



«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР–2009)»

VI САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 28-30 октября 2009 года

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург

2009



«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР–2009)»

VI САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 28-30 октября 2009 года

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург

2009

Информационная безопасность регионов России (ИБРР-2009). VI Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009)». Санкт-Петербург, 28-30 октября 2009 г.: Материалы конференции \ СПОИСУ. – СПб, 2009. – 172с. ISBN 978-5-904031-05-3.

Сборник содержит материалы VI Санкт-Петербургской Межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2009)», учредителями которой являются: Правительство Санкт-Петербурга, Законодательное Собрание Санкт-Петербурга, Правительство Ленинградской области, Министерство связи и массовых коммуникаций Российской Федерации, Министерство образования и науки Российской Федерации, Российская академия образования, Отделение нанотехнологий и информационных технологий Российской академии наук, Санкт-Петербургский научный Центр Российской академии наук, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургская территориальная группа Российского национального комитета по автоматическому управлению, Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления.

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

УДК (002:681):338.98

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

Публикуется в авторской редакции

Подписано в печать 12.10.2009. Формат 60х84 $\frac{1}{8}$. Бумага офсетная.
Печать – ризография. Усл. печ. л. 41,42. Тираж 500 экз. Заказ № 936

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

ISBN 978-5-904031-05-3

© Санкт-Петербургское Общество информатики,
вычислительной техники, систем связи и
управления (СПОИСУ), 2009 г.

© Авторы, 2009 г.



VI ST. PETERSBURG INTERREGIONAL CONFERENCE

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

St. Petersburg, October 28-30, 2009

**PROCEEDINGS
OF THE CONFERENCE**

**St. Petersburg
2009**



УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ «ИБРР-2009»

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

СОУСТРОИТЕЛИ КОНФЕРЕНЦИИ «ИБРР-2009»

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

КООРДИНАЦИОННЫЙ СОВЕТ КОНФЕРЕНЦИИ «ИБРР-2009»

Матвиенко Валентина Ивановна	Губернатор Санкт-Петербурга
Тюльпанов Вадим Альбертович	Председатель Законодательного собрания Санкт-Петербурга
Сердюков Валерий Павлович	Губернатор Ленинградской области
Алферов Жорес Иванович	Вице-президент Российской академии наук, Председатель Президиума Санкт-Петербургского научного Центра Российской академии наук, Лауреат Нобелевской премии
Велихов Евгений Павлович	Академик-секретарь Отделения нанотехнологий и информационных технологий Российской академии наук
Щеголев Игорь Олегович	Министр связи и массовых коммуникаций Российской Федерации
Фурсенко Андрей Александрович	Министр образования и науки Российской Федерации
Никандров Николай Дмитриевич	Президент Российской академии образования
Федоров Александр Вячеславович	Первый заместитель Министра юстиции Российской Федерации
Макаров Евгений Иванович	Помощник полномочного представителя Президента Российской Федерации в Северо-Западном федеральном округе

ПРЕЗИДИУМ КОНФЕРЕНЦИИ «ИБРР-2009»

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

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2009»

Председатель Организационного Комитета

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

Заместитель председателя Организационного Комитета

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

Члены Организационного Комитета

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

Игумнов Владимир Вячеславович	Главный конструктор ФГУП «Научно-производственное объединение «Импульс»
Ипатов Олег Сергеевич	Заведующий кафедрой Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова
Исаев Борис Анатольевич	Директор СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Касаткин Виктор Викторович	Декан ФПК Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова
Котенко Денис Алексеевич	Генеральный директор ЗАО «Ассоциация специалистов информационных систем»
Кузичкин Александр Васильевич	Исполнительный директор Компании «Radio Net»
Кузьмин Юрий Григорьевич	Ученый секретарь Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления, начальник сектора Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова
Куренков Евгений Владимирович	Директор Санкт-Петербургского Научно-технического центра ФГУП «Научно-производственное предприятие «Гамма»
Марков Вячеслав Сергеевич	Ученый секретарь Объединенного научного совета Санкт-Петербургского Научного центра Российской академии наук
Михайлова Анна Сергеевна	Заместитель директора по связям с общественностью Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Молдовян Александр Андреевич	Заместитель директора Санкт-Петербургского института информатики и автоматизации Российской академии наук по информационной безопасности
Николаев Алексей Юрьевич	Генеральный директор ЗАО «Эврика»
Оводенко Анатолий Аркадьевич	Ректор Санкт-Петербургского государственного университета аэрокосмического приборостроения
Остапенко Александр Николаевич	Генеральный директор ЗАО «Лаборатория противодействия промышленному шпионажу»
Пашкевич Константин Эдуардович	И.О. генерального директора ЗАО «Метроком»
Романов Виктор Егорович	Президент Санкт-Петербургского государственного университета технологии и дизайна
Рунеев Анатолий Юрьевич	Генеральный директор ФГУП «Научно-исследовательский институт «Рубин»
Тихомиров Сергей Григорьевич	Генеральный директор ОАО «Центр компьютерных разработок»
Ткач Анатолий Федорович	Заместитель директора Санкт-Петербургского института информатики и автоматизации Российской академии наук
Устинов Игорь Анатольевич	Генеральный директор ФГУП «Научно-производственное объединение «Импульс»
Федорченко Людмила Николаевна	Научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук

Цыулев Сергей Валентинович	Начальник сектора информационно-компьютерной безопасности Комитета по информатизации и связи Санкт-Петербурга
Черешкин Дмитрий Семенович	Заведующий лабораторией Института системного анализа Российской академии наук
Эркин Анатолий Григорьевич	Генеральный директор ЗАО «Санкт-Петербургский Региональный Центр защиты информации»

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2009»

Председатель Программного Комитета

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

Заместители председателя Программного Комитета

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

Члены Программного Комитета — руководители секций

Ученый секретарь Конференции

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

Информационное обеспечение Конференции

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



ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ

Болдов М.Е.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
информационных технологий, механики и оптики**

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В СБЕРБАНКЕ РОССИИ: ОПТИМИЗАЦИЯ ДОКУМЕНТООБОРОТА И НОВЫЕ ВОЗМОЖНОСТИ

В основу доклада положены информация и знания о частичном переводе документооборота Сбербанка РФ в электронную форму, полученные при прохождении автором производственной практики.

Использование информационных технологий в стабильно функционирующих компаниях зачастую связано с оптимизацией бизнес-процессов и предоставлением дополнительных сервисов.

Правовой основой для перевода документооборота в Сбербанке РФ в электронную форму стало законодательство РФ об использовании электронной цифровой подписи (ЭЦП), в соответствии которым её использование придаёт юридическую силу удостоверяемым таким способом документам, а кроме того и обеспечивает защиту содержания подписанного документа от модификации.

Работу с ЭЦП можно разделить на следующие этапы:

- генерация открытого и закрытого ключа ЭЦП для пользователя;
- регистрация полученного ключа в Удостоверяющем Центре;
- подписание пользователем документа с помощью ЭЦП на основе сгенерированных ключей;
- проверка подписанного документа на подлинность ЭЦП.

Ключевым компонентом в системе обращения ЭЦП является сеть Удостоверяющих Центров. Их роль – регистрировать пользователей ЭЦП и подтверждать подлинности подписи в документах на основе имеющихся баз данных созданных при регистрации открытых ключей. Базы не являются централизованными и объединяются в отдельные криптосети по целям использования. Обмен информацией о зарегистрированных пользователях, поддержка сети Удостоверяющих Центров и проверка подлинности подписанных документов составляют основу PKI – инфраструктуры открытых ключей.

Основной задачей PKI является предоставление возможности быстрой проверки подлинности подписанного документа. В зависимости от информации, содержащейся в ЭЦП, она может разделяться на несколько видов:

- проверка по базе открытых ключей
- проверка по базе сертификатов
- проверка по прикрепленному сертификату

Второй способ особенно хорош для систем, нуждающихся в быстром обмене данными: поиск осуществляется только по централизованной неизменной базе данных открытых ключей администраторов, что сильно экономит время и ресурсы.

Хотя сегодня и нельзя говорить о полном отказе от бумажного документооборота, однако внедрение его электронного варианта в Сбербанке и его отделениях позволило, во-первых, оптимизировать доставку и обработку корреспонденции благодаря использованию электронных каналов связи, а во-вторых, реализовать новые услуги (такие, как система «Блиц-переводы»), обеспечив высокую скорость работы, достаточный уровень защиты данных: как информационный, так и юридический. В итоге это привело, как к расширению спектра и повышению качества услуг клиентам, так и к повышению экономической эффективности деятельности самого Сбербанка РФ.

Демидов А.В.

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

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК МЕРА ПРОФИЛАКТИКИ РАСПРОСТРАНЕНИЯ В РОССИИ ДЕСТРУКТИВНЫХ РЕЛИГИОЗНЫХ ОРГАНИЗАЦИЙ

С конце 80-х годов XX века регионы нашей страны подверглись значительной экспансии так называемых новых религиозных организаций, деятельность которых уже в то время была

охарактеризована как деструктивная в ряде государств мирового сообщества и на законодательном уровне была запрещена.

Другая ситуация наблюдалась в постсоветской России, где после крушения советской системы и ликвидации института идеологической цензуры, государство оказалось беззащитно перед лицом угрозы проникновения на территорию российских регионов деструктивных религиозных идеологий, как с Запада, так и с Востока. Последствия фактически бесконтрольной деятельности различного рода религиозных организаций деструктивного характера не заставили себя ждать: разрушенные семьи, факты суицидального поведения, ритуальные убийства, религиозная ненависть и вражда, рост психических заболеваний среди адептов данных сект и культов и т.п.

Говоря о детерминантах обусловивших появление последствий от деятельности деструктивных религиозных организаций необходимо отнести: проблемы экономического, политического и социального характера.

Но особо необходимо отметить отсутствие системы обеспечения информационной безопасности, как на федеральном, так и региональном уровнях. Именно отсутствие системы информирования населения о деятельности деструктивных религиозных организациях, методах вербовки новых членов, методах воздействия на сознание и психику людей, фактах совершения административных правонарушений и преступлений организаторами и духовными лидерами данных организаций под прикрытием религиозной деятельности способствовало массовому распространению тоталитарных сект и деструктивных культов.

В начале 90-х годов лидеры некоторых новых религиозных культов принимались на самом высоком уровне представителями руководства страны, для религиозных собраний им предоставлялись стадионы и концертные залы, они пользовались поддержкой отечественных правозащитников и имели значительную финансовую помощь, из-за рубежа, позволявшую формировать положительный имидж новых религиозных организаций, воплощающих принцип свободы совести на постсоветском пространстве.

В сложившейся ситуации, при отсутствии чётко выраженной государственной политики обеспечения информационной безопасности направленной на информационное противодействие и блокирование деятельности деструктивных культов и тоталитарных сект государство не смогло сдержать массовое распространение на своей территории религиозных организаций подобного толка.

В заключении необходимо отметить, что в данный период проблема информационного противодействия распространению антисоциальной религиозной идеологии, распространяемой через деятельность различного рода сект остаётся не решённой. Хотя у государственной власти в лице её государственных органов имеются средства и возможности для активизации работы в этом направлении через подконтрольные средства массовой информации, посредством использования возможностей социальной рекламы направленной на противодействия различного рода антисоциального поведения. Посредством внесения изменений в законодательные акты, регулирующие деятельность общественных религиозных организаций на территории России, направленных на пресечение возможностей легализации деятельности деструктивных религиозных организаций. Посредством использования возможностей административного ресурса в ликвидации средств массовой информации учреждённых данными религиозными организациями и распространяющими через свою печатную и электронную продукцию деструктивную религиозную идеологию среди населения нашей страны.

Дианов М.М.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
информационных технологий, механики и оптики
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РОССИИ В УСЛОВИЯХ ГЛОБАЛЬНОГО
ИНФОРМАЦИОННОГО ОБЩЕСТВА**

Научные открытия и изобретения ученых, воплощенные инженерами в средства информатизации и телекоммуникаций, приближают общество к качественно новому рубежу своего развития, когда информационные услуги будут определять и обеспечивать основу его существования. Глобальные информационные сети и системы, в том числе и сеть "Интернет", являются важнейшим фактором ускорения мирового прогресса, технологической основой международного информационного обмена. Более того, на них ложится колоссальная экономическая нагрузка, которая возрастает на наших глазах буквально в геометрической прогрессии. В этих условиях информационные ресурсы представляют огромную материальную ценность, а несанкционированный доступ к этим ресурсам, если они недостаточно защищены, может привести к глобальным катастрофам или, в условиях конкуренции корпораций, фирм и целых государств, может радикально изменить ситуацию в пользу получившего такой доступ. Именно поэтому развитие информационных технологий во всем мире и, естественно, в нашей стране, проходит в условиях действия двух противоречивых, но и взаимосвязанных факторов. Первый – это нарастание попыток несанкционированного доступа к информации в целях ее получения, подделки, копирования либо

уничтожения, иного использования в ущерб законному владельцу. При этом интеллектуальная и техническая оснащенность злоумышленников непрерывно возрастает и практически никогда не отстает от возможностей создателей и владельцев информационных ресурсов, подвергающихся таким атакам. Второй фактор, действующий на развитие информационных технологий – это меры и усилия, принимаемые владельцами информационных ресурсов по созданию и внедрению надежных мер их защиты. Важной составляющей систем защиты информации в современных информационных и телекоммуникационных системах являются криптографические средства.

В свете положений утвержденной Президентом России Доктрины информационной безопасности приоритетное значение должно уделяться вопросам информационной безопасности информационных и телекоммуникационных систем. Представляется, что для её надежного обеспечения необходимо сближение, а в идеале – совмещение процессов разработки новых информационных технологий, создания для них систем безопасности информации и формирования необходимой нормативной и законодательной поддержки.

Дончевская Л.В.

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

ИНФОРМАЦИОННАЯ ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ И ЕЕ СТРУКТУРА

Информационная экономическая безопасность представляет качественно новый тип экономической безопасности, так как сама информационная экономика пришла на смену индустриальной, зародилась на ее базе, но вместе с тем имеет и собственные, принципиально отличные черты. Особенность ее функционирования определяется глобализацией современной экономики и осуществлением хозяйственной деятельности на основе разделения труда в едином информационном пространстве.

Содержание информационной экономической безопасности последовательно раскрывается в процессе изучения ее структуры, представляющей собой совокупность важнейших элементов и их взаимосвязей. К элементам структуры информационной экономической безопасности относят четыре главных, тесно связанных между собой, компонента: безопасность информационного производства, безопасность образовательной системы, безопасность материального производства, безопасность системы здравоохранения, социального, правового и иного обеспечения членов общества. Рассмотрим эти компоненты в порядке их значимости для осуществления безопасности информационной экономики.

Выделение в структуре безопасности информационной экономики указанных четырех основных компонентов является довольно условным. Специфика безопасности информационной экономики и всех основных компонентов заключается в том то, что во всех ее основных структурных компонентах либо доминирует, либо хорошо заметно обеспечение безопасности интеллектуального, творческого труда. Это обстоятельство объединяет все сектора безопасности информационной экономики и позволяет рассматривать обеспечение безопасности умственной деятельности в них как безопасность единого интеллектуального производства.

Таким образом, для безопасности информационной экономики характерна своя структура, отличительными особенностями которой являются отсутствие четкого отраслевого деления, характерного для экономической и информационной безопасности, высокая интеллектуальная насыщенность обеспечения безопасности, безопасность единого информационного пространства.

Дудкина О.К., Копыльцов А.В.

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

СОЗДАНИЕ ГОРОДСКОГО МОНИТОРИНГОВОГО ЦЕНТРА ЭКСТРЕМАЛЬНЫХ СИТУАЦИЙ

Во исполнение постановления Правительства Российской Федерации, от 31.12.2004 № 894 «Об утверждении перечня экстренных оперативных служб, вызов которых круглосуточно и бесплатно обязан обеспечить оператор связи пользователю услугами связи, и о назначении единого номера вызова экстренных оперативных служб» Правительством Санкт-Петербурга с января 2007 года проводятся работы по созданию Городского мониторингового центра Санкт-Петербурга (далее ГМЦ) – государственного учреждения, осуществляющего учет, анализ и обработку сообщений об экстренных событиях и нештатных ситуациях, возникающих в черте города, отслеживание оперативной обстановки на городских объектах и в местах проведения массовых мероприятий, формирование доступных механизмов для оперативной передачи информации от населения Санкт-Петербурга по экстренным ситуациям в компетентные учреждения и ведомства, а также обеспечивающего координацию действий оперативных и диспетчерских служб города в рамках обработки данных по экстренным ситуациям.

С этой целью, на базе ГМЦ Санкт-Петербурга, выполнены следующие мероприятия: разработана и согласована всеми заинтересованными ведомствами, схема автоматизированного приема, учета и обработки экстренных вызовов на территории Санкт-Петербурга единой городской службой; создана единая коммуникационная структура города, позволяющая решать вопросы

связанные с приемом экстренных вызовов, их обработки и реагирования; разработан и внедрен в опытную эксплуатацию программно-технологический комплекс Центра обработки экстренных вызовов и обращений граждан на двух территориально-распределенных, взаимно резервирующих площадках, позволяющих одновременно осуществлять прием 60 операторами; разработаны и утверждены регламенты информационного взаимодействия ГМЦ Санкт-Петербурга с ведомственными дежурно-диспетчерскими службами; на основе утвержденных административных регламентов разработана и принята в опытную эксплуатацию система информационного взаимодействия ГМЦ Санкт-Петербурга и дежурной части ГУВД по Санкт-Петербургу и Ленинградской области, обеспечивающая прием, регистрацию и дальнейшую обработку поступающих экстренных вызовов и электронных сообщений; на основе утвержденных административных регламентов начата опытная эксплуатация системы информационного взаимодействия ГМЦ Санкт-Петербурга и ГУ «Центр управления силами ФПС по Санкт-Петербургу»; обеспечена интеграция автоматизированной информационной системы ГМЦ Санкт-Петербурга с городской системой видеонаблюдения и системой мониторинга стационарных и мобильных городских объектов, что позволило обеспечить комплексный подход к мониторингу оперативной обстановки в городской черте; осуществлена необходимая штатная реорганизация учреждения, произведен дополнительный набор и обучение операторов дежурных смен, выполнена полная модернизация аппаратно-программного комплекса и материально-технической базы ГМЦ. Городской мониторинговый центр Санкт-Петербурга является основным структурным элементом системы обеспечения безопасности жизнедеятельности Санкт-Петербурга. ГМЦ обеспечивает эксплуатацию основных подсистем АИС ОБЖ, в том числе: 1. Локальный узел систем мониторинга подвижных и стационарных объектов – интегрирующий узел различных мониторинговых систем, отслеживающих состояние объектов городской инфраструктуры, в т.ч. охранные и пожарные сигнализации, системы экстренного вызова милиции; 2. Главный центр видеонаблюдения 3. Монитор оперативной обстановки – интегрирующий узел дежурных служб 01, 02, 004 (03 в перспективе) формирующий ленту происшествий, зарегистрированных данными службами, а также процесс отработки каждого происшествия. 4. Автоматизированная информационная система ГМЦ – Coll-центр позволяющий осуществлять прием экстренных обращений граждан, обработку их, интеграцию с АИС ведомств при передаче данных обращений по системе электронной связи. В настоящее время завершаются работы по интеграции нового программно-технологического комплекса ГМЦ с информационными системами организаций жилищно-коммунального хозяйства и предприятий инженерно-энергетического комплекса города, а также по обеспечению интеграции с городской геоинформационной системой. Помимо этого прорабатываются вопросы взаимодействия ГМЦ Санкт-Петербурга с городской станцией скорой медицинской помощи.

Иванов В.П.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ИНФОРМАЦИОННЫЕ АСПЕКТЫ КУЛЬТУРНОЙ БЕЗОПАСНОСТИ**

Проводимая в настоящее время борьба за чистоту и сохранение норм русского языка представляет собой только один из аспектов сложной проблемы – культурной безопасности России. Даже беглый взгляд на прилавки книжных магазинов и журнальных киосков показывает, что внедряется определенный стереотип о «герое нашего времени» – как правило, это бандит, бизнесмен или его окружение, сотрудник правоохранительных органов. Причем зачастую по сюжету между этими категориями людей весьма условна. Как следствие, в книжных магазинах найти нормальную литературу также трудно, как и в эпоху дефицита. Практически мало отличаются от выпускаемых книг демонстрируемые на экранах телевизионные фильмы, передачи. Сплошь и рядом через СМИ внедряются в общественное и индивидуальное сознание далеко не лучшие стереотипы западной цивилизации и «популярности», включая явную или неявную пропаганду насилия. Вывески на иностранных языках на улицах городов, раскручивание «шедевров» массовой культуры в итоге увязаны с низким качеством учебников. Несомненно, что указанные факты оказывают негативное влияние на воспитание молодежи. Необходимо отметить, что пониженное внимание к таким проблемам способствует росту деструктивных тенденций в социуме, особенно проявляющиеся в кризисные периоды. Помимо всего прочего это свидетельствует об отсутствии действенной и долговременной государственной и региональной политики обеспечения культурной безопасности. Все виды безопасности государства тесно увязаны между собой. Поэтому, например, не представляется возможным обеспечить достаточный уровень экономической безопасности в отрыве от безопасности культурной.

Формирование и развитие культурного слоя в общественном сознании во многом происходит через многочисленные информационные каналы. До сих пор исследовались только отдельные аспекты этой проблемы. Проведение комплексных исследований – насущная задача нашего времени.

Колин К.К.

**Россия, Москва, Институт проблем информатики РАН
КАЧЕСТВО ЖИЗНИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ**

В Стратегии национальной безопасности Российской Федерации на период до 2020 года, которая утверждена Указом Президента России 13 мая 2009 года, качество жизни населения рассматривается как один из важнейших факторов обеспечения национальной безопасности страны.

В 2007 году в России издана монография известного американского специалиста в области изучения глобальных проблем развития цивилизации Элвина Тоффлера «Революционное богатство». В ней показано, что на современном этапе развития научно-технологической революции традиционные представления о качестве жизни у многих миллионов людей существенным образом изменяются.

Качество жизни современного человека все больше определяется способностью общества предоставлять ему необходимые информационные продукты и услуги, т.е. информационным качеством самого общества. Именно поэтому в последние годы и появились такие новые понятия, как информационная бедность и информационное неравенство.

По мнению Э. Тоффлера, в информационном обществе будут совсем другие, отличные от традиционных, представления о структуре личного, корпоративного и национального богатства.

В феврале 2008 года в области информационного развития нашей страны произошло важное событие – утверждена Стратегия развития информационного общества в Российской Федерации на период до 2015 года.

В настоящее время по темпам развития процесса формирования информационного общества Россия существенно уступает не только передовым странам Запада, но также и таким развивающимся странам, как Китай, Индия и Малайзия. Причем, это отставание в последние годы не сокращалось, а продолжало нарастать.

Главные причины этого отставания эксперты видят в недостаточной развитости информационной инфраструктуры нашей страны, а также в неравномерности информационного развития ее регионов. Называют и еще две причины: снижение эффективности системы административного управления в России после ее реформирования, проведенного в 2004 году, а также недостаточный уровень информатизации сферы образования.

Несмотря на то, что Совет по развитию информационного общества в России возглавил лично Президент РФ Д.А. Медведев, а указанная выше Стратегия развития информационного общества была утверждена еще в феврале 2008 года, комплексный план действий по реализации основных положений этой Стратегии до сих пор не утвержден Правительством РФ.

Развитие информационного общества в России является сегодня не столько инструментально-технологической сколько информационно-психологической проблемой, для решения которой необходимо изменить общественное сознание и, в первую очередь, ментальность наших федеральных и региональных чиновников.

В условиях глобального финансово-экономического кризиса, который сегодня охватил практически все страны мира, в том числе и Россию, социальное значение информационного развития общества существенным образом возрастает.

В России, с ее колоссальной по протяженности территорией, указанные выше проблемы могут быть эффективно решены лишь на основе существенно более широкого использования методов открытого образования и дистанционного обучения на базе современных ИКТ.

По данным официальной статистики, количество безработных в России уже превысило 2,1 млн. человек и продолжает расти. Это серьезная социальная проблема, над решением которой сейчас работают органы государственной власти в центре и на местах, а также руководители структур бизнеса. Однако, возможности новых информационных технологий при этом практически не используются.

Решение о создании в России первых четырех специализированных ИКТ – технопарков было принято Президентом России В.В. Путиным еще в 2004 году после его посещения одного из аналогичных индийских технопарков в штате Бангалор. Сегодня реализуется государственная программа создания таких технопарков в Сарове Нижегородской области, Санкт-Петербурге, Новосибирске и Дубне Московской области. Планируемые сроки ввода в действие технопарков – 2010–2011 гг. Наиболее крупный из них создается в Дубне. В нем будет работать около 10 тыс. программистов, для которых уже строится городок на 30 тыс. жителей.

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

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

Россия, Москва, Институт системного анализа РАН

АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС ОБЕСПЕЧЕНИЯ АНТИТЕРРОРИСТИЧЕСКОЙ БЕЗОПАСНОСТИ (НА ПРИМЕРЕ ТРАНСПОРТНОГО КОМПЛЕКСА)

В докладе описывается созданный коллективом разработчиков ИСА РАН аппаратно-программный комплекс «РискДетектор», реализующий в режиме диалога «ЭВМ – пользователь» основные процедуры обеспечения транспортной безопасности, определенные директивными документами. Идеология комплекса была разработана и опубликована ранее и предполагает, что система управления рисками нарушения транспортной безопасности строится на основе категорирования объектов транспортной инфраструктуры и транспортных средств путем оценки возможного ущерба при реализации угроз террористического воздействия. Комплекс обеспечивает построение структурной модели объекта с выделением уязвимых (критических) точек возможной реализации угроз, построение модели угроз и соответствующих профилей защиты объекта, проверку степени выполнения входящих в состав профиля защиты требований по обеспечению антитеррористической безопасности и расчета рисков возможной реализации угроз. Комплекс также способен определить необходимый состав мероприятий (организационных мер и технических средств) с учетом ограничений на их стоимость и формировать планы мероприятий, необходимых для обеспечения безопасности при изменении внешних и внутренних условий.

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

Корт С.С.

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

ОРГАНИЗАЦИЯ ДОСТУПА НАСЕЛЕНИЯ К ИНФОРМАЦИОННЫМ РЕСУРСАМ МУНИЦИПАЛЬНЫХ ОРГАНОВ

В настоящее время муниципальные органы являются наиболее близкой к населению властной структурой. Как следствие этого целесообразным является использование вычислительной системы муниципальных органов как своеобразного «посредника» между населением и информационными ресурсами региональных и федеральных органов. Являясь таким посредником, вычислительная система муниципальных органов может предоставлять данные о:

- 1) населению в соответствии с требованиями закона о персональных данных для использования в вычислительных системах региональных и федеральных органов;
- 2) деятельности муниципальных органов в вычислительные системы региональных и федеральных органов, а также населению.

На требования по безопасности, предъявляемые к функционированию вычислительных систем муниципальных органов, оказывают влияние следующие федеральные законы: «О персональных данных» от 27 июля 2006 года № 152–ФЗ, «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149–ФЗ. С 1 января 2010 года вступает в силу Федеральный закон от 9 февраля 2009 года № 8–ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

Как следствие данной ситуации желательно внедрить механизмы безопасности в вычислительные сети муниципальных органов и федеральных органов, отвечающие за хранение и обработку информации в вычислительной системе, а также за передачу информации за ее пределы.

Рассматривая архитектурные требования к вычислительной системе можно отметить то, что для связи с федеральными и региональными органами желательно иметь единую точку входа для муниципальных органов к информационным ресурсам федеральных органов. Наличие единой точки входа в виде портала позволяет интегрировать вычислительные системы муниципальных и федеральных органов уже на уровне пользовательского интерфейса, формируя его в унифицированном и единообразном виде.

Кроме того, желательно организовать доступ к ресурсам в форме тонкого клиента на базе веб-браузера, а в качестве форматов данных – *.txt (текстовый документ), *.odt (текстовый документ формата Open Document Text), *.html (гипертекстовый документ).

Рассматривая функции защиты, следует отметить необходимость присутствия в вычислительной системе средств защиты, реализующих следующие функции: надежную аутентификацию абонентов, нормализация и обезличивание информации, а также защищенность системы. При получении пользовательской информации, а также при передаче информации между вычислительными системами муниципальных и федеральных органов должна выполняться нормализация данных, включающая следующие процедуры:

- 1) Проверка отсутствия атак, использующих формы ввода.

2) Очистка данных от персональной информации в том случае, если они могут быть переданы за пределы информационной системы.

3) Очистка конфиденциальной информации.

Рассмотренные выше требования должны найти отражение в профиле защиты, который должен быть разработан для вычислительной системы муниципальной организации в соответствии с требованиями ГОСТ.

Курнос В.И., Хузин В.З.

**Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»
ПРОБЛЕМЫ РАЗВИТИЯ И СОВЕРШЕНСТВОВАНИЯ ТЕРМИНОЛОГИИ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА СОВРЕМЕННОМ ЭТАПЕ**

Анализ имеющихся в ФГУП «НИИ «Рубин» документов по терминологии в области информационной безопасности (ИБ) показал, что выполнение работ по уточнению некоторых терминов в области информационной безопасности связано с проблемами создания единой терминологии для специалистов-разработчиков с учетом изменений, которые произошли в лексическом составе русского языка к началу XXI века, а также в известной нормативно-технической документации и монографиях, опубликованных в период с 2001 по сентябрь 2008 гг.

Предлагается при разработке этой единой терминологии выполнить следующие приоритетные работы по созданию такой терминологии, которая бы обеспечивала доступ к информационным ресурсам (ИР) систем управления различными сетями связи:

1) создание единой терминологии для всех органов управления Российской Федерации (РФ) целесообразно выделить в отдельную целевую программу в рамках Государственной программы вооружения (ГПВ), в которой техническую основу единой терминологии должны составлять унифицированные платформы транспортной сети, комплексной безопасности связи и информации, а также управления связью;

2) уточнение (корректировка при необходимости) ТТЗ на ведущиеся ОКР по созданию автоматизированных и информационных систем с целью обеспечения унифицированного доступа к информационным ресурсам с применением ресурсов органов управления Единой информационной системы связи РФ;

3) корректировка ГОЗ-2009 (ГОЗ-2010), предусматривающая: определение первоочередных информационных потребностей для различных органов военного управления и порядка формирования ИР;

4) создание и выработка механизмов координации работ по проблемам информационных, автоматизированных систем и систем связи РФ.

Выполнение перечисленных выше приоритетных работ невозможно без анализа уже имеющихся в ФГУП «НИИ «Рубин» терминов, вошедших в Путеводитель по терминологии в области связи и их коррекции с учетом новых требований к разработке стандартов на термины и определения. Отсутствие гостированных определений, например, таких терминов, как: ПРОСТРАНСТВО, ИНФОРМАЦИЯ, ЕДИНОЕ, ВООРУЖЕННЫЕ СИЛЫ РОССИИ, не позволяет дать определение термину «Единое информационное пространство Вооруженных Сил России».

Предметом (объектом) исследования является «МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ».

МЕТОДОЛОГИЯ – совокупность приемов исследования, применяемых в научном познании мира. В данном случае речь идет о разработке совокупности приемов исследования, применяемых в научном познании определенного перечня терминов, используемых специалистами-разработчиками и заказчиками специальных систем, сетей и комплексов технических средств Вооруженных Сил РФ. Формирование единого информационного пространства – это ПРОЦЕСС.

ЕДИНОЕ ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ – это ОБЪЕКТ. Поэтому тема «МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ» звучит корректно и является актуальной, так как независимо от нас существуют элементы среды внешнего мира, имеющие отношение к ЕДИНУМУ ИНФОРМАЦИОННОМУ ПРОСТРАНСТВУ ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ, которое в динамике всегда изменяется под воздействием каких-то факторов, способных изменить качество функционирования ОБЪЕКТА.

В постановке задачи на разработку этого ОБЪЕКТА сформулированы основные требования, которые Заказчик предъявляет к ОБЪЕКТУ с учетом всех этапов его жизненного цикла. Остается разобраться в том, как ТЕМА проекта соответствует СОДЕРЖАНИЮ, раскрытого в ДОКУМЕНТЕ, представленном на рассмотрение и как СОДЕРЖАНИЕ соответствует ПРЕДМЕТУ проведенного исследования и как выполнены основные требования, предъявляемые к этому ДОКУМЕНТУ.

Лясович Т.Г.

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

ИЗ ИСТОРИИ СОЗДАНИЯ И ФУНКЦИОНИРОВАНИЯ ОРГАНОВ ФАПСИ В РОССИИ (1991–2003г.)

В современном мире информация давно стала стратегическим национальным ресурсом, одним из основных богатств экономически развитого государства. Быстрое совершенствование информатизации в России, проникновение ее во все основные сферы жизнедеятельности повлекло за собой появление ряда проблем, связанных с защитой информации. Очевидно, что государство, взяв на себя всю полноту ответственности при решении этого вопроса, особое внимание уделяет созданию целой системы защиты информации, которая, в свою очередь, является неотъемлемой частью общей системы безопасности страны.

При этом особую роль приобретает защита правительственной связи и информации как важного инструмента успешной работы органов государственной власти и управления. В свете проводимых реформационных преобразований определенное значение приобретает рецепция исторического опыта создания специализированных структур и их деятельности в сфере обеспечения информационной безопасности. В 90-е годы особое место в этой сфере занимали органы ФАПСИ - Федерального агентства правительственной связи и информации. Примечательно, что большинство сведений, связанных с ФАПСИ, до сих пор носит секретный характер, что не позволяет ссылаться на конкретные источники.

Структурой, непосредственно предшествующей ФАПСИ, был Комитет правительственной связи при Президенте СССР, возникший при разделе КГБ СССР после августовского путча (Указ Президента СССР № УП-2484 от 29 августа 1991 г.) Председателем Комитета 25 сентября 1991 года был назначен А.В.Старовойтов. 10 октября 1991 года Президентом М.С.Горбачевым было утверждено Положение о Комитете правительственной связи, который определялся как союзно-республиканский комитет. В состав Комитета вошли: Главное управление правительственной связи; Главное управление безопасности связи; Главное управление радиоэлектронной разведки средств связи; Информационно-аналитическое управление; Управление правительственной связи РСФСР (по согласованию с Президентом РСФСР); Управление по работе с личным составом; Хозяйственное управление; Военно-строительное управление; Финансово-плановое управление; Коммерческая служба; Организационно-мобилизационный отдел; Юридический отдел; Секретариат; Служба безопасности; Научно-технический совет; Пресс-центр; архивы; Академия криптографии; Орловское высшее военное командное училище связи; Научно-технический центр (в составе Главного управления безопасности связи). 24 декабря 1991 года указом Президента Российской Федерации № 313 было создано Федеральное агентство правительственной связи и информации при Президенте РФ на базе Комитета правительственной связи при Президенте СССР. Генеральным директором ФАПСИ был назначен А.В.Старовойтов.

Правовую основу деятельности федеральных органов правительственной связи и информации составляли: Конституция Российской Федерации, Федеральные законы: "О безопасности" № 196 от 10 декабря 1995 г.; "Об обороне" № 61 от 31 мая 1996 г.; "О внешней разведке" № 5 от 10 января 1996 г.; «О федеральных органах правительственной связи и информации» № 4524 от 19 февраля 1993 г., другие законы Российской Федерации, а также принимаемые в соответствии с ними нормативные акты Президента Российской Федерации и Правительства Российской Федерации.

В ст. 1 Федерального закона «О федеральных органах правительственной связи и информации» (с изменениями от 24 декабря 1993 г.) определялись следующие задачи новой силовой структуры, а именно:

- обеспечение высших органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации, центральных органов федеральной исполнительной власти, Совета безопасности Российской Федерации (далее - государственные органы), организаций, предприятий, учреждений специальными видами связи и информации;
- организация деятельности центральных органов федеральной исполнительной власти, организаций, предприятий, учреждений по обеспечению криптографической и инженерно-технической безопасности шифрованной связи в Российской Федерации и ее учреждениях за рубежом;
- осуществление государственного контроля за этой деятельностью.

Таким образом, основная задача по организации правительственной связи и обеспечению ее безопасности, в соответствии с законодательством Российской Федерации, была возложена на органы правительственной связи и информации. В соответствии с ФЗ «О федеральных органах правительственной связи и информации», система органов правительственной связи и информации включала в себя следующие элементы:

- Федеральное агентство;
- органы правительственной связи и информации в субъектах РФ (центры правительственной связи, информационно - аналитические органы) в субъектах Российской Федерации;
- войска правительственной связи, которые включали части радиоразведки и инженерно - строительные части;
- учебные заведения;
- научно-исследовательские организации;
- предприятия.

Кроме того, при Федеральном агентстве действовала Академия криптографии Российской Федерации.

Так была выстроена целая система органов правительственной связи федерального подчинения, предназначенная для защиты государства от внешних и внутренних информационных угроз. В рамках нее Федеральное агентство ведало организацией и руководством всех работ по направлениям деятельности федеральных органов правительственной связи и информации: издавало приказы, указания, положения, инструкции и другие нормативные акты, обязательные для исполнения в системе федеральных органов правительственной связи и информации. Органы правительственной связи и информации в субъектах Российской Федерации входили в систему органов государственного управления и осуществляли на соответствующей территории руководство в области организации и обеспечения правительственной связи, иных видов специальной связи и информации, сбора и передачи информации экономического характера в интересах государственных органов; в пределах своей компетенции они непосредственно проводили работу по основным направлениям деятельности федеральных органов правительственной связи и информации. К их ведению относились координация и контроль деятельности подчиненных им подразделений, а также обеспечение государственных органов специальными видами связи и информации.

Следует отметить, что важной стороной деятельности органов ФАПСИ являлась и реализация положений Доктрины информационной безопасности РФ, утвержденной Президентом РФ в 2000 году, а именно:

- обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России;
- развитие современных информационных технологий и обеспечение создания и эффективного использования в интересах органов государственной власти отечественных информационных ресурсов (Доклад Генерального директора ФАПСИ В.Г.Матюхина на открытии Всероссийской конференции «Информационная безопасность России в условиях глобального информационного общества» от 5 февраля 2001 г.). При этом отмечалось, что «специалисты ФАПСИ совместно с предприятиями-лицензиатами Федерального агентства ведут кропотливую работу по созданию, внедрению и развитию криптографических средств защиты информации» В целях обеспечения и развития защищенной технологической основы управления страной была создана Информационно-телекоммуникационная система специального назначения в интересах органов государственной власти.

В 2003 году Президентом РФ В.В.Путиным была произведена реорганизация силовых структур, которая «ликвидировала параллелизм» в работе спецслужб (Указ Президента Российской Федерации от 11 марта 2003 г. N 308 "О мерах по совершенствованию государственного управления в области безопасности Российской Федерации"; Указ Президента Российской Федерации N 306 «Вопросы совершенствования государственного управления в Российской Федерации» от 11 марта 2003 г. ФАПСИ прекратило свое существование. Согласно ЦОС ФСБ, решение Президента значительно повысило эффективность работы и управляемость различных звеньев спецслужб, оптимизировав их деятельность. Кроме того, реорганизация существенно сократила расходы бюджета на содержание силовых ведомств, поскольку при образовании ФАПСИ и ФПС в свое время была значительно увеличена численность сотрудников, созданы новые административные, технические и хозяйственные аппараты.

Основными преемниками ФАПСИ стали ФСО и ФСБ. ФСО были переданы: первый главк – правительственная связь, войска правительственной связи, главные управления информационных ресурсов и информационных систем, орловская академия и воронежский институт. В состав ФСБ вошли: второй главк (безопасность связи, дешифрование, криптография), войска радиоэлектронной разведки, научные учреждения и другие подразделения.

Резюмируя сказанное, отметим, что ФАПСИ активно взаимодействовало с Санкт-Петербургским университетом МВД России. В частности, в 1995 – 1999 гг. на базе Университета (тогда Санкт-Петербургского юридического института МВД России, затем – Санкт-Петербургской Академии МВД России) была создана отдельная учебная группа ФАПСИ. Слушатели направлялись на учебу непосредственно федеральным агентством, заключали с ним контракт и по окончании учебы обязывались работать в органах правительственной связи. После обучения большинство слушателей получили назначения в подразделения ФАПСИ. Таким образом, можно говорить об удачном завершении эксперимента и об участии Санкт-Петербургского университета МВД в экспериментальной программе подготовки кадров для Федерального агентства правительственной связи и информации.

Полонский А.М., Космачев В.М.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
аэрокосмического приборостроения**

ПРАКТИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ КОРПОРАТИВНОЙ ПОЛИТИКИ ДОСТУПА В ИНТЕРНЕТ

В любой компании, имеющей достаточно развитую информационную систему с широкополосным доступом в Интернет, весьма актуальным являются вопросы регламентации доступа сотрудников к внешним Интернет-ресурсам. Нецелевое использование Интернет имеет

достаточное количество негативных последствий, из которых основными являются угроза информационной безопасности компании, нецелевое расходование Интернет-трафика и неэффективное использование рабочего времени сотрудников. Проблема может быть решена административными и программно-техническими средствами.

К административным мерам следует отнести различного рода организационно-распорядительные мероприятия, в т.ч. разработку, утверждение и доведение до каждого сотрудника политики информационной безопасности компании, периодического контроля действий сотрудников, выполняемого сотрудниками службы информационной безопасности компании и т.п. Очевидно, что административные меры явно недостаточны для повседневного использования, особенно для компаний с распределенной структурой и ненормированным рабочим днем сотрудников.

Основными источниками угроз и нецелевого использования ресурсов Интернет однозначно можно считать наиболее распространенные социальные сети («В контакте», «Одноклассники» и др.), IP-телефонию и Интернет-мессенджеры (например, Skype, ICQ), сетевые игры и, в определенной степени – «личную» почту сотрудников.

Программно-технические средства защиты основаны на использовании брандмауэров (межсетевых экранов или файерволов), совмещенных, в ряде случаев, с корпоративной биллинговой системой, и на доменной политике безопасности Microsoft Windows, т.е. ограничении прав пользователей на компьютерах-рабочих станциях – в частности запрете на установку программного обеспечения, активно взаимодействующего с Интернетом, без согласования с администраторами и службой безопасности компании.

Биллинговая система осуществляет блокировку нежелательных (нецелевых) ресурсов Интернет, IP-адресов, а также блокировку портов. Отметим, что для этих целей нет необходимости использовать сертифицированные автоматизированные системы расчетов (АСР), а могут быть использованы существенно более дешевые биллинговые системы, например IPStat или т.п.

Анализ работы информационных систем показывает недостаточно высокую эффективность данных решений. Практически все социальные сети имеют своих «двойников» – сайты с иными названиями, с которых осуществляется перенаправление пользователя. Эти двойники формируются достаточно быстро и администратор безопасности информационной системы не имеет возможности оперативно формировать «черный список» данных ресурсов. Данная проблема является весьма актуальной, существует много Интернет-ресурсов, руководств на тему «Если у вас закрыли В контакте», «как обойти ограничения сисадмина» и т.п. Ряд программ, активно взаимодействующих с Интернет-ресурсами (Skype, Tor Browser и др.) при установке не требуют административных привилегий и может быть установлено (и использовано) обычным пользователем.

Выходом из создавшегося положения должно быть отказ от традиционных технологий NAT и использование специальных корпоративных прокси-серверов.

В докладе рассматриваются конкретные программно-технические решения, позволяющие реализовать достаточный уровень информационной безопасности информационной системы компании.

Сальников М.А., Копыльцов А.В.

Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ПЕРСПЕКТИВЫ РАЗВИТИЯ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ В РОССИИ

В 2009-2011 годах Правительством России выделяется следующие направления развития комплексных систем безопасности (КСБ).

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

2. Создание в 2009–2011г.г. пилотных зон ОКСИОН в метрополитенах Москвы и Санкт-Петербурга. В рамках «Межведомственной комплексной программы мероприятий по совершенствованию антитеррористической защищенности метрополитенов России, утвержденной Распоряжением Правительства Российской Федерации от 27.05.2005 №682, создана комплексная автоматизированная система информационной поддержки антитеррористической защищенности метрополитена (КАСИП АЗМ). В целях дальнейшего развития предлагается интегрировать вышеуказанную систему КАСИП АЗМ в систему ОКСИОН. К 2010 году планируется подготовка презентации о взаимодействии служб ГУ МЧС России по г. Санкт-Петербургу, ГУВД по г. Санкт-Петербургу и Ленинградской области и Петербургского метрополитена по отработке сигнала «Радиационная опасность» со станции метрополитена «Чкаловская».

3. Комплексная система безопасности городов (АПК «Безопасный город»). АПК «Безопасный город» – это система, направленная на решение проблем профилактики. Она способна осуществлять реагирование не только на криминальные, в том числе и террористические угрозы, но и обеспечить предупреждение техногенных аварий, экологических катастроф, нарушения устойчивого функционирования органов управления и особо важных или опасных объектов. С этой целью предлагается создать централизованно управляемую комплексную систему обеспечения безопасности г. Санкт-Петербурга на основе созданных уже элементов обеспечения безопасности в рамках субъектов и федеральных программ, в т.ч. автоматизированной системы обеспечения безопасности жизнедеятельности Санкт-Петербурга (АИС ОБЖ), аппаратно-программных комплексов систем обеспечения общественной безопасности городов Российской Федерации (АПК «Безопасный город»), Общероссийской комплексной системы информирования и оповещения населения (ОКСИОН), системы обеспечения вызова экстренных оперативных служб («Система – 112»), комплексной системы обеспечения безопасности объектов социальной инфраструктуры (КСОБ), комплексной автоматизированной системы информационной поддержки антитеррористической защищенности метрополитена (КАСИП АЗМ). В дальнейшем данная комплексная система позволит обеспечить единый подход к развитию и эксплуатации систем безопасности в масштабе субъекта и может быть использована как типовая модель при развертывании в других регионах Российской Федерации.

Федоров А.В.

Россия, Москва, Министерство юстиции Российской Федерации

ГАРМОНИЗАЦИЯ И УНИФИКАЦИЯ ЗАКОНОДАТЕЛЬСТВА О ГОСУДАРСТВЕННОЙ ТАЙНЕ В ГОСУДАРСТВАХ–УЧАСТНИКАХ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

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

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

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

Соответствующими полномочиями наделена Межпарламентская Ассамблея СНГ (Конвенция о Межпарламентской Ассамблее государств-участников Содружества Независимых Государств от 26 мая 1995 г. (ст. 4) // Вестник Межпарламентской Ассамблеи. 1995. № 3(10). С. 224–234.), которой для обеспечения унификации и гармонизации национальных законодательств государств – участников Содружества, в частности, принимаются модельные законодательные акты (модельные кодексы и модельные законы) рекомендательного характера для формирования и осуществления согласованной законодательной деятельности государств-участников СНГ по вопросам, представляющим общий интерес, а также для приведения законодательства государств – участников Содружества в соответствие с международными договорами, как заключенными в рамках Содружества, так и иными.

