3. Хуторецкий Б.И., Медведь И.А. Взаимодействие человека с ЭВМ в сфере управления. М.: Статистика, 1976. 330 с.
4. Ревенко В.Н., Сегал В.М. Комплексы средств отображения информации – М.: Радио и связь, 1985. 216 с.
5. Смоляров А.М. Системы отображения информации и инженерная психология. М: Высшая школа, 1982. 272 с.
6. Гардан И., Люка М. Машинная графика и автоматизация конструирования: Пер. с франц. – М: Мир, 1987.
7. Суханов В.В. Научная графика на компьютере. Владивосток: Дальнаука, 2005. 354 с.
8. Морская радиоэлектроника. Краткий справочник. – СПб.: Политехника, 2003. С. 91–98.
9. Орлов К.М. Информационно-аналитическое обеспечение в системе управления пл / XX Научно-техническая конференция (межвузовская), ФГУП ВМИРЭ им. А.С. Попова. Петродворец, 2009. С.70–80.

Соколова С.П., Горковенко Е.В.

Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Республика Казахстан, Алма-Ата, Институт проблем информатики и управления МОН РК
ПРИМЕНЕНИЕ СОВРЕМЕННЫХ МЕТОДОВ МНОГОУРОВНЕВОГО КОНТРОЛЯ ДОСТУПА В КОРПОРАТИВНОЙ СЕТИ КОСМИЧЕСКОЙ ИНФРАСТРУКТУРЫ

В результате реализации Государственной программы «Развитие космической деятельности в Республике Казахстан на 2005–2007 годы» создается корпоративная спутниковая информационно-телекоммуникационная система (СИТС), в рамках которой уже действуют центры приема данных дистанционного зондирования в Астане, Алма-Ате, Атырау и Приозерске. Полученные тематические информационные продукты (ТБД) накапливаются, хранятся и передаются заинтересованным организациям на оптических носителях. Инфраструктура СИТС предусматривает два крупных коммутационных узла: в Астане в ГП «Аэрокосмический комитет» и Алма-Ате в НК «КазКосмос». Обмен информацией между ними предполагается осуществлять через использование беспроводной связи, создание защищенного оптоволоконного канала и передачу информации на съемных дисках. В Национальном космическом агентстве Республики Казахстан в Астане предполагается организовать базу метаданных, содержащую описание каталогизированной информации по всем ТБД, территориально расположенным в организациях, занимающихся космическими исследованиями в рамках государственных программ: астрофизический институт (АФИ), Институт космических исследований (ИКИ), Институт ионосферы (ИИ) и пр.

В статье предложена система информационной безопасности для обеспечения многоуровневого разграничения доступа к базам данных сканирования поверхности территории Казахстана. Организация информационной безопасности предусматривает защиту информации путем реализации многоуровневого контроля доступа к ТБД в корпоративной сети космической инфраструктуры, криптографического закрытия конфиденциальной информации, проверки целостности передаваемых сообщений и обеспечения авторизации абонентов СИТС. Многоуровневая защита СИТС рассматривается, как свойство самой системы хранить и обрабатывать данные различного уровня и категорий пользования при наличии персонала с различными категориями допуска таким образом, чтобы исключить доступ к информации или ее модификацию лицами, чей допуск не отвечает уровню секретности информации.

Основные компоненты системы мандатного разграничения доступа

Основным объектом защиты является информация – хранимая и передаваемая по проводным и беспроводным каналам. Корпоративные информационные ресурсы организовываются в виде распределенных тематических БД, при работе с которыми обязательно учитываются особенности защиты информации от несанкционированного доступа (НСД). Тематические БД накапливают достаточно большой объем интегрированной информации (топографические карты, графики, аналитические справки, диаграммы, документы) различного уровня конфиденциальности, по различным тематическим направлениям, предназначенной для различных пользователей и распределенной по различным устройствам или узлам сети. Системообразующие базы данных (СБД) содержат рабочую информацию и тематическую информацию, выдаваемую по запросам пользователей. На этапах проектирования, создания и эксплуатации СИТС доступ к метаописаниям СБД должен быть строго ограничен. Информация, содержащаяся в тематических и рабочих БД, структурируется в зависимости от степени важности (секретности) и доступ к ней организуется в соответствии с уровнем полномочий пользователей. Классификация информационных ресурсов по категориям важности необходима для определения относительной ценности и разработки механизмов контроля, сохраняющих данную ценность. Хранящаяся (на жестких или съемных дисках) информация в СБД с высокой меткой чувствительности подвергается шифрованию.

При работе с информационными ресурсами, организованными в распределенные БД, обязательно учитываются следующие особенности защиты информации от НСД:

- в БД может накапливаться большой объем интегрированной информации по различным тематическим направлениям, предназначенной для различных пользователей;
- БД могут быть физически распределены по различным устройствам и узлам сети;
- БД могут включать информацию различного уровня конфиденциальности.

Интегрированная информация, хранящаяся в базах данных по различным тематическим направлениям и предназначенная для различных пользовательских групп, должна иметь многоуровневую систему мандатного разграничения доступа, которая обеспечит класс необходимой защищенности [1]. Ядром системы многоуровневой защиты является монитор обработки запросов, который проверяет каждое обращение пользователя к данным или программам на предмет согласованности со списком действий, допустимых для пользователя (рисунок 1).

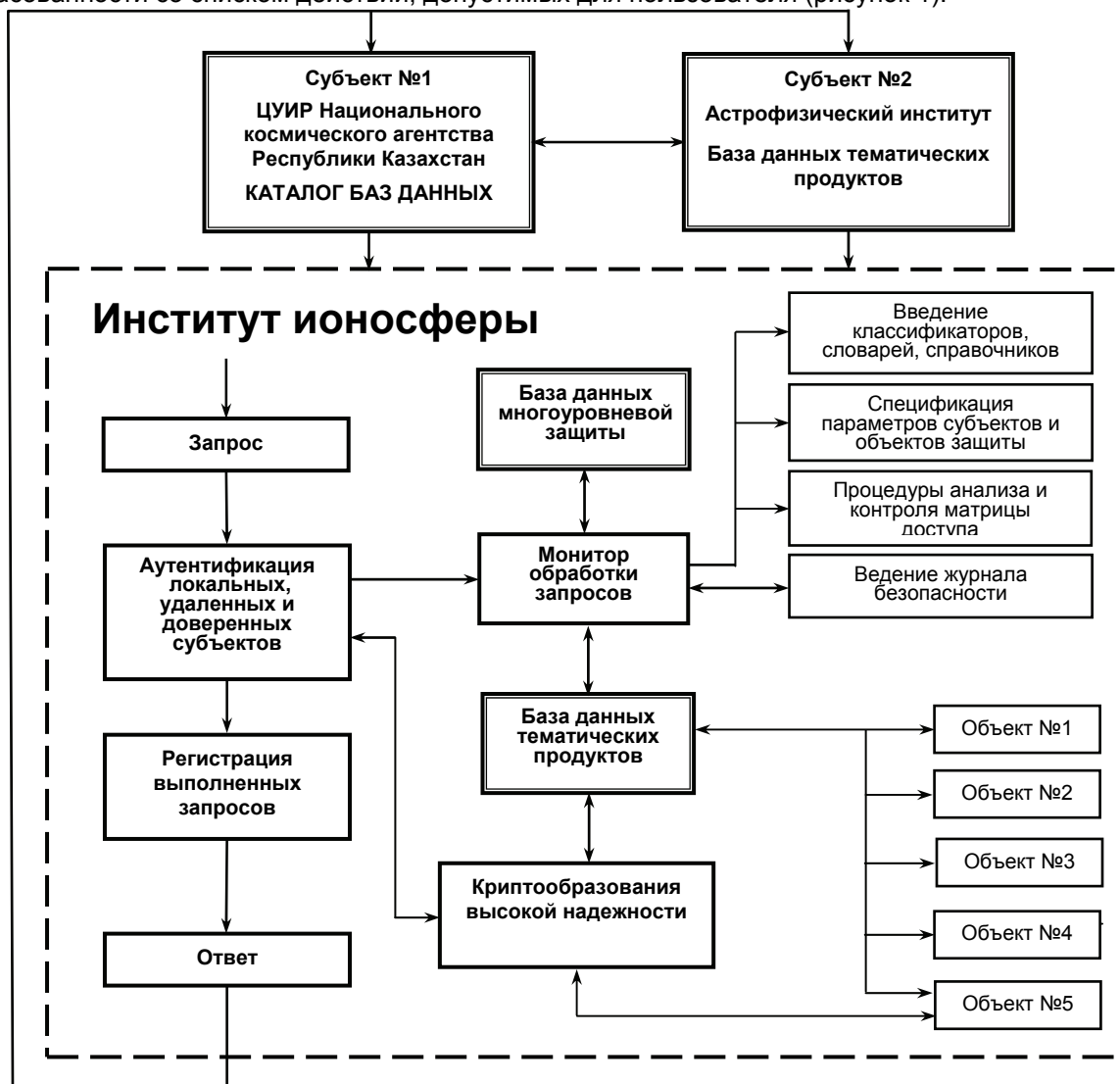


Рис. 1. Многоуровневая система разграничения доступа в корпоративной сети космической инфраструктуры

Монитор связан с базой данных многоуровневой защиты, специфицирующей объекты и субъекты защиты, правила и условия контроля доступа. Основными компонентами системы разграничения доступа являются две подсистемы, одна из которых направлена на выполнение запросов пользователей к информационным ресурсам, а другая - на поддержку работы администратора безопасности без нарушения правил доступа по разрешению запросов к информации различного уровня секретности. Для эффективного и безопасного информационного обмена между компонентами СИТС определяются функциональные требования по каждой подсистеме:

- к типу представления информации в спутниковом сигнале (графическая, текстовая, цифровая) и к видам обработки информации;
- к структуре и способам организации данных в криптосистеме;
- к режиму формирования и рассылки ключей при фиксации попытки НСД;
- по организации защиты данных при авариях и сбоях;
- по организации процедуры хранения, обновления и восстановления данных;

- по использованию классификаторов и возможностей встроенной защиты СУБД.

По каждой подсистеме определяется перечень задач, временной регламент реализации каждой задачи, форма представления выходной информации.

В соответствии с выбранной моделью разграничения доступа выделяются субъекты и объекты защиты, определяются правила доступа (по чтению, редактированию, записи и т.д.) и условия контроля правами доступа (передача прав, лишение прав, порождение объектов, изменение уровня секретности и т.п.) [2]. Субъекты, как активные носители информации, могут перемещать или изменять содержимое объектов. Объекты, как пассивные носители информации, могут хранить ее содержимое (файлы, директории, базы данных). Также они могут быть измененными (сообщения, программы, процедуры, запросы). Классификация информационных ресурсов производится по категориям ценности или ведомственной принадлежности. Вся информация, создаваемая пользователем, может иметь одну из следующих категорий: «свободно доступная», «персональные данные», «конфиденциальная», «для служебного пользования», «секретная», «совершенно секретная», «особой важности». Или следующих типов: «правительственная», «ведомственная», «институтская», «индивидуальная» и т.д. Чем выше степень доверия (категория допуска) субъекта, тем к более секретной информации он имеет доступ. Примеры категорий допуска субъектов: 1-я форма допуска, 2-я форма допуска, 3-я форма допуска.

Основное назначение полномочной политики безопасности, базирующейся на многоуровневой мандатной модели разграничения доступа, заключается в регулировании доступа субъектов системы к объектам с различным уровнем критичности и предотвращении утечки информации с верхних уровней должностной иерархии на нижние. В случае возможного проникновения с нижнего уровня должностной иерархии на верхний уровень осуществляется его блокирование. Полномочное управление доступом подразумевает, что:

- все субъекты и объекты системы, подлежащие защите, должны быть однозначно идентифицированы с возможностью их последующей аутентификации;
- каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;
- каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

Пусть множества $S = \{s_j, j = \overline{1, m}\}$ и $O = \{o_i, i = \overline{1, n}\}$, соответственно, конечные линейно упорядоченные множества субъектов и объектов доступа к корпоративным ресурсам космической инфраструктуры. Каждому субъекту s_j приписывается определенный уровень защиты $J(s_j)$, $j \in J$, остающийся неизменным все время функционирования системы и сохранения статуса субъекта. Этот уровень соответствует категории допуска (уровню прозрачности) субъекта. Каждый субъект $s_j \in S$ представляется парой $\{\lambda(s_j), \mu(s_j)\}$, где $\{\lambda_j\}$ - конечное множество классификаций статуса субъектов, $\{\mu_j\}$ - конечное множество категорий допуска. Каждому объекту $o_i \in O$ присваивается уровень защиты объекта $J(o_i)$, который соответствует уровню секретности (метки критичности) информации $l_n \in L$, хранящейся в объекте o_{i1} (файл) или к которой обращается объект o_{i2} (программа). Каждый объект $o_i \in O$ определяется характеристиками $\{s_j(o_i), l_n(o_i)\}$, где $\{s_j\}$ - множество субъектов-владельцев объектов o_i , $\{l_n\}$ - множество степеней секретности.

Пусть $A = \{\alpha_k, k = \overline{1, K}\}$ - множество видов доступа субъектов к объектам определяется следующими значениями: R - чтение; G - перезапись информации из объекта в объект; D - добавление информации в объект, без предварительного чтения; W - запись, после предварительного чтения; E - исполнение команды; O - отказ в выполнении запроса; C - создание объекта, U - уничтожение объекта, L - лишения прав на доступ, P - право передачи прав между субъектами, PV - наделение правом владения объектом, I - изменение уровня защиты, PR - право порождение объекта, CP - копирование, KL - право классификации объектов, Y - разрешение на реализацию запроса.

Контроль доступа, реализующий базовые требования к мандатному механизму защиты, осуществляется с помощью матрицы прав доступа $M = \|m_{ij}\|$, $i = \overline{1, n}$, $j = \overline{1, m}$. Эта матрица содержит список видов доступа субъекта $s_j \in S$ к объектам $o_i \in O$, на которые он может претендовать, и которые ему в данный момент разрешены. Доступ к информации организован таким образом, что каждый субъект имеет право обратиться к объекту только с тем видом доступа, который имеется в списке. Для всех запросов обязательным является соблюдение основного условия отношения доступов: уровень доступа субъекта должен быть не меньше уровня защиты объекта.

Тогда текущий запрос субъекта $s_j \in S$ к информационным ресурсам представляется в виде $b_t = (s_j, o_i, a_k)$, $a_k \in A$, $b_t \in B$ и выполняется, если затребованный вид доступа субъектов к объектам является разрешенным в данный момент и это разрешение к настоящему моменту не отменено, т.е. право «реализация запроса» активно. Разрешение действует до тех пор, пока субъект не обратится с запросом об отказе от доступа. В алгоритме обработки текущих запросов выполняются следующие условия [3]:

1. Не позволяющие субъекту получить информацию от субъекта $J(s_{j1}) > J(s_{j2})$ или объекта с более высоким уровнем защиты $J(s_j) \geq J(o_i)$;

2. Не позволяющие субъекту получить информацию от объекта при отсутствии права допуска на реализацию текущего запроса, т.е. только если $a_k = "Y"$.

Основные условия задания правил доступа в дальнейшем определяют контроль и анализ заполнения матрицы прав доступа. Рассмотрим несколько случаев, когда доступ будет разрешен субъекту s_{j1} ,

чей уровень защиты выше уровня защиты s_{j2} , т.е. $J(s_{j1}) > J(s_{j2})$ при различных вариантах статусов s_{j1} и s_{j2} .

Случай 1. $\lambda_{j1} = \lambda_{j2}$, $\mu_{j1} > \mu_{j2}$. Субъекты относятся к одному классу, например «научный руководитель проекта», но имеют разные уровни допуска: $\mu(s_{j1}) = \text{«3-я форма допуска»}$ и $\mu(s_{j2}) = \text{«2-я форма допуска»}$.

Случай 2. $\lambda_{j1} = \lambda_{j2}$, $\mu_{j1} > \mu_{j2}$. У субъектов категория допуска одинаковая, однако, субъект s_{j1} относится к классу «научный руководитель проекта», а s_{j2} имеет класс «ответственный исполнитель проекта».

Случай 3. Субъект s_{j1} , безусловно, имеет больше прав доступа, чем s_{j2} , так как имеет большую категорию допуска и относится к более высокому классу.

Случай 4. $\lambda_{j1} = \lambda_{j2}$, $\mu_{j1} > \mu_{j2}$. Это особый случай. Несмотря на то, что субъект s_{j1} может относиться к классу «ответственный исполнитель проекта» с категорией допуска «1-я форма допуска», а субъект s_{j2} относится к классу «руководитель проекта» с категорией допуска «2-я форма допуска», доступ s_{j1} будет разрешен.

Уровни защиты субъектов будут равны, т.е. $J(s_{j1}) = J(s_{j2})$, если $\lambda_{j1} = \lambda_{j2}$, $\mu_{j1} > \mu_{j2}$. Это может иметь место лишь для различных ветвей дерева субъектов, когда субъекты находятся на одной горизонтали, при этом субъекты $s_{j1}, s_{j2} \in S$ будут относиться к одной подгруппе пользователей с одинаковыми правами доступа.

Рассмотрим работу основных компонент системы мандатного разграничения доступа.

Аутентификация субъектов. Применение методов идентификации и аутентификации в целях защиты информации при ее обмене предполагает конфиденциальность образов и имен объектов. При сетевом или беспроводном удаленном обмене информацией необходимо предусмотреть взаимную проверку подлинности полномочий объекта или субъекта. Выделено несколько типов пользователей: локальные, удаленные и доверенные абоненты (типа администратор). Их аутентификация осуществляется через функцию подтверждения подлинности на основе пароля. Пароль необходимо хранить в зашифрованном виде, что существенно снижает риск его раскрытия. Файл, хранящий пароль, и информация о грифе секретности объектов и уровне допуска субъектов системы должны быть защищены от попыток НСД.

Задание параметров многоуровневой защиты. Политика разграничения доступа организации должна быть описана в форме высокоуровневых спецификаций разграничения доступа, где необходимо определить параметры безопасности, которые определяют свойства субъектов и объектов защиты организации, а также разрешенные операции субъектов системы над объектами. В спецификацию субъекта защиты входят параметры, идентифицирующие субъект и определяющие его категорию допуска, классификацию субъектов (куратор, руководитель, исполнитель, гость и пр.), право владения объектами защиты, право порождения субъектов и объектов («отец», «сын»), правила выбора и защиты идентификатора субъекта. Аналогично, в спецификацию объекта защиты входят параметры, идентифицирующие объект и определяющие его тип группы (файл, директория, процедура), степень секретности информации, идентификатор субъекта-владельца, место и способ

хранения информации, статус объекта (первичный, вторичный, порожденный). В матрице задания прав доступа отслеживаются большое количество зависимостей между значениями определенных кортежей пары «субъект–объект» с определением разрешенных видов доступа и правом на реализацию затребованного вида доступа.

Ведение классификаторов. Классификаторы «Типы конфиденциальности», «Виды управления доступом», «Классификация объектов», «Классификация субъектов», «Виды доступа», «Типы НСД» и т.д. позволяют эффективнее заполнять спецификации и матрицу доступа.

Процедуры анализа и контроля. Анализ подразумевает проверку полноты заполнения спецификаций субъектов и объектов защиты, формирование процедур задания правил и условий разграничения доступа и автоматизированное заполнение матрицы доступа в диалоговом режиме. Контроль полномочий доступа, подразумевающий передачу полномочий доступа между субъектами, имеет характерные особенности в соответствии с принятыми в нашей стране процедурами работы с информацией ограниченного пользования. Это накладывает ряд ограничений при формировании правил разграничения доступа и управлении матрицей прав доступа. Изменение состояния вычислительной системы при разрешении запроса должно приводить к защищенному состоянию, если исходное состояние также было защищено. Для этого необходимо строго выполнять решающие правила по разрешению запросов и изменению состояний системы. Монитор обработки запросов выполняет ряд контрольных функций, главными из которых являются:

1. Проверка реализации права владения и права порождения с учетом иерархии субъектов и объектов защиты.

2. Контроль выполнения текущего запроса с учетом выполнения основного правила доступа, не позволяющее субъекту получить или записать информацию от субъекта или объекта с более высоким уровнем защиты и не позволяющее субъекту получить информацию от объекта при отсутствии разрешения на реализацию текущего запроса.

3. Защита матрицы прав доступа от попыток несанкционированной модификации.

4. Блокировка обращений неавторизованных пользователей при аутентификации субъектов защиты.

5. Постоянный контроль и анализ журнала безопасности в процессе выполнения процедур аутентификации и формирования запросов.

Регистрация выполненных запросов и попыток НСД. Если уровень допуска субъекта противоречит правилам доступа выбранной модели многоуровневой защиты или субъект не имеет права на реализацию подобного запроса, то субъекту будет отказано в доступе, а в журнале подобный запрос регистрируется как попытка НСД. Если доступ разрешен, то субъект работает в диалоговом окне с выбранной информацией в соответствии с разрешенным видом доступа, а в журнале регистрируется: субъект, объекты к которым он обращался, виды доступа, время и способы передачи информации по выбранным каналам связи.

Ведение журнала безопасности. В журнале регистрируется шифр субъекта, шифр объекта, все действия, время обращения и работы с базой данных тематических продуктов. Администратор безопасности должен иметь возможность просмотра журнала с установкой фильтра просмотра по дате, по типу транзакций, по имени файла, реакции монитора на попытки НСД неавторизованных пользователей. Анализ журнала безопасности по попыткам нарушения прав доступа авторизованных субъектов защиты должен предусматривать организационные санкции в отношении недобросовестных пользователей.

Организация интерфейсов пользователей и диалогов внутри системы, реализующей многоуровневую защиту в корпоративной спутниковой информационно-телекоммуникационной системе, разделена технологически. Она ориентирована на обслуживание конечных пользователей (идентификация абонента, формирование текущего запроса к информационным ресурсам, работа в диалоговом окне с выбранной информацией) и на выполнение функций администраторов безопасности (аутентификация, управление матрицей доступа, контроль обработки всех видов запросов, аудит системы безопасности).

Заключение

Разработка Национальной системы космического мониторинга территории Республики Казахстан направлена на оперативное предоставление государственным органам управления всех уровней достоверной информации о состоянии и использовании природных ресурсов. Обеспечение безопасности данных и защиты цифровых космических изображений от несанкционированного доступа или модификации целесообразно осуществлять с применением новейших достижений в области криптографии и моделирования многоуровневых систем управления доступом не ниже класса В.

Многоуровневый контроль доступа, реализованный в корпоративной СИТС через механизмы мандатной модели разграничения доступа, позволит реализовать методы формирования иерархических зависимостей внутри выделенных множеств субъектов и объектов защиты. Контроль полномочий доступа, подразумевающий передачу полномочий доступа между субъектами, имеет характерные особенности в соответствии с принятыми в стране процедурами работы с информацией

ограниченного пользования. Это накладывает ряд ограничений при формировании правил разграничения доступа и управлении матрицей прав доступа. Формирование процедур, поддерживающих монитор обработки запросов, базируется на модели мандатного разграничения доступа, в которой реализованы расширенный список прав доступа и управление доступом с учетом права реализации. Выделены условия наделения субъектов защиты «правом владения» объектами защиты и управления «правом реализации запроса», которые отражают реальные ситуации при работе с информацией ограниченного пользования.

Применение криптографических средств в информационных системах с мандатной политикой управления доступом является обязательным условием обработки информации различной степени секретности. В рассматриваемом многоуровневом контроле доступа в корпоративной сети космической инфраструктуры использование криптографических средств может быть реализовано в виде подсистемы нетрадиционных криптопреобразований, которая выполняет следующие функции:

- шифрование паролей субъектов защиты и подтверждение их целостности при попытке несанкционированной модификации;
- шифрование с удовлетворительными характеристиками надежности хранимой или передаваемой по открытым каналам связи информации повышенной степени секретности.

Нетрадиционность использованных криптопреобразований основана на непозиционных полиномиальных системах счисления, которые позволяют производить представление и обработку чисел помодульно независимо по каждому из выбранных оснований системы. Это препятствует распространению ошибок и представляет возможности для выполнения процедур самокоррекции. Криптостойкость предложенных методов шифрования на базе непозиционной полиномиальной системы счисления может задаваться для любого уровня секретности информации, и определяется вероятностью выбора оснований системы (порядка многочлена, их конкретный выбор и размещение) и величины параметра гамма, используемого при шифровании [4]. При таком подходе, криптостойкость незначительно зависит от длины ключа, что позволяет сохранять быстроедействие обработки больших объемов интегрированной информации с различной степенью секретности в корпоративной сети космической инфраструктуры.

Эффективность разработанной системы информационной безопасности продемонстрирована при обеспечении многоуровневого разграничения доступа к базам данных сканирования поверхности территории Казахстана.

СПИСОК ЛИТЕРАТУРЫ

1. Соколова С.П., Горковенко Е.В. Система с мандатной политикой информационной безопасности // Труды XI Санкт-Петербургской международной конференции "Региональная информатика – 2008". СПб.: СПОИСУ, 2009. С. 159–164.
2. Горковенко Е.В. Контроль и анализ задания видов и прав доступа в системах с мандатной политикой информационной безопасности. // Научно-технический и производственный журнал «Вестник компьютерных и информационных технологий». М.: «Машиностроение», №5, 2008. С.51–55.
3. Горковенко Е.В., Соколова С.П. Организация системы с мандатной политикой информационной безопасности. // Сб. «Проблемы информационной безопасности. Компьютерные системы» / под ред. проф. П.Д. Зегжды. СПб.: СПбГПУ, №4, 2008. С. 18–27.
4. Горковенко Е.В. Применение нетрадиционных криптографических преобразований в системах с мандатной политикой управления доступом к информации. // Сб. «Известия ЮФУ». Технические науки. Тематический выпуск. «Информационная безопасность». Россия, Таганрог: издательство Таганрогского технологического института Южного федерального университета, №8, 2008. С.135–141.



СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Алексеев А.В.

Россия, Санкт-Петербург, ОАО «Научно-инженерный центр Санкт-Петербургского электротехнического университета»

КЛАССИФИКАЦИЯ И РЕЙТИНГ-АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОСНОВНЫХ КЛАССОВ

Одной из ключевых задач создания высокоэффективных автоматизированных систем в защищённом исполнении (АСЗИ) сегодня является сравнительный количественный анализ качества и обоснованный выбор представленных на современном IS-рынке технических средств защиты информации (ТСЗИ), их комплексов и систем.

Отсутствие сопоставимых и достоверных исходных данных сравнения, а также методическая сложность выполнения квалиметрических многокритериальных оценок для современных многофункциональных организационно-технических комплексов превращает эту задачу в одну из весьма сложных и практически нерешённых проблем развития АСЗИ.

Одним из возможных и перспективных направлений решения этой проблемы, в том числе для объектов морской инфраструктуры, сложных корабельных и береговых автоматизированных комплексов и систем, комплексов и систем специального назначения является проведение рейтинг-анализа средств по так называемой технологии полимодельной квалиметрической ранговой оптимизации проектных и управленческих решений (технологии КРОПУР) [1,2]. Она прошла успешную апробацию в целом комплексе исследований, посвящённых сравнительному количественному анализу качества (рейтинг-анализу) ТСЗИ, включённых в Государственный реестр сертифицированных ТСЗИ, перечень базовых информационных защищённых компьютерных технологий. Результаты анализа использованы при реализации ряда IS-проектов компаниями-интеграторами [2,3].

В рамках настоящих исследований с целью формирования базы данных квалиметрического сравнения и мониторинга качества ТСЗИ были обобщены результаты многовариантных оценок и рейтинг-анализа основных классов современных сертифицированных средств, классификация которых в обобщённом виде приведена на рисунке 1.



Рис. 1. Классификация специальных технических средств защиты информации

Частота реализации и динамика угроз информационной безопасности по данным [4] приведена на рисунке 2 и подтверждает актуальность решения задачи выявления наиболее предпочтительных технологий и классов используемых ТСЗИ при создании комплексных (интегрированных) систем защиты информации и нейтрализации соответствующих угроз. На рисунке 3 представлена частота используемых технологий защиты информации по данным [5], которая показывает, что при сравнительном количественном (квалиметрическом) анализе эффективности и качества используемых средств (т.е. их рейтинг-анализе) среди первоочередных ТСЗИ должны быть рассмотрены:

- средства разграничения доступа;
- средства межсетевого экранирования;
- VPN-средства;
- средства сканирования и анализа информационной безопасности;
- средства мониторинга-управления информационной безопасностью;
- средства защиты от вредоносных кодов (антиспамовые, антивирусные);
- средства криптографической защиты;
- операционные системы в защищённом исполнении;
- программно-аппаратные комплексы и системы в защищённом исполнении;
- системы электронной цифровой подписи, системы защиты персональных данных.

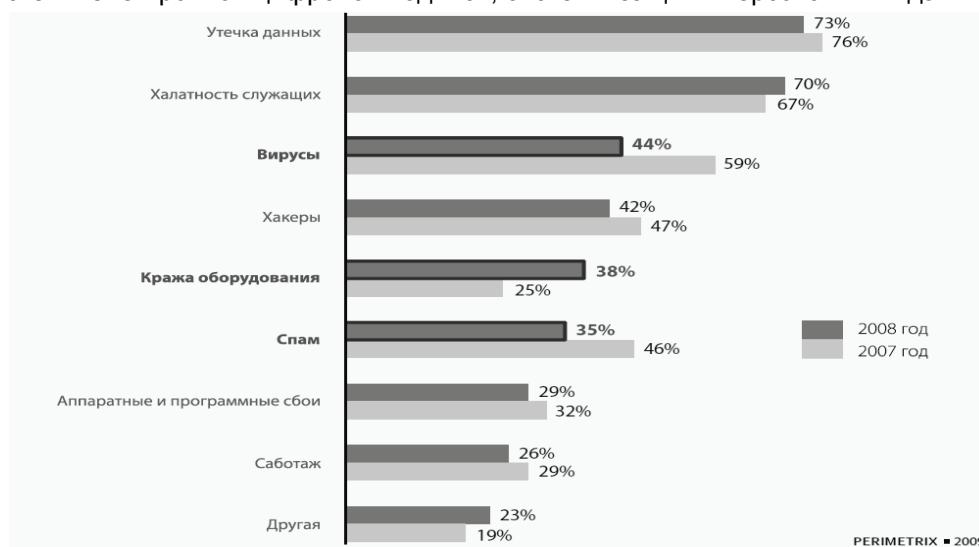


Рис. 2. Динамика частоты реализации угроз информационной безопасности

При проведении исследований особое внимание уделялось систематизации критериев и показателей эффективности использования каждого из классов ТСЗИ, моделированию для различных вариантов их использования наиболее характерных (типовых) вариантов отношений предпочтений заказчиков с соответствующим определением матрицы индексов значимости этих критериев. Полимодельность задания исходных данных по отношениям предпочтений подтвердила возможность получения при рейтинг-анализе альтернативных решений «устойчивой картины» формирования обоснованных проектных и управленческих решений (ПУР).

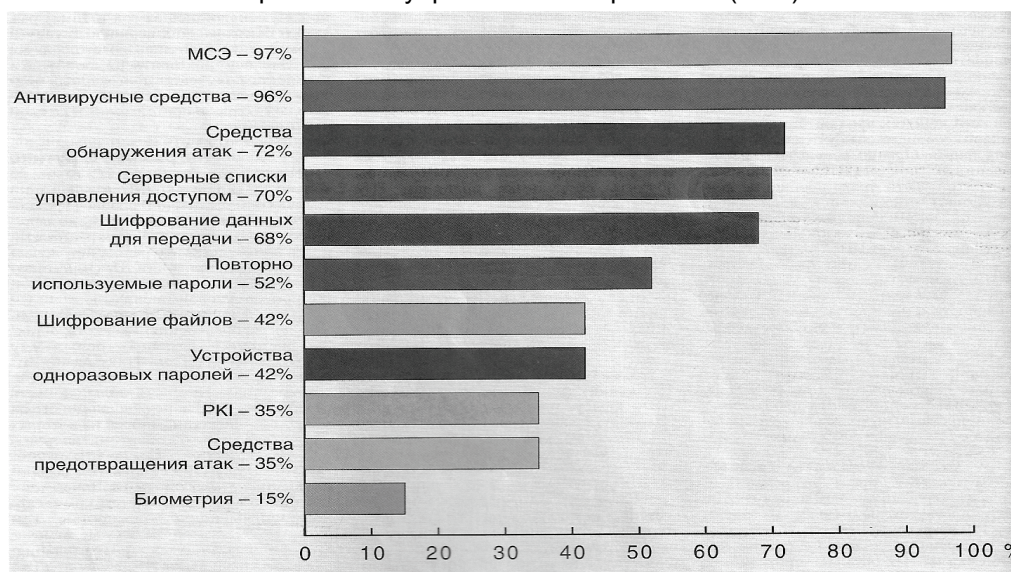


Рис.3. Частота использования технологий защиты информации

Так, например, в соответствии с моделью, алгоритмом и технологией реализации метода КРОПУР при сравнительном анализе комплексных технических средств защиты информации типа «Secret Net 5.0», «Панцирь–К» (класс 3.08 – КСЗИ на рисунке 1) система критериев качества ТСЗИ включала более 10 разнородных критериев, а система моделей предпочтений Заказчика задавалась в виде соответствующих отношений, представленных в таблице 1.

Таблица 1

Пример системы моделей предпочтений Заказчика при рейтинг-анализе ТСЗИ

Тип модели Заказчика	Условное название модели Заказчика	Полнота информации	Точность информации	Предпочтения критериев
M1:	Простая	Неполная (до 4 критериев)	Неточная	Равные
M1.1	Простая	Сравнительная (до 6)	Неточная	Равные
M2:	Неточная	Неполная (до 4 критериев)	Неточная	Определённые
M3:	Неполная	Сравнительная (до 6)	Сравнительная	Определённые
M4:	Бюджетная	Сравнительная (до 6)	Сравнительная	Бюджетные
M5:	Системная	Сравнительная (до 6)	Точная	Системные
M6:	Компромиссная	Сравнительная (до 6)	Точная	Компромиссные
M7:	Равнопрочная	Полная (более 5)	Точная	Равные
M8:	Целенаправленная	Полная (более 7)	Точная	Определённые
M9:	Экономичная	Полная (более 7)	Точная	Бюджетные
M10:	Оптимальная	Полная (более 7)	Точная	Системные
Отношение предпочтений для модели М8 («Целенаправленная»): КС > НСД > = КЦАЧ = КЦ ОС = КЦПО = КЦСЗИ > КЗ > СО > КДП = ЦУ = АД				

Результаты исследований и рейтинг-анализа основных классов ТСЗИ по данным государственного реестра сертифицированных средств защиты информации (реестр ФСТЭК по состоянию на сентябрь 2009 г.) приведены для ТСЗИ классов: МСЭ (класс 3.06 на рисунке 1) – в табл. 2–3, на рисунке 4; НВК (3.03) – на рисунке 5; ОПВ (3.04) – на рисунке 6; СШД (3.05) – на рисунке 7; КСЗИ (3.08) – на рисунке 8. Полученные уникальные данные, безусловно, требуют дальнейшего уточнения, систематизации и наращивания в направлении формирования соответствующих баз данных. Тем не менее, уже полученные и представляемые ниже результаты для разработчиков систем комплексной защиты информации (СКЗИ) в составе АСЗИ имеют большое практическое значение и рекомендуются к соответствующему использованию при проектировании, анализе эффективности эксплуатируемых ТСЗИ и решении других задач.

