ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2011)

VII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 26-28 октября 2011 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург
2011

http://spoisu.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2011)

VII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 26-28 октября 2011 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург
2011

http://spoisu.ru

УДК (002:681):338.98

И 74

И 74 **Информационная** безопасность регионов России (ИБРР-2011). VII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 26-28 октября 2011 г.: Материалы конференции / СПОИСУ. – СПб., 2011. – 222 с.
ISBN 978-5-905183-92-8

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

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

УДК (002:681):338.98

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

Публикуется в авторской редакции

Подписано в печать 12.10.2011. Формат 60x84⅛. Бумага офсетная.
Печать – трафаретная. Усл. печ. л. 25,8. Тираж 400 экз. Заказ № 3016
Отпечатано в ООО «Политехника-сервис»
191011, Санкт-Петербург, ул. Инженерная, 6

ISBN 978-5-905183-92-8

INFORMATION SECURITY OF RUSSIAN REGIONS (ISRR-2011)

VII ST. PETERSBURG INTERREGIONAL CONFERENCE

St. Petersburg, October 26-28, 2011

PROCEEDINGS OF THE CONFERENCE

St. Petersburg

2011

http://spoisu.ru

УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ «ИБРР-2011»

- 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-2011»

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

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

КООРДИНАЦИОННЫЙ СОВЕТ КОНФЕРЕНЦИИ «ИБРР-2011»

Полтавченко Георгий Сергеевич	Губернатор Санкт-Петербурга
Тюльпанов Вадим Альбертович	Председатель Законодательного собрания Санкт-Петербурга
Сердюков Валерий Павлович	Губернатор Ленинградской области
Макаров Евгений Иванович	Помощник полномочного представителя Президента Российской Федерации в Северо-Западном федеральном округе
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
Макаров Евгений Иванович	Помощник полномочного представителя Президента Российской Федерации в Северо-Западном федеральном округе
Никандров Николай Дмитриевич	Президент Российской академии образования

ПРЕЗИДИУМ КОНФЕРЕНЦИИ «ИБРР-2011»

Тихонов Валерий Владимирович	Вице-губернатор Санкт-Петербурга
Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга
Юсупов Рафаэль Мидхатович	Директор Санкт-Петербургского института информатики и автоматизации Российской академии наук
Селин Владимир Викторович	Директор ФСТЭК России
Демидов Александр Алексеевич	Председатель Комитета по информатизации и связи Санкт-Петербурга
Акулич Владимир Александрович	Генеральный директор ОАО «Северо-Западный Телеком»

Васильев Владимир Николаевич	Председатель совета ректоров Санкт-Петербурга, ректор Санкт-Петербургского государственного университета информационных технологий, механики и оптики
Гусев Владимир Сергеевич	Вице-президент Международного Банка «Санкт-Петербург»
Кучерявый Михаил Михайлович	Руководитель Управления Федеральной службы технического и экспортного контроля по Северо-Западному федеральному округу
Лопота Виталий Александрович	Президент - генеральный конструктор Ракетно-космической корпорации «Энергия» им. С.П. Королева
Максимов Андрей Станиславович	Председатель Комитета по науке и высшей школе Санкт-Петербурга
Пешехонов Владимир Григорьевич	Генеральный директор ГНЦ «Центральный научно-исследовательский институт «Электроприбор»
Федоров Александр Вячеславович	Первый заместитель Министра юстиции Российской Федерации
Цивирко Евгений Геннадьевич	Председатель Комитета по работе с исполнительными органами государственной власти и взаимодействию с органами местного самоуправления Администрации Санкт-Петербурга
Шульц Владимир Леопольдович	Заместитель президента Российской академии наук

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2011»

Председатель Организационного Комитета

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

Заместитель председателя Организационного Комитета

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

Члены Организационного Комитета

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

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

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

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2011»

Председатель Программного Комитета

Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга

Заместители председателя Программного Комитета

Жигадло Валентин Эдуардович	Генеральный директор ООО «Максима»
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**

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ

Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

КВАЛИМЕТРИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ СИСТЕМАМИ ЗАЩИТЫ ИНФОРМАЦИИ

Измерение качества (квалиметрическое оценивание) систем защиты информации (СЗИ) с комплексной оценкой их соответствия своему предназначению, т.е. в соответствии с законом №184-2002-ФЗ «О техническом регулировании» оценкой их валидности (оценкой степени достижения СЗИ цели при выполнении соответствующих задач), является методически сегодня более, чем неоднозначной. Несмотря на то, что именно эти количественные одиночные и комплексные оценки должны лежать в основе принимаемых решений о сертификации соответствующих СЗИ по данным сертификационных испытаний, проводимых многочисленными испытательными лабораториями и испытательными центрами. Методически квалиметрическое обеспечение данных решений, в том числе на основе комплексных (интегральных) оценок по сводному показателю качества (СПК), обеспечивает уникальную возможность сравнительного анализа, рейтинг-анализа широкого спектра разнотипных СЗИ и их систем. Кроме того, уникальную возможность перехода от квалиметрического анализа к обоснованному целенаправленному синтезу и оптимизации сложных интегральных проектных и управленческих решений (ПУР) по выбору архитектуры и параметров СЗИ.

Так, например, число соответствующих компаний-интеграторов сегодня непрерывно увеличивается, а используемая методология проектирования сводится в лучшем случае к функциональному наращиванию, «лоскутному» информационно-техническому сопряжению типовых ПУР без каких либо количественных оценок достигаемого при этом качества. Как следствие, необоснованно наращивается избыточность СЗИ и их комплексов, как наличие возможностей, превышающих необходимые для достижения заданных целей и решения поставленных задач.

К другим издержкам подобного «комплексирования» и «интегрирования» относятся увеличение ресурсных (финансовых, людских, энергетических, материальных) затрат, увеличение сроков проектирования, создания и внедрения СЗИ, а также снижение их надёжности, возможности комфортной эксплуатации. Но главное, это приводит к потере конкурентоспособности СЗИ на рынке.

Как следствие подобного развития СЗИ, расширение перечня нормативных требований и соответствующие «специфические» особенности нормативного управления политиками безопасности.

В этих условиях, реализация принципа Доктрины ИБ (2000 г.) об информационной прозрачности обеспечения ИБ на основе единства и открытости данных о качестве СЗИ по СПК, как интегральном показателе качества, получаемых в ходе сертификационных испытаний, может рассматриваться, как главный принцип и методология управления информационной безопасностью и системой защиты информации в целом. При этом, затраты на реализацию данного «доктринного принципа» носят исключительно управленческий и волевой характер, вполне вписываются в функции и возможности заинтересованных ведомств.

Научно-методическая реализация «доктринного принципа» может быть представлена регламентированием использования немногочисленных методик оценивания СПК СЗИ, в том числе на основе мультипликативной модели агрегирования базовых критериев обеспечения ИБ «конфиденциальность – доступность – целостность» (оценки защищённости по СПК «качество СЗИ»). Последующее использование известного полимодельного подхода (например, по технологии «КРОПУР», «АСОР») с заданием соответствующих отношений предпочтений частных моделей качества СЗИ позволит системно целостно и многоаспектно анализировать качество СЗИ. Необходимые для этого исходные данные в полном объёме могут быть заимствованы из соответствующих актов и протоколов проведения сертификационных испытаний. Это, естественно, не только не представляет угроз безопасности при соответствующих регламентах, но и существенно расширит практическую базу развития теории и методологии сертификации.

Наконец, вариантное проектирование с использованием этого же квалиметрического аппарата и соответствующих автоматизированных систем поддержки принятия ПУР позволит информационно прозрачно переходить к решению задач оптимизации ПУР, задач верификации и оценке валидности СЗИ, включая оценку обоснованности качества и оптимальности подсистем управления

безопасностью и в целом эрготехнических систем (ЭТС). В свою очередь, накопление, систематизация подобных данных позволит формировать базы данных и знаний СЗИ в составе различных классов ЭТС для научно-обоснованного выбора направлений развития средств, комплексов и их систем.

С другой стороны, формирование баз данных и знаний ЭТС по СПК обеспечит качественно новый уровень организации и проведения сертификации СЗИ, аттестации объектов информатизации, профессиональной подготовки и лицензирования юридических и физических лиц.

Тем самым, квалиметрическое обеспечение управления системами защиты информации может рассматриваться, как важнейшее системообразующее средство обеспечения и управления качеством ЭТС, включая управление её ключевыми элементами – системами защиты информации.

Барабаш П.А., Советов Б.Я.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

О РАБОТЕ КОМИССИИ ПО ИНФОРМАТИЗАЦИИ И СВЯЗИ ОБЩЕСТВЕННОГО СОВЕТА САНКТ-ПЕТЕРБУРГА В 2011 ГОДУ

В 2011 году работа Комиссии по информатизации и связи Общественного совета Санкт-Петербурга велась по следующим направлениям:

– развитие Информационного общества в Санкт-Петербурге и его
– нормативно-правовое обеспечение;
– электронное правительство Санкт-Петербурга;
– предоставление услуг в электронном виде гражданам и организациям Санкт-Петербурга;
– защита персональных данных в Санкт-Петербурге;
– социальные и технические проблемы, возникающие при внедрении цифрового телевизионного вещания в Санкт-Петербурге.

20 апреля 2011 года состоялось очередное заседание Комиссии по информатизации и связи Общественного совета Санкт-Петербурга, на котором рассматривался вопрос о защите Персональных данных в Санкт-Петербурге.

Актуальность рассмотрения именно этого вопроса объясняется тем, что в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Закон), информационные системы персональных данных, созданные до 1 января 2011 года, должны быть приведены в соответствие с требованиями Закона не позднее 1 июля 2011 года.

В работе Комиссии приняли участие руководящие работники Управления Федеральной службы по техническому и экспортному контролю по Северо-Западному федеральному округу, Управления Роскомнадзора по Санкт-Петербургу и Ленинградской области, Комитета по информатизации и связи.

Заслушав и обсудив представленные доклады и информационные сообщения, Комиссия отметила большую работу, проделанную уполномоченными федеральными органами власти и Правительством города по реализации требований Закона, нормативных правовых актов и методических документов по защите персональных данных в Санкт-Петербурге.

Вместе с тем успешному продолжению этой работы препятствует:

– слабая информированность жителей города о своих правах при обработке персональных данных;
– недостаточное внимание руководителей организаций, являющихся операторами персональных данных (далее – Оператор) к выполнению требований Закона;
– дефицит квалифицированных специалистов;
– отсутствие на рынке в достаточном количестве отечественных средств защиты информации;
– хроническое недофинансирование работ и услуг, касающихся вопросов защиты информации, обеспечения безопасности персональных данных, создания систем защиты персональных данных, подготовки и переподготовки кадров в этой области знаний.

С целью обеспечения защиты прав и свобод граждан Санкт-Петербурга при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, Комиссия решила рекомендовать Губернатору и Правительству Санкт-Петербурга:

1. Рассмотреть на заседании Правительства Санкт-Петербурга вопрос об обеспечении защиты прав и свобод человека и гражданина при обработке его персональных данных в свете Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».
2. Активизировать работу в средствах массовой информации по доведению до граждан прав субъектов и обязанностях Операторов.
3. Разработать для органов государственной власти целевую программу реализации Закона, в которой определить цель, задачи, сроки, а также основные мероприятия и их исполнителей.
4. Сформировать на 2012-2013 годы государственный заказ на подготовку, переподготовку и повышение квалификации ИТ-специалистов и специалистов в области информационной

безопасности органов власти, подведомственных им организаций, а также предприятий малого бизнеса.

5. Сформировать на 2012-2013 годы государственный заказ на разработку современных средств защиты информации.

6. Сформировать на 2012-2013 годы государственный заказ образовательным учреждениям Санкт-Петербурга на разработку учебников и учебных пособий по защите персональных данных.

7. Включать в конкурсную документацию государственных и муниципальных заказов требование выполнения Закона организациям - исполнителями.

8. Разработать методический документ для стандартизации правил работы с персональными данными в многофункциональных центрах Санкт-Петербурга.

Вус М.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

О ЕДИНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ И ТЕРМИНОЛОГИЧЕСКИХ КОЛЛИЗИЯХ В ЗАКОНОДАТЕЛЬСТВЕ СНГ

На протяжении всех двух десятилетий существования СНГ ведется работа по формированию единого информационного пространства. Основой создания условий для формирования единого информационного пространства на просторах Содружества государств – участников СНГ стали подписанное в 1992 году Соглашение «О сотрудничестве в области информации» и принятый в 1993 году МПА СНГ Рекомендательный законодательный Акт «О принципах регулирования информационных отношений».

Концептуальные стратегические документы о сотрудничестве государств – участников СНГ, утверждаемые Решениями Совета глав государств – участников и планы реализации Стратегий предусматривают совершенствование и гармонизацию законодательства и нормативно-технической базы в области информатизации, развитие информационно-коммуникационной инфраструктуры, обеспечение транспарентности информации. Транспарентность информации может рассматриваться при этом как правовой режим, складывающийся из совокупности правоотношений по поводу доступа различных субъектов к интересующей их информации с должной полнотой, достаточностью и достоверностью.

За два десятилетия существования СНГ в его недрах разработано и уже принято большое число законодательных и иных правовых актов. Свои позиции и планы действий в области международной информационной безопасности государства – участники СНГ согласовывают также в рамках других международных организаций (ЕврАзЭС, ОДКБ, ШОС, ООН и др.). При этом становящейся сегодня все более актуальной проблемой является терминологическое многообразие и слабая определенность используемого в различных документах понятийного аппарата. Термины и их определения приводятся, как правило, «в целях настоящего нормативного акта», что неизбежно чревато коллизиями норм. Следует также отметить многоязычие и отсутствие поверенного перевода информационных баз национальных правовых актов.

Показательным примером слабой терминологической определенности может служить ситуация с определением такого базового понятия как информационная безопасность. Модельный закон «О международном информационном обмене», принятый МПА СНГ в 2002 году использует этот термин в следующей трактовке: «Информационная безопасность состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства». Содержательное наполнение этого термина буквально совпадает с определением, данным в принятом и действовавшем ранее в Российской Федерации Федеральном законе «Об участии в международном информационном обмене» (1996 г.). (Термин информационная сфера (среда) определялся при этом как сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.) В то же время, например, в Законе Республики Казахстан «О национальной безопасности» (1998 г.) термин информационная безопасность определен как «состояние защищенности государственных информационных ресурсов, а также прав личности и интересов общества в информационной сфере». Акцент здесь сделан, в первую очередь, на защищенности государственных информационных ресурсов.

Стратегия сотрудничества государств – участников СНГ в сфере информатизации (до 2010 г.), утвержденная в 2006 году Решением Совета глав государств – участников СНГ, включала определение понятия информационная безопасность в трактовке: «Информационная безопасность – состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства». Акцент делался на национальных интересах в информационной сфере, определяемых через интересы субъектов национальной безопасности.

Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности (на период с 2008-2010 гг.), также утвержденная Решением Совета глав государств – участников СНГ в 2008 году использовала уже иное определение термина.

«Информационная безопасность – состояние защищенности от внешних и внутренних угроз информационной сферы, формируемой, развиваемой и используемой с учетом жизненно важных интересов личности, общества и государства». Акцент при таком подходе, как представляется, в известной мере «традиционно – технократический»: в первую очередь – внимание акцентируется на объект (информационную сферу), а только затем – на субъекты информационной безопасности («с учетом жизненно важных интересов»). При этом сама проблема информационной безопасности искусственно сужается до задач защиты информации.

Разработанный Координационным советом государств-участников СНГ по информатизации и представленный к утверждению проект «Стратегия сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2015 года», который наряду с понятием «информационная безопасность» оперирует также и понятием «безопасность в киберпространстве», вообще не содержит определений этих понятий. (Раздел «Термины и определения», в отличие от предшествовавшей редакции документа в новой версии исключен).

В силу всего вышесказанного представляется, что сегодня достаточно актуальной задачей является разработка толкового словаря – глоссария терминов законодательства Содружества Независимых Государств.

Вус М.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ОБ ОДНОМ АСПЕКТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОДКБ

Информационно-коммуникационная революция, происходящая на наших глазах, выражается в переходе к электронным носителям информации. Это переход разрушает границы, в которые заключен традиционный информационно-коммуникационный процесс. При этом растет масштаб влияния информационно-коммуникационной среды на многие стороны жизни общества и государства. Возможность влияния на общественное мнение превратилась в настоящее время в значимый сегмент мировой экономики и весомый фактор развития социально-политических систем, способный в значительной степени определять образ жизни и социальные установки значительной части общества.

Интернет упрощает управление массами. Развитие новых технологий и средств коммуникации изменяет массовое восприятие реальности, в том числе и политической. Информация и коммуникация сегодня не только отражают события предметного мира, но и создают эти события. В новой информационно-коммуникационной среде кратно возрастают возможности контроля и манипулирования. Поэтому недооценка последствий внедрения современных информационно-коммуникационных технологий в повседневную жизнь может стать мощнейшим фактором дестабилизации политической системы.

ООН высказалась за приравнивание возможности доступа к Интернету к базовым правам человека. Вместе с тем в ЮНЕСКО прозвучали призывы обратить внимание и на негативные социальные последствия некритического использования современных информационно-коммуникационных технологий. Одновременно в научной литературе высказываются мнения о необходимости как четких ограничений возможного вмешательства органов власти в регулирование Интернета, так и определения перечня случаев, когда такое вмешательство допустимо. Предлагается даже создать своего рода международный арбитражный суд чести пользователя Интернета.

Проблематика информационной безопасности традиционно рассматривается в контексте доступности, целостности и конфиденциальности информации. При этом основное внимание сосредотачивается, прежде всего, на процессах хранения, обработки и передачи информации.

Минувшее десятилетие демонстрирует изменение сферы медиа (информационно-коммуникационная среда). Возникают такие новые феномены, как социальные сети, блоги, индивидуальные масс-медиа и т.д. Вместе с тем сегодня происходит и конвергенция традиционных СМИ, стирание граней между газетой, телевидением и радио и даже теми, кого называют блогерами и индивидуальными масс-медиа, – все они производят контент всех типов (тексты, аудио, видео), действуют по всем каналам связи и используют все возможные средства доставки.

В настоящее время мы становимся свидетелями обострения проблемы достоверности контента и способов его проверки, ответственности тех, кто распространяет или ложный, или ошибочный контент, вне зависимости от причин этих действий. Поэтому вполне логично с позиций информационной безопасности предъявлять требования не только к совершенствованию технологий связи и к технической надежности средств доставки, но и к качеству контента.

Понятие информационная безопасность сегодня нашло свое отражение в Положении о сотрудничестве государств – членов ОДКБ, утвержденном Решением Совета коллективной безопасности Организации Договора о коллективной безопасности от 10.12.2010 году в формулировке: «Информационная безопасность – состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве». При такой формулировке это базовое понятие охватывает

становящиеся все более актуальными и опасными сегодня угрозы социально-гуманитарного плана, в частности, угрозы распространения информации наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде государства. Источниками подобных угроз могут являться как государства, так и негосударственные структуры, а также частные лица. Представляется, что такое понимание проблемы информационной безопасности и содержательное наполнение понятия должно свидетельствовать и в пользу легитимации работы по противодействию деструктивным воздействиям в информационном пространстве ОДКБ.

Как было отмечено на состоявшихся в текущем году саммите ОДКБ и заседании координационного совета генпрокуроров СНГ: «Практика публикаций в интернете различного рода статей клеветнического характера, инсинуаций, подстрекательства к нарушению законодательства говорит о необходимости подготовки документа, договора, который бы упорядочил пользование интернетом».

Зяблова Е.Г.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций

ПРАКТИКА РЕАЛИЗАЦИИ УНИФИЦИРОВАННОГО ПОДХОДА К ПОСТРОЕНИЮ КОМПЛЕКСНЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В САНКТ-ПЕТЕРБУРГЕ

При создании современных систем защиты информации, как правило, наименьшее значение уделяется второстепенным факторам, влияющим на информационную безопасность, а именно физической защите зданий и помещений.

Согласно Доктрине информационной безопасности Российской Федерации, под информационной безопасностью понимается состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Отдельные сферы деятельности (системы государственного управления, банки, информационные сети и т. п.) требуют специальных мер обеспечения информационной безопасности и предъявляют особые требования к надежности функционирования в соответствии с характером и важностью решаемых задач.

Комплексный подход к созданию системы обеспечения безопасности позволяет организовать высокий уровень информационной безопасности, в том числе защищенность и устойчивость к различного вида угрозам и чрезвычайным происшествиям.

Согласно постановлению Правительства Санкт-Петербурга от 03 июня 2009 года № 636 «Об оснащении комплексными системами обеспечения безопасности объектов социальной инфраструктуры Санкт-Петербурга», все объекты социальной инфраструктуры Санкт-Петербурга, а именно: находящиеся в собственности Санкт-Петербурга здания и помещения, в которых размещены образовательные учреждения, учреждения здравоохранения, учреждения социальной защиты населения, учреждения физической культуры и спорта, учреждения культуры, учреждения противопожарной безопасности, учреждения, осуществляющие деятельность в сфере молодежной политики, а также исполнительные органы государственной власти Санкт-Петербурга, должны быть оснащены комплексными системами обеспечения безопасности (КСОБ).

Целью данных систем является стандартизация систем безопасности, централизованный сбор данных об оперативной обстановке на объектах социальной инфраструктуры Санкт-Петербурга, повышение принятия управленческих решений и организации эффективного взаимодействия со специализированными организациями, отвечающими за работу систем жизнеобеспечения города.

КСОБ представляет собой совокупность взаимосвязанных систем и технических средств, интегрированных в информационную систему обеспечения противопожарной, противокриминальной, антитеррористической защиты имущества объекта, охраны жизни и здоровья, имущества, документов, денежных средств и иных ценностей, и включает в себя: средства инженерно-технической укрепленности, системы и средства автоматической установки охранно-тревожной сигнализации, систему контроля и управления доступом, системы и средства охранного телевидения (видеонаблюдения), систему автоматической установки пожарной сигнализации, системы оповещения и управления эвакуацией людей при пожаре, системы автоматической установки пожаротушения, систему формирования, приема и передачи телематических сигналов.

Классификация объектов позволяет установить дифференцированные требования к КСОБ объектов, обеспечивающие необходимые уровни безопасности, с учетом критериев оценки возможного ущерба интересам личности, общества и государства, который может быть нанесен в случае реализации угроз.

Вопросам информационной безопасности в данной системе уделено большое значение, т.к. сбой работы, несанкционированный доступ к элементам систем, могут стать причиной несвоевременной передачи информации о чрезвычайной ситуации, срабатывании охранно-тревожной и пожарной сигнализации в соответствующие городские службы.

Комплексная система реализуется в защищенном исполнении и обеспечивает безопасность содержащейся в ней информации, что достигается путем проведения комплексных правовых, организационных, технических и методических мероприятий в объеме требований, предъявляемых федеральными законами, регламентирующими порядок защиты информации, а также нормативно-методическими документами ФСБ России и ФСТЭК России в области информационной безопасности, в том числе по защите информации от утечки по техническим каналам.

Используемые при построении КСОБ сертифицированные программно-аппаратные средства, средства криптографической защиты информации, антивирусные средства, межсетевые экраны, средства обнаружения компьютерных атак, телекоммуникационное оборудование обеспечивают выполнение функциональных требований, таких как защита технических и программных средств от несанкционированного доступа к элементам управления, установкам режимов и к информации, автоматический контроль исправности средств, входящих в систему, и линий передачи информации.

КСОБ является сложной системой, обеспечивающей безопасность объектов защиты путем снижения вероятности угроз техногенного, криминального и террористического характера, в том числе предотвращение неавторизованного доступа, повреждения и воздействия в отношении помещений и информации, но в то же время такая система позволяет реализовать единый унифицированный подход к построению систем обеспечения безопасности для исполнительных органов государственной власти Санкт-Петербурга, а также подведомственных им учреждений.

Кононова О.В., Попенко Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Москва, Президиум РАН

О ПРАВОВЫХ АСПЕКТАХ ИНТЕРНЕТ-МАРКЕТИНГА

В настоящее время в условиях глобальной трансформации индустриального общества в информационное наблюдается глубокое изменение характера корпоративных отношений.

Применение инфокоммуникационных технологий в современном обществе порождает проблемы, связанные с информационной безопасностью личности, общества, и государства, обусловленные все большей «прозрачностью» и уязвимостью различных сторон жизни и деятельности людей для внешнего воздействия. На решение этих проблем нацелены различные социальные институты информационной безопасности, определяющие систему «правил игры» в обществе и активно формирующиеся в настоящее время. Это технические, корпоративные, правовые и этические (моральные) нормы. Все они затрагивают глобальные вопросы становления информационного общества.

В докладе рассматриваются правовые аспекты информационного взаимодействия на примере рассмотрения вопросов правового обеспечения Интернет-маркетинговой деятельности компаний.

Декомпозируя проблему, условно разложим Интернет-маркетинг на три составляющие: рекламную, информационную и коммуникационную, базируясь на следующем определении Интернет-маркетинга: это – товар; цена; место реализации, рынок; продвижение товара. Первые три позиции присущи рекламе, а четвертая позиция обозначает предназначенность рекламы. Наличие информационной составляющей обусловлено целью любой рекламы: передачей информации по конкретному товару или услуге для их продвижения на рынок. Коммуникационная составляющая указывает, что только при ее наличии может идти речь о передаче любой информации, в том числе и рекламной.

Предложенное разделение позволяет обосновать в целом правовые аспекты Интернет-маркетинга через правовые аспекты его составляющих.

Интернет-реклама – сегодня самый быстроразвивающийся вид рекламы с постоянно меняющейся количественно и качественно аудиторией, позволяющий презентовать продукт или услугу на уровне, недостижимом для других СМИ, адресовать рекламное сообщение определенной целевой группе и видеть в режиме реального времени реакцию на данное сообщение, а также управлять этой реакцией. Грамотно спланированная и проведенная, комплексная рекламная кампания в Интернете позволит привлечь больше целевых потребителей.

Основными целями Федерального закона о рекламе являются развитие рынков товаров, работ и услуг на основе соблюдения принципов добросовестной конкуренции, обеспечение в РФ единства экономического пространства, реализация права потребителей на получение добросовестной и достоверной рекламы, предупреждение нарушения законодательства РФ о рекламе, а также пресечение фактов ненадлежащей рекламы. Федеральный закон о рекламе применяется к отношениям в сфере рекламы независимо от места ее производства, если распространение рекламы осуществляется на территории РФ, поэтому этот закон распространяется и на Интернет-маркетинг. Законодатель фактически возлагает ответственность на рекламодателя, рекламопроизводителя и рекламораспространителя за информацию. Нарушение ими законодательства РФ о рекламе влечет за собой ответственность в соответствии с законодательством РФ об административных правонарушениях.

Информационная составляющая Интернет-маркетинга основывается на отрасли информационного права в России, которая находится в стадии формирования и, к сожалению, пока в неравномерном и несбалансированном развитии. Однако некоторые правовые аспекты уже можно сформулировать. Например, должны быть заключены Договор о защите коммерческой информации и другие договорные документы, обеспечены потребительские свойства информации по всей цепочке товар => рекламодатель => рекламопроизводитель => рекламораспространитель => внешняя среда.

Правовые аспекты коммуникационной составляющей Интернет-маркетинга можно сформулировать, опираясь на положения Указа Президента РФ от 28 июня 1993 года №966 «О Концепции правовой информатизации России (с изменениями от 22 марта 2005 г.)». Они затрагивают как правовые аспекты того, что передается, т.е. информацию, так и того, как передается, т.е. коммуникации.

Рассмотрение вопросов использования правового обеспечения маркетинговой деятельности в среде Интернет будет способствовать развитию корпоративных отношений и укреплению системы национальной безопасности Российской Федерации.

Кононова О.В., Попенко Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Москва, Президиум РАН

О НЕКОТОРЫХ АСПЕКТАХ БОРЬБЫ СО СПАМОМ

При рассмотрении состояния информационных отношений компаний с точки зрения их соответствия задачам обеспечения информационной безопасности вопрос о спаме является чрезвычайно актуальным.

В компьютерной терминологии слово «спам» обычно используется для обозначения назойливых рекламных рассылок или иного вида информации лицам, не выражавшим желания их получать, обычно с помощью электронных писем. По определению Лаборатории Касперского: спам – это анонимная массовая непрошенная рассылка.

Доля спама в мировом почтовом трафике составляет около 80 %.

По оценке аудиторской и консалтинговой компании ФБК, ежегодные потери российской экономики от спама составляют 1,3–1,9 миллиарда долларов. Сумма ежегодных потерь от спама в США составляет порядка 70 миллиардов долларов. Огромное количество бесполезных сообщений наносит очевидный вред получателям. Расчеты ФБК основаны на денежном выражении снижения производительности участников хозяйственной деятельности. Кроме того, пользователю приходится платить за заведомо ненужные письма в дорогом Интернет-трафике.

Наиболее распространенными видами спама являются: реклама, реклама незаконной продукции, антиреклама, – нигерийские письма, фишинг. Технология спама достаточно проста и эффективна. Самый большой поток спама распространяется через электронную почту. В настоящее время доля вирусов и спама в общем трафике электронной почты составляет по разным оценкам от 70 до 95 %.

В настоящее время борьба со спамом опирается, в основном, на технические и организационные способы.

При использовании технических способов предложения, попавшие в электронный ящик, необходимо разделять на спам, имеющий признаки анонимной массовой рассылки и целевые коммерческие предложения. Первые – фильтруются и сразу удаляются. Вторые – осторожно фильтруются, чтобы нужные коммерческие предложения, аппаратно воспринимаемые как спам, не оказались потерянными. Возможно использование автоматической фильтрации для определения спама, основанной на использовании программного обеспечения, которое предназначено для конечных пользователей или для использования на серверах, при котором анализируется содержание письма и делается вывод, спам это или нет, или опознается отправитель как спамер, не заглядывая в текст письма. Также эффективным средством борьбы со спамом являются системы определения признаков массовости сообщения.

В борьбе со спамом большое значение придается организационным методам, таким как использование нескольких адресов электронной почты для пользователя, выбор для личной переписки трудно угадываемого адреса электронной почты, отказ от ответов на спам-сообщения и просмотра ссылок сообщений, предлагающих «отписаться от рассылки», использование на компьютере последней версии Интернет-обозревателя и всех обновлений безопасности, установка на своем компьютере антиспам-решений, использование так называемых черных списков – перечня физических или юридических лиц, которые по каким-либо причинам признаны недружественными по отношению к субъекту-составителю списка.

В ряде стран принимаются законодательные меры против спамеров. Однако попытки законодательного запрещения или ограничения деятельности спамеров наталкиваются на целый ряд сложностей. Непросто определить в законе, какая рассылка является законной, а какая нет. Хуже всего то, что компания или лицо, рассылающее спам, могут находиться в другой стране. Для того,

чтобы такие законы были эффективными, необходимо выработать согласованное законодательство, которое действовало бы в большинстве стран, что представляется труднодостижимым в обозримом будущем.

В России спам запрещён «Законом о рекламе» (ст. 18): «Распространение рекламы по сетям электросвязи, в том числе посредством использования телефонной, факсимильной, подвижной радиотелефонной связи, допускается только при условии предварительного согласия абонента или адресата на получение рекламы. При этом реклама признается распространенной без предварительного согласия абонента или адресата, если распространитель рекламы не докажет, что такое согласие было получено».

В официальных комментариях Федеральной антимонопольной службы (ФАС), уполномоченной осуществлять функции контроля за соблюдением этого закона, указывалось на применимость данной нормы и к Интернет-рассылкам. За нарушение статьи 18 распространитель рекламы несёт ответственность в соответствии с законодательством об административных правонарушениях. Однако ФАС не имеет полномочий для проведения оперативно-розыскных мероприятий по установлению лица, ответственного за спам, а уполномоченные на это органы не могут их проводить в связи с отсутствием в российском административном и уголовном законодательстве ответственности за рассылку спама. Поэтому, несмотря на периодические публикации материалов о привлечении нарушителей к ответственности, в настоящее время данная законодательная норма малоэффективна.

Таким образом, создание спама и борьба с ним напоминают соотношение «атака-оборона», когда перевес попеременно находится на атакующей или обороняющейся сторонах. Однако в этом случае особое внимание следует обратить на социально-личностное совершенствование пользователей для формирования здоровой корпоративной информационной среды.

Тершуков Д.А.
Россия, Волгоград, Администрация Волгоградской области

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ВОЛГОГРАДСКОЙ ОБЛАСТИ

В 2000 году Президентом Российской Федерации была утверждена Доктрина информационной безопасности Российской Федерации, определяющая концептуальные основы построения системы нормативно-правового обеспечения информационной безопасности.

В Доктрине приведены четыре основные составляющие национальных интересов России в информационной сфере:

– соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею при непременном обеспечении защиты сведений о частной жизни;

– информационное обеспечение государственной политики Российской Федерации, формирование достоверной информации о политике государства. Исключение возможностей манипулирования информацией, соблюдение принципа баланса интересов граждан, общества и государства;

– развитие современных информационных технологий, отечественной индустрии информации, индустрии средств информатизации, коммуникаций и связи, повышение их конкурентоспособности на внутреннем и внешнем рынке;

– защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем на территории России, в том числе систем специального назначения.

В целях развития Доктрины информационной безопасности Российской Федерации применительно к информационной сфере Южного федерального округа в 2007 году на заседании Совета по информационной безопасности и информатизации при полномочном представителе Президента Российской Федерации в Южном федеральном округе была утверждена Концепция защиты информации в Южном федеральном округе.

На территории Волгоградской области региональная система защиты информации начала формироваться с 2000 года.

В апреле 2000 года постановлением Главы Администрации Волгоградской области №252 от 10.04.2000 было утверждено Положение о защите информации от технических разведок и от ее утечки по техническим каналам в Администрации Волгоградской области. Указанное Положение определяет основные задачи системы защиты информации и организацию работ по защите информации в органах исполнительной власти Волгоградской области.

Возглавляет региональную систему защиты информации Совет по информационной безопасности Администрации Волгоградской области.

Совет рассматривает вопросы организации и состояния работ в области защиты информации в Волгоградской области, координирует деятельность по реализации федеральной политики в области технической защиты информации на территории Волгоградской области, осуществляет координацию деятельности подразделений по технической защите информации муниципальных образований,

входящих в состав Волгоградской области. Для предварительной подготовки вопросов, выносимых на заседания Совета, при Совете созданы рабочие группы: по обеспечению безопасности персональных данных; по обеспечению информационной безопасности в ключевых системах информационной инфраструктуры органов государственной власти Волгоградской области.

Организация и координация работ по технической защите информации в Администрации Волгоградской области возложены на отдел специальной документальной связи и защиты информации аппарата Главы Администрации Волгоградской области. В органах исполнительной власти Волгоградской области мероприятия по защите информации осуществляются соответствующими структурными подразделениями или специально назначенными должностными лицами.

В целях дальнейшего совершенствования работ в области защиты информации ограниченного доступа постановлением Главы Администрации Волгоградской области от 25.10.2007 №1839 было утверждено Положение о контроле состояния защиты информации ограниченного доступа в Администрации Волгоградской области от технических разведок и от ее утечки по техническим каналам. Вышеназванное Положение определяет организацию и порядок проведения контроля как в органах исполнительной власти Волгоградской области, в подведомственных учреждениях и организациях, так и на предприятиях негосударственного сектора в случаях, когда органы исполнительной власти Волгоградской области являются заказчиками работ, связанных с использованием информации ограниченного доступа.

В Волгоградской области создана и система подготовки (переподготовки) специалистов в области защиты информации. В систему входят государственные высшие учебные заведения: Волгоградский государственный и Волгоградский государственный технический университеты. В Управлении Федерального казначейства по Волгоградской области создан Пилотный центр повышения квалификации руководителей и специалистов по защите информации территориальных органов Минфина России.

Чудиловская Т.Г.
Беларуссия, Минск, Академия Министерства внутренних дел Республики Беларусь

О ПРОБЛЕМАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

В настоящее время актуальна тема формирования электронного правительства и оказания государственных услуг в электронном виде. В основе деятельности электронного правительства лежит электронное информационное взаимодействие государственных организаций и органов власти всех уровней, как между собой, так и с иными физическими и юридическими лицами. Без развитой системы безопасности для всех этапов этого взаимодействия обойтись невозможно – от идентификации граждан для доступа к тем или иным государственным информационным ресурсам (базам данных), защиты самих баз данных и сетей госорганов от хищения, модификации, перехвата и, наконец, защиты используемых при взаимодействии открытых каналов связи.

Процессы развития электронных услуг остро ставят вопросы цифрового доверия. Доверие граждан и предприятий к государственным услугам, предоставляемым в электронном виде, напрямую зависит от уровня обеспечения информационной безопасности инфраструктуры электронного правительства и взаимодействующих элементов. В процессе получения государственных услуг субъекты информационных отношений заинтересованы в обеспечении:

– конфиденциальности (сохранения в тайне) определенной части информации;
– достоверности, актуальности, целостности информации;
– защиты от навязывания им ложной (недостоверной, искаженной) информации;
– возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
– защиты части информации от незаконного ее тиражирования;
– разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией.

В связи с этим обеспечение необходимого уровня информационной безопасности, в первую очередь персональных данных граждан, является одной из первоочередных проблем реализации программы электронного правительства.

Реальные достижения электронного правительства, в том числе и в области информационной безопасности, могут быть обеспечены благодаря использованию системного подхода к планированию и реализации инициатив в области электронного правительства, основанных на разработке и реализации единой архитектуры электронного правительства.

Однако все еще остается открытым вопрос о единой методологии формирования электронного правительства и установлении единых организационно-технических требований к его формированию и последующему существованию, в том числе и в области информационной безопасности.

Для Республики Беларусь актуальны проблемы:

– создания единой системы идентификации для физических и юридических лиц;

– создания государственной системы управления открытыми ключами, представляющей собой систему взаимосвязанных и аккредитованных в ней удостоверяющих и регистрационных центров;

– широкомасштабного внедрения электронного документооборота и электронной цифровой подписи;

– развития системы хранения государственных информационных ресурсов, используемых при оказании электронных услуг;

– формирования и развития платежного шлюза в интеграции с формируемым банковской сферой единым расчетным информационным пространством;

– разработки типовых политик безопасности для государственных информационных систем электронного правительства.

В результате должны быть сведены к минимуму возможности злоупотребления персональной и иной конфиденциальной информацией. Для юридических и физических лиц должны быть созданы доступные способы, механизмы и средства, обеспечивающие идентификацию и аутентификацию пользователей, конфиденциальность и целостность сообщений в системах и сетях общего пользования. Это позволит расширить сферу использования электронного документооборота, обеспечит возможности предоставления электронных услуг, широкомасштабного внедрения систем электронных платежей, иных форм многостороннего общения между населением, бизнесом и государством.

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Абдразяпов Р.Р.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УЧАСТНИКОВ СЛЕДСТВЕННО-ОПЕРАТИВНОЙ ГРУППЫ В ХОДЕ ПРОВЕДЕНИЯ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ ПО ДЕЛАМ О ХИЩЕНИИ ЭНЕРГОНОСИТЕЛЕЙ

Осмотр места происшествия – это неотложное следственное действие, направленное на установление, фиксацию и исследования обстановки места происшествия, следов преступления и преступников и иных фактических данных, позволяющих в совокупности с другими доказательствами сделать вывод о механизме происшествия и других обстоятельствах расследуемого события.

Чаще всего осмотр места происшествия является первоначальным следственным действием, носящим неотложный характер. От результатов осмотра в значительной степени зависит ход дальнейшего расследования. При получении информации о совершении хищения энергоносителей осмотр места происшествия нужно проводить незамедлительно – с целью обнаружения следов и других доказательств совершенного преступления, то есть следов рук, ног, орудий, хранившихся веществ, их остатков и т.д. Так же это обусловлено переменой погодных условий и, как следствие, невозможностью изъятия и закрепления следов преступления.

Однако, несмотря на необходимость обнаружения, фиксации и изъятия вещественных доказательств, следов преступления и т.д. нельзя забывать о соблюдении мер безопасности в ходе проведения осмотра места происшествия. Зачастую в местах совершения хищения энергоносителей имеется опасность их возгорания, токсического отравления участников осмотра и т.п. «Осмотр в закрытых помещениях не должен быть продолжительным, помещения после 10–15 минут следует оставлять, по возможности проветриваться. Все колодцы, шлюзы должны осматриваться с применением средств химической защиты, при взаимной страховке. На месте осмотра обязательно наличие огнетушителей и других средств пожарной безопасности, по возможности на место происшествия прибывают силы МЧС со специальным оборудованием. Обязательно наличие средств первой медицинской помощи. Применение служебных собак должно быть ограничено в связи с возможной утратой ими своих навыков». Так же при осмотре места происшествия на любых объектах в сфере добычи, хранения, переработки, транспортировки и сбыта энергоносителей запрещается производить какие-либо действия с устройствами (приспособлениями), крутить вентили или задвижки, снимать надетые на устройства приспособления, шланги и т.п. во избежание нанесения ущерба гражданам, организациям и окружающей среде.

При выезде на место происшествия следователь должен заблаговременно позаботиться о вызове соответствующей службы: МЧС, аварийная газовая служба. А также, в случае необходимости, убедиться в наличии у членов следственно оперативной группы средств индивидуальной защиты, химической защиты, средств первой медицинской помощи. По прибытии на место происшествия следователь, как руководитель следственно-оперативной группы, должен оценить характер и размер причиненного вреда, принять меры, в случае необходимости, по предотвращению или ослаблению вредных последствий преступления (разлива нефтепродуктов, утечка газа, загрязнение воды, почвы, ликвидация пожара и т.п.). Для этого целесообразно привлекать соответствующую службу, например аварийную газовую службу, противопожарную, либо иную профильную службу Министерства по чрезвычайным ситуациям. Так же следователь принимает меры по оказанию необходимой медицинской помощи пострадавшим, если она не была оказана.

Таким образом, производство осмотра места происшествия при расследовании хищений энергоносителей требует от следователей высокой степени организации при проведении данного следственного действия, соблюдения мер безопасности в отношении себя и в отношении остальных членов следственно – оперативной группы, а также принятии мер по предотвращению или ослаблению вредных последствий преступления.

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

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ БЕЗОПАСНЫМ ДОСТУПОМ К ВНЕШНИМ УСТРОЙСТВАМ КОМПЬЮТЕРА

Требования правовых норм и внутренняя потребность организации в конфиденциальности и безопасности информации порождают ряд практических вопросов, одним из которых является управление доступом к внешним носителям информации – DVD, USB-устройствам.

Простейшие задачи, которые при этом решаются, – это сделать устройство недоступным для пользователя совсем или ограничить возможность записи на это устройство. Можно иногда видеть, как для этого отключают питание этих устройств или заклеивают их, отсоединяют передающие шины и т.д. В Интернете встречаются рекомендации для защиты от изменений флеш-карты настроить внутренние регистры ее контроллера специальными утилитами, включив режим «только чтение» (раньше у некоторых флешек делали механический переключатель защиты записи). Как вариант предлагают всю память дополнить какими-либо (в том числе ненужными) файлами и назначить им атрибуты «только чтение», «системный» и «скрытый».

Все эти средства являются негибкими, зависящими от аппаратных реализаций, создают неудобства в их использовании и использовании носителей на других, незащищенных компьютерах.

Вместе с тем, ОС Windows предоставляет большие возможности программного управления устройствами и их настройкой. Одной из таких возможностей является компонент, позволяющий редактировать групповые политики безопасности (gpedit.msc). В Windows Vista появились дополнительные возможности управления именно внешними USB-устройствами. Кроме этого, для управления доступом к данным в файловой системе NTFS существует политика безопасности, которая позволяет настроить произвольный доступ к логическим единицам – устройствам, папкам, файлам (чтение, запись, выполнение, создание, удаление и др.) с точностью до пользователя или группы пользователей.

Недостаток этих инструментов (групповой политики и безопасности) в том, что все операции настройки нужно производить вручную, это требует затрат времени и снижает оперативность.

Вместе с тем, эти же действия могут быть автоматизированы прямым изменением настроек с помощью утилит ОС. Например, reg-файл, содержащий текст:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies]
"WriteProtect"=dword:00000001

позволяет напрямую изменить настройки реестра, включив защиту от записи на устройство. Такой же файл, только с параметром 00000000, даст возможность записи. Принципиально, при включенном сервисе «Удаленный реестр», такие операции можно производить и на удаленном компьютере.

Для автоматического произвольного управления настройкой NTFS-устройством удобным инструментом является утилита Microsoft xcacls.exe, она доступна в Интернете. Эксперименты автора с более новой ее версией xcacls.vbs показали недостатки в работе с русскими именами файлов, папок, групп (например, приходится вместо встроенной группы «Все» указывать «All»).

Использование утилиты автоматизируется включением ее вызова в cmd-файл. Например, фрагмент в нем

```
set /p d= Ввведите букву для назначения полного доступа:
xcacls.exe %d%:\ /C /T /E /G %username%:f;f /Y     >NUL
```

для текущего пользователя дает полный доступ к файловой системе; строка

```
xcacls.exe %d%:\ /C /T /E /R %username%  /Y >NUL
```

исключит специальный доступ для текущего пользователя.

Таким образом, существуют простые оперативные способы управления доступом к внешним устройствам данных, которые могут эффективно использоваться в корпоративных компьютерных системах для ограничения отдельных видов доступа со стороны пользователей и защиты от таких же видов доступа вредоносных программ.

Аполлонский А.В., Дементьева Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ НА ОФИЦИАЛЬНОМ САЙТЕ

Сайт – это совокупность электронных документов лица или организации в компьютерной сети, объединенная под одним адресом (доменным именем). Поскольку эти документы и данные расположены в сети, они доступны для корпоративного использования, автоматизации ежедневной работы, уменьшения в ней издержек на поиск информации и повышение эффективности работы.

Другая цель использования сайта – представительство: человек или организация сообщает о себе сведения, представляет справки и свои новости, ведет общение с другими людьми и организациями. Представительские функции сайта государственных органов регулируются Федеральным законом Российской Федерации от 9 февраля 2009 года №8-ФЗ «Об обеспечении

доступа к информации о деятельности государственных органов и органов местного самоуправления».

Современная практика показывает, что две эти функции сайта плохо совмещаются друг с другом. Большинство пользователей Интернета оценивают официальные сайты организаций как малоинформативные, неработоспособные. Это связано со сложными процедурами размещения любой информации на официальном сайте и отсутствием механизмов разделения ответственности за достоверность предоставляемой информации. Это ведет к инерции таких сайтов. Результатом становится то, что значительная часть информации на них все равно становится через некоторое время недостоверной в связи с неактуальностью. Например, выборочное исследование сайтов вузов МВД (сентябрь 2011 года) показало, что информация на некоторых из них не обновлялась более двух лет.

Реалиями современности стали быстро развивающиеся в Интернете социальные сети и другие порталы, предоставляющие пользователям набор сервисов, позволяющих вести в Интернете свои странички, публиковать свои и обсуждать чужие заметки, получать новости, вести переписку с другими пользователями, искать среди них с интересами, похожими на твои, и т.д.

Эти порталы показывают эффективные пути управления информацией, обеспечения ее конфиденциальности, доступности и целостности, а также обеспечение протоколирования действий с информацией, ссылок на источники и подтверждения авторства, то есть определенной ответственности, которую можно возложить на отдельных лиц. Использование подобных механизмов при соответствующем правовом обеспечении позволило бы решить проблему неэффективного управления информацией на официальных сайтах.

Пока же, при отсутствии правового обеспечения, проблема решается разделением этих сайтов на две части и использованием различных движков на этих частях. Самый известный пример такого решения дает фирма 1С-Битрикс («1С-Битрикс: Официальный сайт государственной организации» и «1С-Битрикс: Внутренний портал государственной организации»).

Аполлонский А.В., Шалагинова О.Б.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ НАДЕЖНОСТИ СИСТЕМ В ПОЛИТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Политика информационной безопасности организации – это совокупность правил, норм, которым должны следовать сотрудники организации при работе с корпоративной информацией. Политика безопасности формируется в форме распоряжений и инструкций, имеющих обязательную силу и касающихся должностных обязанностей и прав сотрудников, формы и порядка доступа к различной информации, поддержания ее в актуальном состоянии, резервирования и т.д.

При разработке политики безопасности организации и оценке рисков могут оказаться полезными оценки надежности различных компонентов системы безопасности. Эти оценки позволяют точнее построить политику безопасности, оптимизировать затраты на нее.

Потери, которые несут организации в связи с уязвимостью системы безопасности, происходят непредсказуемо, поэтому этот процесс можно рассматривать как случайный и применять к его оценкам статистические методы.

Пусть непрерывная случайная величина есть продолжительность времени устойчивой работы системы. Чаще всего эта величина распределена по показательному закону. Статистически может быть известна вероятность безотказной работы элемента системы за некоторое время, эту вероятность называют функцией надежности.

Функция надежности позволяет строить оценки рисков, например, того, что в какой-либо промежуток времени безопасность будет или не будет нарушена.

Общая модель, конечно, должна учитывать и оценки потенциальных потерь, которые связаны с тем или иным видом нарушения безопасности – потерей конфиденциальности, невозможностью получения доступа к информации, нарушением ее целостности. Такие оценки могут получаться, например, экспертными методами.

Необходимо понимать и то, что любые ограничения по работе с корпоративной информацией, в том числе накладываемые системой безопасности, снижают эффективность самой этой работы: для выполнения той же работы в условиях политики безопасности требуются дополнительные действия, обеспечивающие безопасность, дополнительные средства и другие накладные расходы.

Таким образом, формальная модель, которая учитывает эти процессы и факторы, позволит найти сбалансированную политику организации, в целом повышающую эффективность деятельности этой организации. Такая политика, возможно, не будет оптимальной в связи с тем, что в ее формировании могут на разных этапах применяться экспертные оценки и неточные статистики. Однако, принятие решения, основанного на теории, статистически эффективнее того, которое получают на основе управленческого общего опыта и интуиции.

Беженцев А.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

НЕКОТОРЫЕ ВОПРОСЫ ЗАЩИТЫ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И РАЗВИТИЮ

С текущего года государство берет на себя обязательство по разработке и реализации единой государственной политики в сегменте защиты детей от информации, причиняющей вред их здоровью и развитию, целевых программ обеспечивающих их информационную безопасность, проведения экспертизы информационной продукции. В конце 2010 года принят федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию». Данный закон направлен на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребенке порочные наклонности, сформировать у ребенка искаженную картину мира и неправильные жизненные ориентации.

Информационную продукцию планируется классифицировать по возрасту: «универсальная», «до 6-ти лет», «с 6-ти лет», «с 12-ти лет», «с 16-ти лет», «с 18-ти лет» и снабжать соответствующей маркировкой (такая обязанность возлагается на производителей и распространителей информации различного рода).

Определяется порядок прекращения распространения продукции средства массовой информации, осуществляемого с нарушением законодательно-установленных требований. Каждый выпуск периодического печатного издания, каждая копия аудио-, видео- или кинохроникальной программы должны содержать знак информационной продукции, а при демонстрации программ и при каждом выходе в эфир радиопрограмм, телепрограмм они должны сопровождаться сообщением об ограничении их распространения.

Новеллой законодательства является запрещение размещения рекламы в учебниках, учебных пособиях, другой учебной литературе, предназначенных для обучения детей по основным образовательным программам начального общего, среднего (полного) образования, школьных дневниках, тетрадях, а также распространение рекламы, содержащей информацию, запрещенную для распространения среди детей, в детских образовательных организациях, медицинских, санаторно-курортных, физкультурно-спортивных организациях, организациях культуры, отдыха, оздоровления детей или на расстоянии менее чем 100 метров от границ территорий указанных организаций.

В КоАП РФ закреплены составы новых административных правонарушений. Так, установлена ответственность за невыполнение установленных требований распространения среди детей продукции средств массовой информации, содержащей сведения, причиняющие вред их здоровью и развитию. Еще один состав административных правонарушений – неприменение операторами, оказывающими телематические услуги связи в пунктах коллективного доступа к данным, распространяемым посредством информационно-телекоммуникационных сетей, технических, программно-аппаратных средств защиты. В рекламе теперь запрещается показывать несовершеннолетних в опасных ситуациях, в том числе побуждающих к совершению действий, представляющих угрозу их жизни и здоровью.

Федеральным законодательством установлены и иные правовые механизмы привлечения к ответственности за невыполнение требований, касающихся защиты детей от информации, причиняющей вред их здоровью и развитию, в частности суд по заявлению уполномоченного органа власти имеет право прекращать распространение продукции средств массовой информации, осуществляемое с нарушением требований законодательства.

Большаков В.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет кино и телевидения

НЕПАРАМЕТРИЧЕСКИЕ МЕТОДЫ ИССЛЕДОВАНИЯ ФАКТОРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одним из важнейших принципов обеспечения безопасности информационных систем является непрерывная реализация и совершенствование средств и методов контроля и защиты этих систем. Этапами процесса защиты информации после выявления источников угроз являются, в частности, определение необходимых мер защиты, оценка их эффективности, экономической целесообразности, а также реализация принятых мер с учетом выбранных критериев, т.е. приоритетов. Для успешной реализации этих этапов необходимо получение всесторонней и наиболее полной информации о рассматриваемых системах, что, как правило, практически невозможно. Неполнота информации и недостаточно высокое качество связано, прежде всего, со следующими причинами:

– статистическая (количественная) информация может быть недостаточно достоверной, например, в виду того, что она получена в прошлом, а существующие условия и обстоятельства претерпели некоторые изменения;

– некоторая часть информации носит качественный характер и не поддается количественной оценке, например, нельзя точно рассчитать степень влияния некоторых, не имеющих количественную характеристику, факторов на реализацию какого-либо этапа процесса защиты информации;

– получение той или иной полной информации связано с большими затратами времени и средств, что является экономически нецелесообразным, поэтому выбирается лишь часть наиболее доступной информации;

– существование некоторых факторов, влияние которых в настоящее время предсказать невозможно, однако оно может возникнуть в будущем.

Задачи обеспечения контроля и защиты информационных систем в условиях неполной информации или в условиях неопределенности предлагается решать комплексным методом, а именно в сочетании строгих математических расчетов с субъективными суждениями и оценками специалистов-экспертов. Эти суждения и оценки позволяют хотя бы частично компенсировать недостаток информации.

Например, при работе с некоторой системой было выделено *n* угроз безопасности этой системе. Для предотвращения каждой из угроз предусмотрены определенные средства защиты, при этом для разных угроз средства защиты могут не совпадать. Было установлено, что для успешной работы системы можно использовать *m* различных средств защиты. Задача заключается в том, чтобы выбрать такое средство защиты, при применении которого защита системы была бы наилучшей в каком-то определенном смысле. Кроме этого, предполагается, что явно доминирующего в этом смысле средства защиты нет. Для решения поставленной задачи предлагается использовать и математические расчеты, и опыт специалистов в данной области (экспертов).

Итак, выбирается некоторая группа экспертов, которой предлагается ранжировать предложенные средства защиты от каждой из угроз, а также ранжировать сами угрозы по степени серьезности. В результате чего каждой угрозе будет приписан некоторый вес и вычислен суммарный ранг каждого средства защиты.

Для получения независимых экспертных заключений необходимо опросить определённое количество специалистов, работающих в нескольких различных организациях и представляющих разные научные направления. Опрос экспертов осуществляется с помощью анкет, в которых перечислены угрозы и средства защиты от них.

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

ОЦЕНКА СТЕПЕНИ ЗАЩИЩЕННОСТИ ОБЪЕКТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пусть рассматривается некоторый объект информационной безопасности (ОИБ). Предположим, что для данного объекта существует ряд угроз. Степень опасности каждой угрозы зависит от факторов, которые можно разделить на две группы:

– факторы риска, т.е. факторы, понижающие защищенность ОИБ от данной угрозы;

– факторы защищенности, т.е. факторы, повышающие защищенность ОИБ от данной угрозы.

Обобщенную оценку защищенности ОИБ можно рассматривать как интегральную функцию его защищенности от совокупности всех видов угроз.

Зависимость степени защищенности ОИБ от факторов может быть описана следующим образом:

1. Если степень опасности каждой угрозы y зависит от одного фактора x, то эту зависимость можно выразить в виде функции одной переменной $y=f(x)$.

2. Если степень опасности каждой угрозы y зависит от нескольких факторов $x_1, x_2,\ldots,x_n$, то эту зависимость можно выразить в виде функции нескольких переменных $y=f(x_1, x_2,\ldots,x_n)$.

3. Если степень опасности некоторых угроз $y_1, y_2,\ldots, y_n$ зависит не только от факторов $x_1, x_2,\ldots,x_n$, но и, прямо или косвенно, от степени опасности других угроз, то зависимость может быть выражена в виде так называемой системы одновременных уравнений.

Для исследования зависимости защищенности ОИБ от факторов предлагается построить математическую модель, т.е. определить вид функции f и найти параметры этой функции на основе эмпирических данных.

Для построения правильной, адекватной действительности, математической модели, прежде всего, необходимо собрать достаточный статистический материал. Это возможно в том случае, когда факторы, рассматриваемые в задаче, имеют количественные характеристики. Иначе говоря, имеется возможность выбрать такую количественную меру, которая позволит измерять степень влияния факторов на защищенность ОИБ. При этом к этой мере предъявляется ряд требований, основными из которых являются интерпретируемость, сопоставимость, вычислимость на основе эмпирических данных.

Если факторы носят качественный характер, то им придают количественные характеристики с помощью процесса ранжирования, который, как правило, производят группы наиболее компетентных в данной области людей (экспертов).

При построении и исследовании предлагаемой модели могут быть решены следующие задачи:

– определение силы и направления действия факторов, влияющих на защищенность ОИБ;

– выделение наиболее существенных и исключение несущественных факторов, влияющих на защищенность ОИБ;

– прогнозирование защищенности ОИБ от системной угрозы при подтверждении адекватности построенной модели;

– выработка рекомендации по оптимизации системы безопасности ОИБ.

Бондуровский В.В., Вус М.А.
Россия, Санкт-Петербург, Секретариат Совета Межпарламентской Ассамблеи государств – участников СНГ, Санкт-Петербургский институт информатики и автоматизации РАН

СОТРУДНИЧЕСТВО МЕЖПАРЛАМЕНТСКОЙ АССАМБЛЕИ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ С НАУЧНЫМИ ОРГАНИЗАЦИЯМИ В ОБЕСПЕЧЕНИИ ПРЕДОТВРАЩЕНИЯ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТА ДЛЯ ТЕРРОРИСТИЧЕСКИХ ЦЕЛЕЙ

Межпарламентская Ассамблея государств – участников СНГ является межгосударственным органом Содружества, обеспечивающим сотрудничество высших законодательных органов государств – участников. Ее участниками на данный момент являются 9 государств Содружества и парламент Афганистана в качестве наблюдателя.

Основой многостороннего регионального сотрудничества государств – участников СНГ в противодействии терроризму является Договор о сотрудничестве в борьбе с терроризмом (1999 год) и утверждаемые Советом глав государств СНГ программы по борьбе с терроризмом и иными насильственными проявлениями экстремизма (в настоящее время действует программа на 2010-2013 годы). Стратегически важным моментом является использование таких форм сотрудничества и взаимодействия, которые позволяют Ассамблее максимально учитывать профессиональные точки зрения различных субъектов, задействованных в предотвращении терроризма.

Ассамблея исходит из того, что ключевым моментом в решении проблемы эффективного противодействия терроризму является создание максимально гармонизированных правовых основ регулирования всей системы безопасности. Ассамблея разрабатывает типовые для государств – участников модельные законодательные акты и рекомендации, направленные на гармонизацию национальных систем законодательства, учитывает при этом международный опыт борьбы с вызовами и угрозами безопасности, фактически создавая механизмы имплементации положений международно-правовых документов в национальные правовые системы своих государств – участников.

Модельные законы чрезвычайно важны для формирования общего информационного пространства и информационных обществ государств – участников СНГ. Они важны также и с позиций правового обеспечения информационной безопасности. Вопросы безопасности информационной сферы, в том числе и вопросы предотвращения использования Интернета в противоправных целях, отражены сегодня во многих документах Ассамблеи.

Важными партнерами МПА СНГ в разработке моделей регулирования отношений в информационной сфере и сфере безопасности являются научные организации и в их числе институты Российской академии наук: Санкт-Петербургский институт информатики и автоматизации РАН и сектор Информационного права Института государства и права РАН. Эффективной формой сотрудничества при этом является постоянное представительство этих учреждений РАН в органах межотраслевого сотрудничества, действующих под эгидой МПА СНГ.

В целях объединения усилий при Межпарламентской Ассамблее создана Объединенная комиссия по гармонизации законодательства в сфере борьбы с терроризмом, преступностью и наркобизнесом в СНГ. Результаты работы Объединенной комиссии свидетельствуют о том, что она стала эффективной формой межотраслевого партнерства, способствующего укреплению атмосферы взаимопонимания и, особенно, в таком важном деле как противодействие терроризму.

Усовершенствованное в результате предпринятых усилий на сегодняшний день модельное антитеррористическое законодательство СНГ предусматривает меры по информационному противодействию терроризму, в том числе по предотвращению использования Интернета для террористических целей.

Бородушко Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет экономики и финансов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СТРУКТУРЕ ФАКТОРОВ ЭФФЕКТИВНОГО УПРАВЛЕНИЯ МАКРОЭКОНОМИЧЕСКИМИ СИСТЕМАМИ

Проблемы управления на макроуровне. Для современной эпохи характерно нарастание сложности и противоречивости предпосылок и факторов эффективности управления

макроэкономическими системами. Так, демократизация общественных отношений позволяет сформировать оптимальный по своим качественным характеристикам кадровый ресурс сферы управления экономическими системами, но это сопровождается нарастанием коррупционной составляющей в профессиональной деятельности всех категорий субъектов управления. Процесс глобализации ускоряет внедрение высокоэффективных инновационных технологий и инструментов управленческого труда, но, одновременно, происходит усиление неопределенности в развитии всех факторов и условий функционирования экономики. Неопределенность и непредсказуемость сдвигов в закономерностях функционирования всех сегментов экономического пространства способны достичь критического уровня, когда возникают прямые угрозы безопасности экономической системы. К числу наиболее динамичных и, следовательно, потенциально опасных факторов результативности управления экономической системой относится состояние информационного ресурса, находящегося в распоряжении субъектов управления.

Специфика механизма влияния информационных рисков на эффективность управления макроэкономическими системами. Информационные риски в области управления макроэкономическими системами относятся, по нашему мнению, к числу наиболее опасных в силу следующих объективных и субъективных причин. Реакция экономических систем и субъектов управления на возникший информационный сигнал может быть мгновенной и радикальной, что усиливает опасность принятия недостаточно взвешенных и ошибочных решений. Информационная составляющая факторов эффективности управления имеет предельно универсальный характер, поскольку касается всех аспектов функционирования экономической системы и, соответственно, способна оказать влияние на любой ее структурный элемент.

Возможно несовпадение подлинной сущности явления и:

1. Содержания информационного сигнала о нем вследствие преднамеренного его искажения, небрежности операторов связи, технических сбоев;
2. Ошибочной интерпретацией смысла информационного сигнала о нем со стороны субъекта управления под влиянием недостаточного профессионализма или небрежности;
3. Информационным сигналом о нем в связи с методическим, организационным или техническим несовершенством модели информационно-аналитического сопровождения функции управления макроэкономической системой.

По своей внутренней природе информационные риски сопряжены, как правило, с возникновением тех или иных противоречий и дисбалансов. Эти дисбалансы могут локализоваться в пределах самой информационной системы (например, несоответствие между значимостью информации и мерами по ее защиты от несанкционированного доступа), либо они могут сложиться между информационной системой и обслуживаемыми ею субъектами управления экономической системой (например, содержание базы данных не соответствует запросам пользователя).

Состояние информационной безопасности детерминировано комплексом условий, в том числе – качеством правового регулирования отношений в данной сфере. Несовершенство нормативной правовой базы и недостаточное соблюдение законности составляют основные формы негативного влияния правового фактора на обеспечение информационной безопасности. Одним из примеров отклонений в данной области может служить государственная целевая программ «Электронная Россия», рассчитанная на период 2002–2010 г. Основные задачи программы были решены. Однако только 70% официальных сайтов федеральных органов государственной власти и органов власти субъектов РФ отвечали требованиям законодательства РФ по характеристикам полноты информации. Данный факт, хотя и не составляет прямую угрозу информационной безопасности, существенно снижает эффективность государственного управления. С явным нарушением плановых сроков была реализована такая задача программы «Электронная Россия», как организация межведомственного электронного взаимодействия при предоставлении государственных услуг.

Основным условием повышения роли информационной составляющей в обеспечении эффективности управления макроэкономикой является обоюдная требовательность и ответственность пользователей официальной информацией и субъектов, ответственных за надлежащее состояние информационных систем.

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

К ВОПРОСУ ОБ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ

Обеспечение экономической безопасности является одной из основных функций государства, поэтому изучение вопроса «экономическая безопасность» в нашей стране ведется уже длительное время. Существенный вклад в изучение вопроса экономической безопасности внес В.К. Сенчагов. Он определяет экономическую безопасность как такое состояние экономики и институтов власти, при котором обеспечивается гарантированная защита национальных интересов, социально направленное развитие страны в целом, достаточный оборонный потенциал даже при наиболее неблагоприятных условиях развития внутренних и внешних процессов.

Проблемы в области экономической безопасности сложны и взаимосвязаны, поэтому не все угрозы экономической безопасности можно нейтрализовать силами федеральных органов власти и органов власти субъектов Федерации. Состояние экономической безопасности государства напрямую зависит от состояния экономической безопасности его составных частей (регионов, муниципальных образований). Решение вопросов местного значения, противодействие угрозам и другим негативным экономическим явлениям конкретного муниципального образования, служит элементом обеспечения экономической безопасности государства.

Конституция РФ закрепляет, что государство признает право населения решать локальные, местные вопросы на свое усмотрение путем осуществления полномочий органов местного самоуправления. Полномочия органов местного самоуправления включают владение, пользование и распоряжение собственностью, которая закреплена за муниципальным образованием. Данные правомочия (владение, пользование и распоряжение) предполагают участие муниципальных образований в лице органов власти в экономических отношениях. Таким образом, муниципальные образования обоснованно можно рассматривать как субъект экономики, на который воздействуют внутренние и внешние угрозы, что определяет необходимость обеспечения экономической безопасности муниципальных образований.

Кроме управления муниципальной собственностью органы местного самоуправления самостоятельно формируют, утверждают и исполняют местный бюджет, устанавливают местные налоги и сборы. Органы местного самоуправления от имени муниципального образования управляют финансовыми потоками на местах. Полный перечень вопросов местного значения приведен для различных типов муниципальных образований в главе 3 Федерального закона от 6 октября 2003 года №131–ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации». Данный закон устанавливает, что сфера экономической безопасности муниципальных образований включает в себя защиту населения от угроз, имеющих различную природу происхождения, снижая при этом неопределенность жизнедеятельности общества.

Местное самоуправление является уровнем власти, который наиболее приближен к населению, поэтому решение вопросов местного значения, противодействие угрозам и другим негативным экономическим явлениям конкретного муниципального образования играет важную роль в обеспечении экономической безопасности государства.

Горбатов В.В., Колибаба А.В., Никифоров М.Ю.
России, Санкт-Петербург, Санкт-Петербургский университет МВД России

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТАХ МАССОВОГО СКОПЛЕНИЯ ЛЮДЕЙ (НА ПРИМЕРЕ АЭРОВОКЗАЛЬНОГО КОМПЛЕКСА)

Гражданский аэропорт (аэровокзальный комплекс) – это сложный с точки зрения охраны объект, отличающийся большой площадью, удаленностью и одновременно являющийся местом массового скопления людей, техники, а также горюче-смазочных материалов. Здесь необходима высокоэффективная, быстродействующая и надежная система безопасности, интегрированная в действующую инфраструктуру комплекса.

Во многих странах в создании и функционировании системы обеспечения безопасности в аэропортах доминирующая роль отводится авиакомпаниям или государственным правоохранительным органам. В ряде аэропортах Европы и Азии, например, вся ответственность за обеспечение безопасности принадлежит авиакомпаниями аэропорта. Для осуществления функций досмотра пассажиров и багажа, а также обеспечения пропускного режима в помещения аэропорта обычно нанимают по контракту специальную компанию, работающую в этой сфере безопасности. Для реализации своих функций обеспечения безопасности аэропорта получают ограниченные права и обязанности правоохранительные государственные органы. Однако в случаях возникновения непосредственно криминальных ситуаций портовая служба безопасности аэропорта обращается к правоохранительным государственным органам.

Задачи системы безопасности аэропорта:

– охрана порядка в залах ожидания и контроль за работой сотрудников в служебных помещениях;

– исключение несанкционированного проникновения на открытые участки территории;

– многоуровневое ограничение доступа в служебные помещения; контроль проезда автотранспорта;

– обеспечение пожарной безопасности объекта;

– предотвращение угроз террористических актов; соблюдение прочих правил авиационной безопасности.

Порядок в залах ожидания, а также предотвращение угроз террористических актов обеспечивается, в частности, видеонаблюдением, выполняемым посредством различных видеокамер. Причем, камеры объединяются в общую систему, с централизованным управлением и определенным набором функций видеоанализа. Минимальный набор аналитических возможностей

системы видеонаблюдения аэропортов – автоматическое обнаружение оставленных предметов, определение изменения фона, выделение толпе человека по определенным признакам. Обычно система видеонаблюдения аэропорта также позволяет определить направление движения нарушителя в охраняемой зоне и т.п.

Кроме того, видеонаблюдение ведется во всех служебных, производственных и административных помещениях аэропорта. При этом создается видеоархив, записи которого хранятся строго определенный временной период.

Значительную роль в обеспечение безопасности аэропортов играет система охраны периметра, исключающая возможность несанкционированного проникновения на открытые участки территории. Для этого используется высокоэффективная система охраны периметра, которая обычно состоит из нескольких рубежей охраны.

Также обеспечивается ограничение доступа транспорта, для чего используются высокоскоростные шлагбаумы, интегрированные с расчетными автоматами. Наиболее ответственные участки, например, подъезды к топливным хранилищам, оснащаются автоматическими воротами и системой считывания автомобильных номеров.

Большое значение в комплексах охраны гражданских аэропортов уделяется пожарной безопасности. В частности, система пожарной сигнализации здесь допустима только автоматическая, с отработанным алгоритмом автоматики. Одновременно устанавливаются несколько систем пожаротушения и система тревожного оповещения.

Непременным правилом авиационной безопасности является документирование всех переговоров и сообщений. В первую очередь это касается переговоров диспетчеров, а также сотрудников прочих служб, отвечающих за безопасность полетов и предотвращение террористических актов. Для этого используются специализированные многоканальные системы аудиорегистрации, исключающие риск потери информации в процессе записи. Обязательным условием этих систем является наличие сертификатов типа МАК, а также Министерства связи и Госстандарта России.

В Санкт-Петербургском университете МВД России разработана и реализуется специальная программа по подготовке сотрудников УВДТ по вопросам транспортной безопасности.

Горбатов В.В., Трабо В.Н., Харламов А.Ю.
России, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПРЕДОТВРАЩЕНИЯ ТЕРРОРИСТИЧЕСКИХ АКТОВ НА ТРАНСПОРТЕ

Защита от террористических актов на транспорте предполагает разработку различных технологий, позволяющих быстро и эффективно предотвращать такого рода явления. Практика показала, что степень защищенности транспортного объекта зависит от применения как можно более широкого спектра научно-практических методик, охватывающих различные области человеческих знаний. С помощью только досмотровой техники невозможно решить проблему выявления потенциального террориста. Восполнить данный пробел призвана методика профайлинга.

Профайлинг – это метод визуальной диагностики, оценки и прогнозирования поведения человека на основе наиболее информативных частных признаков, характеристик внешности, невербального и вербального поведения. Профайлинг служит для обозначения технологии наблюдения и опроса пассажиров в ходе предполетного и предрейсового досмотра с целью выявления потенциально опасных лиц при авиаперелетах и железнодорожных перевозках (предполетный и предрейсовый досмотр). В основе концепции профайлинга лежит предположение о том, что каждый пассажир может оказаться террористом, а каждый предмет взрывным устройством, оружием и.т.д. Мероприятия, проводимые в рамках рассматриваемой технологии, призваны подтвердить или опровергнуть данное предположение.

Наиболее удобным местом при проведении пофайлинга при предполетном (предрейсовым) досмотре является зона перед регистрационными стойками, где пассажир находится со всеми носимыми и перевозимыми им вещами.

В профайлинге разработана специальная система контрольного опроса по багажу, которая позволяет выявить возможное наличие опасных или запрещенных к транспортировке предметов, перевозимых пассажиром или переданных ему другими лицами. Акцентирование внимания пассажира, что опрос проводится в целях его безопасности, создает положительную установку для контакта с профайлером (стандартный опрос занимает по времени три-четыре минуты).

Общение с пассажирами по вопросам, выходящим за рамки проверки билетов и багажа, требует хорошо развитого интеллекта и достаточно высокой эрудиции. Профайлер по роду своей деятельности должен производить общее благоприятное впечатление. Подготовка профайлера занимает в среднем две-три недели (два-три) курса и включает в себя изучение теории профайлинга, прохождение тестовых испытаний, а также деловые игры и тренинги, практику.

Важным пунктом являются накопление базы данных подозрительных признаков, указывающих на возможность совершения теракта, и их систематизация по разным критериям (путевые документы, внешний вид, поведение).

Необходим комплексный подход к проблеме, когда пассажир, его багаж и документы рассматриваются как единый блок.

Технология профайлинга в качестве общего методологического подхода к проблеме выявления потенциального правонарушителя, террориста (преступника) может быть задействована в создании надежной системы безопасности для различных видов транспорта. Так, применение профайлинга возможно на авто- и железнодорожных вокзалах, при осуществлении мер безопасности на морском и речном транспорте.

Внедрение профайлинга, как еще одного из возможных аспектов обеспечения безопасности, вносит существенный вклад в общую ситуацию борьбы с терроризмом. Чем больше осуществляется различных практических мероприятий в данной сфере, охватывается теоретических подходов и направлений, тем выше уровень безопасности на транспорте. Таким образом, происходит опосредованное воздействие на ситуацию, снижается риск возникновения новых террористических актов.

Программа и курс «Основы профайлинга» разработаны и внедрены в учебный процесс в Санкт-Петербургском университете МВД и других образовательных учреждениях системы МВД России.

Гугасари Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В КОНТЕКСТЕ ТЕРРОРИСТИЧЕСКОЙ УГРОЗЫ

Национальная безопасность – один из основных факторов стабильного развития государства. Ее базовым показателем является вероятность негативного воздействия на ее систему, в результате которого ей может быть причинен какой-либо ущерб, ухудшающий состояние и придающий ее развитию нежелательную динамику, иначе говоря, наличие угроз национальной безопасности. В настоящее время по своим масштабам, направленности и тяжести последствий наибольшую угрозу для государства и отдельных граждан представляет терроризм. Анализ правовых средств обеспечения национальной безопасности в контексте террористической угрозы позволяет сделать следующие выводы:

1. Национальная безопасность как политико-правовая категория в рамках институционального подхода обозначает способность нации, выступающей в качестве основного субъекта обеспечения защищенности государственного суверенитета и территориальной целостности, к самосохранению, самовоспроизводству и саморазвитию в условиях геополитической напряженности и глобализационной конфликтогенности, инициирующих пренебрежительное отношение к национальным интересам и общечеловеческую унификацию в космополитическом переустройстве мирового правопорядка. При этом национальные интересы в содержательном плане ограничены политико-правовым обеспечением безопасности личности, общества и государства, а приоритетная защищенность одного из указанных субъектов определяет формы национально-государственной идентичности конкретного общества.

2. Институциональные угрозы национальной безопасности представляют собой объективно и субъективно существующую возможность разрушения национального суверенитета, государственности и юрисдикции, самобытной культуры и образа жизни, традиционных форм идентификации человека и нации любыми средствами: политическими, юридическими, социокультурными и силовыми, используемыми в целях достижения политико-правовой унификации и однополярного мира.

3. Правовая экспертиза терроризма в качестве одной из угроз национальной безопасности подтверждает изменение его современного институционального статуса: от локального политического инструмента в борьбе за власть до глобального средства устрашения путем применения института насилия для достижения политических изменений или оказания длительного психологического и социокультурного влияния, тиражируемого средствами массовой информации. Это выводит данный феномен за рамки его криминологической интерпретации. Благоприятными условиями для возникновения и осуществления террористической деятельности, угрожающей национальной безопасности, являются политическая нестабильность и ослабление государственности, кризисное состояние экономики и социальная напряженность, конфликтогенный характер межнациональных отношений, духовно-нравственная деградация общества и прочее. продуцирующие протестное поведение и повышенную социальную агрессивность, что ограничивает действенность не только правовых форм противодействия терроризму, но также и силовых акций.

4. Международный опыт законодательного обеспечения национальной безопасности в контексте террористической угрозы содержит три основных направления: разработка отдельных конвенций и заключение договоров, касающихся борьбы с различными проявлениями

террористической деятельности; юридическое обоснование антитеррористических действий и определение перечня стандартных ситуаций, в которых эти действия возможны и обязательны; правовая интерпретация международного терроризма, форм противодействия и борьбы с ним. Интеграция данного опыта в российское политико-правовое пространство будет эффективна лишь в том случае, если координация усилий суверенных государств и спецслужб в профилактике и предупреждении терроризма освободится от политики двойных стандартов, маскирующей их собственные геополитические интересы.

5. Правовая политика современного Российского государства в сфере противодействия террористической угрозе национальной безопасности осуществляется на основе адекватной законодательной базы, определяющей первостепенные цели антитеррористической деятельности и всех ее субъектов (защита личности, общества и государства от терроризма; предупреждение, выявление, пресечение террористической деятельности и нейтрализация ее последствий; превенция причин и условий возникновения террористических группировок и т.д.). Для повышения эффективности правовой политики в сфере борьбы с терроризмом необходимо усиление ее правоприменительного аспекта, а также государственного и ведомственного контроля за соблюдением антитеррористического законодательства в рамках персональной ответственности ее субъектов и средств массовой информации.

6. Региональные особенности формирования законодательного обеспечения антитеррористической деятельности на Юге России обусловлены процессами федерализации и полиэтничности, межнациональной конфликтогенности и нелегальной миграции; кризисным состоянием экономики, безработицей и оттоком русского населения из Северо-Кавказских республик; ростом экстремизма, национализма, сепаратизма и ксенофобии. Нормативно-правовые акты, принимаемые субъектами Федерации Южного и Северо-Кавказского федеральных округов, в качестве предмета регулирования определяют, с одной стороны, политический, национальный, религиозный экстремизм, миграционные процессы, деятельность общественных и религиозных объединений; с другой стороны, полномочия органов государственной власти, органов местного самоуправления и институтов гражданского общества в противодействии террористической угрозе и обеспечении национальной безопасности на региональном уровне.

Домбровская Л.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ИСТОРИЧЕСКИЙ АСПЕКТ СИСТЕМЫ БЕЗОПАСНОСТИ В РОССИИ КАК ПРЕДМЕТ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

В соответствии с ФГОС ВПО подготовка специалистов в области безопасности информационных технологий в правоохранительной сфере (направление 090915) предполагает изучение дисциплины «История развития систем защиты информации» (вариативная часть С.3.2 профессионального цикла).

Исторический аспект системы защиты информации (СЗИ) в России является составной частью системного подхода для исследования проблем безопасности как важнейшей составляющей деятельности государства.

Анализ предпосылок создания СЗИ в России, ее движущих сил и закономерностей развития служит основой для эффективного усвоения материала по таким дисциплинам как «Информационное право», «Теория информационной безопасности и методология защиты информации», «Правовая защита информации», «Оперативно-розыскная деятельность органов внутренних дел», «Информационно-аналитическое обеспечение правоохранительной деятельности».

В свою очередь, для изучения дисциплины «История развития систем защиты информации» требуются базовые знания по «Истории».

При рассмотрении становления СЗИ в России в соответствующий исторический период необходимо, по сути, ответить на следующие вопросы: что защищать, где, когда и как. Это обусловливает логику изучения дисциплины в вузе и анализ следующих моментов:

– политическая обстановка внутри России и внешнеполитическая реальность;

– экономическая ситуация в России (уклады экономики, финансовая система, промышленный потенциал и т.п.);

– процессы становления и развития системы защиты информации Российского государства в различные исторические эпохи;

– состав защищаемой информации на разных этапах развития государства;

– специфика ее обладателей в различные исторические периоды;

– виды угроз защищаемой информации и характеристики каналов несанкционированного доступа к ней;

– особенности проводимой государственной политики в области защиты информации;

– процессы, связанные с развитием и совершенствованием нормативной правовой базы по защите информации;

– структуры и функции специализированных органов защиты информации;

– факторы, оказывающие влияние на формирование современной системы защиты информации, и тенденций ее дальнейшего развития.

Раскрывая содержание перечисленных характеристик СЗИ в России, мы получаем универсальную схему ее анализа в рассматриваемый исторический период с целью понимания реальностей сегодняшнего дня и тенденций ее дальнейшего развития.

В качестве временных пределов изучения истории и правовых решений в данном курсе берутся момент возникновения государственности и сегодняшнее состояние государственной и правовой системы в области защиты информации. Хронологически этот период включает XIV – XXI вв. Пространственные пределы – территории, занимаемые Русским или Российским государством на протяжении всего указанного исторического времени.

История изучает как отдельные факты, так и закономерности исторического развития, в том числе применительно и к такому объекту как система защиты информации в России. Ее, прежде всего, интересуют юридические факты и явления. Изучая закономерности развития, она стремится выявить основные причины и следствия таких явлений, как возникновение, расцвет и упадок государственных и правовых систем и институтов. К ним относятся, главным образом, органы власти, управления (центральные и местные) и юстиции. Организация и деятельность этих органов рассматриваются как в отдельности, так и в целом, в системе. Важно представлять цельную картину и обстоятельства их эволюции и взаимодействия. Многочисленные исторические факты, которые дает история разных периодов, требуют сопоставления, сравнительного изучения.

Сравнительно-исторический метод позволяет выявлять общие закономерности становления систем защиты информации в России на разных территориях и в разные исторические эпохи.

Журавков И.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРИМЕНЕНИЕ АВТОМОБИЛЬНОГО ВИДЕОРЕГИСТРАТОРА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДОРОЖНО-ТРАНСПОРТНОГО ДВИЖЕНИЯ

В Российской Федерации за 9 месяцев (январь–сентябрь) 2010 года произошло 143608 дорожно-транспортных происшествий, в результате которых погибли 18333 человека, а 181779 человек получили ранения. Граждан, которые не попадали бы в критические ситуации на дороге практически нет, это могут быть дорожно-транспортные происшествия, конфликты с участниками дорожного движения, спорные ситуации с сотрудниками правоохранительных органов и т.д. Чтобы восстановить объективную картину происшедшего, отстоять свое видение событий и уличить нарушителя, не обойтись без независимого свидетеля, и таким свидетелем в данных случаях будет являться автомобильный видеорегистратор.

Автомобильный видеорегистратор, установленный в салоне транспортного средства, позволяет непрерывно фиксировать фактические события, происходящие на дороге. В суде, при рассмотрении ситуаций о спорных дорожно-транспортных происшествиях, видеозаписи с автомобильного видеорегистратора рассматриваются как доказательство, наравне с другими уликами.

Видеорегистратор (англ. Digital Video Recorder, DVR, цифровой видеорегистратор) – устройство, предназначенное для записи, хранения и воспроизведения видеосигналов, а при наличии микрофона, и аудиосигналов.

Чтобы изображение, полученное с автомобильного видеорегистратора приобрело статус доказательства, при аварии необходимо внести в протокол о дорожно-транспортном происшествии сведения о том, что видеорегистратор был установлен в автомобиле и производил видеозапись, указать модель и номер устройства, а также в последствии нельзя вносить никаких изменений в запись, даже если она не достаточно высокого качества.

Учитывая, что основная цель применения автомобильного видеорегистратора – получение качественного изображения, основными техническими характеристиками автомобильного видеорегистратора будут являться:

– вертикальный угол обзора, который должен быть не менее 90 градусов, горизонтальный угол обзора не менее 120 градусов, чтобы фиксировать обочину дороги, дорожные знаки, светофор и т.п.;

– число входных видеоканалов, должно соответствовать – 4, с возможностью подключения дополнительных видеокамер для фиксации дорожно-транспортного происшествия сзади или сбоку транспортного средства, что позволит фиксировать происходящее вокруг автомобиля;

– разрешение видеокамеры должно быть не менее 1.3 мега пикселя, что позволит получить более качественное изображение.

Необходимо отметить, что при дорожно-транспортных происшествиях происходит столкновение, опрокидывание транспортных средств, наезд на стоящее транспортное средство, на препятствие и т.п., и как следствие влечет за собой удар транспортного средства об указанные объекты, именно поэтому в целях непрерывной фиксации и сохранении изображения необходимо наличие у видеорегистратора датчика удара, который позволит сохранить видеозапись.

Думается, что в целях установления истины при дорожно-транспортных происшествиях необходимо использовать автомобильные видеорегистраторы как эффективное средство получения доказательной информации.

Заболотский В.П., Нестеров М.Ф., Кондратьев В.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ОБЕСПЕЧЕНИЕ ПРАВОВОЙ ОХРАНЫ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Осенью 2010 года был принят «пилотный» Закон №244-ФЗ «Об инновационном центре «Сколково». За это время появилась внутренняя структура фонда и его дочерних компаний, но главное событие – это появление первых участников проекта по созданию и обеспечению функционирования инновационного центра «Сколково», некоторым из которых уже выделено финансирование.

Тем не менее, существует потребность в плане изменения существующих нормативных актов и принятия новых. Накапливаются актуальные вопросы от участников проекта, от иных лиц, заинтересованно следящих за реализацией проекта, в том числе и в плане необходимости изменения законодательства. Существующие в России научные центры в виде технопарков, научных городков и специальных экономических зон принципиально отличаются от «Сколково». Главное отличие в публично-правовом смысле состоит в том, что Фонд «Сколково» построен принципиально иначе, нежели уже существующие научные центры – фонд, не будучи государственным органом, наделен публично-правовыми полномочиями. Например, на основании решений фонда предприятиям предоставляются налоговые и таможенные льготы, преференции в части привлечения иностранной рабочей силы и т.п., которые обыкновенное юридическое лицо предоставлять не может. Это, конечно, совершенно новый подход в правовом поле для России, хотя с точки зрения юриста, просматриваются определенные аналогии с Центральным банком РФ, который тоже имеет аналогичный уникальный статус. Этот статус позволяет фонду выполнять функции регулятора, обеспечивающего создание и развитие среды, благоприятной для осуществления инновационной деятельности. Таким образом, Фонд это прежде всего государственно-правовой регулятор инновационной среды.

Важной задачей Фонда «Сколково» является облегчение взаимодействия участников проекта с органами государственной власти. По ряду вопросов – например, по оформлению необходимых документов для привлечения иностранной рабочей силы, подаче заявок на выдачу патентов в патентное ведомство, получению таможенных льгот участникам проекта - будет достаточно обратиться непосредственно в Фонд «Сколково», а не в соответствующие государственные структуры.

Важное отличие инновационного центра «Сколково» от существующих наукоградов состоит также в том Фонд «Сколково» намерен содействовать не только осуществлению исследований, но и коммерциализации их результатов. В так называемой «экосистеме» инновационного центра «Сколково» разворачивается весь необходимый для этого инструментарий, в том числе венчурные фонды, уделяется огромное внимание междисциплинарным исследованиях и разработкам, использованию международного опыта, знаний и методологий. Кроме сугубо коммерческих бизнес-задач, Фонд планирует поддерживать и фундаментальную науку.

Для достижения целей фонда принципиально важно, чтобы права на результаты интеллектуальной деятельности, созданные в инновационном центре «Сколково», возникали именно у участников проекта и, в случае необходимости, защищались в рамках правовых отношений в течении определенного периода времени.

Однако основной инструмент защиты прав на интеллектуальную деятельность в случае столкновении интересов – суд по интеллектуальным правам, который согласно законопроекту должен заработать с 2012 года. И в настоящее время его правовой статус не определен, что, соответственно, скорее всего, повлечет срыв этого срока. В настоящее время в соответствии с постановлением Пленума Верховного Суда Российской Федерации и Пленума Высшего Арбитражного Суда Российской Федерации № 5/29 от 26 марта 2009 года «О некоторых вопросах, возникших в связи с введением в действие части четвертой ГК РФ» споры о том, кто является автором результата интеллектуальной деятельности, подведомственны судам общей юрисдикции как не связанные с осуществлением предпринимательской и иной экономической деятельности. Подведомственность споров о нарушениях интеллектуальных прав на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, об установлении патентообладателя, о праве преждепользования и послепользования, а также споров, вытекающих из договоров об отчуждении исключительного права и лицензионных договоров, определяется исходя из субъектного состава участников спора, если такой спор связан с осуществлением предпринимательской и иной экономической деятельности.

В настоящее время на рассмотрении в Государственной думе находится законопроект «О государственной поддержке инновационной деятельности», основное внимание в котором уделено

правовому статусу субъектов-участников отношений по государственной поддержки инновационной деятельности.

Таким образом, с правовой точки зрения субъект инновационной деятельности – лицо, которое в силу присущих ему признаков, определяемых юридическими нормами, может быть участником правоотношений в сфере инновационной деятельности. С одной стороны инновационная деятельность – это особая разновидность предпринимательской деятельности, поэтому логично предположить, что субъект инновационной деятельности должен обладать признаками субъекта предпринимательского права. И.А. Смагина выделяет следующие признаки субъекта предпринимательского права:

1. Легитимация в установленном законом порядке;
2. Наличие хозяйственной компетенции, т.е. совокупности хозяйственных прав и обязанностей, которыми наделен субъект в соответствии с законом, учредительными документами, а в отдельных случаях – на основании лицензии;
3. Наличие обособленного имущества как базы для осуществления предпринимательской деятельности;
4. Самостоятельная имущественная ответственность. Однако, в связи с появлением Фонда, соответствующие правоотношения усложняются, расширяется их субъектный состав. В него включается государство, субъекты инновационной инфраструктуры, характеризующиеся уже другими признаками.

По мнению некоторых юристов, критерием субъекта инновационной деятельности является имущественное или личное неимущественное право на объект, которое возникает по закону либо по договору, и которое удостоверяется соответствующим документом (патентом, лицензией и др.). Обладатели указанного права приобретают статус субъекта инновационной деятельности. Этот критерий соответствует одному из популярных подходов к определению инновационной деятельности, при которой она, по сути, отождествляется с созданием и последующей правовой охраной некоторого объекта интеллектуальной собственности. Однако, внедрение инноваций (например, полная модернизация производства, обновление технологической базы, переход на современные стандарты) не всегда обладает признаком охраноспособности, а во-вторых, наличия патента часто недостаточно для признания охраняемого объекта инновацией.

Злоказова Ю.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

МЕТОДЫ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О ТЕНЕВОЙ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ С ПРИМЕНЕНИЕМ КОЛИЧЕСТВЕННЫХ ПОКАЗАТЕЛЕЙ

Объективные данные о количественных параметрах теневой экономической деятельности необходимы для создания системы показателей экономической безопасности в рамках системы индикативного планирования, а также объективной оценки оперативной обстановки подразделениями по борьбе с экономическими преступлениями органов внутренних дел. Однако одной из самых сложных и серьезных проблем в исследовании теневой экономики является именно оценка ее масштабов.

Определение абсолютного объема теневого сектора экономики и отдельных его составляющих затруднено по причине отсутствия прямой информации, поскольку теневая деятельность предполагает сокрытие факта своего существования. Тем не менее, в настоящее время разработан ряд методик, которые на основе косвенных данных дают возможность судить о присутствии в экономике теневой составляющей. В большинстве своем они носят индикативный характер, позволяющий лишь обнаружить признаки наличия нерегистрируемой деятельности.

Существующие методы можно разделить на косвенные (макрометоды) и прямые (микрометоды).

Косвенные методы основаны на сравнении аналогичных или взаимосвязанных макроэкономических показателей, полученных разными способами. Индикатором наличия теневой деятельности служат расхождения значений соответствующих показателей. Так, суть метода «товарных потоков» заключается в том, что суммарные ресурсы по какому-либо товару или товарной группе (производство и импорт) сравниваются с суммарным использованием этих ресурсов (конечное и производственное потребление, накопление и экспорт). Наличие значительных статистических расхождений свидетельствует о недостаточной достоверности первичной информации в каких-то звеньях или о том, что какой-то элемент совокупности просто не был учтен.

Широко используются также методы оценки теневой экономики по затратам электроэнергии и по спросу на наличные деньги.

Прямые методы оценки масштабов теневой деятельности предполагают использование информации, полученной в ходе специальных обследований, опросов, а также информации налоговых служб и правоохранительных органов, полученной при проведении контрольных проверок, расследований и т. п.