В первые годы работы МПА СНГ вопросы защиты государственной тайны были учтены при разработке уголовно-правовых и уголовно-процессуальных модельных актов. В частности, они нашли отражение в принятых в качестве рекомендательных законодательных актов модельном Уголовном (Принят постановлением МПА СНГ от 17 февраля 1996 г. № 7–5. См.: Информационный бюллетень МПА СНГ. 1996. № 10. С. 83; Приложение № 1 к «Информационному бюллетеню». 1996. № 10. С. 84 – 216.) и модельном Уголовно-процессуальном (Принят постановлением МПА СНГ от 17 февраля 1996 г. № 7–6. См.: Информационный бюллетень МПА СНГ. 1996. № 10. С. 83–84; Приложение № 2 к «Информационному бюллетеню». 1996. № 10. С. 3–373.) кодексах.

Следующим этапом унификации и гармонизации в этой сфере стало принятие модельного закона «О государственных секретах» (Принят постановлением МПА СНГ от 16 июня 2003 г. № 21–10. См.: Информационный бюллетень МПА СНГ. 2003. № 31. С. 230–261).

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

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

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

Применительно к Российской Федерации это актуально в части касающейся уголовно-процессуального законодательства. Так, изучение имеющихся проблемных вопросов, возникающих при осуществлении уголовно-процессуальной деятельности по делам, связанным с государственной тайной, показывает, что не все из них получили должное разрешение в Уголовно-процессуальном кодексе Российской Федерации и необходима более детальная регламентация охраны государственной тайны в уголовном процессе (Подробно об этом см.: 1) Защита государственной тайны при осуществлении уголовно-процессуальной и оперативно-розыскной деятельности // Государственная тайна и её защита в Российской Федерации / Под общ. ред. М.А.Вуса и А.В.Федорова. – СПб., 2007. С. 300 – 333; Федоров А.В. Тайноведческий уголовный процесс // От культа секретности к информационной культуре. – СПб., 2008. С. 65 – 81).

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

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

К сожалению, разработчики Уголовно-процессуального кодекса Российской Федерации (См.: Собрание законодательства Российской Федерации. 2001. № 52 (Ч.1). Ст. 4921; 2002. № 22. Ст. 2027) не восприняли нормы модельного законодательства, и принятый кодекс, повторяя и детализируя отраженные ранее в УПК РСФСР нормы, регламентирующие особый порядок производства следственных действий по делам, связанным с государственной тайной, не содержит специальной статьи или специального раздела, отражающих все особенности охраны государственной и иных видов тайн в уголовном процессе.

В этой связи с учетом имеющегося модельного законодательства государств – участников СНГ представляется обоснованным нашедшее отражение в юридической литературе предложение выделить в Уголовно-процессуальном кодексе Российской Федерации по аналогии с разделом XVII «Особенности производства по уголовным делам в отношении отдельных категорий лиц» самостоятельный раздел «Использование в уголовном процессе сведений, составляющих охраняемую законом тайну» (См. напр.: Смолькова И.В. Гласность и тайна в уголовном процессе // Законность. 1998. № 7. С. 42.), в котором предусмотреть основания и пределы получения в процессе следственной проверки и производства по уголовному делу сведений, составляющих ту или иную охраняемую законом тайну, а также другие особенности производства по уголовным делам, связанным с государственной и иными видами тайн, и уголовно-процессуальные средства их защиты.

Кроме того, рассматривая модельное законодательство в качестве основы для унификации и гармонизации законодательств государств – участников СНГ, необходимо дальнейшее совершенствование и этой основы.

В частности, в системе СНГ в настоящее время функционирует ряд международных организаций, деятельность которых требует получения сведений, относимых национальными законодательствами к государственной тайне (государственным секретам). Однако модельное законодательство (ст. 28 модельного закона «О государственных секретах») не предусматривает возможность передачи сведений, составляющих государственную тайну, международным организациям.

В то же время в российский Федеральный закон «О государственной тайне» (ст. 18) уже включены положения о передаче сведений, составляющих государственную тайну, другим государствам или международным организациям.

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



ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Агаев Р.А.

**Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНОВ ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ,
КАК ФАКТОР УЛУЧШЕНИЯ РАБОТЫ СЛЕДОВАТЕЛЯ**

Развитие информационных систем в России привели к сближению в общении между гражданами, улучшению и ускорению производительности труда. Ранее применяемая система производства обмена информации на бумажных носителях уходит в прошлый век.

В органах предварительного следствия Архангельской области, начиная с 2008 года, нарабатан положительный опыт информатизации, который успешно используется на практике. Непосредственно в управлении установлен и функционирует сервер, который включен в общую информационную структуру областного УВД и соответственно имеет выход в общероссийскую «милицейскую» сеть. Данная ситуация привела к возможности подключения к системе городских и районных следственных отделов, что сразу же обеспечило возможность непосредственного общения между руководством и низовыми подразделениями, а также экономию государственных средств на работу с бумажными носителями.

Функцию контроля за техническим состоянием сервера, сети и программного обеспечения в следственном управлении осуществляет соответствующее должностное лицо.

Сотрудникам управления, непосредственно курирующим определенные линии деятельности, присвоены отдельные электронные адреса, так называемые «почтовые ящики». Информация в целях недопущения ей потери сохраняется как на сервере, так и на рабочих компьютерах. Соответственно для исключения несанкционированного доступа все «машины» оборудованы личными паролями включения и выхода в локальную сеть.

Учитывая появившуюся возможность производства обмена информации в режиме реального времени, сотрудниками УВД области разработан сайт, на котором размещена различная информация, касающиеся различных аспектов работы УВД, научные статьи, в том числе методические рекомендации по расследованию отдельных категорий преступлений, обзорные письма и т.д.

Следователями-методистами следственного управления на постоянной основе осуществляется контроль за ходом расследования уголовных дел различной направленности.

Так, производится редакция проектов обвинения, которые предоставляются по средствам электронной почты, производится сбор обвинительных заключений, приговоров, которые в дальнейшем проходят систематизацию и при необходимости незамедлительно направляются в низовые подразделения для практической помощи при расследовании уголовных дел.

Одновременно имеется возможность в режиме реального времени по средствам удаленного доступа запрашивать статистические данные информационного центра УВД, незамедлительно проверять анкетные данные лиц задержанных за совершения различных преступлений, в том числе и по всей территории России. В значительной степени облегчает работу наличие возможности работать с различными правовыми базами («Консультант плюс»), информационными сайтами, разработанными МВД России, СК при МВД России, а также региональными УВД.

Переход организации работы по средствам компьютерной техники привели к сокращению нарушений законности на предварительном следствии, уменьшению сроков предварительного расследования, а также предоставили возможность проводить дистанционное обучение сотрудников низовых подразделений.

Бачило И.Л.

**Россия, Москва, Институт государства и права РАН
О ПРАВЕ В СВЕТЕ СТАНОВЛЕНИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА**

Усложнение взаимодействия права и общества в условиях информатизации стало очевидным. Проблемы виртуального общения всех без исключения субъектов ставят новые вопросы перед правом и в первую очередь перед законодательством. Обостряется значимость вопросов правового регулирования внутригосударственных отношений и еще в большей мере тех отношений, которые формируются в глобальных сетях и охватывают сразу несколько систем юрисдикции. Это с одной стороны. С другой стороны – право само часть информационных ресурсов, и это требует особого внимания к правовой информации, ее состоянию, доступности, степени восприятия, защиты и

обеспечения безопасности. Эта дихотомическая зависимость права и информационных процессов с учетом бурного развития информационно-технологических процессов сильно влияет на состояние развития информационного общества.

Новые задачи, стоящие перед наукой, законодательством, в области подготовки кадров и, конечно, в области развития правосознания как законодателей, управленцев, так и всех граждан нуждаются в квалифицированном правовом регулировании. Процесс затронул сегодня все формы реализации права, и в первую очередь, права информационного.

Концепция развития информационного законодательства, сформированная в институте государства и права РАН за десятилетний период работы Сектора информационного права, определяет как бы три фронта действия законов и иных правовых нормативных актов в данной области. Первое – это развитие правовой основы информационно коммуникационных технологий (ИКТ) в составе: информационных технологий, информационных ресурсов, коммуникаций или сетевой инфраструктуры. Второе – фронтальное направление правового регулирования использования потенциала ИКТ для внедрения его в жизнеобеспечивающие сферы общества. И третье – направление правового регулирования, касающееся интеграции информационного видения всей правовой системы в свете идущих информационных процессов.

Информационные форумы, форумы и конференции по информационной безопасности, теоретический семинар по информационному праву в ИГП РАН позволили выявить ряд весьма существенных проблем для развития информационного общества и углубления взаимодействия всех отраслей права на темах информативности законодательства и его системы.

За последние два года проблемы информационного законодательства РФ, и состояние правового регулирования правоотношений в информационной сфере вызывают немало вопросов. Традиционные методы отраслевого мышления и подготовки проектов правовых регуляторов по ситуации, постфактум и с позиций отдельных отраслей и интересов ведомств сегодня явно неадекватны требованиям времени.

Определяющим сегодня должен быть общегосударственный подход к решению общесистемных проблем информатизации общества с учетом специфики регионов и конкретных областей формирования новых правовых отношений и неизбежной трансформации отношений, сложившихся еще в период т.н. модерна. Сегодня нужны методы гибкого регулирования отношений с учетом процессов вызревания гражданского общества и участия всех его компонентов в выработке согласованных действий в правовом регулировании. Оценка общественностью уже принятых законов в РФ в области информации, ИКТ, состояние правовой основы реализации ФЦП «Электронная Россия» свидетельствует о недостаточной согласованности этих законов, о пробелах в нормативном регулировании и крупных недостатках соблюдения юридической техники.

Факт появления Стратегии развития информационного общества и обновление Стратегии национальной безопасности свидетельствует о значительном повороте к реальности XXI века, к поиску путей более рационального и одновременно гуманного воздействия на развития процессов глобализации во всех направлениях жизни общества. С этих позиций следует подходить и к оценке перспектив формирования и совершенствования законодательства в области информационных процессов. Однако приходится с сожалением констатировать, что в существующих версиях плана реализации Стратегии развития информационного общества в Российской Федерации преобладающее внимание отдано техническому, менее организационному обеспечению мероприятий и их количественному измерению (штуки, число, проценты). Заметно более слабое внимание уделено разделу по правовому обеспечению.

В разделе Плана «Направления», например, по нашему мнению не хватает такой позиции как «использование ИКТ в совершенствовании государственного управления и местного самоуправления в условиях информатизации». В разделе Плана «Мероприятия» наиболее важными в области организационного обеспечения Стратегии представляются позиции, касающиеся создания системно значимых условий для успешного процесса развития информационного общества. Однако в числе раскрываемых мероприятий не отмечены задачи информационного взаимодействия на всех уровнях деятельности организаций гражданского общества и органов исполнительной власти. В Плане предусмотрены пункты по электронному документообороту. Но нет заданий по обеспечению и контролю за процессом внедрения электронных документов, ЭЦП в систему государственного и местного управления.

Важно помнить, что лишь на основе общесистемного решения по правилам документирования информации возможно ожидать эффективного решения всех прикладных направлений информатизации (образование, здравоохранение, безопасность жизнеобеспечения и др.).

Раздел нормативного правового обеспечения плана реализации Стратегии развития информационного общества – наиболее бедный по составу и конкретности. Из проекта выпала, например, связь со Стратегией информатизации судебной системы. Заметим, что упор сделан опять же на технические требования. В то время как не менее важны и организационные решения, связанные с непосредственной деятельностью организаций гражданского общества и органов

исполнительной власти на всех уровнях. А организационные моменты требуют подкрепления и конкретизации через правовые решения.

В Институте государства и права подготовлены предложения к уточнению Плана в части правового регулирования и обеспечения всех его направлений. Одним из важных направлений является укрепление в организационном и технологическом обеспечении института информационного права – правового мониторинга. По инициативе Совета Федерации Федерального Собрания Российской Федерации в этом направлении проводится большая работа, но ближайшего внимания требуют развития вопросы методологии работы с правовой информацией выработка индикаторов оценки результатов мониторинга. Предстоит дифференцированный анализ осуществления системно организованного правового мониторинга как по линии отслеживания динамики законодательства, мониторинга правоприменительной деятельности в управлении, а также в судебной системе.

Состояние законодательства Российской Федерации требует в перспективе сосредоточить внимание на разработке системно согласованного правового регулирования этой перспективной сферы развития гражданского общества и всех его компонентов в форме Информационного кодекса Российской Федерации.

Бирюков В.Ю.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АНАЛИЗ ПРОТИВОПРАВНЫХ ПРОЯВЛЕНИЙ НЕТРАДИЦИОННЫХ РЕЛИГИОЗНЫХ
ОБЪЕДИНЕНИЙ КАК ОДИН ИЗ ЭЛЕМЕНТОВ ОПРЕДЕЛЕНИЯ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ**

При разработке системы признаков противоправных проявлений, имеющих отношение в нетрадиционным религиозным организациям, их руководителям и членам, в качестве основы предлагается использовать положения действующей редакции ст. 14 ФЗ «О свободе совести и религиозных объединениях», регламентирующей основания для ликвидации и запрета деятельности религиозной организации. В настоящее время указанная статья является единственной законодательно оформленной нормой, имеющей прямое отношение к НРО, в которой содержится описание конкретных оснований для ограничения деятельности или ликвидации религиозной организации.

В «Законе о свободе совести и о религиозных объединениях» (в редакции Федерального закона от 8.12.2003 года), в ст. 14 указывается, что «основаниями для ликвидации религиозной организации и запрета на деятельность религиозной организации или религиозной группы в судебном порядке являются:

- нарушение общественной безопасности и общественного порядка;
- действия, направленные на осуществление экстремистской деятельности;
- принуждение к разрушению семьи;
- посягательство на личность, права и свободы граждан;
- нанесение установленного в соответствии с законом ущерба нравственности, здоровью граждан, в том числе использованием в связи с их религиозной деятельностью наркотических и психотропных средств, гипноза, совершением развратных и иных противоправных действий;
- склонение к самоубийству или к отказу по религиозным мотивам от оказания медицинской помощи лицам, находящимся в опасном для жизни и здоровья состоянии;
- воспрепятствование получению обязательного образования;
- принуждение членов и последователей религиозного объединения и иных лиц к отчуждению принадлежащего им имущества в пользу религиозного объединения;
- воспрепятствование угрозой причинения вреда жизни, здоровью, имуществу, если есть опасность реального ее исполнения, или применения насильственного воздействия, другими противоправными действиями выходу гражданина из религиозного объединения;
- побуждение граждан к отказу от исполнения установленных законом гражданских обязанностей и совершению иных противоправных действий».

Принимая во внимание, что главной целью работы является создание методологии предварительной оценки, предназначенной для выявления в основном латентных угрожающих факторов, проявление которых возможно прогнозировать в определённой временной перспективе, представляется оправданным объединение ряда близких по составу преступления статей УК РФ в один признак, свидетельствующий о наличии отдельных элементов противоправной деятельности либо о высокой вероятности их проявления в будущем.

Таким образом, анализ информации в отношении противоправных проявлений, имеющих отношение к нетрадиционной религиозной организации, её руководителям и членам целесообразно осуществлять по следующим параметрам:

- наличие информации об убийствах, совершённых членами организации;
- наличие информации о покушениях на убийство, совершённых членами организации;

- наличие информации о самоубийствах членов организации;
- наличие информации о попытках самоубийства членов организации;
- наличие информации о террористических или экстремистских актах, совершенных членами организации;
- наличие информации о применении организацией физического насилия;
- наличие информации о преследовании (запугивании) бывших членов организации;
- наличие информации о сборе (накоплении, систематизации, хранении) конфиденциальных сведений о лицах, представляющих интерес для организации;
- наличие информации о функционировании в составе организации незаконных вооруженных формирований;
- наличие информации о причастности руководителей или членов организации к получению, хранению или передаче информации, составляющей государственную или коммерческую тайну;
- наличие информации об употреблении руководителями или членами организации наркотических или психотропных веществ;
- наличие информации о попытках изменения существующего конституционного строя на более «совершенный» (соответствующий целям группы);
- наличие информации об отказе членов организации от получения светского образования;
- наличие информации об использовании бесплатного труда членов организации;
- наличие информации об имеющейся материальной зависимости рядовых членов организации от её руководства;
- наличие информации о мошеннических действиях, совершённых руководителями или членами организации;
- наличие информации об отказе от медицинской помощи по религиозным мотивам.

Осуществлённое, таким образом, исследование, опирающееся на анализ фактического материала, имеющего отношение к различным аспектам функционирования нетрадиционного религиозного объединения, позволит со значительной достоверностью установить уровень деструктивности изучаемой структуры.

Основной проблемой, затрудняющей сбор и систематизацию необходимых для проведения процедуры формализованной оценки данных, является низкий уровень информатизации, как исполнительных органов власти, так и правоохранительной системы, в результате чего получение необходимых сведений может занимать определённое время, в особенности, если речь идёт об анализе данных, выходящих за пределы одного региона. В то же время, современные темпы развития информационных технологий позволяют надеяться на устранение этой проблемы в прогнозируемой перспективе.

Гольцов В.Б.

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

АКТУАЛЬНОСТЬ ИССЛЕДОВАНИЯ ЧАСТНОПРАВОВЫХ ВОПРОСОВ СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ОБЩЕСТВА И ПРЕДУПРЕЖДЕНИЕМ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

В современных условиях развития общества Единая государственная система предупреждения и ликвидации чрезвычайных ситуаций Российской Федерации (РСЧС) со сложившимися внутри нее специфическими общественными отношениями охватила практически все сферы деятельности граждан и организаций. Такие общественные отношения обусловлены возникающими чрезвычайными ситуациями и обладают целым рядом особенностей, которые должны учитываться в их правовой регламентации. Тем не менее, исследования различных по своей сути отношений в деятельности РСЧС практически отсутствуют, а имеющиеся научные разработки, описывающие деятельность подразделений РСЧС, посвящены не анализу и комплексному исследованию проблемы, а системе органов названных подразделений, ее структуре, состоящей из различных взаимосвязанных структурных элементов – аппаратов управлений РСЧС, служб, отрядов, частей, инспекций, построенных по иерархическому принципу. Это обуславливает необходимость выяснения состава, структуры и особенностей законодательства, распространяющегося на различные формирования системы РСЧС, а также его места в системе российского законодательства.

Отсутствие единого механизма правового регулирования различных по своей сути правоотношений, возникающих в РСЧС, привело к увеличению количества не только нормативно-правовых актов, связанных с чрезвычайными ситуациями, но и юридических проблем, возникающих в деятельности подразделений РСЧС.

Современное законодательство в этой области является разрозненным, во многом носящим противоречивый и дублирующий характер. Его нормы часто не согласуются как между собой, так и с основополагающими отраслевыми нормативными актами, а положения ГК РФ практически не используются. Данное положение дел, несомненно, сказывается на увеличении правовых пробелов и безопасности нашего общества в целом.

В законодательстве, регулирующем различные отношения, возникающие в деятельности РСЧС, с чрезвычайными ситуациями связаны почти все нормы. Термин «чрезвычайные ситуации» употребляется во всех законах и подзаконных актах, касающихся РСЧС. Отношения в сфере РСЧС, которые связаны с чрезвычайными ситуациями, регулируются различными отраслями права: конституционным, административным, гражданским, трудовым и другими, что обуславливает необходимость изучения чрезвычайной ситуации как межотраслевого понятия, которое используется также в области здравоохранения, психологии, управления и т.д.

Актуальность рассмотрения проблем, связанных с чрезвычайными ситуациями, обусловлена и тем, что отношения, в которых участвуют подразделения РСЧС, образуются не только в области предотвращения и ликвидации чрезвычайных ситуаций, регулируемых, как правило, публично-правовыми мерами воздействия, они весьма разнообразны и имеют неоднородную природу.

Так, в частности, не исследованы, в достаточной мере, общественные отношения с участием подразделений РСЧС, не освещены вопросы правосубъектности таких подразделений, не рассмотрены договорные проблемы в деятельности РСЧС, нуждаются в правовой регламентации вопросы гражданско-правовой ответственности в РСЧС. Разнообразная сфера специфических услуг, оказываемых подразделениями РСЧС, также требует детального изучения в целях внедрения гражданско-правового регулирования. Указанные обстоятельства и определяют необходимость их тщательного изучения и исследования.

Разрешение частноправовых вопросов, которым практически не уделяется внимания в РСЧС, является оправданным и с позиции глобализации катастроф, увеличении различных аварий и других непредвиденных ситуаций. В условиях рыночной экономики частноправовые отношения приобретают свою значимость, а их правовое регулирование должно осуществляться в надлежащем порядке с помощью норм законодательства и детального выяснения юридической природы исследуемого феномена.

Дементьева Н.В., Примакин А.И.

**Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ ОВД**

Эффективность борьбы с преступностью определяется уровнем организации оперативной, следственной, профилактической работы, проводимой органами внутренних дел. В свою очередь, результаты этой работы зависят от качества информационной поддержки, поскольку основные усилия практических работников в расследовании, раскрытии и предотвращении преступлений так или иначе связаны с получением необходимой информации, именно эти функции и призваны обеспечить система информационного обеспечения органов внутренних дел, которая поддерживает в настоящее время значительный объем информации.

Широкие возможности по информационной поддержке принимаемых решений предоставляют информационно-аналитические системы.

Центральную роль здесь играет оперативный доступ к распределенным базам данных на внутриведомственном и межведомственном уровнях, а также внедрение аналитических приложений, позволяющих оперативно формировать агрегированные отчеты и рассчитывать ключевые интегрированные индикаторы, определять проблемные области, проводить многомерный анализ данных в различных разрезах и обслуживать специализированные запросы. Внедрение автоматизированных информационных систем и интегрированных банков данных в МВД России помогло более чем в 2 раза повысить раскрываемость по некоторым видам преступлений.

Создание централизованных ведомственных (в перспективе государственных) регистров позволяет существенно поднять уровень эффективности работы за счет оперативного доступа к актуальной, полной и точной информации.

Значительный эффект дает внедрение автоматизированных систем сбора и обработки данных.

Вместе с тем, большинство ОВД испытывают нехватку высококвалифицированных сотрудников в области ИТ. Их привлечение затруднено из-за недостаточного уровня оплаты труда служащих и проводимой на местах непродуманной кадровой политики.

Потребность в высокоразвитых информационных технологиях наиболее высока при обработке структурированной и регулярно обновляемой информации о большом количестве объектов, где зачастую наличие высокоавтоматизированной информационной системы является единственным экономически обоснованным способом для обеспечения прозрачности и контроля над управленческим процессом.

В своей деятельности в области обеспечения информационной безопасности и сохранности персональных данных МВД России руководствуется Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», который регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти. В соответствии с данным федеральным законом в МВД России создана информационная система персональных данных.

Для предотвращения угроз информационной безопасности используется комплексный подход, включающий правовые, организационные, технические, криптографические, программные и иные механизмы, способные обеспечить конфиденциальность персональных данных при работе с ними сотрудников ОВД в соответствии с их полномочиями. Для обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных привлекаются квалифицированные специалисты, современные средства защиты информации и эффективная система управления информационной безопасностью.

Довнар Н.Н.

Беларуссия, Минск, Институт журналистики Белорусского государственного университета
ДОСТУП ЖУРНАЛИСТОВ К ИНФОРМАЦИИ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Редакции газет, журналов, Интернет-изданий по праву относятся к субъектам информационной сферы, поскольку сбор, хранение и распространение информации – главные составляющие деятельности СМИ. Доступ к ней журналистов, с точки зрения свободы массовой информации, – это тот механизм, который помогает реализовать конституционное право каждого на получение, хранение и распространение информации. Конституция Республики Беларусь и специальное законодательство в области СМИ содержат нормы – гарантии этого права, согласно которым, физические лица имеют правомочия получать, хранить и распространять полную, достоверную и своевременную информацию о деятельности государственных органов, политических партий, других общественных объединений, иных юридических лиц, о политической, экономической, культурной и международной жизни, состоянии окружающей среды.

Однако осуществление указанных Конституцией правомочий может затрагивать права и свободы других граждан, интересы общества и государства, поэтому необходимо, чтобы пределы этих правомочий были определены как можно более точно. Уточнение пределов прав личности осуществляется по-разному, главным образом путем определения характера действий, выходящих за рамки содержания права. Иногда эти пределы можно установить исходя из принципа единства прав и обязанностей. Так, гражданин имеет право получить объективную информацию, а журналист, соответственно, обязан проверить достоверность передаваемых сведений. Однако чаще в качестве правовых средств, при помощи которых устанавливаются ограничения свободы массовой информации, что собственно и влияет на информационную безопасность, выступают юридические запреты, т.е. когда пределы правомочий определяются через указание действий, подлежащих запрету.

В новом Законе Республики Беларусь «О средствах массовой информации», который вступил в действие в начале этого года, эти ограничения устанавливаются через режим информации. Так, ограничивается доступ к сведениям, составляющим государственные секреты, коммерческую, личную или иную охраняемую законом тайну; сведениям о системе организации, об источниках, о способах, методах, планах и результатах оперативно-розыскной деятельности; материалам дознания, предварительного следствия и судебного разбирательства до окончания производства по уголовному делу; иной информации, предусмотренной законодательными актами Республики Беларусь (к законодательным актам относятся: Конституция, законы, декреты и указы Президента Республики Беларусь). Порядок, который позволяет получить информацию может быть установлен как законом, так и подзаконными актами. Например порядок предоставления информации о деятельности судов определен постановлением Министерства юстиции Республики Беларусь от 7 апреля 2006 г. "О порядке предоставления информации о деятельности общих судов Республики Беларусь для освещения в средствах массовой информации".

Определить критерии ограничений, которые достаточны в демократическом обществе, сложно, но необходимо, поскольку от обеспечения информационной безопасности зависит нормальная жизнедеятельность человеческого общества. Особенностью сегодняшнего дня является глубокая взаимосвязь свободы массовой информации, информационной безопасности со средствами информатизации, телекоммуникаций и связи, обеспечением накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Завражина С.В.

Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ВЗАИМОДЕЙСТВИЕ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ С ОРГАНАМИ
ВНУТРЕННИХ ДЕЛ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ

Функционирование каждого социального института осуществляется в рамках достижения своих целей и задач, способы решения которых индивидуальны. Эффективное взаимодействие социальных институтов возможно лишь при условии согласования их усилий, направленных на реализацию общих интересов, или посредством достижения компромисса, когда интересы различны. Mass media – главный канал формирования общественного мнения о деятельности правоохранительных органов, позитивного отношения населения к милиции. СМИ акцентируют «объект всеобщего интереса» и

одновременно выступают в качестве проводника, по которому в массовое сознание внедряют «нужные образы рациональных и эмоциональных оценок и отношений».

Одним из факторов укрепления информационной безопасности Российской Федерации является успешное плодотворное взаимодействие СМИ и ОВД, основанное на взаимном сотрудничестве и условии выполнения задач по обеспечению общественной безопасности и общественного порядка, стоящих перед правоохранительными органами и ОВД в частности. Особенно это актуально в современных условиях, когда информация, распространяемая через СМИ, а также способы и скорость ее передачи определяют ход и результаты важных, порой судьбоносных событий происходящих как на территории нашей страны, так и за ее пределами.

Применение обширных возможностей современных СМИ позволяет оперативно информировать широкий слой населения о совершенных преступлениях, осуществлять розыск преступников и вести профилактическую деятельность. Однако есть и негативные моменты при освещении деятельности органов внутренних дел, которые препятствуют осуществлению правоохранительных функций ОВД посредством разглашения конфиденциальной информации, тем самым создавая угрозу информационной безопасности страны. Примером тому может служить освещение ряда спецопераций по освобождению заложников, когда из-за низкого уровня согласованности и не продуманного взаимодействия ОВД со СМИ последние выдавали в прямой эфир все, происходящее вблизи места проведения спецоперации, подробно освещали и комментировали все действия, предпринимаемые правоохранительными органами, таким образом, информируя преступников о расстановки сил и средств, а также методах и способах, осуществляемых представителями силовых структур для предотвращения совершаемого преступления и обезвреживанию лиц его совершающих. Данная несогласованность при взаимодействии правоохранительных органов со средствами массовой информации приводила к неоправданным человеческим жертвам, значительно осложняла работу сотрудников силовых подразделений, порой ставя под угрозу срыва дальнейшее проведение спецоперации. Кроме того не редкий случай распространения оперативной информации, полученной незаконными методами, при этом представители СМИ в погоне за сенсацией и возможностью получения материальной выгоды не задумываются о последствиях разглашения данной информации, что негативно сказывается на обеспечении информационной безопасности Российской Федерации.

Подводя итог всему вышесказанному необходимо подчеркнуть, что на современном этапе развития и функционирования российского государства первостепенное значение отводится продуманной, грамотной и обоснованной государственной политики в обеспечении информационной безопасности страны, одними из основных субъектов которой являются правоохранительные органы с одной стороны, и средства массовой информации с другой, и от эффективного взаимодействия этих субъектов непосредственно зависит сохранение целостности этой безопасности.

Иванова О.М.

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

МЕСТО КОНСТИТУЦИОННОГО СУДА В СУДЕБНОЙ СИСТЕМЕ РОССИЙСКОЙ ФЕДЕРАЦИИ: ПРОБЛЕМЫ ТЕОРИИ ТОЛКОВАНИЯ ПРАВА

В науке ведется давний спор о том, что такое толкование в целом, из каких элементов оно состоит, какова его внутренняя структура как процесса, каким образом оно соотносится с юридической практикой, а также в отношении многих других проблемных вопросов теории толкования. На наш взгляд, под интерпретацией правовых актов понимается результат познавательной деятельности, совокупность значений (смыслов), которые придаются предложению правового текста и его отдельным словам и терминам, выраженный в языковой форме.

К сожалению, в нормативных актах, созданных во исполнение положений предусмотренных Конституцией не содержится понятия «толкования» и не определены его принципы и механизм. Для правоприменительной практики наибольшее распространение и значение имеет легальное толкование. Однако, возникает ряд вопросов относительно нормативного закрепления статуса судов как субъектов толкования, процедуры толкования и юридической силы актов толкования.

Этому вопросу посвящен ряд нормативно-правовых актов, закрепляющих положение судов в Российской Федерации. Полномочия на толкование закреплены в Конституции Российской Федерации только у Конституционного Суда РФ (ч. 5 ст. 125 Конституции), причем только на толкование Конституции. Ни в одном из указанных нормативных актов не дано понятия «толкования». Нормативно-правового акта, закрепляющего процессуальные основания деятельности Конституционного Суда (за исключением Регламента Конституционного Суда) не существует. Таким образом, наблюдаются некоторые пробелы в правовом статусе Конституционного Суда как субъекта толкования правовых норм.

Толкование конституционных норм имеет некоторую специфику, по сравнению с толкованием иных актов. Основным методом толкования Конституции следует считать системный способ

толкования. В основе этого способа толкования применительно к толкованию конституционных норм лежат такие технико-юридические принципы как:

- деятельность Конституционного Суда осуществляется только по запросам компетентных государственных органов или жалобам граждан, а также выражена в особом независимом судьей и механизме толкования, состоящем из нескольких этапов;

- основанием для интерпретационных выводов и их оценки выступают принципы самой Конституции – принцип самодостаточности Конституции;

- принцип самоограничения Конституционного Суда. Трудно представить что, толкуя Конституцию, Конституционный Суд не вносит политических оттенков в её содержание в соответствии с «духом времени». Корни самоограничения судей лежат в их правосознании и уровне профессиональной квалификации;

- принципы деятельности Конституционного суда коллегиальность и гласность работы судей. Нельзя не обратить внимания на особенность присущую только процедуре принятия решения Конституционным Судом как наличие и обязательное опубликование особого мнения судей;

- решение суда (постановление, определение) – содержащее в себе любое толкование, данное Конституционным Судом, является нормативным и имеет юридическую силу равную практически силе закона.

Подытоживая, отметим, роль Конституционного Суда как органа обладающего исключительным правом толкования Конституции, заключается в том, что он, не подменяя законодателя, может путем интерпретационной практики конкретизировать положения Конституции в целях снятия их неопределенности, восполнять пробелы, вызванные правотворческими ошибками. Решения конституционного Суда обладают юридической силой сопоставимой с силой самой Конституции, что оказывает существенное влияние на систему источников права. Конституционный Суд, являясь судебным органом при этом является единственным органом осуществляющим конституционную юстицию.

Кабанов А.А.

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

КЛАССИФИКАЦИЯ ИНФОРМАЦИИ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Специфическое содержание информации в органах внутренних дел продуктивнее искать не в конструировании особого определения, а путем ее классификации. Классификационные методы и процедуры являются эффективным инструментом научного познания.

В научном плане проблема классификации информации относится к одной из сложнейших в информационной проблематике деятельности органов внутренних дел. Справедливо отмечается принципиальная невозможность разработки универсальной для всех случаев классификации информации.

По источникам поступления информация классифицируется на поступающую от граждан, организаций, прокуратуры, суда, медицинских учреждений, инспекций исправительных работ, и др. К носителям розыскной информации относятся: постановления, сообщения, заявления, протоколы, заключения. Получателями же информации могут быть: подразделения уголовного розыска, исправительно-трудовые учреждения, информационные центры, адресные бюро, ГИЦ МВД России и т.д.

Информационные системы, как и любые другие системы, помимо структуры характеризуются функциями, которые они выполняют. С технологической точки зрения их функции можно подразделить на подготовительные и основные. Первые заключаются в фиксации, сборе данных, кодировании и записи их на машинные носители, вводе в память ЭВМ (в случае автоматизации) и систематизированном хранении. Вторые – сводятся к поиску или содержательной обработке информации, документальному оформлению и размножению результатов поиска и обработки, передаче выходной информации потребителям.

Для того чтобы управление было непрерывным, эффективным и безопасным, нужна определенная организация информационных процессов. С усложнением управления, а вместе с тем и с возрастанием объемов информационной работы началось постепенное отделение сбора и обработки информации от непосредственной функциональной деятельности.

Для правоохранительной сферы источниками внутренних угроз являются:

- 1) недостаточная информационно-правовая культура личного состава, которая включает в себя отсутствие у большинства сотрудников минимально необходимых знаний и навыков по обеспечению информационной безопасности;

- 2) отсутствие или ослабление общережимных мер в служебных помещениях, отсутствие или неправильное построение технических систем общей безопасности;

- 3) отсутствие или неисправность организационно-технических средств защиты информации, отсутствие звукоизоляции;

4) текучесть кадров и несвоевременное информирование вновь принятых сотрудников о мерах информационной безопасности.

Внешние угрозы создают:

- 1) действия преступников, направленные на несанкционированное получение информации;
- 2) нарушение функционирования телекоммуникационных систем, иных коммуникаций;
- 3) нарушение функционирования электропитающих сетей и устройств;
- 4) нарушения почтовой безопасности;

5) информационное воздействие, к которому относятся заведомо ложные сообщения, доносы, телефонное и радиохулиганство, выведение из строя или нарушение функционирования технических средств управления и контроля и т.п.

Карпов А.М.

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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БОРЬБЕ С НАЛОГОВОЙ ПРЕСТУПНОСТЬЮ

В нынешних условиях особую актуальность проблема защиты информации приобрела в деятельности оперативных подразделений органов внутренних дел по линии налоговых преступлений. Осуществляя первичное накопление информации о криминальной обстановке на обслуживаемой территории оперативно, управления по налоговым преступлениям ОВД аккумулируют значительный объем информации. Значительная часть накапливаемой информации относится к сведениям ограниченного распространения.

Систематизированная в результате деятельности оперативно розыскных частей по линии налоговых преступлений информация представляет огромный интерес как для отдельных криминальных элементов и группировок, так и для организаций антиконституционной направленности, партий, общественно-политических движений и средств массовой информации, стремящихся использовать для своих целей оперативно-служебную информацию органов внутренних дел.

Объективно существующие уязвимости информации оперативных подразделений органов внутренних дел по линии налоговых преступлений порождают серьезную проблему обеспечения ее защиты.

В этих условиях необходимость совершенствования организационного и нормативного обеспечения защиты информации в деятельности оперативных подразделений органов внутренних дел по линии налоговых преступлений очевидна.

Спецификой информации, получаемой в результате оперативно-розыскной деятельности, является высокая степень ее конфиденциальности. Особенностью блока информации, связанного со служебной перепиской органов внутренних дел, является то, что степень конфиденциальности содержащихся в документах сведений чаще всего изначально предопределяется отправителем. Однако если это правило безусловно выполняется по отношению к сведениям, составляющим государственную тайну, то по отношению к конфиденциальной информации (прежде всего, персональным данным, коммерческой тайне субъектов предпринимательской и иной деятельности) отправители документов не всегда в состоянии адекватно оценить уровень их конфиденциальности, и чаще всего они попадают в органы внутренних дел в потоке общей переписки открытого характера.

Спецификой блока информации, аккумулируемой оперативными подразделениями ОВД по линии налоговых преступлений в результате предварительного следствия по уголовным делам, является, безусловно (вне зависимости от содержания) высокая конфиденциальность данных, поступающих от внешних источников.

Особенностью блока информации, получаемой в результате обмена информацией с органами обеспечения государственной безопасности, является регламентация степени ее конфиденциальности этими органами.

Значительная ценность информации, накапливаемой в результате деятельности оперативных подразделений ОВД по линии налоговых преступлений, делает ее объектом внимания со стороны злоумышленников. Это обуславливает необходимость проработки организационно-правовых проблем защиты информации в деятельности оперативных подразделений ОВД по линии налоговых преступлений.

Киикова Л.К.

Россия, Санкт-Петербург, Санкт-Петербургского университета МВД России

ИДЕЙНО-ПСИХОЛОГИЧЕСКИЕ ОСНОВЫ ПРЕСТУПЛЕНИЙ ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ

В последнее время было опубликовано большое количество хранившихся ранее в архивах программных документов террористических организаций, выступлений на судебных процессах людей, осужденных за совершение террористических актов во второй половине XIX века. В этих документах, как правило, имеются данные, объясняющие причины становления той или иной организации на путь террора.

Это дает определённую возможность для изучения в политических организациях некоторых личностей революционно – террористического движения второй половины XIX века, а также то, что привело Российскую империю к такому скачку актов терроризма.

Человек сложен, в массе своей отнюдь не примитивно добр, как проповедовали просветители. В нём есть всякое, разные люди являют разные пропорции добра и зла, ума и чувства, общительности и автономности, самоуверенности и робости. И есть люди, у которых какие-то свойства доминируют.

Причины, создающие бунтарские характеры, пишет Ф.М. Лурье, могут быть очень разные: зависть ко всему и вся; комплекс неполноценности; авантюризм, желание любым способом обогатиться или какому-нибудь из образов проявить себя; жажда власти и так далее. Этот список можно продолжать достаточно долго, главное, что такие характеры весьма жалки в нравственном смысле: чем больше страсти и фанатичного стремления, тем скорее человек может переступить через моральные запреты (см.: Лурье Ф.М. Нечаев: Созидатель разрушения. М.: Мол. гвардия, 2001. С. 8.)

Идеологи того времени, по мнению автора, были уверены, в том, что с убийством самодержца и его «приспешников», они могут изменить политическую ситуацию в империи, не понимая, что на место убитого императора или других высокопоставленных лиц придут новые, продолжая политику старого режима.

Некоторые исследователи психоаналитической ориентации в качестве мотива террористической деятельности выделяют *влечение отдельных людей к смерти* (некрофилия). В частности, Ю.М. Антонян писала: «Я полагаю, что одним из таких мотивов, если иметь в виду терроризм, влекущий человеческие жертвы, выступает влечение отдельных людей к смерти, к самоуничтожению, столь же сильное, как и влечение к жизни. Иного и не может быть, поскольку влечение к смерти в известном смысле адекватно влечению к жизни, а у конкретного человека могут наличествовать обе амбивалентные тенденции. Влечение к смерти (некрофилия) объединяет значительную группу людей, считает Ю.М. Антонян, «...которые решают свои главные проблемы, сея смерть, прибегая к ней или максимально приближаясь» (Антонян Ю.М. Терроризм. Криминологическое и уголовно-правовое исследование. М., Издательство «Цит–М», 1998. С. 255.).

У них выделяется такой мотив террористической деятельности, как *самопожертвование*. Данный мотив реализуется в следующих вариантах:

а) субъект, стремится к гибели при учинении данного преступления и все делает для этого, причем он может хотеть такой «славной» смерти, чтобы напоследок привлечь к себе внимание, которого он до этого был лишен;

б) человек вполне понимает, что обязательно погибнет, но сознательно жертвует собой ради «высокой» идеи. Индивид идет на весьма рискованное для него террористическое преступление, но его сознание не охватывает реально существующий мотив самоубийства (Антонян Ю. М. Терроризм. Криминологическое и уголовно-правовое исследование. С. 257.).

На политических процессах второй половины XIX века, в качестве самооправдания своих поступков «революционеры» пытались «обелить» себя с помощью понятия «месть». Как правило, мотив мести, выражался по отношению к нежелательным политическим, государственным или религиозным деятелям в связи с их государственной, религиозной или общественно – политической деятельностью, но бывает так, что это месть простым людям, представляющим нацию, которой принадлежит государственная власть, или нацию, с которой ведется борьба, например, за спорную территорию. Объектом мести могут выступать верующие, принадлежащие к другой конфессии, их церкви, священные символы и т. д. В первую очередь это касалось южных территорий Российской империи. Отказ от мести в этих регионах, пишет В. В. Цмай, являлся позором. Обязанность по исполнению кровной мести возлагалась на старшего мужчину в роду. Время исполнения кровной мести значения не имело (Цмай В.В. Некоторые аспекты концепции насилия в арабо-мусульманской культуре // Антропология насилия / Отв. ред. В.В. Бочаров и В.А. Тишков. СПб.: Наука, 2001. С. 290). Для таких личностей гибель родных от рук властей расценивалась как оскорбление рода и являлось достаточным основанием для кровной мести.

Достаточно широкий спектр причин приводил людей к терроризму – многие из них были чисто личного характера и возникали от эмоциональных проблем и конфликтов, а не от приверженности революционной идеологии.

По мнению специалистов, психология террористической деятельности имеет существенную специфику, иногда мало понятную, если исходить из общепринятых мотивационных и поведенческих стандартов. «Эффективная антитеррористическая политика, – пишет американский исследователь Д. Хаббард, зависит от понимания того, что думают террористы, и того, почему они делают то, что делают; если мы берём самих себя в качестве модели, поведение террористов будет казаться необъяснимым» (Hubbard D.G. Winning back the sky. A Tactical Analysis of terrorism. San Francisco, 1989. P. 122.).

Можно прийти к выводу, что в какие бы одежды не рядились террористы, какие бы цели они не преследовали, какая бы не была у них мотивация преступлений – в большинстве случаев за всем этим стояло стремление испытать власть во всех ее проявлениях, привлечь к своей личности всеобщее внимание.

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

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
О РАЗРАБОТКЕ МОДЕЛЬНОГО ЗАКОНОДАТЕЛЬСТВА ГОСУДАРСТВ – УЧАСТНИКОВ СНГ
В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Процессы интеграции и формирования основ информационного общества на пространстве бывшего Союза требуют совершенствования и гармонизации национального законодательства в информационной сфере. Эти вопросы стоят в повестке дня работы Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств (СНГ). В перспективе речь идет о разработке проекта Модельного закона об информационной безопасности. Одним из ключевых моментов в этой работе представляется необходимая унификация терминологического и понятийного аппарата.

Уже сегодня необходимо обеспечить однозначность понимания терминологии. В существующей в настоящее время нормативной правовой базе законодательных актов государств СНГ основным классифицирующим признаком для понятия «база данных», например, в одних законодательных актах выступает форма её организации (Республика Беларусь), а в других – предназначение («множество данных криминального характера» - Республика Молдова). Понятие «банк данных», например, в одних случаях трактуется как «организационно-техническая система» (Республика Беларусь, Республика Молдова), а в других – как «совокупность средств» (Кыргызская Республика, Республика Таджикистан).

Отработка и согласование основных понятий для модельного законодательства является достаточно сложной задачей еще и потому, что многие, достаточно часто и широко используемые в сегодняшней практике понятия, встречающиеся в различных национальных и международных правовых и подзаконных актах, фактически не являются официально, «де-юре», принятыми на уровне законодательств. К тому же и сами формулировки ряда используемых в законодательных актах понятий далеки от строгости. (Вряд ли, например, можно считать строгим такое определение: «криптография – способ тайного письма, понятного лишь посвященным, тайнопись».)

Константинова Т.В.

**Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ИСПОЛЬЗОВАНИЕ ПОТЕНЦИАЛА ТРАДИЦИОННЫХ РЕЛИГИЙ В ОБЕСПЕЧЕНИИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОТИВОДЕЙСТВИИ ВНУТРИСЕМЕЙНЫМ
ПРЕСТУПЛЕНИЯМ**

В условиях постмодерна человек оказывается под колоссальным информационным воздействием, характеризующимся относительностью: истины и лжи, добра и зла, мира и войны, реальным и воображаемым.

Семейные ценности приобретают второстепенное значение в сравнении с ролью и значимостью индивида. Определение другого человека, как «свой» либо «чужой» затрудняется в связи с проблемой самопознания и самоидентификации. В обществе существует большое количество ложных образов и образцов поведения. Даже члены одной семьи воспринимают друг друга чужими людьми, не имея общих традиций, представляют своё прошлое и будущее по-разному. Человек готов принять виртуальные общности, «симуляционные машины». Возможно, этим объясняется совершение, так называемых немотивированных преступлений внутри семьи.

По мнению Ф. Адлера, любовь к семье является главным фактором, удерживающим от уголовной деятельности.

Профилактические возможности содержит потенциал традиционных религий. Они обеспечивают благодаря своим символам единство идеала, а значит и стремление к подобию. Во всех мировых религиях существуют указания на должное и возбраняемое поведение. Чадолюбие и семейственность особенно приветствуется в православии, семья – школа любви, домашняя Церковь.

Вера в Бога открывает масштабные цели для человека и его семьи и требует отказа от большинства субъективных интересов, вследствие чего возникает ощущение свободы. Человек чувствует единство с другими на основе духовных и гуманистических ценностей, удовлетворение от полноты жизни, сопричастность природе, смысл всего обретается в бессмертии, продолжении жизни в детях, делах, идеях.

Потакание страстям обусловлено тем, что человек забывает о себе, он как бы умирает, его «Я» прекращает своё существование, существует только страсть, но именно в этот момент возникает ощущение победы над смертью, а значит – бессмертия, которое достигается путём приношения жертвы своего «Я». Страсть сужает «Я» до размеров столь мелких, которыми можно пренебречь, любовь расширяет духовные границы человека до пределов жизни во всех её проявлениях от порхающего мотылька и растущего цветка до жизни солнечной системы и т.д.