Таблица 2

Исходные данные рейтинг-анализа межсетевых экранов (МСЭ)

Метод КРОПУР. 9.2: Исходные данные	Критерии сравнения: Дата анализа - 6.11.2009	ОУС	Стоимость объекта, т.руб.	Интеграция с СЗИ, ед.	Цикло сетевых интерфейсов, ед.	Поддержка VPN	Устойчивость	Сервисная фильтрация	Пропускная способность	Централизованное управление	Используемая ОС	Цифровое управление, 0/1	Гибкая конфигурирование, 0/1
Объект сравнения, сертифицирован / 0,6	Автор варианта, производитель, модельный ряд функций	1.ОУС	2.СО	3.ИССЗИ	4.СИ	5.ПВПН	6.У	7.СФ	8.ПС	9.ЦО	10.ОС	11.ЦУ	12.СК
VipNet 545; 1/1	Департамент электронных	0,66	9000	1	6	1	2	1	100	0	0	1	1
WatchGuard Firebox	ООО «Рейнбоу Технолоджи»	0,25	15000	1	7	1	1	1	150	0	1	1	0
Cisco ASA 5510	ОАО «ЭЛВИС ПЛЮС»	0,83	2700	1	4	1	1	1	35	0	1	1	0
Cisco FWSM	Дирекция по строительству	0,33	1700	0	10	1	1	1	35	1	0	0	1
Cisco FWSM	ООО «Инлайн Технолоджи»	0,33	1900	0	10	1	1	1	35	1	0	0	0
NetScreen-500	ОАО «Московская телеком	0,66	2000	1	10	1	1	1	100	0	1	0	1
УБМ-АЛСИ. 1.285	ООО «Ладаком»	0,66	2000	1	10	1	1	1	100	0	1	0	1
Cisco 7301. 1.286	ООО «АлСи-Телеком»	0,25	17000	0	10	1	1	1	250	0	1	1	0
Cisco PM-515E. 1.287	ЗАО «Компания ТрансТеле	0,75	12000	1	10	1	1	1	250	0	1	0	1
Cisco Catalyst 4950-СЭ500	ОАО «Национальное бюро	0,33	2500	1	10	1	1	2	80	0	1	0	0
Cisco PIX. 1.289	ОАО «Национальное бюро	0,20	40000,0	0,1	0,2	1,0	1,5	1	1	1,0	1,0	0,1	0,1
БРИЗ. 1.290	ОАО «РИВЦ-Пулково»	0,20	40000,0	0,1	0,2	1,0	1,5	1	1	1,0	1,0	0,1	0,1
Cisco PI* 1.291	ЗАО «НПЦ Фирма «Нелк»	0,20	40000,0	0,1	0,2	1,0	1,5	1	1	1,0	1,0	0,1	0,1
Cisco PI* 1.292	Комитет по земельным р	0,20	40000,0	0,1	0,2	1,0	1,5	1	1	1,0	1,0	0,1	0,1

Таблица 3

Результаты рейтинг-анализа МСЭ

Сертификат	Срок действия	Шифр средства, сертификат	Заявитель, производитель	M1-Прос-та	R1	M2-Нето-чая	R2	M3-Непол-ная	R3	M4-Бюдже-тная	R4	M5-Систе-мная	R5	M6-Компро-мис	R6	M7-Равноп-рочная	R7	M8-Целепа-равленн	R8	M9-Эконом-ичная	R9	M10-Оптим-альная	R10	M11.2-Полимо-д-Сист	R11	M12-Полимо-д-Адапт	R12
1601	...	Cisco ASA 5510	ОАО «ЭЛВИС ПЛЮС»	0,84	4	0,968	1	0,926	1	0,960	1	0,914	1	0,890	2	0,7082	4	0,857	1	0,857	1	0,853	1	0,848	7	0,877	1
1287	...	Cisco PIX-515E, 1287	ЗАО «Компания ТрансТелеКом»	0,91	2	0,873	3	0,892	3	0,816	4	0,896	3	0,856	3	0,8029	1	0,851	2	0,851	2	0,823	3	0,859	1	0,875	2
1285	...	УБМ-АПСи, 1285	ООО «Ладаком»	0,95	1	0,887	2	0,916	2	0,946	2	0,911	2	0,896	1	0,7654	2	0,814	3	0,814	3	0,846	2	0,836	3	0,824	3
545/1/1	...	MrNet, 545/1/1	Департамент земельных ресурсов г. Москвы	0,8	5	0,82	4	0,819	4	0,780	7	0,804	4	0,759	4	0,8328	8	0,728	4	0,728	4	0,73	4	0,654	6	0,740	4
1288	...	Cisco Catalyst WS-C2950G	ОАО «Национальное бюро кредитных историй»	0,84	3	0,869	5	0,754	5	0,843	3	0,739	5	0,754	5	0,5578	12	0,557	6	0,557	6	0,663	6	0,756	4	0,584	5
1361	...	WatchGuard Firebox	ООО «Рейнбоу Технолоджи – компоненты и системы»	0,86	7	0,514	10	0,598	6	0,812	10	0,581	8	0,575	10	0,6872	5	0,533	9	0,533	9	0,591	10	0,754	5	0,545	6
1641	...	Cisco FWSM	Дирекция по отроительству сетей связи – филиал ОАО «РЖД»	0,6	8	0,534	6	0,586	7	0,815	5	0,612	6	0,667	8	0,6278	9	0,562	5	0,562	5	0,661	5	0,536	10	0,497	7
1668	...	Cisco FWSM	ООО «Инлайн Технолоджи»	0,6	9	0,533	7	0,585	8	0,812	6	0,611	7	0,665	9	0,5441	13	0,526	10	0,526	10	0,624	9	0,501	11	0,486	8
1734	...	NetScreen-500	ОАО «Московская телекоммуникационная корпорация»	0,54	10	0,521	8	0,504	10	0,756	8	0,513	9	0,689	6	0,5979	10	0,535	7	0,535	7	0,631	7	0,444	12	0,458	9
1298	...	NetScreen-025-005	ЗАО «АМТ-Групп»	0,54	10	0,521	8	0,504	10	0,756	8	0,513	9	0,689	6	0,5979	10	0,535	7	0,535	7	0,631	7	0,444	12	0,458	9
Нет	...	3D. Вариант - Резервный	RN-500 (итай), нет	0,68	6	0,386	11	0,531	9	0,599	11	0,511	11	0,555	11	0,7276	3	0,439	13	0,439	13	0,559	11	0,859	1	0,436	11
1286	...	Cisco 7301, 1286	ООО «Алси-Телеком»	0,48	12	0,37	12	0,445	12	0,553	12	0,478	12	0,515	12	0,6585	6	0,497	11	0,497	11	0,546	12	0,567	8	0,425	12
1295	...	Cisco PIX, 1295	ООО «ИБМ Восточная Европа/Азия»	0,48	12	0,37	12	0,445	12	0,553	12	0,478	12	0,515	12	0,6585	6	0,497	11	0,497	11	0,546	12	0,567	8	0,425	12
1289	...	Cisco PIX, 1289	ОАО «Национальное бюро кредитных историй»	0,09	14	0,144	14	0,171	14	0,122	14	0,189	14	0,102	14	0,4201	14	0,290	14	0,290	14	0,25	14	0,244	14	0,283	14
1290	...	БРИЗ, 1290	ОАО «РИБЦ-Пулково»	0,09	14	0,144	14	0,171	14	0,122	14	0,189	14	0,102	14	0,4201	14	0,290	14	0,290	14	0,25	14	0,244	14	0,283	14
1291	...	Cisco PIX, 1291	ЗАО «ИПЦ-Фирма Чоко»	0,09	14	0,144	14	0,171	14	0,122	14	0,189	14	0,102	14	0,4201	14	0,290	14	0,290	14	0,25	14	0,244	14	0,283	14
1292	...	Cisco PIX, 1292	Комитет по земельным ресурсам и землеустройству г. Санкт-Петербурга	0,09	14	0,144	14	0,171	14	0,122	14	0,189	14	0,102	14	0,4201	14	0,290	14	0,290	14	0,25	14	0,244	14	0,283	14

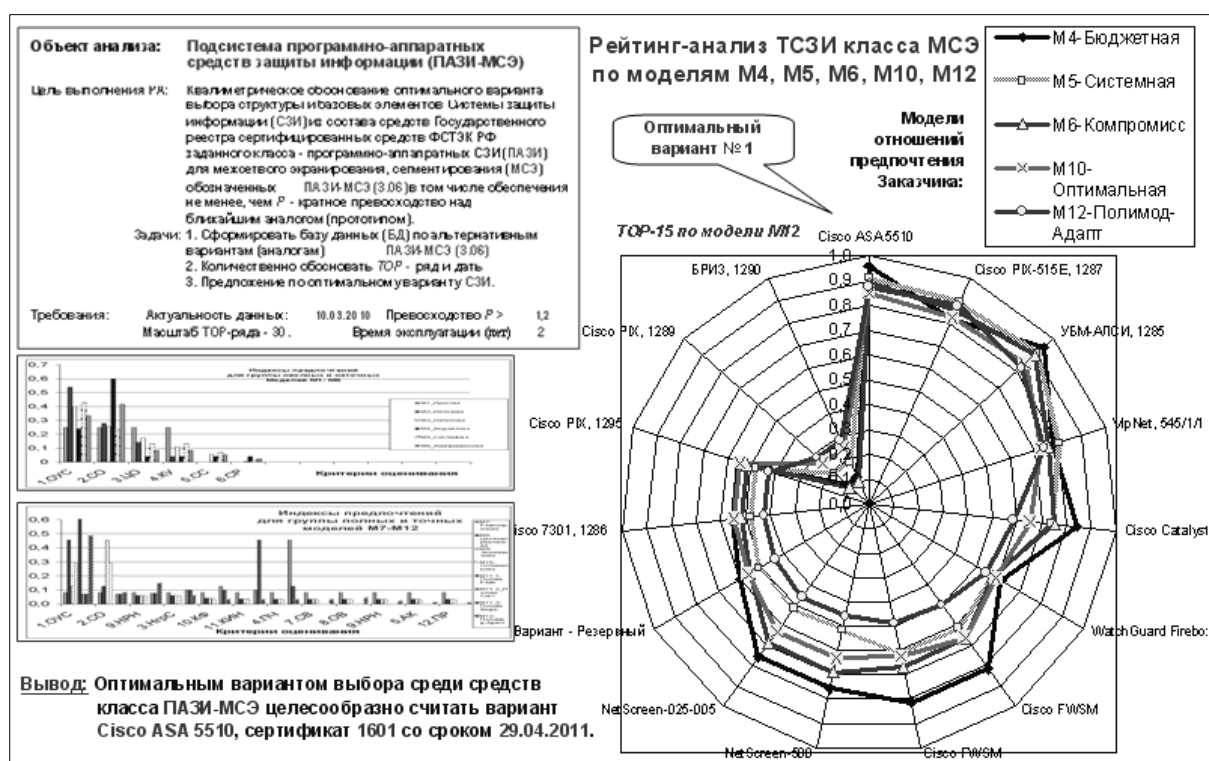


Рис. 4. Результаты рейтинг-анализа МСЭ

Результаты проведенного квалиметрического анализа и ранжирования ТСЗИ основных классов показали, прежде всего, реальную возможность и актуальность оптимизации структуры и параметров интегрированных СКЗИ в составе АСЗИ, а также проектных и управленческих решений по их созданию, эксплуатации и развитию с использованием непрерывно актуализируемых баз данных рейтинг-анализа ТСЗИ.

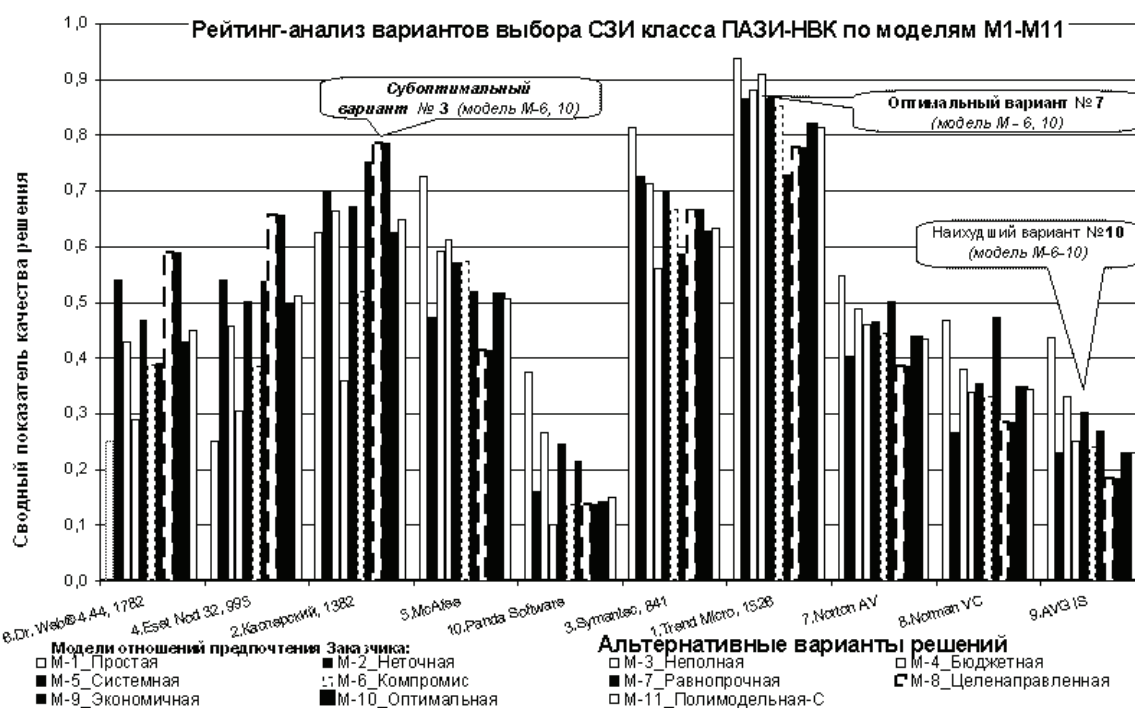


Рис. 5. Результаты рейтинг-анализа средств защиты от вредоносных кодов (НВК)

Объекты	Название сканера безопасности, производитель
IS (I)	Internet Scanner 7.0 (Internet Security Systems, сертификат № 862-2004)
PC (P)	Сетевой сканер "Ревизор сети" 1.2.1.0 ("ЦБИ-сервис", сертификат № 845/1-2004)
MBSA_	Microsoft Baseline Security Analyzer v.2.0 (Microsoft)
XP (X)	XSpider 7.0 (Positive Technologies)
Retina (R)	Retina 4.9.221 (eEye Digital Security)
TNeWT (T)	Tenable NeWT 2.0 (Tenable Network Security)
AppDet_	AppDetective (Application Security)
I+P+X+R+T	Комплекс 5 сканеров: IS+PC+XP+Retina+TNeWT
I+P+X+R	Комплекс 4 сканеров: IS+PC+XP+Retina
I+P+X	Комплекс 3 сканеров: IS+PC+XP
I+X	Комплекс 2 сканеров: IS+XP
T+X	Комплекс 2 сканеров: TNeWT+XP
T+X+R	Комплекс 3 сканеров: TNeWT+XP+Retina
T+I	Комплекс 2 сканеров: TNeWT+IS

Рис. 6. Результаты рейтинг-анализа средств обнаружения и предотвращения вторжений (ОПВ)

Одной из актуальных задач компаний-интеграторов сегодня является квалиметрическое оценивание альтернативных вариантов построения, эксплуатации и развития систем комплексной защиты информации. Сложность задачи оптимального выбора архитектуры и параметров СКЗИ определяется, прежде всего, проблематичностью адекватного учёта и количественного оценивания их многофункциональности, существенного влияния на оценки качества СКЗИ пресловутого «человеческого фактора», многовариантности условий функционирования и оценивания качества.

Один из типовых вариантов архитектуры СКЗИ в составе АСЗИ подобного рода в обобщённом виде приведён на рисунке 8 и, прежде всего, иллюстрирует многовариантность решения задачи поиска эффективных проектных и управленческих решений. Как показывает практика, при синтезе предпочтительных и оптимальных вариантов построения, создания и эксплуатации АСЗИ, прежде всего, необходимо безошибочно и результативно выбирать технические средства реализации подобных структур. Это возможно лишь на основе соответствующих квалиметрических оценок и ранжирования альтернативных вариантов решения задачи поиска ПУР, в том числе подобных представленным выше данным.

Так, на рисунке 9 приведён один из примеров рейтинг-анализа и квалиметрического обоснования выбора комплекса средств защиты информации (КСЗИ) из состава сертифицированных по требованиям ФСТЭК РФ.

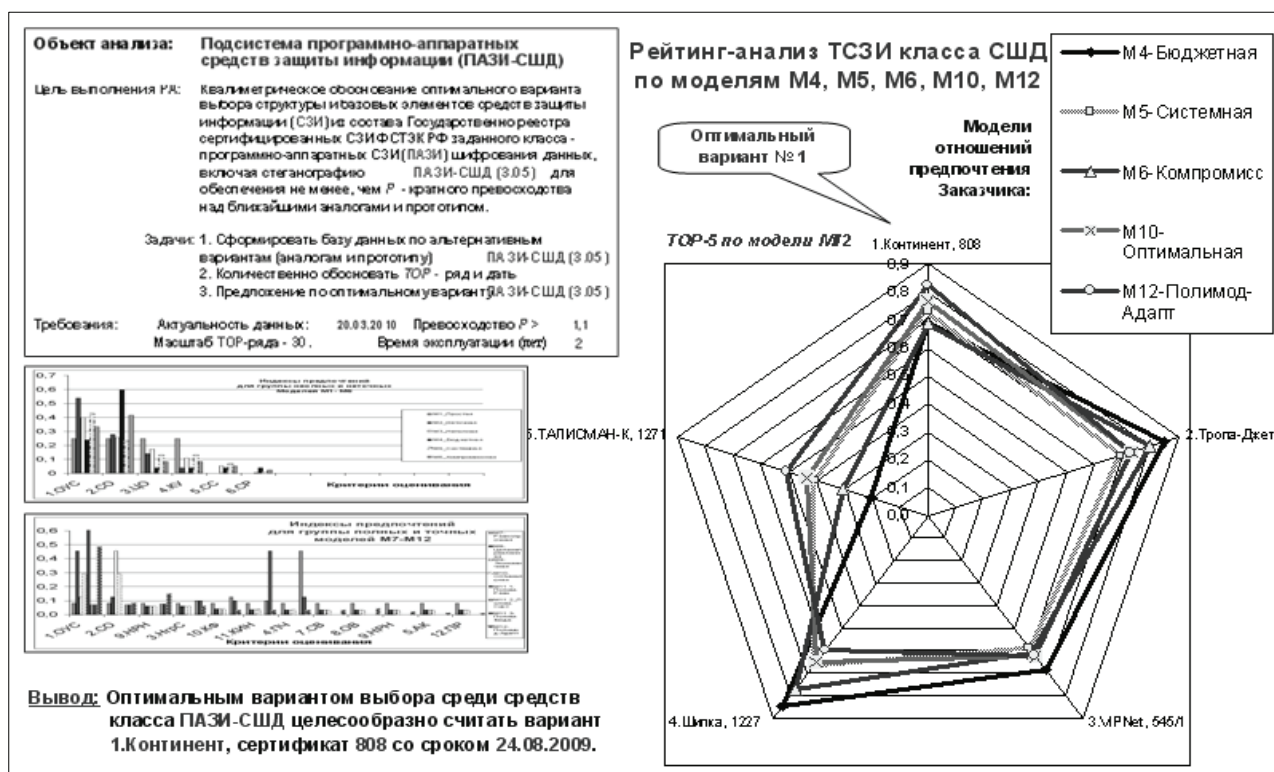


Рис. 7. Результаты рейтинг-анализа средств шифрования данных (СШД)

Как показали оценки, наиболее предпочтительным вариантом выбора при модели предпочтений Заказчика «М-10_Оптимальная» рекомендован вариант №4 с максимальной оценкой качества, превосходящей прототип, как ближайший альтернативный вариант (вариант №3), более, чем на 15% и более, чем в 5 раз превосходящий наихудший из рассматриваемых вариант №5

Понятно, что подобные количественные комплексные оценки имеют весьма существенное ресурсное, в том числе финансовое (денежное) выражение и для Заказчика весьма значимы. Именно поэтому принятие Разработчиком ПУР должно основываться на подобных многовариантных итерационных оценках с обязательной их интерпретацией и согласованием с Заказчиком. При этом, сам процесс многоаспектного полимодельного анализа и синтеза, по существу представляет собой не что иное, как процесс регуляризации (доопределения) задачи многокритериальной оптимизации.

С учётом того обстоятельства, что затраты на развитие СКЗИ составляют, как известно, порядка (20...30)% от бюджета развития компании, получаемые при этом выигрыши от оптимизации затрат представляются весьма значительными и экономически обоснованными.

Тем самым, при использовании предлагаемой технологии [1–3] обеспечиваются условия одновременного учёта при обосновании ПУР как функциональных, информационно-технических, так и технико-экономических факторов с одновременным учётом системы предпочтений Заказчика и ранжирования получаемых при этом многокритериальных оценок.

Следует также отметить, что управление эффективностью комплексного использования ТСЗИ в составе современных сложных (многофункциональных и масштабируемых) информационно-коммуникационных АСЗИ (как правило, с гетерогенными структурами) должно основываться на использовании контуров мониторинга и управления состоянием защищённости информационных ресурсов АСЗИ. В сочетании с соответствующим прогнозированием обстановки на базе непрерывного получения квалиметрически состоятельных оценок и контроля заданных Заказчиком параметров это позволит создать высоко эффективный и высоко технологический контур управления информационной безопасностью АСЗИ.

В свою очередь, повышение точности и достоверности квалиметрической ранговой оптимизации проектных и управленческих решений, соответствующих результатов рейтинг-анализа ТСЗИ для СКЗИ в составе АСЗИ должно непрерывно наращиваться. Среди первоочередных направлений повышения точности оценок следует считать: повышение точности задания исходных данных; проведение специальной научно-технической экспертизы публикуемых (в литературе и других средствах информации) характеристик и параметров ТСЗИ; публикацию результатов сертификационных испытаний.

Ещё более результативным следует признать проведение «межведомственных» сравнительных тестовых испытаний, в том числе на базе универсальных информационно-моделирующих стендов и комплексов [1, 2, 6], а также формирование и непрерывную актуализацию специализированных баз данных ТСЗИ с соответствующими информационно-техническими параметрами, эксплуатационными данными результатами полимодельного рейтинг-анализа.

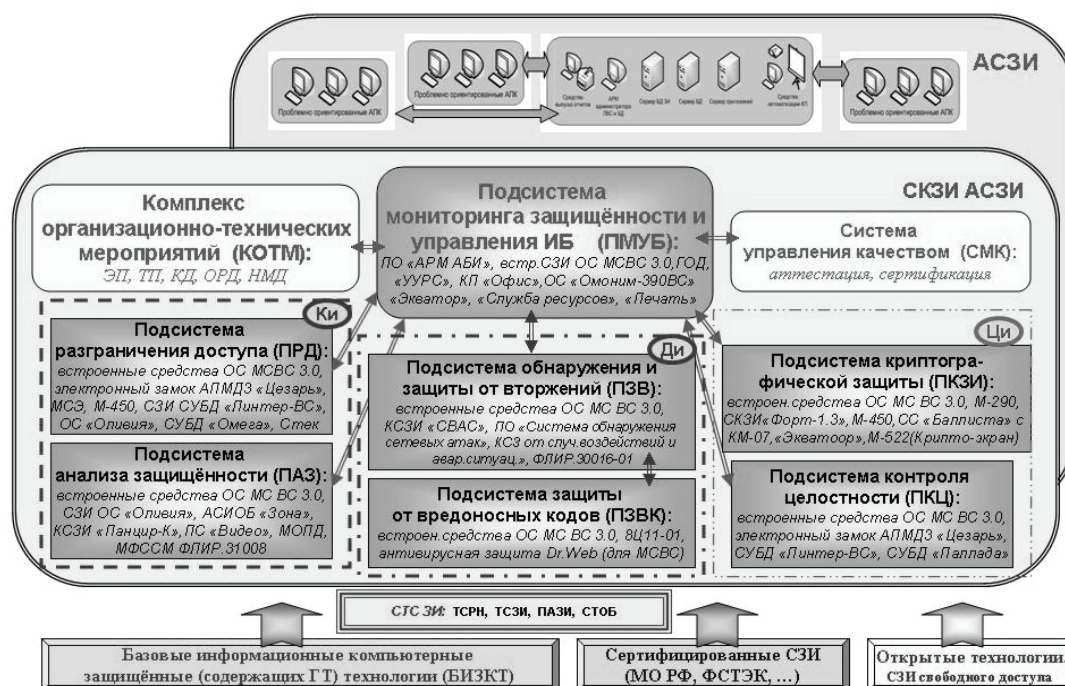


Рис. 8 – Типовая архитектура СКЗИ в составе АСЗИ и многовариантность поиска ПУР

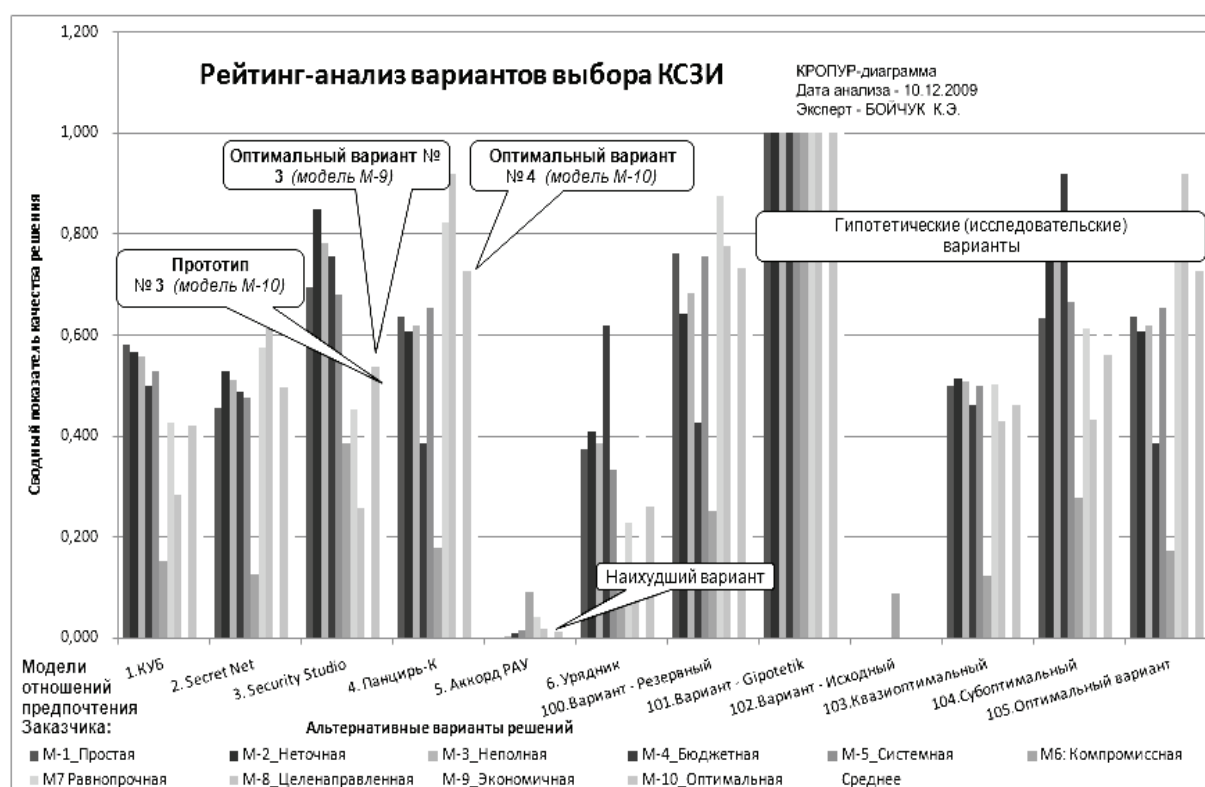


Рис. 9. Результаты рейтинг-анализа комплексных средств защиты информации

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В. Технология и программный комплекс квалиметрической ранговой оценки качества сложных информационно-аналитических систем. / Материалы IX всероссийской научно-практической конференции МОРИНТЕХ–ПРАКТИК «Информационные технологии в судостроении – 2008». СПб. 2008. С.110–118.
2. Алексеев А.В. Технология квалиметрической ранговой оптимизации проектных и управленческих решений / Труды Международной Научной Школы «Моделирование и Анализ Безопасности и Риска в Сложных Системах (МА БР–2007)». СПб. ГОУ ВПО «СПбГУАП» 2007. С.285 – 290.
3. Алексеев А.В. Оптимизация проектных и управленческих решений при комплексном обеспечении безопасности большого города // Безопасность большого города / Сб. ст. под ред. Э.И.Слепая. С.-Петербург: Издательство Сергея Ходова, 2007. С. 400–418.
4. [Электронный ресурс]: Сайт компании Perimetrix . URL: <http://www.perimetrix.ru> (дата обращения: 09.03.2010)
5. Грибуни В.Г. IT–Security. 2006. С.18.
6. Алексеев А.В. Универсальный информационно-моделирующий комплекс. СПб.: ЗАО «Ниеншанц». 2007.

Галанов А.И., Дернова Е.С., Молдовян Д.Н.

Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
НОВЫЕ СХЕМЫ СЛЕПОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Введение

Системы электронных денег, анонимной регистрации сообщений и тайного электронного голосования используют криптографические протоколы, известные как схемы слепой электронной цифровой подписи (ЭЦП) или просто слепой подписи. Слепая подпись используется для решения задачи обеспечения анонимности. Протоколы такого типа позволяют подписать электронное сообщение M таким образом, что подписывающий не может ознакомиться с сообщением в процессе генерации ЭЦП, а в будущем при получении M и соответствующей этому сообщению подлинной подписи не может идентифицировать однозначно пользователя, который предоставлял ему это сообщение для подписи (подписывающий знает всех пользователей, которые предоставляли сообщения для формирования подписи вслепую, но точно узнать какое сообщение с каким-либо пользователем он не может).

Известны протоколы слепой подписи, которые основаны на одной трудной математической задаче, которой является задача факторизации составных чисел вида $n = qr$, где q и r — два больших простых числа [1] или задача нахождения дискретного логарифма в конечной группе большого простого порядка [2]. Для повышения стойкости протоколов слепой подписи представляет интерес разработка таких протоколов слепой подписи, взлом которых требует одновременного решения двух различных трудных вычислительных задач [3].

В настоящей работе строятся протоколы слепой коллективной подписи и схемы слепой ЭЦП, взлом которых требует одновременного решения двух различных вычислительно трудных задач.

1. Протокол коллективной подписи на основе алгоритма Шнорра

Механизм построения коллективной ЭЦП, основанный на свертке открытых ключей подписывающих и свертке индивидуальных долей подписи [6, 8], может быть применен и в случае использования схемы подписи Шнорра [9] в качестве базового алгоритма. Алгоритм ЭЦП Шнорра основан на сложности задачи дискретного логарифмирования в подгруппе Γ мультипликативной группы конечного простого поля. При этом для обеспечения 80-битовой стойкости характеристика поля p должна иметь размер не менее 1024 бит, а размер порядка генератора подгруппы Γ — не менее 160 бит. Открытый ключ подписывающего вычисляется по формуле $y = \alpha^x \bmod p$, где α — генератор подгруппы Γ , имеющей простое значение порядка q сравнительно малого размера (160 бит), а проверочное уравнение имеет вид $R \equiv \alpha^S y^{-E} \bmod p$. Подписью является пара 160-битовых чисел (E, S) . Вычисление подписи к сообщению M включает следующие шаги:

1. Генерируется случайное число k , $1 < k < q$, и вычисляется значение $R = \alpha^k \bmod p$.
2. К сообщению M присоединяется число R и вычисляется значение некоторой специфицированной 160-битовой хэш-функции F_H от аргумента $M \| R$: $E = F_H(M \| R)$. Число E является первым элементом цифровой подписи.
3. Второй элемент S подписи вычисляется по формуле: $S = k + xE \bmod q$, где x — секретный ключ.

Процедура проверки подлинности подписи осуществляется следующим образом:

1. Вычисляется значение R' : $R' \equiv \alpha^S y^{-E} \bmod p$, где y — открытый ключ.
2. К сообщению M присоединяется число R' и вычисляется значение хэш-функции $E' = F_H(M \| R')$. Если $E = E'$, то подпись считается подлинной.

На основе схемы ЭЦП Шнорра протокол слепой коллективной подписи строится следующим образом. Пусть m подписывающих желают участвовать в протоколе слепой коллективной подписи, т. е. подписывать вслепую передаваемые им сообщения со стороны некоторых пользователей. Каждый i -й подписывающий формирует открытый ключ вида $y_i = \alpha^{x_i} \bmod p$, где x_i — личный (секретный) ключ и $i = 1, 2, \dots, m$. Для проверки коллективной ЭЦП используется коллективный открытый ключ, представляющий собой свертку индивидуальных открытых ключей, вычисляемую как следующее произведение $y_{\text{кол}} = y_1 y_2 \dots y_m \bmod p$. Подписью является пара 160-битовых чисел $(E_{\text{кол}}, S_{\text{кол}})$. Подлинность коллективной ЭЦП проверяется по следующему проверочному уравнению

$$R_{\text{кол}} \equiv \alpha^{S_{\text{кол}}} y_{\text{кол}}^{-E_{\text{кол}}} \pmod{p}.$$

Коллективная подпись к сообщению M формируется следующим путем.

1. Каждый подписывающий выбирает разовый случайный секретный ключ k_i , затем вычисляет разовый открытый ключ $R_i = \alpha^{k_i} \pmod{p}$ и затем вычисляется свертка всех разовых открытых ключей $R_{\text{кол}} = R_1 R_2 \dots R_m \pmod{p}$.