В настоящее время наиболее авторитетным признан итальянский метод, который используется итальянской статистической службой (ИСТАТ). Он основан на исследовании затраченного каждым человеком своего рабочего времени. Первичная информация получается в результате специально организованного обследования домашних хозяйств, в ходе которого выясняется, какое количество часов члены домашних хозяйств дополнительно отработали в той или иной отрасли в течение определенного временного периода (неделя, месяц и т.п.). Затем полученная информация обрабатывается, распространяется на генеральную совокупность и пересчитывается в средние, нормальные отработанные человеко-дни. Параллельно обследуются предприятия с целью определения нормальной выработки в отрасли и затрат на производство. При наличии информации о времени, отработанном в неформальном секторе, о нормальной выработке и доходах в той или иной отрасли, рассчитываются показатели объема производства и доходов теневого сектора для соответствующих отраслей.

Многообразие применяемых методов свидетельствует об отсутствии единой методики количественной оценки масштабов теневой экономической деятельности. Каждая отдельно взятая методика не может претендовать на совершенство ни с точки зрения критериев достоверности, ни универсальности, ни трудоемкости расчетов.

Иванов В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ЭЛЕКТРОННАЯ ЦЕНЗУРА В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Телекоммуникационные сети сегодня являются одним из важнейших средств электронных СМИ. Несмотря на значительную роль, которую они играют в развитии информационного обмена, в ряде случаев информация, распространяемая в сети, противоречит Конституции Российской Федерации, основам ее законодательства. Нелишне отметить, что передача сообщений по сети способствовала деятельности международного терроризма в «войне небоскребов» (сентябрь 2001 г.). Если в США затем были предприняты определенные, в том числе и законодательные, усилия по ограничению распространения информации в интересах терроризма, то в других странах отношение к этой проблеме остается пока благодушным. Отметим также негативную роль сетевой информации, распространяемой через западные страны, во время грузинского конфликта. Поэтому проблема соответствия информации в сети основам национального законодательства и международного права с каждым годом будет приобретать все большее значение как неразрывная составляющая информационно-психологической и национальной безопасности, в том числе во все критические моменты жизни государства, в условиях чрезвычайной ситуации, стихийных бедствий и т.д.

Для реализации указанной политики требуется проведения большого объема работ.

Необходимо ввести систему электронной цензуры любой информации, поступающей извне, а также циркулирующей внутри страны, на предмет ее соответствия Конституции Российской Федерации. Необходимо организационно и структурно оформить указанную систему, увязав ее со структурой органов государственной власти. Необходимо разработать соответствующие технические и программно-алгоритмические средства, организовать систему подготовки и переподготовки кадров. Необходимо ввести соответствующие дополнения и изменения в основы законодательства РФ, регламентирующие деятельность новых структур в различные периоды обстановки. Необходимо ввести шкалу ответственности в отношении лиц и организаций, распространяющих в сети информацию, противоречащую Конституции РФ. Необходимо провести кампанию в СМИ по разъяснению существа предпринимаемых усилий.

Можно надеяться, что система электронной цензуры явится важным элементом укрепления системы национальной безопасности страны.

Кадулин А.В., Кадулин В.Е.
Россия, Москва, Московский университет МВД России

ПУТИ ПРОТВОДЕЙСТВИЯ ИНФОРМАЦИОННОМУ ТЕРРОРИЗМУ В СОВРЕМЕННОМ МИРЕ

В последние годы, наряду с понятием «информационная война», появился термин «информационный терроризм», применяемый часто в качестве синонима первого понятия.

Под информационным терроризмом понимается целенаправленное информационное воздействие на сознание людей с целью подавления их воли и дезорганизации деятельности с применением современных телекоммуникационных и компьютерных средств в интересах нанесения материального и морального ущерба идейным, политическим и экономическим конкурентам.

Понятие информационный терроризм можно связывать с различными уровнями организации социальных организмов (лицо), технических средств (предмет) и событий. Такими уровнями могут быть: отдельные личности; коллективы людей в семье и на работе; коллективы предприятий одинаковых и различных форм собственности; население отдельных регионов и стран; отдельное

средство телекоммуникационной системы, ее часть или вся система в целом; ЭВМ, локальные и глобальные (распределенные) вычислительные сети и их виды обеспечения. Локальные конфликты могут возникать на каждом из этих уровней организации.

В период, предшествующий локальному конфликту, информационный терроризм может носить характер периодического или постоянного воздействия на противодействующую ему сторону и создавать дезинформирующее пространство в местах дислокации сил противодействующей стороны.

Информационный терроризм всегда предполагает наличие умышленных действий заинтересованной стороны.

Последствия информационного терроризма еще мало изучены, хотя ущерб от его применения очевиден на различных уровнях, начиная от регионального и заканчивая международным.

Экономические потери от информационного террора еще требуют всеобъемлющего анализа и всесторонней оценки, однако, уже сейчас можно констатировать, что потери моральные, а, в некоторых случаях, материальные и военные имеют непредсказуемые и даже катастрофические последствия.

Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

Очевидно, что государство не способно справиться в полном объеме с задачей обеспечения безопасности всех субъектов информационных отношений. Если сегодня в соответствии с законом оно полностью отвечает лишь за вопросы защиты государственной тайны, то в большинстве остальных случаев при неопределенности доли государственного участия бремя обеспечения информационной безопасности ложится на плечи граждан и общества. Это отвечает конституционному принципу самозащиты своих интересов всеми способами, не запрещенными законом. Вот почему органы государственной власти должны четко определить свой интерес, исходя из реальных возможностей и заявленных приоритетов в обеспечении безопасности.

Целью государственной политики должно стать создание условий для максимально быстрого роста негосударственного компонента системы информационной безопасности на основе объединения усилий отдельных субъектов и установления диалога и эффективного взаимодействия с ними со стороны государства. Только при условии понимания государством в лице органов власти своих интересов, формулирования, заявления и реализации единой государственной политики, обеспечения понимания этой политики в обществе и организации взаимодействия со всеми структурами гражданского общества и действенного контроля с их участием возможно превращение России в правовое государство и создание действительно защищенного от негативного воздействия информационного общества.

Системное решение проблемы информационной безопасности может быть осуществлено при условии реализации следующих задач:

1. Одной из первоочередных задач по созданию действительно надежной системы информационной безопасности и защиты информационного пространства России является своевременное развитие законодательства.

2. В целях конкретизации основных положений Доктрины необходимо разработать концепцию системы информационной безопасности России, к созданию которой должны быть привлечены как государственные, так и общественные институты.

3. Необходимо способствовать развитию общественных институтов в области обеспечения национальной безопасности вообще и информационной безопасности в частности. При этом взаимодействие между государством и общественными институтами должно строится не на принципах создания оппозиционных противовесов, а в творческом содружестве, в поиске общих точек приложения усилий и всестороннем учете сфер взаимных интересов.

4. В сфере образования Российской Федерации назрела настоятельная необходимость разработки современной комплексной программы подготовки специалистов в области обеспечения информационной безопасности.

Таким образом, создание эффективной системы информационной безопасности России – это комплексная проблема, успешное решение которой возможно при целенаправленной совместной работе государственных, коммерческих и общественных институтов страны. Одна из главных задач высшей школы в сфере преодоления информационной опасности – это кадровое обеспечение системы информационной безопасности России путем реализации соответствующей учебной подготовки, переподготовки и повышения квалификации специалистов, а также организации обучения населения страны.

Кадулин В.А.
Россия, Москва, Управление МВД Северо-восточного административного округа г. Москвы

К ВОПРОСУ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Целью данного тезиса является: определение путей совершенствования информационного обеспечения оперативно-розыскной деятельности с точки зрения ее защиты.

В Программе МВД РФ «Создание единой информационно-телекоммуникационной системы ОВД» указаны основные направления и механизмы повышения эффективности системы информационного обеспечения ОВД посредством оборудования новыми и перспективными телекоммуникационными и программно-техническими комплексами с использованием современных информационных, телекоммуникационных и биометрических технологий.

Это весьма актуально, поскольку около трети совершаемых в стране преступлений остаются нераскрытыми. Одной из причин такого положения является слабое информационное обеспечение оперативно-розыскной деятельности.

Существующая система сбора и обработки значимой розыскной информации в виде локальных, региональных и федеральных картотек, коллекций и автоматизированных банков данных не в состоянии эффективно поддерживать деятельность по раскрытию, расследованию и профилактике преступлений. Это обусловливает необходимость совершенствования информационного обеспечения оперативно-розыскной деятельности (ОРД). Последнее приобретает безусловную актуальность в связи с активизацией деятельности на территории России организованных преступных формирований и террористических группировок.

Модернизация единого информационного пространства органов внутренних дел Российской Федерации дает возможности сократить сроки проведения поиска в интегрированных банках данных федерального («ИБД-Ф») и регионального уровней («ИБД-Регион»), содержащих сведения о лицах, судимых и находящихся в розыске, утерянном, украденном оружии, автомототранспорте, антиквариате, номерных вещах, мобильных телефонов и ряде других субъектов учета, что в конечном итоге способствует оперативному раскрытию преступлений.

Особую актуальность приобрел данный вопрос в связи с активизацией деятельности на территории России организованных преступных формирований и террористических группировок.

Правовое регулирование информационного взаимодействия наряду с другими видами деятельности (сбор, обработка, хранение информации, доступ к базам данных информационно-поисковых систем и др.) в настоящее время выступает одной из важнейших проблем. Было бы не совсем справедливо утверждать, что в этом плане на сегодня мало, что сделано. Даже Федеральный закон «Об оперативно-розыскной деятельности» как универсальный многосубъектный акт, несколько несовершенен. Именно нормы этого закона, в силу его специфики, должны закреплять, наряду с другими вопросами, исходные начала информационного взаимодействия. Тогда принимаемые в их соответствии подзаконные нормативные правовые акты вряд ли будут противоречить нормам данного закона.

Можно констатировать, что практически в любом подразделении ОВД сложилась парадоксальная ситуация – недостаток информации при ее избыточности, ее даже много, но она неструктурированна, несогласованна, разрознена, не всегда достоверна, и ее практически невозможно найти и получить в нужное время. В результате можно говорить об отсутствие информации при ее наличии и избыточности.

Выходом из положения могут быть информационные системы, представляемые в виде конструктора баз данных, позволяющие легко создать новый вид учета, при необходимости определить политику интеграции с уже существующими учетами.

Компромисс всех этих противоречивых требований, особенно при создании информационных систем оперативно-розыскного назначения, достигается применением принципов открытых систем при их создании, сопровождении и развитии. При этом определение набора базовых стандартов, которые комплексно определяют интерфейсы, протоколы взаимодействия и форматы обмена данными составляет предмет, так называемой, функциональной стандартизации.

Казанцев Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций

ПРАВОВЫЕ АСПЕКТЫ КАРТОГРАФИИ КАК ОБЪЕКТ ЗАЩИТЫ

В современном обществе картографические материалы (далее – КМ), будь то специализированные топографические планы или спутниковая фотосъемка, используются повсеместно, и не только для решения производственных вопросов, но и физическими лицами. Примером могут служить различные сервисы, такие как Google Maps, OpenStreetMap и пр.

Общемировая тенденция движения в сторону открытых информационных систем, позволяющих пользователям получать максимальный объем информации, а так же самим участвовать в ее

обновлении, в России сталкивается с проблемой устаревшего законодательства в области отнесения КМ к информации ограниченного доступа, в том числе содержащей сведения составляющие государственную тайну. В качестве регулирующих документов до сих пор действуют Советские стандарты, при издании которых даже не предполагалось, что потребность в использовании КМ будет повсеместной. Потребность государства в сохранении сведений о своей территории в тайне понятна, но подход, основанный на закрытии этих сведений для всех, чьи интересы отличны от интересов государства, не может успешно применятся в наше время.

Так, например, согласно устаревшему, но еще действующему законодательству, КМ масштаба 1:50 000 (500 м в одном см) и выше должны иметь гриф «Для служебного пользования», а если их площадь превышает 25 кв. км, то данный массив должен иметь гриф «Секретно». Для организаций, обрабатывающих массивы площадью свыше 25 кв. км это означает необходимость получения соответствующей лицензии ФСБ на работу с сведениями, составляющими государственную тайну со всеми вытекающими затратами и обременениями. Такой путь еще приемлем для государственных структур и учреждений, но для небольших организаций он перекрывает доступ к данной сфере работ. С точки зрения формального исполнения законодательства конечно существует возможность выполнить все требования с наименьшими затратами. Так, например, секретный массив можно разделить на несколько частей таким образом, чтобы в каждой части суммарная площадь не превышала 25 кв. км и получить несколько массивов, не содержащих сведений, составляющих государственную тайну.

Но даже без грифа «Секретно», гриф «ДСП» отсекает возможность открытого опубликования и использования КМ. Если же преобразовать КМ в предназначенные для открытого опубликования согласно действующему законодательству, на выходе получается материал, не отвечающий современным потребностям и теряющий всякую стоимость.

Картография – это как раз тот случай, когда стоит задуматься не о том, как защищать объект, а о том, нужно ли его защищать. Стоит поставить вопрос таким образом – насколько губительно для развития данной отрасли в России существующее отношение к картографии как к объекту защиты.

Несоответствие существующего законодательства потребностям общества безусловно видно и первым лицам государства, установлен приоритет на снижение избыточных ограничений, что отражено, в частности, в новой Концепции развития геодезии и картографии на ближайшие 10 лет.

Для развития картографической отрасли в России необходимо снять ограничения, наложенные искусственно. При этом, безусловно, будут задеты интересы множества субъектов, так или иначе участвующих в процессе обслуживания КМ, содержащих сведения ограниченного доступа. Излишние ограничения так или иначе будут сняты. Вопрос лишь в том, когда это произойдет и как далеко в своем развитии за это время уйдет весь западный мир.

Клепикова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ОБЕСПЕЧЕНИЕ КОНТРОЛЯ ОСТАТОЧНЫХ ЗНАНИЙ ПО СПЕЦИАЛЬНОСТИ 090103.65 – ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В различных вузах при подготовке по специальности 090103.65 – «Организация и технология защиты информации» в значительной степени используется компьютерная техника. Этой техникой обеспечиваются специальные классы. Многие студенты и слушатели приносят свои ноутбуки. Данное обстоятельство создает возможность помимо эффективного обучения использовать и эффективные процедуры проверки знаний обучающихся.

В настоящее время среди путей повышения эффективности процесса обучения можно выделить отдельное направление – совершенствование методов оценки знаний.

Реализация качественного контроля на всех стадиях учебного процесса в современных условиях невозможна без использования средств информационных и коммуникационных технологий (ИКТ). К ним можно отнести комплекс технических, программно-аппаратных, программных средств, систем и устройств, функционирующих на базе вычислительной техники; современных средств и систем информационного обмена, обеспечивающих автоматизацию ввода, накопления, хранения, обработки, передачи и оперативного управления информацией. Более конкретно, средствами ИКТ являются: ПЭВМ, периферийное оборудование; средства технологии мультимедиа и систем «виртуальная реальность»; системы машинной графики и искусственного интеллекта; средства коммуникации (сетевое оборудование, программные комплексы, телефонные линии, волоконно-оптические и спутниковые каналы связи) и их инструментарий. К этим же средствам можно отнести такие автоматизированные системы на базе ЭВМ, как автоматизированные обучающие системы (АОС) или комплексы (АОК), автоматизированные учебные курсы (АУК), автоматизированные системы управления (АСУ) вузом, автоматизированные контролирующие системы (АКС) и другие.

Все указанные средства и системы обязательно решают функцию контроля знаний, автономно или в роли подсистем. Однако нацелены они в основном на диагностику текущего уровня знаний, умений и навыков учащихся. Менее проработаны вопросы измерения остаточных знаний (ОЗ), под которыми будем понимать тот минимальный их объем, который остается в памяти обучаемого по истечении какого-то времени после завершения изучения дисциплины (темы). В силу отдаленности по времени контроль остаточных знаний (КОЗ) в ныне используемых формах мало влияет на текущий ход учебного процесса, хотя является одновременно мощным диагностирующим средством и средством совершенствования системы обучения в вузе в целом.

Актуальность исследования и решения проблем в области измерения остаточных знаний учащихся обусловлена необходимостью разработки быстрого, точного и гибкого механизма оценивания именно этой разновидности знаний для реализации следующих задач (целей):

– создание эффективного средства обратной связи для более объективной и кардинальной корректировки всего процесса обучения, в первую очередь, на основе совершенствования системы внутривузовского контроля;

– проведение объективной аттестации и аккредитации вуза по распоряжению вышестоящих органов управления;

– сравнительная оценка качества образования в однопрофильных вузах, разных городах, республиках и регионах страны, а также сравнение качества образования в разных странах.

Указанные задачи можно решить только на базе использования тестового метода, переживающего в нашей стране как бы второе рождение, и современных средств информационных и коммуникационных технологий (ИКТ).

Кургин А.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

К ВОПРОСУ О ЗАЩИТЕ ДЕТЕЙ ОТ ВРЕДНОЙ ИНФОРМАЦИИ: ПРАВОВОЙ АСПЕКТ

Современный уровень развития информационных технологий не позволяет родителям ограждать детей от опасной для них информации. В связи с переизбытком насилия и жестокости в общедоступных источниках массовой информации у детей раннего возраста повышается уровень агрессии, повышается уровень психических заболеваний (неврозов), происходит приобщение к вредным привычкам, таким как курение и алкоголь.

В интернете в достаточно свободном доступе находятся видеофайлы, побуждающие детей к социально-опасным действиям, подвергающим риску их здоровье. Например, видео «зацеперов» (молодых людей «прицепляющихся» к вагонам и крышам электричек и проезжающих, таким образом, путь до станции).

В обществе возникла проблема ограничения вредной для детей информации, побуждающую к употреблению наркотиков, табака, алкоголя, к причинению вреда своему здоровью, самоубийству, обосновывающей или оправдывающей допустимость насилия и жестокости. В связи с этим был принят ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», вступающей в действие с 1 сентября 2012 года. Данный закон вводит маркировки для информации и подразделяет её на несколько категорий: для детей, не достигших возраста 6 лет; старше 6 лет; старше 12 лет; достигших возраста 16 лет; запрещенная для детей информация. Но на данный момент не представлено никакой методики или требований оценки информации по данной классификации, издатель или вещатель информации определяет её сам.

Доступные исследования взаимозависимости информации, содержащей насилие, и моральным уровнем общества достаточно противоречивы. Иногда просмотр видеофильмов, содержащих сцены насилия, носят не только отрицательный характер. Ярким примером является книга Энтони Бёрджесса «Заводной апельсин» 1962 года, где несовершеннолетнему преступнику насильно показывали кровавые сцены. Спустя время, любая мысль о причинении вреда человеку вызывала у него реакцию отторжения. Но данные факты, не отменяют того, что, в другом случае, насилие, наоборот, может сформировать у детей неправильные жизненные ценности и установки.

Другое исследование представляет доказательства об обратной реакции на запрет вредной информации: мальчики, просматривающие в течение месяца агрессивные программы, проявляли меньший уровень агрессии, чем их сверстники, ограниченные от видеофайлов, содержащих насилие. Хотя при учете влияния интеллекта и социально-экономического статуса детей, оказалось, что данные факторы сильнее воздействуют на уровень насилия и агрессии среди детей, чем просмотр видеофайлов, содержащих сцены насилия. В соответствии с этим, как представляется, принятый закон «О защите детей от информации, причиняющей вред их здоровью и развитию» может вызвать Последствия, противоположные ожидаемым. В этой связи, вероятно, следует обратить внимание на развитие программ, способствующих повышению уровня интеллекта и образования у детей.

Лавренов В.В.
Беларуссия, Минск, Академия МВД Республики Беларусь

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

В условиях развития цивилизации, перехода к информационному обществу, научное знание и информация становятся определяющим фактором общественной жизни. Информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств. В связи с этим информационная безопасность играет важную роль в существовании и развитии любого государства.

Информационная безопасность – защищенность информационной сферы и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Выделяют следующие составляющие информационной безопасности:

– законодательная, нормативно-правовая и научная база;
– органы, обеспечивающие безопасность информационных технологий;
– организационно-технические и режимные меры и методы обеспечения информационной безопасности;
– программно-технические способы и средства обеспечения информационной безопасности.

На уровне государства основой законодательной и нормативно-правовой составляющей информационной безопасности является конституция Республики Беларусь, Концепция национальной безопасности Республики Беларусь, закрепившая совокупность официальных взглядов на сущность и содержание деятельности по обеспечению баланса интересов личности, общества, государства и их защите от внутренних и внешних угроз, в том числе и в информационной сфере. В 2001 году вступил в силу новый уголовный кодекс Республики Беларусь. Как следует из Особенной части Уголовного кодекса Республики Беларусь, информационные правоотношения в целом получили в нем широкую уголовно-правовую защиту. Среди преступлений, впервые введенных в Уголовный кодекс, законодателем определены шесть преступлений, предметом преступного посягательства которых является компьютерная информация (ст.349–ст.355), эти статьи составили новую главу – «Преступления против информационной безопасности».

Выработку политики информационной безопасности, подготовку законодательных актов и нормативных документов, контроль над выполнением установленных норм обеспечения безопасности информации осуществляют государственные органы. Анализ нормативных актов и других руководящих документов позволяет констатировать, что к числу государственных органов исполнительной власти и иных учреждений Республики Беларусь, участвующих в выполнении координирующих функций в области обеспечения информационной безопасности, следует отнести Совет Безопасности, Совет Министров, Администрацию Президента Республики Беларусь, КГБ, Государственный центр безопасности информации, Министерство информации, Комитет по науке и технологии и межведомственная комиссия по вопросам информатизации при Совете Министров Республики Беларусь и Оперативно-аналитический центр при Президенте Республики Беларусь. При этом большое значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством.

Достижение высокого уровня безопасности невозможно без принятия должных организационных мер. Организационные меры – это единственное, что остается, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности. В основе организационных мер защиты информации лежат политики безопасности. От их эффективности в наибольшей степени зависит успешность любых мероприятий по обеспечению информационной безопасности. В республике Беларусь это достигается деятельностью субъектов обеспечения информационной безопасности по защите личности, общества и государства от внутренних и внешних угроз, реализации национальных интересов, созданию необходимых условий для устойчивого развития Республики Беларусь. Субъектами обеспечения информационной безопасности являются: государство, осуществляющее свои полномочия в данной сфере через органы законодательной, исполнительной и судебной власти; общественные и иные организации; граждане.

Четвертая составляющая системы – программно-технические способы и средства обеспечения информационной безопасности направлены на обеспечение безопасности информационных систем и сетей связи, разработку и внедрение современных методов и средств защиты информационных технологий, являющихся жизненно важными для страны.

Таким образом, в Республике Беларусь создана и успешно функционирует система информационной безопасности, направленная на реализацию интересов Республики Беларусь в информационной сфере.

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

АВТОМАТИЗАЦИЯ ИНФОРМАЦИОННЫХ ПОТОКОВ: ЮРИДИЧЕСКИЕ АСПЕКТЫ

Развитие и становление современного общества связано с увеличением объема информации, которая в нем циркулирует. Причем эта тенденция приобретает гиперболизированные формы. Так, к примеру, по оценкам специалистов объемы информации (всей) в Южной Корее удваиваются примерно каждые 11–12 дней. Очевидно, что такое количество информации нуждается с одной стороны в упорядочении, путем ее целенаправленного движения от источника информации к ее потребителю (назовем этот процесс условно информационным потоком) и с другой – в организационном и юридическом его закреплении. Причем предметная сфера информационного обеспечения общественной жизни взаимосвязана с необходимостью детального нормативного закрепления (к примеру, информация о культурной жизни общества объективно нуждается в менее четком юридическом закреплении, чем информация в правоохранительной сфере или о членах этого общества).

Как мы уже отмечали, существует необходимость автоматизации информационных потоков, обусловленная упорядочением информации с целью ее рационального использования. Поскольку принятие грамотных управленческих решений в любой сфере общественной деятельности невозможно без полной, достоверной и своевременной информации. В этой связи, развитие компьютерной техники обусловило возможность создания различных автоматизированных информационных систем и банков данных (АИС И АБД) для накопления, обработки и использования информации в соответствующей предметной области.

Полагаем, что такая деятельность имеет в первую очередь положительную направленность, и направлена на должное информационное обеспечение соответствующей сферы общественной жизни. Однако, анализ юридического закрепления формирования информационных массивов в различных сферах показал, что нет единого подхода к объему, порядку и основаниям использования информации. И, видимо, этого и никогда не будет в силу специфики жизни и циркулирующей в ней информации.

Следует отметить что, необходимость четкого правового оформления форм и видов ответственности объективно существует. При разглашении либо утечке информации в определенной мере это компенсируется правовыми институтами тайн, которых, для примера, только в Республике Беларусь насчитывается порядка 30. Однако, правовая охрана информации в целом и более того упорядоченной информации содержащейся в виде различных АИС и АБД зачастую заключается лишь в констатации факта самой тайности той или информации, без четких юридических форм и видов ответственности при ее нарушении ее конфиденциальности.

Более того, актуальность юридического закрепления процессов автоматизации информационных потоков вызвана широким внедрением различных информационных компьютерных сетей и средств передачи и обработки информации. Так, развитие сети Интернет наряду с большим количеством положительных моментов, несет в себе угрозы конфиденциальности и сохранности информации в первую очередь о членах общества, то есть фактически мы можем говорить, что информация в сети Интернет фактически не защищена, особенно с учетом свойства экстерриториальности этой сети.

Таким образом, объективно назрела необходимость единого юридического закрепления на межгосударственном уровне процессов сбора, обработки и использования информации содержащейся в различных информационных системах международного уровня, а также имплементация этих норм в национальные законодательства государств.

Лепёхин А.Н.
Беларуссия, Минск, ГУВД Мингорисполкома МВД Республики Беларусь

ГЕНЕЗИС ЮРИДИЧЕСКОЙ ОЦЕНКИ ХИЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ ПЛАСТИКОВЫХ КАРТОЧЕК В РЕСПУБЛИКЕ БЕЛАРУСЬ

Внедрение банковских пластиковых карточек в быстро развивающиеся экономические отношения явилось одной из важнейших тенденций функционирования технологий безналичных расчетов в банковской сфере. Однако применение высоких технологий в различных отраслях финансово-хозяйственной деятельности повлекло за собой усовершенствование способов хищения денежных средств. Именно хищения путем использования компьютерной техники становятся все более изощренными и трудно выявляемыми преступлениями. Появление пластиковых платежных средств как альтернативы бумажных денег породило новые способы совершения преступлений с банковскими пластиковыми карточками.

Особенностью хищения, предусмотренного статьей 212 Уголовного кодекса Республики Беларусь («Хищение путем использования компьютерной техники»), является способ посягательства на отношения собственности. Такое хищение может быть совершено путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой

по сетям передачи данных, либо путем введения в компьютерную систему ложной информации. Частью второй статьи 212 УК Республики Беларусь в качестве квалифицированного способа совершения данного деяния предусмотрен несанкционированный доступ к компьютерной информации. Неправильное понимание указанных способов хищения, ответственность за совершение которых предусмотрена статьей 212 УК Республики Беларусь, приводит к ошибкам квалификации данного деяния. По нашему мнению, под введением ложной информации в компьютерную систему следует понимать введение в компьютерную систему информации, отличающуюся от той, которая должна быть введена в компьютерную систему при осуществлении определенной операции. Исходя из этого, введение злоумышленниками в компьютерную систему процессингового центра банка подлинного пин-кода банковской пластиковой карты, принадлежащей третьему лицу, не образует введения в компьютерную систему ложной информации. В данном случае содеянное следовало квалифицировать по соответствующей части статьи 205 УК Республики Беларусь (кража), а не статьи 212 УК Республики Беларусь. В свою очередь ранее, судебные и правоохранительные органы в процессе квалификации, хищений, совершаемых с использованием пластиковых банковских карт, учитывали, что несанкционированный доступ к компьютерной информации предполагает преодоление систем защиты, то есть нарушение установленных правил доступа к компьютерной информации. Это могло быть: противоправная расшифровка кода доступа, пароля, ключа; модификация программного обеспечения; изменение физических адресов технических средств и иные подобного рода манипуляции с использованием программных и аппаратных средств компьютерной техники. Применение для завладения чужих денежных средств подлинного нерасшифрованного и немодифицированного пин-кода банковской пластиковой карты, принадлежащей третьему лицу, не могло рассматриваться в качестве хищения с использованием компьютерной техники, сопряженного с несанкционированным доступом к компьютерной информации. В этом случае содеянное квалифицировали по соответствующей части статьи 205 УК Республики Беларусь, а не статьи 212 УК Республики Беларусь. Однако в процессе правоприменительной практики, были выработаны изменения в Постановление Пленума Верховного суда Республики Беларусь от 21 декабря 2001 года №15 «О применении судами уголовного законодательства по делам о хищениях имущества», где было разъяснено, что хищение путем использования компьютерной техники (ст.212 УК) возможно лишь посредством компьютерных манипуляций, заключающихся в обмане потерпевшего или лица, которому имущество вверено или под охраной которого оно находится, с использованием системы обработки информации, где данное хищение может быть совершено как путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, так и путем введения в компьютерную систему ложной информации. Несанкционированным при хищении с использованием компьютерной техники (часть 2 ст.212 УК) считается доступ к компьютерной информации лица, не имеющего права на доступ к этой информации либо имеющего такое право, но осуществляющего его помимо установленного порядка.

Таким образом, вопросы квалификации хищений путем использования компьютерной техники достаточно сложны в своем разрешении и не имеют единой позиции среди правоохранительных органов, а требуют выработки единообразных подходов к юридической оценке таких противоправных деяний со стороны органов предварительного расследования, прокуратуры и суда.

Макаров О.С., Вус М.А.
Беларуссия, Минск, Институт национальной безопасности Республики Беларусь
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

К ВОПРОСУ РЕКОМЕНДАЦИЙ ПО СОВЕРШЕНСТВОВАНИЮ ЗАКОНОДАТЕЛЬСТВА ОДКБ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Глобальные процессы, характерные для социально-экономического развития мира в преддверии информационного общества, определяют особую роль информационной безопасности. Информационная безопасность стала сегодня важнейшим компонентом национальной и международной безопасности. При этом с позиций обеспечения и национальной и международной безопасности проявляется дилемма: путь общественного развития пролегает через процессы информатизации, однако информатизация общества порождает геометрическое возрастание угроз национальной безопасности (при этом, формируется целый ряд новых угроз, методологии противодействия которым до настоящего времени не разработаны).

Информатизация и телекоммуникационные технологии пронизывают все стороны жизнедеятельности общества. Информационная сфера стала системообразующей, и от ее состояния в значительной степени зависит сегодня уровень экономического, социального и политического развития. В то же время в рамках экономического, коммерческого и военного противоборства сама информация и информационно-коммуникационные технологии могут выступать (и уже используются) в качестве угроз интересам конкурентов. Негативные последствия реализации угроз информационной безопасности, могущих проявляться в самых разных сферах жизнедеятельности личности, общества

и государства, прямо и опосредовано влияют на национальную безопасность в политической, экономической и иных сферах.

Интенсивно развиваются социальные сети, сети в бизнесе, финансах, в экономике. При их формировании во многом превалируют интересы прибыли в бизнесе, что не всегда совпадает с потребностями и ожиданиями общества. Как следствие проявляются новые угрозы и риски в информационной сфере, мало управляемые психологические, политические и экономические факторы и их связи. Не случайно уже на уровне ЮНЕСКО звучат призывы начать оценивать возможные последствия некритического применения новых информационных технологий.

Нередко являющиеся открытым пространством социальные сети сегодня создаются с надеждой бесконтрольности со стороны государства и используются для негативных воздействий на психику, мнение и поведение неорганизованной массы населения. Так, например, широкое распространение получила практика публикаций в Интернете различного рода статей клеветнического характера, инсинуаций, прямого подстрекательства к нарушению законодательства. Поэтому все явственнее выступает необходимость контролировать социальные сети в Интернете. Однако сегодня практика расширения позитивного регулирования в социальной и информационной сферах, (предполагающее установление и соблюдение порядка), реализуется в системах обеспечения безопасности, включая и область информационной безопасности, в относительно скромных масштабах. При этом сильное воздействие на выстраивание отношений в экономической и социальной сферах оказывает технологический подход к пониманию социальной сети в Интернете.

Традиционные меры обеспечения информационной безопасности можно подразделить на две группы: охранительные (например, защита государственной тайны, конфиденциальности персональных данных и др.) и обеспечивающие (сюда следует отнести и обеспечение информационной политики государства). Базовые структурные составляющие системы обеспечения информационной безопасности можно условно разделить на три группы.

1). Жизненно важные интересы общества, государства и личности как отражение объективных экзистенциональных потребностей личности, общества и государства; научные знания и информация, дающие представление об опасностях и угрозах экзистенциональным потребностям личности, общества и государства; декларируемые концептуальные положения – взгляды на цели и принципы обеспечения безопасности (концепции и доктрины безопасности в каждой из сфер жизнедеятельности общества);

2). Субъекты и объекты системы обеспечения национальной безопасности и правовые нормы, регулирующие отношения, как в информационной сфере, так и в каждой из видовых сфер обеспечения безопасности;

3). Силы и средства, нацеленные на обеспечение безопасности; методы и способы её обеспечения, а также собственно деятельность по обеспечению безопасности и ее результаты.

Однако традиционно используемая в рамках исследований проблем безопасности концептуальная архитектура (интересы – угрозы – меры) оказывается не всегда адекватной при анализе проблематики информационной безопасности. Особенность последней заключается в том, что угрозы могут быть направлены не только непосредственно на интересы, но и а на способы их реализации. В силу этого в ряду проблем обеспечения безопасности, наряду с вопросами создания необходимых условий для обеспечения безопасности функционирования информационно-телекоммуникационных систем, следует рассматривать вопросы защиты прав граждан в информационных системах и сетях. Необходим, в частности, разумный контроль за социальными сетями в рамках защиты интересов граждан и недопущения роста преступности.

Представляется, что в интересах обеспечения безопасности в рамках Организации Договора о коллективной безопасности целесообразно выработать единые правила пользования Интернетом и социальными сетями и закрепить их на уровне международных договоров и соглашений.

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

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Примечательная особенность нынешнего периода – переход от индустриального общества к информационному обществу, в котором информация становится более важным ресурсом, чем материальные или энергические ресурсы. Ресурсами, принято называть элементы экономического потенциала, которыми располагает общество и которые при необходимости могут быть использованы для достижения конкретной цели хозяйственной деятельности. Давно стали привычными
и общеупотребительными такие категории, как *материальные, финансовые, трудовые, природные* ресурсы, которые вовлекаются в хозяйственный оборот, и их назначение понятно каждому. Но вот появилось понятие «информационные ресурсы», и хотя оно узаконено, но осознано пока еще недостаточно. Информационные ресурсы – отдельные документы и отдельные массивы, документов в информационных системах (библиотеках, архивах, фондах, банках данных, других

информационных системах). Информационные ресурсы являются собственностью, находятся в ведении соответствующих органов и организаций, подлежат учету и защите, так как информацию можно использовать не только для товаров и услуг, но и превратить ее в наличность, продав кому-нибудь, или, что еще хуже, уничтожить. Собственная информация для производителя представляет значительную ценность, так как нередко получение (создание) такой информации – весьма трудоемкий и дорогостоящий процесс. Очевидно, что ценность информации (реальная или потенциальная) определяется в первую очередь приносимыми доходами.

Особое место отводится информационным ресурсам в условиях рыночной экономики. Важнейшим фактором рыночной экономики выступает конкуренция. Побеждает тот, кто лучше, качественнее, дешевле и оперативнее (время-деньги!) производит и продает. В сущности, это универсальное правило рынка. И в этих условиях основным выступает правило: кто владеет информацией, тот владеет миром.

В конкурентной борьбе широко распространены разнообразные действия, направленные на получение (добывание, приобретение) конфиденциальной информации самыми различными способами, вплоть до прямого промышленного шпионажа с использованием современных технических средств разведки. Установлено, что большая часть охраняемых сведений добывается с помощью технических средств, промышленного шпионажа.

В этих условиях защите информации от неправомерного овладения ею отводится весьма значительное место. При этом целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

Основное внимание уделяется защите конфиденциальной информации, с которой большей частью встречаются предприниматели негосударственного сектора экономики.

Люди осознают и отдают себе отчет в сложности проблемы защиты информации вообще, и с помощью технических средств в частности. Тем не менее, считается, что этим охватываются не все аспекты сложной проблемы, а лишь определенные ее части.

Информационная безопасность является состоянием защищенности информационной среды общества, обеспечивающая ее формирование, использование и развитие в интересах граждан, организаций, государств. Информация – это всеобщее свойство материи. Любое взаимодействие в природе и обществе основано на информации. Всякий процесс совершения работы есть процесс информационного взаимодействия. Информация – продукт отражения действительности. Действительность отражается в пространстве и времени. Ничего не происходит из ничего. Информация сохраняет значение в неизменном виде до тех пор, пока остается в неизменном виде носитель информации – память.

Понятие «информация» сегодня употребляется весьма широко и разносторонне. Трудно найти такую область знаний, где бы оно ни использовалось. Огромные информационные потоки буквально захлестывают людей. Объем научных знаний, например, по оценке специалистов, удваивается, каждые пять лет. Такое положение приводит к заключению, что XXI век будет веком торжества теории и практики информации – информационным веком.

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

ПРАВОВЫЕ ВОПРОСЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ ПОЛИЦИИ

Персональные данные – это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация (статья 3 ФЗ №152 «О персональных данных» от 27.07. 2006 года).

Сотрудники полиции также являются субъектами персональных данных согласно той же статье 3 Федерального Закона «О персональных данных». Данный Федеральный закон должен был вступить в силу 1 января 2010 года. К сожалению, перед самым Новым годом объявили, что вступление в силу этого закона отложено еще на год.

26 июля 2011 года президент РФ Дмитрий Медведев подписал поправки к закону «О персональных данных». Документ ужесточает требования к обеспечению мер безопасности

персональных данных. В частности, компаниям и индивидуальным предпринимателям необходимо использовать средства защиты персональных данных, которые прошли соответствующую сертификацию ФСБ.

Какие же правовые вопросы необходимо решить, чтобы защитить персональные данные при вступлении вышеназванного закона?

В данной статье рассмотрим некоторые правовые вопросы защиты персональных данных сотрудников полиции.

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

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

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

1. Конституция РФ (Статья 23, 24).
2. Трудовой кодекс РФ (Глава 14).
3. Федеральный закон «О полиции»Федеральный закон №152-ФЗ «О персональных данных» от 27 июля 2006 года. Положение «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждено постановлением Правительства Российской Федерации №781 от 17 ноября 2007 года.
4. Положение «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждено постановлением Правительства Российской Федерации №687 от 15 сентября 2008 года.
5. Приказ Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия №154 «Об утверждении Положения о ведении реестра операторов, осуществляющих обработку персональных данных» от 28 марта 2008 года.
6. «Порядок проведения классификации информационных систем персональных данных», утверждён приказом ФСТЭК России, ФСБ России и Мининформсвязи России №55/86/20 от 13 февраля 2008 года.
7. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержден приказом Гостехкомиссии России №282 от 30 августа 2002 года (ДСП).
8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15 февраля 2008 года. (Выписка, при рассмотрении угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН) необходимо применять полную версию данного документа – ДСП).

Невыполнение требований вышеназванных документов может привести к конфликту с государственными органами, осуществляющими контроль и надзор в данной сфере деятельности, и привлечению организации или ее руководителя к административной или иным видам ответственности.

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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИЗИЧЕСКИХ ЛИЦ В СЕТИ ИНТЕРНЕТ

К настоящему времени основные направления развития законодательства в информационной сфере определены, в основном соответствуют зарубежной практике правового регулирования информационных отношений и осуществляются в соответствии с международно-правовыми требованиями к обеспечению свободы слова и иных прав и законных интересов граждан в области производства, хранения и распространения информации.

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

На современном этапе законодательные инициативы должны затрагивать два основных направления регулирования в информационной деятельности общества: информационное экономическое право (регулирует порядок осуществления в информационной сети электронной экономической деятельности: электронной торговли, Интернет – банкинга, электронного консалтинга, электронного рекламинга, Интернет – страхования и т.д.); информационное гуманитарное право

(регулирует порядок осуществления в информационной сети электронной гуманитарной деятельности по обеспечению государством реализации информационных прав физических лиц, в том числе путем создания и функционирования систем электронного администрирования). Одним из направлений здесь является развитие существующих более чем в 30 странах мира так называемых систем электронного правительства (управления). Несмотря на принятие соответствующих концепций и развития системы электронного правительства существует много проблем и в основном правового характера. К 2017 году поэтапно предполагается выдать всем дееспособным гражданам России пластиковую карту, с помощью которой можно будет совершить большинство уведомительных, регистрационных и платежных операций через инфоматы. В рамках этой системы реализация прав граждан на оказание им публичных услуг осуществляется органами государства с помощью глобальных компьютерных сетей. В частности, уже сейчас граждане получают возможность через специальные сайты государственных органов в сети Интернет получать доступ к соответствующей публичной информации о деятельности этих государственных органов, обращаться с жалобами и обращениями, направлять заявки на выдачу всевозможных справок, разрешений, оказание услуг социального характера.

Но недостаточное информирование общества вызывает неадекватные действия со стороны граждан, недостаточно осведомленных в сфере информационных технологий и своих прав на защиту персональных данных. Указанная система должна способствовать упрощению диалога между обществом и властью, повышать эффективность и адресность государственного и муниципального управления. Другим направлением выступает обеспечение государством информационных прав граждан, в том числе на свободный оборот незапрещенной (находящейся в открытом доступе) информации, ее сбор, обработку и распространение в электронной форме.

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

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

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

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

ПРОБЛЕМЫ СОЧЕТАНИЯ ТРАДИЦИОННЫХ И СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ПРИ ПОДГОТОВКЕ И ПЕРЕПОДГОТОВКЕ ЮРИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Интеграция России в мировое правовое сообщество привела к скачкообразному росту числа законов во всех областях деятельности. Одной из текущих проблем сейчас является проблема подготовки юристов в области информационной безопасности. Особенность этой задачи заключается в том, что, в идеале, подобный юрист, если бы его удалось подготовить, должен был быть универсально компетентным как в правовой, так и в информационно-программной и технической областях данного направления.

В докладе рассматривается концепция системы управления процессом модульного обучения для повышения качества и сокращения сроков подготовки юристов в области информационной безопасности, в том числе и по безотрывной, от основной профессиональной деятельности, форме обучения, что позволяет экономить время и значительные средства, затрачиваемые в настоящее время на организацию заочного обучения в ОВД.

Учитывая высокий уровень компьютеризации правоохранительных органов в Санкт-Петербурге и Москве, развитые телекоммуникационные сети в этих регионах, а также значительно возросшую за последние годы степень насыщения компьютерной техникой отдельных граждан, следует признать существование необходимых и достаточных условий для внедрения дистанционного обучения в процесс подготовки слушателей заочного факультета Санкт-Петербургского университета МВД России.

Учитывая особенности контингента обучаемых на ФЗО, где преобладают слушатели среднего начальственного состава, относительно молодого возраста и со значительными перспективами служебного роста, следует при разработке индивидуальных планов дистанционного обучения учитывать особенности их повседневной служебной деятельности в ОВД с целью корректировки рабочих учебных планов в направлении увязывания их содержательной части с практической деятельностью обучающегося.

Анализ гуманитарной составляющей учебного плана специальности юриспруденция позволяет провести обоснование возможности построения резидентных модулей технического содержания, связанных с информационной безопасностью и, таким образом, начать обучение по данной специализации без существенных изменений структуры учебного плана и большинства учебных программ.

Новизна предлагаемого способа решения проблемы заключается в обосновании возможности взвешенного сочетания базовой гуманитарной подготовки юристов с их специализацией в области информационной безопасности за счет применения методики использования модульного подхода, ориентированного на избирательное освоение основных положений специализации.

Развитие новых направлений в области правовой защиты в настоящее время опережает возможности высших учебных заведений, в том числе и министерства внутренних дел, по подготовке и переподготовке юристов в новых областях, таких как информационная безопасность и других.

Экстенсивное развитие подготовки кадров соответствующей квалификации в настоящее время потребовало бы больших ресурсов и создания новых учебных планов, что значительно повысило бы время выпуска специалистов по высоко – дефицитным направлениям. Альтернативой такому подходу могла бы стать интенсивная подготовка по требуемым направлениям в рамках существующего учебного плана специальности юриспруденция.

Однако, ограниченный объем учебных часов, отводимых учебным планом для аудиторных занятий, делает подобный подход проблематичным. Предлагаемый в докладе подход к подобной ситуации заключается не только в динамичном перераспределении учебных часов между аудиторными занятиями и самостоятельной работой, но и во введении модульного подхода к освоению дисциплин выбранного направления подготовки.

В докладе развиваются и детализируются методы структурной декомпозиции существующего учебного плана с целью выявления семантически значимых составляющих целевой подготовки для формирования блоков обучающих модулей по направлению информационной безопасности.

Для формирования структуры системы управления процессом модульного обучения анализируются результаты предварительного тестирования слушателей с целью определения их адаптации к условиям перехода на модульное обучение и предлагаются методики отбора на конкретную специализацию, в том числе и в области компьютерной безопасности, в рамках специальности юриспруденция.

Предложены принципы построения модулей специализации «Информационная безопасность», ориентированные на различные подходы к резиденции модулей в учебный план специальности юриспруденция.

Практическая значимость предлагаемого подхода заключается в существенном сокращении затрат на подготовку остродефицитных специальностей юристов в области борьбы с компьютерными преступлениями.

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

УНИВЕРСАЛЬНАЯ СИСТЕМА ТЕСТИРОВАНИЯ ДЛЯ ОРГАНИЗАЦИИ МОНИТОРИНГА ЗНАНИЙ УЧАЩИХСЯ В РАМКАХ ДИСТАНЦИОННО-МОДУЛЬНОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧЕБНЫХ ЗАВЕДЕНИЯХ СИСТЕМЫ МВД РОССИИ

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

Разработанная программная оболочка предназначена для контроля знаний учащихся по различным учебным дисциплинам (прежде всего, по специальности 090103.65 – организация и технология защиты информации), преподаваемым в Санкт-Петербургском университете МВД России. Однако, реализованные в работе принципы контроля знаний могут быть использованы и в любой другой предметной области.

Рассматривая проблему повышения эффективности обучения, можно с полной уверенностью заключить, что его перевод на новые информационные рельсы даст толчок для качественно иного, лучшего развития всех стадий образовательного процесса. Использование на этой почве технологии модульного обучения позволит совместить преимущества одной и другой технологий. Тем самым

построение модульного обучения на основе новых информационных технологий, по мнению автора, представляется наиболее перспективным и целесообразным в силу указанных преимуществ данных технологий.

Из всех рассмотренных форм организации контроля наиболее простой является форма тестирования. При проведении контроля она не требует творческого участия преподавателя в процессе, его функции сводятся к простому подсчету правильно указанных ответов. Эту функцию можно поручить даже обычному специальным образом не подготовленному человеку. Единственное, что от него будет требоваться – это умение считать. Компьютер – это тот инструмент, на который можно и представляется целесообразным возложить данную функцию.

В силу указанных причин, возникла необходимость создания специализированного средства позволяющего автоматизировать входной и выходной контроль в дистанционно-модульном обучении. Так авторский коллектив кафедры СИТиИБ приступил к разработке программного средства «Компьютерная система тестирования».

Система может быть использована как в высших учебных заведениях системы МВД, так и в других случаях обучения и переобучения, когда требуется однозначная дифференцированная оценка знаний тестируемого для последующего принятия решения о направлении его текущей подготовки или об изменении дальнейших планов обучения.

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

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

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

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

Примакина Е.И.
Россия, Кострома, Костромская государственная сельскохозяйственная академия

РАЗРАБОТКА ТЕХНОЛОГИИ ОЦЕНКИ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одним из важных факторов при подготовке специалистов в области информационной безопасности является оценка роли их в качестве операторов при взаимодействии с техническими системами. В настоящее время решение этой проблемы осуществляется предъявлением выходных откликов технической системы без учета эволюционных возможностей человека, как основного элемента в системе приема и обработки информации. Эти исследования, как правило, носят узко специализированный характер, результаты их трудно использовать при изменении постановки задачи.

В данной работе приводится решение проблемы оценки эффективности операторской деятельности осуществить путем предъявления воздействий не одного класса, а целого набора классов различной физической природы. Решение задачи осуществляется изучением откликов операторов на воздействия этих классов и рассмотрение только тех классов, которые вызвали наибольшую ответную реакцию. Для решения этой проблемы введены определения операторской деятельности, ее моделей, а так же критерии оценки функции операторской деятельности. Результаты работы подтверждаются экспериментальными исследованиями.

Технология оценки эффективности деятельности специалистов включала в себя:

– рассмотрение операторской деятельности как системы (канала) передачи и обработки информации;

– описание предложенных характеристик помех и сигналов при тестировании операторов;

– применение критериев оценки операторской деятельности:

а) приложение меры Кульбака для непрерывного канала, как базового критерия оценки эффективности операторской деятельности;

б) приложение меры Кульбака для дискретного канала, как базового критерия оценки эффективности операторской деятельности;

в) использование информационной меры Шеннона при оценке пропускной способности непрерывного и дискретного каналов для случая операторской деятельности.

Экспериментальные исследования оценки эффективности системы операторской деятельности проводились:

– по оценке моторных функций операторов для различных классов сигналов;

– по оценке эффективности слуховой функции оператора;

– по оценке интеллектуальных способностей оператора.

Таким образом, на основе последних достижений теории обработки сигналов, новых информационных технологий, поставлена и решена научно-техническая задача по разработке технических решений в области количественной оценки моторных реакций операторов и их интеллектуальных способностей в системе технических средств обучения и тестирования.

Сиденко А.Г.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ИННОВАЦИОННО-ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОВД СУБЪЕКТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Сущность термина «информационная безопасность» в современном информационном сообществе раскрывается с двух позиций:

1. Это состояние (качество) некоторого объекта, в качестве которого могут выступать данные, информация, организация, государство и т.д.

2. Целенаправленная деятельность заинтересованных субъектов по обеспечению защиты объекта.

В современной науке нет универсального определения «информационная безопасность», разные ученые трактуют ее по-своему в соответствии с предметом изучаемого вопроса, при этом сущность остается неизменной. В Доктрине информационной безопасности Российской Федерации под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Информационная безопасность органов внутренних дел представляет собой состояние защищенности информационной среды, обеспечиваемое за счет целенаправленной деятельности ее органов и должностных лиц с использованием разрешенных сил и средств по достижению состояния защищённости информационной среды ОВД, обеспечивающее её нормальное функционирование и динамичное развитие. Информационная безопасность всего МВД будет аккумулировать информационную безопасность каждого субъекта и его информационных связей с другими субъектами.

В данном тезисе рассмотрим некоторые инновационные и экономические аспекты информационной безопасности. Во-первых, следует отметить, что инновации должны быть направлены на повышение эффективности деятельности МВД России. В данном конкретном случае повышение эффективности деятельности МВД России будет заключаться в стремлении достичь 100% информационной безопасности. Во-вторых, следует отметить, что необходимость внедрения инновационных решений в деятельность ОВД диктуется объективной реальностью, с каждым днем преступления совершаются с использованием все более новых и современных технологий, что требует соответствующей реакции.

Таким образом, МВД не может принимать риск на не достаточное обеспечение информационной безопасности.

При этом, очевидно, что если затраты на внедрение инноваций будут слишком высоки, т.е. несоразмерно выше чем возможный эффект от повышения эффективности, то встает вопрос о целесообразности таких инноваций, а с учетом дефицита федерального бюджета, даже о невозможности таких инноваций. Таким образом, в Министерстве необходимо решить задачу о соотношении объемов финансирования на внедрение инноваций и повышения эффективности деятельности МВД России. При этом ограничением по сути будет выступать социальный эффект от деятельности МВД России.

Смирнов А.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ПРОЦЕССЕ РЕФОРМИРОВАНИЯ МОНОПОЛИЙ В ГАЗОВОЙ ОТРАСЛИ РОССИИ

В России нет необходимости специально форсировать разделение добывающего сегмента самого газового монополиста. Активными игроками на рынке газа могут стать нефтяные компании и другие независимые газодобытчики. При этом для нормального развития конкуренции важно обеспечить для всех субъектов рынка равный доступ к трубопроводам и хранилищам. Одновременно решать и проблему перекрестного субсидирования, которая для газовой отрасли является еще более острой.

Специфика газовой отрасли России обуславливает особенности ее реформирования по сравнению с другими естественными монополиями. Для реформирования газовой отрасли первостепенное значение приобретает не столько создание конкурентной среды, сколько достижение необходимой финансово-экономической прозрачности в деятельности газового монополиста. Одной из главных проблем реформирования «громадных» монополистов (ОАО «Газпром») может стать сохранение и совершенствование информационной безопасности компании.

Поскольку тенденции повсеместной информатизации наиболее характерны для крупных компаний, всерьез рассматриваются проблемы, непосредственно связанные с возможным проявлением технологического терроризма. В этих условиях задача обеспечения защиты информационных ресурсов таких предприятий приобретает одно из первостепенных значений. Опасность технологического терроризма вполне реальна, так как степень зависимости экономики и органов власти от информационных технологий возросла настолько, что нарушение установленных режимов работы информационных систем может иметь катастрофические последствия. Это подтверждается производственной практикой газовой отрасли, которая свидетельствует о том, что между информационной безопасностью предприятия и безопасностью населения страны существует прямая связь. К примеру, неполадки в работе Единой системы газоснабжения могут создать угрозу для жизни и здоровья людей.

Одна из основных проблем – отсутствие регламентации по безопасности информации автоматической системе управления в критичных производствах. Однако автоматическая система управления крупных предприятий не относится к категории, подлежащей защите. В настоящее время единственный существующий в России документ Гостехкомиссии, который регулирует вопросы защиты автоматизированных систем управления от несанкционированного доступа, не охватывает всех аспектов проблемы.

В этом направлении органами государственной власти России предпринимаются определенные шаги по созданию в стране механизма противодействия технологическому терроризму:

– уточнено понятие акта технологического терроризма как выведение из строя и разрушение систем жизнеобеспечения городов и иных населенных пунктов;

– определены потенциально опасные объекты инфраструктуры РФ, к числу которых отнесены объекты производства, переработки, хранения, транспортировки пожаро- и взрывоопасных веществ;

– определен государственный орган (ФСТЭК России), ответственный за организацию работ по обеспечению безопасности информации в системах информационной и телекоммуникационной инфраструктуры страны, оказывающих существенное влияние на ее безопасность;

– издан документ, определяющий признаки критически важных объектов информационной инфраструктуры РФ;

– организована подготовка нормативных документов, определяющих требования по безопасности к информационным системам критически важных объектов информационной инфраструктуры.

И, тем не менее, нормативно-методическое обеспечение деятельности по противодействию технологическому терроризму пока еще не соответствует требуемому уровню. Необходимо согласовать понятия технологического терроризма и информационной безопасности, определить особенности подходов к реализации мероприятий по противодействию терроризму на данных направлениях.

А поскольку в ходе реформирования российские монополии сохраняют форму крупных вертикально интегрированных компаний, и отсутствует ясность выделения из них устойчивого и жизнеспособного естественно монопольного ядра, то проблема совершенствования информационной безопасности таких предприятий является наиболее значимой в условии Российского рынка.

Смирнова О.Г.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОВД

Под информационной безопасностью органов внутренних дел следует понимать состояние защищенности интересов ОВД в информационной сфере в соответствии с возложенными на них задачами.

К элементам информационной сферы органов внутренних можно отнести следующие:

– ведомственную информацию и информационные ресурсы;

– ведомственную информационную инфраструктуру – средства и системы информатизации;

– субъектов осуществления информационной деятельности – сотрудников органов внутренних дел;

– и, наконец, систему нормативно-правового регулирования этой деятельности.

Очевидно, если речь идет об информационной безопасности, именно эти элементы, включая собственно информационную деятельность, должны стать объектами защиты.

В настоящее время актуальность проблемы обеспечения информационной безопасности ОВД определяется рядом взаимосвязанных факторов, многие из которых являются следствием процесса бурной информатизации современного общества.

Среди этих факторов, с одной стороны – формирование правовых основ информатизации, расширение применения современных информационных технологий в деятельности отрасли, с другой – высокая уязвимость инфраструктуры в силу сложности используемых систем, стремительный прогресс в развитии технических средств разведывательного назначения и, так называемого, информационного «оружия».

Особенности современной социально-экономической ситуации, отсутствие реальных ограничений в обороте таких средств, приводят к многочисленным фактам их применения криминальными структурами в отношении органов государственной власти и управления, в том числе правоохранительных органов.

Массив законодательных актов, регулирующих правовые основы деятельности органов внутренних дел в этой части достаточно велик, противоречив, а потому относительно сложен для использования на практике.

Объем подзаконного уровня регламентации оперативной работы также достаточно велик. В нем, в зависимости от различных критериев, можно выделить отдельные массивы нормативных правовых актов, которые систематизируются на ведомственном и межведомственном уровнях.

Основными факторами, препятствующими эффективному добыванию, обработке и использованию оперативно-розыскной информации, по мнению практических работников, являются следующие.

1. Активное противодействие правоохранительным органам со стороны уголовно-преступного мира, которое оказывается в самых различных формах, включая противодействие технической разведке ОВД с помощью специальных средств защиты информации.

2. Широкое использование криминальными структурами средств и тактики оперативно-розыскной деятельности.

3. Низкий уровень профессиональной подготовки оперативных сотрудников органов внутренних дел.

4. Недостаточное ресурсное обеспечение оперативно-розыскной деятельности.

5. Наконец, еще одним фактором, препятствующим эффективному добыванию, обработке и использованию оперативно-розыскной информации, является несовершенство законодательства.

При исполнении своих профессиональных обязанностей, сотрудники ОВД нередко затрагивают частную жизнь отдельных граждан, решая возложенные на них задачи, что полностью нарушает конституционный принцип о неприкосновенности частной жизни, личной и семейной тайны. Поэтому важно, чтобы данный процесс всегда протекал в правовом русле, строго соответствуя целям и задачам заданных мероприятий.

В тех случаях, когда субъекты ОВД после получения конфиденциальной информации обретают статус ее пользователей, данная информация превращается в служебную тайну и их основная задача заключается в обеспечении защиты этих сведений от дальнейшего неправомерного доступа к ним.

В том случае, если подобные деяния причинили вред правам и законным интересам гражданина, то они образуют состав преступления и преследуются уже в уголовном порядке по ст. 140 УК РФ.

Разглашение или утрата сведений, составляющих служебную тайну, не угрожают напрямую безопасности государства, однако при определенных условиях эти действия могут причинить существенный вред его охраняемым интересам. Поэтому соблюдение правового режима служебной тайны в ходе осуществления оперативно-розыскных мероприятий в полной мере отвечает интересам обеспечения информационной безопасности не только отдельных граждан и общества, но и государства в целом.

Смирнова Ю.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

РОЛЬ ГОСУДАРСТВА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЖИЛИЩНОЙ СФЕРЕ

Безопасность является важнейшей потребностью человека наряду с его потребностью в пище, воде, одежде, жилище, информации. Эта общенаучная категория выступает интегральной формой выражения жизнеспособности и жизнестойкости различных объектов конкретного мира во внутренней и внешней политике, обороне, экономике, экологии, социальной политике, здоровье народа, информатике, технологии и т. п.

Под информационной безопасностью в жилищной сфере понимается состояние защищенности, которое обеспечивается созданием условий для эффективного развития информационной инфраструктуры в указанной области.

Роль государства в обеспечении информационной безопасности заключается в реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Все эти интересы государства характерны и в ходе реализации гражданами конституционного права на жилище.

Целенаправленное применение информационных технологий в сфере жилищно-коммунальной инфраструктуры и строительства позволяет обеспечить органам государственной власти: повышение эффективности распределения бюджетных средств на строительство, реформирование и модернизацию коммунальных систем, повышение эффективности координации деятельности организаций технического учета и инвентаризации, мониторинг технического состояния коммунальных систем жизнеобеспечения, контроль за ходом реализации региональных и муниципальных программ реформирования и модернизации, повышение экономической обоснованности тарифов на жилищно-коммунальные услуги и эффективности системы тарифного регулирования.

При использовании информационных технологий в органах государственной власти, применяемых при хранении, обработке и передаче по каналам связи информации ограниченного доступа, формировании открытых официальных информационных ресурсов, а также в критически важных сегментах информационной инфраструктуры Российской Федерации, необходимо обеспечить безопасность информационных ресурсов, их целостность, доступность и конфиденциальность, а также возможность установления авторства электронных документов.

Основные направления повышения уровня защищенности объектов информационно-технической инфраструктуры федеральных органов государственной власти включают:

1. Обеспечение комплексного подхода к решению задач информационной безопасности с учетом необходимости дифференцирования ее уровня в различных органах государственной власти.
2. Разработку модели угроз информационной безопасности, политики безопасности и заданий по безопасности.
3. Определение технических требований и критериев отнесения объектов к критической информационно-технологической инфраструктуре, создание реестра критически важных объектов, разработка особых мер по их защите и средств надзора за их соблюдением.
4. Обеспечение эффективного мониторинга состояния информационной безопасности.
5. Развитие нормативной правовой и методической базы в области защиты информации, оценки безопасности информационных технологий.
6. Единый порядок согласования технических заданий на обеспечение информационной безопасности государственных информационных систем, ресурсов и технологий.
7. Проведение аттестации и организацию контроля государственных информационных систем, ресурсов и технологий, используемых в деятельности федеральных органов государственной власти, на соответствие требованиям информационной безопасности уполномоченными федеральными органами власти.
8. Развитие систем обеспечения безопасности электронного документооборота, системы мониторинга и контроля действий государственных служащих по работе с информацией, развитие и совершенствование средств защиты информации, защищенных средств обработки информации общего применения, систем удостоверяющих центров, а также систем их сертификации и аудита.

В целях обеспечения информационной безопасности государственных информационных систем, ресурсов и технологий необходимо применение единых требований защиты информации от несанкционированного доступа или изменения, при осуществлении доступа в открытые сети связи, в том числе в интернет или по другим каналам, а также от воздействия компьютерных атак и вирусов.

Трифонова Ю.В., Башун В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ

Безопасность персональных данных – это развивающийся раздел информационной безопасности, который последнее время привлекает к себе все больше внимания.

Обработка персональных данных является неотъемлемой частью работы любого образовательного учреждения. Однако законодательство в области защиты прав субъектов персональных данных в Российской Федерации появилось достаточно недавно, в связи с чем, нет четкого представления о его практическом применении. В работе рассмотрены особенности законодательства Российской Федерации в области защиты прав субъектов персональных данных с точки зрения приведения обработки персональных данных в высшем учебном заведении в соответствие с ним. В ходе работы была выделена структура и наиболее важные аспекты законодательства Российской Федерации в области защиты прав субъектов персональных с точки зрения обработки персональных данных в высшем учебном заведении.

Принятие Федерального закона от 25.07.2011 №261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»» уточнило некоторые моменты обработки персональных данных, например, необходимость согласия субъекта персональных данных на обработку их персональных данных. Для высших учебных заведений этот момент интересен с точки зрения последствий отказа субъекта персональных данных от обработки его персональных данных в высшем учебном заведении.

Обработка персональных данных, в частности в высших учебных заведениях, происходит в двух видах систем: автоматизированных и неавтоматизированных. В данной работе рассмотрены варианты распределения персональных данных между двумя видами систем обработки персональных данных и последствия таких распределений с точки зрения соответствия законодательству Российской Федерации.

В работе предлагается план действий, который поможет привести обработку персональных данных в соответствие с законодательством Российской Федерации. Этот план включает в себя как организационные, так и технические меры. Несмотря на то, что этот вопрос рассматривался с точки зрения высших учебных заведений, он может быть полезен любой организации, которая столкнулась с вопросом приведения обработки персональных данных в соответствие с законодательством Российской Федерации.

Кроме теоретических сведений, особое внимание уделяется часто встречающимся нарушениям при обработке персональных данных в высших учебных заведениях, что позволит избежать их при реализации требований законодательства Российской Федерации в конкретных организациях.

Уварова Ю.А., Копыльцов А.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

КВАЛИФИКАЦИЯ КИБЕРПРЕСТУПЛЕНИЙ ПРОТИВ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

На сегодняшний день, информационная структура (программы и информация) не может быть предметом преступления против собственности, поскольку машинная информация не отвечает ни одному из основных критериев предмета преступления против собственности, в частности не обладает физическим признаком. Что касается компьютера, как орудия преступления, то его следует рассматривать в ряду таких средств, как оружие или транспортные средства. В этом смысле использование компьютера имеет прикладное значение при совершении преступлений, например, применение компьютерных технологий при хищении денежных средств или сокрытии налогов. Такие действия не рассматриваются в качестве самостоятельных преступлений, а подлежат квалификации по другим статьям УК РФ в соответствии с объектом посягательства.

Незаконное изъятие носителей информации, содержащих персональные данные, в широком смысле может пониматься как хищение компонентов техники и квалифицироваться как обыкновенная кража (ст.158 УК РФ). Вместе с тем, некоторые ученые, в частности Ю.И.Ляпунов, считают, что предметом рассматриваемых преступлений является компьютерная информация (в том числе персональные данные), содержащиеся на машинных носителях в системе ЭВМ или их сети. Поэтому действия лица, прибегнувшего к хищению компьютера, подлежат квалификации по правилам совокупности преступлений – преступления против собственности и преступления в сфере компьютерной информации – лишь в том случае, если имеет место цель получения неправомерного доступа к охраняемой законом информации. В случае неправомерного доступа к охраняемым законом персональным данным объектом преступного посягательства являются информационные отношения.

Широкая сфера применения компьютерных технологий затрагивает чаще уже известные виды преступлений, но только совершенные в новой форме или новым способом. Неправомерные

действия с применением компьютерных технологий могут быть квалифицированы по традиционным составам, но исключительные особенности таких деяний не позволяют в полной мере этого сделать.

Характеристики преступления в указанной сфере должны формироваться в зависимости от событийного описания модели состояния информационной системы персональных данных с уточнением используемых для их совершения средств. Состояния должны определяться негативными последствиями для информационной системы персональных данных определенного класса – компрометации, распространения, разрушения определенного объема персональных данных (например, сведения о более 100 тысячах субъектах персональных данных) конкретной категории (например, медицинские сведения) и т.п.

Событиями могут являться – чтение, уничтожение, блокирование, модификация, копирование, использование (например, для неправомерного доступа к счетам) персональных данных, нарушение работы ЭВМ, системы ЭВМ или их сети (например, временные задержки). Средства могут быть как программные (software), так и аппаратные (hardware). В упрощенном представлении модель может иметь 3 измерения: события, средства, состояния. Полученная модель может сопрягаться с оценкой опосредованного ущерба при неправомерном использовании персональных данных. Стратификация состояний позволит более объективно определить тяжесть возлагаемой на злоумышленника ответственности за содеянное. Рассмотрим конкретный пример.

С целью получения персональных данных пользователей (данные авторизации) игры World of Warcraft злоумышленники проводят атаку «man-in-the-middle». Злоупотребляя доверием пользователя к компьютерной игре, киберпреступники обманным путем провоцируют загрузить и запустить на своем компьютере вредоносную программу для ЭВМ замаскированную под игровую. Получив данные авторизации жертвы, они выдают себя перед игровым сервером Blizzard за этого пользователя («кража личности») и, получив неправомерный доступ к компьютерной информации, распоряжаются виртуальным имуществом игрока.

В связи с вышеуказанным предлагается в главе 21 УК РФ конкретизировать статью 159 «Мошенничество» с целью введения в действие уголовно-правового поля такого вида мошенничества, как «кража личности». Расширить перечень санкций, позволяющий отразить масштабность ущерба и отягчающие обстоятельства. А именно добавить пункт 5 в статью 159 УК РФ: «Мошенничество, совершенное путем выдачи себя за другое лицо, наказывается штрафом в размере от ста тысяч до пятисот тысяч рублей или лишением свободы на срок от двух до двадцати лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от пяти лет либо без такого и с ограничением свободы на срок от двух лет».

Чернышева Ю.Н.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

К ВОПРОСУ О ВЛИЯНИИ РЕЙДЕРСТВА НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ГОСУДАРСТВА

Институт слияний и поглощений в России в настоящее время включает в себя естественную легитимную составляющую, которая регулируется Гражданским кодексом Российской Федерации, и недружественные поглощения и слияния, противозаконные по своей природе, наносящие ущерб экономике страны и подрывающие основы ее экономической безопасности.

О криминальном характере рейдерства в России свидетельствует механизм захвата предприятий, первоначальным этапом которого является разведка. Эта типичная процедура предполагает получение максимальной информации об объекте захвата и включает:

– легальную;
– криминальную разведку.

Легальная разведка основывается на изучении доступных (открытых) источников информации, например раскрываемых ОАО годовых отчетов общества, бухгалтерских отчетов, проспектов эмиссий и других сведений. Криминальная разведка ориентирована, во-первых, на сбор закрытой информации, во-вторых, на получение сведений компрометирующего характера. Кроме того, криминальная разведка зачастую осуществляется незаконными средствами: скрытое наблюдение, прослушивание телефонных переговоров.

Информацию, используемую для рейдерского захвата, принято делить на три типа:

1. О персонале предприятия-цели: анализируются интересы, слабости, характер топ-менеджеров и рядовых исполнителей, их взаимоотношения. Определяются неформальные лидеры в коллективе, находящиеся в оппозиции к формальным руководителям, т.е. выявляются потенциальные очаги конфликтов.

2. О деятельности предприятия-цели: история приватизации предприятия-цели, ее план приватизации и договор купли-продажи приватизированного имущества, учредительные документы, внутренние положения и регламенты, договоры с поставщиками и потребителями, а также договоры по неосновной деятельности, кадровые приказы и распоряжения, бухгалтерская документация.

3. Об акционерах, реестре и реестродержателе: конфликты между акционерами часто используются для начала захвата, в свою очередь структура капитала – основа для разработки

стратегии захвата. Сведения о реестре и реестродержателе используются захватчиком для реализации наиболее распространенных методов захвата: скупки акций, организации двойного реестра и формирования двойных органов управления.

Отметим, что при определенных условиях лица, осуществляющие сбор информации, могут быть привлечены к уголовной ответственности, если сбор информации осуществляется в отношении компании-цели и ее акционеров:

– юридических лиц – по ст. 183 УК РФ (незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну);

– физических лиц – по ст. 137 УК РФ (неприкосновенность частной жизни, т.е. нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений).

Сказанное выше дает основание для вывода о том, что информация является одним из главных ресурсов рейдерской атаки, а приоритетными мерами по обеспечению информационной безопасности государства являются:

1. Разработка комплекса превентивных мер индивидуально для каждого предприятия (с учетом его специфики), касающихся совершенствования контроля за информацией и документооборотом предприятия;

2. Выстраивание четкой схемы управления предприятием, регулярный мониторинг текущего состояния документов, формирование позитивного имиджа организации, работа со СМИ, укрепление связей с местными регистрирующими органами, внедрение технических средств сбора, обработки, накопления и хранения конфиденциальной информации, работа с сотрудниками при подборе и расстановке персонала;

3. Разработка и принятие законодательных нормативно-правовых актов по борьбе с рейдерством, в том числе позволяющих пресекать получение информации о предприятии из различных органов власти: ИФНС, Арбитражных судов, правоохранительных органов.

Шакиров М.З.
Россия, Обнинск, Центральный институт повышения квалификации

ВОПРОСЫ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ НА СОВРЕМЕННОМ ЭТАПЕ

Правовые основания защиты государственной тайны регулируются законом РФ «О государственной тайне», а также рядом подзаконных актов Президента РФ.

Правоприменительная практика положений закона и подзаконных актов выявила ряд серьезных недостатков в этой сфере. Рассмотрим некоторые из них.

Первым вопросом, который вызывает трудности в реализации положений закона о государственной тайне, является система засекречивания сведений, отнесенных к государственной тайне.

К недостаткам перечневой системы засекречивания сведений относятся:

– иерархическая сложность и громоздкость системы;

– как следствие первого, ограниченные возможности по оперативному управлению системой и обновлению перечней;

– закрытость системы, что приводит к затруднениям во взаимодействии различных ведомств и органов государственной власти, а также при возникновении судебных споров между государством и личностями по вопросам разглашения государственной тайны;

– возложение на государство в виде руководителей органов государственной власти, наделенных полномочиями по отнесению сведений к государственной тайне, всей полноты ответственности за эти действия.

Указанные недостатки приводят к конкретным коллизиям в правоприменительной практике положений закона о «Государственной тайне». В частности, при разработке развернутых ведомственных перечней сведений, отнесенных к государственной тайне, встречаются случаи как излишне включения в него излишних сведений, подлежащих засекречиванию, так и случаи, когда в перечне отсутствовали ссылки на сведения, действительно требующих отнесения к государственной тайне.

Вторым серьезным недостатком действующей системы правового регулирования в области защиты государственной тайны является декларативность объявленного в законе принципа однозначной связи степени секретности информации, составляющей государственную тайну, со степенью ущерба, который может быть нанесен государству, ведомству или организации вследствие ее разглашения. Декларативность этого принципа связано с положениями статьи 8 федерального закона, в которой определено, что «порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну и правила отнесения указанных сведений к той или иной степени секретности, устанавливаются Правительством Российской Федерации. До настоящего времени такая методика отсутствует.

Третий существенный недостаток в области правового обеспечения защиты государственной тайны заключается в том, что решение вопросов защиты государственной тайны в РФ находится в компетенции в основном исполнительной власти (ст. 30). В качестве недостатка можно также отметить несогласованность терминологии и понимания сущности таких понятий, как «перечень сведений, составляющих государственную тайну», «перечень сведений, отнесенных к государственной тайне», «перечень сведений, подлежащих засекречиванию» с требованиями ст. 275, 283 УК РФ.

В каких направлениях должно развиваться законодательство о государственной тайне?

Необходимо искать решение в дилемме между необходимостью сохранять в тайне отдельные перечни (разделы) сведений, составляющих государственную тайну, и максимально широким доступом к перечням лиц, которые могут быть по роду своей деятельности могут столкнуться с такого рода информацией.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

АНАЛИЗ И СИНТЕЗ КАЧЕСТВА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ В СЛОЖНЫХ ЭРГОТЕХНИЧЕСКИХ СИСТЕМАХ

Особую роль в развитии современных сложных эрготехнических систем (ЭТС) приобретают системы управления качеством и, прежде всего, на основе мониторинга их эффективности по сводным показателям качества (СПК). Именно квалиметрические оценки ЭТС позволяют конструктивно решать задачи минимизации угроз, рисков, защиты ресурсов предприятий, успешного конкурирования.

Вместе с тем, анализ и синтез качества сложных ЭТС сдерживается проблемой моделирования качества сложных объектов, многообразием методологических подходов при практическом отсутствии данных их сравнительной верификации. Именно в этих условиях как никогда актуальным и результативным становится полимодельный подход и технологии квалиметрического сравнения (на основе одновременного многоаспектного использования оценок по нескольким моделям).

Опыт проведения многовариантных исследований качества широкого спектра ЭТС и, в первую очередь, систем управления и обеспечения их информационной безопасности (ИБ), позволяет отметить особую важность и конструктивность:

1. Использования системных аспектов, методологии и технологии проведения анализа качества структурно и функционально сложных ЭТС, в том числе на основе использования оценок СПК типа «качество ИБ (информационная защищённость)» по мультипликативной модели вида «конфиденциальность – доступность – целостность».
2. Анализа динамики эмерджентных свойств ЭТС при синтезе их качества (исследовательском проектировании оптимальных вариантов), характеризующих качество взаимосвязей элементов в составе ЭТС, что наиболее «рельефно» проявляется при анализе СПК ЭТС.
3. Синтеза эффективных алгоритмов управления, включая алгоритмы управления ИБ, при обосновании качества ПУР на основе мониторинга данных квалиметрического анализа.
4. Использования при мониторинге СПК ЭТС хорошо апробированных концепций, алгоритмов и технологий полимодельного анализа-синтеза ПУР типа «ASPID», «APIS», «КРОПУР», «АСОР».
5. Обоснования и оптимизации (выбора наилучшего варианта из возможных альтернативных) ПУР, подлежащих внедрению при создании современных структурно и функционально сложных ЭТС, что обеспечивает их эффективное и безопасное, в том числе катастрофоустойчивое использование.
6. Моделирования и анализа качества ИБ и ЭТС в целом при различных вариантах их построения и использования с соответствующим ранжированием. Например, только число межсетевых экранов (МСЭ) на рынке средств защиты информации (СЗИ) сегодня согласно Госреестра сертифицированных СЗИ составляет более 180. Выбор наиболее предпочтительных МСЭ (оптимального варианта) представляет собой весьма сложную проблему в связи с отсутствием в доступной литературе необходимых сведений для их сравнения и ранжирования.
7. Анализа факторов и проблем, а также обоснования программ внедрения новых технологий и ПУР с учётом «операторского компонента» ЭТС, то есть «пресловутых» человеческих факторов, имеющих сегодня, как известно, ключевой характер. При этом традиционно особое внимание должно уделяться систематизации критериев и показателей эффективности использования каждого типа ЭТС. Полимодельность задания исходных данных по отношениям предпочтений подтвердила возможность получения при рейтинг-анализе альтернативных решений более полной картины для лиц, обосновывающих (ЛОР) и принимающих ПУР (ЛПР). Соответствующее формирование матрицы индексов интегральных критериев качества и СПК для соответствующих классов ЭТС позволяет по существу создать равные условия и сопоставимость всего ряда сравниваемых ПУР. С другой стороны, согласование получаемых результатов с разработчиками ЭТС обеспечивает минимизацию информационного дефицита при квалиметрическом рейтинг-анализе по СПК и повышает точность задания исходных данных, а также получаемых оценок качества.

В свою очередь, формирование баз данных и знаний ЭТС по СПК обеспечит качественно новый уровень организации и проведения сертификации средств, аттестации объектов информатизации, профессиональной подготовки и лицензирования юридических и физических лиц.

Пожалуй, наибольшую полезность для разработчиков-проектировщиков и управленцев различных уровней изложенный подход к квалиметрическому сравнению вариантов проектного выбора имеет при использовании и актуализации (по результатам испытаний) подобных баз данных и знаний и их публикации испытательными лабораториями и органами сертификации в целом для различных ведомств и корпораций.

Приведенные полимодельные оценки СПК обеспечения ИБ и в целом, эффективности ЭТС количественно подтвердили то важное обстоятельство, что системные аспекты внедрения ПУР при развитии сложных ЭТС являются наиважнейшими и требующими непременного системно обоснованного учёта при развитии сложных комплексов и их систем ИБ, а также в целом ЭТС.

Андреева Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ОНТОЛОГИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Практическое внедрение стандартов в области информационной безопасности в настоящее время связано с некоторыми трудностями, возникающими, в частности, из-за несогласованности требований к организации одной и той же деятельности, содержащихся в стандартах различных семейств, что обусловлено различиями в их методологиях (цели, точки зрения, области определения и других параметрах). Как следствие возникает недопонимание требований, содержащихся в стандартах, конечными пользователями. Для решения подобных проблем можно использовать методику интегрального инжиниринга стандартов информационной безопасности, основанную на построении системы согласованных полуформальных моделей для методологии каждого из семейств стандартов. Данная система включает в себя три уровня или три согласованные модели: функциональную (структурную), объектную и онтологическую.

В докладе представлены структура, принципы построения и возможные сферы применения онтологической модели системы управления информационной безопасностью (СУИБ), требования и рекомендации по созданию, развитию и поддержанию которой представлены в семействе стандартов ISO/IEC 27000.

Одним из основных преимуществ онтологических моделей по сравнению с моделями, использующими стандартные языки полуформального моделирования (UML, SysML и др.) является возможность использования машины логического вывода – например, для автоматизации некоторых операций с моделями за счёт формального логического представления семантики моделируемых концептов и связей между ними в машиночитаемом формате. Таким образом, возможными сферами применениями онтологической модели СУИБ могут быть:

– автоматизированная проверка внутренней согласованности и непротиворечивости представления практик организации ИБ в стандартах семейства ISO 27000;

– согласование концептов методологий информационной безопасности, представленных в различных семействах стандартов информационной безопасности (ОК, ЦБ РФ, РД ФСТЭК, законодательство РФ);

– использование в качестве источника корректировок и инструмента согласования моделей других уровней;

– разработка гибридных ведомственных и корпоративных стандартов и систем защиты информации, учитывающих требования стандартов различных семейств.

Структура онтологической модели СУИБ обусловлена структурой соответствующей объектной модели СУИБ, на базе которой предполагается её построение. Онтологическая модель должна состоять из двух взаимосвязанных частей: а) концептуальная онтологическая модель СУИБ, содержащая абстрактные концепты, использующиеся в предметной области, и связи между ними; б) онтологическая модель требований к СУИБ, содержащая все типы концептов (процессы, ресурсы и внешние сущности) из методологии стандарта ISO/IEC 27001 и связи между ними.

В качестве базовой методологии создания модели была выбрана методология Европейского проекта NeOn, которую необходимо модифицировать и дополнить с учётом следующих специфичных для разработки онтологической модели СУИБ факторов:

1) в модели должны быть представлены только концепты, содержащиеся в методологии стандартов семейства ISO/IEC 27000;

2) поскольку онтологическую модель СУИБ предполагается разрабатывать на основе существующей объектной UML-модели СУИБ, необходим метод трансформации UML-модели в онтологическую, одним из компонентов которого является определение семантического базиса для двух языков моделирования (минимального набора элементов языка моделирования, позволяющего представить большую часть концептов предметной области);

3) необходимо учесть, что объектная модель содержит несколько взаимосвязанных пакетов, внутри каждого из которых может находиться ноль, одна или несколько диаграмм. Соответственно, необходимо сохранить имеющиеся связи при трансформации;

4) онтологическая модель СУИБ должна содержать, в том числе, концепты, необходимые для представления процессов СУИБ, однако существующие языки и методы онтологического анализа не предоставляют достаточных средств описания динамических аспектов организации деятельности в предметной области. На данный момент рассматриваются следующие варианты представления процессов (каждый из которых имеет свои преимущества и недостатки):

– представление процесса в виде отношения между двумя концептами – субъектом и объектом действия.

– представление процесса в виде концепта с префиксом «process».

Атисков А.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ТРАНСФОРМАЦИИ ДИАГРАММ ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ АНАЛИЗА И ГАРМОНИЗАЦИИ СТАНДАРТОВ БЕЗОПАСНОСТИ

Безопасность является одним из важнейших факторов в современном мире информационных систем. Но оценка степени безопасности является комплексной и складывается из множества компонентов. Данные компоненты в свою очередь считаются исходя из довольно обширного перечня стандартов безопасности. Причем они могут быть пересекающимися, могут в одной стране считаться обязательными, а в другой иметь вспомогательный характер.

Для их комплексного применения требуются методики сопоставления одних стандартов другим. Как с точки зрения синтаксиса, так и семантически. Для такой «гармонизации» было бы полезно использовать разработанную технологию связывания нотаций проектирования IDEF0 с нотацией диаграмм классов UML, заключающуюся в следующем:

1. Построении моделей нотаций проектирования в виде OWL-описания и записи диаграмм проектирования в виде RDF-файлов;

2. Проведении трансформации функциональной модели в объектно-ориентированную модель с применением правил трансформации на основе SPARQL-запросов.

В процессе разработки OWL-описания, объединяющего функциональный подход (диаграммы IDEF0) и объектно-ориентированный (диаграммы классов UML), были использованы следующие понятия: классы owl:Class и свойства owl:Property, включая owl:ObjectProperty и owl:DatatypeProperty.

Посредством использования предопределенного в OWL отношения owl:subClassOf были описаны элементы IDEF0 диаграмм, связанные с родительским классом tf:Functional, а именно: tf:Arrow — класс, обозначающий «стрелку» в диаграммах IDEF0; tf:Block — класс, обозначающий «блок» в диаграммах IDEF0; tf:ArrowEnd – связь между конкретной «стрелкой» и «блоком».

К элементам диаграмм UML (связанным с главным классом tf:ObjectOriented) относятся: tf:Type — класс, представляющий условное понятие «тип»; tf:Attribute — обозначает атрибут класса tf:Class; tf:Method — обозначает метод класса tf:Class; tf:Parameter — обозначает параметр метода tf:Method. Для формального (в виде множества логических троек) описания правил трансформации диаграмм IDEF0 в диаграммы UML были введены дополнительные понятия и отношения в язык RDF. Для непротиворечивого преобразования данных IDEF0 используется список логических троек (субъект–предикат–объект). При этом извлечение данных из IDEF0-диаграммы производится за счет стандартизованного языка запросов SPARQL.

Для стандартов безопасности следует составить их онтологическое описание (с использованием языка OWL), определить общие элементы и связи, как это было сделано для нотаций проектирования. На основе OWL-описаний вывести правила связывания стандартов в виде логических троек, которые можно оформить в виде SPARQL-запросов. Далее можно строить оценку безопасности информационной системы по связанным стандартам безопасности.

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

ОНТОЛОГИЯ ТАКСОНОМИИ И БЕЗОПАСНОСТИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Термин «облачные вычисления» основан на ряде многих старых и немногих новых понятиях таких, как Архитектура, Ориентированная на Сервис (SOA), распределенные вычисления и вычисления в грид-технологии, виртуализация вызывали в последнее время интерес и послужили основой для облачных вычислений. Основное отличие облачных вычислений от распределенных вычислений и грид вычислений в том, что в последних задается жесткая структура нахождения данных и сервисов, в то время как в облачных вычислениях структура не определена и может меняться.

Для облачных вычислений необходим релевантный поиск данных и соответствующих сервисов. Для облачных вычислений целесообразно использовать семантический поиск, т.е. онтологическое описание данных и сервисов, что позволит автоматически строить структуру облака и обеспечит

релевантный поиск данных и сервисов. Кроме того, онтологическое описание данных и сервисов в облачных вычислениях может существенно повысить безопасность вычислений в облаке.

Вектор развития IT-сервисов явно указывает в сторону «облачных вычислений». Это заставляет задуматься о переходе к конкретным предложениям и реализациям SaaS-решений (Software as a Service) в различных сферах деятельности. То есть «облака» имеют тенденцию быстрого расширения, объединения различных корпоративных облаков и т.д. Поэтому возникает проблема быстрого и релевантного поиска данных и сервисов.

Онтологическое описание позволит автоматически строить структуру и таксономию данных и сервисов в вычислительных облаках. Онтология показывает целостную перспективу операций безопасности и обеспечивает категории оперативной информации безопасности.

Облачная модель должна обеспечивать высокую степень готовности и безопасности вычислительных ресурсов в облаке. Необходима релевантная таксономия данных и сервисов в облачных вычислениях и безопасность в части SaaS, на основе онтологического описания таксономии доступа к данным и сервисам (доступность) и онтологического представления безопасности вычислений в облаке, используя базы данных и базы знаний, в которых накапливается и анализируется доступность и риски безопасности вычислений в данном облаке.

Ахремцева В.Л.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Дистанционное банковское обслуживание (далее – ДБО) – это современный способ предоставления банковских услуг системой кредитно-финансовых институтов, обеспечивающий клиенту возможность удаленного управления денежными потоками. В зависимости от типа программно-аппаратных средств реализации банковских операций технологии ДБО можно классифицировать на PC-banking (системы типа «Клиент-Банк»), интернет-банкинг, телефонный банкинг, а также обслуживание с использованием банкоматов и устройств банковского обслуживания (ATM-banking). Количество пользователей услуг ДБО в последнее время активно растет, однако, вместе с этим растет и количество интернет-мошенников, ввиду этого, проблема обеспечения безопасности ДБО представляется весьма актуальной.

Вопрос подготовки решения по обеспечению безопасности ДБО ложится на отдел информационной безопасности банка, причем выбор технологий обуславливается спецификой конкретного кредитно-финансового института. При этом учитываются следующие критерии: организационная структура, объем финансирования, клиентура («портрет клиента»), уровень технической оснащенности, специфика реализации бизнес-процессов, интенсивность использования технологий ДБО и пр.

Основными угрозами безопасности ДБО являются следующие:

– работа в открытой среде Интернет;

– выманивание информации с использованием методов социальной инженерии (фишинг, подставные сайты, специально разработанные вирусы);

– угрозы для серверной части (инсайд, коммерческий подкуп).

Среди основных схем дестабилизации функционирования системы ДБО можно выделить следующие:

– атака на ключ ЭЦП пользователя (в качестве защиты используются защищенные ключевые носители или токены (eToken), выполняющие внутри себя операции с закрытым ключом пользователя);

– атака на криптографические возможности токена (наиболее эффективная мера – комбинация средств защиты, например, дополнение аппаратной поддержки (токенов) подтверждением транзакций одноразовым паролем);

– действия злоумышленника со стороны клиента (инсайд);

– подмена документа в момент его подписания ЭЦП (или расчета HASH) – основным инструментом реализации выступает «банковский троян»; мера защиты – комплексное использование аппаратных средств (токенов) в сочетании с антивирусными средствами.

Схема работы вредоносного программного обеспечения включает в себя последовательность следующих этапов: внедрение, сбор данных, атака и заметание следов.

В качестве мер обеспечения безопасности ДБО особо следует отметить следующие:

– строгая идентификация пользователей;

– проверка целостности транзакций;

– аудит операций (юридическое подтверждение операций).

На сегодняшний день выбор инструментов обеспечения безопасности ДБО определяется группой риска пользователей (физические лица, малые и средние предприятия, крупные

организации). Следует отметить обратную зависимость между степенью уязвимости пользователя и вероятной величиной материального ущерба от атаки.

Ввиду того, что в основе технологии ДБО лежит осуществление банковских операций посредством удаленного доступа, то целесообразно в качестве основного средства обеспечения безопасности ДБО выделить аутентификацию. Выделяют следующие инструменты аутентификации пользователей: одноразовые пароли на основе времени или события, система запрос-ответ, EMV механизмы, инструменты на основе несимметричных алгоритмов (PKI).

Внедрению решения по обеспечению безопасности ДБО предшествует финансово-экономическое обоснование, которое включает анализ возможных потерь, но здесь следует учесть, что помимо прямых убытков, которые несет клиент, банк несет также потери недополученной прибыли и репутационные потери. Наличие данной двусторонней заинтересованности инициировало появление в последнее время тенденции к включению в стоимость обслуживания клиентов затрат на приобретение средств обеспечения безопасности пользователей в системах ДБО.

Полностью исключить вероятность возникновения угроз безопасности ДБО невозможно, так как данная система является открытой, однако следует стремиться к минимизации их воздействия посредством эффективного внедрения экономически целесообразных решений и комплексного использования инструментов.

Беззатеев С.В., Волошина Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНОГО КЛАССА КОДОВ ДЛЯ ИДЕНТИФИКАЦИИ МУЛЬТИМЕДИА ДАННЫХ

В настоящее время активное развитие получили цифровые технологии. Расширяются компьютерные сети, технологии передачи данных, растут объемы мультимедийных (видео, звук, изображения и т.д.) данных, циркулирующих в компьютерных сетях. При передаче мультимедиа данных зачастую встает задача дальнейшей их идентификации. Например, определение авторства, идентификация отправителя или получателя, определение дополнительных свойств мультимедиа данных. Существование большого количества форматов представления таких данных приводит к появлению проблем при их идентификации. Применение простых способов добавления информации, связанных с использованием свойств форматов (форматные методы) сильно ограничено из-за потери данных при переформатировании. По этой причине для идентификации мультимедиа данных часто применяют методы внедрения цифровых водяных знаков (ЦВЗ). Цифровой водяной знак, это набор информации, которая накладывается (добавляется) на данные и может служить для их идентификации.

В целях увеличения надежности вставки идентификационных данных при условии сохранения качества исходных мультимедиа данных применяют методы встраивания невидимых ЦВЗ неформатного типа. Например, встраивание может осуществляться либо в значения цветовых преобразований (RGB, YCbCr и других), либо значения частотных преобразований (вейвлет, DCT и DFT). При этом, в обоих случаях используется свойство избыточности мультимедиа данных. Отдельной задачей является обеспечение устойчивости ЦВЗ к различным воздействиям.

В настоящее время помехоустойчивое кодирование используется лишь с целью защиты цифрового водяного знака от случайных или преднамеренных искажений. При этом помехоустойчивое кодирование встраиваемой информации осуществляется на этапе формирования самого цифрового знака, то есть исходная информация, подлежащая встраиванию в контейнер, первоначально кодируется помехоустойчивым кодом, что естественно приводит к увеличению ее объема. В дальнейшем, полученные кодовые слова помещаются в контейнер любым известным способом. Очевидно, что такой способ использования помехоустойчивых кодов не учитывает специфические особенности структуры информации в контейнере. Известно, что значимость отдельных фрагментов контейнера различна, а, следовательно, и допустимые искажения в них тоже. Учет таких особенностей позволяет более эффективно встраивать информацию, используемую в дальнейшем для идентификации.