Ф. Фильзер утверждает, что возможно уменьшить преступность, ориентируясь на сохранение традиционных духовных и гуманистических ценностей. Каждая религия заключает в себе экстракт духовной культуры, которая при ассимиляции обогащает, но не все люди могут принять плоды, чтобы

при этом не впасть в соблазн духовного блуда по православному определению. Необходимо одному человеку исповедовать одну религию для более устойчивой информационной безопасности.

Религиозные обряды с их символикой подтверждают существование социального порядка и его устойчивость. Вера в Бога рождает стремление к нравственной жизни, без чего не представляется благополучие семьи.

Масловский В.М.

**Россия, Москва, Региональный учебно-научный центр «Безопасность» МГТУ им. Н.Э. Баумана
КТО ОТВЕЧАЕТ ЗА ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ?**

Что бы ответить на вопрос, поставленный в названии надо рассмотреть взаимосвязь множества вариантов накопления, хранения, обработки и передачи персональных данных. Законодательство требует защищать персональные данные (ПД). Выпущен ФСТЭК, ФСБ и Россвязькомнадзором пакет документов, определяющих требования по защите и контролю защищенности ПД, но остаются вопросы: как выполнить эти требования и будет ли при этом создано защищенное пространство обработки и хранения ПД?

ПД граждан – это собственность государства, организации или конкретного гражданина? Это товар или нематериальный не включенный в товарооборот объект? Ответить на эти вопросы однозначно сложно, так как кроме закона о персональных данных действует ряд законов о различных видах тайн. Специалисты отмечают, что в настоящее время существует 21 категория “тайной” информации, которая закрепляется 12 Кодексами, 4 Основами законодательства, 116 законами, 53 указами Президента РФ, 142 постановлениями Правительства РФ, 546 нормативными актами министерств и ведомств, не считая, очевидно, сотен закрытых документов по этому вопросу, за накопление и сохранность которых отвечают соответствующие должностные лица и организации (обладатель информации). Документы и информация, которая в них храниться, содержит ПД гражданина (как минимум Ф.И.О. и паспортные данные или данные о документе, удостоверяющем личность) не являются собственностью гражданина. Мало того, в соответствии с этими законами получается, что данные о конкретном гражданине отделены от него и защищаются в первую очередь от него самого. Когда информация подшита в дело, (например в медицинскую карту), гражданин может только знакомиться с ней (и то только с разрешения соответствующего должностного лица), а распоряжаться ей не может, так как данная информация храниться в соответствии с требованиями законодательства в организациях или архивах.

Принят и введен в действие целый ряд нормативных документов, определяющих порядок защиты ПД, в которых требуется от любой организации выполнение одинаковых мер: 1) ведение делопроизводства; 2) контроль состояния объекта и соответствие его строго определенным требованиям по защите от утечки по каналам ПЭМИН, по защите от НСД при обработке на средствах ВТ и передаче по каналам связи. Но при этом отсутствуют требования по совместимости средств защиты различных защищенных систем и создания единого защищенного пространства жизненного цикла персональных данных.

Любое, даже самое маленькое, предприятие (менее 10 работников) обязано предоставлять информацию, относящуюся к персональным данным в налоговую инспекцию, в органы государственной власти и местного самоуправления. И каждая организация выдвигает свои требования по предоставлению информации (форматы передачи данных, средства защиты, в том числе и криптографические). Рынок средств обработки и защиты информации разнообразен, от Майкрософт до ООО «Центр безопасности информации». И, как правило, средства защиты разных организаций при установке на одну вычислительную машину «не дружат».

Крупные организации, например, налоговая инспекция, вводят свои требования к формам документов и средства защиты, а также определяют операторов связи обеспечивающих защищенную передачу информации по каналам связи, так например, «Временный регламент обмена электронными документами с ЭЦП по телекоммуникационным каналам связи в унифицированной системе приема, хранения и первичной обработки налоговых деклараций и бухгалтерской отчетности» устанавливает средства защиты и порядок передачи по защищенным каналам связи персональных данных по налоговой инспекции.

Аналогично поступает пенсионный фонд РФ и местная администрация, но каждый устанавливает свой порядок и средства защиты, не согласовывая вопросы взаимодействия, а исходя из принципа минимизации затрат. И при этом никто не несет персональной ответственности за нарушение конфиденциальности персональных данных, так как не являются собственниками персональных данных, а являются «обладателями» этой информации.

Поэтому персональные данные свободно продаются на рынке, например как базы данных налогоплательщиков, ГИБДД и городских телефонных сетей. В этой связи представляется целесообразным создание системы государственного регулирования не только требований и контроля, но и технологии защиты персональных данных.

Мефёд А.В., Старков А.А.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

О ПРАВОВОМ АСПЕКТЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ПРИМЕРЕ «SKYPE»

Действующие сегодня в Российской Федерации законы в сфере информационной безопасности отстают от технического развития и не являются достаточно гибкими для правового регулирования новых информационных технологий. В российском законодательстве практически нет ни слова про VoIP — одни белые пятна, поэтому непонятно, как серьезным игрокам развивать подобные сервисы. Действующее в России законодательство сдерживает эволюцию развития VoIP, в то время как на практике рынок VoIP в России фактически развивается согласно международным тенденциям. Напрашивается очевидное решение: сервисы на основе VoIP должны быть включены в регулятивное поле, то есть целесообразно инициировать комплексную проработку правовой модели VoIP.

Действующий сегодня федеральный закон «О связи» от 07.07.2003 № 126-ФЗ (статья 70, часть 3) требует создания российских операторов связи, отвечающих требованиям, предъявляемым к ним этим законом. В то же время компания «Skype Technologies S.A.» не имеет представительств в России. А использование IP-телефонии не позволяет государству вести контроль за переговорами, так как программы Skype не подключены к системе прослушивания телефонных переговоров, созданной в рамках СОПМ. Кроме того, в Skype используется шифрование трафика. Все это создает ситуацию, не охваченную правовым регулированием.

Интересен для изучения опыт других стран. Так, например, федеральная комиссия по связи США еще 5–6 лет назад сформировала рабочую группу для изучения вопроса. Сейчас в Соединенных Штатах от операторов VoIP требуется поддержка переноса номера от одного оператора к другому, обеспечение доступа к сервису инвалидов, выплата требуемых регулятором и другими госорганами сумм и помощь правоохранительным органам в расследовании. В Великобритании в 2007 году регулятор Ofcom представил правила работы операторов VoIP. Это требования по защите прав потребителей – в частности, операторы обязаны четко указывать, могут ли они обеспечивать связь со службами спасения и позволяют ли перенести номер к другому оператору. Регулирование в этих странах либеральное.

В Южной Корее, например, услуги VoIP могут предоставлять только зарегистрированные в госорганах операторы. Это позволяет правительству при желании добиваться от иностранных компаний необходимых уступок. И это далеко не единственная возможность влиять на рынок. Существует и другая практика. Можно, как в Панаме, обложить VoIP налогом. Можно, как в Гайане, запретить эту технологию. Или как в ОАЭ, поставить ее вне закона и заблокировать доступ к сайту Skype. Можно, как в Эфиопии, объявить использование VoIP уголовным преступлением. Эфиопское правительство пошло на такие меры, когда его доходы от услуг связи уменьшились из-за перехода жителей страны на VoIP.

Российская практика организации связи значительно отличается от сервисов других стран, где так или иначе решены вопросы регулированием VoIP. У нас сегодня, к примеру, нет даже обычного для зарубежной практики переноса номера между российскими операторами «большой тройки», о чем неоднократно говорилось. Рыночные же механизмы регулирования применяются слабо.

Осипов Я.В.

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

К ВОПРОСУ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРИМЕНЕНИЮ ПОЛИГРАФА В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Использование достижений научно-технического прогресса в уголовном процессе приобретает порой довольно неожиданные формы, о которых лет тридцать назад в России и мечтать не приходилось. К числу подобного рода новшеств в отечественной практике борьбы с преступностью относится метод тестирования с помощью полиграфа – испытания на полиграфе, «детекторе лжи». В течение последних десятилетий эти «механические следователи» получили широкое распространение: с помощью специальных аппаратов – полиграфов определяют частоту дыхания, кровяное давление, влажность ладоней и т.п. В литературе высказываются неоднозначные мнения о возможности применения данного прибора на практике.

Быстрое развитие технологии использования полиграфа привело к методически обоснованной и нормативно закреплённой необходимости его использования при опросе ряда категорий лиц.

Полиграфное устройство представляет собой многоцелевой прибор, предназначенный для одновременной регистрации нескольких (от 4 до 16) физиологических процессов, связанных с возникновением эмоций: дыхания, кровяного давления, биотоков.

Накопленный в течение десятилетий за рубежом опыт применения полиграфа в целях обнаружения у человека скрываемой информации, привел к формированию системы принципов организации тестирования с помощью этого прибора. Испытание на полиграфе складывается из трех этапов:

- предтестовой беседы;
- непосредственного тестирования с помощью полиграфа;
- послетестового собеседования (или допроса).

По мнению специалистов, предтестовая беседа является строго обязательной. Одна из первейших задач предтестовой беседы — ознакомить проверяемого с его правами в ходе предстоящей процедуры проверки (испытаний на полиграфе). Тем самым удастся снять напряжение с добропорядочных лиц и повысить тревогу у тех, кто намеревается давать ложные ответы.

После завершения предтестовой беседы проводится непосредственно сама проверка на полиграфе, которая длится в зависимости от количества решаемых задач и психофизиологических особенностей опрашиваемого от одного до нескольких.

Появление ярко выраженных, интенсивных реакций на те или иные вопросы свидетельствует о том, что эти вопросы являются для него более значимыми, чем остальные. Сопоставляя выраженность и устойчивость реакций на задававшиеся в ходе СПФИ вопросы различных вопросников, оператор полиграфа выносит суждение о субъективной значимости для данного человека этих вопросов в условиях проводимой проверки.

Общую правовую основу тестирования с помощью полиграфа в РФ создают нормы УПК об участии специалиста в следственных действиях и о возможности применения технических средств для собирания, фиксации и использования информации, а также закон «Об оперативно-розыскной деятельности» от 5 июля 1995 г. В настоящее время действует инструкция «О порядке применения полиграфа при опросе граждан» (утверждена Генеральной прокуратурой, ФСБ, МВД РФ, зарегистрирована в Минюсте России 28.12.1994 г.).

Однако отсутствие специальных законодательных актов, допускающих признание в качестве доказательств результатов тестирования с помощью полиграфа во время допроса, сдерживает развитие научных исследований в этом направлении, не позволяет в полной мере использовать возможности указанного метода для сбора доказательств. Поэтому в настоящее время этот метод на практике реализуется в основном лишь в целях получения ориентирующей, а не доказательственной информации.

Пономарев А.Л., Язовских А.Н.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
информационных технологий, механики и оптики
ПРАВОВЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ПРОТОКОЛА BITTORENT**

Одноранговые, децентрализованные или пиринговые (от англ. peer-to-peer, P2P — точка-точка) сети — это компьютерные сети, основанные на равноправии участников. В таких сетях отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и сервером. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Так сказать «С глазу на глаз».

Автор протокола BITTORENT Брэм Коэн написал этот протокол исключительно во благо человечества. Изначально идея использования пиринговых сетей преследовала цель разгрузить клиентскую машину и повысить скорость обмена информационными ресурсами. Но информационное общество несмотря на идеи создателя, превратило торрент в «пиратскую яму» нарушающую копирайт. В результате чего проецируется целый ряд конфликтных ситуаций. Так, например, если посредством пиринговой сети некто распространяет «пиратские» копии лицензионного ПО, то этим нарушается копирайт отдельных фирм-правообладателей и наносятся им огромные убытки. Если же в ответ эти фирмы инициируют приостановку работы самих пиринговых сетей, то это уже нарушает права добросовестных пользователей сети — пользователей средств информационного обмена. (Согласно российской Конституции, например, « каждый имеет право получать, искать, хранить и распространять информацию любым законным способом»). Главный вопрос заключается в том как же организовать и регламентировать эксплуатацию систем данного типа с минимизацией возможности нарушения чьих-либо либо прав.

Рзаев И.М.

**Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ МОНИТОРИНГА ЗА
СОСТОЯНИЕМ ПРИРОДНО-РЕСУРСНОГО КОМПЛЕКСА РОССИИ**

Природно-ресурсный комплекс, его состояние, качество, и изменения, обусловленные факторами естественного и антропогенного характера, — это одна из глобальных проблем, привлекающих к себе внимание многих исследователей. Для России с ее огромной территорией и запасами природных ресурсов нерешенной остается проблема их учета и контроля. Именно поэтому в 2003 году при Министерстве природных ресурсов было создано ФГУ «Российский фонд информации по природным ресурсам и охране окружающей среды Минприроды России» (ФГУ «РФИ Минприроды России»). Среди основных целей и задач фонда можно выделить:

- создание территориально-распределенного банка данных информации о недрах, водных, лесных и иных природных ресурсах, о состоянии и охране окружающей среды, экологической безопасности;

- сохранение, развитие и эффективное использование информационных ресурсов по вопросам природопользования и охраны окружающей среды и др.

При решении указанных задач используется большое количество пространственно-распределенной информации о параметрах природной среды. Часто большая часть этой информации содержится на различных географических и тематических картах, на аэро- и космоснимках. Работу с такими данными, их визуализацию, пространственный анализ и представление результатов анализа значительно облегчает использование технологий географических информационных систем (ГИС). Обладая мощными инструментами визуализации (графического представления), анализа и моделирования, позволяющими свести воедино наши знания об окружающем мире, измерения и расчеты, ГИС-технологии получают широкое распространение в сфере мониторинга, управления и планирования, предоставляя информационную основу для процедуры принятия решений.

На современном этапе в процедуре геоэкологического мониторинга центральное место занимают проблемы создания национальных информационных ресурсов по экологическим и природо-ресурсным программам на основе методов исследования Земли из космоса. Выполнен анализ влияния сетевой среды и передовых информационных технологий на структуру электронной коллекции данных дистанционного зондирования. Показано, что учет этих факторов приводит к существенным изменениям самой инфраструктуры архивации и обмена данными геоэкологического мониторинга для возможно большего круга внешних пользователей. Отмечено, что электронный архив геоэкологического мониторинга является по существу цифровой библиотекой космической информации, принципиально общедоступен и ориентирован на максимально широкое использование электронной коллекции. Использование гипертекстовых и интерактивных технологий приводит к тому, что статус архивных материалов совпадает со статусом текущих данных. Сокращается интервал между архивированием и доступом пользователя к данным. Архив мониторинга превратился в электронную коллекцию, максимально приближенную к моменту контроля экологических условий региона.

Активное построение архива спутниковых данных на базе компьютерных информационных технологий создает предпосылки к превращению электронной коллекции в место перераспределения и упорядочивания данных. Интернет обеспечивает ускоренную циркуляцию информации, что создает предпосылки для интеграции данных геоэкологического мониторинга территории России в мировую систему информационных ресурсов исследования Земли из космоса.

Савельев А.И.

Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Что бы обеспечить информационную безопасность, необходимо создать систему законодательных актов, построить на их основе институты, структуры и механизмы, взаимодействующие между собой в сфере защиты интересов субъектов правоотношений. При этом устойчивость такого комплекса должна основываться на всеобщем согласии и принятии.

Решение проблемы несовершенства системы информационной безопасности играет важную роль в современной России, так как информационная безопасность есть одна из основных составляющих системы обеспечения национальной безопасности государства в целом, во многом определяет современные условия ее (системы) успешного функционирования. Какие шаги можно предпринять, дабы изменить ситуацию?

Думается, реализация следующих задач:

- научное прогнозирование и моделирование решения возникающих проблем на альтернативной основе;

- законодательное регулирование и защита информационной деятельности при обеспечении достоверности, открытости и свободы информации;

- освобождение сознания людей от стереотипов, прекращение информационной войны политического руководства против народа.

В современной России существует целый комплекс проблем, без решения которых невозможно сдвинуть дело с мертвой точки. Что это за проблемы? Прежде всего:

- отсутствие единой системы отбора информации, подготовки и принятия решений на высшем уровне;

- отсутствие должного взаимодействия между существующими структурами обеспечения безопасности;

- отсутствие системы эффективного контроля за обеспечением безопасности как государственных структур с одной стороны, так и общества и граждан с другой.

Россия сегодня стоит перед необходимостью совершенствования системы обеспечения безопасности, в том числе в информационной сфере, и это не голословное утверждение.

Важной самостоятельной проблемой является обеспечение информационной безопасности в субъектах Российской Федерации. Эта проблема во многом обусловлена пробелами в правовом регулировании взаимодействия федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации при решении задач обеспечения информационной безопасности. Как известно, Конституцией РФ, задачи обеспечения безопасности отнесены к ведению Российской Федерации. Но вопросы информатизации, развития информационных инфраструктур отнесены к ведению субъектов Российской Федерации. Таким образом, выделяется целый большой сегмент в информационной сфере, который охватывает возможности использования современных информационных технологий в организации деятельности субъектов Российской Федерации, предполагает большую работу органов государственной власти субъектов Российской Федерации по обеспечению безопасности создаваемых ими информационных систем, сохранности государственных информационных ресурсов. Для решения этой проблемы необходимо разработать механизмы взаимодействия федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации в этой области.

Смирнова О.Г.

**Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
СПЕЦИФИКА ОБРАЩЕНИЯ С МАШИНЫМИ НОСИТЕЛЯМИ ПРИ РАССЛЕДОВАНИИ
КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ**

Одними мерами предупреждения не всегда удастся предотвратить преступное посягательство. В связи с этим возникает необходимость заниматься не только вопросами защиты средств компьютерной техники и предупреждения правонарушений, но и решать вопросы расследования преступлений в сфере компьютерной информации.

Именно информация является предметом преступных посягательств в компьютерной сфере. Она может храниться как на носителе, так и на жестком диске (винчестере) в электронно-вычислительной машине, разновидностью которой является персональный компьютер, а также в системе и сети ЭВМ на сервере (компьютере большой мощности, предназначенном для централизованного хранения и обработки информации в сети компьютеров).

Особенностями расследования преступлений в области компьютерной информации являются: привлечение специалистов при проведении следственных и оперативно-розыскных действий; особенности выдвижения и проверки следственных версий; и главное – специфические приемы работы (осмотры, изъятие, хранение и т.п.) с машинными носителями в ходе производства следственных действий.

Для следственных действий, сопряженных с изъятием ЭВМ, машинных носителей и информации, характерны ряд проблем, связанных со спецификой изымаемых технических средств. Так, например,

- необходимо предвидеть меры безопасности, предпринимаемые преступниками с целью уничтожения вещественных доказательств;
- следует иметь в виду возможность возрастания в ходе обыска напряжения статического электричества, которое может повредить данные и магнитные носители;
- при проведении обысков, выемок и изъятии машинных носителей в протоколах следует детально фиксировать не только факт обнаружения и (или) изъятия того или иного объекта, но и описывать местонахождение этого объекта во взаимосвязи с другими найденными на месте обыска объектами по правилам фиксации результатов осмотра;
- в случае если изъятие носителей информации невозможно, требуется принять меры к исключению доступа к ним заинтересованных лиц;
- недопустимо приклеивать что-либо непосредственно к магнитным носителям, пропускать через них бечеву, пробивать отверстия, наносить подписи, пометки, печати, и так далее;
- если на объекте было отключено электроснабжение, например, в связи с пожаром или взрывом, то до его включения следует проверить, находятся ли все компьютеры и периферийные устройства в отключенном состоянии;
- транспортировка и хранение компьютерной техники и информации должны осуществляться в условиях, исключающих ее повреждение;
- учитывая нестандартность обстановки, в которой может производиться осмотр места происшествия, вопрос о возможности изъятия компьютерной техники и информации, способе упаковки, транспортировки и хранения изъятых объектов должен решаться следователем в каждом конкретном случае совместно со специалистом и так далее.

Оценивая современное состояние теории и учитывая потребности оперативно-следственной практики, приходится признать, что проблемы раскрытия, расследования и предупреждения преступлений в сфере компьютерной информации изучены явно недостаточно. Между тем необходимость исследования данных проблем диктуется потребностью как практики, так и криминалистической теории и усиления ее влияния на результативность борьбы с преступлениями, совершаемыми в сфере информации и интеллектуальной собственности.

Сухов Д.К.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ВОПРОСЫ КЛАССИФИКАЦИИ И СИСТЕМАТИЗАЦИИ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ
ЭКСПЕРТИЗЫ ПО ПОИСКУ ИНФОРМАЦИИ, ОТНОСЯЩЕЙСЯ К УГОЛОВНОМУ ДЕЛУ**

Доклад посвящен разработке методики классификации и систематизации данных, полученных в результате восстановления информации расположенной на предоставленном к экспертизе носителе информации, например, накопитель на жестких магнитных дисках.

В процессе восстановления информации возникает ситуация, такая что, программа восстановления не может соотнести найденную последовательность байт к определенному формату данных, в связи с этим некоторая полезная информация разбивается на мелкие фрагментированные файлы и не может быть просмотрена стандартными средствами.

Разработана методика классификации и систематизации информации на основе бинарных сигнатур для определения формата данных и последующего приобщения этих данных к материалам экспертизы.

Проведенные с реальными машинными носителями информации эксперименты показали, что чаще в результате классификации и систематизации обнаруживаются файлы Интернет страниц (расширение htm и html), а также файлы почтовых сообщений.



БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Александров А.М.

**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»
ДЕКОМПОЗИЦИЯ ИНТЕГРАЛЬНЫХ ТРЕБОВАНИЙ ПО ВЕРОЯТНОСТИ ЛОЖНЫХ
СИГНАЛОВ В МНОГОКАНАЛЬНЫХ СИСТЕМАХ КОНТРОЛЯ**

Рассматривается некоторый сложный объект, состояние которого контролируется автоматизированной системой контроля, обеспечивающей контроль объекта по совокупности параметров. Результаты контроля образуют во времени случайный поток обрабатываемый системой. Поступающие сигналы от средств контроля могут нести информацию как об истинном состоянии контролируемого объекта (истинная информация), так и ложную, искажающую состояние объекта (ложная информация).

Рассматривается несколько алгоритмов обработки системой поступающих сигналов. По одному из них, например, для получения правильного решения системой, отражающего истинное состояние объекта, необходима истинная информация от всех контрольных средств. Ложное решение будет получено, если среди поступающих сигналов будет хотя бы один ложный. Решается задача определения требований по допустимым уровням вероятностей ложных сигналов, поступающих от контрольных средств, исходя из допустимой интегральной вероятности ложного решения системой о состоянии объекта. Исследуется влияние соотношения истинной и ложной информации, получающей от контролируемых средств, количество этих средств и др. Показано, в частности, что увеличение контролируемых средств не всегда приводит к уменьшению интегральной вероятности ложного решения системой.

Алексеев А.В., Скородумов Е.Н.

**Россия, Санкт-Петербург, ОАО «Научно-инженерный центр Санкт-Петербургского
электротехнического университета»
ОЦЕНКА ОБОБЩЁННОГО УРОВНЯ КАЧЕСТВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПРИ ИХ СЕРТИФИКАЦИИ**

При оценке качества современных технических средств защиты информации (СЗИ) одним из главных показателей их соответствия требованиям по назначению является наличие сертификата соответствующего органа по сертификации. Более того, как известно, наличие сертификата соответствия для СЗИ является в соответствии с отечественным законодательством обязательным условием для их использования в составе автоматизированных систем в защищённом исполнении (АСЗИ).

Вместе с тем, при комплексной оценке качества СЗИ, обеспечивающих одновременно решение ряда задач обеспечения информационной безопасности (ОИБ), в составе интегрированных комплексов сегодня часто используются СЗИ, имеющие одновременно несколько сертификатов. Например, сертификат, подтверждающий соответствие СЗИ техническим условиям (ТУ), т.е. подтверждающий реализацию декларированных возможностей (РДВ), сертификат по классу (от 1 до 6) средств вычислительной техники (СВТ), сертификат по классу (от 1 до 3 с соответствующими подклассами А, Б, В, Г, Д для класса 1 и А, Б – для классов 1 и 2) СЗИ от несанкционированных действий (НСД), сертификат по классу (от 1 до 5) СЗИ от недеklarированных возможностей (НДВ), сертификат по классу (от 1 до 5) СЗИ для межсетевых экранов и другие.

В этих условиях при оценке качества СЗИ, например, при рассмотрении вариантов и выборе оптимального варианта проектного решения в ходе разработки АСЗИ актуален вопрос оценки некоторого обобщённого уровня качества подсистемы или/и средств защиты информации (ПЗИ) по данным сертификации СЗИ.

В качестве такого обобщённого уровня качества СЗИ при их сертификации на основе аддитивной модели качества предложен методический подход и алгоритм расчёта интегрального уровня качества сертификации АСЗИ, а также приведена таблица соответствия, позволяющая производить необходимые оценки.

Использование представляемого интегрального уровня качества сертификации АСЗИ позволяет непосредственно количественно сравнивать средства с различными уровнями их

«сертификационного обеспечения» и по критерию его максимизации обоснованно выбирать предпочтительный вариант ПЗИ (СЗИ) в составе АСЗИ.

Примеры практической реализации предлагаемого подхода показывают возможность сопоставления и количественного (квалиметрического) сравнения разнородных ПЗИ (СЗИ), возможность обоснованного принятия соответствующих проектных и управленческих решений АСЗИ на всех этапах их жизненного цикла.

Андреева Н.В., Васильев Ф.Р., Любимов А. В.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

информационных технологий, механики и оптики

МЕТОДЫ ИНТЕГРАЦИИ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ И СИСТЕМ ДОКУМЕНТООБОРОТА В ОРГАНИЗАЦИЯХ

Одним из важнейших активов организации является информация, которая должна быть должным образом защищена вне зависимости от формы её выражения, средств распространения или хранения. Раздел 15.1.3 стандарта ISO/IEC 27002:2005, входящего в семейство международных стандартов по управлению информационной безопасностью, за подробными сведениями по управлению документацией в организации отсылает к стандарту ISO 15489-1 (в России адаптированному как ГОСТ Р ИСО 15489-1-2007). Семейство стандартов ISO 15489 содержит единые требования к управлению документами на всех видах носителей, в любых типах организаций (государственных или коммерческих), а также содержит методические рекомендации по проектированию и внедрению документной системы.

На основе анализа двух частей международного стандарта ISO 15489, а также российского ГОСТа, строится интегральная система согласованных моделей, которая представляет методологию управления документами в целом и содержит функциональную, объектную, процессную и онтологическую проекции. На первом этапе построения интегральной системы проводится первичный анализ и структуризация информации, результатом которого является функциональная проекция методологии. Её базовые параметры представлены ниже.

В качестве нотации моделирования функциональной проекции выбрана методика диаграмм потоков данных (Data Flow Diagrams, DFD), инструментального средства – AllFusion Process Modeler (ранее BPwin).

Основное назначение модели – представление функциональной проекции методологии управления документами и, в первую очередь, проектирования, разработки и внедрения документных систем (ДС) – в соответствии с семейством международных стандартов ISO 15489.

Модель содержит представление иерархической системы всех процессов, потоков ресурсов, внешних сущностей и информационных хранилищ, необходимых при создании (проектировании, разработке и внедрении) и функционировании ДС, которые описаны в русскоязычной версии стандарта ISO 15489-1. Для обеспечения полноты и связности модели она в необходимых случаях дополняется элементами, представленными в англоязычной версии нормативного документа ISO 15489-2.

Уровень детализации модели выбирается таким образом, чтобы процессы проектирования и внедрения ДС, представленные в разделе 8 стандарта, детализировать до максимального уровня, допустимого текстом раздела и не ниже, чем уровень вложенности подразделов.

Процессы проектирования и внедрения ДС, представленные в других разделах стандарта, детализируются до уровня, на котором порождаются входные или потребляются выходные ресурсы процессов проектирования и внедрения ДС.

Построение модели выполняется с точки зрения системного аналитика.

Варианты использования функциональной модели могут быть различными. Например, модель может использоваться в качестве настраиваемого шаблона при специфицировании, проектировании, разработке и внедрении ДС в конкретной организации, при разработке внешних спецификаций для программных средств поддержки ДС, как конкретной организации, так и универсальных или для обучения персонала организации, занимающегося внедрением и эксплуатацией ДС.

Артамонов А.В., Васильев П.Н., Маховенко Е.Б.

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

ГРУППОВАЯ ПОДПИСЬ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ НА ОСНОВЕ ТЕХНОЛОГИИ J2EE

Групповые подписи обеспечивают анонимность подписывающего. Любой член группы может подписать сообщение, но подпись, получающаяся в результате, не позволяет узнать личность подписавшего. Групповые подписи могут быть использованы для скрытия организационных структур, например, в случае, когда компания выпускает подписанное постановление.

Схема подписи BBS позволяет получить подпись размером порядка 200 байт, обеспечивающую примерно такой же уровень безопасности, что и стандартная подпись RSA такой же длины, позволяет эффективно добавлять пользователей в группу, дает возможность отзываться ключи подписи, и, таким образом, является на сегодняшний день одной из наиболее перспективных схем групповой подписи.

Для построения распределенного J2EE-приложения разработана архитектура, использующая для запуска клиентского приложения технологию Java Web Start. Взаимодействие осуществляется по протоколам JNLP и RMI. При данном подходе браузер не является принципиально необходимым звеном для работы приложения. Клиент класса А (пользователь, который имеет право подписывать документ) имеет отдельное заранее установленное java-приложение. Клиент класса В (пользователь, осуществляющий проверку подписи), чтобы запустить программу, верифицирующую подпись, обращается к web-серверу и получает HTML-страницу со ссылкой на jnlp-файл запуска java-приложения. При переходе по этой ссылке автоматически запускается приложение jawaws, входящее в JRE или JDK, которое автоматически скачивает файлы приложения с web-сервера, кэширует их и запускает данное Java-приложение, функционирующее независимо от браузера.

Все необходимые для работы программы JAR-библиотеки кэшируются на клиентском компьютере, что позволяет избежать повторной передачи java-кода при запуске нового сеанса. При последующих запусках приложения на клиентском компьютере автоматически выполняется проверка обновлений приложения, и все изменившиеся компоненты выкачиваются заново. За время сеанса работы с приложением исполняемый код загружается с сервера при необходимости и не более одного раза. Далее по каналам связи передаются лишь данные самого приложения, что не требует передачи HTML-страниц и кода javascript для каждой страницы (как в веб-приложениях), которые перед выполнением необходимо проверять на целостность, что может снизить производительность всего приложения. В данной архитектуре нарушитель может повлиять на исполняемый код лишь при начальной загрузке приложения, однако после нее java-машина автоматически проверяет наличие и корректность подписи каждого компонента приложения, что делает подобные действия нарушителя бессмысленными.

Данный подход является удобным с точки зрения разработки, эффективным с точки зрения конечного пользователя, а также удовлетворяет требованиям безопасности к приложению, использующему групповую подпись: любое изменение содержания HTML-страниц нарушителем не приводит к нарушению безопасности; конфиденциальные данные не передаются в открытом виде; подписываются все данные, для которых должна быть обеспечена целостность, а также весь передаваемый исполняемый код; производится контроль доступа к EJB-контейнеру посредством сервиса JAAS; ведется учет пользователей, сеансов и сообщений, передаваемых в системе.

Афанасьев С.В., Евневич Е.Л., Белаш Е.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО КОДА НА СТАДИИ РАЗРАБОТКИ**

С целью повышения качества и сокращения расходов на разработку и сопровождение средства анализа программного кода и его уязвимостей целесообразно интегрировать в жизненный цикл разработки программного обеспечения (ПО). Особую важность приобретает усиление безопасности ПО на этапе разработки, начиная с возможно более ранней стадии.

Одним из существенных препятствий по внедрению тестирования безопасности в жизненный цикл является разрыв между разработкой и обеспечением безопасности. Поскольку, этими двумя проблемами занимаются, как правило, разные люди или рабочие группы, синергетический эффект присущ процессу в целом в очень незначительной степени. В то время как разработчики фокусируют внимание на функциональности и выполнении графика разработки приложения, персонал, ответственный за безопасность приступает к устранению уязвимостей и осуществлению контроля безопасности только после завершения разработки приложений и их внедрения. Для эффективного устранения уязвимостей, возникающих в процессе разработки, между этими двумя группами должно быть установлено сотрудничество, так чтобы процессы разработки и обеспечения безопасности шли параллельно, и, соответственно, осуществлялось поэтапное интегрирование средств безопасности в жизненный цикл ПО.

В свете вышесказанного автоматизированный анализ кода признан наиболее эффективным методом тестирования защищенности ПО на ранних стадиях жизненного цикла, поскольку он позволяет оценить любую часть кода до завершения разработки всего приложения. Наилучшие из этих технологий обнаруживают каждую уязвимость с точностью до конкретной строки кода и предоставляют подробную информацию, касающуюся типа обнаруженного недостатка, степени его критичности и способа его исправления. Проникающее тестирование также является важным элементом безопасности ПО, но представляет наибольшую ценность на более поздних стадиях жизненного цикла и используется для анализа завершенного приложения с функциональным интерфейсом.

Баранюк Т.Н., Нестерук Ф.Г., Нестерук Г.Ф.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МИНИМИЗАЦИЯ БАЗЫ ЗНАНИЙ ПРИ РАЗРАБОТКЕ АДАПТИВНОГО УРОВНЯ
КЛАССИФИКАЦИИ В СОСТАВЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ**

Рассмотрены аспекты минимизации базы знаний (БЗ) специалистов в процессе разработки адаптивных уровней классификаторов для системы защиты информации (СЗИ) на базе средств интеллектуального анализа информации (ИАИ).

Актуальность тематики исследования обусловлена тем, что СЗИ должны быть ориентированы на обеспечение безопасности информационно-коммуникационных сетей (ИКС) в условиях высокой динамики угроз, изменения качественных и количественных характеристик компьютерных атак. Сформулированная задача может быть решена за счет применения средств ИАИ к разработке адаптивных средств классификации (АСК) в составе СЗИ.

Рассмотрим методику разработки АСК в составе системы защиты, которая состоит из трех эшелонов защиты: первый эшелон защиты соответствует выходу корпоративной сети в глобальную телекоммуникационную среду (почтовые шлюзы и межсетевые экраны – МСЭ); второй эшелон защиты – уровень серверов сети; третий эшелон защиты – рабочие станции и отдельные машины корпоративной сети.

Методика разработки АСК для СЗИ включает этапы формирования:

- множества механизмов защиты (МЗ);
- структуры СЗИ;
- перечня угроз;
- базы данных (БД);
- базы знаний (БЗ);
- топологии нечеткой нейронной сети (НС) путем отражения БЗ уровней СЗИ в информационных полях НС, когда каждому правилу логического вывода ставится в соответствие формальный нейрон (ФН) слоя логического вывода нечеткой НС;
- матриц экспертных или статистических оценок;
- рейтинговых показателей защищенности ИКС.

На этапе обучения АСК происходит коррекция информационных полей НС и соответствующих БЗ, так как в процессе обучения нечеткой НС (на достоверных данных обучающей выборки) изменяются веса связей выходного слоя сети, которые несут информацию о достоверности отдельных правил баз знаний. Изменение значений весов связей выходного слоя приводит к изменению значений экспертных оценок в БД и, следовательно, рейтинга защищенности ИКС.

На этапе корректировки баз знаний и баз данных (по результатам обучения АСК) источником информации об изменении ИКС и внешнего окружения являются специализированные датчики или процедуры операционной системы, посредством которых формируются входные векторы для нейросетевых классификаторов.

На этапе оптимизации ИКС и средств защиты в соответствии с критерием не убывания интегрального показателя качества (рейтинга) адаптивной СЗИ для каждого из уровней ИКС решается оптимизационная задача, целевой функцией которой являются показатели качества, формируемые в п. 9.

В данной методике не акцентировалось внимание на объеме БЗ, в то время как уменьшение числа правил логического вывода в формируемых базах знаний существенно упрощает структуру нейросетевых АСК, а, следовательно, повышает оперативность реакции СЗИ на компьютерные атаки.

Блюм В.С., Заболотский В.П.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ИНДЕКС ЗДРАВООХРАНЕНИЯ КАК ФАКТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА**

Ущерб, который наносят некачественные медицинские услуги, исчисляется сотнями тысяч человеческих жизней. Решение указанной проблемы лежит на пути создания единого информационного пространства здравоохранения, в основу которого следует положить систему полной, достоверной и доступной первичной медицинской документации.

Решение задачи информационной безопасности такой системы состоит в том, чтобы создать условия, при которых были гарантированы целостность, конфиденциальность и доступность информации.

Возможность применения методов и средств защиты информации напрямую связана с составом, объемом и организацией информации, для которой требуется защита.

Предложен метод оценки объема первичной медицинской информации. Определены условия, при которых состав и структура этой информации могут рассматриваться в качестве факторов информационной безопасности системы здравоохранения.

Информация о здоровье (точнее, о нездоровье) пациентов признаётся государством, если она имеет статус информационной услуги, которую вправе оказать только две категории объектов системы охраны здоровья – это множество действующих дипломированных врачей и множество лицензированных диагностических лабораторий. Именно эти и только эти деятели системы охраны здоровья допущены государством к оценке и фиксации оценки состояния здоровья пациента. Только они имеют право и обязаны генерировать информацию (писать тексты, строить графики, фиксировать изображения) о состоянии здоровья граждан своей страны, а также предлагать и записывать алгоритмы их лечения.

В результате проведенного анализа построено два информационных источника здравоохранения, которые определяют полный набор данных о нездоровье нации. Этот набор соответствует современному уровню развития системы охраны здоровья и является единственным, безальтернативным источником информации такого рода. Благодаря выбранному способу нормировки (размещение данных об одной медицинской услуге на CD стандартного размера) мы можем не только посчитать количество оказанных медицинских услуг, но и измерить объем накопленной информации как в традиционных битах, так и в условных «метрах».

В результате первого шага эксперимента собраны две коллекции ранжированных по времени создания документов, сумма которых, по нашему мнению, обладает свойством полноты. Можно утверждать, что не существует иной первичной медицинской информации о состоянии здоровья нации, кроме собранной в указанных двух коллекциях документов, суммарная величина которой определяется на заданном интервале времени.

Выполнен анализ разнообразия современных врачебных специализаций, а также методов и результатов лабораторных исследований. Сделан вывод о том, что данное разнообразие не может быть препятствием к формированию единого информационного пространства первичных медицинских документов, которое должно быть полным и достоверным. Очевидно, что изъятие любого документа из сформированной коллекции может привести к фатальной врачебной ошибке.

Количество достоверной информации определяется как удвоенное количество полной информации.

Для оперативного доступа к информации необходима специализированная поисковая машина, в основе которой лежит постоянно корректируемый поисковый индекс здравоохранения.

Поисковый индекс здравоохранения – это база данных (локальная или распределенная), в которой хранится полный перечень используемых в современном здравоохранении терминов, связь этих терминов с содержащими их сетевыми ресурсами, а также локальные ссылки на документы и их весовые характеристики.

Борьба за оперативный доступ к медицинской информации имеет свою цену – объем базы данных индекса имеет тот же порядок, что и исходный объем хранимых данных.

Количество полной, достоверной и индексированной информации на заданном интервале времени определяется как утроенное количество полной информации.

В результате эксперимента определена система полной и достоверной первичной медицинской информации, к которой гарантирован оперативный доступ. Этот результат следует рассматривать как основу и необходимое условие построения социальной искусственной иммунной системы (СИИМ), в которой цена компьютерной памяти стремительно падает, а цена человеческой жизни неизменно растёт.

Построение единого информационного пространства здравоохранения – это, в первую очередь, формирование полной и достоверной системы первичных медицинских документов, к каждому из которых гарантирован оперативный доступ. Объединяющей компонентой пространства здравоохранения является поисковый индекс, который следует рассматривать как важнейший фактор информационной безопасности государства.

Богачева А.В.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики
ОРГАНИЗАЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРА НА УРОВНЕ ФИЗИЧЕСКОГО ДОСТУПА**

Безопасность конкретного объекта является составной частью общей системы информационной безопасности. Защитить себя от взлома и похищения ценной информации в два клика решить не получится. Решать проблему сетевой безопасности нужно поэтапно.

Основными направлениями работ по защите информации являются: защита на уровне физического доступа к компьютеру; организация безопасной работы в локальной сети и защита при подключении к глобальным сетям. В докладе рассматриваются различные методы защиты информации на этапе получения доступа к компьютеру.

Процесс входа в систему нужен для идентификации пользователя. Получив эти сведения, операционная система разрешает или запрещает доступ к соответствующим системным ресурсам. Если злоумышленник узнает пароль пользователя, он сможет входить в систему под именем этого пользователя. Поэтому одной из главных задач обеспечения безопасности компьютера является организация хранения паролей. Алгоритмы шифрования типа AES и Bloufish, используемые в менеджерах паролей не вскрываемы. Асимметричные, с так называемым открытым или публичным ключом, алгоритмы шифруют файлы одним ключом, а расшифровываются – другим, полученным из первого. Менеджер сам придумает пароли, необходимо запомнить лишь один пароль к самому менеджеру. Причем, данный пароль должен быть 15020 символов сложного сочетания букв и цифр. Пароли в виде слов элементарно подбираются по словарю. Примером парольного менеджера может служить KeePass.

Следующим этапом защиты личной информации должно стать скрытие каких-либо документов и папок от посторонних лиц. Для этого существуют программы, подобные TrueCrypt. Эта программа позволяет создавать виртуальный зашифрованный логический диск, хранящийся в виде файла. С помощью TrueCrypt также можно полностью шифровать раздел жёсткого диска или иного носителя информации, такой как флоппи-диск или USB флеш-память. Шифруются полностью все данные, включая названия файлов и папок.

Способом гарантированного уничтожения данных с компьютера являются специальные программы, например Eraser – инструмент для безопасного стирания файлов, который позволяет полностью удалять данные с жесткого диска, записывая поверх них несколько раз сложные образцы, чтобы невозможно было восстановить стертые данные. У инструмента Eraser есть ещё одна замечательная функция – эта программа чистит свободное место жестких дисков от кусков когда-то давно удаленных файлов, делая тем самым невозможность их восстановления.

Грамотно реализованный комплекс мер по защите информации на компьютере позволяют даже при получении злоумышленником физического доступа максимально снизить возможность похищения информации.

Богданов А.Г., Ростовцев А.Г.

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

ГОМОМОРФИЗМЫ КОЛЕЦ И ЗАЩИЩЁННАЯ ОБРАБОТКА ДАННЫХ

При построении защищенных информационных систем часто требуется обеспечение обработки зашифрованной информации. При этом вычислительная среда не должна иметь доступ к открытым данным, а результаты вычислений должны допускать эффективную проверку. Создание такого вычислительного процесса позволит строить защищенные корпоративные базы данных, системы мобильных агентов и т.д.

Рассмотрим возможность построения защищенного вычислительного процесса на примере симметричного шифра, когда недоверенный вычислитель (НВ) управляется с помощью доверенной машины (ДМ). При этом ДМ готовит данные, ключ и программу шифрования. НВ предположительно выполняет эту программу, но может наряду с этим выполнять и другие программы. Для простоты предположим, что НВ не имеет энергонезависимой памяти, не способна к обучению и не имеет каналов связи с нарушителем. ДМ должна иметь механизм контроля правильности выполненного шифрования, не шифруя данные.

Алгебраической основой безопасного шифрования служат секретные гомоморфизмы кольца полиномов Жегалкина

Любое вычисление строится с использованием унарных и бинарных операций. Здесь унарной операцией может быть произвольное обратимое отображение множества векторов в себя, а бинарные операции должны кроме того задавать на множестве векторов структуру кольца.

В общих чертах безопасное шифрование n -битового текста выполняется следующим образом. ДМ знает рабочий и контрольный открытый текст, рабочий и контрольный ключ и контрольную шифропрограмму как результат шифрования контрольного текста на контрольном ключе. Кроме того, ДМ знает алгоритм шифрования. Для зашифрования рабочего открытого текста на рабочем ключе ДМ строит случайный гомоморфизм кольца.

На основе алгоритма шифрования и указанного гомоморфизма колец ДМ адаптирует входные данные и программу шифрования на уровне битовых операций, программа оперирует с 2^m -битовыми векторами и передает их в НВ. При этом каждая битовая операция, выполняемая в ходе шифрования, кодируется своим полиномом и своей парой контрольных и рабочих точек.

Результатом шифрования является набор из векторов, представляющих зашифрованный текст, которые НВ передает в ДМ. ДМ проверяет, что значения полиномов в контрольных точках равно зашифрованному тексту. Если это так, то, по-видимому, шифрование выполнено правильно, то есть значения полиномов в рабочих точках задает шифропрограмму.

Такой подход к построению вычислительного процесса создает предпосылки к построению защищенных информационных систем, когда вычислительная среда выполняет обработку секретных данных, не зная значение этих данных, и не может подменить результат обработки.

Верхолат А.М., Гаврилов В.А.

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

К ВОПРОСУ ПОСТРОЕНИЯ БЕЗОПАСНЫХ ГЕТЕРОГЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Не секрет, что операционные системы (ОС), включая серверные, фирмы Microsoft являются одним из слабых звеньев самых разных информационных систем. Происходит это в основном по той причине, что прикладные программы (ПП) при работе используют системные сервисы. Поэтому сервисы ОС доступны ПП, что делает ОС в принципе слабо защищенными. Одним из путей

устранения этой уязвимости является замена ОС Microsoft на ОС Linux, лишенная этого недостатка. В докладе рассмотрены вопросы замены одной ОС на другую.

В настоящее время сложился следующий подход к построению корпоративных информационных систем на основе программных продуктов Microsoft:

- ядром системы является контроллер домена (один или несколько для большей надежности или в случае удаленных филиалов) со службой каталогов Active Directory (AD) на основе серверных ОС с аутентификацией пользователей по защищенному протоколу Kerberos;
- база данных, централизованная или распределенная, реализована на MS SQL Server;
- рабочие станции пользователей в качестве ОС используют MS Windows Vista/XP/2000.

Во многих случаях замена ОС Microsoft на Linux повышает производительность системы и ее защищенность. В качестве Linux сервера может быть выбрана одна из многочисленных систем: Ubuntu, Alt Linux, Red Hat и т.д. Для администраторов систем, которые привыкли к графическому интерфейсу Windows, для удаленного управления сервером целесообразно установить `openssh-server` на сервере и `ssh-клиента` (например, `PutTY`) на консоли администратора. На консоли нужно также установить X Server для Windows, например Xming. Служба каталогов, аналогичная AD Microsoft, реализуется на LDAP сервере и клиентах, и позволяет организовать хранение и доступ к централизованной или распределенной базе системной информации. В этой базе данных хранится информация обо всех реальных объектах, имеющих отношение к системе: компьютерах, группах, пользователях, принтерах, общих ресурсах и т.д. Вся эта информация реализована в виде древовидного каталога, содержащего атрибуты всех объектов. Логическое местоположение объектов в дереве отражает какую-либо подчиненность (географическую, физическую, организационную). Доступ пользователей и прикладных программ к каталогу осуществляется по защищенному протоколу.