2. Подписывающие вычисляют первый элемент коллективной ЭЦП по формуле $E_{\text{кол}} = F_H(M \| R_{\text{кол}})$.

3. Каждый i -й подписывающий вычисляет свою долю в коллективной подписи в виде значения $S_i = k_i + x_i E_{\text{кол}} \pmod{q}$, такого что выполняется соотношение $R_i \equiv \alpha^{S_i} y_i^{-E_{\text{кол}}} \pmod{p}$.

4. Вычисляется свертка всех долей S_i , где $i = 1, 2, \dots, m$, коллективной подписи в виде суммы $S_{\text{кол}} = S_1 + S_2 + \dots + S_m \pmod{q}$. Значение $S_{\text{кол}}$ является вторым элементом коллективной ЭЦП.

Процедура проверки коллективной ЭЦП состоит в следующем. Вычисляется значение $R^* = \alpha^{S_{\text{кол}}} y_{\text{кол}}^{-E_{\text{кол}}} \pmod{p}$ и затем значение $E^* = F_H(M \| R^*)$. Если $E^* = E_{\text{кол}}$, то коллективная подпись является подлинной. Для коллективной ЭЦП, сформированной в соответствии с описанным выше протоколом коллективной подписи, последнее равенство выполняется, т. е. протокол работает корректно. Действительно, это доказывается с помощью следующих преобразований:

$$R^* \equiv \alpha^{S_{\text{кол}}} y_{\text{кол}}^{-E_{\text{кол}}} \equiv \alpha^{\sum_{i=1}^m S_i} \left(\alpha^{\sum_{i=1}^m x_i} \right)^{-E_{\text{кол}}} \equiv \alpha^{\sum_{i=1}^m (k_i + x_i E_{\text{кол}})} \alpha^{-E_{\text{кол}} \sum_{i=1}^m x_i} \equiv \alpha^{\sum_{i=1}^m k_i} \equiv R_{\text{кол}} \Rightarrow E^* = E_{\text{кол}}.$$

2. Слепая коллективная подпись на основе сложности дискретного логарифмирования в конечном поле

Протокол слепой коллективной подписи можно построить на основе схемы ЭЦП Шнорра [7] следующим образом. Пусть указанные выше m подписывающих желают участвовать в протоколе слепой коллективной подписи, т. е. подписывать вслепую передаваемые им сообщения со стороны некоторых пользователей. При этом проверка коллективной ЭЦП будет выполняться в соответствии с процедурой проверки коллективной подписи с использованием коллективного открытого ключа, вычисляемого в виде свертки индивидуальных открытых ключей (см. раздел 1).

Слепая коллективная подпись формируется следующим путем.

1. Каждый подписывающий выбирает разовый случайный секретный ключ k_i , затем вычисляет разовый открытый ключ $R_i = \alpha^{k_i} \pmod{p}$.

2. Вычисляется свертка $R_{\text{кол}} = R_1 R_2 \dots R_m \pmod{p}$.

3. Подписывающие отправляют пользователю, который желает, чтобы некоторое его сообщение M было подписано вслепую, значение $R_{\text{кол}}$. Этот пользователь вычисляет значения $R' = R_{\text{кол}} \alpha^{-\varepsilon} y_{\text{кол}}^{-\tau} \pmod{p}$ (τ и ε — случайные числа, не превосходящие простое число q) и $E'_{\text{кол}} = F_H(M \| R')$, затем — значение $E_{\text{кол}} = E'_{\text{кол}} + \tau \pmod{q}$, которое отправляет коллективу подписывающих.

4. Каждый i -й подписывающий вычисляет свою долю в коллективной подписи в виде значения $S_i = k_i + x_i E_{\text{кол}} \pmod{q}$, такого, что выполняется соотношение $R_i \equiv \alpha^{S_i} y_i^{-E_{\text{кол}}} \pmod{p}$.

5. Вычисляется свертка всех долей S_i , где $i = 1, 2, \dots, m$, коллективной подписи в виде суммы $S_{\text{кол}} = S_1 + S_2 + \dots + S_m \pmod{q}$. Вычисленная свертка $S_{\text{кол}}$ направляется пользователю.

6. Пользователь вычисляет подпись $(E'_{\text{кол}}, S'_{\text{кол}})$, где $E'_{\text{кол}} = E_{\text{кол}} - \tau \pmod{q}$ и $S'_{\text{кол}} = S_{\text{кол}} - \varepsilon \pmod{q}$, которая является подлинной коллективной подписью для сообщения M .

В соответствии с процедурой проверки коллективной ЭЦП вычисляется значение $R^* = \alpha^{S_{\text{кол}}} y_{\text{кол}}^{-E_{\text{кол}}} \pmod{p}$ и затем значение $E^* = F_H(M \| R^*)$. Если $E^* = E'_{\text{кол}}$, то коллективная подпись является подлинной. Для коллективной ЭЦП, сформированной в соответствии с рассмотренным протоколом слепой коллективной подписи, последнее равенство выполняется, т. е.

протокол работает корректно. Действительно, это доказывается с помощью следующих преобразований:

$$\begin{aligned} R^* &\equiv \alpha^{S'_{\text{кол}}} y_{\text{кол}}^{-E'_{\text{кол}}} \equiv \alpha^{S_{\text{кол}} - \varepsilon} y_{\text{кол}}^{-(E_{\text{кол}} + \tau)} \equiv \alpha^{-\varepsilon} y_{\text{кол}}^{-\tau} \alpha^{S_{\text{кол}}} y_{\text{кол}}^{-E_{\text{кол}}} \equiv \alpha^{-\varepsilon} y_{\text{кол}}^{-\tau} \alpha^{\sum_{i=1}^m S_i} y_{\text{кол}}^{-E_{\text{кол}}} \equiv \\ &\equiv \alpha^{-\varepsilon} y_{\text{кол}}^{-\tau} \alpha^{\sum_{i=1}^m (k_i + x_i E_{\text{кол}})} \left(\alpha^{\sum_{i=1}^m x_i} \right)^{-E_{\text{кол}}} \equiv \alpha^{-\varepsilon} y_{\text{кол}}^{-\tau} R_{\text{кол}} \equiv R'_{\text{кол}} \pmod{p} \Rightarrow E^* = E'_{\text{кол}}. \end{aligned}$$

Рассмотренный протокол обеспечивает анонимность пользователя, предоставляющего документ для получения коллективной подписи вслепую. Проблема анонимности состоит в том, что коллектив подписывающих не может однозначно установить, кто конкретно предоставлял данный документ, подписанный их коллективной подписью. Известно, что различные документы предоставлялись некоторой совокупностью пользователей. Однако с равной вероятностью каждый из этих пользователей мог предоставлять на подпись заданный документ M .

Действительно, любая тройка $(R_{\text{кол}}, E_{\text{кол}}, S_{\text{кол}})$ из множества таких троек, которые формировались подписывающим, может быть ассоциирована с подписью $(E'_{\text{кол}}, S'_{\text{кол}})$ к данному документу M . Это связано с тем, что имеют место соотношения $R_{\text{кол}} = \alpha^{S_{\text{кол}}} y_{\text{кол}}^{-E_{\text{кол}}} \pmod{p}$ и $R'_{\text{кол}} = \alpha^{S'_{\text{кол}}} y_{\text{кол}}^{-E'_{\text{кол}}} \pmod{p}$. Поэтому выполняется соотношение

$$R'_{\text{кол}} / R_{\text{кол}} \equiv \alpha^{S'_{\text{кол}} - S_{\text{кол}}} y_{\text{кол}}^{-E'_{\text{кол}} + E_{\text{кол}}} \pmod{p} \equiv \alpha^{-\varepsilon} y_{\text{кол}}^{\tau} \pmod{p},$$

т.е., при равновероятном случайном выборе «ослепляющих» степеней τ и ε подпись $(E'_{\text{кол}}, S'_{\text{кол}})$ с равной вероятностью была порождена из любой тройки, входящей в множество троек указанного выше типа, которые были сформированы подписывающим.

3. Слепая коллективная подпись на основе сложности задачи логарифмирования на эллиптической кривой

По аналогии с протоколом слепой коллективной подписи, описанной в предыдущем разделе, может быть построен протокол такого типа, использующий вычисления над точками ЭК. Переход от одной схемы к другой обеспечивается заменой операций умножения и экспоненцирования в мультипликативной группе на операции сложения точек ЭК и умножения точки ЭК на число, соответственно. С учетом такой замены формулы проверки коллективной подписи (e', s') имеют вид:

$$R = e'P + s'G \quad \text{и} \quad e' = F_H(M \| x_R),$$

где P – коллективный открытый ключ, x_R – значение абсциссы точки R , вычисленной по первому проверочному уравнению, и $F_H(M \| x_R)$ – используемая в протоколе хэш-функция. Значение P вычисляется как сумма точек $P_i = z_i G$, где G – генератор подгруппы точек достаточно большого простого порядка q' , являющихся открытыми ключами каждого из пользователей, входящих в коллектив из m подписывающих, т.е. коллективный открытый ключ вычисляется как следующая свертка $P = P_1 + P_2 + \dots + P_m$.

Протокол слепой коллективной подписи включает следующие действия.

1. Каждый подписывающий выбирает разовый случайный секретный ключ k_i , затем вычисляет разовый открытый ключ $R_i = k_i G$, и затем вычисляется свертка всех разовых открытых ключей

$$2. \quad R = R_1 + R_2 + \dots + R_m.$$

3. Значение R направляется пользователю, который желает, чтобы сообщение M было подписано вслепую. Этот пользователь вычисляет значения $R' = R - \varepsilon G - \tau P$ (τ и ε – случайные числа, не превосходящие простое число q') и $E' = F_H(M \| x_{R'})$, где $x_{R'}$ – значение абсциссы точки R' , а затем – значение $e = e' + \tau \pmod{q'}$, после чего отправляет подписывающим значение e .

4. Каждый i -й подписывающий вычисляет свою долю в коллективной подписи в виде значения $s_i = k_i - z_i e \pmod{q'}$, такого что выполняется соотношение $R_i = s_i G + e P_i$.

5. Вычисляется свертка s всех долей s_i , где $i = 1, 2, \dots, m$, коллективной подписи в виде суммы $s = s_1 + s_2 + \dots + s_m \pmod{q'}$. Вычисленная свертка s направляется пользователю.

6. Пользователь вычисляет подпись (e', s') , где $e' = e - \tau \pmod{q'}$ и $s' = s - \varepsilon \pmod{q'}$,

7. Подпись (e', s') является подлинной коллективной ЭЦП для сообщения M , которая была сформирована вслепую. Корректность работы этого протокола легко показать по аналогии с доказательством корректности протокола слепой коллективной подписи, описанной в предыдущем разделе. Также не трудно показать, что этот протокол обеспечивает анонимность пользователей, предоставляющих свои электронные сообщения на подпись.

4. *Протокол слепой подписи, основанный на задачах дискретного логарифмирования в простом поле и на эллиптической кривой*

Для построения протокола слепой подписи, взлом которого потребует одновременного решения задачи дискретного логарифмирования в простом поле и задачи дискретного логарифмирования на эллиптической кривой (ЭК), воспользуемся алгоритмом ЭЦП Шнорра [4], реализуемым с использованием конечного простого поля, и его версией, использующей вычисления на ЭК. Подписывающий формирует открытый ключ в виде двух параметров: 1) числа $y = g^{z_1} \bmod p$, где p — достаточно большое простое число, g — генератор подгруппы достаточно большого простого порядка q (т. е. $g^q \bmod p = 1$) и z_1 — первый элемент личного (секретного) ключа; 2) точки P ЭК, вычисляемой по формуле $P = z_2 G$, где G — генератор подгруппы точек ЭК, порядок которой равен достаточно большому простому числу q , и z_2 — второй элемент личного ключа. Заметим, что в протоколе требуется, чтобы элементы g и G имели одинаковое значение порядка q . Это легко достигается путем предварительной генерации ЭК и последующей генерации простого числа p такого, что q делит $p-1$.

Слепая подпись генерируется следующим путем.

1. Подписывающий выбирает пару случайных k_1 и k_2 , вычисляет число $r_1 = g^{k_1} \bmod p$ и точку $R_2 = k_2 G$. Затем подписывающие отправляют пользователю, который желает, чтобы некоторое его сообщение M было подписано вслепую, значение r_1 и точку R_2 .

2. Получив значение r_1 и точку R_2 , указанный пользователь вычисляет значение $r' = r_1 g^{-\varepsilon} y^{-\tau} \bmod p$ (τ и ε — случайные числа, не превосходящие простое число q) и точку $R' = R_2 - \mu G - \tau P$. Затем этот пользователь вычисляет значение $e' = F_H(M \parallel r' \parallel x_{R'})$, где « $\parallel$ » — операция конкатенации, $x_{R'}$ — абсцисса точки R' и F_H — некоторая специфицированная хэш-функция, и значение $e = e' + \tau \bmod q$. Значение e пользователь отправляет подписывающему.

3. Подписывающий вычисляет значения s_1 и s_2 : $s_1 = k_1 - z_1 e \bmod q$ и $s_2 = k_2 - z_2 e \bmod q$ (очевидно, что для вычисленных значений s_1 и s_2 выполняются соотношения $r_1 = g^{s_1} y^e \bmod p$ и $R_2 = s_2 G + eP$). Значения s_1 и s_2 подписывающий отправляет пользователю.

4. Пользователь вычисляет подпись (e', s_1, s_2) , где $e' = e - \tau \bmod q$, $s'_1 = s_1 - \varepsilon \bmod q$ и $s'_2 = s_2 - \mu \bmod q$, которая удовлетворяет процедуре проверки подлинности ЭЦП, в которой используются следующие шаги.

Процедура проверки подписи выполняется следующим образом.

1. Вычислить значение $r_1^* = g^{s'_1} y^{e'} \bmod p$ и точку $R_2^* = s'_2 G + e' P$.

2. Вычислить значение $e^* = F_H(M \parallel r^* \parallel x_{R^*})$. Если $e' = e^*$, то подпись верна.

Данный протокол работает корректно, что можно показать следующим образом. В соответствии с процедурой проверки ЭЦП вычисляется значение $r_1^* = g^{s'_1} y^{e'} \bmod p$ и точка $R_2^* = s'_2 G + e' P$. Если при этом будут выполняться равенства $r_1^* = r'$ и $R_2^* = R'$, то очевидно будет выполняться и условие $e' = e^*$. Действительно, если подпись подлинная, то имеем следующие преобразования:

$$\begin{aligned} r_1^* &\equiv g^{s'_1} y^{e'} \equiv g^{s'_1 - \varepsilon} y^{e' - \tau} \equiv g^{k_1 - z_1 e - \varepsilon} g^{z_1 e} y^{-\tau} \equiv g^{k_1} g^{-\varepsilon} y^{-\tau} \equiv r_1' \pmod{p}; \quad (r_1^* < p, r' < p) \Rightarrow r_1^* = r'; \\ R_2^* &= s'_2 G + e' P = (s_2 - \mu)G + (e - \tau)P = (k_2 - z_2 e - \mu)G + (e - \tau)P = (k_2 - z_2 e - \mu)G + e z_2 G - \tau P = \\ &= k_2 G - \mu G - \tau P = R'_2. \end{aligned}$$

Таким образом, показано, что для правильно сформированной ЭЦП выполняются соотношения $r_1^* = r'$ и $R_2^* = R'$, а значит и равенство $e' = e^*$, т. е. протокол работает корректно.

Предложенный в этом разделе способ построения протоколов слепой подписи может быть применен и для случаев следующих пар трудных задач:

- дискретное логарифмирование в простом поле и дискретное логарифмирование в конечной группе невырожденных матриц;
- дискретное логарифмирование на эллиптической кривой и дискретное логарифмирование в конечной группе невырожденных матриц;
- дискретное логарифмирование на эллиптической кривой и дискретное логарифмирование в конечной некоммутативной группе векторов, заданных над конечным полем.

Рассматриваемый способ также может быть использован для разработки схем слепой подписи, взлом которых требует одновременного решения задачи дискретного логарифмирования и задачи факторизации. Однако для комбинирования двух последних задач более эффективным представляется способ, предлагаемый в следующем разделе.

5. Протокол слепой подписи, основанный на задачах дискретного и факторизации

Протокол слепой подписи, взлом которого потребует одновременного решения задачи дискретного логарифмирования в простом поле и задачи факторизации, можно построить на основе схемы ЭЦП Шнорра [4], в которой используется простой модуль p со специальной структурой $p = 2n + 1$, где $n = q'q$; q' и q — большие простые числа размером не менее 512 бит. Простой модуль с такой структурой ранее применялся для построения рандомизированных алгоритмов ЭЦП, стойкость которых основывалась на сложности факторизации значения $n = (p - 1) / 2$ [5]. Схема цифровой подписи из [5] описывается следующим проверочным уравнением $r = F(\alpha^{HSr} \bmod p)$, где открытым ключом является тройка чисел (p, α, λ) , а подписью — пара чисел (r, S) , в которой длина второго числа равна $|S| \leq \lambda$; H — значение хэш-функции, вычисленное от подписанного документа M ; F — некоторая сжимающая однонаправленная функция, в качестве которой может быть использована, например, функция хеширования F_H , используемая для вычисления значения $H = F_H(M)$; α — число, относящееся по модулю p к показателю q , являющемуся секретным значением (личным секретным ключом). Значение λ — это битовая длина числа q , являющегося простым делителем значения n . Уравнение генерации параметра S в случае имеет вид следующего выражения $S = k(Hr)^{-1} \bmod q$, в котором используется предварительно генерируемое число r , получаемое по формуле $r = F(\alpha^k \bmod p)$, где k — случайное секретное число. При использовании 1024-битового простого числа p и сжимающей функции F , размер значений которой равен 160 битам, длина цифровой подписи составляет $|F| + |q| \approx 160 + 512 = 672$ бит. Важной частью процедуры верификации подлинности ЭЦП является проверка выполнимости условия $|S| \leq \lambda$, поскольку некоторая подпись (r, S') с размером $|S'| \approx 512$ бит (при $|p| \approx 1024$ бит) может быть легко сгенерирована без знания секретного параметра q . Подпись (r, S') будет удовлетворять проверочному уравнению, однако сгенерировать подпись (r, S') , удовлетворяющую условию $|S'| \leq \lambda$, не проще, чем факторизовать число n [5].

Алгоритм ЭЦП, предложенный в работе [5], может быть использован в качестве прототипа схемы ЭЦП, взлом которой требует решения двух трудных задач — факторизации числа n и дискретного логарифмирования в простом поле характеристики p . Отметим, что в последнем случае в данной работе делается отличие между задачами дискретного логарифмирования в конечном поле, решаемой методом вычисления индексов, который имеет субэкспоненциальную сложность [6], и задачей дискретного логарифмирования в подгруппе этого поля, решаемой общими методами дискретного логарифмирования, которые имеют экспоненциальную сложность [6]. Рассмотрим следующую схему ЭЦП с открытым ключом в виде четверки чисел (p, α, λ, y) , где первые три параметра задаются также как и в схеме [5], а значение y вычисляется по формуле $y = \alpha^x \bmod p$, в которой x является еще одним элементом секретного ключа. Данная схема ЭЦП построена по аналогии со схемой Шнорра. Подпись к сообщению M генерируется следующим образом.

1. Генерируется параметр $R = \alpha^k \bmod p$, где k — случайно генерируемое число, $k < q$.

2. Вычисляется значение E : $E = F_H(M \parallel R)$.

3. Вычисляется значение $S = k - xE \bmod q$, что обеспечивает выполнение условия $R = \alpha^S y^E \bmod p$. В качестве ЭЦП берется значение (R, S) .

Проверка подлинности подписи (R, S) осуществляется следующим образом:

1. Если $|S| \leq \lambda$, то вычисляется значение $R^* = \alpha^S y^E \bmod p$. В противном случае подпись отвергается как недействительная.

2. Вычисляется хэш-функция от сообщения M с присоединенным к нему значением R^* : $E^* = F_H(M \parallel R^*)$.

3. Сравниваются значения E^* и E . Если $E^* = E$, то подпись признается подлинной.

Отметим, что на шаге 1 процедуры проверки подлинности подписи важным условием является требование того, что размер подписи не превышает размер секретного ключа $|q| = \lambda$. Этот момент является принципиальным, поскольку после решения только одной трудной задачи — нахождения дискретного логарифма по модулю P — вычислить ЭЦП, в которой для параметра S выполняется соотношение $|S| \leq |n|$. Это может быть осуществлено по формуле $S = k - xE \bmod n$ при условии, что задача дискретного логарифмирования в конечном поле решена и определено значение секретного ключа x . Формирование элемента подписи S длины $|S| \leq \lambda$ является вычислительно сложной задачей, требующей решения проблемы факторизации целого числа n .

Взлом описанной схемы подписи может быть осуществлен, решая одновременно задачу дискретного логарифмирования (позволяет найти секретный ключ x) и задачу факторизации, что позволяет найти значение q , требуемое для вычисления элемента подписи S , размер которого не будет превышать значение $\lambda = |q|$. Однако одновременное решение указанных двух трудных задач не является необходимым для взлома системы. Действительно, секретные параметры схемы можно вычислить, решая только задачу дискретного логарифмирования. Это можно осуществить следующим путем. Выберем произвольное число t , битовая длина которого не превышает значения $\lambda - 1$. Затем вычислим значение $Z = \alpha^t \bmod p$. После этого найдем логарифм от Z при основании α , используя метод вычисления индексов [6]. Это даст некоторое значение T , вычисленное по модулю $n = p - 1$. С вероятностью, близкой к единице, размер этого значения равен $|T| \approx |n| > |t|$. Поскольку по модулю P число α имеет порядок q , то имеем $T = t \bmod q$, поэтому число q делит нацело разность $T - t$. Это означает, что, выполнив факторизацию числа $T - t$, можно найти секретный параметр q . Вероятность того, что факторизация числа $T - t$ будет иметь сравнительно малую сложность, является достаточно высокой. Это означает, что выполнив несколько раз описанную процедуру, будет найдено значение $T - t$, которое легко факторизуется.

Таким образом, чтобы сделать необходимым решение двух различных сложных задач для взлома последней схемы ЭЦП требуется сделать ее модифицирование. Взлом следующей модифицированной схемы ЭЦП требует решения двух различных трудных задач — дискретного логарифмирования в конечном поле характеристики P и факторизации числа n . Это достигается тем, что при построении схемы ЭЦП выбирается параметр α , порядок которого равен n , а вместо значения S в уравнение проверки подписи вводится S^2 . Подпись к сообщению M генерируется следующим образом.

1. Генерируется параметр $R = \alpha^k \bmod p$, где k — случайно генерируемое число, $k < q$.

2. Вычисляется значение E : $E = F_H(M \parallel R)$.

3. Вычисляется значение S , такое что $S^2 = k - xE \bmod n$, что обеспечивает выполнение условия $R = \alpha^{S^2} y^E \bmod p$. В качестве ЭЦП берется значение (R, S) .

Проверка подлинности подписи (R, S) осуществляется следующим образом:

1. Вычисляется значение $R^* = \alpha^{S^2} y^E \bmod p$.

2. Вычисляется хэш-функция от сообщения M с присоединенным к нему значением $R^* : E^* = F_H(M \parallel R^*)$. Если $E^* = E$, то подпись признается подлинной.

Взлом модифицированной схемы не может быть осуществлен путем решения только задачи дискретного логарифмирования. Теперь для взлома схемы подписи требуется знать факторизацию числа n . Решение задачи дискретного логарифмирования приводит к вычислению секретного ключа x и возможности вычислить значение $S^2 = k - xE \bmod n$. Однако для вычисления элемента подписи S требуется извлечь квадратный корень из последнего значения. Это требует факторизации модуля n . Построенный алгоритм ЭЦП, использующий две вычислительно трудные задачи, может служить в качестве базового алгоритма для построения протокола слепой подписи, аналогичного схеме слепой подписи, построенной на основе алгоритма ЭЦП Шнорра и описанной в работе [7]. В рамках такого подхода был разработан следующий протокол слепой подписи, взлом которого требует одновременного решения указанных двух трудных задач:

1. Подписывающий отправляет пользователю значение $R = \alpha^k \bmod p$ ($k < n$).

2. Пользователь вычисляет значения $R' = R\alpha^\varepsilon y^\tau \bmod p$ (τ и ε — случайные числа размера $\lambda = 160$ бит), $E' = F_H(M \parallel R')$ и $E = E' - \tau$, после чего отправляет подписывающему значение E (в протоколе предполагается использование 512-битовой хэш-функции F_H).

3. Подписывающий вычисляет значение $D = k - xE \bmod n$, что обеспечивает выполнение условия $R = \alpha^D y^E \bmod p$. Значение D направляется пользователю.

4. Пользователь генерирует случайное число $\mu < n$ (маскирующий множитель), вычисляет значение $D' = \mu^2(D + \varepsilon) \bmod n$ и направляет значение D' подписывающему.

5. Подписывающий проверяет, является ли D' квадратичным вычетом по модулю n . Если нет, то сообщает об этом пользователю и протокол переходит к шагу 2. Если да, то вычисляет значение $D'' = \sqrt{D'} \bmod n$ и направляет его пользователю.

6. Пользователь вычисляет подпись (E', S') , где $E' = E + \tau \bmod n$ и $S' = D'' / \mu \bmod n$, которая является подлинной по отношению к сообщению M .

Процедура проверки ЭЦП в описанном протоколе слепой подписи такая же как и в предыдущей схеме ЭЦП, т. е. используется проверочное уравнение $R^* \equiv \alpha^{S'^2} y^{E'} \bmod p$. В соответствии с шагами 4, 5 и 6 имеем $S'^2 \equiv D'' \mu^{-2} \equiv D' \mu^{-2} \equiv \mu^2(D + \varepsilon) \mu^{-2} \equiv D + \varepsilon \bmod n$. Используя условие $S'^2 = D + \varepsilon \bmod n$, корректность протокола доказывается следующим образом:

$$R^* \equiv \alpha^{S'^2} y^{E'} \equiv \alpha^{D+\varepsilon} y^{E+\tau} \equiv \alpha^D y^E \alpha^\varepsilon y^\tau \equiv R \alpha^\varepsilon y^\tau \bmod n \Rightarrow E^* = E.$$

Проверка, является ли значение D' квадратичным вычетом, выполняемая на шаге 5, требует выполнения нескольких итераций протокола (вероятность того, что D' является квадратичным вычетом по модулю n равна 1/4). Чтобы устранить эту проблему пользователь на шаге 2 может вычислить от 4 до 8 различных значений E , соответствующих различным парам значений (τ, ε) , и одновременно направить их подписывающему. Подписывающий на шаге 3 для каждого из этих значений вычисляет соответствующее значение D . На шаге 4 пользователь для каждого значения D генерирует случайный маскирующий множитель μ и вычисляет значение D' . Все значения D' направляются подписывающему, который находит среди них квадратичный вычет и извлекает из него квадратный корень.

Предложенный протокол обеспечивает анонимность пользователя, предоставляющего документ для получения коллективной подписи вслепую, т. е. в случае получения документа M (и его подлинной подписи к этому документу) подписывающий не сможет однозначно установить, кто конкретно предоставлял данный документ, подписанный им (предполагается, что различные документы предоставлялись некоторой совокупностью пользователей).

С равной вероятностью каждый из пользователей, участвовавших в протоколе слепой подписи, мог предоставлять на подпись документ M . Последнее утверждение следует из того, что любая тройка (R, D, E) из множества таких троек, которые формировались подписывающим, может быть

связана с подписью (E', S') к данному документу M . Действительно, поскольку $R = \alpha^D y^E \bmod p$ (см. п. 3 последнего протокола) и $R' = \alpha^{S'^2} y^{E'} \bmod p$, то выполняется соотношение

$$R'R^{-1} \equiv \alpha^{S'^2 - D} y^{E' - E} \equiv \alpha^\varepsilon y^\tau \pmod{p},$$

следовательно, при равновероятном выборе случайных значений τ и ε подпись (E', S') с равной вероятностью могла быть порождена с участием любого пользователя в процедуре формирования подписи вслепую.

Заключение

В настоящей работе показана возможность эффективной реализации протоколов слепой коллективной подписи и протоколов слепой ЭЦП, взлом которых требует одновременного решения двух различных вычислительно трудных задач. Для построения протоколов последнего типа предложены два конструктивных варианта. Первая конструкция основана на объединении двух различных рандомизированных схем ЭЦП, путем использования единого для обеих схем параметра рандомизации, что позволяет сократить размер подписи по сравнению с формированием вслепую подписей в рамках двух независимых схем ЭЦП. Такой способ позволяет комбинировать задачи дискретного логарифмирования, заданные в произвольных парах конечных групп. Однако он не позволяет так же легко построить протоколы слепой подписи, комбинирующие задачи дискретного логарифмирования и факторизации. Второй тип построения дает вариант такого комбинирования.

Работа поддержана грантом РФФИ № 08-07-00096-а.

СПИСОК ЛИТЕРАТУРЫ

1. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. – Санкт-Петербург, БХВ-Петербург, 2007. 298 с.
2. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory. 1985. Vol. IT-31, No. 4. P. 469–472.
3. Дернова Е.С., Молдовян Н.А. Синтез алгоритмов цифровой подписи на основе нескольких вычислительно трудных задач // Вопросы защиты информации. 2008. № 1. С. 22–26.
4. Schnorr C.P. Efficient signature generation by smart cards // Journal of Cryptology. 1991. Vol. 4. P. 161–174.
5. Гортинская Л.В., Молдовян Д.Н. Основанная на сложности факторизации схема ЭЦП с простым модулем // Вопросы защиты информации, 2005, №4, С. 7–11.
6. Menezes A. J., Vanstone S.A. Handbook of Applied Cryptography. – CRC Press, 1996. – 780 p.
7. Pointcheval D., Stern J. Security arguments for digital signatures and blind signatures // J. Cryptology. 2000. Vol. 13. No 3. P. 361–396.

Гордеев Л.В., Чистяков Ю.В.

Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»
АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

В настоящее время в Российской Федерации в преддверии января 2010 года в связи с необходимостью выполнения требования п.3 ст.25 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» особенно остро встал вопрос организации защиты персональных данных граждан.

Несмотря на то, что, согласно закону Российской Федерации от 05 марта 1992 года №2446-1 «О безопасности» обеспечение безопасности личности по степени важности позиционировано перед обеспечением безопасности общества и государства, вопросы становления системы защиты персональных данных граждан были подняты сравнительно недавно.

В целях регулирования государственной политики по защите конституционных прав и свобод граждан (в части защиты персональных данных) приняты Государственной Думой и одобрены Советом Федерации Федеральные законы «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» и «О персональных данных».

Вопросы методического обеспечения и защиты персональных данных распределены между органами исполнительной власти – Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Федеральной службой безопасности Российской Федерации (ФСБ России) и Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) – в пределах их компетенции.

При создании методической базы защиты персональных данных федеральный орган исполнительной власти (ФСТЭК России), отвечающий за обеспечение защиты информации некриптографическими методами, отошел от устоявшегося подхода к защите информации ограниченного доступа. Требуемые меры защиты персональных данных, указанные в отдельных положениях документов, явно завышены и превышают требования, предъявляемые к защите сведений, составляющих государственную тайну, что не может не сказаться на стоимости их внедрения. Кроме того, новый подход поставил под сомнение легитимность использования «Специальных требований и рекомендаций по технической защите конфиденциальной информации

(СТР-К)» в процессе создания системы защиты персональных данных. Однако в настоящее время полностью отказаться от выполнения требований СТР-К не представляется возможным.

Одним из наиболее распространенных вариантов обработки персональных данных в большинстве организаций является совместное использование кадровыми и финансовыми подразделениями специализированных систем управления базами данных, автоматизирующих процессы ведения кадрового и финансового учета. Особенностью таких автоматизированных систем (информационных систем персональных данных) является совместная обработка как информации, содержащей персональные данные граждан, так и информации, содержащей сведения конфиденциального характера, а в отдельных случаях и сведения, составляющие государственную тайну.

Разделение информации по уровню конфиденциальности, в частности, выделение персональных данных, весьма непростая задача, как для собственников информационных ресурсов, так и для лицензиатов, осуществляющих внедрение системы защиты информации.

Наиболее широко используемыми программными средствами являются «1С», «ПАРУС» и «Галактика». Эти средства позволяют должностным лицам вести автоматизированный учет и анализ данных в пределах их компетенции. Для этого создаются некоторые типовые профили пользователей – «роли», позволяющие каждому легальному пользователю получить доступ к необходимой информации. С точки зрения выполнения основных функций эта, безусловно, необходимая возможность, в то же время, является проблемным местом с точки зрения обеспечения безопасности информации в рамках действующих правовых и нормативных документов.

Суть проблемы состоит в том, что некоторое разграничение полномочий пользователей необходимо и реализуется фактически, что по формальному признаку относит указанные программные средства к категории средств защиты информации от несанкционированного доступа, а это, в свою очередь, вызывает необходимость выполнения требований по сертификации. При этом информационная система попадает в группу многопользовательских автоматизированных систем, пользователи которых имеют различные права на доступ к информации.

В соответствии с требованиями руководящих документов ФСТЭК (Гостехкомиссии) России: «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» и «СТР-К» – класс защищенности автоматизированной системы от НСД к информации должен быть установлен не ниже 1Г.

Согласно требованиям, предъявляемым к средствам защиты информации от НСД, предназначенным для использования в автоматизированных системах указанного класса, эти средства должны быть отнесены к классу не ниже пятого по уровню защищенности от НСД к информации как средство вычислительной техники – в терминах руководящего документа ФСТЭК (Гостехкомиссии) России «Средства вычислительной техники Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» – и к уровню контроля отсутствия не декларированных возможностей не ниже четвертого – в терминах руководящего документа ФСТЭК (Гостехкомиссии) России «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей».

Кроме того, в рамках создания системы защиты персональных данных в сертификате должен быть указан максимально возможный класс с точки зрения защиты персональных данных.

В связи с отсутствием гарантированного разграничением доступа средствами СУБД возникает вопрос о корректности реализации разграничения сертифицированными средствами защиты информации, поскольку вся информация в СУБД, как правило, хранится централизованно в одном файле. При этом средство защиты не способно разграничить доступ пользователей к конкретным данным, находящимся в «контейнере» СУБД. Для устранения указанного недостатка необходимо проводить сертификацию подобного программного обеспечения или разрабатывать и сертифицировать средства защиты информации от несанкционированного доступа, способные интегрироваться в программную среду приложения и, функционируя на уровне ядра СУБД, гарантировать необходимый уровень защищенности информации.

Классификация систем обработки персональных данных является еще одним сложным вопросом. Согласно «Рекомендациям по обеспечению безопасности персональных данных при их обработке в системах персональных данных» выделяются четыре класса типовых информационных систем и специальные информационные системы. К специальным информационным системам относятся информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К типовым классам из общего количества существующих информационных систем относится не более 5%, так как к абсолютному большинству систем кроме требования по обеспечению конфиденциальности предъявляется ряд других требований. Несмотря на отнесение

информационной системы к разряду специальной, для неё необходимо обеспечить выполнение требований ближайшего типового класса.