В данной работе предлагается схема внедрения водяного знака на основе использования специального класса кодов Гоппы с неравной защитой символов на длине кодового слова. В отличие от обычных помехоустойчивых кодов такие коды обладают специальными свойствами, позволяющими исправлять ошибки, имеющие неравномерное распределение на длине кодового слова. Такая модель позволяет согласовать свойства кодов из этого специального класса со специфической особенностью структуры информации в контейнере, а именно различной значимостью фрагментов мультимедиа информации. В общем случае кодовое слово используемого кода может быть представлено, как набор компонент различной длины и соответственно различной значимости. Процесс декодирования такого кода может быть легко описан с помощью взвешенной метрики Хэмминга, что позволяет учесть неравномерное распределение ошибок или неодинаковую

значимость символов на длине кодового слова. Использование такого специального класса кодов, например, позволяет внедрять водяной знак в изображение с учетом специфики используемого цветового преобразования. Данный подход позволяет сочетать эффективное встраивание дополнительной информации при сохранении высокого качества контейнера с одновременной защитой встраиваемой информации от некоторых типов искажений.

Блюм В.С., Заболотский В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПАЦИЕНТОВ И ГОСУДАРСТВЕННАЯ СОЦИАЛЬНАЯ СЕТЬ ПЕРВИЧНОЙ МЕДИЦИНСКОЙ ИНФОРМАЦИИ

«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.» [доклад ВОЗ, 2008].

Проблемы информированной безопасности пациентов и оперативного обнаружения дефектов оказания медицинской помощи без сомнения относятся к сфере информационной безопасности государства. Ущерб, который наносят некачественные медицинские услуги, исчисляется сотнями тысяч человеческих жизней и миллиардными финансовыми потерями.

По оценкам ВОЗ около 20% врачебных ошибок связано с неполнотой данных или невозможностью оперативного получения необходимой информации.

Задача состоит в том, чтобы идентифицировать источники первичной медицинской информации (ПМИ), оценить объём и интенсивность производства полной достоверной и доступной ПМИ, а, на основе полученных данных, предложить эффективную технологию сбора, хранения и мониторинга ПМИ для повышения уровня безопасности пациентов.

Анализ историй болезни указывает на два основных класса источников ПМИ (данных 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 объекты системы охраны здоровья допущены государством для оценки состояния здоровья пациентов, обязаны фиксировать данные (писать тексты, строить графики, фиксировать изображения) о здоровье граждан, а также предлагать и записывать схемы их лечения.

Ежедневно указанные источники ПМИ создают до 12 Гбайт текстовой и графической информации. Мониторинг такого потока информации на предмет оперативного обнаружения дефектов оказания медицинской помощи возможен только при условии её локального (централизованного) размещения.

В докладе будут рассмотрены принципы и структура медицинской информационной системы, в основу которой положена государственная социальная сеть, предназначенная для обслуживания источников ПМИ. Вводятся новые первичные структуры данных: персональная электронная история врачебных записей (история записей врача) и индивидуальная электронная история записей диагностической лаборатории.

Предложен способ идентификации основных участников информационного процесса: пациентов, врачей и диагностических лабораторий.

Обосновывается способ обнаружения дефектов оказания медицинской помощи путём обработки текстовой ПМИ методами иммунокомпьютинга. Рассмотрен подход к представлению и обработке ПМИ средствами формальной иммунной сети.

Василишин И.И., Полончик О.Л., Ястребов А.С.
Россия, Архангельск, Северный арктический федеральный университет
Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

О СПОСОБЕ СОКРЫТИЯ ДАННЫХ, ПЕРЕДАВАЕМЫХ РАДИОСООБЩЕНИЕМ

Физическая теория микроструктуры электромагнитного поля, впервые представленная на VIII Международной научно-технической конференции «Физика и технические приложения волновых процессов» (Санкт-Петербург, 14–19 сентября 2009 года), позволяет объединить воедино полевую и корпускулярную теории электромагнитного поля. Такое объединение осуществляется введением уровня микроструктуры электромагнитного излучения (ЭМИ) во всём пространстве за пределами излучателя. Уровень микроструктуры включает каждый фотон ЭМИ, как основополагающий трёхвекторный объёмный элемент Реального Мира, своим движением формирующий электромагнитное поле в ближней и в дальней зонах излучения. При этом уровень макроструктуры

ЭМИ определяется совокупностью вложений всех фотонов, данного электромагнитного поля, и представляется полевой теорией, изложенной уравнениями Максвелла. Достигнуть единения уровней микро- и макроструктуры ЭМИ разрешает использование понятий:

– луча – геометрической составляющей пространственного движения фотона;

– траектории колоиды – геометрической составляющей луча, определяющей координатное движение фотона в пространстве распространения электромагнитной волны.

– Введение луча, а особенно траектории колоиды и трёхвекторной модели фотона, объясняет следующие положения:

– поворот фотона вокруг вектора J (вектор динамического момента инерции – третий вектор фотона) – микроструктура поля – считать определяющим, при формировании периода (частоты) электромагнитной волны – макроструктура поля, не только в дальней, но и в ближней зонах излучения, когда исключено влияние излучателя на фотон;

– фотоны электрического либо магнитного типа определяются наклоном траектории их движения в пространстве (наклон либо к оси E, либо к оси H) – микроструктура поля, что определяет амплитуду электрической и магнитной составляющих поля потока излучения в целом – уже как макроструктуру поля;

– электрическая нейтральность фотона – макроструктура поля – определяется изменением положения двух его векторов E и H – микроструктура поля – на противоположную в течение полупериода, а затем на исходную через период.

На основании положения об электрическом либо магнитном типе фотона, полученном физической теорией микроструктуры электромагнитного поля, выдвигается следующее научное предположение: «Формируя специальным материалом излучателя передающей антенны различные наклоны траектории, по которым происходят движения фотонов в пространстве, предоставляется возможность передавать несколько сообщений на одной частоте». Другими словами можно сказать, что происходит пространственное уплотнение сигнала: частота передачи одинакова для всех сообщений, а разделение сообщений происходит по углу наклона движения фотона по колоиде.

Для приёма таких сообщений требуется антенна, созданная из материала со специальной структурой кристаллической решетки. Используя приёмную антенну, созданную из обычного проводящего материала, будет принято одно сообщение, независимо от того какое количество сообщений передавалось, т.е. просто будет зафиксирован факт передачи сообщения на излучаемой частоте.

Вывод. Используя физическое свойство наклона движения фотона в пространстве, можно создать новый способ сокрытия передаваемых данных. Содержание радиосообщения, переданное таким способом, определить принципиально невозможно традиционными способами, невзирая на то, что приёмник настроен на частоту передаваемого сообщения.

Верхолат А.М., Фарсеев А.И.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОНОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ОБУЧЕНИЯ

В настоящее время в процессе обучения находят широкое применение автоматизированные системы обучения (АСО), которые обеспечивают информационно-методическую поддержку процесса обучения и тестирования знаний по различным дисциплинам.

В данном докладе рассматриваются вопросы информационной безопасности при работе в среде АСО, предназначенной для обучения инфологическому моделированию баз данных (БД). Разработка этой системы ведется на кафедре информационных систем и компьютерных технологий университета для информационно-методической поддержки учебных дисциплин «Базы данных» и «Управление данными».

В качестве архитектуры построении АСО была выбрана клиент-серверная архитектура. Структурно АСО включает две составные части: клиентскую и серверную. Основными блоками серверной части являются:

– блок хранения баз данных и баз знаний (загрузка и сохранение);
– блок сетевого взаимодействия.

В состав блоков клиентской части входят:

– блок описания структур данных;
– блок пользовательского интерфейса;
– блок авторизации и разграничения прав доступа;
– блок сетевого взаимодействия.

Информационная безопасность в системе обеспечивается на различных уровнях работы с данными. Первый уровень безопасности определяется использованием средств авторизации и разграничения прав доступа для пользователей. После прохождения процедуры аутентификации

пользователю предоставляется доступ к АСО в соответствии с группой пользователя и назначенным ему набором прав. В системе предусмотрены три группы пользователей («обучаемый», «преподаватель» и «администратор») с соответствующими наборами правил.

Второй уровень безопасности определяется архитектурой построения системы и выбранными проектными решениями ее реализации. Клиент-серверная архитектура построения АСО предусматривает хранение всех данных на сервере, что обеспечивает надежность их хранения.

В качестве инструмента хранения данных на сервере был выбран формат XML. Такой выбор был сделан по следующим причинам информационной безопасности. Во-первых, язык XML интуитивно прост, что позволяет с одной стороны не усложнять приложение и не использовать систему управления базами данных, которая вносит зависимость от платформы и увеличивает вероятность появления ошибок, а с другой – позволяет быстро и легко обмениваться по сети сериализованными структурами с клиентом. Во-вторых, в выбранной для программной реализации системы среде .Net имеется удобный механизм работы с XML, который позволяет быстро и удобно сохранять, загружать и редактировать XML файлы. В-третьих, при частичном разрушении XML файлов остается возможность чтения их неразрушенных частей, а значит, это позволит в некоторых случаях сохранить такую важную информацию, как задания, пройденные тесты, оценки результатов тестирования и т.п. В-четвертых, использование отдельного файла XML для каждого пользователя практически исключает возможность доступа этих пользователей к другим XML файлам.

В докладе подробно рассмотрены алгоритмы и проектные решения, обеспечивающие информационную безопасность в системе обучения, а также их программная реализация.

Викторов В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций

ОТКАЗОУСТОЙЧИВОЕ ХРАНЕНИЕ ИНФОРМАЦИИ

Современные технологии позволяют хранить на носителях информации большое количество данных, но надежность этих носителей не сильно шагнула вперед с момента их изобретения. Что увеличивает вероятность потери ценной информации в нужный момент, поэтому, в виду недостаточной надежности встроенных систем отказоустойчивости следует задуматься об организации отказоустойчивого хранилища данных. Ведь построить надежную систему хранения данных можно при помощи бесплатно распространяемого ПО фирмы – производителя вашего носителя данных.

Ключевым моментом разработки отказоустойчивой системы является обеспечение резервного дублирования (защита за счет избыточности) на базе как аппаратного, так и программного обеспечения. Избыточность реализует алгоритмы обнаружения ошибок, которые используются вместе с алгоритмами диагностики, позволяющими выявить причину ошибки. Отказоустойчивая система должна обеспечивать переключение на альтернативное устройство в случае сбоя, а также информировать пользователя о любых изменениях конфигурации так, чтобы он мог восстановить вышедшие из строя устройства, прежде чем перестанут работать их дубликаты.

Дисковые системы RAID.

В 1987 году трое специалистов из университета Беркли (Калифорния) опубликовали статью с описанием методов обеспечения отказоустойчивости с помощью массивов небольших дисков. Эта технология получила название RAID – Redundant Array of Inexpensive Disks. Этот массив имеет несколько уровней, каждый из которых соответствует определенному кругу задач.

Например, RAID-0 служит для увеличения скорости обмена информации, но увеличивает вероятность отказа системы хранения данных в два раза. Сразу после создания этого типа массива, появился RAID-1, он основан на принципе «зеркалирования» данных на носителях, что в два раза увеличивает стоимость хранения информации, но в то же время, в два раза снижает риск ее безвозвратной потери. Далее появились массивы RAID-2,RAID-3,RAID-4. Наиболее современными на сегодняшний день выглядят массивы уровней 5 и 6. По своему принципу построения они похожи – использую массивы дисков с чередованием, либо с выделением дополнительных дисков четности, либо без.

Так же, существуют принципы организации массивов, которые сочетают в себе несколько уровней RAID (10,60,50). Они основаны на создании массива повышенной производительности RAID-0 на основе таких массивов, как RAID-5 (соответственно RAID-6+0 и т.д.).

Дисковые архитектурные массивы, не относящиеся к RAID.

JBOD (Just a bunch of disks, просто пачка дисков) – дисковый массив данных, в котором объем дискового пространства распределяется последовательно. Такой массив не повышает отказоустойчивости, но позволяет построить файловое хранилище на дисках с маленьким объемом и, соответственно, ценой.

RAID 7 – зарегистрированная торговая марка компании Storage Computer Corporation, отдельным уровнем RAID не является. В состав RAID 7 входит контроллер с встроенным

микропроцессором под управлением операционной системы реального времени. Она позволяет обрабатывать все запросы на передачу данных (как между отдельными дисками, так и между массивом и компьютером) асинхронно и независимо. Здесь один диск используется для накопления блоков четности. Этот массив обязательно следует использовать вместе с источниками бесперебойного питания, так как кэш, хранящийся в контроллере очень важен: без него информация на дисках будет утеряна.

Так же, немаловажным фактором является тип используемых носителей данных. Недавно вышли на массовый рынок SSD (твердотельные накопители). Это – запоминающее и устройство без движущихся механических частей (против классических HHD, где используется связка механика+электроника, что уменьшает надежность). Существуют энергозависимые и энергонезависимые SSD. Современные энергозависимые накопители содержат в себе аккумулятор и резервное хранилище, созданные для того, что бы сохранить данные хранимые на них. Их огромным преимуществом является скорость обмена информацией.

Энергонезависимые накопители более современные, обладают так же высокой скоростью передачи данных и не требуют системы копирования в случае отключения питания. Но имеют свой своеобразный недостаток: ограниченное число циклов перезаписи. Так же все твердотельные накопители имеют еще один недостаток- высокая цена объема. Их использование следует рассматривать в тех случаях, где работа ведется в помещениях с большим количеством пыли или при наличии вибраций (например, судно),а так же, когда необходима высокая скорость передачи данных (работа с графикой).

Воробьев В.И., Евневич Е.Л., Шкиртиль В.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МОДЕЛИРОВАНИЕ КОМПОЗИЦИИ И КАЧЕСТВА СЕРВИСОВ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Новые парадигмы, такие как сервис-ориентированные архитектуры и облачные вычисления, привели к превращению информационных технологий в стратегический фактор. Жизненные циклы программ и сервисов становятся все короче за счет использования интероперабельных продуктов. Современные SaaS, PaaS и IaaS архитектуры часто оказываются недостаточно гибкими, чтобы удовлетворить разнообразные требования потребителя, касающиеся композиции и качества сервисов. Предлагается онтологическая модель, позволяющая провайдерам и потребителям подбирать оптимальные композиции ресурсов, основываясь на пользовательском запросе. Онтология на OWL для описания ресурсов аппаратного и программного обеспечения, включая ограничения интероперабельности, мета информацию, некоторые критерии поиска, граф композиций ресурсов, основывающиеся на абстрактном запросе, позволяет найти приемлемое решение. Онтология содержит набор понятий предметной области и связей между ними, способствуя тем самым обмену информацией между компьютерной средой и пользователем, и применяется для извлечения запрашиваемых пользователем ресурсов.

Описание представления функциональных требований поступает на вход онтологической модели, которую можно рассматривать в качестве базы знаний. Для представления знаний используется онтология Semantic Web и управляющие языки OWL и SWRL в комбинации с возможностями SPARQL-запросов.

Создается представление графа, содержащего различные варианты выбора, базирующиеся на абстрактных отношениях зависимости, которые могут существовать между различными ресурсами. Граф зависимости может быть выведен автоматически с использованием различных запросов к онтологической системе. Этот граф трансформируется в целочисленную программу и может быть использован для получения всех возможных инфраструктурных композиций и нахождения оптимальной конфигурации в соответствии с предпочтениями потребителя, стоимостью продукта и рядом других требований.

Воробьёв В.И., Федорченко Л.Н., Шишкин В.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ОНТОЛОГИЧЕСКИЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ СТАНДАРТОВ И ВОЗМОЖНОСТИ ИХ ГАРМОНИЗАЦИИ

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

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

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

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

– ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования»,

делают невозможной сертификацию по «Общим критериям» (ISO/IEC 15408:2005 Information technology — Security techniques — Evaluation criteria for IT security) (из доклада А Лунина).

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

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

– улучшение применимости криптографических стандартов,
– активный пересмотр существующих криптографических стандартов,
– исключение слабых и противоречивых схем;
– включение новых и более эффективных схем.

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

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

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

Горбашко А.В.
Россия, Санкт-Петербург, Санкт- Петербургский государственный университет водных коммуникаций

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ В МОРСКОМ ПОРТУ

Информационные потоки морского порта

Информационная система (ИС) современного морского порта объединяет в себе множество подсистем и в настоящее время рассматривается как АСУ транспортного узла. Помимо собственно порта она обслуживает его дочерние предприятия, а также примыкающие к порту железнодорожный узел, таможню, экспедиторские, стивидорные (обеспечивающие погрузку и выгрузку судов), брокерские фирмы, а также представительства судоходных компаний. Для участников логистических цепочек ИС исполняет роль шины для информационного обмена.

Интеграция ИС и доступ к информации

Интеграция подсистем порта основана на договоре, участники которого получают права на доступ к данным и приложениям ИС (в объеме, необходимом для работы со своими грузами, если речь идет о технологических процессах) и берут на себя ряд обязательств. В частности, каждый участник обязан своевременно регистрировать свои данные, которые используются другими участниками транспортного процесса. Соблюдение этого правила дает всем компаниям взаимовыгодную возможность оперативно получать и использовать свежую информацию практически

сразу же, как только она появляется в ИС. Доступ к ИС позволяет компаниям повысить качество информационного обслуживания своих клиентов и партнеров. В результате улучшается работа как транспортного узла в целом, так и каждого отдельного участника соглашения ИС, существенно снижается общее время обработки грузов в порту на всех звеньях единой технологической цепочки.

Проблемы доступа пользователей к ИС и безопасности

Абсолютно все клиенты порта при заключении контракта получают пароль, который дает возможность доступа к ИС порта. Это входит в систему комплексного обслуживания клиентов. Они имеют возможность получить текущую информацию о статусе своего груза не только со своего рабочего места, но и из любой точки страны и мира, где есть Internet.

Необходимо обеспечить надежную защиту информации в условиях, когда у системы большое число пользователей, работающих в различных фирмах и организациях, полную ее сохранность и конфиденциальность как коммерческой информации.

Проблемы и способы аутентификации

Аутентификация с помощью аппаратных средств бывает двух видов: по схеме запрос-ответ; по схеме аутентификации с синхронизацией.

Электронно-цифровая подпись может использоваться в качестве средства аутентификации, если она помещена на аппаратные средства. Используется технология открытых ключей, которая подтверждается сертификатом.

Одноразовые пароли на основе стандартов MD4, MD5 используют хэш-функции и случайные числа в протоколе аутентификации.

Протокол RADIUS является примером построения распределенной архитектуры аутентификации и авторизации. Сервер RADIUS реализован обычно с помощью «домена» на UNIX- или NT-машине и может поддерживать различные методы аутентификации пользователя.

Выводы

Так как в морском порту информационная система является интегрированной и распределенной, то для обеспечения ее безопасности необходимо использование комплексных мер защиты информации. Для аутентификации пользователей целесообразно применять ЭЦП. Поэтому можно применить следующие продукты российского рынка: USB-ключ Rutoken для безопасного хранения паролей, ключей; средство криптографической защиты информации «КриптоПро CSP» для формирования и ввода секретных ключей; CRYPTO IDENITY для реализации аутентификации и идентификации с помощью алгоритма RSA с использованием нестандартных механизмов паролей и хранения ключей.

Григорьева М.В., Маврин П.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО МЕТОДОЛОГИИ SCRUM

В настоящем докладе будут рассмотрены вопросы применения инновационных подходов к разработке программного обеспечения с точки зрения постановки и реализации требований информационной безопасности.

Организации, применяющие гибкие методики разработки программного обеспечения часто плохо подготовлены, чтобы справиться с возросшими рисками в ИТ-среде. Принятие решений о стратегии безопасности, накладываемых ограничениях и требованиях безопасности в архитектуре приложений по-прежнему является серьезной проблемой. В этой статье мы предполагаем, что одной из основных проблем в организационной защите информации и защите информации при разработке программного обеспечения является то, что текущему подходу не хватает инноваций в применении методов управления рисками и стандартов безопасности / приложений.

Хотя разработка требований по безопасности в разработке ПО является быстро развивающейся областью исследований, в настоящее время основной процесс принятия решений, который применяется повсеместно в области информационной безопасности, – Plan-Do-Check-Act цикл (в соответствии с действующими стандартами безопасности). Однако, модель PDCA, не совсем подходит для ситуаций более динамичных и запутанных, с неустоявшимся набором требований.

Более того, наиболее распространен подход к информационной безопасности на основе комплексного процесса, который начинается с подробного анализа рисков, за которым следует развитие политики безопасности и осуществления этой политики. Этот процесс более похож на подход в разработке программного обеспечения «водопад». На практике ряд недостатков есть и в том и в другом подходе.

Одна из основных проблем, с которыми сталкиваются организации в том, что динамичная среда безопасности вынуждает их к сокращению сроков реализации их системы безопасности. Таким образом, организации сокращают временные затраты как на фазе оценки риска, так и в стадии реализации программного обеспечения.

Девянин П.Н.
Россия, Москва, Институт криптографии, связи и информатики Академии ФСБ России

МОДЕЛИ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ ДОСТУПОМ И ИНФОРМАЦИОННЫМИ ПОТОКАМИ И ИХ ПРИМЕНЕНИЕ ПРИ РАЗРАБОТКЕ ОТЕЧЕСТВЕННЫХ ЗАЩИЩЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Одно из наиболее динамично развивающихся направлений современной теории компьютерной безопасности – разработка и исследование моделей логического управления доступом и информационными потоками в компьютерных системах. В соответствии с ГОСТ Р ИСО/МЭК 15408-2002 применение таких моделей требуется при создании компьютерных систем с высоким уровнем доверия к их безопасности. На основе классических дискреционных (Харрисона-Руззо-Ульмана, типизированной матрицы доступов, Take-Grant), мандатных (Белла-ЛаПадулы, систем военных сообщений, Биба) и ролевых (семейство моделей RBAC) моделей зарубежными и отечественными специалистами строятся новые модели, позволяющие более точно учесть специфику функционирования существующих и перспективных защищенных компьютерных систем, в том числе, операционных систем (ОС). Например, разрабатываются модели типизированного управления доступом, делегирования доверия, изолированной программной среды и механизмов виртуализации компонент ОС, Интернет-сервисов (электронной почты, блогов, конференций, облачных вычислений).

В то же время отечественный опыт применения моделей безопасности логического управления доступом и информационными потоками при создании защищенных ОС трудно признать успешным. Часто при реализации востребованного в защищенных ОС мандатного управления доступом используется устаревшая модель Белла-ЛаПадулы или ее интерпретации. Данная модель не позволяет анализировать условия возникновения запрещенных информационных потоков по памяти между сущностями (файлами, каталогами) функционально или параметрически ассоциированными с субъектами (процессами) ОС, что может позволить недоверенным субъектам, функционирующим от имени нарушителя, получить контроль над доверенными субъектами, например, реализующими механизмы защиты ОС. Также эта модель не позволяет исследовать запрещенные информационные потоки по времени от сущностей с высоким уровнем конфиденциальности к сущностям с низким уровнем конфиденциальности, возникающие при кооперации субъектов, например, при их совместном доступе к сущностям или при использовании буферов обмена (clipboard). Кроме того, применение моделей на практике часто является только формальным, при этом не осуществляется адаптация моделей к условиям функционирования ОС, не выполняется формальное обоснование безопасности ОС в рамках модели, или используется одновременно несколько моделей (иногда для различных видов управления доступом) без теоретического исследования свойств такой композиции.

Реализация «Национальной программной платформы» и плана перехода федеральных органов исполнительной власти Российской Федерации в течение 2011–2015 годов на использование свободного программного обеспечения (СПО) включают разработку национальной ОС, основой которой вероятно станет ОС семейства Linux, что открывает перспективы построения отечественной защищенной ОС, безопасность которой будет обоснована, в том числе, в рамках существующих или новых моделей управления доступом и информационными потоками.

В настоящее время отечественными специалистами, включая автора, разрабатывается семейство дискреционных, мандатных и ролевых моделей безопасности управления доступом и информационными потоками (ДП-моделей). В моделях семейства учтен ряд существенных особенностей функционирования ОС, в том числе: возможность кооперации части субъектов при передаче прав доступа и создании информационных потоков по памяти или по времени, возможность реализации противодействующих друг другу доверенных и недоверенных субъектов с различными условиями функционирования, возможность изменения функциональности субъекта при реализации информационного потока по памяти на функционально ассоциированные с ним сущности или от параметрически ассоциированных с ним сущностей, необходимость в ряде случаев определения различных правил управления доступом и информационными потоками для распределенных компонент ОС. Наиболее активно исследуются свойства мандатной модели защищенной ОС (ЗОС ДП-модель) и ролевой ДП-модели для ОС семейства Linux (РОСЛ ДП-модель). Кроме того, на базе СПО ОС AltLinux производится макетирование механизма управления доступом, основанного на реализации ЗОС и РОСЛ ДП-моделей. В дальнейшем планируется развитие ДП-моделей с целью включения в них новых элементов, более точно учитывающих особенности функционирования ОС семейства Linux, формулирования и обоснования в рамках моделей условий передачи прав доступа и реализации запрещенных информационных потоков по памяти или по времени, а также выработки научно-обоснованных технических решений, направленных на совершенствование механизмов защиты информации в ОС.

Таким образом, разработка на основе СПО отечественных защищенных ОС, стимулирует развитие технологий обеспечений информационной безопасности и дает существенный толчок научным исследованиям российских специалистов в области теории компьютерной безопасности, включая модели безопасности логического управления доступом и информационными потоками и поиск научно-обоснованных методов их адекватной реализации в защищенных ОС.

Десницкий В.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ОЦЕНКА ЭФФЕКТИВНОСТИ КОНФИГУРИРОВАНИЯ КОМБИНИРОВАННЫХ МЕХАНИЗМОВ ЗАЩИТЫ НА ОСНОВЕ РЕШЕНИЯ ОПТИМИЗАЦИОННОЙ ЗАДАЧИ

Объектом исследования в работе является механизм защиты системы встроенных устройств, предоставляющий защиту на основе комбинированного использования отдельных компонентов защиты. Процесс нахождения наиболее эффективной конфигурации защиты осуществляется путем постановки и решения оптимизационной задачи с учетом функциональных и нефункциональных характеристик отдельных компонентов защиты. Каждый компонент защиты предоставляет одно или несколько функциональных свойств защиты, таких как свойство целостности хранимой на устройстве информации или конфиденциальность, формируемых на устройстве данных. При этом используемые компоненты защиты характеризуется также набором нефункциональных требований, определяющих объемы ресурсов устройства, которые должны быть предоставлены компоненту для его корректного функционирования.

Оценка эффективности предложенной стратегии конфигурирования на основе решения оптимизационной задачи определяется путем ее сравнения с другими стратегиями конфигурирования, в частности стратегией «произвольного конфигурирования». Стратегия произвольного конфигурирования представляет сценарии действий администратора защищаемой системы, проводящего конфигурирование вручную, без использования автоматизированных средств анализа имеющихся в наличии компонентов защиты и поиска эффективных конфигураций.

Сравнение обеих стратегий производится экспериментальным путем, включая определение начальных условий задачи и проведение конфигурирования на некотором модельном примере, а также оценку и сравнение результатов. В работе построена программная реализация конфигурирования на основе решения оптимизационной задачи, а также разработана модель, представляющая обобщенный сценарий применения стратегии произвольного конфигурирования. Используются два следующие типа критериев эффективности. Во-первых, рассматривается критерий оптимальности, используемый для решения оптимизационной задачи. Во-вторых, критерий эффективности может задаваться исходя из внешних параметров системы, механизма конфигурирования и отдельных компонентов защиты. В первом случае стратегия на основе оптимизационной задачи будет оптимальной по построению. При этом использование критерия оптимальности позволяет сравнить, эта стратегия эффективнее альтернативных стратегий конфигурирования.

Стратегия произвольного конфигурирования характеризуется элементом случайности, в частности заранее не фиксированным порядком последовательности рассмотрения функциональных свойств. Поэтому для сравнения стратегий вводятся следующие вероятностные показатели: вероятность получения допустимой конфигурации; вероятность получения оптимальной конфигурации. Под допустимой понимается такая конфигурация, которая предоставляет все требуемые функциональные свойства защиты и не выходит за рамки нефункциональных ограничений. Для веществennознозначных критериев оптимальности также вводится показатель, определяющий критериальное значение для заданной стратегии в процентном отношении по отношению к оптимальному значению.

Работа выполнена при финансовой поддержке РФФИ (проект №10-01-00826), программы фундаментальных исследований ОНИТ РАН (проект №3.2), государственного контракта 11.519.11.4008 и проектов Евросоюза SecFutur и MASSIF, а также в рамках других проектов.

Десницкий В.А., Котенко И.В., Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

КОНФИГУРАЦИОННАЯ МОДЕЛЬ КОМБИНИРОВАННОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ СО ВСТРОЕННЫМИ УСТРОЙСТВАМИ

Работа посвящена разработке и исследованию конфигурационной модели для построения комбинированных механизмов защиты информационных систем со встроенными устройствами на основе решения оптимизационной задачи. Предлагаемая модель описывает процесс конфигурирования, который включает нахождение и последующее применение оптимального набора специализированных программных компонентов защиты, используемых для поддержки безопасности информационной системы, которые, во-первых, реализуют все необходимые функциональные требования защиты и, во-вторых, позволяют достичь наиболее эффективного расхода ресурсов системы в процессе осуществления защиты.

Работа ориентирована на построение и практическое применение комбинированных механизмов защиты для широкого круга распределенных информационных систем со встроенными и мобильными устройствами. Характерный пример такой системы − мобильная и быстро разворачиваемая коммуникационная сеть поддержки и оперативного управления в чрезвычайных ситуациях, которая позволяет организовать совместную работу различных служб и задействованных

устройств. Такие системы характеризуются динамически изменяемой топологией сети и отличающимися типами коммуникаций между ее отдельными узлами, а также заранее не фиксированным кругом функционирующих агентов и задействованных устройств.

Как составные элементы информационной системы встроенные устройства обладают, как правило, достаточно слабыми вычислительными возможностями и поэтому характеризуются низкой производительностью. Поэтому задача поддержки защиты таких систем требует принципиально новых путей решения, которые помимо реализации защиты системы от заданного вида угроз учитывали бы также нефункциональные («ресурсные») требования к механизму защиты. Подход к нахождению оптимальной конфигурации компонентов защиты, предлагаемый в работе, базируется на получении серии численных нефункциональных показателей защиты, и затем, путем постановки и решения оптимизационной экстремальной задачи при ограничениях на значения этих показателей и заданной целевой функции позволяет построить наиболее эффективную конфигурацию компонентов защиты для обеспечения безопасности информационной системы.

В рамках модели как функциональные, так и нефункциональные свойства защиты, присущие встроенным устройствам, рассматриваются в виде иерархической древовидной структуры («дерево свойств»). Для каждого нефункционального свойства формируются численные показатели, а также методики получения их значений для заданных видов компонентов защиты. На базе дерева свойств и численных показателей формируются критерии оптимальности, используемые, во-первых, для нахождения оптимальных конфигураций и, во-вторых, для оценки эффективности и сравнения различных стратегий конфигурирования, включая стратегию «произвольного конфигурирования».

Программный прототип механизма конфигурирования, разработанный в рамках кросс-платформенной среды «Java 2» с использованием принципов объектно-ориентированного проектирования и универсального языка моделирования UML, демонстрирует особенности процесса конфигурирования, включая возможность задания определенного критерия оптимальности, а также функцию проверки эффективности выбранной конфигурации.

Работа выполнена при финансовой поддержке РФФИ (проект №10-01-00826), программы фундаментальных исследований ОНИТ РАН (проект №3.2), государственного контракта 11.519.11.4008 и проектов Евросоюза SecFutur и MASSIF, а также в рамках других проектов.

Дойникова Е.В., Котенко Д.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

РАСШИРЕНИЕ МЕТОДИКИ ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ ЗАСЧЕТ ИСПОЛЬЗОВАНИЯ ГРАФОВ ЗАВИСИМОСТЕЙ СЕРВИСОВ

Распределенность современных информационных систем приводит к широкому распространению воздействия от сетевых атаки через зависимости сервисов. Поэтому актуальной задачей управления безопасностью таких систем является использование графов зависимостей сервисов при построении моделей атак.

Для определения возможных последовательностей атак и целей нарушителя хорошо подходит подход на основе построения графов атак. Однако при этом не учитываются следующие аспекты:

1. Динамический характер распространения атаки (графы атак прослеживают зависимости между элементарными шагами и, таким образом, строится план действий нарушителя; каждому узлу графа присвоено абстрактное статистическое значение);
2. Отрицательный эффект реакции на атаку;
3. Стоимостные потери от атаки и воздействия.

В данной работе предлагается методика, которая объединяет информацию о возможных действиях нарушителя и текущих конфигурациях сервиса, т.е. объединяет использование графов атак и графов зависимостей сервисов. Первые позволяют отслеживать позицию нарушителя, а вторые – динамически отслеживать влияние на целевую систему, пока нарушитель продвигается по узлам атакуемой сети. Это позволяет получить более точную информацию о распространении ущерба от вторжения и распространении ущерба от реакции на него.

В процессе работы были исследованы существующие подходы к использованию моделей зависимостей сервисов и их недостатки. В результате предлагается использовать подход, позволяющий оценить распространение ущерба от атаки и вторжения на основе системы оценки уязвимостей CVSS и получить количественные показатели. Такой подход подходит к разработанному ранее прототипу оценки безопасности.

Чтобы включить зависимости сервисов в модель была выполнена модификация этого прототипа. Для построения графа зависимостей сервисов (определение существующих сервисов и зависимостей между ними) изменен компонент конструирования модели сети. К свойствам создаваемого сетевого объекта добавлено свойство «Сервис», которое позволяет определить все сервисы для этого объекта. Таким образом, формируется дополнительный уровень зависимостей сервисов. Сущности сервисов связаны с соответствующими сетевыми объектами. Сущность «Сервис» имеет следующие три свойства:

1. Запрос (определяет привилегии/учетные записи сервиса);
2. Доверие (определяет отношение доверия, которое должно быть удовлетворено зависимым сервисом);
3. Разделение привилегий (определяет разделяемые с зависимым сервисом привилегии, если зависимость удовлетворена).

На следующем шаге, при анализе безопасности сети, также необходимо проделать некоторые модификации. Этот компонент генерирует дерево атак на основе входных данных (файл, содержащий данные по сети в определенном формате; база данных, заполненная списком уязвимостей; выбранный хост со злоумышленником). Выходные данные компонента для каждой атаки: некоторые привилегии отменены или изменены на целевом компоненте.

К этому компоненту был добавлен дополнительный зависимый компонент, позволяющий управлять зависимостями сервисов. Для каждой элементарной атаки злоумышленника (отдельный шаг в графе атак) зависимый компонент создает дополнительный граф зависимостей сервисов. В качестве входных данных он получает привилегии/учетные записи на некотором сервисе после атаки (вектор ущерба для уязвимости, сформированный на данном шаге в графе атак позволяет заполнить свойство «Запрос» для сервиса), список уязвимостей и структуру сервисов. Эти привилегии/учетные записи (свойство «Запрос») определяют разделяемые между зависимыми сервисами привилегии (свойство «Разделение привилегий»), если удовлетворено отношение доверия (свойство «Доверие»). В результате обхода всех существующих зависимостей определяется выигрыш нарушителя (итоговый набор привилегий), который является предусловием для следующего шага атаки.

В дальнейшей работе предполагается разработка системы показателей защищенности для графов атак и зависимостей сервисов с использованием показателей CVSS.

Работа выполняется при финансовой поддержке РФФИ (проект 10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект 3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

Дойникова Е.В., Чечулин А.А., Котенко И.В., Котенко Д.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

РАСШИРЕНИЕ МЕТОДИКИ ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ ДЛЯ УЧЕТА АТАК НУЛЕВОГО ДНЯ

В настоящее время для анализа защищенности недостаточно учитывать только известные уязвимости. Большие сети могут содержать неизвестные уязвимости, которые зачастую используются для атак нулевого дня. Поэтому актуальной проблемой является учет таких атак при оценке защищенности информационной системы.

Атаки нулевого дня – атаки, которые используют неизвестные уязвимости или уязвимости, для которых нет соответствующих заплаток (патчей). В процессе работы авторами были проанализированы последние исследования в области проблемы учета атак нулевого дня для оценки защищенности. Есть, по крайней мере, две проблемы, связанные с уязвимостями нулевого дня:

1. Определение вероятности наличия уязвимости нулевого дня;
2. Корреляция известных уязвимостей с уязвимостями нулевого дня.

В работе предлагается использовать в качестве основы для оценки информационных рисков с учетом атак нулевого дня подход, базирующийся на следующих процедурах:

1. Предположение существования уязвимости нулевого дня в отдельном приложении сети;
2. Построение графа атак на базе модели сети с учетом существования уязвимости нулевого дня;
3. Вычисление процента угрожаемых активов на основе скомпрометированных хостов;
4. Возврат к первому шагу и предположение уязвимости нулевого дня в другом приложении (необходимо перебрать последовательно все приложения сети);
5. Расположение приложений в порядке выигрыша злоумышленника в случае наличия уязвимости нулевого дня.

Выбор данного подхода объясняется тем, что он позволяет выявить хосты, уязвимости на которых могут привести к наибольшему ущербу и принять соответствующие контрмеры. Наличие уязвимости нулевого дня предполагается в каждом приложении сети последовательно. На основании этого генерируются графы атак. Для улучшения подхода предлагается добавить дополнительные характеристики, которые позволяют определить вероятность наличия уязвимости нулевого дня. Основная идея состоит в том, чтобы автоматизировать процесс выбора хостов, которые имеют наибольшую вероятность наличия уязвимостей нулевого дня.

В исходный прототип оценки защищенности информационной системы добавляется дополнительный компонент – генератор графа атак на базе уязвимостей нулевого дня. Он включает анализатор наличия уязвимости нулевого дня и генератор графа.

Анализатор наличия уязвимости нулевого дня получает в качестве входных данных конфигурацию сети из базы данных. Результат работы анализатора – список хостов/приложений с уязвимостями нулевого дня.

Для каждого хоста предлагается использовать следующий набор показателей:

– количество активных сетевых приложений;
– количество активных приложений, которые не имеют доступа к сети;
– наличие системы защиты на хосте.

Для каждого приложения предлагается следующий набор показателей: дата последнего обновления приложения; наличие поддержки приложения от производителя; распространенность в сети Интернет; критичность ресурса, который контролируется или используется данным приложением; использование сетевых портов.

Для получения этих данных используется стандарт Common Platform Enumeration (CPE) 2.2, задающий список и словарь аппаратуры, операционных систем и приложений.

На основе предложенного набора показателей определяется вероятность наличия уязвимости нулевого дня для каждого хоста/приложения. Если эта вероятность достаточно высока, считается, что уязвимость нулевого дня существует для хоста/приложения. В рамках предлагаемого подхода уязвимость нулевого дня характеризуется тремя параметрами: тип доступа (удаленный или локальный), получаемые права (обычного пользователя, администратора) и влияние на доступность (есть/нет). Наличие уязвимости предполагает полное нарушение конфиденциальности/целостности информации.

Набор уязвимых хостов/приложений является входными данными для следующего шага. Генератор графа получает в качестве входных данных информацию о сети в определенном формате, данные об известных уязвимостях, данные об уязвимостях нулевого дня и выбранный хост со злоумышленником. На выходе – дерево атак. Далее граф атак перестраивается с учетом уязвимостей нулевого дня. Полученный граф используется для анализа защищенности системы.

Работа выполняется при финансовой поддержке РФФИ (проект 10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект 3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

Дрождин В.В., Зинченко Р.Е.
Россия, Пенза, Пензенский государственный педагогический университет имени В.Г. Белинского, Москва

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В САМООРГАНИЗУЮЩЕЙСЯ ИНФОРМАЦИОННОЙ СИСТЕМЕ БЕЗ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ СРЕДСТВ

Самоорганизующаяся информационная система (СИС), кроме предоставления более широких возможностей по обработке данных, обеспечивает более высокий уровень защиты по сравнению с существующими автоматизированными информационными системами. Показана целесообразность взаимодействия СИС с системой иерархически организованных пользователей и приведены возможности существенного упрощения подсистемы обеспечения безопасности за счет более точного разграничения областей видимости пользователей на уровне концептуальной модели предметной области.

В докладе освещается решение проблем обеспечения безопасности в СИС по следующим направлениям:

1. Обеспечение защиты на уровне концептуальной модели предметной области.
2. Реализация исходной концепции «все запрещено».
3. Возможность определения более точной области видимости для каждого пользователя, включая как конкретные, так и обобщенные данные.
4. Обеспечение действий пользователей только в пределах своей области видимости и разрешенных действий.
5. Информирование вышестоящих пользователей о приближении и наступлении некорректных ситуаций в предметной области.
6. Организация пользователей в виде сетевой системы иерархически организованных пользователей.
7. Контроль деятельности подчиненных пользователей вышестоящими пользователями.
8. Определение областей видимости и действий по обработке данных для подчиненных пользователей.
9. Просмотр любых действий, выполненных подчиненными пользователями.
10. Запрос у вышестоящего пользователя подтверждения разрешения действий, ранее не выполнявшихся подчиненным пользователем.
11. Информирование вышестоящих пользователей о некорректных действиях подчиненных пользователей.

Пользователи СИС самостоятельно формируют и поддерживают концептуальную модель предметной области, а СИС самостоятельно создает и поддерживает соответствующую ей эволюционную базу данных.

Одна из особенностей СИС заключается во взаимодействии с внешней средой не как с множеством отдельных пользователей, а как с системой иерархически связанных пользователей. Поэтому каждый пользователь имеет определенную позицию в сетевой модели пользователей, что позволяет решать два типа задач:

– вышестоящие пользователи могут контролировать и управлять деятельностью подчиненных пользователей;

– система при взаимодействии с конкретным пользователем всегда знает, к кому ей целесообразно обратиться при возникновении сложных ситуаций.

Возможность формирования пользователями собственной системы понятий и наличие иерархических отношений между пользователями позволяют естественным образом реализовать механизм областей видимости для каждого пользователя СИС, что существенно повышает защищенность системы без использования специальных средств защиты.

Хорошее знание пользователями модели предметной области, постоянная адаптация системы к потребностям пользователей и высокий уровень защищенности обеспечат пользователям более интенсивное взаимодействие с СИС, что создаст реальные условия для возникновения системы принципиально нового типа, которая будет включать СИС и систему пользователей как равноправные подсистемы. Коэволюция СИС и системы пользователей будет поддерживать более высокий темп эволюции (развития) новой системы и обеспечит устойчивое развитие и более длительное существование предприятия, а также высокую эффективность и продолжительную эксплуатацию информационной системы.

Иванова Н.В., Коробулина О.Ю.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Международный стандарт ИСО/МЭК 27001 предлагает для управления обеспечением информационной безопасности в организации использовать методы из области менеджмента качества. Одним из таких методов является метод количественного и качественного анализа, позволяющий проводить всестороннюю и полную оценку. В частности, данный метод может быть использован в процессе оценки рисков информационной безопасности, которые неизбежно присутствуют в любой информационной системе.

Под риском информационной безопасности понимается вероятный ущерб, который понесет компания при раскрытии, модификации, утрате или недоступности своей информации. Величину риска информационной безопасности определяют два фактора: стоимость информации, обрабатываемой в информационной системе, и защищенность самой информационной системы.

Анализ рисков информационной безопасности включает в себя оценку рисков, а также методы снижения рисков или уменьшения связанных с ними неблагоприятных последствий.

Цель качественной оценки рисков состоит в определении факторов риска, областей возникновения рисков и видов рисков. Количественная оценка позволяет численно определить размеры отдельных рисков и риска для предприятия в целом. Итоговые результаты качественной оценки служат исходной информацией для проведения количественной оценки.

Удобным инструментом для систематизации и обработки результатов анализа рисков информационной безопасности является логико-структурная матрица. Данные, представленные в логико-структурной матрице, удобно передавать для обработки в экспертную систему аудита информационной безопасности для последующей выдачи рекомендаций о возможных способах повышения степени защищенности информационной системы.

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

О НЕОБХОДИМОСТИ СОЗДАНИЯ НОВОГО ВИДА ВООРУЖЕННЫХ СИЛ – КИБЕРНЕТИЧЕСКИХ ИНФОРМАЦИОННЫХ ВОЙСК

В связи с развитием информационных технологий их роль в обществе существенно повышается. Уже сейчас почти каждый житель планеты имеет свой мобильник-коммуникатор и может быть подвергнут специальному информационному воздействию, что открывает дополнительные возможности по манипуляции сознанием больших групп людей в интересах отдельных государств и мировых сообществ. В США эту опасность уже осознали и зам. министра обороны США обнародовал новую стратегию действий в киберпространстве. Компьютерное пространство объявляется полем оперативной деятельности для вооруженных сил США – наряду с сушей, морем, воздухом, космосом.

В условиях надвигающегося кризиса информационные войны будут усиливаться.

Наша страна в киберпространстве должна действовать на опережение, опираясь на имеющиеся у нас научно-технические заделы (см., например, наши книги «Архитектура виртуальных миров», второе изд. 2009, «Кибернетическая картина мира», 2010, мою статью «О необходимых и достаточных условиях синтеза нанороботов», опубликованную в Докладах РАН, 2010, т.433, №5, и др.). В настоящее время вырисовывается следующая картина – по сигналам компьютерных сетей могут не только осуществляться хакерские атаки и информационные воздействия на группы людей, но и синтезироваться в заданных точках планеты нанороботы, которые смогут производить разрушительную или созидательную работу, что неизмеримо усилит возможности той страны, которая обладает такой технологией.

В настоящее время необходимо сформировать новый вид вооруженных сил – кибернетические информационные войска, которые должны непрерывно действовать в масштабах всей планеты. В настоящее время разработка и использование новых информационных технологий в нашей стране производится лишь в отдельных организациях, и нет единой перспективной программы в этом направлении, что наносит большой ущерб обороноспособности страны, информационной безопасности. Необходимо разработать новую технологическую платформу по технологии виртуальных миров. Сейчас примерно такой же момент, когда создавались ракетные войска стратегического назначения.

В докладе анализируется предполагаемая структура нового вида вооруженных сил.

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

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПРИ ВЗАИМОДЕЙСТВИИ ВИРТУАЛЬНЫХ МИРОВ

В настоящее время островки автоматизации объединяются в виртуальные миры, возникают виртуальные миры финансовых банков, транспортных систем, структур здравоохранения и другие. Структуры виртуальных миров включают в себя население – людей-пользователей, аватаров, территорию в киберпространстве, производственные функции (например, производство финансовых операций, процедуры по поддержанию здоровья и др.), системы безопасности (например, защиту от хакерских атак и компьютерных вирусов), системы взаимодействия с другими виртуальными мирами.

Взаимодействие с другими виртуальными мирами жизненно необходимо для любого виртуального мира для обмена ресурсами и информацией, но именно через это взаимодействие осуществляется большинство покушений на безопасность.

В докладе анализируются структуры виртуальных миров и меры по обеспечению их безопасности, как пассивные, так и активные.

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

НАНОРОБОТЫ КАК ОСНОВА ЭЛЕМЕНТНОЙ БАЗЫ НОВОГО ПОКОЛЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Вопреки мнению виталистов, в мертвой природе возможна реализация многих жизненных функций за счет использования возможностей программного управления. Ведь ДНК – это тоже программный комплекс управления. Сейчас технологии направлены на то, чтобы что-то собрать. Но важно после использования и разобрать, наша планета и ближний космос уже превратились в свалку отработанной техники. Задачу нужно решать комплексно. Земной шар – это неупорядоченная память, где хранятся различные химические элементы, их находят по адресу, который отыскали геологи, добываю, обрабатывают, строят машины, используют эти машины, потом нужно их утилизировать – все это можно делать на основе нанороботов, похожих на элементы Лего.

В настоящее время накоплен большой опыт по созданию человекоразмерных роботов, которые широко используются для автоматизации и которые обладают функциями перемещения в пространстве. С другой стороны разработана элементная база вычислительной техники, выпускаются все новые и новые серии больших интегральных схем, которые обладают большими возможностями по обработке информации, но не обладают возможностями по перемещению, по самосборке и саморазборке комплексов.

На основе нанороботов возможно объединить эти два опыта.

В докладе анализируется набор функций нанороботов, определяются необходимые и достаточные условия для их синтеза и анализируется влияние появления нанороботов на проблемы безопасности.

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

ПРОБЛЕМА УСТРАНЕНИЯ КОСМИЧЕСКОГО МУСОРА КАК ВАЖНАЯ СОСТАВЛЯЮЩАЯ БЕЗОПАСНОСТИ

В настоящее время в ближнем космосе летают останки космических кораблей и другой мусор, которые представляют большую опасность для спутников.

В докладе рассматривается вопрос создания специальных систем для устранения космического мусора, которые включают в себя специальные спутниковые системы, ориентированные на захват наиболее опасных фрагментов мусора с последующим торможением для вхождения в плотные слои атмосферы. Системы используют данные по мониторингу космического мусора.

Создание мусороуборщиков является частью международного проекта по экологии космоса для обеспечения информационной безопасности.

Каторин Ю.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций

АНАЛИЗ ВОЗМОЖНОСТЕЙ ТСР ПО ПЕРЕХВАТУ ИНФОРМАЦИИ В СЕТЯХ СОТОВОЙ ЦИФРОВОЙ СВЯЗИ

Традиционные аналоговые системы сотовой связи хотя и могут создавать определенные трудности для радиоразведки, но не считаются особенно сложными противниками. В таких сетях электронный перехват сотовой связи не только легко осуществить, он, к тому же, не требует больших затрат на аппаратуру, и его почти невозможно обнаружить. Более серьезные опасения вызывает предстоящий массовый переход на цифровые системы. Хотя системы сотовой цифровой радиосвязи работают в том же диапазоне радиочастот, что и традиционные аналоговые системы, в них применяются более сложные сигналы и, самое главное, они имеют встроенные средства защиты информации, например, криптографические. Три действующих стандарта на системы цифровой сотовой радиосвязи предусматривают применение многократного доступа с временным разделением TDMA, означающего возможность одновременной передачи трех разговоров по одному каналу с последовательным разделением их передачи во времени (что эквивалентно одному вызову). Это в три раза затрудняет ведение радиоразведки. Другой стандарт цифровой сотовой радиосвязи с использованием многократного доступа с кодовым разделением CDMA дает возможность применения техники широкополосных систем с малой вероятностью обнаружения сигналов. Практически никакие другие системы связи не представляют таких трудностей для ведения радиоразведки, как широкополосные.

В докладе проанализированы основные методы перехвата информации в сетях сотовой цифровой связи и сделан вывод, что существующая система перехвата работает с любым типом кодирования, включая алгоритмы A5/1 и A5/2. Хотя цифровые сотовые телефоны, передающие информацию в виде цифрового кода более совершенны с точки зрения защиты информации. Однако, используемый в них алгоритм шифрования Cellular Message Encryption Algorithm (CMEA) может быть вскрыт опытным специалистом в течение нескольких минут с помощью персонального компьютера. Таким образом, даже современное состояние ТСР обеспечивает быстрый и надежный перехват, а также запрос и создания помех для трафика GSM сигналов, а так же режим работы оффлайн. Система перехвата, дешифровки, обработки и мониторинга GSM сигналов полностью пассивная. Алгоритмы защиты сотовой связи, которые берут своё начало в 80-х годах на сегодня не могут обеспечить полной конфиденциальности переговоров.

Комашинский Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ И ДИНАМИЧЕСКОЕ ДЕТЕКТИРОВАНИЕ MALWARE

Одним из подходов к обнаружению новых образчиков вредоносного программного обеспечения (malware) является использование методов классификации. Его применение обязывает исследователя в процессе получения обученного классификатора выполнять ряд шагов, определяющих его конечные качественные показатели:

1. Подготовку обучающей и тестовой выборок объектов;
2. Выделение базовых признаков, которые предполагается использовать при формировании модели;
3. Поиск среди базового набора признаков наиболее значимых;
4. Выбор метода классификации;
5. Выбор метода оценки модели.

Правильное выделение базовых признаков и поиска среди них наиболее значимых определяют такие характеристики полученной модели классификации, как скорость и простота ее переобучения,

скорость классификации отдельного объекта и ее точность. В идеале, количество признаков, обеспечивающих функционирование классификатора с заданными показателями точности, должно быть минимальным, их смысл – очевиден, а количество их возможных значений – конечно. Практика показывает, что в подавляющем числе случаев данные условия не выполняются. К примеру, одним из наиболее популярных путей формирования базового набора признаков для классификаторов программных приложений по поведению является применение «скользящего окна» фиксированной длины. Одной из основных проблем данного подхода является большая размерность получаемого пространства, затрудняющая выполнение последующих шагов получения обученного классификатора, что способно в итоге снизить показатели оперативности и точности получаемого процесса принятия решения. Представляемая работа посвящена снижению размерности пространства базовых признаков за счет введения иерархичности в процессы обучения и принятия решения за счет предварительной статической обработки обучающей выборки.

В докладе высказывается предположение, что определенные статические свойства анализируемых программных приложений определяют их поведенческие особенности. Для проверки предположения были проведены практические эксперименты на наборах вредоносных и безопасных исполняемых файлов формата PE32. Начальный эксперимент был проведен с целью получения дерева решений, относящего исследуемый объект к одной из двух базовых категорий (опасен/неопасен) на всей обучающей выборке. Серия контрольных экспериментов проводилась на расширенном наборе категорий, который помимо двух базовых, включал в себя категории, определяемые значениями некоторых статических атрибутов, доступных из структуры исполняемых файлов. При этом, в зависимости от значений базовых и дополнительных категорий объектов, обучающая выборка была разбита на более мелкие группы. Сравнение результатов экспериментов показало, что совместное применение статических и динамических атрибутов позволяет значительно повысить показатели точности для отдельных групп вредоносных приложений и в среднем упростить решающие модели за счет снижения количества используемых ими поведенческих признаков, а также существенно уменьшить объем базовой выборки поведенческих признаков за счет исключения из нее признаков, наличие которых коррелировало бы с включенным в рассмотрение статическими категориями. Итоговая решающая модель классификации представляет собой иерархический метаклассификатор, производящий на начальных уровнях принятия решения уточнение структурных свойств объекта с последующим выделением наиболее эффективной для обработки конкретного объекта модели классификации по заданным категориям. Наиболее эффективными статическими атрибутами в рамках данной модели показали себя поля SubSystem, Characteristics заголовков формата PE32 и обобщенные данные о типе компилятора, используемого при получении исполняемого файла. Для начального сокращения размерности пространства признаков использовался фильтрующий метод выделения значимых признаков на основе значения относительного коэффициента усиления, в качестве базового метода классификации использовался метод дерева решений. Эксперименты проводились с использованием среды Rapid Miner 5.0. Работа выполнена при финансовой поддержке РФФИ (проект №10-01-00826), программы фундаментальных исследований ОНИТ РАН (проект №3.2), государственного контракта 11.519.11.4008 и проектов Евросоюза SecFutur и Massif, а также в рамках других проектов.

Комашинский Д.В., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ В СИСТЕМАХ ПРОТИВОДЕЙСТВИЯ КИБЕРУГРОЗАМ

Понятия киберпростанства и киберугроз являются неотъемлемой частью современного общества в его активной, постиндустриальной фазе развития. На протяжении последнего десятилетия, по мере усиления процессов интеграции информационных технологий в критические сектора государственной и частной деятельности, возрастает необходимость в высокоэффективных, адаптивных методах противодействия сетевым атакам, критическим уязвимостям и вредоносному программному обеспечению (malware). Подтверждением этому служат как частичный перенос криминалитетом сферы своих интересов в киберпространство, так и официальное принятие и использование развитыми государствами концепции сетецетецентрической войны.

Задача противодействия современным кибератакам характеризуется наличием большого объема неупорядоченных, а зачастую и противоречивых данных, которые должны быть обработаны как заблаговременно, так и по мере возникновения инцидентов. Это объясняет необходимость в реализации интеллектуальных подходов к анализу данных, позволяющих своевременно оценить обстановку и принять решение на отражение атаки. Дисциплина машинного обучения (Machine Learning, ML) представляет ряд полезных методов и практик, облегчающих решение этой задачи.

К наиболее важным следует отнести:

1) методы обучения с учителем, традиционно связанные с задачей классификации, применяемой для поиска вредоносного программного обеспечения по некоторым предварительно выделенным наборам признаков;

2) методы обучения без учителя, решающие задачу кластеризации, позволяющую выявлять новые паттерны сокрытия уже известных атак, новые атаки, и методы их реализации.

Обзор публикаций, посвященных теме обнаружения и категоризации malware, показывает, что исследовательская деятельность в данном направлении в основном нацелена на решение следующих вопросов:

1. Поиск признаков, способных наиболее адекватно отражать структурные, функциональные и другие аспекты вредоносных и безопасных приложений и их отдельных групп;
2. Поиск отдельных методов машинного обучения и их комбинаций, обеспечивающих наиболее точные результаты выполнения задач обнаружения и категоризации malware;
3. Анализ и проектирование систем обнаружения и категоризации, отвечающих отдельным требованиям, предъявляемым к существующим системам обнаружения вредоносного программного обеспечения.

Следует отметить, что подавляющее большинство работ не нацелено на формирование полного методологического базиса решения данной задачи, что подчеркивает отсутствие единого взгляда на проблему обнаружения malware обеспечения средствами ML. Это часто приводит к появлению решений, ценность которых является ограниченной в силу сложности их практического внедрения и несоответствия стандартам, предъявляемым к существующим системам данного класса. С точки зрения авторов, причинами этого являются:

1. Отсутствие формального описания требований к подобным системам;
2. Отсутствие обоснованных взаимосвязей данных требований с основными процессами, формирующими базис дисциплины машинного обучения;
3. Отсутствие четкой и полной онтологии основных групп используемых признаков и применимых методов анализа.

Данная работа посвящена комплексному анализу выделенных проблем и призвана обозначить основные вехи в общем процессе проектирования систем обнаружения вредоносного программного обеспечения на основе методов ML. Исследования в контексте данной работы производятся на базе четко детерминированных требований к системам обнаружения и категоризации malware. При этом основное внимание уделяется вопросам оперативности процессов обслуживания систем данного класса и точности принятия ими решений. В настоящее время проводится анализ указанного набора требований применительно к общей методологии машинного обучения и обозначаются основные задачи, требующие решения. В частности, показывается важность задач оптимизации процедур обучения и устранения ошибок, требующих более глубокого изучения свойств методов ML и природы используемых признаков. Полученный перечень задач позволяет по-новому взглянуть на текущее состояние дел в затронутой предметной области и обозначает направления перспективных исследований. Работа выполнена при финансовой поддержке РФФИ (проект №10-01-00826), программы фундаментальных исследований ОНИТ РАН (проект №3.2), государственного контракта 11.519.11.4008 и проектов Евросоюза SecFutur и MASSIF, а также в рамках других проектов.

Корт С.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ПРИМЕНЕНИЕ N-ГРАММ АНАЛИЗА ПОЛЕЗНОЙ НАГРУЗКИ СЕТЕВЫХ ПАКЕТОВ ДЛЯ АНАЛИЗА БЕЗОПАСНОСТИ ВЗАИМОДЕЙСТВИЙ

При передаче данных в сети Интернет существенной с точки зрения безопасности характеристикой являются тип протокола, с использованием которого передаются данные, а также тип полезной нагрузки передаваемых пакетов (бинарное содержимое, текстовое, графическое, шифрованное содержимое и т.п.). Эти характеристики могут быть полезными при обнаружении многих типов сетевых атак. Настоящий доклад посвящен задаче классификации сетевого трафика на прикладном уровне модели OSI ISO, а также ее применению для решения задач, связанных с обеспечением сетевой безопасности.

Под полезной нагрузкой трафика сетевого протокола понимается последовательность байт сетевого пакета без учета заголовка. В отличие от заголовков пакетов сетевых протоколов, полезная нагрузка обычно не имеет фиксированных рамок формата, небольшого количества ключевых слов или ожидаемых значений. Теоретически любой символ или значение байта может оказаться в любой позиции полезной нагрузки. В отличие от заголовков сетевых пакетов, полезная нагрузка в общем случае не имеет фиксированных рамок формата, небольшого количества ключевых слов или ограниченного варианта возможных значений.

Главная проблема методов, исследующих полезную нагрузку, заключается в их сильной чувствительности к потере пакетов и сегментации первой фазы сессии, создание сигнатур протоколов по-прежнему трудоемкая задача требующая достаточно много времени, шифрованный трафик, который делает невозможным доступ к данным прикладного уровня и вычислительные затраты, не позволяющие проводить классификацию на высокой скорости.

В докладе для представления полезной нагрузки используется ее представление в виде n-грамм (под n-граммой понимается последовательность из n соседних байт в блоке полезной нагрузки). Для получения представления полезной нагрузки в виде n-грамм в процессе обучения и классификации через всю полезную нагрузку проходит скользящее окно с шириной n, и подсчитывается появление каждой из n-грамм в пределах окна. Тогда полезная нагрузка может быть представлена вектором признаков, компонентами которого будут оценки относительных частот каждой из n-грамм, которые рассчитываются путем деления количества появления каждой из n-грамм на общее количество n-грамм. Для классификации трафика на основании выборок, полученных в процессе обучения строится алгоритм классификации а, основанный на расстоянии Махаланобиса.

Полученная в результате модель используется для:

А). Распознавание типа протокола. Для каждого моделируемого взаимодействия собиралось примерно по 7000 пакетов. В качестве анализируемых протоколов прикладного уровня использовались следующие протоколы: FTP (управляющий канал на 21 порт), HTTP, POP, SMTP, SSH и telnet. По итогам тестирования типа протокола было корректно распознано 99,16% пакетов.

Б). Распознавание типа полезной нагрузки. Тестирование проводилось на следующих группах файлов: текстовые данные (*.txt); офисные документы ms office 2010 (*.docx, *.xlsx); офисные документы ms office 2003 (*.doc, *.xls); документы формата *.pdf; исполняемые файлы (*.exe) и сжатые данные (*.zip, *.rar). В результате тестирования были корректно распознаны 93% данных.

В). Обнаружение аномалий. На данном этапе работы проводилось исследование для HTTP трафика, как наиболее показательного. Для обучения системы использовались данные дампов трафика 1999 DARPA IDS первой и третей недели, разделенные в соотношение 80% (обучение + калибровка системы) к 20% (тестирование). В качестве второго этапа тестирования был проведен ряд опытов на эксплойтах, использующих уязвимости CVE-2010-0425, CVE-2009-1955 для Apache и CVE-2009-1676 для Microsoft IIS. Атаки были распознаны корректно.

Модель полезной нагрузки показала себя как достаточно простая и эффективная. Также она может быть успешно применена в виде инкрементального метода обучения без учителя. Как оказалось, модель полезной нагрузки очень хорошо решает проблему распознавания типа передаваемой по сети информации: типа сетевого протокола, типа полезной нагрузки протокола и пр. Данная модель (в применении к практической задаче обнаружения атак) может использоваться совместно с другими методами распознавания для снижения количества ложных срабатываний и увеличения количества обнаруженных атак.

Котенко Д.А., Рудакова С.А, Логинов А.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Главное управление Банка России по Санкт-Петербургу

ПРОБЛЕМА МОНИТОРИНГА СОБЫТИЙ ДОСТУПА К ИНФОРМАЦИОННЫМ АКТИВАМ БАНКОВСКОГО ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

Современный подход к обеспечению информационной безопасности (ИБ) банковских платежных систем, предполагает разработку подсистем ИБ (ПИБ) для решения задач управления доступом, регистрации и учета, контроля целостности, защиты информации от воздействия вредоносного кода, кодовой аутентификации, контроля локальной вычислительной сети и управления. В соответствии с существующими требованиями к обеспечению ИБ объектов Банковской системы, ПИБ представляет собой комплекс организационных мер (приказы, регламенты, инструкции) и технических средств защиты информации (сертифицированные системы защиты информации, средства защиты от воздействия вредоносного кода, штатные средства ОС и СУБД). Следует отметить, что одним из основных требований является оптимизация состава комплекса средств защиты информации за счет минимизации количества дополнительных программно-аппаратных средств, расширяющих штатные функции защиты ОС и СУБД.

На этапах технического проектирования ПИБ, учитывая сложность банковских технологических процессов и критичность информационных активов, возникают нетривиальные задачи, связанные с выполнением предъявляемых требований к обеспечению ИБ. Одной из таких задач, возникающих в рамках разработки подсистемы регистрации, является фиксация событий доступа к информационным активам в БД и анализ электронных журналов аудита с использованием штатных средств ОС и СУБД. Следует отметить, что современные СУБД предоставляют широкие возможности по ведению аудита, однако в условиях разделения ответственности и полномочий персонала связанного с администрированием БД и ПИБ, необходим соответствующий механизм, позволяющий администраторам ПИБ осуществлять как контроль доступа пользователей автоматизированной системы к БД, так и фиксацию и анализ событий доступа администраторов БД к информационным активам. Очевидно, что факт наличия неограниченных полномочий учетных записей администраторов в СУБД накладывает определенные сложности по контролю их действий.

Предлагается механизм контроля доступа к информационным активам, позволяющий с использованием встроенных средств аудита СУБД, утилит ОС и сетевых технологий осуществлять

регистрацию в СУБД в соответствии с требованиями внутренних документов организации Банковской системы, сведений о запускаемых программах (процессах, задачах), дате и времени запуска, попытках доступа к информационным активам, идентификаторах субъектов доступа, результатах попыток доступа, видах запрашиваемых операций и т.п.

Предложенный способ позволяет администраторам ПИБ централизовано контролировать события доступа к информационным активам пользователей автоматизированной системы и администраторов, обладающих неограниченными полномочиями по модификации объектов БД, с использованием штатных средств СУБД и ОС.

Котенко И.В., Саенко И. Б., Полубелова О.В., Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕТОДЫ И СРЕДСТВА ПОСТРОЕНИЯ РЕПОЗИТОРИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ В КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ

Управление информацией и событиями безопасности (SIEM – Security Information and Event Menegement) считается новой и достаточно быстро развивающейся технологией в области защиты информации. Центральным компонентом SIEM-системы является репозиторий, или информационное хранилище, в котором хранятся данные о событиях, правилах и инцидентах безопасности. Задача построения репозитория является ключевой для SIEM-системы. Особую значимость данная задача приобретает в критической информационной инфраструктуре, где учитываются не только традиционные события безопасности компьютерной инфраструктуры, но также параметры безопасности физического уровня.

Для разработки архитектуры репозитория SIEM-системы был проведен анализ стандартов в области управления событиями (Common Event Expression, Common Base Event, XDAS, CIM и других), наиболее известных реализованных SIEM-систем (OSSIM, AccelOps, Qradar, Splunk, Prelude, ArcSight и других), а также требований в части состава и структуры хранимых данных и механизмов их обработки, выдвигаемых со стороны отдельных сценариев применения SIEM-системы. В результате был сделан вывод, что наиболее приемлемым стандартом является стандарт CIM. Данный стандарт может быть положен в основу создания модели данных верхнего уровня.

Для обоснования выбора языка внутреннего представления данных, содержащихся в репозитории, был проведен обзор ряда XML-ориентированных языков, которые можно использовать для доступа, обработки и логического вывода данных в репозитории. К числу таких языков были отнесены: Web Ontology Language (OWL), Semantic Web Rule Language (SWRL), SPARQL Protocol and RDF Query Language (SPARQL), Event calculus, SPIN и другие. Данный анализ привел к выводу, что эти языки могут быть использованны при применении онтологического подхода.

Для построения архитектуры репозитория предлагается метод, базирующийся на использовании сервис-ориентированной архитектуры (SOA). Основными принципами SOA, применяемыми для построения репозитория, являются: множественное использование сервисов, однородная безопасность, интеграция с процессом программирования, использование открытых стандартов, независимость от местоположения компонентов, высокая управляемость.

Согласно принципами SOA, архитектура репозитория может быть разделена на три базовых уровня: уровень доступа к данным, уровень презентации данных и уровень реализации сервисов. Уровень доступа к данным интерпретирует запросы на поиск данных от клиентских приложений во внутренний язык, используемый СУБД. Уровень презентации данных охватывает все, что связано с взаимодействием с системой. Уровень реализации сервисов позволяет абстрагировать взаимодействие между двумя и более объектами, потоками и сервисами через промежуточный интерфейс API, предоставляемый менее детализированным сервисом.

В предлагаемой архитектуре репозитория выделяются два типа баз данных: кратковременного хранения и длительного хранения. В базе данных кратковременного хранения содержится детальная информация обо всех событиях безопасности, поступивших в репозиторий. В базе данных долговременного хранения содержатся обобщенные данные, а также формализованное представление на внутреннем языке правил политик и инцидентов безопасности, которые используются для получения логического вывода.

Вместе взятые, эти базы образуют слой хранения данных репозитория. Другой функциональный слой представляет собой набор различных услуг, которые выполняются по отношению к хранимым данным.

Для выбора программно-инструментальных средств построения репозитория был проведен анализ СУБД следующих классов: традиционного класса реляционных СУБД, XML-ориентированных СУБД (BaseX, Apache XIndice и других) и хранилищ триплетов (4store, BigData, BigOwlim, TDB и Virtuoso). В результате был сделан выбор в пользу сервера программной системы Virtuoso, которая рационально сочетает в себе возможности всех трех классов СУБД.

Программный макет репозитория, выполненный с использованием Virtuoso, был протестирован для хранения и обработки данных, используемых в модуле анализа и моделирования атак на

критически важную информационную инфраструктуру. Результаты тестирования подтвердили правомерность принятых решений по выбору и использованию методов и средств построения репозитория SIEM-системы.

Работа выполняется при финансовой поддержке РФФИ (проекты 10-01-00826-а и 11-07-00435-а), программы фундаментальных исследований ОНИТ РАН (проект 3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

Львович Я.Е., Яковлев Д.С.
Россия, Воронеж, Воронежский институт высоких технологий

СОВРЕМЕННЫЕ СТАНДАРТЫ В ОБЛАСТИ УПРАВЛЕНИЯ РИСКАМИ

Общеизвестно, что стандартизация является основой всевозможных методик определения качества продукции и услуг. Одним из главных результатов подобной деятельности в сфере систематизации требований и характеристик защищенных информационных комплексов стала Система международных и национальных стандартов безопасности информации, которая насчитывает более сотни различных документов.

В настоящее время стандарты в области управления информационной безопасностью находятся в стадии развития. Это касается как международной, так и российской практики. В 2000 году был принят международный стандарт ISO IEC 17799, содержащий практические правила управления информационной безопасностью для произвольных систем. В 2005 году разработан международный стандарт ISO IEC 27001, который определяет требования к построению систем менеджмента информационной безопасности и определяет методы защиты информации. Этот стандарт дополняет и расширяет существующий стандарт ISO IEC 17799.

В России данный стандарт ISO IEC 17799 введен в действие с 1 января 2007 года в виде национального стандарта ГОСТ Р ИСО/МЭК 17799-2005, а стандарт ISO IEC 27001 соответственно как ГОСТ Р ИСО/МЭК 27001-2005. Таким образом, налицо небольшое отставание в области внедрения стандартов управления информационной безопасностью в нашей стране.

В данный момент времени в разработке находятся несколько международных стандартов серии ISO IEC 27000. В частности разрабатываются следующие стандарты: ISO IEC 27003. Руководство по внедрению системы управления информационной безопасностью, ISO IEC 27004. Измерение эффективности системы управления информационной безопасностью.

Разработка этих стандартов чрезвычайно важна для внедрения методов мониторинга и управления рисками информационных систем, поскольку они должны отражать методы оценки рисков и принятие решений на основе этих оценок.

Также с точки зрения оценки и управления рисками информационных систем стоит отметить руководящий документ ФСТЭК России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий».

Недостаток отечественной нормативной базы в области информационной безопасности состоит в отсутствии российского ГОСТа по управлению информационными рисками.

Подводя итог, отметим, что практически не существует информационных систем, которые не подвергались бы риску. Осуществляемые мероприятия защиты не могут устранить риск полностью, они предназначаются для снижения уровня риска.

Ляпидов К.В.
Россия, Самара, Самарский государственный университет

ПРЕДЛОЖЕНИЯ ПО ПОВЫШЕНИЮ УРОВНЯ БЕЗОПАСНОСТИ РАСЧЁТНЫХ ПЛАСТИКОВЫХ КАРТ

На сегодняшний день, в связи с широким распространением расчётных пластиковых карт, всё более серьёзно встаёт проблема их защиты от взлома. По подсчётам специалистов ежегодный ущерб мировой экономике от действий интернет-мошенников (кардеров), ворующих деньги с виртуальных счетов, кредитных и дебетовых карт, а также других платёжных систем, с каждым годом растёт и приближается к 100 миллиардам долларов США. Об актуальности данной проблемы свидетельствует ещё и тот факт, что на долю электронных денег приходится около 90% от общей денежной массы.

В настоящее время существует два основных типа расчётных пластиковых карт: карты с магнитной полосой (традиционная) и карты со встроенной микросхемой (смарт-карты). Основное различие этих двух типов заключается в принципе шифрования данных о счёте. На традиционных картах сведения зашифрованы на магнитной полосе, что делает их крайне уязвимыми, т. к. карты с магнитной полосой легко поддаются копированию при помощи специального устройства – скиммера (устройство для считывания информации с карты). Кроме того, карта с магнитной полосой всегда имеет одинаковые идентификационные данные, которые передаются в банк-эмитент. В связи с этим существует возможность их перехвата и изготовления поддельной карты.

В отличии от карт с магнитной полосой, в смарт-картах используется более сложный алгоритм шифрования и каждая транзакция подтверждается специальным одноразовым кодом, т.е. для проведения каждой следующей транзакции требуется новый код. Таким образом, использование данных для уже прошедших транзакций становится бессмысленным. Создание дубликата смарт-карты на сегодняшний день практически невозможно. В настоящее время смарт-карты являются единственной действенной защитой от различных форм скимминга.

Несмотря на очевидные преимущества смарт-карт, в России ни один банк их не выпускает. Связано это с отсутствием полноценной инфраструктуры по их приёму. Альтернативой на сегодня являются комбинированные карты, имеющие как микропроцессор, так и магнитную полосу. Несмотря на универсальность комбинированных карт, они имеют все недостатки карт с магнитной полосой, в связи с этим рассматривать их следует только как переходную форму к полноценным смарт-картам.

Одним из самых распространённых способов в последнее время становится оплата товаров и услуг через Интернет, однако этот способ является также и одним из самых опасных с точки зрения надёжности. Связано это с тем, что при проведении транзакции невозможно полностью идентифицировать законного держателя карты. Идентификация в большинстве случаев осуществляется посредством введения данных, указанных на карте. Таким образом, кардер, скопировав информацию с карты (посредством скиммера) или зафиксировав её данные посредством видеокамеры (или иных устройств), получает возможность от лица законного держателя карты производить оплату товаров и услуг в своих корыстных целях.

Внедрение в российском сегменте Интернета 3-D Secure – технологии аутентификации владельца карты в режиме on-line при проведении платежей через Интернет, позволяет исключить вероятность проведения незаконной транзакции. В основе безопасности 3-D Secure лежат следующие положения:

– проверка личности владельца карты в реальном времени посредством специального пароля, известного только законному держателю карты и банку-эмитенту;

– защита результатов проверки путём использования цифровой подписи;

– защита конфиденциальной информации пользователя посредством использования защищённых страниц платёжного сервера.

Учитывая всё вышесказанное, с целью повышения надёжности, предлагается введение обязательного подтверждения о проведении транзакции по магнитной и комбинированной пластиковой карте при помощи SMS-оповещения на сотовый телефон держателя карты. Таким образом, все движения по счёту будут всегда контролироваться как со стороны банка-эмитента, так и со стороны держателя карты. Введение дополнительных сервисов для комбинированных карт позволит в более сжатые сроки создать инфраструктуру для полноценных смарт-карт.

Наиболее перспективной на сегодняшний день является технология PayPass, она позволяет проводить экспресс оплату, прикладывая карту к специальному считывающему устройству (терминалу). Данная технология уже довольно долго и успешно используется в странах Европы и США.

Несмотря на относительно высокую стоимость технологии 3-D Secure, необходимость её внедрения в российский сегмент Интернета очевидна. Внедрение технологии 3-D Secure также позволит увеличить объёмы электронной коммерции, кроме того, она закладывает перспективы развития универсальной коммерции т.е. проведения коммерческих операций с любого устройства, в любое время и из любой точки, практически исключая проведение незаконных транзакций.

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

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ МОДЕРНИЗАЦИИ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ СИСТЕМЫ

В основе модернизации организационно-технической системы (ОТС) лежит технология реинжиниринга бизнес-процессов. Эта технология учитывает совместную эксплуатацию элементов «старой» и «новой» ОТС, многоструктурность и динамику изменения этих структур на всех этапах жизненного цикла изделия.

Основные проблемы и факторы, сдерживающие распространение и использование реинжиниринга, связанны с его начальной стадией – построением представлений унаследованной (модернизируемой) ОТС.

Методика модернизации структуры и функционирования ОТС или корпоративной информационной системы должна учитывать сохранность данных, циркулирующих в информационной среде.

Различные элементы системы связаны сетью. Отсюда вытекают условные уровни, нуждающиеся в защите:

– сетевая безопасность,

– безопасность баз данных,
– безопасность на уровне сервера приложений,
– защита информации на клиентском компьютере.

Безопасность сетевой инфраструктуры может обеспечить шифрование трафика и аутентификация пользователя на основе цифровых сертификатов.

Сервер баз данных необходимо изолировать программно и физически от общей компьютерной сети. У пользователей не должно быть прямого доступа к базе данных, а только через сервер приложений.

Сервер приложений помимо обработки данных обеспечивает авторизацию пользователя. Учетная запись пользователя вместе с именем и паролем должна содержать роль, то есть полномочия, которые допускают пользователя к тем или иным данным.

Рабочее место – клиентский компьютер также необходимо обеспечить защитой. Для удобства пользователя, чтобы не запоминать различные пароли необходимо использовать единый вход в систему (одинаковые имя и пароль для операционной системы и информационной системы). Необходима система электронных ключей – отдельное запоминающее устройство с паролем. В случае кражи ключа злоумышленник не будет знать пароль и, наоборот, выкрав пароль, без ключа он не сможет войти в систему. Также можно использовать программы, контролирующие устройства ввода/вывода информации. Для непрерывной работы корпоративной информационной системы необходимо разработать стратегию резервного копирования данных, горячей замены оборудования и др.

При разработке методики модернизации организационно-технической системы необходимо учесть указанные рекомендации по обеспечению сохранности данных, циркулирующих в системе.

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

К ВОПРОСУ О ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ АВТОМАТИЗИРОВАННОМ ПОСТРОЕНИИ ТЕЗАУРУСА ТЕКСТОВОЙ ИНФОРМАЦИИ

Тезаурус (от греч. thesuarus «сокровище, сокровищница») – упорядоченный перечень терминов, в котором отражены семантические отношения между ними, каждому отношению приписывается явно указываемый тип.

При разработке тезауруса необходимо учесть тот факт, что информация, содержащаяся в нем, может быть доступна по сети большому числу пользователей. Для обеспечения целостности и сохранности информации, необходимо разработать меры безопасности.

Применение тезаурусов является классическим методом в задачах информационного поиска и началось до применения автоматизированных систем в этой области. В информационной системе тезаурус является не только самостоятельным информационным ресурсом, но и инструментом для классификации или индексации ресурсов.

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

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

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

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

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

Мульганов С.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций

ОЦЕНКА ИНФОРМАЦИОННЫХ ПОТЕРЬ ПРИ ПЕРЕДАЧЕ СИГНАЛОВ ПРИ НАЛИЧИИ ПРОПУСКОВ

Хорошо известно, что при расчете пропускной способности канала связи всякий перерыв в приеме сигнала вызывает, вообще говоря, потерю части полезной информации. В количественном смысле такую потерю можно оценивать, сравнивая энтропию исходного сигнала S(A) с энтропией сигнала после «вырезания» окон пропускания S(B). Такие окна могут иметь естественное происхождение (например, грозовые разряды), носить и производственный характер (например, многолучевое распространение сигнала), но могут иметь и антропогенное происхождение как неосознанное, так и умышленное (например, подавление сигнала, наведение шумов и т.д.).

При передаче сигнала на значительное расстояние необходимо учитывать тот факт, что сигнал имеет свойство затухать. При этом при небольших амплитудах исходного сигнала, местами в полезный сигнал сливается с фоновым шумом. В этом случае использование цифрового сигнала имеет преимущество в том, что он состоит из дискретных значений, а значит его легко обнаружить и регенерировать.

Разность S(A)-S(B), в отсутствии подключения посторонней информации, определяет величину потерянной информации. Для соответствующей оценки приведем сравнительно простой пример в условиях, когда исходный сигнал представляет собой не просто набор независимых импульсов (тогда они безвозвратно терялись бы в окне пропускания), а цепь Маркова, в которой из взаимной зависимости импульсов возможно частичное восстановление последних. Зависимость импульсов в цепи Маркова – один из факторов информационной безопасности.

Передаваемые для различных цепей длительные сигналы часто можно рассматривать как стационарные случайные процессы. В дальнейшем мы будем постоянно подразумевать дискретное время и какое-либо раз и навсегда заданное конечное множество состояний. При таких условиях, как известно, для заданного процесса A существует как энтропия Sn{A} его отрезка из n звеньев, так и предел в виде удельной энтропии.

Данная статья посвящена такой схеме передачи A как сигнала, при которой он не проходит в первоначальной форме, а вместо этого отдельные участки целиком выпадают. Мы останавливаемся на частной схеме, когда чередуются участки из m звеньев, не подверженные искажениям, с участками из l звеньев, полностью теряющимися (можно, например, представлять, что все эти звенья заменяются нулями).

Для полученного сигнала с пропусканиями, обозначаемого как B, также можно определить как энтропию Sn{B} достаточно длительного отрезка, так и удельную энтропию.

Очевидно, процесс B получается детерминированным функциональным преобразованием. В таких случаях всегда $Sn\{B\} \le Sn\{A\}$ и в пределе аналогичное неравенство справедливо и для удельной энтропии. При этом разность удельных энтропий исходного и полученного сигнала естественно трактовать как информацию, потерянную при переходе от процесса A к процессу B, также в расчете на одно звено.

Если же процесс A, кроме стационарности, к тому же обладает еще и свойством марковости, то в результате получается общая закономерность: доля потерянной информации из стационарного процесса с произвольной корреляцией его звеньев не превышает доли времени с замираниями.

Этот вывод верен лишь асимптотически для длинных сигналов, и во всей работе предполагается отсутствие налагающихся помех, иначе исходное утверждение о разности удельных энтропий исходного и получаемого сигналов становится несправедливым.

Нестерук Ф.Г.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ОСНОВНЫЕ ЭТАПЫ РАЗРАБОТКИ АДАПТИВНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Механизмы обеспечения информационной безопасности современных информационных технологий (ИТ) далеки по возможностям от биологических прототипов, поэтому разработка адаптивных ИТ-систем, основанных на биосистемной аналогии, представляется актуальной.

Автором предложена технология разработки адаптивных систем защиты информации (СЗИ), в основу которой положен биосистемный принцип представления функций в виде структур, каждая из которых описывается как взаимосвязанная совокупность элементов:

– Структура системы ИТ представляется в виде иерархии топологий, выполненных с различной степенью детализации, что позволяет производить анализ и защиту информационных потоков на различных уровнях иерархии ИТ-системы.

– Функциональным блокам структуры системы ИТ соответствуют командные пакеты, информационным потокам – пакеты данных и т.д.

– Использование для представления информационных потоков, соответствующих различным уровням детализации, различного кодирования при представлении пакетов данных позволяет разграничить и упростить контроль целостности информационных потоков.

– Описание информационной структуры ИТ-системы с помощью графического языка дает возможность представить иерархию топологий ИТ-системы в едином виде – как совокупности командных пакетов различной функциональной мощности, ориентированных на пакеты данных для передачи сообщений различного объема.

– Формирование структуры адаптивной СЗИ в соответствии с топологией системы ИТ. В зависимости от степени детализации структуры ИТ-системы разрабатывается иерархическая адаптивная СЗИ, на разных уровнях которой используется соответствующая совокупность механизмов защиты.

– Размещение уровней адаптивных классификаторов в структуре СЗИ. В иерархии адаптивных СЗИ, соответствующей уровням ИТ-системы, необходимо присутствие средств интеллектуального анализа данных на каждом из иерархических уровней, а именно, экспертных систем, систем нечеткой логики и нейронных сетей.

– Формирование базы знаний экспертных систем в виде правил логического вывода для каждого из уровней адаптивных классификаторов структуры СЗИ. На каждом из уровней ИТ-системы используются знания специалистов о механизмах и средствах обеспечения конфиденциальности, целостности и доступности информации, соответствующей данному иерархическому уровню. Знания представляются в виде систем правил логического вывода.

– Формирование базы данных в виде экспертных или статистических оценок для каждого из уровней адаптивных классификаторов структуры СЗИ с целью определения достоверности каждого из правил логического вывода базы знаний. Как правило, используются методы байесовских рассуждений или факторов уверенности.

– Расчет интегрального показателя качества адаптивной СЗИ, используемого в качестве целевой функции для оптимизации как структуры СЗИ, так и топологии системы ИТ, производится с учетом оценок достоверности каждого из правил логического вывода базы знаний и специфики иерархических уровней ИТ-системы.

– Отражение баз знаний соответствующих уровней иерархии СЗИ в информационных полях нейронных сетей с целью их последующего обучения и коррекции. Известно, что обучение нейронных сетей (коррекция их информационных полей) производится по достаточно простым алгоритмам.

– Коррекция баз знаний и данных в процессе функционирования системы ИТ с использованием механизмов адаптации нейросетевых средств. Обучение адаптивных средств классификации, коррекция, классификационные заключения, расширение классификации.

– Оптимизация топологии системы ИТ и структуры адаптивной СЗИ в соответствии с критерием не убывания интегрального показателя качества СЗИ.

Вышеперечисленные этапы охватывают все основные аспекты разработки адаптивных СЗИ, что значимо для будущих исследований.

Следующим этап работы является продолжение моделирования этих этапов.

Работа выполнена при финансовой поддержке Комитета по науке и высшей школе Правительства Санкт-Петербурга, РФФИ (проект №10-01-00826), программы фундаментальных исследований ОНИТ РАН (проект №3.2), государственного контракта 11.519.11.4008 и проектов Евросоюза SecFutur и MASSIF, а также в рамках других проектов.

Нестерук Ф.Г., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

КОМПОНЕНТЫ РАЗРАБОТКИ АДАПТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ КОМПЬЮТЕРНОЙ СЕТИ

Актуальность исследований в области создания адаптивных систем защиты информации (СЗИ) обусловлена ростом сложности современных информационных систем, опережающим рост защищенности сетей от угроз, объёмами финансовых вложений в сферу обнаружения атак, тенденцией интеллектуализации средств защиты и их интеграцией с иными средствами системы защиты информации.

В работе ставится цель практической реализации процесса разработки и оптимизации системы защиты компьютерной сети, способной адаптироваться к динамике угроз путем решения задач формирования структуры СЗИ, в соответствии с топологией сети, размещения уровней адаптивных средств классификации (АСК) в структуре СЗИ, формирования базы знаний (БЗ) в виде правил логического вывода для каждого из уровней АСК, формирования базы данных (БД) – экспертных или статистических оценок для уровней АСК в составе СЗИ, определения интегрального критерия эффективности адаптивной СЗИ – целевой функции для оптимизации системы защиты, коррекции БЗ и БД в процессе функционирования сети с использованием механизмов адаптации нейросетевых

средств, оптимизации адаптивной СЗИ в соответствии с критерием неубывания интегрального показателя качества СЗИ.

Предложена модель адаптивной СЗИ компьютерной сети, в состав которой входят уровни адаптивных средств классификации, каждый из которых включает базу данных для формирования показателей эффективности СЗИ и базу знаний для классификации угроз безопасности сети (представленные нейронной сетью), компонент, позволяющий оптимизировать структуру СЗИ по критерию возрастания рейтинга, методика моделирования процесса разработки адаптивного уровня в среде MATLAB (инструмент Fuzzy logic toolbox), процедура, включающая автоматическое формирование, прореживание и минимизацию нечеткой базы знаний в среде MATLAB.

Детально описана процедура, включающая автоматическое формирование, прореживание и минимизацию нечеткой базы знаний, обеспечивающая следующие возможности:

– извлечение знаний из массива первичной информации посредством двух алгоритмов кластеризации;

– автоматическое формирование нечеткой базы знаний в виде системы конъюнктивных правил в соответствии с моделью нечеткого логического вывода Сугено;

– отображение нечеткой базы знаний на топологию специализированной нейро-нечеткой сети ANFIS;

– коррекция нечеткой базы знаний в процессе обучения нейро-нечеткой сети ANFIS на массиве достоверных данных;

– анализ откорректированной базы знаний в силу логической прозрачности специализированных слоев нейро-нечеткой сети ANFIS.

Предложенная методика прореживания нечеткой базы знаний с учетом минимизации исходных данных посредством карты Карно дает возможность сделать БЗ достаточно компактными, следовательно, быстродействующими, что важно для оперативности адаптивных СЗИ.

Перечисленные возможности достаточны для организации, моделирования, проектирования адаптивных уровней классификации адаптивных СЗИ, базирующихся на использовании только широко распространенного и хорошо зарекомендовавшего себя программного обеспечения.

Работа выполнена при финансовой поддержке Комитета по науке и высшей школе Правительства Санкт-Петербурга, РФФИ (проект №10-01-00826), программы фундаментальных исследований ОНИТ РАН (проект №3.2), государственного контракта 11.519.11.4008 и проектов Евросоюза SecFutur и MASSIF, а также в рамках других проектов.

Пайгусов В.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

DNS С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ

DNS или Domain Name System – это механизм, устанавливающий соответствие между числовыми IP-адресами и текстовыми именами – доменными именами. DNS является одним из широко использующихся элементов инфраструктуры IP-сетей, но в то же время слабо защищённым.

Для подтверждения верности полученной от DNS сервера информации ресолвер (клиент DNS) проверяет лишь IP адрес отправителя, имя, содержашееся в DNS ответе, ID ответа и порт получателя. Подобную информацию просто подделать, что даёт возможность проведения трёх типов атак:

1. Создание собственного DNS сервера, для перехвата запросов;
2. Создание собственного DNS сервера, для создания ложных ответов, при этом ID ответа и номер порта находятся методом перебора;
3. Отравление кэша DNS сервера.

В докладе описаны следующие шаги по устранению уязвимостей:

1. Настройки базовых средств DNS сервера;
   - ограничение на обслуживаемые хосты
   - скрытые версии DNS сервера
   - генерация более сложных ID
2. Настройка операционной системы;
   - запуск DNS сервера в chroot-окружении
3. Использование спецификаций DNSSEC для устранения уязвимостей;
4. Сетевые настройки.

Перервенко А.В.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»

МОДЕЛИ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Облачные технологии или технологии распределенной обработки данных основываются на принципе предоставления доступа по требованию к набору настраиваемых вычислительных ресурсов (процессорное время, оперативная память, дисковое пространство, сетевые каналы, специализированные контроллеры, программное обеспечение и т. д.)

Модель облачных вычислений имеет ряд преимуществ перед традиционной клиент-серверной моделью:

– высокая емкость ресурсов;

– высокая доступность за счет возможности масштабирования ресурсов при изменении нагрузки;

– высокая надежность и обеспечение сохранности данных.

– Концепция облачной обработки данных основывается также на представлении ресурса как услуги и включает в себя следующие модели:

– инфраструктура как услуга (IaaS – Infrastructure as a Service);

– платформа как услуга (PaaS – Platform as a Service);

– программное обеспечение как услуга (SaaS – Software as a service);

– и другие, имеющие в общем случае обозначение XaaS («всё как услуга» – архитектура как услуга, данные как услуга, голос как услуга, безопасность как услуга и т.д.).

Практической реализации идей облачной концепции способствовало развитие технологий виртуализации и рост проникновения широкополосного Интернета. В настоящее время наблюдается стремительное развитие продуктов по модели SaaS и предоставление услуг в соответствии с IaaS и PaaS.

IaaS – предоставление компьютерной инфраструктуры (как правило, в форме виртуализации) как услуги.

Основные компоненты IaaS – аппаратные средства (серверы, системы хранения данных, клиентские системы, сетевое оборудование), операционные системы и системное программное обеспечение (средства виртуализации, автоматизации, основные средства управления ресурсами), связующее программное обеспечение.

PaaS – предоставление интегрированной платформы для разработки, тестирования, развертывания и поддержки веб-приложений.

Поставщик SaaS разрабатывает приложение и самостоятельно управляет им. Потребитель услуги, работая с приложением через Интернет, избегает затрат, связанных с установкой, обновлением и поддержкой работоспособности оборудования и работающего на нём программного обеспечения.

Обычно SaaS рассматривают как развитие модели ASP (Application Service Providing). Отличие состоит в более широкой функциональности и архитектуре приложений, используемых для предоставления услуг. В ASP используются обычные приложения, отличающиеся лишь тем, что размещены они на стороне провайдера, а одному заказчику соответствует одно приложение. В SaaS одно приложение эксплуатируется несколькими клиентами.