Для организации контроллера домена под Linux используется широко распространенный пакет программ Samba. Основная сложность для администраторов заключается в настройке пакета Samba для работы в качестве контроллера домена и стыковке его с сервером каталогов LDAP. Samba может быть также настроен в качестве главного просмотрщика домена – Domain Master Browser, который формирует и рассылает списки просмотра всех общих ресурсов домена. Как и все программы Linux Samba настраивается через конфигурационный файл, имеющий достаточно много взаимозависимых параметров. Для облегчения этого процесса можно использовать одну из графических утилит для настройки пакета Samba – “System-config-samba” или “SWAT”.

К сожалению, в настоящий момент Samba реализует только идеологию Primary Domain Controller (PDC) и в нем отсутствуют такие функциональности, реализованные в AD Microsoft, как равноправные контроллеры домена, репликации и другие. В следующей версии пакета Samba эти возможности должны быть добавлены в полном объеме.

Войцеховский С.В.

Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского
КОМБИНИРОВАННЫЙ МЕТОД СОГЛАСОВАНИЯ ЭКСПЕРТНЫХ ОЦЕНОК ДЛЯ СИСТЕМ
ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ВЫЧИСЛИТЕЛЬНЫХ КОМПЛЕКСОВ И СЕТЕЙ

Рассматривается метод согласования мнений экспертов, предназначенный для повышения достоверности экспертных оценок и формирования базы нечетких правил для обнаружения атак на автоматизированные системы.

В основе комбинированного метода экспертных оценок предлагается использовать метод Демпстера-Шеффера. Суть данного метода заключается в том, что если несколько мнений экспертов совпадают, то оно считается истинным. Если совпадений мнений несколько, то вероятность наступления события будет выше там, где больше мнений экспертов совпали. Комбинированная базовая вероятность вычисляется по специальной формуле. Недостатком этого метода является то, что довольно часто мнения экспертов противоречат друг другу, а значит, этот метод не всегда может применяться для согласования мнений экспертов.

В случае если мнения экспертов противоречат друг другу, и коэффициент вариации больше или равен 33%, то в комбинированном методе для проверки того, насколько эти мнения рассогласованы и отсеечения единичных мнений экспертов необходимо проводить парное сравнение мнений экспертов.

Для поиска и исключения особых мнений экспертов предлагается использовать специальный алгоритм. Ответы экспертов задаются в диапазоне от 0 до 1, при этом состояние 0 означает полное отсутствие атаки, а 1 означает, что автоматизированная система подверглась атаке с вероятностью 100%. Суть работы специального алгоритма заключается в следующем: если при исключении особого мнения экспертов (максимального или минимального) коэффициент вариации будет менее 33%, то перейти к расчёту обобщённого мнения экспертов по методу среднего арифметического с учётом весовых коэффициентов без учёта этого рассогласованного мнения.

Таким образом, предложен комплексный метод для согласования результатов прогнозирования экспертных суждений, а также алгоритм поиска и исключения особых (несогласованных) мнений

экспертов. Идеи комплексного метода могут быть использованы для разработки процедур построения общего согласованного экспертного суждения на основе отдельных суждений экспертов и в частности для формирования базы нечётких правил для систем обнаружения вторжений вычислительных комплексов и сетей.

Воробьев Е.Г.

Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского

ОПТИМИЗАЦИЯ ПРЕДСТАВЛЕНИЯ ДАННЫХ В ГЛОБАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ЕДИНОГО ИНФОРМАЦИОННОГО ПОЛЯ И КВАНТОВЫХ ТЕХНОЛОГИЙ

Ряд задач создания единого информационного пространства Российской Федерации находят удобное решение путем применения глобальных информационных систем. К таким задачам могут быть отнесены проблемы одновременного доступа к процедурам записи и чтения информационных кластеров. При этом, как показывает анализ мировой практики, схемы коллективного доступа построены по идеологии использования при хранении, обработке и передаче информации уникальных «твердых» копий, имеющих значительный объем, особенно, когда речь идет о миллионах пользователей и использовании спутниковых каналов связи. Возникают проблемы скорости передачи, целостности и доступности информации в базах знаний, особенно в условиях воздействия антропогенных, техногенных и стихийных факторов. Уничтожение даже части записи информации на носителях ведет к тяжелым последствиям для вычислительной системы. Если системное программное обеспечение имеет сравнительно небольшой объем и время восстановления, то данные в случае потери в ряде случаев из-за их уникальности на момент инцидента или объема потерь не могут быть восстановлены. Проблемой является значительное количество различных видов представления данных и их интерпретаторов. Все это требует решения задачи создания единой системы представления данных, которая может быть концептуально выполнена на основе двоичного информационного поля. При этом могут быть использованы все достоинства архитектуры фон Неймана.

Двоичная система представления информации дает возможность объединения различных видов информации, которые на прикладном уровне представления составляют информационный кластер в составе: "голос + текст + фото + видео + инфракрасное фото/видео + карта + координаты" за счет единства представления на уровне машинного кода и безразличия к его интерпретаторам на высоком уровне. Это же касается и отсутствия различия между программами и данными.

В результате выполненных исследований построено матричное представление двоичных чисел, которое имеет постоянную единую фрактальную структуру в отличие от современных подходов с попытками поиска фрактальных структур в случайных двоичных матрицах информационных объектов. По мнению автора, решением является поиск и привязка случайных объектов в едином информационном поле. Данный вид представления поля оптимален при применении в квантовых компьютерах.

Предложен метод стягивания двоичной записи произвольной длины в геометрическую точку единого информационного поля, что является развитием методов сжатия и адресного представления информации. Это позволит любому пользователю хранить информацию во внешних физических процессах на случай полной потери вычислительных систем в любом объеме. Иерархический подход к формированию баз знаний позволит восстановить информацию по мере наращивания разрядности имеющихся вычислительных ресурсов.

Предложен метод геоцентрического многомерного углового представления топопривязки объектов на поверхности Земли и в околоземном пространстве в двоичном виде, позволяющий получить любую точность описания координат (например, с точностью до миллиметра) с возможностью привязки информационного паспорта объекта и представлением данной совокупности в едином информационном поле.

Эффективная обработка оперативной информации сотрудниками министерств и ведомств за счет организации мобильных рабочих мест (карманных персональных компьютеров) для персональной и коллективной работы требует организации сети мобильных и стационарных серверов и комплексов связи и управления. Предложен метод оптимизации подключения пользователей на основе зональной модели ведомственных объектов с программной привязкой к единому информационному полю.

Построен защищенный квантовый протокол передачи информации, позволяющий производить развязку несущей сигнала, например параметра управляемой поляризации и информационной составляющей, что является развитием модели эффекта спутанности динамических процессов, взлом которого требует одновременного решения двух трудных задач различного типа, в отличие от простого криптоанализа после перехвата в канале. Протокол может быть использован для создания маскираторов магистральных линий, борьбы с программными закладками, компьютерными вирусами предназначенными для передачи информации по сети, селекции принимающих ЭВМ при разграничении информации и передачи данных при представлении их на основе сферы Блоха.

Обсуждаются области применения единого информационного поля и факторы, благоприятствующие быстрому их внедрению в практику.

Вус М.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
КОМПЬЮТЕРНЫЕ ИГРЫ И ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ЮНОГО ПОКОЛЕНИЯ**

Компьютеры прочно вошли в нашу жизнь. Менее чем за два десятилетия ИКТ существеннейшим образом изменили характер среды жизнеобитания, сферы деятельности и способы общения социума. Сегодня дети рождаются и растут в мире, где компьютер – такая же привычная вещь, как телевизоры, автомобили, электрическое освещение. Ребенок, который с детства ориентируется в компьютере, чувствует себя более уверенно, потому что ему открыт доступ в мир современных технологий. Компьютер может стать помощником, учебным пособием для ребенка. Он разовьет его творческие способности, откроет перед ним огромный, интересный мир. Но при одном условии – кем будет компьютер в жизни ребенка, добрым помощником или монстром, разрушающим его жизнь, зависит от того, как мы, родители, научим нашего ребенка общаться с ним.

Значительный акцент в использовании ИКТ приходится сегодня на сферу досуга и, прежде всего, на игровые применения. Корыстные интересы сферы бизнеса и обслуживающие их масс-медиа навязчиво и агрессивно пропагандируют это. Споры же относительно пользы и вреда от компьютерных игр ведутся на всех социальных уровнях.

Самый большой вред компьютера в том же, в чем и его достоинство – в его бесконечной увлекательности. Умение быстро щелкать мышкой еще не означает владения компьютером. Если взрослые (родители) своим примером покажут, что компьютер – умный помощник человека, он таким и будет для наших детей. В противном случае, компьютер может заменить ребенку реальную жизнь, научит его жестокости, выльет на него море грязной информации, покажет мир насилия и ужасов.

По данным экспертов ВОЗ, например, до 92% взрослых, работающих на компьютере, жалуются в конце рабочего дня на различные неприятные ощущения и усталость, которые в дальнейшем приводят к неблагоприятным последствиям. Чаще всего страдают глаза; через несколько часов работы появляется чувство жжения – «словно в глаза попал песок», болят веки. Чтобы компьютер не повредил здоровью, важно регламентировать время, которое проводится за компьютером. Дети же нередко увлекшись компьютерными играми и испытывая большой эмоциональный подъем, даже не замечают наступившего утомления и продолжают работать дальше.

Конфликты поколений были всегда, но в современном динамичном, жестком и жестоком мире детям порой трудно найти общий язык, трудно общаться с взрослыми. Родители могут быть довольны, что их дети не поддаются «уличным» соблазнам, а дома сидят за компьютером. Однако они порой и не подозревают, какую информацию черпает их ребенок из компьютера. Машина нередко становится для ребенка не только игрушкой или источником знаний, но начинает эмоционально заменять ему родителей, особенно много работающих родителей. Погружаясь в виртуальный мир, «уходя» в компьютер, дети прячутся от семейных неурядиц, компенсируя собственное одиночество.

В игре ребенок испытывает сильные эмоции – восторг, раздражение, радость. Компьютерные игры развивают произвольную память и внимание, формируют познавательную мотивацию. Однако оценивая пользу или вред конкретных игр, нельзя «зацикливаться» только на одном каком-то параметре. Игра развивает логическое мышление. Но попутно она может развивать и тщеславие, и раздражительность, и чувство зависимости. Хотя ситуации в играх вымышленные, но чувства, которые при этом испытывает человек играющий – вполне реальные. Играющий ребенок приучается легко относиться к тем или иным ситуациям (поражение в игровом бою можно переиграть). В игре он бесстрашен – но его бесстрашие основано на безответственности.

И это возвращенное играми бесстрашие человек может, а нередко и переносит в реальную жизнь – вместе с его оборотной стороной, безответственностью. Есть даже анекдот про заядлого игромана, который, попав в дорожную аварию, недоуменно произносит: «Ну и что? Перегружаемся и едем дальше»».

Галанов А.И., Костина А.А., Молдовян У.А., Сухов Д.К.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПОДГОТОВИТЕЛЬНАЯ ПРОЦЕДУРА ИССЛЕДОВАНИЯ ЦИФРОВОГО НОСИТЕЛЯ
ИНФОРМАЦИИ В ПРОЦЕССЕ ЭКСПЕРТИЗЫ**

Подготовительная процедура необходима для сохранения исходного состояния исследуемых объектов (для обеспечения возможности повторной экспертизы). В докладе рассматриваются вопросы такой процедуры.

Внешний осмотр представленных на экспертизу системного блока и жесткого диска ПЭВМ на наличие повреждений, определение их исправности и характеристик. Разделение системного блока и жесткого диска для обеспечения их неизменного состояния. Перед вскрытием системного блока оценить наличие специальных устройств, могущих автоматически уничтожить информацию в памяти накопителей блока при его вскрытии. Фиксация соответствия даты и времени текущему, установленных на часах системной платы системного блока.

Подбор двух жестких дисков, одного для хранения точной копии диска (эталонный дубликат), предоставленного на экспертизу, другого для создания рабочего дубликата.

Создание автоматизированного рабочего места для исследования представленного на экспертизу жесткого диска (подбор и настройка ЭВМ, системного и прикладного ПО, оснащение СЗИ НСД и специализированным ПО). Использование ЭВМ, представленной на экспертизу, допускается только в случае невозможности подбора альтернативной и только с разрешения субъекта, назначившего экспертизу.

Полное посекторное копирование содержимого представленного на экспертизу жесткого диска в файл-образ на первый диск (создание эталонного дубликата).

Копирование содержимого диска необходимо выполнять с использованием исключительно операций чтения диска, без единой операции записи на предоставленный носитель. Диск необходимо копировать целиком, со всеми разделами, загрузочными записями и всем остальным содержимым, без монтирования имеющихся файловых систем, без интерпретации находящейся на нем информации. При этом будет создана точная информационная копия, дубликат магнитной поверхности, без внесения изменений в оригинальный носитель.

В процессе копирования определить наличие внутренних повреждений жесткого диска, предоставленного на экспертизу.

В процессе копирования производить фиксацию контрольных сумм информационного содержимого жесткого диска, предоставленного на экспертизу, для возможности проверки его неизменности и доказательства отсутствия каких-либо модификаций информации, либо ее подлога.

Обеспечение ответственного хранения представленного на экспертизу жесткого диска и организационных мер по предотвращению доступа посторонних лиц к нему в процессе проведения экспертизы и до момента возврата органам следствия.

Создание из файла-образа рабочего дубликата (второй точной копии диска), который будет использоваться для проведения экспертизы. Проверка контрольных сумм для оценки безошибочности проведения работ по созданию рабочего и эталонного дубликата.

Обеспечение организационных мер по предотвращению доступа посторонних лиц к материалам, предоставленным на экспертизу. Обеспечение конфиденциальности проводимого исследования.

Изучение запроса экспертизы, состояния и характеристик, представленных на экспертизу материалов, анализ возможностей информационных технологий и доступных эксперту ресурсов, составление плана исследования для решения задач экспертизы и обеспечение максимально возможного подтверждения полученных выводов и результатов для следствия и суда.

Григорьева М.В.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

ВЕДЕНИЕ ИНФОРМАЦИОННОГО ПРОТИВОДЕЙСТВИЯ МЕЖДУ КОНКУРИРУЮЩИМИ СУБЪЕКТАМИ

Многообразие угроз в области информационных операций и взаимодействий можно свести к двум важнейшим проблемам: защите информации и защите от информации, то есть противодействию информационным воздействиям.

Цель и задачи данной работы. Исследование ведения информационного противодействия, перехода к противостоянию с применением информационных операций, а также построение моделей, с разной степенью формализации описывающих стратегии ведения информационного противоборства между конкурирующими субъектами, в зависимости от их целей, стратегической информации о конкуренте и других факторов.

Для достижения поставленной цели решаются следующие задачи:

- определение смысла, вкладываемого в понятие «информационное противодействие», формулирование основных признаков ведения информационного противодействия;
- исследование методов информационного противодействия, факторов, влияющих на ведение противодействия;
- выделение и характеристика основных сущностей, участвующих в информационном противодействии, определение их составляющих;
- построение модели, описывающей выбранные сущности и их отношения.

Используемые методы. Для выявления основных сущностей применялся онтологический анализ текстов, при построении модели использован объектно-ориентированный подход.

По результатам анализа нескольких систем взглядов на сущность информационного противодействия сформирован контекст моделирования и построена общая объектная модель. Создан методический задел и разрабатываются уточненные модели стратегий взаимодействия субъектов. Модели взаимодействия двух конкурирующих субъектов в условиях дуального конфликта, могут являться базой разработки функциональных и проектных спецификаций для программного

обеспечения поддержки проектирования средств защиты информации в соответствии с «Общими критериями». Важным результатом моделирования является возможность установления зависимостей для конкретных субъектов между различными факторами взаимодействия, например, временем и вероятностью доступа к информации.

Григорьева А.И., Колодин М.Ю.

Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОСНОВНЫЕ ПРИНЦИПЫ И ПРАКТИЧЕСКИЕ ДЕЙСТВИЯ ДЛЯ ОБЕСПЕЧЕНИЯ
БЕЗОПАСНОСТИ В СВОБОДНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Принципы свободного программного обеспечения (СПО): свобода использования, модификации и распространения ПО с доступом к исходным кодам — дают широкие возможности, но и требуют особого внимания при рассмотрении вопросов безопасности.

Нужно выявить положительные стороны СПО и научиться их использовать, наряду со знанием проблем и путей их преодоления.

Доступ всех желающих к исходному коду программ позволяет вносить улучшения и закладки, выявлять ошибки и злонамеренности, отлаживать и клонировать ПО. В целом, «где есть 1000 глаз, ошибки исправляются быстро».

Полные программные комплексы (напр., операционные системы (ОС)) на СПО имеют, как правило, более высокие степени защиты и доверия. СПО в целом имеет существенную поддержку сообществ, помимо традиционной поддержки фирмами-разработчиками.

Есть проблемы в лицензировании и сертификации СПО, во взаимодействии с государством вообще и его конкретными исполнителями.

Безопасные методы нужно применять на всех уровнях: от ОС до плагинов в браузере конечного пользователя. На системном и сетевом уровне это открытые защищённые протоколы, антивирусы и фаерволы, чёткая система разграничения прав, пароли и ключи, защита переписки и содержимого дисков и памяти, обнаружение и противодействие вторжениям, установка необходимых и достаточных полномочий каждого пользователя для решения конкретных задач, контроль за устанавливаемым системным и прикладным ПО, управление доступом к ресурсам, в т. ч. в гетерогенных средах, регулярные обновления, особенно рекомендуемые разработчиком для повышения безопасности, настройка автоматической установки обновлений и патчей, отслеживание угроз по форумам и рассылкам и т.д. На пользовательском уровне это установка надёжных паролей и регулярная их смена, понимание опасностей и ответственности при установке и использовании ПО, взаимодействии с посторонними, в т.ч. по сети.

Полезно использование открытых государственных и международных стандартов на форматы документов, технологии разработки и сопровождения ПО, учебных курсов. ГОСТы и рекомендации, в т.ч. по безопасности, должны быть открытыми.

Нужно применять те средства, которые выгодно отличает именно открытость и переносимость: системы с асимметричным шифрованием (gpg), открытые офисные средства (особенно из комплекта OpenOffice.org, имеющие упакованный структурированный текстовый формат, что облегчает обработку и обеспечивает отсутствие закладок), распространённые системные и прикладные утилиты для автоматизации и технологизации процессов, повышения надёжности и безопасности работы.

Строго необходимо регулярное повышение квалификации сотрудников, как в правовой области, так и в части конкретных действий на рабочем месте как в повседневной работе, так и в критических ситуациях.

В целом имеются все возможности для построения защищённых и безопасных систем именно на основе СПО, но для этого нужна постоянная работа: ежедневная практика, обмен опытом (форумы, семинары, конференции, рассылки, пр.), изучение литературы и документации.

Группа ИГИТО СПИИРАН активно работает в этом направлении и готова к сотрудничеству с другими подразделениями и организациями: мы проводим свои семинары и участвуем во внешних семинарах и конференциях; СПО установлено на всех компьютерах, как учебных, так и системных, как в составе коммерческих ОС, так и в полностью свободных ОС; значительная часть организационной, прикладной, учебной и производственной деятельности выполняется именно на СПО; вопросы построения надёжных, безопасных, отказоустойчивых, защищённых систем рассматриваются в приоритетном порядке.

Домбровская Л.А.

Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Важной составляющей анализа угроз — действий или событий, способных нарушить безопасность информационных систем, является изучение, так называемых агентов — людей или организаций, представляющих угрозу.

Дадим общую характеристику этого компонента угроз.

Агентами угроз являются люди, которые стремятся нанести ущерб организации. Для этого они должны иметь следующее:

1. Доступ. Способность для достижения цели.
2. Знания. Уровень и тип имеющейся информации о цели.
3. Мотивация. Причина для сокрушения цели.

Доступ. Агент должен иметь доступ к нужной системе, сети, оборудованию или информации. Этот доступ бывает прямым (например, у него есть учетная запись в системе) или косвенным (он получает доступ к оборудованию другим способом). Прямой доступ позволяет воспользоваться существующей уязвимостью и, следовательно, становится угрозой. Кроме того, следует обратить внимание на составную часть доступа – благоприятную возможность. Такая возможность существует в любой системе или сети только потому, что сотрудники просто оставляют двери открытыми.

Знания. Агент должен обладать некоторыми знаниями о цели:

- идентификатор пользователя;
- пароли;
- расположение файлов;
- процедуры выполнения физического доступа;
- имена служащих;
- доступные номера телефонов;
- сетевые адреса;
- процедуры обеспечения безопасности.

Чем больше агент знаком с целью, тем больше вероятность, что он знает о наличии уязвимых мест и о том, как ими воспользоваться.

Мотивация. Агенту нужна мотивация для совершения действия. Мотивация является побуждающим действием, ее можно определить как первичную цель.

Мотивацией обычно является:

- привлечение внимания – желание похвастаться своими «победами»;
- алчность – жажда выгоды (денег, товаров, услуг или информации);
- злые намерения – желание причинить вред организации или отдельному лицу.

В докладе рассматриваются разновидности агентов, которых следует принимать во внимание при построении системы защиты информационных систем, а также цели угроз (атак), их содержание.

Емелин В.И.

**Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Вектор»
ИНФОРМАЦИОННАЯ УСТОЙЧИВОСТЬ УПРАВЛЕНИЯ СОЦИАЛЬНО-ТЕХНИЧЕСКИМИ
СИСТЕМАМИ**

Среди наиболее важных явлений, определяющих выбор рациональных решений при управлении объектами социально-техническими системами, выделим динамику изменения обстановки в реальном масштабе времени.

Наблюдаемый объект, характеризующийся качеством поступившей информации Ψ_1 при заданном фиксированном его объеме (количестве информации) I_0 в условиях информационного воздействия, в результате отражения угрозы повышает этот показатель до значения Ψ_2 . Разница величин $\Delta \Psi = \Psi_2 - \Psi_1$ представляет меру сохраненного качества информации. Будем считать, что уровень выполнения требований к качеству информации (количественные значения каждого показателя) и их влияние на эффективность решения функциональных задач управляемой системы ВМФ предлагается оценивать тремя показателями:

достоверность, d – способность информационной системы к адекватному информационному описанию оперативной обстановки;

полнота, p – способность информационной системы к учету необходимого перечня реальных значений характеристик обстановки;

оперативность, to – способность информационной системы решать свои задачи за промежутки времени не более чем те, которые необходимы для эффективного функционирования обслуживаемой технической системы.

Информационная устойчивость как в результате действий органа управления, так и в результате информационного возмущающего воздействия противоборствующей стороны характеризуется следующими состояниями.

I. Состояние неравновесия – состояние АСУ СТС, в котором заданный уровень качества информации обеспечивает нормальное функционирование системы на основе непрерывного целенаправленного обновления данных.

II. Предкризисное состояние – состояние СТС, при котором малые ухудшения информации переводят систему в кризисное состояние.

III. Кризисное состояние – состояние, при котором из-за низкого уровня качества информации исключается достижение цели СТС.

Разработанная концептуальная схема защиты автоматизированных систем в своей структуре содержит модели двух типов, выбор которых определяется направлениями развития информационного оружия и методов защиты: 1) информационно-техническая защита АСУ, 2) обеспечение информационно-психологической безопасности

Для решения проблемы обеспечения информационной устойчивости системное моделирование позволяет выделить специальным образом организованный моделирующий комплекс, состоящий из следующих типовых компонентов:

- а) имитационных моделей, отражающих определенную предметную область;
- б) аналитических моделей, дающих упрощенное (агрегированное) описание различных сторон моделируемых явлений в процессе информационного противоборства;
- в) информационной подсистемы, включающей базу (банк) данных, а в перспективе базу знаний системы защиты;
- г) системы управления и сопряжения, обеспечивающей взаимодействие всех компонент системы и работу с пользователем, лицом, принимающим решения в интерактивном режиме.

Зегжда Д.П.

Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ВИРТУАЛИЗАЦИЯ – ОСНОВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Предлагается в качестве подхода к обеспечению безопасности использовать технологию гибридных операционных систем суть которой заключается в том, что в рамках одной операционной системы (её называют «базовой») создаётся среда, в которой может функционировать другая операционная система (её называют «встроенной»), что позволяет запускать на компьютере одновременно несколько разных ОС и переключаться между ними без перезагрузки.

Для реализации технологии гибридных систем используется известный достаточно давно механизм виртуальных машин, который позволяет организовать на одном компьютере несколько виртуальных машин, на каждой из которых можно запустить отдельную встроенную ОС. Виртуальная машина включает в себя все устройства, необходимые для работы встроенной ОС: процессор, оперативную память, дисковые накопители, сетевые устройства, устройства ввода-вывода. Эти устройства эмулируются виртуальной машиной при помощи ресурсов реальной вычислительной системы посредством обращения к сервисам, предоставляемым базовой ОС. Задействованные виртуальной машиной ресурсы либо отдаются в монопольное потребление виртуальной машине и исключаются из основного пула ресурсов (как, например, происходит с оперативной памятью), либо используются базовой и встроенной системами совместно – как это происходит с процессором, накопителями и сетевыми адаптерами. Поскольку все эти возможности предоставляются за счет разделения ресурсов одного реального компьютера, то требования к его аппаратным ресурсам повышаются, однако при современном уровне развития компьютерной техники выполнение этих требований не требует существенных затрат.

Основная задача виртуальной машины – изолировать встроенную ОС от аппаратуры и создать подходящую для нее вычислительную среду на основе прикладного программного интерфейса базовой ОС. При этом виртуальная машина может поддерживать различные аппаратные конфигурации – например, можно задать, сколько памяти получит та или иная виртуальная машина и будет ли в ней доступна работа с сетью.

С точки зрения безопасности важно, что в гибридной системе базовая ОС полностью контролирует аппаратуру вычислительной системы, а встроенная ОС не имеет доступа к аппаратуре и взаимодействует только с виртуальной машиной. Таким образом, базовая ОС полностью контролирует работу встроенной ОС и при этом может быть полностью прозрачна для пользователей и приложений встроенных ОС.

Благодаря этим свойствам технология гибридных ОС может быть применена для построения защищенной и доверенной операционной среды, в которой базовая защищенная ОС и система виртуализации обеспечивают безопасность и доверие, а встроенные ОС – удобный пользовательский интерфейс и совместимость с приложениями и технологиям их разработки. Для этого необходимо, во-первых, обеспечить возможность запуска встроенной ОС в составе обычного пользовательского процесса базовой ОС и, во-вторых, реализовать возможность доступа приложений встроенной ОС к ресурсам базовой ОС, под контролем входящих в ее состав средств защиты.

При соблюдении этих условий можно получить гибридную систему, безопасность и доверенность которой будут определяться только свойствами базовой и системы виртуализации ОС и не зависеть от свойств встроенных ОС, так же как безопасность и доверенность обычных ОС не зависят от безопасности и доверенности используемых в ней приложений.

В такой гибридной операционной системе средства безопасности базовой операционной системы, должны решать две основные задачи: обеспечивать защиту компонентов встроенных

операционных систем от влияния друг на друга, и осуществлять контроль доступа к ресурсам базовой системы со стороны приложений встроенных систем.

Следовательно, использование при построении доверенных защищенных ОС технологии гибридных систем позволяет избежать постоянного процесса исследования степени доверия новых операционных систем, которых требуют новые приложения, поскольку обеспечив один раз безопасность и доверенность базовой ОС и системы виртуализации в качестве встроенных можно безопасно использовать не только ОС, существующие в настоящее время, но и те, что появятся в будущем.

Это позволит создать защищенную и доверенную вычислительную среду, обладающую способностью адаптироваться к быстро меняющимся требованиям современных технологий обработки информации.

Перечисленные свойства гибридных систем позволяют использовать эту технологию в качестве платформы для типовых решений, представляющих собой специализированные системы с несколькими изолированными средами для обработки различной информации.

Зегжда Д.П., Рудина Е.А.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
МОДЕЛИРОВАНИЕ БЕЗОПАСНОСТИ ОБРАБОТКИ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ СИСТЕМАХ**

Виртуализация – это представление вычислительных ресурсов, которое позволяет получить новые качества при их использовании. Виртуализация вычислительных машин открывает широкие возможности по увеличению эффективности использования высокопроизводительных компьютерных систем и повышению их отказоустойчивости.

В данном докладе для виртуализация определяется традиционным образом через понятие гипервизора. Гипервизор должен обеспечивать выполнение по крайней мере, двух условий: инвариантность функционирования виртуальной системы по отношению к реальной, полная изоляция виртуализуемых ресурсов. Гипервизор работает как обычная программа под управлением (обычно реальной) системы и не исключает одновременного использования других прикладных программ в этой системе. Таким образом, могут быть рассмотрены как гипервизоры, реализующие аппаратную виртуализацию вычислительных машин, так и программные гипервизоры, работающие под управлением базовой ОС.

В последнее время наблюдается тенденция к использованию виртуализации процессов обработки информации с целью повышения ее безопасности, например, использование программной виртуализации для выполнения недоверенных приложений и систем под управлением безопасной базовой ОС. Программы, которые не могут быть выполнены непосредственно под управлением этой ОС, могут быть запущены на ней под управлением виртуальной машины. При этом доступ этих приложений к данным, безопасность которых критична, должен контролироваться механизмами базовой ОС. В этом случае расширение функциональности базовой ОС с одновременным сохранением присущих ей свойств безопасности, будет достигнуто с наименьшими затратами.

В то же время нельзя наверняка утверждать, какие свойства (в том числе формально обоснованные), как базовой системы, так и виртуализуемой, будут выполнены для виртуальной машины. Для описания свойства инвариантности поведения программ можно рассмотреть множество состояний виртуальной машины как гомоморфный образ множества состояний реальной машины. Какие свойства виртуализуемой системы сохраняет этот гомоморфизм? При каких условиях виртуальная машина сможет унаследовать свойства не только виртуализуемой, но и базовой системы?

Для разрешения поставленных вопросов описана формальная модель вычислительной системы, включающая множества процессов ВС, ресурсов, функций, описывающих архитектуру системы в целом, программ, описываемых как алгоритмические последовательности функций и сопоставляемых процессам. Ресурсы ВС типизированы.

С использованием данной модели сформулированы условия, при выполнении которых виртуальная система под управлением защищенной базовой ОС обеспечивает безопасность выполнения любых программ исходной (не виртуализованной) системы.

Эти условия могут быть использованы при построении безопасных вычислительных систем путем виртуализации небезопасных систем (реализующих требуемую функциональность).

Зозуля Ю. В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОПРЕДЕЛЕНИЕ КАТЕГОРИИ ВЕБ-САЙТА ДЛЯ РЕШЕНИЯ ЗАДАЧИ РОДИТЕЛЬСКОГО КОНТРОЛЯ**

Представляемая работа посвящена разработке общего подхода и реализующего его программного комплекса, решающих актуальную в настоящее время задачу категорирования веб-сайтов для программ родительского контроля.

Задача родительского контроля сводится к обеспечению защиты ребенка от вредоносной информации при его работе в Интернет, в частности, решению вопроса о запрете доступа ребенка к определенным веб-сайтам, которые содержат неприемлемую информацию.

В работе предлагается подход, в которой родитель может определить список категорий, по которым будет оцениваться каждый посещаемый ребенком сайт. Примерами таких категорий могут послужить такие, как: насилие, наркотики, эротическое содержание, вредоносное наполнение сайта и другие.

В соответствии с выбранными родителем категориями странице ставится оценка с учетом информации из разных источников. Оценка сайта заносится в базу данных, а затем используется и обновляется при последующем доступе к этому или другим сайтам.

При этом анализируется не только содержимое сайта, но и контекстная информация, включающая в себя историю оценок данного сайта, оценки связанных с ним сайтов, а также оценки просматриваемого сайта, доступные из внешних источников.

Первичная оценка сайта включает анализ текстового содержимого на наличие ключевых слов и выражений, анализ картинок, сканирование сайта на наличие вредоносного содержимого, контроль появления всплывающих окон.

Далее выполняется контекстный анализ просматриваемой веб-страницы. При этом анализируются перекрестные ссылки, проводится анализ информации, публикуемой на ссылающихся на эту страницу сайтах. В данном случае интерпретируется околоссылочный текст, поскольку подразумевается, что автор сайта со ссылкой в сжатом виде передает информацию, размещенную на просматриваемой странице. Данный подход позволяет выявить мнение других сайтов об оцениваемой странице. Кроме того, учитывается информация об оценке сайтов, на которые ссылается просматриваемая страница, если такая информация уже занесена в базу.

Дополнительно используется информация о сайте, публикуемая в открытых источниках, посвященных решению данной проблемы, а также учитывается внутренняя оценка сайта родителем.

Вся полученная информация комбинируется для каждой выбранной категории, в результате чего на выходе формируется вектор оценок для данного сайта.

В соответствии со значимостью категорий, которая выставляется пользователем, формируется вектор метрик для категорий. Затем полученный вектор оценок сопоставляется с вектором метрик для категорий, а на завершающем этапе нормируется. Метрики определяют весовые коэффициенты влияния определенной категории на внутреннюю оценку данного сайта. В свою очередь, внутренняя оценка используется для принятия решения о предоставлении или запрете доступа к этому сайту. При этом учитывается то, что родитель может задать различный уровень опасности сайта для своего ребенка, например, в зависимости от возраста.

Работа выполнена при финансовой поддержке РФФИ (проект №07–01–00547), программы фундаментальных исследований ОНИТ РАН (контракт №3.2/03) и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST (контракт № 021186–2) и других проектов.

Иванов С.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПОДСИСТЕМА РАЗГРАНИЧЕНИЯ И ОБЕСПЕЧЕНИЯ ДОСТУПА
В МОДЕЛИ ГРИД ПОРТАЛА САНКТ-ПЕТЕРБУРГСКОГО НАУЧНОГО ЦЕНТРА РАН**

В данный момент возможности грида доступны пользователю только с рабочих станций с установленными личными сертификатами пользователя и компонентом интерфейса пользователя грида. При этом интерфейс пользователя грида, посредством которого осуществляется доступ к грид-сервисам, представляет собой интерфейс командной строки. Такой способ доступа к гриду предъявляет завышенные требования к знаниями пользователя в сфере информационных технологий, затрудняет работу с гридом и его администрирование.

Следующим этапом в развитии грида является упрощение доступа к нему для обеспечения возможности пользователям со средним и низким уровнем знаний в сфере ИТ (фактически, всем пользователям, имеющим навыки работы в Интернете посредством веб-браузера). Инструментом, способным обеспечить такой доступ, является грид-портал – графический пользовательский веб-интерфейс к UI грида.

Грид-портал предъявляет особые требования к обеспечению универсальности, комфортности и безопасности. Он должен быть доступен с любых типов устройств, поддерживающих работу с Интернетом посредством веб-браузера, обеспечивать интуитивно понятный интерфейс и обеспечивать «избыточную» безопасность (безопасность соединения, параметров доступа пользователя, аутентификации и виртуальных организаций).

В процессе разработки модели грид-портала Санкт-Петербургского научного центра РАН особое внимание уделяется его интеграции в существующий веб-портал научного центра. Продукт этой интеграции в последствии и должен образовать единую систему – грид-портал СПбНЦ РАН. Поэтому в портале существуют локальные ресурсы и сервисы портала и ресурсы и сервисы грида.

Безопасность соединения, параметров доступа пользователя и аутентификации не требуют отдельного обсуждения – на данный момент существуют устоявшиеся общепринятые стандарты, которые должны использоваться для обеспечения этих требований (HTTPS, различные алгоритмы

шифрования). Наибольший интерес представляет подсистема разграничения и обеспечения доступа к двум описанным выше видам ресурсов и сервисов. Она состоит из ACL-модуля, вспомогательных подсистем, обеспечивающих стабильность и быстродействие, а также модуля управления привилегиями пользователей как на уровне локальных ресурсов и сервисов грид-портала, так и на уровне ресурсов и сервисов грида.

Отметим особо, что данная подсистема призвана не только разграничивать доступ пользователей, но и обеспечивать взаимодействие между грид-порталом и гридом в части, касающейся инфраструктуры безопасности грида.

В докладе подробно описывается модель подсистемы разграничения и обеспечения доступа пользователей в грид-портале, описываются некоторые проблемы безопасности, возникающие при обеспечении доступа к грид-сервисам посредством грид-портала, и методы их решения.

Калинин М.О.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
СОЗДАНИЕ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**

Указанная в нормативных документах (ГОСТ семейства 27001, 13335, 18044) номенклатура задач, решаемых системами организационного менеджмента информационной безопасности, определяют необходимость и актуальность создания систем управления информационной безопасностью (СУИБ), на системном уровне выполняющих функции регулятора защитных механизмов в информационно-телекоммуникационных системах (ИТКС), а также позволяют сформулировать перечень требований, выдвигаемых к СУИБ. Являясь частью общей системы обеспечения безопасности, СУИБ должна реализовывать и поддерживать защиту активов, адекватную угрозам, как случайным, так и преднамеренным, с соблюдением принципа постоянного контроля, анализа и улучшения средств защиты, используемых в ИТКС (т.н. модель PDCA). Поэтому жизненный цикл СУИБ состоит из следующих этапов:

- формирование условий функционирования и безопасности активов ИТКС;
- контроль текущей системной конфигурации на предмет соблюдения этих условий;
- управление безопасностью информации.

Указанный перечень определяет состав и назначение структурных компонентов СУИБ. Задачей СУИБ является контроль и удержание безопасности на приемлемом уровне. Поэтому при построении СУИБ требуется обеспечить задание необходимого уровня безопасности. Поскольку он определяется набором условий функционирования и безопасности, сформированных из целей создания ИТКС, ее назначения, особенностей эксплуатации, актуального множества угроз информационной безопасности, требований безопасности, сформулированных в стандартах, правилах корпоративной политики информационной безопасности, ТУ функционирования сертифицированного ПО, то данные действия сопряжены с набором мероприятий по системному анализу ИТКС. Для описания этих условий широко применяются языковые средства, так как они обеспечивают универсальное и формализованное представление ограничений. Для определения источников актуальных угроз информационной безопасности в ИТКС и оценки вероятности их реализации полезным является перечень наиболее часто встречающихся угроз (примеры типовых угроз приведены в приложении С стандарта ГОСТ 13335-3). Также необходимо использовать каталоги угроз, соответствующие конкретной сфере применения ИТКС. Для анализа угроз безопасности ИТКС необходимо:

- установить область безопасности ИТКС;
- проанализировать уязвимости ИТКС;
- оценить риски информационной безопасности

В область безопасности должны быть включены наиболее ценные активы ИТКС, для которых необходимо управление. При установлении активов используется два способа. Первый заключается в инвентаризации всех активов и согласовании масштабов возможного ущерба. При этом оценка важности активов может быть как количественной (например, в денежном выражении), так и качественной (например, по шкале "низкий-высокий"). Второй подход основан на оценке рисков и финансовых затрат организации по причине утраты конфиденциальности, целостности или доступности активов вследствие инцидентов. Анализ уязвимостей ИТКС заключается в идентификации источников (причин угроз) и объектов (элементов ИТКС, которые могут подвергнуться воздействию) угроз информационной безопасности. При этом необходимо оценить, насколько велика степень уязвимости или насколько вероятно ее использовать. Оценка рисков информационной безопасности позволяет связать оценку важности активов и оценку угроз. Методики оценки рисков разнообразны, что позволяет выбрать наиболее удобные для организации и применения в рассматриваемой ИТКС.

Реализованные в ИТКС защитные меры должны удовлетворять требованиям, выявленным на этапах оценки и обработки активов. Активная составляющая СУИБ заключается в контроле соблюдения заданных условий функционирования и безопасности, а также в управлении

безопасностью информации в случае возникновения нарушений данных условий. При этом безопасность ИТКС обеспечивается следующим набором защитных мер:

- идентификация и аутентификация пользователей;
- выполнение правил контроля доступа;
- обеспечение регистрации происходящих в ИТКС событий;
- функционирование криптографических подсистем.

ИТКС и среда ее функционирования постоянно изменяются в результате функционирования самой системы, применяемых средств защиты и срабатывания угроз. С целью обеспечения взаимосогласованности (функциональной совместимости) защитных средств и реализации заданного уровня безопасности ИТКС СУИБ должна содержать средства подключения/отключения, контроля состояния и управления конфигурацией. Для этого средства СУИБ должны реализовывать следующие процедуры:

- обнаружение нарушений условий функционирования и безопасности в текущем состоянии ИТКС;
- определение результативности мер защиты при нарушениях;
- осуществление надлежащих корректирующих и предупреждающих действий.

Для осуществления контрольных и управленческих функций СУИБ должна содержать средства фиксации и изменения параметров безопасности ИТКС (состава используемых средств защиты; параметров их совместимости; конфигураций безопасности системного и пользовательского ПО). На этапе контроля также допустимо выполнение периодического анализа рисков нарушений безопасности и остаточных рисков с целью оценки возможных финансовых затрат организации. Необходимым условием реализации приведенного функционала является наличие интерфейса, позволяющего обеспечить необходимый уровень безопасности при осуществлении функций фиксации, проверки и тестирования параметров безопасности ИТКС путем настройки параметров безопасности. Подсистема управления безопасностью на основании информации по инцидентам и заданным условиям функционирования и безопасности ИТКС должна обеспечить устранение выявленных нарушений безопасности. Средства настройки должны выполнять:

- подготовку, включая предупреждающие меры, рекомендации и процедуры по обработке инцидентов (включая сохранение доказательных данных, обслуживание файлов регистрации событий и уведомительную связь);
- оценку, включая процедуры по анализу состава нарушений и определению уровня их опасности;
- управление, включая процедуры по обработке нарушений, снижению ущерба от них и уведомлению пользователей;
- восстановление, включая процедуры по возобновлению нормальной работы ИТКС после серьезных нарушений безопасности.

СУИБ должна содержать механизмы документирования для обеспечения прослеживаемости действий и воспроизводимости результатов управления.

Таким образом, содержание процесса управления информационной безопасностью определяет необходимый состав и функциональное назначение компонентов СУИБ, а также технологию их построения.

Комашинский Д.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПОСТРОЕНИЕ МОДЕЛИ СТАТИЧЕСКОГО ДЕТЕКТИРОВАНИЯ ВРЕДНОСНОГО
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА БАЗЕ МЕТОДОВ DATA MINING**

Представляемая работа посвящена проблеме выявления вредоносного программного обеспечения (malware) на начальных фазах его жизненного цикла. Результаты работы рассматриваются в качестве базиса, необходимого для формирования общей объединительной модели детектирования malware, использующей сильные стороны существующих процедур извлечения, выделения, конструирования групп признаков и обучения классификаторов, обеспечивающих точное выявление отдельных структурных и функциональных аспектов исследуемых потенциально вредоносных файловых объектов.

В работе проанализированы сильные и слабые стороны существующих методик анализа исполняемых файлов на базе информации, доступной без их исполнения в вычислительной среде. Показано, что, как правило, подходы статического обнаружения malware на основе методов Data Mining являются эффективными на ограниченных наборах данных, использованных для обучения и проверки. Основной причиной этого является использование злоумышленниками средств противодействия статическому анализу исполняемых файлов (обфускаторы, протекторы и т.д.). Для смягчения остроты данной проблемы предлагается итерационное уточнение контекста задачи статического анализа исполняемых объектов, позволяющее применять на разных этапах процедуры принятия решения отдельные классификаторы, использующие для обучения наиболее применимые группы структурных и поведенческих признаков. Применение данного подхода позволяет

последовательно уточнять отдельные аспекты исследуемых объектов и на базе выявленных особенностей принимать наиболее оптимальное решение о выборе последующих этапов обработки. Конечное приложение, использующее данный подход, нивелирует проблему ресурсопотребления, и в виду своей модульности требует меньших усилий по сопровождению, а также обеспечивает потенциально большую точность детектирования новых, ранее неизвестных образцов malware.

В качестве исходных данных, используемых на различных шагах анализа, рассматриваются содержимое заголовочной информации, строковые данные, байтовые последовательности, позиционно-зависимые данные (таблицы, секции, директории) и данные дизассемблирования кода. В силу специфики статического анализа и доказанной на практике эффективности, опорными классификаторами для экспериментов являются статистические Байесовские классификаторы, деревья решений и генераторы правил. Базовой стратегией выделения значимых признаков выбран метод оценки признаков по информационному усилению. Для построения структуры системы принятия решения применяются методы построения деревьев решений, работающие на пространстве признаков, характеризующих существенные структурные и функциональные аспекты объектов, выявляемые ее отдельными элементами.

Сбор признаков осуществляется специально разработанными средствами, обеспечивающими извлечение информации из файлов формата PE32. Экспериментальная часть исследований выполняется с помощью программных пакетов Weka Classifier и Rapid Miner.

Полученные результаты планируется применить при реализации общей модели детектирования malware, интегрирующей динамические средства анализа.

Работа выполнена при финансовой поддержке РФФИ (проект №07–01–00547), программы фундаментальных исследований ОНИТ РАН (контракт №3.2/03) и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST (контракт № 021186–2) и других проектов.

Конобасов А.М., Королев С.Н.

Россия, Санкт-Петербург, Балтийский государственный технический университет

«ВОЕНМЕХ» им. Д.Ф. Устинова

ДВУХКРИТЕРИАЛЬНЫЙ АЛГОРИТМ ПЕРЕДАЧИ ДАННЫХ

Концепция системного подхода к подготовке кадров по направлению 230200 «Информационные системы» предусматривает изложение учебного материала по вопросам информационной безопасности в рамках курса «Проектирование информационных систем». Очевидно, что реализация такого подхода требует развития учебно-методического комплекса образовательных программ.

При изложении учебного материала по проектированию сетей передачи данных могут быть рассмотрены модификации классических алгоритмов, ориентированные на решение многокритериальных задач. Так, например, алгоритм Дейкстры позволяет решать задачу поиска минимальных (s-t)-путей с учетом минимизации загрузки маршрутизаторов сети передачи данных, заданной в виде графа.

В ходе выполнения двухкритериального алгоритма, каждой вершине V_j графа, отображающего топологию сети передачи данных, присваивается число q_j , равное значению минимального пути от вершины V_s до вершины V_j .

Шаг 1. Положить $n_{\max}=1$.

Шаг 2. Пометить вершину V_s . Положить $q_s=0$, $q_j \rightarrow \infty$, ($j \neq s$).

Шаг 3. Положить $i=s$. Положить $n=0$ (n – количество непересекающихся (s-t)-путей).

Шаг 4. Для каждой неотмеченной вершины j вычислить значение $q_j = \min\{q_j, q_i + p_{i,j}\}$.

Шаг 5. Проверить условие $q_j < \infty$. Если $q_j = \infty$, то перейти к шагу 9, так как (s-t)-пути в графе не существует. Если $q_j < \infty$, отметить ту из вершин V_j , у которой минимальное значение q_j , и отметить дугу выбранную на данном шаге.

Шаг 6. Положить $i=j$.

Шаг 7. Проверить условие $j=t$. Если условие не выполняется перейти к шагу 4. Если $j=t$, (s-t)-путь найден. Этот путь состоит из отмеченных дуг и является минимальным.