Особенно неоднозначной является ситуация с классом КЗ, так как согласно действующим документам к этому классу информационных систем не предъявляются требования по обязательной аттестации. Вместо аттестации предлагается проводить процесс декларирования. Однако в настоящее время декларирование фактически не может быть реализовано ввиду того, что декларирование соответствия – это процесс подтверждения соответствия требованиям технического регламента, которого в настоящее время не существует.

Еще одним сложным вопросом, возникающим при создании системы защиты персональных данных, является защита информации от утечки по техническим каналам. В каком-то смысле он «перешел по наследству» от организации работ по созданию системы защиты конфиденциальной информации. В связи с отсутствием нормативно-методических документов в области защиты персональных данных приходится руководствоваться «Сборником временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам». Проблема заключается в том, что в указанном сборнике отсутствуют методики по оценке эффективности применения средств активной защиты информации, что влечет невозможность адекватной оценки достаточности принятых мер.

В данной статье отражены далеко не все проблемы, с которыми приходится сталкиваться при создании системы защиты персональных данных, однако вышеизложенное позволяет сделать вывод о том, что реализация установленных требований представляет собой сложную и дорогостоящую задачу как для операторов персональных данных, так и для специалистов в области защиты информации.

Фактически, созданные и сегодня эффективно функционирующие в большинстве организаций системы защиты информации не способны обеспечить выполнения требований новых руководящих и нормативных документов в области защиты персональных данных. Это, как минимум, потребует внесения существенных изменений в структуру и техническое оснащение существующих систем защиты (с заменой отдельных устройств, целых сегментов, а в ряде случаев – всех технических средств). В качестве примера можно привести необходимость замены периметрового межсетевого экрана на сертифицированный. Может потребоваться также замена свободно распространяемого программного обеспечения информационной системы (например, для некоторых Unix-систем) на коммерческие версии, для которых разработаны сертифицированные средства защиты.

В условиях финансового кризиса далеко не все организации располагают денежными средствами, необходимыми для осуществления указанных мероприятий, что может привести к применению санкций со стороны государства и, как следствие, к банкротству.

Создание и совершенствование системы защиты персональных данных граждан, несомненно, должно являться одной из первоочередных целей государства, однако нецелесообразно не учитывать при этом сложившуюся экономическую ситуацию в стране.

Костин А.А., Дернова Е.С., Молдовян Д.Н.

Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

РЕАЛИЗАЦИЯ ПРОТОКОЛОВ СЛЕПОЙ ПОДПИСИ НА ОСНОВЕ СТАНДАРТОВ

ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 И СТБ 1176.2-99

Введение

Протоколы электронной цифровой подписи (ЭЦП) различного типа широко применяются для аутентификации электронных сообщений и документов. Важным типом таких протоколов является коллективная подпись [1,2]. Протокол коллективной ЭЦП (КЭЦП) позволяет сформировать единую подпись, которая удостоверяет, что заданная совокупность подписывающих действительно подписала заданное сообщение. При этом размер КЭЦП для произвольного числа подписывающих равен размеру обычной индивидуальной подписи. Протоколы КЭЦП впервые были разработаны на основе вычислительно сложной задачи извлечения корней большой простой степени k по модулю

большого простого числа $p = Nk^2 + 1$, где N – четное число и длина чисел k и p составляет не менее 160 и 1024 бит [3]. Затем, используя аналогичное построение были предложены протоколы КЭЦП на основе сложности дискретного логарифмирования [4], включая случай построения базовой процедуры формирования и проверки КЭЦП в соответствии с российскими стандартами ЭЦП [5–7].

Другим важным типом протоколов ЭЦП является слепая подпись, применяемая в ряде криптосистем, в которых решается задача обеспечения неотслеживаемости (анонимности) – в системах тайного электронного голосования и системах электронных денег. Протоколы слепой подписи позволяют подписать электронное сообщение M таким способом, что подписывающий 1) не может ознакомиться с сообщением в процессе выполнения процедур формирования подписи и 2) впоследствии при получении сообщения M и соответствующей этому сообщению подписи не может идентифицировать однозначно пользователя, предоставлявшего данный документ на подпись.

Известные протоколы слепой подписи реализуются на основе алгоритмов ЭЦП, использующих три вычислительно сложные задачи: 1) факторизацию составных чисел вида $n = qr$, где q и r – два больших простых числа [8]; 2) нахождение дискретного логарифма по простому модулю p [9]; 3) нахождение дискретного логарифма на эллиптической кривой (ЭК) специального вида [10].

В работе [11] разработан протокол слепой КЭЦП, основанный на сложности нахождения корней большой простой степени k по простому модулю $p = Nk^2 + 1$. Этот протокол объединяет свойства протоколов КЭЦП и слепой подписи и может найти применение в системах анонимной регистрации электронных документов в коллективных регистрационных центрах, а также в системах тайного электронного голосования. Однако размер КЭЦП, формируемый по этому протоколу достаточно велик и составляет не менее 1184 бит при обеспечении криптостойкости, соответствующей 1024-битовому алгоритму RSA ($\approx 2^{80}$ операций модульного умножения [12]). Для практического применения представляется целесообразным разработка протоколов слепой КЭЦП, в которых размер подписи будет значительно меньше 1000 бит при сохранении исходного значения криптостойкости. Еще большую привлекательность для разработчиков приложений такие протоколы будут представлять в случае их построения с использованием процедур формирования и проверки ЭЦП, рекомендуемых стандартами ГОСТ Р 34.10–94 [13], ГОСТ Р 34.10–2001 [14] и СТБ 1176.2–99 [15].

В настоящей работе рассматриваются протоколы слепой КЭЦП, основанные на сложности задачи дискретного логарифмирования в конечном поле и на ЭК, причем в качестве базового алгоритма ЭЦП в первом случае используется стандарт ЭЦП России ГОСТ Р 34.10–94 и стандарт ЭЦП Беларуси СТБ 1176.2–99, а во втором – ГОСТ Р 34.10–2001. Предварительно на основе этих стандартов строятся протоколы слепой подписи, а затем – протоколы слепой коллективной подписи.

1. Реализация протокола коллективной и слепой подписи на основе ГОСТ Р 34.10–94

Стандарт ЭЦП ГОСТ Р 34.10–94 рекомендует использование простого числа p , такого что $510 \leq |p| \leq 512$ бит либо $1022 \leq |p| \leq 1024$ бит, где $|p|$ – разрядность числа p в двоичном представлении, причем число $p-1$ содержит большой простой делитель q , удовлетворяющий условию $2^{255} \leq q \leq 2^{256}$ либо $2^{511} \leq q \leq 2^{512}$, соответственно. Специфицируемые алгоритмы генерации и проверки ЭЦП используют число $\alpha < p$, такое что $\alpha \neq 1$ и $\alpha^q \bmod p = 1$ (α – генератор подгруппы достаточно большого простого порядка q). Открытый ключ (ОК) y формируется по формуле $y = \alpha^z \bmod p$, где z – личный (секретный) ключ. Вычисление ЭЦП к сообщению M осуществляется следующим образом:

1. Генерируется случайное число k , $1 < k < q$.
2. Вычисляется значение $R = (\alpha^k \bmod p) \bmod q$, являющееся первой частью подписи.
3. По стандарту ГОСТ Р 34.11–94 вычисляется хэш-функция H от M .
4. Вычисляется вторая часть подписи: $S = kH + zR \bmod q$, где z – секретный ключ.

Если $S = 0$, процедура генерации подписи повторяется. Процедура проверки подлинности ЭЦП:

1. Проверяются выполнение условий $r < q$ и $s < q$. Если они не выполняются, то подпись признается недействительной.
2. Вычисляется значение

$$R' = (\alpha^{S/H} y^{R/H} \bmod p) \bmod q. \quad (1)$$

3. Сравниваются значения R и R' . Если $R' = R$, то подпись признается действительной.

Рассмотрим реализацию КЭЦП на основе этого стандарта. Каждый i -й пользователь формирует ОК вида $y_i = \alpha^{z_i} \bmod p$, где z_i – личный (секретный) ключ i -го пользователя, $i = 1, 2, \dots, m$. Коллективным ОК является произведение $y_{\text{кол}} = \prod_{i=1}^{i=m} y_i \bmod p$. Коллективная подпись формируется следующим путем. Каждый подписывающий выбирает разовый, случайный секретный ключ – число k_i , затем вычисляет $R_i = (\alpha^{k_i} \bmod p) \bmod q$ и предоставляет это значение для коллективного использования. Далее вычисляется произведение $R_{\text{кол}} = \prod_{i=1}^{i=m} R_i \bmod q$. Затем каждый пользователь по своему значению R_i и величине H вычисляет свою долю подписи

$$S_i = k_i H + z_i R_{\text{кол}} \bmod q.$$

Коллективной подписью является пара чисел $(R_{\text{кол}}, S_{\text{кол}})$, где $S_{\text{кол}} = \sum_{i=1}^{i=m} S_i \bmod q$.

Проверка коллективной подписи осуществляется по проверочной формуле

$$R' = \left(\alpha^{S_{\text{кол}}/H} y_{\text{кол}}^{R_{\text{кол}}/H} \bmod p \right) \bmod q. \quad (1')$$

Если $R' = R_{\text{кол}}$, то КЭЦП совокупности пользователей $i = 1, 2, \dots, m$ является подлинной, так как она могла быть сформирована только при участии каждого пользователя из этой группы, поскольку для ее формирования требуется использование секретного ключа каждого из них. Отметим, что аутентификация значений R_i осуществляется автоматически при проверке подлинности коллективной ЭЦП: при вмешательстве нарушителя будет получено $R' \neq R_{\text{кол}}$. Легко видеть, что размер КЭЦП не зависит от m . Покажем корректность предложенного алгоритма КЭЦП. Подставив подпись $(R_{\text{кол}}, S_{\text{кол}})$ в проверочное уравнение (1') убеждаемся, что оно выполняется:

$$\begin{aligned} R' &= \left(\alpha^{H^{-1} \sum_{i=1}^{i=m} S_i \left(\prod_{i=1}^{i=m} y_i \right)^{R_{\text{кол}}/H}} \bmod p \right) \bmod q = \left(\prod_{i=1}^{i=m} \alpha^{H^{-1} S_i} \cdot \prod_{i=1}^{i=m} y_i^{R_{\text{кол}}/H} \bmod p \right) \bmod q = \\ &= \left(\prod_{i=1}^{i=m} \left(\alpha^{H^{-1} (k_i H + z_i R_{\text{кол}})} y_i^{R_{\text{кол}}/H} \right) \bmod p \right) \bmod q = \left(\prod_{i=1}^{i=m} \alpha^{k_i} y_i^{H^{-1} R_{\text{кол}}} y_i^{R_{\text{кол}}/H} \bmod p \right) \bmod q = \\ &= \left(\prod_{i=1}^{i=m} ((\alpha^{k_i} \bmod p) \bmod q) \right) \bmod q = \prod_{i=1}^{i=m} R_i \bmod q = R_{\text{кол}}. \end{aligned}$$

При построении протокола слепой подписи на основе стандарта ГОСТ Р 34.10–94 используются два «ослепляющих» множителя, задаваемых в виде y^μ и α^ε , которые использовались при построении схемы слепой подписи на основе алгоритма ЭЦП Шнорра [16]. Кроме того, используется два дополнительных «ослепляющих» параметра τ и δ , что связано со спецификой данного стандарта. Протокол слепой подписи реализуется следующим образом.

1. Подписывающий генерирует случайное число $k < q$, вычисляет $\rho = \alpha^k \bmod p$ и направляет ρ пользователю А, который намерен получить слепую подпись к сообщению M .
2. Пользователь А генерирует случайные значения $\mu, \varepsilon, \delta, \tau \in \{1, 2, \dots, q-1\}$, вычисляет значения $\rho' = \rho^{1/\delta} y^\mu \alpha^\varepsilon \bmod p$, $R' = \rho' \bmod q$, $H = \tau H' \bmod q$ и $R = \delta \tau (R' + \mu H') \bmod q$, где H' – значение хэш-функции от подписываемого документа, вычисленное по процедуре, специфицируемой стандартом ГОСТ Р 34.11–94 (или по другому стойкому алгоритму вычисления хэш-функции, значение которой имеет размер не менее 160 бит). Значение R' , которое остается неизвестным подписывающему, представляет собой первый элемент формируемой подписи.
3. Пользователь А отправляет подписывающему значения R и H , из которых нельзя вычислить ни R' , ни H' , поскольку для любой пары (R', H') существует пара значений (τ, μ) , которые связывают (R', H') с полученной парой значений (R, H) .
4. Подписывающий вычисляет значение $S = kH + zR \bmod q$, где z – его секретный ключ, передает вычисленный элемент слепой подписи пользователю А.
5. Пользователь А вычисляет значение $S' = \delta^{-1} \tau^{-1} S + \varepsilon H' \bmod q$, которое является вторым элементом подписи.

Полученная в соответствии с этим протоколом ЭЦП (R', S') является подлинной, т. е. она вместе с хэш-значением H' от сообщения M проходит уравнение проверки подписи, регламентируемое стандартом ГОСТ Р 34.10–94.

Доказательство корректности протокола. Элемент слепой подписи S вычисляется на шаге 4 по формуле $S = kH + zR \bmod q$, из которой с учетом того, что число α имеет порядок q по модулю p ,

следует справедливость сравнения $\alpha^S \equiv \alpha^{kH} \alpha^{zR} \bmod p$, из которого имеем $\rho \equiv \alpha^k \equiv \alpha^{S/H} \alpha^{-zR/H} \bmod p$. Учитывая, что $R' = (\delta^{-1} \tau^{-1} R - \mu H') \bmod q$, вычислим правую часть проверочного уравнения (1) в случае проверяемой подписи (R', S') и значения хэш-функции H' :

$$\begin{aligned} & \left(\alpha^{\frac{S'}{H'}} y^{\frac{R'}{H'}} \bmod p \right) \bmod q = \left(\alpha^{\frac{\delta^{-1} \tau^{-1} S + \varepsilon H'}{H'}} y^{\frac{\delta^{-1} \tau^{-1} R - \mu H'}{H'}} \bmod p \right) \bmod q = \\ & = \left(\alpha^{\frac{S}{\delta \tau H'} + \varepsilon} y^{\frac{R}{\delta \tau H'} + \mu} \bmod p \right) \bmod q = \left(\left(\alpha^{\frac{S}{H}} y^{\frac{R}{H}} \right)^{1/\delta} \alpha^{\varepsilon} y^{\mu} \bmod p \right) \bmod q = \\ & = (\rho^{1/\delta} y^{\mu} \alpha^{\varepsilon} \bmod p) \bmod q = \rho' \bmod q = R'. \end{aligned} \quad (2)$$

Правая часть проверочного уравнения равна элементу R' проверяемой подписи, следовательно, подпись (R', S') к сообщению M является подлинной.

Рассмотренный протокол обеспечивает анонимность пользователя, предоставляющего документ для получения коллективной подписи вслепую, т. е. при предъявлении подписи (R', S') к сообщению M подписавший не может установить пользователя, который предоставлял ему этот документ на подпись, с вероятностью выше значения d/N , где N – количество документов подписанных (данным подписывающим) с помощью протокола слепой подписи; d – число документов, предоставлявшихся данным пользователем. Это требование выполняется, если любая подпись (R', S') может быть с равной вероятностью отнесена к каждой из N выполненных процедур протокола слепой подписи (предполагается, что все значения, получаемые подписывающим в процессе протокола, регистрируются им). Описанный протокол удовлетворяет этому требованию.

Действительно, любая четверка значений (ρ, R, S, H) из множества таких четверок, которые известны подписывающему, может быть ассоциирована с произвольной подлинной подписью (R', S') к произвольному сообщению, представленному значением хэш-функции H' . Это связано с тем, что четверка (ρ, R, S, H) и тройка (R', S', H') в соответствии с протоколом связаны случайными параметрами μ, ε, δ и τ . Для произвольно заданных четверки и тройки значения μ, ε, δ и τ вычисляются однозначно следующим путем. Вычисляется множитель $\tau = H/H' \bmod q$, значение $\rho' = \alpha^{S/H} y^{R/H} \bmod p$ и логарифм $L = \log_{\alpha} \rho'$ по $\bmod p$ (так как значение ρ' есть целочисленная степень числа α , то указанное значение логарифма существует и является единственным в области $L < q$). Учитывая, что $\log_{\alpha} \rho' = k/\delta + z\mu + \varepsilon$, получаем следующую систему из трех линейных уравнений с тремя неизвестными δ^{-1}, μ и ε :

$$\begin{cases} k\delta^{-1} + z\mu + \varepsilon \equiv L \bmod q, \\ \delta^{-1} R \tau^{-1} - \mu H' \equiv R' \bmod q, \\ \delta^{-1} S \tau^{-1} + \varepsilon H' \equiv S' \bmod q. \end{cases} \quad (3)$$

Вероятность того, что главный определитель этой системы равен нулю, пренебрежимо мала, а именно, равна $q^{-1} < 2^{-160}$. Практически всегда система (3) будет иметь решение. Это означает, что подписывающий может ассоциировать данную тройку (R', S', H') с каждой из сохраненных им (в процессе выполнения протокола слепой подписи) четверок (ρ, R, S, H) . При равновероятном случайном выборе значений δ, ε, μ и τ на шаге 2 протокола тройка (R', S', H') , сформированная по протоколу слепой подписи с равной вероятностью могла бы быть порождена из любой четверки (ρ, R, S, H) , фигурировавшей в одной из выполненных процедур слепого подписания сообщений.

2. Реализация на основе ГОСТ Р 34.10–2001

Стандарт ЭЦП ГОСТ Р 34.10–2001 регламентирует использование простого числа p – модуля ЭК, которая задается в декартовой системе координат уравнением $y^2 = x^3 + ax + b \bmod p$ с коэффициентами a и b – элементами простого поля $GF(p)$; простого числа q – порядка

циклической подгруппы точек ЭК; точки G с координатами (x_G, y_G) , такой что $G \neq O$ и $qG = O$, где O – бесконечно удаленная точка, являющаяся нейтральным элементом (нулем) группы точек ЭК. Секретным ключом является достаточно большое целое число $z < q$, а открытым ключом (ОК) – точка $Q = zG$. Формирование подписи (r, s) осуществляется следующим путем:

1. Генерируется случайное число целое число k , $0 < k < q$.
2. Вычисляется точка $C = kG$ и значение $r = x_C \bmod q$, где x_C – абсцисса точки C .
3. Вычисляется значение $s = (rz + ke) \bmod q$, где $e = H \bmod q$, H – значение хэш-функции от подписываемого сообщения M .

Проверка подписи (r, s) заключается в вычислении координат точки C :

$$C = \left(\frac{s}{e} \bmod q \right) G + \left(\frac{q-r}{e} \bmod q \right) Q, \quad (4)$$

определения значения $r' = x_C \bmod q$ и проверке выполнимости равенства $r' = r$.

Протокол КЭЦП реализуется следующим образом. Каждый i -ый пользователь формирует ОК вида $Q_i = z_i G$, z_i – личный (секретный) ключ и $i = 1, 2, \dots, m$. Коллективным ОК является сумма $Q_{\text{кол}} = Q_1 + Q_2 + \dots + Q_m$.

Коллективная подпись формируется следующим путем. Каждый подписывающий генерирует случайное число k_i , затем вычисляет $C_i = k_i G$ и предоставляет это значение для коллективного использования. Далее вычисляется сумма всех точек C_i : $C = C_1 + C_2 + \dots + C_m$, по которой вычисляется значение $r_{\text{кол}} = x_C \bmod q$. После этого каждый i -ый пользователь по своему секретному ключу z_i и величине e вычисляет свою долю подписи $s_i = (rz_i + k_i e) \bmod q$.

Коллективной подписью является пара чисел $(r_{\text{кол}}, s_{\text{кол}})$, где второй элемент вычисляется по формуле $s_{\text{кол}} = s_1 + s_2 + \dots + s_m \bmod q$.

Проверка КЭЦП осуществляется по проверочной формуле. Если $r' = x_{C'} \bmod q = r$, где точка C' вычисляется по проверочной формуле (4), то КЭЦП пользователей $i = 1, 2, \dots, m$ является подлинной, так как она могла быть сформирована только при участии каждого пользователя, поскольку для ее формирования требуется использование секретного ключа каждого из них.

Протокол слепой подписи реализуется следующим образом.

1. Подписывающий генерирует случайное число k , $0 < k < q$, вычисляет точку ЭК $C = kG$ и направляет ее пользователю А, который намерен получить слепую подпись к электронному сообщению M .

2. Пользователь А генерирует случайные значения $\mu, \varepsilon, \delta, \tau \in \{1, 2, \dots, q-1\}$, вычисляет точку ЭК $C' = (\delta^{-1} \bmod q)C + \mu Q + \varepsilon G$ с координатами $(x_{C'}, y_{C'})$, значения $r' = x_{C'} \bmod q$, $e = e' \tau \bmod q$ и $r = \tau \delta (r' + \mu e') \bmod q$, где $e' = H \bmod q$; H – значение хэш-функции от подписываемого сообщения. Значение r' , которое остается неизвестным для подписывающего, представляет собой первый элемент формируемой подписи.

3. Пользователь А отправляет подписывающему значения r и e , из которых нельзя вычислить ни r' , ни e' , поскольку для произвольной пары (r', e') существует пара значений (τ, μ) , которые связывают (r', e') с полученной парой значений (r, e) .

4. Подписывающий вычисляет значение $s = (rz + ke) \bmod q$, где z – его секретный ключ, передает вычисленный элемент слепой подписи пользователю А.

5. Пользователь А вычисляет значение $s' = (\delta^{-1} \tau^{-1} s + \varepsilon e') \bmod q$, которое является вторым элементом подписи.

Формируемая протоколом ЭЦП (r', s') является подлинной и соответствует сообщению M .

Доказательство корректности протокола. Элемент слепой подписи s вычисляется на шаге 4 по формуле $s = (ke + rz) \bmod q$, из которой с учетом того, что точка G имеет порядок q по модулю p , следует справедливость уравнения $sG = keG + rzG$, из которого имеем $C = kG = e^{-1}sG - e^{-1}rzG$.

Учитывая, что $r' = (\tau^{-1}\delta^{-1}r - \mu e') \bmod q$, вычислим правую часть проверочного уравнения (4) в случае проверяемой подписи (r', s') и значения хэш-функции $H = e'$:

$$\begin{aligned} & \left(\frac{s'}{e} \bmod q \right) G + \left(\frac{q-r'}{e} \bmod q \right) Q = \left(\frac{\tau^{-1}\delta^{-1}s + \varepsilon e'}{e} \bmod q \right) G + \left(\frac{q - \tau^{-1}\delta^{-1}r + \mu e'}{e} \bmod q \right) Q = \\ & = \left(\frac{s}{\delta e'} \bmod q \right) G + \varepsilon G + \left(\frac{q-r}{\delta e'} \bmod q \right) Q + \mu Q = (\delta^{-1} \bmod q) C + \mu Q + \varepsilon G = C' \Rightarrow x_{C'} = r'. \end{aligned}$$

Таким образом, проверочные соотношения базового алгоритма выполняются для подписи (r', s') , т. е. она относится к сообщению M и является подлинной. Рассмотренный протокол обеспечивает анонимность пользователей, предоставляющих электронные сообщения для слепой подписи, поскольку любая предоставляемая подписывающему может быть соотнесена с каждым совершенным им актом формирования слепой подписи. Это можно легко показать, используя схему рассуждений приведенных выше для первого протокола слепой подписи. При этом возникает система из трех линейных сравнений с тремя неизвестными, совпадающая с формулой (3) с точностью до обозначения некоторых коэффициентов при неизвестных.

3. Протоколы слепой коллективной подписи на основе российских стандартов ЭЦП

Протоколы слепой КЭЦП на основе стандартов ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001 были разработаны путем комбинирования протоколов слепой подписи, предложенных в предыдущем разделе и протоколов КЭЦП, описанных ранее в работах [5-7]. Рассмотрим реализацию на основе стандарта ГОСТ Р 34.10-94. Пусть некоторый пользователь А желает подписать вслепую электронное сообщение M у m подписывающих, являющихся владельцами открытых ключей (ОК)

$y_i = \alpha^{z_i} \bmod p$, где z_i – личный секретный ключ i -го подписывающего ($i = 1, 2, \dots, m$). Предполагается, что проверка КЭЦП осуществляется по проверочному уравнению, специфицируемому стандартом ГОСТ Р 34.10-94, за исключением того, что в это уравнение вместо индивидуального ОК подставляется коллективный ОК $y_{\text{КОЛ}}$, представляющий собой произведение ОК всех подписывающих: $y_{\text{КОЛ}} = y_1 y_2 \dots y_m \bmod p$. Выполнение процедуры формирования КЭЦП вслепую обеспечивается с помощью следующего протокола.

1. Каждый i -й подписывающий генерирует случайное число k_i , $1 < k_i < q$, и вычисляет значение $\rho_i = \alpha^{k_i} \bmod p$.

2. Подписывающие вычисляют свертку ρ все своих значений ρ_i в виде произведения $\rho = \rho_1 \rho_2 \dots \rho_m \bmod p$, которую передают пользователю А.

3. Пользователь А генерирует случайные значения $\mu, \varepsilon, \delta, \tau \in \{1, 2, \dots, q-1\}$, вычисляет значения $\rho' = \rho^{1/\delta} y^\mu \alpha^\varepsilon \bmod p$, $R' = \rho' \bmod q$, $H = \tau H' \bmod q$ и $R = \delta \tau (R' + \mu H') \bmod q$, где H' – значение хэш-функции от подписываемого документа. Значение R является первым элементом слепой коллективной подписи, а R' – первым элементом коллективной подписи к сообщению M .

4. Пользователь А отправляет подписывающим значения R и H .

5. Каждый i -й подписывающий вычисляет значение $S_i = k_i H + z_i R \bmod q$, где z_i – его секретный ключ.

6. Подписывающие вычисляют свертку значений S_i в виде суммы $S = S_1 + S_2 + \dots + S_m \bmod q$ и направляют ее пользователю А. Значение S является вторым элементом слепой КЭЦП.

7. Пользователь А вычисляет значение $S' = \delta^{-1} \tau^{-1} S + \varepsilon H' \bmod q$ – второй элемент КЭЦП.

Полученная в соответствии с этим протоколом КЭЦП (R', S') является подлинной.

Доказательство корректности протокола. Элемент S слепой КЭЦП, вычисляемый на шаге 6, может быть представлен в виде

$$S = \sum_{i=1}^{i=m} S_m \bmod q = \sum_{i=1}^{i=m} (k_i H + z_i R) \bmod q = \left(H \sum_{i=1}^{i=m} k_i + R \sum_{i=1}^{i=m} z_i \right) \bmod q.$$

Из последнего соотношения с учетом того, что число α имеет порядок q по модулю p , следует справедливость сравнения

$$\alpha^S \equiv \alpha^{H \sum_{i=1}^m k_i} \alpha^{R \sum_{i=1}^m z_i} \equiv \rho^H y^R \pmod{p},$$

из которого имеем $\rho \equiv \alpha^{S/H} y^{-R/H} \pmod{p}$. Учитывая, что $R' = (\delta^{-1} \tau^{-1} R - \mu H') \pmod{q}$. Вычисление правой части проверочного уравнения (1) в случае проверяемой коллективной подписи (R', S') и значения хэш-функции H' дает соотношения, в точности совпадающие с (2), т. е. Правая часть проверочного уравнения равна элементу R' проверяемой подписи, следовательно, КЭЦП (R', S') к сообщению M является подлинной.

Протокол слепой КЭЦП на основе стандарта ГОСТ Р 34.10–2001:

1. Каждый i -й подписывающий генерирует случайное число k_i ($1 < k_i < q$) и вычисляет точку ЭК $C_i = k_i G$.

2. Подписывающие вычисляют результирующую точку $C = C_1 + C_2 + \dots + C_m$ и направляют ее пользователю А, который намерен получить слепую подпись к электронному сообщению M .

3. Пользователь А генерирует случайные значения $\mu, \varepsilon, \delta, \tau \in \{1, 2, \dots, q-1\}$, вычисляет точку ЭК $C' = (\delta^{-1} \pmod{q})C + \mu Q + \varepsilon G$ с координатами $(x_{C'}, y_{C'})$, значения $r' = x_{C'} \pmod{q}$, $e = e' \tau \pmod{q}$ и $r = \tau \delta (r' + \mu e') \pmod{q}$, где $e' = H \pmod{q}$; H – значение хэш-функции от подписываемого сообщения. Значение r' , которое остается неизвестным подписывающему, представляет собой первый элемент формируемой подписи.

4. Пользователь А отправляет подписывающим значения r и e .

5. Каждый i -й подписывающий вычисляет значение $s_i = k_i e + z_i r \pmod{q}$, где z_i – его личный секретный ключ (это доля i -го подписывающего во втором элементе коллективной подписи).

6. Подписывающие вычисляют значение $s = s_1 + s_2 + \dots + s_m \pmod{q}$, которое является вторым элементом слепой КЭЦП, и передают значение s пользователю А.

7. Пользователь А вычисляет значение $s' = \delta^{-1} \tau^{-1} s + \varepsilon e' \pmod{q}$, которое является вторым элементом КЭЦП.

Подписывающие не могут вычислить пару чисел (r', s') , которая представляет собой подпись полученную пользователем А в результате выполнения протокола слепой КЭЦП. Подпись (r', s') является подлинной и соответствует сообщению M . Корректность последнего протокола легко доказать по аналогии с доказательствами корректности приведенных выше протоколов.

3. Протоколы слепой коллективной подписи на основе стандарта ЭЦП СТБ 1176.2—99

Стандарт ЭЦП Беларуси СТБ 1176.2—99 специфицирует алгоритмы формирования и проверки подписи, заданные над конечной группой, включающей числа $\{1, 2, \dots, p-1\}$, где p – достаточно большое простое число. В качестве групповой операции используется операция “ $\circ$ ”, определенная

следующим выражением $u \circ v = uv\mu^{-1} \pmod{p}$, где $\mu = 2^{l+2}$. Использование операции “ $\circ$ ” вместо обычного умножения по модулю простого числа используется для упрощения реализации умножения по способу Монтгомери, который позволяет значительно уменьшить временную сложность операции возведения в большую степень. Операция возведение в степень k в рассматриваемой подгруппе обозначается $a^{(k)}$ и определяется как $(k-1)$ -кратное выполнение операции “ $\circ$ ” над одним и тем же элементом a , т.е. по формуле $a \circ a \circ \dots \circ a = a^{(k)}$. Стандарт определяет использование l -битового простого числа p , такого что число $p-1$ содержит h -битовый простой делитель q . Стандарт специфицирует 10 уровней стойкости, которым соответствуют согласованные пары значений l и h .

Открытый ключ (ОК) генерируется по формуле $y = a^{(z)}$, где z – секретный ключ ($1 < z < q$) и a – генератор подгруппы порядка q .

Генерация ЭЦП (E, S) к сообщению M выполняется по следующей процедуре:

1. Выработать случайное секретное число $k < q$ и вычислить значение $R = a^{(k)}$.
2. Присоединить к сообщению M значение R , что дает сообщение $M' = R \parallel M$, где знак " $\parallel$ " обозначает операцию конкатенации.
3. Вычислить хэш-функцию E от сообщения M' : $E = F_H(M')$, где F_H – хэш-функция специфицированная стандартом. Значение E представляет собой первый элемент ЭЦП.
4. Вычислить второй элемент цифровой подписи по формуле: $S = (k - zE) \bmod q$.

Процедура проверки подлинности подписи (E, S) описывается следующим образом:

1. Проверить выполнимость условий $1 < S < 2^{h-1}$ и $0 < E < q$ (если хотя бы одно из этих условий не выполняется, то подпись признается недействительной).
2. Вычислить $R^* = a^{(S)} \circ y^{(E)}$ и $E^* = F_H(R^* \parallel M)$. Если $E^* = E$, то подпись верна.

Протокол КЭЦП. Пусть m пользователей, владеющих ОК $y_i = a^{(z_i)}$ ($i = 1, 2, \dots, m$; z_i – личный секретный ключ i -го пользователя) желают подписать документ M с помощью КЭЦП. Предполагается, что проверка КЭЦП осуществляется по проверочному уравнению, специфицируемому стандартом СТБ 1176.2—99, за исключением того, что в это уравнение вместо индивидуального ОК используется коллективный ОК y , представляющий собой произведение индивидуальных ОК всех подписывающих $y = y_1 \circ y_2 \circ \dots \circ y_m$.

Генерация КЭЦП к документу M выполняется следующим образом:

1. Каждый i -й пользователь ($i = 1, 2, \dots, m$) генерирует случайное число $k_i < q$, вычисляет значение $R_i = a^{(k_i)}$ и предоставляет это значение для коллективного использования.
2. Вычисляется произведение $R = R_1 \circ R_2 \circ \dots \circ R_m$, играющее роль общего рандомизирующего элемента, представляющего собой свертку индивидуальных значений R_i ($i = 1, 2, \dots, m$). Вычисление указанного произведения может выполнить один из пользователей и разослать его остальным. Это может сделать каждый пользователь самостоятельно. Выбор одного из этих вариантов не влияет на достигаемый уровень безопасности КЭЦП.
3. Кто-то один из пользователей или каждый из них вычисляет значение $E = F_H(R \parallel M)$. Полученное значение E рассылается всем пользователям, подписывающим документ.
4. Каждый i -й пользователь ($i = 1, 2, \dots, m$) по своему значению k_i , по своему секретному ключу z_i и по значению E вычисляет свою долю в КЭЦП в соответствии со следующей формулой $S_i = (k_i - z_i E) \bmod q$. Все значения S_i рассылаются каждому пользователю.
5. Вычисляется второй параметр S КЭЦП в виде свертки индивидуальных долей S_i по формуле $S = S_1 + S_2 + \dots + S_m \bmod q$.

Коллективной подписью является пара чисел (E, S) . Размер КЭЦП не зависит от числа пользователей, подписавших документ, и равен суммарной длине числа q и значения хэш-функции. Проверка КЭЦП выполняется следующим образом.

1. Проверить выполнимость условий $1 < S < 2^{h-1}$ и $0 < E < q$.
2. Вычислить коллективный ОК в виде свертки $y = y_1 \circ y_2 \circ \dots \circ y_m$ индивидуальных ОК пользователей, участвующих в разделении коллективной подписи (E, S) к сообщению M .
3. Вычислить значения $R^* = a^{(S)} \circ y^{(E)}$ и $E^* = F_H(R^* \parallel M)$. Если $E^* = E$, то КЭЦП признается действительной, в противном случае подпись отвергается.