Главные отличительные свойства модели SaaS:

– программное обеспечение работает на стороне провайдера;

– модернизация и обновление приложения происходит плавно и прозрачно для клиентов;

– программное обеспечение развёртывается в виде единого программного ядра, с которым работают все клиенты (приложение коммунально);

– условия использования сочетают в себе правила лицензирования и хостинга;

– программное обеспечение предоставляется на условиях аренды и предполагает периодические платежи;

– доступ к программе осуществляется через любой браузер или тонкий клиент;

– программа подстраивается под специфические требования пользователя, а не однократно конфигурируется специальным образом.

Несмотря на очевидные преимущества модели предоставления услуг на основе концепции облачных вычислений, существует ряд ограничивающих факторов, влияющих на более активное ее использование. Одним из таких факторов является проблема обеспечения конфиденциальности информации при обмене, обработке и хранении. Как правило защита информации на стороне провайдера организована на высоком уровне, а стоимость репутационных рисков, связанных с проблемами информационной безопасности достаточно высока. Тем не менее, наиболее продуктивным видится применение эффективных криптографических средств защиты информации, гарантирующих ее конфиденциальность.

Печенкин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ПОСТРОЕНИЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ НА БАЗЕ АРМ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ

В настоящее время сети распределённых вычислений получают всё большее распространение. Эффективность работы во многом зависит от используемой архитектуры сети, от организации взаимодействия узлов и алгоритмов, применяемых для поддержания работоспособности сети. Кроме того, в настоящее время получают распространение сервисы, которые позволяют пользователям выделять мощности своих персональных компьютеров для решения вычислительных задач. На похожей системе построена стремительно развивающаяся виртуальная криптовалюта Bitcoin. Компьютер создает виртуальные монеты (биткоины) путем выделения мощности процессора для решения математической задачи. Каждый раз, когда найдено решение данной задачи, создаются биткоины.

Существующие модели построения сетей распределённых вычислений основываются на статичности сети (добавление и отключение узлов от сети будет происходить не часто), и принимают за основу наличие стабильного канала связи между узлами, что не позволяет применять их в мобильных устройствах. Большинство моделей используют централизованную архитектуру, что требует поддержания отдельных серверов. Необходимо разработать децентрализованную отказоустойчивую многосвязную сеть распределённых вычислений, которая будет подходить для использования в сетях с высокой вероятностью добавления/отключения узлов. Использование такой архитектуры позволит динамически изменять связи между узлами, создавать сети распределённых вычислений без поддержания отдельных серверов, что приведет к улучшению масштабируемости сети. Одинаково легко и без больших финансовых вложений это позволяет объединить как два, три, четыре, так и тысячи компьютеров в единую сеть распределённых вычислений. Кроме того, данный подход позволит объединять разрозненные сети между собой.

Сравнение различных подходов к реализации подобных сетей целесообразно проводить по следующим параметрам:

- цена связей в сети;
- распределение связанности;
- коэффициент кластеризации;
- задержка распространения сообщений по сети;
- надежность доставки сообщения;
- связанность при единовременном отключении нескольких узлов;
- скорость генерации трафика для каждого узла.

Существующие подходы к реализации подобных сетей направлены на их использование в основном в научных целях. При коммерческой реализации они основываются на наличии сервера, что усложняет развёртывание сети. Внедрение такой сети в условиях с нестабильными каналами связи позволит пользователю совместно использовать ресурсы его мобильного телефона, планшетного и домашнего компьютеров, что даст возможность распределять имеющиеся мощности.

Печенкин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ОБНАРУЖЕНИЕ НЕСАНКЦИОНИРОВАННОЙ СЕТЕВОЙ АКТИВНОСТИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Нарушение конфиденциальности в виде кражи информации является одной из основных целей вредоносного программного обеспечения (ПО). Вредоносное ПО внедряется (используя уязвимости или другие способы) на рабочие станции локальной сети, получая доступ к закрытой информации организации. Собрав необходимые данные, вредоносное ПО осуществляет их несанкционированную отправку нарушителю. Для противодействия несанкционированной отправке информации используются сетевые и персональные межсетевые экраны (МЭ).

Недостаток сетевых МЭ заключается в том, что они никак не связаны с действиями пользователя, т.е. не могут отделить активность пользователя от активности вредоносного ПО, установленного на компьютере этого пользователя. Проблемой же персональных МЭ является то, что они функционируют в той же среде, что и вредоносное ПО и имеют столько же возможностей. Если попробовать совместить данные подходы, то получится, что необходимо реализовать персональный межсетевой экран, работающий не на компьютере пользователя.

Для противодействия несанкционированной отправке данных предлагается создание средства обнаружения и предотвращения несанкционированной отправки данных. Данное средство состоит из двух составляющих: монитора действий пользователя и анализатора сетевого трафика. Средство производит мониторинг за действиями пользователя, анализирует сетевой трафик и выявляет несоответствие сетевого трафика действиям пользователя.

Для того чтобы вредоносное ПО не могло изменять результаты мониторинга, необходимо создать такой монитор действий пользователя, на который вредоносное ПО не сможет воздействовать. Для этого монитор действий пользователя должен находиться вне рабочей станции этого пользователя, то есть представлять собой отдельное устройство.

Для мониторинга действий пользователя можно использовать устройства ввода – клавиатуру и мышь. Пользователь использует клавиатуру и мышь, подключенные к промышленному компьютеру (небольшого размера), который и обеспечивает мониторинг. Данный компьютер служит шлюзом для основного компьютера пользователя. Компьютер-монитор принимает все данные, введенные с клавиатуры, и активность мыши, обрабатывает их и передает непосредственно на рабочую станцию по сети. Вредоносное ПО не имеет возможности подменить данные, введенные с клавиатуры, так как она подключена к другому компьютеру.

Компьютер-монитор анализирует данные, введенные пользователем, и отсылает их на анализатор сетевого трафика. Анализатор сетевого трафика выявляет несоответствия между активностью пользователя и сетевым трафиком. Для мониторинга можно использовать и другие методы, например визуальный контроль, то есть мониторинг путем анализа изображения на мониторе пользователя. Наилучших результатов можно достичь использованием всех способов мониторинга действий пользователя одновременно. Отслеживание использования программного обеспечения, событий клавиатуры, мыши, и графической информации, поступающей на монитор, в совокупности, даёт возможность составления чёткого списка действий пользователя без помех для его работы.

Полубелова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПРИМЕНЕНИЕ ЛИНЕЙНОЙ ТЕМПОРАЛЬНОЙ ЛОГИКИ ДЛЯ ВЕРИФИКАЦИИ ПРАВИЛ ФИЛЬТРАЦИИ ПОЛИТИКИ БЕЗОПАСНОСТИ МЕТОДОМ «ПРОВЕРКИ НА МОДЕЛИ»

В рамках решения задачи обеспечения корректности и непротиворечивости правил политики безопасности для систем безопасности решается задача анализа правил фильтрации для выявления аномалий. Под аномалией фильтрации понимается такое противоречие между правилами фильтрации или между правилами и описанием сети, при котором одно или несколько правил никогда не будут активированы. Аномалии в политиках приводят к скрытому игнорированию правил, заданных системным администратором, создавая при этом видимость успешной работы системы защиты. Это может привести к нарушению таких свойств безопасности, как доступность и конфиденциальность. В качестве подхода для решения задачи анализа предлагается использовать метод проверки на модели. Отличием верификации методом проверки на модели от других подходов является возможность использования линейной темпоральной логики (LTL).

Методы «проверки на модели» основаны на переборе состояний, в которые может перейти система в зависимости от запросов пользователей или других подсистем и ответов компонента, принимающего решения о разрешении или отклонении такого запроса. Последовательность действий при переборе зависит от условий, которые сформулированы на языке линейной темпоральной логики и выражают корректные состояния системы. Состояние системы определяется набором значений переменных, а изменение состояния вызывается выполняющимися в ней параллельными процессами. Система рассматривает все возможные последовательности шагов для заданных процессов и сигнализирует о потенциальном некорректном состоянии.

Общая модель, разработанная для верификации правил фильтрации, включает в себя модель компьютерной сети, модель системы безопасности и модель аномалий фильтрации. В работе была использована классификация аномалий Аль-Шаэра, которая включает в себя аномалии затенения, обобщения, корреляции и избыточности.

Для построения формулы введем обозначения следующих свойств: время активации правила R1 (ATR1), время активации правила R2 (ATR2), время деактивации правила R1 (DTR1), время деактивации правила R2 (DTR1), приоритет правила R1 (OrderR1), приоритет правила R2 (OrderR2), привилегия правила R1 (PrivilegeR1), привилегия правила R2 (PrivilegeR2).

Также необходимо сформулировать следующие события, которые реализуются как логические функции, имеющие значение истина или ложь:

– адресный диапазон правила Rn является подмножеством диапазона адресов правила Rm (IsSubset(Rn, Rm));

– адресный диапазон правила Rn является пересечением диапазона адресов правила Rm (IsIntersection(Rn, Rm));

– адресный диапазон правила Rn совпадает с диапазоном адресов правила Rm (IsEqual(Rn, Rm)).

При построении формул использовался темпоральный оператор G, который обозначает, что формула должна иметь значение истины сейчас и всегда в будущем.

По результатам проведенных экспериментов было показано, что предлагаемый подход позволяет выявлять все аномалии в правилах фильтрации политики безопасности, однако имеет экспоненциальную вычислительную сложность в зависимости от количества верифицируемых правил. Таким образом, можно заключить, что предложенная методика может быть применима для малых и средних компьютерных сетей.

В настоящее время продолжается реализация компонентов верификации, служащих для выявления внешних аномалий при работе сети с несколькими межсетевыми экранами.

Кроме того, планируется расширить верифицируемую модель другими категориями политик безопасности, такими как авторизация и защита каналов. Также планируется дальнейшее улучшение системы верификации с удобным для пользователя интерфейсом загрузки первоначальных данных и интерпретацией результатов с использованием графических средств.

Работа выполняется при финансовой поддержке РФФИ (проекты 10-01-00826-а и 11-07-00435-а), программы фундаментальных исследований ОНИТ РАН (проект 3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

Полубелова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

РЕШЕНИЯ ПО РАЗРАБОТКЕ РЕПОЗИТОРИЯ В SIEM СИСТЕМЕ НА ОСНОВЕ ОНТОЛОГИЧЕСКОГО ПОДХОДА

Современные информационные системы, применяемые для управления крупными корпоративными или промышленными системами, формируют огромное количество логов. Анализ этой информации позволяет выявлять различные нарушения безопасности и оперативно на них реагировать. Поэтому автоматизированные системы управления информацией и событиями безопасности (SIEM системы) активно развиваются. Центральным связующим звеном такой системы является репозиторий.

Популярные SIEM-системы как правило базируются на реляционных базах данных, но в настоящее время новым направлением организации управления информацией внутри SIEM-системы является применение онтологического подхода.

Основными преимуществами данного подхода являются:

– слабое связывание и модульность, что облегчает добавление, удаление и поддержку отдельных онтологий;

– компоненты онтологии могут быть динамически объединены во время исполнения для удовлетворения требованиям конкретных приложений.

Потребность выбора онтологического представления данных в SIEM-системе обусловлена тем, что необходимо хранить разнородную информацию, которая может быстро изменяться, выполнять глубокий и разнородный анализ это информации, а также визуализацию в самых разных аспектах. Математический аппарат, положенный в основу систем поиска, основанных на онтологиях, позволяет аналитическим модулям значительно ускорить время, затрачиваемое на выборку информации из репозитория для анализа.

Основные требования, предъявляемые к репозиторию: хранение данных и метаданных, возможность корректировки метаданных, управление данными с различным уровнем детализации, организация параллельного доступа к данным на основе привилегий, поддержка целостности, поддержка версионности, возможность хранения как реляционных данных, так и онтологий.

Для решения организации хранилища был выполнен анализ различных хранилищ, удовлетворяющих заданным требованиям, таких как OpenAnzo, Semantics.Server, Virtuoso, PelletDb, BigOWLIM, AllegroGraph.

В рамках проекта был выбран Virtuoso, благодаря реализации гибридного подхода, мощной документационной поддержки и наличия бесплатной версии. Серверная часть репозитория была реализована с применением технологий web services, spring framework, Java Persistence API, SOAP. Особое внимание уделяется системам логического вывода, позволяющим проводить анализ информации, хранящейся в виде набора триплетов (при онтологическом подходе).

В настоящее время продолжается реализация серверной части репозитория, тестирование скорости доступа к различным хранилищам (реляционной базе данных, хранилищу триплетов), выполнение запросов на различных объемах выборки.

Работа выполняется при финансовой поддержке РФФИ (проекты 10-01-00826-а и 11-07-00435-а), программы фундаментальных исследований ОНИТ РАН (проект 3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

Пунда Д.И.
Россия, Самара, ООО «Наукомп»

ТЕХНОЛОГИЯ СО-УПРАВЛЕНИЯ, КАК КОГНИТИВНАЯ ТЕХНОЛОГИЯ УПРАВЛЕНИЯ СОВРЕМЕННОЙ СЛОЖНОСТЬЮ. ПРИНЦИПЫ И МЕТОДОЛОГИЯ ЕЕ ПОСТРОЕНИЯ

Одним из основных обеспечений информационной безопасности является решение проблем управления сложностью. Современное большое многообразие технологий деятельности общества привело к ощутимому влиянию природных ментальных ограничений на управление этими технологиями. Появилось заметное число сложных в управлении организационных систем (структур регулирования экономики и рынка, крупных и высокотехнологических корпораций…). К влиятельным в деятельности общества сложностям социально-политического, экономического, научно-технического, конъюнктурного, кланового и иного общественно-деятельного характера, сегодня добавилась природная метальная сложность. И в сложных организациях появилась потребность в дополнительной к формальным технологиям и моделям (IT-моделям, нормам, приказам…) технологии управления, «оперирующей с пониманием» тех, кто принимает решения.

И если развитые (и интенсивно развивающиеся) сегодня технологии решения задач, в основном IT, позволяют эффективно управлять любой сложной формализуемой информацией, то управлять не полностью формализуемыми технологиями деятельности человек по природе своего мышления может только ограниченно (например, он не может эффективно управлять «более чем шестью» подчиненными). Хотя его познание и творчество относительно неограниченны.

Для методологии построения технологий управления, снижающих влияние ментальных ограничений на управление нами обобщены-сформулированы основные когнитивные особенности управления:

1. «Эгоистичность» индивидуального управления.
2. Очень высокая чувствительность руководителя к соответствию предлагаемых «кем-то» моделей и суждений его представлениям.
3. Ментальное ограничение управления количеством подконтрольных технологий.
4. Мышление, как его реакция на внутренние и внешние возмущения, предполагает «быстро» чередующуюся смену построений представления и конструирований вариантов его развития.
5. Сложное управление, возникающее с ростом количества подконтрольных технологий, проявляется в резком падении возможностей руководителя моделировать представления и варианты их развития. Оно в первую очередь снижает ментальную возможность построения вариантов развития, а затем возможность моделирования представлений, «картинок» деятельности управляемой организационной системы.

Согласно этим когнитивным особенностям можно сформулировать следующие принципы построения технологии управления: Технология управления может и должна «моделировать мир и понимание конкретной деятельности». Для выполнения требования максимального соответствия представления руководителя и используемых им моделей – моделировать инструментарий должен руководитель. Для уменьшения влияния ментальных ограничений на управление нужно создать такое устойчивое коллективное управление, которое реализует режим «использования стороннего ментального ресурса». Все это требует построения руководителем обеспеченных представлений, как результата создания интегрированных «картин» деятельности с адекватными приоритетами и степенями формализации. В этом случае анализ вариантов развития – управленческих решений, происходит после относительно «полного» построения обеспеченных представлений.

В качестве одной из технологий управления, соответствующих данным принципам, нами предложена технология со-управления. Она основана на разделении ответственности управления на две части – за обеспеченность представлений и за эффективность принимаемых решений, при сохранении всех функций управления для «со-руководителя» и основного руководителя.

Методология построения такой технологии (в поэтапном порядке):

1. Построение формальной модели деятельности предприятия – Заказчика такой технологии, на базе существующих на предприятии моделей и с нашей (Исполнителя) предметной доработкой.
2. Построение «модели мира». Учет внешних связей, моделирование рынка и всех аспектов, касающихся деятельности предприятия. Выбор и укрупнение активных параметров деятельности.
3. Построение структуры конкретной модели деятельности для руководителя.
4. Инженерия. Построение методологии для IT-версий модели и выбор программных средств.
5. Построение IT-версии модели для первого руководителя (его сложного «калькулятора»).
6. Составление регламентов работы и оперативной модернизации модели для руководителя и «модели мира», передача технологии подразделению со-управления предприятия Заказчика.

Программная версия модели деятельности «для первого руководителя» может существенно отличаться от таковой для другого, пусть даже очень похожего предприятия. И отличаться от модели для «вторых» руководителей-замов предприятия (в том случае, если деятельность замов настолько «сложна», что требует создания технологии со-управления не только для первых, но и для вторых уровней управления организации). В первую очередь отличаться из-за различия для них приоритетов

и степеней адекватной (не полной) формализации представлений одной и той же деятельности, с полной ее формализацией в конкретных случаях. По аналогии с тем, что говорит арабская мудрость «У погонщика верблюдов свои планы, а у верблюда – свои».

Пунда Д.И.
Россия, Самара, ООО «Наукомп»

ПОТРЕБНОСТЬ В ПОСТРОЕНИИ ОБЕСПЕЧЕННЫХ ПРЕДСТАВЛЕНИЙ АКТИВНОСТИ ОРГАНИЗАЦИОННЫХ СИСТЕМ, КАК ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данной работе предпринята попытка проанализировать все те основные и присутствующие сегодня на рынке интеллектуальные технологии обеспечения управления, которые в той или иной степени можно отнести к «инструменту для руководителя». И анализируются их возможности и недостатки в решении современных проблем управления сложностью, и объективные тенденции развития технологий обеспечения управления современными сложными организационными системами. Рассмотрены современные возможности и потребности в построении обеспеченных представлений деятельности (в тех формах и содержании, которые сформировались и доступны сегодня «как результатов длительного развития человеческого мышления от незнания к меньшему незнанию»). В части анализа интеллектуальных технологий обеспечения управления речь идет об интегральных IT-технологиях информационно-коммуникационного обеспечения, о концептуальном проектировании и IT-инженерии, о сетевых технологиях, об интегральном моделировании и СППР (системах поддержки принятия решений), об оптимизационных технологиях, о коллективных и психологических методах управления, об управленческом консалтинге.

Особенность современного кризиса (2008-2011) состоит в том, что кроме двух основных путей выхода из кризиса, – экономии и внедрения инновационных производственных, организационных, финансовых и иных предметных технологий деятельности, в сегодняшнем кризисе существенное влияние приобрели механизмы перераспределения благ. А именно – сворачиваются социальные программы, казавшиеся ранее обеспеченными экономическим развитием стран, реализуется политика увеличения пенсионного возраста. Кроме этого вводятся дополнительные ограничения или налоги в банковской деятельности в Америке и Европе. Финансовые войны, искусственная инфляция и необеспеченная инъекция денежных масс. Даже символичен призыв американских бизнесменов «поделиться с согражданами половиной личных активов». Доминирование этого третьего варианта выхода из кризиса говорит о существенной необеспеченности принимаемых ранее решений, как об одной из основных причин сложности этого кризиса. Решений в области формирования норм регулирования рынка и в предметном управлении-регулировании экономики в целом (как рост отставания норм регулирования в банковской, фондовой, монопольной и иной сверхприбыльной деятельности). Или в области выплат по социальным Программам. Или в части планирования необеспеченной деятельности крупных частных и смешанных компаний…. В этом смысле современный кризис является кризисом управления.

Технологии из разряда «инструмент для руководителя» занимают малую часть общего рынка интеллектуальных технологий, – они в среднем мало востребованы. Они обычно моделируют для руководителя детерминируемую часть деятельности, превращаясь в технологии для исполнителя, либо создаются в таких формальных концепциях, которые не всегда соответствуют пониманию реально существующего процесса управления, т.е. «пониманию руководителя об управлении».

Проведенный нами анализ современных, широко предлагаемых и используемых на практике технологий обеспечения управления, с учетом практических знаний, полученных при выполнении нами Проектов «создания инструментов для руководителя», показал, что современное управление сложностью требует разделения организационных систем на относительно простые и сложные в управлении организации. И если для управления сложностью, не связанной с влиянием на него ментальных ограничений, принципиально достаточно формальное информационное обеспечение, то для снятия этого влияния необходимо создание обеспеченных представлений деятельности.

Понятие «обеспеченный», так же как и понятия «порядок» или «определение», относится к основополагающим понятиям. Для него приемлемы такие характеристики, как: однозначность, не избыточность, всеобъемлющее, соответствие практике, возможность и тому подобные.

Обеспеченность представлений предполагает построение содержательно адекватных интегральных представлений знаний (в «пространстве и времени»). С адекватно расставленными приоритетами. С адекватной степенью формализации, так как «недостаточная формализация» приводит к многовариантности (неопределенности) там, где ее не должно быть, а «излишняя формализация» дает единственное определенное развитие там, где возможны многие варианты, то есть где развитие не определено. Обеспеченные представления должны соответствовать возможностям их восприятия, – с учетом наших ментальных и технических возможностей.

Построение обеспеченных представлений требует интеграции научных и прикладных знаний и возможностей. Но требует не их суммирования и согласования (так называемой конвергенции наук и

прикладных методологий, которая при современном многообразии видов знаний не реальна). А, на наш взгляд, требует построения конкретных интегральных методов и технологий, на их основе.

Таким образом, в построении обеспеченных представлений нужны такие технологии, которые увеличивают индивидуальные возможности управления, снимают или уменьшают влияние ментальных ограничений, оперируя не полностью формализованным пониманием деятельности.

Саенко И.Б., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

УСОВЕРШЕНСТВОВАННЫЙ ГЕНЕТИЧЕСКИЙ АЛГОРИТМ ДЛЯ РЕШЕНИЯ ЗАДАЧИ «ИЗВЛЕЧЕНИЯ РОЛЕЙ» В RBAC-СИСТЕМАХ

Задача «извлечения ролей» (Role Mining Problem – RMP) достаточно хорошо известна в области построения систем ролевого разграничения доступа (RBAC-систем). Сущность этой задачи заключается в нахождении матриц «субъекты-роли» (CP) и «роли-объекты» (PO) при заданной матрице «субъекты-объекты» (CO) и принятом критерии оптимизации. Чаще всего таким критерием является требование минимизации количества ролей. Задача RMP относится к NP-полным задачам. Для ее решения предложено много различных подходов: графовый, вероятностный, кластерный, семантический и другие. Однако все они имеют определенные ограничения в своем применении.

Авторами был предложен другой подход, основанный на применении генетического алгоритма (ГА). Однако разработанный ранее авторами ГА, несмотря на достаточно высокую точность решения оптимизационной задачи, обладал низкой сходимостью при высоких размерностях задачи. Поэтому целью настоящей работы является усовершенствование предложенного ранее ГА в направлении существенного снижения его вычислительной сложности.

В разработанном ранее ГА был предложен ряд существенных новшеств, которые касаются практически всех аспектов работы ГА. Например, каждая особь в популяции ГА имела не одну, а три хромосомы. Две из них отображали матрицы CP и PO, причем генами хромосом являлись столбцы данных матриц. Третья матрица отображалась битовой строкой и являлась управляющей. Она показывала, какие из ролей являются активными либо пассивными. Под пассивной ролью понималась роль, формально присутствующая в схеме RBAC, но не имеющая никаких связей с субъектами и с объектами.

Наличие управляющей хромосомы изменяло традиционной содержание базовых операций ГА – скрещивания и мутации. При выполнении первой операции вначале выполнялось скрещивание родительских управляющих хромосом и определение состава активных и пассивных ролей. В соответствии с эти результатом затем подвергались скрещиванию хромосомы, отображающие матрицы CH и PO. Гены, которые в полученных матрицах соответствуют пассивным ролям, обнулялись.

При выполнении мутации также вначале подвергалась случайной модификации третья хромосома. Затем осуществлялась мутация генов первых двух хромосом. Гены пассивных ролей в завершении данной операции обнулялись.

Разработанный авторами ГА, содержащий указанные выше особенности, обладал высокой точностью решения задачи оптимизации. Однако большое количество хромосом являлось причиной, из-за которой при высоких размерностях задачи вычислительная сложность алгоритма начинала значительно возрастать. Поэтому в основу усовершенствования ГА было положена идея уменьшения числа хромосом.

Для этой цели было предложено внесение в разработанный ранее ГА следующих модификаций:

1. Отказ от управляющей хромосомы и объединение двух оставшихся хромосом в одну, которые являются строками переменной длины и содержат не столбцы матрицы, а более сложные объекты;
2. Обновление базовых операций кроссовера и мутации в соответствии с новой формой хромосом;
3. Использование дополнительной обработки дочерних хромосом после выполнения базовой операции кроссовера.

Для реализации базовой операции селекции была слегка модифицирована функция пригодности. Получившаяся в результате функция позволяет при отборе оставлять в популяции особи, имеющие, во-первых, наименьшее расхождение между требуемой и результирующей матрицами CO, а во-вторых, наименьшее количество ролей в RBAC-схеме. Сравнение матриц CO осуществляется отдельно по случаям «1–0» и «0–1», соответствующим нарушениям свойств конфиденциальности и доступности информации.

Для оценки эффективности применения ГА для решения задачи RMP был проведен вычислительный эксперимент. ГА для RMP был реализован в среде Borland Delphi Enterprise v.7.0. Основная цель оценки заключалась в определении зависимости производительности усовершенствованного ГА от размерности задачи и от специально введенной показателя схемы

RBAC – «ролевой значимости» схемы. Результаты оценки показали, что усовершенствованный ГА обладает более высокой производительностью, чем его предшественник, и может считаться достаточно эффективным средством решения задачи RMP при высоких размерностях.

Работа выполняется при финансовой поддержке РФФИ (проекты 10-01-00826-а и 11-07-00435-а), программы фундаментальных исследований ОНИТ РАН (проект 3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

Саенко И.Б., Полубелова О.В., Агеев С.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

ПРЕДЛОЖЕНИЯ ПО КОНЦЕПТУАЛЬНОМУ МОДЕЛИРОВАНИЮ ПОДСИСТЕМЫ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В ЗАЩИЩЁННЫХ МУЛЬТИСЕРВИСНЫХ СЕТЯХ

Развитие системы административного управления различных министерств и ведомств, имеющих иерархическую структуру уровней управления, характеризуется тенденцией к объединению различных информационных ресурсов в единое информационное пространство предметной области. Одним из основных технических решений, обеспечивающих реализацию этой тенденции, являются защищённые мультисервисные сети (ЗМС). ЗМС обеспечивают реализацию возможностей электронного документооборота, распределённых баз данных и баз знаний, оперативное функционирование информационно-справочных и управляющих систем автоматизированного управления в интересах органов административного управления и т. д.

ЗМС является территориально распределённой гетерогенной телекоммуникационной системой, предоставляющей пользователям набор телематических услуг заданного качества, и создаётся на основе общих для всех ее элементов системных, функциональных и технических принципов функционирования и управления как единая сеть. ЗМС относится к классу больших сложных систем.

Важнейшей проблемой при разработке и функционировании ЗМС является проблема обеспечения защиты пользовательской, управленческой и технологической информации. Функции безопасности информации, управления и связи обеспечиваются службами информационной безопасности. Для их управления применяют автоматизированные подсистемы управления безопасностью ЗМС.

При создании подобных систем необходимо:

1. Провести анализ ЗМС и информационных ресурсов, подлежащих защите;
2. Определить возможные направления эволюционного развития ЗМС;
3. Провести анализ угроз безопасности информации;
4. Осуществить построение модели нарушителя;
5. Определить методы и способы обеспечения защиты информационных ресурсов ЗМС;
6. Провести оценку оперативности, надёжности и устойчивости подсистемы управления защитой информационных и технических ресурсов ЗМС.

Начальным этапом построения подсистемы защиты информации является анализ информационных ресурсов, подлежащих защите, а также исследование ЗМС на предмет выявления особенностей, существенных с точки зрения защиты информации. Основными направлениями исследования ЗМС при этом являются следующие:

– физическое, в рамках которого исследуется топология ЗМС с учетом имеющихся физических средств разграничения доступа;

– техническое, которое предполагает анализ используемых в ЗМС технических (аппаратных и программных) средств;

– функциональное, где анализируется место и роль ЗМС в функциональном процессе и задачи, для выполнения которых предназначена ЗМС;

– организационное, которое предполагает изучение персонала, задействованного в работе ЗМС, и его функциональные обязанности;

– нормативное, предполагающее изучение документов, регламентирующих функционирование ЗМС;

– информационное, в рамках которого осуществляется анализ видов передаваемой информации.

Результаты, полученные на данном этапе, являются основой для реализации всех последующих этапов.

Неотъемлемым этапом создания подсистемы управления безопасностью в ЗМС является рассмотрение возможных угроз безопасности информации, то есть условий и факторов, создающих потенциальную или реально существующую опасность защищаемой информации.

Модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия, возможную деградацию функционирования ЗМС при тех, или иных

воздействиях модельного нарушителя, а также другие характеристики потенциального нарушителя, существенные с точки зрения защиты информации в ЗМС.

Далее следует этап разработки и создания подсистемы мониторинга состояния безопасности ЗМС, который предполагает разработку достоверных оперативных методов мониторинга сетевой безопасности с заданными техническими характеристиками. Как правило, оценка параметров ЗМС по данным мониторинга имеет статистическую природу, поэтому для получения достоверных показателей требуется определённое время.

Таким образом, одними из важнейших задач являются задачи разработки эффективных методов обработки статистик для получения оперативных данных мониторинга состояния ЗМС и построения прогноза состояния ЗМС на время, достаточное для реализации управленческих решений по обеспечению информационной и технической безопасности ЗМС.

Работа выполняется при финансовой поддержке РФФИ (проект 11-07-00435-а).

Саенко И.Б., Шоров А.В., Морозов И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Военная академия связи им. С.М. Буденного

СИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА В ГЕОИНФОРМАЦИОННЫХ СИСТЕМАХ

Использование современных геоинформационных систем (ГИС) в качестве основы построения крупно масштабных информационных систем (ИС), работающих с картографической информацией, тесно связано с проблемой разграничения доступа пользователей к хранимой информации. Однако не стоит при этом забывать, что ГИС может содержать конфиденциальную информацию, требующую разработки соответствующих решений по организации защиты информации от несанкционированного доступа.

В результате возникает необходимость разработки моделей и механизмов разграничения доступа к информации в ГИС. Системы разграничения доступа (СРД) являются необходимым и важным элементом защиты ресурсов в информационных системах. СРД на практике реализуют какую-либо модель, формализующую правила доступа субъекта к объектам.

Наибольшую практическую направленность и ценность имеют две основные модели – это дискреционная и мандатная модели доступа.

Эти модели имеют ряд преимуществ, но не лишены недостатков. Дискреционная модель имеет простую реализацию и логику, существенным недостатком является контроль доступа к объекту, а не потоки информации между ними.

Мандатная модель устраняет недостатки дискреционной модели и предполагает формализацию процедуры назначения прав доступа посредством назначения меток конфиденциальности (классификационных меток), назначаемым субъектам и объектам доступа. Однако «чистое» мандатное управление доступом не различает сущностей (объекты, субъекты), которым присвоен одинаковый уровень безопасности. Поэтому если возникает необходимость более гибкого подхода, мандатная модель применяется совместно с дискреционной.

Достоинством систем мандатного доступа является контроль потоков информации: от объекта к субъекту – чтение, и от субъекта к объекту – запись. Это позволяет предотвратить возможность несанкционированного понижения ценности информации. Кроме того, с помощью мандатных моделей возможно существенное упрощение задачи администрирования в масштабных ИС как исходной настройки, так и последующего включения в схему администрирования новых объектов и субъектов доступа.

На сегодняшний день существует небольшой ряд систем реализующих мандатный контроль доступа. Так, отечественная разработка компании РЕЛЭКС – СУБД Linter – реализует полноценный мандатный доступ.

Информация ГИС хранится в базе данных ИС, следовательно, СРД должна контролировать все потоки информации между субъектами доступа и базой данных через все точки доступа. Доступ к этим данным необходимо разграничить так, чтобы каждый пользователь видел только то, что ему предназначено и мог наносить только те объекты, к которым имеет доступ.

Решение данной задачи заключается в следующем: необходимо разграничить доступ субъектов к объектам в соответствии с «ролью» (должностным предназначением), а объекты распределить по слоям таким образом, чтобы количество слоев было минимальным. Решение данной задачи позволит в первую очередь исключить дублирование объектов в базе данных, введения ложной информации в обход мандатной модели доступа.

Для решения данной задачи предлагается использовать подход, связанный и применением генетических алгоритмов оптимизации. Суть данного подхода заключается в следующем. Вначале, в результате формализации исходных данных и переменных, математическая постановка задачи сводится к задаче целочисленного (булевого) математического программирования. Задача имеет две булевы матрицы переменных. Переменные первой матрицы определяют принадлежность картографических объектов к тому или иному слою оперативной обстановки, нанесенной на

цифровой карте. Переменные второй матрицы определяют доступность пользователей ГИС к тому или иному слою. Целевая функция задачи дает оценку степени соответствия текущей итоговой схемы разграничения доступа ГИС к требуемой и вычисляется как взвешенная сумма количества ошибок первого и второго рода.

Программный макет предложенного алгоритма был реализован в среде Delphi. Эксперименты, проведенные на данном макете, показали, что предложенный алгоритм обладает достаточно приемлемой вычислительной сложностью, позволяющей достаточно эффективно использовать его для задач создания систем разграничения доступа в ГИС высокой размерности.

Работа выполняется при финансовой поддержке РФФИ (проект 11-07-00435-а).

Санкин П.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ВТОРИЧНАЯ ИНФОРМАЦИЯ В ПОТОКОВЫХ АУДИОДАННЫХ

Современные системы передачи данных ориентированы на использование цифровых технологий и уменьшения за счет них загрузки канала. Алгоритмы сжатия широко применяются в цифровых линиях связи для уменьшения объемов данных передаваемых текстов, изображений и звука.

Большинство современных стандартов передачи звука применяют разбитие звукового потока на отдельные фрагменты с последующим их сжатием. Например, кодек GSM разбивает звук на 20-миллисекундные посылки, аналогично работают кодеки для передачи речи по IP-сетям. Разбиение позволяет сохранять разборчивость речи при небольших потерях пакетов. В тоже время пропускная способность каналов передачи данных превосходит минимальные требования необходимые для непрерывной передачи. Пакеты передаются последовательно и, в моменты, когда один пакет передан, а отправка второго еще не началась, между ними возникают временные интервалы. Таким образом, можно выделить посылки данных, характеризующие фиксированные интервалы (несколько миллисекунд) передаваемого звука. Это образует уязвимость в виде возможности анализировать вторичные характеристики потока.

Наличие вторичной информации в потоковых данных рассмотрено в предыдущих работах при исследовании видеопотока. Там же было введено понятие вторичной информации, которая позволяет не прямо, а косвенно охарактеризовать передаваемое изображение.

Подход, используемый при анализе последовательностей изображений, можно применить и к анализу последовательностей звуковых фрагментов. И в том и другом случае можно выявить вторичную информацию, характеризующую размер отдельных порций данных.

Данные перед оправкой в канал сжимаются. Стандарты сжатия данных в подавляющем большинстве не предусматривают установление нижней границы для результата. В итоге мы имеем переменных размер пакетов в канале связи. Так, например, однородный звуковой поток будет обладать большой избыточностью и лучше сжимается, а неоднородный хуже. Наиболее высокую степень сжатия получит поток по своим характеристикам близкий к тишине. Однородный фоновый шум будет сжиматься однородно, при разбиении на равные интервалы будут получены схожие порции данных. Неравномерный звук для различных интервалов получит переменную степень сжатия.

Таким образом, анализируя размер передаваемых последовательностей пакетов можно сделать вывод о наличии или отсутствии речевой информации в канале связи. На основе этого можно реализовать простейший детектор звука, позволяющий в реальном времени определить изменение звукового фона в цифровой линии связи. Применительно к анализу линий связи, это позволит выявить наличие пауз между словами и выделить отдельные лексемы. Такой статистический анализ для своей реализации не требует существенных вычислительных ресурсов.

Сметанина О.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет информационных технологий, механики и оптики

К ВОПРОСУ О ЗАЩИТЕ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

Стремительно развивающиеся информационные технологии повлекли за собой развитие различных электронных платежных систем (ЭПС). ЭПС – это комплекс аппаратных и программных средств, позволяющий переводить денежные суммы между различными организациями и Интернет-пользователями при осуществлении определенных услуг или покупок через Интернет. Такой перевод сопровождается протоколом электронного платежа.

Необходимым условием использования ЭПС является защита передаваемых по сети данных с целью предотвращения использования платежной информации в мошеннических целях. Обеспечение этого представляет собой достаточно сложную задачу, решением которой занимаются разработчики ЭПС.

Практика выработала минимально необходимые требования, которым должны удовлетворять транзакции с соображений безопасности, а именно:

– неделимость – для осуществления транзакции должны быть выполнены все составляющие ее операцию, в противном случае ни одна из них не должна быть выполнена;

– целостность – не должно быть изменений информации в участвующих в проведении операции объектах;

– изолированность – транзакции не должны зависеть друг от друга;

Надежность и безопасность переводов обеспечивается сегодня, главным образом, защитой серверов и протоколом электронных платежей. Все сведения о плательщике хранятся на серверах ЭПС, защищаемых физическим и аппаратно-программным способами. Защита данных при этом достигается за счет использования симметричных алгоритмов шифрования, обеспечивающих высокий уровень криптостойкости. Для соблюдения конфиденциальности могут использоваться сертификаты, которые позволяют провести аутентификацию взаимодействующих пользователей.

Конкуренция в сфере применения ЭПС побуждает их производителей разрабатывать новые решения проблем надежности и конфиденциальности. В докладе будут исследованы два вида используемых сегодня сертификатов, проведено их сравнение и оценены перспективы применения. Будут также рассмотрены дополнительные способы защиты данных плательщиков, используемые разными ЭПС. В частности, планируется проанализировать уязвимости широко используемого сегодня протокола SSL.

Фаткиева Р.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ИССЛЕДОВАНИЕ СЕТЕВЫХ АТАК НА ОСНОВЕ СТЕНДА ПОЛУНАТУРНОГО МОДЕЛИРОВАНИЯ

Распространение простых в использовании операционных систем и программного обеспечения снижает требования к уровню знаний пользователя информационной системы, а применение общедоступных сетей передачи данных позволяет осуществлять как простые, так и более сложные атаки. Разновидности сетевых атак, таких как Ddos, присутствующие в сети плохо поддаются анализу стандартными средствами защиты информации. Особая опасность этих атак – в крайней простоте их организации. Для тщательного анализа атак предложена архитектура стенда включающего: атакующий хост, атакуемый хост и хост-анализатор. В ходе экспериментов, атакующий хост производит генерирование трафика, содержащего исследуемую атаку. Трафик поступает на концентратор, направляющий его на атакуемый хост. Анализатор осуществляет мониторинг выбранных параметров атакуемого хоста и сохраняет данные для последующей обработки. Оба рассматриваемые сегмента подключены к сети Интернет через порты Fast Ethernet, в распоряжении каждого канал с пропускной способностью 100 Мбит/с.

Обнаружение появления атаки осуществляется изменением параметров системы, характеризующие процесс несанкционированной активности. Параметры выбираются таким образом, чтобы резкое изменение их поведения во времени смогло дать возможность выявить возможную атаку. Для исследуемых типов атак, перечень параметров будет различный.

На основе стенда появляется возможность генерации атак, позволяющая исследовать механизмы их проведения и разработку средств их предотвращения. Проведены исследования разновидности Ddos атак (SYN flood, TCP-flood, ICMP-flood), которые можно использовать для моделирования атак, тестирования средств защиты информации и в учебном процессе для демонстрирования процессов протекающих в системах находящихся под атакой.

Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

КООПЕРАЦИЯ МЕХАНИЗМОВ ОБНАРУЖЕНИЯ СЕТЕВОГО СКАНИРОВАНИЯ

Актуальной задачей защиты информации в компьютерных сетях является исследование перспективных механизмов обнаружения и предотвращения сканирования сети. Сканирование сетей может использоваться как злоумышленниками для сбора информации об атакуемой компьютерной сети, так и сетевыми червями в процессе их распространения. В данной работе предлагается подход к обнаружению сканирования на основе согласованного использования (кооперации) комплекса различных механизмов обнаружения.

Решение поставленной задачи производится за счет решения следующих задач:

1. Определение наиболее эффективных механизмов защиты;
2. Выбор наиболее важных характеристик трафика и классификация трафика по этим характеристикам;
3. Определение метрик эффективности обнаружения;
4. Объединение механизмов защиты.

Последняя задача включает в себя разработку и подготовку алгоритма выбора оптимального механизма защиты для каждого из классов трафика, а также исследование и реализацию алгоритмов для объединения механизмов защиты.

Основными требованиями к разрабатываемой системе автоматической защиты от сканирования являются:

1. Точность работы (определяется по количеству ошибок классификации первого и второго рода);
2. Своевременность (определятся по скорости реакции системы на поступающую информацию);
3. Автоматизация. Это требование тесно связано со своевременностью. Система защиты должна требовать минимального участия администратора для принятия решений;
4. Обнаружение атак, растянутых во времени.

В данной работе предлагается использование комбинированной схемы, использующей отдельные классификаторы или группы классификаторов, ориентированные на обнаружение определенных типов сканирования, для принятия решения о блокировании опасных хостов в сети.

Полученная в результате использования данного подхода комбинированная схема обнаружения сетевого сканирования использует три уровня классификаторов:

1. Классификаторы, принимающие решение о наличии или отсутствии в исследуемом трафике подозрительных участков;
2. Аспектные классификаторы, которые на основе данных полученных от классификаторов 1-го уровня, принимают решение о наличии или отсутствии сканирующих последовательностей разных типов в исследуемом трафике;
3. Общий классификатор, принимающий решение о том, является ли исследуемый трафик сканирующим или нет. Особенностью классификаторов 1-го уровня в этой схеме, является то, что каждый из них использует группу параметров, характерных для различных типов подозрительной сетевой активности. Этот подход позволяет добавлять новые типы обнаруживаемого сканирования без переобучения всей системы – достаточно добавить новый классификатор 1-го уровня (или модифицировать уже существующий) и переобучить соответствующие классификаторы 2-го и 3-го уровней.

На основе предложенного подхода была проведена серия экспериментов, позволившая оценить эффективность работы отдельных и комбинированных механизмов обнаружения сканирования. По полученным данным можно судить о том, что использование предложенных методов комбинирования, а также настройка параметров для отдельных механизмов защиты в зависимости от статистических показателей трафика позволяет существенно улучшить эффективность работы этих механизмов.

В дальнейшей работе планируется проведение большого количества экспериментов для анализа эффективности методов комбинирования для различных смесей исследуемого сетевого трафика, разработка новых и совершенствование существующих отдельных механизмов обнаружения, исследование других схем кооперации отдельных механизмов, развитие разработанного программного средства с целью создания среды моделирования для механизмов защиты от сканирования.

Работа выполняется при финансовой поддержке РФФИ (проект №10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект №3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

Чечулин А.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

АНАЛИЗ ПРОИСХОДЯЩИХ В РЕАЛЬНОЙ СЕТИ СОБЫТИЙ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ МОДЕЛИРОВАНИЯ СЕТЕВЫХ АТАК

Основной задачей систем управления инцидентами и событиями (SIEM) является сбор и анализ событий, происходящих в контролируемой сети. В данной работе предлагается внедрить в существующие SIEM-системы дополнительную функциональность – подсистему моделирования атак, которая позволит расширить возможности и повысить точность выявления инцидентов, связанных с информационной безопасностью.

Поскольку результаты работы подсистемы моделирования атак часто не могут быть вычислены в реальном времени, их использование в процессах реального времени затруднено. Однако, построенные графы атак сохраняют актуальность достаточное время (до значительных изменений в политике безопасности или физической топологии сети). Благодаря этому в рамках общей системы анализа событий предлагается использовать построенные заранее графы атак. Эти графы атак могут применяться для решения двух основных типов задач – для предсказания последующих действий нарушителя и для анализа и выявления его прошлых действий, приведших систему к текущему состоянию. Также следует отметить, что для повышения эффективности в рамках моделирования атак используются не отдельные текущие события, а инциденты, распознанные с помощью корреляции отдельных событий. Таким образом, в подсистеме моделирования будут анализироваться не отдельные события вида «Хост С получил пакет на 80 порт от хоста В», а инциденты вида «производится сканирование хоста С хостом В», что позволит эффективнее обнаруживать графы атак, включающие в себя такие инциденты.

Предсказание же последующих действий нарушителя производится на основе анализа следующих элементов:

1. Моделей нарушителя, на основе которых были построены наиболее близкие к реальным графы атак;
2. Использованных нарушителем видов атак и уязвимостей;
3. Возможных целей, специфицированных в графах атак.

Таким образом, на основе анализа инцидентов с учетом данных полученных от подсистемы моделирования атак становится возможным делать выводы о том, что существует большая вероятность того, что инциденту «производится сканирование хоста С хостом В» предшествовал необнаруженный инцидент «хост В был атакован хостом А», и что последующим действием нарушителя будет «хост С подвергается атаке со стороны хоста В».

Кроме того результатом работы подсистемы моделирования атак могут быть следующие характеристики:

1. Слабые места в топологии сети (хосты, через которые проходит наибольшее число графов атак);
2. Выбранные контрмеры, позволяющие снизить вероятность максимального количества графов атак;
3. Возможные последствия реализации контрмер, учитывающие зависимости сервисов.

В настоящее время продолжаются теоретические исследования способов построения графов атак, учитывающих существующие уязвимости и уязвимостей нулевого дня, политики безопасности, зависимости сервисов и т.д., и осуществляется разработка программного прототипа подсистемы моделирования атак, как базового компонента общей SIEM-системы, разрабатываемой в рамках проекта MASSIF.

Работа выполняется при финансовой поддержке РФФИ (проект №10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект №3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

Шишкин В.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПРИМЕНЕНИЯ «ПРАВИЛА ЗОЛОТОГО СЕЧЕНИЯ» К ОБОСНОВАНИЮ ЗАТРАТ НА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

Определение разумного уровня затрат различных ресурсов на обеспечение безопасности функционирования сложных организационно-технических систем в условиях присущей им нелинейности, плохой прогнозируемости поведения и неизбежной ограниченности ресурсов является насколько важной настолько же нетривиальной и неоднозначной задачей.

С одной стороны, очевидно, неразумны большие затраты при умеренных рисках, но, с другой стороны, может быть, ещё более опрометчивой будет «экономия» при их недооценке. Основная сложность при этом состоит в недостаточной определенности идентификации и оценок рисков, возможность которых ограничена знанием (незнанием) и неизбежным субъективизмом экспертов. Особенно неопределенной данная задача становится, если рассматривать более узкую предметность информационной безопасности, к экономике которой плохо применимы традиционные подходы, а практика демонстрирует парадоксальное явление одновременного роста как затрат на защиту информационных активов, так и ущерба от нарушений их безопасности. Кроме того, не всегда оценки стоимостных показателей в номинальном денежном измерении адекватно отражают реальность.

В докладе рассматривается достаточно не редкая ситуация, когда соображения здравого смысла, обстоятельства или долговременные интересы требуют принятия проекта, решения, несмотря на то, что соотношение «цена-результат» для них с формально экономической точки зрения неприемлемо. Конфликт оценок становится разрешимым, если «цена» ситуативно будет нелинейно преобразована. Представлена методика такого преобразования натуральных шкал через шкалу меры риска с использованием функции степенного распределения.

На представленной модели анализируется выдвинутая на основе статистических данных гипотеза (А.И.Фесечко, ВЦ РАН, 2011) о том, что «при прогнозном планировании мероприятий по повышению уровня безопасности объектов оптимальным соотношением затрат на создание системы защиты и вероятными потерями» будет «правило золотого сечения». Показано, что данная гипотеза хорошо согласуется с полученными нами результатами, как в линейном так и нелинейном случае, являясь частным случаем для определенного класса функций затрат, и может быть формально обоснована в рамках модели, давая возможность идентифицировать параметры таких «оптимальных» функций.

Учитывая фундаментальное значение золотых пропорций и связанных с ними представлений во многих отраслях знания, данное направление применения модели заслуживает внимания.

Шишкин В.М., Савков С.В., Котенко Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

РАЗРАБОТКА КОМПЛЕКСА СРЕДСТВ РИСК-АНАЛИЗА В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Современные крупномасштабные вычислительные сети представляют собой сложные системы, состоящие из множества взаимодействующих компонент. Построение риск-модели для такой системы представляет собой достаточно трудоемкую задачу. В целях автоматизации построения структурированной модели угроз и выбора соответственно результатам анализа рисков наиболее эффективной СЗИ предлагается использовать создаваемый на основе разработанной ранее в СПИИРАН методики анализа рисков программно-аппаратный комплекс. Работа выполняется при поддержке программы «Академия ИнфоТеКС 2011».

Рассматриваемый комплекс анализа рисков позволяет:

– реализовать возможность обработки плохо определенных и разнородных данных;

– обеспечить расчет стохастических характеристик используемых для принятия решений показателей.

При проектировании программно-аппаратного комплекса приняты следующие требования:

– организация единой точки доступа к высокопроизводительным вычислительным ресурсам (кластерам);

– организация возможности централизованного хранения данных риск-модели.

В разрабатываемом комплексе выделяются следующие функциональные подсистемы: клиентская часть, сервер приложений, сервер баз данных, высокопроизводительный вычислительный ресурс (кластер). Клиентская часть комплекса предполагает два режима взаимодействия с базами данных: «конструктор» и «аналитик». В первом режиме реализуется наиболее трудоемкая и сложная в содержательном отношении базовая функция моделирования – создание структуры типовых риск-моделей, их модификация, поддержание в актуальном состоянии, адаптация к конкретному объекту и предметная специализация, т.е. создание предметно-ориентированных риск-моделей, включающих потенциальные средства защиты. Структура модели формируется путем последовательного добавления (исключения) ее элементов, называемых факторами риска, и фиксации связей между ними, представляющих отношение непосредственной причинности на множестве факторов. Аналогично, но проще создаётся структура, задающая отношение между множествами факторов риска и возможными средствами противодействия им.

В режиме «аналитик» происходит подготовка данных для расчётов, получение и отображение их результатов для анализа, подготовки и принятия решений. В этом режиме пользователь работает с готовыми структурами и не имеет права их изменять. Функциональность в данном режиме сводится к вариативному оцениванию связей с возможностями широкого разнообразия представления исходных данных (числовое и нечисловое, точечное, интервальное, лингвистическое, вероятностное и т.д.). В результате формируется «взвешенная» структура, которая является исходной информацией для последующих расчётов показателей профиля риска и эффективности СЗИ.

На кластере реализуется наиболее ресурсоемкая часть приложения, а именно гомогенизация и рандомизация исходных данных путём генерации множества допустимых (удовлетворяющих исходным данным) векторов и расчет конечных показателей. Поскольку вектора независимы друг от друга, их вычисление может быть организовано в параллельных ветвях алгоритма.

Клиентская часть программы реализована посредством веб-интерфейса. Программа формирует запрос, который транслируется серверу приложений. Сервер приложений, в свою очередь производит анализ поступившего запроса. В случае запроса ранее занесенной в хранилище информации, производится обработка запроса сервером баз данных. В случае запроса вычислительного ресурса производится подготовка, запуск задания и сбор результатов. Структура модели и набор исходных оценок содержатся в теле запроса. Полученные от сервера баз данных или кластера ответы транслируются в программу на компьютере клиента. Взаимодействие с сервером баз данных осуществляется по протоколу SQL, а с вычислительным ресурсом (кластером) по протоколам SSH/SCP.

Вычислительный модуль обеспечивает программную реализацию методики, количественного оценивания рисков в условиях неполноты и разнородности исходной информации. Её основное отличие в своем классе состоит в том, что получаемые оценки факторов риска и эффективности СЗИ представляют не точечные значения показателей, а распределения их вероятностей. Данная методика позволяет детально оценить угрозы для конкретной вычислительной сети и предложить наиболее эффективную для неё систему защиты.

Оценки, полученные программно-аппаратным комплексом, могут быть представлены в виде, требуемом нормативными документами, что позволяет автоматизировать процесс создания директивной отчетности.

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Аль-Рахми Р.Я.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

ЗАЩИТА ИНФОРМАЦИИ И НЕОТСЛЕЖИВАЕМОСТЬ ТРАФИКА В ВИРТУАЛЬНЫХ СЕТЯХ

В последнее время становится актуальной защита от атак через Интернет на сети организаций с целью похищения информации удаленной локальной сети. В то время как содержимое передаваемой в сети информации можно защитить, используя шифрование трафика, остается востребованной защита самого факта передачи рабочих пакетов между конкретными узлами сети.

В настоящем сообщении рассматривается новый подход к защите сервера удаленного доступа виртуальной сети организации от данного вида хищения информации. Данный метод основан на том, что сервер удаленного доступа отправляет случайные данные на случайные IP адреса сети. Для успешного применения данного метода в первую очередь необходимо удостовериться в способности работы сервера удаленного доступа с определенным количеством исходящего трафика. В начале работы данный сервер создает список IP адресов, на которые будет отправляться случайный трафик. Когда какой-либо компьютер удаленного пользователя устанавливает связь, его IP адрес удаляется из списка IP адресов, и вплоть до окончания сессии между ними, сервер обменивается с ним рабочим трафиком. При этом параллельно сервер продолжает отправлять случайный данные по сети на оставшиеся IP адреса. Когда закрывается сессия между компьютером удаленного пользователя и сервером, IP адрес клиента вновь добавляется в список IP адресов. При этом похититель передаваемой информации не может зафиксировать реальные данные и реальные компьютеры, соединяющиеся с сервером удаленного доступа. Данный метод можно реализовать с помощью двух способов:

1. Использовать готовый протокол ESP (Encapsulation Security Payload), в зашифрованной части в заголовке данного протокола можно прикрепить флажок истинного данного пакета в зашифрованном виде. Когда компьютер удаленного пользователя получает пакет от сервера по сети, заголовок данного пакета расшифровывается, и, если флажок истинный, клиент принимает данный пакет и обрабатывает его, в противном случае пакет отбрасывается и исключается.
2. Разработать новый протокол защиты виртуальных каналов на сетевом уровне. Разработанный протокол должен поддерживать защиту содержимого пакета и прикреплять в зашифрованном виде флажок истинности данного пакета.

Для работы сервера удаленного доступа необходимо выполнить следующие задачи:

– Сбалансировать трафик сервера, чтобы сервер не был отключен от работы в связи с большим трафиком, превышаемым допустимый для данного сервера.

– Внедрить протокол, зашифровывающий пакеты и прикрепляющий флажок истинности (также в зашифрованном виде) к каждому отправляющемуся пакету.

Настроить сервер таким образом, чтобы тот мог работать со всеми соединяющимися клиентами и параллельно высылать случайные пакеты по списку IP адресов, последовательно исключив из него те IP адреса, которые подключены в данный момент к нему в рамках сессии.

Андрущенко Д.М.
Украина, Запорожье, Запорожский национальный технический университет

МЕТОД ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Производители программного обеспечения несут большие убытки из-за нелегального использования их продукции, так называемого «пиратства». Поскольку юридические методы борьбы с правонарушителями чаще всего не являются эффективными, разработчики прибегают к техническим средствам защиты программного продукта от нелегального использования, к которым относят программные и программно-аппаратные средства, а также использование программ как онлайн-сервисов. Программные средства, как правило, характеризуются недостаточной устойчивостью к взлому. Программно-аппаратные средства – более надежны, но обычно создают неудобство для легального пользователя. Использование программ как онлайн-сервисов иногда может потребовать передачи слишком больших объемов трафика, а в некоторых случаях и вовсе не возможно в связи с требованием конфиденциальности к данным пользователя.

Сравнительный анализ известных подходов показывает, что наиболее перспективным методом защиты многих программ является метод авторизации через Интернет. Он подразумевает первоначальную активацию продукта на вычислительной машине пользователя, а также авторизацию пользователя на сервере разработчиков при каждом запуске программы. Анализ возможности реализации данного способа показывает, что для обеспечения высокой эффективности необходимо обеспечить защиту трех разных элементов:

– защита кода программы путем обфускации (запутывание кода);
– защита удаленного сервера, на котором хранятся данные о пользователе программой;
– защита данных передаваемых между программой и удаленным сервером во время запуска.

Однако до настоящего времени применительно к методу авторизации через Интернет третья задача не достаточно решена, что ограничивает возможность реализации данного подхода. Поэтому в работе основное внимание было уделено защите данных передаваемых между удаленным сервером и программным продуктом. В результате предложен протокол передачи данных для защиты программного обеспечения, который основан на использовании механизма электронной цифровой подписи (ЭЦП). Суть его состоит в следующем.

Пусть имеется защищаемое приложение Prog, установленное на компьютере пользователя U, и удаленный сервер S, принадлежащий разработчикам приложения либо их доверенному лицу.

Разработчик должен выбрать систему электронной цифровой подписи и сгенерировать пару ключей – открытый ключ e и закрытый ключ d. Закрытый ключ d должен храниться на сервере S, а открытый ключ e – в приложении Prog. Перед первым запуском программы пользователь должен получить идентификатор (логин) I и пароль P. Каждый раз, когда пользователь U пытается выполнить одно из действий установленных разработчиком, например запуск программы, создание, открытие или сохранение документа, программа Prog должна посылать запрос серверу S о возможности продолжить работу, совершив следующие шаги передачи данных:

1. В программе Prog генерируется случайное число RND.
2. В программе Prog вычисляется некоторое число F – привязка к программно-аппаратному обеспечению вычислительной машины, где она установлена.
3. Программа Prog передает данные I, P, RND, F серверу S.
4. Сервер S проверяет возможность использования программы пользователю с идентификатором I, паролем P и привязкой F.
5. В случае подтверждения возможности запуска программы Prog, S вычисляет электронную цифровую подпись C(RND), используя закрытый ключ d.
6. Сервер S отправляет значение C(RND) программному обеспечению Prog.
7. В программе Prog осуществляется проверка подлинности подписи сервера C(RND) по известному открытому ключу e. Если подпись подлинная, то программа продолжает выполняться, в противном случае завершает работу.

Авторизация пользователя при каждом запуске программы позволяет разработчику следить за статистикой использования программы, выявлять случаи нарушения лицензий, лишать лицензий недобросовестных пользователей, а также гибко изменять лицензионную политику в соответствии со своими нуждами. Кроме того у разработчиков программы появляется возможность вводить период бесплатного использования программы как на стадии бета-тестирования, так и при первом ее использовании пользователем.

Связь с сервером может осуществляться через публичную глобальную сеть Интернет по его доменному имени либо IP-адресу. Разрешение на запуск программы дается удаленным сервером и может основываться на следующих данных: количество совершенных успешных запусков программы, время использования программы, оплачиваемый пользователем баланс, количество созданных документов при использовании программы и др. Перед первым использованием программы пользователь должен получить идентификатор и пароль для запуска программы, что может обеспечить правообладатель программы либо третья доверенная сторона.

Баранов В.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

МЕТОД ОПРЕДЕЛЕНИЯ ВТОРЖЕНИЯ НА ОСНОВЕ РАЗЛАДКИ ПРОЦЕССА НАБЛЮДЕНИЙ

Представим компьютерную систему, в качестве дискретного автомата с последовательностью внутренних состояний, принимающих значения из некоторого конечного множества возможных состояний. Каждое из возможных состояний в свою очередь описывается некоторым набором параметров, определяющих важные для обеспечения функционирования компьютерной системы аспекты процесса. Каждый параметр принимает значение из определенного диапазона, в зависимости от активного или пассивного состояния соответствующей отдельно взятой части системы. При выборе описания системы путем ее декомпозиции на части следует стремиться к уменьшению количества составляющих частей и степеней измерения активности. Это требование объясняется ориентировкой на дальнейшее применение статистических методов оценки состояния

системы. Известно, что статистические оценки становятся более эффективными, когда число наблюдений над каждым из состояний системы достаточно велико. Подобное качественное понятие описывается определенными математическими условиями.

При помощи теоретико-вероятностной схемы, называемой «разладкой», были смоделированы проявления вторжения в компьютерную систему. В ходе моделирования решались три задачи.

Задача 1. Эта задача возникает при попытке ответа на вопрос, является ли сеанс работы за n тактов корректным или результат работы может быть искажен вследствие вторжения.

Задача 2. Отражает проблему выявления момента начала вторжения и определения способов и условий его реализации.

Задача 3. Является некоторым уточнением постановок, описанных в задачах 1 и 2, поскольку вносит дополнительную информацию о возможном значении параметра, отражающего момент разладки, в виде его распределения.

Важно отметить, что основной целью работы было решение вопроса о наличии или отсутствия вторжения в систему по массиву данных мониторинга или, иначе говоря, по «апостериорному» определению, а также, имело место или отсутствовало вторжение в систему.

Была рассмотрена эффективность предлагаемой схемы на конкретных примерах сбойных ситуаций, возникающих в результате вторжения. Следует отметить, что предложенные статистики ориентированы на применение в ситуациях, когда возможно предварительное обучение в виде получения и накопления информации о распределении наблюдений до и после разладки, а так же о распределении момента появления вторжения. Указанные требования по обучению в определенной мере ограничивают область возможного применения предложенных алгоритмов.

Проведен эксперимент по наблюдениям работы приложения Internet Explorer для ОС Windows XP в штатном режиме и в режиме заражения исполняемого файла приложения вирусом типа Trojan. Наблюдения были представлены набором таких возможных действий, как доступ (чтение, редактирование, создание) к файлам, к записям системного реестра и библиотекам, которые фиксировались. В рассмотрение были включены только те действия, которые имели место, как при штатной работе, так и при нештатной.

Наблюдалось различие значений предлагаемой статистики при штатной работе приложения и при наличии воздействия вируса. В результате выяснилось, что величина различия позволяет делать предположения об устойчивом обнаружении воздействия вируса предлагаемой статистикой.

Баранов В.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ПОСТРОЕНИЕ ДОВЕРИТЕЛЬНОГО ИНТЕРВАЛА РАЗЛАДКИ ПРИ ОБНАРУЖЕНИИ ВТОРЖЕНИЙ

Рассмотрим ситуацию, когда работу компьютерной системы сопровождает подсистема мониторинга, которая через определенные промежутки времени фиксирует состояния наблюдаемых параметров системы, принимающих значения из определенного конечного алфавита. Будем полагать, что последовательность зафиксированных наблюдений есть реализация последовательности независимых дискретных случайных одинаково распределенных величин, если компьютерная система (КС) находится в штатном режиме и не подвергается негативному воздействию. Предлагаемая модель работы КС весьма груба, однако если временные промежутки между наблюдениями содержат хотя бы несколько десятков тактов работы центрального процессора, то предположение о независимости соответствующих им случайных величин можно проверить экспериментально.

Естественно предположить, что если в некоторый промежуток тактов работы процессора между соседними моментами наблюдений произошло вторжение, то его следствием являлось изменение характера работы и изменение распределения соответствующих случайных величин.

В предыдущей работе предполагалось, что параметр, отражающий момент разладки, есть реализация случайных величин с некоторым известным распределением. В настоящей работе рассматривается возможность оценки указанного параметра как некоторой фиксированной величины. Методы построения классических оптимальных статистических оценок в такой постановке применить не удается. Поэтому приходиться идти по пути поиска и построения частных решений, выбирая оптимальное статистическое правило оценки упомянутого параметра, дающих наименьший доверительный интервал при одном и том же объеме наблюдений. Вместе с тем, очевидно, что в ряде случаев эта задача имеет простое решение.

В ходе работы было предложено построение упомянутого выше доверительного интервала, размер которого был оценен порядка корень квадратный из n, где n соответствует количеству зафиксированных наблюдений.

На основании полученных теоретических результатов планируется провести ряд экспериментов, позволяющих рассуждать о применимости рассматриваемого метода обнаружения вторжений в КС в реальных условиях.

Боршевников А.Е.
Россия, Владивосток, Дальневосточный федеральный университет

СОВРЕМЕННЫЕ КРИПТОГРАФИЧЕСКИЕ ПРОГРАММНЫЕ СРЕДСТВА, КАК СРЕДСТВА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Современный мир не может обойтись, без такого понятия, как персональные данные. И, конечно же, большое значение имеет защита персональных данных от несанкционированного доступа (утечки). Однако, предлагаемые современные криптографические программные средства или по-другому средства криптографической защиты информации (далее СКЗИ) наиболее известными компаниями на рынке защиты информации (несмотря на широкий спектр возможностей и высокую надежность этих программных средств) может позволить не каждый обычный гражданин или организация. Остается обратить взгляд на более простые по содержанию и дешевые/бесплатные СКЗИ.

Было изучено бесплатное СКЗИ TrueCript 6.2a. Данное приложение имеет возможность создания зашифрованных файловых контейнеров, подобных виртуальным жестким дискам. Эти жесткие диски можно заполнять необходимыми файлами. Шифрование происходит во время переноса файлов на виртуальный жесткий диск. Программа позволяет создание шифрованных файлов на съемном носителе, которые будут сразу же инициализироваться, как виртуальные жесткие диски при обнаружении носителя операционной системой. Приложение реализовано для работы в разных операционных системах (Windows, OS X, Linux).

Программа предоставляет возможность шифрования одним из трех симметричных шифров: AES, Twofish, Serpent. Также можно выбрать из пяти комбинаций перечисленных шифров: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent. Помимо этого программа предоставляет возможность выбрать один из трех алгоритмов для выработки имитовставки: RIPEMD-160, SHA-512, Whirpool. Стойкость перечисленных криптоалгоритмов доказана ведущими зарубежными криптологами. Алгоритмы выработки имитовставки соответствуют международным стандартам. Ключи для криптоалгоритмов формируются самой программой. Скорость шифрования колеблется от 61 до 497 МБ/с (в зависимости от выбранного алгоритма шифрования). Дешифрование файлов имеет скорость, колеблющуюся от 58 до 489 МБ/с (в зависимости от выбранного алгоритма шифрования). Это обеспечивает достаточно низкое время переноса файлов в зашифрованный файловый контейнер и обратно.

Также программа позволяет, кроме создания зашифрованного файлового контейнера, произвести еще две процедуры: шифрование несистемного носителя/диска, шифрование раздела или всего диска с системой. Данные процедуры подобны процедуре создания зашифрованного файлового контейнера.

Помимо возможностей самого приложения, для более надежного обмена информацией между двумя или более пользователями, можно использовать схему совместной выработки пароля, который используется для доступа к зашифрованному файлу.

Используя передачу зашифрованных файлов вместо обычных, пользователи увеличат защищенность своих персональных данных от несанкционированного доступа. Хотя это не предотвратит непосредственно утечки данных, но сделает сложным непосредственный доступ к данным. Бесплатность, доступность, надежность самого СКЗИ позволяют создать достойный уровень защиты персональных данных для граждан и малых предприятий.

Булов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций

БЕЗОПАСНОСТЬ СЕРВЕРА MEMCACHED

Memcached – одна из популярнейших key-value система кеширования. Она используется на многих крупных и средних веб-сайтах.

Особенностью сервера является доступ по сетевому интерфейсу, что дает возможность удаленного доступа, распределенность и отказоустойчивость, однако создает возможность для многих атак.

Протокол взаимодействия сервера с клиентом основан на простых командах (get, set), также возможно получение всех ключей кеша. Подключение к серверу возможно осуществить через обычный терминал.

Одной из неприятных особенностей сервера является полное отсутствие систем аутентификации и авторизации. Возможность соединения по SSL также отсутствует.

Многие разработчики и администраторы забывают блокировать порт memcached, оставляя сервер полностью открытым для любого подключения. Из этого следует, что сервер на котором установлен memcached, обязательно должен быть защищен межсетевым экраном.

Некоторые разработчики хранят в кеше данные закрытых разделов сайта, а иногда и персональные данные пользователей, e-mail адреса, хеши паролей.

При правильных политиках безопасности и безопасном написании приложения, использование memcached становится абсолютно безопасным. Среднее время жизни кешированного значения как правило не превышает минуты. Как показали результаты исследования, использование кеша позволяет не только обеспечить безопасность сервера но и повысить скорость работы практически любого веб-приложения, даже если его применение не было заложено архитектурно. Кроме того, memcached поддерживается реверсивным прокси сервером nginx, что позволяет кешировать не просто результаты запросов, а целые страницы. Это серьезно снижает нагрузку на сервер приложений, если динамические данные на страницах меняются редко.

Булыгин Р.А.
Россия, Екатеринбург, Уральский радиотехнический колледж им. А.С. Попова

ИНТЕГРАЦИЯ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ В РАМКАХ УЧЕБНОГО ПРОЦЕССА

В условиях интеграции ССУЗов в систему высшего образования необходимо обеспечить возможность конкурентной борьбы. Фурсенко А.А. и Дорожкин Е.М. отмечают, что основным козырем СПО является практико-ориентированное обучение.

При практико-ориентированном обучении выпускники колледжей и техникумов с большей долей вероятности смогут получить преимущество на рынке труда по сравнению с выпускниками университетов т.к. работодателям требуются сотрудники с опытом работы, навыками работы на конкретном оборудовании или в конкретных программных продуктах для выполнения реальных задач. Поэтому некоторые учебные задачи студенты специальности «Информационная безопасность автоматизированных систем» реализуют в качестве проектов для предприятий и организаций.

На данный же момент система образования по большей части выпускает людей, знающих процесс работы только в теории, и лишь после получения работы они понимают разницу между теорией и практикой. В связи с этим было принято решение провести дополнительные практические занятия по специальности «Информационная безопасность автоматизированных систем».

Одна из неотъемлемых частей любого комплекса защиты информации – это система визуального контроля, или видеонаблюдения. Один из проектов, реализованных в процессе практико-ориентированного обучения студентов – это установка системы видеонаблюдения с трансляцией потокового видео в Интернет.

Один из магазинов требовалось оборудовать системой видеонаблюдения. В том же здании располагается офис компании и складские помещения. Переход из торгового зала в офис и склад осуществляется через коридор общего пользования.

На основании этих данных были определены задачи:

1. Разработать проект системы видеонаблюдения, отвечающей следующим требованиям:

– система должна с максимальной эффективностью обеспечивать визуальный контроль над всеми торговыми рядами в магазине;

– система должна обеспечивать наблюдение за всеми перемещениями людей между помещениями, принадлежащими предприятию: из торгового зала на склад и в офис;

– система должна стабильно и самостоятельно работать в режиме 24/7, при этом сохраняя запись всех событий, произошедших в магазине за последнюю неделю;

– необходима возможность просмотра трансляции и обращения к архиву через Интернет с помощью стандартных браузеров;

– требуется возможность расширения системы, подключения дополнительных камер (требование заказчика).

2. Провести нагрузочное тестирование системы.
3. Ввести систему в эксплуатацию.

Первый этап реализации проекта – выбор оборудования, оптимального для выполнения данной задачи. Исходя из выделенных на оборудование средств, было решено строить систему видеонаблюдения на базе цифрового видеорегистратора и аналоговых камер, так как для организации эффективной системы требуется не менее 7 камер, Также любая система безопасности должна обладать автономным питанием – на случай диверсии либо внезапного форс-мажорного отключения электричества.

Второй этап реализации проекта – установка системы видеонаблюдения. Проблемой реализации была установка и настройка камер так, чтобы максимально обеспечивался визуальный контроль над всем происходящим в магазине, что мне и удалось реализовать в дальнейшем.

Заключение. Система визуального контроля – это неотъемлемая часть любого комплекса защиты информации. Мне удалось разработать и ввести в эксплуатацию работоспособный и стабильный комплекс визуального контроля с возможностью удалённого доступа к нему.

Васильев В.Н., Головачев Д.А., Латышев Д.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

УТВЕРЖДАЕМАЯ ГРУППОВАЯ ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Аутентификация информации с помощью двухключевых схем электронной цифровой подписи (ЭЦП) нашла широкое применение в информационных технологиях, связанных с циркуляцией электронных сообщений и документов, имеющих юридическое значение. В разнообразных практических приложениях используются протоколы ЭЦП различного типа: обычная (индивидуальная) ЭЦП, коллективная ЭЦП, слепая ЭЦП и др. Одним из интересных протоков является групповая ЭЦП. Данный протокол обеспечивает возможность формирования ЭЦП от имени некоторого коллегиального органа – группы подписывающих, один из которых является лидером (руководителем). При этом реализуются следующие свойства:

1. Подписать документ имеет возможность любой член группы;
2. Лидер по значению ЭЦП и соответствующему ей документу может определить лицо, сформировавшее данную конкретную подпись;
3. Лица, не состоящие в штате органа, не могут установить, кто конкретно сформировал групповую подпись к заданному документу.

Известны различные разновидности протоколов групповой подписи, удовлетворяющие некоторым дополнительным требованиям. В частности схемы пороговой групповой ЭЦП характеризуются тем, что групповую подпись может сформировать подмножество подписывающих, число которых равно или превышает некоторое пороговое число *t*. Если для формирования групповой ЭЦП объединяются *t-1* подписывающих или менее, то они этого сделать не смогут. Недостатком ряда известных схем пороговой групповой подписи является то, что в протоколе участвует доверенное лицо, которому подписывающие передают свои секретные ключи.

Несмотря на разнообразие известных протоколов групповой подписи, отсутствуют их варианты, которые удовлетворяют следующим дополнительным свойствам:

– личные секретные ключи подписывающих не разглашаются кому бы то ни было;
– формирование групповой подписи осуществляется в два этапа, т.е. на первом этапе формируется «групповая предподпись», а на втором этапе лидер из «предподписи» вычисляет значение групповой подписи (выполнение процедуры утверждения подписанного документа);
– предподпись может быть сформирована любым подписывающим или любым подмножеством подписывающих;
– по некоторому документу и групповой подписи к нему идентифицировать подписавшего или подмножество подписавших может только лидер.

Целесообразность придания протоколу групповой ЭЦП перечисленных дополнительных свойств связана с обеспечением близкой аналогии процедуры обработки электронных документов с практикой подготовки, подписывания и утверждения бумажных документов.

В настоящей работе предлагается новый протокол групповой ЭЦП, удовлетворяющий перечисленным дополнительным требованиям. В протоколе данного типа вопрос о том, кто подписывает конкретный документ, является прерогативой руководителя (лидера), который распределяет работу по подготовке электронных документов. Исполнитель (или несколько исполнителей) после выполнения процедуры подготовки документа формируют «групповую предподпись», которая фактически является их цифровой подписью, прилагаемой к этому документу. Если руководитель решает утвердить документ, то он по «предподписи» вычисляет групповую подпись. Таким образом, групповая подпись в предложенном протоколе включает в себя подписи разработчиков документа и утверждающую подпись руководителя.

Используя общую конструктивную схему предложенного протокола и ее основные механизмы, можно разработать протоколы групповой ЭЦП, имеющие аналогичный набор свойств, с применением других проверочных уравнений и других конечных групп. Значительный интерес представляет построение таких протоколов с использованием эллиптических кривых, что позволит построить схемы групповой ЭЦП с размером подписи, равным примерно 480 бит при обеспечении 80-битовой стойкости.

Работа, выполняемая в представленном докладе, поддержана грантом РФФИ №11-07-00004-а.

Васильев В.Н., Кишмар Р.В., Головачев Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

КРИПТОСХЕМЫ НА ОСНОВЕ КОМБИНИРОВАНИЯ ДВУХ НЕЗАВИСИМЫХ ТРУДНЫХ ЗАДАЧ

Под стойкостью криптосхем понимается сложность наилучшего известного алгоритма ее взлома. Стойкость криптосхем является одним из параметров, определяющих уровень ее безопасности. Понятие безопасности криптосхемы означает достаточно высокий уровень стойкости и низкую вероятность того, что будут найдены новые более эффективные алгоритмы взлома

криптосхемы. Оценка стойкости двухключевых криптосхем связана с предположением о достаточно низком значении вероятности появления в обозримом будущем прорывных решений трудных задач, положенных в основу криптосхем данного типа. Получить количественную оценку порядка этой вероятности является весьма проблематичным делом. Однако само применение криптосистем с открытым ключом говорит о признании того, что ее значение настолько мало, что вероятностью появления прорывного решения можно пренебречь. Таким образом, уровень безопасности криптосхем определяется не только сложностью решения базовой трудной задачи, но и тем фактом, что вероятность нахождения прорывных решений базовой трудной задачи в обозримом будущем является достаточно малой. Вероятность появления прорывных решений в течение ближайшего месяца или года можно оценить некоторым малым значением, например 0,000001. Следовательно, повышение уровня безопасности предполагает как увеличение стойкости криптосхем, так и снижение вероятности их взлома за счет появления прорывных решений. Это положение лежит в основе направления синтеза протоколов электронной цифровой подписи (ЭЦП), взлом которых требует одновременного решения двух независимых вычислительно трудных задач. В литературе известен ряд схем ЭЦП данного типа, однако ранее не предлагались протоколы открытого распределения ключей, протоколы открытого шифрования и протоколы с нулевым разглашением, взлом которых требует одновременного решения двух вычислительно трудных задач.

В настоящем сообщении решается данная задача построения перечисленных протоколов на основе следующих трудных задачи: 1) факторизации составного числа специального вида, 2) дискретного логарифмирования в мультипликативной группе. Во всех трех указанных протоколах используется открытый ключ, включающий тройку чисел α, p=2n+1, где n = qr (q и r – простые числа, являющиеся частью секретного ключа) и y=α^x mod p, где α - примитивный элемент по модулю p ; x – значение, являющееся элементом секретного ключа.

В протоколе открытого распределения ключей каждый из взаимодействующих абонентов A и B формируют разовые открытые ключи, формируемые по формуле y=α^x mod p и значениям α и p, взятым из открытого ключа другой стороны. С помощью разовых и основных открытых ключей каждый из абонентов вычисляет первую часть общего секрета, а вторая часть общего секрета формируется в виде произведения двух случайных значений, одно из которых выбирается абонентом A, а другое – абонентом B. Выбранные секретные значения передаются другой стороне в зашифрованном виде. Шифрование осуществляется путем возведения в квадрат по модулю n, вычисляемому по соответствующему значению p.

Схема открытого шифрования строится как вложение алгоритма открытого шифрования Рабина в процедуру открытого шифрования, предложенную Эль-Гамалем. Предлагаемый протокол с нулевым разглашением использует разовый секретный ключ k и значение разового открытого ключа, вычисляемого путем двукратного возведения значения y в степень k по модулю p.

Васильев И.Н., Головачев Д.А., Молдовян Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

КОММУТАТИВНОЕ ШИФРОВАНИЕ С ВЕРОЯТНОСТНЫМ КОДИРОВАНИЕМ СООБЩЕНИЙ ТОЧКАМИ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Алгоритмы коммутативного шифрования (АКШ) применяются в ряде специальных криптографических протоколов. Для построения АКШ используется трудность задачи дискретного логарифмирования (ЗДЛ) в конечных полях, имеющая субэкспоненциальную сложность. При таком подходе каждое сообщение, кроме сообщения, представляющего нулевую битовую цепочку, интерпретируется ненулевым элементом поля. Однако для задания высокой стойкости АКШ требуется использовать поля, порядок которых выражается простым числом или степенью простого числа размером не менее 1024 бит, что существенно ограничивает производительность АКШ. В настоящей работе обсуждаются способы и варианты построения АКШ с использованием эллиптических кривых (ЭК), заданных над конечными полями.

Основным интересом к ЭК как примитиву криптосистем с открытым ключом является то, что ЗДЛ на ЭК специального вида имеет экспоненциальную сложность, благодаря чему обеспечивается более высокая производительность криптосхем данного типа по сравнению со случаем реализации последних с использованием конечных полей. Это также относится и к случаю построения АКШ. При шифровании обычно предполагается, что любое сообщение, размер которого не превосходит некоторое заданное значение, может быть корректно зашифровано и расшифровано, т.е. на входные значения АКШ не накладывается ограничений. При использовании ЭК для синтеза АКШ возможны следующие два подхода: 1) для шифрования выбираются сообщения, которые могут быть интерпретированы точками используемой ЭК; 2) размер сообщений задается на h бит меньше, чем размер порядка конечного поля, над которым задана ЭК.

Первый подход может быть применен в протоколах, в которых пространство шифруемых сообщений ограничено (например, в протоколах честной игры в покер по телефону) и имеется возможность табличной кодировки шифруемых сообщений точками ЭК.

Во втором подходе обеспечивается практическая возможность корректного преобразования любого сообщения. Входное сообщение интерпретируется как часть абсциссы точки ЭК, к которой справа (или слева) присоединяются h случайных битов. Полученное значение принимается за абсциссу и проверяется существование точки ЭК с данным значением абсциссы. Если такой точки на используемой ЭК не существует, то присоединяются новые случайные h битов, и проверка повторяется. Если такая точка M существует, то вычисляется ее ордината. Точка M шифруется путем умножения ее на число e, которое является ключом зашифрования. Полученная точка C может быть корректно расшифрована по формуле M=dC, где d – значение, обратное числу e по модулю, равному порядку ЭК. Сообщение извлекается из расшифрованной точки путем удаления из значения ее абсциссы правых h битов. Таким образом, второй подход состоит в вероятностном кодировании шифруемых сообщений точками ЭК.

Для построения АКШ с использованием вероятностного кодирования представляет интерес использование ЭК, порядок которых является простым числом или равен простому числу, умноженному на достаточно малое натуральное число. В этом случае можно пренебречь вероятностью получения шифруемых точек малого порядка, что могло бы позволить потенциальному нарушителю вычислить часть секретного ключа.

Васильев П.Н., Маховенко Е.Б.
Россия, Санкт-Петербург, ООО «Яндекс», Санкт-Петербургский государственный политехнический университет

РАСШИРЕНИЕ ДИНАМИЧЕСКОЙ СХЕМЫ ГРУППОВОЙ ПОДПИСИ

По совокупности свойств, в том числе свойств безопасности, обеспечиваемых схемой групповой подписи, эффективности процедур формирования, проверки и раскрытия подписи, ее длины, а также набору криптографических предположений, одной из наиболее гибких и расширяемых схем групповой подписи является схема Boneh-Boyen-Shacham (BBS; Shacham H. New paradigms in signature schemes // http://hovav.net/dist/thesis.pdf, 2005), безопасность которой основана на предоставлении в подписи знания решения задачи Strong Diffie-Hellman: пары (A, x), где Ax+w = g1, g1 – элемент циклической группы G1 простого порядка p; x, w – элементы циклической группы (Z/pZ)*. Базовую схему групповой подписи BBS можно назвать статической, поскольку она не предусматривает возможность динамического вступления в группу после ее формирования, что является одним из основных требований, возникающих при решении задачи аутентификации в распределенных приложениях. Кроме того, для данной схемы не выполняются свойства полной анонимности и «строгой» невозможности ложного обвинения, так как в ней, в частности, существует сторона, которая знает секретные ключи всех пользователей и может сформировать подпись от чужого имени.

Предлагается доработать схему BBS до динамической, включив в нее протокол Join добавления пользователя в группу. Этот протокол выполняется пользователем, желающим стать членом группы, и менеджером, выпускающим сертификаты. В результате успешного выполнения данного протокола пользователь становится обладателем членского сертификата (A, x, y), а менеджер – части этого сертификата (A, x), что дает ему возможность в дальнейшем отслеживать подписи, генерируемые этим пользователем. Значение y формируется на стороне пользователя и остается известным только ему. Такой сертификат должен удовлетворять условию: Ax+w = g1hy, где h – элемент группы G1. Изменение сертификата влечет за собой модификацию алгоритмов формирования и проверки подписи.

Разработана спецификация протокола Join. Доказано, что расширенная схема BBS удовлетворяет основным требованиям, предъявляемым к групповой подписи [1]: невозможность фальсификации, «строгая» невозможность ложного обвинения, устойчивость к сговору, несопоставимость подписей.

Для обеспечения полной анонимности CPA-стойкая схема линейного шифрования части членского сертификата, используемая в схеме BBS, заменена CCA2-стойкой линейной схемой Крамера-Шоупа (Shacham H. A Cramer-Shoup Encryption Scheme from the Linear Assumption and from Progressively Weaker Linear Variants // http://eprint.iacr.org/2007/074.pdf). Это позволило доказать безопасность предложенной схемы в соответствии с требованиями динамической модели (см., например Bellare M., Shi H., Zang C. Foundations of Group Signatures: The Case of Dynamic Groups // CT – RSA'05. Springer-Verlag, 2005. LNCS. Vol. 3376. P. 136–153).

Галанов А.И., Кишмар Р.В., Сухов Д.К.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Среди большого числа различных типов схем электронной цифровой подписи (ЭЦП) особое внимание привлекают протоколы коллективной ЭЦП. Одним из важнейших требований к протоколам коллективной ЭЦП является обеспечение свойства целостности коллективной ЭЦП, которое заключается в том, чтобы по данной коллективной ЭЦП нельзя было бы сформировать какие-либо другие подписи, проходящие процедуру проверки как подлинные подписи. По отношению к протоколам обычной ЭЦП целостность можно интерпретировать как вычислительную невозможность формирования по имеющейся подлинной индивидуальной ЭЦП к документу D другой подлинной подписи, относящейся к D и некоторому другому открытому ключу (ОК). В настоящем сообщении рассматриваются механизмы придания целостности ЭЦП.

Под корректностью генерации ОК понимается то, что ОК, регистрируемые и распространяемые удостоверяющим центром, сформированы в строгом соответствии с процедурой, специфицированной используемой схемой ЭЦП. В отличии от отсутствия строгой необходимости выполнения процедур проверки корректности ОК в схемах индивидуальной ЭЦП в схемах коллективной ЭЦП это требование является принципиальным. Без контроля корректности ОК нарушители имеют возможность зарегистрировать специальным способом сгенерированные ОК, которые не могут быть использованы для генерации индивидуальных ЭЦП, но могут быть использованы для подделки коллективной ЭЦП. Протокол коллективной подписи должен быть таким, что формируется целостная коллективная ЭЦП (если все пользователи, участвующие в протоколе, действуют корректно) либо протокол не приводит к формированию какой бы то ни было подписи, которая могла бы быть интерпретирована как корректная подпись для некоторого числа подписывающих $m \geq 1$.

Проверка корректности формирования ОК в протоколах коллективной ЭЦП является необходимым требованием обеспечения целостности подписи. Полное решение проблемы обеспечения целостности коллективной и индивидуальной ЭЦП связано с заданием вычисления подписи по значению хэш-функции, вычисляемой от подписываемого документа с присоединенным к нему значением ОК (или некоторого значения, зависящего от ОК подписывающих). Этот механизм связывает подписываемый документ с заданным составом подписывающих уже на уровне вычисления значения хэш-функции. Это обеспечивает невозможность подменить ни подписываемый документ ни состав подписывающих.

При использовании предложенного механизма проблема обеспечения целостности ЭЦП решается «по определению». Нарушение целостности ЭЦП потребует от потенциального атакующего выполнить успешную атаку на хэш-функцию, используемую в составе протокола коллективной ЭЦП. Предложенный механизм решает проблему целостности ЭЦП в протоколах коллективной подписи, в схеме ЭЦП Шнорра, в стандартах ЭЦП России ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, США DSA, ECDSA, Беларуси СТБ 1176.2–99, Украины ДСТУ 4145–2002 и др.

Можно показать, что протоколы коллективной ЭЦП, использующие предложенные механизмы, при значении $m = 1$ реализуют протокол индивидуальной ЭЦП, обеспечивающий целостность подписи. Протоколы коллективной подписи могут быть реализованы с использованием процедур формирования и проверки ЭЦП, рекомендуемых любым из перечисленных стандартов.

Работа поддержана грантом РФФИ № 10-07-90403-Укр_а.

Головачев Д.А., Васильев В.Н., Кишмар Р.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

СОКРАЩЕНИЕ РАЗМЕРА ЦИФРОВОЙ ПОДПИСИ В СХЕМАХ, КОМБИНИРУЮЩИХ ЗАДАЧИ ФАКТОРИЗАЦИИ И ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

С целью повышения уровня безопасности протоколов электронной цифровой подписи (ЭЦП) предложено построение криптосхем, взлом которых требует одновременного решения двух независимых трудных задач. Известен ряд схем ЭЦП, основанных на трудности решения задач факторизации чисел специального вида и дискретного логарифмирования в мультипликативной группе простого поля. Однако данные построения приводят к существенному возрастанию размера ЭЦП, что является существенным недостатком для некоторых приложений. В настоящем сообщении предлагается подход к построению сем ЭЦП, взлом которых требует одновременного решения задачи факторизации и дискретного логарифмирования по простому модулю, обеспечивающий 80-битовую стойкость при размере ЭЦП, равным 320 и даже 240 бит.

В предлагаемом подходе используется открытый ключ, включающий тройку чисел α, $p=2n+1$, где $n = qr$ (q и r – простые числа, являющиеся частью секретного ключа) и $y=\alpha^x \bmod p$, где α - число, порядок которого по модулю p равен 160-битовому простому числу γ; x – значение , являющееся элементом секретного ключа. Значение γ не является секретным, причем γ делит числа $q - 1$ и $r - 1$.

Размер числа q выбирается равным 512 бит, а числа r – 1024 бит. Таким образом, предполагается выполнение вычислений по 1536-битовому модулю, что увеличивает сложность вычислений примерно в два раза. Конкретные процедуры формирования и проверки подлинности ЭЦП могут быть заданы по аналгии с известными протоколами ЭЦП с сокращенным размером подписи, например по аналогии со схемой ЭЦП Шнорра, стандартами ЭЦП ГОСТ Р 34.10-94 и DSA. В этом случае 80-битовая стойкость обеспечивается при размере ЭЦП, равном 320 бит. При этом небольшое изменение схемы ЭЦП может обеспечить снижение размера подписи до 240 бит. Например в схеме ЭЦП, построенной по аналогии со схемой Шнорра, это достигается использованием 80-битовой хэш-функции для вычисления рандомизирующего элемента ЭЦП и 160-битовой хэш-функции для вычисления хэш-кода h от подписываемого сообщения. При этом значение h входит в уравнение проверки ЭЦП (значение α возводится в степень, равную значению суммы h и одного из элементов ЭЦП).

Обоснование стойкости построенных 240-битовых схем ЭЦП проводится путем их «вывода» из протоколов с нулевым разглашением, использующих 80-битовое значение фиксатора (разового открытого ключа), направляемого проверяющему на первом шаге выполнения указанного протокола. Схема ЭЦП выводится из протокола, путем вычисления значения хэш-функции от документа с присоединенным к нему фиксатором. Вычисленное значение является первым элементом ЭЦП, который имеет размер 80 бит, и служит запросом, правильный ответ на который может быть вычислен только владельцем открытого ключа и служит вторым элементом ЭЦП, который имеет размер 160-бит.

В предложенном подходе используется тот факт, что задачи дискретного логарифмирования по простому модулю и по составному модулю являются существенно различными, а наиболее эффективные алгоритмы дискретного логарифмирования по составному модулю связаны с его факторизацией и последующим решением задачи дискретного логарифмирования мо простым модулям, являющимися делителями составного модуля. Таким образом, за счет двукратного повышения вычислительной сложности процедур генерации и верификации ЭЦП достигнуто сокращение размера подписи в схемах ЭЦП, взлом которых требует одновременного решения задачи факторизации и дискретного логарифмирования по простому модулю.

Горячев А.А., Кирюшкин С.И., Кишмар Р.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

ВЛИЯНИЕ ВЫБОРА ПАРАМЕТРОВ НА ПРОИЗВОДИТЕЛЬНОСТЬ КРИПТОСХЕМ НА ОСНОВЕ ЗАДАЧ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ И ФАКТОРИЗАЦИИ

В криптосхемах с открытым ключом, основанных на трудности задачи дискретного логарифмирования (ЗДЛ) и задачи факторизации (ЗФ) основной вклад в трудоемкость вычислений, связанных с выполнением функциональных процедур, вносит операция возведения в большую дискретную степень по большому модулю, значение которого фиксировано. Даже быстрый алгоритм возведения в степень требует выполнения более 200 операций умножения по модулю. В связи с большим числом умножений по одному и тому же модулю в общем случае может быть реализовано модульное умножение по способу Монтгомери, что позволит ускорить операцию возведения в степень примерно в 3 раза. В случае криптосхем на основе ЗФ также используется и дополнительный механизм ускорения вычислений, состоящий в применении китайской теоремы об остатках, однако основной вклад в повышении производительности вносит реализация умножения по Монтгомери.

В случае криптосхем, основанных на ЗДЛ по простому модулю *p,* имеется еще более эффективный метод снижения вычислительной сложности функциональных процедур. Он состоит в выборе простых чисел *p*, двоичное представление которых имеет специальную структуру (в частном случае содержит два или три единичных бита, а остальные – нулевые биты). В этом случае при выполнении умножения по модулю такого вида требуется выполнить только одно арифметическое умножение и несколько арифметических сложений. Операция арифметического деления, трудоемкость которой во много раз превышает трудоемкость операции арифметического умножения, устраняется.