Шаг 8. Положить $n=n+1$. Удалить из графа вершины и дуги найденного (s-t)-пути. Перейти к шагу 2.

Шаг 9. Проверить условие $n < n_{\max}$. Если условие выполняется (количество путей нового множества меньше ранее найденного, поэтому его использование вызовет увеличение загрузки некоторых элементов сети), то процедура завершается. Если $n \geq n_{\max}$, то положить $n_{\max}=n$, добавить n найденных путей в множество (s-t)-путей и перейти к шагу 2. При этом далее рассматривается исходный граф с нулевыми значениями тех дуг, которые не вошли в полученное множество (s-t)-путей.

Представленный алгоритм передачи данных позволяет решать задачи проектирования сетевого уровня, обеспечивающего, по возможности, более равномерную нагрузку на маршрутизаторы и линии связи.

Коновалов А.М.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МОДЕЛИРОВАНИЕ БОТНЕТОВ НА ОСНОВЕ МНОЖЕСТВА ВЗАИМОДЕЙСТВУЮЩИХ
ИНТЕЛЛЕКТУАЛЬНЫХ АГЕНТОВ**

Настоящая работа посвящена моделированию крупномасштабных ботнетов, на основе рассмотрения компонент ботнета в виде обособленных интеллектуальных агентов. В работе анализируется протекание типичного жизненного цикла ботнета, а так же реализации различных сценариев инфраструктурных атак, проводимых злоумышленниками с их помощью. Проводится исследование стадии формирования ботнета и стадии реализации DDoS-атаки. Основными объектами исследования являются: архитектура ботнета, способы управления ботнетом, механизмы вовлечения новых участников в бот-сеть, типы реализуемых атак посредством ботнета.

Работа также включает исследование современных методов обнаружения бот-сетей и методов борьбы с ними, анализ их эффективности и выработку рекомендаций по построению эффективных систем защиты от данного типа угроз.

Основной парадигмой используемой в данной работе является представление узлов бот сети в виде множества интеллектуальных автономных агентов. Алгоритм поведения отдельного агента определяется его целевым назначением. Агенты имеют возможность непосредственно выполнять свою целевую задачу и обмениваться информацией друг с другом, образуя команды, ориентированные на достижение одной общей цели.

В работе моделируются два типа бот-сетей с различным типом управления: ботнет с централизованным командным центром и децентрализованный ботнет. Общими для данных типов моделей ботнетов являются агенты: «сетевое приложение», «хозяин», «зомби». Агент «хозяин» отдаёт приказы для выполнения ботнетом, агент «зомби» является вычислительным узлом и выполняет команды «хозяина». Фоновый трафик моделируется на пакетном уровне. Его формирование в модели возложено на специальный агент – «сетевое приложение», в задачу которого входит эмуляция сетевых приложений различного типа. Алгоритм эмуляции сетевых приложений включает в себя формирование и отправку пакетов, в соответствии с заранее установленными статистическими характеристиками моделируемого трафика.

Цель атаки так же представляется в виде агента «сетевое приложение». В модели ботнета с централизованным командным центром вводится агент «командный центр» отвечающий за регистрацию взаимодействия между агентом «хозяин» и агентами типа «зомби». В модели децентрализованного ботнета агенты «зомби» включают в себя функциональность по формированию пиринговых сетей. Моделирование сценария начинается с фазы скрытого формирования ботнета, далее реализуется фаза ожидания и затем – фаза атаки.

В качестве инструментального средства построения модели ботнетов была выбрана система моделирования дискретных событий OMNET++ с библиотекой классов INET Framework. Агенты реализуются в виде подключаемых модулей, которые включают в себя описание логики поведения агента. Так же предполагается создание моделей противодействия ботнетам, проведение экспериментов и оценка эффективности моделей противодействия.

Работа выполнена при финансовой поддержке РФФИ (проект №07–01–00547), программы фундаментальных исследований ОНИТ РАН (контракт №3.2/03) и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE–RUST (контракт № 021186–2) и других проектов.

Кононов В.О.

**Россия, Санкт-Петербург, Санкт-Петербургский институт управления и права
ПРАКТИКА ИНТЕРНЕТ-ПРОДВИЖЕНИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Появление Интернета как элемента строящегося информационного общества позволило обеспечить беспрецедентные возможности инфокоммуникационного взаимодействия его пользователей, насчитывающих сегодня во всем мире более миллиарда человек. Интернет стал широко использоваться в качестве канала передачи рекламной информации для реализации маркетинговых коммуникаций, обеспечивая максимально тесный контакт между рекламодателями и конечными потребителями при минимальных затратах. Сформировался новый атрибут информационно-технологического способа производства – Интернет-маркетинг.

С момента своего появления в начале 90-х годов Интернет-маркетинг развивался достаточно медленно вследствие ограниченности аудитории и Интернет-образованности пользователей, а самым действенным способом продвижения продукта была баннерная реклама, появившаяся в 1994 году.

В 1997 году из-за активизации недобросовестных Интернет-маркетологов появилась ощутимая проблема спама, обладавшая высокой эффективностью вследствие упомянутой выше неосведомленности пользователей. Следующие 10 лет в неконвенциональном Интернет-маркетинге наблюдалась высокая активность. Сегодня эффективность спама значительно упала в связи с все

растущей Интернет-образованностью и применением почтовыми системами методов борьбы с ним. Однако проблема по-прежнему остается не решенной: возросли возможности спамеров по мощностям, и чтобы добиться прежних результатов, они рассылают еще больше спама.

В настоящее время Интернет-маркетинг быстро развивается, каждый год появляются все новые методы и совершенствуются методики продвижения в сети Интернет. Сегодня в распоряжении Интернет-маркетолога находится множество методов продвижения, как конвенциональных, так и запрещенных неконвенциональных: поисковая оптимизация, контекстная реклама, баннеры, сайты-спутники, грамотная организация интерфейсов, дорвеи, спам и др.

Для некоторых проектов допустимо использование «серых» и «черных» методов маркетинга, что является очень рискованным и требует значительного опыта от ведущих маркетологов для «балансирования на грани». В случае их успешного применения требуемый результат превосходит ожидания и достигается за сроки в разы и десятки раз меньше планируемых.

Из-за активности Интернет-маркетологов в области запрещенных направлений, приводившей к перенасыщенности выдачи поисковыми системами не релевантных результатов, за последние три года сложилась тенденция улучшения и оптимизации алгоритмов поиска информации, определения ее качества и релевантности. В 2006 году ситуация особенно обострилась: по самым «дорогим» запросам всю первую десятку результатов нередко занимали дорвеи. Поисковые системы приняли вызов, что послужило катализатором положительных изменений в отношении качества информации. Улучшение ведущими поисковыми системами алгоритмов поиска и определения важности информации вылилось в повышение позиций информационных сайтов и значительное повышение качества поисковой выдачи. Значительно усложнилась работа Интернет-маркетологов, использующих запрещенные методы продвижения. При этом сложнее стало добиваться результатов и в конвенциональных направлениях, так как для успешного продвижения стало необходимо учитывать новые повышенные требования как к контенту, так и к методам поисковой оптимизации и рекламы. Однако снижение конкуренции со стороны некачественных сайтов и дорвеев дало дополнительное пространство для развития конвенциональных направлений Интернет-маркетинга. Кроме того, по-прежнему неизменно весомым при ранжировании результатов поиска остается показатель уровня цитируемости сайта авторитетными Интернет-ресурсами. Таким образом, качество информации и формат ее представления начинают играть важнейшую роль в Интернет-продвижении продукта.

С приходом финансового кризиса наметился спад в области крупных Интернет-проектов, снизились уровни продаж в Интернет-магазинах. Небольшим компаниям, занимающимся Интернет-продвижением, предстоит борьба за выживание, так как суммарный спрос на данный тип услуг падает из-за сокращения бюджетов на продвижение. Однако Интернет-маркетинг будет и дальше занимать лидирующие позиции, так как реклама в Интернете требует значительно меньших финансовых вложений по сравнению с другими средствами маркетинговых коммуникаций. При этом вес конвенциональных методов продвижения будет становиться все больше при возрастающем внимании к качеству и безопасности информации в Интернете.

Копыльцов А.В., Сорокин И.В.

**Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ЭНТРОПИЙНЫЙ АНАЛИЗ ФАЙЛОВ ДЛЯ ВЫЯВЛЕНИЯ И КЛАССИФИКАЦИИ
ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

Вредоносное программное обеспечение для затруднения и обхода обнаружения может использовать различные методы шифрования и сжатия своего кода и данных. Для этих целей могут использоваться и стандартные упаковщики (например, VMProtect, Themida, ASProtect и т.п.), но это лишь ненадолго отсрочивает обнаружение таких вредоносных программ. Поэтому за последние годы стали появляться различные нестандартные упаковщики, которые и реализуют методы препятствующие обнаружению (полиморфизм, антиэмуляция и т.п.) упакованных вредоносных программ, т.е. выступают в роли защитного слоя. Чтобы преодолеть этот слой необходимо, чтобы либо в антивирусной системе был очень хороший эмулятор исполняемых файлов, либо в антивирусной компании был большой штат вирусных аналитиков, которые будут разрабатывать индивидуальные методы выявления вредоносных программ. В силу очевидных причин, по которым ни первое, ни второе не является приемлемым решением, для выявления подобного вредоносного программного обеспечения должны применяться новые комбинированные подходы, использующие различные методы анализа.

В данной работе рассмотрен энтропийный анализ, позволяющий грубо оценить принадлежность файла к тому или иному упаковщику. Основная идея, которая лежит в системе классификации заключается в том, что в большинстве случаев расположение участков с одинаковой энтропией в файле для одного и того же упаковщика имеет определенный порядок.

Таким образом, для построения подобной системы необходимо решить две задачи: сегментации и распознавания. Под задачей сегментации понимается адекватное разбиение файла на

характерные участки, имеющие определенный уровень энтропии, т.е. которые могут быть расценены как данные или как исполняемый код. После того как файл будет описан в виде последовательностей сегментов с определенными характеристиками, необходимо ввести функцию расстояния между такими образами, т.е. решить задачу распознавания. При разбиении файла на участки, наилучшим образом описывающих его структуру, в работе используется принцип минимальной длины описания. Основная идея заключается в следующем.

Среди множества моделей следует выбрать ту, которая позволяет минимизировать сумму: 1) длины описания модели; 2) длины данных, описанных посредством этой модели. Для задания функции расстояния между паттернами, представленных в виде последовательности сегментов в определенном порядке с определенными характеристиками, используется лингвистический подход, а именно вводится функция редактирования (Левенштейна). Эта функция задает минимальное количество операций редактирования необходимое для преобразования одной последовательности в другую. На последнем этапе экспертом задаются классы образов, представляющие конкретные программы-упаковщики, где каждый класс описывается набором эталонных образов, составленных из обучающей выборки.

В итоге решение о принадлежности нового файла к тому или иному упаковщику будет приниматься по правилу к – ближайших соседей. В силу того, что энтропийный анализ позволяет судить только о некоторой приближенной структуре файла, описанная система классификации может использоваться, как часть в комбинированном подходе по выявлению и классификации вредоносного программного обеспечения.

Корт С.С.

Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ПЕРИОДИЧНОСТЬ ОБУЧЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Во многих существующих подходах к построению системы обнаружения вторжений обычно используется статическое обучение классификатора. Однако, данный процесс подразумевает стационарность распознаваемого процесса. В общем случае данные, поступающие в систему, не является стационарным по следующим причинам:

- изменение поведения пользователя в течение времени;
- изменение окружения (появление в сети новых компьютеров и сервисов);
- изменение природы атак на систему;
- зависимости поведения пользователя в определенный момент времени от его поведения до этого момента времени.

Список этих причин можно расширить, но уже он показывает, что говорить о стационарности соответствующих процессов в системе некорректно. Как следствие этого, в идеальном случае обучение должно быть динамическим, а система должна быть адаптивной, периодически переобучаясь. Можно выделить три подхода к переобучению системы:

1) Переобучение системы инициируется пользователем. В том случае, если в системе отсутствует переобучение, она может оценивать поведение пользователя, которое можно охарактеризовать как стационарное.

2) Система обучается постоянно. Каждое новое событие вызывает переобучение. Переобучение при поступлении каждого события приводит к необходимости построения самообновляющегося профиля. К достоинствам данного подхода можно отнести преодоление проблемы адекватного описания модели системы, включающего условие стационарности. К недостаткам подхода можно отнести подверженность атакам на механизм обучения и неэффективность подхода, выражающаяся в слишком частой необходимости перестроения базы знаний.

3) Система переобучается при наступлении какого-то особого события. Данный подход к переобучению является адаптивным и устраняющим недостатки предыдущих двух подходов. Переобучение в данном случае выполняется при наступлении некоторого события, после возникновения которого соответствующий процесс не может оцениваться как стационарный и появляется необходимость перестроения базы знаний системы.

Вне зависимости от типа информации, на основании которой обучается система (нормальному поведению или данным об атаках), можно выделить три типа операций: разрешенные политикой безопасности, запрещенные политикой безопасности и неопределенные.

С точки зрения системы обнаружения вторжений неопределенной является операция, которая может быть оценена как принадлежащая и безопасному поведению и поведению нарушителя. Неопределенная операция может выполняться как нарушителем, так и авторизованным пользователем, как безопасной программой, так и разрушающим программным обеспечением. Необходимо отметить, что четко определенная политика безопасности системы должна уменьшать количество неопределенных операций.

Таким образом, факт выполнения неопределенной операции, являясь большой проблемой систем обнаружения вторжений, может служить событием-триггером, по которому целесообразно проводить переобучение системы обнаружения вторжений. Тогда переобучение системы обнаружения вторжений можно выполнять следующим образом:

- в том случае, если пользователь выполнил запрещенную политикой безопасности операцию: соответствующую аномальному поведению (система обучалась нормальному поведению) или атаку (система обучалась атакам);

- в том случае если пользователь выполнил неопределенную операцию: неспецифицированную как нормальную операцию политикой безопасности, или операцию, разрешенную политикой безопасности, которая может быть выполнена при вторжении.

Корт С.С., Павличенко М.В., Рудина Е.А.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
АЛГОРИТМ ОБНАРУЖЕНИЯ РАСПРЕДЕЛЕННЫХ ВТОРЖЕНИЙ**

Система обнаружения вторжений "Авгур" использует при своей работе алгоритм анализа динамики развития атаки. В основу этого алгоритма заложены типовые сценарии вторжений, основанные на взаимосвязи их различных этапов. Этот алгоритм анализирует состояние внешних станций по отношению к защищаемым сетевым сервисам. Данные для анализа с использованием метода верификации сценария атаки поступают от генератора событий. Далее, поток событий для каждого защищаемого сервиса (идентифицируемого по IP адресу сервера и номеру порта) демультиплексируется в соответствии с IP адресами удаленных станций.

Верификация сценария вторжения производится на основе установленной классификации сообщений генератора событий: сообщениях о попытках сканирования защищаемых сервисов и операционной системы сервера, сообщениях о попытках непосредственной эксплуатации уязвимостей – атаках, о консолидации по окончании атаки, об обращениях с неконтролируемых портов защищаемого сервера и т.п. Кроме того, при верификации учитываются данные о версиях операционной системы и программного обеспечения защищаемого сервера. Определенным образом упорядоченные события, атрибуты которых скоррелированы как между собой, так и с известными данными о сервисе, могут быть объединены в единый сценарий вторжения.

СОВ "Авгур" может эффективно использоваться для обнаружения и верификации сценариев вторжений по схеме "один нарушитель – одна жертва", где нарушитель однозначно определяется по IP-адресу. Но данный подход не позволяет обнаруживать даже простейшие распределенные атаки.

Предлагаемое обобщение алгоритма динамики развития сетевого вторжения исключает из схемы обработки потока событий демультиплексор по адресу источника события. Попытка восстановления сценария развития вторжения в этом случае будет производиться по общему потоку событий. Предполагается, что условий верификации сценария вторжения достаточно для приблизительной оценки связи событий между собой даже без гарантии того, что каждое из них инициировано одним и тем же источником. При верификации сценария по общему потоку событий можно произвести уточнение возможности связи источников составляющих его событий между собой по ряду корреляционных признаков.

Для корреляции источников предполагаемого вторжения можно предложить следующие группы признаков, используемые как по отдельности, так и совместно друг с другом.

1. Корреляция по IP адресам. Признаком является совпадение IP адресов или принадлежность этих адресов к одной подсети. Возможно формирование более сложных методов корреляции на основе IP адресов (например, базирующихся на их статистической обработке).

2. Корреляция по расстоянию до подозрительных хостов. Расположенные рядом хосты должны иметь близкие значения времени жизни пакета.

3. Корреляция на основе дополнительных полей протоколов сетевого и транспортного уровня.

4. Корреляция по содержимому сетевых пакетов. В основе лежит предположение о том, что при выполнении распределенных атак генерируются пакеты с одинаковым или схожим содержимым.

5. Корреляция на основе соответствия конфигурации ОС и сетевых сервисов подозрительных хостов. Подразумевает использование активных методов сетевой разведки системой обнаружения вторжений относительно атакующих станций. По результатам обратного сканирования можно выполнить анализ схожести версии и конфигурации ОС и сетевых сервисов этих станций (как правило, при организации бот-сети нарушитель использует одну и ту же известную уязвимость ОС или сетевого сервиса).

Описываемое обобщение алгоритма динамики развития вторжения (дополненного некоторыми сценариями вторжений) позволит применить этот алгоритм к обнаружению распределенных вторжений, в том числе распределенных атак отказа в обслуживании, вторжений с использованием т.н. бот-сетей.

Крыжановский О.В., Субботин Р.В.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

информационных технологий, механики и оптики

ИСТОРИЧЕСКИЕ АСПЕКТЫ ВОЗНИКНОВЕНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Объективно категория «информационная безопасность» возникла с появлением средств информационных коммуникаций между людьми, а также с осознанием человеком наличия у людей и их сообществ интересов, которым может быть нанесен ущерб путём воздействия на средства информационных коммуникаций, наличие и развитие которых обеспечивает информационный обмен между всеми элементами социума.

Учитывая влияние средств информационных коммуникаций на трансформацию подходов к информационной безопасности, в их развитии можно выделить несколько этапов.

I этап характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.

II этап связан с началом использования искусственно создаваемых технических средств электро- и радиосвязи. Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

III этап связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.

IV этап связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности первоначально решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

V этап обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.

VI этап связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. При этом угрозы информационной безопасности стали гораздо серьезнее. Для обеспечения информационной безопасности в компьютерных системах с беспроводными сетями передачи данных потребовалась разработка новых критериев безопасности. Образовались сообщества людей – хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности – важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право – новая комплексная отрасль правовой системы.

VII этап связан с созданием и развитием глобальных информационно-коммуникационных сетей, с использованием космических средств обеспечения. Можно предположить, что очередной этап развития информационной безопасности, очевидно, будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности, как представляется, необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

В настоящее время информационные технологии очень активно развиваются. Осваиваются новые возможности и технологии, например, нанотехнологии. Вследствие этого осложняются и задачи обеспечения информационной безопасности.

Лохвицкий В.А.

Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского

МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ СЕТЕВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ФОРМИРОВАНИЙ КОСМИЧЕСКИХ ВОЙСК В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

В работе решается задача анализа влияния воздействий на производительность информационной системы и мероприятий по их нейтрализации (дополнительных временных

задержек, снижения производительности сети), оценки возможных мер защиты и разных комбинаций этих мер.

Рассмотрено несколько основных подходов к моделированию функционирования сетевых информационных систем: вероятностные полиномиальные процедурные модели, искусственная нейронная сеть (ИНС), потоковые модели.

В основу математической модели процесса функционирования вычислительной сети положен аппарат сетей массового обслуживания с отрицательными заявками (G-сетей), который относится к потоковому типу. В качестве отрицательных заявок считаются любые факторы, влияющие на нормальное функционирование узлов системы, приводящие к потере заявок, выводу из строя узла, опустошению очереди заявок и т.д.

Модель может использоваться как инструмент для проектирования сетей различного назначения, их анализа функционирования в условиях неблагоприятного воздействия, а так же их оптимизации.

Лукомский Е.А.

Россия, Санкт-Петербург, ООО «НеоБИТ»

ТЕХНОЛОГИЯ ВИРТУАЛИЗАЦИИ ЗАЩИТЫ ДЛЯ КОНТРОЛЯ ФУНКЦИОНИРОВАНИЯ И ВЗАИМОДЕЙСТВИЯ ПРИЛОЖЕНИЙ

При построении защищенных информационных систем встает задача безопасного исполнения недоверенных приложений в доверенной среде и задача контроля взаимодействия приложений, в частности, доверенного разделения информационных потоков различных категорий при взаимодействии приложений друг с другом.

С точки зрения обозначенных задач, современные технологии аппаратной и программной виртуализации позволяют реализовать две важные функции контроля по отношению к гостевым ОС:

1. Контроль функционирования гостевой ОС и ее приложений.
2. Контроль взаимодействия гостевой ОС и хостовых аппаратных ресурсов.

Применение технологий виртуализации позволяет свести задачу безопасного исполнения недоверенных приложений (и даже ОС) в доверенной среде к задаче контроля функционирования приложений гостевой ОС.

Виртуализация в данном контексте позволяют разработать доверенную систему мониторинга и управления процессами гостевых ОС.

Технологически достижимым для такой системы является следующий набор функций контроля:

- разграничение доступа к ресурсам между прикладными процессами и процессами администрирования;
- изоляция процессов различных гостевых ОС друг от друга, процессов гостевой ОС от хостовой ОС и наоборот;
- управление механизмами планирования гостевых ОС;
- подтверждение работоспособности приложений.

Реализация такой системы предполагает ее настройку для работы с конкретными гостевыми ОС, что в случае закрытых ОС является достаточно трудоемкой, но решаемой задачей.

Возможности механизмов аппаратной виртуализации по контролю взаимодействия гостевой ОС с аппаратными ресурсами хостовой ОС позволяют предложить решение обозначенной задачи доверенного разделения на одной физической машине.

На основе данной технологии разделения может быть разработана система, реализующая мультиплексирующий удаленный терминал для нескольких Windows-машин с гарантией не влияния и изоляции информации между ними.

Гипервизор, как программная основа средства виртуализации в такой системе, позволит гарантировать:

- взаимодействие драйвера сетевой карты только с назначенным ему устройством;
- формирование канала с участием только двух сетевых карт и исключение участия в канале данных других сетевых карт.

Предложенный подход к построению такой системы также позволяет использовать готовую реализацию драйверов сетевых карт для распространенных ОС. В этом случае изоляция в гипервизоре может основываться на унифицированных механизмах взаимодействия драйверов сетевых карт с устройствами.

Современные технологии виртуализации значительно упрощают построение защищенных информационных систем, обрабатывающих конфиденциальную информацию различных категорий и обеспечивающих с помощью контроля функционирования заданный уровень доверия без предъявления требований к исполняемым приложениям.

Мамутова О.В.

Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

ВОПРОСЫ ОРГАНИЗАЦИИ ПАМЯТИ В ВЫСОКОНАДЕЖНОЙ СИСТЕМЕ

Организация многоуровневой памяти в высоконадежной вычислительной системе с резервированием (ВВСП) определяет характеристики надежности, информационной безопасности и производительности системы. На информационную безопасность ВВСП, как и на ее надежность, влияет тип и архитектура используемой памяти, соотношение объемов локальной и общей системной памяти, производительность памяти, а также надежность и производительность каналов связи процессоров с памятью.

Так, при обращениях процессора к локальной памяти используются высокоскоростные каналы связи, для которых сложно реализовать меры по повышению надежности с использованием структурной избыточности. При этом следует отметить, что в случае, когда локальная память и процессор расположены на одном кристалле, надежность канала связи значительно возрастает. В случае обращения к общей системной памяти используются менее скоростные каналы связи, и существует целый ряд методик по повышению достоверности передачи информации по таким каналам связи. Кроме того, одним из параметров функции надежности ВВСП является общая производительность вычислительной системы, на которую влияет соотношение объемов локальной и общей системной памяти. Тип и архитектура используемой памяти определяет характеристики надежности самой памяти.

Поставлены следующие задачи: разработать метод определения оптимальной конфигурации оперативной памяти в ВВСП, обеспечивающий максимальную производительность при заданной надежности; разработать методику выбора надежных каналов связи процессоров с блоками памяти; разработать методику выбора надежной архитектуры памяти.

В рамках проводимого исследования рассматриваются различные архитектуры блоков памяти. Блоки памяти могут строиться на базе различных моделей: с использованием кодов с обнаружением/исправлением ошибок, например кодов Хэмминга, или с использованием блочных корректирующих кодов. Каждая такая модель имеет свои характеристики надежности и производительности, которые должны учитываться при рассмотрении ВВСП.

Традиционно оценка надежности системы с фиксированной структурой осуществляется на основе параметров надежности ее элементов. Такой способ не подходит для решения поставленной задачи, поскольку не учитывает производительность отдельных элементов системы, в частности, блоков памяти и каналов связи (контроллер связи рассматривается как составная часть канала связи и его производительность включается в общую производительность канала связи). Для исследования архитектуры ВВСП предлагается имитационная модель, которая позволяет оценить надежность с учетом производительности элементов системы.

Модель обеспечивает обращение к блокам памяти и анализ условий выполнения характеристик надежности и производительности; расчет сравнительных оценок характеристик систем при различных показателях надежности и производительности их основных компонентов (процессоров, блоков памяти и каналов связи). Модель строится на основе временных сетей Петри, что позволяет задать вероятностные параметры надежности и временные параметры производительности. В качестве инструмента моделирования выбрана среда Mobius, позволяющая решать поставленные задачи за счет возможности построения гибких иерархических моделей на основе различных формализмов.

Мандригин И.С.

Россия, Санкт-Петербург, Балтийский государственный технический университет

«ВОЕНМЕХ» им. Д.Ф. Устинова

РОЛЬ СИСТЕМ АВТОМАТИЗАЦИИ УПРАВЛЕНЧЕСКИХ БИЗНЕС-ПРОЦЕССОВ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

Обеспечение информационной безопасности предприятия – задача, важность которой сложно переоценить. Рассмотрим эту задачу с точки зрения бизнес-процессов, необходимых для её решения. Она решается некоторым множеством бизнес-процессов различных уровней. Прежде всего можно выделить два уровня процессов: уровень управления и уровень исполнения задач. Также как и любые другие бизнес-процессы, процессы этих уровней можно выявить и формализовать. Польза от выявления процесса очевидна, основным достоинством формализации является обеспечение регулярности этого процесса и возможности его автоматизировать, частично или полностью.

Рассмотрим возможности формализации и автоматизации бизнес-процессов на вышеописанных уровнях. На уровне исполнения существует много инструментов, так или иначе формализующих и автоматизирующих эти процессы: от систем резервного копирования и антивирусных сканнеров, работающих по расписанию, до сложных систем, разрабатываемых специально для конкретного предприятия.

На уровне управления предложения рынка гораздо скуднее. Если для формализации управленческих процессов существует целый класс программного обеспечения – систем управления

проектами, то для автоматизации практически ничего нет. Однако, автоматизация подобных процессов имеет несколько неоспоримых преимуществ. Во-первых, с помощью автоматизации можно разгрузить управляющий состав от рутинной работы. Во-вторых, она позволяет обеспечить регулярность процессов управления.

Однако, использование формализованных моделей бизнес-процессов порождает одну серьезную проблему: не всегда процесс развивается по запланированному сценарию. Подобные незапланированные события можно условно подразделить на два больших класса: предсказуемые(или прогнозируемые), и непредсказуемые(исключения, говоря в терминологии разработки программного обеспечения). Для обработки событий первого класса в формальную модель процесса должна входить возможность ветвления, и выполнения по конкретной ветке сценария. Для второго – должна быть возможность приостановить или полностью остановить выполнение процесса, для того, чтобы взять ситуацию под контроль.

Вышеизложенный функционал практически не представлен на сегодняшний день на рынке. Следовательно, необходима разработка новой системы. Основными требованиями к этой системе являются: автоматизация и формализация процессов уровня управления, возможность внедрения, ветвлений в формальные модели бизнес-процессов, возможность как остановки, так и временной приостановки выполнения бизнес процесса.

Создание и внедрение такой системы позволит: выявить, формализовать и автоматизировать процессы обеспечения информационной безопасности предприятия, разгружая управленческий персонал и обеспечивая регулярность исполнения процессов.

Мирин А.Ю., Сухов Д.К.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ВОПРОСЫ ВОССТАНОВЛЕНИЯ УДАЛЕННОЙ ИНФОРМАЦИИ ПРИ ИССЛЕДОВАНИИ
ЦИФРОВЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ В ПРОЦЕССЕ ЭКСПЕРТИЗ**

Важным аспектом при исследовании цифровых носителей информации является процедура восстановления удаленной информации. В докладе рассматривается реализация такой процедуры, включающей следующие аспекты.

Поиск и восстановление ранее удаленной информации (электронных документов, их фрагментов, других информационных компонент) на всей поверхности жесткого диска.

Поиск и восстановление ранее удаленной информации в имеющихся информационных компонентах. Это необходимо, так как при наличии на жестком диске базы данных, в ней могут существовать записи, помеченные как удаленные, и не отображаемые в программах работы с данными базами данных, но фактически не стертые с диска. Например, удаленные, но не стертые записи могут присутствовать в почтовых и других базах данных, где удаление может происходить в несколько этапов. Существует остаточная информация и на участках машинного носителя уже приписанных к новым документам. Это связано с техническими особенностями функционирования прикладных программ, операционных систем, систем управления базами данных и др.

Процедура восстановления данных выполняется с использованием специальных программных средств, знаний и опыта эксперта.

Михайлов Н.С.

**Россия, Санкт-Петербург, Балтийский государственный технический университет
«ВОЕНМЕХ» им. Д.Ф. Устинова
ОРГАНИЗАЦИЯ БЕЗОПАСНОЙ МОДЕРНИЗАЦИИ ИНФОРМАЦИОННОЙ СРЕДЫ
ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ**

Промышленные предприятия, в условиях конкурентного рынка требуют оперативного реагирования на динамически изменяющиеся внешние условия. Для автоматизации процесса управления предприятием на различных уровнях используются информационные системы (ИС).

Необходимо построение единого информационного пространства предприятия или корпоративной информационной системы (КИС).

Существует два основных пути перехода к КИС:

1. Внедрение КИС целиком, разработанной сторонней организацией.
2. Разработка КИС или каких-либо ИС самой организацией.

В первый вариант необходимо вкладывать материальный ресурс сразу в полном объеме на приобретение и внедрение системы.

Во втором варианте материальные ресурсы расходуются последовательными этапами, но требуется больше времени на исполнение.

Оптимальным будет использовать срединный вариант: часть ИС приобретать, а остальные разрабатывать собственными силами. Таким образом, внедренные системы, которые успешно справляются с поставленными задачами, следует использовать с максимальной отдачей,

оптимизируя их функциональность. Так же предстоит автоматизировать еще ряд подразделений или БП и обеспечить информационную связь между всеми ИС в оптимальной форме.

В основе плавной модернизации ИС лежит технология реинжиниринга бизнес-процессов. Эта технология учитывает совместную эксплуатацию элементов «старой» и «новой» ИС, многоструктурность и динамику изменения этих структур на всех этапах жизненного цикла изделия.

Основные проблемы и факторы, сдерживающие распространение и использование реинжиниринга, связаны с его начальной стадией – построением представлений унаследованной (модернизируемой) ИС.

Методика модернизации структуры и функционирования КИС 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, выкраив 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 структуры и функционирования КИС необходимо учесть указанные рекомендации по обеспечению сохранности данных, циркулирующих в информационной среде предприятия.

Михайлова А.С.

Россия, Санкт-Петербург, Балтийский государственный технический университет

«ВОЕНМЕХ» им. Д.Ф. Устинова

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ АВТОМАТИЗИРОВАННОМ ПОСТРОЕНИИ ТЕЗАУРУСА УЧЕБНОГО ТЕКСТА

Тезаурус (от греч. thesaurus "сокровище, сокровищница") – идеологический словарь, в котором показаны семантические отношения между лексическими единицами.

При разработке тезауруса учебного текста следует учитывать то, что информация, содержащаяся в тезаурусе, может быть доступна по сети большому числу пользователей. Для того, чтобы обеспечить целостность и сохранность информации, необходимо разработать меры безопасности.

При разработке компьютерной учебной среды для изучения любой дисциплины возникает проблема описания понятийной структуры учебного курса. Термины и семантические связи между ними составляют «скелет» любой дисциплины. В традиционно построенном учебном процессе учащийся усваивает терминологию постепенно, а взаимосвязи (и то далеко не все) между понятиями, а также контексты (семантические окружения) понятий более или менее начинают проясняться только после изучения курса. Это обусловлено тем, что ни специальных аудиторных занятий, ни специальной научной и методической литературы, кроме словаря терминов, где указаны только определения понятий, учащемуся не предоставляется. Объясняется это сложностью подачи такого материала в традиционном виде. Тезаурусы (в котором указаны отношения между терминами) позволяют решить некоторые из этих сложностей.

Применение компьютерного тезауруса в учебном процессе, в частности, позволяет:

- изучать основную терминологическую лексику данной дисциплины, используя также средства визуализации объектов-понятий;
- ассоциативно усваивать элементы знаний на основе многоаспектного использования информации тезаурусной структуры, генерируемой в компьютерной учебной среде;

- моделировать учебные ситуации и решать задачи из данной предметной области на понятийном уровне, без метрических соотношений;
- получать доступ к компьютерному тезаурусу одновременно многим пользователям в удобное для них время;
- разрабатывать личные тезаурусы преподавателя и студента и формировать учебные базы знаний в виде тезаурусов по различным дисциплинам;
- обмениваться моделями знаний в форме тезауруса;
- встраивать созданные тезаурусы в компьютерные учебные среды более сложной структуры;
- размещать разработанные тезаурусы по различным учебным дисциплинам в Интернете для обучения и развития.

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 интуиционных методов исследования при формировании тезауруса;
4. определение связи между понятиями вручную и единожды одним экспертом;
5. некомпетентное установление связей между терминами экспертом, потому что мнения экспертов могут быть различными и нет такого текста, где бы не затрагивались другие области, кроме той, которой посвящен материал;
6. невозможность одновременной многопользовательской работы с системой.

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

Передача информации из тезауруса учебного текста 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/полный просмотр, изменение информации и другие.

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

Некрасова Е. А., Шустиков С. В.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
информационных технологий, механики и оптики**

РАЗРАБОТКА СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ С ПРИМЕНЕНИЕМ ФУНКЦИОНАЛЬНОЙ МОДЕЛИ

В докладе рассмотрены вопросы практического применения обобщенных функциональных моделей системы менеджмента информационной безопасности при построении СМИБ конкретных организаций на примере телекоммуникационной компании.

На первом этапе построения проводится аудит существующих процессов информационной безопасности. Его результаты представляются в виде функциональной «as is» модели.

На втором этапе полученная «as is» модель анализируется, сравнивается с обобщенной (эталонной) моделью, вырабатываются рекомендации по составу и структуре «to be» модели, затем строится собственно «to be» модель.

На третьем этапе планируются изменения, необходимые для приведения модели «as is» к модели «to be», которые затем реализуются на практике путем изменения соответствующих процессов информационной безопасности.

В результате применения изложенного подхода достигается повышение качества процессов информационной безопасности по сравнению с традиционными способами разработки системы менеджмента информационной безопасности.

Нестерук Ф.Г., Нестерук Л.Г., Нестерук Т.Н.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МОДЕЛИРОВАНИЕ СРЕДСТВ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ ДЛЯ
СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ И ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ**

Рассмотрена методика минимизации нечеткой базы знаний в составе средств интеллектуального анализа данных (ИАД) для систем защиты информации (СЗИ) и поддержки

принятия решений (ППР). Иллюстрируются основные этапы минимизации нечеткой базы знаний с использованием универсальной среды моделирования MATLAB.

Средства интеллектуального анализа данных находят широкое применение при построении адаптивных средств классификации в составе современных СЗИ и ППР. Оперативность реакции СЗИ на динамику угроз и изменение характера компьютерных атак напрямую связана с объемом нечеткой базы знаний (БЗ) в составе средств ИАД. Устранение избыточности БЗ, а, следовательно, и повышение производительности анализа данных при решении задач защиты информации представляется актуальным.

Цель публикации – обсуждение методики минимизации нечеткой БЗ в составе средств интеллектуального анализа данных для СЗИ и ППР с использованием функциональных возможностей универсальной среды моделирования MATLAB.

Функциональных возможности инструментария Fuzzy Logic Toolbox среды MATLAB позволяют исходя из массива данных, отображающих искомую взаимосвязь входных и выходных значений, посредством методов кластеризации автоматически сформировать базу знаний, соответствующую модели нечеткого логического вывода Сугено, и отобразить ее на топологию нейронной сети (НС) ANFIS. Возможность обучения НС позволяет адаптировать нечеткую БЗ на обучающей выборке для восстановления точности формируемых значений после выполнения этапов сокращения и минимизации системы правил согласно методике минимизации нечеткой базы знаний.

Выполнению преобразований знаний согласно предлагаемой методике предшествует формирование исходного массива данных для обучающей выборки и его сохранение в виде текстового файла, оформленного в соответствии с требованиями Fuzzy Logic Toolbox. Методика минимизации нечеткой БЗ включает этапы.

Извлечение закономерностей, скрытых в исходных данных, и описание их системой правил, соответствующих модели нечеткого логического вывода Сугено. Основным недостатком автоматически формируемой нечеткой базы знаний – существенная избыточность, которая, с одной стороны, приводит к потере наглядности логической взаимосвязи знаний, а, с другой, – снижению оперативности формирования заключений.

Сокращение избыточной БЗ путем удаления значительной части правил логического вывода без потери знаний, зафиксированных в системе правил, что обусловлено возможностью альтернативного представления знаний в нормальных формах: либо дизъюнктивной – ДНФ, либо конъюнктивной – КНФ. Сокращенная нечеткая БЗ остается избыточной, т.к. для ряда правил логического вывода можно выделить переменные, не влияющие на формируемые базой знаний заключения. Обучение нейронной сети ANFIS на массиве исходных данных восстанавливает точность преобразования.

Минимизация сокращенной БЗ согласно одному из методов отыскания простых импликант, например, Квайна-МакКласки или посредством карт Карно. Применение названных методов минимизации обусловлено использованием в качестве термов двух противоположных функций принадлежности S (малая величина) и L (большая величина). Коррекция сокращенной базы знаний приводит к некоторому снижению точности преобразования, которая, как правило, восстанавливается после цикла обучения нейронной сети ANFIS.

Нечай А.А.

Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского
МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ СЕРВЕРА В УСЛОВИЯХ РАЗРУШЕНИЯ
ПРОГРАММНО- АППАРАТНОЙ СРЕДЫ

В современных информационных системах роль замыкания модели объекта и модели действий принадлежит администратору. В конечном счете, именно на администратора ложится ответственность за соблюдение атрибутов информации и программного обеспечения. Поэтому обычному персоналу для корректной работы с сервером требуется знания системного уровня вычислительных комплексов и сетей. Поэтому, несмотря на самые сложные системы защиты, всегда остается возможность нарушения работоспособности программно-аппаратной системы за счет использования режима суперпользователя.

Предлагаемая модель обладает потенциальными возможностями по обеспечению адекватного функционирования системы в условиях разрушения программной среды. Правильно построенная система должна строиться на целевой, обеспечивающей и защитной системе. В настоящее время реализуется только целевая подсистема. В данной модели предусматривается реализация всех трех подсистем: целевой, обеспечивающей и защитной, на основе полинома интерполирующего последовательность символов реализующих свойства целостности объекта в философском понимании этого свойства. Модель сформирована на основе применения алгебраических операций связанных со свойствами несущих множеств.

Главной идеей является вывод недостающих элементов множества на основе целостного описания данного множества. Представление информации в ЭВМ в цифровом виде позволяет

строить самовосстанавливающиеся системы, основываясь только на правилах математического вывода и имеющихся, не уничтоженных элементах информации. То же самое касается и системного программного обеспечения, когда речь идет о восстановлении последовательности утраченных команд. Таким образом, модель является универсальной для любых типов информации.

Никифоров В.В., Скорлышев Д.Ю., Шкиртиль В.И.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МОДЕЛИРОВАНИЕ ЗАЩИТЫ ЦЕЛОСТНОСТИ ДАННЫХ В СИСТЕМАХ РЕАЛЬНОГО ВРЕМЕНИ**

Программное обеспечение компьютерных комплексов, предназначенных для управления сложным автоматизированным оборудованием, составляет особый класс программных систем. Поскольку такие системы должны работать в структуре времени, определяемой ходом процессов в физической сфере, они относятся к разряду систем реального времени (СРВ). Ввиду разнообразия автоматизируемых узлов и агрегатов, разнообразия их взаимосвязей, различиях в темпах их функционирования, программные приложения СРВ должны строиться в виде множества относительно самостоятельных тесно взаимодействующих задач. По мере роста сложности внешних процессов расширяются и усложняются требования к функциональным возможностям многозадачных программных приложений СРВ. Во избежание поломок дорогостоящего управляемого оборудования, а в ряде случаев во избежание человеческих жертв к функционированию таких многозадачных систем предъявляются повышенные требования надежности, предсказуемости, своевременности выполнения возлагаемых на систему функций. В этой связи их относят к классу жестких СРВ. Для обеспечения отмеченных повышенных требований к жестким СРВ необходимо совершенствовать технологии разработок соответствующих программных средств.

К ряду существенных достижений в разработке технологий создания сложных программных систем (в том числе жестких СРВ) относится создание элементов технологий визуального графического моделирования, и, в частности, универсального языка моделирования UML. Разрабатываются специальные средства автоматизации перевода архитектурных решений, представляемых графическими конструкциями UML, в коды программ на стандартных языках программирования. Один из подходов к такого рода автоматизации связан с промежуточным преобразованием графических конструкций UML в конструкции текстовых языков моделирования – например, языков Express, XML. В представляемом докладе предлагаются такие форматы спецификаций внешних и программных объектов на языке XML, которые ориентированы на проверку корректности проектируемых программных конструкций в отношении защиты целостности разделяемых данных в жестких СРВ.

XML-модель СРВ включает модель внешнего оборудования СРВ и модель программного приложения. Внешнее оборудование представляется элементами, соответствующими внешним объектам – датчикам и эффекторам. Датчик представляется пустым XML-элементом с атрибутами: имя датчика (для связи с элементами, моделирующими программные компоненты СРВ), значение периода срабатывания датчика и, возможно, указатель элемента, моделирующего программную компоненту – обработчик прерываний (в случае, если датчик является активным – при его срабатывании возникает аппаратное прерывание). Срабатывание пассивного датчика состоит в генерации цифрового кода, выставляемого на интерфейсном регистре соответствующего периферийного блока компьютерной системы. Такие коды считываются по инициативе прикладных задач – либо обработчиков прерываний, либо программно активизируемых задач (потоков). Эффектор также представляется пустым XML-элементом с атрибутами: имя эффектора, указатель того датчика, срабатыванием которого начинается очередной цикл вычисления управляющего воздействия, выдаваемого на данный эффектор, максимальная продолжительность цикла вычислений выдаваемого на эффектор управляющего воздействия.

Программное приложение представляется XML-элементами, соответствующими прикладным задачам (аппаратно активизируемым обработчикам прерываний, и программно активизируемым задачам), а также XML-элементами, которые представляют межзадачные интерфейсы. Целостность глобальных структур данных, обеспечивается интерфейсными механизмами типа мьютексов, которые охраняют участки кода задач имеющие доступ к разделяемым системным ресурсам (критические интервалы). Порядок доступа к критическим интервалам определяется принятым в системе протоколом доступа к разделяемым ресурсам (важнейший атрибут представляющего программное приложение). Еще один необходимый вид межзадачных интерфейсов – очереди сообщений, которые используются в первую очередь для транзита аппаратных прерываний в программно-активизируемые задачи. Внутренняя организация программных компонент (задач) представляется в виде последовательности сегментов. Сегментом является участок кода задачи, который заканчивается операцией обращения к интерфейсному элементу. Полная XML-модель СРВ позволяет оценить своевременность выполнения отдельных задач и программного приложения в целом.

Ноздрачев С.О.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
информационных технологий, механики и оптики
IP-ТЕХНОЛОГИИ В СКУД**

Появление IP-технологий позволило сделать значительный шаг вперед и подтолкнуло разработчиков СКУД (Системы Контроля и Управления Доступом) на использование локальных сетей, а иногда и сети Интернет для объединения не только отдельных компьютеров, но и для объединения нескольких комплексов, отдельных систем. Тенденция увеличения такого оборудования на рынке уже заметна. Это объясняется удобством использования IP-технологии и перспективами её развития. Вместо сверления дыр в стенах с прокладкой новых кабелей можно использовать уже существующий для подключения СКУД. Большая удаленность частей объекта – один из главных факторов использования сети Интернет для коммуникации между ними. Такое решение обосновано и с экономической точки зрения и с точки зрения эффективности.

Становится очевидным, что IP-технология будет развиваться дальше и постепенно будет все больше доминировать. По сути, происходит слияние или интеграция двух отраслей – IT и ТСБ. Объединяя возможности этих двух комплексов, можно получить системы защиты с еще большей эффективностью. Простой пример: Если сотрудник не прошел через систему контроля доступа (например на КПП), то его рабочее место (компьютер) будет заблокирован. Однако, как бы ни были радужны перспективы использования IP-технологий, здесь есть и свои минусы, как и в любом другом способе передачи информации.

Одной из таких проблем является возможность задержки при передаче информации по сети при её сильной загрузке. Однако при использовании выделенной линии для СКУД эта проблема может быть решена.

Чрезвычайно важная проблема при использовании сети – это безопасность данных, передаваемых СКУД. Пока существует возможность заблокировать канал или подать ложное сигнальное сообщение для снятия системы с режима охраны – эффективность всей системы стоит под вопросом. В таких ситуациях становится актуальным использование защищенных каналов связи и шифрования. Конечно, существуют объекты, на которых категорически нельзя использовать открытый канал Интернета. Такими объектами могут являться, например, предприятия, работающие с государственной тайной или другие особо важные объекты. Однако когда речь заходит о каком-либо магазине или бизнес-центре, то несанкционированный съём информации с СКУД и СУРВ (систем учета рабочего времени) вряд ли способен привести к нанесению серьезного ущерба.

Эффективность работы СКУД, зависит от того, насколько грамотно построено администрирование сети на объекте. Эта роль ложится на IT-отдел. Именно это подразделение распределяет трафик, управляет загруженностью каналов и может обеспечить необходимые условия для эффективного функционирования СКУД и других систем на основе сети.