Схема слепой коллективной подписи. Процедура генерации слепой КЭЦП к документу M выполняется следующим образом:

1. Каждый i -й подписывающий ($i = 1, 2, \dots, m$) генерирует случайное число k_i , $1 < k_i < q$, вычисляет значение $R_i = a^{(k_i)}$ и предоставляет это значение для коллективного использования.
2. Вычисляется произведение $R = R_1 \circ R_2 \circ \dots \circ R_m$, затем R передается пользователю A .

3. Пользователь А генерирует случайные числа $\tau < q$ и $\varepsilon < q$, вычисляет значения $R' = R \circ y^{(\tau)} \circ a^{(\varepsilon)}$, $E' = F_H(R' \parallel M)$ и $E = E' - \tau \bmod q$. Затем он направляет значение E коллективу подписывающих.

4. Каждый i -й подписывающий ($i = 1, 2, \dots, m$) по своему значению k_i , по своему секретному ключу z_i и по значению E вычисляет свою долю в слепой КЭЦП в соответствии со следующей формулой $S_i = (k_i - z_i E) \bmod q$.

5. Вычисляется второй параметр S слепой КЭЦП в виде свертки индивидуальных долей S_i : $S = S_1 + S_2 + \dots + S_m \bmod q$. Затем значение S направляется пользователю А.

6. Пользователь А вычисляет значение $S' = S + \varepsilon \bmod q$.

Пара чисел (E', S') представляет собой подлинную КЭЦП к сообщению M . Докажем корректность протокола, т.е. то, что сформированная КЭЦП (E', S') распознается процедурой проверки как подлинная подпись. В соответствии с процедурой проверки КЭЦП имеем

$$\begin{aligned} R^* &= a^{(S)} \circ y^{(E)} = a^{(\varepsilon + \sum_{i=1}^m S_i)} \circ y^{(E+\tau)} = a^{(\varepsilon)} \circ a^{(\sum_{i=1}^m S_i)} \circ y^{(E)} \circ y^{(\tau)} = \\ &= a^{(\sum_{i=1}^m (k_i - z_i E))} \circ a^{(\varepsilon)} \circ y^{(E)} \circ y^{(\tau)} = a^{(\sum_{i=1}^m k_i)} \circ a^{(-E \sum_{i=1}^m z_i)} \circ y^{(E)} \circ y^{(\tau)} \circ a^{(\varepsilon)} = \\ &= R \circ y^{(\tau)} \circ a^{(\varepsilon)} = R'. \end{aligned}$$

Из условия $R^* = R'$ следует равенство $E^* = E'$, которое означает, что подпись (E', S') признается подлинной.

Рассмотренный протокол обеспечивает анонимность пользователя, предоставляющего документ для получения КЭЦП вслепую, т.е. при предъявлении подписи (E', S') к сообщению M подписавший не может однозначно установить пользователя, который предоставлял ему этот документ на подпись. Действительно, пусть раскрыта КЭЦП (E', S') и соответствующее ей сообщение M . Возьмем произвольную слепую КЭЦП (E, S) и параметр R , которые формировались коллективом подписывающих в процессе выполнения протокола слепой КЭЦП (предполагается, что подписывающие сохраняют значения, которые становятся им известными в процессе выполнения протокола). Для подписей (E', S') и (E, S) выполняются соотношения

$R' = a^{(S')} \circ y^{(E')}$ и $R = a^{(S)} \circ y^{(E)}$, соответственно. Из последних двух соотношений получаем

$R' = R \circ a^{(\varepsilon')} \circ y^{(\tau')}$, где $\varepsilon = S' - S \bmod q$ и $\tau = E' - E \bmod q$ – пара случайных чисел, связывающих заданную раскрытую подпись с произвольной слепой подписью. Поскольку в процессе протокола числа ε и τ генерируются случайно, то все слепые подписи могут быть соотнесены с заданной раскрытой подписью и подписывающие не могут однозначно установить пользователя предоставлявшего на подпись сообщение M , соответствующее раскрытой КЭЦП (E', S') .

Результатом выполненного исследования является расширение функциональности стандартов ЭЦП России и Беларуси.

Работа поддержана грантом РФФИ № 08–07–00096–а.

СПИСОК ЛИТЕРАТУРЫ

1. Молдовян А.А., Молдовян Н.А. Способ формирования и проверки подлинности электронной цифровой подписи, заверяющей электронный документ // Патент РФ № 2356172, МПК H04L 9/30, G09C 1/00. Бюл. № 14 от 20.05.2009.
2. Галанов А.И., Еремеев А.М., Молдовян Н.А. Множественная подпись: новые решения на основе понятия коллективного открытого ключа // Информационно-управляющие системы. 2008. № 1. С. 34–36.
3. Moldovyan N.A. Digital Signature Scheme Based on a New Hard Problem // Computer Science Journal of Moldova. 2008, Vol.16. No.2(47). P.163–182.
4. Молдовян Н.А., Морозова Е.В., Костин А.А., Доронин С.Е. Системы композиционной электронной цифровой подписи // Программные продукты и системы. 2008. № 4. С. 161–164.
5. Ананьев М.Ю., Гортинская Л.В., Костин А.А., Молдовян Н.А. Реализация протокола коллективной подписи на основе стандартов ЭЦП // Известия вузов. Приборостроение. 2009. № 1. С. 26–30.
6. Молдовян А.А., Молдовян Н.А. Новые алгоритмы и протоколы для аутентификации информации в АСУ // Автоматика и телемеханика. 2008. № 7. С.157–169.
7. Ананьев М.Ю., Гортинская Л. В., Молдовян Н.А. Протоколы коллективной подписи на основе свертки индивидуальных параметров // Информационно-управляющие системы. 2008. № 2. С. 22–27.
8. Chaum D. Blind Signatures for Untraceable Payments. Advances in Cryptology: Proc. of CRYPTO'82. Plenum Press, 1983. P. 199–203.
9. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. – Санкт-Петербург, БХВ-Петербург, 2007.-298 с.
10. Koblitz N. Elliptic curve cryptosystems // Mathematics of Computation Advances. 1987. Vol. 48. P. 203–209.

11. Молдовян Н.А., Молдовяну П.А. Новые протоколы слепой подписи // Безопасность информационных технологий. 2007. № 3.
12. International Standard ISO/IEC 14888-3:2006(E). Information technology – Security techniques – Digital Signatures with appendix – Part 3: Discrete logarithm based mechanisms.
13. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. ГОСТ Р 34.10-94. – Госстандарт России. М., Издательство стандартов. 18 с.
14. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. ГОСТ Р 34.10-2001. – Госстандарт России. М., ИПК Издательство стандартов. 12 с.
15. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. 381 с.
16. Pointcheval D., Stern J. Security arguments for digital signatures and blind signatures // Journal of Cryptology. 2000. Vol. 13. No 3. P. 361–396.

Молдовян Д.Н., Дернова Е.С.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
КРИПТОГРАФИЧЕСКИЕ ПРИМИТИВЫ НАД КОНЕЧНЫМИ ВЕКТОРНЫМИ ПРОСТРАНСТВАМИ**

Введение

Синтез быстродействующих схем электронной цифровой подписи (ЭЦП) является актуальной задачей прикладной криптографии. Для ее решения в качестве примитивов алгоритмов ЭЦП были предложены конечные группы векторов [1,2], формируемые в конечномерных векторных пространствах над конечными полями. Вектора размерности m представляются в виде $(a, b, \dots, q)$ или в виде $ae + bi + \dots + qw$, где $e, i, \dots, w$ – формальные базисные вектора; $a, b, \dots, q$ – координаты вектора, являющиеся элементами конечного поля $GF(p^s)$, где p – простое число (характеристика поля) и s – степень расширения поля ($s \geq 1$). Сложение векторов определяется по формуле:

$$(a, b, \dots, q) + (x, y, \dots, z) = (a + x, b + y, \dots, q + z).$$

Одномерные вектора вида εv , где $\varepsilon \in GF(p^s)$ и v – некоторый формальный базисный вектор, представляют собой компоненты вектора. Операция умножения векторов определяется как попарное перемножение всех компонентов векторов-сомножителей по формуле:

$$(ae + bi + \dots + qw) \circ (xe + yi + \dots + zw) = axe \circ e + aye \circ i + \dots + aze \circ w + \\ + bxi \circ e + byi \circ i + \dots + bzi \circ w + \dots + qxw \circ e + qyw \circ i + \dots + qzw \circ w,$$

в которой произведения пар базисных векторов заменяются на однокомпонентный вектор, задаваемый таблицей умножения базисных векторов (ТУБВ), координата которого называется структурным коэффициентом. В случае, когда определенная с помощью ТУБВ операция умножения векторов является ассоциативной, конечное векторное пространство является векторным конечным кольцом (ВКК).

Ранее в качестве примитивов схем ЭЦП рассматривались коммутативные ВКК, формируемые по ТУБВ, обладающими симметрией относительно главной диагонали и задающими коммутативное умножение векторов [3]. Однако некоммутативные ВКК также представляют значительный интерес для синтеза алгоритмов ЭЦП, которые могут быть построены по аналогии со схемами ЭЦП на основе конечных групп матриц [4]. Интерес к некоммутативным группам векторов как примитивам алгоритмов ЭЦП связан с потенциальной возможностью наличия изоморфизма между конечными коммутативными кольцами векторов и конечными кольцами многочленов. При наличии такого изоморфизма атака на алгоритмы ЭЦП, построенные с использованием сложности задачи дискретного логарифмирования в коммутативных группах векторов, может быть полиномиально сведена к атаке на алгоритмы ЭЦП, построенные на основе конечных мультипликативных групп многочленов, причем сложность задачи дискретного логарифмирования в группах последнего типа имеет субэкспоненциальную сложность [5]. Это означает, что построение алгоритмов ЭЦП на основе коммутативных групп векторов потенциально потребует использования векторов достаточно большой длины, что приведет к ограничению производительности алгоритмов ЭЦП на основе коммутативных групп векторов. Однако и в последнем случае существенное ускорение криптографических алгоритмов на основе конечных коммутативных групп над векторными пространствами достигается при возможности распараллеливания вычислений. Для некоммутативных групп векторов указанного изоморфизма не существует, поэтому их исследование в качестве примитивов для синтеза алгоритмов ЭЦП представляет самостоятельный интерес. Кроме того, на основе некоммутативных конечных групп имеется возможность построения криптосистем с открытым ключом нового типа [6, 7], в которых используются вычислительно сложные задачи, отличные от задачи факторизации и дискретного логарифмирования. Строение групп векторов имеет важное значение для синтеза на их основе криптосистем с открытым ключом.

В настоящей работе рассматривается построение ТУБВ, задающих формирование как коммутативных, так и некоммутативных конечных колец векторов. Изучается строение мультипликативной группы колец такого типа и рассматриваются подходы к синтезу на их основе криптоалгоритмов с открытым ключом.

1. Строение мультипликативных групп конечных коммутативных колец векторов

В общем случае коммутативная конечная группа порождается некоторым базисом $\{G_1, G_2, \dots, G_r\}$, где G_r – некоторые элементы группы, имеющие различные значения порядка $\omega(G_i)$, $i = 1, \dots, r$. Базис представляет собой некоторую минимальную систему образующих группы, такую что любой элемент группы может быть представлен единственным способом в виде произведения степеней элементов, входящих в минимальную систему образующих. Вопрос строения группы в смысле описания числа элементов группы всех возможных порядков представляет интерес для выбора конкретных групп в качестве криптографического примитива. Известна теорема о том, что коммутативная группа представима в виде прямого произведения ее примарных подгрупп [5], поэтому получение формулы, описывающее строение примарных подгрупп, позволит описать все случаи строения коммутативных групп векторов. Рассмотрим строение примарных подгрупп для случая, когда известна их минимальная система образующих.

В общем случае базис примарной подгруппы Γ включает μ_i элементов Z_{ij} ($j = 1, \dots, \mu_i$) порядка p^{α_i} , $i = 1, 2, \dots, t$. Порядок такой примарной подгруппы выражается формулой вида

$$\Omega(\Gamma) = (p^{\alpha_1})^{\mu_1} (p^{\alpha_2})^{\mu_2} \dots (p^{\alpha_t})^{\mu_t}.$$

Без потери общности рассмотрения можно считать, что $\alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_t$. Очевидно, что элементы примарной подгруппы могут иметь значения порядков p^γ , где $\alpha_1 \leq \gamma \leq \alpha_t$. Для случая $\gamma = \alpha_1$ для числа элементов порядка p^γ легко выводится формула

$$N_{\omega=p^\gamma} = p^{(\alpha_1-1)\sum_{i=1}^t \mu_i} \left(p^{\sum_{i=1}^t \mu_i} - 1 \right).$$

Пусть $\alpha_{i-1} \leq \gamma \leq \alpha_i$. Элементы рассматриваемой примарной подгруппы, порядок которых равен или меньше p^γ образуют некоторую подгруппу Γ_γ порядка

$$\Omega(\Gamma_\gamma) = (p^{\alpha_1})^{\mu_1} (p^{\alpha_2})^{\mu_2} \dots (p^{\alpha_{i-1}})^{\mu_{i-1}} (p^\gamma)^{\mu_i} (p^\gamma)^{\mu_{i+1}} \dots (p^\gamma)^{\mu_t} = p^{\sum_{k=1}^{i-1} \alpha_k \mu_k + \gamma \sum_{k=i}^t \mu_k}.$$

Элементы рассматриваемой примарной подгруппы, порядок которых равен или меньше $p^{\gamma-1}$, образуют некоторую подгруппу $\Gamma_{\gamma-1}$ порядка

$$\Omega(\Gamma_{\gamma-1}) = (p^{\alpha_1})^{\mu_1} (p^{\alpha_2})^{\mu_2} \dots (p^{\alpha_{i-1}})^{\mu_{i-1}} (p^{\gamma-1})^{\mu_i} (p^{\gamma-1})^{\mu_{i+1}} \dots (p^{\gamma-1})^{\mu_t} = p^{\sum_{k=1}^{i-1} \alpha_k \mu_k + (\gamma-1) \sum_{k=i}^t \mu_k}.$$

Число элементов порядка $\omega = p^\gamma$ найдем как разность значений $\Omega(\Gamma_\gamma)$ и $\Omega(\Gamma_{\gamma-1})$, что дает следующую формулу:

$$N_{\omega=p^\gamma} = p^{\sum_{k=1}^{i-1} \alpha_k \mu_k + (\gamma-1) \sum_{k=i}^t \mu_k} \left(p^{\sum_{k=i}^t \mu_k} - 1 \right)$$

При экспериментальном исследовании строения конечных групп векторов различной размерности для задания операции умножения векторов была использована таблица 1, которая для произвольных значений размерности векторов $m \geq 3$ и произвольных значений структурных коэффициентов ε , τ и λ ($\lambda \neq 0$) обеспечивает свойства ассоциативности и коммутативности.

В выполненном вычислительном эксперименте определялось число векторов, содержащихся в мультипликативной группе векторов, для каждого возможного значения порядка. Вектора задавались над простым полем. Порядок некоторого вектора Z определялся путем последовательного вычисления значений Z^i для последовательно возрастающих значений $i = 1, 2, \dots, \omega$. В качестве

порядка вектора Z принималось значение ω , при котором имеет место равенство $Z^\omega = E$, где $E = (\lambda^{-1}, 0, 0, \dots, 0)$ – единичный элемент группы векторов. Кроме вариантов операции умножения, задаваемых таблицей 1, было исследовано строение групп векторов и для случая коммутативного векторного умножения, задаваемого с помощью ТУБВ с большим числом других распределений структурных коэффициентов. Во всех случаях строение оказывалось идентичным одному из строений, получаемых с помощью таблицы 1 при соответствующем выборе набора значений структурных коэффициентов.

Таблица 1

Общий тип таблицы умножения базисных векторов (ТУБВ)

$\circ$	e	i	j	k	u	v	...	...	z
e	λe	λi	λj	λk	λu	λv	$\lambda \dots$	$\lambda \dots$	λz
i	λi	εj	εk	εu	εv	$\varepsilon \dots$	$\varepsilon \dots$	εz	$\varepsilon \tau \lambda^{-1} e$
j	λj	εk	εu	εv	$\varepsilon \dots$	$\varepsilon \dots$	εz	$\varepsilon \tau \lambda^{-1} e$	τi
k	λk	εu	εv	$\varepsilon \dots$	$\varepsilon \dots$	εz	$\varepsilon \tau \lambda^{-1} e$	τi	τj
u	λu	εv	$\varepsilon \dots$	$\varepsilon \dots$	εz	$\varepsilon \tau \lambda^{-1} e$	τi	τj	τk
v	λv	$\varepsilon \dots$	$\varepsilon \dots$	εz	$\varepsilon \tau \lambda^{-1} e$	τi	τj	τk	τu
...	$\lambda \dots$	$\varepsilon \dots$	εz	$\varepsilon \tau \lambda^{-1} e$	τi	τj	τk	τu	τv
...	$\lambda \dots$	εz	$\varepsilon \tau \lambda^{-1} e$	τi	τj	τk	τu	τv	$\tau \dots$
z	λz	$\varepsilon \tau \lambda^{-1} e$	τi	τj	τk	τu	τv	$\tau \dots$	$\tau \dots$

Примечание: В таблице: 1. $\varepsilon, \tau, \lambda \in GF(p^s)$ – структурные коэффициенты ($\lambda \neq 0$);

2. $GF(p^s)$ – конечное поле, над которым определено конечномерное векторное пространство.

В таблице 2 представлены экспериментальные результаты для некоторых частных случаев строения групп векторов. Установлено, что минимальная система образующих коммутативных групп векторов включает от одного до m элементов в зависимости от выбранных значений структурных коэффициентов. Если минимальная система образующих включает векторы, имеющие одинаковый порядок, то порождаемая ими группа характеризуется как имеющая однородное циклическое строение. Если минимальная система образующих включает векторы, имеющие различные порядки, то порождаемая ими группа характеризуется как имеющая неоднородное циклическое строение. Изучая полученные экспериментальные результаты и выделяя значения порядков элементов, принадлежащих примарным подгруппам, легко синтезировать формулы, приведенные в последней строке таблицы 2 и описывающие порядок группы. Правильность полученной формулы подтверждается следующей проверкой: $\sum_{\omega} N_{\omega} = \Omega - 1$.

Таблица 2

Примеры строения конечных групп векторов с неоднородной многомерной циклическостью

$m = 10; p = 5; \varepsilon = 3$		$m = 8; p = 13; \varepsilon = 9$		$m = 7; p = 11; \varepsilon = 3$	
ω	N_{ω}	ω	N_{ω}	ω	N_{ω}
2	1	2	63	2	7
3	2	3	728	5	124
4	2	4	4032	7	48
5	390624	6	45864	10	868
6	2	7	48	14	336
8	4	8	12288	19	360
10	390624	12	2935296	35	5952
12	4	14	3024	38	2520
15	781248	21	34944	70	41664
20	781248	24	8945664	95	44640
24	8	28	193536	133	17280
30	781248	42	2201472	190	312480
40	1562496	56	589824	266	120960
60	1562496	84	140894208	665	2142720
120	3124992	168	429391872	1330	14999040
$\Omega = p^8(p^2 - 1)$		$\Omega = (p-1)^4(p^2 - 1)^2$		$\Omega = (p-1)(p^3 - 1)^2$	

2. Задание некоммутативных конечных колец векторов и строение их мультипликативной группы

Общим способом построения ТУБВ, обеспечивающих ассоциативность умножения m -мерных векторов, является использование таблиц Кэли для групп порядка m . Такие таблицы, используемые в качестве ТУБВ, обеспечивают ассоциативность операции векторного умножения. Затем в определенные клетки такой (исходной) ТУБВ вносятся структурные коэффициенты так, чтобы сохранилось свойство ассоциативности векторного умножения. Для заданной исходной ТУБВ обычно можно найти много различных вариантов распределения структурных коэффициентов, сохраняющих свойство ассоциативности. Это позволяет по одной таблице Кэли построить достаточно большое число ТУБВ. Некоммутативных групп порядка 4 не существует, поэтому для этого случая использовалась симметричная исходная ТУБВ, в которую вносилось несимметричное распределение структурных коэффициентов. За счет последнего достигалась некоммутативность ассоциативного умножения четырехмерных векторов. Пример такого построения дает табл. 3 при $\varepsilon = -1$ и $\rho = 1$ или при $\mu = -1$ и $\varepsilon = 1$. При других значениях структурных коэффициентов μ и ε не выполняется ассоциативность, а при $\rho = -1$ и $\varepsilon = -1$ таблица становится симметричной относительно главной диагонали, что задаст коммутативность векторного умножения. На указанные два варианта «некоммутативного» распределения структурных коэффициентов можно наложить симметричные распределения других структурных коэффициентов A, B и $C \in GF(p^s)$ (см. табл. 4), которые могут принимать произвольные значения при сохранении исходной некоммутативности операции умножения векторов.

Таблица 3

Задание некоммутативной ТУБВ для случая $m = 4$

Базисные векторы	Базисные векторы			
	e	i	j	k
e	e	i	j	k
i	i	$\rho \varepsilon e$	ρk	εj
j	j	εk	$\rho \varepsilon e$	ρi
k	k	ρj	εi	$\rho \varepsilon e$

Таблица 4

Задание некоммутативной ТУБВ с дополнительными структурными коэффициентами, распределенными симметрично

Базисные векторы	Базисные векторы			
	e	i	j	k
e	e	i	j	k
i	i	$-ACe$	Ak	$-Cj$
j	j	$-Ak$	$-ABe$	Bi
k	k	Cj	$-Bi$	$-BCe$

Другим способом задания некоммутативного векторного умножения является применение несимметричных исходных ТУБВ, которые не связаны с табличным заданием групповой операции. Если такие ТУБВ существуют, то их достаточно легко можно найти с помощью компьютерного перебора. Пример таких ТУБВ представлен в таблице 5, где при структурном коэффициенте, равном нулю, не указано никаких базисных векторов, так как это не изменяет задаваемую операцию умножения. Наличие ТУБВ данного типа для случая $m = 4$ подсказывает, что они могут иметь место и при некоторых других значениях размерности векторов.

Таблица 5

Специальный вариант ТУБВ для четырехмерных векторов ($A \neq 0$)

Базисные векторы	Базисные векторы			
	e	i	j	k
e	Ae	Ai	0	0
i	0	0	$A^{-1}e$	i
j	Aj	k	0	0
k	0	0	j	k

При четных размерностях векторов $m \geq 6$ может быть применен следующий общий способ построения таблиц Кэли, задающих над множеством базисных векторов некоммутативные группы порядка m . В первой строке слева направо записываются базисные вектора в некоторой исходной последовательности. В первом столбце сверху вниз записывается та же последовательность базисных

векторов. В каждой четной строке базисные вектора записываются, начиная с элемента, указанного в первом столбце, в обратной последовательности (относительно исходной последовательности). Такая таблица может использоваться в качестве исходной несимметричной ТУБВ, задающей некоммутативную и ассоциативную операцию умножения m -мерных векторов. В данную ТУБВ могут быть внесены структурные коэффициенты различными способами. Для ТУБВ данного типа имеется общий способ внесения структурных коэффициентов, сохраняющих свойство ассоциативности операции умножения для произвольных четных значений m . Этот способ состоит в том, что заданный структурный коэффициент

A вносится в каждую клетку, находящуюся на пересечении четной строки и четного столбца. Такое распределение обеспечивает свойство ассоциативности умножения при произвольном значении $A \in GF(p^s)$. Таблица 6 дает пример реализации описанного общего построения для случая $m = 8$.

Возможны и другие типы распределений структурных коэффициентов в описанной выше исходной некоммутативной ТУБВ общего вида, в том числе и несимметричные распределения. Однако несимметричные распределения были найдены только для структурного коэффициента равного минус единице. Пример таких распределений для случая $m = 6$ дает табл. 7, где симметрично распределенный коэффициент A может принимать любое значение в базовом поле $GF(p^s)$, а несимметрично распределенные коэффициенты ρ, β, τ и ε – только значения 1 и -1 , поскольку при других значениях этого коэффициента нарушается свойство ассоциативности операции умножения векторов (возможны и другие несимметричные распределения коэффициентов, равных -1). Существуют также некоммутативные исходные ТУБВ (см., например, табл. 8), которые не представляют собой таблицу Кэли для некоторой некоммутативной группы. Однако такие варианты построения некоммутативных ТУБВ, видимо, ограничены частными значениями четных размерностей векторов.

Таблица 6

Общий способ построения некоммутативных ТУБВ для четных значений размерности векторов

$\circ$	e	i	j	k	u	v	w	x
e	e	i	j	k	u	v	w	x
i	i	Ae	x	Aw	v	Au	x	Ax
j	j	k	u	v	w	x	e	i
k	k	Aj	i	Ae	x	Aw	v	Au
u	u	v	w	x	e	i	j	k
v	v	Au	k	Aj	i	Ae	x	Aw
w	w	x	e	i	j	k	u	v
x	x	Aw	v	Au	k	Aj	i	Ae

Таблица 7

Несимметричные распределения структурных коэффициентов $\rho, \beta, \tau, \varepsilon \in \{1, -1\}$, наложенные на симметричное

распределение коэффициента $A \in GF(p^s)$, для случая $m = 6$

$\circ$	e	i	j	k	u	v
e	e	i	j	k	u	v
i	i	$\tau\beta Ae$	$\varepsilon\tau\beta\rho v$	$\tau\beta Au$	k	$\varepsilon\rho Aj$
j	j	$\varepsilon\tau k$	τu	$\varepsilon\beta\rho v$	$\varepsilon\tau e$	$\varepsilon\tau\beta\rho i$
k	k	$\varepsilon\beta Aj$	$\varepsilon\tau i$	$\tau\beta Ae$	$\tau\beta\rho v$	ρAu
u	u	$\beta\rho v$	$\varepsilon\tau e$	i	εj	$\tau\beta\rho k$
v	v	$\tau\rho Au$	$\varepsilon\beta\rho k$	$\varepsilon\tau\rho Aj$	$\beta\rho i$	$\tau\beta Ae$

Таблица 8

Специальный случай некоммутативной исходной ТУБВ для $m = 8$

$\circ$	e	i	j	k	u	v	w	x
e	e	i	j	k	0	0	0	0
i	i	e	k	j	0	0	0	0
j	0	0	0	0	e	i	j	k
k	0	0	0	0	i	e	k	j
u	u	v	w	x	0	0	0	0
v	v	u	x	w	0	0	0	0
w	0	0	0	0	u	v	w	x
x	0	0	0	0	v	u	x	w

С целью изучения строения некоммутативных конечных групп векторов были выполнены вычислительные эксперименты, в которых определялось число векторов N_ω , имеющих некоторый заданный порядок ω . Эксперименты выполнялись для различных значений характеристики базового поля (т.е. для различных значений p), различных размерностей и различных ТУБВ. Значение порядка вектора определялось путем многократного умножения вектора на самого себя до тех пор, пока не будет получено значение единичного вектора. Число выполненных умножений λ задавало значение порядка вектора $\omega = \lambda + 1$. В случае колец четырехмерных векторов, задаваемых по таблицам 4 и 5, установлено, что при заданном значении p и $s=1$ строение не зависит от выбора ненулевых значений структурных коэффициентов A , B и C . Типичное строение некоммутативных групп векторов в этом случае представлено в табл. 9.

Случай шестимерных векторов был исследован для варианта задания операции векторного умножения по табл. 7 при $\varepsilon = \tau = \beta = \rho = 1$ и различных значениях коэффициента A . Установлены два типа строения таких некоммутативных групп векторов, один из которых имеет место при значении A , являющемся квадратичным вычетом по модулю p , а второй – в случае, когда A является квадратичным невычетом.

В результате обобщения экспериментальных результатов установлено, что рассмотренные варианты некоммутативных групп векторов содержат элементы, порядок которых ω равен нетривиальным делителям чисел $(p-1)p$ и p^2-1 (для случая $m=4$) и $(p^2-1)p$ (для случая $m=6$).

Таблица 9

Строение частных вариантов некоммутативных групп векторов (N_ω – число элементов порядка ω)

$m = 4$; табл. 4; $A \neq 0, B \neq 0$				$m = 6$; табл. 7 $\varepsilon = \mu = \beta = \alpha = 1$			
$p = 13$		$p = 37$		$p = 11$; $A = 1, 3, 4, 5$		$p = 11$; $A = 2$	
ω	N_ω	ω	N_ω	ω	N_ω	ω	N_ω
2	183	2	1407	2	535	2	267
3	548	3	4220	3	110	3	332
4	912	4	7032	4	440	4	708
6	2004	6	15468	5	33124	5	6624
7	468	8	2664	6	770	6	1524
8	312	9	46404	8	880	8	2736
12	8376	12	64680	10	561340	10	5268
13	168	18	147636	11	120	11	120
14	468	19	11988	12	880	12	5376
21	936	24	5328	15	13640	15	21168
24	624	36	598968	20	54560	20	69792
26	168	37	1368	22	840	22	360
28	936	38	11988	24	1760	24	21312
39	336	57	23976	30	95480	30	128976
42	936	72	15984	40	109120	33	240
52	336	74	1368	55	14880	40	171264
56	1872	76	23976	60	109120	44	480
78	336	111	2736	110	104160	55	2880
84	1872	114	23976	120	218240	60	274624
156	672	148	2736	-	-	66	720
168	3744	152	47952	-	-	88	960
-	-	171	71928	-	-	110	8640
-	-	222	2736	-	-	120	722688
-	-	228	47952	-	-	132	960
-	-	333	8202	-	-	165	5760
-	-	342	71928	-	-	220	11520
-	-	444	5472	-	-	264	1920
-	-	456	95904	-	-	330	17280
-	-	666	8202	-	-	440	23040
-	-	684	143856	-	-	660	23040
-	-	1332	16416	-	-	1320	46080
-	-	1368	287712	-	-	-	-

3. Реализация криптосхем с открытым ключом

Одним из способов синтеза криптосистем с открытым ключом на основе некоммутативных конечных групп является использование их подгрупп, обладающих остаточным простым порядком. Такие подгруппы являются циклическими, а групповая операция в них коммутативна. В этом случае синтез криптосхем, основанных на сложности задачи дискретного

логарифмирования, аналогичен синтезу в случае коммутативных групп. Обоснованием данного подхода является ожидание, что сведение задачи дискретного логарифмирования в циклической подгруппе некоммутативной группы к задаче дискретного логарифмирования в конечном поле или конечном кольце многочленов будет невозможным. В частных случаях такое сведение возможно, поэтому требуется выполнить выбор подгрупп, обладающих соответствующим значением простого порядка.

Более интересным является подход, использующий задачу вычисления элемента некоммутативной группы X и числа x (пара этих элементов служит секретным ключом) в уравнении $Y = X \circ G^x \circ X^{-1}$, где пара умножений на взаимно обратные элементы X и X^{-1} реализует операцию автоморфизма; G – элемент достаточно большого простого порядка; Y – элемент группы, используемый в качестве открытого ключа (последние два элемента считаются известными). Решение этого уравнения представляет собой самостоятельную трудную вычислительную задачу, отличную от задачи дискретного логарифмирования. При известном X возникает задача дискретного логарифмирования $Y' = X^{-1} \circ Y \circ X = G^x$. Ожидается, что при известном x сравнительно легко вычислить X . Однако одновременное нахождение X и x является сложной задачей, несмотря на то, что существует очень большое число различных решений (если X и x – некоторое решение, то для произвольного элемента группы λ , коммутирующего со всеми другими элементами, пара λX и x также является решением).

Схема открытого согласования ключа на основе предлагаемой задачи описывается следующим образом. Пусть два удаленных абонента имеют открытые ключи $Y_1 = X_1 \circ G^{x_1} \circ X_1^{-1}$ и $Y_2 = X_2 \circ G^{x_2} \circ X_2^{-1}$, где (X_1, x_1) и (X_2, x_2) – личные секретные ключи первого и второго абонентов, такие что $X_1 \circ X_2 = X_2 \circ X_1$. После открытого обмена открытыми ключами первый абонент вычисляет общий секретный ключ по формуле $K_{12} = X_1 \circ Y_2^{x_1} \circ X_1^{-1}$, а второй – по формуле $K_{21} = X_2 \circ Y_1^{x_2} \circ X_2^{-1} = K_{12}$. Комбинируя аналогичным образом операцию автоморфизма и операцию возведения в большую дискретную степень, можно построить алгоритмы коммутативного и открытого шифрования. Техническим вопросом является согласование секретных значений X_1 и X_2 , который решается заданием дополнительного известного элемента Q , такого что $Q \circ G \neq G \circ Q$, который также обладает большим простым порядком. В этом случае открытый ключ вычисляется как

$$Y = Q^w \circ G^x \circ Q^{-w},$$

где (w, x) – личный секретный ключ. В случае, когда порядки элементов Q и G равны большому простому числу q , имеющего размер $|q|$ бит, вычисление пары неизвестных (w, x) может быть выполнено методом, аналогичным методу больших и малых шагов [5], с трудоемкостью $2^{|q|}$ операций возведения в степень. Из этой оценки следует, что рассмотренная схема открытого согласования ключа имеет приемлемую для практического применения криптостойкость при $q \geq 2^{80}$.

Работа поддержана грантом РФФИ № 08-07-00096-а.

СПИСОК ЛИТЕРАТУРЫ

1. Молдован Д.Н., Молдован Н.А. Способ формирования и проверки подлинности электронной цифровой подписи, заверяющей электронный документ // Патентная заявка РФ от 25.12.2007. № 2007147826/09(052419).
2. Молдован Н.А. Алгоритмы аутентификации информации в АСУ на основе структур в конечных векторных пространствах // Автоматика и телемеханика. 2008. № 12. С. 163–177.
3. Дернова Е.С., Молдован Д.Н., Молдовану П.А. Синтез конечных расширенных полей для криптографических приложений // Вопросы защиты информации. 2008. № 3(82). С. 2–7.
4. Дернова Е.С., Костина А.А., Молдовану П.А. Конечные группы матриц как примитив алгоритмов цифровой подписи // Вопросы защиты информации. 2008. № 3(82). С. 8–12.
5. Menezes A. J., Vanstone S.A. Handbook of Applied Cryptography. – CRC Press, 1996. – 780 p.
6. K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang, C. Park. New Public Key Cryptosystems Using Braid Groups // Advances in Cryptology – Crypto 2000 / Lecture Notes in Computer Science. Springer-Verlag, 2000. Vol. 1880. P. 166–183.
7. E. Lee, J.H. Park. Cryptanalysis of the Public Key Encryption Based on Braid Groups // Advances in Cryptology – Eurocrypt 2003 / Lecture Notes in Computer Science. Springer-Verlag, 2003. Vol. 2656. P. 477–489.