В результате этого трудоемкость модульного умножения уменьшается в 10 раз и более. Однако применение этого метода связано с некоторым увеличением размера электронной цифровой подписи (ЭЦП), поскольку в схемах ЭЦП на основе ЗДЛ используется основание дискретного логарифма, порядок которого *q* равен значению определенной битовой длины, которая определяет длину одного из элементов ЭЦП. При выборе простого модуля произвольного вида его можно генерировать по формуле $p = Nq + 1$, где N – случайно генерируемое четное число (подбираются различные N до тех пор, пока не будет получено простое число с указанной структурой), поэтому нет ограничений на выбор значения *q* нужного размера.

При использовании простого модуля со специальным битовым представлением следует выполнить разложение числа $p - 1$ и проверить содержится ли в этом разложении простое число, которое можно выбрать в качестве q. Поскольку простых чисел со специальной структурой сравнительно мало, то не для всех размеров параметра q удастся найти в указанном разложении простой множитель с размером близким к размеру q. Потребуется выбрать множитель несколько большего размера (выбор меньшего размера приводит к снижению стойкости криптосхемы), а это приводит к увеличению размера подписи.

В криптосхемах, основанных на трудности ЗДЛ на эллиптической кривой (ЭК), заданной над простым полем $GF(p)$ ограничений на выбор простого числа со специальной структурой двоичного представления не имеется, поскольку для заданного значения p порядок кривой определяется коэффициентами, входящими в уравнение ЭК. Добиться нужного значения порядка кривой можно путем перебора указанных коэффициентов. Аналогичные замечания имеют силу и в случае задания ЭК над двоичными многочленами.

Горячев А.А., Кирюшкин С.И., Новикова Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

ОСОБЕННОСТИ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ ПО РАЗЛИЧНЫМ МОДУЛЯМ И СИНТЕЗ КРИПТОСХЕМ НА ЕЕ ОСНОВЕ

Вычислительная трудность задачи дискретного логарифмирования (ЗДЛ) широко используется для синтезе криптосхем с открытым ключом. Эта задача определяется над конечными циклическими группами, например над мультипликативной группой колец классов вычетов по модулю m, в частном случае m равно 1024-битовому простому числу p или составному числу n, данному произведению 512-битовых сильных простых чисел. В современной криптографии важнейшие практически используемые алгоритмы электронной цифровой подписи (ЭЦП) основаны на ЗДЛ на эллиптической кривой (ЭК), заданной над конечными полями. Известны общие методы дискретного логарифмирования, которые абстрагируются от конкретного вида групповой операции и вида элементов группы. Эти методы имеют экспоненциальную трудоемкость.

Наибольшую трудоемкость данные методы имеют в случае, когда порядок группы является простым числом. Трудоемкость общих методов решения ЗДЛ (метод Полларда, метод больших и малых шагов) определяется наибольшим простым делителем порядка группы. При правильном выборе ЭК для задачи логарифмирования на кривой известны только общие методы, поэтому на практике могут применяться крпитосхемы на основе ЭК, порядок которых равен от 160 бит до 320 бит. Для решения ЗДЛ в конечном простом поле известны специальные методы решения, имеющие субъэкспоненцильную сложность (метод вычисления индексов).

В случае ЗДЛ по составному модулю m известные специализированные методы решения связаны с факторизацией модуля, вычислением дискретного логарифма по модулю равному каждому простому делителю m и последующим применением китайской теоремы об остатках. Если составной модуль равен трудно разложимому числу n, то сложность ЗДЛ будет определяться сложностью факторизации числа n.

Задача факторизации (ЗФ) рассматривается как трудная задача, не зависящая от ЗДЛ по простому модулю. Тем не менее, наиболее эффективные методы решения двух последних задач имеют примерно равную сложность при равном размере модулей. Можно показать, что алгоритм вычисления дискретного логарифма по составному модулю может быть преобразован в метод факторизации модуля (решение ЗДЛ может быть использовано для вычисления функции Эйлера от модуля, а по последнему значению легко вычислить делители модуля). Это означает, что ЗФ не проще, чем ЗДЛ по составному модулю n, и показывает принципиальное отличие ЗДЛ, заданной над простым и трудно разложимым модулем. Появление прорывных методов решения ЗДЛ по простому модулю не означает появление прорывных решений ЗФ.

Принципиальное отличие ЗДЛ по простому и составному модулю дает основание рассматривать ряд схем ЭЦП, основанных на ЗДЛ по составному модулю. Интерес к синтезу схем ЭЦП данного типа связан с тем, что для них достижим уровень 80-битовой стойкости при длине подписи, равной 320 и даже 240 бит, что существенно меньше размера подписи для известных схем ЭЦП, основанных на ЗФ (криптосистема Рабина, RSA).

Другое применение ЗДЛ по модулю n связано с разработкой алгоритмов коммутативного шифрования, основанных на трудности ЗФ, а также основанных на трудности одновременного решения ЗФ и ЗДЛ по простому модулю.

Отдельный случай составляет ЗДЛ по простому модулю вида $p = 2n + 1$, где n – трудно разложимое число, при основании, порядок которого равен одному из двух больших простых делителей n. Если значение p использовать как элемент открытого ключа, то тогда порядок основания может быть использован как секретное значение. Тогда непосредственное применение метод вычисления индексов затрудняется.

Емелин В.И.
Россия, Санкт-Петербург, ОАО «Научно-исследовательский институт Вектор»

ИНФОРМАЦИОННЫЕ УГРОЗЫ И МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АСУ КРИТИЧЕСКИМИ СИСТЕМАМИ В РЕЖИМЕ САНКЦИОНИРОВАННОГО ДОСТУПА

Анализ существующих исследований в области информационной безопасности показывает, что значительное число публикаций посвящено защите АСУ от угроз несанкционированного доступа, в то время как продолжают совершенствоваться методы и средства информационного воздействия на подсистемы добывания, передачи и обработки данных в процессе реализации ими своих функций.

Выделим два типа информационных угроз АСУ критическими системами, которые осуществляются в режиме санкционированного доступа:

1. Радиоэлектронное воздействие на средства наблюдения, связи и обработки информации, что приводит к снижению ее достоверности, полноты и своевременности, возникновению дезинформации;

2. Воздействие человеческого фактора на процесс ввода и обработки информации, что приводит к «загрязнению» базы данных неполной, несвоевременной и недостоверной информацией.

Соответственно, если методы обеспечения информационной безопасности от первого типа угроз можно определить как защиту от высокопрофессионального противника, то защиту от второго типа угроз – как защиту от своих и их преднамеренных или случайных действий.

Информационная безопасность АСУ критическими системами (по определению) обеспечивается: 1) нейтрализацией возмущения, благодаря чему предотвращается или снижается его уровень; 2) повышением порога безопасности, преодоление которого переводит систему в неустойчивое состояние. При теоретико-множественном описании по критерию информационной безопасности задается множество двух состояний АСУ: устойчивое (защищенное) S_1 и неустойчивое (незащищенное) S_2. Каждому свойству S_i назначается переменная X_i, с помощью которой определяются его изменения. Процедура наблюдения свойств АСУ S_i по изменению переменной X_i определяется в системе информационной безопасности по значению параметров $F_i(p,d,t)$, где p – полнота, d – достоверность и t – своевременность информации. Таким образом, отношения между переменными X_i и параметрами F_i характеризуются оцениваемым значением качества информации. При задании порога качества информации (порога устойчивости) определяется состояние защищенности АСУ. Соответственно информационная безопасность АСУ критических систем обеспечивается методами, связанными с повышением полноты, достоверности и своевременности информации.

Жаринов Р.Ф., Башун В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

АДАПТАЦИЯ ПРОДУКТА RSA DLP ДЛЯ РОССИЙСКОГО РЫНКА

В докладе рассматривается средство защиты от утечки конфиденциальной информации (Data Leak Prevention, DLP). Основными задачами DLP-продукта являются обеспечение возможности обнаружения случайного или умышленного несанкционированного использования информации сотрудниками компании, наличие возможностей автоматического или ручного анализа произошедших событий и передаваемой информации.

DLP-продукт может быть использован для предотвращения утечки конфиденциальных данных организации. Примером таких данных может быть финансовая информация, персональные данные сотрудников, проектная информация, и т.п.

Существует несколько основных программных комплексов, которые могут быть отнесены к классу DLP систем. В докладе рассматривается продукт RSA DLP. Несмотря на большое количество внедрений за рубежом, данный продукт слабо представлен на российском рынке. В докладе рассмотрены основные функциональные возможности системы, каналы передачи данных, которые может контролировать RSA DLP. Рассматривается, как именно определяются принадлежность данных к конфиденциальным, объясняются такие элементы системы, как элемент информации, сущность, политика безопасности.

RSA DLP позволяет выделять конфиденциальные данные при:

– передаче по сетям,

– обработке на личных компьютерах сотрудников,

– хранении в корпоративной сети (общих ресурсах хранения файлов, базах данных и других депозитариях данных).

Рассматриваются основные достоинства и недостатки данного продукта. К основным недостаткам, которые препятствуют успешному внедрению системы на российском рынке, можно отнести:

– отсутствие локализированных политик, адаптированных словарей и их официальной поддержки для Российской Федерации;

– поддержка узкого круга кодировок.

В результате проведенных исследований можно сделать вывод, что продукт RSA DLP является перспективным, но требующим адаптации для работы с русским языком и продвижения на российском рынке. Необходимо отметить, что RSA Data Technologies предпринимает активные шаги для поддержки русскоязычных кодировок. Вместе с тем, представляется необходимым сделать ряд шагов в целях успешного внедрения данного продукта в России для его локализации. В докладе рассматриваются возможные направления дальнейшего развития продукта:

– анализ и разработка национальных шаблонов и общих политик безопасности (словарные базы, регулярные выражения и т.д.);

– локализация интерфейса и форм отчетности.

В связи с вступлением в действие федерального закона №152-ФЗ «О персональных данных» и ростом внимания крупных коммерческих и государственных организаций к проблемам утечки персональных данных клиентов и сотрудников, отдельное внимание уделено разработке политик для обнаружения и/или блокировки несанкционированной передачи персональных данных.

Зегжда Д.П., Зегжда П.Д., Калинин М.О., Коноплев А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ПОСТРОЕНИЕ БЕЗОПАСНЫХ ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ИТКС

Постоянный рост скоростей передачи данных, прежде всего за счет появления и внедрения новых аппаратных платформ, актуализирует задачу обеспечения информационной безопасности в высокопроизводительных инфотелекоммуникационных системах (ИТКС). Внедрение в инфраструктуру современной сети существующих средств (в том числе сертифицированных) обеспечения безопасности приводит к значительному снижению производительности защищаемой системы. С целью взаимоувязывания скоростных показателей средств защиты и ИТКС необходим комплекс средств активного мониторинга безопасности, позволяющий оперативно анализировать состояние каждого узла сети, своевременно выявлять нарушения правил политик информационной безопасности и сигнализировать персоналу, ответственному за принятие ответных управляющих мер.

Построение высокопроизводительной системы мониторинга безопасности инфотелекоммуникационных систем (ВСМБ) сопряжено с необходимостью решения комплекса технических задач:

– представление обобщенного состояния ресурсов инфраструктуры ИТКС в реальном масштабе времени;

– сбор, обработка и анализ (включая ретроспективный анализ) информации о параметрах, характеризующих состояние контролируемой инфраструктуры ИТКС;

– автоматический мониторинг безопасности в реальном времени, проводимый над разветвленными и гетерогенными ресурсами инфраструктуры ИТКС с минимальной нагрузкой на сеть;

– оперативное оповещение администраторов сети о потенциальных нарушениях безопасности и функционирования контролируемых ресурсов.

У контролируемым ресурсам относятся объекты и процессы ИТКС: аппаратно-программные комплексы, ПО, информационные ресурсы, технологические процессы обработки информации.

Важной функциональной составляющей ВСМБ является анализ поведения меняющихся со временем показателей и расчет прогноза состояния ИТКС в будущем. С этой целью система анализирует накопленную статистическую информацию с применением математических алгоритмов, основанных на теории нейросетей, генетических алгоритмов и теории хаоса, что позволяет предвидеть поведение различных элементов инфраструктуры сети и своевременно принимать решение о нарушении правил политики безопасности.

Условием успешного решения задачи активного мониторинга безопасности ИТКС в реальном масштабе времени является осуществление высокопроизводительного сбора и обработки параметров безопасности, поступающих от различных источников. При этом уровень пропускной способности ВСМБ должен быть сопоставим с тем, что обеспечивают современные активные сетевые устройства. Это способствует значительному повышению стоимости внедрения, усложняет процесс конфигурирования такой системы, а также приводит к возникновению конфликтов между взаимодействующими элементами распределенной системы. Решением является предлагаемый авторами подход к использованию многопроцессорного кластера, выполняющего обработку и анализ данных мониторинга в параллельном режиме за счет применения универсальной аппаратной сетевой вычислительной платформы RSCB-X.

Основные преимущества ВСМБ:

– использование в качестве основы многопроцессорного кластера, позволяющего повысить эффективность обработки и расширить возможности используемых интеллектуальных методов;

– постоянный автоматизированный контроль безопасности информационно-телекоммуникационных ресурсов в масштабе реального времени позволит придать мониторингу активный характер;

– высокопроизводительная платформа кластерной системы позволяет решить задачу прогнозирования событий в сети, что обеспечивает опережающую стратегию мониторинга.

Отличительные особенности ВСМБ – поддержка балансировки нагрузки поступающих данных и распределение потоков между экземплярами ПО, выполняющего анализ безопасности, которые функционируют на виртуальных машинах кластера.

Благодаря аппаратной реализации механизма виртуализации исполняющихся экземпляров ПО, разделению трафика на контролируемый и прочих типов, балансировке нагрузки, становится возможен мониторинг безопасности в масштабе реального времени без снижения пропускной способности ИТКС.

Совокупность этих преимуществ позволит контролировать безопасность сложных ИТКС, что особенно важно в свете решения задач электронного государства, включая защищенную обработку персональных данных и оказание цифровых услуг населению.

Зегжда Д.П., Москвин Д.А., Босов Ю.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

РАСПОЗНАВАНИЕ ОБРАЗОВ НА ОСНОВЕ ФРАКТАЛЬНОГО СЖАТИЯ

В настоящее время методы распознавания образов широко применяются в сфере обеспечения безопасности, начиная с идентификации и аутентификации пользователей компьютеров и закачивания обнаружением террористов в местах массового скопления людей. Эффективность применяемых методов определяется двумя основными параметрами: точность и время распознавания. Эти параметры связаны и, как правило, обратно пропорциональны, т.е., чем выше точность распознавания, тем больше для этого требуется времени.

Большинство современных методов распознавания образов позволяют обеспечить достаточно высокую точность (более 90%), но время, которое требуется для этого, ограничивает сферу применения данных методов. Особенно это заметно при реализации различных поисковых задач, например, поиск в Интернете человека по его фотографии (эталонному изображению). Поэтому на сегодняшний день актуальной является задача повышения скорости распознавания образов с сохранением высокой точности.

Для решения данной задачи авторами предлагается метод распознавания образов, основанный на фрактальном сжатии. Данный метод позволяет за счет сравнения характеристик найденных фракталов, а не самих изображений, существенно увеличить скорость сравнения (классификации) образов, сохраняя при этом высокую точность.

С использованием предлагаемого метода распознавание образов осуществляется в следующем порядке:

1. Построение базы характеристик фрактальных областей эталонного изображения.
2. Поиск образа (лица человека) на сравниваемом изображении методом Виолы-Джонса.
3. Выделение признаков образа – поиск фрактальных областей на сравниваемом изображении.
4. Сравнение характеристик выделенных фрактальных областей с характеристиками фрактальных областей эталонного изображения.
5. Принятие решение о «похожести» образов на основании метода пороговых значений.

В качестве метода поиска лица на изображении может также использоваться любой другой метод, позволяющий с достаточной точностью выделить область лица. Аналогично для принятия решения о «похожести» образов вместо метода пороговых значений могут использоваться методы нечеткой логики, нейронные сети и др.

Сравнение данного метода с аналогами (метод выделения ключевых точек, метод анализа частотных характеристик, метод анализа геометрических характеристик лица и т.д.) показывает, что скорость сравнения изображений по методу фрактального сжатия выше примерно в два раза. Точность сравнения при этом остается на уровне ≈95%.

К недостаткам разработанного метода можно отнести медленную скорость создания базы характеристик фрактальных областей эталонного изображения. Однако этот недостаток несущественен, т.к. построение такой базы выполняется всего один раз для каждого эталонного изображения.

Таким образом, авторами разработан метод распознавания образов, основанный на фрактальном сжатии, который обеспечивает высокую скорость распознавания с высокой точностью. Данный метод может применяться для идентификации и аутентификации пользователей, автоматизации работы пропускных пунктов, поиска людей по фотографии в сети Интернет или в специализированных базах данных, выделения интересующих изображений из фото – или видеоданных, передаваемых по каналам связи.

Зуров Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций

АКТУАЛЬНЫЕ УГРОЗЫ УТЕЧКИ КОРПОРАТИВНЫХ СЕКРЕТОВ И СПОСОБЫ ЗАЩИТЫ

Как известно, ценность корпоративных секретов или инсайдерской информации измеряется прибылью, которую могут получить третьи лица, за счет неправомерного использования такой информации. Далее для краткости будем называть такую информацию защищаемой, как это принято в нормативных документах в области информационной безопасности. Статистические исследования угроз указывают на основной канал утечки защищаемой информации, проходящий через сотрудников компании допущенных к обработке защищаемой информации.

При этом основными факторами, воздействующими на защищаемую информацию, являются:

– передача информации по открытым линиям связи;
– копирование защищаемой информации на незарегистрированный носитель информации;
– передача носителя с защищаемой информацией лицу, не имеющему права доступа к ней;
– утрата носителя с защищаемой информацией;
– доступ к защищаемой информации в обход установленных правил разграничения доступа.

Таким образом, цель защиты информации от инсайдеров может быть сформулирована как недопущение возможности использования сотрудниками защищаемой информации за пределами заданного периметра. В формулировке цели присутствует противоречие с одной стороны необходимо обеспечить пользователей всем необходимым инструментарием для эффективного решения поставленных задач, связанных с автоматизированной обработкой информации, а с другой стороны ограничить функционал этого инструментария, сделав автоматизированную систему обработки информации замкнутой.

Произведём оценку возможности применения существующих способов решения. Средства защиты информации от несанкционированного доступа позволяют ограничить круг лиц, допущенных к той или иной защищаемой информации, наделив их полномочиями по её использованию, в том числе строго запретив либо полностью разрешив копирование всей информации, (включая защищаемую) на съёмные носители информации, что не разрешает упомянутого выше противоречия. Применение избирательного ограничения вывода защищаемой информации на съемные носители информации удаётся достичь при реализации требования руководящих документов Гостехкомисии РФ – управление потоками конфиденциальной информации. Но при этом у лиц, наделённых полномочиями записи защищаемой информации на маркированные носители информации, остаётся потенциальная возможность несанкционированного размножения такой информации, несмотря на наличие в системе защиты информации подсистемы регистрации.

Криптографические методы, обладая широким спектром решаемых задач, по своему первоначальному замыслу направлены на защиту информации от аутсайдеров и не должны обеспечивать защиту информации от инсайдеров в силу известности ключа обладателю информации.

Но если предложить скрыть значение ключа или его части от его законного обладателя путём инкапсуляции ключа внутри автоматизированной системы обработки информации, при этом, обеспечив невозможность его экспортирования, а также невозможность получения пользователями ключевых носителей удастся достичь поставленной цели.

Предлагаемый способ сокрытия ключа от его владельца позволяет:

– полностью исключить возможность работы пользователей с защищаемой информацией за пределами охраняемой территории путём выноса носителей с защищаемой информацией;
– обеспечить защиту от утечки защищаемой информации, путём её передачи через открытые линии связи с возможностью оперативного оповещения о несанкционированных попытках отправки защищаемой информации;
– производить маркировку электронных сообщений, содержащих защищаемую информацию;
– усилить разграничение доступа пользователей к защищаемым ресурсам информационной системы, путём распределения ключей между ними.

Калинин М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

МЕТОД ОБЕСПЕЧЕНИЯ ВЫСОКОЙ ДОСТУПНОСТИ И ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА ОСНОВЕ КОНТРОЛЯ ФУНКЦИОНАЛЬНОЙ ЦЕЛОСТНОСТИ

При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Научные и научно-педагогические кадры инновационной России» (государственный контракт №02.740.11.0659/140808001 от 29 марта 2010 г.)

При обеспечении высокой доступности и защищенности информационно-телекоммуникационных систем (ИТКС) одной из ключевых проблем является обеспечение

устойчивой безопасности ИТКС в ходе эксплуатации, т.е. необходимость постоянно поддерживать выполнение предъявляемых требований, касающихся обеспечения стабильного функционирования и информационной безопасности, что становится особенно актуальным при установке новых компонентов и при любых изменениях параметров при управлении безопасностью. Это обуславливает необходимость в расширении понятия целостности до фиксации допустимого диапазона варьирования среды, в котором одновременно выполняются требования безопасности (ТБ) и сохраняется необходимый функционал ИТКС.

В дополнение к нормативному пониманию целостности как свойства сохранения правильности и полноты информационных активов (согласно ГОСТ Р ИСО/МЭК 13335-1) введем понятие функциональной целостности ИС, т.е. взаимосогласованности параметров компонентов ИТКС, включая параметры системного и прикладного программного обеспечения, а также средств защиты информации (СЗИ).

Все компоненты ИТКС разделяются на два класса:

– стабильные компоненты;

– изменяемые компоненты.

К стабильным компонентам относятся функциональные модули, которые создавались при разработке ИТКС. Их изменение требует дополнительного проектирования и связано с модификацией системы, повторными испытаниями, настройками и т.д.

К изменяемым компонентам относятся модули, которые могут быть произвольно модифицированы или внедрены в ИТКС, и этот процесс осуществляется в результате управления системой. Применение криптографических методов позволяет решить проблему целостности стабильных компонентов. В то же время в ходе управления ИТКС проявляются изменения, которые серьезно влияют на безопасность и стабильность функционирования ИТКС, но для которых криптографические методы неприменимы, например:

– настройка безопасности установленных приложений (например, изменение опций безопасности прикладного программного обеспечения или применение пакета обновлений);

– изменение пользовательского состава, приводящее к модификации операционной среды и ее настроек (например, задание прав доступа или нового профиля пользователя).

Для обеспечения функциональной целостности ИТКС, учитывающей параметрический состав системы и его изменчивость в ходе функционирования, в работе представлен метод контроля, базирующийся на определении области пересечения всех парных областей согласующихся параметров (пространства целостности). Мерой целостности является мощность построенного пространства целостности. При этом любые парные отношения в пространстве целостности являются толерантными, т.е. рефлексивными и симметричными. Указанное свойство показывает, что предложенная модель и мера целостности сохраняются при любой комбинации элементов ИТКС, для которых построено пространство целостности.

При соблюдении ТБ в пространстве целостности образуется пространство безопасности ИТКС, что позволяет перейти от жесткого понимания безопасности как точечной характеристики к области параметров, в которой как соблюдаются требования информационной безопасности, так и обеспечена взаимосогласованность параметров компонентов ИТКС.

Калинин М.О., Коноплев А.С., Марков Я.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

КОНТРОЛЬ ВЫПОЛНЕНИЯ ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В GRID-СИСТЕМАХ

Технология Grid – разновидность распределенных компьютерных вычислений, в которой «виртуальный суперкомпьютер» представлен кластером вычислительных систем, соединенных с помощью сети и обеспечивающих совместное выполнение огромного количества заданий. Одна из проблем обеспечения безопасности в Grid-системах – отсутствие гарантированности защиты ресурсов Grid-систем. Решение, предлагаемое авторами, – анализ выполнения требований политик информационной безопасности, что позволит верифицировать безопасность Grid-систем и выявлять изъяны защиты, обусловленные небезопасной конфигурацией механизмов защиты.

Анализ механизмов безопасности наиболее популярных Grid-сред Globus Toolkit, UNICORE, gLite, Gridbus, BOINC позволяет выделить два ключевых механизма безопасности: аутентификацию и авторизацию. ПО Globus Toolkit представляет наиболее полный «срез» подсистемы безопасности Grid-систем, что позволяет его рассматривать в качестве универсального объекта исследования.

Известно два способа доступа пользователя к ресурсам, которые предоставляет провайдер ресурсов:

1. С помощью сервиса контроля доступа GRAM (Grid Resource Allocation and Management), с помощью которого пользователь может передавать и запускать свои приложения на провайдере, а затем получать результат их исполнения;

2. С помощью Web-сервисов, когда каждому сервису соответствует набор операций, к которым пользователь Grid-ресурсов может получать доступ.

Механизмы авторизации в каждом случае различны: в GRAM используются механизмы gridmap и VOMS, в web-сервисах – расширенный набор, включающий gridmap, CAS, VOMS и т.д. Тогда модель контроля доступа Grid-системы может быть представлена формально в виде логических функций:

1. Проверка наличия у пользователя прав доступа к объекту файловой системы, расположенному на провайдере ресурсов;
2. Проверка для пользователя наличия доступа к операции веб-сервиса, расположенного на провайдере ресурсов, либо наличие права доступа из множества к свойству веб-сервиса.

Анализ выполнения политик безопасности заключается в том, что в зависимости от типа требования определяется набор параметров (состояние) Grid-системы, которые необходимы для проверки данного требования. Требование представляет собой совокупность параметров соответствующей функции контроля доступа (для требований первого типа – функция 1, для второго – функции 2). Верификация безопасности выполняется путем сопоставления требований политики информационной безопасности и текущего состояния Grid-системы. Результатом верификации является отчет о нарушениях безопасности.

Пример алгоритма проверки выполнения ограничений пользовательского доступа для объектов файловой системы Grid-системы будет представлен в докладе. Авторами реализовано программное средство, автоматизирующее верификацию требований политик информационной безопасности в Grid-системах, что позволяет автоматизировать процедуру анализа безопасности, придать ей объективный характер и тем самым повысить эффективность обеспечения безопасности ресурсов в Grid-среде.

Кишмар Р.В., Молдовян Д.Н., Сухов Д.К.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

ОБОСНОВАНИЕ СТОЙКОСТИ СХЕМ ЦИФРОВОЙ ПОДПИСИ И ИХ ПОСТРОЕНИЕ ОТ ПРОТОКОЛОВ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ

При разработке протоколов электронной цифровой подписи (ЭЦП) важным вопросом является обоснование их стойкости. В качестве одного из приемов обоснования стойкости может быть использован вывод протокола ЭЦП из предварительно построенного протокола с нулевым разглашением. В настоящем сообщении обсуждается общая схема преобразования протокола с нулевым разглашением в схему ЭЦП.

Криптографические протоколы с нулевым разглашением секрета используются для аутентификации удаленных пользователей. Они основаны на некоторых вычислительно трудных задачах и относятся к криптосистемам с открытым ключом. Общая схема функционирования таких протоколов состоит в следующем. Некоторый субъект А (доказывающий) демонстрирует знание секретного ключа, связанного с его открытым ключом. В процессе выполнения протокола субъект А доказывает некоторому другому субъекту Б (проверяющему), что он действительно знает решение задачи. Протокол с нулевым разглашением может быть реализован в виде многошаговой интерактивной процедуры, в результате которой проверяющий убеждается в том, что доказывающий знает секретный ключ, связанный с его открытым ключом, т.е. доказывающий убеждает проверяющего, что он действительно является владельцем своего ОК. При этом в ходе протокола проверяющий не получает никакой информации о секретном ключе.

В качестве примитивов протоколов с нулевым разглашением секрета используются следующие вычислительно трудные задачи:

1. Задача дискретного логарифмирования в конечной группе;
2. Задача факторизации;
3. Задача извлечения корней по модулю большого числа;
4. Задача о раскраске графа;
5. Задача поиска сопрягающего элемента в некоммутативных группах и некоторые другие.

Любой протокол с нулевым разглашением может быть преобразован с схему ЭЦП, однако вычислительно эффективные схемы ЭЦП с малым размером подписи могут быть получены не во все случая. Это достигается при использовании первых трех задач из представленного перечисления. Идея общего «вывода» протокола ЭЦП из протокола с нулевым разглашением состоит в использовании значения h-битовой хэш-функции, вычисляемого от подписываемого документа и фиксатора в качестве битовой цепочки запроса, которую можно рассмотреть как h запросов проверяющего. При этом задаются условия, при которых владелец открытого ключа (подписывающий) должен формировать h различных разовых открытых ключей до выполнения процедуры вычисления битовой цепочки запроса. Это достигается заданием процедуры вычисления хэш-функции от подписываемого документа, к которому присоединяется фиксатор в виде h сформированных разовых открытых ключей. Такое значение хэш-функции рассматривается как последовательность запросов проверяющего. Поскольку подписывающий знает секретный ключ,

соответствующий его открытому ключу, то он может вычислить правильный ответ на каждый запрос. Подпись представляет собой две последовательности значений: упорядоченное множество разовых открытых ключей (фиксатор) и упорядоченное множество ответов. Процедура проверки ЭЦП состоит в вычислении хэш-функции от подписанного документа с присоединенным к нему фиксатором и проверки всех ответов на h запросов, заданных значением хэш-функции. При использовании стойкой хэш-функции выведенная таким образом схема ЭЦП может рассматриваться как доказуемо стойкая, поскольку в результате оглашения ответов на случайные запросы никаких знаний о секретном ключе не представляются (т.е. сформированная ЭЦП не дает никакой дополнительной информации о секретном ключе).

Для сокращения размера используются такие вычислительно трудные задачи, которые позволяют реализовать протокол с нулевым разглашением всего за три шага. Примерами построений такого типа являются схема Фиата–Шамира и алгоритм ЭЦП Шнорра.

Работа выполнена в рамках ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009-2013 гг. (контракт №П635).

Клеймёнов А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

ОБЪЕДИНЕНИЕ РЕЗУЛЬТАТОВ АВТОМАТИЗИРОВАННОЙ КЛАСТЕРИЗАЦИИ ВРЕДОНОСНОГО КОДА, ВЫПОЛНЕННОЙ НЕСКОЛЬКИМИ МЕТОДАМИ

В современном мире информационные технологии выходят на первое место во всех сферах нашей повседневной жизни. Автоматизированным системам доверена обработка информации, касающейся каждого человека в большинстве стран мира. Очевидно, что доступ и манипуляция этими данными могут дать злоумышленникам огромные возможности, и с каждым годом число преступлений в данной сфере растет. Для того, чтобы преломить эту тенденцию, необходимо совершенствование как нашего законодательства, так и эффективные инструменты, призванные помочь специалистам в борьбе с киберпреступниками. Одним из таких инструментов является программный комплекс, позволяющий группировать образцы программного кода и соотносить их с конкретными людьми. В ходе разработки данной системы на текущем этапе развития выделились два принципиально отличных метода кластеризации. Первый представляет собой реализацию алгоритма на основе использования цепей Маркова в применении к бинарным данным, второй базируется на нейронных сетях. Однако очевидно, что в ходе дальнейшей разработки будет реализована поддержка новых алгоритмов. В этом случае возникнет проблема, касающаяся компоновки получаемых результатов каждого метода с целью вынесения единого решения. Предлагается присваивать каждому алгоритму свой «вес», исходя из степени его точности для анализируемых файлов. Данная характеристика устанавливается экспертом в ходе разработки программного комплекса и затем выставляется автоматически при каждом запуске на этапе определения типа данных, поданных на вход системе. Основным достоинством данного подхода является его абсолютная гибкость в случае применения к новым внедряемым алгоритмам кластеризации. Минусом является необходимость дополнительного привлечения эксперта в случае добавления в комплекс поддержки новых типов данных. Предполагается проверка выбранных экспертом коэффициентов на больших объемах данных, а также их корректировка с целью получения максимально возможной точности.

Крук Е.А, Беззатеев С.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЛЕГКОЙ КРИПТОГРАФИИ

В настоящее время с увеличением числа устройств обработки информации, имеющих ограниченные вычислительные ресурсы и используемых для хранения и передачи конфиденциальных данных, особую актуальность приобретает проблема разработки криптографических алгоритмов с низкими требованиями к производительности процессора и объему используемой памяти. Такие алгоритмы принято называть «легкими», и именно они в настоящее время наиболее востребованы в системах мобильной связи, сенсорных сетях, RFID – структурах и т.д.

Алгоритмы легкой криптографии на основе кодов, исправляющих ошибки, находят применение при решении задач практически во всех системах информационной безопасности:

1. Системы аутентификации.

– Аутентификация сообщений – использование одноразовых подписей, на основе хэш-цепочек. При этом особый интерес представляет задача увеличения числа возможных использований одного открытого ключа. Одним из возможных вариантов решений этой задачи является построение систем одноразовых подписей на основе множеств, свободных от покрытий.

– Аутентификация пользователей – наиболее сложной и востребованной задачей является задача удаленной аутентификации. Для ее решения может быть использован модифицированный алгоритм Мак Эллиса.

2. Системы обеспечения защиты информации от случайных и преднамеренных искажений. Естественным вариантом решения такой задачи является использование модифицированного алгоритма Мак Эллиса, позволяющего гибко распределять имеющуюся корректирующую способность кода на защиту от преднамеренных и случайных искажений при передаче или хранении конфиденциальных данных, а так же на защиту от несанкционированного доступа. Такой подход позволяет решить в одном устройстве задачи помехозащищенности и конфиденциальности.

3. Системы безопасного хранения и обработки информации.

– Разграничение доступа к информации. В этом случае, обычно рассматривают многоуровневые структуры доступа и коалиционные структуры. И в том и другом случае имеется возможность использования легкой криптографии основанной на хэш-цепочках и конструкциях, использующих помехоустойчивые коды.

– Обеспечение анонимности при доступе к информации, хранящихся в «облачных» сетях. Легкая криптография здесь подразумевает так же использование специальных модификаций алгоритма Мак-Элиса.

– Реализация систем скрытых вычислений, особенно актуальная при активном использовании «облачных» хранилищ баз данных.

В докладе обсуждаются возможности решения основных задач информационной безопасности алгоритмами легкой криптографии.

Козина Г.Л.
Украина, Запорожье, Запорожский национальный технический университет

ПРОТОКОЛЫ СЛЕПОЙ ПОДПИСИ НА БАЗЕ СТАНДАРТА ДСТУ 4145-2002

Стандарт цифровой подписи ДСТУ 4145-2002 основан на группе точек эллиптической кривой над расширенным полем большого порядка. Для вычисления подписи в стандарте используются преобразования элементов поля в двоичные и десятичные числа.

Предложены два протокола слепой подписи.

В первом протоколе используется традиционный подход при «затемнении» документа, что в дальнейшем позволяет подписавшему при сохранении вспомогательных параметров «узнать» свою подпись под предъявленным документом.

Во втором протоколе для затруднения «узнавания» при «затемнении» используется хеш-образ документа, возведенный в некоторую секретную степень. В качестве такой степени можно взять секретный ключ лица, формирующего документ.

Безопасность протоколов основана на вычислительной сложности задачи дискретного логарифмирования в группе точек эллиптической кривой над расширенным полем и в группе вычетов по большому простому модулю.

Кузьмина Н.Г., Маховенко Е.Б.
Россия, Санкт-Петербург, ЗАО «Регионального центра защиты информации «ФОРТ»,
Санкт-Петербургский государственный политехнический университет

ПАРАМЕТРЫ КРИПТОСИСТЕМ НА СКРЫТЫХ ОТОБРАЖЕНИЯХ ПОЛЕЙ НЕЧЕТНЫХ ХАРАКТЕРИСТИК

В настоящее время в криптографии с открытым ключом широко распространены криптосистемы, основанные на задачах разложения на множители и дискретного логарифмирования. Недостатком этих задач является их уязвимость по отношению к квантовому компьютеру: если удастся создать квантовый компьютер достаточно большой разрядности, то задачи разложения составного числа и дискретного логарифмирования в произвольной циклической группе могут быть решены с полиномиальной сложностью. Одной из «альтернативных» криптосистем, предположительно стойких к квантовому компьютеру, является криптосистема на скрытых отображениях полей (см., например Patarin J. Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. Доступно с http://www.cryptosystem.net/hfe.pdf). До сих пор основное внимание исследователей уделялось криптосистеме над полем характеристики 2. Однако требования к параметрам криптосистемы, обеспечивающим приемлемую стойкость, таковы, что алгоритм расшифрования является неэффективным и практическое использование криптосистемы затруднено.

Представлены результаты анализа криптосистем на скрытых отображениях полей нечетных характеристик. Проведены исследования зависимости характеристик криптосистемы, таких как скорость зашифрования, скорость расшифрования и время генерации ключей, от параметров криптосистемы. Даны рекомендации относительно выбора параметров и, вследствие этого, выбора используемых в криптосистеме алгоритмов. Так, чтобы не использовать трудоемкие алгоритмы

Берлекэмпа и Кантора-Цассенхауса, предлагается в качестве закрытого полинома выбирать полином второй степени, а характеристику поля сравнимой с 3 по модулю 4. Проведен анализ безопасности криптосистемы над полями нечетных характеристик. Для различных значений стойкости криптосистемы (сложность наилучшего алгоритма вскрытия 280, 2128, 2256) приведены безопасные значения параметров. Использование в криптосистеме рекомендуемых параметров и алгоритмов позволяет значительно улучшить характеристики криптосистемы при обеспечении не меньшей стойкости к атакам.

Сравнение характеристик криптосистем показало, что сложность наилучшей известной атаки для криптосистемы над полем характеристики 59 превышает 280, тогда как для полей характеристики 2 эта сложность >2128; при этом степень d закрытого полинома для поля характеристики 59 равна 2, для поля характеристики 2 имеем d = 129.

Время генерации ключей, скорость зашифрования и скорость расшифрования для расширения степени n = 19 поля характеристики 59 равны, соответственно, 0,56 сек, 2831 бит/сек, 660 бит/сек. Для расширения степени n = 80 поля характеристики 2 указанные параметры составляют 70,8 сек, 32 бит/сек и 7,4 бит/сек. Размер открытого ключа для поля характеристики 59 равен 41,5 Кб.

Латышев Д.М., Аль-Рахми Р.Я., Хо Нгок Зуй
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

ХЭШ-ФУНКЦИИ И ШИФРЫ НА БАЗЕ АЛГЕБРАИЧЕСКИХ ОПЕРАЦИЙ

Как правило в блочных шифрах (БШ) в качестве примитивов используются подстановочные и перестановочные операции преобразования входных данных, при этом подстановочные операции реализуются как табличные подстановки или с помощью управляемых подстановочно перестановочных сетей. Более редким типом БШ являются алгебраические шифры, отличающиеся использованием алгебраических операций в качестве основного криптографического примитива. Алгоритм IDEA является наиболее известным алгебраическим БШ. Основной операцией в нем является умножения по модулю простого числа 65537. Данный алгоритм обладает достаточно высокой производительностью как при аппаратной, так и при программной реализации. Технический интерес к алгебраическим БШ состоит в том, что при соответствующем построении программный код, реализующий такие шифры, имеет достаточно малый размер. Это представляет интерес для применения в средствах защиты информации от несанкционированного доступа для реализации контролируемой загрузки ЭВМ и электронных ключах с встроенными криптографическими функциями. Достоинством алгебраических блочных шифров и хэш-функций является также и то, что для них не так остро стоит вопрос об отсутствии потайных лазеек, которые потенциально могли быть встроены разработчиками алгоритмов. В настоящей работе рассматриваются подходы к разработке алгебраических БШ и хэш-функций, а также обсуждаются различные типы конечных алгебраических структур, перспективных для разработки производительных криптосистем.

Значительный интерес для синтеза алгебраических БШ и итеративных хэш-функций представляют операции умножения в различных алгебраических структурах: кольцах вычетов по модулю, простых конечных полях, конечных кольцах и полях многочленов, конечных кольцах и полях, заданных в явной векторной форме и конечных кольцах матриц. Все эти виды операций умножения обладают хорошим лавинным эффектом и могут быть выполнены с помощью стандартных арифметических операций, реализуемых как элементарные команды микропроцессора.

В качестве одного из основных принципов проектирования алгебраических БШ и хэш-функций было использовано комбинирование алгебраических операций из различных структур. Данный принцип ориентирован на обеспечение стойкости к атакам на основе известных и специально подобранных текстов. Исследования статистических свойств ряда разработанных шифров и итеративных хэш-функций показали, что их статистическое тестирование не позволяет отличить шифрующее и «хэширующее» преобразование от случайного блочного преобразования.

Используя простые числа со специальной структурой, обеспечивающей достаточно низкую сложность операции модульного умножения (за счет исключения операции арифметического деления) были разработаны хэш-функции и БШ, имеющие достаточно высокое быстродействие. В разработанных алгоритмах входные блоки данных разбиваются на подблоки интерпретируемые как элементы коммутативной группы конечного поля, как многочлены, как вектора или как матрицы в зависимости от конкретного варианта используемой алгебраической структуры.

Разработанные алгоритмы представляют интерес для построения вероятностных шифров и алгоритмов «отрицаемого» шифрования. Рассмотрены варианты построения на основе алгебраических операций алгоритмов защитного контрольного суммирования различных типов.

Лернер В.Д., Беззатеев С.В.
Россия, Санкт-Петербург, ООО «Космос СПб», Санкт-Петербургский государственный университет аэрокосмического приборостроения

ОСНОВНЫЕ ПРИНЦИПЫ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ДЛЯ ДОСТУПА К ИНФОРМАЦИИ В «ОБЛАЧНЫХ» ХРАНИЛИЩАХ ДАННЫХ

Информационные технологии активно мигрируют в сторону «облаков», а одним из приоритетных направлений развития являются «облачные» хранилища данных.

«Облачное» хранилище позволяет держать корпоративные данные на распределенных серверах, представляющих с точки зрения клиента один большой виртуальный сервер («облако»). При этом сам клиент не имеет какой-либо информации о том, что из себя представляют эти виртуальные сервера, где они находятся, какой они производительности, какие на них установлены операционные системы, базы данных, какие технологии по ускорению доступа к данным используются. Для клиента важен лишь безопасный доступ к данным с гарантированной скоростью.

При этом, очевидно, что клиент не может полагаться на системы безопасности, предлагаемые как интернет-провайдерами трафика, так и владельцами «облачных» хранилищ, в связи с тем, что администраторы вышеупомянутых серверов имеют неограниченные права доступа к системам, а производители коммуникационного оборудования, зачастую, отказываются его продавать без наличия у них неограниченных прав по администрированию. Следовательно, информация хранимая и обрабатываемая в «облачных» хранилищах должна быть зашифрована, а пользователи с различными привилегиями должны иметь доступ только к той информации, на которую они обладают полномочиями, согласно своей корпоративной иерархии. При этом алгоритм шифрования информации выбирается единый для всех пользователей, а задача построения таких систем сводится к созданию алгоритма распределения ключей, удовлетворяющего требованиям конкретной иерархической структуры компании.

Существует два основных подхода к решению задачи распределения ключей в иерархических системах. В первом ключи рассчитываются снизу-вверх и для добавления нового пользователя требуется перерасчет всех ветвей иерархии, а следовательно – дешифрование, а затем шифрование всей информации в «облачном» хранилище, в другом – ключи рассчитываются сверху вниз, и изменение структуры иерархии не приводит к перерасчету всех ключей пользователей, а только в определенной ветви иерархии.

При первом подходе стоимость интернет трафика будет значительной и данные алгоритмы экономически невыгодны. Распределение ключей при использовании второго подхода основывается на получении ключей отдельными пользователями при помощи некой хэш-функции и позволяет вычислять ключи подчиненных пользователей любого яруса, что приводит к минимальным затратам при изменении структуры иерархии и организации эффективного доступа к информации, находящейся в «облачных» хранилищах. В докладе предлагается вариант построения такой системы распределения ключей, оценивается эффективность и защищенность предложенного метода.

Нечаев Ю.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

УЯЗВИМОСТИ МОБИЛЬНОЙ ПЛАТФОРМЫ APPLE IOS

Структура операционной системы iOS основана на MacOS, обладает ядром Darwinи имеет четыре слоя абстракции. Это ядро системы, его сервисы, медиа и APICocoaTouch. Само по себе приложение с расширением .ipa представляет собой архивный файл, который содержит приложение для устройства Apple. Все ipa-файлы предназначены только для запуска на архитектуре ARM устройств iPhone, iPodtouchи iPad. Эти файлы имеют четко выраженную структуру для распознавания магазином iTunesStore. Каждый ipa-файл имеет электронную подпись разработчика, и данный факт в некоторой мере предотвращает возможность установки нелегально скопированных приложений на устройство. Тем не менее, уже давно были найдены способы, благодаря которым все попытки обезопасить разработчиков от финансовых потерь свелись на нет.

На сцене взлома устройства и механизма подписки приложений за уже довольно продолжительное время засветилось несколько ключевых фигур. Прежде всего, это создатель программы Cydia–JayFreeman, так же известный, как Saurik. Основной задачей Cydia является предоставление графического интерфейса для устройств, которые были взломаны. С помощью этой программы можно легко добавить новые репозитории, устанавливать пакеты, в том числе и те, которые позволяют устанавливать на устройство неподписанные приложения. Так же стоит отметить команду Dev-Team, которая выпускает утилиты для взлома мобильных устройств Apple и разблокировки оператора. Мы знаем, что Apple подписывает контракты с различными операторами связи для взаимовыгодных условий. Вместе с тем, когда пользователь покупает устройство, он подписывает контракт, благодаря которому он тратит намного меньше денег на покупку, а разницу платит в течение года как плату за услуги связи. Как пример можно привести оператора AT&T в США

и Orangев Англии. Так или иначе, у людей возникала потребность в разблокировке аппарата для работы с другими операторами, и Dev-Team знала, как эту потребность удовлетворить. Отдельно хочется упомянуть comex, который в 2007 году представил свой первый продукт JailbreakMe 1.0, созданный с группой из 9 разработчиков. Это приложение устанавливало в телефон специальный пакетный менеджер, который открывал широкие возможности для дальнейших действий с помощью уязвимости в TIFF файлах браузера Safari. Но самым ошеломляющим был продукт JailbreakMe 2.0 “Star”, который позволял пользователю просто зайти на специальный сайт, сделать жест пальцем по сенсорному дисплею, подобный разблокировке экрана, и процедура взлома запускалась прямо из браузера. Это можно было сделать даже в магазинах Apple, где аппараты были подключены к WiFi и установлены на специальных стендах. Уязвимость была в библиотеке FreeType, использовавшейся для рендеринга PDF-страниц.

Программным методом защиты устройства от взлома является, прежде всего, выпуск новых версий iOS с новыми версиями ядра, так как именно с его модификациями связаны некоторые аспекты работы взломщиков. Так же стоит отметить то, что каждая версия обновленной системы iOS обновляет и прошивку на модеме устройства. Этот процесс необратим, поэтому зачастую приходится заново собирать модифицированное ядро, исходя из новой архитектуры устройства. Это и является главным сдерживающим фактором для быстрого выходя нового ПО для взлома.

Так что же именно нужно сделать, чтобы установить взломанное приложение на устройство? Прежде всего, его нужно переподписать в среде разработки XCode. Эта среда работает в MacOS и представляет возможности для разработки приложений на Cocoa и CocoaTouchфреймворке для MacOS и iOS соответственно. Помимо этого нужно произвести процедуру взлома самого устройства (jailbreak) для того, чтобы оно не отклоняло попытки установки приложений с легитимной подписью. Для этого используется разнообразный набор утилит, который зависит от версии операционной системы и версии прошивки модема устройства. Стоит отметить, что в более ранних версиях iOS была возможность сохранения SHSH таблицы, которая позволяла установить более раннюю версию системы, если что-то пойдет не так. Эта таблица уникальна для каждого устройства. Но такой возможности уже нет, а те, кто успел это сделать до запрета Apple, до сих пор могут установить старые версии системы. После проведения всех описанных выше действий приложение установится в устройство через стандартный медиа плеер iTunes, который используется для синхронизации музыки, приложений, контактов и календарей.

Стоит отметить, что потери от нелегального копирования приложений огромны. За первый квартал 2011 года из iTunesStore было загружено 15 миллиардов приложений. Для сравнения, за первый квартал 2010 года было загружено 3 миллиарда. Даже при небольшом проценте нелегального копирования убытки огромны. Существует и обратная сторона медали. Как показало исследование некоторых компаний, занимающихся разработкой софта для iOS, выпуск пиратской версии продукта способствует его активному распространению в платном магазине. Но такая динамика сохраняется только на начале продаж. Тем не менее, не стоит напоминать, как важно для группы разработчиков «выстрелить» проект.

Никифоров В.В., Шкиртиль В.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ЗАЩИТА ЦЕЛОСТНОСТИ ДАННЫХ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ РЕАЛЬНОГО ВРЕМЕНИ

Проблема обеспечения целостности информационных ресурсов, стоит в ряду ключевых проблем логической корректности программных приложений для систем реального времени (СРВ). Защита информационных ресурсов, доступных различным задачам (разделяемых информационных ресурсов), обеспечивается использованием специальных синхронизирующих механизмов (например, мьютексов). Локальные статические информационные ресурсы конкретной задачи недоступны другим задачам, но при периодической активизации задачи могут использоваться однотипными заданиями (экземплярами этой задачи), порождаемыми в результате каждой такой активизации. Необходимость защиты целостности статических информационных ресурсов возникает в том случае, если интервалы существования однотипных заданий могут пересекаться. Подобные пересечения возможны, если время отклика задачи (максимально возможная длина интервала существования соответствующих ей заданий) превышает продолжительность периода ее активизации. В таком случае защита целостности статических информационных ресурсов может быть обеспечена использованием тех же синхронизирующих механизмов, которые используются для защиты разделяемых информационных ресурсов. Однако, для большинства задач СРВ время отклика не превышает периода, для таких задач угроза нарушения целостности локальных ресурсов отсутствует и в этом случае использование синхронизирующих механизмов защиты означало бы ненужные затраты памяти и процессорного времени. Это обстоятельство является одной из причин, вызывающих актуальность разработки методов, обеспечивающих оценку величины времени отклика задач для многозадачных программных приложений и в частности для программных приложений СРВ.

Исследования, направленные на создание методов оценки времени отклика задач в СРВ развиваются с 1980-х годов. Были, в частности, разработаны алгоритмы оценки времени отклика для систем с независимыми вытесняемыми и невытесняемыми задачами в программных приложениях с фиксированными приоритетами при их реализации компьютерами с классическими одноядерными процессорами. Были построены обобщения этих алгоритмов на случай программных приложений с взаимозависимыми задачами, разделяющими общие информационные ресурсы. В последнее десятилетие предложены методы, ориентированные на оценку времени отклика задач в программных приложениях СРВ, реализуемых многоядерными процессорами. Но для распределенных СРВ, проблема создания методов оценки времени отклика задач остается открытой. В работах по этой тематике трудности, связанные с проверкой выполнения временных ограничений для распределенных систем, отмечаются, в такой форме: «Мы не знаем, как определить устойчивые, эффективные и точные методики для оценки времени отклика задач распределенных системах».

Авторами разработаны методы оценки времени отклика задач в распределенных программных приложениях, представляемых вычислительными моделями, отвечающими ряду ограничений. Особенностью вычислительных моделей программных приложений для распределенных систем является наличие отношений предшествования между задачами, размещаемыми в различных узлах. В общем случае отношения предшествования для задач, вовлекаемых в реакцию СРВ на определенный тип внешних событий, представляются ориентированным графом без контуров.

Конкретные вычислительные модели, используемые для анализа программных систем, могут накладывать те или иные ограничения на топологию таких графов, например, чтобы ограничения предшествования имели вид дерева. Большинство практических систем отвечает более строгому ограничению — графы предшествования имеют вид цепочек. Еще более глубокое ограничение — две соседние задачи в цепочке принадлежат различным узлам системы. Тогда каждая дуга графа предшествования соответствует сообщению, посылаемому из одного узла системы в другой узел. Время отклика всей последовательности задач, соответствующих цепочке, на внешнее событие получается суммированием продолжительностей исполнения каждой из задач и продолжительностей передачи каждого из сообщений. Проблема оценки времени отклика сводится к оценке величины каждого из слагаемых этой суммы. Время исполнения отдельной задачи цепочки зависит от состава задач, претендующих на процессорное время в этом узле и используемой дисциплины планирования. Расчет этого времени выполняется с использованием методов, разработанных для однопроцессорных систем с учетом задержек регистрации некорневых задач цепочки. Разработан подход, обеспечивающий использование тех же методов для оценки времени передачи пакетов сообщений и элементарных сообщений в локальных коммуникационных сетях со встроенными механизмами арбитража (например, с интерфейсами типа CAN).

Нурдинов Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

CISCO SECURITY AGENT

Система предотвращения атак на уровне хоста Cisco Security Agent обеспечивает защиту серверов, настольных компьютеров и ноутбуков. В отличие от систем обнаружения атак, которые регулярно нуждаются в обновлении сигнатур, CSA активно отслеживает поведение приложений, код, исполняемый на машине, локальные сетевые соединения и выявляет аномалии в их работе, чтобы определить следуют ли разрешать эту активность.

Возможности CSA превышают возможности типовых решений для защиты конечных узлов, объединяя в рамках одного программного средства передовые функции защиты от целенаправленных атак, шпионских программ, вредоносного программного обеспечения для скрытого удаленного управления, утечки информации и многих других типов нарушения безопасности компьютера.

Агент позволяет контролировать работу всех приложений в операционных системах Windows, Solaris и Linux, запрещая эксплуатацию имеющихся в этих приложениях уязвимостей, как удаленно по сети, так и локально, при случайном запуске злонамеренного кода. Пользователь сам может добавлять те или иные приложения в «black list» или «white list», в зависимости от степени доверия к ним. Разрешая программам делать только то, что разрешено и запрещая делать все остальное, Agent позволяет обнаруживать неизвестные атаки.

В CSA присутствует возможность создания политик (наборов правил), для разных пользователей или групп пользователей, которые разрешают или запрещают те или иные действия при работе за конечным хостом. Существует также возможность автоматического создания политик.

В Cisco security agent предусмотрен модуль, отвечающий за защиту от утечки данных (Data Theft Prevention Module). Можно создать папку с именем TopSecret и хранить в ней документы, не боясь, что они могут быть сохранены где-то в сети, на другом локальном устройстве или даже переданы в другое приложение через буфер обмена. Система работает достаточно просто: как только приложение открывает файл в защищенной папке, оно сразу же ограничивается в правах - оно не может записать ничего и никуда кроме этой папки. Есть вариант скопировать данные в буфер обмена – но буфер обмена тоже защищен – передать эту информацию из буфера обмена в другое приложение нельзя.

Все настройки агентов производятся через WEB интерфейс, через подключение по HTTPS на сервер управления, на котором они хранятся в базе данных MS SQL. Все агенты эти настройки периодически проверяют и скачивают новые правила после их появления.

CSA позволяет производить инвентаризацию с генерацией отчетов. К примеру, он может собрать информацию обо всех приложениях, установленных на узле, а также о том, какие из них используются и насколько часто. Также он может произвести проверку антивирусных баз на всех конечных узлах сети.

CSA свободно интегрируется с другими программами, например Network Admission Control или антивирусом Касперским, что позволяет делать защиту отдельного компьютера и всей сети в целом более надежной.

Cisco Security Agent – это мощное средство для защиты корпоративной сети предприятия от угроз безопасности информации. В настоящее время в России оно используется всего лишь десятками компаний, например, некоторыми дочерними предприятиями «ОАО Газпром», но в ближайшие годы, вероятнее всего, число компаний, использующих Cisco Security Agent будет расти.

Ожегов С.В.
Россия, Москва, Компания SearchInform

КОНТРОЛЬ КАНАЛОВ УТЕЧКИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ И НАИБОЛЕЕ ТИПИЧНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ И ПРЕДПРИЯТИЙ

Информация сегодня является одним из критически важных факторов успеха деятельности любой организации. Средняя стоимость одной утечки информации в мире составляет около 2,7 млн. долларов.

Как «утекает» информация? Существует несколько каналов передачи данных: электронная почта, социальные сети (Facebook, Одноклассники, вКонтакте), форумы, блоги, службы мгновенного обмена сообщениями (ICQ, MSN, Jabber, Mail.ru-Агент), внешние носители информации, принтеры, и, что сейчас особенно актуально, Skype.

Пути утечки конфиденциальных данных из организации могут быть самыми разнообразными:

1. Письмо с ценной информацией может быть отослано по электронной почте;
2. Информация может быть отправлена посредством клиентов для мгновенного обмена сообщениями (ICQ, MSN Messenger, QIP, Jabber);
3. Голосовые или текстовые сообщения, отправленные через Skype, также могут содержать важную корпоративную информацию;
4. Информация может быть размещена на форумах, блогах, передана по социальным сетям;
5. Ценные данные могут быть переписаны на съёмный носитель (USB-флешку или CD/DVD);
6. Информация может быть распечатана на принтере.

В свете повсеместной информатизации бизнеса и быстрого накопления колоссальных объемов электронных документов критичной становится функция поиска больших объемов данных, которые, как свидетельствует практика, зачастую на 90% состоят из «информационного мусора».

Наиболее важным компонентом любой системы информационной безопасности является аналитический модуль. Именно он позволяет сотрудникам службы информационной безопасности оперативно и точно принимать решения о степени конфиденциальности перехваченных данных. Поисковые механизмы позволяют эффективно работать со всеми видами конфиденциальной информации, содержащейся в перехваченных данных.

В системе информационной безопасности SearchInform применяются следующие виды поиска, значительно упрощающие работу по обеспечению информационной безопасности:

- поиск по словам с учетом морфологии;
- поиск по фразам с учетом порядка слов и расстояния между ними.

Оба названных вида поиска – наиболее простые, и могут использоваться лишь как вспомогательные в комплексе с более сложными:

- поиск по регулярным выражениям;
- поиск по цифровым отпечаткам;
- запатентованный SearchInform «Поиск похожих»;
- поиск с использованием синонимов.

Именно совместное использование всех типов поиска позволяет максимально эффективно защищать конфиденциальные данные в корпоративной сети и резко сократить трудозатраты на их анализ.

Нередко сотрудники берут с собой лэптопы, чтобы поработать дома или в командировке. Необходимо иметь ввиду, что лэптопы могут быть использованы для передачи конфиденциальных данных третьим лицам. Поэтому важно осуществлять полный контроль отсылаемых корпоративных данных, даже если сотрудник находится вне сети. Данные передаются для анализа в отдел информационной безопасности, как только лэптоп снова оказывается в корпоративной сети.

Инсайдеры сегодня являются одной из главных угроз информационной безопасности любой компании. Остальные угрозы (хакеры, вирусы и т.п.) более-менее успешно нейтрализуются специализированным софтом и сотрудниками IT-отделов. Именно на совести инсайдеров большинство громких утечек конфиденциальной информации, зафиксированных по всему миру в последние годы.

Вот несколько примеров того, как можно противостоять инсайдерских рискам и эффективно защищать организацию от утечек конфиденциальных данных.

Таким образом, современная система безопасности должна позволять сотруднику использовать все каналы для передачи информации, однако необходимо перехватывать и анализировать все информационные потоки, идущие по этим каналам.

Озорнин А.С.
Россия, Екатеринбург, Уральский радиотехнический колледж им. А.С. Попова

АЛГОРИТМ FNP: НОВЫЙ ПОДХОД К СИГНАТУРНОМУ АНАЛИЗУ

Актуальность систем предотвращения вторжений (IDS) объясняется тем, что ставшие стандартом фаерволлы не позволяют обеспечить полную защиту от вторжений: например, распознать вредоносные действия пользователя, если они производятся с соблюдением правил фаерволла.

Существует два распространённых подхода к анализу траффика: статистический и сигнатурный. Первый – это сбор содержимого заголовков пакетов, их статистический анализ и сравнение результатов с имеющимися в базе разновидностями атак. Второй применяет статическую базу шаблонов, с которыми сравнивается трафик, проходящий через IDS. Известная IDS, Snort, использует их оба. Производительность сигнатурного анализа определяется скоростью сравнения строк содержимого пакетов с сигнатурами. Её повышение оставит больше процессорного времени для проведения эффективного статистического анализа.

В своей работе я предлагаю реализацию алгоритма быстрого поиска подстроки, разработанного Rong-Tai Liu из университета Tsin-Hua в 2003 году, оптимизированную для работы на компьютерах x86-совместимой архитектуры. Данный проект, кроме IDS, позволит использовать алгоритм FNP в антивирусных и анти-Spyware сканерах и другом ПО для обеспечения безопасности рабочих станций.

Наша разработка станет дополнением к реализациям других, уже использующихся, алгоритмов. В первую очередь, алгоритма поиска строки Бойера-Мура: он эффективен при поиске подстроки по одному шаблону. С помощью предварительных вычислений над шаблоном часть проверок пропускаются как заведомо не дающие результата. Однако практика показывает, что его реализации в IDS Snort и антивирусе ClamAV медленны при поиске по нескольким шаблонам.

Алгоритм FNP

Алгоритм основывается на простом принципе: Пусть дан текст T = t0, t1, ... , tn, и набор шаблонов P = {P1,P2,…, Pr}. Задача поиска подстроки заключается в нахождении позиции и определении соответствия части строки T шаблону Pj = a j 0, a j 1, a j m-1, 1 ≤ j ≤ r, где

ts+i = aji, 0 ≤ i ≤ m-1.

Данное выражение может быть представлено также как:

ts ... ts+m−1 = aj0 ... ajm−1

Реализуемый нами алгоритм FNP основывается на следующем простом утверждении: для произвольного шаблона Pj = a j 0, a j 1, a j m-1 если w соседних байт строки T находятся на позиции s, где

ts+i ... ts+w−1 ≠ aj0 ... ajw−1−i, i = 0,1,2, ... , w – 1,

то эти w байт не содержат первых i соседних байт шаблона Pj, где 1 ≤ j ≤ w. Значит, следующие w байт могут быть пропущены. С другой стороны, если байты, находящихся в строке T, совпадают с первыми байтами Pj, то имеет смысл сравнение следующих m-w байт начиная с текущей позиции.

Результаты тестирования на сетевых процессорах

Согласно тестированию, проведённому автором алгоритма, алгоритм FNP на сетевых процессорах дал результаты, превосходящие по производительности другие алгоритмы. Выигрыш напрямую зависит от количества сигнатур.

При использовании алгоритма FNP становится возможным увеличить до 500% производительность обработки базы сигнатур большой длины. Время обработки сигнатур алгоритмом FNP практически не меняется при изменении размеров базы сигнатур, в отличие от других алгоритмов. При интеграции алгоритма на сетевые процессоры с включенной кэш-памятью результаты становятся ещё более впечатляющими.

При относительно маленьком количестве сигнатур выгоднее использовать алгоритм нахождения наибольшего паросочетания. Однако вместе с преодолением отметки в 2048 сигнатур, алгоритм FNP показывает себя лучше других.

Тестирование на x86-совместимых процессорах

Для тестирования были сгенерированы случайные шаблоны, распределение количества которых по их длине аналогично базе сигнатур Snort, а также случайные наборы байт, в которых производится поиск. На данный момент время сравнения строк по множеству шаблонов с помощью алгоритма FNP примерно аналогично показателям алгоритма Ахо-Корасик. С введением таблицы пропускаемых значений и после дальнейшей оптимизации кода время выполнения будет снижено. Работа над реализацией алгоритма FNP для систем на базе процессоров стандартной архитектуры ещё не завершена, проект находится на стадии отладки и оптимизации кода. Дальнейшие шаги: введение в программу таблицы количества пропускаемых значений, которая позволит увеличить скорость работы алгоритма.

Заключение

Внедрение этого алгоритма в сетевые системы обнаружения вторжений позволит снизить стоимость конечного продукта за счёт снижения стоимости аппаратной части устройства при сохранении достаточной производительности, а также значительно повысить КПД пассивных IDS. При использовании данного алгоритма в антивирусном и анти-Adware ПО возможно будет добиться освобождения ресурсов системы под другие задачи за счёт более эффективного сканирования.

Павлов И.В.
Россия, Санкт-Петербург, Северо-Западный государственный заочный технический университет

СОВРЕМЕННЫЕ СПОСОБЫ ЗАЩИТЫ ДОКУМЕНТОВ

В последнее время круг окружающих нас документов значительно расширился. Здесь и внутренний и заграничные паспорта, водительское удостоверение, технический паспорт на автомобиль, паспорт на квартиру, гараж, дачу, многие другие документы, и конечно, деньги.

Как обезопасить себя от разнообразных видов мошенничества в этой сфере: не купить автомобиль, квартиру, дачу с подложными документами, быть уверенными в подлинности заграничного паспорта, турваучера, оформленных в незнакомой турфирме, не оказаться за границей без средств к существованию, но с полным кошельком «фантиков», проданных нам под видом евро или долларов. Как спокойно и с достоинством отстоять подлинность вашего паспорта или водительского удостоверения, объявленного «подозрительным и на этом основании изымаемым» недобросовестному представителю ГИБДД за тысячи километров от родного города – рассмотрению этих вопросов и посвящен доклад.

Что наши документы защищены от подделки, знают все. Но вот как проконтролировать наличие этих защитных признаков и вообще, что контролировать – знают немногие. Сложилась тревожная ситуация: практически все наши документы защищены от подделки, имеются инструментальные и просто визуальные методы контроля подлинности, имеются отличные отечественные приборы для контроля, а вот доступных широкому кругу граждан методик нет!

Многочисленные газетные страшилки о наличии «суперподделок», целых подразделений ГИБДД регистрирующих ворованные машины и выдающих поддельные «свидетельства о регистрации транспортного средства» туристических агентствах выдающих поддельные заграничные паспорта, мошенниках многократно продающих одну и ту же квартиру и т.д. не позволяют нам спать спокойно. Многие уверены, что защитные признаки являются секретными и не подлежат контролю обычными гражданами. И это, правда, секретные признаки действительно есть, но есть и большое количество защитных признаков, специально предназначенных для контроля гражданами и специализированными службами.

Контроль документов, денег, ценных бумаг (далее ЦБ) чисто дефектоскопическая задача или шире – задача неразрушающего контроля. ЦБ в процессе установления подлинности не может быть разрушена, подвергнута воздействию различных реактивов, кислот и т.д. А методы контроля, применяемые дл контроля ЦБ – это общеизвестные ультрафиолетовые, визуальные, инфракрасные, магнитные, магнитно-оптические и т. д. Широко используются различные оптические эффекты (кипп-эффект, муаровый эффект (MVC), растрирование изображения и т.д.). Всё дело в методике применения этих методов и знании защитных признаков.

Защита от подделки ЦБ осуществляется с помощью комплекса защитных элементов, вносимых в ценную бумагу на разных стадиях её изготовления. Защита ценных бумаг от подделок

обеспечивается за счет использования особых технологий, определенного сочетания способов и приемов нанесения полиграфического оформления, а также за счет применения специальных материалов. Условно можно выделить три основных вида защиты:

– технологическая защита, которая представляет собой специфические технологии подготовки исходных компонентов и их переработки, не применяемые при изготовлении обычных бумаг обычными методами полиграфии из-за их дороговизны и ограниченного доступа к ним;

– полиграфическая защита, которая выражается в использовании определенного сочетания способов и приемов полиграфической печати, а также в нанесении на ценные бумаги специальных элементов полиграфическими способами. В ценных бумагах данный вид защиты доминирует по количеству используемых защитных элементов;

– физико-химическая защита основанная, на использовании в составах бумаги бланков ЦБ, красок и защитных волокон добавок химических веществ, наличие которых может быть определено специальными методами.

В докладе подробно, на примере российских паспортов, водительских удостоверений, отечественной и иностранной валюты рассматриваются методы их защиты и методы контроля защитных признаков, позволяющие контролировать подлинность этих ЦБ, а также перспективные способы защиты документов на бумажном носителе.

Перепелица С.Н.
Россия, Санкт-Петербург, ООО «Интехсервис»

ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ КОНСОРЦИУМА ОРГАНИЗАЦИЙ-ЛИЦЕНЗИАТОВ ПО ВОПРОСАМ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

В докладе рассматривается деятельность консорциума организаций-лицензиатов по вопросам защиты информации и объектов информатизации. В данном направлении проводятся следующие виды работ по аттестации в рамках выполнения организациями любой формы собственности требований законодательства Российской Федерации в области информационной безопасности, нормативных документов ФСТЭК и ФСБ, в частности, при создании ИСПДн:

– консалтинговые услуги по обеспечению экономической, физической и информационной безопасности;

– консалтинг, разработка, внедрение и техническое сопровождение комплексных систем защиты персональных данных в ИСПДн;

– создание средств защиты информации, содержащей сведения, составляющие коммерческую и государственную тайну;

– осуществление мероприятий и (или) оказание услуг в области защиты коммерческой и государственной тайны;

– распространение (продажа, передача), техническое обслуживание (монтаж, наладка, установка) шифровальных средств;

– проектирование, производство защищенных с использованием шифровальных средств информационных систем и комплексов телекоммуникаций;

– монтаж, наладка, установка (инсталляция) шифровальных средств;

– сертификация и сертификационные испытания средств защиты информации;

– специальные исследования, специальные проверки основных и вспомогательных технических средств;

– специальные обследования категорированных помещений;

– аттестация объектов информатизации по требованиям безопасности информации;

– проектирование, монтаж, установка, сервисное обслуживание охранной, пожарной сигнализации, систем видеонаблюдения.

Более подробно в докладе представлены востребованные услуги по выполнению работ по аттестации объектов информатизации, которые предлагаются лицензиатам СКБ «Контур»:

1. Работы по аттестации ПЭВМ, АС.
2. Работы по аттестации выделенных помещений.
3. Работы по проверке технических устройств на наличие в них специально встроенных устройств съема информации
4. Работы по специальному обследованию помещений.
5. Работы по проведению проверок экранированных сооружений
6. Работы по проверке защищенности средств изготовления и размножения документов.
7. Работы по разработке руководящих документов организации по вопросам защиты информации.

Проведение специальных экспертиз предприятий (для соискателей лицензии ФСТЭК России, ФСБ России, аудит соответствия требованиям ФЗ №152 «О персональных данных»)

Платонов В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

БЕЗОПАСНОСТЬ ИНФРАСТРУКТУРЫ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

Главной целью формирования электронного правительства является повышение качества государственного управления. Электронное правительство затрагивает деятельность исполнительной власти на всех уровнях управления. Основное внимание проектов ориентировано на деятельность федеральных органов исполнительной власти, их территориальных органов и подведомственных организаций. Необходимо отметить, что построение электронного правительства на региональном и муниципальном уровнях рассматривается с точки зрения обязательных требований к инфраструктуре. Информационно-технологическая и инженерная компоненты электронного правительства, как отмечается в системном проекте, выполняет хорошо стандартизованные инфокоммуникационные услуги: организация и предоставление каналов связи, предоставление доступа к сети Интернет, поддержка центров обработки данных, формирование открытых и защищенных контуров компьютерных сетей, поддержка функционирования общесистемного программного обеспечения, обеспечение информационной безопасности и т.п.

Деятельность электронного правительства будет способствовать значительному расширению использования государственных информационных систем для целей управления, увеличению обмена информацией и, одновременно с этим, повысит уровень информационных рисков, несанкционированной утечки, искажения, уничтожения и снижения доступности хранимой, обрабатываемой и передаваемой информации. Поэтому одним из направлений государственной политики в сфере информатизации является формирование и защита информационных ресурсов государства.

Обеспечить информационную безопасность систем электронного правительства предлагается путем создания защищенной сети передачи данных и построения подсистем обеспечения информационной безопасности для основных информационно-технических компонентов электронного правительства: портала государственных услуг, информационно-платежного шлюза для региональных правительств и прикладных государственных информационных систем федеральных органов исполнительной власти.

В докладе рассматриваются основные угрозы безопасности основных информационно-технических компонентов и особенности построения подсистем защиты на различных уровнях систем электронного правительства.

Платонов В.В., Целов И.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ЗАЩИТА В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

В стране создана и продолжает развиваться инфраструктура электронного правительства. Под электронным правительством понимается новая форма организации деятельности органов государственной власти, которая за счет широкого применения информационно-коммуникационных технологий обеспечивает качественно новый уровень оперативности и удобства получения организациями и гражданами государственных услуг и информации о результатах деятельности государственных органов. Одной из составляющих инфраструктуры электронного правительства является система электронного документооборота (СЭД) – организационно-техническая система, обеспечивающая процесс создания, управления доступом и распространения электронных документов в компьютерных сетях, а также обеспечивающая контроль над потоками документов в организации. В современной организации СЭД становится обязательным элементом IT-инфраструктуры. С их помощью повышается эффективность деятельности коммерческих компаний и промышленных предприятий, а в государственных учреждениях на базе технологий электронного документооборота решаются задачи внутреннего управления, межведомственного взаимодействия и взаимодействия с населением.

Анализ обеспечения информационной безопасности существующих СЭД позволяет выделить следующие положительные стороны:

Все без исключения СЭД поддерживают разграничение прав доступа, как для отдельных пользователей, так и пользовательских групп. Кроме того, осуществляется полноценная поддержка ролевой модели обеспечения безопасности и протоколирование действий пользователей.

Шифрование данных в системе и при передаче, а также применение сертифицированных средств криптозащиты является общепринятым стандартом.

Использование ЭЦП является повсеместным.

К числу основных недостатков можно отнести следующее:

Чаще всего СЭД используют системы аутентификации, основанные исключительно на сочетании имени пользователя и пароля. Другие способы, как, например, использование сертификатов, встречаются редко.

Практически все системы обеспечивают протоколирование действий пользователей, но полноценные средства мониторинга и анализа событий (процессов) встречаются достаточно редко.

Программные средства контроля целостности документов практически не встречаются.

С технологической точки зрения, СЭД представляет собой ни что иное, как реализацию SOA (Service Oriented Architecture). Технология SOA – модульный подход к разработке программного обеспечения, основанный на использовании сервисов (служб) со стандартизированными интерфейсами. Компоненты программы могут быть распределены по разным узлам сети, и предлагаются как независимые, слабо связанные, заменяемые сервисы-приложения. Программные комплексы, разработанные в соответствии с SOA, часто реализуются как набор web-сервисов, интегрированных при помощи известных стандартных протоколов (SOAP, WSDL, и т.д.)

Интерфейс компонентов SOA-программы предоставляет инкапсуляцию деталей реализации конкретного компонента (операционной системы, платформы, языка программирования и т.п.) от остальных компонентов. Таким образом, SOA предоставляет гибкий и элегантный способ комбинирования и многократного использования компонентов для построения сложных распределённых программных комплексов.

Данный подход имеет свои достоинства и недостатки. К первостепенным недостаткам можно отнести проблемы, связанные с обеспечение целостности и доступности, предоставляемых данных, а также сложность обеспечения высокой пропускной способности подсистем аутентификации.

В докладе рассматриваются основные проблемы безопасности SOA применительно к СЭД, поскольку именно благодаря SOA процесс интеграции с различными системам является чрезвычайно простым и эффективным. Формируется программа исследований, целью которых является рассмотрение и обнаружение новых и пока недостаточно исследованных проблем базовой технологии. Программа включает исследования и разработку перспективных подходов к построению эффективных систем мониторинга и анализа событий (процессов) происходящих в СЭД.

На данный момент, в целом, уровень защищенности СЭД можно оценить, как уровень разумной достаточности. Разработчики СЭД, не ограниченные строгими рамками законодательства, стремятся к максимальной унификации, предлагают универсальные решения и подходы. Однако, это ведет к тому, что потребность во внедрении таких систем в организациях, для которых необходим более высокий уровень обеспечения безопасности данных, остается неудовлетворенной. Требуется ужесточение существующих и разработка новых подходов к защите не только хранимых, но и передаваемых данных, что собственно и является целью проводимых исследований.

На данный момент, в целом, уровень защищенности СЭД можно оценить, как уровень разумной достаточности. Разработчики СЭД, не ограниченные строгими рамками законодательства, стремятся к максимальной унификации, предлагают универсальные решения и подходы. Однако, это ведет к тому, что потребность во внедрении таких систем в организациях, для которых необходим более высокий уровень обеспечения безопасности данных, остается неудовлетворенной. Требуется ужесточение существующих и разработка новых подходов к защите не только хранимых, но и передаваемых данных.

Ростовцев А.Г.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ОЦЕНКА ДЛИНЫ ИДЕАЛА БУЛЕВА КОЛЬЦА

Поскольку кольцо полиномов Жегалкина $G_n[x]$ от переменных $x = (x_1, \ldots, x_n)$ конечно, то оно артиново, это кольцо и его идеалы имеют нулевую размерность Крулля, каждый идеал однозначно представляется произведением главных простых идеалов и, следовательно, главный. Простой идеал максимален и состоит из полиномов, обращающихся в нуль на данном наборе переменных, существует 2^n простых идеалов. Каждый идеал A биективно соответствует многообразию $V(A)$ – множеству точек, в которых все полиномы идеала обращаются в 0. Условия $f = gh$ и $V(f) \supseteq V(g)$ эквивалентны и задают упорядоченность полиномов по делению.

Назовем длиной полинома число слагаемых. Обычно идеал кольца представим суммой главных идеалов $A = ((f_1), \ldots, (f_k))$. Назовем длиной идеала $A = ((f_1), \ldots, (f_k))$ наибольшую из длин полиномов $f_1, \ldots, f_k$, а задание идеала суммой главных идеалов – аддитивным разложением. Обычно если нетривиальное аддитивное разложение существует, то оно неоднозначно. Среди возможных длин идеала существует минимальная. Например, простой идеал, задающий нуль в точке $(e_1, \ldots, e_n)$, представим суммой линейных биномов $((x_1 + e_1), \ldots, (x_n + e_n))$ и имеет минимальную длину не более 2.

Алгебраические методы криптоанализа симметричных шифров предполагают решение системы булевых уравнений, то есть нахождение (единственного) нуля идеала, заданного полиномами Жегалкина. При этом идеал отображения $y = f(x)$ может быть задан полиномами из

G2n[x, y], обращающимися в 0 в точках, удовлетворяющих равенству y = f(x). Системы полиномов, задающих ключ при атаке на основе подобранных открытых текстов, в зависимости от зашифрованного текста различаются константами лишь в нескольких полиномах.

Традиционно при решении системы методом базисов Гребнера идеал отображения стараются задать полиномами минимальной степени. Так, идеал любой 4 и 5 битовой подстановки, а также идеал 8-битовой подстановки AES задается полиномами степени 2. Вычисление базиса Гребнера заключается в нахождении сизигии для каждой пары полиномов из базиса идеала. При этом длина и степень сизигий быстро возрастает, что обусловливает экспоненциальную емкостную и временную сложность метода. Сложность метода заметно зависит от очередности вычисления сизигий.

Более перспективным представляется задание идеала полиномами малой длины. Например, сизигия от двух биномов является биномом. Если идеал задается полиномиальным числом триномов, то решение системы облегчается. Действительно, длина сизигии от полинома и тринома превышает длину полинома не более чем на 1. Сокращение длины идеала как правило ведет к ускорению вычисления базиса Гребнера. Таким образом, решение системы тесно связано с задачей представления идеала отображения в виде суммы наиболее коротких главных идеалов, то есть с поиском минимальной длины идеала.

Каждый полином f = a0 + a1x1 + … + anxn + … + a12…nx1x2…xn может быть задан 2n-мерным двоичным вектором коэффициентов a, а также 2n-мерным двоичным вектором значений f, причем a = Lnf, где L1 = {{1,0},{1,1}}, Li+1 = {{Li, 0},{Li, Li}}. Поскольку Ln = Ln−1, то f = Lna. Таким образом, биному соответствует вектор a с не более чем двумя единичными координатами, триному – вектор с не более чем тремя единичными координатами. Каждое многообразие можно задать двоичным 2n-мерным вектором. Множество двоичных векторов образует кольцо с операциями покоординатного сложения и умножения по модулю 2, это кольцо изоморфно Gn[x]. Сумма идеалов ((f1), …, (fk)) задается суммой всевозможных симметрических функций от f1, …, fk, ей соответствует пересечение многообразий.

Существуют идеалы, двойственные простым, не допускающие аддитивного разложения.

Теорема. 1. Аддитивно неразложимые идеалы кольца Gn[x] биективно соответствуют многообразиям из 2n − 1 нулей. 2. Каждый идеал однозначно представим суммой аддитивно неразложимых идеалов.

В кольце Gn[x] при увеличении числа нулей идеала его минимальная длина склонна к возрастанию. При проектировании шифров целесообразно выбирать подстановки, идеалы которых имеют большую минимальную длину. Понятие минимальной длины допускает обобщение с учетом аффинной эквивалентности.

Множество идеалов B(k), имеющих минимальную длину не более k, и множество соответствующих идеалов кольца двоичных векторов образуют изоморфные моноиды, в моноиде полиномов сложение идеалов задается формулой ((f), (g)) = (f + g + fg), в моноиде векторов сложение идеалов задается покоординатной операцией ИЛИ. Базисом моноида B(k) является множество полиномов, содержащих не более k слагаемых.

Идеал подстановки y = S(x) задается короткими полиномами из G2n[x, y] следующим алгоритмом.

1. Найти многообразие V(S) идеала подстановки.
2. Найти все биномы из $G_{2n}[x, y]$, обращающиеся в 0 на V(S), и многообразие V_2, задаваемое биномами. Удалить лишние биномы.
3. Если $V(S) \supset V_2$, найти все триномы, обращающиеся в 0 на V(S), и заданное ими многообразие V_3. Удалить лишние триномы. Если $V(S) = V_2 \cup V_3$, то конец, иначе искать все полиномы длины 4 и т.д.

Ростовцев А.Г., Богданов А.Г., Михайлов М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

К ВОПРОСУ БЕЗОПАСНОСТИ ВЫЧИСЛЕНИЯ ПОЛИНОМОВ НАД НЕКОТОРЫМИ КОЛЬЦАМИ

В современных информационных системах часто возникает задача безопасной обработки информации в вычислительной среде, которую нельзя считать доверенной. В результате конфиденциальность обрабатываемой информации и полученного результата, а также правильность результата гарантировать нельзя. Как правило, под вычислениями понимают вычисление значения полинома y = F(x) (вычислимые функции, не представимые в виде полиномов, не известны). Предлагается способ безопасных вычислений полинома над некоторыми кольцами.

Будем считать, что недоверенная среда контролируется нарушителем. Целью нарушителя является нарушение конфиденциальности входных данных и результата или нарушение подлинности результата.

Естественной математической основой обеспечения безопасности вычислений являются конфиденциальные гомоморфизмы колец. Здесь программа F может быть рассмотрена как последовательность операций в некотором кольце (сложение, умножение, а также деление и обращение, если такие операции допустимы), при гомоморфизме эти операции сохраняются. Такие

гомоморфизмы легко реализуются над кольцом $\wedge/n\wedge$, где $p \neq q$ — большие простые числа и $n = pq$. Кольцо $\wedge/n\wedge$ используется в криптосистемах RSA Фиата–Шамира, Палье.

Случайный инъективный гомоморфизм кольца $\wedge/n\wedge$ определяется вложением $\wedge/n\wedge \rightarrow \wedge/n\wedge[z]/(f(z))$, где $f(z)$ раскладывается на линейные множители. Разложение полинома $f(z)$ эквивалентно разложению числа n. В случае пассивной модели $\deg(f) = 2$, обратный гомоморфизм колец задается подстановкой вместо переменной z данного корня w1 полинома $f(z)$. В случае активной модели $\deg(f) = 3$, для контроля правильности вычислений используется контрольная точка $v = F(u)$ и второй корень полинома w2. Подготовка входных данных для недоверенного компьютера заключается в генерации случайного полинома $f(z)$ и вычислении гомоморфного образа $X(z) \equiv x \pmod{z - w1}$ входных данных. В случае активной модели дополнительно должно выполняться сравнение $X(z) \equiv u \pmod{z - w2}$, поэтому входные данные представлены полиномом степени 2. Вычисляемая функция F задается текстом программы.

Функция F вычисляется на недоверенном компьютере. Результат вычислений $Y(z)$ представляет собой полином из $\wedge/n\wedge[z]/(f(z))$. Для получения истинного результата в доверенном компьютере вместо переменной z подставляется корень w1. В случае активной модели контролируется правильность вычислений, для чего проверяется сравнение $Y(z) \equiv v \pmod{z - w2}$.

С помощью указанных гомоморфизмов можно выполнять шифрование с открытым ключом по схеме RSA, Фиата-Шамира, Палье на недоверенном компьютере, причем недоверенный компьютер не может подменить результат вычислений.

Поскольку промежуточные результаты вычисления в кольце $\wedge$ имеют ограниченную длину, можно получить правильный результат и при переходе к кольцу $\wedge/n\wedge$ для достаточно большого n. Вычисления в поле рациональных чисел сводятся к вычислениям в $\wedge$ для числителя и для знаменателя и следовательно могут быть выполнены в кольце $\wedge/n\wedge$. По лемме Гензеля данный способ может быть использован для безопасных вычислений в кольце $\wedge n$ n-адических чисел. Заметим, что поскольку кольцо $\wedge/n\wedge$ в отличие от кольца $\wedge$ является неупорядоченным, деление с остатком не может быть реализовано в $\wedge/n\wedge$.

По-видимому, данный способ защиты может быть использован не только для защиты криптосистем с открытым ключом, но и для финансовых расчетов, например, расчета зарплаты и налогов, при которых облагаемая сумма и размер налога остаются в секрете, а результат вычислений не может быть подменен.

Для обеспечения безопасности указанные случайные гомоморфизмы колец должны быть одноразовыми, а контрольная точка (u, v) секретной. В вычислительном плане безопасность указанного способа защиты эквивалентна разложению составного числа n.

Семьянов П.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

УЯЗВИМОСТЬ СХЕМ ДОПОЛНЕНИЯ БЛОКА AES В АЛГОРИТМАХ ПРОВЕРКИ ПРАВИЛЬНОСТИ ПАРОЛЕЙ

Широкое внедрение криптографических стандартов (AES) и стандартных схем применения криптографических алгоритмов (PKCS, PBKDF, HMAC), безусловно, повышают стойкость приложений, использующих криптографическую защиту. Тем не менее, бездумное их применение, особенно совместное, может приводить к недоработкам и уязвимостям различной степени.

В данной работе рассматриваются проблемы, связанные с применением схемы дополнения (padding) блока AES, описанные в PKCS7 и RFC 5652. Эта схема рекомендует дополнять блок AES до величины, кратной 16 байтам, с помощью N байт со значением N. При этом, если сообщение уже кратно 16 байтам, то необходимо вставлять еще один лишний блок из 16 байтов со значением 16.

В том случае, когда исходное сообщение по сути представляет собой криптографически случайную последовательность (например, привязка (salt) или синхропосылка (IV)), вводимая при дополнении блока регулярность приводит к нарушению случайности сообщения при расшифровке.

В частности, на практике данная уязвимость была встречена в двух современных прикладных программах – Microsoft Office 2007/2010 и PKZip 6.0 и выше. В обоих случаях случайные последовательности, применяемые в алгоритмах проверки правильности введенного пароля, зашифровываются с помощью AES, при этом блок AES дополняется неслучайным образом. Поэтому при проверке пароля на правильность удается не выполнять несколько шагов из предполагаемого разработчиками алгоритма (для MS Office – 2 шага, для PKZip – 5 шагов), что приводит к росту скорости перебора паролей (на 1% и в 2.5 раза соответственно).

Можно заметить, что первоначально в обоих случаях алгоритмы проверки правильности паролей не предполагали использование AES и не содержали подобной уязвимости. Более поздняя замена алгоритма шифрования на AES без должной проверки деталей реализации могла привести к данной уязвимости.

Сорокин И.В., Копыльцов А.В.
Россия, Санкт-Петербург, ООО «Доктор ВЕБ», Российский государственный педагогический университет им. А.И. Герцена

МОДЕЛИРОВАНИЕ СТРУКТУРЫ ВРЕДОНОСНЫХ ФАЙЛОВ С ИСПОЛЬЗОВАНИЕМ СТОХАСТИЧЕСКИХ ГРАММАТИК

В области антивирусных средств защиты для выявления вредоносных программ широкое применение находят различные алгоритмы распознавания образов. При этом, как правило, в качестве объекта распознавания выступает исполняемый файл, реализующий вредоносный функционал. Представленное решение основывается на том, что исполняемый файл, в независимости от платформы, обладает структурой, характеризующейся расположением участков кода и данных. Такого рода элементы структуры не только обладают набором характеристик, но и взаимосвязаны между собой. Для изучения таких структурных свойств файла предлагается использовать алгоритмы синтаксического анализа. В терминах теории формальных языков, каждый файл может быть рассмотрен как предложение, состоящее из символов алфавита. Множество файлов, относящихся к одному семейству вредоносных программ, может трактоваться как язык, порождаемый отдельной грамматикой.

При анализе файлов, защищенных с использованием методов полиморфизма и обфускации, появляется доля случайности в результате зашумленности кода и неполноты информации о характеристиках классов вредоносных программ. В таких случаях обычные формальные грамматики неэффективны, потому что возникает проблема неопределенности в том смысле, что одна и та же цепочка символов может быть корректно разобрана несколькими грамматиками, описывающие разные семейства вредоносных программ. Для более правдоподобного моделирования таких ситуаций предлагается использовать стохастические грамматики, которые позволяют эффективно использовать накопленные статистические данные.

Основными проблемами при данном подходе является выбор терминальных и нетерминальных символов, определение правил подстановки, оценивание их вероятностных мер и в целом задача грамматического вывода.

Решение этих проблем играет важную роль в дальнейшем применении синтаксического распознавания образов для выявления вредоносных программ.

Степанова Т.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ВЗАИМОСВЯЗЬ МЕЖДУ ДЕЙСТВИЯМИ ПОЛЬЗОВАТЕЛЯ И СОДЕРЖАНИЕМ ИСХОДЯЩЕГО СЕТЕВОГО ТРАФИКА ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ

Одной из наиболее трудоемких в плане анализа является угроза наличия в составе прикладного программного обеспечения (ПО) недекларированных возможностей (НДВ), которые могут быть активированы нарушителем и действовать в обход средств защиты. Для решения проблемы контроля деятельности пользователей ERP-систем предлагается использовать подход, основанный на тотальном мониторинге каналов взаимодействия пользователей с системой.

Результатом взаимодействия пользователя с терминалом ERP-системы является запрос к базе данных (БД) ERP-системы. В основе подхода лежит обнаружение взаимосвязи между действиями пользователя и исходящим сетевым трафиком терминала. Отсутствие взаимосвязи считается аномалией и свидетельствует о наличии НДВ.

Действия пользователя описываются данными, введенными с помощью клавиатуры и мыши. Для сбора данных используется доверенный контролирующий блок, через который клавиатура и мышь подключены к компьютеру пользователя. Данные ввода клавиатуры и мыши описывают взаимодействие пользователя с терминалом. Реакцией терминала на действия пользователя является формирование сетевого трафика, содержащего последовательность SQL-запросов к БД ERP-системы. Последовательность SQL-запросов состоит из двух частей: SQL-команда (описывает структуру SQL-запроса) и SQL-данные (данные, передаваемые в SQL-запросе). Каждой SQL-команде соответствует одно или более множеств активированных управляющих элементов в интерфейсе терминала.

На этапе обучения данные ввода пользователя кластеризуются, а на основе собранного сетевого трафика формируется полный набор SQL-команд, включающий все SQL-команды, которые может сформировать терминал. Каждый кластер соответствует одному элементу интерфейса. Каждой SQL-команде ставится в соответствие набор кластеров элементов интерфейса. То есть, в результате обучения формируются связи между наборами кластеров элементов интерфейса и SQL-командами.

К алгоритму кластеризации предъявляются следующие требования:

1. количество кластеров заранее неизвестно;
2. должна учитываться плотность распределения объектов.

С учетом этих требований выбран алгоритм кластеризации OPTICS.

На этапе эксплуатации метода данные ввода пользователя собираются до тех пор, пока не будет выполнена последовательность SQL-запросов, относящаяся к фоновым. Фоновыми считаются SQL-запросы, возникающие в отсутствии взаимодействия пользователя с устройствами ввода.

Из последовательности SQL-запросов выделяется SQL-команда. Если полученная SQL-команда отсутствовала в обучающем множестве, текущая последовательность SQL-запросов считается активностью НДВ. Если полученная SQL-команда присутствовала в обучающем множестве, то выбирается набор кластеров элементов интерфейса X, связанный с этой командой, и сопоставляется с полученным множеством данных ввода пользователя Y. Для каждого из кластеров из набора X ищется нажатие левой клавишей мыши из множества Y, расстояние до которого минимально. Затем полученные минимальные расстояния суммируются и полученная сумма сравнивается с заранее заданной величиной α.

Если полученная сумма ≤ α, это означает, что данные, введенные пользователем, соответствуют выполненной последовательности SQL-запросов (пользователь активировал все элементы интерфейса, необходимые для формирования выполненной последовательности SQL-запросов). Если полученная сумма > α, это означает, что выполненная последовательность SQL-запросов не является результатом действий пользователя, противоречит результатам обучения и является активностью НДВ.