Используя IP-технологии необходимо учитывать, насколько критично будут влиять сбои в работе на эффективность работы систем СКУД или СУРВ. Так, например, при задержке передачи информации в системе СУРВ не принесет практически никаких проблем, так как во многих современных контроллерах есть встроенные часы. И при возникновении задержки – в отчете будет находиться реальное время использования идентификатора – т.е. вся информация будет достоверной, хотя итоговый результат отчета будет сформирован немного позже из-за задержки. Однако в других системах задержка передачи информации может создать более существенные проблемы. Так, например, при возникновении задержки в СКУД, мы тратим не пару секунд для идентификации, а гораздо больше. А если в компании несколько сот человек, и каждый на прохождение КПП тратит по несколько десятков секунд – тут уже и опоздания и «толпа» перед пропускным пунктом.

Однако, поскольку сетевые технологии развиваются очень быстро, и пропускная способность каналов увеличивается буквально каждые полгода, то сетевые технологии представляются наиболее перспективными.

Ноздрачев С.О.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
информационных технологий, механики и оптики
IP ВИДЕОНАБЛЮДЕНИЕ С ИСПОЛЬЗОВАНИЕМ WIMAX**

При решении задач обеспечения безопасности важную роль играют системы IP-видеонаблюдения. IP-видеонаблюдение выполняет 2 основные задачи – мониторинг (текущий контроль) и наблюдение. Современные видеокамеры дают возможность преобразовывать изображение в IP пакеты, которые можно передавать с помощью прямого соединения или многопунктовой связи. Данные с камер пересылаются в контрольный центр безопасности организации. Быстродействующие прямые решения могут быть использованы для видеонаблюдения за объектом на расстояниях в десятки километров.

При наличии двух основных компонентов: беспроводной передачи данных и сетевых камер IP-видеонаблюдение обеспечивает мониторинг и контроль с очень высоким уровнем экономии и характеристик.

Есть ряд особенностей, связанных с использованием беспроводных систем IP-видеонаблюдения. При использовании Интернета, например, для передачи данных применяются такие меры защиты как межсетевой экран и пароли. Так как фиксированные беспроводные мосты передают сигнал через эфир, то существует возможность перехвата информации.

Провайдеры услуг беспроводной связи принимают различные меры по обеспечению безопасности данных: пароли, кодирование и др. Другой проблемой беспроводного способа передачи информации является то, что провайдеры постоянно увеличивают количество беспроводных соединений. Это может привести к интерференции между системами, работающими на близких частотах. Защиту от интерференции может обеспечить грамотный выбор частоты для конкретного применения. Существуют специальные устройства, которые в сочетании с приборами активного подавления интерференции обеспечивают защиту беспроводных сетей от помех в режиме реального времени.

Большое количество беспроводных IP-систем работают в стандарте IEEE 802.11. Однако, 802.11-е решение не обеспечивает большую область охвата, что делает его пригодным преимущественно внутри помещений. Но Wi-Fi можно использовать и на улице в прямой видимости от 112 м – 54 Мбит/с до 500 м – 6 Мбит/с. В настоящее время появляются новые поколения беспроводных IP-систем. Для беспроводной мегаполисной цифровой сети IEEE предложил новый беспроводной стандарт 802.16, аналогичный WIMAX.

Технология WIMAX действует на большие расстояния и поддерживает более высокую скорость передачи данных, чем конкурирующие технологии. Стандарт WIMAX способен поддерживать максимальную скорость 72 Мбит/с. Это почти в 7 раз выше, чем поддерживает стандарт IEEE 802.11b и в 2 раза выше, чем стандарт IEEE 802.11a/g. Проводное исполнение обеспечивает скорость передачи данных 1 Мбит/с, на коаксиальном кабеле – 10 Мбит/с, на витой паре – до 1000 Мбит/с. Расстояние, которое охватывает WiMAX-сеть, составляет десятки километров; для сравнения – сеть Wi-Fi охватывает расстояние 100 м и несколько сот метров с понижением скорости.

Даже без прямой видимости, стандарт IEEE 802.16 (WiMAX) покрывает площадь радиусом до 112,6 км. Базирующийся на технологии OFDM (мультиплексирование с ортогональным разделением каналов), этот стандарт позволяет более эффективно, чем Wi-Fi, решать проблемы невидимых участков среды (Non-Line of Sight - NLOS). По причине этих невидимых участков может появиться задержка сигнала. В WIMAX для борьбы с NLOS используется больше поднесущих. Для сравнения, в IEEE 802.11 a/g используется 64 поднесущих, в то время как в WIMAX – 256. По сравнению с Wi-Fi, в WIMAX отношение неиспользуемых данных к общему числу поднесущих гораздо меньше. Это способствует более высокой эффективности и более лучшим характеристикам WIMAX в противодействии NLOS. Выявленные преимущества стандарта WIMAX будут способствовать быстрому распространению этой технологии в области систем видеонаблюдения. Однако влияние метеорологических условий все же делает данную технологию уязвимой.

Для предотвращения хищения информации в WIMAX имеется встроенная возможность кодирования. Для кодирования данных используется стандарт DES и тройной DES для кодирования ключа. Учитывая особенности и постоянно растущие потребности систем видеонаблюдения, можно сделать положительный прогноз об использовании технологии WIMAX. Но для надежного и грамотного альянса, необходимо будет преодолеть ряд трудностей, связанных со слабыми местами беспроводной технологии WIMAX.

Обухов А.В.

Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского
ПОВЫШЕНИЕ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ОПЕРАЦИОННОЙ СРЕДЫ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ ПРИ НАЛИЧИИ ВОЗДЕЙСТВИЯ ВРЕДОНОСНОГО
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Современный уровень развития вычислительной техники, а также сложность решаемых задач, связанных с управлением летающими объектами, сделали информационно-управляющую систему (ИУС) неотъемлемой частью автоматизированной системы управления (АСУ) входящей в состав наземного автоматизированного комплекса управления. Эксплуатация ИУС связана с необходимостью оценивания её состояния и принятием решений по распределению функций между её компонентами для достижения цели функционирования наземных средств. Более того, функционирование ИУС оценивается различными показателями надёжности, производительности, живучести и т.д. Основным фактором, влияющим на функционирование ИУС, является устойчивость системного программного обеспечения и его невосприимчивость к различным видам вредоносного воздействия.

Научная новизна. В современной технической литературе встречаются различные методы обнаружения вредоносного воздействия. Наиболее перспективным является направление, связанное с разработкой систем обнаружения аномалий программного обеспечения. Все методы обнаружения

аномалий делятся на две группы: с контролируемым обучением («обучение с учителем»), и с неконтролируемым обучением («обучение без учителя»). Основное различие между ними заключается в том, что методы контролируемого обучения используют фиксированный набор параметров оценки и некие априорные сведения о значениях параметров оценки. Время обучения фиксировано. В неконтролируемом же обучении множество параметров оценки может изменяться с течением времени, а процесс обучения происходит постоянно.

Общим недостатком всех существующих методов обеспечения функциональной устойчивости является реактивность их действий, т.е. различные виды систем обнаружения вторжений и антивирусных средств начинают свое действие только после заражения системы, а не в процессе распространения вредоносного программного обеспечения по ней, что значительно повышает вероятность поражения системы.

Наиболее перспективным направлением решения данной проблемы является разработка систем обнаружения аномалий (СОА), функционирование которых основано на принципиально новых методах и алгоритмах.

Основная идея метода состоит в наделении операционной среды ИУС свойствами искусственной иммунной системы (ИИС) (системы обладающей рядом свойств иммунной системы человека) для поддержания баланса между антителами (элементами системы, поддерживающими устойчивость функционирования) и антигенами (вредоносным программным обеспечением и/или процессами) в системе для обеспечения функциональной устойчивости ИУС.

Помимо основной задачи необходимо решить задачи прогнозирования, обнаружения и парирования воздействий. Кроме того интересной представляется задача разработки алгоритма обучения СОА на основе ИИС.

Орлов К. М

Россия, г. Санкт-Петербург, 24 Центральный НИИ Министерства обороны Российской Федерации

ПОСТАНОВКА НОВОЙ ЗАДАЧИ ВИЗУАЛИЗАЦИИ ИНФОРМАЦИИ

АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Одним из ключевых элементов современных автоматизированных систем в защищенном исполнении (АСЗИ) являются средства и подсистемы визуализации (отображения, представления) информации (ПВИ), обеспечивающие интерфейс в системе «человек-машина». Как и любая другая функциональная подсистема, ПВИ представляет собой сложную многофункциональную систему операторов и аппаратно-программных комплексов, обеспечивающую представление руководителям (ЛПР) результатов информационно-аналитической обработки информации в виде, удобном для принятия соответствующих проектных и управляющих решений (ПУР).

Синтез эффективных проектных решений по созданию современных средств и ПВИ в автоматизированных системах управления сопряжён, прежде всего, с поиском адекватных методов и алгоритмов оценки их качества и эффективности в составе АСЗИ с учётом возможностей современных технологий визуализации данных.

Современное развитие методов оценивания качества и эффективности сложных организационно-технических комплексов и АСЗИ по-новому ставит задачу комплексного квалиметрического (количественного измерения качества) учёта наряду с организационно-техническими показателями и характеристиками использования АСЗИ также потенциально-достижимых и ожидаемых (при эксплуатации – реальных) результатов целенаправленного использования каждой подсистемы и АСЗИ в целом с учётом степени соответствия этих результатов главным целям (по предназначению) функционирования АС (выполнения оценок валидации) на полном множестве входных ситуаций и состояний системы, включая типовые и нетиповые (нештатные) ситуации, воздействие внешних и внутренних факторов (инсайдеры и т.п.).

С учётом интенсивного развития IT- и IS-технологий и появления на рынке большого числа вариантов аппаратно-программной реализации современных методов обработки информации по-новому остро встаёт и вопрос оптимизации ПУР с соответствующим их количественным и многоаспектным (полимодельным) обоснованием, естественно, включая весь блок вопросов ресурсного обеспечения, обеспечения информационной безопасности, минимизации критичности.

Одним из перспективных направлений, по мнению автора, в этой связи следует рассматривать постановку задачи, разработку и реализацию так называемого метода многомерного комплексного визуального отображения информации (МКВОИ) сложных объектов для принятия эффективных решений в автоматизированных информационно-управляющих системах в защищённом исполнении (специального назначения).

Его отличительными особенностями, прежде всего, могут быть названы: многоаспектное и многокритериальное описание свойств поступающей, обрабатываемой и визуализируемой в АСЗИ информации; валидность анализа, синтеза вариантов и оптимизации архитектур и алгоритмов ПВИ, в том числе по критерию минимизации информационной избыточности и максимизации оперативности управления АСЗИ, ценности и достоверности используемой и визуализируемой информации, устойчивости, скрытности и непрерывности функционирования АСЗИ, качества принятия ПУР при использовании визуализируемой в АСЗИ информации.

При этом сформулированы подходы и возможные алгоритмы реализации МКВОИ в процессе решения ряда специфических задач АСЗИ, включая рассмотрение особенностей реализации предлагаемых критериев и показателей на всех этапах жизненного цикла ПВИ в составе АСЗИ.

Пашков М.П.

Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»
ИССЛЕДОВАНИЕ ПРОБЛЕМЫ РАССИНХРОНИЗАЦИИ ГРАНЕЙ В ТРОИРОВАННЫХ СИСТЕМАХ
ОБРАБОТКИ И ПЕРЕДАЧИ ИНФОРМАЦИИ

Современные бортовые вычислительные системы специального назначения, бортовые системы управления летательных аппаратов, космические системы имеют повышенные требования по надежности и информационной безопасности. К таким системам предъявляются повышенные требования обеспечения безотказной работы и достоверности обработки информации в течение всего срока эксплуатации, без какого либо технического обслуживания, так как системы не достигаемы для обслуживания.

Для обеспечения надежности в подобных системах применяется аппаратно реализованное двукратное резервирование канала обработки информации. Это означает, что в состав изделия входят три аналогичных комплекта аппаратных средств (три одинаковых грани), объединенных электрическими связями, в которых одновременно и синхронно выполняются идентичные вычислительные процессы.

Все внутренние связи изделия и модули являются троированными. Жесткую синхронизацию и мажоритирование потоков информации в каналах резервирования выполняют аппаратно мажоритарные элементы. При этом, на практике существует проблема возникновения рассогласования каналов резервирования из-за рассинхронизации граней системы, приводящая к отказу всей системы при работоспособном состоянии всех модулей.

Проблема синхронизации возникает из-за того, что в каждой грани используется свой тактовый генератор, и частота генерируемых импульсов может «плавать» друг относительно друга. А для побитного аппаратного мажоритара важно чтобы все вычисления производились четко одновременно.

Для решения рассматриваемой проблемы в докладе предлагается отойти от принципа жесткой аппаратной синхронизации и программно синхронизировать все грани системы. Предлагаемый метод позволяет устранить проблему рассинхронизации граней системы. Надежность работы системы и достоверность обработки информации возрастает ввиду того, что все грани работают независимо по времени друг от друга. Таким образом, исключается жесткая зависимость от потактовой синхронизации при незначительном усложнение всей системы. Вместе с тем дополнительно появляется возможность в случае наличия программного доступа к временным регистрам контролировать результаты выполнения элементов транзакций для каждой грани, что сокращает время отладки системы.

Перервенко А.В.

Россия, Санкт-Петербург, ЗАО «АСИС»
ПРОБЛЕМА НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
ПРИ ИСПОЛЬЗОВАНИИ АУТСОРСИНГА В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В условиях финансового кризиса многие компании ставят своей целью снижение затрат и повышение эффективности бизнес-процессов.

Одним из возможных способов оптимизации затрат является аутсорсинг.

Аутсорсинг — передача организацией определенных бизнес-процессов или производственных функций на обслуживание другой компании, специализирующейся в соответствующей области. В отличие от услуг сервиса и поддержки, имеющих разовый, эпизодический, случайный характер и ограниченных началом и концом, на аутсорсинг передаются обычно функции по профессиональной поддержке бесперебойной работоспособности отдельных систем и инфраструктуры на основе длительного контракта.

Наиболее перспективным кажется использование аутсорсинга в сфере ИТ — передача стороннему подрядчику ряда внутренних услуг и (или) внутренних сервисов компании-заказчика, в том числе на основе использования (например, аренды) его программных продуктов, приложений, технических средств и фрагментов инфраструктуры.

В то же время эксперты выделяют следующие проблемы развития ИТ-аутсорсинга в России: отсутствие регламентированных методологий, стандартизации предложений, общепринятых моделей ценообразования; взаимное недоверие заказчиков и поставщиков, отсутствие механизмов страхования рисков аутсорсинговых контрактов; отсутствие услуги выкупа ИТ-инфраструктуры; отсутствие поставщиков, обеспечивающих глобальное покрытие территории страны; отсутствие координации усилий государства, поставщиков и заказчиков в решении перечисленных проблем.

При этом необходимо особо отметить такой недостаток аутсорсинга в сфере ИТ, как риск утечки сведений конфиденциального характера, в результате предоставления нерегулируемого доступа к документам, данным и материальным ценностям предприятия.

Наиболее вероятным источником угрозы утечки информации являются недеklarированные возможности программного обеспечения.

Недекларированные возможности ПО — функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

В связи с этим проблема выявления недеklarированных возможностей является как никогда актуальной и требует разработки современных методик и соответствующих инструментов оценки.

Платонов В.В.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК НА ОСНОВЕ МУЛЬТИКАТЕГОРИЙНОЙ КЛАССИФИКАЦИИ**

Нарастающее количество сетевых атак остро ставит проблему их обнаружения. Применение систем обнаружения вторжений (COB), построенных на принципах обнаружения сигнатур, имеет существенные недостатки, главным из которых является принципиальная невозможность обнаружения новых атак. Поэтому в последние годы все большее число исследователей разрабатывают модели и подходы, позволяющие устранить главный недостаток COB обнаружения сигнатур. К числу таких подходов относится метод опорных векторов (SVM, Support Vector Machine), разработанный Вапником В.Н. Основная идея метода опорных векторов в случае линейной границы между классами состоит в построении параллельных разделяющих гиперплоскостей с максимальным зазором между ними. Алгоритм построения использует скалярное произведение объектов и построение оптимальной разделяющей гиперплоскости сводится к минимизации квадратичной формы. Две параллельных гиперплоскости строятся по обеим сторонам гиперплоскости, разделяющей классы данных. Метод основывается на предположении, что чем больше разница или расстояние между этими параллельными гиперплоскостями, тем меньше будет средняя ошибка классификатора. В случае невозможности линейного разделения метод использует переход от исходного пространства в новое пространство большей размерности, в котором возможно построение линейной разделяющей гиперплоскости. Такое пространство называется спрямляющим. При этом в алгоритме скалярное произведение $\langle x_i, x_j \rangle$ в исходном пространстве можно формально заменить скалярным произведением $\langle K(x_i), K(x_j) \rangle$ в новом пространстве. Причем можно не строить спрямляющее пространство. А использовать только соответствующие ядра.

В настоящее время появилось значительное число публикаций, посвященных применению SVM для решения различных задач, в том числе для обнаружения вторжений. Определенным минусом данного подхода являлось то, что сам метод был предложен для разделения двух классов. Поэтому одним из важных направлений исследований являлось построение SVM для разделения множества классов (более двух). Основным подходом являлось сведение многоклассовой классификации к последовательному решению нескольких задач двухклассовой классификации. В работе (Hsu C.-W., Lin C.-J. A comparison of methods for multi-class support vector machines. IEEE Trans. on Neural Networks. 13 (2002), 415-425) проводится сравнение этих подходов: каждый против всех, каждый против каждого и др. Несмотря на возможность реализации данных подходов, применение их для обнаружения сетевых атак оказывается проблематичным в силу необходимости обработки данных в реальном масштабе времени. Поэтому наиболее перспективными являются попытки построения метода SVM для разделения множества классов – мультিকатегорийной классификации. В докладе рассматриваются основные подходы к построению мультিকатегорийной классификации и их применимость к обнаружению сетевых атак. Анализ предлагаемых подходов проводился с учетом производительности алгоритмов, поскольку одним из важнейших требований к COB, является необходимость функционирования в реальном масштабе времени.

В общем случае проблема обнаружения сетевых атак заключается, в частности, в построении классов атак, которые послужат исходными данными для алгоритма работы SVM. Такое разбиение позволяет сформировать модульную структуру COB и разрабатывать модули SVM, предназначенные для разделения классов атак.

Для любого метода обучения с учителем (в том числе и для SVM) встаёт задача подготовки обучающего множества (или рабочей выборки). Эту задачу можно разбить на два этапа:

- экспертная оценка принадлежности каждого вектора к классу нормального/аномального поведения;
- снижение размерности рабочей выборки (избавление от лишних и доминирующих атрибутов).

При этом можно воспользоваться результатами, которые позволяют получить оценку ошибки в исходных данных для классификации.

Отмечается, что открытыми вопросами, которые требуют дополнительных исследований, являются следующие: формирование непересекающихся классов сетевых атак, исследование вида ядерных функций для разделения атак данного класса и др.

Применение метода SVM для обнаружения сетевых атак опирается и на общие вопросы построения систем обучения с учителем. В их числе необходимо отметить выбор значимых характеристик для обучения и классификации, подготовка обучающих и тестовых множеств исходных данных.

Платонов В.В., Поникаровский К.В.

Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
МОДЕЛИРОВАНИЕ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК МЕТОДОМ ОПОРНЫХ ВЕКТОРОВ

Одна из главных характеристик и одновременно критерий классификации систем обнаружения вторжений (СОВ) - подход к обнаружению вторжений. Традиционно различают СОВ с подходом к обнаружению вторжения на основе сигнатур и на основе обнаружения аномалий. Анализ видов существующих СОВ позволяет выделить главные недостатки двух существующих подходов к обнаружению вторжений. Поиск сигнатур требует глубокого анализа сущности атаки для выделения ее сигнатуры. Отсюда следует и другой недостаток - никакие новые атаки этот метод выявить не может, все сигнатуры могут появиться лишь после обнаруженного факта вторжения. Так же довольно остро стоит проблема обновления сигнатурных баз конечных пользователей. Поэтому большое внимание в последние годы уделяется методам выявления аномалий. Сложность данного подхода заключается в трудности составлении профилей нормального и аномального поведения системы, пользователя или процесса, другими словами существует проблема определения того, что считать нормальным, а что аномальным поведением. Поэтому некоторые коммерческие СОВ реализуют ограниченные формы обнаружения аномалий, однако лишь отдельные производители полагаются исключительно на эту технологию.

Одним из возможных решений является метод "объединенных сигнатур", который позволяет уменьшить ошибки первого и второго рода. Главная идея метода состоит в составлении так называемых объединённых сигнатур, которые включают в себя как обычные сигнатуры, характерные для сигнатурных систем, так и признаки аномального поведения. Для проведения исследований использовался метод USAID (United Signature And Anomalous Detection) [1], который позволяет автоматически строить объединённые сигнатуры.

Поскольку обучающие множества не могут содержать все значения характеристик анализируемых параметров, метод USAID при формировании обобщенной сигнатуры использует принцип обобщения диапазонов для каждого параметра, когда интервалы значений разбиваются поровну. Это является существенным недостатком метода, приводящим к увеличению ошибок первого и второго рода. Для устранения этого недостатка предлагается подход к построению обобщенных диапазонов с использованием метода опорных векторов, Метод опорных векторов (SVM, Support Vector Machine) – это набор алгоритмов вида «обучение с учителем», использующихся для задач классификации и регрессионного анализа. Основная идея метода опорных векторов – построение разделяющих гиперплоскостей для значений параметров с максимальным зазором между ними. Две параллельных гиперплоскости строятся по обеим сторонам гиперплоскости, разделяющей классы данных. В этом случае можно считать, что чем больше зазор или расстояние между этими параллельными гиперплоскостями, тем меньше будет средняя ошибка классификатора. В предлагаемом подходе обобщение границ значений параметров для построения обобщенных сигнатур производится на основании расстояния до определенной методом опорных векторов гиперплоскости.

Для формирования обучающего множества были разработаны программные модули, формирующие данные для обучения в виде базы данных, а так же в виде текстовых файлов. В качестве атрибутов (входных векторов для SVM) используются поля из каждого из наиболее распространенных протоколов, вкладываемых в IP пакет - TCP, UDP и ICMP.

Для снижения размерности предлагается использовать метод "перекрестную проверку". Перекрестная проверка (Cross-validation) - метод формирования обучающего и тестового множеств для обучения аналитической модели в условиях недостаточности исходных данных или неравномерного представления классов. В основе метода лежит разделение исходного множества данных на k примерно равных блоков. Затем на $k-1$ блоках производится обучение модели, а k -й блок используется для тестирования. Эта процедура повторяется k раз, при этом на каждом проходе для проверки выбирается новый блок, а обучение производится на оставшихся. На практике, чаще всего выбирается $k=10$ (10-проходная перекрестная проверка), когда модель обучается на 9/10 данных и тестируется на 1/10. Исследования показали, что в этом случае получается наиболее достоверная оценка выходной ошибки модели. Эксперименты по обучению проводились с использованием бесплатных и общедоступных библиотек и программ, таких как libSVM и WEKA. В настоящее время идет этап накопления экспериментальных данных

Потравнов А.В., Черемушкин Д.В.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

информационных технологий, механики и оптики

**ФУНКЦИОНАЛЬНОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ СОГЛАСНО
СТАНДАРТУ ISO/IEC 27005:2008**

Ключевым элементом систем управления информационной безопасностью (СУИБ) в соответствии с международным стандартом ISO/IEC 27001:2005 является система процессов управления рисками информационной безопасности. Для наиболее эффективного внедрения этой системы процессов на практике предлагается описать ее с помощью полужформальных моделей, то есть в наглядном и систематизированном виде представить иерархию подпроцессов, исходные данные и результат выполнения каждого из них, а также средства осуществления подпроцессов и регулирующие их правила. Объектом исследования в работе является методология управления рисками, закрепленная в международном стандарте ISO/IEC 27005:2008. Этот стандарт был принят в 2008 году, относится к семейству стандартов по системам управления информационной безопасностью ISO/IEC 27000 и регламентирует деятельность по анализу, обработке и мониторингу рисков информационной безопасности.

Поскольку управление рисками представляет собой не структуру статичных сущностей, а деятельность, то целесообразно использовать процессно-ориентированную методику моделирования. В результате сравнительного анализа методик IDEF0, DFD, WFD (IDEF3) и BPMN, выбор был остановлен на DFD. Факторами, обусловившими выбор данной методики, явились: простотой для понимания синтаксис, широкая область и эффективность применения на практике, ориентированность на потребности как менеджеров и руководителей организации, так и исполнителей, наличие средств языка, позволяющих уменьшить сложность диаграмм низкого уровня, доступность, наличие инструментальных средств, доступных непрофессиональному (в области моделирования) пользователю.

Базовые свойства разрабатываемой модели приведены ниже:

- Цель моделирования – полужформальное описание методологии управления рисками, содержащейся в стандарте ISO/IEC 27005:2008, с использованием функциональных моделей.

- Точка зрения моделирования – системный аналитик.

- Границы моделирования – процессы и ресурсы, определенные в стандарте ISO/IEC 27005:2008.

- Глубина моделирования – детализация деятельности по управлению рисками до процессов второго уровня.

Полученная модель планируется к использованию для решения следующих задач: анализ, коррекция и гармонизация международных и национальных стандартов информационной безопасности (ИБ), применение в качестве шаблона при планировании и внедрении процесса управления рисками ИБ в конкретной организации, обучение и повышение квалификации специалистов в области ИБ, как основа для разработки инструментальных средств поддержки стандартов ИБ. Необходимо отметить, что закрепленный в стандарте ISO/IEC 27005:2008 подход к управлению рисками в первом приближении имеет общий характер и может быть применим не только к рискам информационной безопасности, что расширяет сферу применения модели.

Романова К.Н., Бабкова М.И., Привалов А.А.

Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»

МОДЕЛЬ ПРОЦЕССОВ РЕАЛИЗАЦИИ ПРОГРАММНО-АППАРАТНЫХ ВОЗДЕЙСТВИЙ

Автоматизированная система управления телекоммуникационными сетями (АСУ ТКС) специального назначения, являясь важным элементом телекоммуникационной сети, влияющим на работу сети в целом, наиболее подвержена программно-аппаратным воздействиям со стороны противника. Поэтому АСУ рассматривается нарушителем как объект первоначального поражения и подвергается активным программно-аппаратным воздействиям.

Предлагается подход к моделированию процессов реализации нарушителем программно-аппаратных воздействий на АСУ ТКС специального назначения, основанный на использовании метода анализа иерархий и метода топологического преобразования стохастических сетей. В результате моделирования синтезируется множество реализаций программно-аппаратных воздействий с подробным описанием действий нарушителя. Каждое программно-аппаратное воздействие характеризуется:

- временем реализации;
- функцией распределения;
- вероятностью выбора воздействия.

Результаты моделирования процессов реализации воздействий применяются в модели программно-аппаратных воздействий на АСУ ТКС, основанной на представлении процессов ведения

технической разведки, выбора и реализации наиболее эффективных программно-аппаратных воздействий в виде смешанной стохастической сети.

Полученные модели процессов реализации программно-аппаратных воздействий применимы для анализа и оценки влияния воздействия на эффективность функционирования современных систем управления телекоммуникационными сетями специального назначения, могут быть использованы в качестве исходных данных для предъявления требований к защищенности АСУ ТКС.

Русских Я.Ю.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

информационных технологий, механики и оптики

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ ИНТЕРНЕТ-БАНКИНГА В РОССИИ

Интернет-банкинг зародился в США в середине 1990х годов из-за необходимости дистанционного банковского обслуживания. В Россию пришел в конце 1990х годов. Сначала специализировался на предоставлении услуг юридическим лицам. Но в настоящее время спектр банковских онлайн-сервисов стремительно расширяется. Если в США количество пользователей услуг интернет-банкинга в год увеличивается на 6–10%, то в России этот показатель не ниже 40% в год. Уже сейчас пользователей Интернета в России более 30 млн и, по данным маркетинговых исследований, каждый третий из них готов воспользоваться услугами интернет-банкинга. Перспективы и привлекательность рынка интернет-банкинга очевидны.

Существуют следующие методы обеспечения безопасности интернет-банкинга:

1. Защищенное соединение с Интернетом. HTTPS-соединение с Интернетом – действенная мера защиты при работе с системой интерактивного банковского обслуживания, если компьютеры клиентов дополнительно оснащены системами антивирусной и антихакерской защиты. Не требует от клиента получения специального цифрового сертификата и установки дополнительного клиентского ПО на свою машину; для интерактивной работы достаточно обычного современного браузера. HTTPS, по сути, обычный http протокол, но работающий через механизмы SSL (Secure Sockets Layer) или TLS (Transport Layer Security), используемые для шифрования транзакций.

2. Таблица кодов/токены. Однако главная угроза исходит от программ перехвата нажатий клавиш клавиатуры (keyloggers), с помощью которых злоумышленник может узнать Web-адрес банка и логин/пароль для доступа к нему. Для повышения степени защиты банки предлагают применять систему дополнительных паролей доступа, генерация которых не связана с использованием ПК.

3. Таблица дополнительных кодов. Это обычная пластиковая карта стандартных размеров, на которой записаны разовые пароли, спрятанные под защитным слоем. При обращении в банк клиент получает в свое распоряжение этот уникальный набор паролей, и в дальнейшем банк может проверять по ним достоверность проводимых через Интернет транзакций – выполняет ли их непосредственный владелец карты кодов (клиент банка) или мошенник.

4. Использование токенов, внутри которых находится шифровальная машина (DES или TripleDES), отвечающая за генерацию паролей и сигнатур. Процедура аутентификации при использовании токена выглядит следующим образом. При попытке зайти на защищенный ресурс пользователю предлагается ввести свой идентификационный номер (login) и пароль, состоящий из PIN-кода и числа, которое показано на токене. Для его получения надо ввести на брелоке тот же PIN-код, и токен выдает свою часть пароля, используя таймер времени и стартовый вектор генерации (seed), аппаратно «прошитый» на стадии производства брелока. Данные отсылаются на сервер аутентификации, где хранятся PIN-коды зарегистрированных пользователей, а также стартовые векторы генерации токенов. Зная текущее значение времени, сервер восстанавливает полученный пользователем токен-код и сам пароль.

Поскольку в России интернет-банкинг находится на стадии развития, это направление является перспективным и интересным для изучения и перспективным разработки и внедрения новых технологий безопасности.

Савчук М. Н., Фесенко А. В., Заболотный А.П.

Украина, Киев, Институт кибернетики им. В.М. Глушкова НАН Украины,

Национальный технический университет Украины «КПИ»,

Россия, Санкт-Петербург, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

АНАЛИЗ ИСПОЛЬЗОВАНИЯ КОММУТАТИВНЫХ ШИФРОВ В КВАНТОВОЙ МОДЕЛИ ВЫЧИСЛЕНИЙ

Квантовая модель вычислений позволяет получить новые алгоритмы решения ряда задач с существенно улучшенными оценками для их сложности по сравнению со сложностью решения в классической модели вычислений на компьютере традиционной архитектуры. В частности, уже известны случаи, когда улучшение носит качественный характер и удалось найти полиномиальный алгоритм решения, хотя даже по истечении многих лет анализа в классической модели так и не получен подобный результат. Примерами таких задач являются задачи факторизации и дискретного логарифмирования, на

сложности решения которых основаны стойкость и надежность большинства схем асимметричной криптографии. Полиномиальный в квантовой модели вычислений алгоритм Шора позволяет быстро получить решения этих задач. Однако в квантовой модели вычислений все же остаются трудно решаемые задачи. Например, поиск по неупорядоченному списку длины N улучшается всего лишь от $O(N)$ в классической модели до $O(N^k)$, где $k=1/2$. Также большинство специалистов сходятся во мнении, что достаточно стойкие симметричные шифры останутся стойкими и в квантовой модели вычислений.

В настоящем сообщении предлагается построение криптографических схем, основанных на коммутативных или локально-коммутативных (коммутативность выполняется только на некотором подмножестве сообщений) симметричных шифрах, а также проводится анализ стойкости полученных схем в квантовой модели вычислений. Свойство коммутативности симметричного шифра, а также его стойкость к атакам на основе открытого текста позволяют использовать его для построения асимметричных схем. В частности, с использованием коммутативных и локально-коммутативных шифров построены схемы Месси-Омуры, схема направленной подписи, система шифрования Эль-Гамала, схемы групповой и слепой подписей. Предлагаемый подход позволяет строить аналоги для многих других криптографических протоколов.

Проведенные исследования новых схем в квантовой модели вычислений показали, что задача эффективного криптоанализа в подобных схемах сводится к частному случаю задачи о скрытой подгруппе – задачи о восстановлении образующих элементов подгруппы по отображению, которое принимает одинаковые значения на всех левых классах смежности относительно этой подгруппы. Искомая скрытая подгруппа в данном случае принадлежит конечной абелевой группе. Как известно из работ Китаева и Шора, для этого случая существует эффективный алгоритм решения в квантовой модели вычислений. Таким образом, требование коммутативности или локальной коммутативности от симметричного шифра является слишком сильным для построения асимметричных схем стойких в постквантовой криптографии, и требует замены на другие свойства шифра, которые предоставили бы возможность построить стойкие в квантовой модели вычислений асимметричные протоколы. Вопрос о поиске необходимых свойств симметричного шифра остается открытым для исследований.

Садченко К.И., Мироненко М.К.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
информационных технологий, механики и оптики
О ПРОТИВОДЕЙСТВИИ РАЗВИТИЮ БОТНЕТОВ**

Сегодня, как показывает статистика, значительную долю кибер-преступлений занимают преступления с использованием ботнетов.

«Ботнет» или «зомби-сеть» — это сеть компьютеров, зараженных вредоносной программой, позволяющей злоумышленникам удаленно управлять зараженными машинами без ведома пользователей. С помощью этих сетей можно рассылать спам, производить DDoS атаки на сервера, использовать вычислительные мощности зараженных компьютеров, красть информации, устанавливать софт, накручивать клики в сервисах контекстной рекламы. И все это – без ведома владельца компьютеров.

Почему существует такая проблема? Большинство зараженных машин являются домашними компьютерами. Мало кто при работе на домашнем ПК задумывается о его безопасности. И ущерб нанесенный пользователю рядового ПК зомби сети может быть не соизмерим с ущербом, нанесенным нормальному функционированию этой сети. Выходит, что проблема не лежит на плечах пользователей.

Существует два решения проблемы. Это противостояние заражению вредоносной программой на уровне отдельного пользователя потенциальной зомби-машины и предотвращение, парирование угроз путем разработки нормативных правил и методик эксплуатации компьютерной сети, что, вероятно, потребует совершенствования нормативно-правовой базы.

Противостояние со стороны отдельного пользователя заключается в использовании им программного обеспечения, обеспечивающего безопасность его ПК, и сегодня остается в границах его компетентности и на его совести. Не обсуждая необходимость совершенствования нормативной базы противодействия кибер-преступлениям, полагаем, что наиболее действенным методом сегодня будет профилактическая работа с пользователями сети, привитие им навыков обеспечения безопасности и чувства корпоративной ответственности за последствия его действий, а также расширение рынка и доступности конечному пользователю средств обеспечения безопасности.

Суконщиков А.А., Яковлев С.А.

**Россия, Вологда, Вологодский государственный технический университет,
Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
СИТУАЦИОННОЕ МОДЕЛИРОВАНИЕ ДЛЯ ИССЛЕДОВАНИЯ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ**

Развитие современных инфокоммуникационных систем (ИКС) характеризуется внедрением новых технологий передачи данных, среди которых особое место занимают системы с поддержкой качества обслуживания (ПКО), включая оценку информационной безопасности (ИБ).. Системы ПКО

позволяют обеспечивать обслуживание таких потоков информации, как IP-телефония, видеоконференции, мультимедийные потоки и т.д., которые становятся все более популярными в информационной деятельности различных типов организаций.

Возрастающие сложности по управлению ИКС требуют от лиц, принимающих решение, кроме знаний в области управления сложными корпоративными сетями, еще знаний о характеристиках качества обслуживания, режимов обслуживания, типов информационных потоков, требуемых ресурсов, алгоритмов обслуживания очередями и т.д., что сказывается на скорости и правильности принятия решения. К тому же корпоративные ИКС, с одной стороны, должны обеспечивать согласование принимаемых решений в иерархической структуре, а с другой стороны, должны быть системами интегрированными, обеспечивающими выполнение совместных функций и достижение общих целей.

В качестве метода решения задачи правильного выбора стратегии управления ИКС для обеспечения требуемого уровня ИБ предлагается метод ситуационного имитационного моделирования, на основе многоагентной модели. Система ситуационного моделирования (ССМ) состоит из следующих подсистем: имитационного моделирования, событийного моделирования, ситуационного моделирования, продукционных правил для оценки ситуаций и выработки управляющих действий, баз данных для хранения результатов моделирования, подсистема баз знаний для хранения и модификации знаний, информационного обмена, прогнозирования.

Разработанная структура ССМ состоит минимум из 8 различных по формализации, языкам, принципам, математическому описанию подсистем. Поэтому одной из главных задач является разработка математического аппарата, который бы охватывал все этапы анализа, проектирования и реализации ССМ и использовался во всех подсистемах. Исходя из анализа математических методов, можно сделать вывод, что наиболее подходящим математическим аппаратом является аппарат сетей Петри, в который можно трансформировать такие средства как системы, построенные на нечеткой логике, нейронные сети, нечеткие продукционные системы. На базе расширений сетей Петри можно провести моделирование как на структурном уровне модели СИАМ, так и на событийном и ситуационном уровне.

Титов И.Е.

Российская Федерация, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

КОНКУРЕНТНАЯ РАЗВЕДКА В УСЛОВИЯХ ФИНАНСОВОГО КРИЗИСА

Одной из основных форм добросовестного противостояния в промышленном масштабе по праву является конкурентная разведка, основательно закрепившаяся во всех областях современной экономики.

Цель ее – своевременное выявление и нейтрализация угроз экономическому благополучию компании, информационно-аналитическая поддержка принятия оптимальных управленческих решений, обеспечивающих достижение конкурентного превосходства над другими участниками рынка. К тому же, в условиях мирового финансового кризиса средств на научно-исследовательскую работу и масштабную модернизацию производства на предприятиях явно не хватает, что напрямую способствует обострению конкурентного противостояния.

Это вполне справедливо и в отношении межгосударственной борьбы, где к вопросам экономической конкурентоспособности добавляются и вопросы национальной безопасности. Но в этих условиях большее применение получило такое явление, как промышленный шпионаж. Хотя при этом предприятие не имеет полномочий государственных разведок и, поэтому в случае провала операции промышленного шпионажа, рискует быть привлеченным к уголовной и административной ответственности, а также может значительно пострадать репутация компании.

По аналогии с разведслужбами государств в области сбора информации, только в более скромных масштабах, действуют практически все корпорации, так как это является неременным условием их выживания в мире с жесткой конкурентной борьбой.

Мировой финансовый кризис повлиял не только на уровень доверия между банками и компаниями, но и на увеличения влияния внешней среды. За счет новых условий промышленного выживания активизируются крупные федеральные и иностранные игроки, снижается доля местных предприятий на основных рынках, усиливается госрегулирование в экономике, в том числе и в пользу отдельных компаний.

Объективная ограниченность сил и средств, выделяемых владельцами и менеджментом из бюджета предприятия на решение задач конкурентной разведки, вынуждает отделы безопасности акцентировать свое внимание и на положении дел внутри компании. Современные средства и технологии обработки разведывательной информации позволяют оценивать динамику лояльности персонала, выявлять центры напряженности. Анализ информации от внутренних источников и клиентов помогает службам безопасности выявлять факты утечки конфиденциальной информации и неправомерной деятельности персонала против компании.

В силу существенного роста неопределенности будущего мировой экономики, нарушения стабильности, многократно помноженные угрозы и риски напрямую воздействуют на цену ошибочного решения, поскольку запас прочности хозяйствующего субъекта в кризис естественно снижается.

Безусловно, в нынешнем положении предприятиям давно уже было необходимо включить в антикризисные планы меры повышения экономической безопасности. Большинство из них – часть конкурентной разведки: более тщательная проверка партнеров и клиентов, оценка деловой активности конкурентов, мониторинг быстрых изменений на рынке. Эти действия частично позволяют компенсировать возросшие риски.

Чистяков И.В., Орлов Д.Р.

**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»
КРИПТОГРАФИЧЕСКАЯ ФАЙЛОВАЯ СИСТЕМА С ИЕРАРХИЧЕСКИМ РАЗГРАНИЧЕНИЕМ
ДОСТУПА**

В современных корпоративных информационных системах с целью экономии затрат на хранение все возрастающих объемов данных начинает широко внедряться практика использования услуг внешних организаций для хранения информации. В этих условиях безопасность корпоративной информации (конфиденциальность и целостность) могут быть обеспечены только с использованием криптографических механизмов. С другой стороны необходимость совместного использования сотрудниками корпоративных информационных ресурсов требует учета того факта, что значительное число организационных систем имеет иерархическую структуру. Применительно к проблеме доступа к информационным ресурсам это означает, что множество субъектов разбивается на непересекающиеся классы безопасности, отличающиеся полномочиями по доступу к ресурсам, причем пользователи старших классов должны иметь возможность доступа к информационным ресурсам всех своих подчиненных. При использовании криптографических методов каждому классу безопасности назначается свой ключ, обеспечивающий возможность доступа к защищенным файлам данного класса для шифрования файлов. Таким образом, доступ к ключу означает получение доступа к информации. Поэтому основой криптографического разграничения доступа в иерархических системах является схема назначения и вывода ключей классов безопасности субъектов.

Проблема разграничения доступа в иерархических системах в настоящее время активно обсуждается в современной научной литературе. Однако вопросам практической реализации, использующей эти теоретические разработки, уделяется существенно меньше внимания.

В докладе рассматривается криптографическая файловая система с иерархическим разграничением доступа, имеющая следующие особенности:

- использование криптографических протоколов на базе стандартов РФ, учитывающих особенности, связанные с их применением при хранении информации;
- использование современных итеративных алгоритмов управления криптографическими ключами для иерархических структур общего вида, а не только типа дерево, минимизирующих объем хранимых секретных ключей и трудоемкость их смены;
- информационный ресурс, сопоставленный каждому классу безопасности субъектов, имеет структуру <папка – файл – запись>;
- каждый файл при создании получает статус Конфиденциальная информация или Открытая информация;
- для конфиденциальной информации реализуется шифрование и контроль целостности, а для открытой информации – только контроль целостности.

Для реализации криптографической файловой системы с иерархическим доступом использована свободно распространяемая библиотека FUSE for Linux, обеспечивающая «прозрачность» функций защиты для существующих файловых систем и средства работы с метаданными.

Проведена оценка объема метаданных, необходимых для обеспечения предлагаемой системы криптографической защиты, и дополнительных накладных расходов.

Реализован прототип криптографической файловой системы с иерархическим доступом для ОС Linux.

Шишкин В.М.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПРОБЛЕМЫ ЭКСПЕРТИЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ**

Не вдаваясь в детали, содержание любой экспертизы безопасности ИС состоит в выявлении и идентификации (априори или в режиме реального времени) факторов и событий риска нарушения ИБ, их оценке и выработке упреждающих, проактивных, или реактивных противодействующих мер. Экспертизой можно назвать и проверку соответствия системы нормативным требованиям. Под этим термином приходится понимать очень разнообразные по назначению, целям, методическому и инструментальному обеспечению подходы, и здесь он использовано в собирательном смысле, чтобы обсудить многообразие подходов в совокупности и взаимоотношении. Объективно вся эта многообразная деятельность должна способствовать повышению уровня безопасности ИС или, точнее, уровня доверия к ним. Основная проблема состоит в том, что само понятие безопасности, а тем более доверия, неизбежно имеет субъективную природу.

Не претендуя на полноту классификации, выделим следующие направления, относящиеся к экспертизе безопасности ИС, с условными названиями: выявление уязвимостей; анализ состояния; обнаружение аномального поведения. Каждое из них представляет огромное предметное и методическое разнообразие и может быть объектом специального рассмотрения.

Задачи поиска уязвимостей с точки зрения технического содержания разнообразны, самодостаточны и даже изолированы, находятся в компетенции специалистов совершенно разного профиля. По отдельности их решение никак не может существенно повлиять на безопасность.

Разнообразие, но другого рода, наблюдается и в следующем направлении. С одной стороны это специализированные средства, предназначенные для анализа защищённости ИС от некоторых классов угроз, с другой – системы комплексного анализа и аудита, часто называемые системами анализа рисков. И те, и другие, как правило, в своей основе содержат структурную модель факторов риска, на которой, используя тот или иной математический аппарат, делается качественный или количественный вывод о значимости этих факторов для выработки указаний для дальнейших действий, повышающих уровень безопасности объекта. Специализированные модели по определению решают локальные задачи, но с точки зрения потенциального качества вывода имеют преимущество, поскольку оперируют с количественно ограниченным и относительно однородным множеством факторов. При комплексном анализе приходится иметь дело с очень сложными структурами, либо, упрощая их, жертвовать качеством оценок.

Выгодно отличаются от рассмотренных представители третьего направления экспертизы безопасности. Они применяются в режиме реального времени, дают видимый результат и поэтому с практической точки зрения, пожалуй, наиболее эффективны и вызывают наибольшее доверие. Однако та же практика показывает, что, несмотря на повсеместное использование таких систем в настоящее время, не заметно снижения успешности атак. Кроме того они по сути своей реактивны, даже если способны реагировать на неизвестные аномалии. Так что в отличие от эффективности при всей полезности их эффективность вопрос дискуссионный.

Таким образом, ни один из рассмотренных подходов к экспертизе по отдельности не может обеспечить необходимого доверия к безопасности ИС, и лишь при взаимосвязанном их применении возможно наилучшим образом анализировать ситуацию и противодействовать рискам. Основная проблема взаимодействия методов – разномасштабность представления объектов и процессов во времени и пространстве, её преодоление необходимо и возможно.

Шустиков С. В.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

ОСНОВНЫЕ ПРОБЛЕМЫ СООТВЕТСТВИЯ РЕГУЛИРУЮЩИМ ТРЕБОВАНИЯМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В связи с возрастающим количеством регулирующих требований, предъявляемых к обеспечению информационной безопасности, на практике остро встаёт вопрос управления соответствием.

В качестве примера возьмем организацию, обрабатывающую данные о платежных картах. Ею может быть банк, центр обработки данных, торгово-сервисное предприятие, предприятие электронной коммерции, количество которых непрерывно возрастает. Пример такой организации показателен, поскольку на неё распространяется ряд обязательных к исполнению нормативных документов – PCI DSS, ФЗ–152, а в случае кредитной организации – стандарт СТО БР ИББС–1.0–2008, носящий рекомендательный характер с прогнозом превращения в обязательный.

При выполнении работ по аудиту информационной безопасности, а также при оказании услуг по приведению информационной инфраструктуры организации в соответствие требованиям стандарта PCIDSS были выявлены типовые проблемы, затрудняющие достижение соответствия. Среди них следует отметить такие проблемы, как:

- проблема понимания;
- проблема отношения;
- проблема подхода;
- проблема ресурсов;
- проблема управления.