Харинов М.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
СЕГМЕНТАЦИЯ ИЗОБРАЖЕНИЯ С СОХРАНЕНИЕМ ЗРИТЕЛЬНОГО ОБРАЗА**

Введение

Сегментация является ключевой процедурой обработки изображений и, тем не менее, относится к недостаточно формализованным понятиям, поскольку непосредственно связана с интерпретацией зрительного восприятия. В широком смысле под сегментацией понимается упрощение изображения для автоматизированной обработки, например, за счет увеличения повторений элементарных сегментов изображения (пикселей), которое существенно не меняет его восприятия в целом, но позволяет нивелировать различия между пикселями объектов. В узком смысле под сегментацией понимается вычисление (моделирование) сегментов, занимаемых объектами, которые на изображении видит человек.

На практике для адекватной сегментации, как в первом, так и во втором случае обычно требуется в той или иной степени описать конкретные объекты, для анализа которых используется данная техническая система обработки изображений. Привлечение априорных предположений об объектах заведомо ограничивает возможности машинного зрения по сравнению со зрительным восприятием человека и препятствует решению задач, связанных с анализом произвольных изображений, как например, при стеганографическом встраивании и обнаружении скрытых сообщений [1]. Поэтому формализация понятия сегментации независимо от конкретного содержания изображения, а также развитие методов сегментации и выделения объектов, применимых в различных задачах и к сигналам различной природы (изображениям, аудиосигналам и др.) является одним из актуальных направлений исследований в современной обработке сигналов.

1. Сегментация изображений с сохранением зрительного образа

В задачах, связанных с автоматизированным анализом и распознаванием, сегментация является характерной стадией первоначальной обработки изображений, в результате которой пиксели группируются в составные сегменты, рассматриваемые вместо отдельных исходных элементов сигнала при продолжении обработки. В настоящее время известны тысячи подобных алгоритмов, которые применяются в различных приложениях. Развиваются алгебраические методы комбинирования и отбора алгоритмов для автоматизации решения новых прикладных задач [2]. С другой стороны, в связи с расширением множества алгоритмов, возникает проблема их унификации или нахождения общих правил, которыми полезно руководствоваться при создании новых алгоритмов сегментации.

Требуемые правила получаются, если трактовать сегментацию как один из двух противоположных процессов преобразования информации — процесса ее формирования при записи в сигнал некоторого «сообщения» [3] и процесса фильтрации информации при ее извлечении в виде упрощенного (сегментированного) сигнала для дальнейшего анализа и распознавания. Для обсуждаемых процессов устанавливаются общие алгебраические свойства преобразования информации. Первое свойство состоит в идемпотентности преобразования сигнала, которая в приложении к сегментации означает, что повторная сегментация не меняет однажды сегментированный сигнал. Второе свойство состоит в том, что сегментация сохраняется также при преобразовании сигнала в инвариантное представление [4], которое не зависит от предусмотренных линейных и нелинейных преобразований изображения и получается из него идемпотентным изотонным преобразованием H , сохраняющим порядок значений пикселей.

В отношении преобразования изображения при записи сообщения указанные свойства обсуждаются в [3], а в приложении к сегментации описываются коммутационными соотношениями:

$$H^2 = H, \quad S^2 = S, \\ SHS = HS,$$

где S — преобразование изображения в сегментированное представление.

Под H и S удобно понимать программы преобразования изображения в инвариантное и сегментированное представление, соответственно.

Смысл идемпотентности сегментации S прозрачен и состоит в том, что при повторной фильтрации информации изображения оно не меняется, поскольку уже не содержит избыточной информации. Кроме того, благодаря выписанным коммутационным соотношениям чередование сегментации с преобразованием изображения в инвариантное представление не приводит к закликиванию, что позволяет работать с сегментированным изображением в инвариантном представлении и обеспечивает устойчивость результата сегментации по отношению к определенным искажениям изображения.

Согласно коммутационным соотношениям в качестве тривиального варианта сегментации S может рассматриваться преобразование H , порождающее последовательность представлений

изображения в различном числе градаций [3, 4]. Однако преобразование H в инвариантное представление вычисляется по гистограмме, которая не зависит от порядка чередования отсчетов в изображении, и поэтому в качестве алгоритма сегментации недостаточно эффективно. Тем не менее, оно позволяет определить инвариантную близость между элементами сигнала, зависящую только от порядка отсчетов по величине, и тем самым обеспечивает возможность разработки унифицированных алгоритмов сегментации с учетом пространственного чередования элементов сигнала. При этом, в отличие от преобразования H , к алгоритмам сегментации S не предъявляется условия коммутативности с преобразованием изображения из позитива в негатив.

Пример результатов обработки стандартного изображения «Лена» (<http://sipi.usc.edu/database/>) по алгоритму, удовлетворяющему требуемым коммутационным соотношениям, демонстрируется на рисунке 1.



Рис. 1. Сегментация изображения с сохранением зрительного образа

На рисунке 1 слева показано исходное изображение. В центре и справа показаны результаты сегментации исходного изображения и изображения в негативном представлении.

В обоих случаях обеспечивается выраженная сегментация изображения с сохранением зрительного образа, что проявляется наглядно и выражается в сохранении целостности воспринимаемого образа изображения, а также образов объектов. Характерно, что на центральном и правом изображениях сегментация объектов выполняется по-разному. Если в одном представлении объект выделяется как целое, то на другом разделяется на части. На каком именно, — зависит от объекта (рисунок 1). Подобные преобразования изображения несложно выполнить, если видеть объекты, и обратно, сегментация изображений с различной детализацией объектов может оказаться полезной при компьютерном моделировании зрительного восприятия для автоматической идентификации объектов по признаку «часть–целое».

Предлагаемый алгоритм сегментации мы относим к обозначившемуся в последнее время классу алгоритмов, решающих проблему моделирования, так называемой, подпороговой («perceptual», «preattentive») сегментации [5], которая предшествует выделению объектов и исследуется в контексте моделирования как зрительного, так и слухового восприятия. К основным техническим требованиям, предъявляемым к алгоритмам подпороговой сегментации, относятся:

- применимость к любому изображению независимо от его конкретного смыслового содержания;
- отсутствие управляющих параметров (ориентировочного числа сегментов, предельного числа итераций и пр.);
- высокая скорость обработки, сравнимая с выполнением пороговых преобразований изображения.

Первое требование означает, что для создания эффективных алгоритмов сегментации желательно опираться не на признаки объектов конкретной предметной области, а прибегать к общим предположениям, в качестве которых мы используем соображения инвариантности и правила коммутации алгоритмов преобразования сигнала. Второе требование, по существу, является условием для начальных версий алгоритмов подпороговой сегментации. При этом вопрос о параметризации целесообразно решать по мере обнаружения классов изображений, для которых рассматриваемые алгоритмы оказываются неэффективными. Третье условие выражает роль алгоритмов подпороговой сегментации, предназначенных для грубого, предварительного распознавания, которое утрачивает практический смысл, если занимает продолжительное время.

Скорость для алгоритмов сегментации является одним из наиболее важных параметров. При моделировании подпороговой сегментации условие быстродействия существенно ограничивает применение ресурсоемкой обработки изображений. В общем случае сегментации изображений для выделения объектов условие быстродействия обязывает предусмотреть оптимизацию вычислений, обеспечивающую моделирование зрительного восприятия на современных компьютерах, которые по памяти и быстродействию, по всей видимости, значительно превосходят возможности человека.

2. Адекватная сегментация изображения

Прежде, чем сравнивать автоматическое выделение объектов с объектами, доступными зрительному восприятию человека, полезно представлять объекты, которые «видит» техническая система при той или иной реализации алгоритмов сегментации. В этом случае, задача распознавания сводится к обнаружению и отбору характерных сегментов объектов из числа сегментов изображения, устойчиво выделяемых технической системой и оцениваемых с точки зрения адекватности зрительному восприятию.

Если содержание изображения и изображенные на нем объекты не предполагаются заранее известными, то перечисление объектов, выделяемых технической системой, можно описать посредством приближений изображения представлениями с последовательно возрастающим числом сегментов (рисунок 2).

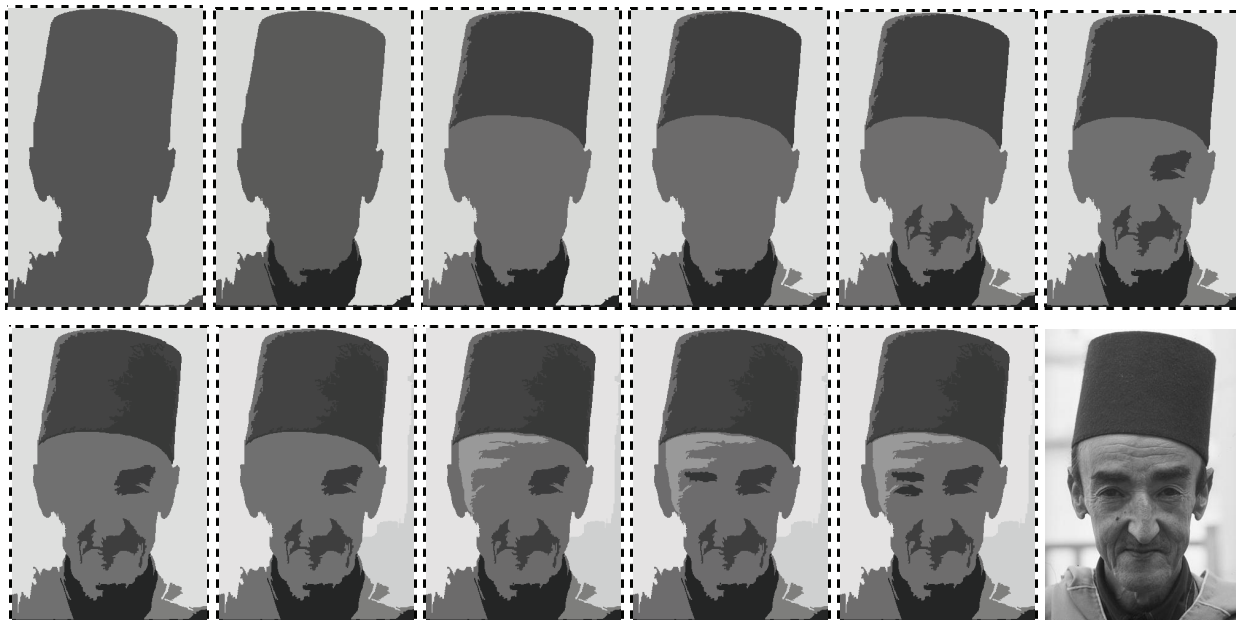


Рис. 2. Приближения изображения с возрастающим числом сегментов

На рисунке 2 в правом нижнем углу показано изображение из Берклиевской базы данных (Berkely Segmentation Dataset, <http://www.eecs.berkeley.edu/Research/Projects/CS/vision/bsds/>), в которой систематизируются результаты, полученные в экспериментах с человеком. Остальные изображения в первом и втором рядах иллюстрируют последовательность приближений изображения представлениями из 2–12 сегментов.

Обсуждаемые приближения получаются разбиением изображения на заданное число сегментов с последующим замещением значений пикселей средним значением яркости, вычисленным для данного сегмента. Каждое последующее приближение отличается от предыдущего одним сегментом. При сравнении представлений с различными номерами возникает аналогия с известной художественной головоломкой «Найди десять отличий», для которой изготавливаются пары похожих изображений путем удаления или добавления к одному из них малозаметных объектов. В данном случае процесс создания подобных изображений выполняется автоматически. При этом «отличия» описывают объекты, которые выделяет или «видит» автоматизированная система.

Для воспроизведения деталей относительно простых изображений (рисунок 2) оказывается достаточным построить представление из нескольких десятков сегментов. Для аппроксимации большинства объектов на более сложных изображениях требуются представления, содержащие сотни и тысячи сегментов. Эффективность сегментации, оцениваемая по среднему количеству пикселей в расчете на один сегмент, возрастает с ростом разрешения изображения. Полноцветные изображения обрабатываются по цветовым компонентам как три независимых полутоновых. При этом наблюдается выраженная корреляция между сегментами, вычисляемыми для цветовых компонент, и общее число сегментов достаточно большой величины существенно не возрастает.

В обсуждаемом способе «адекватной» сегментации устанавливается и анализируется метрическая близость между сегментами изображения, а не отдельными пикселями, как в случае сегментации «с сохранением зрительного образа». При этом метрические соотношения меняются по мере формирования сегментов и вычисляются итеративно, что повышает требования к используемым вычислительным средствам и, в свое время, ограничивало эффективность методов сегментации [6], разработанных на компьютерах прошлого поколения. На современных компьютерах методы [6] не сталкиваются с принципиальными ограничениями по памяти и быстродействию и развиваются (рисунок 2) с учетом известных приемов оптимизации критерия метрической близости

сегментов [7]. Важно обратить внимание, что использование неоптимального критерия близости сегментов по средней яркости и накопление ошибок округления может вместо выделения объектов приводить к разрушению изображения [8].

Среднеквадратичное отклонение $StdDev$ приближений от изображения в зависимости от числа сегментов выражается монотонной невозрастающей функцией (рисунок 3).

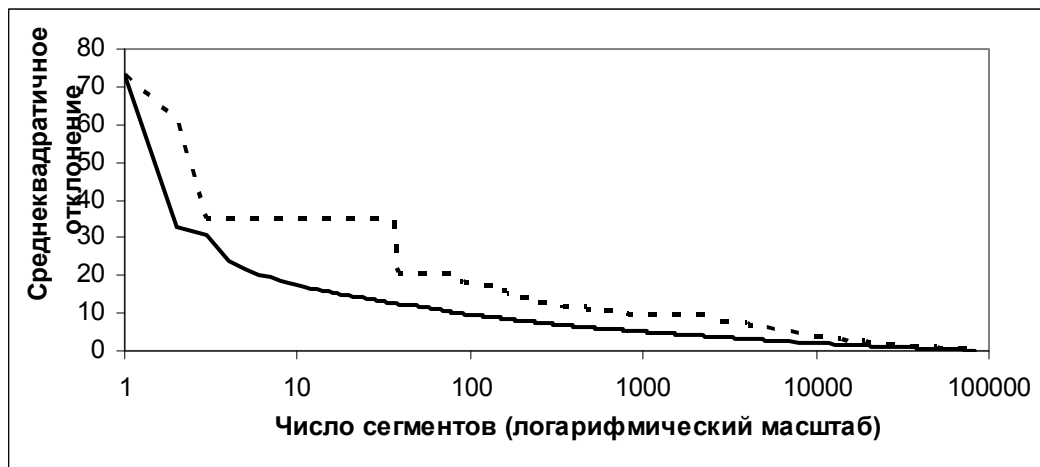


Рис. 3. Среднеквадратичное отклонение в зависимости от числа сегментов

На рисунке 3 сплошной линией показана зависимость среднеквадратичного отклонения от числа сегментов, полученная при использовании современного критерия метрической близости ([7], рисунок 2). Для сравнения пунктиром обозначена зависимость среднеквадратичного отклонения от числа сегментов, которая описывает вычисление приближений изображения при оценке близости сегментов по средней яркости. На графике неудачный выбор критерия метрической близости проявляется в наличии участков стабилизации среднеквадратичного отклонения при относительно малом числе сегментов, а на изображении при этом выделяются сегменты, отвечающие зрительно не значимым объектам.

В сравнении с традиционными иерархическими представлениями [6, 9] приближения с последовательно возрастающим числом сегментов позволяют повысить точность аппроксимации изображения по среднеквадратичному отклонению, которое устанавливается в пределах гораздо большего числа значений. Эксперименты показали, что эффективность использования среднеквадратичного отклонения $StdDev$ для оценки визуального сходства существенно повышается, если сравниваемые изображения выравниваются по числу сегментов.

Рисунки 2–3 описывают пример аппроксимации изображения представлениями с последовательно возрастающим числом сегментов. Варианты приближений получаются при изменении способа оценки метрической близости сегментов. Для оптимизации построения приближений наряду со способом [7], в качестве критерия экспериментально исследована величина SE («square error»), которая определяется для сегмента как сумма квадратов отклонений значений пикселей от среднего значения и минимизируется для объединения смежных сегментов. В качестве критерия использовалось также изменение суммы величин SE при объединении сегментов и ряд других функций от аддитивных характеристик сегментов изображения (площади, интегральной яркости и пр.). Для повышения устойчивости результатов к определенным искажениям изображения и применяется замещение изображения его инвариантным представлением [4] и предусмотрены другие приемы оптимизации вычислений. Всего рассматривалось около 20 вариантов способов анализа метрической близости, которые помимо эффективности аппроксимации изображения по среднеквадратичному отклонению, сравнивались между собой по скорости вычислений, имеющей в обсуждаемом классе алгоритмов принципиальное значение.

Действительно, исходное изображение (рисунок 2) содержит 91663 сегмента. Если вычисления производятся посредством итеративного слияния сегментов, то требуемая последовательность вычисляется за 31175 итераций. При этом на одной итерации объединяются в среднем по 3 сегмента, причем на последних тысячах итераций выполняется объединение преимущественно единственной пары сегментов, и число сегментов уменьшается на единицу. С ростом размера изображения число итераций квадратично растет и для стандартных изображений из 1024×1024 пикселей достигает нескольких сотен тысяч, что влечет резкое увеличение времени обработки и для хранения представлений в традиционной матричной форме требует сотен гигабайт памяти.

Для оптимизации вычислений анализ представлений с последовательно возрастающим числом сегментов (рисунок 2) выполняется опосредованно. При этом для получения требуемых приближений изображения согласно идее, предложенной Ф.Р. Гальяно, применяется способ [6], ранее

разработанный для «конструирования» объектов из заданного базового иерархического множества сегментов. Базовые сегменты вычисляются в стратегии разделения изображения на части как сегменты «компактной» иерархии, в которой на различных уровнях не допускается повторений составных сегментов, и повторения элементарных сегментов группируются в разбиениях изображения с высокой детализацией [9,10]. При разделении на части сегменты анализируются как самостоятельные изображения. Дополнительным требованием к обсуждаемой компактной иерархии сегментов, предназначенной для «конструирования» приближений (рисунок 2), является, очевидно, условие регулярности, согласно которому при построении иерархии каждый сегмент разделяется преимущественно на два вложенных сегмента. При этом на начальных этапах построения иерархической сегментации получается бинарной и состоит из разбиений изображения на 1, 2, 4, 8, ... сегментов, а на последующих этапах допускается нарушение строгой регулярности из-за появления неделимых сегментов, а также их разделение более чем на две части для исключения предпочтения одной из равноправных возможностей. Скорость построения дихотомической (преимущественно бинарной) компактной иерархической сегментации и последующего получения приближений изображения с заданным среднеквадратичным отклонением тем больше, чем меньше уровней она содержит. При этом, как показывают эксперименты, для оптимизации вычислений в качестве критерия метрической близости смежных сегментов оказывается предпочтительнее использовать величину SE .

Для уменьшения среднеквадратичного отклонения $StdDev$ и повышения эффективности аппроксимации изображения представлениями с установленным числом сегментов может применяться комбинирование критериев метрической близости, при котором из вариантов разделения сегмента на две части, полученных с использованием различных критериев, выбирается вариант, который приводит к максимальному уменьшению среднеквадратичного отклонения.

Таким образом, «объекты» независимо от конкретного контекста изображения описываются как сегменты из иерархии его приближений представлениями с последовательным числом сегментов при минимальном среднеквадратичном отклонении.

Заключение

Если сегментация «с сохранением зрительного образа», на сегодняшний день, представляет собой определенный алгоритм, программу упрощения изображения для грубого распознавания, удовлетворяющую установленным формальным условиям, то «адекватная» сегментация, фактически, является вычислительной технологией выделения объектов независимо от конкретного контекста изображения. Указанная технология обеспечивает высокую скорость вычислений дихотомической иерархии приближений изображения в 1–2 гигабайтах оперативной памяти современного компьютера за счет применения аппарата «динамических» деревьев и исключение систематических ошибок округления за счет применения «псевдотроичной» системы счисления [6,9].

Разработанные алгоритмы сегментации и технологию выделения объектов планируется применить для повышения эффективности программной системы распознавания изображений [11], а в дальнейшем развить в приложении к аудиосигналам.

СПИСОК ЛИТЕРАТУРЫ

1. Оков И.Н. Аутентификация речевых сообщений и изображений в каналах связи / Под ред. В.Ф.Комаровича. — СПб.: Изд-во Политехнич. ун-та, 2006. — 392 с.
2. Gurevich I. B. and Yashina V. V. Descriptive Approach to Image Analysis: Image Models // Pattern Recognition and Image Analysis: Advances in Mathematical Theory and Applications / Vol. 18, № 4, 2008. — P. 518–541.
3. Kharinov M.V. Algebraic Description of Data Embedding Basing on Idempotent Image Transformations // Pattern Recognition and Image Analysis: Advances in Mathematical Theory and Applications / Vol. 19, No 3, 2009. — P. 491–496.
4. Kharinov M.V. Invariant Representation of Information and Information Quantity in Image-Processing Tasks // Pattern Recognition and Image Analysis / Vol. 18, No 4, 2008. — P. 643–648.
5. Marfil R., Sandoval F. Energy-Based Perceptual Segmentation Using an Irregular Pyramid // LNCS Vol. 5517/2009 Bio-Inspired Systems: Computational and Ambient Intelligence. Springer-Verlag: Berlin/Heidelberg, 2009. — P. 424–431.
6. Харинов М.В. Разработка динамических структур данных системы автоматизированного распознавания изображений / руков. В.В. Александров / Автореф. Дис. канд. технич. наук. — СПб. 1993. — 20с.
7. Robinson D. J., Redding N. J., Crisp D. J. Implementation of a fast algorithm for segmenting SAR imagery // Scientific and Technical Report, Australia: Defense Science and Technology Organization, 01 January 2002. — 42 p.
8. Зайцева А.А. Адаптивно-динамическая сегментация и семантическая селекция видеоданных / руков. В.В. Александров / Автореф. Дис. канд. технич. наук. — СПб. 2009. — 20 с.
9. Харинов М.В. Запоминание и адаптивная обработка информации цифровых изображений / Под ред. Р. М. Юсупова. — СПб.: Изд-во С.-Петербург. ун-та, 2006. — 138 с.
10. Kharinov M.V., Nesterov M.M. Intelligent Program for Automatic Image Recognition based on Compact Object-Fitting Hierarchical Image Representation in terms of Dynamic Irregular Ramified Trees // Международная Академия. Вестник / Специальный выпуск межакадемического бюллетеня МАИСУ № 12-С, — СПб. 1997. — С. 1–35.
11. Харинов М. В. , Гальяно Ф. Р. Распознавание изображений посредством представлений в различном числе градаций // Математические методы распознавания образов (ММРО–14) / Сб. докл. 14-й Всерос. конф. Владимирская обл., г. Суздаль. — М.: МАКС Пресс, 21–26 сентября 2009. С. 465–468.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Примакина Е.И.

Россия, Кострома, Костромская государственная сельскохозяйственная академия
**МЕТОДИКА ОЦЕНКИ ПРОФЕССИОНАЛЬНО ЗНАЧИМЫХ НАВЫКОВ СПЕЦИАЛИСТОВ
 В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

При формировании и развитии профессионально значимых навыков специалистов в области информационной безопасности, существенное значение имеет количественная оценка их психофизиологических особенностей. Так при решении оператором специальных задач связанных с классификацией звуковых сигналов, предъявляются повышенные требования к его сенсорным функциям, т.е. необходимостью обладать высокой абсолютной и дифференциальной чувствительностью слухового анализатора.

По многим характеристикам, слуховая система человека (САЧ) не имеет себе равных среди технических решений. Однако, при использовании слухового анализатора, как элемента принятия решения о классификации объекта, возникает две задачи. Первая заключается в диагностике специальных способностей оператора, являющихся основой профессионально важных качеств, вторая – в оценке классификационных характеристик слуховой системы человека.

Для решения этих задач необходимо определить выбор тестирующих сигналов, определить меры измерения качества многоальтернативных решений приемными системами.

В данной работе восприятие звуковых сигналов оценивалось оператором информационными мерами Шеннона и Кульбака. Известно, мера Шеннона чувствительна к анализу ансамблей сигналов, а мера Кульбака оценивает близость той или иной гипотезы [1]. Под качеством восприятия звуковых сигналов понимаются выходные количественные характеристики оператора, измеренные мерами Шеннона и Кульбака.

Рассматривается следующая модель функции оператора, представленная на рисунке 1.

Причина введения в модель физиологического шума объясняется тем, что решения оператора носят вероятностный характер.



Рис. 1. Модель операторской деятельности при классификации акустических сигналов

Сигналы имеют признаки, по которым человек формирует ответы (выборку), позволяющих судить об успешности решения оператором задачи их распознавания.

Практические задачи обработки сигналов слуховой системой человека показали, что эффективность приемных систем определяется объемом априорной информации о сигнале. При этом важно формирование таких процедур обработки, которые используют наибольшее количество симметрий, приводящих к инвариантности ответных реакций слуховой функции человека. Поэтому при исследованиях САЧ необходимо выбирать такие параметры входных стимулов, которые инвариантны относительно большего класса преобразований [2]. Эту задачу в психофизике можно формулировать как задачу классификации симметрий, присущих слуховой функции человека [3, 4, 5]. Очевидно, что задача выбора симметрий слуха (определения слуховых инвариантов) решается только экспериментально, путем сравнительной оценки откликов слуховой функции человека и подтверждения выдвинутых гипотез.

Первым шагом исследования слуховой функции человека является получение ответа, какова природа преобразований сигналов [5]. В соответствии с принятой точкой зрения, базовым действием в понимании механизмов слуховой функции человека являются исследования преобразований сигнала, т.е. действий среды и кинематики источника и приемника на носитель сигнала.

Самым простейшим и наиболее часто встречающимся преобразованием сигнала является операция сдвига $t \rightarrow t + \tau$, где t – время, а τ – параметр сдвига. Другим примером

преобразованием является, например, действие по правилу: $t \rightarrow \alpha t$, где α – параметр мультипликативного (доплеровского) преобразования, обусловленного взаимным движением источника и приемника сигналов.

Представленные выше преобразования являются коммутативными группами преобразований. Известно, что неприводимыми представлениями этих групп являются гармоники. При этом преобразование сдвига порождает аддитивную гармонику: $s(t) = \exp(i2\pi f t)$ (тональный сигнал) фундаментально устойчивую к этому преобразованию, а мультипликативное – порождает мультипликативную гармонику вида: $s(t) = \exp(i2\pi f \ln(t))$ – фундаментально устойчивую к мультипликативному преобразованию [6,7].

Исторически наиболее ранним являлось исследование слуха человека стимуляцией анализатора тональными сигналами. При указанном способе воздействия неявно принималась гипотеза, что слуховая система является стационарной системой, т.е. устройством инвариантным относительно сдвига входного сигнала во времени. Применение в данном случае тональных сигналов оправдано тем, что указанные гармоники являются неприводимым унитарным представлением для группы сдвига [6]. Тональные сигналы с точностью до фазового множителя инвариантны относительно сдвига. Только этим можно объяснить широкое применение в психофизике при стимуляции САЧ указанных сигналов.

Принятие гипотезы стационарности слуховой системы позволяет по откликам на гармонические сигналы оценить амплитудно-частотную характеристику системы. По существу амплитудно-частотная характеристика САЧ оценивается по измерениям пороговых откликов слуха на гармонические воздействия при условии, что маскирующей помехой является внутренний шум системы или в других экспериментальных условиях – внешний шум.

Оценки пороговых характеристик слуха в функции несущей частоты сигнала стали первым функциональными характеристиками слуха, позволяющими судить об эффективности этой системы как приемника. С их помощью удалось ввести понятие критических полос слуха, т.е. полос частот, в пределах которых мощность маскирующей помехи соизмерима с мощностью тонального сигнала и соответствует пороговому уровню обнаружения сигнала.

Последующие исследования слуха были связаны с выбором, в качестве стимулирующих воздействий, отрезков гармонических сигналов при условии, что воздействия сравниваются не по мощности, а по энергии сигналов. Исследования слуха операторов показали, что отклик слуховой системы на указанный класс сигналов не только инвариантен относительно сдвига во времени, но и масштабно инвариантен. Другими словами, сигналы с одинаковым количеством волн и разными масштабами (различными частотами заполнения) формируют при постоянной энергии один и тот же вероятностный отклик [3].

В исследованиях слуха при кинематике акустических источников предполагается, что справедлива гипотеза инвариантности относительно одновременно сдвига и операции сжатия (расширения). В данном случае применение для стимуляции САЧ тональных посылок не желательно, т.к. тональные сигналы не инвариантны относительно масштаба и поэтому их применение в динамических исследованиях слуха бесполезно. В качестве входных сигналов для указанной симметрии необходимо выбирать сигналы инвариантные относительно преобразования масштаба, а именно гиперболические гармоники [8].

Для гиперболической симметрии также необходимо фиксировать функционал энергии сигнала. Вычислить энергию отрезка гиперболической гармоники можно с помощью соотношения:

$$E = (A^2 / 2) \cdot \ln(t_k / t_n),$$

где $\ln(t_k / t_n)$ – длительность сигнала в гиперболическом масштабе.

Выбор той или иной реакции диктуется условиями близости признаков сигналов друг к другу. В дальнейшем решении задачи классификации сигналов оператором будем связывать с его системой «интеллектуальной деятельности», под которой будем понимать относительно устойчивую структуру способностей, в основе которых лежат процессы, обеспечивающие переработку разнокачественной информации о симметрии сигналов и осознанную оценку ее свойств. Интересно заметить, что в теории музыки положена симметрия линейной группы преобразований. Согласно этого подхода, в качестве акустических сигналов целесообразно использовать стандартные формы сигналов с известными симметричными музыкальными частотами [9].

Математическая модель распознавания входных сигналов с учетом искажения физиологическим шумом записывается правилом:

$$y_k = \Phi(x_k(t) \times h(t) + n(t)), \quad (1)$$

где

$n(t)$ – физиологический шум, снижающий эффективность распознавания сигналов оператором;

$h(t)$ – импульсная характеристика процедуры фильтрации сигнала;

$x_k(t)$ – входной k – стимул;

y_k – отклик оператора;

$\times$ – индекс операции свертки;

$\Phi(\dots)$ – процедура распознавания.

Оператор прослушивает входной сигнал $x_k(t)$ и за счет процедуры распознавания формирует отклик y_k из условия близости признаков сигнала к признакам эталона, формируемых субъективно оператором. Результатом оценки является формирование матрицы ответов и фактически предъявляемых сигналов.

Будем рассматривать входные сигналы дискретными событиями x_k , а ответы оператора – выходными событиями y_k . Это означает, что заданы дискретные случайные величины x и y , причем вероятности событий имеют вид:

$$p_{i,j} = P(x = x_i, y = y_j), \quad i = 1, \dots, M, \quad j = 1, \dots, N,$$

$$p_i = \sum_{j=1}^N p_{i,j}, \quad p_j = \sum_{i=1}^M p_{i,j}, \quad p_{i,j} > 0, \quad i = 1, \dots, M, \quad j = 1, \dots, N,$$

$$\sum_{i=1}^M \sum_{j=1}^N p_{i,j} = \sum_{i=1}^M p_i = \sum_{j=1}^N p_j = 1.$$

Совместная энтропия определяется равенством обмена между входом и выходом,

$$H(x, y) = - \sum_{i=1}^M \sum_{j=1}^N p_{i,j} \log_2(p_{i,j})$$

следовательно равна , энтропия на входе

$$H(x) = - \sum_{i=1}^M p_i \log_2(p_i)$$

, тогда переданную информацию можно оценить по формуле

$$I(X, Y) = \sum_{i=1}^M \sum_{j=1}^N p_{i,j} \log_2 \frac{(p_{i,j})}{p_i p_j}, \quad (2)$$

а обобщенное отношение сигнал/помеха определится соотношением:

$$J(X, Y) = \sum_{i=1}^M \sum_{j=1}^N (p_{i,j} - p_i p_j) \log_2 \frac{(p_{i,j})}{p_i p_j}. \quad (3)$$

Оценки мер Шеннона и Кульбака были реализованы в соответствии со следующим алгоритмом. Из банка данных (сигналов) случайным механизмом выбирался k – сигнал. Оператору представлялась возможность провести выбор сигнала из k альтернатив. Накопленные данные ответов позволяли оценить матрицу ответов и с учетом соотношений (2,3) оценить меры Шеннона и меры Кульбака. Индивидуальные данные обрабатывались и консервировались в виде числовых и графических представлений.

Предлагается применить следующую последовательность оценки индивидуальных способностей классификации сигналов операторами:

- инструктаж оператора по работе с программным продуктом на ПЭВМ;
- обучение в течение часа оператора решению задачи классификации сигналов;
- фактическое проведение эксперимента.

На первом этапе в качестве стимулирующих сигналов можно выбрать тональный ряд октавы [9]. При этом важно, чтобы излучаемые сигналы имели одинаковое количество волн и одну и ту же энергию.

При успешном распознавании операторами сигналов можно сблизить частоты операцией одновременного сжатия частот с коэффициентом в $\alpha > 1$ раз.

Для исследования динамических свойств слуховой системы предлагается использовать звуко ряд из N гиперболических $n \in (1, \dots, N)$ гармоник $\text{Re} \{ \exp(i 2 \pi f_m \alpha^n t) \}$ с одинаковым числом

волн, одинаковой энергией и с различными значениями меллиновских частот $f_m \alpha^n$, где $\alpha > 0$ – параметр сжатия (расширения).

Представленная методика, оценки эффективности операторов решения задачи классификации стандартизованных акустических сигналов может найти применение при количественной оценке их психофизиологических особенностей.

СПИСОК ЛИТЕРАТУРЫ

1. С. Кульбак. Теория информации и статистика, М.: Изд. Наука, 1967. 408 с.
2. Лямов К.Г., Сапрыкин А.В. Некоторые общие принципы инвариантной обработки сигналов // X Санкт-Петербургская международная конференция «Региональная информатика 2006 (РИ–2006)»: тез. докл. СПб.: СПОИСУ, 2006. С. 41–42.
3. Сапрыкин В.А., Сагал А.А. Инвариантность способности к обнаружению тональных звуков относительно операции сжатия (расширения) сигнала // «Биофизика». 1972. Т. 17. №3. С. 503.
4. Закиров А.Д., Сапрыкин В.А. Отчет о НИР «Эхолокатор для ориентации инвалидов по зрению» / грант Правительства Санкт-Петербурга. Петродворец. 2004. 96 с.
5. Закиров А.Д. Преобразования сигналов в акустике слуха // XIV Межвузовская НТК «Военная радиоэлектроника: Опыт использования и проблемы, подготовка специалистов»: тез. докл. / ВМИРЭ. Петродворец, 2003. С. 215.
6. Виленкин Н.Я. Специальные функции и теория представления групп. М.: Наука. 1965. 588 с.
7. Сапрыкин В.А., Рокотов С.П. Теория гидроакустики и цифровая обработка сигналов. Петродворец: ВВМУРЭ им. А.С.Попова, 1991. Ч. 2.
8. Ковалевский Н.Г., Лямов К.Г., Сапрыкин А.В. Природа симметрии акустических сигналов // Сб. трудов «Высокие интеллектуальные технологии в образовании и науке». СПб.: СПбГПУ, февраль 2007. С. 214–223.
9. Шилов Г.Е. Простая гамма (устройство музыкальной шкалы). М.: Физматгиз. 1963. 20 с.