Сухов Д.К., Латышев Д.М., Галанов А.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

РЕАЛИЗАЦИЯ ПРОТОКОЛОВ КОЛЛЕКТИВНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НАД СТАНДАРТАМИ DSA И ECDSA

Подход к разработке протоколов коллективной электронной цифровой подписи (ЭЦП) с использованием коллективного открытого ключа (ОК), формируемого в виде свертки индивидуальных ОК всех подписывающих был применен к ряду известных схем ЭЦП, основанных на сложности задачи дискретного логарифмирования, включая стандарты ГОСТ Р 34.10-94, ГОСТ Р 34.10–2001, СТБ 1176.2–99 и ДСТУ 4145–2002, однако ранее не удавалось синтезировать схему коллективной ЭЦП с использованием процедур генерации и верификации подписи, специфицируемых американскими стандартами DSA и ECDSA. В настоящем сообщении предлагается вариант реализации протоколов коллективной ЭЦП на основе последних двух стандартов.

Особенностью алгоритмов DSA и ECDSA является то, что они построены из схемы ЭЦП Эль-Гамаля, в которую был встроен механизм сокращения размера подписи. Это привело к тому, что в уравнении проверки ЭЦП открытый ключ возводится в степень, равную отношению R/S двух элементов подписи R и S. Первый элемент является рандомизирующим параметром ЭЦП. В протоколах коллективной ЭЦП этот элемент формируется как свертка индивидуальных рандомизирующих значений, формируемых каждым из подписывающих. Это обусловливает необходимость небольшого изменения процедуры вычисления второго элемента коллективной ЭЦП. В ранее предложенных схемах коллективной ЭЦП элемент S вычислялся как сумма индивидуальных долей, формируемых подписывающими по значению подписываемого документа и по коллективному значению R.

С учетом особенностей алгоритмов DSA и ECDSA предлагается следующая схема вычисления второго элемента коллективной ЭЦП S. В соответствии с уравнением формирования ЭЦП, в котором используется коллективный параметр рандомизации, каждый из подписывающих вычисляет свою долю во втором элементе коллективной ЭЦП. Затем вычисляется обратное значение от каждой доли. Все обратные значения суммируются. После этого элемента S вычисляется как обратное значение к ранее полученной сумме обратных долей. В соответствии с предложенным механизмом можно построить коллективную ЭЦП и при использовании схемы Эль-Гамаля.

Были предприняты попытки разработать на основе стандартов DSA и ECDSA схемы ЭЦП следующих типов:

1. Слепой подписи;
2. Коллективной слепой ЭЦП;
3. Утверждаемой групповой подписи.

Однако не было найдено приемлемых решений, при которых обеспечивается решение проблемы неотслеживаемости (анонимности). Трудности были связаны с описанными выше особенностями процедуры проверки подлинности ЭЦП.

Протоколы утверждаемой групповой подписи удалось разработать. Они были построены путем встраивания предложенного механизма формирования коллективной ЭЦП в схемы утверждаемой групповой ЭЦП, описанные ранее. Протоколы последнего типа могут быть реализованы также и над стандартами ГОСТ Р 34.10–94, ГОСТ Р 34.10–2001, СТБ 1176.2–99 и ДСТУ 4145–2002.

Полученные результаты дополняют предложенные ранее варианты расширения функциональности принятых стандартов ЭЦП в плане возможности реализации на их основе не только коллективной, слепой и слепой коллективной ЭЦП, но также и утверждаемой групповой подписи. Работа, представленная в докладе, поддержана грантом РФФИ №10-07-90403-Укр_а.

Уваров П.Е., Копыльцов А.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

РАСШИРЕНИЕ ФУНКЦИОНАЛА СКАНЕРА БЕЗОПАСНОСТИ

На сегодняшний день одним из важных аспектов информационной безопасности компьютерных систем является своевременное обнаружение и устранение уязвимостей программного обеспечения компьютерных систем, ключевую роль при этом играют сканеры безопасности. Сканеры безопасности можно разделить на две части: антивирусы и сетевые сканеры безопасности.

В результате анализа материалов о современных сетевых сканерах была разработана расширенная модель сетевого сканера. Сканер состоит из нескольких компонент: ядро – экспертная система, сателлиты – компоненты, выполняющие непосредственное сканирование в соответствии с запросами ядра, компоненты-плагины, реализующие необходимые механизмы для проверки систем, графический интерфейс.

Ядро представляет собой экспертную систему, которая, основываясь на определённых правилах продукции, вычисляет текущее состояние тестируемой компьютерной системы. Правила продукции могут поставляться как в виде скриптов (текстового представления задания для сателлитов, в котором прописываются также и способы вычисления результата), так и в виде предварительно скомпилированных в исполняемый код задач. Для обеспечения кросс-платформенности ядро выгодно реализовать на языке Java, поскольку высокая производительность от него не требуется.

Саттелиты представляют собой скомпилированные в самостоятельно исполняемый код компоненты, которые создают распределённую систему тестирования. Данные компоненты непосредственно исполняют задания, получаемые от ядра, и передают обратно результат выполнения. Такие компоненты также разумно делать кросс-платформенными, поэтому также можно использовать Java, однако для обеспечения необходимой производительности и эффективности в ряде задач при тестировании данная компонента должна использовать JNI, через которую можно подключать подготовленный и оптимизированный код для конкретной системы.

Компоненты-плагины обеспечивают для саттелитов необходимый функционал для проведения необходимых проверок. По мере необходимости могут загружаться сателлитами из ядра. С использованием данных плагинов в модели реализуется дополнительная проверка, которая отсутствует в исследованных сканерах — поиск скрытых от системы портов с помощью RootKit технологий. Данный анализ очень важен для оценки компьютерной системы, поскольку вирусы по- прежнему являются одной из серьёзных проблем, при этом сами вирусы могут реализовывать сетевую службу, в которой могут находиться уязвимости.

Графический интерфейс – swing-интерфейс и веб-сервис, предоставляющие возможность настройки следующего сканирования и просмотра, анализа и обработки полученных результатов. Также графический интерфейс будет предоставлять возможность подключения пользователями дополнительных правил продукции, реализованных в соответствии с заданным API.

Уварова Ю.А., Копыльцов А.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КОНТЕКСТНОГО АНАЛИЗАТОРА PHP КОДА

В программной среде «Информационная система поддержки принятия решений в аудите информационной безопасности операторов информационных систем персональных данных» АИС «Джульетта» для поддержки деятельности аудитора по выявлению угроз несанкционированного доступа к персональным данным, реализуемых программными средствами, использующими уязвимости в PHP коде программных сред, предусмотрен контекстный анализатор PHP кода.

С помощью диалогового окна актант загружает PHP-файл или HTML-файл с PHP-кодом, который он хочет проверить на наличие уязвимостей.

Контекстный анализатор на основе регулярных выражений ищет переменные. Как только он находит очередную переменную, то проверяется, также регулярным выражением, не передается ли она в качестве параметра в потенциально уязвимую функцию языка PHP. Перечень потенциально опасных функций хранится в базе знаний программной среды и содержит по умолчанию функции: fopen, opendir, Handler_open, imageCreateFromPng, loadHTML, include, require, eval, system, exec, popen, http_build_query, mysql_result и др. Если функция, в которую передается переменная входит в этот перечень, то узнаем применялись ли функции обработки передаваемых данных. Список интересующих нас фунций языка PHP, занимающихся обработкой данных, формируется экспертом по защите информации. В список входят такие функции как: addslashes, escapeshellcmd,

mysql_escape_string и т.п. В итоге мы знаем имя переменной, в какую функцию она передается и обработано ли значение входящего параметра.

Система логического вывода обрабатывает результат работы контекстного анализа PHP кода с помощью правил продукции вида:

– IF в потенциально уязвимую функцию передается «необработанный» параметр
– THEN появляется возможность реализации такого-то типа атаки.

Информация об уявимостях хранится в базе знаний программной среды «Информационная система поддержки принятия решений в аудите информационной безопасности операторов информационных систем персональных данных» в виде дерева классификации атак со структурой:

– тип атаки (например, SQL-инъекция)
– условия ее осуществления (например, передача «необработанной» переменной в функцию mysql_query).

Модуль логического вывода на основе правил продукции, использующих дерево атак, определяет есть ли в данном случае уязвимость.

Когда найден потенциально опасный участок кода о нем выводится на экран информация:

– имя класса, в котором она находится;
– номер строки с уязвимостью;
– название функции, через которую может быть реализована угроза;
– имя передаваемой в эту функцию переменной;
– значение, которым проинициализиврована переменная;
– информация о функциях, с помощью которых проверяются передаваемые в переменную значения;
– тип атаки для реализации которой используются уязвимости данного типа.

Контекстный анализатор PHP кода сокращает примерно в 10 раз время затрачиваемое специалистом на поиск уязвимостей в коде программы и составление отчета.

Халиуллин Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

АЛГОРИТМЫ РАБОТЫ РУТКИТА TDL-4

Руткит TDL-4 является продолжением развития руткита TDL (TDSS), в данное время входящего в число наиболее сложных руткитов. Отличительной особенностью руткита является его постоянное совершенствование — механизмы сокрытия и защиты усложняются, добавляется новая функциональность, исправляются ошибки.

Отличия TDL-4 от предыдущих версий TDL:

– установка на 64-битные операционных систем Microsoft Windows;
– заражение главной загрузочной записи (MBR);
– подмена системного драйвера kdcom.dll для ранней загрузки и противодействия отладке.

Руткит хранит свои файлы в зашифрованной файловой системе, которая расположена в последних секторах жесткого диска. Для шифрования файлов используется алгоритм RC4.

TDL-4 заражает главную загрузочную запись и получает управление при загрузке с жесткого диска, перехватывает функции чтения секторов жесткого диска и передает управление на оригинальную главную загрузочную запись.

Далее руткит ожидает, когда операционная система начнет загружать системный драйвер kdcom.dll. Руткит подменяет считанный в память драйвер на свой компонент Ldr32/64, получает управление во время загрузки драйвера и изменяет параметры загрузки ОС Windows таким образом, что целостность системного драйвера kdcom.dll не проверятся. Заменив драйвер kdcom.dll на свой компонент, руткит не только получает управление во время загрузки ОС Windows, но и оказывает противодействие отладчикам.

Во время загрузки ядра Windows из драйвера kdcom.dll вызывается функция KdDebuggerInitialize1, подмененная в памяти на код из компонента LDR32/64. Подмененная функция загружает из зашифрованной файловой системы руткита основной компонент — Drv32/64 и передает ему управление. Основной компонент выполняет следующие действия:

– скрывает факт наличия руткита;
– противодействует обнаружению;
– создает потоки, которые следят за перехватами, установленными руткитом, а также проверяют наличие зараженной загрузочной записи, и перезаписывают ее при попытках ее восстановления;
– реализует необходимую функциональность.

Использование данных механизмов позволяет руткиту получать управление на стадии загрузки ОС Windows, обойти контроль целостности ОС, скрыть свое наличие и противодействовать обнаружению.

Харинов М.В., Заболотский В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПОДХОД К ПРОБЛЕМЕ СЕГМЕНТАЦИИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ ПОСРЕДСТВОМ ОПТИМИЗАЦИИ ПОСЛЕДОВАТЕЛЬНОСТИ РАЗБИЕНИЙ

В современной обработке цифровых изображений одной из ключевых продолжает оставаться, так называемая, «проблема сегментации», которая в постановочной части сводится к формальному определению понятия сегментированного изображения. Определить сегментированное изображение, значит отличить, выделить его среди изображений, тем или иным способом разделенных на сегменты, не ссылаясь на конкретные алгоритмы разбиения изображения на сегменты, а также на неформализованное зрительное восприятие сегментов, занимаемых «объектами».

Требуемым условиям удовлетворяет определение сегментированного изображения как оптимального приближения. При этом каждому разбиению изображения сопоставляется некоторый функционал (вещественное число), и оптимальным разбиением считается разбиение, для которого значение функционала оказывается минимальным. Один из первых подходов к сегментации на основе оптимизации предложен в модели Мамфорда–Шаха (D. Mumford, J. Shah, А.С. Бугаев, А.В. Хельвас). Более поздним является популярный в настоящее время подход, реализуемый в методе «разрезов графов» (Y. Boykov, V. Kolmogorov, Ю.В. Визильтер и др.). В обоих подходах минимизируется функционал, который состоит из двух слагаемых, «компенсирующих» друг друга при изменении разбиения изображения. Смысл введения составного функционала состоит, прежде всего, в том, чтобы при определенных условиях получить алгоритмы точного решения задачи сегментации, которая сводится к нахождению оптимального разбиения изображения.

В докладе развиваются вычисления в модели Мамфорда–Шаха, в которой приближения изображения получаются заполнением сегментов средними значениями яркости. В качестве функционала рассматривается «однокомпонентное» среднеквадратичное отклонение приближения от изображения, которое имеет тривиальный минимум при разбиении изображения на отдельные пиксели или связные сегменты из одинаковых пикселей. Особенностью постановки проблемы сегментации является то, что сегментированное изображение определяется как оптимальное приближение при каждом значении числа сегментов от единицы до N , где N — число пикселей в изображении. В такой постановке пока не найдено точного решения задачи сегментации даже для случая разбиения изображения на два сегмента, а прямой перебор вариантов оказывается не эффективным уже для изображений размером 10×10 пикселей из-за недостатка быстродействия современных компьютеров.

Тем не менее, для решения задачи оказываются применимыми алгоритмы слияния сегментов, выработанные для минимизации оригинального функционала модели Мамфорда–Шаха, в котором, помимо среднеквадратичного отклонения, учитывается суммарная длина границ между сегментами. В случае редуцированного функционала алгоритмы слияния упрощаются, но оказываются недостаточными для оптимизации приближений, поскольку в последовательности оптимальных приближений сегменты из различных разбиений, в общем случае, могут перекрываться.

Для вычисления приближений, более близких к изображению по среднеквадратичному отклонению, слияние сегментов дополняется операцией коррекции границ, которая выполняется при условии сохранения при этом целостности сегмента. Поочередное выполнение операций слияния/коррекции сегментов позволяет для каждого числа сегментов улучшить визуальное качество приближений изображения и построить модель оптимального приближения изображения, в которой пиксели приближения разделяются на пиксели «площадок» и пиксели «соединений» шириной в один пиксель. Первые зрительно воспринимаются как «объекты», а вторые описывают близость объектов между собой. При этом с уменьшением числа сегментов каждый сегмент покрывает несколько объектов, что позволяет избежать «стирания» объектов, характерного для выполнения сегментации в алгоритмах обычного слияния сегментов.

Таким образом, в докладе:

1. Сегментированное изображение определяется как оптимальное приближение для каждого числа сегментов;
2. Показывается недостаточность слияния сегментов для получения оптимальных приближений изображения;
3. В дополнение к слиянию сегментов вводится операция их коррекции с сохранением целостности;
4. Предлагается модель сегментированного изображения, состоящего из «площадок» и «соединений» шириной в один пиксель.

Следует отметить, что инновации в области хранения, передачи, анализа и распознавания изображений применяются, прежде всего, в аппаратно-программных комплексах специального назначения. Поэтому развитие отечественных решений ключевых проблем обработки изображений, в частности, проблемы сегментации, имеет немаловажное значение для компенсации традиционного отставания аппаратных средств.

Работа поддержана грантом РФФИ (проект №11-07-00685а).

Царьков А.Н., Цимбал В.А., Шиманов С.Н.
Россия, Серпухов, МОУ «Институт инженерной физики»

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА ДОВЕДЕНИЯ СООБЩЕНИЯ В РАДИОСЕТИ БЕЗ ОБРАТНОЙ СВЯЗИ С ПОВТОРЕНИЯМИ И НАКОПЛЕНИЕМ ИНФОРМАЦИИ

Сети оповещения и другие сети доведения циркулярной информации до абонентов, распределенных на большой территории, строятся, как правило, в виде радиосетей передачи данных без обратной связи. Особенностью их функционирования является передача сообщений путем их многократного повторения. При этом приемник каждой абонентской станции (АС) осуществляет повышение достоверности принятого сообщения путем накопления повторов информации с последующей их мажоритарной обработкой. Основными задачами построения таких радиосетей являются: нахождение вероятностно- временных характеристик (ВВХ) и числовых характеристик (ЧХ) доведения сообщений в сети; обоснование требуемого числа повторов сообщения, нужного для обеспечения заданной достоверности его доведения.

Рассматривается радиосеть циркулярной передачи информации с большим количеством АС, на каждой из которых расположен приемник. Передача сообщений осуществляется из передающего центра (ПДРЦ) путем передачи конечного числа повторов этого сообщения с фиксированной скоростью передачи. При этом каждое сообщение (повтор) для повышения достоверности кодируется некоторым помехоустойчивым кодом. Затем каждый символ сообщения превращается в сигнал с заданным видом модуляции и излучается в эфир. Качество дискретного канала связи от ПДРЦ ко всем АС одинаково и характеризуется вероятностью ошибки на элементарный символ.

В приемнике АС радиосигналы обрабатываются (демодулируются) в блоке обработки сигнала (БОС) согласно используемому методу модуляции, и сформированные символы поступают в декодер повтора сообщения (ДПС). В ДПС осуществляется декодирование сообщения согласно используемому алгоритму. Причем ДПС может работать как в режиме обнаружения, так и в режиме исправления ошибок. Если ошибок в принимаемом сообщении нет, или они все исправлены (или не обнаружены), то декодированное сообщение из ДПС выдается получателю сообщения (ПС). Если ошибки есть, то данный повтор поступает в блок логической обработки (БЛО) повторов сообщения.

Если в БЛО накоплено три и более повторов, то последний осуществляет их логическую обработку, а именно: производит мажоритарные проверки (МП) по всем возможным типам (при этом на текущем повторе не используется те МП, которые проведены на предыдущем шаге). МП повторов сообщения происходит поразрядно.

После выполнения текущей МП в БЛО «собирается» сообщение, которое отправляется на декодирования в ДПС. После успешного декодирования в ДПС оно поступает к ПС. Если в нем обнаружены ошибки, то ДПС ожидает результат следующей МП и т.д. Применение МП накопленных повторов информации обеспечивает повышение достоверности сообщения и, соответственно, снижение вероятности ошибки на элементарный символ.

В начале строится математическая модель процесса доведения сообщения в соединении «точка- точка» (радионаправлении ПДРЦ – одна АС). Нахождения искомых характеристик доведения сообщений во всей сети (ко всем АС) требует знания характеристик доведения сообщения от ПДРЦ к одной АС. Назначение математической модели - расчет ВВХ процесса доведения сообщения от ПДРЦ к одной АС с учетом логики работы БЛО.

Рассматриваемый процесс доведения имеет конечное число состояний, является дискретным по времени и в нем соблюдается основное марковское свойство. Тогда данный процесс является конечной марковской цепью (КМЦ). Расчет ВВХ процесса доведения сообщений осуществляется по уравнению Колмогорова- Чепмена (УКЧ). ВВХ показывают изменение вероятности доведения сообщения от ПДРЦ до АС в зависимости от числа шагов (от числа повторов сообщения). На базе расчета ВВХ находится численно среднее время доведения сообщения через фундаментальную и дисперсионную матрицы. При этом для упрощения процедуры обращения матриц используется формула Фробениуса. Матрица переходных вероятностей (МПВ) синтезируется по новым правилам.

Затем строится математическая модель процесса доведения сообщения в соединении «точка-многоточка» (радиосеть ПДРЦ – все АС). Назначение математической модели - расчет ВВХ и ЧХ процесса доведения сообщений от ПДРЦ ко всем АС сети. Основу данной модели составляет аппарат неоднородных КМЦ.

Сформированы правила синтеза МПВ как для первой, так и для второй модели. Дана модификация УКЧ для случая неоднородной КМЦ. Таким образом, сформирован математический аппарат, позволяющий адекватно описывать процесс доведения сообщений в радиосети без обратной связи с повторениями и накоплением информации (повторов сообщений) и их мажоритарной обработкой на каждом повторе.

Приводятся результаты численных расчетов ВВХ для исходных данных типовой радиосети без обратной связи с повторениями и накоплением информации.

Обосновывается требуемые типы МП сообщения в радиосети и их количество, нужное для обработки в БЛО приемника АС.

Шемякина О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ОБ ОЦЕНКЕ ХАРАКТЕРИСТИК РАЗБИЕНИЙ РАЗЛИЧНЫХ АЛГЕБРАИЧЕСКИХ СТРУКТУР

Рассматриваются перемешивающие свойства различных групповых операций, заданных на одном множестве, относительно фиксированного преобразования.

Пусть на множестве $\{0, \dots, 2^n - 1\}$ заданы две алгебраические структуры, определяемые операциями сложения по модулю 2^n и сложения по модулю 2. Исследуются перемешивающие свойства данных операций, действующих на классах разбиения исходной алгебраической структуры, относительно операции дискретного логарифмирования в поле $GF(2^n + 1)$. Выбор операции дискретного логарифмирования в конечном поле обусловлен ее использованием в алгоритме хэширования MCSSHA-3. Задача заключается в изучении возможности построения разбиений, обеспечивающих большое количество запретов переходов кортежей классов, и сравнение характеристик данных разбиений для обеих структур.

Традиционно разбиения строятся с использованием гомоморфизма в подгруппу исходной группы. При этом групповая операция сохраняет смежные классы, однако преобразование, задаваемое дискретным логарифмированием в конечном поле, хорошо перемешивает элементы классов такого разбиения. В частности, известно, что оно обеспечивает минимально возможное количество нулей в матрице переходов биграмм.

Предлагается новое разбиение группы на непересекающиеся классы, при котором ни групповая операция, ни действие операции дискретного логарифмирования не сохраняют классы полностью, однако достаточно плохо их перемешивают, в частности, матрица переходов кортежей классов существенно отличается от равномерной. Для данного разбиения удается установить нижнюю границу количества нулевых элементов в матрице переходов кортежей классов.

В качестве примера рассматривается применение предложенного подхода для $n = 4$. Для сравнения предложенного разбиения и разбиения на смежные классы по подгруппе порядка 4 используются следующие характеристики матрицы переходов пар классов под действием композиции групповой операции и операции дискретного логарифмирования в конечном поле: количество нулей, значение максимального элемента и значение среднего квадратического отклонения элементов матрицы от среднего значения. Для разбиения на смежные классы по подгруппе порядка 4 значения характеристик матрицы переходов пар классов для группы сдвигов превосходят значения соответствующих характеристик для кольца; для предложенного разбиения – частично превосходят.

Штаненко А.В.
Россия, Санк-Петербург, Санкт-Петербургский государственный университет водных коммуникаций

БИОМЕТРИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ

Благодаря высоким оперативно-техническим характеристикам биометрические средства защиты уже почти 20 лет пользуются заслуженным вниманием специалистов. Эти средства нашли применение, в основном, в государственных учреждениях, требующих наиболее высоких уровней защиты, в частности, в военных организациях, вычислительных и научных центрах, в банковских хранилищах и др. Однако, основным сдерживающим фактором до настоящего времени являлась высокая стоимость биометрических средств защиты (например, стоимость дактилоскопических систем \$2000 – 5000), которая ограничивала массовое их использование. И вот, наконец, то, о чем мечтали специалисты по обеспечению безопасности, свершилось: в настоящее время после создания миниатюрного микроэлектронного дактилосканера стоимость биометрической защиты компьютеров снижена до \$50 – 100 США, что предвещает широкое массовое использование биометрических средств защиты в самое ближайшее время.

Все биометрические системы характеризуются высоким уровнем безопасности, прежде всего потому, что используемые в них данные не могут быть утеряны пользователем, похищены или скопированы. В силу своего принципа действия многие биометрические системы пока еще отличаются сравнительно малым быстродействием и низкой пропускной способностью. Тем не менее, они представляют собой единственное решение проблемы контроля доступа на особо важных объектах с малочисленным персоналом. Например, биометрическая система может контролировать доступ к информации и хранилищам в банках, ее можно использовать на предприятиях, занятых обработкой ценной информации, для защиты ЭВМ, средств связи и т.д. По оценкам специалистов, более 85% установленных в США средств биометрического контроля доступа предназначались для защиты машинных залов ЭВМ, хранилищ ценной информации, исследовательских центров, военных установок и учреждений.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Авраменко В.С., Козленко А.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

МЕТОДИКА КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ НА ОСНОВЕ СЕТИ ЗАЩИЩЕННОСТИ

Нарушение нормального функционирования автоматизированных систем (АС) большинства промышленных, правительственных, банковских, оборонных и правоохранительных организаций вследствие несанкционированного доступа (НСД) к обрабатываемой в них информации влечет за собой значительный ущерб. Достижение научно-обоснованного уровня защищенности информации обуславливает необходимость проведения оценки защищенности информации от НСД. Оценка защищенности должна производиться на всех этапах жизненного цикла автоматизированных систем при различной степени полноты и достоверности имеющейся информации.

Среди известных отечественных и зарубежных методик количественной оценки защищенности информации от НСД наибольшее распространение получил подход на базе анализа информационных рисков (например, модель системы обеспечения безопасности Клементса). На основе анализа рисков созданы такие средства оценки защищенности как CRAMM, Counter Measures, BCM-Analyser, а также отечественные «Гриф» и «РискМенеджер». Однако у данного подхода есть ряд недостатков, не позволяющих напрямую использовать данные методы и средства для оценки защищенности информации в АС специального назначения, а именно: не учитывается реальная структура автоматизированной системы; оценивается стоимость потерь от несанкционированного доступа к информации в денежных единицах, что не приемлемо для АС специального назначения; не полностью учитывается вариативность сценариев реализации НСД и динамические характеристики процесса защиты информации.

Для устранения указанных недостатков предлагается подход к оценке защищенности на основе комплексного показателя – коэффициента защищенности, учитывающего как процессы нарушения безопасности ресурсов в АС, так и процессы контроля и восстановления их защищенного состояния. Методика количественной оценки защищенности информации от НСД состоит из следующих этапов:

1. Анализ исходных данных.
   1.1. Анализ структуры, параметров и алгоритмов функционирования АС.
   1.2. Определение состава защищаемых ресурсов.
   1.3. Определение состава и параметров функционирования средств защиты ресурсов.
   1.4. Определение характеристик потока нарушений безопасности ресурсов (интенсивности нарушений безопасности ресурсов). Данную интенсивность целесообразно определять в расчете на наихудший случай, когда нарушитель «идеальный» (имеет высокую квалификацию, постоянно отслеживает появление новых уязвимостей, а также имеет возможность мгновенно использовать их для осуществления НСД к информации, обрабатываемой в АС организации). При использовании такой модели нарушителя интенсивность нарушений безопасности ресурсов АС соответствует интенсивности появления уязвимостей в программном обеспечении АС.
   1.5. Определение характеристик потока восстановления защищенности ресурсов (интенсивности восстановления защищенности ресурсов). Данная интенсивность зависит как от количества должностных лиц, ответственных за защиту информации в организации, так и от квалификации указанных лиц по устранению угроз безопасности ресурсов организации.
2. Расчет показателей защищенности отдельных ресурсов (коэффициентов защищенности отдельных ресурсов).
3. Синтез сетей защищенности от основных типов угроз безопасности информации. Под сетью защищенности понимается совокупность связанных элементов, характеризующих состояние защищенности ее ресурсов. Сеть защищенности формируется на основе данных, полученных на этапе 1, при этом сеть защищенности может иметь последовательные и параллельные соединения.
4. Расчет показателя защищенности всей информации в АС. Проводится в зависимости от типа соединения с использованием значений показателей защищенности отдельных ресурсов.
5. Оценка защищенности информации от НСД по принятому критерию.
6. Выработка рекомендаций по повышению уровня защищенности АС должностным лицам, ответственным за защиту информации в организации.

7. Данный подход может представлять интерес как для разработчиков систем защиты информации, так и для должностных лиц, ответственных за защиту информации от НСД в организациях.

Башкирцев А.С.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ПРОБЛЕМЫ АУТЕНТИФИКАЦИИ АБОНЕНТОВ В СЕТЯХ ШИРОКОПОЛОСНОГО БЕСПРОВОДНОГО ДОСТУПА РЕГИОНАЛЬНЫХ ЦЕНТРОВ УПРАВЛЕНИЯ

В настоящее время широкое распространение, в нашей стране получили технологии сетей широкополосного беспроводного доступа (ШБД), основу которых составляет сетевое оборудование семейства стандартов 802.11. Одним из возможных вариантов использования сетей ШБД является их применение в региональных центрах управления (РЦУ), для обеспечения руководителей региона и прочих должностных лиц органов государственной власти возможностью получения доступа к сетевым ресурсам.

Известно, что любая система связи должна соответствовать требованиям, предъявляемым к ней, а именно, требованиям по своевременности, достоверности и безопасности доставки информации. Одним из ключевых аспектов, влияющих на безопасность доставки информации является процесс установления «личности» конечного пользователя или устройства, то есть процесс аутентификации. Значимость данного аспекта обуславливается возможностью несанкционированного подключения злоумышленника к сети ШБД РЦУ и ввода им, например, ложной информации.

В семействе стандартов 802.11, на начальном этапе их применения, предусматривались следующие механизмы аутентификации пользователей сети:

1. Открытая аутентификация, которая, по сути, не является алгоритмом аутентификации в привычном понимании. Точка радиодоступа удовлетворит любой запрос открытой аутентификации, такая простота определяется тем, что изначально сети ШБД были ориентированы на быстрое логическое подключение абонентов к беспроводной локальной сети. Очевидно, что открытая аутентификация не позволяет точке радиодоступа определить, является абонент легитимным или нет, что является заметной брешью в системе безопасности.

2. Аутентификацию с общим ключом. Аутентификация с общим ключом требует настройки у абонента статического ключа шифрования WEP. Между точкой доступа и абонентом происходит обмен служебной информацией, если точка радиодоступа в состоянии успешно расшифровать запрос аутентификации от абонента и содержащуюся в нем служебную информацию, то она посылает абоненту подтверждение аутентификации, таким образом, предоставляя доступ к сети.

Недостаток такого метода заключается в том, что обмен фреймами, содержащими служебную информацию, происходит по открытому радиоканалу, а значит, злоумышленник может принять как нешифрованную служебную информацию, так и ту же, но уже в шифрованном виде (данное обстоятельство обусловлено особенностями алгоритма аутентификации). Таким образом, злоумышленник достаточно легко может вычислить сегмент ключевой последовательности.

3. Идентификатор беспроводной локальной сети представляет собой атрибут сети ШБД, позволяющий логически отличать сети друг от друга. В общем случае абонент сети ШБД должен задать у себя соответствующий идентификатор для того, чтобы получить доступ к требуемой беспроводной локальной сети.

Однако такие идентификаторы сети регулярно передается точками радиодоступа в специальных фреймах. Несмотря на то, что эти фреймы играют чисто информационную роль в радиосети, т. е. совершенно «прозрачны» для абонента, сторонний наблюдатель в состоянии с легкостью определить идентификатор с помощью анализатора трафика протокола и подключиться к такой сети.

4. Аутентификация абонента по его MAC–адресу. Аутентификация абонента по его MAC–адресу поддерживается многими производителями оборудования для сетей ШБД. При аутентификации по MAC–адресу происходит сравнение MAC–адреса абонента либо с хранящимся локально списком разрешенных адресов легитимных абонентов, либо с помощью внешнего сервера аутентификации. Такой механизм, как правило, используется в дополнение к открытой аутентификации и, аутентификации с общим ключом, для уменьшения вероятности доступа посторонних абонентов.

Недостатком такого механизма является то, что передачи MAC–адресов абонента и точки радиодоступа происходит в открытом виде. В результате злоумышленник может обмануть метод аутентификации путем подмены своего MAC–адреса легитимным.

Зная недостатки и «бреши» рассмотренных выше механизмов аутентификации, производители применяли различные способы для их устранения, появлялись дополнения к семейству стандартов 802.11, направленные на повышение безопасности, однако настоящим прорывом в области обеспечения безопасности сетей БШД, стало появление стандарта 802.1x/EAP (Enterprise-режим).

В данном стандарте были выделены три компоненты, обеспечивающие высокий уровень безопасности в сетях БШД, а именно: архитектура аутентификации, механизм аутентификации и механизм обеспечения конфиденциальности и целостности данных.

Таким образом, в настоящее время перевод сетей ШБД РЦУ на оборудование поддерживающее стандарт 802.1x/EAP станет эффективным способом повышения их безопасности, за счет усложнения механизма аутентификации пользователей.

Башмаков А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций

ОСНОВНЫЕ ПОДХОДЫ К ПОСТРОЕНИЮ ЗАЩИЩЕННЫХ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

В процессе построения защищенных беспроводных локальных сетей передачи данных (БЛС) с использованием современной методологии проектирования и технологических комплексов, могут применяться экспериментальные методы исследования, аналитическое и имитационное моделирование. На стадиях опытной и рабочей эксплуатации БЛС основным методом оценки их качества и защищенности следует считать экспериментальное исследование, которое на основе статистических данных позволяет сделать заключение о качестве решений, заложенных при их проектировании.

Экспериментальные методы проектирования БЛС используются при необходимости получения реальных характеристик БЛС. Эти сведения собираются с помощью специальных средств на реально развернутой сети. Измерение параметров БЛС, характеризующих динамику ее функционирования можно производить с помощью программных и аппаратных измерителей, тестерами, сетевыми анализаторами, встроенными средствами мониторинга, средствами обнаружения вторжений. Основной проблемой при проведении экспериментов является определение состава и требуемой точности регистрации измеряемых параметров.

Для измерения параметров радиоинтерфейса и анализа передаваемого в сети трафика можно использовать сетевые анализаторы или программы – снифферы.

Применение экспериментальных методов исследования БЛС позволяет достаточно точно разработать ее структуру, но при этом требуются большие затраты на создание сети, лабораторий, стендов, на подготовку научных сотрудников и детальное планирование проводимого эксперимента.

Использование аналитических методов связано с необходимостью математического моделирования БЛС в строгих математических терминах. Аналитические модели носят обычно вероятностный характер и строятся на основе понятий аппарата теории вероятностей, теории массового обслуживания, Марковских процессов, методов диффузионной аппроксимации, а также с применением дифференциальных и алгебраических уравнений. Поскольку события, происходящие в БЛС, носят случайный характер, то для их изучения наиболее подходящими являются вероятностные математические модели теории массового обслуживания. В целом, БЛС может быть представлена в виде сети массового обслуживания, которые бывают открытыми, замкнутыми и смешанными.

Причем потоки заявок, поступающие в БЛС, не являются пуассоновскими. Это объясняется тем, что БЛС способны предоставлять передачу данных, пакетную телефонию, потоковое видео, а также служебную информацию. Поэтому, основываясь на результатах экспериментальных исследований, можно говорить о проявлении трафиком БЛС свойства самоподобия. Модели таких сетей называются неэкспоненциальными. При анализе неэкспоненциальных сетей в общем случае отсутствуют точные решения, поэтому наибольшее применение здесь находят приближенные методы.

Одним из таких методов является метод диффузионной аппроксимации. Использование диффузионной аппроксимации позволило к настоящему времени получить приближенные аналитические зависимости для определения характеристик практически всех типов систем массового обслуживания (СМО). При этом не требуется точного знания функций распределения случайных величин, связанных с данной СМО (интервалов между поступлениями заявок и временем обслуживания в приборах), а достаточно только знание первого (математического ожидания) и второго (дисперсии или квадрата коэффициента вариации—ККВ) моментов этих величин.

Аналитические методы, в основном, используются при исследовании БЛС в первом приближении или при решении специфических задач. Это обусловлено рядом причин:

- сложностью аналитического описания их функционирования;
- значительными упрощениями, свойственными большинству моделей;
- громоздкостью вычислений для сложных моделей;
- сложностью выделения и выбора наиболее важных характеристик БЛС.

Имитационное моделирование позволяет отразить реальные процессы функционирования БЛС, с учетом комплексной взаимосвязи между параметрами и показателями эффективности

системы. Создание имитационных моделей – более трудоемкий процесс, но при этом сами модели просты в использовании и полученные результаты наиболее близки к моделируемой сети.

В общем случае модель БЛС должна представлять совокупность аналитических и имитационных моделей, апробированных в ходе физических экспериментов. Однако, во многих случаях для принятия обоснованных предварительных решений может быть вполне достаточно аналитических моделей, учитывающих наиболее существенные внутренние характеристики анализируемых технологий построения БЛС и внешние характеристики условий функционирования данных сетей.

Винокуров М.Е.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ЗАЩИТА БЕСПРОВОДНОЙ ТОЧКИ ДОСТУПА ОТ ГАРМОНИЧЕСКИХ И СТРУКТУРНЫХ ПОМЕХ МЕТОДОМ АНАЛИЗА НЕЗАВИСИМЫХ КОМПОНЕНТ

В настоящее время стремительно растет число радиоэлектронных средств в разрешенных для передачи информации диапазонах частот, при этом системы передачи информации должны обеспечивать высокую достоверность приема информации в условиях сложной помеховой обстановки. Типовые или специальные устройства, работающие в том же диапазоне радиочастот, что и защищаемые беспроводные сети, могут стать причиной значительного ухудшения условий работы пользователя, больших задержек и, в некоторых случаях, полного отключения беспроводной сети. Возможность определить и предотвратить появление таких помех представляет особую важность при поддержании нормального функционирования сети.

Широко известно, что большинство беспроводных сетей работают на скорости, которая меньше указанной в спецификации. Это связано с различными причинами, включая помехи от бытовых приборов с СВЧ генераторами, беспроводных телефонов, а также наложение зон покрытия разных точек доступа, в том числе и чужих. Кроме того, часто десятки пользователей работают по одному сетевому каналу. При развертывании больших беспроводных локальных вычислительных сетей рекомендуется предварительно провести обследование площадки и определить оптимальное физическое размещение каждой точки доступа, а также выбрать каналы. Обследование площадки связано с большими расходами и занимает много времени, поэтому им часто пренебрегают. В связи с этим проблема защиты радиоприемных систем беспроводных точек доступа от различного рода помех по-прежнему остается актуальной.

Одним из перспективных направлений в решении указанных проблем без участия оператора является слепое разделение источников радиоизлучения. При разделении источников используется принцип пространственного разнесения. Реализация данного принципа проявляется в том, что разные антенные элементы осуществляют прием реализаций сигналов, обслуживающих различные смеси источников радиосигналов.

Задача слепого разделения источников сигналов решается посредством применения принципа анализа независимых компонент. Метод анализа независимых компонент требует статистической независимости отдельных компонентов сигналов антенной решетки. В контексте данного метода в частотной области размешивающая матрица каждой частотной компоненты может интерпретироваться как формирователь адаптивной диаграммы направленности с контролируемыми нулями в направлениях подавляемых источников, формируемыми посредством слепого алгоритма анализа независимых компонент.

Прямая реализация нахождения оптимального решения (вычисление размешивающей матрицы) итерационным градиентным методом или его аналогом с использованием натурального градиента, достаточно сложна и имеет относительно большое время сходимости. В связи с этим предлагается заменить схему итерационной градиентной оптимизации на оптимизацию методом Ньютона. Данных подход отличается значительно высокой скоростью сходимости при сохранении точности решения задачи разделения источников. Помимо этого, оптимизация методом Ньютона обладает сравнительно высокой численной стабильностью так как не зависит от итерационного коэффициента спуска.

В предлагаемой реализации процессора пространственной адаптации приемной системы точки доступа выбор рабочего канала осуществляется последовательным подключением демодулятора и оценкой демодулированного потока данных. После выбора рабочего канала, оптимизация диаграммы направленности приемной системы осуществляется только в этом канале, при условии что приемная и передающая точки доступа неподвижны в пространстве.

Практическая значимость заключается в том, что в результате оперативной автоматической адаптации по пространству приемной системы к помеховой обстановке отпадает необходимость или снижаются требования к частотному, временному и пространственному планированию в процессе развертывания беспроводной локальной вычислительной сети. А также значительно увеличивается помехозащищенность и соответственно производительность беспроводной локальной вычислительной сети.

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

СРЕДСТВА КОМПЛЕКСНОГО РЕТРОСПЕКТИВНОГО АНАЛИЗА СОБЫТИЙ БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

В плане обеспечения требуемого уровня информационной безопасности телекоммуникационных сетей (ТКС) интерес может представлять комплексный ретроспективный анализ событий, зафиксированных различными средствами мониторинга. Так, например, сопоставление содержимого разного рода журналов событий (протоколов функционирования) собственно средств телекоммуникаций и средств управления ТКС за отдельный узел ТКС и сеть в целом может позволить выявить определенные аномалии поведения элементов ТКС и цепочки событий, в совокупности свидетельствующие о попытках несанкционированных воздействий на ТКС.

Реализация средств комплексного ретроспективного анализа событий безопасности в ТКС может быть осуществлена в виде совокупности средств сбора данных и средств обработки данных.

Средства сбора данных осуществляют периодическое получение сведений от источников данных – агентов управления средств телекоммуникаций, разного рода средств мониторинга событий и т.д., и выполняют передачу накопленных сведений на центральный узел сети.

Средства обработки данных функционируют на центральном узле и состоят из следующих компонентов:

- средства импорта данных;
- хранилище данных;
- средства выборки и отображения данных.

Основой для создания средств обработки данных служат технологии хранилищ и витрин данных, оперативной аналитической обработки данных (OLAP), интеллектуального анализа данных (DataMining).

Одной из основных задач создания средств обработки данных является разработка структуры хранилища данных, предназначенного для хранения данных, получаемых от разнородных источников. Методика синтеза структуры такого хранилища предполагает создание таблиц фактов и их расширений, а также справочных таблиц с учетом логических взаимосвязей и семантической эквивалентности сведений, получаемых от разнородных источников. На основе известной структуры хранилища данных, создаваемого в виде реляционной базы данных, в соответствии с OLAP могут быть сформированы многомерные кубы данных.

Учитывая аналитический характер использования собираемых данных, для их выборки и отображения целесообразно использовать генераторы запросов, позволяющие гибко задавать состав отбираемых сведений и правила их отбора.

Давыдов А.Е., Агеев Д.А.
Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Масштаб»

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСНОГО УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМ ОБОРУДОВАНИЕМ ЗАКРЫТОГО И ОТКРЫТОГО СЕГМЕНТОВ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ИЗ ЕДИНОГО УДАЛЕННОГО ЦЕНТРА УПРАВЛЕНИЯ

Современное общество характеризуется высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти. Использование этих технологий в современных автоматизированных системах управления (АСУ) является необходимым условием обеспечения их эффективного функционирования.

В настоящее время системы управления гетерогенными телекоммуникационными системами организованы по принципу – для каждого сегмента телекоммуникационной сети (закрытого и открытого) – свое управляющее устройство. При этом информация управления закрытым сегментом не может быть использована для управления открытым сегментом и наоборот.

В настоящем докладе изложен другой возможный способ построения защищенной системы управления открытым и закрытым сегментами телекоммуникационной системы. Управление производиться с одного управляющего устройства, посредством специального модуля защиты передаваемой информации управления.

Специальный модуль защиты обеспечивает выполнение функций доверенного транзитного обмена информацией между оборудованием открытого и закрытого сегментов, путем контроля передаваемой и принимаемой информации с использованием криптографических функций в целях обеспечения удаленного защищенного управления.

Также в докладе показаны принципы построения АСУ, с учетом работы специального модуля защиты, с рассмотрением маршрутов прохождения информации управления.

Наличие одного управляющего устройства для обоих сегментов (открытого или закрытого) приводит к уменьшению количества операторов в два раза, что соответственно уменьшает затраты

на эксплуатацию всей системы управления, а так же к уменьшению вероятности ошибки обусловленной человеческим фактором.

Предлагаемый подход к решению данной проблемы позволяет организовать удаленное защищенное централизованное управление оборудованием открытого и закрытого сегментов сети из единого центра управления, а также избежать несогласованность конфигурационных настроек оборудования различных сегментов и как следствие нестабильную и неоптимальную работу защищённой телекоммуникационной гетерогенной сети.

Зарипов В.Д., Шерстюк Ю.М.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

ПОСТРОЕНИЕ СРЕДЫ РАЗРАБОТКИ МЕТАОПИСАНИЙ ДЛЯ УПРАВЛЕНИЯ СЕТЕВЫМИ ЭЛЕМЕНТАМИ В ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Существует способ создания программных средств управления сетевыми элементами в защищенных телекоммуникационных сетях, основанный на использовании метаописаний.

Каждое метаописание разрабатывается применительно к одному классу средств телекоммуникаций (одному типу агента управления в составе сетевых элементов) и содержит описания:

– информационной базы управления (MIB), поддерживаемой агентом управления данного класса;

– правил интегральной оценки состояния сетевого элемента – как функция, заданная на подмножестве MIB;

– структуры и экранных форм интерфейса пользователя для управления сетевыми элементами данного класса.

Основным языком представления метаописаний является XML.

Метаописание регистрируется в службе технологического управления, после чего сетевые элементы соответствующего класса могут быть включены в контур управления.

Разработка метаописаний в общем случае представляет собой довольно трудоемкий процесс. Для повышения эффективности разработки метаописаний разработана инструментальная среда, основными компонентами которой являются:

– интегрированная среда пользователя;
– специализированный XML-редактор;
– множество компиляторов (для разных частей метаописаний);
– программа-отладчик для метаописаний.

Инструментальная среда обеспечивает ряд дополнительных сервисных возможностей и позволяет создавать метаописания весьма больших объемов (десятки тысяч строк).

Кий А.В., Копчак Я.М.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ПОДХОД К УПРАВЛЕНИЮ ДОСТУПОМ НА ОСНОВЕ ИЕРАРХИЧЕСКИХ ИНФОРМАЦИОННЫХ ПРОФИЛЕЙ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ С РЕГЛАМЕНТИРОВАННЫМ ПОРЯДКОМ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ И СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Важным направлением защиты информации в автоматизированных системах (АС) является защита от внутренних угроз создаваемых авторизованными пользователями АС. Наличие у данной категории потенциальных нарушителей полномочий по доступу к защищаемой информации создает условия для реализации разнообразных сценариев несанкционированного доступа (НСД). В связи с этим особое значение приобретает соблюдение принципа минимизации предоставляемых пользователям полномочий по доступу к защищаемым ресурсам АС, являющегося одним из основных принципов построения АС с высокими требованиями к безопасности процессов обработки информации.

Средства управления доступом, применяемые в современных АС, реализуют статический принцип разграничения доступа, так как функционируют на основе предварительно заданных на весь период функционирования АС правил разграничения доступа (ПРД). Это требует, на этапе разработки ПРД, учета всех потенциально возможных потребностей пользователя в защищаемых ресурсах, вне зависимости от периодичности и очередности их возникновения в рамках решаемых функциональных задач. В связи с этим в процессе функционирования АС пользователю постоянно предоставлен весь объем ранее запланированных полномочий, являющийся, как правило, избыточным по отношению к задачам, решаемым пользователем в текущий момент времени на средствах вычислительной техники (СВТ). Это создает предпосылки для реализации случайных или преднамеренных нарушений безопасности и снижает уровень защищенности информационных ресурсов АС от НСД.

Одним из возможных подходов к решению задачи минимизации полномочий пользователей по доступу к информационным ресурсам АС является динамическое управление доступом, основанное на применении иерархических информационных профилей действий пользователей АС. Регламентированный порядок использования информационных ресурсов АС создает предпосылки для реализации данного подхода. Для каждого пользователя АС в его должностных обязанностях, а также в соответствующих руководящих документах и инструкциях закреплен перечень решаемых им функциональных задач и правила их выполнения. В результате каждым из них реализуется типовая схема использования ресурсов АС, которая формируется на основании:

– правил, установленных политикой безопасности;
– регламента выполнения работ;
– приемов выполнения работ, сформировавшихся в результате регулярного выполнения пользователем АС своих функциональных обязанностей на средствах вычислительной техники.

Данный подход предполагает предварительное наблюдение за работой пользователей в рамках предоставленных полномочий, регистрацию и обработку событий доступа, реализуемых пользователем в процессе выполнения функциональных задач. При этом под событием доступа понимается комбинация разрешенной операции доступа и идентификатора информационного ресурса. Формирование иерархического информационного профиля действий пользователя осуществляется путем выделения и накопления фрагментов деятельности пользователя (ФДП). Под ФДП понимается последовательность событий доступа, которая представляет собой реализацию некоторого этапа функциональной задачи. Каждый ФДП представляется в виде матрицы вероятностей переходов между входящими в его состав событиями доступа, что позволяет учесть не только необходимые для выполнения функциональной задачи информационные ресурсы АС, но и порядок их использования. Последующая иерархическая кластеризация полученных ФДП позволяет выявить иерархически упорядоченные устойчивые схемы использования информационных ресурсов АС.

Решение задачи динамического управления доступом осуществляется путем контроля действий пользователя на предмет соответствия классам ФДП в рамках каждого уровня иерархии информационного профиля пользователя. С этой целью применен алгоритм кумулятивных сумм. Для каждого класса, входящего в множество классов n-го уровня иерархии в дискретные моменты времени с учетом контекста идентификации рассчитываются значения частных и обобщенных кумулятивных сумм. Под контекстом идентификации понимается последовательность событий доступа фиксированной длины, используемая для проверки соответствия текущих действий пользователя его информационному профилю. Критерием о несоответствии действий пользователя его информационному профилю является превышение допустимого порогового значения либо обобщенной, либо одной из частных кумулятивных сумм классов ФДП n-го уровня. Проверка выполнения указанного критерия осуществляется на каждом уровне иерархического информационного профиля, начиная с нижнего. При этом наибольший номер уровня, на котором выполняется критерий является оценкой степени соответствия действий пользователя его информационному профилю.

Таким образом, решение о предоставлении запрашиваемого вида доступа принимается на основании сравнения текущей оценки степени соответствия действий пользователя его иерархическому информационному профилю с требуемой, задаваемой исходя из требований к безопасности процесса функционирования АС.

Климов И.З.
Россия, Ижевск, Удмуртский государственный университет

ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Наиболее точными методами оценки безопасности сети являются методы, основанные на тестовых последовательностях. Однако во многих случаях их невозможно применить из-за необходимости использования дополнительного времени на получение оценки и её частого обновления в нестационарных условиях. Поэтому в ряде случаев контроль целесообразно проводить по информационным последовательностям, если их структура содержит какие-либо неизменяемые во время сеанса связи параметры. К таким параметрам относятся: постоянный вес кодовых групп, постоянный средний вес кодовых последовательностей определенной длины, повторяемость кодовых последовательностей или их частей. В результате нарушения как конфеденциальности сети, так и воздействия внешних факторов, приводящих к угрозам типа отказа в обслуживании, возникают некоторые отличия в распределениях входных и выходных информационных потоках. Для определения отличия между распределениями целесообразно вопользоваться мерой отличия, основанной на статистическом расстоянии Бхаттачария. Выполненные расчеты показали, что в качестве переменных для построения распределений, могут быть использованы веса кодовых векторов. Исследования показали, что расстояние Бхаттачария зависит от нормированных порога и отношения сигнала к помехе так же, как вероятности ошибки зависит от тех же параметров.

Расстояние Бхаттачария определяет влияние отклонения априорного распределения веса информационной последовательности от апостериорного. Различие между распределениями монотонно уменьшается для оптимального порога с увеличением отношения сигнала к помехе. Имеет место уровень порога, для которого расстояние стабилизируется и не изменяется с ростом отношения сигнала к помехе.

Проведенные расчеты показывают, что на апостериорное распределение веса в принимаемой последовательности кодовых векторов сильное влияние оказывают параметры значений угроз – вероятность ошибки приема символа и симметрия канала связи, что подтверждает, что отклонения апостериорных распределений от априорных существенно зависят от основных показателей угроз. Определены параметры, используемых для оценки угроз анализируемому каналу связи. Рассчитаны зависимости отклонения первого и второго начальных моментов отклонения веса принятого кодового вектора от априорного среднего веса, рассчитанные для тех же значений, для которых были получены расстояния Бхаттачария. Предложен алгоритм использования совместного использования отклонений первого и второго начальных моментов, что позволяет исключить выдачу ложной оценки безопасности. Значения отклонения максимальны в том случае, если одна из вероятностей битовой составляющей близка к нулю, а другая – к единице. Такой же вывод следует и из анализа расстояния Бхаттачария. Зависимость среднего квадрата отклонения веса принимаемой кодовой последовательности от априорного среднего веса показывает, что для сигналов, как и для моментов, существует зависимость между отклонением и вероятностью приема элемента сигнала. В отличие от отклонения моментов такая зависимость стремится к нулю только в том случае, если вероятности ошибок приема бита близка к нулю.

Для оценки информационной безопасности телекоммуникационной сети предложена весовая структура сигнала как наиболее стабильная для большинства используемых сигналов. Разработан ряд алгоритмов измерения апостериорного распределения веса для сигналов с произвольной структурой, основанных, в частности, на неизменности вероятностей ошибок на длине кодового вектора. Показано, что независимо от структуры сигнала отличие распределений тем выше, чем выше численный уровень угроз. В качестве параметров для оценки безопасности использованы отклонения апостериорных значений от априорных значений первого и второго начальных моментов и среднего квадрата отклонения принятого веса от его априорного значения. Определено, что для отклонения первого и второго начальных моментов, при неудовлетворительном состоянии канала связи, имеются такие соотношения вероятностей ошибок в приеме посылки и паузы, при которых они равны нулю. Это приводит к неправильной оценке безопасности сети связи, так как такая ситуация характерна для хорошего состояния канала связи. Предложен алгоритм, позволяющий исключить такие ситуации путем совместной оценкой отклонения первого и второго начальных моментов, поскольку для них такие ситуации возникают при разных значениях вероятностей ошибок в приеме посылки и паузы. Более информативной оценкой является средний квадрат отклонения принятого веса от его априорного среднего значения. Он лишен неоднозначности и сильно коррелирован с вероятностью ошибки приема символа.

Для канала с аддитивным белым шумом выполнен анализ контроля безопасности телекоммуникационной системы по отклонению параметров весовой структуры сигнала от отношения сигнала к шуму и выбранного порога решающей схемы для различных видов модуляции и структуры сигнала. Анализ проводился по расстоянию Бхаттачария, отклонению первого и второго начальных моментов и квадрату отклонения принятого веса от его априорного среднего. Показано, что независимо от вида модуляции, применяемого демодулятора и структуры сигнала расстояние Бхаттачария тем меньше, чем больше отношение сигнала к помехе и чем ближе порог к своему оптимальному значению. Вид модуляции и способ приема влияют только на величину отклонения.

Козленко А.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

МОДЕЛИРОВАНИЕ НАРУШЕНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ НА РАЗЛИЧНЫХ ЭТАПАХ ФУНКЦИОНИРОВАНИЯ

Информация, циркулирующая в автоматизированных системах (АС) различного назначения, является принципиально важным ресурсом, во многом определяющим национальную безопасность государства. В большинстве промышленных, правительственных, банковских, оборонных, правоохранительных организациях для сбора, хранения, обработки и передачи информации создаются АС на основе вычислительных сетей. Нарушение нормального функционирования АС организации вследствие НСД к обрабатываемой в ней информации влечет за собой значительный ущерб. Исследование вопросов оценки защищенности информации от НСД в АС является основой для разработки количественных требований к создаваемым системам защиты информации и их подсистемам.

В соответствии с руководящим документом ФСТЭК России в качестве нарушителя, осуществляющего действия, направленные на НСД к информации, обрабатываемой в АС

рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего, всего выделено четыре уровня:

1. Ведение диалога в АС – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.
2. Возможность создания и запуска собственных программ с новыми функциями по обработке информации.
3. Возможность управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.
4. Определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты. Очевидно, что данный подход является качественным, ориентирован на статические условия функционирования систем защиты, что неприемлемо в современных условиях развития технологий НСД к информации в АС, в том числе и в рамках приятой ведущими странами концепции «информационных войн».

Защищенность информации в АС от НСД определяется защищенностью ее ресурсов. В предлагаемой количественной модели воздействий нарушителя основной характеристикой является интенсивность нарушений безопасности ресурсов. Например, в наихудшем случае, если нарушитель «идеальный» (имеет высокую квалификацию, постоянно отслеживает появление новых уязвимостей, а также имеет возможность мгновенно использовать их для осуществления НСД к информации), итенсивность нарушений безопасности информации АС соответствует интенсивности появления уязвимостей в программно-аппаратном обеспечении АС. Интенсивность нарушений безопасности ресурсов целесообразно рассчитывать отдельно для трех основных типов угроз безопасности информации – угроз конфиденциальности, целостности и доступности.

Для АС специального назначения, являющихся первоочередным объектом атак в рамках информационных войн, можно выделить характерные периоды времени, отличающиеся видом зависимости интенсивности нарушений безопасности от времени:

1. Период обычного функционирования АС,
2. Период непосредственной угрозы информационных воздействий,
3. Период проведения в отношении АС информационных воздействий.

В период обычного функционирования АС зависимости интенсивностей нарушений безопасности ресурсов АС от времени для всех типов угроз безопасности информации в целом имеют стационарный характер, могут наблюдаться разовые всплески интенсивностей на небольшом по сравнению с оцениваемым периодом функционирования АС интервале времени. В период непосредственной угрозы информационных воздействий данные интенсивности увеличиваются, для угроз конфиденциальности информации интенсивность нарушений безопасности ресурсов имеет стационарный характер, для угроз целостности и доступности информации интенсивности нарушений безопасности ресурсов с течением времени монотонно возрастают. В период проведения в отношении АС информационных воздействий интенсивности нарушений безопасности ресурсов для угроз целостности и доступности информации имеют стационарный характер, интенсивность нарушений безопасности ресурсов для угроз конфиденциальности информации с течением времени монотонно убывает. Коэффициенты изменения интенсивностей нарушений безопасности ресурсов АС для периода непосредственной угрозы информационных воздействий и периода проведения в отношении АС информационных воздействий относительно периода обычного функционирования АС могут быть определены на основе статистических исследований или экспертным путем.

Данный подход может представлять интерес для специалистов, занимающихся вопросами защиты информации от НСД как на этапе разработки, так и в процессе эксплуатации систем защиты информации в автоматизированных системах.

Мошак Н.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ФОРМАЛИЗАЦИЯ ПРОЦЕССОВ ПЕРЕНОСА ТРАФИКА БЕЗОПАСНОСТИ В СИГНАЛЬНОЙ СИСТЕМЕ МУЛЬТИСЕРВИСНОЙ СЕТИ

Обеспечение доступа к глобальным национальным и международным информационным ресурсам требует обеспечения информационной безопасности, так как это затрагивает интересы мирового социума (медицинские базы данных; социальные, финансовые, производственные данные; сетевая информация (телефон и данные) и т. д.). В этой связи защита национальных информационных ресурсов сегодня является одной из составных задач обеспечения информационной безопасности и в

Российской Федерации. В рамках концепции по построению мультисервисных сетей (МСС) на Взаимоувязанной сети связи Российской Федерации защита сетей и систем управления от несанкционированного доступа, а также обеспечение заданного качества инфокоммуникационных услуг связи в условиях воздействия нарушителя определяются в качестве приоритетных задач.

Организация защищенной мультимедийной сессии в МСС является многофазным процессом и включает в себя:

1. Фазу регистрации пользователя;
2. Фазу формирования многокомпонентного потокового соединения;
3. Фазу подтверждения взаимной подлинности отправителя и получателя (peer-to-peer authentication);
4. Фазу авторизации на серверах инфокоммуникационных услуг (инфоуслуг) соответствующих поставщиков;
5. Фазу включения мультимедийного соединения.

Фаза регистрации пользователя выполняется в конечной мультимедийной станции пользователя EMS и предполагает исполнения в сети трех процедур, которые относятся к каждому легальному (зарегистрированному в сети) пользователю и являются средствами его защиты – это процедуры идентификации, аутентификации и авторизации. Процедура идентификации пользователя по его зарегистрированному в сети индивидуальному идентификатору выполняется в первую очередь, когда он делает попытку входа в сеть. Следующая процедура – верификация идентификатора – связана с процессом установления подлинности пользователя и называется его аутентификацией, после чего устанавливается сфера его действия и доступные ресурсы сети, т. е. осуществляется авторизация пользователя.

После успешной регистрации, сеть разрешает пользователю приступить к фазе формирования многокомпонентного потокового соединения заданной структуры и объема. Эта фаза всегда присутствует в сетях указанного класса. При этом требуемые объемы сетевых ресурсов в МСС для каждой из потоковых компонент (в зависимости от применяемой технологии коммутации) указываются либо в сигнальном сообщении, либо заранее оговариваются в «трафик-контракте». Потоковая структура, а также количественные и качественные показатели отдельной потоковой компоненты для различных мультимедийных соединений всегда определяются заказываемой инфокоммуникационной услугой. Мультимедийное соединение будет установлено при наличии необходимых сетевых ресурсов для переноса каждой из его потоковых компонент по проложенным для них маршрутам. В противном случае процесс установления соединения блокируется, о чем пользователь уведомляется сетью.

В случае успеха выполняется фаза подтверждения взаимной подлинности соединения отправителя и получателя (peer-to-peer authentication), для определения того, что соединение установлено между двумя взаимосвязанными легальными объектами сети и вся информация, предназначенная для обмена, верифицирована и подтверждена. После подтверждения взаимной подлинности поставщик инфоуслуг осуществляет процедуру авторизации пользователя на сервере инфоуслуг, т. е. на сервере инфоуслуг проверяются его полномочия по доступу к запрашиваемому сервису, после чего (при их наличии) осуществляется установление мультимедийного соединения.

Для организации защищенного информационного обмена в сессии могут быть востребованы четыре процедуры, а именно;

1. Аутентификация отправителя;
2. Аутентификация данных отправителя;
3. Аутентификация получателя;
4. Аутентификация доставленных данных.

Известно, что спецификации каждого логического уровня архитектуры МСС всегда включают в себя спецификацию протокола и спецификацию сервиса, который обеспечивается соответствующей службой и поддерживается этим протоколом для вышерасположенного уровня. При этом услуга защиты может включаться в процесс обслуживания уровневого протокольного примитива для каждого типа информации и/или представлять собой отдельную услугу уровня. В первом случае процесс предоставления механизмов защиты моделируется как система массового обслуживания (СМО) с протокольной услугой безопасности, во втором – отдельной однофазной или многофазной СМО с услугой безопасности (СМО УБ) и включает в себя как фазу передачи сервисных примитивов уровня, так и процесс их обработки в конечных и/или промежуточных системах. В любом случае реализация механизмов защиты осуществляется по принципам предоставления сервиса ВОС. Логические уровни, которые не содержат отдельных служб безопасности, могут запросить их на низших уровнях в процессе установления сеанса связи.

В докладе формализованы процессы подтверждения взаимной подлинности соединения отправителя и получателя с использованием механизмов простой и строгой аутентификации в МСС с центром авторизации при установлении защищенной мультимедийной сессии. Показано, что влияние указанных механизмов на информационное окружение МСС сводится в общем случае к трем аспектам: временной, протокольной и потоковой избыточности, которые должны быть учтены в критериях качества, а также в ограничениях задач анализа МСС.

Олимпиев А.А., Шерстюк Ю.М.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

РАСШИРЕНИЕ ОБЪЕКТНОЙ МОДЕЛИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ДЛЯ МОНИТОРИНГА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Одним из возможных способов информационного моделирования гетерогенной телекоммуникационной сети (ТКС) в средствах сетевого мониторинга и управления является использование объектной модели.

Данный способ предполагает, что модель ТКС создается на основе учетных сведений и данных мониторинга, и ее содержанием является коллектив взаимодействующих объектов – экземпляров соответствующих классов. Объекты создаются на основании описаний классов сетевых элементов, к которым они принадлежат.

Стандартная комплектация множества классов не учитывает наличия средств защиты информации (ЗИ) в рамках сети. Существующие требования к безопасности современных ТКС определяют необходимость в разработке расширения объектной модели с целью обеспечения мониторинга и управления средств ЗИ с учетом их специфики, классификации и организационной принадлежности.

Такое расширение объектной модели должно содержать описание следующих классов сетевых элементов:

– класс Средства ЗИ – компонент класса Узел связи;

– классы Программные средства ЗИ, Аппаратные средства ЗИ, Программно-аппаратные средства ЗИ – компоненты класса Средства ЗИ;

– классы, описывающие специфику отдельных средств ЗИ как объектов мониторинга и управления.

Для обеспечения динамики состояния таких объектов в соответствии с динамикой состояния их прототипов необходимо расширить механизм шлюзования данных мониторинга правилами обработки для данных мониторинга средств ЗИ.

Сбор данных мониторинга должен осуществляться средствами технологического мониторинга.

Паращук И.Б.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

К ВОПРОСУ О ЦЕЛОСТНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ ПРИ РЕАЛИЗАЦИИ ПРОЦЕССА ЗАЩИТЫ ИНФОРМАЦИИ В РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Вектор показателей целостности данных при реализации процесса защиты информации (ЗИ) в рамках процедур функционирования региональных телекоммуникационных сетей (РТС), должен содержать показатели (параметры), численно характеризующие точность, достоверность и полноту защищаемых данных, а также защищенность хранимой, обрабатываемой, передаваемой и принимаемой информации от возможных непреднамеренных и злоумышленных искажений. Иными словами, это свойство процесса ЗИ обеспечивать без чрезмерного ухудшения, с соблюдением требований (границ) по безошибочности и по точности (достоверности) и неискаженности хранимой, обрабатываемой, передаваемой и принимаемой информации, т.е. с соблюдением требований по числу ошибок и искажений данных.

Иными словами, целостность данных при реализации процесса ЗИ включает два компонента – достоверность (точность, безошибочность) и неискаженность (отсутствие искажений) в процессе ЗИ при ее хранении, обработке, передаче и приеме.

Целостность данных с точки зрения сохранения достоверности и точности информации при реализации процесса ЗИ, может оцениваться коэффициентом потери достоверности информации, хранимой, обрабатываемой, передаваемой и принимаемой в РТС. Этот коэффициент, с учетом мультисервисной информации, хранимой, обрабатываемой, передаваемой и принимаемой в РТС, включает потери слоговой разборчивости в виде количества утерянных (непонятых, искаженных до неузнаваемости) слов и словосочетаний для IP-телефонии, количество неправильно опознанных образов при реализации в РТС видеоконференцсвязи, а также количество ошибочно (искаженно) принятых, обработанных, хранимых и переданных данных при реализации услуг в РТС, ориентированных на передачу данных. В общем виде, с учетом многообразия угроз безопасности информации для каждого конкретного из множества сервисов (услуг), реализуемых и предоставляемых пользователям в РТС, интегральный коэффициент потери достоверности информации можно представить в виде соотношения, численно увязывающего: относительную опасность (сложность преодоления) конкретной угрозы; количество ошибочно (искаженно) принятых, обработанных, хранимых и переданных данных и вероятность достоверной передачи данных при функционировании системы защиты информации (С-ЗИ) в условиях воздействия угроз.

Показатель неискаженности (отсутствия искажений) информации при реализации процесса ЗИ численно характеризует способность процесса ЗИ реализовать противодействие модификации или разрушению информации, хранимой, обрабатываемой, передаваемой и принимаемой в РТС и может

быть численно представлен в виде коэффициента искажений (пакетов, блоков данных и т.п.). Физический смысл данного коэффициента – отношение количества искаженных данных к общему числу хранимых, обрабатываемых, передаваемых и принимаемых в РТС данных, причем, данный коэффициент должен быть минимальным и стремиться к нулю.

Таким образом, векторный показатель сохранения целостности данных при реализации процесса защиты информации включает вектор показателей достоверности (безошибочности, точности) и вектор показателей (показатель) неискаженности информации.

Вектор показателей сохранения конфиденциальности данных характеризует свойство процесса ЗИ обеспечивать доступность к информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи). В качестве элементов вектора показателей конфиденциальности данных могут выступать показатели защищенности от несанкционированного использования ресурсов РТС, включающие параметры, численно характеризующие свойства процесса ЗИ по защите от несанкционированного доступа (НСД) к информации и несанкционированного использования оборудования РТС.

Реализация этих свойств осуществляется с использованием механизма аутентификация пользователей РТС и идентификации оборудования РТС (например, с использованием паролей и модулей подлинности пользователей, индивидуального идентификационного номера оборудования, механизма секретности пользователей и введением механизмов авторизации – контроля приоритетов, исключающих доступ к ресурсам пользователям более низкого уровня иерархии, т.е. управление доступом по приоритетам, контроль полномочий объектов обслуживания). Показателями качества реализации данных свойств в рамках процесса ЗИ могут служить: коэффициент аутентификации пользователей, имеющий смысл обратный риску компрометации алгоритма и данных аутентификации; коэффициент идентификации оборудования, имеющий смысл обратный риску компрометации идентификационного номера оборудования, заложенному в каждый терминал РТС и коэффициент авторизации, имеющий физический смысл обратный риску доступа пользователя более низкого приоритета к услугам РТС, предназначенным для уровня пользователей более высокого приоритета.

Паращук И.Б.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ПОКАЗАТЕЛИ ДОСТУПНОСТИ АВТОРИЗИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ К ЗАЩИЩАЕМОМУ ИНФОРМАЦИОННОМУ РЕСУРСУ

Внутренними свойствами процесса защиты информации (ЗИ), характеризующими качество и эффективность данного процесса (т.е. степень удовлетворения пользователя региональных телекоммуникационных сетей предоставляемыми ему услугами по ЗИ), на наш взгляд, являются: доступность авторизированных (легальных) пользователей региональных телекоммуникационных сетей к защищаемому информационному ресурсу при реализации процесса защиты информации, непрерывность ЗИ, целостность информации (ее достоверность) при реализации процесса ЗИ, конфиденциальность информации, а также затраты ресурсов на реализацию процесса ЗИ.

Показатели доступности при реализации процесса ЗИ является одним из важнейших в структуре показателей качества процесса ЗИ, а входящие в него параметры призваны количественно описывать способность (свойство) процесса ЗИ:

– предоставлять пользователям региональных телекоммуникационных сетей (РТС) услуги безопасного доступа к защищенной информации тогда, когда это им необходимо,

– в необходимом пользователям услуг месте,

– и в течение требуемого времени (продолжительность предоставления услуг) с требуемым качеством (достоверность и целостность предоставления услуг).

Вектор показателей доступности авторизированных (легальных) пользователей РТС к защищаемому информационному ресурсу имеет две составляющие – временную (когда, своевременность) и топологическую (где).

В качестве одного из основных свойств процесса ЗИ выступает временная доступность или своевременность, рассматриваемая как способность процесса ЗИ обеспечивать доступ пользователей РТС к защищаемым ресурсам телекоммуникационной системы и предоставление им требуемого перечня безопасных услуг в установленные сроки. Показатель своевременности доступа авторизированных пользователей РТС к защищаемому информационному ресурсу – к требуемой n – ой (из перечня возможных N) услуге, может быть выражен через время ожидания доступа к n–ой услуге и включает в себя время, затрачиваемое пользователем РТС на формирование и передачу запроса на оказание n–ой услуги, время, затрачиваемое процессом ЗИ на проверку полномочий терминала РТС, пользователя (аутентификация, идентификация, полномочия, приоритетность) и обработку запроса пользователя на оказание n–ой услуги, время, затрачиваемое процессом ЗИ на обеспечение безопасной реализации запроса в рамках запрашиваемой n–ой услуги или на передачу сигнала пользователю о невозможности обеспечения безопасной реализации запроса.

С учетом многообразия угроз безопасности информации для каждого конкретного из множества сервисов (услуг) N, реализуемых и предоставляемых пользователям, своевременность доступа авторизированных (легальных) пользователей РТС можно охарактеризовать средним временем доступа пользователей к защищаемому информационному ресурсу, интегральным, по всему перечню услуг и соответствующих им угроз, показателем.

Кроме того, временная доступность авторизированных (легальных) пользователей РТС к защищаемому информационному ресурсу может количественно характеризоваться интенсивностью отказов в доступе, вызванных сбоями (ошибками) при реализации процесса ЗИ, а также средним временем между отказами в доступе. Так, например, интенсивность отказов в доступе авторизированных (легальных) пользователей РТС к защищаемому информационному ресурсу может определяться как отношение количества полученных (по вине процесса ЗИ) пользователями отказов в доступе к общему числу запросов на доступ к защищаемому информационному ресурсу.

Помимо обеспечения услугами в (за) необходимое время, легальным пользователям РТС должна быть обеспечена топологическая доступность к защищаемому информационному ресурсу, т.е. доступ к защищенным услугам в необходимом ему месте. Должны соблюдаться требования по топологической доступности к защищаемой информации, причем как для пользователей РТС, построенных на основе кабелей, так и для пользователей беспроводных РТС. В этом случае топологическая доступность зависит от радиуса контролируемой зоны, от радиуса зоны охвата точки доступа беспроводных РТС, от удаленности пользователя, от флуктуаций параметров радиосигнала беспроводных РТС, вызванного многолучевостью, от уровня потерь при распространении сигналов по кабелю и при распространении радиоволн с учетом неровностей земли, препятствий и др.

Таким образом, показатели доступности, составляющие содержание вектора показателей топологической доступности, количественно характеризуют способность процесса ЗИ не препятствовать доступу авторизированных (легальных) пользователей РТС к защищаемому информационному ресурсу и не затруднять предоставление им требуемого перечня услуг в установленном месте их нахождения и при перемещении пользователя.

Паращук И.Б., Паращук Е.И.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного, ООО «Максима»

НАПРАВЛЕНИЯ ПОВЫШЕНИЯ ТОЧНОСТИ И ОПЕРАТИВНОСТИ АНАЛИЗА ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Эффективное государственное, региональное и муниципальное управление на современном этапе, в соответствии с новыми общемировыми реалиями развития инфокоммуникаций, требует организации взаимодействия вычислительных сетей региона и региональных телекоммуникационных сетей (РТС) с сетями общего пользования, в частности, с глобальной сетью Интернет. Достоинства взаимодействия РТС с сетями общего пользования обуславливают доступ должностных лиц региона к мировым информационным ресурсам, возможность работы информационных систем регионов между собой, а также с информационными системами других органов власти страны.

Однако, анализ современных условий, в которых осуществляется функционирование РТС, позволяет выделить ряд противоречий, обусловленных ужесточением требований к качеству процессов защиты информации (ЗИ) в рамках обмена всеми видами информации и постоянно растущими возможностями нарушителей по реализации угроз ЗИ. Основными противоречиями являются ограниченная устойчивость систем ЗИ (С-ЗИ) к современным угрозам информационной безопасности и иным преднамеренным и непреднамеренным воздействиям, низкий уровень автоматизации процесса управления функционированием С-ЗИ.

Анализ состава современных С-ЗИ, особенностей их функционирования, анализ методов и средств ЗИ, принципов их построения, анализ основных требований к современным С-ЗИ показывают, что разрешение указанных противоречий возможно на пути развития защищенных информационных систем по пути интеграции различных видов услуг по защите информации в рамках комплексных и высокоэффективных С-ЗИ, внедрения новейших достижений с точки зрения управления процессом ЗИ, а также внедрения современных методов перераспределения ресурсов С-ЗИ с целью обеспечения заданной эффективности ЗИ при ограниченных затратах.

Основой методологии построения таких С-ЗИ являются методы оценивания эффективности их функционирования. Разработке методов оценивания эффективности функционирования сложных организационно-технических систем посвящен целый ряд исследований. Разработаны методы анализа эффективности, которые легли в основу существующих частных методик оценивания эффективности сложных технических систем. Вместе с тем, дальнейшее их использование для сравнительного анализа существующих С-ЗИ РТС и выработки перспективных направлений их развития, с точки зрения ЗИ, становится затруднительным в силу следующих причин:

Во-первых, учет протекающих в работающей С-ЗИ переходных процессов, многокритериальный характер современных требований, предъявляемых к качеству ЗИ и управлению процессом ЗИ, приводят к постановке не только векторной, но и динамической задачи анализа эффективности С-ЗИ такого класса, решение которой в рамках существующих методик не проводилось.

Во-вторых, существующие частные методики, в подавляющем своем большинстве, не обеспечивают учет параметров органов и процессов управления С-ЗИ при разработке систем показателей качества (СПК) С-ЗИ, или (если такая задача решается) не учитывают значения отклонений показателей качества С-ЗИ от требований к ним, что для анализа качества и эффективности таких сложных систем является немаловажным.

В-третьих, необходимый в существующих методиках сбор статистики о состоянии элементов С-ЗИ, требует значительного времени и снижает оперативность анализа, и следовательно – повышает время реакции подсистемы автоматизированного управления (ПАУ) С-ЗИ на реализуемые нарушителем угрозы и вводимые управляющие воздействия.

Что касается точности оценивания, то в существующих методиках дисперсия ошибки оценивания остается на уровне априорной дисперсии самого исследуемого процесса ЗИ, что в рамках современных высокоточных систем управления недопустимо.

Все это обуславливает объективную необходимость развития существующих методик оценивания эффективности функционирования С-ЗИ на случай учета переходных процессов, вызванных изменением структуры, режимов и условий их функционирования с целью повышения точности и оперативности анализа эффективности функционирования С-ЗИ при ВЛсСОП.

Это позволит, на основе методов стохастического оценивания показателей качества С-ЗИ, повысить точность и оперативность анализа эффективности функционирования С-ЗИ в условиях различного вида воздействий. В свою очередь, это позволит сформулировать организационно-технические предложения по совершенствованию структуры и алгоритмов работы подсистем автоматизированного управления С-ЗИ, что, несомненно, выразится в повышении общей эффективность процесса ЗИ при взаимодействии вычислительных сетей региона и региональных телекоммуникационных сетей с сетями общего пользования.

Пунанов М.С.
Россия, Санк-Петербург, Санкт-Петербургский государственный университет водных коммуникаций

БЕЗОПАСНОСТЬ IP-СЕТЕЙ ДЛЯ ПРОВАЙДЕРА УСЛУГ

Основная проблема, с которой сталкиваются сегодня провайдеры услуг, – это лавинный трафик злоумышленников, источниками которого служат различные оконечные точки, разбросанные по различным границам сети. В современной терминологии этот тип поведения ассоциируется, в частности, с такими угрозами, как распределенные атаки типа «отказ в обслуживании» (DDoS), современные Интернет-черви, почтовый спам, фишинг и вирусы. Количество трафика, которое генерируется вследствие инфицирования, и последующие всплески трафика могут нарушить нормальную работу сети и создают дополнительный риск для сетевых устройств, которые ответственны за выполнение базовых функций маршрутизации и коммутации пакетов. В настоящее время безопасность становится критической характеристикой всех сервисов и играет исключительно важную роль в прибыльности работы провайдеров услуг.

Сегодня для поддержания более высокого уровня сетевой безопасности провайдерам услуг необходимо перейти от традиционного реактивного подхода к поэтапному проактивному подходу, уменьшая количество существующих уязвимостей, улучшая показатели времени реакции и эффективно подавляя атаки. Вместе с тем существует определенный кадровый дефицит квалифицированных специалистов в сфере информационной безопасности и дефицит систем обеспечения безопасности, использующих механизмы корреляции, для формирования комплексного представления состояния сети в целом. Время совершенствовать операции по обеспечению безопасности уже настало. Наиболее передовые средства и решения по обеспечению безопасности будут переживать эволюционное развитие по мере перестройки IP-сетей провайдеров. Эффективное обеспечение безопасности сетей – сложная и многогранная задача.

Рожнов М.Д., Шерстюк Ю.М.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

БЕЗОПАСНОСТЬ ПРОГРАММНЫХ СРЕДСТВ ДЛЯ УПРАВЛЕНИЯ РАЗНОРОДНЫМ ТЕЛЕКОММУНИКАЦИОННЫМ ОБОРУДОВАНИЕМ

В условиях использования разнородного телекоммуникационного оборудования интерес представляют унифицированные программные средства узлового и сетевого управления, позволяющие осуществлять управление этим оборудованием и сетями, образованными на его основе.

По соображениям информационной безопасности программные средства управления телекоммуникациями подлежат сертификационным испытаниям на отсутствие недекларированных возможностей и соответствие разного рода требованиям. Процедура сертификации предполагает фиксацию контрольной суммы программных средств, что делает процесс их дальнейшего изменения достаточно проблематичным. В то же время динамика парка средств телекоммуникаций приводит к необходимости своевременной адаптации средств управления – обеспечению возможности включения в контур управления оборудования новых типов.

В данной ситуации программные средства управления телекоммуникационным оборудованием целесообразно создавать в виде инвариантного программного ядра, адаптируемого к парку управляемого оборудования посредством метаописаний. Такие метаописания, представленные на декларативном языке, являются информационными изделиями и не требуют сертификационных испытаний. Основным содержанием метаописаний является описание MIB агентов управления средств телекоммуникаций и экранных форм, предназначенных для отображения и изменения значений MIB. Тем самым интерпретация формального смысла метаописаний позволяет «настроить» средства управления на взаимодействие с агентами управления средств телекоммуникаций. Для сетевого уровня управления метаописания содержат абстракции, соответствующие этому уровню (сети, тракты, услуги и т.д.) и правила оценки их состояния по данным технологического мониторинга.

Данный подход реализован на практике и применим не только для средств управления телекоммуникациями.

Сазонов В.В.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

О НЕОБХОДИМОСТИ РАЗРАБОТКИ МЕТОДИКИ СИНТЕЗА АНСАМБЛЕЙ ДИСКРЕТНЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ ДЛЯ ЗАЩИЩЕННЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ

С бурным развитием информационной инфраструктуры нашей страны, увеличивается значение систем передачи дискретной информации по каналам связи. Особое место занимают системы передачи информации с дискретными ортогональными сигналами, например, сотовые системы подвижной радиосвязи стандарта CDMA. В них реализована технология многостанционного доступа с кодовым разделением каналов. Данная технология легла в основу большей части проектов стандартов, разрабатываемых для глобальных систем подвижной связи третьего поколения. В связи с чем, в настоящее время к системам передачи информации с кодовым разделением каналов (СПИ КРК) предъявляются повышенные требования к защищенности.

Защищенность передачи сообщений по радиоканалам СПИ КРК может быть достигнута путем обеспечения энергетической скрытности сигналов – переносчиков информации, структурной скрытности этих сигналов и информационной скрытности самого сообщения. При этом лишь направление повышения структурной скрытности, где основополагающую роль играет количество структур ансамблей дискретных ортогональных сигналов (АДОС), наименее проработано в существующих СПИ КРК.

Оценка защищенности существующих СПИ КРК в рамках повышения структурной скрытности показывает, что:

Во-первых, для формирования АДОС используются линейные псевдослучайные последовательности (М-последовательности и коды Голда), которые не обеспечивают структурной скрытности шумоподобного сигнала из-за его предсказуемости.

Во-вторых, для формирования АДОС используется всегда лишь одна структура, причем известная (функции Уолша).

В-третьих, корреляционные свойства используемых АДОС не удовлетворяют условию малости боковых пиков функций корреляции сигналов в ансамбле.

Таким образом, в практике обнаруживается противоречие, заключающееся в том, что для формирования большого количества структур АДОС для защищённых СПИ КРК необходимо значительное увеличение их аппаратной сложности, поскольку единый принцип формирования структур АДОС не используются.

Оценку подходов формирования АДОС удобно вести разделив на три основные направления:

Первое направление базируется на анализе свойств сигналов, для описания которых используется широкий класс известных в математике ортогональных полиномов Якоби, Гегенбауэра, Чебышева, Лагерра, Эрмита, дискретных ортогональных функций Уолша, Хаара, Радемахера, Виленкина-Крестенсона, Трофимова - Ласунского. Среди работ этого направления следует выделить публикации Л.Е. Варакина, А.Г. Леонтьева, М.К. Размахнина, В.П. Яковлева, Х. Хармута.

Второе направление связано с построением производных сигналов на базе перемножения специально подобранных производящих последовательностей на известные ортогональные функции и достаточно полно представлено работами Л.Е. Варакина, Н.Г. Дядюнова, Д. Стиффлера.

Третье направление связано с векторным синтезом АДОС по совокупности требований к ним. Среди работ этого направления известны работы В.С. Попенко, А.П. Жука, З.В. Черняка и других.

Анализ работ первого направления показывает, что оно ограничено и остается только на уровне рассматриваемых систем сигналов, а работы второго направления ограничиваются синтезом АДОС всего лишь по одной характеристике и не могут быть использованы для решения задачи синтеза систем сигналов по совокупности предъявляемых требований и ограничений. Третье направление имеет математические ограничения по размерности синтезируемых АДОС.

На основании вышеизложенного видно, что для повышения защищённости систем передачи информации с кодовым разделением каналов, необходимо на основании модернизации третьего направления разработать методику построения АДОС с заданными параметрами структурной скрытности.

Саид Моджиб А.С., Комашинский В.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

УПРАВЛЕНИЕ АДАПТИВНОЙ OFDM МОДУЛЯЦИЕЙ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ

В настоящее время основными направлениями развития систем передачи данных являются увеличение скорости передачи, увеличение мобильности, создания самоорганизующихся сетей и стремление переход к когнитивным (интеллектуальным) системам управления. Наиболее перспективными для создания интеллектуальных систем управления представляются такие технологии как: нечеткая логика и нейронная сеть. Основная идея в этих технологиях заключается в переходе от строго формализованных алгоритмов, которые предлагают метод решения задачи, к логическому программированию с указанием на то, что нужно решать на базе знаний, накопленных специалистами в конкретных предметных областях.

Одним из подходов повышения скорости передачи в перспективных беспроводных сетях является создание систем с адаптивной OFDM модуляций (AOFDM). Интересной является задача по построению системы когнитивного управления адаптивной OFDM на основе мягких вычислений, например, нечеткая логика.

Для решения задачи, соответственно вся зона покрытия, охватываемая конкретной точкой доступа или радио терминалом, разбита на участки с ранней достигаемой энергии сигнала т.е. вся зона покрытия возможно обеспечить разные скорости передачи соответствие применению разных схем модуляции (адаптивная модуляция). Для управления скорости передачи (т.е. управления адаптивной модуляцией) в зоне охвата радио терминалом строятся функции принадлежности в тригонометрической форме. Разработка системы нечеткой логики объясняется следующим образом, соответственно полученному значению SNR и существующему типу модуляции в системе управляется схемой модуляции для передачи следующего кадра.

Решение принимается на основе правил Мамдани нечетких множеств в таком виде:

1. Если принимаемая схема модуляции в системе была низкая и значение отношения сигнал-шум увеличивается, то используется более высокую схему модуляции для передачи следующего кадра.
2. Если принимаемая схема модуляции в системе была высокая и значение отношения сигнал-шум уменьшается, то используется более низкую схему модуляции для передачи следующего кадра.

И т.д. надо считывается все возможные варианты.

Использование нечеткой логики в системах принятия решения позволяет очень эффективно изменять схему модуляции при изменении состояния канала. В результате показывается, что OFDM модуляция с применением нечеткой логики представляет более эффективности разработки системы по вероятности ошибки и по пропускной способности одновременно, по сравнению с OFDM системой, использующей классической логики управления.

Стародубцева Ю.И., Бухарин В.В., Балясова А.Е.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Развитие встраиваемых и других автономных вычислительных устройств, построенных на базе электронных вычислительных машин, свидетельствует о том, что все более и более ответственные задания возлагаются на электронные системы принятия решения. Это диктует достаточно жесткие требования к надежности функционирования таких систем, которая складывается из показателей надежности самой электронной вычислительной машины и исполняемого на ней программного обеспечения. При этом важность второго аспекта неоправданно занижается.

В настоящее время известно большое количество теоретических исследований и практических рекомендаций по организации процесса разработки программного обеспечения для сокращения числа ошибок, повышения эффективности и надежности его функционирования, но для этого, по сути, необходимо выполнить заново проектирование и разработку существующего программного

обеспечения, что на практике неосуществимо. Использование предлагаемого подхода призвано обеспечить безопасное и надежное функционирование программного обеспечения с учетом уже существующих в этом программном обеспечении недостатков, а также с учетом возможных случайных и преднамеренных воздействий на программное обеспечение с целью нарушения его работоспособности.

В контексте рассматриваемой проблемы под безопасностью функционирования программного обеспечения понимается отказоустойчивое выполнение его функциональных возможностей за счет противодействия следующим негативным факторам:

– зависание программного обеспечения в целом или одной из его подсистем;

– случайные воздействия на программное обеспечение, приводящие к нарушению его функционирования (аварийное завершение работы);

– преднамеренные воздействия на программное обеспечение, нацеленные на нарушение его функционирования.

Это требует применения дополнительных мер противодействия.

Для решения рассматриваемой проблемы может использоваться метод, заключающийся в том, что перед запуском модуля контроля и контролируемого программного обеспечения (ПО) в модуле контроля формируют данные контролируемого ПО, состоящие из характеристик ПО, набора контролируемых подсистем, конфигурации программного обеспечения в различных режимах функционирования, ожидаемой интенсивности сигналов оповещения. Далее производится измерение реальных значений характеристик ПО и формируются эталонный уникальный идентификатор по значениям характеристик ПО с использованием функции преобразования. После запуска программного модуля контроля и контролируемого ПО передаются уникальные идентификаторы от контролируемого ПО программному модулю контроля. Сравнивают эталонный уникальный идентификатор ПО с полученным уникальным идентификатором от контролируемого ПО. В процессе функционирования ПО через криптографически защищенный канал на ключе s измеряют интенсивность сигналов оповещения от контролируемого ПО. Сравнивают ожидаемые и реальные интенсивности сигналов оповещения. После определения контролируемой подсистемы в которой нарушено функционирование осуществляется выделение контролируемых подсистем, влияющих на подсистему, в которой нарушено функционирование по конфигурации программного обеспечения в определенном режиме функционирования. В дальнейшем осуществляется либо перезапуск контролируемых подсистем ПО, приводящих к сбоям функционирования данной подсистемы либо перезапуск ПО в полном объеме при повторном несовпадении ожидаемой и реальной интенсивности сигналов оповещения.

Таким образом, рассмотренный метод за счет определения подлинности программного обеспечения путем введения эталонного уникального идентификатора по значениям характеристик программного обеспечения, определения подсистем программного обеспечения нарушающих его функционирование и уменьшения временных затрат на реализацию действий по обеспечению отказоустойчивого выполнения программного обеспечения позволяет обеспечить повышение достоверности контроля функционирования программного обеспечения от случайных и преднамеренных воздействий, повышение точности контроля функционирования программного обеспечения и обеспечения требуемых временных затрат на выполнение функций автоматизированной системы.

Суравикин Д.В.
Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»

ОСОБЕННОСТИ УПРАВЛЕНИЯ УСЛУГАМИ В ЗАЩИЩЕННОЙ МУЛЬТИПРОТОКОЛЬНОЙ СЕТИ

Производители современных сетевых устройств наделяют их богатой функциональностью, что позволяет операторам связи строить на их основе мультисервисные сети, обеспечивающие передачу разнородного трафика с различными приоритетами обслуживания. При этом мультипротокольность сетевого оборудования с одной стороны дает возможность оператору связи самому выбирать технологию построения мультисервисной сети (Ethernet, IP/MPLS, ATM) в зависимости от требований, предъявляемых пользователями к услугам связи, и других факторов, а с другой стороны – предоставляет широкий функционал механизмов и протоколов управления качеством предоставления (QoS) услуг при использовании этой технологии.

Например, перенос кадров Ethernet может осуществляться на основе значений полей метки, определенной стандартом 802.1Q. В IP-сетях используются архитектуры интегрированных (IntServ) и дифференцированных (DiffServ) услуг. Технология MPLS поддерживает механизмы управления QoS канального и сетевого уровней, а также имеет собственные средства – MPLS QoS, управление трафиком (TE – Traffic Engineering) и виртуальные частные сети (VPN – Virtual Private Network). Особо стоит отметить механизм управления трафиком, который предоставляет возможность устанавливать явный путь, по которому будут передаваться потоки данных. Применение этого механизма позволяет администратору сети управлять направлением прохождения трафика, распределять нагрузку в сети, планировать резервирование ресурсов. Технология ATM использует собственные уникальные механизмы QoS. Таким образом, механизмы и протоколы QoS мультисервисной сети позволяют

оператору связи оперативно подстраиваться под изменяющиеся требования пользователей к предоставляемым услугам связи.

Одной из особенностей защищенных мультисервисных сетей является задача обеспечения QoS с учётом выполнения требований по безопасности, что обусловливает дополнительные сложности в управлении качеством обслуживания. Все сетевые параметры условно разделяются на параметры функционирования, имеющие отношение к функционированию определенной технологии передачи трафика (формат кадра, синхронизация, IP-адрес и др.) и параметры безопасности (контроль целостности ПО и конфигурации, параметры идентификации и аутентификации и др.), имеющие отношение к обеспечению сетевой безопасности.

По нашему мнению, параметры механизмов и протоколов QoS также должны быть отнесены к параметрам безопасности, так как они управляют сетевыми ресурсами (полосой пропускания, количеством и длиной очередей, правилами обслуживания очередей и др.), а обеспечение доступности сетевых ресурсов является одним из требований по обеспечению безопасности защищенной сети. Стоит также отметить, что трафик о состоянии параметров безопасности является частью общего трафика системы управления сетью, который обычно передается по «собственным» направлениям связи, т.е. организованным управляемыми сетевыми элементами. Поэтому несанкционированное изменение параметров QoS за счёт внешнего воздействия или ошибочных действий администратора сети может привести к резкому ухудшению качества обслуживания пользователей, вплоть до полного прекращения обслуживания, а также к блокированию передачи управляющей информации, чем может воспользоваться нарушитель.

Как правило, за мониторинг и управление параметрами безопасности в сложных системах управления отвечает специальный программный модуль, который администрируется специальным должностным лицом – администратором безопасности.