В докладе рассмотрены способы решения указанных проблем. Необходимо с одной стороны сломать устойчивые стереотипы и изменить взгляды на информационную безопасность, а с другой – разработать применимые на практике к организациям среднего и малого бизнеса методы управления информационной безопасности. То есть необходимо создать систему менеджмента информационной безопасности, адекватную размерам бизнеса и способную обеспечить практическую применимость средств снижения информационных рисков.

Щиголева М.А.

Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

РАЦИОНАЛЬНАЯ ТАКТИКА ЗАЩИТЫ ДИАГНОСТИЧЕСКИХ ДАННЫХ ПРИ ФОРМИРОВАНИИ ПРОГРАММЫ ОЗДОРОВЛЕНИЯ НАСЕЛЕНИЯ

Большая часть пациентов считает нужным сакраментировать состояние своего здоровья и причины его ухудшения. Пациенты не готовы предоставить эти сведения в качестве исходных данных для компьютерной обработки без гарантии сохранения их конфиденциальности.

Объяснение технологии обеспечения информационной безопасности личных данных в совокупности с обезличенными алгоритмами обработки при составлении карты здоровья пациента снимает внутреннее напряжение на этапе диагностики и в ходе реализации программы оздоровления. Происходит трансформация культа секретности в сторону формирования информационной культуры современного отношения к потреблению продуктов компьютерных технологий. При составлении и анализе анамнеза обрабатывается обезличенная информация по логико-процедурным траншам составления этиологии и нозологии заболеваний. Методологические формы диагностики и профилактики, оздоровления и реабилитации, экспертизы и прогноза состояния пациента используют параметрическую матрицу физиологических данных без персонификации пациентов. Внесение рациональной закрытости позволяет перейти к рационализации оздоровления, обработки форм диагностики, снизить неполноту и нечеткость исходных сведений, устранить психо-эмоциональные искажения диагностики, сгладить разбросы целевой функции общего оздоровления при наличии многофункциональных нарушений.

За пределами диагностических и лечебных мероприятий при выборе форм и графиков процедур оздоровления степень конфиденциальности смягчается и обработка плана групповых и поточных мероприятиях оздоровления ведется на базе взаимоувязанных психо-физиологических, медико-биологических и социальных факторов, подвергнутых совокупной компьютерной обработке.

Степень конфиденциальности персональных сведений маркируется при формировании пространства признаков в диагностическом процессе с простановкой метки ограничения доступа в классификации признаков для матриц значимых параметров обработки. Подход к разметке информационных признаков по степени конфиденциальности позволяет осуществить формирование пространства и процедур обработки информационно-ценных признаков.



СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Алексеев А.В.

Россия, Санкт-Петербург, ОАО «Научно-инженерный центр Санкт-Петербургского электротехнического университета»

РЕЙТИНГ-АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОСНОВНЫХ КЛАССОВ

Одной из ключевых задач создания высокоэффективных автоматизированных систем в защищённом исполнении (АСЗИ) сегодня является сравнительный количественный анализ качества и обоснованный выбор представленных на современном IS-рынке технических средств защиты информации (ТСЗИ), их комплексов и систем.

Отсутствие сопоставимых и достоверных исходных данных сравнения, а также методическая сложность выполнения квалиметрических многокритериальных оценок для современных многофункциональных организационно-технических комплексов превращает эту задачу в одну из весьма сложных и практически нерешённых проблем развития АСЗИ.

Одним из возможных и перспективных направлений решения этой проблемы, в том числе для объектов морской инфраструктуры, сложных корабельных и береговых автоматизированных комплексов и систем, является проведение рейтинг-анализа средств по технологии полимодельной квалиметрической ранговой оптимизации проектных и управленческих решений (технологии КРОПУР).

Последняя прошла успешную апробацию в целом комплексе исследований, посвящённых сравнительному количественному анализу качества (рейтинг-анализу) ТСЗИ, включённых в Государственный реестр сертифицированных ТСЗИ, перечень БИЗКТ. Результаты анализа использованы при реализации ряда IS-проектов компаниями-интеграторами.

В рамках настоящих исследований с целью формирования базы данных квалиметрического сравнения и мониторинга качества ТСЗИ были обобщены результаты многовариантных оценок и рейтинг-анализа основных классов современных сертифицированных средств, включая: средства разграничения доступа; средства межсетевого экранирования; VPN-средства; средства сканирования и анализа информационной безопасности; средства мониторинга-управления информационной безопасностью; средства защиты от вредоносных кодов (антиспамовые, антивирусные); средства криптографической защиты; операционные системы в защищённом исполнении; программно-аппаратные комплексы и системы в защищённом исполнении; системы электронной цифровой подписи и другие.

При проведении исследований особое внимание уделялось систематизации критериев и показателей эффективности использования каждого из классов ТСЗИ, моделированию для различных вариантов их использования наиболее характерных (типовых) вариантов отношений предпочтений заказчиков с соответствующим определением матрицы индексов. Полимодельность задания исходных данных по отношению предпочтений подтвердила возможность при рейтинг-анализе альтернативных решений получения «устойчивой картины» формирования обоснованных проектных и управленческих решений (ПУР).

Результаты испытаний и исследований показали, прежде всего, реальную возможность и актуальность оптимизации структуры, ПУР и системных параметров комплексного использования ТСЗИ, необходимость и возможность получения квалиметрически состоятельных оценок за счёт повышения точности задания исходных данных путём проведения сравнительных тестовых испытаний, в том числе на базе универсальных информационно-моделирующих стендов и комплексов (УИМК).

Ананьев М.Ю., Баженов А. А., Галанов А.И., Щербаков В.А.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций, Санкт-Петербургский институт информатики и автоматизации РАН, Молдова, Кишинев, Институт математики и информатики АН Республики Молдова
СТАНДАРТЫ И ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЦИФРОВОЙ ПОДПИСИ

Ряд задач практической информатики находят удобное решение путем применения протоколов коллективной электронной цифровой подписи (ЭЦП). К таким задачам могут быть отнесены проблемы одновременного подписания контракта и делегирования права подписи. При этом схемы коллективной ЭЦП (КЭЦП) дают решение некоторых проблем в расширенной формулировке. Например, они обеспечивают решение проблемы одновременного подписания пакета контрактов, причем предполагается, что в общем случае различные контракты подписываются различными

подмножествами пользователей. Достоинством решения последней проблемы путем применения протокола КЭЦП является то, что размер коллективной подписи равен размеру индивидуальной подписи и не зависит от числа подписанных контрактов и общего количества подписывающих. Такие протоколы коллективной подписи строятся на основе рандомизированных алгоритмов ЭЦП, использующих трудность дискретного логарифмирования или трудность извлечения корней по простому модулю со специальной структурой. При этом при формировании КЭЦП каждый участник протокола формирует свою долю в общей подписи, после чего вычисляется свертка от всех индивидуальных долей, которая и представляет собой значение КЭЦП. Таким образом, в процессе вычисления КЭЦП все подписывающие участвуют в протоколе одновременно.

Построены протоколы слепой коллективной подписи и схемы КЭЦП, взлом которых требует одновременного решения двух трудных задач различного типа. Большой интерес для практического использования представляют протоколы КЭЦП, основанные на стандартах ЭЦП. В связи с этим представляет интерес изучение возможности реализации протоколов КЭЦП, основанных на процедурах генерации и проверки подлинности подписи, предписываемых официальными стандартами.

В данной работе были изучены стандарты различных стран и установлено, что стандарты России (ЭЦП ГОСТ Р 34.10–94 и ГОСТ Р 34.10–2001), Украины (ДСТУ 4145–2002) и Беларуси (СТБ 1176.2–99) позволяют реализовать рассматриваемые протоколы КЭЦП, основанные на свертке индивидуальных параметров, вычисляемых отдельными пользователями в параллельной процедуре генерации конечного значения КЭЦП. Анализ американских стандартов цифровой подписи DSA и ECDSA показал, что они не могут быть применены без внесения изменений в выражения для генерации и верификации ЭЦП. Уравнение проверки КЭЦП совпадает с уравнением проверки ЭЦП, задаваемом базовым алгоритмом, исключая то, что вместо индивидуального открытого ключа в базовом алгоритме в протоколе КЭЦП используется коллективный ключ, вычисляемый как свертка индивидуальных открытых ключей. Обсуждаются области применения протоколов КЭЦП и факторы благоприятствующие быстрому их внедрению в практику.

Данная работа поддержана грантом РФФИ № 08–07–00096–а и грантом АН Молдовы № 08.820.08.08 РФ.

Ананьев М.Ю., Доронин С.Е., Мирин А.Ю., Морозова Е.В.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций, Санкт-Петербургский институт информатики и автоматизации РАН
ВАРИАНТ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ БУМАЖНЫХ ДОКУМЕНТОВ ОТ ПОДДЕЛКИ**

В настоящее время возрастает роль электронных документов во всех сферах общественной деятельности, включая информационные технологии, связанные с оборотом юридически значимых электронных сообщений и документов. Однако в человеческом обществе продолжают иметь хождение и бумажные документы – паспорта, удостоверения, аттестаты, дипломы, ценные бумаги, сертификаты и т.п. Современные типографские технологии значительно повысили уровень защищенности таких документов от подделки, однако возросли и возможности фальсификаторов, позволяющие им подделывать документы с более высоким уровнем защищенности. Это делает актуальным поиск новых механизмов защиты от подделки, позволяющих обеспечить защиту от подделки на новом уровне. В качестве такого механизма недавно была предложена технология криптографической защиты материальных объектов от подделки, в которой для проверки подлинности используется уникальность микроструктура материального объекта. Эта технология применима для защиты бумажных документов. Ее суть состоит в формировании 1) эталонного цифрового образа (ЭЦО) бумаги, на которой изготавливается документ, 2) первой машиночитаемой метки, содержащей ЭЦО и содержательную информацию документа, 3) цифровой подписи, вносимой в документ в виде второй метки.

В данной работе решается задача повышения защищенности документов от несанкционированного выпуска путем использования коллективной цифровой подписи, формируемой несколькими удостоверяющими органами.

Предложен вариант структурно-функциональной схемы построения архитектуры автоматизированной системы поддержания технологии криптографической защиты бумажных документов от подделки, основанный на использовании коллективной цифровой подписи и имеющихся в современном обществе компонентов информационных и телекоммуникационных технологий. В качестве коммуникационной среды предполагается использовать Интернет, для распространения открытых ключей, необходимых для проверки подлинности документов – имеющуюся в современном обществе развитую инфраструктуру открытых ключей. Для хранения эталонных образов выпущенных бумажных документов предлагается создать централизованную базу данных. Рассматриваются ошибки процедуры проверки подлинности двух типов 1) принятие подлинного документа за фальсифицированный и 2) принятие фальсифицированного документа за подлинный. Показано, что вероятность ошибок первого вида значительно превышает вероятность ошибок второго типа. Обсуждаются варианты резкого снижения вероятности ошибок первого типа за

счет внесения новых технологических элементов в изготовление бумаги. В качестве другого способа предполагается нанесение специальных меток, обладающих физико-химической стойкостью и создающих при их сканировании невоспроизводимые случайные цифровые образы.

Данная работа поддержана грантом РФФИ № 08–07–00096–а.

Артамонов А.В., Маховенко Е.Б.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ПРОТОКОЛЫ ГРУППОВОЙ ПОДПИСИ В СИСТЕМЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
НА БАЗЕ ПЛАТФОРМЫ DOCUMENTUM**

Отправной точкой теоретического и практического развития протоколов групповой подписи стала статья Чома и ван Хейста в 1991 году (D. Chaum and E. van Heyst (1991). "Group signatures". *Advances in Cryptology — EUROCRYPT '91*, vol. 547 of *Lecture Notes in Computer Science*: 257–265).

С тех пор теме групповой подписи было посвящено множество статей и выявлен ряд практических областей применения. Одной из таких областей являются системы электронного документооборота (СЭД).

Применительно к СЭД, протоколы групповой подписи позволяют эффективно решить следующие задачи, решение которых посредством обычных протоколов электронно-цифровой подписи (ЭЦП) является не оптимальным или не возможным:

- формирование ЭЦП анонимно от имени отдела (для внутренних документов) или компании (для исходящих документов);

- выявление конкретного автора подписи в случае спорной ситуации;

- поддержка динамического изменения состава участников группы, обладающих правом подписи (эта возможность есть в некоторых протоколах групповой подписи) (M. Bellare, H. Shi and C. Zhang. *Foundations of Group Signatures: The Case of Dynamic Groups*. *Topics in Cryptology – CT-RSA 2005 Proceedings*, *Lecture Notes in Computer Science* Vol. 3376, A. Menezes ed, Springer-Verlag, 2005. (<http://www-cse.ucsd.edu/users/mihir/papers/dgs.html>)).

В рамках данной работы разрабатывается архитектура функционального модуля СЭД на базе платформы Documentum, использующего протокол групповой подписи BBS (D. Boneh, X. Boyen, H. Shacham. *Short Group Signatures*. M. Franklin (Ed.): *CRYPTO 2004*, LNCS 3152, pp. 41–55, 2004.). Сама платформа Documentum предполагает построение СЭД по клиент-серверной архитектуре со взаимодействием пользователей с системой посредством браузера.

Архитектура обеспечивает возможность подписи версии произвольного документа (dm_document и производных типов) в любом формате, с произвольным количеством объектов контента. В подпись включаются только основные (rendition=0) объекты контента, то есть, представления (в терминах Documentum) не подписываются.

Функциональный модуль разработан с учётом возможности увеличения в будущем количества различных типов подписей для одного документа, то есть, возможности для одного пользователя подписать документ несколько раз, но не более одного экземпляра подписи каждого типа на документ от одного пользователя системы (из соображений здравого смысла) – например, для многоэтапного согласования с подтверждением визирования.

Функциональный модуль проверяет назначение сертификата, используемого при подписи, при выполнении подписи и при всех проверках валидности.

Обеспечивается подпись атрибутов документа. Набор подписываемых атрибутов определяется на уровне типа документа и наследуется всеми подтипами, если для подтипа не указан собственный набор атрибутов. Настройка атрибутов для подписи выполняется при установке системы и не может быть изменена в дальнейшем без потери валидности всех ранее подписанных документов. Документ может быть подписан одним или несколькими пользователями системы.

В дальнейшем в рамках работы предполагается опытная реализация разработанной архитектуры.

Баженов А.А., Галанов А.И., Костин А.А.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций, Санкт-Петербургский институт информатики и автоматизации РАН
ТЕХНОЛОГИЯ ЗАЩИТЫ БУМАЖНЫХ ДОКУМЕНТОВ ОТ ПОДДЕЛКИ НА ОСНОВЕ ЦИФРОВЫХ
СЕРТИФИКАТОВ**

Несмотря на то, что в настоящее время широко применяется технология электронного документооборота, роль бумажных документов практически во всех сферах общественной деятельности остается чрезвычайно важной. Одной из актуальных проблем связанным с хождением бумажных документов является их подделка. Подделываются паспорта, удостоверения об образовании, аттестаты званий, дипломы ученых степеней, ценные бумаги, сертификаты и т.п. Откликом на проблему защиты бумажных документов явилась новая технология из защиты, основанная на применении современных достижений криптографии. Эта технология известна как

«Технология криптографической защиты материальных объектов от подделки», основанная на уникальности микроструктуры бумаги, с использованием которой изготавливается документ. Однако эта технология требует изготовления массового использования специализированного оборудования, что сдерживает ее широкое применение. В связи с этим является актуальным разработка альтернативных решений в области защиты бумажных документов от подделки.

В данном исследовании разрабатывается способ и система реализующая его, в котором механизмом повышения защищенности бумажных документов от подделки является сопровождение документов цифровыми сертификатами (ЦС). Создание ЦС бумажного документа используется как один из этапов санкционированного выпуска бумажного документа. Проверка подлинности документа включает проверку подлинности ЦС. Сертификаты не являются жестко привязанными к бумажному документу. Могут быть применены следующие три варианта обеспечения доступа к ЦС при проверке подлинности документа: 1) они могут быть представлены в виде машиночитаемой метки на вкладыше к документу, 2) они могут быть представлены в виде файла, хранимого на машинных носителях, 3) они могут быть представлены в виде записи в централизованной базе данных. В последнем случае предполагается получение ЦС через глобальную сеть Интернет. Возможны комбинированные решения, однако предполагается, что во всех случаях следует использовать механизм хранения ЦС в централизованной базе данных.

Сертификат формируется специальным органом, участвующим в выпуске документов. Подлинность ЦС проверяется по открытому ключу этого органа. Распределение подлинных открытых ключей реализуется с помощью имеющейся инфраструктуры открытых ключей, которая в настоящее время достаточно развита в России и других развитых странах. В этой схеме фальсификаторы сталкиваются с проблемой формирования ЦС, которые бы подтверждали изготавливаемые ими фальсифицированные документы. Для этого им потребуется взломать используемый алгоритм ЭЦП, что практически невыполнимо для современных схем цифровой подписи. Таким образом, рассмотренный способ повышения степени защищенности от подделки резко снижает возможности фальсификаторов.

Работа поддержана грантом РФФИ № 08–07–00096–а.

Бакланов Ф.С.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
информационных технологий, механики и оптики
К ВОПРОСУ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В XXI веке у человечества появляется все больше новых объектов, нуждающихся в защите путем закрепления соответствующих норм в законе. Важнейший такой объект на сегодняшний день – это информация. В современном мире к защите конфиденциальных сведений предъявляют все большие требования. Особой ценностью обладает информация, несущая в себе данные о личной, индивидуальной или семейной жизни человека. Ст.2 Конституции Российской Федерации закрепляет основной принцип современного демократического общества: «Человек, его права и свободы являются высшей ценностью». Соответственно и информация, непосредственно затрагивающая частные интересы человека должна уважаться и защищаться государством. Государственная политика должна быть направлена на усиление защиты персональных данных граждан. Усилению должен быть подвержен не только технический аспект этой проблемы, но и юридический. Издание новых федеральных законов, руководящих документов и ГОСТов в области защиты персональных данных способствует уменьшению риска утечки персональных данных граждан из СУБД. Обязательное лицензирование соответствующими органами власти операторов, несущих ответственность за персональные данные, и периодические проверки аттестационными комиссиями объектов, обслуживаемых и защищаемых этими операторами, помогут добиться улучшения качества услуг защиты данных.

Сегодня в нашей стране разглашение коммерческой тайны или промышленный шпионаж не могут иметь настолько тяжких юридических последствий для злоумышленника, как, например, в Европе. Представляется, что ужесточение наказаний будет способствовать более аккуратному и конфиденциальному отношению граждан РФ к «чувствительной» информации. В настоящее время множество коммерческих организаций запрашивают у своих клиентов, подчас, совсем не нужную информацию. Снизить риски граждан и экономически выгодно подойти к решению вопроса о защите персональных данных операторам помогут дополнительные руководящие документы, приводящие перечни сертифицированных технических и программных средств защиты персональных данных.

Идеальным выходом из сложившегося положения, на мой взгляд, было бы создание крупных Центров Обработки Данных (ЦОД) на территории РФ. Такие комплексы могли бы быть построены и, в дальнейшем, обслуживаться на средства коммерческих структур и организаций, чьи базы данных будут храниться на серверах, и иметь класс защищенности в зависимости от хранимой информации. Архитектура терминального доступа, как представляется, позволяет унифицировать защиту и многократно снизить затраты на её обслуживание. Так же стоит систематизировать ЦОД по хранимой на их территории информации. Одни «Банки Данных» будут хранить информацию, например, обо

всех купленных билетов на ж/д и авиа транспорт на территории РФ, другие же – номера страховых полисов. В настоящее время, в нашей стране существует более двух сотен страховых компаний. В каждой из них есть Автоматизированные Системы (АС). Уровень этих АС соответствует классу не ниже 1Г. Данный класс АС подразумевает немалые финансовые затраты на защиту информации. Представляется, что экономически выгодным будет решение установить одну АС вместо двух сотен, но уже классом выше.

Фактически сегодня защита персональных данных в нашей стране только начинает зарождаться. Нормативная база должна совершенствоваться и развиваться. Думается, что Федеральный Закон N 152-ФЗ «О персональных данных», скорее всего, не останется единственным в своём роде. Ведь от сохранности персональных данных каждого гражданина зависит национальная безопасность всего государства.

Баранов Ю.А.

Россия, Москва, Институт проблем информатики РАН

СТАТИСТИЧЕСКИЙ МЕТОД АВТОРУБРИКАЦИИ ТЕКСТОВ ПРИ РЕАЛИЗАЦИИ МЕХАНИЗМА ТЕМАТИЧЕСКОГО РАЗГРАНИЧЕНИЯ ДОСТУПА К ТЕКСТОВЫМ ДОКУМЕНТАМ

Требование разграничения доступа является одним из основополагающих моментов при создании информационно поисковых систем (ИПС), в которых обрабатывается конфиденциальная информация или информация ограниченного распространения. Методы и способы реализации этого требования могут быть различными в зависимости от степени жесткости ограничений.

Разработанная математическая модель и построенная на ее основании методика предлагается для применения при решении задачи информационной безопасности, состоящей в тематическом разграничении доступа.

Решение задачи разграничения доступа к сведениям ограниченного распространения, хранящимся в виде неструктурированных текстовых документов, может быть основано на разделении данных на тематические классы. Тематическое разграничение доступа к сведениям может заключаться в определении смысловой направленности запрашиваемого документа (авторубрикации), и принятии решения о доступе или отказа в доступе к нему пользователю. В этом случае решение принимается на основании таблицы доступа каждого пользователя к заранее созданным тематикам существующих в системе документов. Тогда, с целью автоматизации процесса принятия решения, подобная система разграничения доступа может быть основана на подсистеме автоматического определения тематики запрашиваемого документа.

Построение подсистемы автоматической рубрикации текстов, в свою очередь основывается, на определении меры статистической близости рубрицируемого текста к обучающим текстовым массивам рубрикатора. Теоретической базой данного механизма является векторное представление текстов из обучающего массива и рубрицируемого текста в виде частот появления s-цепочек последовательных символов текста, и вычисление по ним статистики мощности рассеивания. На основании получаемых значений определяется принадлежность рубрицируемого текста к каждой рубрике рубрикатора.

С целью экспериментального исследования правильности работы описываемого механизма тематического разграничения доступа была смоделирована система хранения электронных документов с документами заведомо известных рубрик. Каждый из запрашиваемых документов проходил процедуру авторубрикации, по результатам которой устанавливалась возможность доступа к нему. Эксперименты показали, следующие результаты: для документов объемом 5.000 символов и более, при обучающих массивах объемами 250.000 для каждой рубрики рубрикатора содержащего 20 рубрик вероятность правильного определения «чужого» для рубрикатора текста равна 0.92, а вероятность правильного распознавания тематики «своего» для рубрикатора текста равна 0.9.

Биденко С.И., Чопенко О.А., Исаенко А.Н.

Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

СОДЕРЖАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ ФЛОТА

В основе построения структуры комплексной защиты информации лежит принцип эшелонирования защиты. Этот принцип устанавливает ряд защитных барьеров между поражающими воздействиями и защищаемой системой (ее структурными элементами).

В структуре выделяются два функционально независимых защитных барьера: активная защита и пассивная. В подобной схеме недостаточная защитная способность каждого из барьеров повышается за счет их взаимного резервирования: сначала решается задача активной защиты, а в случае ее «отказа» срабатывает барьер пассивной защиты.

Активная защита предназначена для предотвращения факта преднамеренного воздействия и, следовательно, решает первую задачу комплексной защиты. Вероятность сохранения

защищаемого элемента будет определяться вероятностью недопущения соответствующих воздействий.

Барьер пассивной защиты начинает «функционировать», если активная защита не смогла предотвратить факт воздействия, и оно свершилось.

Следовательно, пассивная защита предназначена для того, чтобы исключить или снизить результаты воздействия поражающих факторов (ПФ) как в момент их возникновения, так и в течение времени сохранения их поражающего действия. В свою очередь, пассивная защита подразделяется на три составляющие (подсистемы) – структурную, инженерно-техническую (ИТЗ) и организационную защиту.

Инженерно-техническая защита предназначена для обеспечения защищенности (стойкости) элементов системы при комплексном воздействии ПФ.

Для обеспечения живучести структуры в целом проводятся следующие основные мероприятия, образующие в совокупности подсистему структурной защиты.

1) Рассредоточение элементов структуры информационной системы в пространстве, т.е. выбор взаимоудалений, исключающих возможность одновременного поражения более одного элемента при локальном воздействии по ним.

2) Структурная избыточность, достигаемая при помощи дублирования и резервирования.

Организационная защита представляет собой совокупность организационных и инженерно-технических мероприятий, проводимых непосредственно в подразделениях флота и направленных на обеспечение их готовности и ликвидацию последствий воздействия ПФ.

Содержание организационной защиты определяется необходимостью решения ею следующих трех основных задач.

1. Обеспечение дополнительной защиты информационной системы, прежде всего от механических и других ПФ.

2. Обеспечение безопасности и защиты персонала.

3. Ликвидация последствий чрезвычайных ситуаций в интересах восстановления готовности информационной системы.

Таким образом, организационная защита по своей целевой функции и решаемым задачам дополняет структурную и ИТЗ.

Борисов В.В.

Россия, Санкт-Петербург, ЗАО «НПП «Системные технологии защиты информации»

ЗАЩИТА СИСТЕМ УПРАВЛЕНИЯ СЕТЕВЫМИ УСТРОЙСТВАМИ

Необходимость создания и сертификации защищенной системы управления сетевыми устройствами: коммутаторами, маршрутизаторами, серверами и шлюзами обусловлена наличием большого количества распределенных систем и сетей, требующих стойких механизмов защиты информации.

В отличие от традиционных систем хранения и обработки данных, для систем управления характерны не только основные угрозы нарушения конфиденциальности, целостности и доступности. Для систем управления также имеют место угрозы отказа администратора от ответственности за конфигурацию управляемого оборудования и угроза распространения атакующих воздействий на всю сетевую инфраструктуру.

Защищенная система управления должна реализовывать централизованный унифицированный контроль доступа к различным объектам управления, что позволит использовать один экземпляр системы управления для управления множеством экземпляров разнородного сетевого оборудования, обрабатывающего информацию различных категорий. При этом система контроля доступа должна позволять использовать дискреционный и мандатный контроль доступа администраторов к управлению сетевым оборудованием, обеспечивать возможность гибкой настройки политики безопасности.

Централизованный аудит всех событий управления с установлением ответственности администратора также является необходимым условием решения задач доверенного управления. Подсистема хронологического контроля событий, выявления ошибок в настройках сетевого оборудования, фактов злоупотребления или нарушений со стороны обслуживающего персонала позволит формализовать процесс управления и задания критериев корректной конфигурации. Отдельными задачами при этом являются: обеспечение резервного копирования журналов, а также создание доверенного сервиса регистрации событий уровня сетевого оборудования, информация о которых передается с управляемого оборудования на систему управления.

Защищенное управление сетевыми устройствами должно осуществляться с использованием доверенного канала передачи информации (управления) на основе стека протоколов TCP/IP, защищаемого с помощью средств криптографической защиты информации, что должно обеспечить защиту от внешнего нарушителя и недобросовестных поставщиков каналов связи. Отдельной

задачей является обеспечение изоляции скомпрометированных сетевых сегментов, обеспечение невлияния локальных ошибок на распределенную систему в целом.

Для эффективного управления в распределенных сетях передачи данных требуется решение задач графического представления, мониторинга производительности и других параметров сетевых ресурсов в рамках модели FCAPS (ISO/IEC 10040). Защищенная система управления должна реализовывать функции управления отказами, конфигурацией, учетом, производительностью и безопасностью. Указанные функции могут быть реализованы самой системой управления или с помощью внешних систем представления, мониторинга и управления информационной инфраструктурой, основанных на общепринятом протоколе управления сетевым оборудованием SNMP. Средства защищенной системы управления должны обеспечивать контроль функционирования указанных внешних систем.

Разрабатываемые варианты защищенных систем управления должны основываться на доверенных компонентах и сопровождаться полным комплектом конструкторской и эксплуатационной документации, а также набором исходных текстов. Это позволит провести сертификацию на заданный уровень требований к информационной безопасности, и далее использовать разработанную систему управления в реальных защищенных информационных средах с предъявлением требований к информационной безопасности.

Построение защищенных систем управления на основе предлагаемых технологий обеспечит соответствие современным требованиям к информационной безопасности и защиты от компьютерных атак, отвечая потребностям конечных потребителей.

Верещагин В.Л.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ВОПРОСЫ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ (НА ОТСУТСТВИЕ ПРОГРАММНЫХ ЗАКЛАДОВ
И НДВ) ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ОБРАБАТЫВАЮЩЕГО СВЕДЕНИЯ ОГРАНИЧЕННОГО
РАСПРОСТРАНЕНИЯ**

Исследования программно-аппаратной продукции, поступающей в ряд ведомств, проводятся на основании руководящего документа (РД). Каждая испытательная лаборатория разрабатывает уникальную методику для выполнения требований РД, применяемая для конкретного объекта сертификации. Строгое соответствие методики требованиям РД контролирует орган по сертификации (ФСТЭК, МО РФ, ФСБ, ФСО и т.д.). РД разрабатывался в конце XX века и имеет множество недоработок, в частности предполагается проводить проверки в два этапа: первый – работа с исходными текстами и второй – с исполняемыми файлами. Для компилируемых языков (Си, С++, Pascal и т.п.) такой подход справедлив, а для интерпретируемых весьма затруднителен, т.к. исполняемый код находится в основном в оперативной памяти компьютера и, например, расчет контрольных сумм для текущего состояния памяти не будет однозначно идентифицировать программу. Возникают особенности при контроле избыточности исходных текстов и определении соответствия исходных текстов программного обеспечения (ПО) его загрузочному коду. В настоящей работе рассматривается возможный подход к испытанию программного продукта, написанного на языках PHP 4.1.2 и html 1.0.

Далее будем применять методики к объекту испытаний, состоящему из 4-х независимых программ, вызываемых из одного html-интерфейса и обрабатывающие одни и те же секретные данные, но для решения различных задач (сбор, обработка, подсчет статистики и т.п.). Все данные хранятся в SQL-базе, размещенной на удаленном сервере.

Формирование представления об архитектуре проекта, полезное для контроля избыточности, начинается с выявления главного файла, который предоставляет интерфейсы остальных программ. Принимая во внимание способы подключения остальных файлов, в автоматическом режиме формируются все связи, которые сравниваются с общим списком файлов и в результате обнаруживаются не только избыточные файлы, но и «мертвые» ссылки, которые следует заведомо рассматривать как уязвимость (как программную закладку, если угодно). Контроль избыточности функций облегчается обозначением всех таких объектов зарезервированным словом «function». При этом, удобно разобрать текст по схеме: файл – линейный участок – вызываемая функция. Если функция не вызывается ни в одном из линейных участков (как родного файла, так и в других файлах проекта), то впору отнести её к потенциально избыточным. Если во время динамического анализа они также не были вызваны, то функция считается избыточной. Полнота исходных текстов проверяется в процессе динамического анализа, опорным моментом является последовательное выполнение инструкций в памяти и контроль ошибок во время выполнения. Стоит отметить, что часто ошибки возникают из-за плохой проработки взаимодействия с пользователем. Наличие же ошибок является вспомогательной информацией для злоумышленника, что в условиях секретности недопустимо. Важно отметить, что пункт РД о соответствии исходных текстов ПО его объектному коду самое разумное не рассматривать по той причине, что бинарный код в ОЗУ на различных машинах может быть отличен для одних и тех же исходных текстов.

Исследование показало, что наиболее распространенными ошибками, обнаруживаемыми при анализе, являются следующие: высокая избыточность файлов, некорректные ссылки (предмет ссылки

отсутствует), передача имени пользователя и пароля к БД в открытом виде, слабый пароль, избыточная информация в сообщениях об ошибках, низкая устойчивость проекта и использование настроек безопасности интерпретатора по умолчанию. Все приведенные ошибки позволяют пользователю нарушить конфиденциальность, целостность и доступность данных и поэтому в обязательном порядке должны быть устранены в процессе сертификации разработчиками.

Воробьев В.И., Фаткиева Р.Р., Помецко В.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ ПРОГРАММНОГО КОДА**

Исключительная необходимость, а в некоторых случаях даже зависимость современного человека от информационных технологий, ставит такие вопросы как удобство пользователя, отказоустойчивость и безопасность ежедневно используемого программного обеспечения (ПО) на первое место.

Наличие дефектов ПО влечет проведение комплекса работ по обеспечению безопасности конкретной компьютерной системы и неразрывно связано с понятием качества, которое из абстрактного и неосязаемого преобразуется в численную характеристику на основании метрик оценки программного решения.

В качестве метрической шкалы для описания характеристик программного кода удобно использовать численный показатель, представляющий собой вероятность появления той или иной уязвимости в программе, определенную согласно способу оценки свойств метрики. На основе проведенного анализа информации об уязвимостях и методах тестирования предложен метод оценки программного продукта на наличие потенциальных уязвимых мест в программном коде, суть которого состоит в использовании метрик для выявления основных возможных видов уязвимостей. Предполагается, что применение подобных метрик возможно в первую очередь на этапе автоматизированного статического тестирования. Таким образом, исходный код тестируемой программы сканируется и далее анализируется в соответствии с введенными параметрами. К достоинствам вышеописанного метода можно отнести:

- применение не сканирования на соответствие с шаблонами, а более полный анализ основных признаков наличия уязвимости;
- применение метрик, как ко всей программе, так и к ее модулям по отдельности позволяет провести более тонкий анализ и способствует уменьшению количества ложных срабатываний;
- расширяемость.

Однако выявление той или иной уязвимости предполагает наличие соответствующей метрики.

Галанов А.И., Костин А.А., Молдовян У.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПРОТОКОЛЫ СЛЕПОЙ КОЛЛЕКТИВНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ**

Специальные задачи прикладной информатики решаются с помощью криптографических протоколов. Протоколы слепой электронной цифровой подписи (ЭЦП) используются при решении задач обеспечения анонимности в системах тайного электронного голосования или в системах электронных денег. Некоторые задачи требуют, чтобы электронные документы или сообщения были подписаны несколькими субъектами. В этих случаях ряд преимуществ может быть получен с использованием протоколов коллективной ЭЦП (КЭЦП). В настоящее время разработаны протоколы КЭЦП в которых подпись размера 320 бит удостоверяет, что электронное сообщение подписано двумя или более (до десятков и сотен) субъектами. При этом КЭЦП возникает как единое неделимое целое, поэтому применение этих протоколов автоматически решает проблему одновременного подписания пакета контрактов на расстоянии.

В настоящем сообщении предлагается схема построения протоколов слепой КЭЦП, которые представляют интерес для применения в системах тайного электронного голосования с контролем за выдачей избирательных бюллетеней несколькими независимыми сторонами. Данные протоколы строятся на основе рандомизированных алгоритмов ЭЦП, использующих сложные вычислительные задачи следующих двух типов: 1) дискретное логарифмирование в конечной группе большого простого порядка и 2) извлечение корней большой простой степени в конечных группах известного порядка со специальной структурой.

В предложенном способ построения протоколов слепой КЭЦП обеспечивается внутренняя целостность слепой коллективной подписи. Слепая КЭЦП формируется на основе двух процедур свертки параметров, вырабатываемых всеми подписывающими. Благодаря этому подлинная подпись может быть сформирована только для случая, когда документ подписан всеми участниками протокола, т. е. вычислительно невозможно сформировать урезанную слепую КЭЦП, которая бы соответствовала меньшему числу пользователей. Это свойство решает проблему одновременного подписания одного документа несколькими пользователями вслепую, что актуально для построения

систем регистрации времени создания электронных документов конфиденциального характера без раскрытия информации, содержащейся в документе.

Предложенные протоколы слепой КЭЦП перспективны для применения в системах тайного электронного голосования и системах коллективного формирования штампа времени создания файлов. Показано, что данные протоколы могут быть построены с использованием конечных групп векторов, конечных групп матриц, эллиптических кривых над конечным полем, а также с применением конечных полей следующих типов: простых полей, полей многочленов и векторных полей.

Работа поддержана грантом РФФИ № 08–07–00096–а.

Гаскаров В.Д.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций

ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ МОДЕЛЕЙ АБСТРАКЦИЙ

При решении задачи унификации понятийных средств необходимо развивать формальные методы представления и обработки знаний. На основе анализа формы и содержания, употребляемых в виде языков спецификаций понятий, можно ввести обобщенное понятие модели абстракции.

Модель абстракций – это интегральная логическая модель представления алгебраической или программной системы, отражающая специфику различных стадий инженерного проектирования в функциональном (базовые элементы), информационном (структура базовых элементов), организационном (структура системы в целом в виде исполнительных компонент) аспектах.

При описании моделей абстракций введем ряд понятий, таких как абстракция, вид абстракции, параметры абстракции, вид модели абстракции, модель абстракции, спецификации.

Абстракция – Понятие, которое отождествляет специфику элементов с образом – представлением. Абстракция идентифицирует множество элементов, на основании которого строится природа рассматриваемого явления.

Вид абстракции – Классификация элементов одной природы. Вид абстракции отражает функциональный аспект, характеризует форму образа – представления класса и сопоставим с семантической составляющей объективирования.

Параметры абстракции – Структура элементов одного класса. Параметры абстракции отражают информационный аспект, характеризует содержательную составляющую абстракции как образа – представления одного класса и сопоставляются с синтаксической составляющей объективирования.

Вид модели абстракции – Типизация задачи объективирования путем задания на множестве абстракций классов элементов и классов отношений.

Модель абстракций – Структура, заданная разработчиком в терминах абстракций определенного вида модели.

Спецификация – Объект – абстракция, с идентифицированными данными параметрами.

Задать вид модели абстракций – значит, задать два множества абстракций: множество классов элементов и множество классов отношений, которые определяют множество абстракций вида модели как объединение этих множеств. Тогда модель абстракций формально представима как заданное отношение структуры на множестве классов элементов и классов отношений.

Гнидко К.О., Горемыкин Д.В.

Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского

ИССЛЕДОВАНИЕ ФРАКТАЛЬНЫХ СВОЙСТВ ВНУШАЮЩИХ ТЕКСТОВ В ИНТЕРЕСАХ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ СУГГЕСТИВНЫХ ВОЗДЕЙСТВИЙ

Со второй половины 20-го столетия в ряде западных государств ведутся интенсивные исследования возможностей оказания суггестивного воздействия (скрытого изменения убеждений и поведения) на индивидуальное и коллективное сознание с применением средств массовой информации и вычислительной техники. Необходимость использования вербальных средств для достижения суггестивных целей определяет связь данной проблемной области не только со сферой психологии, но и с лингвистикой. Таким образом, актуальной задачей в русле современной концепции информационной безопасности является разработка теоретических основ и практических методик оценивания внушающего воздействия текста и речи.

Установлено, что суггестивные свойства текста находятся в непосредственной зависимости от частотно-динамических характеристик составляющих его фонетических и лексических единиц. Известно также, что эффект внушения усиливается при условии многократного повтора элементов текста. Введение в гипнотический транс, например, сопровождаются многократным и монотонным повторением речевых стимулов. Итеративность и устойчивое самоподобие отдельных элементов текста наблюдается в молитвах, мантрах, заговорах различных народов, независимо от этнической, исторической и культурной принадлежности. Вместе с тем, самоподобие является важнейшим свойством объектов фрактальной природы. Высокая чувствительность биологических систем к проявлениям фрактальных свойств в организации внешней среды доказана экспериментально.

Предположим, что внушающее воздействие текста, помимо прочего, определяется особой упорядоченностью его элементов, сходной в некотором отношении со структурой фрактала. Подобная организация обеспечивает «естественность» восприятия и повышает эффективность внушения. Для проверки данного предположения рассмотрим текст как линейно развертываемую во времени последовательность фонетических единиц (звукобукв), который может быть закодирован в виде численного ряда. Для различения случайных и фрактальных временных рядов использовался метод нормированного размаха, предложенный Х.Е.Херстом. Для преобразования текста в численный ряд и его последующего компьютерного анализа использовались значения кодов символов, определенные стандартами ASCII и Unicode. Все расчеты выполнены с использованием пакета Matlab 2008. В качестве материала исследования были использованы психотерапевтические тексты, заведомо рассчитанные на внушение, а также заговоры и заклинания различного содержания. Кроме того, для контрольно-сопоставительного анализа была сформирована группа нейтральных информационных текстов. Всего в рамках данного исследования проанализировано около сотни текстов различной тематики.

Полученные значения показателя Херста для текстов, априорно отнесенных к классу суггестивных, соответствовали неустойчивым (антиперсистентным) рядам. Помимо этого, графики, полученные в результате анализа суггестивных текстов методом нормированного размаха, обладали характерным общим свойством – наличием самоподобных периодически повторяющихся участков спад-подъем на различных уровнях детализации. Данные факты являются отражением особой ритмической структуры текстов внушающего воздействия. Для нейтральных текстов информационного содержания значение оценки показателя Херста соответствовало трендоустойчивым (персистентным) временным рядам, при этом самоподобие внутренней структуры не наблюдалось. Существенным является тот факт, что указанные свойства проявлялись вне зависимости от языка, на котором тексты были составлены.

Таким образом, по результатам проведенного исследования может быть сделан следующий вывод: анализ текстовых массивов методом нормированного размаха, в целом, позволяет в автоматизированном режиме выявлять подозрительные на оказание суггестивного воздействия тексты на основании проявляемых ими фрактальных свойств.

Гордеев Л.В.

**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»
АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В связи со скорым вступлением в силу требований Федерального закона Российской Федерации от 27 июля 2006 г. N 152–ФЗ «О персональных данных» у многих организаций и предприятий начались сложности с их выполнением.

Недостаточно отработанная нормативная база только усугубляет ситуацию, требуя от операторов персональных данных не только значительных затрат, но и, в ряде случаев внесения изменений, у установивший процесс обработки информации.

Отдельно стоит отметить тот факт, что представленные в настоящее время на рынке сертифицированные средства защиты информации от несанкционированного доступа не позволяют в полной мере использовать имеющиеся у заказчиков современное программное обеспечение.

Основные проблемы:

Аттестацию на соответствие требованиям по безопасности информации имеют право проводить лицензиаты ФСТЭК, которые имеют лицензию на деятельность по технической защите конфиденциальной информации, при этом наличие Аттестата аккредитации органа не является обязательным условием. В связи с этим в настоящее время начало появляется множество организаций не имеющих достаточного опыта работы в системе защиты информации, что не может не сказаться на качестве выполняемых работ.

Остаются не вполне ясными различия между 2-й и 3-й категориями персональных данных, определения которых даны в совместном приказе ФСТЭК, ФСБ и Мининформсвязи от 13.02.2008 – формулировка "позволяет получить дополнительную информацию" понимается не однозначно. Что, в свою очередь, затрудняет определение минимально необходимого комплекса мероприятий, необходимого в каждом конкретном случае.

В случае если в одной и той же системе обрабатывается информация, содержащая коммерческую, банковскую тайну и персональные данные, то собственник информационной системы вправе самостоятельно выбрать в каком режиме защиты и по требованиям каких документов обеспечивается защита информации

В большинстве организаций уже сформирована некая система защиты информации, но по ряду параметров не обеспечивающая выполнения требований руководящих документов, в этом случае приходится её перекраивать с заменой, как отдельных устройств, так и целых сегментов, а в ряде случаев в всю архитектуру системы.

Из примеров можно привести замену периметрового межсетевого экрана на сертифицированный, замену программного обеспечения информационной системы со свободно

распространяемого (например, некоторые Linux системы) на коммерческие версии, под которые имеются сертифицированные средства защиты.

Отдельно стоит отметить использование в информационной системе СУБД, которая может рассматриваться как прикладное программное обеспечение (ППО), но и как система защиты информации от несанкционированного доступа. По требованиям должно использоваться сертифицированное на отсутствие недеklarированных возможностей ППО, однако, при наличии в СУБД функций разграничения доступа, также необходима сертификация по классу СВТ. Примером такой СУБД может послужить продукция компании 1С, на базе которой функционируют финансовые отделы большинства организаций. Производителю не выгодно проводить сертификацию т.к. стоимость сертификации зачастую очень сильно удорожает такие продукты, к тому же при сертификации потребуется проведение инспекционного контроля всех обновлений. Таким образом, проблемы, возникающие при использовании подобных средств ложатся на операторов.

В условиях прогрессирующего финансового кризиса далеко не все организации способны выделять деньги на указанные цели, что может привести к применению против них санкций и даже банкротству.

Установление системы защиты персональных данных граждан, несомненно, должно быть одной из первоочередных целей государства, однако, оно не должно идти в разрез в реальной экономической ситуации в стране.

Григорьева М.В.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

информационных технологий, механики и оптики

ПРОГРАММНЫЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ ДЛЯ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Важным элементом построения любой защищенной компьютерной системы являются программные и программно-аппаратные средства генерации псевдослучайных чисел (ПСЧ). Генерация случайных чисел – одна из главных трудностей при реализации любой системы безопасности, в частности криптографической системы. Актуальной задачей является развитие теории генераторов ПСЧ, в том числе создание новых алгоритмов генерации ПСЧ, отвечающих требованию применимости в системах ЗИ.

Цель и задачи работы. Разработка и реализация программно-ориентированного алгоритма генерации ПСЧ с применением скоростного программного алгоритма криптографического преобразования. Разработанный алгоритм генерации должен отвечать требованиям непредсказуемости, обеспечения высокого быстродействия и эффективной и безопасной программной реализации.

Для достижения поставленной цели решаются следующие задачи:

- разработка алгоритма генерации ПСЧ с применением скоростного программного алгоритма криптографического преобразования «СПЕКТР–F»;
- разработка структуры, состава и интерфейса программы, предназначенной для генерации ПСЧ и реализации алгоритма. Разработка программной документации (спецификация, руководство оператора, описание программы);
- исследование скорости генерации и оценка качества выдаваемых псевдослучайных последовательностей с использованием методов статистического тестирования.

Практическая значимость работы состоит в возможности применения результатов, а именно созданных алгоритма генерации ПСЧ и программы, реализующей разработанный алгоритм, в качестве составных частей (элементов) систем безопасности. Разработанная программа реализует следующие функции:

- генерация расширенного ключа шифрования;
- реализация алгоритма шифрования дискового пространства «СПЕКТР–F»;
- генерация псевдослучайных чисел;
- шифрование/дешифрование блоков данных по заданным пользователем параметрам.

Предлагаемая вашему вниманию работа реализуется в рамках проекта, поддержанного грантом Правительства Санкт-Петербурга от 2009 года для студентов, аспирантов вузов и академических институтов.

Гриняев С.Н., Довнар С.Е.

Россия, Москва, Военный университет Министерства обороны Российской Федерации

Беларуссия, Минск, Белорусский государственный университет

О НЕКОТОРЫХ НЕДОСТАТКАХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Сегодня информация становится главным отличительным признаком современного мира. При всем многообразии и противоречивости точек зрения относительно становления нового типа информационного общества все ученые соглашаются в одном: информация есть нечто особенное.