Хвостунов Ю.С.

**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»
АВТОМАТИЗИРОВАННЫЙ КОМПЛЕКС СРЕДСТВ СКОРОСТНОЙ АДАПТИВНОЙ
ПОМЕХОЗАЩИЩЕННОЙ СИСТЕМЫ РАДИОСВЯЗИ**

Перспективные автоматизированные системы радиосвязи декаметрового диапазона должны удовлетворять следующим требованиям:

- обеспечивать устойчивую (с надежностью не хуже 0.9 – 0.99) многоканальную связь при воздействии различных дестабилизирующих факторов;
- обеспечивать одновременную передачу и прием данных, обмен речевой информацией на расстоянии до 3000 км на трассах со стационарными и подвижными объектами;
- обеспечивать работу с существующим парком систем радиосвязи.

Одним из дестабилизирующих факторов в декаметровом радиодиапазоне является, как известно, сами условия распространения сигнала. В декаметровом радиодиапазоне распространяется земной и ионосферной волной. Земная волна распространяется параллельно земной поверхности, дальность ее распространения зависит от мощности передатчика, высот передающей и приемной антенн, характера и проводящих свойств поверхности Земли. Обычно с помощью земной волны осуществляют связь на расстояние не более нескольких десятков километров. Ионосферные волны позволяют устанавливать сверхдальнюю связь при относительно небольших мощностях передатчика. Однако случайность свойств ионосферы как отражающей поверхности делают связь в декаметровом диапазоне неустойчивой. В ионосфере различают несколько слоев с максимумами ионизации. Степень ионизации зависит от времени года, суток и географического положения. Как правило, в декаметровом радиоканале сигнал распространяется по нескольким путям. Это приводит к интерференции лучей и, как следствие, к замиранию принимаемого сигнала. Уровень сигнала из-за замираний может меняться на несколько порядков. Условия отражения для различных частотных составляющих спектра сигнала в радиоканале оказываются различными, что обуславливает амплитудно-частотные искажения принимаемого сигнала.

Также на качество связи существенное влияние оказывают действующие в радиоканале помехи. Помехи по их происхождению можно подразделить на естественные и искусственные. Естественные помехи создаются электромагнитными процессами в земной атмосфере (грозовые разряды и так далее). Мощными источниками помех является космос и тропосфера. Искусственные помехи создаются промышленными установками, посторонними радиостанциями (непреднамеренные и специально организованные). Учет индивидуальных свойств различных помех – задача неразрешимая. Различают четыре вида помех: сосредоточенная, флуктуационная, импульсная и квазиимпульсная. Под сосредоточенной понимается помеха, энергетический спектр которой сосредоточен в узкой частотной области. Обычно ширина спектра сосредоточенной помехи соизмерима или уже ширины спектра полезного сигнала. Источником сосредоточенных помех являются сигналы сторонних станций, генераторы высоких частот. Сосредоточенные помехи разделяются на внутрисполосные и внеполосные. Методы борьбы с ними различные. Мощность сосредоточенной помехи может превышать мощность полезного сигнала на 20 дБ и более. Флуктуационная помеха неизбежно присутствует во всех реальных электронных устройствах в виде тепловых шумов. Сумма любых помех от различных источников также имеет характер

флуктуационной помехи. Космические, атмосферные помехи, различные помехи, прошедшие через радиоприемник также имеют свойства флуктуационной помехи.

Импульсная помеха представляет собой непериодическую последовательность одиночных импульсов. Ее характерная особенность – широкий частотный спектр. Примерные длительности помехи, создаваемой промышленными и атмосферными источниками – $10 \text{ нсек} \div 10 \text{ мсек}$. Переходные процессы в радиоприемнике под действием мощной импульсной помехи могут составлять $0,1 \dots 3,0 \text{ мсек}$.

Таким образом, декаметровая связь отличается сложностью и нестационарностью условий распространения радиоволн и помеховых ситуаций. Для обеспечения устойчивой связи в декаметровом диапазоне волн требуется применение адаптивных устройств, входящих в систему связи. Под адаптацией мы будем понимать способность системы оптимизировать себя или свое окружение при неблагоприятных для нее изменениях для частичного или полного восполнения качества своего функционирования. Это достигается путем автоматической смены используемых частот для получения канала с приемлемым распространением и приемлемым уровнем помех, использования помехоустойчивого кодирования и информационной обратной связи, оптимизацией скоростей работы и так далее.

Адаптация позволяет достичь в условиях нестационарности распространения радиоволн и помеховых ситуаций высокую пропускную способность организуемых каналов связи, что, в свою очередь, используя временное уплотнение, позволяет организовать несколько независимых каналов связи через один комплект радиосредств.

В известных существующих автоматизированных системах радиосвязи декаметрового диапазона, предназначенных для организации передачи данных и речи:

- отсутствуют эффективные алгоритмы адаптации по условиям распространения радиоволн и помеховых ситуаций, что не позволяет достичь требуемого надежности и пропускной способности организуемого канала связи;
- при создании многоканальных систем не решены вопросы устойчивого и надежного разделения организуемых каналов методами временного уплотнения.

Рассматриваемый комплекс базируется на использовании технологии псевдослучайной перестройки рабочей частоты (ППРЧ) во всем используемом диапазоне радиочастот, при этом:

- время работы на одной рабочей частоте $\sim 50 \text{ мс}$;
- период псевдослучайной последовательности перестройки рабочей частоты существенно больше периода функционирования системы (равен $2^{128} - 1$);
- применяется синхронно перестраиваемый пассивный узкополосный преселектор (полоса пропускания $\sim 3\%$), что исключает блокирование мощной помехой радиоприемного тракта.

Предлагаемый автоматизированный комплекс средств скоростной адаптивной помехозащищенной системы радиосвязи обеспечивает:

- передачу и прием информации по радиоканалам декаметрового диапазона в адаптивном режиме с ППРЧ при работе со скоростями до 64 Кбит/с с реализацией алгоритма исправления ошибок;
- ведение радиосвязи с адаптацией (в зависимости от качества канала связи) по частоте, скорости приема/передачи, помехоустойчивому коду, виду модуляции, длине пакета;
- обеспечение одновременной работы (включая речь) с несколькими корреспондентами через один комплект аппаратуры (с суммарной скоростью работы до 64 Кбит/с);
- сопряжение с установленным и перспективным оборудованием передачи данных по интерфейсам информационного обмена, выдаваемого заказчиком;
- устойчивую работу при воздействии различных дестабилизирующих факторов;
- дуплексный, полудуплексный или симплексный обмен информацией между различными абонентами сети по каналам связи на дальности связи до 3000 км в условиях внешних воздействий;
- высокий коэффициент готовности предоставляемого канала связи в организованной сети (более $0,9 \div 0,99$).

Одним из важнейших параметров, на которых базируется работа комплекса – это возможность адаптации по рабочей частоте в фоновом режиме в процессе обмена информацией. Переключение радиочастот на передаче и приеме для корреспондентов в случае необходимости замены рабочей частоты происходит синхронно. Синхронизация режима переключения рабочих частот устанавливается при вводе звена в эксплуатацию без использования системы единого времени. После этого аппаратура переходит в режим радиомолчания и будет постоянно готова в течение $1 \div 1,5$ месяцев к приему информации без потерь времени на синхронизацию.

Для каждого корреспондента устанавливается набор рабочих частот. Для всех абонентов сети определяется начальный комплект рабочих частот, который является набором, позволяющим осуществить установление соединения и дальнейшую адаптацию по рабочей частоте и скорости для получения в канале связи максимальной пропускной способности.

Во время обмена информацией устройства управления на обоих концах радиоперехвата при неудовлетворительном прохождении сигнала на отдельных рабочих частотах автоматически заменяются новыми из заранее оговоренного списка до получения прохождения на всех используемых частотах. К концу адаптации пропускная способность канала связи достигает предельной величины и поддерживается на максимальном уровне. Постоянная оценка качества прохождения сигнала во время передачи информации абонента позволяет реализовать режимы адаптации по рабочим частотам и скоростям обмена информацией во всем диапазоне частот и скоростей. Этим самым обеспечивается максимально возможная пропускная способность используемой сети связи.

Обмен между двумя любыми абонентами (обмен «точка-точка») производится в дуплексном режиме, т.е. для передатчика и приемника выделяются пара разнесенных рабочих частот. Для компактных подвижных абонентов из-за невозможности разнести передающую и приемную антенны (используется универсальная приемопередающая антенна) связь осуществляется в полудуплексном режиме с автоматическим переключением режимов «передача» – «прием».

Постоянная готовность к приему информации с учетом отсутствия потерь на синхронизацию делает возможным передачу коротких сообщений (в пределах 1–2 Кбит) за доли секунды с заданной надежностью, что является важнейшим параметром для систем управления. Применение алгоритмов компенсации эффекта Доплера в канале связи позволяет работать с быстро движущимися объектами (самолет, вертолет).

В процессе установившегося обмена информацией с определенным интервалом возможна передача тестовой последовательности на радиочастотах из списка разрешенных для определения условий прохождения сигнала. Результаты тестирования заносятся в банк данных и являются фактически данными о состоянии ионосферы (т.е. система автоматически выполняет функции средства сбора данных о состоянии ионосферы).

Комплекс не требует использования систем единого времени, зондирования радиозвезд, а также не использует в процессе обмена информацией специальные сигналы или кодограммы синхронизации.

В настоящее время:

- разработаны и изготовлены функциональные блоки аппаратуры быстродействующей телекодированной связи, проведены испытания;
- разработан и изготовлен наземный комплекс управления, проведены необходимые испытания;
- разработаны и изготовлены макеты широкополосных АФУ различного вида (в том числе с возможностью размещения на самолете), проведены испытания.

В процессе испытаний проведены:

- всесторонние лабораторные испытания всех составляющих адаптивной системы радиосвязи с ППРЧ на имитаторах декаметрового радиоканала, и с использованием реальных радиосредств;
- длительные трассовые испытания, подтвердившие основные заявленные характеристики.

Основные технические характеристики автоматизированного комплекса средств скоростной адаптивной помехозащищенной системы радиосвязи приведены ниже в таблице.

Таблица

Основные технические характеристики автоматизированного комплекса средств скоростной адаптивной помехозащищенной системы радиосвязи

Наименование характеристики	Значение
Диапазон частот, МГц	1,5-30
Ширина полосы сигнала, кГц	3,1 (0,3-3,4) 4,5 (0,3-4,8) 9,0 (0,3-9,3) 40
Скорость передачи информации, Кбит/с: – минимальное значение – максимальное значение в зависимости от полосы сигнала: 3,1 КГц 4,5 КГц 9,0 КГц 40 КГц	1,2 7,2 9,6 19,2 64
Дальность связи при мощности радиопередатчика 300-1000 Вт, км	3000
Время нахождения на одной рабочей частоте в режиме ППРЧ, мс	50; 100; 200
Режим перехода с одной рабочей частоты на другую	по псевдослучайному закону
Количество назначаемых и заранее устанавливаемых рабочих частот	до 128 для каждого времени суток
Количество одновременно используемых рабочих частот	до 32

Количество независимых дуплексных каналов радиосети с полной пропускной способностью	до 15
Вероятность обеспечения связи в любое время года и суток (в течение 99,8% времени работы радиолинии)	0,95–0,99
Количество абонентов сети, использующих один комплект радиочастот	несколько сотен
Возможность межсетевого обмена	обеспечивается
Длительность сетевой синхронизации для нового абонента сети (при вводе в эксплуатацию), с.	20-40
Время поддержания сетевой синхронизации в режиме радиомолчания, суток	не менее 30 (возможно до 1 года)
Необходимость использования систем единого времени	отсутствует
Необходимость использования систем ионосферного зондирования	отсутствует
Возможность обмена данными на ходу с быстро движущимися объектами (самолет, вертолет)	обеспечивается
Возможность встречной работы со старым парком радиосредств	обеспечивается

Примечания:

1. Скорость передачи информации устанавливается оператором связи или выбирается автоматически системой адаптации.
2. При необходимости обеспечения работы оконечного оборудования со скоростями 50; 100; 150; 200; 600; 1000 бит/с используются средства уплотнения/разуплотнения одиночного группового канала радиосети, имеющего скорость от 1200 до 19200 (64000) бит/с.

Штубов А.С.

Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»
АНАЛИЗ БЕЗОПАСНОСТИ СЕТЕЙ АВИАЦИОННОЙ ЭЛЕКТРОСВЯЗИ

Введение. Модернизация и развитие Единой системы организации воздушного движения (ЕС ОрВД), её поэтапное реформирование являются неотъемлемой частью развития гражданской авиации (ГА), важнейшим этапом на пути внедрения Концепции ICAO CNS/ATM (связь, навигация, наблюдение/обслуживание воздушного движения) в Российской Федерации [1]. Создание современной аэронавигационной системы позволит более эффективно использовать воздушное пространство с позиции улучшения экономики и обеспечения национальной безопасности страны. В рамках данной концепции в регионах РФ предполагается установление речевой связи/передачи данных на основе авиационной подвижной спутниковой службы, линии передачи данных режима «S», вторичного радиолокатора SSR (Secondary Surveillance Radar) и, в целом, сети ATN (Aeronautical Telecommunication Network). В рамках Федеральной целевой программы «Модернизация Единой системы организации воздушного движения Российской Федерации (2009–2015 годы)» осуществляется процесс создания укрупненных районных центров (РЦ) [2].

Процесс укрупнения включает поэтапную модернизацию и объединение ныне действующих районных центров в общую подсеть передачи, обработки и отображения данных о воздушной обстановке. Указанная реорганизация сети авиационной электросвязи, включает постепенный отход от использования низкоскоростных телеграфных каналов и каналов тональной частоты (используемых до недавнего времени) в пользу цифровых каналов передачи данных, которые так же планируется использовать для передачи радиолокационной информации, обмена сообщениями, файлами и интерактивными транзакциями. В этих условиях вопросы обеспечения информационной безопасности приобретают особую важность. Так как системы сети передачи и хранения информации подвержены множеству дестабилизирующих факторов, то вопросы практической оценки защищенности существующих и проектируемых сетей авиационной электросвязи приобретают особую актуальность.

Анализ степени безопасности. Существующие системы управления воздушным движением (УВД) на основе речевых обменов «борт-земля» являются внутренне небезопасными, так как достаточно простого технического устройства, чтобы создать помехи командам, прослушать УВД связь или выдать себя за диспетчера. Предотвращение возможности ложной выдачи за диспетчера зависит, главным образом, от профессиональной способности пилота и диспетчера распознать самозванца (обманщика). Безопасность обеспечивается несколькими слоями наблюдения и системами сигнализации о наличии конфликтной ситуации. Система линии передачи данных должна обеспечить лучшую безопасность, чем речевая система, поскольку она требует больших технических усилий для несанкционированного контроля связи по линии передачи данных или для выдачи себя за пилота или диспетчера. С другой стороны не существует ничего правильно организованного, для противостояния самозванцам, кроме профессионализма пилота или диспетчера [3].

Анализ безопасности сети ATN позволяет выявить следующие угрозы для этой сети:

1. Имитация пилота, приводящая к неразберихе (например, выдача разрешения раньше времени).
2. Имитация диспетчера, приводящая к потере эшелона из-за недостоверного разрешения.

3. Ухудшение сервиса вследствие постановки помех или искажения или модификации маршрутной информации.

4. Модификация «восходящих» сообщений, приводящая к потере эшелонирования из-за выполнения недостоверного разрешения.

5. Модификация «нисходящих» сообщений, приводящих к путанице (например, выдача разрешения раньше времени).

Модификации сообщений реальны только в наземной системе ATN. Теоретически тщательно разработанный помеховый сигнал может модифицировать реальную передачу «борт-земля». Однако, потребуется технический опыт высокого уровня и без знания сути передачи будет очень трудно прогнозировать правильный сигнал модификации. На практике, динамические аспекты, вероятно, затруднят такую попытку. Физическая защита в центре УВД и у провайдеров услуг связи основана на предотвращении изменения CPDLC (система передачи данных «диспетчер-пилот») и других сообщений в наземной сети ATN. Разработка подходящих механизмов для предотвращения уязвимости потери конфиденциальности была отложена до тех пор, пока не будут изучены аспекты, связанные с экспертизой криптографического оборудования.

Расширение безопасности сетей ATN обусловленное модернизацией единой системы организации воздушного движения должно обеспечивать:

- Проверку целостности на уровне приложения и проверки подлинности каждого переданного сообщения.

- Проверку целостности и проверку маршрутной информации переданной по линии передачи данных «борт-земля».

- Общедоступную ключевую инфраструктуру, основанную на алгоритмах построения эллиптических кривых и использующую контекстное управление для переговоров по ключам сеансов связи.

Существует возможность объединения расширений безопасности с режимом CPDLC (используя «защищенный режим» CPDLC), обеспечивающий высокоэффективный механизм для проверки подлинности посланного сообщения, анализа целостности и защиты от неисправной передачи сообщений. Имитации «нападения» с целью отказа от обслуживания, основанные на постановке помех, необходимо учитывать с помощью средств обнаружения передатчика и физической защиты. Уменьшение возможности отказа от обслуживания за счет обеспечения альтернативных маршрутов через другие технологии «бор-земля» является свойством межсети ATM (Air Traffic Management) и одной из причин, почему сеть ATN предпочитает более сложный из возможных сценариев маршрутизации, т.е. разрешение самолету соединяться с многочисленными совпадающими сетями «борт-земля». Средства защиты сети ATN обычно ограничивается такими способами как физическая защита, контроль доступа (защита паролем) и т.п. методами, связанными с вопросами уязвимости.

Организацией ICAO в документе SARP (Standards and Recommended Practices) установлены и рекомендованы следующие механизмы, предотвращающие получение незарегистрированного доступа к наземной станции ATN и имитацию законного пользователя:

- сеть ATN функционирует как виртуальная часть сети (VPN), которая направляет свои собственные протоколы через сеть IP, делая ее недоступной для других пользователей сети IP;

- механизмы физической защиты могут и будут развернуты администрацией и провайдерами услуг для предотвращения доступа к ее наземным сетям для несанкционированных сторон, снижая тем самым возможности для этого режима «нападения»;

- связь должна наблюдаться, и протоколы должны быть полностью понятны, если сообщение динамично создается, т.е. последовательно и приемлемо для приемника, а природа режима связи протоколов ATN делает трудным простое «вброс» разрешенного сообщения в установленный диалог CPDLC между пилотом и органом передачи данных;

- другой пользователь может взять на себя полномочия самолетного органа передачи данных, когда назван существующим органом передачи данных, существенно снижая тем самым возможности неразрешенной связи;

- система наблюдения, включая вторичный обзорный радиолокатор (SSR) наземного базирования, должна обнаруживать результаты неразрешенного профиля, изменяющего сообщения и потерю эшелона, предотвращенную, благодаря вмешательству диспетчера или через автоматический отклик системы;

- системы наблюдения, включающие систему SSR наземного базирования, должны обнаруживать результаты неразрешенного профиля обмена информацией и потерю эшелона, предотвращенные вмешательством диспетчера или посредством автоматического отклика системы.

Применение модели телетрафика к задачам безопасности сетей ATN. Задачи информационной безопасности авиационной электросвязи связаны с параллельным доступом многих пользователей к общим данным, и затрагивают вопросы обеспечения достоверности и целостности информации, а значит, распределения ресурсов системы при возрастании величины трафика.

Транспортную основу построения таких сетей составляют сети с коммутацией пакетов TCP/IP, ATM, Frame Relay, Ethernet и другие, различающиеся возможностями обеспечения качества обслуживания QoS (Quality of Service) и информационной безопасностью. Решение задач по планированию информационной загруженности и безопасности телекоммуникационных систем предусматривает рассмотрение методов повышения достоверности, применяемых в теории массового обслуживания и применение имитационного моделирования для анализа потоков ошибок в каналах связи.

Ошибки, возникающие в цифровых каналах связи по основным свойствам можно разделить на несколько классов:

1. Случайные битовые ошибки без группирования, характерны при низком соотношении сигнал/шум в физических каналах. Описываются постоянной во времени вероятностью возникновения в принятом бите.

2. Битовые ошибки с группированием, характерны для импульсных радиопомех, для связи в коротковолновом (КВ) диапазоне, когда величина вероятности возникновения ошибки изменяется во времени вследствие замираний несущего радиосигнала.

3. Блочные ошибки без группирования, это случайные потери пакетов, например, речевых данных целиком. Описываются постоянной во времени вероятностью пропадания или возникновения ошибочного сигнала.

4. Блочные ошибки с группированием, характерны для периодических кратковременных или долговременных срывов или пропадании отдельных каналов связи.

На примере разработанной в [4] математической модели обобщенного пуассоновского потока аппроксимирующей потоки ошибок в каналах связи, рассматривается возможность её последующего применения к потокам с признаками самоподобия [5,6], с целью изучения их влияния на безопасность и качество функционирования телекоммуникационных систем авиационной электросвязи [7]. Суть данного подхода заключается в том, что реальный случайный поток рассматривается как поток, порожденный первичным, порождающим потоком (пуассоновский поток), параметр которого является случайной величиной с соответствующей функцией распределения. Осредненный по значениям этой величины пуассоновский поток, названный обобщенным пуассоновским (или рандомизированным) потоком, обладает свойствами, присущими самоподобным потокам (группирование событий, «длинные хвосты» распределений и др.) [8]. В качестве порождающих рассматриваются классические модели телетрафика со случайными параметрами потока.

Поток ошибок дискретного канала рассматривается как ступенчатый случайный процесс. Задавая потоки ошибок данным способом необходимо для любого натурального числа $r \geq 1$ и произвольного набора чисел $0 < \tau_1 < \tau_2 < \dots < \tau_r$ указать $r \geq 1$ — мерную функцию распределения случайного вектора $\{x(\tau_i), i = \overline{1, r}\}$, где $x(\tau)$ — количество ошибок, появившихся на интервале $[0, \tau)$, где τ — начало отчета времени, или найти

$$P\{[x(\tau + \tau_i) - x(\tau + \tau_{i-1})] = m_i, i = \overline{1, r}\} = \mathfrak{G}_{m_1, \dots, m_r}(\tau; t_1, \dots, t_r), \quad (1)$$

$$m_i \geq 0, r \geq 1, t_i = \tau_i - \tau_{i-1},$$

где $\mathfrak{G}_{m_1, \dots, m_r}(\tau; t_1, \dots, t_r)$ — вероятность того, что на последовательно расположенных промежутках времени $t_1, t_2, \dots, t_r$, откладываемого от момента времени τ , появится соответственно $m_1, \dots, m_r$ ошибок. Это распределение полностью определяет поток ошибок. Тогда, одномерное (при $r = 1$) распределение числа ошибок $\mathfrak{G}_m$ на промежутке времени $[\tau, \tau + t)$ равно:

$$\mathfrak{G}_m(\tau, t) = P\{x(\tau + t) - x(\tau) = m\}, m \geq 0. \quad (2)$$

Для стационарного потока зависимость от τ отсутствует, тогда распределение числа ошибок обозначается через $\mathfrak{G}_m(t)$. Для любого стационарного потока существует предел, который назван параметром потока λ , равный математическому ожиданию числа событий потока в единицу времени.

$$\lambda = \lim_{t \rightarrow 0} \frac{1 - \mathfrak{G}_0(t)}{t} = -\mathfrak{G}_0'(0). \quad (3)$$

Для нестационарного потока соответствующий предел, называемый мгновенным параметром, определяется соотношением

$$\lambda(\tau) = -\frac{\mathfrak{G}_0(\tau, t)}{t} \Big|_{t=0}, \quad (4)$$

а математическое ожидание числа ошибок в промежутке времени $[\tau, \tau + t)$ вычисляется по формуле

$$\Lambda(\tau; t) = \sum_{m=1}^{\infty} m \vartheta_m(\tau; t) = \int_{\tau}^{\tau+t} \lambda(x) dx. \quad (5)$$

Это позволяет для нестационарного пуассоновского потока получить следующее соотношение:

$$\vartheta_{m_1, \dots, m_r}(\tau; t_1, \dots, t_r) = \prod_{s=1}^r \frac{\Lambda_S^m \left(\tau + \sum_{i=1}^{S-1} t_i; t_S \right)}{m_S!} \exp \left[-\Lambda \left(\tau + \sum_{i=1}^{S-1} t_i; t_S \right) \right], \quad (6)$$

тогда, производящая функция определяется как

$$\Phi(\tau; t_1, \dots, t_r; z_1, \dots, z_r) = \sum_{m_1, \dots, m_r} z_1^{m_1} \dots z_r^{m_r} \vartheta_{m_1, \dots, m_r}(\tau; t_1, \dots, t_r) = \prod_{i=1}^r \exp \left[-\Lambda \left(\tau + \sum_{i=1}^{S-1} t_i; t_S \right) (1 - z_i) \right]. \quad (7)$$

Рассмотрим функцию Пальма – Хинчина $\varphi_m(t)$, представляемую как вероятность появления m ошибок в промежутке времени t при условии, что в начальный момент времени появилось событие потока (ошибки). При определении взаимосвязи $\vartheta_m(t)$ и $\varphi_m(t)$ этот промежуток времени отсчитывается от произвольно выбранного времени.

$$\vartheta_m(t) = \lambda \int_0^t [\varphi_{m-1}(x) - \varphi_m(t)] dx, \quad (8.1)$$

$$\lambda = \sum_{m=1}^{\infty} m \vartheta_m(t) = -\vartheta_0'(0) = \left[\int_0^{\infty} \varphi(t) dt \right]^{-1}. \quad (8.2)$$

В потоке с непрерывным временем отсчет последовательно расположенных на оси времени блоков $n_1, \dots, n_r$, которые являются целыми числами, ведется от любого из последовательности дискретных моментов времени. Модель обобщенного пуассоновского потока математически определяется в следующем виде

$$\Psi(t; z) = \sum_{m=0}^{\infty} z^m \vartheta_m(t) = \int_0^{\infty} e^{-\lambda t(1-z)} dF(\lambda), \quad (9)$$

где

$$\vartheta_m(t) = P \{ \xi(\tau_i) - \xi(\tau_{i-1}) = m_i, i = \overline{1, n} \} = \int_0^{\infty} \frac{(\lambda t)^m}{m!} e^{-\lambda t} dF(\lambda). \quad (10)$$

Здесь

$F(\lambda)$ – функция распределения случайного параметра исходного пуассоновского потока (зависит от вида используемого канала связи);

$\xi(\tau)$ – количество событий обобщенного пуассоновского потока, появившихся на промежутках времени $(0; \tau)$;

$\vartheta_m(t)$ – вероятность появления m событий (ошибок) пуассоновского потока на интервале t ;

$\vartheta_0(t)$ – вероятность отсутствия событий (ошибок) ОПП на промежутке времени t ;

$m = \{m_1, m_2, m_3 \dots m_n\}$, $t = \{t_1, t_2, t_3 \dots t_n\}$, $m = m_1 + m_2 + \dots m_n$, $\tau_n = t_1 + t_2 + t_3 + \dots t_n$.

Использование данной модели возможно, в случае, если функция распределения $\vartheta_0(t)$ является преобразованием Лапласа – Стильтеса искомой функции $F(\lambda)$. Удостовериться в этом можно с помощью теоремы С.Н.Бернштейна (или из эксперимента). Так, функция $\vartheta_0(t)$, заданная на промежутке $(0, \infty)$, является преобразованием Лапласа – Стильтеса функции $F(\lambda)$ тогда и только тогда, когда она вполне монотонна и $\vartheta_0(0) = 1$. Функция $\vartheta_0(t)$, заданная на промежутке $(0, \infty)$, называется вполне монотонной, если она имеет производные $\vartheta_0^{(m)}(t)$ всех порядков и $(-1)^m \vartheta_0^{(m)}(t) \geq 0, t > 0$. Из теоремы выявляются следующие правила определения будет ли данная

функция $\vartheta_0(t)$ преобразованием Лапласа – Стильеса искомой функции $F(\lambda)$: если φ вполне монотонна и Ψ – положительная функция с вполне монотонной производной, то $\varphi(\Psi)$ вполне монотонна.

Рассмотрим одномерную функцию распределения интервалов $\varphi(t)$ между событиями потока

$$\varphi(t) = \exp \mu \alpha^{1-\nu} \exp[-\mu(\alpha+t)^{1-\nu}] \left(\frac{\alpha}{\alpha+t} \right)^{\nu}, t \geq 0, \quad (11)$$

$$0 < \nu < 1,$$

где

α, μ, ν – некоторые вспомогательные параметры $\varphi(t)$.

Этот вид обобщенного пуассоновского потока хорошо аппроксимирует поток ошибок в КВ-радиоканалах. Отсюда, параметр потока равен

$$\alpha = \left\{ \int_0^{\infty} \varphi(x) dx \right\}^{-1} = (1-\nu) \mu \alpha^{-\nu}, \quad (12)$$

на основе (1) можно написать вид вероятности $\vartheta_0(t)$ для КВ-радиоканала

$$\vartheta_0(t) = \exp \mu \alpha^{1-\nu} \exp[-\mu(\alpha+t)^{1-\nu}]. \quad (13)$$

Функция $(\alpha+1)^{1-\nu}$ имеет вполне монотонную производную и $e^{-\mu t}$ вполне монотонна, поэтому на основе второго критерия для преобразования Лапласа – Стильеса функция $\vartheta_0(t)$ вполне монотонна. Так как $\vartheta_0(t)=1$, то на основе теоремы С.Н.Бернштейна функция (12) является преобразованием Лапласа-Стильеса некоторой функции распределения $F(\lambda)$, то данный поток можно рассматривать как обобщенный пуассоновский поток.

Производящая функция $\Phi(t; z)$ для рассматриваемого потока есть

$$\Phi(t; z) = \exp \mu \alpha^{1-\nu} \exp\{-\mu[\alpha + (1-z)t]^{1-\nu}\}. \quad (14)$$

Кроме модели КВ – радиоканала в [4,8] рассматривается применение математической модели обобщенного пуассоновского потока к полученным экспериментальным путем распределениям числа ошибок на основе модели двоично-симметричного канала связи. На рисунке 1 приведена схема сети организации передачи данных в Северо-Западном регионе РФ. При передаче данных от территориально разнесенных на большие расстояния объектов в АС УВД укрупненного РЦ, рассматривается возможность использования КВ-радиоканала или двоично-симметричного канала связи между маршрутизаторами – концентраторами Кемь РЦ и Вологда РЦ в качестве резервного, для наличия обходных путей маршрутизации и восстановления работоспособности сети в случае возникновения неисправностей (отказов, конфликтов и перегрузок). Модель потоков ошибок на основе обобщенного пуассоновского потока применимая к самоподобным (фрактальным) потоком в указанных каналах связи и упростит расчет характеристик метода повышения достоверности передачи информации.

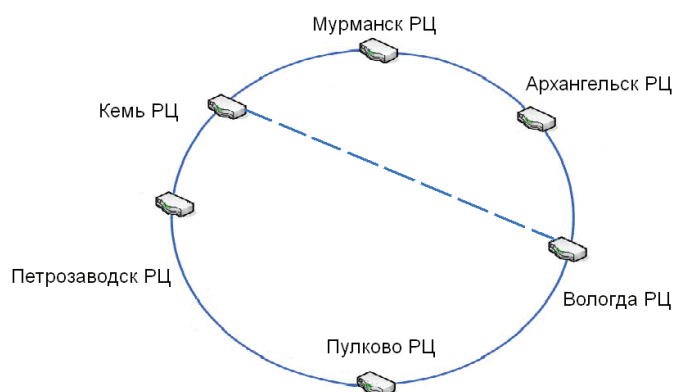


Рис 1. Схема организации сети передачи данных Северо-Западного региона РФ

Заключение. Реорганизация сетей авиационной электросвязи, производимая в рамках Федеральной целевой программы модернизации ЕС ОрВД, предусматривает решение ряда задач по планированию информационной загруженности и безопасности обмена данными между средствами воздушной и наземной связи, наблюдения и автоматизированными системами УВД. Централизация

процесса УВД ведет к резкому возрастанию требований к пропускной способности и качеству используемых каналов связи, в условиях повышения гибкости использования воздушного пространства. В данной статье анализируются угрозы сетям АТН и степень их защищенности от преднамеренных воздействий со стороны нарушителя и оцениваются воздействия случайного характера на безопасность телекоммуникационных систем авиационной электросвязи, на примере влияния самоподобного трафика на качество предоставляемых услуг связи.

СПИСОК ЛИТЕРАТУРЫ

1. Кузьмин Б.И. Современные аспекты концепции ИКАО CNS/ATM в области специальной авиационной электросвязи // электросвязь. – 2007 №11.
2. Постановление Правительства Российской Федерации от 01.09.2008 г. №652.
3. Планирование сети LINK 2000+: Проект. – Eurocontrol, 01.05.07. №3,4. 43с.
4. Аксенов Б.Е., Александров А.М. Повышение достоверности передачи информации в системах управления. Л. ЛПИ им. И.М. Калинина, 1981, №3. С.77.
5. Фомин Л.А., Линец Г.И., Шлаев Д.В., Калашников С.В. Причины самоподобности в сетевом трафике сети // электросвязь. – 2008, №2. С.20–23.
6. Шелухин О.И., Теняков А.М., Осин А.В. Фрактальные процессы в телекоммуникациях. М: Радиотехника, 2003, 408с.
7. Штубов А.С. Применение модели безопасности на основе самоподобных процессов в сетях авиационной электросвязи. // Труды XI Санкт-Петербургской Международной конференции "Региональная информатика–2008" (РИ–2008). Материалы конференции. СПб, 2008. С.166–169.
8. Александров А.М. Информационная безопасность телекоммуникационных систем и их самоподобный трафик // Труды V Межрегиональной конференции "Информационная безопасность регионов России" (ИБРР-2007). Материалы конференции. СПб, 2007. С.203–207.



ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мельник И.А., Примакина Е.И., Щапков Д.А.