Отметим, что в защищенных мультисервисных сетях механизмы и протоколы QoS могут также использоваться в качестве дополнительных средств разграничения доступа к информации пользователей (изолирование трафика различных виртуальных сетей), а также в качестве дополнительных средств защиты от компьютерных атак (ограничение интенсивности трафика определенного протокола).

Исследование вопросов обеспечения заданного качества обслуживания в защищенных мультисервисных сетях, где важная роль отводится безопасности информационного обмена, требует повышенного внимания. В докладе рассматриваются особенности применения механизмов обеспечения качества обслуживания в защищенных мультисервисных сетях.

Таран В.В., Шерстюк К.Ю.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

ИСПОЛЬЗОВАНИЕ СЛУЖБЫ ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ ДЛЯ ПРОТИВОДЕЙСТВИЯ АТАКАМ НА СРЕДСТВА ТЕЛЕКОММУНИКАЦИЙ

Любое средство телекоммуникаций (СТК), имеющее в своем составе вычислительную среду с выполняемым в ней программным обеспечением и с возможностью сетевого доступа к ней потенциально является объектом компьютерной атаки (КА).

Важнейшей особенностью абсолютного большинства СТК как объекта защиты от КА является их «закрытость» – отсутствие возможности размещения средств защиты (СЗ) от атак непосредственно в их вычислительной среде. Типовой вариант СТК представляет собой программно-аппаратное средство, в состав которого входит агент управления (АУ), поддерживающий некую информационную базу управления (MIB) и способный взаимодействовать с внешними по отношению к СТК средствами управления по определенному протоколу. Практически никогда в имеющихся СТК внутреннее программное обеспечение не решает все задачи, связанные с защитой от КА, а в ряде случаев решение таких задач является технически невозможным (например – легитимность полученного запроса на изменение параметров СТК, имеющего все необходимые формальные признаки). Соответственно, средства защиты в этом случае должны являться внешними по отношению к СТК, и их целесообразно объединить со средствами технологического управления СТК.

Известен способ построения средств технологического управления (ТУ) СТК, в соответствии с которым создается служба технологического управления (СТУ) телекоммуникациями. Одной из особенностей такой СТУ является постоянный циклический опрос АУ СТК для получения актуальных значений объектов MIB. Подобная СТУ может выступать в качестве средства обнаружения КА (детектора атак) определенных разновидностей.

Так, если из множества параметров MIB можно выделить подмножество таких параметров, факт и/или скорость изменения которых означают наличие некоего нелегитимного воздействия на СТК, несанкционированного доступа к нему, попытки нарушить его механизмы управления/защиты, то наличие в СТУ средств контроля изменения значений таких параметров превращает СТУ в средство обнаружения целого класса возможных атак.

Например, в случае, когда АУ поддерживает MIB согласно RFC-1215, свидетельством попытки несанкционированного обращения к СТК будет факт формирования АУ извещения autentificationFailure, полученного СТУ от АУ.

Свидетельством оказанного нелегитимного воздействия на АУ также может служить факт расхождения значения параметра MIB, доступного для установки/изменения со стороны СТУ, при условии, что команда на такое изменение в СТУ не выдавалась (в СТУ фиксируются все выполненные управляющие воздействия). Например, если у мультиплексора между двумя опросами менеджером его АУ произошло изменение таблицы коммутации трактов, а подобная команда не выдавалась, то данное изменение осуществлено в обход СТУ.

Существенно, что в ряде случаев нелегитимно измененные значения могут быть автоматически восстановлены благодаря наличию в СТУ «правильных» значений. Более того, могут быть подготовлены сценарии управляющих воздействий на СТК (необязательно только на атакованные), подлежащие их автоматическому выполнению в СТУ как реакция на определенные обнаруженные ситуации (зафиксированные события).

Таким образом, средства ТУ при их соответствующем расширении могут сыграть существенную роль в обеспечении безопасности и устойчивости функционирования СТК и телекоммуникационных сетей в целом.

Тупико О.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций

ВЫБОР ПОДХОДА К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ

Так уж сложилось, что, несмотря на понимание важности значения вопросов информационной безопасности, руководители продолжают уделять им наименьшее внимание. В качестве основных причин чаще всего указывают недостаток финансирования и низкая приоритетность вопросов информационной безопасности при распределении ресурсов. В частности это касается обеспечения информационной безопасности сети предприятия.

Обычно выделяют два подхода к проблеме обеспечения безопасности компьютерных систем и сетей (далее КС): «фрагментарный» и комплексный.

«Фрагментарный» подход направлен на противодействие четко определенным угрозам в заданных условиях. В качестве примеров реализации такого подхода можно указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т. д.

Достоинством такого подхода является высокая избирательность к конкретной угрозе, а соответственно и экономическая выгода его использования. Существенным его недостатком можно назвать отсутствие единой защищенной среды обработки информации. Фрагментарные меры защиты информации обеспечивают защиту конкретных объектов КС только от конкретной угрозы. Даже небольшое видоизменение угрозы ведет к потере эффективности защиты. Чаще всего руководители ограничиваются этим методом из-за его относительно дешевизны.

Альтернативным «фрагментарному» подходу является комплексный подход. Он ориентирован на создание защищенной среды обработки информации в КС, объединяющей в единый комплекс различные меры противодействия угрозам. Организация защищенной среды обработки информации позволяет гарантировать определенный уровень безопасности КС, что является несомненным достоинством комплексного подхода. К недостаткам этого подхода относятся: ограничения на свободу действий пользователей КС, чувствительность к ошибкам установки и настройки средств защиты, а также сложность управления.

Комплексный подход применяют для защиты КС крупных организаций или небольших сетей, выполняющих ответственные задачи или обрабатывающих особо важную информацию. Нарушение безопасности информации в КС крупных организаций может нанести огромный материальный ущерб как самим организациям, так и их клиентам. Поэтому такие организации должны уделять особое внимание гарантиям безопасности и реализовывать комплексную защиту. Комплексного подхода придерживаются большинство государственных и крупных коммерческих предприятий и учреждений. Этот подход нашел свое отражение в различных стандартах.

Комплексный подход к проблеме обеспечения безопасности основан на разработанной для конкретной КС политике безопасности. Политика безопасности регламентирует эффективную работу средств защиты КС. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях. Надежная система безопасности сети не может быть создана без эффективной политики сетевой безопасности.

Комплексный подход к решению проблемы обеспечения безопасности, рациональное сочетании законодательных, административно-организационных и программно-технических мер и обязательное следование стандартам – это тот фундамент, на котором строится вся система защиты корпоративных сетей.

Руководители отделов информационной безопасности должны научиться четче разъяснять, насколько важна информационная безопасность для стратегии бизнеса компании. Вопросы информационной безопасности более не являются областью компетенции лишь компьютерных экспертов, к их решению необходимо привлекать высшее руководство компаний. Для эффективного обеспечения информационной безопасности организациям необходимо увязать свои потребности в этой области с задачами бизнеса, проводить оценку экономической эффективности вложений в информационную безопасность и стремиться внедрять комплексные решения в этой области.

Шоров А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

АРХИТЕКТУРА МЕХАНИЗМА ЗАЩИТЫ ОТ ИНФРАСТРУКТУРНЫХ АТАК НА ОСНОВЕ ПОДХОДА «НЕРВНАЯ СИСТЕМА СЕТИ»

Повсеместное использование вычислительной техники, подключенной к глобальной сети Интернет, а также недостаточный уровень информационной безопасности, позволяют злоумышленникам осуществлять широкомасштабные атаки на инфраструктуру компьютерных сетей, вовлекая в криминальную деятельность большое количество вычислительных узлов. Для защиты компьютерных сетей от инфраструктурных атак необходимо исследовать механизмы их реализации и постоянно осуществлять поиск новых механизмов защиты способных противодействовать им.

Одним из механизмов, призванных обеспечить защиту от инфраструктурных атак, является подход «нервная система сети». В работе рассматриваются архитектура механизма защиты основе подхода «нервной системой сети». Подход «нервная система сети» использует распределенный механизм сбора и обработки информации для обнаружения атак и противодействия им. В каждой автономной системе имеется специальный сервер, который выполняет функции сбора и обработки информации, координации подключенных к нему узлов и обмена данными об атаках с серверами в других сетях.

Узлы выполняют функции обнаружения и блокировки атак, а также передачи информации об обнаруженных атаках на сервер к которому они подключены. Каждый узел «нервной системы сети» состоит из функциональных блоков со стандартным интерфейсом передачи данных, что обеспечивает большую гибкость при динамическом обновлении и обслуживании узлов. Алгоритм работы узла «нервной системы сети» следующий. На первом этапе обработки узел распределяет потоки, исходя из IP-адреса отправителя и IP-адреса получателя. Далее он определяет типы пакетов, отправляемых источником. После этого производится анализ трафика, полученного с помощью модуля анализа и противодействия. К модулю анализа и противодействия подключена база данных правил и сигнатур. Из этой базы он получает информацию об угрозах для анализа трафика. Модуль анализа и противодействия работает следующим образом. Пакеты из модуля классификации попадают в компонент анализ на основе правил, где на основе правил фильтрации принимается решение о блокировке трафика. Далее трафик проходит модули поиска аномалий и сигнатурного анализа. Если какой-либо модуль принял решение о блокировке трафика, пакет, не проходя через последующие фильтры, попадает на модуль блокировки, который в случае положительного решения удаляет пакет и передает информацию о нем в модуль сдерживания атак. Модуль сдерживания атак, с помощью компонентов осуществляющих обмен данными, пересылает информацию об обнаруженных угрозах серверу и другим узлам, а также получает информацию от них и обновляет базу данных правил и сигнатур.

Если узел обнаруживает вредоносные потоки трафика, он отправляет сообщение об этом серверу «нервной сети», с которым он связан. Сообщение содержит следующие поля: идентификатор маршрутизатора, идентификатор вредоносного потока, идентификатор маршрутизатора от которого получен пакет, идентификатор маршрутизатора которому передается пакет, количество маршрутизаторов на верхнем уровне, количество маршрутизаторов на нижнем уровне, состояние маршрутизатора. Сервер «нервной системы сети» имеет модуль обмена данными с подчиненными ему узлами, а также с серверами находящимися в других подсетях. Модуль обмена данными соединен с компонентом, отвечающим за анализ данных и принятие решений. С помощью него, модуль обмена данными получает команды и информацию для отправки на узлы и другие сервера «нервной системы» и доставляет ему информацию о событиях, происходящих в сети. К модулю анализа и принятия решений подключена база данных, которая служит хранилищем информации полученной из внешних источников и поставляет ранее сохраненную информацию. Работа модуля анализа и принятия решений осуществляется следующим образом. Информация, полученная от модуля обмена данными с узлами и серверами «нервной системы сети», попадает в модуль приоритезации, где в соответствии с установленными политиками, события классифицируются, и определяется, насколько важна та или иная информация, на основе чего будет принято решение об очередности выполнения действий в следующих блоках. Затем данные попадают в модуль корреляции, который, в соответствии с приоритетом, выбирает события и запрашивает похожие события из базы данных с помощью компонента обмен данными с БД. После этого происходит сопоставление набора событий, и определяется уровень угрозы. Далее в блоке решение о блокировке, на основе политик и порогов, определяется реакция на текущую ситуацию в сети. В случае необходимости

данные отправляются серверам и узлам «нервной системы сети», информация о принятом решении и текущем уровне угрозы записываются в базу данных.

В настоящее время архитектура «нервной системы сети» реализуется в виде имитационных моделей с помощью среды моделирования OMNeT++.

Работа выполнена при финансовой поддержке РФФИ (проект №10-01-00826), программы фундаментальных исследований ОНИТ РАН (проект №3.2), государственного контракта 11.519.11.4008 и проектов Евросоюза SecFutur и Massif, а также в рамках других проектов.

Щелованов Н.В., Никулина Н.О.
Россия, Санкт-Петербург, ЗАО «Телрос»

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ЗАЩИТЫ СЕТИ ОКС-7

В настоящее время остро стоит вопрос проектирования и разработки специальных методов и средств защиты телекоммуникационных сетей. Неспособность защитить телекоммуникационное оборудование от вторжения может привести к самым разнообразным негативным последствиям, таким как несанкционированный доступ к конфиденциальной информации, убытки из-за оплаты чужих международных переговоров, ущерб деловой репутации компании, финансовые потери в связи с дефектами в работе системы связи и другим.

Система ОКС–7 является ключевым элементом цифровых сетей связи и представляет собой стандартизированную в международном масштабе систему сигнализации по общему каналу универсального назначения. Необходимость обеспечения безопасности сети ОКС–7 обусловлена динамикой развития сетей связи и их интеграцией с глобальными сетями, а также недостаточностью в сетях электросвязи необходимых механизмов обеспечения безопасности.

В результате несанкционированных воздействий на сеть сигнализации, может быть нарушена функциональность сети связи, вплоть до недоступности ряда направлений и ограничено предоставление услуг связи значительным группам абонентов. Существующие системы мониторинга сетей связи не обеспечивают полноценной защиты и основываются, в общем, на методе пассивного анализа. Для обеспечения полноценной защиты сетей связи необходимо создание распределенной системы мониторинга с возможностями активного воздействия на сеть сигнализации при возникновении критических ситуаций.

Детальное исследование подсистем ОКС-7 (MTP, ISUP, SCCP, TCAP, MAP, INAP,OMAP) с целью выявления уязвимостей и последствий несанкционированного воздействия позволило разработать модель нарушителя и модель угроз, сформировать типовые профили атак для сети ОКС-7.

На основании проведенного исследования была предложена концепция защиты сети ОКС-7 и разработан прототип автоматизированной системы защиты, основным элементом которой является Сенсор ОКС-7. Сенсоры ОКС–7 подключаются к сети сигнализации в разрыв тракта ИКМ 2,048 Мбит/с и осуществляют прозрачную передачу сообщений MTP-3. Сенсоры обеспечивают сбор сигнальных сообщений, циркулирующих в сети, а также анализ сообщений подсистемы ISUP, для реализации механизмов черных / белых списков и подстановки групповых номеров. Собранная Сенсорами информация передаётся в централизованную базу данных для проведения дальнейшего статистического анализа. На основе анализа собранных сообщений производится мониторинг элементов сигнальной сети, а также расчет сигнальной и голосовой нагрузки, показателей качества, формируются записи CDR. Управление Сенсором в части постановки правил экранирования осуществляется удаленно. Структура базы данных проектировалась на основе разбора структур сигнальных единиц ОКС–7.

Информация из базы данных используется для отображения в реальном времени состояния элементов сети сигнализации, нагрузки сигнальных звеньев и маршрутов, загрузки голосовых каналов, а также значений показателей качества связи. Формируются детализированные записи о предоставленных услугах, производится анализ причин завершения вызова между абонентами, формируются профили абонентов на основе временной и номерной информации.

В прототипе системы защиты реализована возможность детального декодирования в реальном времени сигнальных сообщений подсистем ОКС-7 (MTP, ISUP, SCCP, TCAP, MAP, INAP,OMAP) и мультипротокольной трассировки вызовов.

Пользовательский интерфейс прототипа системы состоит из отдельных подсистем, выполняющих дискретные функции. Обеспечивается возможность фильтрации собираемой информации по временным характеристикам, по типам подсистем ОКС–7 и по отдельным параметрам сигнальных сообщений. Для тестирования прототипа системы защиты использовался симулятор ОКС-7, были созданы сценарии, моделирующие основные атаки на сеть сигнализации ОКС-7.

Реализация системы защиты в сети ОКС-7 позволит:

- противодействовать единичным и массированным атакам;
- локализовать аварийные события;
- гарантировать предоставление основных услуг связи в условиях перегрузок;
- ограничивать услуги абонентам при выявлении попыток мошенничества.

Юрков В.А., Семенов С.С., Дыбко Л.К., Гусев А.П.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

ОБОСНОВАНИЕ ВЫБОРОВ ЗАКОНОВ РАСПРЕДЕЛЕНИЯ СЛУЧАЙНЫХ ВЕЛИЧИН ПРИ ИМИТАЦИОННОМ МОДЕЛИРОВАНИИ СИСТЕМ СВЯЗИ

При имитационном моделировании систем связи различного назначения неизбежно встает вопрос о выборе законов распределения случайных величин. Для моделирования стохастических процессов предлагается использовать аппарат теории вероятностей и математической статистики, центральными категориями которого являются: случайная величина, вероятность, закон распределения случайной величины.

Случайной величиной называют числовую функцию от события, могущего носить как количественный, так и качественный характер. Вероятность – это числовая функция, определенная на множестве событий. Закон распределения случайной величины ставит в соответствие каждому ее возможному значению определенную вероятность наступления.

Из этого следует, что каждый неточно определенный показатель исследуемой системы связи должен быть представим в виде случайной величины, иначе числовое моделирование невозможно, и для каждого значения случайной величины должна быть определена вероятность, что позволит рассчитать числовые значение показателей.

Вероятности можно задать с помощью закона распределения или определить «вручную» для каждого диапазона значений случайной величины. Субъективизм, допущенный при принятии данных условий, является неизбежным свойством любой модели, открывающий представления исследователя о поведении системы связи в контексте неопределенности.

Аналитический способ задания вероятности на множестве элементарных событий является наиболее предпочтительным. Его достоинством является абсолютная формализация и упорядоченность вероятностей определенных значений случайной величины в зависимости от рассеяния ее возможных значений от ожидаемого значения и удаления определенного значения случайной величины от ожидаемого значения. При задании вероятности аналитическим способом, на выбор закона распределения в наиболее значимой степени влияют физическая природа анализируемого показателя, а также набор факторов, влияющих на значения, принимаемые показателем. Доминирование какого-либо фактора выражается через смещение ожидаемого значения исследуемого показателя в сторону одной из границ его доверительного интервала, а также через значение асимметрии и эксцесса эмпирического распределения.

С помощью известных статистических выводов и практических навыков, полученных при решении конкретных задач в области моделирования систем связи, из множества существующих законов распределения случайной величины, были определены некоторые их варианты.

Отметим, что определение показателей закона распределения, происходит исходя из данных, полученных в ходе прогнозирования значений анализируемого показателя в будущих периодах и построения доверительного интервала прогноза. Для случаев, в которых информация о влиянии факторов на вариацию исследуемого показателя отсутствует полностью, следует использовать равномерное распределение.

Для решения конкретной задачи могут быть использованы особые, проблемно ориентированные формы представления неопределенности. Мощным подспорьем являются эмпирические данные о «поведении» исследуемого показателя, для обработки которых может быть применим аппарат кривых Пирсона, получивший солидное теоретическое обоснование в трудах отечественных и зарубежных специалистов в области теории вероятностей. Общая идея метода кривых Пирсона заключается в построении кривой распределения, форма и область определения которой зависят от имеющихся данных о распределении случайной величины (выборки). То есть можно подогнать закон распределения, наиболее адекватно описывающий случайный характер исследуемого показателя, наблюдаемый в ходе статистических исследований, опытов, экспериментов. При подгонке закона распределения под конкретные данные принимается, что полученная выборка является репрезентативной, т.е. адекватно представляет характер вариаций исследуемой случайной величины.

Таким образом, аппарат кривых Пирсона может быть эффективно использован при задании законов распределения исследуемых показателей, независящих от природы их происхождения.

В большинстве практических случаев непрерывные законы распределения могут быть легко дискретизированы. Преимущество применения типовых законов распределения состоит в их хорошей изученности и возможности получения состоятельных, несмещенных и относительно высокоэффективных оценок параметров.

Таким образом, при допущениях весьма общего характера, используя законы распределения случайной величины, можно моделировать неопределенность исследуемых параметров систем связи различного назначения во всех практически значимых случаях.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Азаров А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК РЕКОМПЕНСАЦИОННОГО ТИПА В ОТНОШЕНИИ ПОЛЬЗОВАТЕЛЕЙ

Новости о нарушении информационной безопасности систем все чаще возникают как в отечественных, так и в зарубежных новостных лентах. Это происходит от того что именно информационные системы содержат в себе конфиденциальную информацию различных организаций, которые могут быть интересны людям, для которых подобная информация не предназначена. Таким образом, как никогда остро встает вопрос об обеспечении защиты конфиденциальных данных. И, если современные технические средства почти полностью устраняют угрозу проникновения злоумышленника в систему, то пользователи этой системы порой сами дают прекрасную возможность злоумышленнику воспользоваться их невнимательностью, доверчивостью и незнанием основ информационной безопасности и проникнуть в систему. Именно такое воздействие на пользователей и называется социоинженерной атакой. Таким образом, чтобы в полной мере оценивать защищенность информационной системы необходимо научиться прогнозировать социоинженерные атаки на информационные системы. Для этого на базе лаборатории ТиМПИ СПИИРАН был разработан программный продукт, позволяющий оценивать защищенность информационных систем от социоинженерных атак рекомпенсационного типа. Такого типа атаки подразумевают, что на пользователя оказывается финансовое воздействие с целью или получения авторизационных данных в системе, или получения определенных данных, которые пользователь может скопировать на электронный носитель.

Программный комплекс состоит из двух частей: модуль создающий информационные системы и моудль имитирующий социоинженерные атаки. Автоматизированная информационная система представляет собой достаточно сложную модель содержащую в себе большое количество атрибутов, таких как программно-аппаратные средства (компьютеры, серверы, хабы, роутеры и так далее), группы пользователей (как в смысле прав доступа, так и в смысле групп людей, разбитых по должностным обязанностям), контрольные зоны и другие.

Программный продукт дает возможность построить информационную систему и проверить ее защищенность на стадии ее проектирования от социоинженерных атак, построенных на уязвимостях по рекомпенсационному типу персонала этой системы. Также поддерживается возможность отображения результата подобной атаки, как в текстовом, так и в графическом виде.

Программный продукт позволяет создавать сколь угодно расширенную автоматизированную информационную систему и сохранять ее в базу данных в удобном для пользователя виде. Впоследствии работу с сохраненной информационной системой можно продолжить, загрузив ее в программу. Кроме того, в программный продукт включен программный модуль для анализа защищенности информационной системы от социоинженерных атак. Анализ защищенности системы осуществляется с помощью переработанного и расширенного метода деревьев атак. Данный метод генерирует все возможные атакующие воздействия до положительного результата, то есть до того как злоумышленник получит необходимую ему информацию.

Таким образом, полученные программный продукт является основой для дальнейших внедрений новый методов воздействия социальной инженерией на пользователей. Кроме того, успешное применение алгоритма деревьев атак позволяет предположить, что данный алгоритм будет успешен также и в реализации последующих социоинженерных атак на пользователей информационных систем.

Азаров А.А., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

РАЗВИТИЕ МЕТОДОВ И МОДЕЛЕЙ АНАЛИЗА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК НА ОСНОВЕ ПРИМЕНЕНИЯ РЕЛЯЦИОННО-АЛГЕБРАИЧЕСКИХ ПРЕДСТАВЛЕНИЙ И АЛГОРИМОВ

Проблема хищения конфиденциальной информации заставляет создавать все более изощренные системы защиты, которые почти полностью нивелируют возможность технического

проникновения в систему. При этом информационная система, хранящая конфиденциальную информацию, остается беззащитной перед социоинженерными и инсайдерскими (внутренними, совершаемыми пользователями) атаками. Поэтому необходимо научиться анализировать защищенность информационных систем от социоинженерных атак. Существующие программные комплексы осуществляют оценку защищенности только технической составляющей информационной системы, оставляя без внимания ее пользователей.

На базе лаборатории ТиМПИ СПИИРАН разработан прототип программного продукта, позволяющего оценить защищенность информационных систем от социоинженерных атак рекомпенсационного типа.

Дальнейшее развитие предложенного подхода, кроме внесения в существующий программный комплекс возможностей обработки новых типов социоинженерных атак на пользователей информационных систем, состоит в том, чтобы представить формальные данные и знания об информационной системе с помощью реляционно-алгебраического, а впоследствии – вероятностного реляционно-алгебраического подхода. Это даст возможность строго структурировать все данные об информационной системе, пользователях этой системы, а также связях между ними. Кроме того данный подход представления данных и знаний дает возможность использовать реляционно-алгебраические алгоритмы, которые значительно ускорят анализ защищенности системы в сравнении с обычными переборными алгоритмами.

Предполагается разбить всю модель информационной системы на четыре логических части (компонента): злоумышленник, пользователи, программно-техническая составляющая системы и критичная информация (набор документов, содержащийся в информационной системе). Взаимодействие между критичной информацией и остальными моделями возможно только через модель программно-технической составляющей системы, в то время как взаимодействие между злоумышленником и программно-технической составляющей возможно как через пользователей (социоинженерные атаки), так и без их участия (технический взлом систем).

Кроме того возможны связи и внутри всех предложенных моделей (кроме модели критичной информации). То есть злоумышленник может обращаться к другим злоумышленникам, которые, например, имеют более высокую квалификацию, чем он, пользователи также могут общаться между собой при условии предоставления злоумышленником большого объема благ, способного удовлетворить сразу несколько пользователей, а также при наличии положительных (дружественных, эмоциональных и так далее) связях между пользователями.

Данный подход планируется совместить с имеющимся подходом к анализу деревьев атак, существенно переработав последний. Предполагается, что это даст существенное уменьшение времени работы алгоритмов анализа при работе с большими объемами данных. Кроме того, новый подход позволит формализовать более широкий класс данных и знаний об информационных системах и их персонале, что сделает анализ защищенности более точным.

Александров А.М.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

РАЗЛОЖЕНИЕ ИНТЕГРАЛЬНЫХ ТРЕБОВАНИЙ ПО ВЕРОЯТНОСТЯМ ЛОЖНЫХ СИГНАЛОВ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Рассматривается некоторая критическая инфраструктура (КИ), состояние пространственно распределенных объектов которой контролируется по совокупности параметров. Результаты контроля объектов образуют случайный поток, который поступает в центр для обработки по соответствующим логическим правилам и анализа состояния КИ. Поступающие в центр сигналы от средств контроля объектов могут нести информацию как об истинном состоянии объекта (истинная информация), так и ложную информацию о его состоянии (ложная информация).

Исходя из требования допустимого уровня вероятности ложной оценки общего состояния КИ, решается задача определения требований к индивидуальным вероятностям ложных сигналов от соответствующих объектов КИ.

Рассматривается несколько логических правил обработки центром КИ поступающих сигналов. По одному из них, например, для получения истинного заключения о состоянии КИ необходима истинная информация от каждого объекта. Если хотя бы от одного объекта поступит ложная информация, центр КИ выдаст ложное заключение о состоянии КИ.

Решается задача определения требований по допустимым уровням индивидуальных вероятностей ложных сигналов, поступающих от контрольных средств объектов, исходя из допустимого уровня интегральной вероятности ложного решения задачи о состоянии КИ.

Исследуется влияние соотношения истинной и ложной информации, поступающей от объектов КИ, количество контрольных средств и др. В частности показано, что увеличение этих средств не всегда приводит к уменьшению интегральной вероятности ложного решения системой.

Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ДВЕНАДЦАТЬ ПРОБЛЕМ ВНЕДРЕНИЯ НОВЫХ ТЕХНОЛОГИЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проектирование сложных объектов, включая объекты морской инфраструктуры, основано, как известно, на применении идей, принципов, методов и технологий их реализации, изложенных в ряде теорий и подходов, которым в практической деятельности, к сожалению, с ростом сложности проектируемых комплексов и систем уделяется всё меньшее значение.

Как следствие названных издержек, в практике современного проектирования сложных организационно-технических эрготехнических систем (ЭТС) имеют место существенные погрешности и системные ошибки. Их масштаб и роль по критериям критичности систем возрастают, подчас, непредсказуемо. В этом ряду – техногенные, социальные, экологические и многие другие катастрофы и кризисы, число которых в последнее время не только не снижается, но и непрерывно возрастает. Возникающие при этом риски заказчика могут превосходить его ресурсные возможности, что порождает принципиально новую проблему обоснования методов и технологии управления рисками системного развития, в том числе проблему внедрения технологий информационной безопасности.

В этих условиях системный подход, как научный метод, инвариантен к структуре, функциональному составу, свойствам и характеристикам объектов анализа и синтеза, представляет собой фундаментальный способ обоснования организации процедур. Способ, который принципиально можно использовать для любого рода деятельности и любых систем с целью выявления закономерностей и взаимосвязей в интересах обоснования их эффективного использования.

С другой стороны, бурное развитие информационных технологий, как никогда ранее, побуждает лиц, обосновывающих (ЛОР) и принимающих (ЛПР) высоко ответственные проектные и управленческие решения (ПУР), выполнять качественный и количественный сравнительный квалиметрический анализ (измерение и анализ качества, рейтинг-анализ) вариантов этих системных решений. Среди них ПУР по обеспечению информационной безопасности (ИБ) – наиболее сложные.

Сегодня процесс квалиметрического сравнения при обосновании развития и создании сложных систем ИБ, информационно-коммуникационных систем (ИКС), можно утверждать, по существу не обеспечен методически. При этом используются, как правило, отдельные «лоскутные» и эмпирические подходы с крайне редким использованием «сугубо» системных критериев, как количественных мер свойств объектов, отражающих их соответствие целевому предназначению. Показатели качества, как средства количественного выражения критериев качества и эффективности, а тем более критериев оптимизации используются крайне редко и, особенно, при анализе и синтезе сложных ПУР.

Системные аспекты технологического обеспечения развития систем ИБ, ИКС, разработки и внедрения новых структурных, функциональных, технических и технологических решений особенно ярко проявляются при рассмотрении всего жизненного цикла изделий (ЖЦИ). Выбор предпочтительных информационных технологий ИБ в обеспечение ЖЦИ в настоящее время представляет собой практически для большинства предприятий наисложнейшую и крайне ресурсоёмкую задачу. Но не менее сложную проблему при этом приобретают вопросы эффективного внедрения, освоения и результативного использования новых информационных технологий (ИТ), технологий ИБ, включая технологии PLM, на предприятиях, в том числе морской инфраструктуры.

На примере обоснования выбора ПУР при создании систем электронного документооборота в защищённом исполнении (СЭД-ЗИ) представляются результаты систематизации данных специально проведённых исследований и приведены 12 основных факторов и проблем внедрения новых ПУР.

Выполнена количественная оценка возможности внедрения технологий класса СЭД-ЗИ по трём программам внедрения (силами службы информационных технологий предприятия, силами компании по аутсорсингу и на основе комбинирования этих способов).

Показано, что учёт названных факторов при внедрении новых высокотехнологичных ПУР с соответствующими упреждающими управленческими мероприятиями позволяют повысить успешность внедрения проекта более, чем на (20…35)% и минимизировать, прежде всего, возможность системных ошибок, системных рисков заказчиков и разработчиков соответствующих сложных комплексов и систем. При этом, существенно сокращаются риски, обусловленные так называемым человеческим фактором, а внедрение новых технологий обеспечения ИБ систем типа СЭД в составе единой ЭТС приобретает качественно новый управляемый характер.

Приведенные многовариантные оценки, с другой стороны, количественно подтвердили то важное обстоятельство, что системные аспекты внедрения ПУР при развитии современных сложных ЭТС являются наиважнейшими и требующими непременного системно обоснованного учёта. При развитии сложных организационно-технических комплексов и их систем, среди которых представленный пример СЭД-ЗИ в сравнении с системами тира ERP, PLM, ECM, CAD, CAE, CAM, ITIL в защищённом исполнении может рассматриваться, как менее сложная, что только подчёркивает особую актуальность поднимаемой проблемы.

Антонов А.А., Ридигер В.К., Федотов А.А., Филиппов А.С.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»,
Санкт-Петербургский государственный политехнический университет

ИСПОЛЬЗОВАНИЕ ВЫСОКОУРОВНЕВЫХ СРЕДСТВ ПРОЕКТИРОВАНИЯ ДЛЯ РАЗРАБОТКИ СНК НА БАЗЕ БМК 5516БЦ1Т1-002 В КРИТИЧЕСКИХ СИСТЕМАХ

На данный момент в нашей стране активно развивается навигационная система ГЛОНАСС. В ближайшее время планируется запуск очередных спутников, которые необходимо снабдить высоконадежными отечественными вычислительными системами. В связи с этим ОАО «РИРВ» совместно с каф. КСПТ ФТК СПбГПУ ведет разработку специализированной СнК на базе радиационно-тойкого БМК 5516БЦ1Т1-002.

Назначение СнК: ИС для бортового синхронизирующего устройства спутников ГЛОНАСС. Функции разрабатываемой ИС:

- синтез частоты для квантового стандарта частоты на рубидиевой газовой ячейке;
- формирование частоты подмешивания;
- формирование сетки частот и шкалы времени;
- передача данных внешней телеметрии.

Цель работы – разработка тестопригодного устройства с переносимой архитектурой, минимизируя на всех этапах разработки риски внесения ошибок. Также была поставлена цель: использовать современные средства проектирования и верификации в рамках данной разработки для повышения скорости и качества разработки.

В докладе рассматривается маршрут проектирования данной СнК. Маршрут логически разбит на два этапа: первый – разработка опытных образцов на базе БМК 1592ХМ1Т, второй – перенесение разработанного устройства на 5516БЦ1Т1. Кроме того разработке на БМК 1592ХМ1Т предшествует прототипирование на ПЛИС, позволяющее отсеять большинство ошибок Рассмотрен ряд проблем, возникших в ходе разработки и пути их решения. В докладе представлен положительный опыт применения высокоуровневых языков проектирования и верификации (класса SystemC) в маршруте проектирования цифровых устройств на базе отечественных БМК. Детально освещены вопросы, связанные с тестированием разрабатываемого устройства. Рассматриваются вопросы встраиваемого тестирования, а также концепции Design For Testability применительно к данной разработке. Разработка находится в стадии выполнения второго этапа. Основным научно-практическим результатом данной работы является разработанный маршрут проектирования, зарекомендовавший себя как эффективный. Он основывается на использовании современных средств синтеза и верификации, и применим для разработки отечественных БМК.

Баракин В.Н., Панькин А.В., Потрясаев С.А., Соколов Б.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕТОДИКА ПАРАМЕТРИЧЕСКОЙ И СТРУКТУРНОЙ АДАПТАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В АСУ ПОДВИЖНЫМИ ОБЪЕКТАМИ

В настоящее время конкретные технологии адаптивной защиты автоматизированных систем управления подвижными объектами (АСУ ПО) опираются, прежде всего, на многовариантность формального описания как объектов управления, так и управляющих подсистем, входящих в соответствующую комплексную систему защиты информации (КСЗИ), что открывает широкие перспективы по постановке и решению задач адаптивного выбора (синтеза) комплекса моделей и алгоритмов программного управления и регулирования соответствующими объектами (элементами и подсистемами КСЗИ в АСУ ПО) в условиях постоянно изменяющейся обстановки.

Анализ ранее выполненных работ по данной проблематике показывает, что в этом случае состав традиционно решаемых задач управления КСЗИ должен быть дополнен задачами структурной и параметрической адаптации специального программно–математического обеспечения управления (СПМО) её элементами и подсистемами. При этом, реализация концепции адаптивного управления КСЗИ должна включать в себя следующие основные этапы: адаптация параметров и структур моделей, алгоритмов управления структурной динамикой (УСД) КСЗИ к прошлому и текущему состоянию объектов управления (ОУ, в нашем случае АСУ ПО), управляющих подсистем (УП) и внешней среды; комплексное планирование применения КСЗИ (разработка программ управления её структурной динамикой); имитация (упреждающее моделирование) условий реализации планов применения КСЗИ с учётом различных вариантов организации оперативного управления её элементами и подсистемами в конкретных ситуациях; структурная и параметрическая адаптация плана и регулирующих воздействий, моделей, алгоритмов, программ специального программно-математического обеспечения (СПМО) управления структурной динамикой (УСД) КСЗИ к возможным (прогнозируемым, в том числе, и на имитационных моделях) состояниям ОУ, УП и среды.

Для конструктивной реализации рассматриваемой концепции адаптивного управления необходимо, прежде всего, в составе разработанных моделей и алгоритмов УСД КСЗИ выделить

две группы параметров: параметры, настраиваемые на основе экспериментов с имитационными моделями, в которых проигрываются возможные сценарии развития будущих событий. Организационно процедуры адаптации перечисленных параметров в этом случае целесообразно осуществлять в рамках двух блоков (моделей): блок (модель) внешнего адаптера ИС; блок (модель) внутреннего адаптера ИС. Для повышения степени адекватности процессов моделирования наряду с параметрической адаптацией СПМО УСД КСЗИ (в том случае, когда все её возможности будут исчерпаны) предлагается проводить и структурную адаптацию соответствующих моделей. Принято выделять два основных подхода к решению проблемы структурной адаптации. В рамках первого подхода из фиксированного множества моделей осуществляется выбор той модели, которая с наибольшей степенью адекватности описывает заданные ОУ и УП. При реализации второго подхода осуществляется конструирование моделей УСД КСЗИ с требуемыми свойствами на основе некоторого множества элементарных составляющих моделей (модулей). Данная работа выполнялась при финансовой поддержке РФФИ (гранты 09-07-00066, 10-07-00311,11-08-01016, 10-08-90027-Бел_а), ОНИТ (проект 2.3).

Великовская С.А.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

ГОРОДСКОЙ ИНТЕРНЕТ ДНЕВНИК

Вовлечение ребенка, педагогов и родителей в образовательный процесс через новые информационные технологии направлено на повышение качества образования, обеспечение соответствия его содержания актуальным потребностям развития российского общества.

В муниципальной системе образования городов России Электронный Журнал и Электронный Дневник чаще всего реализованы в форме программного комплекса АСИОУ+ГИД (автоматизированная система информационного обеспечения управления + городской интернет-дневник).

Возможности программного комплекса АСИОУ+ГИД:

– для родителей: просмотр расписания, тем уроков, домашних заданий, объявлений, новостей любой другой информации, выложенной для всеобщего ознакомления; просмотр отметок своих детей с указанием типа произведенного контроля знаний и комментариями учителя; общение с учителем, администрацией, другими родителями, обучающимися;

– для обучающихся: просмотр расписания, тем уроков, домашних заданий, объявлений, новостей и любой другой информации, выложенной для всеобщего ознакомления; просмотр своих отметок с указанием типа произведенного контроля знаний и комментариями учителя; размещение в «Личном кабинете» своих материалов; общение с учителем, директором, другими обучающимися;

– для учителей: ввод отметок с указанием типа произведенного контроля знаний и по желанию, снабжение их комментариями; размещение домашних заданий и тем уроков, просмотр расписания, тем уроков, домашних заданий, объявлений, новостей и любой другой информации, выложенной для всеобщего ознакомления размещение в «Личном кабинете» своих материалов; общение с учениками, их родителями, администрацией школы, другими учителями; тестирование обучающихся по различным тестам с автоматической обработкой закрытых вопросов;

– для администрации: просмотр всей информации по школе, за исключением личной переписки статистика активности пользователей Интернет-дневника по школе; просмотр динамики успеваемости обучающихся по классам/ по школе; получение результатов обработки успеваемости в табличных и графических формах; возможность массовой рассылки сообщений по всем участникам зарегистрированных по школе в Интернет-дневнике; общение с учениками, их родителями, учителями; проведение опросов обучающихся, родителей, педагогов по различным основаниям с автоматической обработкой закрытых вопросов.

Этот комплекс использует персональные данные, поэтому требуется защита персональных данных. Выделение категории персональные данные из более общей категории частная жизнь связано, прежде всего, с распространением автоматизированных систем обработки и хранения информации, в первую очередь компьютерных баз данных, к которым возможен несанкционированный доступ.

Именно эти системы, по сути, сделавшие революцию в вопросах структурирования, хранения и поиска необходимых данных, создали предпосылки для возникновения проблемы защиты сведений персонального характера – персональных данных с целью защиты прав и свобод граждан.

Технические меры защиты информации предполагают использование программно-аппаратных средств защиты информации.

При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов предприятия.

Технические средства защиты информации делятся на два основных класса:

– средства защиты информации от несанкционированного доступа (НСД): системы разграничения доступа к информации; антивирусная защита; межсетевые экраны; средства блокировки устройств ввода-вывода информации, криптографические средства и т.п.

– средства защиты информации от утечки по техническим каналам: использование экранированных кабелей; установка высокочастотных фильтров на линии связи; установка активных систем зашумления и т.д.

Организационные меры по защите персональных данных включают в себя разработку организационно–распорядительных документов, которые регламентируют весь процесс получения, обработки, хранения, передачи и защиты персональных данных.

Перечень мероприятий по защите персональных данных:

– определение круга лиц, допущенных к обработке персональных данных;
– организация доступа в помещения, где осуществляется обработка ПДн;
– разработка должностных инструкций по работе с персональными данными;
– установление персональной ответственности за нарушения правило бработки ПДн;
– определение продолжительности хранения ПДн и т.д.

Реализация организационных мер защиты информации осуществляется с учетом категорий персональных данных – чем выше категория, тем выше требования их защиты.

Виноградов А.А.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

ДОВЕРИТЕЛЬНАЯ ОТЕЧЕСТВЕННАЯ ПРОГРАММНО-АППАРАТНАЯ ПЛАТФОРМА

Необходима целостная государственная технологическая политика по созданию доверительной отечественной программно-аппаратной платформы и технологий её создания, охватывающая весь комплекс работ, которые необходимо возобновить или поставить заново на территории страны.

Доверительные технологии, должны исключать появление в платформе недекларированных возможностей, должны давать платформе свойство киберустойчивости и сведение к минимуму ошибок разработчика системы, аппаратуры, программного обеспечения, также нарушающих функционирование систем.

Совершенно не достаточно ограничиваться только вопросом создания отечественной ЭКБ, хотя это одна из ключевых задач.

Государственная технологическая политика должна включать в себя следующие направления работ:

– Технологии оптимизации и верификации на моделях требований к системам и к ЭКБ в зависимости от условий их применения.

– Интегрированные доверительные технологии проектирования систем специального назначения, их программных, аппаратных средств и ЭКБ.

– Независимые технологии изготовления специализированной ЭКБ, материалов и конструкций.

– Технологии автономной и комплексной отладки систем специального назначения.

– Технологии испытаний специализированных систем с учётом проверки алгоритмов негативного управления, предельных и разрушающих испытаний.

Проблемные вопросы:

– Нет комплексного подхода и целевого финансирования по проблеме создания доверительной отечественной программно-аппаратной платформы.

– Нет перечня доверительных САПР, единой политики по обеспечению предприятий САПР-ами в требуемой полной комплектации и моделей отечественных ЭРИ для современных САПР.

– Нет единой политики по отечественным ЭРИ, отстаёт отечественное технологическое сопровождение современных ЭРИ: нет отечественных пластин с кристаллами, корпусов микросхем, стеклотекстолита, автоматизированный монтаж невозможен и т.д.

– Находящиеся в эксплуатации ответственные системы не обеспечены страховым запасом ЭРИ на будущее, или хотя бы на период создания нового поколения платформ.

Волкова А.В.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

СИНТЕЗ ОПТИМАЛЬНОГО МАНИПУЛЯЦИОННОГО КОДА ДЛЯ СИГНАЛЬНО-КОДОВОЙ КОНСТРУКЦИИ НА ОСНОВЕ ТРЁХМЕРНОЙ СИМПЛЕКС-РЕШЁТКИ

Производится синтез оптимального манипуляционного кода для сигнально-кодовой конструкции (СКК) на основе трёхмерной симплекс-решётки. При разработке метода манипуляционного кодирования предполагалось, что СКК использует помехоустойчивый код Хэмминга (7, 4), и сигнал будет распространяться в канале с белым гауссовым шумом (БГШ).

Построение СКК на основе трёхмерной симплекс-решётки основывается на разделение потока бит на первичные группы по n бит. Такой группе ставится в соответствие скаляр. К ним же можно

независимо применить помехоустойчивое кодирование (например, код Хэмминга (7, 4)). Три первичные группы образуют вторичную группу, которой можно поставить в соответствие вектор из трёхмерного пространства, координаты которого будут данным скалярами. Каждый вектор проекции на плоскости, перпендикулярной главным диагоналям куба, представляет собой одну посылку физического сигнала, параметры которого могут быть описаны в комплексной форме. Две, три или четыре такие посылки, переданные в канал, однозначно определяют передаваемую информацию.

Задача сводится к нахождению способа сопоставления скаляра первичной группе таким образом, чтобы снизить вероятность ошибки на бит для заданной энергии и полосы при использовании описанной выше СКК в канале с БГШ, т. е. разработать оптимальный манипуляционный код с точки зрения помехоустойчивости рассматриваемой СКК.

Поскольку сопоставление скаляра первичным группам эквивалентно амплитудной модуляции, то можно сформулировать подзадачу, которая заключается в нахождении оптимального манипуляционного кода для амплитудной модуляции при использовании кода Хэмминга (7, 4).

Формулировка требований к методу манипуляционного кодирования: в случае, если искажение физического сигнала приводит к неисправляемой ошибке, то неверно декодированное информационное слово должно иметь наименьшее расстояние Хэмминга от переданного информационного слова.

Согласно данной формулировке был разработан алгоритм построения манипуляционного кода, при котором наиболее вероятные искажения физического сигнала приводят к однократным ошибкам (искажения находятся в области исправления ошибок). Если же имеет место область неисправляемых ошибок, то неверно декодированное информационное слово, отличается от переданного информационного слова с большей вероятностью на один бит. Эта особенность предложенного манипуляционного кодирования даёт возможность предположить, что помехоустойчивость такого сигнала улучшиться.

Для проверки данного предположения была построена модель в пакете MatLab. Моделирование подтвердило преимущество разработанного манипуляционного кода по сравнению с кодом Грея, как при амплитудной модуляции, так и при использовании СКК на основе трёхмерной симплекс-решётки.

Гейда А.С., Лысенко И. В., Седлов Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕТОД ПЛАНИРОВАНИЯ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ РИСКА

Практика свидетельствует, что при планировании инновационной деятельности, в частности – инновационной деятельности в критических инфраструктурах, часто возникает необходимость учета возможностей того, что инновационная деятельность, реализуемая в критической инфраструктуре, приведет к неблагоприятным последствиям и в последующей минимизации ущерба за счет изменения плана инновационной деятельности. Так, инновационная деятельность может приводить не только к благоприятным и желаемым результатам, таким, как новые возможности информационной системы, увеличение объемов заказов, но и к задержкам с началом использования, перерасходу выделенных средств, потере части заказчиков в результате неблагоприятных событий при реализации инновационной деятельности. Для учета этой особенности предлагается реализовывать планирование инновационной деятельности с учетом возможностей наступления неблагоприятных событий, то есть – в условиях риска.

Возможности неблагоприятных событий возникают при внедрении новаций в критические инфраструктуры, то есть – при их модернизации. Под критической инфраструктурой (КИ) понимается подсистема, без успешного функционирования которой невозможно достижение целей заданной системы при своем функционировании.

Рассматривается такая инновационная деятельность, которая приводит к модернизации КИ. Инновация определена, как новация, внедренная в практику. Введено определение инновационной деятельности (ИД), как деятельности по созданию и реализации новации. Обоснованы показатели качества ИД в условиях риска. Предложено оценивать план ИД в условиях риска с использованием пары показателей: показателя инновационного потенциала модернизируемой КИ; показателя риска при модернизации КИ.

Инновационный потенциал определен как потенциал системы, получаемый в результате ИД при модернизации КИ. В свою очередь, потенциал системы определен, как свойство системы, позволяющее использовать её для достижения любой из возможных целей.

С использованием введенных понятий предложена вербальная и математическая постановки задачи планирования ИД в условиях риска, как многокритериальной оптимизационной задачи распределения ограниченных ресурсов. Для решения поставленной оптимизационной задачи разработан комплекс моделей, позволяющий получить рекуррентные соотношения для расчета значений показателей инновационного потенциала и показателей риска при модернизации КИ, а затем – пересчитывать эти значения при изменении плана ИД.

Предложен метод фрагментарно контролируемого случайного поиска, использующий особенности разработанных моделей и решаемой задачи. Метод позволяет сократить объем вычислений в несколько раз, в зависимости от особенностей исходных данных. Описаны алгоритмы пересчета характеристик эффектов ИД, используемые для решения задачи планирования. Приводится пример.

Гук И.И., Путилин А.Н., Сиротинин И.В., Хвостунов Ю.С.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

РЕЗУЛЬТАТЫ ПРОВЕДЕНИЯ ТРАССОВЫХ ИСПЫТАНИЙ КОМПЛЕКСА ТЕХНИЧЕСКИХ СРЕДСТВ «ИМПУЛЬС-АПР»

Безопасная передача информации по радиоканалам в настоящее время не представляется без использования специальных методов формирования и приёма сигналов, организации защищённых алгоритмов работы радиолиний и радиосетей. Для решения этих задач в мировой практике широко используются системы, как с прямым так и с последовательным расширением спектра. В 2003–2006 годах во ФГУП «НПО «Импульс» была спроектирована одна из таких систем – комплекс декаметровой радиосвязи с псевдослучайным переключением и адаптацией во всём диапазоне рабочих частот. Его реализация имела в своем составе элементы как отечественной, так и импортной разработки. Комплекс был успешно испытан как на имитаторах НЧ-каналов (стандарт ITU-R F.1487), так и на трассах в России и Китае. В 2010 году на ФГУП «НПО «Импульс» была поставлена инициативная задача создания полностью отечественного комплекса технических средств декаметровой радиосвязи с аналогичными характеристиками – КТС «Импульс-АПР».

КТС «Импульс-АПР» предназначен для создания симплексных, полудуплексных и дуплексных каналов радиосвязи декаметрового диапазона на дальности до 3000 км в движении и с остановки. Его функционирование основывается на следующих принципах:

– работа осуществляется в режиме единого времени;
– для организации работы сети назначается набор из N рабочих частот (частотный план);
– одновременно используются только n рабочих частот (n < N);
– передача ведется пакетами равной длительности на каждой из выделенной рабочей частоте;
– текущие номера частот переключаются радиостанциями синхронно по псевдослучайному закону;
– в случае отсутствия приема на какой-либо частоте – передающая радиостанция исключает эту частоту из списка рабочих частот и заменяет следующей из общего набора (таким образом реализуется адаптация).

Для создания КТС «Импульс-АПР» была сформирована кооперация в составе ОАО «ОмПО «Иртыш», ОАО «Завод «Вибратор» и ФГУП «НПО «Импульс». Решение поставленной задачи потребовало:

1. Создания принципиально нового возбудителя ОАО «Завод «Вибратор».
2. Модификации существующего приёмника декаметровой радиосвязи «Радикс-2П».
3. Существенной модификации усилителя мощности декаметрового диапазона из состава РПДУ Р-646.
4. Модификации аппаратуры передачи данных АПД-003, реализующей функции модема и контроллера адаптивной линии и сети декаметровой радиосвязи.

В августе–сентябре 2011 года были проведены испытания КТС «Импульс-АПР» на трассе протяжённостью 2640 км: город Омск, антенный полигон ОАО «Омский НИИ приборостроения»; поселок Песочное, Ленинградской области, антенный полигон Военной академии связи им. С.М. Буденного.

В процессе испытаний были подтверждены следующие характеристики:

– гарантированная скорость при выходе в эфир 2400 бит/с при отношении сигнал/шум от 6 дБ;
– вероятность обеспечения связи в любое время суток более 0.95;
– увеличение скорости без разрыва соединения до 19200 бит/с за счёт частотной адаптации;
– работа в симплексных и полудуплексных каналах;
– поддержание синхронизации в радиосети без выхода в эфир в течение месяца.

Ефимов Е.А.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПРИ ЗАСЕКРЕЧИВАНИИ

Информационная безопасность обеспечивается применением аппаратуры засекречивания для информационных потоков, выходящих за пределы охраняемых зон.

Применяются два вида засекречивания – линейное и блочное.

Линейное засекречивание производится кодированием потоков информации, передаваемых по каналам связи. Для линейного засекречивания применяется покупная аппаратура засекречивания,

которая кодирует информацию выходящую из модемов, и декодирует информацию, входящую в модемы. Для предотвращения выхода высокочастотных составляющих, подлежащих засекречиванию информационных потоков, питание схем обработки этих потоков проводится через специальные фильтры, подавляющие высокочастотные составляющие сигналов.

До передачи засекреченной информации в каналы связи используются специальные фильтры, подавляющие высокочастотные составляющие незасекреченного сигнала, которые могут проникнуть на выходы и на входы передатчиков из-за паразитных связей.

Частоты срезов и глубина подавления этих фильтров зависит от скорости передачи и спектров сигналов во время обработки, подлежащих засекречиванию.

Кроме линейного засекречивания используется блочное засекречивание блоков информации отдельными приборами засекречивания.

В стыках аппаратуры блочного засекречивания и аппаратуры помехоустойчивого кодирования используются фильтры высокочастотного подавления спектров засекречиваемых сигналов для предотвращения попадания составляющих засекречиваемых сигналов на входы аппаратуры передачи данных.

Частоты срезов этих фильтров определяются скоростью передачи информации и спектрами засекречиваемых сигналов.

Для разблокировки пультов управления и задания кодов в аппаратуру засекречивания используются устройства контроля разрешения доступа (КРД). В КРД записываются специальные коды. КРД представляет собой бесконтактное устройство записи и считывания кодов. КРД закрыто герметичным металлическим экраном.

Иванов В.И.
Россия, Санкт-Петербург, ЗАО «Региональный центр защиты информации «ФОРТ»

МЕТОДЫ ОБРАБОТКИ И АНАЛИЗА ДАННЫХ ПРИ АДАПТИВНОМ УПРАВЛЕНИИ ИНЦИДЕНТАМИ В ГЕТЕРОГЕННЫХ СЕТЯХ СВЯЗИ

Современные методы обработки и анализа данных при адаптивном управлении инцидентами базируются на оценках событий информационной безопасности, которые имеют различные источники происхождения и средства регистрации.

В основе таких методов лежит зависимость идентификации событий от объема и формата разнородно поступающей информации, возможностей сил и средств ее регистрации, обработки и анализа.

Пытаясь решить проблему адаптивного управления инцидентами, специалисты по безопасности информационных сетей отдают приоритет построению многоуровневой комплексной системы обработки и анализа данных на основе создания периметров безопасности. При этом корреляционным, сигнатурным и инвариантным методам решения задач на всех уровнях (прикладного программного обеспечения, системы управления базами данных, операционной системы, сети) предшествуют процедуры нормализации, фильтрации, классификации, агрегации, корреляции и приоритезации данных о событиях информационной безопасности по административно установленным критериям и приоритетам.

Другими словами, из многих сотен тысяч исходных многоуровневых событий безопасности оцениванию подлежат только условно значимые, идентифицируемые по установленным правилам автоматизированными средствами учетных и аналитических систем.

Средства мониторинга, аудита и обработки данных этих систем, построенные по принципу «воронки», оставляют вне поля обработки и анализа события с функциями принадлежности нечетких множеств, истинное значение которых было утеряно, либо преднамеренно подвергнуто сомнению. В результате при существующих методах обработки и анализа данных качество оценивания событий теряет полноценную совокупность своих характеристик и сводится, в лучшем случае, к пятибалльной шкале, а механизмы безопасности сети настраиваются на отражение только видимых явных угроз, что в условиях интеграции межведомственных информационных систем только усложняет задачу идентификации и нивелирования ошибок первого и второго рода.

Основными причинами, вызывающими данную проблему, являются ограниченные вычислительные возможности средств обработки и анализа данных, распределенная неоднородная инфраструктура гетерогенной сети связи, трудность интеграции приложений, обрабатывающих и предоставляющих информацию о событиях в единую информационную систему.

Организация на платформе промежуточного программного обеспечения выделенных контуров текущей обработки и комплексного анализа данных о событиях информационной безопасности методом сервис ориентированной технологии объединения и совместного использования удаленных вычислительных ресурсов в системе безопасности гетерогенной сети связи позволит решить проблему и в реальном масштабе времени повысить эффективность и качество управления инцидентами.

В основу предлагаемого метода, в отличие от применяемых методов оптимизации и минимизации вычислений, положена концепция организации виртуальной системы текущей обработки и комплексного анализа данных обо всех мало-мальски значимых событиях информационной безопасности, что в свою очередь позволяет строить долгосрочные прогностические модели безопасности.

Задачами такой системы является эффективное распределение имеющихся вычислительных, сетевых и информационных ресурсов безопасности, ресурсов хранения данных о событиях, а также их координация в зависимости от состава и масштаба виртуальной модели, временных факторов реализации текущих задач и целей, условий конфиденциальности и наличия требуемых программно-аппаратных компонентов сервисно-ориентированной архитектуры.

Каретников А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ ПРИ ПОСТРОЕНИИ ЗАЩИЩЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ

В классическом виде технология виртуализации описывается через концепцию виртуальной машины и монитора виртуальных машин. При этом виртуальной машиной называют изолированный дубликат реальной машины. За счет такого подхода внутри виртуальной машины может работать практически любое программное обеспечение, включая полноценные операционные системы с набором прикладных программ. Монитор виртуальных машин обеспечивает надлежащее функционирование каждой виртуальной машины, работающей в информационной системе. В системе может выполняться одновременно несколько виртуальных машин, а монитор виртуальных машин обеспечивает их совместное использование аппаратных ресурсов, имеющейся реальной аппаратуры в системе.

Можно заметить, что описанный подход очень похож на концепцию операционных систем как таковых. Условно можно поставить в соответствие понятие процесса (изолированный дубликат некоторой программы) понятию виртуальной машины, а ядро операционной системы (которое обеспечивает совместное использование имеющихся аппаратных ресурсов всеми процессами в системе) можно поставить в соответствие монитору виртуальных машин.

Чаще всего технология виртуальных машин используется независимо и обособлено. Другими словами, информационные системы строятся по следующей схеме: на имеющееся аппаратное обеспечение устанавливается программное обеспечение, называемое гипервизором, выполняющее роль монитора виртуальных машин. После старта гипервизор запускает и обеспечивает одновременную работу нескольких виртуальных машин, внутри которых уже функционирует требуемое прикладное программное обеспечение.

Рассмотрим основные преимущества и недостатки применения технологии виртуализации. Абстракция виртуальной машины обеспечивает дублирование программного интерфейса аппаратного обеспечения реальной машины. Это означает, что концепция виртуальных машин обеспечивает свойство переносимости программного обеспечения, что является большим достоинством такого подхода. Наличие монитора виртуальных машин, контролирующего выполнение всех виртуальных машин в системе, позволяет обеспечить свойство изоляции функционирования программного обеспечения. При этом изоляция может быть обеспечена на более низком уровне, чем в случае изоляции процессов в операционной системе. Технология виртуализации также обеспечивает контроль за функционированием программного обеспечения внутри виртуальной машины на более низком уровне. В качестве недостатка технологии можно выделить более сложный интерфейс, с которым приходится работать программному обеспечению, внутри виртуальной машины, чем в случае программного обеспечения, работающего внутри процесса некоторой операционной системы. Одна из главных задач, которую решает абстракция процесса – сокрытие сложности работы с аппаратурой и предоставление удобных сервисов со стороны операционной системы. В свою очередь, абстракция виртуальной машины позволяет выполнять готовое программное обеспечение в изолированной и контролируемой среде.

Возникает идея совместить два рассмотренных подхода путем их комбинирования и создания концепции гибридных операционных систем. Такой подход оказывается очень удобным при создании систем безопасности и защищенных операционных систем. В защищенных операционных системах много внимания уделяется обеспечению надежной авторизации и аутентификации пользователей, контролю доступа к ресурсам системы и другим сервисам, обеспечивающим безопасность работы программного обеспечения и пользователей с системой. Важно понимать, что атомарным функциональным элементом, на который накладывается весь контроль и мониторинг систем безопасности, является абстракция процесса операционной системы. Это означает, что если поместить абстракцию виртуальной машины внутрь абстракции процесса защищенной операционной системы, то все системы контроля и мониторинга, реализованные в защищенной операционной системе, автоматически применяются к программному обеспечению внутри виртуальной машины. При этом

можно сохранить свойство изоляции виртуальной машины от монитора виртуальных машин (сам монитор виртуальных машин можно реализовать средствами имеющейся защищенной операционной системы). Таким образом, автоматически на программное обеспечение внутри виртуальной машины накладываются все ограничения и правила политик безопасности, которые применяются для процесса защищенной операционной системы. Программное обеспечение внутри виртуальной машины никак не может повлиять на защищенную операционную систему за счет свойства изоляции.

Киричек Р.В.
Россия, Санкт-Петербург, ФГУП «ЦентрИнформ»

ЭЛЕКТРОМАГНИТНАЯ УГРОЗА: ОТ МИФА – К РЕАЛЬНОСТИ

Одной их характерных тенденций нового века стало широкое внедрение средств информатизации в критических инфраструктурах. Применяемые меры и средства информационной безопасности защищают такие системы, с использованием программно аппаратных средств, не учитывают возможность проведения атак с использованием генератор электромагнитных импульсов сверхкороткой длительности. Особенностью таких генераторов является их доступность для приобретения, низкая потребляемая мощность, формирование воздействующих импульсов соизмеримых с длительностью рабочих сигналов электронной аппаратуры и сетей передачи данных. В результате воздействия происходит искажение исходной последовательности символов на физическом уровне модели OSI.

Таким образом, поражающий потенциал электромагнитного импульса становится все более опасным в связи с нарастающей информатизацией общества, особенно в передовых промышленно развитых странах и регионах, для нормального функционирования которых насущно необходимы объекты, такие как АСУ ТП, управления системами и средствами защиты от природных, техногенных и террористических угроз, мониторинга оперативной обстановки и кризисного реагирования, управления системами жизнеобеспечения, связи и телекоммуникаций, транспортом, банковской инфраструктурой и пр.

Автор считает необходимым обратить самое пристальное внимание на то, что сопоставимой с последствиями прямых террористических актов по катастрофичности последствий может стать значительно менее энергоемкая массированная электромагнитная атака группы террористов непосредственно на комплекс критически важных узлов информационной инфраструктуры региона.

В настоящее время разработаны и быстро совершенствуются портативные генераторы, источники сверхкоротких (сверхширокополосных) электромагнитных импульсов, имеющих следующие параметры:

- мощность в импульсе до 10 МВт;
- длительность импульса от 0,2 до 10 нс;
- частота повторения до 10 кГц.

Такие генераторы в состоянии сформировать критические уровни электромагнитного воздействия на расстояниях до 100 м, вызывающие сбои и отказы в работе электронной инфраструктуры следствием чего является уничтожение или блокирование информации на объекте информатизации. Мобильность базирования позволяет злоумышленникам за достаточно короткое время проехать с таким источником на автомобиле (или с источниками на нескольких автомобилях) мимо десятков критически важных объектов информатизации региона и обеспечить сопоставимый с ЯВ по масштабам эффект воздействия на информационную инфраструктуру региона. Это, в свою очередь, вызовет катастрофические последствия для систем связи и управления, энергетики, транспорта, банковской, финансовой и т.д.

Организационно и технически такая атака, очевидно, значительно проще, чем проведение любого другого террористического акта, как в плане сравнительной простоты, дешевизны и доступности технических устройств для ее реализации, так и в плане возможностей скрытной подготовки. Важной особенностью такого способа электромагнитной атаки является то, что идентифицировать факт атаки и выявить его источник (источники) практически невозможно, а также отсутствие в действующем законодательстве нормативной базы, предусматривающей уголовную и административную ответственность за проведение электромагнитных атак.

Все вышеизложенное является сильным аргументом в пользу создания государственной системы организационных и технических мер по защите информационной инфраструктуры России от возможных электромагнитных атак террористов.

ФГУП «ЦентрИнформ», как специализированная профильная организация-разработчик системы целевых ГОСТ по защите информации от преднамеренных электромагнитных воздействий, обладает достаточным научным потенциалом для разработки комплектов нормативных документов в интересах ведомств/отраслей. Помимо этого, наша организация имеет необходимое испытательное оборудование (модельный полигон) и методическое обеспечение для проведения работ по защите оборудования в составе объектов информатизации с их последующей аттестацией.

Ларионов С.М
Россия, Санкт-Петербург, ФГУП «ЦентрИнформ»
ОПЫТ ПРОВЕДЕНИЯ ИСПЫТАНИЙ ОБОРУДОВАНИЯ НА УСТОЙЧИВОСТЬ К ЭЛЕКТРОМАГНИТНЫМ ВОЗДЕЙСТВИЯМ СОГЛАСНО ГОСТ Р 52863-2007

Проведение испытаний электронного оборудования, входящего в состав ТСО и АСЗИ, к электромагнитным воздействиям согласно ГОСТ Р 52863-07 необходимо для определения критериальных уровней его устойчивости, что в свою очередь является основой для построения адекватной защиты. В качестве испытываемых образцов оборудования были выбраны средства мобильной связи и навигации, элементы технических средств охраны (СКУД, охранно-пожарная сигнализация, теленаблюдение) и защиты информации.

В состав испытательной установки, созданной на базе модельного полигона ФГУП «ЦентрИнформ», вошли: генераторы СК ЭМИ, средства измерения параметров воздействия, средства диагностики испытываемого оборудования. Изменение уровня воздействия осуществлялось путём изменения параметров генерируемых СК ЭМИ (амплитуда, длительность, частота).

Проведение испытаний позволило выявить деструктивные эффекты в работе оборудования вплоть до его зависания при различных параметрах воздействий.

Мартьянов А.Г.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Информационная безопасность предприятия включает в себя большой спектр различных направлений:

– это и современные средства защиты информации;
– информационная безопасность телекоммуникационных сетей;
– подготовка и переподготовка кадров в области обеспечения информационной безопасности;
– безопасные информационные технологии.

Теперь представим себе на минуту, что все наши современные средства и системы, разработанные и изготовленные по суперсовременным технологиям, остались без электрической энергии. Или часть лабораторий с уникальным оборудованием оказалась залита водой из-за прорыва сетей водоснабжения, или еще хуже – произошел большой пожар. Поэтому необходимо включать в понятие «информационная безопасность предприятия» и такие направления как:

– энергетическая безопасность и эффективность (развитие энергетической составляющей, включающей в себя, в том числе и аварийные источники электроэнергии – дизельные электростанции, аккумуляторы);
– все мероприятия по линии МЧС (пожарная безопасность, защита от стихийных бедствий, наводнений, чрезвычайных ситуаций);
– создание современных систем охраны и видеонаблюдения;
– кадровая политика в области инженерной безопасности.

Поэтому одна из крупных составляющих информационной безопасности предприятия – поддержание, совершенствование и развитие инженерной инфраструктуры предприятия, слаженная и четкая работа всех служб главного инженера.

Панькин А.В., Соколов Б.В, Цивирко Е.Г., Дилоу-Рагиня Э.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МЕТОДЫ И АЛГОРИТМЫ КОМПЛЕКСНОГО ПЛАНИРОВАНИЯ МОДЕРНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ КАТАСТРОФОУСТОЙЧИВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Анализ существующих и прогнозируемых кризисных и чрезвычайных ситуаций, повсеместно возникающих в настоящее время в различных предметных областях, показывает, что они перестают быть отраслевыми, а перерастают в аварии и катастрофы, имеющие уже межотраслевой характер. При этом под катастрофоустойчивостью информационных систем (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. 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. В докладе предложены методологические и методические основы решения фундаментальной задачи комплексной автоматизации и интеллектуализации процессов адаптивного планирования и управления модернизацией и функционированием катастрофоустойчивых ИС (КАИС) на основе скоординированной и обоснованной разработки и реализации полимодельного, многокритериального подхода к описанию исследуемой предметной области. Предлагаемое в докладе рассмотрение вопросов комплексного адаптивного

планирования и управления модернизацией и функционированием КАИС в общем контексте УСД позволяет, во-первых, непосредственно связать те общие цели, на достижение которых ориентировано функционирование конкретной бизнес-системы (БС) и соответствующей ИС, с теми целями, которые реализуются в ходе управления структурами БС и КАИС, во-вторых, обоснованно определить и выбрать соответствующие последовательности решаемых задач и выполняемых операций (действий), связанных со структурной динамикой (другими словами, синтезировать технологию управления как БС, так и КАИС), и, в-третьих, осознанно находить компромиссные решения при распределении ограниченных ресурсов, выделяемых на управление структурной динамикой указанных систем в условиях возможных кризисных, чрезвычайных и аварийных ситуаций. Предложена оригинальная обобщенная методика решения задач комплексного планирования модернизации и функционирования КАИС в условиях динамично изменяющейся обстановки, которая включает две основные фазы. На первой фазе должно осуществляться формирование (генерирование) допустимых вариантов многоструктурных макросостояний КАИС или, говоря другими словами, оперативный структурно-функциональный синтез нового облика КАИС, соответствующего целям проводимой модернизации и складывающейся (прогнозируемой) обстановке, связанной с возможной деградацией структур создаваемой и существующей КАИС. На второй фазе проводится выбор конкретного варианта многоструктурного макросостояния КАИС с одновременным синтезом (построением) адаптивных комплексных программ управления ее переходом из текущего в требуемое макросостояние. Данная работа выполнялась при финансовой поддержке РФФИ (гранты 09-07-00066, 10-07-00311, 11-08-01016, 10-07-01071, 10-08-90027-Бел_а), ОНИТ (проект 2.3).

Расторгуев В.Я.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

УСИЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРИТИЧЕСКИХ СИСТЕМАХ НЕПРЕРЫВНОГО ФУНКЦИОНИРОВАНИЯ ПУТЕМ ВИРТУАЛИЗАЦИИ ЭЛЕМЕНТОВ ИХ СИСТЕМ УПРАВЛЕНИЯ

Важнейшим условием правильной работы Критической Системы (КС) непрерывного функционирования является сохранение целостности информации (точнее: данных, программ, информационных потоков и т.д.), которая м.б. нарушена, в частности, из-за угроз:

– физического старения и, как следствие, отказа аппаратуры Системы Управления (СУ);

– морального старения аппаратуры, а также Общего и Системного Программного Обеспечения СУ (ОСПО СУ) и, как следствие, необходимости их модернизации с неизбежным риском внесения необнаруженных ошибок ОСПО.

Использование Виртуальных Процессоров (ВП) в СУ вместо физических имеет, как минимум, два полезных следствия, увеличивающие информационную безопасность, а именно:

– исключение возможности отказов ВП, т.к. виртуальный процессор физически не стареет;

– возможность достичь практического устранения морального старения ВП, так как темп морального старения ВП никак не связан с темпом морального старения физического процессора.

Известно, что виртуализация, широко используемая в современных технологиях, например, для организации «облачных» сервисов и вычислений, м.б. выполнена различными способами.

В докладе обсуждаются варианты виртуализации, перспективные для применения в СУ КС.

Тимохин А.П., Бочкарёв В.В.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

МЕТОДЫ ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ КОНСТРУКЦИИ АППАРАТУРЫ ДЛЯ СИСТЕМ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ И ДВОЙНОГО НАЗНАЧЕНИЯ

Аппаратура предусматривает поузловое экранирование электрических и магнитных полей. Экранирующие корпуса приборов аппаратуры представляют собой замкнутые объемы со съемными крышками. Неразъемные сочленения выполнены сварными или паяными по всей длине швов. При применении разъемных сочленений применяется клёпка или винты, при этом по поверхности сочленения нанесено антикоррозийное электропроводное покрытие.

Корпуса приборов выполнены из стали не менее одного миллиметра. Съемные крышки приборов имеют контакты для сигнализации, включенной в систему диспетчеризации.

В контактных сочленениях обеспечен надежный электрический контакт всех лепестков контактных пружин с экранирующим корпусом.

Вентиляционные отверстия на стойках закрыты сеткой с размером ячейки 3×3 мм. Сетка покрыта электропроводящим покрытием.

Составные части аппаратуры, содержащие информацию, защищены прочными корпусами.

Корпуса приборов изготовлены из стали толщиной не менее одного миллиметра, выдерживающие механические нагрузки в соответствии с условиями эксплуатации.

Составные части аппаратуры, содержащие информацию, защищены от воздействия пожара и взрывов. Материалы из которых изготовлены составные части аппаратуры, экологически безопасны и выбраны в соответствии с «Перечнем материалов и покрытий разрешенных к применению в аппаратуре изделий, разрабатываемых НПО «Импульс» от 27.03.2007 года.

Двери стоек, пультов, приборов содержащих информацию имеют места пломбирования заводом – изготовителем и службой эксплуатации, ограничивающих доступ к составным частям аппаратуры посторонним лицам.

В конструкции специальных приборов предусмотрены средства самоуничтожения.

Тарасов Е.Н., Кулагин А.Ф., Блохин С.М., Роговой С.П.
Россия, Москва, ФГУП «НПЦ автоматики и приборостроения им. акад. Н.А. Пилюгина»

КОНФИГУРИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ КАК СРЕДСТВО ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ ОТ НСД

Рассматривается автоматизированная система обработки данных (АСОД) – многопользовательская распределённая система, хранящая и обрабатывающая информацию с высокой степенью конфиденциальности. Информационные и вычислительные ресурсы системы централизованы. Для защиты информации от НСД использованы программные средства из состава входящих в БИЗКТ.

АСОД предназначена для решения ряда целевых задач по обработке данных, вводимых и хранящихся в системе. Для обеспечения выполнения тактико-технических требований к системе в ней использовано централизованное управление: работой системы управляет «лицо, принимающее решения» (ЛПР), которое со своего рабочего места управляет состоянием системы и ходом решения целевых задач.

Угрозам несанкционированного доступа к данным, обрабатываемым в системе, достаточно успешно противостоят штатные средства защиты о НСД (КСЗИ НСД). Однако, существует угроза проникновения нарушителя в систему с удалённых рабочих мест под прикрытием санкционированного доступа.

Для повышения защищённости АСОД от подобных угроз предлагается использовать конфигурирование системы: ЛПР определяет в соответствии с решаемой целевой задачей в сеансе работы АСОД состав АРМ, которые должны быть задействованы в вычислительном процессе. Остальным АРМ системы сетевой доступ к информационным и вычислительным ресурсам блокируется средствами управления, находящимися в распоряжении ЛПР.

Тулупьев А.Л., Тулупьева Т.В., Пащенко А.Е., Суворова А.В., Мусина В.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ОЦЕНКА ИНТЕНСИВНОСТИ УГРОЗООБРАЗУЮЩЕГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ НЕПОЛНЫХ И НЕТОЧНЫХ ДАННЫХ: ГАММА-ПУАССОНОВСКАЯ МОДЕЛЬ ПОВЕДЕНИЯ

Мониторинг степени защищенности автоматизированных информационных систем (АИС) должен вестись постоянно, иначе все мероприятия, входящие в комплекс мероприятий по защите информации, окажутся неэффективными, утратят свой смысл. При этом следует отметить, что мониторинг лишь программно-технической составляющей автоматизированных информационных систем необходим, но явно не достаточен. Он должен охватывать также персонал (т.е. санкционированных пользователей) таких систем.

Достаточно широким классом угроз безопасности критической информации, хранящейся в АИС, являются социоинженерные атаки, направленные на персонал системы. То, что такая атака осуществляется, проявляется, в частности, в изменении поведения пользователя или группы пользователей: частота угрозообразующих действий (и даже более широко – действий, которые могут оказаться угрозообразующими) таких пользователей может измениться. Мониторинг степени защищенности АИС должен позволять своевременно обнаруживать такие изменения.

Поскольку обнаружение изменений в поведении пользователя или группы пользователей должно выполняться достаточно оперативно (иначе результаты могут оказаться уже неактуальными), оценка интенсивности (частоты) угрозообразующих действия должна будет осуществляться в условиях информационного дефицита, когда доступны сведения о небольшом числе событий, вызвавших подозрения (например, один, два или три эпизода угрозообразующих действий, в которых принял участие отдельный пользователь)

Предлагается в качестве модели угрозообразующего поведения пользователя использовать обобщенный гамма-пуассоновкий случайный процесс, уравнения которого модифицированы с учетом систематической ошибки, возникающей из-за работы с ограниченным числом последних эпизодов. Такая систематическая ошибка описана в статистической литературе как lengthbias (систематическая ошибка, связанная с длительностью наблюдений). При такой постановке задачи, интенсивность поведения является параметром указанной модели и оценивается стандартными статистическими методами.

Уланов А.В.
Россия, Мытищи, НИИЦ систем связи ФГУ «27 ЦНИИ Минобороны России»

ОБЕСПЕЧЕНИЕ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ УЗЛОВ СВЯЗИ МОБИЛЬНЫХ ПУНКТОВ УПРАВЛЕНИЯ В УСЛОВИЯХ ПРОГРАММНО-АППАРАТНЫХ ВОЗДЕЙСТВИЙ

В настоящее время ситуация в области информационного противоборства характеризуется ростом его масштабов и эффективности, становятся всё более заметными преимущества успешной борьбы в информационной сфере для решения традиционных и качественно новых задач, стоящих перед ведущими мировыми государствами. В этой связи особенно важное значение приобретает защита систем управления критически важными объектами страны от воздействий информационного характера.

Как известно, в чрезвычайных ситуациях наиболее уязвимыми для всех видов воздействий местами в системе управления становятся узлы связи мобильных пунктов управления (УС МПУ), обеспечивающие в любой географической точке обмен основными потоками оперативной информации, необходимой для эффективного управления. При этом основные свойства управления – оперативность и непрерывность в большей степени определяются способностью узлов связи устойчиво функционировать, то есть сохранять значения параметров и показателей в пределах установленных норм при всех воздействующих факторах внешней среды.

Практика показывает, что современные УС МПУ в большей степени подвержены программно-аппаратным воздействиям (ПАВ), поскольку они являются наиболее эффективным и легко реализуемым видом информационного воздействия, не требуют больших материальных и людских затрат и могут осуществляться в большинстве случаев независимо от расстояния между объектом и субъектом воздействия. Данное обстоятельство обусловлено тем, что входящие в состав современных УС МПУ средства связи и автоматизации управления связью разрабатываются на основе международных открытых стандартов и протоколов, являются программно управляемыми, а доступ к ним и управление ими возможно осуществлять по каналам связи, вследствие интеграции современных систем связи в глобальную информационную инфраструктуру.

В большинстве случаев ПАВ будут направлены на добывание, искажение и уничтожение информации, а также блокирование (затруднение) информационного обмена в интересах должностных лиц органов управления критически важными объектами (КВО).

В соответствии с выше изложенным при определении интегрального показателя устойчивости функционирования современного УС МПУ, на наш взгляд, необходимо учитывать свойство устойчивости к ПАВ, поскольку оно будет влиять:

– на способность узла связи выполнять поставленные задачи в условиях отказов средств связи в результате ПАВ;

– на способность скрытия от сетевой разведки маршрутно-адресной и технологической информации, которая может быть использована для реализации ПАВ;

– на время выполнения определенного комплекса работ по развертыванию узла связи, включающего настройку автоматизированных рабочих мест и программного обеспечения для управления средствами связи и КВО;

– на способность технических средств связи осуществлять контроль своего состояния, передавать данные о своем состоянии, принимать и исполнять команды технологического управления связью.

Помимо этого, существующий научно-методический аппарат, направленный на обеспечение устойчивости функционирования УС МПУ, на сегодняшний день не может быть достаточен по следующим причинам:

– не в полной мере учитывает особенности функционирования современного УС МПУ в условиях ПАВ, обусловленные информационной неопределенностью – дефицитом, недостоверностью, либо полным отсутствием информации о субъекте ПАВ;

– не учитывает особенности функционирования современного УС МПУ в условиях ПАВ, обусловленные информационной нечеткостью – представлением большей части информации об объекте и внешней среде в неклассическом (нечетком) виде, неподходящем для стандартной обработки с использованием ЭВМ;

– не в полной мере учитывает технические особенности используемых в современных УС МПУ информационно-телекоммуникационных средств;

– не в полной мере учитывает сегодняшние средства и возможности по ведению сетевой разведки и осуществлению ПАВ;

– основан на применении традиционных математических методов и не позволяет получать достаточно достоверные результаты при условии функционирования УС МПУ в неопределенности, нечеткости и динамически изменяющейся информационной обстановке.

В связи с этим возникает необходимость совершенствования существующего научно-методического аппарата обеспечения устойчивости функционирования УС МПУ в направлении его применения в условиях ПАВ при информационной нечеткости и неопределенности. В частности

видится актуальной разработка новых моделей и методов обеспечения устойчивого функционирования УС МПУ в условиях ПАВ, позволяющих при имеющейся информационной нечеткости и неопределенности оперативно их обнаруживать, находить оптимальные решения по противодействию, а также оценивать эффективность мер, применяемых в целях повышения устойчивости функционирования.

Устинов И.А., Игумнов В.В.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Информационная безопасность (ИБ) относится к числу важнейших характеристик критических инфраструктур (КИ). Это относится как к информационной безопасности в целом, так и к безопасности информатики в частности.

Решение этой фундаментальной проблемы и её контроль проходит на всех этапах жизненного цикла КИ (от замысла и проектирования до эксплуатации). Меры, принимаемые для её решения, должны быть сопоставимы с размером возможного ущерба от деструктивных воздействий на КИ со стороны эвентуального противника.

Ведущая роль в обеспечении ИБКИ принадлежит ключевой информационно-управляющей системе критической инфраструктуры (КСКИ).

Требования к КСКИ определяются классом решаемых функциональных задач. Отсюда определяются соответственно и требования к элементной базе, схемно-конструкторским решениям, аппаратной платформе, программному обеспечению, системе контроля звеньев, стендовой базе, вопросы авторского сопровождения и др.

В ФГУП НПО «Импульс» разработана и успешно применяется технология создания защищённых ключевых систем для критической инфраструктуры (оборона, транспорт и др.). Разработаны и успешно эксплуатируются несколько поколений систем, созданных на базе этой технологии.

В докладе рассматриваются основные положения указанной технологии.

Фильченков А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДИАГНОСТИЧЕСКОЙ МОДЕЛИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ КОМБИНИРОВАНИЯ НЕПОЛНОЙ И НЕТОЧНОЙ АНАЛИТИЧЕСКОЙ ИНФОРМАЦИИ

Защита информации должна носить комплексный характер, и при разработке и дальнейшей диагностике системы важно с высокой степенью точности оценивать существующие угрозы и предлагать механизмы их предотвращения для того, чтобы, с одной стороны, процессы защиты по каждому возможному направлению превосходили процессы атаки, и с другой стороны, процессы защиты не были избыточными, так как избыточность может повлечь за собой неоправданные финансовые и материальные расходы. В связи с этим крайне важным является построение диагностической модели защищенности информационной системы, оценки которой максимально полно отражают известные оценки угроз и состояний системы безопасности.

Одним из основных понятий, связанных с информационной безопасностью, является риск, который традиционно формализуется вероятностной мерой. Однако используемый в ряде аналитических методов вероятностный подход не является исчерпывающим, поскольку его выразительная мощность зачастую оказывается недостаточной для представления предметной области. Во-первых, одним из источников знаний для моделирования является опрос экспертов по безопасности. Вероятностной меры оказывается недостаточно для несогласующихся между собой оценок экспертов (так, если один эксперт указал вероятность 24%, а другой – 46%, то точное отображение этой информации в рамках использования вероятностной меры представляется достаточно затруднительным). Во-вторых, другим источником знаний являются полученные на основе анализа статистических данных вероятностные распределения процессов, сопряженных с попытками получить несанкционированный доступ к информационной системе или повредить ее. Представление возможных распределений на основе скалярных (точечных) оценок вероятности приводит к существенной потере информации, и, как следствие, недостаточной точности исследуемой модели.

Одним из способов преодолеть указанные ограничения, связанные с использованием вероятностной меры, является создание модели, оперирующей интервальными оценками вероятности. Интервальные оценки позволяют реализовать более выразительно мощное представление вероятностной информации, чем скалярные оценки, при этом вычислительная сложность математической обработки такого представления все еще остается допустимой с точки зрения современного уровня аппаратного обеспечения. Математический формализм, использующий интервальные оценки вероятности для представления неточности, рассматривается в теории алгебраических байесовских сетей.

Алгебраические байесовские сети относятся к классу вероятностных графических моделей; каждая такая сеть представляет собой граф, построенный над семействами совместных вероятностных распределений над идеалами конъюнктов. Такие идеалы, называемые фрагментами знаний, позволяют декомпозировать предметную область на наборы связных утверждений, которым присваивается интервальная оценка вероятности истинности. Использование алгебраических байесовских сетей для диагностирования защищенности информационной системы позволит уточнить вероятностное представление процессов и направлений совершения атак, а тем самым позволит оптимизировать распределение ресурсов для предотвращения этих атак.

Чванов В.П.
Россия, Санкт-Петербург, ФГУП «ЦентрИнформ»

ОРГАНИЗАЦИЯ И СОДЕРЖАНИЕ РАБОТ ПО ЗАЩИТЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ ПРЕДНАМЕРЕННЫХ ДЕСТРУКТИВНЫХ ЭЛЕКТРОМАГНИТНЫХ И ЭЛЕКТРИЧЕСКИХ ВОЗДЕЙСТВИЙ

В соответствии с планом работ ТК-362 в 2010 году авторами доклада разработан ГОСТ Р «Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных деструктивных электромагнитных и электрических воздействий. Общие положения». Этот документ является связующим в системе целевых стандартов по защите автоматизированных систем в защищенном исполнении (АСЗИ) от данной угрозы.

Общими положениями стандарта определяются и устанавливаются: роль и место работ по защите АС от ПД ЭМВ во взаимодействии с работами по построению комплексных систем безопасности, структурные компоненты защиты, этапы и содержание работ, их исполнители и возлагаемые на них функции, ответственность за обеспечение требований по защите при эксплуатации АСЗИ.

Работы по защите предусматриваются при создании АС в защищённом от ПД ЭМВ исполнении и при их эксплуатации в составе объектов информатизации.

При создании АСЗИ, в соответствии с положениями стандарта, осуществляются:

– разработка концепции защиты информации в АС от ПД ЭМВ, имеющая целью формирование проектных решений защиты;
– реализация проектных решений;
– ввод в действие АС в защищенном от ПД ЭМВ исполнении.

При эксплуатации АСЗИ проводятся:

– использование по назначению технических средств обнаружения и защиты от ПД ЭМВ;
– организационно-технические мероприятия по защите;
– техническая эксплуатация средств обнаружения и защиты;
– контроль защищённости АС от ПД ЭМВ.

В приложениях стандарта приведены типовые формы разрабатываемых документов и некоторые информационные данные, необходимые для проведения работ.

Хвостунов Ю.С.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

АДАПТИВНАЯ СИСТЕМА ДЕКАМЕТРОВОЙ РАДИОСВЯЗИ С ПОЛНОДИАПАЗОННОЙ ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКОЙ РАБОЧЕЙ ЧАСТОТОЙ И ПРЕДВАРИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ ТРАССОВЫХ ИСПЫТАНИЙ ЕЕ ФРАГМЕНТА

Адаптивная система коротковолновой радиосвязи с полнодиапазонной псевдослучайной перестройкой рабочей частоты (АСДР ППРЧ) предназначена для создания симплексных, полудуплексных и дуплексных каналов радиосвязи декаметрового диапазона на дальности до 300 км в движении и до 3000 км между стационарными пунктами связи со скоростями работы абонента от 2400 до 19 200 бит/с.

Принципы работы АСДР ППРЧ.

Для каждой отдельной сети:

– выделяется пул рабочих частот (N рабочих частот);
– назначается n (n < N) начальных рабочих частот;
– назначается ключ закона перестройки рабочей частоты;
– устанавливается время t работы на одной рабочей частоте.

Для каждого абонента отдельной сети:

– назначается двухбайтный сетевой адрес;
– назначается одна из ортогональных строк частотно-временной матрицы рабочих частот.

При воде абонента в сеть через радиоканал осуществляется начальная синхронизация переключения начальных рабочих частот (сетевая синхронизация). В дальнейшем в течение 1–1,5 месяцев абонент готов к обмену информацией из состояния радиомолчания без предварительного этапа зондирования канала связи и установления синхронизации. Если с течение

этого времени в сети состоялся обмен информацией, то для всех абонентов сети время готовности продлевается на 1–1,5 месяца. Адресная передача («точка» – «точка», «точка» – «многоточка») ведется пакетами длительностью 53 мс на каждой из n начальных рабочих частот.

Принимающая радиостанция в процессе обмена информацией без снижения пропускной способности подтверждает передающей успешный прием по каждой используемой рабочей частоте. В случае отсутствия приема на данной рабочей частоте принимающая радиостанция дает команду передающей радиостанции на замену на резервную рабочую частоту из общего набора.

Предварительные результаты трассовых испытаний фрагмента системы

Трассовые испытания фрагмента системы проходили в период с 10.08.2011 г. по 06.09. 20011г. на трассе Санкт-Петербург – Омск. Получены первые предварительные результаты трассовых испытаний:

– диапазон используемых радиочастот (определялся выделенными для трассовых испытаний рабочими частотами) – 4 ÷ 19 МГц;

– техническая текущая скорость работы адаптивно менялась в пределах 3,6 ÷ 25 Кбит/с;

– текущая скорость обмена информацией между оконечным оборудованием данных менялась в пределах 2,4 ÷ 15,2 Кбит/с;

– количество рабочих частот в пакете перестройки – 32;

– время адаптации по рабочим частотам и скорости передачи в зависимости от качества рабочей частоты менялась в пределах 5 – 52 с;

– вероятность связи в любое время суток – выше 0,99 (не наблюдалось ни разу отсутствия связи).

Черкесов Г.Н.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

ОЦЕНКА ЖИВУЧЕСТИ И ОТКАЗОБЕЗОПАСНОСТИ МАЖОРИРОВАННОЙ ПАМЯТИ С КЛАСТЕРНОЙ СТРУКТУРОЙ

Для повышения надежности и достоверности функционирования оперативной памяти в системах связи, системах управления, бортовых вычислительных системах самолетов, судов, космических аппаратов и других объектов с высокими требованиями к отказобезопасности применяют резервирование типа параллельного мажорирования по схеме «два из трех». При кластерной структуре памяти возможно мажорирование на уровне одного кластера. Таким образом, структурно память может быть представлена как последовательное соединение мажорированных групп из трех кластеров. При этом процедура голосования может быть проведена как в процессоре, так и в специализированных мажорирующих элементах (МЭ). В необслуживаемых вычислителях возможно накопление отказов отдельных кластеров, возникающих вследствие естественных процессов или в результате внешнего воздействия (например, потоков космических частиц), без потери работоспособности системы. В связи с этим возникает вопрос о том, каков риск потери работоспособности памяти при заданном числе отказавших элементов (кластеров). Это зависит от распределения отказавших элементов по полю памяти. Мерой риска могут быть показатели живучести (отказоустойчивости): вероятность того, что в системе из n групп неработоспособно ровно m групп при условии неисправности k структурных элементов (кластеров); вероятность потери работоспособности не более m групп из n. В общем случае уровень деградации структуры можно охарактеризовать четырьмя параметрами (n, m, k, i), где i – число групп с тремя отказавшими элементами. Поскольку с увеличением m вероятность можно сколь угодно близко приблизить к единице, то не трудно решить задачу о таком значении числа резервных групп кластеров, который обеспечит практически гарантированный уровень вероятности сохранения важной для системы информации (программ и данных). Причем этот уровень гарантируется при любых показателях надежности элементов памяти. Иначе говоря, для принятия решения об уровне резервирования в памяти вообще не надо знать статистики отказов памяти.

Для обеспечения отказобезопасности и живучести могут использоваться следующие методы: процедуры периодической принудительной регенерации, регулирование размера кластеров, использование резервных кластерных групп, помехоустойчивое кодирование с коррекцией ошибок.

В докладе излагаются модели функционирования мажорированной памяти и приводятся формулы для расчета показателей живучести и отказобезопасности памяти с учетом возможных способов улучшения этих характеристик.

Анализируя зависимость вероятности потери m групп из n при k отказавших кластеров, можно определить наиболее вероятное значение числа отказавших кластеров k0 , при котором не исправны m групп. Оказывается, что это число во много раз превосходит минимальное число kmin = 2m, которое достаточно для вывода из строя m групп. Для m = 1 отношение δ = k0 / kmin = 7 при n = 64 и δ = 10 при n = 128. Для m = 2: δ = 5 и 7 соответственно, а для m = 3: δ = 4,25 и 5,83 соответственно. Доля отказавших кластеров (из k), которые оказались в работоспособных группах, снизив в них избыточность, но не вызвав отказа группы, значительна. При различных m и n она колеблется в

пределах от 50 до 90%. С увеличением n эта доля растет. Этот феномен очень важен для правильной оценки возможности изделия успешно выполнять свои функции в будущем. При относительно малом m создается видимость благополучия, поскольку отказавших групп не много, но надежность памяти низкая. При фиксированном k существует наиболее вероятное число m0 отказавших групп. Оно значительно меньше максимально возможного mmax = [k/2]. Например, при n = 64, k = 19: m0 = 2, mmax=9; при n = 128, k = 19: m0 = 1, mmax = 9; при n = 128, k = 34: m0 = 3, mmax = 17.

Рассчитывая значения вероятности, можно найти такое максимальное значение числа отказавших кластеров, при котором вероятность отказа не более m групп остается на уровне не менее заданного значения p. Результаты оценки показывают, что весьма много отказавших кластеров расположено в работоспособных группах. Так при n = 64, m = 2, вероятность потери не более двух групп будет не менее 0,9. При этом возможны отказы 16 кластеров, из которых только 4–6 кластеров находятся в отказавших группах, а остальные 10-12 (что составляет 63-75%) находятся в работоспособных группах. При n = 128 еще большая доля отказавших кластеров (73-82 %) находится в работоспособных группах.