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

Россия, Кострома, Костромская государственная сельскохозяйственная академия

**ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ТРЕНИРОВОЧНОГО ПРОЦЕССА НА ОСНОВЕ ДАННЫХ
О ПСИХОФИЗИОЛОГИЧЕСКОМ СОСТОЯНИИ СПОРТСМЕНА, ПОЛУЧЕННЫХ ПОСРЕДСТВОМ
ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

В настоящее время большинство специалистов пришли к общему мнению о том, что спортивная практика разделилась на два направления: массовый спорт и спорт высших достижений для ограниченного числа наиболее одаренных в двигательном и психическом развитии людей. Цель данной статьи – рассмотреть возможности внедрения информационных технологий в область массового спорта, а именно, применение различного рода современных измерительных мини-компьютеров для получения, обработки, анализа и хранения достоверной, точной информации о психофизиологическом состоянии организма человека, занимающегося тем или иным видом спорта, что позволит снизить уровень травматизма и обеспечит безопасность тренировочного процесса [1].

На современном этапе среди спортсменов-любителей популярен метод анализа данных, полученных в результате тренировочного процесса. Целью метода является получение статистических данных спортсмена о его психофизиологическом состоянии в ходе тренировки: частота пульса, ритм сердца, уровень нагрузки на организм, скорость и темп передвижения, пройденное расстояние, количество шагов, время движения, количество калорий потраченных в процессе выполнения упражнений или приемов и так далее. При получении и анализе этих данных, спортсмены и тренеры смогут спланировать и построить график оптимального, с низким уровнем травматизма тренировочного процесса. На сегодняшний день, как правило, применяется ручной метод обработки полученных данных, который сопровождается значительным количеством временных и материальных затрат [2].

В современном спорте уже существуют информационные технологии, позволяющие оптимизировать управление тренировочным процессом и облегчить данную работу. В настоящее время имеется возможность заменить весь процесс сбора и анализа информации простым устройством, в состав которого входят измерительные приборы и средства программного обеспечения. Примерами таких устройств являются спортивные навигаторы, которые зарекомендовали себя при подготовке спортсменов в спорте высших достижений. Подобным устройством может быть спортивный GPS-навигатор «Garmin Forerunner 305 HR», который обладает следующими преимуществами:

- возможностью интеграции с персональным компьютером и использованием прилагаемой программы «Garmin Training Center», позволяющей хранить архивы тренировок (возможность анализировать данные с навигатора позволяет оперативно вносить коррективы в методики тренировок, повышая качество и понижая уровень травматизма процесса физической подготовки);
- возможностью вывода на экран необходимых параметров (время, расстояние, скорость, пульс, навигационные данные и др.) из имеющегося большого количества разнообразных полей данных для оперативного мониторинга во время тренировки (возможна настройка нескольких страниц с данными);
- достаточно удобной формой в виде наручных часов, подходящей для любого размера запястья;
- удобным беспроводным пульсометром, а так же возможностью установки сигнализации при достижении определенного уровня пульса;
- защитой от влаги, позволяющей тренироваться практически в любую погоду;
- возможностью тренироваться в соревновательном режиме по установленной программе с помощью уникальной функции «Виртуальный партнер».

Необходимо отметить, что прибор «Garmin Forerunner 305 HR» создавался для различных спортивных дисциплин (бега, велосипедных тренировок, лыжного спорта, занятий в фитнес-клубах, спортивных единоборств и др.).

Приведем краткие характеристики «Garmin Forerunner 305 HR» [3]:

1. GPS-приёмник нового поколения.
2. Возможность помечать и сохранять до ста мест траектории передвижения.
3. Предусмотрены электронный компас, а также режим карты, отображающий положения ближайших помеченных точек; беспроводной пульсометр с цифровой передачей данных по радиоканалу.
4. Существует возможность подключения беспроводного датчика скорости/частоты вращения педалей.
5. Предусмотрена автоматическая сигнализация в случае пониженного или повышенного пульса спортсмена.
6. Имеется возможность накопления полной статистики о работе сердца во время тренировок.
7. Предусмотрено подключение функции «виртуальный партнер», позволяющей сравнивать предыдущие тренировочные показатели с текущими.

Наличие беспроводного пульсометра – ещё одно отличительное достоинство модели «Garmin Forerunner 305 HR». Он представляет собой эластичный пояс, который надевается на грудь спортсмена. С внутренней стороны этого пояса размещаются два датчика, плотно прилегающие к рёбрам испытуемого. Пояс не имеет выключателя – он включается автоматически при инициализации и выключается так же сам, когда вы его снимаете с тела. Необходимо отметить, что многие аналогичные пульсометры не имеют такой возможности, и замена питающего элемента там превращается в сложную работу. Таким образом, фиксируются основные параметры психофизиологического состояния.

Однако, такое большое количество информации не поместится на одном экране. Поэтому в «Garmin Forerunner 305 HR» предусмотрено наличие нескольких страниц с полями данных, количество которых варьируется от вида спорта. На этих страницах могут отражаться электронный компас, график высоты, карта, отставание или опережение вашего виртуального партнёра и т.д. Меню навигатора простое, с древовидной структурой, как на сотовых телефонах. Прибор ориентирован на использование в беге, на велосипеде или в другом циклическом виде спорта, к примеру, на лыжах, так же допустимо его использование и в других видах спорта.

«Garmin Forerunner 305 HR» обладает возможностью настраиваться в зависимости от вида спорта, который не относится к бегу, спортивной ходьбе или езде на велосипеде, при этом можно самим задавать границы скорости и нагрузки тренировочного цикла.

В приборе предусмотрена функция «многоборье» для тех, кто одновременно тренируется по нескольким направлениям. С помощью этой функции возможно тренироваться и в беге, и в заездах на велосипеде. Если тренировочный цикл предусматривает дополнительный груз (например, спортивный рюкзак), прибор будет учитывать эту нагрузку.

Для тех же, кто не стремится к рекордам, предусмотрена более простая функция – «виртуальный партнёр».

Любой пройденный маршрут записывается в памяти прибора, возможно просмотреть его, выбрав конкретный день, неделю или месяц тренировок. Любой маршрут можно превратить в трассу, чтобы снова и снова проходить её, улучшая результат.

В состав устройства входит программное обеспечение (ПО) «Garmin Training Center» – это мощная система обработки статистики тренировок. При подключении «Garmin Forerunner 305 HR» к компьютеру программа автоматически запускается и считывает из памяти навигатора свежие данные тренировок.

В программе «Garmin Training Center» предусмотрен удобный планировщик, с помощью которого можно создавать собственные программы тренировок. Например, пройти 5 километров с определённой скоростью, затем бежать, поддерживая ритм сердца в определённой зоне, после этого отдохнуть, а дальше бегать, пока не сожгутся 500 калорий. Любую собственную программу можно записать обратно в прибор и воспользоваться ею в любое время.

Программа «Garmin Training Center» позволяет создавать разные профили для разных пользователей, что может быть полезным для командной тренировки, в которой один тренер сможет на одном компьютере просматривать данные разных спортсменов.

Экспериментальная часть статьи описывает работу устройства «Garmin Forerunner 305 HR», а так же его программного обеспечения «Garmin Training Center».

В ходе тренировок (бег на дистанции в 4500 метров) Пививарова Николая Леонидовича, 1992 года рождения, не профессионального спортсмена, были сняты следующие показатели и приведены в графиках (рисунок 1):

- средний пульс по всей дистанции, а так же его максимальные показатели;
- средняя скорость по всей дистанции, а также его минимальные и максимальные показатели;
- количество калорий потраченных в процессе тренировки;
- общее время тренировки, с учетом фиксирования каждого пройденного этапа;
- график отображает полную информацию за определенный период времени.

Еще одной возможностью обладает данное ПО «Garmin Training Center», позволяет проецировать траекторию движения на реальную карту, взятую со спутника, например карты «Google».

После неоднократных тестов данного устройства можно сделать определенные выводы:

во-первых, есть возможность систематизировать упражнения, после которых появится дополнительный стимул повышать нагрузку и планировать тренировки;

во-вторых, изометрический компьютер «Garmin Forerunner 305 HR» своевременно предупредит о превышении допустимых нагрузок, которые могут негативно отразиться на работе сердца и организма в целом;

в-третьих, «Garmin Forerunner 305 HR» – это современный и функциональный компьютер, который фиксирует не только скорость и расстояние, но и высоту, уклон, темп и десятки других показателей, необходимых для организации тренировочного процесса, что снижает уровень травматизма спортсменов.

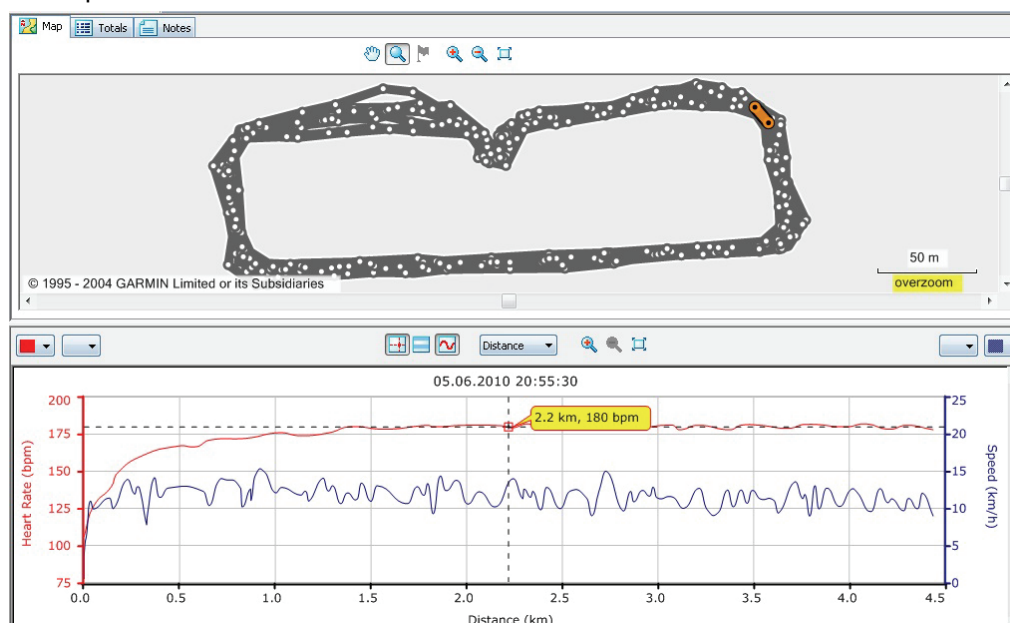


Рис.1. График отображения данных ПО «Garmin Training Center»

На рисунке 2 представлена полная информация, о том, где конкретно тренировался Пивоваров Н.Л.

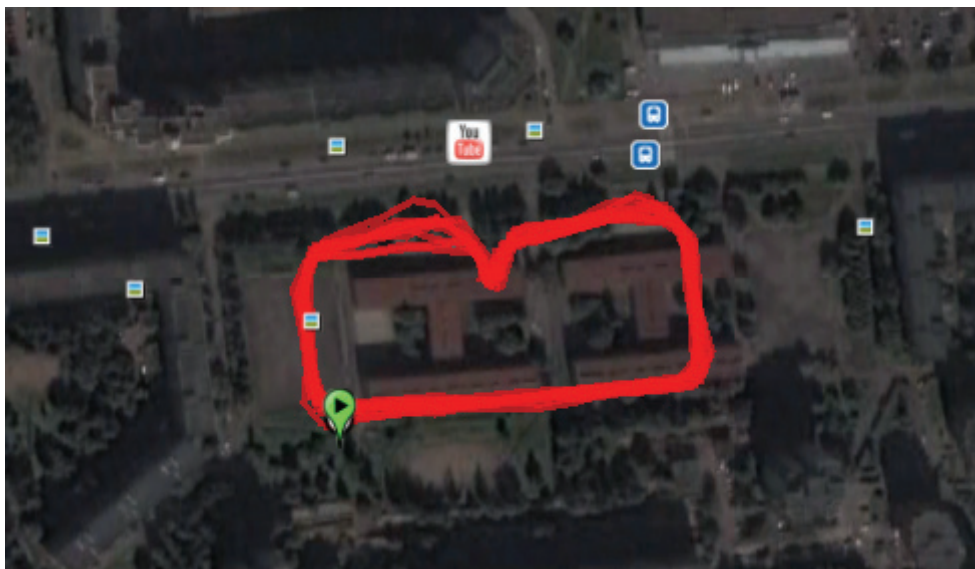


Рис. 2. Траектория движения Пивоварова Н.Л.

СПИСОК ЛИТЕРАТУРЫ

1. Богданов В.М., Пономарев В.С., Соловов А.В. Использование современных информационных технологий в теоретической и методико-практической подготовке студентов по физическому воспитанию /Материалы всероссийской научно-практической конференции. СПб., 2000. С. 21–34.
2. Шестакова М.П., Попова Г.И. Статистика. Обработка спортивных данных на компьютере: Учебное пособие для студентов высших учебных заведений физической культуры. М.: СпортАкадемПресс, 2002. 278 с.
3. Информационный портал URL: [http:// www.sat-tech.ru/garmin-erunner.shtml](http://www.sat-tech.ru/garmin-erunner.shtml)
4. Информационный портал URL: [http:// www.divi.ru/articles/gps/garmin-forerunner-305](http://www.divi.ru/articles/gps/garmin-forerunner-305)

Примакин А.И.

**Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
К ВОПРОСУ О ПОДГОТОВКЕ СОТРУДНИКОВ ОВД В САНКТ-ПЕТЕРБУРГСКОМ
УНИВЕРСИТЕТЕ МВД РОССИИ ПО СПЕЦИАЛЬНОСТИ 090103 – ОРГАНИЗАЦИЯ
И ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ**

В статье Министра внутренних дел РФ, генерала армии Нургалиева Р.Г. «Электронный патруль» («Российская газета» от 16 октября 2009 года) дается оценка новым видам преступности в сфере информационных технологий, основным формам, методам и результатам оперативно-служебной деятельности в этой области. Одной из актуальных задач, которую, как отметил министр, необходимо решить на сегодняшний день – одготовка собственных кадров и привлечение к работе в правоохранительных органах высококвалифицированных специалистов способных эффективно бороться с киберпреступностью.

Анализ статистических данных о преступлениях, совершаемых в сфере компьютерной информации, показывает, что в России, начиная с 2000-х годов, наблюдается 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 с января по май 2009 года ОВД еженедельно возбуждали от 50 до 100 уголовных дел. За шесть месяцев этого года было зарегистрировано 11 333 преступления.

Природа компьютерных преступлений придает проблеме глобальный, транснациональный характер. Так называемый виртуальный мир стал не только высокотехнологичным достижением современности, но и источником угроз. Вот почему сегодня важно еще и международное сотрудничество в данной сфере.

Россия активно участвует в международном многостороннем и двустороннем сотрудничестве по борьбе с киберпреступностью, выступает за разработку международной стратегии комплексного противодействия киберугрозе и создание единых международно-правовых механизмов с целью унификации национальных уголовных законодательств.

МВД России является постоянным участником международных семинаров и симпозиумов в форматах ОБСЕ, «восьмерки», Интерпола и других. Только в 2009 году министерство приняло участие в 22 международных мероприятиях, посвященных различным аспектам этой деятельности: от кибертерроризма до мошенничества с пластиковыми карточками и детской порнографии в Интернете.

Так в апреле 2009 года в Германии прошел III международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму». В нем приняли участие представители Совета Европы, аппарата ООН, университетских центров Европы и США. Россию представляли управление «К» МВД, Совет безопасности РФ, МИД, Минкомсвязь, ФСБ. Мероприятие способствовало взаимопониманию сторон, укреплению контактов и продвижению в странах-участниках политики активного обмена информацией о преступлениях в информационной сфере между правоохранительными органами.

Особое внимание было обращено к организации и проведению в 2009 году в Москве Конференции Россия – ЕС «Детская безопасность в Интернете – предотвращение, обучение, сотрудничество».

В июне 2009 г. в Казани состоялся V Евразийский форум информационной безопасности «Инфофорум – Евразия», участники которого обсудили актуальные проблемы безопасности личности, общества и государства в условиях развития глобального информационного общества, поделились опытом создания комплексных решений для внедрения технологий «электронного правительства». Итогом встречи явилось принятие резолюции «Международные аспекты информационной безопасности» – «ИНФОФОРУМ – Казань».

Касаясь темы организации и проведения международных и межрегиональных форумов, хотелось бы отметить, что 28-30 октября 2009 года в рамках VI Санкт-Петербургской

межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2009) на базе Санкт-Петербургского университета МВД России работала одна из шести секций – «Правовые аспекты информационной безопасности». В программу работы секции было заявлено 22 доклада, зарегистрировано 27 человек. Тезисы выступлений были опубликованы к началу работы 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 Лаврентьевну.

Секция рекомендовала отразить в итоговых документах конференции:

- 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;
- необходимость отражения в образовательных стандартах нового поколения вопросов информационного права и информационной безопасности, включая институты тайн и конфиденциальности информации, а также усилить внимание к изучению возможных негативных последствий влияния «социально-вредной» информации.

В заключительной части статьи «Электронный патруль» министр обратил внимание на техническое перевооружение ведомства. Если еще в 2005 году количество приобретаемых новых образцов техники и вооружения составляло 7 % от общего объема закупок, то в 2008 году – уже третью часть.

На заседании расширенной коллегии МВД (февраль 2009 г.) были отмечены две тенденции: снижение уровня тяжких и особо тяжких преступлений и повышение уровня их раскрываемости. Но особо подчеркнуто, что результаты достигнуты благодаря разработкам Бюро специальных технических мероприятий и их внедрению в практику министерства.

Важнейшим шагом по развитию современных подходов к борьбе с преступностью стало создание Единой информационно-телекоммуникационной системы органов внутренних дел (ЕИТКС). Ее использование уже сегодня предоставляет милиции широчайшие информационные возможности: от моментального получения информации из специализированных баз данных федерального и регионального уровней до проведения видеоконференций и осуществления образовательных программ для сотрудников органов внутренних дел. В рамках реализации Программы ЕИТКС серьезно укреплен и криминалистический блок – создана сеть автоматизированных лабораторий по идентификации голоса, ДНК-анализа, автоматизированных дактилоскопических информационных систем. По итогам 2008 года применение технологического оборудования и аппаратно-программных комплексов, поставляемых в рамках ЕИТКС новых технических возможностей, способствовало раскрытию более 689 тысяч преступлений.

Компьютерные технологии открывают совершенно новые, еще не исследованные технологические варианты обучения, связанные с уникальными возможностями современных компьютеров и телекоммуникаций. Компьютерная технология может осуществляться в следующих двух вариантах:

- как «проникающая» технология (применение компьютерного обучения по отдельным темам и разделам);
- как «основная», монотехнология (когда все обучение, все управление учебным процессом, включая все виды диагностики, мониторинг, опираются на применение компьютера).

Кафедра информационной безопасности и математических методов Санкт-Петербургского университета МВД России (ИБиММ) имеет десятилетний опыт преподавания учебной дисциплины «Основы информационной безопасности в ОВД», объем которой небольшой (30 часов), но она изучается на всех факультетах университета.

Можно считать, что при изучении данной дисциплины применение компьютерных технологий максимально приближенно к использованию их в качестве «основных», как монотехнологий.

В рамках отмеченной дисциплины рассматриваются как теоретические вопросы об основах информационной безопасности в информационных системах, о возможных каналах утечки информации и несанкционированном доступе к ней, так и практические – связанные с криптографическими и стеганографическими способами защиты информации, с изучением и практической отработкой алгоритма электронной цифровой подписи. Вполне естественно, что для лучшего понимания и освоения курсантами этих вопросов, необходим лабораторный практикум, который и был разработан совместно с преподавателями Военно-морского института радиоэлектроники им. А.С. Попова.

Криптография наука не простая (тем более, для гуманитариев), но данный лабораторный практикум позволяет не только достаточно просто и наглядно изложить курсантам основы криптографии, но и дает им возможность самостоятельно проверить себя – насколько правильно они

поняли учебный материал, обратившись к разделу практикума «Проверка знаний и методов шифровки».

Новые информационные технологии применимы при изучении различных разделов еще одной учебной дисциплины изучаемой на кафедре ИБиММ – математики.

Для визуализации математических знаний возможно использование:

- специализированных электронных учебных комплексов, сочетающих в себе фундаментальный теоретический материал, практикум, контрольные тесты, интерактивные модели, позволяющие эффективно изучать курс даже самостоятельно;

- прикладные пакеты программ, например, MathCAD, Mathematica и другие;

- повсеместно применяемая программа из пакета Microsoft Office – Excel.

Следует отметить, что применение математических пакетов при решении задач следует сочетать с традиционными методами, ибо понимание содержания задачи имеет главенствующее значение. При обучении математике компьютер выполняет различные функции, позволяющие обучаемому глубже разобраться в сути вопроса, а также закрепить приобретенные знания, выработать твердые умения и навыки.

В данном случае, компьютерные технологии можно рассматривать как «проникающие» технологии. Например, применение компьютерных средств при решении уравнений ориентируется на личные установки (мотивации) обучаемого: он имеет возможность совершенствовать свои знания и осмысливать полученную информацию, используя как графические средства, так и аналитические методы.

Следующая учебная дисциплина, изучаемая на кафедре – концепции современного естествознания.

Предметная область ее достаточно обширная – это и физика, и химия, и биология, и основы культурологи и философии, и астрономия. Поэтому традиционное применение презентаций, помимо наглядности и удобства записи студентами темы занятия, учебных вопросов и основных ключевых определений учебной дисциплины, позволяет преподавателю четче держать нить изложения, сопровождать излагаемый материал иллюстрациями, делая его более интересным и понятным для восприятия учащимися. Существенна в этом роль видеофильмов, тематика которых максимально охватывает изучаемые разделы дисциплины.

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»;

- «Программно-аппаратная защита информации»;

- «Инженерно-техническая защита информации»;

- «Комплексная система защиты информации на предприятии»;

- «Применение информационных технологий в аналитической разведке»;

- «Компьютерные информационные системы»;

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

В план развития учебно-материальной базы Санкт-Петербургского университета МВД России до 2012 года было включено создание лаборатории «Технические средства разведки и защиты информации» с приобретением комплекса оборудования для проведения лабораторных практических работ.

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.

Он 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. Он позволяет обеспечить проведение

следующих лабораторных работ по учебной дисциплине «Комплексная система защиты информации на предприятии»:

- 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:

1. 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).

2. Устройства виброакустической защиты (генератор виброакустических помех для защиты помещений от аппаратуры съёма речевых сигналов, использующей вибропреобразователи на стенах, потолках, окнах, воздуховодах прослушиваемого помещений).

3. Поисковые приборы (быстрое автоматическое обнаружение сигналов, излучаемых нелегальными радиопередатчиками и подавление каналов их приема).

4. Индикаторы поля (обнаружение, распознавание и определение местонахождения различных источников радиоизлучения).

5. Устройства подавления диктофонов.

Таким образом, наряду с изучением различных теоретических дисциплин, в процессе обучения в данной лаборатории, курсант:

1. Получит представление о программном и аппаратном обеспечении средств защиты информации, основах построения компьютерных сетей и их защиты от внешних угроз.

2. Ознакомится с различными сетевыми технологиями глобальных и локальных вычислительных сетей.

3. Освоит методы и средства сбора, обработки, хранения, накопления, передачи информации.

4. Научится разбираться в различных способах разграничения прав доступа к информации и средствах её защиты.

При проведении лабораторных работ курсант приобретёт практические навыки по использованию базовых системных программных продуктов и пакетов прикладных программ.

ОГЛАВЛЕНИЕ

ПЛЕНАРНЫЕ ДОКЛАДЫ	11
Цивирко Е.Г. Россия, Санкт-Петербург, Комитет по информатизации и связи Санкт-Петербурга ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ САНКТ-ПЕТЕРБУРГА	11
Федоров А.В. Россия, Москва, Министерство юстиции Российской Федерации О ГАРМОНИЗАЦИИ И УНИФИКАЦИИ ЗАКОНОДАТЕЛЬСТВА О ГОСУДАРСТВЕННОЙ ТАЙНЕ В ГОСУДАРСТВАХ – УЧАСТНИКАХ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ.....	12
Кононов А.А., Стиславский А.Б., Цыгичко В.Н., Черешкин Д.С. Россия, Москва, Институт системного анализа РАН АВТОМАТИЗИРОВАННЫЙ КОМПЛЕКС СРЕДСТВ ОБЕСПЕЧЕНИЯ АНТИТЕРРОРИСТИЧЕСКОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ ТРАНСПОРТНОЙ СИСТЕМЫ	15
Бачило И.Л. Россия, Москва, Институт государства и права РАН ПРОБЛЕМЫ РАЗВИТИЯ ИНФОРМАЦИОННОГО ЗАКОНОДАТЕЛЬСТВА.....	21
Зегжда Д.П., Калинин М.О. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет ТЕХНОЛОГИЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ СРЕД ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ	27
Молдовян А.А., Молдовян Н.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ПЕРСПЕКТИВЫ РАЗВИТИЯ КРИПТОГРАФИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ	35
Вус М.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН О ГАРМОНИЗАЦИИ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА В ГОСУДАРСТВАХ – УЧАСТНИКАХ МЕЖПАРЛАМЕНТСКОЙ АССАМБЛЕИ СНГ	40
ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ	45
Блашков В.И., Ермохин К.М. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России, ООО НПП «Аналитическая геофизика» ФИЗИЧЕСКАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО ПОЛЯ И ЕГО ВЗАИМОДЕЙСТВИЯ С МАТЕРИЕЙ В СВЕТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧЕЛОВЕКА И ОБЩЕСТВА	45
Воропаев Д.Б. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН АНАЛИЗ МЕТОДОВ ФОРМИРОВАНИЯ СТОИМОСТИ ЭЛЕМЕНТОВ СЛОЖНЫХ ВОЕННО-ТЕХНИЧЕСКИХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	48
Воропаев Д.Б. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН АНАЛИЗ СОВРЕМЕННЫХ ПРОБЛЕМ ЦЕНООБРАЗОВАНИЯ НА ЭЛЕМЕНТЫ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИЛОВЫХ СТРУКТУР.....	58

Дудкина О.К., Копыльцов А.В. Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена СОЗДАНИЕ ГОРОДСКОГО МОНИТОРИНГОВОГО ЦЕНТРА ЭКСТРЕМАЛЬНЫХ СИТУАЦИЙ.....	63
Колин К.К. Россия, Москва, Институт проблем информатики РАН КАЧЕСТВО ЖИЗНИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИИ	67
Сальников М.А., Копыльцов А.В. Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена ПЕРСПЕКТИВЫ РАЗВИТИЯ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ В РОССИИ.....	73
ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	76
Абламейко М.С., Абламейко С.В. Белоруссия, Минск, Белорусский государственный университет ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ОТ КИБЕРАТАК: МЕЖДУНАРОДНЫЕ АКТЫ	76
Алексеев А.А. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России О СТИМУЛИРОВАНИИ ТРУДОВОЙ ДЕЯТЕЛЬНОСТИ ПЕРСОНАЛА, ОБЕСПЕЧИВАЮЩЕГО ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ	76
Вус М.А., Кондратьев В.В., Заболотский В.П., Старков А.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный университет информационных технологий, механики и оптики О СОВЕРШЕНСТВОВАНИИ ЗАКОНОДАТЕЛЬСТВА ГОСУДАРСТВ – УЧАСТНИКОВ СНГ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	78
Домбровская Л.А. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России УТЕЧКА ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ	81
Журавков И.А. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ПОЛИГРАФ КАК СРЕДСТВО ПОЛУЧЕНИЯ ИНФОРМАЦИИ НА СТАДИИ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ	84
Никишкин А.В., Оськин Ф.Ф. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ СИСТЕМЫ ФУНКЦИОНИРОВАНИЯ ПОДРАЗДЕЛЕНИЙ ГОСУДАРСТВЕННОЙ ИНСПЕКЦИИ БЕЗОПАСНОСТИ ДОРОЖНОГО ДВИЖЕНИЯ ГОРРАЙОРГАНОВ ВНУТРЕННИХ ДЕЛ.....	85
Ороева О.Д. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России СОСТОЯНИЕ НОРМАТИВНОГО ПРАВОВОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПРАВ И СВОБОД ЧЕЛОВЕКА И ГРАЖДАНИНА, РЕАЛИЗУЕМЫХ В ИНФОРМАЦИОННОЙ СФЕРЕ	89
Осипов Я.В. Россия, Архангельск, Следственное управление при УВД по Архангельской области КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ ДИАГНОСТИКИ ЛЖИ.....	91
Потапов Ю.А. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России РЕАЛИЗАЦИЯ МЕЖДУНАРОДНО-ПРАВОВЫХ АКТОВ О СВОБОДЕ ИНФОРМАЦИИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ.....	97

Примакин А.И., Мельник И.А., Щапов Д.А. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ СВЯЗИ НА ПРИМЕРЕ ТЕЛЕФОНИИ	99
Черепанова Ю.Е. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России К ВОПРОСУ О ТЕРМИНЕ «ЗАЩИТА ИНФОРМАЦИИ»	102
БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ	104
Асанович В.Я., Зеленцов В.А., Соколов Б.В., Цивирко Е.Г. Беларуссия, Минск, Белорусский государственный экономический университет Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Комитет по информатизации и связи Санкт-Петербурга МЕТОДОЛОГИЧЕСКИЕ И МЕТОДИЧЕСКИЕ ОСНОВЫ КОМПЛЕКСНОГО ПЛАНИРОВАНИЯ РАЗВИТИЯ КАТАСТРОФУСТОЙЧИВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	104
Афанасьев С.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО КОДА НА СТАДИИ РАЗРАБОТКИ	108
Блюм В.С., Заболотский В.П. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПАЦИЕНТОВ КАК КОМПОНЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА	111
Гарбук С.В., Завируха В.К., Комаров А.А. Россия, Санкт-Петербург, Арктический и антарктический научно-исследовательский институт, Москва, ЗАО «Научно-технический центр «Станкоинформзащита» ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА КРИТИЧЕСКИ ВАЖНЫХ ТЕХНОЛОГИЧЕСКИХ ОБЪЕКТАХ	118
Десницкий В.А., Котенко И.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН РАЗРАБОТКА И АНАЛИЗ ПРОТОКОЛА УДАЛЕННОГО ДОВЕРИЯ	121
Колодин М.Ю., Федорченко Л.Н. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН МЕТАТЕХНОЛОГИИ В СИСТЕМАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	129
Копыльцов А.В., Сорокин И.В. Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена ЭНТРОПИЙНЫЙ АНАЛИЗ ФАЙЛОВ ДЛЯ ВЫЯВЛЕНИЯ И КЛАССИФИКАЦИИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	135
Любимов А.В. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет СОГЛАСОВАНИЕ ПОЛУФОРМАЛЬНЫХ МОДЕЛЕЙ ПРИ ИНЖИНИРИНГЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	140
Нестеров М.Ф., Кондратьев В.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ТАКТИКА НАРАЩИВАНИЯ СИЛ И СРЕДСТВ АУТСОРСИНГА ДЛЯ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА КОММЕРЧЕСКОМ ПРЕДПРИЯТИИ	145
Никифоров В.В., Шкиртиль В.И. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ЗАЩИТА ЦЕЛОСТНОСТИ ДАННЫХ В ПРОГРАММНЫХ ПРИЛОЖЕНИЯХ РЕАЛЬНОГО ВРЕМЕНИ	150

Орлов К.М. Россия, Санкт-Петербург, 4 филиал ВУНЦ ВМФ «Военно-морская академия» ФОРМИРОВАНИЕ СИСТЕМЫ ОЦЕНКИ КАЧЕСТВА ВИЗУАЛИЗАЦИИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ.....	156
Соколова С.П., Горковенко Е.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Республика Казахстан, Алма-Ата, Институт проблем информатики и управления МОН РК ПРИМЕНЕНИЕ СОВРЕМЕННЫХ МЕТОДОВ МНОГОУРОВНЕВОГО КОНТРОЛЯ ДОСТУПА В КОРПОРАТИВНОЙ СЕТИ КОСМИЧЕСКОЙ ИНФРАСТРУКТУРЫ	160
СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ	166
Алексеев А.В. Россия, Санкт-Петербург, ОАО «Научно-инженерный центр Санкт-Петербургского электротехнического университета» КЛАССИФИКАЦИЯ И РЕЙТИНГ-АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОСНОВНЫХ КЛАССОВ	166
Галанов А.И., Дернова Е.С., Молдовян Д.Н. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» НОВЫЕ СХЕМЫ СЛЕПОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ	173
Гордеев Л.В., Чистяков Ю.В. Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс» АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	180
Костин А.А., Дернова Е.С., Молдовян Д.Н. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН РЕАЛИЗАЦИЯ ПРОТОКОЛОВ СЛЕПОЙ ПОДПИСИ НА ОСНОВЕ СТАНДАРТОВ ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 И СТБ 1176.2-99	182
Молдовян Д.Н., Дернова Е.С. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» КРИПТОГРАФИЧЕСКИЕ ПРИМИТИВЫ НАД КОНЕЧНЫМИ ВЕКТОРНЫМИ ПРОСТРАНСТВАМИ	191
Харинов М.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН СЕГМЕНТАЦИЯ ИЗОБРАЖЕНИЯ С СОХРАНЕНИЕМ ЗРИТЕЛЬНОГО ОБРАЗА.....	198
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ	203
Примакина Е.И. Россия, Кострома, Костромская государственная сельскохозяйственная академия МЕТОДИКА ОЦЕНКИ ПРОФЕССИОНАЛЬНО ЗНАЧИМЫХ НАВЫКОВ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	203
Хвостунов Ю.С. Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс» АВТОМАТИЗИРОВАННЫЙ КОМПЛЕКС СРЕДСТВ СКОРОСТНОЙ АДАПТИВНОЙ ПОМЕХОЗАЩИЩЕННОЙ СИСТЕМЫ РАДИОСВЯЗИ	206
Штубов А.С. Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс» АНАЛИЗ БЕЗОПАСНОСТИ СЕТЕЙ АВИАЦИОННОЙ ЭЛЕКТРОСВЯЗИ.....	209
ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	215

Мельник И.А., Примакина Е.И., Щапов Д.А. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России Россия, Кострома, Костромская государственная сельскохозяйственная академия ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ТРЕНИРОВОЧНОГО ПРОЦЕССА НА ОСНОВЕ ДАННЫХ О ПСИХОФИЗИОЛОГИЧЕСКОМ СОСТОЯНИИ СПОРТСМЕНА, ПОЛУЧЕННЫХ ПОСРЕДСТВОМ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.....	215
Примакин А.И. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России К ВОПРОСУ О ПОДГОТОВКЕ СОТРУДНИКОВ ОВД В САНКТ-ПЕТЕРБУРГСКОМ УНИВЕРСИТЕТЕ МВД РОССИИ ПО СПЕЦИАЛЬНОСТИ 090103 – ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ.....	218
ОГЛАВЛЕНИЕ.....	222