Показатели живучести (отказоустойчивости) резервированной памяти позволяют уже на ранних стадиях проектирования установить приемлемые параметры системы памяти: число групп, размеры кластера, объем резервной части емкости памяти, а также оценить эффект от применения гибкой адресации, помехоустойчивого кодирования и возможности перезагрузки файлов в работоспособную часть памяти.

Чистяков И.В., Орлов Д.Р.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

МЕТОДЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ УСТРОЙСТВ ХРАНЕНИЯ

Современный подход к обеспечению безопасности информационных технологий требует обеспечения безопасности информации не только при ее передаче по каналам и сетям связи, но и при хранении на запоминающих устройствах различного типа.

Рассматриваются два типа систем:

– с локальным устройством хранения;

– с сетевым устройством хранения и модели безопасности информационных технологий для них.

Устройства хранения как среда безопасности имеет ряд особенностей:

– длительный срок нахождения информации с возможностью ее частичного обновления;

– отсутствие on-line взаимодействия между пользователями и ряд других, которые должны быть учтены при разработке системы криптографической защиты. При этом необходимо минимизировать увеличения времени доступа и требуемый объема дополнительной памяти.

Основными сервисами, обеспечиваемыми криптографическими механизмами для систем, хранения являются: конфиденциальность, имитостойкость и криптографическое разграничение доступа.

Конфиденциальность обеспечивается путем шифрования, имитостойкость – путем шифрованием с аутентификацией, использования функции хэширования или цифровой подписи, а криптографическое разграничение доступа предполагает использование гибкой схемы управления криптографическими ключами.

Механизмы безопасности могут быть размещены на различных уровнях хранения. В докладе рассматриваются следующие уровни: блок/запись и файловая система.

На уровне блок/запись необходимо учитывать организацию хранения данных (например, блок-сектор для дисковых накопителей). Для обеспечения конфиденциальности рассматривается возможность использования стандартных режимов шифрования ГОСТ 28147-89 (простой замены, гаммирования, гаммирования с обратной связью), а также специально разработанного для систем хранения протокола «tweakable encryption». Для контроля целостности анализируются протоколы шифрования с аутентификацией (режим выработки имитовставки, а также на базе протокола «tweakable encryption»).

Для обеспечения безопасности файловых систем наиболее сложными являются вопросы обеспечения защиты от навязывания неактуальных версий файла и криптографического разграничения доступа.

Рассматривается схема контроля актуальности файла (как часть сервиса имитостойкости) на основе цифровой подписи и виртуальных нумераторов версий файлов, не требующая on-line взаимодействия между пользователями.

Основой криптографического разграничения доступа с учетом иерархии полномочий пользователей является итеративная схема назначения и вывода ключей, которая может быть использована также для реализации схемы регрессии ключей, используемой для уменьшения пиковых нагрузок при смене криптографических ключей.

Чуднов А.М.
Россия, Санкт-Петербург, Военная академия связи им. С.М. Буденного

МЕТОДОЛОГИЧЕСКИЙ ПОДХОД И ЧАСТНЫЕ СЛУЧАИ ОЦЕНКИ ПОКАЗАТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ

В работе развивается общий подход и рассматриваются частные случаи оценки показателей информационной безопасности информационно-управляющей системы (ИУС).

Для задания показателей информационной безопасности используется обобщенная модель взаимодействия ИУС как динамической системы с системой потенциального нарушителя.

В общем случае воздействия нарушителя осуществляются с учетом информации об ИУС, получаемой по легальным и нелегальным средствам (каналам), которые должны быть учтены в обобщенной модели.

При задании объектов модели ИУС в виде стохастических операторов стохастически определенным является поведение системы и, следовательно, показатель эффективности можно представить в зависимости от операторов, определяющих стратегию ИУС U и стратегию нарушителя V:

$$Q = Q\,[U,V]$$

Полагается, что стратегия нарушителя выбирается (и соответственно может оптимизироваться) после задания (ввода в действие) технологии ИУС. Таким образом, рассматривается задача оптимизации ИУС в минимаксной постановке:

$$Q = Q\,[U,\ V^*(U,CV)] \rightarrow m\ a\ x\ /\ U \in U\ (CU),$$

где U (C_U) – множество допустимых ИУС при ограничениях C_U, $V^*(U,C_V)$] – оптимальная стратегия нарушителя для оператора ИУС U и ограничения C_V.

Рассмотрены формализованное представление и интерпретация показателей безопасности. Приведен пример оценки показателей безопасности фрагмента ИУС.

Штогрин И.Р.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

ОБЕСПЕЧЕНИЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ЭТАПЕ СТЕНДОВОЙ ОТРАБОТКИ ИЗДЕЛИЙ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ СИСТЕМ

Обеспечение безопасности информации в критических информационно-управляющих системах имеет главенствующие значение для их устойчивости к разного рода воздействиям.

На этапе разработки и отработки изделий и систем в целом, процесс обеспечения безопасности информации включает:

– определение требований по безопасности информации и выработку технических решений по порядку их реализации;

– реализацию требований по безопасности информации в конструкторской документации и технологиях проектирования;

– обеспечение требований нормативно-технической документации по безопасности при отработке и испытаниях;

– подтверждение реализации заданных требований по безопасности в процессе испытаний изделий и систем в целом;

В данной статье рассматриваются принимаемые меры по обеспечению безопасности информации на этапе отработки изделий на комплексных стендах «ФГУП НПО «Импульс».

Поскольку на этапе отработки изделий технические решения по обеспечению безопасности информации в большинстве не внедрены, или не проведена оценка их эффективности, то защиту информации в изделиях, возможно обеспечить в основном только мерами, предусмотренными в нормативно-технической документации, ограничивающими доступ к информации, и обеспечивающими сохранение информации и которые подразделены на технические и организационные. Среди основных технических и организационных мер защиты информации на этапе стендовой отработки необходимо отметить:

– размещение объектов и технологического оборудования для разработки в экранированном помещении, обеспечивающем защиту от утечек информации, в том числе по цепям электроснабжения, телефонным линиям связи и местным компьютерным сетям.

– применение технологической аппаратуры (ПЭВМ), прошедшей соответствующие проверки и имеющей предписание на эксплуатацию, исключение использования съемных носителей информации;

– исключение прямого выхода соединения локальной компьютерной сети с внешними сетями;

– ограничение и контроль допуска сотрудников в помещения с использованием автоматизированной системы контроля допуска;

– многоуровневый контроль за перемещением и хранением всех видов носителей информации.

Обеспечение реализации указанных мер на практике осуществляется соответствующим графиком проверки уровня экранирования помещений, периодическим обновлением списков допущенных, совершенствованием системы допуска и документирования посещения.

Многолетний опыт по созданию информационно управляющих систем для обеспечения управления в критических условиях подтверждает, что применение и выполнение выше указанных в докладе мер позволяет обеспечить выполнение всех требований по обеспечению безопасности информации на этапе стендовой отработки.

Щёткин И.Е.
Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»,
Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

ИНВЕСТИЦИОННО-ИННОВАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ ПРЕДПРИЯТИЯ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ В ЦЕЛЯХ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Исторически сложившаяся система обмена информацией на предприятиях критической инфраструктуры позволила сформировать основные принципы и методы защиты информации как внутри предприятия, так и во внешней среде. С появлением и широким применением вычислительной техники резко увеличились объемы информационных потоков, методы ее передачи, хранения, доступа к ней. Остается актуальным вопрос информационной безопасности современных систем, а также растет сложность осуществления данной задачи.

Владение информацией создает конкурентоспособность предприятия на рынке товаров и услуг, задает новые требования и предпосылки модернизационных и инновационных внедрений в уже сложившиеся системы. Инновационные подходы в производстве, внедрение безбумажного документооборота, формирование единых информационных пространств формируют задания к осуществлению безопасности, особенно в критической инфраструктуре, где несанкционированное использование информационных ресурсов может привести к необратимым последствиям для предприятия.

Одновременно с применением уже отработанных схем свою значимость доказывают новые решения в области защиты информации, основой которых являются автоматизированные системы. В связи с большим вниманием к этой сфере и постоянной необходимостью совершенствования для осуществления безопасности и конкурентоспособности предприятия необходимым условием развития является плановое инвестирование в инфраструктуру информационной защиты и обучение людей современным методам и технологиям.

Внедрение инновационных решений в эту сферу достаточно дорогая и высоко рискованная мера, но она необходима в связи тем, что с одной стороны недофинансирование данного направления может привести к отсталости методов и необеспеченности персонала для осуществления работ, с другой стороны каждая организация ограничена финансовыми и трудовыми ресурсами. Рациональное использование финансирования и привлечение инвестиций в инновационные проекты данной сферы серьезная проблема каждого предприятия и одной из основных ее особенностей является скорость изменения и внедрения инноваций в сферу по всему миру, что делает необходимым постоянный мониторинг современных методов и быстрое реагирование на изменяющуюся среду.

Специфичность критических инфраструктур заключается в значительных последствиях неправильной реализации проектов и незащищенности информационных ресурсов. Несанкционированный доступ к информации атомной, оборонной и других видов деятельности государства может привести к большим жертвам среди населения и разворачиванию военных действий, экономической блокаде государства. В связи с этим сложная задача осуществления информационной безопасности получает еще значительную прибавку ответственности и становится еще более трудоемкой, но остается необходимой мерой для государства и конкретного предприятия.

Одной из основных задач предприятия критической инфраструктуры является выработка обоснованных и современных подходов осуществления информационной безопасности, а проблему инвестирования в данную сферу поможет решить постоянное совершенствование методов инвестиционной и инновационной деятельности предприятия.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГИДРОМЕТЕОРОЛОГИИ

Басов И.С.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

РАЗРАБОТКА ПРОГРАМНОГО КОМПЛЕКСА ШИФРОВАНИЯ НА ОСНОВЕ АЛГОРИТМА AES ДЛЯ НУЖД ГИДРОМЕТЕОРОЛОГИИ

В современном информационном обществе вопрос защиты информации становится всё более важным. При решении задач по обеспечению безопасности данных зачастую прибегают к использованию шифрования.

Стандарт шифрования AES является официальным стандартом правительства США для симметричного шифрования, который определяется публикацией FIPS #197 (2001). AES представляет собой блочный шифр, кодирующий 128-битный текстовый блок в 128-битный шифрованный блок, или дешифрует 128-битный шифрованный блок в 128-битный текстовый блок. Данный стандарт широко используется в разнообразных приложениях, где предъявляются повышенные требования к производительности и безопасности. Также представляется возможным использование AES для построения криптосистемы, реализующей формирование защищенного канала связи. В июне 2003 года Агентство национальной безопасности США постановило, что шифр AES является достаточно надёжным, чтобы использовать его для защиты сведений, составляющих государственную тайну (classified information). Вплоть до уровня SECRET было разрешено использование ключей длиной 128 бит, для уровня TOP SECRET требуются ключи длиной 192 и 256 бит. С 2006 года все WiFi-устройства обязаны поддерживать новый стандарт WPA2, который использует алгоритм шифрования AES с 256-битным ключом. Поддержка AES (и только его) введена фирмой Intel в семейство процессоров x86 начиная с Intel Core i7-980X Extreme Edition.

Алгоритм представляет каждый блок кодируемых данных в виде двумерного массива байт размером 4x4, 4x6 или 4x8 в зависимости от установленной длины блока. AES-128, AES-192, AES-256 обрабатывают блоки данных за соответственно 10, 12 или 14 итераций.

Каждая итерация представляет собой определенную последовательность трансформаций. Под трансформациями понимаются перестановки и замены. Перестановка – это изменение порядка данных, а замена – замещение одного блока данных другим, данные преобразования производятся либо над независимыми столбцами, либо над независимыми строками, либо вообще над отдельными байтами в таблице. В AES используются следующие виды перестановок и замен: табличная подстановка 8x8 бит, сдвиг строк в двумерном массиве на различные смещения, математическое преобразование, перемешивающее данные внутри столбца, добавление материала ключа операцией XOR. В последнем раунде операция перемешивания столбцов отсутствует, что делает всю последовательность операций симметричной. Все преобразования в шифре имеют строгое математическое обоснование. Сама структура и последовательность операций позволяют выполнять данный алгоритм эффективно как на 8-битных так и на 32-битных процессорах. В структуре алгоритма заложена возможность параллельного исполнения некоторых операций, что на многопроцессорных рабочих станциях может еще поднять скорость шифрования в 4 раза.

На сегодняшний день не выявлено никакой эффективной атаки на данный алгоритм, кроме простого перебора ключей, вследствие чего разработка программных комплексов шифрования по стандарту AES является очень актуальным направлением в информационной безопасности. Подобный программный комплекс нашёл бы применение при практическом решении задач связанных с шифрованием в разнообразных приложениях, где предъявляются повышенные требования к производительности и безопасности.

Вараксин С.И.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ НАЗЕМНЫМ И ВОДНЫМ ТРАНСПОРТОМ

Проблема безопасности автоматизированных систем и информации остается актуальной на сегодняшний день. Каждый день разрабатываются новые механизмы, способы управления и защита продукта в технической среде. В том числе и транспорте.

По данным прогноза компании McAfee (занимающаяся разработкой защиты компьютерной безопасности; была основана в 1987 году; дочернее предприятие корпорации Intel) к 2020 году к внешней Сети будут подключены около 50 млрд. устройств. Из них львиную долю будут составлять встроенные устройства в транспортные средства: от магнитол до различных систем контроля. Следовательно, велика вероятность появления нового вида киберпреступлений: взлом охранной или управление автоматизированной системы транспорта с помощью программное обеспечение через GPS, Bluetooth, Wi-Fi.

На сегодняшний день ученые и специалисты тестируют запуск двигателей и других транспортных средств с помощью смартфона. Также исследователям Университета Сан-Диего удалось взломать охранную систему автомобиля с помощью ноутбука и Bluetooth. Ученые из Южной Каролины смогли вскрыть автомобиль благодаря бреши в системе датчиков давления.

Самыми уязвимыми местами в транспортах будут, несомненно, системы контроля над безопасностью. Именно здесь будут усиленно работать хакеры и взломщики. Дополнительную роль могут сыграть также следующие факторы: наличие погрешности приборов, показывающих полученную извне информацию, например, актуальное состояние пробок на дорогах, осуществляющих прокладку маршрута на карте как для наземного, так и для водного транспорта; принимающих информацию о надвигающемся шторме и т.д.

С уверенностью можно говорить о дальнейшем развитии транспортных систем, которое с одной стороны улучшит работу транспортного ПО, с другой – обусловит появление новых возможностей для взлома. В связи с последующим ростом потенциала уязвимости безопасности необходимо создавать и совершенствовать способы защиты автоматизированных систем транспорта.

Гомзяков В.М.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ГИДРОМЕТЕОРОЛОГИЧЕСКИХ ПРОГНОЗАХ

Построение нейронной сети есть не что иное, как попытка создания искусственной нервной системы, в состав которой входит человеческий мозг. Сами нейроны это десятки миллиардов элементарных объектов, которые за нас «думают», и исследователю в этой области необходимо понять, каким образом человеческий мозг обучается обрабатывать информацию и делать соответствующие выводы. Смысл существования нейронной сети заключается в обучении и адаптации. Можно назвать некоторые из широко известных областей, где эффективно работают так называемые нейросетевые технологии. Это страховая деятельность банков: прогнозирование банкротств, денежных потоков, налоговых поступлений; оценка кредитного риска, эффективности биржевой деятельности; предсказание результатов займов. Имеет смысл попытаться использовать нейронные технологии для составления гидрометеорологических прогнозов.

Погода является хаотической системой. Небольшие ошибки в исходных условиях прогноза могут быстро расти, и в итоге повлиять на качество прогноза. Кроме того, предсказуемость ограничивается моделью ошибок, связанных с приближенным характером моделирования атмосферных процессов в численных моделях. Эти два источника неопределенностей ограничивают точность прогнозов в отдельной точке, полученных в результате запуска численной модели даже с тщательно подобранными начальными условиями. Проблема прогноза погоды может быть описана в терминах временной эволюции соответствующей функции плотности вероятности в фазовом пространстве атмосферы. Оценка данной функции позволяет разработчикам прогноза объективно оценить неопределенность в точечных прогнозах. Ансамбль прогнозов служит для получения более сложных оценок функции плотности вероятности.

Нейронные сети позволяют оценить потенциально нелинейные модели без необходимости указывать точную функциональную форму. Ансамбль прогнозов является подходящим объектом для моделирования с помощью нейронных сетей, так как представляет собой нелинейную функцию некоторого количества переменных. Кроме того, часто большое количество данных доступны для моделирования ансамбля прогнозов, что является необходимым условием для эффективного использования нейронных сетей.

Исходные данные для нейронных сетей могут быть выбраны исходя из переменных, используемых в течение многих лет в обычных линейных регрессионных моделях. Кратко- и среднесрочные модели должны хорошо описывать сезонную и краткосрочную изменчивость. Для качественного учета авторегрессии следует также использовать сдвиговые переменные. В частности, рекомендуется брать сдвиги в один, пять и семь дней. Погодные переменные могут быть следующими: эффективная температура, скорость охлаждения и эффективность освещения.

Для оценки качества прогноза возможно использование метода хи-квадратов. Получаемые оценки следует сравнивать с соответствующими оценками, основанными на долгосрочных наблюдениях. Предполагается, что наиболее эффективно использовать нейронные сети для прогноза на срок от одного до десяти дней.

Иванова А.К.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ПЕРЕДАЧА ДАННЫХ ПОВЫШЕННОЙ НАДЕЖНОСТИ В КОРАБЕЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

Для корабельной информационной системы (КИС), как и для любой другой ИС, важно быть надёжной и безопасной. КИС разделяется на внутреннюю, когда речь идёт о компьютерах на корабле, каждый из которых подключён к главному корабельному серверу; и внешнюю, когда кораблю необходимо получить какую-либо информацию путём подключения ко внешним базам данных.

Внутренняя КИС представляет собой терминальную систему – один главный сервер и терминалы, расположенные в каютах, рубке, машинном отделении. Главный сервер защищён от вирусов, сбоев системы путём использования RAID, антивирусных программ; также настраиваются политики доступа. Защите подлежат не только терминальные серверы, но и сами терминалы. При этом необходимо контролировать доступ пользователя к портам ввода-вывода терминала с тем, чтобы запретить подключение неразрешенных внешних устройств, например, принтеров или флэш-дисков; также необходимо обеспечивать контроль целостности программных средств, с помощью которых пользователь взаимодействует с терминальным сервером. Кроме этого используются навесные средства защиты, обеспечивающие процедуры идентификации/аутентификации пользователей и создающие изолированную программную среду на тонком клиенте (терминале). Помимо данных способов защиты организовывается точечная защита тонких клиентов, если доступ к ним предоставлен не только сотрудникам организации.

Внешняя КИС нужна для обмена информацией судна с главным сервером организации и для объединения с другими территориально-удалёнными объектами. Для этого используется VPN канал. VPN сервера делает пребывание с сети свободным, конфиденциальным и безопасным, выступает в качестве посредника между пользователем компьютера и Интернетом. При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации. Подключение удаленных пользователей к VPN производится посредством сервера доступа (шлюза), который подключен как к внутренней, так и к внешней (общедоступной) сети. При подключении удаленного пользователя (либо при установке соединения с другой защищенной сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов, удаленный пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс авторизации с последующей авторизацией на сервере БД. Средства защиты информации – протоколы шифрования. Для реализации защиты передаваемой информации существует множество протоколов, которые защищают VPN, но все они подразделяются на два вида и работают в паре: протоколы, инкапсулирующие данные и формирующие VPN соединение; протоколы, шифрующие данные внутри созданного туннеля.

Существуют такие каналы передачи, как: GPS/GPRS, спутниковая связь, выделенный радиосигнал, Wi-Fi. Морская навигация так же, как и дорожная, осуществляется с применением GPS. GPRS позволяет пользователю сети сотовой связи производить обмен данными с другими устройствами в сети GSM и с внешними сетями, в том числе Интернет. При использовании спутникового канала защищенность секретных данных и сведений находится под угрозой, поскольку практически каждый спутниковый канал может систематически прослушиваться и обрабатываться. Избежать всего этого можно только используя последовательное шифрование всех передаваемых данных и сведений. Оператор спутниковой связи передает все данные исключительно по собственным каналам, при этом используются средства встроенной шифрации как на программном, так и аппаратном уровнях. Пользователей сети Wi-Fi также может подстерегать несколько опасностей, например: перехват трафика администратором, прослушивание посторонними лицами, атака со стороны сетевых червей, возможность взлома и прослушивания трафика непосредственно с радиоканала. Для защиты возможно использование регулировки мощности передатчика, что позволяет ограничить «видимость» беспроводной сети злоумышленниками. Наиболее надёжными системами передачи данных являются оптические системы. Например, при лазерной технологии передачи перехватить сигнал можно только установив сканеры-приемники непосредственно в узкий луч от передатчиков. Таким образом, реальная сложность выполнения этого требования делает перехват данных практически невозможным, разнообразные собственные протоколы передачи данных обеспечивают дополнительную конфиденциальность.

С развитием новейших информационных технологий, возможностей связи и передачи данных растет вероятность перехвата конфиденциальной информации, возможность вмешательства в работу информационных систем. Все это является стимулом для постоянного развития информационной безопасности.

Котяхова А.Ю.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ПРИМЕНЕНИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В ДОКУМЕНТООБОРОТЕ ВУЗА (НА ПРИМЕРЕ РГГМУ)

В российских вузах используется значительный объем документов, которые необходимо оперативно регистрировать и обрабатывать. Поэтому внедрение системы электронного документооборота (СЭД) оптимизирует ведение документации и позволяет перевести работу ВУЗа на современный технический уровень. Благодаря новой системе упрощается персонифицированный учет, назначение стипендий, процессы зачисления, восстановления или отчисления студентов и другие организационно-учебные процессы.

Одной из важных задач, после внедрения электронного документооборота, является обеспечение юридической силы документов. В соответствии с законом об использовании электронной цифровой подписи (ЭЦП), стало возможным придание электронным документам юридического статуса. Кроме этого, применение ЭЦП имеет большие преимущества, такие как:

– защиту от изменения (подделки) документа: любое изменение документа делает подпись недействительной, так как она соответствует только исходному состоянию документа;
– контроль целостности;
– подтверждение авторства документа;
– невозможность отказа от авторства;
– ЭЦП уникальна для каждого документа и не может быть перенесена на другой документ.

Таким образом, можно быть уверенным в авторстве документа, а также в том, что текст документа не был изменен.

На данный момент наиболее распространены ЭЦП на основе алгоритмов ассиметричного шифрования. Эта схема цифровых подписей содержит в себе следующие этапы:

– генерация ключа;
– формирование подписи;
– проверка документа на подлинность ЭЦП.

Для получения открытого ключа используется система распределения – инфраструктура открытых ключей (PKI), которая основана на сертификатах, выдаваемых Удостоверяющим центром. Цифровой сертификат содержит в себе открытый ключ, данные для идентификации владельца и дополнительную информацию. В основе PKI лежит несколько принципов:

– закрытый ключ известен только его владельцу;
– все стороны доверяют удостоверяющему центру;
– удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

Таким образом, использование ЭЦП позволит:

– гарантировать достоверность документации;
– значительно сократить время, затрачиваемое на ведение и обмен документацией;
– усовершенствовать процедуры поиска, учета и хранения документов.

На сегодняшний день вряд ли получится полностью отказаться от использования традиционного метода ведения документооборота, но внедрение СЭД может значительно оптимизировать работу с документацией.

Силин П.И.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

СОВМЕСТНОЕ ИСПОЛЬЗОВАНИЕ СИММЕТРИЧНЫХ И АССИМЕТРИЧНЫХ КРИПТОСХЪЕМ ДЛЯ ЗАЩИТЫ TCP СОЕДИНЕНИЙ

На сегодняшний день актуальным остается вопрос об использовании различных методов шифрования данных для обеспечения их защиты от несанкционированного доступа. Это важное условие при передаче информации через открытые каналы связи. При этом канал связи должен обеспечивать высокую скорость шифрования, а также защиту от известных криптоатак.

Разработано программное обеспечение, с помощью которого можно осуществить связь между двумя компьютерами в локальной сети путем передачи текстовых сообщений в режиме реального времени через протокол TCP/IP. Для обеспечения безопасности канала, был использован симметричный криптографический алгоритм шифрования IDEA. Данный алгоритм требует наличие секретного канала связи для передачи ключа. Для решения этой задачи был использован двухключевой алгоритм RSA. Низкая скорость шифрования не позволяет алгоритму шифровать большие сообщения, однако его можно использовать для передачи ключа другого более быстрого алгоритма, в данном случае IDEA. Это позволяет клиенту и серверу шифровать сообщения со скоростью около одного миллиона символов в секунду на современных компьютерах. Такая скорость обеспечивает мгновенную доставку сообщений.

Программа поддерживает два режима работы:

1. Создание сервера.
2. Подключение к серверу.

При этом клиент может самостоятельно вводить IP адрес сервера. При отключении сервера или клиента ключи удаляются, и, если устанавливается новое соединение, то они генерируются вновь и используются для шифрования последующих сообщений. Также пользователь имеет возможность изменять отображающее его имя.

Общую схему работы программы можно представить в виде:

– на первом этапе получатель сообщает отправителю открытый ключ RSA;
– отправитель высылает получателю зашифрованный по RSA ключ IDEA;
– отправитель высылает получателю зашифрованной по IDEA сообщение.

Программное обеспечение разработано на языке C++ Builder и обладает удобным интерфейсом.

В дальнейшем планируется добавить возможность передачи файлов, защищенных шифрованием или цифровой подписью, добавить возможность многоканальной связи, а также увеличить размер ключа для повышения ее криптостойкости.

Татарникова Т.М.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ОБЗОР МЕТОДОВ ЗАЩИТЫ САЙТОВ

Доступность и популярность Интернета породили огромную и пока неразрешенную проблему защиты сайтов. Сегодня сайты представляют собой концентрированное выражение человеческой мысли, то есть результат интеллектуальной деятельности в различных областях деятельности. Другими словами интеллектуальную собственность. В первую очередь это области программирования, дизайна, маркетинга, логики, а также инновации в соответствующих областях деятельности. С практической точки зрения вся эта ценность очень слабо защищена, в том числе по вине авторов и собственников сайтов.

Посягательства на сайт осуществляются различными методами. Среди них можно выделить следующие:

– Хакерские атаки, вирусы и вредоносные программы, взлом сайта.
– Специальные приемы интернет-маркетинга.
– Кража программного, текстового и графического контента.

Для защиты от хакеров, вирусов, взлома сайта используются специальные программы.

К специальным приемам интернет-маркетинга относятся приемы, приводящие к понижению рейтинга сайта и его популярности. Это так называемый черный пиар – распространение ложной информации и рекламы, фальшивые объявления, создание клонов сайта, неверные ссылки. Защита сайта очень трудная задача и подразумевает специальную тактику и стратегию. Общий смысл интернет-маркетинга заключается в повышении рейтинга и популярности своего сайта.

Противостоять краже контента можно программными средствами и юридически с помощью норм авторского права.

Защита от кражи содержания сайта программными средствами заключается в основном в предотвращении возможности выделения и копирования контента сайта.

В любом случае, какая бы техническая или организационная защита не осуществлялась, встает вопрос о правовом статусе защиты интеллектуальной собственности сайтов.

Интеллектуальная собственность сайтов – программная составляющая, текстовое содержание, графические материалы охраняются нормами авторского права, изложенными в IV части Гражданского кодекса РФ. Это означит, что законом охраняются авторские права на совокупность контента сайта (и его составляющие) в случае его творческого содержания в различных объективных формах представления – в виде текста, графических изображений, программного содержания, аудио, видио. В этом вопросе содержатся две проблемы – авторство и доказательство.

Автор тот, творческим трудом которого создано произведение. На практике авторство доказывается фиксацией наличия произведения на данную дату с помощью третьих лиц. Под произведением следует понимать контент сайта. Контент или его составляющие могут быть представлены в текстовой, графической, электронной форме, в том числе и в виде программных кодов. В настоящее время используют следующие методы фиксации авторских прав на сайт:

– Регистрация программного кода сайта.
– Депонирование контента сайта в текстовой, графической, электронной форме.
– Нотариальное заверение контента в той или иной форме.
– Свидетельские показания.
– Отправка самому себе заказного письма с содержанием контента сайта.

Каждый из указанных методов имеет свои достоинства и недостатки. Но общим недостатком являются отсутствие доступности или труднодоступность к депонированному или зарегистрированному материалу и трудность представления доказательств.

Несмотря на богатую практику доказательства авторских прав с помощью регистрации среди авторов и в литературе до сих пор идет дискуссия о полезности, целесообразности и правомочности. Вопросы полезности и целесообразности разрешаются практикой применения. Если на протяжении многих лет регистрация осуществляется и это используется для доказательств, то это полезно и целесообразно. Что касается регистрации, то она разрешена законом для «программ для ЭВМ», а программы тоже относятся к объектам авторского права.

Необходимо отметить, что ни один из известных методов защиты не позволяет достаточно надежно защитить сайт. Повышение степени надежности защиты достигается использованием комплекса методов – технических и правовых. Следует использовать специальные программные и технические методы и одновременно позаботиться об юридических основаниях доказательства авторского права. К вопросам защиты надо подходить комплексно.

Татарникова Т.М., Яготинцева Н.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ПРИНЦИПЫ ОРГАНИЗАЦИИ ЭКСПЕРТНОЙ СИСТЕМЫ ВЫБОРА НАДЕЖНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Положения, содержащиеся в стандарте ИСО 17799, позволяют получить оценку соответствия системы защиты информации предъявляемым требованиям. Общая оценка складывается из «взвешенных» коэффициентов по отдельным направлениям. «Вес» для каждого направления определяется экспертом-аналитиком на этапе обследования предприятия. При этом учитывается различие в требованиях к защите информации в государственных, финансово-кредитных, коммерческих, телекоммуникационных и других организациях. Учитывается также стадия жизненного цикла, на которой находится информационная система: проектирование, ввод в действие или эксплуатация.

Очевидно, что нарушители (источники угроз) обладают разными возможностями для реализации своих замыслов и имеют разную степень заинтересованности в достижении цели, то есть угрозы различаются по степени опасности. Специфика и конкретные условия проявления угроз учитываются в модели нарушителей.

Модель нарушителя общего вида может быть представлена в виде четырех компонент:

– организация нападения на информационный ресурс (зависит от заинтересованности нарушителя, связей и принадлежности нарушителя к криминальной группе);

– технология доступа к информационному ресурсу (определяется квалификацией нарушителя, возможностями технологического планирования атаки, используемыми методами);

– технические и интеллектуальные ресурсы (определяются технической оснащенностью и сторонней поддержкой);

– разведка параметров и уязвимостей (определяется способами получения исходных сведений).

Модель нарушителя является многопараметрической. Применение методов нечеткой логики позволяет увеличивать число учитываемых параметров и сделать модель более приспособленной к конкретному случаю и варианту защиты.

На основе этой модели можно выполнить оценку потенциала нарушителя.

Для оценки наносимого ущерба также используется качественная шкала, например пятиуровневая:

– малый уровень ущерба - приводит к незначительным потерям материальных средств и ресурсов, которые быстро восполняются;

– заметный уровень ущерба – приводит к заметным потерям материальных активов, существенному влиянию на репутацию компании;

– большой уровень ущерба – приводит к большим потерям материальных активов или ресурсов или наносится большой урон репутации компании и ее интересам;

– критический уровень ущерба – наносится значительный урон репутации компании и ее интересам, что может представлять угрозу для компании и продолжения ее бизнеса;

– катастрофический уровень ущерба – приводит к разрушительным последствиям и невозможности ведения бизнеса.

Введенные уровни ущерба и риска далее могут быть использованы при формировании правил вывода экспертной системы, позволяющей автоматизировать процесс выбора надежных средств защиты информации.

При формировании правил вывода необходимо также определить вероятность успешной атаки. Допустим, что для представления вероятности несанкционированного доступа (НСД), используется также пятиуровневая шкала, содержащая уровни:

A – событие практически никогда не происходит;

B – событие случается редко;

C – событие вполне возможно;

D – событие, скорее всего произойдет;

E – событие обязательно произойдет.

При обосновании правил вывода будем исходить из следующих предположений. Предположим, что, если эффективность защиты выше потенциала нарушителя, вероятность успешной атаки соответствует уровню ***A***. Если эффективности защиты равна потенциалу нарушителя, то вероятность успешной атаки соответствует уровню ***B***. Наконец, если эффективность защиты меньше потенциала нарушителя, то вероятность НСД будет тем выше, чем больше превышение потенциала нарушителя над эффективностью защиты (уровни ***C***, ***D*** и ***E***).

Таким образом, такая логическая модель позволяет оценить вероятность успешной атаки в зависимости от потенциала угрозы и эффективности защиты.

Татарникова Т.М., Яготинцева Н.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ИЗБИРАТЕЛЬНЫЙ И ОБЯЗАТЕЛЬНЫЙ ПОДХОДЫ К ВОПРОСУ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

В современных системах управления базами данных (СУБД) поддерживается один из двух наиболее общих подходов к вопросу обеспечения безопасности данных: избирательный подход и обязательный подход. В обоих подходах единицей данных или «объектом данных», для которых должна быть создана система безопасности, может быть как вся база данных (БД) целиком, так и любой объект внутри БД.

Эти два подхода отличаются следующими свойствами.

В случае обязательного управления, наоборот, каждому объекту данных присваивается некоторый классификационный уровень, а каждый пользователь обладает некоторым уровнем допуска. При таком подходе доступом к определенному объекту данных обладают только пользователи с соответствующим уровнем допуска. Такой подход имеет место в организациях с жесткой структурой управления, например, правительственных, военных и т.д.

В случае избирательного управления некоторый пользователь обладает различными правами (привилегиями или полномочиями) при работе с данными объектами. Разные пользователи могут обладать разными правами доступа к одному и тому же объекту. Избирательные права характеризуются значительной гибкостью и находят большее применение.

Для реализации избирательного принципа предусмотрены следующие методы.

В базу данных вводится новый тип объектов БД – это пользователи. Каждому пользователю в БД присваивается уникальный идентификатор. Для дополнительной защиты каждый пользователь кроме уникального идентификатора снабжается уникальным паролем, причем если идентификаторы пользователей в системе доступны системному администратору, то пароли пользователей хранятся чаще всего в специальном кодированном виде и известны только самим пользователям.

Пользователи могут быть объединены в специальные группы пользователей. Один пользователь может входить в несколько групп. Для каждой группы определен набор привилегий.

Привилегии или полномочия пользователей или групп пользователей – это набор действий (операций), которые они могут выполнять над объектами БД.

В последних версиях ряда коммерческих СУБД появилось понятие «роли». Роль – это поименованный набор полномочий. Пользователю может быть назначена одна или несколько ролей.

Объектами БД, которые подлежат защите, являются все объекты, хранимые в БД: таблицы, представления, хранимые процедуры и триггеры. Для каждого типа объектов есть свои действия, поэтому для каждого типа объектов могут быть определены разные права доступа.

На самом элементарном уровне концепции обеспечения безопасности баз данных исключительно просты. Необходимо поддерживать два фундаментальных принципа: проверку полномочий и проверку подлинности (аутентификацию).

Проверка полномочий основана на том, что каждому пользователю или процессу информационной системы соответствует набор действий, которые он может выполнять по отношению к определенным объектам. Проверка подлинности означает достоверное подтверждение того, что пользователь или процесс, пытающийся выполнить санкционированное действие, действительно тот, за кого он себя выдает.

Система назначения полномочий имеет в некотором роде иерархический характер. Самыми высокими правами и полномочиями обладает системный администратор или администратор сервера БД. Традиционно только этот тип пользователей может создавать других пользователей и наделять их определенными полномочиями.

СУБД в своих системных каталогах хранит как описание самих пользователей, так и описание их привилегий по отношению ко всем объектам.

Далее схема предоставления полномочий строится по следующему принципу. Каждый объект в БД имеет владельца – пользователя, который создал данный объект. Владелец объекта обладает всеми правами-полномочиями на данный объект, в том числе он имеет право предоставлять другим пользователям полномочия по работе с данным объектом или забирать у пользователей ранее предоставленные полномочия.

Ткаченко Г.Н.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ПОСТРОЕНИЕ ЗАЩИЩЕННОЙ СЕТИ ВУЗА (НА ПРИМЕРЕ РГГМУ)

Для построения эффективно защищенной сети ВУЗа необходимо применять комплексную защиту от внешних угроз системы, так как атаки можно ожидать не только извне, но и из локальной сети, так ВУЗ оборудован компьютерными классами со свободным доступом.

Первым этапом защиты сети является брандмауэр или межсетевой экран, который является программой (или неотъемлемой частью операционной системы) контролирующей входящие и исходящие потоки данных при подключении к общедоступной сети связи (например, Интернет).

Для более эффективного контроля процесса обмена информацией и мониторинга подключения посторонних устройств внутри локальной сети целесообразно использовать управляемые свитчи, которые будут отслеживать передачу пакетов данных согласно mac адресу и порту доступа, а также VPN технологию, которая позволяет обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

Также необходимо использовать комплексные системы обнаружения атак (к которым относятся системы обнаружения несанкционированного доступа, сканеры уязвимости и т.д.) в связи с тем, что изменение сети (появление новых рабочих станций, реконфигурация программных средств и т.д.) может привести к появлению новых уязвимых мест, угроз и возможностей атак как на информационные ресурсы, так и на систему защиты.

Необходимо разграничение прав доступа к информационным ресурсам, посредством объединения пользователей в определённые группы и подгруппы, обладающие разными правами и уровнями доступа.

Контроль доступа к особо ценным данным следует устанавливать с использованием защиты информации на файловом уровне, которая позволяет скрыть их путём кодирования содержимого файлов, каталогов и дисков. Доступ к данной информации осуществляется по предъявлению ключа, который может вводиться с клавиатуры, храниться и предоставляться со смарт-карты, HASP- или USB- ключей и прочих е-токенов.

В связи с наличием во внешних сетях огромного количества вирусов и прочих вредоносных программ, необходимо, чтобы сеть ВУЗа была защищена специализированным антивирусным комплексом, который будет производить поиск и уничтожение известных или неизвестных (с помощью эвристических механизмов поиска) вирусов, и блокировку проявления вирусов.

Подобная совокупность методов позволяет обеспечить максимальную защиту локальной сети ВУЗа на данный момент.

Ткаченко Н.Н., Александрова Л.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ЗАЩИТЫ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ И ГИДРОМЕТЕОРОЛОГИЧЕСКИХ БАЗ ДАННЫХ

Ценность гидрометеорологической информации, будь то метеорологические прогнозы обеспечения авиации и судов, прогноз ледовой обстановки в Арктике или вовремя предсказанное наводнение, представляет значительную государственную и общественную ценность. Геопространственное моделирование является одним из перспективных направлений, развиваемых в Российском государственном гидрометеорологическом университете. Особую актуальность оно приобретает в связи со строительством «Северного потока», а так же вводом в эксплуатацию новых портовых и нефтеналивных сооружений. Мониторинг, выявление и ликвидация возможных техногенных катастроф неосуществимы без развития инновационных технологий в области геоинформатики и организации геоинформационных систем (ГИС). Подобные системы позволяют проводить комплексный анализ состояния вод, в который входят: оперативное наблюдение за течениями, волнами, изменениями в морфологической структуре прибрежной зоны, качеством воды и переносом загрязнений, а также возможностью выявления антропогенных катастроф и подводного терроризма. Для создания и развития геоинформационной системы района Балтийского моря необходимо использовать гидрометеорологические данные из различных источников. Это могут быть:

- изображения земной поверхности, полученные со спутников;
- данные численного моделирования;
- данные полевых наблюдений;
- архивные данные и т.д.

Точность и эффективность работы ГИС зависит от качества входящей информации, иными словами должны быть предусмотрены средства и методы защиты передаваемой гидрометеорологической информации.

Выходные данные подобной геоинформационной системы могут быть как гражданского назначения (прогноз ледовой обстановки, штормовые предупреждения и пр.), так и для служебного пользования. Организации, составляющие прогнозы должны быть уверены в том, что информация доходит до потребителей без искажений (как случайных, так и искусственно внесенных). В некоторых случаях, государство должно иметь возможность закрывать отдельные гидрометеорологические данные и прогнозы. Для этих целей должны быть использованы новейшие методы защиты информации такие как: организация выделенных каналов для обмена информацией с использованием шифрования высокой степени криптографической стойкости, использование СУБД и клиент-серверных систем для хранения и доступа к информации, позволяющих гибко настраивать права доступа локальных и удалённых пользователей и групп пользователей к данным и любым локальным устройствам, что обеспечивает существенное снижение риска утечек как через устройства, подключаемые к внешним портам (USB, LPT, COM, IrDA, PCMCIA, IEEE 1394 и т.д.), так и через внутренние устройства (сетевые карты, модемы, Bluetooth, Wi-Fi, CD/DVD-дисководы и т. д.). Установка активного и пассивного сетевого оборудования в банке данных, позволяющего на физическом уровне управлять использованием сети – ограничивать нежелательный трафик внутри сети и попытки несанкционированного доступа извне. Использование IDS (intrusion detection system) и IPS (intruision prevention system) для обнаружения и предотвращения атак, которые обошли Firewall, и оповещения администратора сети, который, в свою очередь, предпримет дальнейшие шаги по предотвращению атаки. Также предполагается использование гибридного контент-анализа, позволяющего анализировать все данные, передаваемые за пределы локальной сети организации банка данных, и позволяет предотвращать утечки определенной информации по сетевым каналам в т.ч. через электронную почту, социальные сети, интернет-мессенджеры и т. д. и детального аудита доступа к данным как таковым и системе хранения и передачи данных в целом. Подобный аудит ещё на ранней стадии обнаруживает подозрительную активность, что позволяет дополнительно сократить риски утечки данных.

Устинов И.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

АППАРАТНОЕ ШИФРОВАНИЕ DES

Необходимость в шифровании всегда будет присутствовать в таких отраслях жизни общества как финансовая, военная, корпоративная. Если есть спрос на шифрование как таковое, то будет и предложение, выраженное в различных алгоритмах и методах оного. В данной статье я рассмотрю такие понятия как «алгоритм шифрования DES», аппаратное шифрование, и аппаратные средства обеспечивающие данный вид шифрования. DES (Data Encryption Standard) – симметричный алгоритм шифрования, разработанный фирмой IBM и утвержденный правительством США в 1977 году как официальный стандарт (FIPS 46-3). DES имеет блоки по 64 бита и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит. Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований. Так как объяснение самого алгоритма займет слишком много времени выделим основную черту, важную для любого криптографического шифрования, а именно:

Криптостойкость. Для криптостойкости алгоритма должны быть соблюдены следующие условия:

- Каждая строка каждого блока должна быть перестановкой множества {0, 1, 2, …, 15}
- S-блоки не должны являться линейной или афинной функцией своих аргументов
- Изменение одного бита на входе S-блока должно приводить к изменению по крайней мере двух битов на выходе.

Из-за небольшого числа возможных ключей (всего 2^{56}), появляется возможность их полного перебора на быстродействующей вычислительной технике за реальное время. В 1998 году Electronic Frontier Foundation используя специальный компьютер DES-Cracker, удалось взломать DES за 3 дня. Так же чтобы увеличить криптостойкость DES существует несколько его вариантов: double DES (2DES), triple DES (3DES), DESX, G-DES.

На сегодняшний день наиболее применимы три вида шифраторов: программные, аппаратные и программно-аппаратные. Основные различия заключается не только в способе реализации шифрования и степени надежности защиты данных, но и в цене. Наиболее дешевыми средствами шифрования данных являются программные, затем идут программно-аппаратные и самые дорогостоящие – аппаратные. Несмотря на то, что цена программных шифраторов существенно ниже, разница в цене не сравнима со значительным повышением качества защиты информации при применении аппаратных средств. Все большее количество средств шифрования данных создается в виде специализированных физических устройств. Программные шифраторы и в ряде случаев способны обеспечить большую скорость обработки информации, однако этим, пожалуй, список их преимуществ исчерпывается.

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

МЕТОДИКА И ПРАКТИКА ПРОВЕДЕНИЯ МАСТЕР-КЛАССОВ ПРИ ПОВЫШЕНИИ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ

Подготовка и переподготовка кадров в области обеспечения информационной безопасности в настоящее время характеризуется широкомасштабностью и системностью проведения комплекса учебно-методических мероприятий, обеспечивающих достаточно качественную реализацию требований государственных образовательных стандартов по широкому спектру специализаций.

Проблема нетрадиционно большого объёма разнородной и разнокачественной информации, с которой специалистам в области обеспечения информационной безопасности (ИБ) приходится работать в поиске эффективных проектных и управленческих решений (ПУР), а также сложность выбора при создании систем безопасности и, особенно, систем комплексной защиты информации (СКЗИ) предпочтительных, а тем более оптимальных ПУР, побуждает при подготовке и переподготовке кадров искать новые и наиболее эффективные формы обучения.

Такими формами, в том числе для объектов морской инфраструктуры, сложных автоматизированных комплексов, СКЗИ и систем специального назначения, являются специализированные практические занятия с отработкой технологических приёмов защиты информации, деловые игры с моделированием процессов поиска проектных решений, ситуаций сетецентрического противоборства, а также проведение круглых столов и мастер-классов.

Так среди апробированных тем деловых игр хорошо себя зарекомендовали: «Тендер на получение специального заказа», «Программа внедрения новой информационной технологий», «Доклад Главному конструктору проекта по выбору оптимальной архитектуры и основных характеристик СКЗИ», «Оптимальная система электронного документооборота в защищённом исполнении для проектной (судостроительной, учебной) организации», «Аналитическая справка по базовым IS-технологиям для Объединённой судостроительной корпорации», «Презентация продукции Компании на международном IS-форуме», «Защита персональных данных порта» и т.п.

Высшей формой переподготовки кадров категории «Главный специалист-начальник отдела комплексной защиты информации», «Руководитель организации» и т.п. следует считать проведение мастер-классов. Опыт проведения ряда мастер-классов позволяет определить эту форму подготовки следующим образом. Мастер-класс – (от англ. masterclass: master – лучший в какой-либо области + class – занятие, урок) – современная форма проведения обучающего тренинга-семинара для отработки практических навыков по различным методикам и технологиям с целью повышения профессионального уровня и обмена передовым опытом участников, расширения кругозора и приобщения к новейшим областям знания. Мастер-класс (МК) отличается от специализированного для ведущих специалистов семинара тем, что, во время мастер-класса ведущий МК (мастер) рассказывает и, что еще более важно, показывает, как применять на практике новую технологию или метод.

Тем самым целенаправленно реализуется принцип личностно-ориентированного обучения участников МК в предметной области. Например, обоснования технологий выбора и принятия оптимальных решений в тендерных закупках и инвестиционных проектах на основе ознакомления с аналитическими обзорами и авторскими методами ведущих-мастеров, передачи ими своего опыта, совместной отработки результативных методик и подходов, обсуждения лучших практик, специфических вопросов и предложений участников МК. Кроме того, мотивирования осознанной деятельности участников МК на: повышение уровня личной теоретической и методической подготовки; профессиональное совершенствование и саморазвитие участников МК; их готовность к развитию собственной деятельности на научной основе; активизацию деятельности в процессе собственной практики; обеспечение высокой результативности и целеустремлённости.

При этом, следует особо подчеркнуть важность качественной подготовки МК ведущим (мастером) и его проведения, максимально полного использования в ходе МК наряду с полномасштабным использованием мультимедийных технологий действующих нормативных

документов, реально исполненных документов, реализованных программ, актов комиссий. При этом, с системной точки зрения одним из важнейших методических аспектов следует считать обучение участников МК и передача им опыта, вытекающего из лучших практик в данной предметной области.

Особый динамизм, как показывает практика, в проведение МК вносит правильный подбор мастеров (ведущих) с учётом их личностных качеств, уникального уровня профессионализма и опыта проведения групповых учебных занятий. Кроме того, предметного и высоко профессионального обсуждения различных аспектов государственной политики обеспечения ИБ как отдельных объектов информатизации, так и регионов в целом, а также правовых аспектов и судебной практики обеспечения ИБ. Безусловно, на основе глубокого анализа технологических особенностей обеспечения ИБ, практического ознакомления с возможностями современных средств защиты информации, в том числе в телекоммуникационных сетях, в критических инфраструктурах и ключевых объектах автоматизации.

Барабаш П.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

О ПОДГОТОВКЕ КАДРОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Одним из серьезных препятствий на пути реализации № 152-ФЗ «О персональных данных» является отсутствие квалифицированных кадров. Мероприятия по обеспечению безопасности обработки персональных данных (далее ПДн) технически сложны, требуют высокой квалификации исполнителей, специальных знаний, глубокого понимания сущности процессов обработки и средств защиты информации.

Российские компании обрабатывают огромный объем данных, доступ к которым имеют корпоративные подразделения и департаменты. В большинстве случаев отсутствие контроля приводит к высоким рискам утечки ПДн.

Учитывая эти обстоятельства, на факультете информационных технологий Смольного института Российской академии образования для студентов специальности 090105 (075500) «Комплексное обеспечение информационной безопасности автоматизированных систем» в разделе «Специальные дисциплины» в течение трех лет читается учебная дисциплина: «Защита информации в информационных системах персональных данных».

В 2011-2012 учебном году Смольный институт Российской академии образования приступил к подготовке бакалавров по направлениям подготовки, отвечающим Федеральным государственным образовательным стандартам высшего профессионального образования третьего поколения.

Учебная дисциплина «Защита информации в информационных системах персональных данных» введена в рабочие учебные планы всех форм обучения: по направлению подготовки бакалавров 090900 «Информационная безопасность», в цикл профессиональных дисциплин по выбору; по направлению подготовки бакалавров 230400 «Информационные системы и технологии», в цикл профессиональных дисциплин по выбору; по направлению подготовки бакалавров 230100 «Информатика и вычислительная техника», в цикл профессиональных дисциплин по выбору. Элементы этой учебной дисциплины предполагается ввести в раздел курса «Гуманитарные аспекты информационной безопасности» в качестве отдельного модуля.

В институте реализуется программа дополнительного профессионального образования «Организация и техническое обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных» объемом 74 часа, включающая следующие разделы:

– правовые и организационно-распорядительные документы в области обеспечения безопасности ПДн, обрабатываемых в информационных системах персональных данных (ИСПДн);

– структура, задачи и функции государственной системы технической защиты информации.

Задачи и функции государственной системы технической защиты информации в области обеспечения безопасности ПДн при их обработке в ИСПДн;

– порядок выявления угроз безопасности ПДн при их обработке в ИСПДн;

– типовые модели угроз безопасности ПДн, обрабатываемых в ИСПДн;

– мероприятия по организации обеспечения безопасности ПДн;

– мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн;

– перечень, содержание и порядок разработки организационно-распорядительных документов по защите ПДн, обрабатываемых в ИСПДн.

Принятые институтом решения позволяют познакомить студентов и слушателей курсов повышения квалификации с задачами, вытекающими из реализации № 152-ФЗ «О персональных данных».

Барабаш П.А., Советов Б.Я.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

О НАУЧНО-МЕТОДИЧЕСКОМ ОБЕСПЕЧЕНИИ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СРЕДЫ СИСТЕМЫ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Современный этап развития отечественного образования обусловил выход проблемы формирования безопасной информационной среды системы профессионального образования на приоритетные направления исследований не только в области психологии, философии, социологии, но и педагогики. Переход образовательных учреждений высшего профессионального образования от регламентированной линейной - к пространственной организации образовательной среды, обеспечивающей самоактуализацию и продуктивную самореализацию студентов, актуализировал необходимость поиска оснований для ее модернизации, способствующих повышению качества и безопасности.

Концепция национальной безопасности Российской Федерации, Закон РФ «О безопасности» рассматривают безопасность как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Понятие “безопасность” рассматривается нами в качестве педагогической категории как защищенность жизненно важных образовательных потребностей и интересов субъектов образования, в нашем случае студентов и преподавателей технических вузов, в различных сферах педагогической деятельности от внутренних и внешних угроз, обеспечивающую устойчивость и качество образования в условиях перехода к информационному обществу.

Вместе с тем, существует иной аспект безопасности образования, связанный с регуляцией опасностей и рисков не только по отношении к личности, но и к государству, обществу, самому образовательному учреждению. Этот подход имеет собственно образовательный, социокультурный смысл, ориентированный на предупреждение источников опасностей и рисков снижения качества образования педагогически целесообразными средствами.

Целью исследования является выявление условий безопасной реализации модернизации информационной среды системы профессионального образования при реализации Россией решений Болонской конвенции.

В частности, актуально выявить теоретические основания и принципы безопасной реализации структурно-функциональной модели безопасной информационной среды, включающей в себя два уровня защиты от угроз и рисков – внешнего и внутреннего. Внешний уровень – нормативный, внутренний - ценностно-смысловой, определяющий ценностно-ориентационное единство субъектов образования по отношению к смыслам, целям профессионального образования и ценностям, значимым для обеспечения качества подготовки и защиты образовательных потребностей субъектов от возможных угроз и рисков.

В докладе рассмотрены основные задачи, которые необходимо решить в рамках Болонского процесса, в частности, ввод системы модулей и кредитных единиц, создание объективной системы оценки качества образования и т. д.

Делается вывод об угрозе потери системного образования, что неизбежно приводит к снижению уровня массового образования, а в перспективе – к потере гражданами Российской Федерации возможности получения бесплатного высшего образования. Это в свою очередь может привести к глубокому расслоению общества по образовательному уровню (наряду с экономическим) и как следствие – к социальной нестабильности, представляющей серьезную угрозу для национальной безопасности Российской Федерации.

Давлеткиреева Л.З.
Россия, Магнитогорск, Магнитогорский государственный университет

ПОДГОТОВКА НАУЧНО-ПЕДАГОГИЧЕСКИХ КАДРОВ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИКТ-НАСЫЩЕННОЙ СРЕДЕ

Современное понимание информационной безопасности (ИБ) Российской Федерации (РФ) как совокупности сбалансированных интересов личности, общества и государства, нахождение их оптимального баланса в информационной сфере, обеспечение защиты жизненно важных интересов в информационной сфере от внутренних и внешних угроз представлено в Доктрине ИБ РФ. Однако, несмотря на чрезвычайную важность данной проблемы для современного общества, для сферы науки и образования мы все-таки не можем говорить о существовании целостного подхода к ее решению.

Реализация Стратегии развития информационного общества в России, выполнение Федеральной Целевой Программы «Электронная Россия (2002–2011 годы), Приоритетного национального проекта «Образование» и целого ряда Федеральных целевых программ обеспечивает доступность электронных информационных ресурсов (ЭИР) практически для каждого студента, преподавателя, аспиранта и молодого ученого в России. Однако, как показывает опыт, оснащение научных и образовательных учреждений вычислительной техникой, программным обеспечением,

повсеместное подключение к глобальной сети Интернет еще больше обостряет вопросы, связанные с обеспечением ИБ. Очевидно, что в сфере защиты информационной инфраструктуры сферы науки и образования сегодня существуют определенные проблемы.

Использование ЭИР в научной и образовательной деятельности актуализирует проблему, связанную с необходимостью формирования культуры информационного общества, компонентом которой является безопасное применение информациионно-коммуникативных технологий (ИКТ) в науке и образовании. Наряду с программно-техническими аспектами характерными для обеспечения ИБ научных исследований (технологии безопасного хранения, обработки и использования научных данных; защита средств взаимодействия, устройств передачи и распределения научно-образовательной информации и др.), немаловажными являются и гуманитарные задачи (сохранение и развитие культурно-нравственных ценностей в условиях глобализации экономической, социально-политической и духовной жизни общества; соблюдение этических и академических норм при использовании ЭИР в науке и образовании; оценка возможных рисков нарушения безопасности ИКТ-насыщенной среды; исследование проблем противодействия злоупотреблениям свободой распространения информации в сети Интернет и др.).

Однако решение проблемы обеспечения ИБ в сфере науки, образования и высоких технологий, невозможно без необходимого и достаточного количества высококвалифицированных научно-педагогических кадрах компетентных не только в программно-технической сферах, но и в гуманитарных аспектах. Неотложность принятия специальных мер по обучению кадров основам ИБ прямо отмечается в Федеральной целевой программе «Электронная Россия», формирование ИКТ-компетентности в «Национальной доктрине образования в РФ», «Концепции Федеральной целевой программы развития образования на 2006-2011 годы», «Концепции модернизации российского образования на период до 2011 года» и др.

На основании вышесказанного, мы сформулировали проблему научно-исследовательского проекта, поддержанного РГНФ, №11-06-01006а «Разработка и апробация модели подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде».

Актуальность проблемы обусловлена:

1. Возросшей потребностью в специалистах, владеющих современными методами и средствами защиты информационных структур в системе открытого информационного пространства науки и образования;
2. Недостаточной теоретико-методологической разработанностью оснований подготовки, повышения профессиональной и научной квалификации и переподготовки научно-педагогических кадров в данной области;
3. Возрастающей потребностью науки и образования в педагогах-исследователях, которые обладают устойчивой компетентностью в области обеспечения ИБ, общечеловеческими качествами, отвечающими гуманистическим идеалам развития информационного общества;
4. Опережающей направленностью подготовки студентов, аспирантов, молодых ученых, готовых к решению актуальных научно-педагогических задач в условиях информатизации всех сфер общества;
5. Недостаточной представленностью психолого-педагогической проблематики ИБ в спектре научных исследований научных психологических и педагогических школ;
6. Потребностью научно-педагогической практики в действенном инструментарии для обеспечения и диагностики безопасности в ИКТ-насыщенной среде.

Таким образом, реализация и апробация модели даст новые перспективы для достижения научных результатов мирового уровня в области теоретической разработки и экспериментальной апробации инновационных механизмов подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде и обеспечит защиту информационной инфраструктуры сферы науки и образования.

Жигадло Н.В., Семенова Е.Б.
Россия, Санкт-Петербург, Гимназия № 652 Выборского района

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ В НАЧАЛЬНОЙ ШКОЛЕ

В современном мире важной задачей школы, в том числе и начальной, является формирование у детей устойчивых знаний в области информатики, умения быстро ориентироваться в огромных потоках информации, критически ее оценивать и эффективно использовать. В условиях широкого внедрения компьютерных и Интернет-технологий во все сферы жизни современного общества дети с дошкольного возраста уже имеют начальное представление о компьютерах и сети Интернет, при этом особо остро встает вопрос эффективного и безопасного использования в учебном процессе информационных и коммуникационных технологий, которые предоставляют широкие возможности:

- для организации и управления учебным процессом;
- индивидуализации учебного процесса при сохранении его целостности;

– построения открытой системы образования;
– создания эффективной системы методического обеспечения образовательного процесса;
– формирования информационной образовательной среды.

Спектр применения информационных и коммуникационных технологий в образовательном процессе в начальной школе достаточно широк – от формирования информационной культуры школьника до применения компьютеров в предметном обучении, дополнительном образовании младших школьников и в управлении образованием. Поэтому сегодня перед начальным образованием встала задача совершенствования процесса обучения с точки зрения организации, структуры, содержания, используемых средств и электронных образовательных ресурсов в условиях формирования информационной образовательной среды.

Однако, широкое использование компьютерных технологий в учебном процессе, направленное как на формирование знаний и умений школьников, так и на обеспечение образовательного процесса, в начальной школе вызывает серьезные трудности, которые заключаются с одной стороны в несовершенной методологии использования методов компьютеризации в учебном процессе, а с другой стороны – в нерешенности вопросов безопасности компьютерных технологий.

Не смотря на то, что системная работа по интегрированному использованию в обучении информационных и компьютерных технологий позволяет ориентировать детей на саморазвитие, умение добывать нужные им знания, применять их в жизненных ситуациях, влиять на мотивацию учащихся, раскрывая практическую значимость изучаемого материала, предоставляя им возможность проявить оригинальность индивидуальной мысли, фантазию и творческие способности не только на уроках, но и во внеклассной и внешкольной деятельности, существуют серьезные негативные факторы тотальной информатизации, особенно в начальной школе. Среди них - дополнительная нагрузка на зрительную систему и опорно-двигательный аппарат, психологическая зависимость школьников младших классов от компьютера и сети Интернет. Факторы риска первую очередь связаны с компьютерными играми и бесконтрольным использованием Интернета. Врачебная статистика констатирует в последнее десятилетие существенный рост детской патологии, связанной с компьютерной зависимостью. Это обуславливает необходимость внимательного изучения проблемы дозированного использования компьютера в начальной школе, важность освоения младшими школьниками основ эргономики, культуры общения с компьютером, элементов информационной культуры, необходимой каждому члену информационного общества. Уроки с компьютерной поддержкой должны строиться методически грамотно, с соблюдением эргономических требований к организации учебного процесса (общей продолжительности, периодичности, использования релаксационные и динамических пауз, в том числе для выполнения специальных упражнений, ограничения доступа и т.д.).

В докладе рассматриваются проблемы формирования информационной образовательной среды, предлагается подход к решению вопросов защиты от деструктивного влияния виртуального пространства сети Интернет.

Кононов О.А., Кононова О.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования,
Санкт-Петербургский государственный университет аэрокосмического приборостроения

СОЦАЛЬНО-ЛИЧНОСТНОЕ РАЗВИТИЕ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Сегодня значительная часть рабочего времени расходуется людьми главным образом на различные виды инфокоммуникационного взаимодействия с информационными системами, коллегами и внешними контрагентами. При этом, по экспертной оценке, до 80% всех инцидентов информационной безопасности происходят в процессе такого взаимодействия и только 20% обусловлены внешними атаками.

Слабейшим звеном в любой системе защиты от угроз безопасности информационному корпоративному пространству оказываются пользователи инфокоммуникационных систем. Поэтому при анализе угроз, разработке регламентов и политики безопасности, проектировании комплексной защиты от внешних и внутренних угроз, внедрении и настройке необходимого для защиты инструментария и сопровождении систем защиты необходимо уделять особое внимание человеческому фактору, оказывающему существенное влияние на уровень рисков информационной безопасности компании.

Для противодействия угрозам безопасности информационного корпоративного пространства необходимо учитывать влияние всех регуляторов информационных отношений.

На техническом уровне противодействия человеческому фактору наряду с внедрением и совершенствованием систем защиты от утечек информации весьма целесообразно автоматизировать насколько возможно обработку конфиденциальной информации. При этом сотрудники будут более лояльны к работе с конфиденциальной информацией и уменьшится число сокрытий персоналом фактов утечек. С техническими рисками бороться проще, так как они более предсказуемы.

На организационном уровне в зависимости от типов информации (конфиденциальная, секретная, совершенно секретная и т.д.), с которой работает фирма, разрабатывается конкретный набор процедур, ограничивающий распространение данных только среди допущенных до них лиц.

Кроме технических и организационных методов защиты от влияния человеческого фактора чрезвычайно важное значение имеет кадровый менеджмент, который обеспечивает соответствие личных качеств сотрудников профессиональным требованиям.

Особое место в этой деятельности занимает система обучения, которая должна адаптировать сотрудников к внутренним требованиям компании, объективно оценить их отношение к порученному делу, обеспечить внедрение в сознание участников информационного взаимодействия необходимости соблюдения норм компьютерной этики, привитие навыков её применения и, таким образом, наряду с другими средствами управления персоналом способствовать формированию здоровой корпоративной информационной среды.

В докладе рассматриваются вопросы влияния человеческого фактора на корпоративную информационную безопасность, а также организация процесса обучения с учетом социально-личностного развития обучаемых, имеющего чрезвычайно важно значение для обеспечения

Королева Н.Л.
Россия, Тамбов, Тамбовский государственный университет имени Г.Р. Державина

СОДЕРЖАНИЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПЕРЕХОДЕ НА СТАНДАРТЫ ТРЕТЬЕГО ПОКОЛЕНИЯ

Ассоциацией предприятий компьютерных и информационных технологий в 2010 году сформулирован следующий тезис «Недостаточное количество ИТ-специалистов в ИТ-индустрии и других отраслях экономики при реализации может стать тормозом формирования информационного общества и становления инновационной экономики России. Для создания национальной интегрированной системы ИТ-образования, направленной на массовую подготовку конкурентоспособных специалистов международного уровня, требуется интеграция усилий науки, образования, индустрии и государства».

Государственные образовательные стандарты высшего профессионального образования нового поколения открывают для российских вузов широкие возможности относительно формирования содержания подготовки специалистов, и это, безусловно, является одним из положительных моментов при переходе на двухступенчатую систему образования. Однако при формировании образовательных программ вузам необходимо учитывать и потенциальные потребности регионального рынка труда, что в настоящее время довольно трудно сделать из-за того, что большинство руководителей предприятий и организаций, являющиеся потенциальными работодателями, не могут сформулировать конкретные требования к специалистам в области информационной безопасности вследствие устаревших либо узкоустоявшихся взглядов на решение типичных задач обеспечения информационной безопасности.

Проведя анализ численности специалистов по информационной безопасности, направленных региональными предприятиями и организациями на повышение квалификации в Тамбовский государственный университет имени Г.Р. Державина, следует отметить, что основная масса руководителей испытывает потребность в специалистах по инженерно-технической защите информации (67,7% слушателей соответствующих курсов),17,6% – составили слушатели курсов по защите сведений, составляющих гостайну, 11,8% – по организационной защите информации, 2,9% – по криптографической защите информации. На основе полученных данных можно сделать вывод о неумении или нежелании руководителей использовать современные средства, позволяющие реализовать работу отделов по информационной безопасности, отвечающую современным требованиям. Одним из вариантов решения данной проблемы является переосмысление способов использования новейших разработок в сфере программного обеспечения ведущих зарубежных и российских IT-корпораций.

В связи с реализацией государственной программы «Информационное общество (2011–2020 годы)» и переходом России на электронное государство проблема подготовки IT-специалистов и специалистов по информационной безопасности приобретает первоочередное значение. Выбор Тамбовским государственным университетом имени Г.Р. Державина профиля «Безопасность компьютерных систем» направления подготовки «Информационная безопасность» ориентирован на перспективу и связан с возрастающей потребностью в специалистах, способных создавать и развивать специальные информационные и информационно-технологические системы обеспечения деятельности органов государственной власти, в том числе защищенный сегмент сети Интернет и систему межведомственного электронного документооборота. Так при разработке основной образовательной программы высшего профессионального образования по направлению подготовки «Информационная безопасность» (профиль «Безопасность компьютерных систем» в вариативную часть профессионального цикла дисциплин были включены следующие курсы: Безопасность средствами операционных систем, Защита документооборота в компьютерных системах, Безопасные

информационные технологии, Безопасность Web-сайтов, Разработка безопасных Windows-приложений на C++, Разработка защищенных Java-приложений, Защита конфиденциальной информации с использованием криптографических средств, Защита информационных процессов в компьютерных системах и др., позволяющие сформировать у студентов профессиональные компетенции в области обеспечения безопасности в информационном обществе, а именно: навыки противодействия использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам Российской Федерации; разработки и развития технологий защиты информации, обеспечивающих неприкосновенность частной жизни, личной и семейной тайны, а также обеспечения безопасности информации ограниченного доступа.

Коршунов И.Л.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет сервиса и экономики

О НЕОБХОДИМОСТИ ПОДГОТОВКИ БАКАЛАВРОВ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ В СФЕРЕ СЕРВИСА

Защита персональных данных в информационных системах сегодня является одной из важнейших проблем для большинства российских компаний. Обеспечение требований Федерального Закона №152 «О персональных данных» является обязательным как для коммерческих, так и для государственных организаций. Соответственно все компании, работающие в сфере сервиса (туриндустрия, гостиничный бизнес, жилищно-коммунальный комплекс, муниципальное управление, здравоохранение и др.), обязаны выполнять требования данного Закона. Поэтому проблема подготовки кадров для решения задач защиты персональных данных (ПДн) в информационных системах в сфере сервиса является актуальной.

С целью определения направления подготовки бакалавров, способных обеспечить защиту ПДн в информационных системах в сфере сервиса, был проанализирован Общероссийский классификатор специальностей по образованию (2010 года) и выбраны два направления подготовки бакалавров: 090900 «Информационная безопасность» и 230400 «Информационные системы и технологии» (профиль «Безопасность информационных систем»). Проведен анализ федеральных государственных образовательных стандартов этих двух направлений, который позволил сделать следующие выводы.

Объекты профессиональной деятельности бакалавра «Информационные системы и технологии» более точно соответствуют предметной области, для которой готовятся выпускники университета сервиса и экономики. В частности, в ФГОС 230400 указано: «Объектами профессиональной деятельности бакалавров являются: информационные процессы, технологии, системы и сети, способы и методы эксплуатации информационных технологий и систем в областях: сфера сервиса, а также предприятия различного профиля и все виды деятельности в условиях экономики информационного общества».

Одним из видов профессиональной деятельности (перечисленных в стандарте), к которой готовится бакалавр по направлению подготовки «Информационные системы и технологии», являетсясервисно-эксплуатационная, что соответствует профилю университета.

Базовая часть профессионального блока основной образовательной программы бакалавра «Информационные системы и технологии» сориентирована на обучение специалиста, подготовленного к эксплуатации информационных систем, что важно для сферы сервиса.

Вопросы, связанные с защитой информации в информационных системах, сосредоточены в вариативной части. И в этом случае университет, определяя дисциплины вариативной части, может более точно учитывать особенности той предметной области, для работы в которой готовятся выпускники.

Таким образом, проведенный анализ позволяет констатировать, что для подготовки бакалавров по защиты персональных данных в информационных системах в сфере сервиса целесообразно осуществлять подготовку в рамках направления «Информационные системы и технологии» (профиль «Безопасность информационных систем»).

Москалева О.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ОБУЧЕНИЕ ВОПРОСАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТУДЕНТОВ ЭКОНОМИЧЕСКИХ НАПРАВЛЕНИЙ В КУРСЕ ИНФОРМАТИКА

Отбор содержания обучения информатике студентов экономических направлений с точки зрения современной педагогики проводится на основании сформулированных стандартами третьего поколения требований профессиональной компетентности специалиста.

Стандарт по направлению подготовки 230700 Прикладная информатика формулирует общекультурные компетенции в области информационной безопасности: выпускник «способен

понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОК-13)». Кроме того, этот же стандарт, формулирует профессиональные компетенции в области информационной безопасности: выпускник «способен анализировать и выбирать методы и средства обеспечения информационной безопасности (ПК-18)».

Стандарт по направлению подготовки 080100 Экономика формулирует общекультурные компетенции в области информационной безопасности: выпускник «способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОК-12)».

Стандарт по направлению подготовки 080500 Бизнес-информатика напрямую не формулирует компетенции в области информационной безопасности, но прописывает, что выпускник «осознает сущность и значение информации в развитии современного общества; владеет основными методами, способами и средствами получения, хранения, переработки информации (ОК-12)».

Стандарт по направлению подготовки 080200 Менеджмент также напрямую не формулирует компетенции в области информационной безопасности, но прописывает, что выпускник должен «владеть основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-17)». Это подразумевает наличие у выпускников знаний, умений и владение навыками в области информационной безопасности достаточными для того, чтобы не допустить случайных или преднамеренных действий, которые могут привести к утечке защищаемой информации.

Экономисту необходимо знать основные угрозы, которые могут нанести ущерб организации, в которой он работает. Конфиденциальность, целостность, сохранность информации, с одной стороны, предполагают ее доступность для сотрудников, а с другой, способствуют обеспечению конкурентоспособности, ликвидности, доходности, соответствия законодательству и деловой репутации организации.

Что должны знать экономисты в области информационной безопасности?

Основных угроз не так много. Во-первых, физическая потеря данных. Причиной потери данных может стать разрушение носителей, износ накопителя на жестком диске. Возможен выход из строя источника питания из-за сбоя напряжения в электрической сети, кража компьютеров и носителей, их неправильное хранение, использование и т. д. Отсюда вытекает требование владеть навыками по обеспечению физической защиты данных, обеспечению резервного копирования информации с четким соблюдением требований, предъявляемых к носителям, регулярности копирования, методам хранения копий. Экономист должен уметь правильно сформулировать требования системному администратору, чтобы содержать свой компьютер постоянно в работоспособном состоянии.

Во-вторых, утечка конфиденциальной информации. К данной угрозе относится шпионаж, кража данных, передача паролей для доступа к данным, пренебрежение сложными паролями и т.д. Отсюда вытекает требование владеть знаниями в области кодирования и хеширования информации. Экономист должен знать о возможностях несанкционированного доступа в компьютерные сети, внешней атаке на узлы компьютерной сети организации, о возможностях взлома пароля и логина.

В-третьих, несанкционированный доступ к данным. Отсюда вытекает требование знать и выполнять внутри объектовый и пропускной режим организации, нормативные документы при эксплуатации компьютера.

В-четвертых, действия неквалифицированного пользователя. Самое популярное действие – случайное непреднамеренное форматирование данных. Экономист должен знать о возможных методах повреждения данных пользователем в результате неосторожных действий.

В-пятых, компьютерные вирусы, спам. Компьютерные вирусы и другие вредоносные программы представляют собой реальную опасность для организации, использующей компьютерные сети, интернет и электронную почту. Необходимо знать признаки появления компьютерных вирусов. Основными признаками являются: замедление работы компьютера, частые зависания и сбои в работе компьютера, невозможность загрузки операционной системы, увеличения количества файлов на диске и их размеров, изменение даты и времени создания файлов. Вирус и спам может привести к потерям рабочего времени, утрате данных, краже конфиденциальной информации, может предоставить злоумышленникам контроль над деятельностью компании. За последние годы спам из незначительного раздражающего фактора превратился в одну из серьезнейших угроз безопасности. Отсюда вытекает требование владеть современными антивирусными технологиями, фильтрацией спама.

Таким образом, определен перечень основных угроз информационной безопасности использования вычислительной техники на основе требований профессиональной компетентности.

Перевозник Ю.Я.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ОСНОВНЫЕ ЗАДАЧИ И НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ввиду того, что современные системы защиты становятся все более сложными и комплексными как по целям, так и по используемым методам и средствам защиты, необходимо расширять номенклатуру специальностей по защите. Причем подготовка кадров должна осуществляться комплексно в нескольких уровнях: подготовка молодых специалистов на базе школьного образования (срок обучения 5-5,5 лет); подготовка специалистов по информационной безопасности на базе высшего технического образования (срок обучения 2-2,5 года); переподготовка кадров на краткосрочных курсах повышения квалификации специалистов и руководителей подразделений (срок обучения 2-4 недели); подготовка специалистов на базе среднетехнического образования через колледж со сроком обучения 4-5 лет на базе 9 классов; подготовка специалистов высшей квалификации через аспирантуру и защиту диссертационных работ в специализированных советах.

По-прежнему актуальна проблема развития системы подготовки кадров в области информационной безопасности как по «вертикали» – с охватом всех уровней подготовки, так и по «горизонтали» – с выходом на проблемы информационной безопасности в гуманитарной сфере и на стыке естественнонаучных, технических и гуманитарных направлений. В первую очередь это относится к подготовке и переподготовке специалистов правоохранительных органов, органов суда и прокуратуры в области борьбы с преступлениями в сфере компьютерной информации. Представляется необходимым создать систему непрерывного профессионального образования специалиста в области информационной безопасности.

Основными задачами системы подготовки и переподготовки кадров в области обеспечения информационной безопасности являются:

– удовлетворение потребностей в квалифицированных специалистах федеральных и региональных органов исполнительной власти, критически важных объектов инфраструктуры страны, государственных и негосударственных предприятий и организаций, научно-исследовательских и образовательных учреждений;

– реализация основных направлений государственной политики в области кадрового обеспечения информационной безопасности Российской Федерации, развитие и совершенствование форм, методов и средств подготовки квалифицированных специалистов с учетом перспектив информатизации различных сторон экономической, политической и общественной жизни;

– повышение уровня информационной грамотности населения страны, включая обучение информационной этике, соответствующему поведению при пользовании Интернетом и другими средствами связи, формирование общественного мнения по проблеме необходимости обеспечения совершенной системы информационной безопасности;

– расширение взаимодействия с международными и зарубежными органами и организациями с целью использования передового опыта организационного и методического обеспечения подготовки, повышения квалификации и переподготовки кадров по проблемам информационной безопасности.

Основные направления совершенствования подготовки и переподготовки кадров в области обеспечения информационной безопасности:

– расширение комплекса образовательных программ (в том числе общеобразовательных) по правовым, управленческим, экономическим, культурологическим, политическим, социологическим, математическим, естественнонаучным и техническим проблемам обеспечения информационной безопасности, развитие университетского (естественнонаучного и гуманитарного) образования в области информационной безопасности;

– приоритетное развитие системы повышения квалификации и переподготовки руководителей и специалистов государственных органов, учреждений и организаций, органов местного самоуправления, коммерческих и некоммерческих структур по широкому кругу проблем обеспечения информационной безопасности;

– формирование эффективной системы целевой подготовки и закрепления квалифицированных кадров в области обеспечения информационной безопасности;

– развитие системы региональных учебно-научных центров по проблемам информационной безопасности, создаваемых при ведущих высших учебных заведениях, для приоритетного решения проблем кадрового обеспечения федеральных и региональных органов исполнительной власти;

– существенное совершенствование системы аттестации и контроля качества подготовки, повышения квалификации и переподготовки специалистов в области обеспечения информационной безопасности.

Полонский А.М. Усикова И.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ВОПРОСЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных» установлены правила в отношении порядка обработки и обеспечения конфиденциальности персональных данных, которые обрабатываются в организациях. Вступившие в силу нормативные правовые акты и иные руководящие документы, регламентируют порядок технической защиты персональных данных.

Невыполнение требований соответствующих правовых актов и нормативных документов ФСБ и ФСТЭК может привести к негативным последствиям для организации и ее руководителей, таким как выплата штрафов, а при определенных условиях возможно приостановление действия или аннулирование лицензий на основной вид деятельности компании. Технические средства и программные средства для защиты информационных систем персональных данных (ИСПДн) должны подбираться с учетом требований регуляторов и класса ИСПДн.

Защита персональных данных (ПДн) в частных компаниях, государственных и муниципальных организациях различного вида деятельности и форм собственности, а также физическими лицами, выполняющими сбор, хранение, обработку и передачу ПДн (в дальнейшем – операторами ПДн) является актуальной задачей и вытекает из требований федерального закона от 27.06.2006 №152-ФЗ «О персональных данных». Симптоматично, что данный федеральный закон (ФЗ), принятый более пяти лет назад и подвергшийся доработкам и уточнениям (в том числе – и во многочисленных подзаконных актах) по настоящее время в полной мере не действует, что может испытать на себе каждый гражданин РФ, обнаруживший свои персональные данные в массовых рассылках (почтовых, SMS), на общедоступных Интернет-порталах и т.п.

Одной из причин такого неудовлетворительного состояния можно считать отсутствие квалифицированных специалистов по защите ПДн, способных организовать и обеспечить защиту информационной системы оператора и/или оказывать соответствующие услуги. Соответственно, операторы ПДн должны иметь в своем составе штатного специалиста (специалистов, подразделение) по защите ПДн, либо привлекать для данной деятельности специалистов из специализированных компаний. Защита ПДн – одно из направлений деятельности по технической защите конфиденциальной информации (ТЗКИ), данный вид деятельности является лицензируемым, соответственно – чтобы оказывать услуги в области ПДн необходимо быть лицензиатом ФСТЭК России. Зачастую компании, имеющие в своем составе IT-отдел, считают, что для организации защиты ПДн в пределах собственных компаний лицензий на ТЗКИ не требуется. Формально данное утверждение правильное, но при этом остается вне поля рассмотрения квалификация специалистов IT-отдела в области защиты ПДн в частности и ТЗКИ в целом.

Требования к лицензиату в области ТЗКИ определены нормативными документами ФСТЭК России: необходимо иметь защищенное помещение, аттестованную информационную систему (в минимальном виде – ПЭВМ), комплект измерительной аппаратуры (может быть оформлено временное использование до договору) и не менее двух штатных сотрудников организации, имеющих высшее профессиональное образование в области технической защиты информации, либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации. Таковы формальные требования к квалификации сотрудников соискателю лицензии и лицензиату на деятельность в области ТЗКИ. В докладе рассматриваются учебные программы ВУЗов и курсов повышения квалификации с точки зрения соответствия требованиям нормативным требованиям и реальными потребностями в деятельности специалиста по защите ПДн и/или конфиденциальной информации.

В настоящее время в системе высшего профессионального образования предусмотрены следующие направления подготовки (специальности):

– 090301 Компьютерная безопасность (квалификация (степень) «специалист»),

– 090302 Информационная безопасность телекоммуникационных систем (квалификация (степень) «специалист»),

– 090303 Информационная безопасность автоматизированных систем (квалификация (степень) «специалист»),

– 090305 Информационно-аналитические системы безопасности (квалификация (степень) «специалист»).

Предполагается, что выпускник будет обладать необходимым набором компетенций, т.е. знаний, навыков и опыта, которые непосредственно сможет использовать при решении организационных, программных и технических вопросов в области ТЗКИ (защиты ПДн). Если рассмотреть государственные образовательные стандарты (ГОС) данных направлений (специальностей), но вопросам реализации всех аспектов ТЗКИ (ПДн) уделено относительно немного учебных часов, рассматриваемые нормативные документы актуальны на время изучения соответствующих курсов, в то же время любые нормативные документы в сфере ТЗКИ устаревают и

выпускники не обязаны для подтверждения своей квалификации периодически обучаться на курсах переподготовки. Данные программы ориентированы в большей степени на разработчика средств защиты информации, но не на специалиста, использующего данные знания на практике. Самостоятельное изучение специалистами по защите информации методических материалов не всегда возможно, поскольку данные материалы в ряде случаев имеют ограничительные грифы.

В докладе рассматриваются учебные заведения Санкт-Петербурга, предлагающие курсы по повышению квалификации в области ТЗКИ.

В целях повышения качества защиты ПДн и снижения риска их утечки представляется целесообразным ввести в качестве обязательного условия работы специалиста по ТЗКИ – периодическое (не реже 1 раза в 3–5 лет) повышение квалификации по программе курсов, согласованной с ФСТЭК России.

Райкин И.Л.
Россия, Нижний Новгород, Нижегородский государственный технический университет им. Р.Е.Алексеева

СОВРЕМЕННЫЙ ПОДХОД К ПРЕПОДАВАНИЮ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ»

Как показывает практика, традиционные формы подготовки специалистов в ВУЗах не вполне устраивают заказчиков таких специалистов, равно как и самих студентов, а так же преподавателей. С одной стороны постоянно меняются и все возрастают возможности новых информационных технологий, что требует постоянной корректировки всего учебно-методического материала. С другой – ограниченные временные рамки контакта со студентами и традиционные формы подачи информации, практической работы и контроля не позволяют студентам освоить необходимые объемы.

Наиболее прогрессивной формой предоставления образовательных услуг в настоящее время считается открытая, реализуемая посредством дистанционного подхода. Информационная компонента кейс- и Web-CD технологии, используемые в дистанционном образовании, наполняется создаваемым (или приобретаемым) контентом.

Информационная безопасность является существенным аспектом активно развивающейся в последнее время интегральной безопасности, на каком бы уровне она ни рассматривалась – национальном, отраслевом, корпоративном или персональном.

В известных учебниках и учебных пособиях по информационной безопасности и защите информации недостаточно описан ряд тем, связанных с современными правовыми нормами, компьютерными средствами реализации защиты информации в новейших информационных системах.

В учебнике «Информационная безопасность и защита информации» предпринята попытка осветить широкий спектр вопросов современного состояния дел в области информационной безопасности, а также аппаратных и программных средств защиты информации, что является одним из наиболее важных аспектов при подготовке специалистов по информационным системам.

Все главы содержат важный при изучении дисциплины «Информационная безопасность и защита информации» материал, снабженный большим числом иллюстраций.

В учебнике полно и на современном уровне изложены важные в теоретическом и практическом плане вопросы информационной безопасности и защиты информации. Этот материал дополняет существующие методические материалы в важных разделах дисциплины «Информационная безопасность и защита информации». Вместе с тем, предлагаемый учебник включает новые, появившиеся в последние годы материалы, обусловленные продвижением технологий защиты информации, и является компактным обзорным материалом по основным разделам дисциплины.

Учебник, в целом, характеризуется наличием практически полезных примеров, которые имеют большое учебно-методическое значение и необходимы для закрепления основных тем дисциплины, а так же для практических занятий и при самостоятельной работе студентов. Содержание глав учебника сопровождается примерами и контрольными вопросами.

Учебнику «Информационная безопасность и защита информации» присвоен гриф УМО по университетскому политехническому образованию.

В электронном комплексе учебно-методических материалов (ЭКУММ) «Информационная безопасность и защита информации» изложены разделы правового обеспечения информационной безопасности, организационных, технических и общесистемных средств защиты информации, принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа, принципы уничтожения остаточных данных и специфические особенности защиты информации в глобальных и локальных компьютерных сетях.

Комплекс рассчитан на студентов высших учебных заведений, институтов повышения квалификации и школ подготовки специалистов, изучающих проблемы защиты информации.

В создании ЭКУММ непосредственное участие принимали выпускники НГТУ (бакалавры инженеры и магистры) по направлению «Информационные системы», у части которых в качестве темы выпускной работы или дипломного проекта выступает разработка подобных ЭКУММ по той или иной учебной дисциплине.

В марте 2011 г. автором данного электронного издания был зарегистрирован разработанный ресурс в Научно-техническом центре «Информрегистр», который в соответствии с Федеральным Законом «Об обязательном экземпляре документов» выполняет функции федерального депозитария электронных изданий. С точки зрения авторских прав электронные издания, зарегистрированные в «Информрегистре», приравниваются к изданным печатным материалам.

Советов Б.Я.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

ПРОБЛЕМЫ ПОСТРОЕНИЯ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА В САНКТ-ПЕТЕРБУРГЕ НА БАЗЕ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Руководством страны поставлена задача предоставления государственных услуг населению в электронном виде. В настоящее время это формулируется как этап создания электронного правительства. В современном понимании электронное правительство представляет собой способ предоставления информации и оказания уже сформировавшегося набора государственных услуг гражданам, бизнесу, ветвям государственной власти и государственным чиновникам, при котором личное взаимодействие между государством и заявителем минимизировано и максимально возможно используются инфокоммуникационные технологии. Под электронным правительством понимается новая форма организации деятельности органов государственной власти, обеспечивающая за счёт широкого применения инфокоммуникационных технологий качественно новый уровень оперативности и удобства получения гражданами и организациями государственных услуг и информации о результатах деятельности государственных органов. Создание электронного правительства на базе инфокоммуникационных технологий предусматривает на современном этапе решение задачи предоставления электронной услуги жителю по запросу. Запрос реализуется через систему приема заявок, подключенную к единому порталу государственных услуг. Доступ осуществляется по сети или путем посещения многофункционального центра, или обращения через специальный терминал, который доступен любому жителю. Естественно таких терминалов должно быть достаточно много и с их помощью должны предоставляться все необходимые жителю города услуги. Доступ от терминалов к единому порталу осуществляется по сети связи с использованием современных инфокоммуникационных технологий. Инфраструктура электронного правительства включает в себя: центр общественного доступа, центр телефонного обслуживания, систему приема заявок, единый портал государственных услуг, систему безопасности, реестр государственных услуг, удостоверяющий центр, систему межведомственного электронного взаимодействия.

Предполагается, что введение системы доступа к электронным услугам на базе предложенной инфраструктуры позволит устранить коррупцию, упростить процесс получения государственных и муниципальных услуг, повысить оперативность взаимодействия заявителя с органами государственной власти. В настоящее время в ряде крупных городов, в том числе в Санкт-Петербурге созданы многофункциональные центры по обеспечению работы органов власти с населением. Они нацелены на создание оперативного межведомственного взаимодействия в процессе подготовки документов для заявителей, сбор необходимых документов без привлечения граждан с выдачей готового документа. Тем самым реализуются некоторые функции оператора Электронного правительства Санкт-Петербурга. Дальнейшее развитие идеологии электронного правительства базируется на предложении реализации оператора электронного правительства в структуре мультисервисных городских сетей. Необходимо совершенствовать и организационное обеспечение решения данной проблемы, объединяя в единую сеть такие службы как: жилищно-коммунальное хозяйство, службы регистрации недвижимости, налоговую инспекцию, полицию и т.д.

Советов Б.Я., Цехановский В.В., Касаткин В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СРЕД ОБРАЗОВАНИЯ

Проблема обеспечения информационной безопасности телекоммуникационной и информационной среды образования становится крайне актуальной и требует быстрого и эффективного решения при ограниченных средствах. Данная проблема должна рассматриваться в трех аспектах: защита интеллектуальной собственности, защита служебной информации, ограничение доступа учащихся к информационным ресурсам. Не секрет, что многие сотрудники вузов работают в коммерческих структурах, и происходит несанкционированная утечка ресурсов научного

потенциала вузовской науки. Это приводит к значительным экономическим потерям. С другой стороны, широкое внедрение информационных технологий в систему управления образованием сопровождается утечкой конфиденциальной служебной информации. В первую очередь, это касается таких служб, как бухгалтерия, отдел кадров, спецотделы, другие службы. Не менее важным для нужд Минобразования России является внедрение скоростного документооборота с высоким уровнем доказуемости авторства документов.

Другой важной областью является обеспечение информационной безопасности вводимого единого государственного экзамена. В опубликованных нормативных материалах Центра тестирования Минобразования России эта проблема решается в основном организационными мероприятиями, что не обеспечивает требуемого уровня конфиденциальности.

Широкое внедрение информационных технологий в сферу образования приводит к необходимости решения проблем, связанных с защитой от несанкционированного доступа к информационным и компьютерным ресурсам. Эти проблемы становятся особенно острыми при интеграции содержимого компьютерных сетей общеобразовательных учреждений с информационными ресурсами глобальной сети Интернет. При этом речь идет как о защите интеллектуальной собственности и служебной информации, так и предотвращении доступа обучаемых к нежелательной информации.

В условиях модернизации образования необходимо также разработать теоретические основы безопасности модернизации информационной среды профессионального образования. Выполнение Россией решений Болонской конвенции возможно на основе рассмотрения современных образовательных траекторий, характерных для подготовки кадров в области техники и технологий с целью выявления условий их безопасной реализации при формировании информационной среды. Качество образования должно рассматриваться как результат организации безопасной образовательной среды, выбора траекторий подготовки кадров в технических вузах, выявления условий их безопасной реализации при формировании образовательной среды как среды прогнозирования, обнаружения, регуляции и ликвидации на различных уровнях опасностей и рисков достижения требуемого на современном этапе качества образования.

Советов Б.Я., Крук Е.А., Касаткин В.В., Цехановский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Санкт-Петербургский государственный университет аэрокосмического приборостроения, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

ПОДГОТОВКА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ПРОФИЛЯ НАПРАВЛЕНИЯ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

В рамках высшего профессионального образования в соответствии с федеральными государственными образовательными стандартами III поколения предусмотрена подготовка бакалавров, магистров и специалистов по направлению «Информационная безопасность». Выпускники этого направления ориентированы на работу в структуре различных организаций разных отраслей и должны иметь всестороннюю подготовку в области защиты информации. Открытие направления «Информационные системы и технологии» преследовало цель подготовки в нашей стране разработчиков информационных систем и новейших информационных технологий. В связи с тем, что в настоящее время это направление является двухуровневым (бакалавр, магистр), специализация может быть реализована введением соответствующего профиля на уровне подготовки бакалавра.

Компьютерная безопасность является одной из важнейших составляющих обеспечения жизненного цикла информационных систем, что обусловило необходимость введения профиля «Безопасность информационных систем». При разработке содержания подготовки бакалавров по этому профилю основной проблемой был выбор из двух подходов:

– информационная безопасность, обеспечиваемая в процессе проектирования информационной системы;

– информационная безопасность, обеспечиваемая в рамках организации сопровождения процесса функционирования информационной системы, как готового продукта.

С позиций системной инженерии сложившийся подход к обеспечению информационной безопасности на стадии готового проекта информационной системы является недостаточно эффективным, как с позиций технических, так и экономических. Пример отраслей, достигших высокого уровня технологий, демонстрирует четкое разделение: безопасность, обеспечиваемая в процессе проектирования и безопасность, обеспечиваемая в рамках организации сопровождения процесса функционирования.

Проектирование информационных систем является коллективным процессом и специалист предлагаемого профиля должен участвовать во всех стадиях создания конечного продукта. При этом он получает необходимые знания в области системного подхода, теории информационных процессов

и систем, информационных технологий, проектирования и эксплуатации информационных систем. Благодаря этому у выпускника возникает возможность обеспечить высокие показатели проектируемой информационной системы при оптимальном использовании финансовых, материальных и трудовых ресурсов.

Данный подход был реализован при разработке федерального государственного образовательного стандарта подготовки бакалавра по направлению «Информационные системы и технологии» в рамках профиля «Безопасность информационных систем». При формировании перечня дисциплин большое внимание уделено вопросам проектирований и сопровождения защищенных информационных систем. В докладе рассматривается структура примерного учебного плана и содержание примерных программ дисциплин указанного профиля подготовки бакалавра.

ОГЛАВЛЕНИЕ