При этом очень важно установить, каким образом она заняла центральное место в обществе, что же есть такого в информации, что она становится проблемой нашего времени и её следует защищать?

На современном этапе для защиты информационных ресурсов используется множество средств и методов защиты информации, основанных на классических моделях разграничения доступа. К недостаткам этих моделей относится их “статичность”, замкнутость внутреннего пространства модели. По существу все имеющиеся сегодня системы защиты информации – это конечные автоматы и получение нового знания в них невозможно. Отсутствие интеллектуальной составляющей обуславливает то, что противник знает результат своей атаки и в случае неудачи может при повторном нападении выбрать иную стратегию атаки, которая не будет обнаружена и окажется успешной.

Указанный недостаток становится все более существенным с увеличением масштабов и разнородности телекоммуникационных сетей, спектра услуг, количества и качества информационных ресурсов. Положение еще более усугубляется с ростом количества способов атак, направленных не только на данные, но и на многочисленные сетевые службы, которые работают практически на всех уровнях эталонных моделей и имеют множество уязвимостей.

Кроме моделей разграничения доступа существуют вероятностные модели защиты информации, например, игровая модель. Конечно, данная модель реально не показывает направлений совершенствования системы защиты и не предлагает эффективные средства борьбы. Однако, констатируя тот факт, что кто-то “выиграл”, а кто-то “проиграл” при имеющемся наборе средств она весьма наглядно отражает противостояние злоумышленника и администратора системы.

К числу факторов, влияющих на эффективность методов защиты информационных ресурсов, относится теоретическая проработка данной проблемы. Однако значительная часть наработанного учеными теоретико-методического аппарата относится либо к информационно-психологической составляющей информационной борьбы, либо только к области защиты информации путем разграничения доступа. Методы организации и ведения противостояния в информационных системах, практически, отсутствуют.

В целом в моделировании систем защиты информации ярко выражена тенденция к формализму и определенному отрыву от практики. Поэтому на практике системы защиты строятся чаще всего интуитивно, а не на основе анализа соответствующих моделей. Это зачастую приводит к избыточности средств защиты на одном направлении и провалу на другом. Возникает проблема бесконечного “латания дыр” в системе защиты информации.

Гурьянов Д.Ю.

Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

КОНЕЧНЫЕ ГРУППЫ ДВУХМЕРНЫХ ВЕКТОРОВ: ВАРИАНТЫ ЗАДАНИЯ И СЛОЖНОСТЬ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФИМИРОВАНИЯ

В данной работе рассматривается строение конечных групп двумерных векторов и задача дискретного логарифмирования. В качестве групповой операции вводятся два различных варианта умножения векторов. Для каждого из вариантов устанавливаются гомоморфизмы группы, с помощью которых задача дискретного логарифмирования в группе сводится к логарифмированию в базовом поле.

В обоих вариантах задания операции умножения векторов над простым конечным полем она вводится как перемножение каждой компоненты одного вектора-сомножителя с каждой компонентой другого вектора-сомножителя и замене произведений пар базисных векторов на однокомпонентные векторы, координаты которых представляет собой структурные коэффициенты, являющиеся элементами базового конечного поля. Правила замены представляются в виде таблицы умножения базисных векторов (ТУБВ). Изученные варианты отличаются выбором ТУБВ. В обоих случаях ТУБВ выбраны таким образом, что умножение векторов обладает свойствами ассоциативности и коммутативности при произвольных ненулевых значениях структурных коэффициентов, а нейтральным элементом по умножению является пара $E = (e, 0)$, где e – ненулевой элемент базового поля, который в общем случае не равен единице.

В зависимости от значений структурных коэффициентов множество обратимых векторов представляет собой мультипликативную группу расширения базового поля, которая является циклической, или нециклическую конечную группу. Показано, что задача дискретного логарифмирования в конечной нециклической группе векторов не сложнее задачи дискретного логарифмирования в базовом поле, т.е. она имеет субэкспоненциальную сложность и для обеспечения стойкости алгоритмов электронной цифровой подписи (ЭЦП) на основе групп двумерных векторов при использовании конструктивных схем с ключом вида $Y = G^x$ требуется выбирать параметр p длиной 1024 бит и более.

Рассмотрено строение мультипликативной группы конечных колец двумерных векторов над конечным полем при различных вариантах задания операции умножения векторов. Показано, что для всех исследованных вариантов задача дискретного логарифмирования в группе векторов сводится к задаче дискретного логарифмирования в базовом поле или расширенном поле (степень расширения

равна двум). Полученные результаты показали, что при заданном уровне стойкости алгоритмов ЭЦП, построенных с использованием конечных групп двумерных векторов, наименьшую временную сложность операция умножения имеет при выборе структурных коэффициентов, задающих образование конечного поля двумерных векторов.

Гурьянов Д.Ю., Молдовян Д.Н., Молдовяну П.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ВАРИАНТЫ РЕАЛИЗАЦИИ КОНЕЧНЫХ ГРУПП С МНОГОМЕРНОЙ ЦИКЛИЧНОСТЬЮ**

Недавно предложены схемы построения алгоритмов электронной цифровой подписи (ЭЦП) на основе нециклических групп частного вида, строение которых описывается в терминах многомерной цикличности. В предложенных схемах были использованы конечные группы векторов, заданные над конечными полями или кольцами специального вида. В настоящем сообщении обсуждаются варианты задания конечных групп с многомерной цикличностью и возможность их применения для разработки алгоритмов ЭЦП. Рассматриваемым типом строения обладают коммутативные группы конечных колец классов вычетов по модулю составного числа, не равного произведению простого числа $p > 3$ на число 2. В этом случае легко могут быть заданы группы, включающие подгруппы порядка q^r , обладающие r -мерной цикличностью (такие группы порождаются минимальной системой образующих, включающей r значений порядка q). Однако данный тип групп не может быть использован для построения производительных алгоритмов ЭЦП, поскольку задача вычисления многомерного логарифма в таких группах с помощью греко-китайской теоремы об остатках легко сводится к задаче дискретного логарифмирования в простом поле, причем последняя задача имеет субэкспоненциальную сложность.

Многомерным циклическим строением обладают также мультипликативные группы конечных колец многочленов над простым полем. При этом для произвольного заданного значения порядка групп векторов над конечным простым полем можно указать кольцо многочленов, мультипликативная группа которого обладает таким же значением порядка и одинаковым строением. В случае мультипликативных групп конечных колец многочленов задача вычисления «многомерных» логарифмов также с помощью греко-китайской теоремы об остатках сводится к решению задачи дискретного логарифмирования в поле многочленов, имеющей также субэкспоненциальную сложность. Совпадение строения мультипликативных групп векторов и многочленов, заданных над простым полем заданной характеристики, ставит актуальный вопрос об изоморфизме колец векторов и колец многочленов. Если для некоторого кольца векторов такой изоморфизм может быть найден, то тогда это означает, что и в мультипликативных группах векторов, обладающих многомерной цикличностью сложность нахождения «многомерных» дискретных логарифмов имеет субэкспоненциальную сложность и для построения стойких алгоритмов ЭЦП могут быть использованы только группы векторов, обладающих размером не менее 1024 бит. Для таких алгоритмов высокая производительность может быть достигнута преимущественно за счет возможности распараллеливания операции умножения в векторном поле. В связи этим актуально построение векторных конечных колец, для которых бы отсутствовал изоморфизм с кольцами многочленов, что вызывает интерес к некоммутативным кольцам векторов.

Работа поддержана грантом РФФИ № 08–07–00096–а.

Гурьянов Д.Ю., Захаров Д.В., Молдовян Н.А.

Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

**СТРОЕНИЕ МУЛЬТИПЛИКАТИВНЫХ ГРУПП ВЕКТОРОВ НАД КОЛЬЦАМИ ВЫЧЕТОВ
ПО МОДУЛЮ, РАВНОМУ КВАДРАТУ ПРОСТОГО ЧИСЛА**

Конечные мультипликативные группы двумерных векторов, заданных над кольцами вычетов по модулю, равному квадрату простого числа p , были предложены недавно как примитивы алгоритмов ЭЦП, основанных на сложности вычисления корней большой простой степени в группах известного порядка, делящегося на квадрат степени. Представляет интерес изучение вопроса о возможности применения групп векторов большей размерности, заданных над указанными конечными кольцами, для построения алгоритмов ЭЦП. Этот вопрос связан с изучением строения указанных групп векторов, которые являются нециклическими.

В данном сообщении рассматривается строение групп векторов различной размерности и показывается, что строение этих нециклических групп может быть описано в терминах многомерной цикличности. Получена формула $\Omega = p^{2m-1}(p-1)$, описывающая строение этих групп, и выполнен вычислительный эксперимент, подтвердивший интерпретацию строения в терминах многомерной цикличности.

Минимальная система образующих группы m -мерных векторов включает $m-1$ векторов порядка, равного квадрату числа p , и один вектор порядка $p(p-1)$. Группы включают подгруппу порядка p^m , содержащую p^m-1 векторов порядка p , которые составляют $p^{m-1} + p^{m-2} + \dots + p + 1$ циклических подгрупп порядка p .

Для случаев размерностей $m = 2$, $m = 3$ и $m = 4$ предложены алгоритмы ЭЦП, основанные на сложности извлечения корней степени p . В данных алгоритмах секретный ключ представляет собой некоторый вектор X , порядок которого равен или превосходит значение Ω/p , а открытым ключом является вектор $Y = X^p$. Стойкость алгоритмов определяется сложностью извлечения корня степени p из открытого ключа. Предложены два подхода к решению этой задачи. Первый подход состоит в построении алгоритма непосредственного вычисления корня, а второй к разработке алгоритма дискретного логарифмирования по «многомерному» основанию. Построены алгоритмы двух типов. Трудоемкость W обоих алгоритмов описывается соотношением $W = O(p^m(m/2))$, где O – обозначение порядка. Построенный алгоритм нахождения «многомерного» дискретного логарифма представляет собой модификацию хорошо известного алгоритма дискретного логарифмирования «больших и малых шагов». В алгоритме непосредственного вычисления корней в качестве одного из шагов используется нахождение векторов, которые являются корнями p -й степени из единичного вектора.

Для случая $m = 2$ обсуждается возможность сведения задачи вычисления секретного ключа к решению уравнения достаточно большой степени, заданного над базовым конечным полем. Однако построение атак на схему ЭЦП в рамках этого подхода связано с проблемой выражения корней степенного уравнения в радикалах.

Работа поддержана грантом РФФИ № 08–07–90100–Мол_а.

Дернова Е.С., Костина А.А., Синев В.Е.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Санкт-Петербургский институт информатики и автоматизации РАН
ВЫБОР ХАРАКТЕРИСТИКИ И СТЕПЕНИ РАСШИРЕНИЯ КОНЕЧНЫХ ПОЛЕЙ ДЛЯ
СХЕМ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ КОНЕЧНЫХ ГРУПП МАТРИЦ**

Конечные группы невырожденных квадратных матриц представляют интерес в качестве примитивов алгоритмов электронной цифровой подписи (ЭЦП), обладающих достаточно высокой скоростью формирования и проверки подлинности ЭЦП. Для аппаратной реализации представляет интерес реализация таких алгоритмов на основе конечных групп матриц, заданных над конечными расширенными полями. При этом также следует учитывать, что с ростом размера матриц повышается временная сложность операции матричного умножения, поскольку число умножений в базовом поле (поле над которым заданы матрицы) растет пропорционально третьей степени от размера матрицы.

В настоящем сообщении рассматриваются факторы, определяющие выбор характеристики и степени расширения базового поля для задания конечных групп невырожденных матриц $n \times n$, ориентированных на применение в алгоритмах ЭЦП. Дано обоснование выбору матриц размера 2×2 и выбору степени расширения базового поля, равной натуральной степени числа 2. Показано, что в этом случае имеется возможность выбрать такую характеристику базового поля, при которой порядок группы матриц содержит в качестве своего делителя большое простое число, причем для данного размера матриц и данного размера порядка базового поля обеспечиваются наибольшие простые делители порядка группы матриц по сравнению с другими случаями выбора степени расширения.

Выбором соответствующего значения характеристики p базового поля обеспечивается простота значения $q = (p^{2^m} + 1)/2$, которое всегда делит порядок группы невырожденных матриц размера 2×2 , заданных над полем степени расширения m .

В качестве расширенных полей для задания матриц могут быть использованы поля многочленов или векторные конечные поля, причем во втором случае обеспечивается более низкая сложность групповой операции матричного умножения, а также возможность эффективного распараллеливания, что имеет существенное значение при использовании многоядерных микропроцессоров, так как позволяет существенно повысить скорость формирования и проверки ЭЦП.

Для аппаратной реализации представляют интерес поля многочленов характеристики 2. В этом случае в качестве степени расширения следует выбирать значения, равные простому числу или степени числа 2, что обеспечивает возможность получения большого простого делителя порядка группы матриц, размер которого примерно равен размеру базового поля. Например, при степени расширения, равной 167, порядок группы матриц размера 2×2 содержит простой делитель $q = (2^{107} + 1)/3 = 62357403192785191176690552862561408838653121833643$.

Дернова Е.С., Костина А.А., Синев В.Е.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
ВЫБОР ПОРОЖДАЮЩЕГО ЭЛЕМЕНТА В СХЕМАХ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ
КОНЕЧНЫХ ГРУПП МАТРИЦ И ВЕКТОРОВ**

Предложенные недавно схемы ЭЦП на основе конечных групп векторов и матриц обеспечивают достаточно высокое быстродействие и возможность реализации протоколов коллективной электронной цифровой подписи (ЭЦП). В этих схемах используется вычислительно сложная задача

дискретного логарифмирования в циклических подгруппах достаточно большого простого порядка. Мотивировкой использования групп матриц и векторов в качестве примитива алгоритмов ЭЦП является поиск новых групп, в которых задача дискретного логарифмирования имеет экспоненциальную сложность, что дает принципиальную возможность достижения более высокого быстродействия. Последнее определяется тем, что в таких группах можно задавать размеры элементов меньшего размера, благодаря чему уменьшается временная сложность групповой операции. Анализ стойкости алгоритмов ЭЦП на основе конечных групп матриц и векторов связан с изучением возможности нахождения и использования изоморфизмов и гомоморфизмов, связанных с этими группами.

В настоящем сообщении рассматривается гомоморфное отображение конечного множества матриц и конечного множества векторов в конечное поле, над которым они заданы.

Функция от элементов конечного кольца квадратных матриц над конечным полем, значение которой является значением определителя матрицы, определяет гомоморфизм конечного кольца матриц в поле над которым определены матрицы. Наличие такого гомоморфизма при синтезе алгоритмов ЭЦП на основе циклических подгрупп матриц диктует необходимость использования таких подгрупп большого простого порядка, в которых все матрицы имеют единичное значение определителя. Это требование устраняет возможность получения какой-либо информации о секретном ключе на основе использования указанного гомоморфизма.

Для конечных колец векторов над конечными полями установлен гомоморфизм в базовое поле, определяемый функцией от элементов кольца векторов, имеющей значение, равное главному определителю системы линейных уравнений, по которой вычисляется обратный вектор к заданному вектору. Справедливость данного гомоморфизма доказана формально для сравнительно малых значений (от 2 до 6) размерности векторов для произвольных базовых полей и продемонстрирована экспериментально для размерностей от 2 до 55. Данное гомоморфное отображение кольца векторов в базовое поле определяет необходимость использования при синтезе алгоритмов ЭЦП таких подгрупп векторов, для которых указанный определитель имеет единичное значение.

Доказано, что значения соответствующих определителей матриц и векторов, принадлежащих подгруппам простого порядка, не делящего порядок мультипликативной группы базового поля, равны единичному значению.

Работа поддержана грантом РФФИ № 08–07–90100–Мол_а.

Десницкий В.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
КОНФИГУРИРОВАНИЕ МЕХАНИЗМА ЗАЩИТЫ ПРИ ПОМОЩИ ПОЛИТИК БЕЗОПАСНОСТИ**

Работа посвящена исследованию механизма защиты программного обеспечения на основе принципа удаленного доверия. В соответствии с данным принципом, контроль над выполнением клиентской программы делегируется специализированной удаленной сущности – доверенному серверу. Неотъемлемой частью механизма является набор отдельных (атомарных) методов защиты, таких как проверка контрольных сумм, метод проверки инвариантов, методы Barrier Slicing, Control Flow Checking, Crypto Guards, Orthogonal Replacement и другие, которые различаются как по уровню предоставляемой защиты, так и принципу защиты.

Важнейшей проблемой, возникающей при реализации механизма на практике и требующей разрешения, является проблема соотношения масштабируемости и безопасности. Требование масштабируемости механизма сводится к минимизации объема вычислений, выполняемых на стороне сервера для поддержки работы методов защиты на клиенте, тогда как безопасность механизма (т.е. уровень предоставляемой им защиты) во многом базируется на переносе и/или дублировании части вычислений методов защиты на сторону доверенного сервера. Представляемая работа посвящена разработке подхода по управлению доверенным сервером с использованием политик безопасности.

В соответствии с задачей поиска компромисса между масштабируемостью и безопасностью механизма защиты, использование политик безопасности позволит регулировать поведение доверенного сервера в случае изменения объема серверных ресурсов, доступного для поддержки методов защиты, и в частности случая его нехватки. Выбор конкретной политики может происходить автоматически, а также задаваться вручную проектировщиком или администратором системы на стороне доверенного сервера. Так, в соответствии со сценарием работы механизма на момент его запуска определяется некоторая текущая политика, которая впоследствии может подвергаться пересмотру.

В работе представлены различные варианты политики безопасности, определяющие особенности работы механизма при изменении доступного объема ресурсов. Рассматриваются два возможных типа политики, применяемой при нехватке ресурсов сервера: принудительное ограничение количества одновременно обслуживаемых клиентов и снижение предоставляемого уровня безопасности механизма через конфигурирование методов защиты. Конфигурирование

представляет собой подбор наиболее благоприятных параметров метода защиты, которое происходит на обеих сторонах соединения. В частности, рассматриваются подходы на основе репутаций, в зависимости от значений которых, для тех или иных групп клиентов степень защиты может быть ограничена на некоторое время. Также в работе был проведен анализ классов целевых программ, для которых каждую конкретную политику разумно было бы применять.

Предполагается развитие настоящего подхода посредством формализации рассматриваемых политик и построения автоматизированных процедур их выбора. Также планируется создание общей среды управления политиками на основе имеющихся данных о производительности и уровню защиты, предоставляемой каждым методом.

Работа выполнена при финансовой поддержке РФФИ (проект №07–01–00547), программы фундаментальных исследований ОНИТ РАН (контракт №3.2/03) и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST (контракт № 021186–2) и других проектов.

Десницкий В.А.

Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МАСШТАБИРУЕМОСТЬ И БЕЗОПАСНОСТЬ МЕХАНИЗМА ЗАЩИТЫ НА ОСНОВЕ
ПРИНЦИПА УДАЛЕННОГО ДОВЕРИЯ

Объектом исследования в данной работе является механизм защиты программного обеспечения на основе принципа удаленного доверия. В рамках данного подхода контроль за выполнением клиентской программы делегируется удаленной доверенной сущности – доверенному серверу. Механизм предполагает в качестве своей составной части реализацию отдельных (атомарных) методов защиты, таких как проверка контрольных сумм, метод проверки инвариантов, метод Barrier Slicing, метод Control Flow Checking, Crypto Guards, Orthogonal Replacement, характеризующихся различными подходами к защите целевой программы, и различающихся по уровню предоставляемой защиты. Одной из важнейших функций, возлагаемой на доверенный сервер, является работа по поддержке таких атомарных методов защиты на серверной стороне. Иначе говоря, сервер должен, во-первых, осуществлять проверку поступающих от клиента тегов, характеризующих текущее состояние программы, и, во-вторых, выполнять определенные действия, требуемые со стороны метода защиты.

Представляемая работа посвящена разработке методики, делающей возможным достижение компромисса между уровнем предоставляемой защиты (безопасностью) и масштабируемостью механизма. Такой компромисс достигается за счет выбора некоторой комбинации атомарных методов защиты, характеризующихся определенными значениями производительности и безопасности, при заданных ограничениях на потребляемые ресурсы сервера. Помимо этого, каждый метод защиты может иметь свои специфические параметры, также влияющие на характер его работы.

Были выработаны метрики, позволяющие оценивать методы защиты по отношению к их зависимости от разного типа ресурсов. Также на основе эмпирических исследований получены значения метрик для некоторых из рассматриваемых методов.

Вследствие достаточно слабой применимости техник определения безопасности на основе формальных подходов в качестве методики по оцениванию степени защиты, предоставляемой каждым из методов, была предложена методика с использованием экспертных мнений. Экспертам было предложено, во-первых, определить степень своей компетентности в области каждого из рассматриваемых методов и, во-вторых, упорядочить все множество методов защиты по возрастанию их силы, а также оценить каждый из них по пятибалльной шкале. Обработка полученных от экспертов данных учитывала, как априорную компетентность, определенную каждым из экспертов самостоятельно, так и апостериорную, как степень согласованности группового мнения.

В работе также представлены возможные политики безопасности, определяющие поведение доверенного сервера в случае нехватки того или иного ресурса сервера. Так, например, возможным действием в такой ситуации может быть непродолжительное снижение уровня предоставляемой защиты для клиентов имеющих наивысшую репутацию.

В дальнейших исследованиях предполагается развитие методики, в том числе разработка более точных техник оценивания безопасности методов защиты. Также планируется продолжение практической работы по получению значений метрик производительности для существующих реализаций методов защиты, и моделированию методов и алгоритмов защиты, не имеющих полноценных реализаций, которые были бы пригодны для использования в рамках механизма защиты ПО.

Работа выполнена при финансовой поддержке РФФИ (проект №07–01–00547), программы фундаментальных исследований ОНИТ РАН (контракт №3.2/03) и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST (контракт № 021186–2) и других проектов.

Доронин С.Е., Молдовяну П.А., Щербаков В.А.

Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,

Молдова, Кишинев, Институт математики и информатики АН Республики Молдова

**ПОСТРОЕНИЕ СХЕМ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ КОНЕЧНЫХ ГРУПП
ТРУДНОВЫЧИСЛИМОГО ПОРЯДКА**

Широко известные схемы электронной цифровой подписи (ЭЦП) основаны на группах, порядок которых вычисляется легко. К этому же классу схем ЭЦП можно отнести и криптосистему RSA, хотя значение порядка используемой в ней мультипликативной группы вычисляется только владельцем личного секретного ключа, соответствующему заданному открытому ключу.

В настоящей работе рассматривается вариант построения алгоритмов ЭЦП на основе групп порядок которых является трудно вычислимым по их определению. В этом случае нельзя использовать значение порядка в качестве личного секретного параметра, поскольку порядок трудно вычислим. Синтез схем ЭЦП на основе таких групп предлагается построить по аналогии с недавно предложенными схемами ЭЦП, основанными на сложности вычисления корней большой простой степени k по простому модулю p со специальной структурой. Требованием к структуре модуля является то, что число $p - 1$ должно делиться на квадрат степени корня. В этом случае при достаточно больших размерах модуля p задача извлечения корней является практически невыполнимой. Открытый ключ генерируется по формуле $Y = X^k$, где X – секретный ключ, представляющий собой случайно выбранный примитивный элемент по модулю p . Алгоритм ЭЦП строится по рандомизированной схеме [Автоматика и телемеханика. 2008. № 7. С.157–169] и использованием разового случайного секретного ключа, по которому вычисляется разовый открытый ключ, используемый в процедуре проверки ЭЦП (разовый открытый ключ непосредственно задается как один из двух параметров цифровой подписи или вычисляется при проверке подлинности ЭЦП). В такой схеме значение порядка (хотя оно является известным) не используется при выполнении процедур генерации и проверки подлинности ЭЦП. Таким образом, эта конструктивная схема может быть применена и при синтезе схем ЭЦП, основанных на группах, порядок которых вычислить практически невозможно.

В отличие от случая использования групп известного порядка, обладающего специальной структурой, применение групп трудно вычислимого порядка связано со следующей проблемой: сложная вычислительная задача, лежащая в основе стойкости алгоритма ЭЦП является менее известной, а значит и менее изученной. Однако предложенная схема представляет интерес, поскольку она расширяет число вычислительно трудных задач различного типа, которые могут быть применены для синтеза алгоритмов ЭЦП. Кроме того, возможность синтеза алгоритмов ЭЦП без необходимости вычисления порядка группы усиливает интерес к изучению таких групп, что будет способствовать более детальному изучению задачи вычисления порядка.

Работа поддержана грантом РФФИ № 08–07–90100–Мол_а и грантом АН Молдовы № 08.820.08.08 РФ.

Евневич Е.Л., Белаш Е.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПРИМЕНЕНИЕ HONEYPOT ДЛЯ ЗАЩИТЫ ГРИД-СИСТЕМ**

Грид-технологии приняты научным сообществом EGEE в качестве вычислительной инфраструктуры научных вычислений. Наблюдается тенденция к переходу от приложений с низким уровнем безопасности к приложениям, в которых происходит концентрация на безопасности. Грид-системы должны быть защищены не только от внешних атак, но, поскольку Грид предполагает совместное использование ресурсов и создание виртуальных организаций, необходимой является защита пользователей друг от друга. Многонациональная и многоорганизационная структура Грид-сред усложняет решение вопросов безопасности вследствие распределенной природы технических и законодательных требований в различных странах и организациях, в которых располагаются части Грид.

Для обеспечения сетевой безопасности используются преимущественно пассивные средства, такие как межсетевые экраны, системы обнаружения вторжений и др. Honeypot действует по принципу "приманки", моделируя реальную систему с низким уровнем защиты, привлекающую внимание злонамеренных пользователей и регистрирующую данные о предпринятых на нее атаках, включая попытки доступа, набранные команды, затронутые файлы и выполненные программы. Таким образом собирается информация о злоумышленнике, его намерениях и методах, а также своевременно обнаруживаются уязвимые места защищаемой системы.

Honeypot предполагается использовать в качестве дополнительного инструментального средства обеспечения безопасности Грид путем отвлечения хакеров от реальных систем и заманивания их в ловушку. Существенной частью является перенаправляющий модуль. В случае попыток подозрительного пользователя получить доступ к ресурсам Грид перенаправляющий

модуль обнаруживает его и перенаправляет к фальшивому ресурсу, в отличие от пассивных средств защиты, которые пытаются препятствовать доступу подозрительного пользователя.

В распределенных системах желательно устанавливать только одну ловушку Honeypot, и организовать централизованное управление по перенаправлению в нее подозрительных пользователей, сбору статистики по ним и анализа этих данных.

Honeypot базируется на IDS Snort, межсетевом экране IPTables и системе RedHeat 9.0 Linux. Сбор данных производится на трех уровнях: Snort собирает данные проверки пакетов и сохраняет их в системном файловом журнале syslog, межсетевой экран IPTables фиксирует все попытки доступа в журналах syslog и msyslog, и журнал операционной системы также используется при сборе данных.

Методы обнаружения, использованные в IDS, применяются при реализации перенаправляющего модуля. Модули перенаправления подозрительных пользователей в Honeypot устанавливаются у каждого поставщика ресурсов Грид.

Егорова К.С.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
информационных технологий, механики и оптики
НАНОТЕХНОЛОГИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Вопросы защиты информации становятся все более актуальными ввиду глобальной информатизации. Данные о структуре и динамике рынка безопасности за последние 5 лет, опубликованные изданием CnewsAnalytics, позволяют сделать вывод об актуальности проблемы информационной безопасности. В трех основных сегментах рынка (программные решения, аппаратные решения и услуги по информационной безопасности) наблюдается стабильный рост.

Важными компонентами информационной защиты являются инженерно-техническая и программно-аппаратная защита информации. Разработчикам систем защиты необходимо учитывать требования стандартов информационной безопасности, законодательство и социально-психологические аспекты защиты информации.

Одно из перспективных направлений создания систем безопасности, адекватных современным угрозам, связано с возможным использованием достижений из области нанотехнологий. Представляется, что достижения из сферы нанотехнологий могут быть использованы практически на всех уровнях защиты информации, при разработке и создании:

- новых средств и методов контроля и защиты документов от подделки, например, на основе наноматериалов, микропечати, тонких электронных схем, бумаги с добавлением наночастиц, компактных устройств считывания данных;
- систем контроля доступа в помещения на основе наносенсоров, например, считывателей отпечатков пальца, теплового рисунка вен руки или головы, геометрической формы руки в динамике;
- биосенсоров, простых или многофункциональных типа «электронный нос», для обнаружения и идентификации сверхмалых количеств взрывчатых веществ и компонентов оружия массового поражения;
- компактных чувствительных портативных и стационарных металлоискателей и детекторов движения на основе массивов наносенсоров;
- распределенных массивов наносенсоров типа «умная пыль» («Smart Dust») для охраны границ и периметров объектов;
- магниторезонансных (MRI) установок для анализа содержимого закрытых емкостей и грузов в аэропортах, на таможне, на проходных;
- автоматических систем ведения огня по наземным и воздушным целям – на основе наносенсоров, наноэлектронных компонентов и искусственных нейронных сетей.

В докладе затрагиваются проблемы обеспечения безопасности коммуникаций и сетей связи, обсуждаются методы их решения с использованием нанотехнологий. Также рассматриваются вопросы аутентификации и технологии защиты документов от подделки. Представляется, что особого внимания в современных условиях требует защита от террористических актов, поэтому уделяется внимание и этой проблеме.

Еремеев М.А., Палицын Б. А., Пономарев Ю.А.

**Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского
К ВОПРОСУ О МЕТОДАХ ОБНАРУЖЕНИЯ ВРЕДНОСНЫХ ВТОРЖЕНИЙ И
ИХ НЕЙТРАЛИЗАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ**

Появление новых технологий приводит не только к усовершенствованию процессов доступа к информации, но и к практически ежедневному появлению новых уязвимостей и разработке атак, эксплуатирующих выявленные уязвимости. Одним из самых распространенных вредоносных информационных вторжений является распределенный отказ в обслуживании (DDoS-атаки).

Задачи обнаружения вторжений сводятся к двум основным направлениям:

- обнаружение аномальной деятельности, на основе мониторинга некоторой пороговой величины и проявлении отклонений от нормального поведения;
- обнаружение злоумышленной деятельности (злоупотреблений), на основе заданного набора правил, определенных в виде последовательности действий субъектов.

В современных системах обнаружения вторжений (СОВ) применяются разнообразные методы анализа, основными из них являются: сигнатурный анализ, метод анализа состояний, методы экспертных систем, статистические методы, метод на основе нестатистических профилей пользователей, методы обнаружения на основе нейронных сетей, смешанные методы обнаружения атак и др.

Все методы обнаружения можно условно разделить на три группы: это методы, различные по технологии, уровню и типу обнаружения. Проведен сравнительный анализ этих методов. Предлагается применять следующие количественные показатели, по которым можно сравнить СОВ и осуществлять их адекватный выбор.

Показателем точности обнаружения является отношение суммарного числа ошибок, возникающих в процессе анализа (ложных срабатываний и пропусков атак) к общему числу операций анализа. Данный показатель характеризует практическую применимость СОВ для выявления атак. Основную проблему для вычисления значения данного показателя представляет получение общего числа операций анализа. Проведенные исследования показали, что способ вычисления общего числа операций анализа зависит от используемого в СОВ метода анализа и особенностей его реализации.

Показателем, характеризующим смещение в реализации компонентой СОВ метода анализа, является показатель сбалансированности, представляющий собой отношение числа ложных срабатываний к числу пропущенных атак. Показатель сбалансированности предоставляет возможность численно оценить увеличение затрат ресурсов системы защиты информации, необходимое для снижения возможности пропуска атаки.

Показателем, характеризующим производительность компоненты анализа, является возможное число операций анализа в единицу времени.

В качестве показателя, характеризующего степень полноты обнаружения, может быть использовано отношение числа обнаруживаемых СОВ атак к общему числу известных атак. Будем считать, что СОВ обеспечивает полное обнаружение атак, если она обнаруживает все известные атаки. Данная характеристика является наиболее трудной для оценивания, поскольку невозможно получить глобальные сведения обо всех атаках и способах злоупотреблений привилегиями. Для расширения практической применимости рассмотренного показателя полноты обнаружения, целесообразно при его расчете использовать общее число атак известных на данный момент времени.

В докладе предлагается методика для оценивания функциональных возможностей СОВ на основе системы количественных показателей и способов вычисления их значений, которая позволяет обосновать выбор СОВ, соответствующей требованиям политики безопасности информационно-телекоммуникационной системы вне зависимости от архитектуры СОВ и реализованных в ней методов обнаружения.

Предполагается осуществить моделирование воздействий DDoS-атак на информационно-телекоммуникационную систему методами теории массового обслуживания и нечетких множеств.

Замятин В.Ю., Гарбузова Т.Г.

**Россия, Санкт-Петербург, ГУ «Арктический и антарктический научно-исследовательский институт»
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СПЕЦИАЛИЗИРОВАННЫХ СИСТЕМ ФОНДА ДАННЫХ
АРКТИЧЕСКОГО И АНТАРКТИЧЕСКОГО НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО ИНСТИТУТА (ААНИИ)**

В рамках выполнения научно-исследовательских работ, направленных на реализацию Целевой научно-технической программы Росгидромета «Научные исследования и разработки в области гидрометеорологии и мониторинга окружающей среды» в ГУ «ААНИИ» в течение нескольких лет производится разработка и внедрение новых методов технической защиты специализированных информационно-справочных систем, к основным из которых отнесены системы для работы с:

- 1) материалами авиационных ледовых разведок;
- 2) геомагнитными данными;
- 3) ледовой фактической и справочной информацией (в рамках интеграции материалов Госфонда и Мирового центра данных по морскому льду).

С расширением количества Web-ориентированных и открытых информационно-справочных систем (отдела) фонда данных ГУ «ААНИИ» аспекты информационной безопасности становятся все более актуальными.

Для обеспечения информационной безопасностью фонда данных ААНИИ широко используются следующие административные, процедурные программно-технические регуляторы.

В число используемых административных регуляторов входят:

- 1) оценка рисков;
- 2) планирование безопасности;
- 3) организация внедрения систем и сервисов (поставка, СМР, ПНР и т.п.);
- 4) сертификация, аккредитация и оценка безопасности.

Основными применяемыми процедурными регуляторами выступают:

- 1) кадровая безопасность;
- 2) физическая защита;
- 3) планирование и обеспечение непрерывности бизнеса (business continuity);
- 4) управление конфигурацией;
- 5) сопровождение;
- 6) целостность систем и данных;
- 7) защита носителей;
- 8) планирование и обеспечение восстановления после бедствия (disaster recovery);
- 9) реагирование на нарушения информационной безопасности;
- 10) информирование и обучение.

В качестве программно-технических регуляторов задействованы:

- 1) идентификация и аутентификация;
- 2) управление доступом;
- 3) протоколирование и аудит;
- 4) защита систем и коммуникаций.

В число ближайших мероприятий, запланированных в ГУ «АНИИ», является приведение системы управления информационной безопасностью в соответствие требованиям международного стандарта безопасности информационных систем ISO 27001:2005.

В соответствии с требованием стандартов определяющих, что все меры по снижению рисков должны быть документально зафиксированы, производится разработка ряда методик и инструкций, описывающих процедуры обеспечения информационной безопасности и управления ею.

К числу основных методик отнесены:

- 1) методика инвентаризации активов;
- 2) методика категорирования активов;
- 3) методика оценки информационных рисков;
- 4) методика обработки информационных рисков.

Базовыми разрабатываемыми инструкциями являются следующие:

- 1) инструкция по обеспечению сохранности конфиденциальной информации (соглашение о конфиденциальности);
- 2) инструкция пользователя по обеспечению информационной безопасности;
- 3) инструкция системного администратора по обеспечению информационной безопасности;
- 4) инструкция администратора безопасности;
- 5) инструкция по управлению доступом пользователей к информационной системе;
- 6) инструкция по защите от вредоносного программного обеспечения;
- 7) инструкция по выполнению резервного копирования;
- 8) инструкция по обращению со съемными носителями информации;
- 9) инструкция по использованию мобильных компьютеров;
- 10) инструкция по использованию средств криптографической защиты информации;
- 11) инструкция по внесению изменений в информационную систему;
- 12) инструкция по управлению инцидентами информационной безопасности;
- 13) план непрерывности ведения бизнеса;
- 14) регламент обеспечения физической безопасности.

При реализации мероприятий в соответствии с ISO 27001:2005 основой для управления информационной безопасностью фонда данных ГУ «АНИИ» является PDCA-модель (модель Шухарта-Деминга), определяющая четыре этапа, которые последовательно должны выполняться для каждого процесса:

- 1) «Планируй» - создание (P – Plan);
- 2) «Выполняй» - внедрение и функционирование (D – Do);
- 3) «Проверяй» - мониторинг и проверка (C – Check);
- 4) «Действуй» - поддержание и улучшение (A – Act).

Предполагается, что наряду с разработкой новых информационных систем, проводимые в ГУ «АНИИ» мероприятия в области информационной безопасности позволят в сжатые сроки обеспечить требуемые уровень сохранности и интеграции накопленных за многие годы в ГУ «АНИИ» уникальных специализированных данных с внешними отечественными и международными информационно-справочными системами.

Захаров Д.В., Хо Нгок Зуй, Молдовян Д.Н., Молдовяну П.А.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
СПОСОБ ЗАДАНИЯ НЕКОММУТАТИВНЫХ КОНЕЧНЫХ ГРУПП ВЕКТОРОВ ЧЕТНОЙ РАЗМЕРНОСТИ

Конечные коммутативные кольца векторов над конечными полями, предложенные недавно в качестве примитивов алгоритмов электронной цифровой подписи (ЭЦП), представляют интерес для задания над ними эллиптических кривых, используемых для реализации криптографических алгоритмов, для ускорения алгоритмов коммутативного шифрования, а также для задания мультипликативных групп, применяемых для синтеза схем ЭЦП, основанных на сложности дискретного логарифмирования в конечной группе. Однако исследование строения мультипликативных групп векторов показало, что их строение таково, что всегда можно построить кольцо многочленов, мультипликативная группа которых имеет идентичное строение. Это позволяет сделать предположение о возможном изоморфизме групп векторов и групп многочленов с одинаковым строением. Предположительное наличие такого изоморфизма означает, что задачу дискретного логарифмирования в группе векторов можно свести к решению задачи дискретного логарифмирования в группе многочленов, где ее сложность является субэкспоненциальной. В связи с этим возникает задача построения некоммутативных колец векторов, для которых изоморфизм с кольцами многочленов отсутствует ввиду коммутативности последних.

В данном сообщении рассматривается построение некоммутативных конечных колец векторов над конечными полями. Для решения указанной задачи используется подход, примененный ранее для синтеза коммутативных колец векторов, в котором операция векторного умножения определяется посредством задания таблицы умножения формальных базисных векторов (ТУБВ). Отличие состоит в использовании четных значений размерности векторов $m \geq 4$ и некоммутативных ТУБВ. Значение $m = 4$ является минимальной размерностью для которой возможно построение некоммутативных конечных колец векторов. При такой размерности некоммутативность достигается несимметричным распределением (относительно главной диагонали ТУБВ) коэффициентов растяжения в используемой ТУБВ. При $m \geq 6$ некоммутативность достигается несимметричным распределением самих формальных базисных векторов. Во всех случаях обеспечивается свойство ассоциативности умножения базисных векторов. Для построения ассоциативных и некоммутативных ТУБВ предложен общий способ для произвольных четных размерностей. Составлена компьютерная программа, позволяющая построить требуемую ТУБВ для заданного четного значения размерности и проверить то, что обеспечивается свойство ассоциативности. Используемый способ построения состоит в следующем. В первой строке ТУБВ записываются базисные вектора. В четной (нечетной) i -ой строке базисные вектора записываются в обратной (прямой) последовательности, сохраняя на месте первый базисный вектор. Затем эта строка сдвигается вправо (влево) на $i - 1$ клетку.

Работа поддержана грантом РФФИ № 08-07-00096-а.

Зегжда П. Д., Калинин М.О.

Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ТЕХНОЛОГИЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ СРЕД ФУНКЦИОНИРОВАНИЯ
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Эффективность противодействия угрозам информационной безопасности определяется не столько составом средств защиты, а тем, насколько параметры безопасности операционной среды целостны в контексте безопасности информационно-телекоммуникационных систем (ИТКС). Контекст безопасности ИТКС образован такими характеристиками среды, как актуальные угрозы безопасности и особенности эксплуатации ИТКС; назначение и состав используемого системного и прикладного программного обеспечения, в том числе средств защиты; функциональные и информационные взаимосвязи между перечисленными составляющими.

Под термином "целостность" понимается взаимоувязанность и взаимосогласованность параметров среды (комплекса системного, прикладного ПО и средств защиты), что является необходимым условием безопасности ИТКС.

Решение задачи контроля целостности среды функционирования ИТКС в контексте безопасности ИТКС невозможно без учета разнообразия программного обеспечения с множеством функциональных свойств и настроек, предназначенного для обработки огромных объемов разнородной информации, поступающей из различных источников; гетерогенности ИТКС, в которых взаимодействуют различные операционные среды (например, MS Windows, UNIX/Linux); необходимости оперативной передачи информации между территориально удаленными подразделениями; необходимости учитывать изменения в среде ИТКС, связанные с ее обновлением, установкой функциональных дополнений; необходимости контроля, предупреждения и предотвращения нарушений информационной безопасности. Контрольное суммирование в данном случае бесполезно, поскольку не учитывает системность среды: совпадение сумм для каждого

контролируемого компонента не может гарантировать цельность функционала безопасности для всей системы. В то же время, нарушения целостности делают бесполезным применение любых систем защиты. Для решения обозначенной проблемы авторами реализована технология, основанная на автоматическом контроле целостности среды функционирования ИТКС. Данная технология позволяет не только фиксировать изменения, происходящие в системе, но и управлять информационной безопасностью ИТКС, реализуя стратегию упреждающей защиты.

Предлагаемая технология контроля целостности основывается на принципах использования логической модели, описывающей и предсказывающей поведение операционной среды и ИТКС в целом; задания отношений между требованиями безопасности и состояниями операционной среды в виде критериев; применения механизма допустимых отклонений уровня безопасности вместо контрольного суммирования; цикличности и перманентности выполняемых проверок безопасности ИТКС; и адаптации среды функционирования ИТКС к нарушениям безопасности путем установления состава нарушений, их устранения и переконфигурирования параметров безопасности систем.

Данные принципы позволяют контролировать целостность среды функционирования ИТКС с учетом ее изменений, которые не нарушают конгруэнтность самой среды и связи между ними и внешними факторами. Реализация технологии достигается путем применения парадигмы параметрического управления информационной безопасностью, которая предусматривает адаптацию параметров к происходящим воздействиям в рамках допустимых отклонений.

Зегжда Д.П., Калинин М.О.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
СПЕЦИФИКА СЕРТИФИКАЦИИ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**

Система обеспечения информационной безопасности (СОИБ) интегрирует систему информационной безопасности (СИБ), включающую средства защиты информации (СЗИ), их ресурсное и административное обеспечение и процессы эксплуатации, а также систему управления информационной безопасностью (СУИБ), образованную средствами установления, мониторинга и совершенствования средств защиты (см. Стандарт Банка России СТО БР ИББС-1.0-2008. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. 2008.)

Для установления и подтверждения того факта, что СОИБ выполняет поставленные перед ней задачи, применяется сертификация разрабатываемых решений. Система сертификации СЗИ в РФ представляет собой устоявшийся институт. В рамках процедуры сертификации при испытаниях и исследованиях заявленных СЗИ верифицируется, что данные средства обеспечивают указанный уровень безопасности. При успешном прохождении испытаний производителю СЗИ выдается сертификат, удостоверяющий, что СЗИ допускается использовать при осуществлении деятельности, требующей по закону обязательного использования сертифицированных средств. Однако наличие сертификата на СЗИ не гарантирует стационарности выполнения технических условий работы СЗИ и, как следствие, стабильного обеспечения работоспособности, безопасности защищаемых систем и постоянного соблюдения защитных мер, адекватных рискам реализации угроз информационной безопасности.

Для выполнения сертифицированными СЗИ заявленных функций должен соблюдаться установленный для них режим эксплуатации, который определяется совокупностью параметров самих СЗИ (в т.ч. системной конфигурацией, настройками совместимости ПО, рабочими установками, настройками безопасности, пользовательским составом). В этой связи, главные причины инцидентов информационной безопасности, происходящих с сертифицированными СЗИ, обусловлены не ошибками производителей и сертификационных лабораторий, а нарушениями, допущенными при управлении программной рабочей средой этих средств. Поскольку подобные просчеты характерны для любого СЗИ, а постоянно контролировать соблюдение регламента функционирования сертифицированного СЗИ в современных гетерогенных системах весьма затруднительно, то в настоящее время для решения данной проблемы наряду с СЗИ развивается целый класс средств сопряжения, осуществляющих мониторинг и воздействие на СЗИ и рабочую среду. Совокупность таких средств образует СУИБ. В рамках информационных систем СУИБ обеспечивает поддержку параметров основных и вспомогательных процессов информационной безопасности в заданных пределах и их корректировку в случае изменения внешних и внутренних условий функционирования и безопасности.

Поскольку СУИБ не только контролирует СЗИ, но и оказывают управляющие воздействия на их параметры, а также на параметры рабочей среды, то одновременно с осознанием потребности в СУИБ возникает необходимость в подтверждении корректности их работы. В этой связи становится весьма актуальной задача сертификации СУИБ.

Согласно постановлению правительства РФ "О сертификации средств защиты информации" №608, 26.06.1995 к СЗИ относятся технические, криптографические, программные и др. средства, предназначенные для защиты сведений, составляющих гостайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Следуя данному

определению, СУИБ не относится к СЗИ, хотя непосредственным образом обеспечивает безопасность информационных систем путем настройки и поддержания стабильности параметров СЗИ и цельности характеристик рабочей среды. Таким образом, СУИБ не подпадает под действие нормативных документов и стандартов, определяющих процедуру сертификации СЗИ. С другой стороны, на корпоративном уровне для СУИБ, называемых в этом случае системами менеджмента информационной безопасности (СМИБ), проводятся сертификационные испытания в рамках международной системы стандартов ИСО 27001 (ГОСТ Р ИСО/МЭК 27001. Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования. 2005).

С учетом этого и на основе анализа требований стандартов, касающихся верификации СМИБ, авторами поднимается вопрос о необходимости разработки совокупности требований для программных СУИБ с целью расширения существующей в РФ нормативной базы сертификации программных средств обеспечения информационной безопасности и привязки СУИБ к уровням защиты СЗИ и классам обрабатываемой информации.

Исследование задач, перечисленных в стандартах семейств ИСО 27001, 13335, 18044, приводит к заключению об этапности и цикличности процесса управления информационной безопасностью, что позволяет сформулировать по отношению к СУИБ требования, затрагивающие управляющие процедуры: формирование условий функционирования и безопасности активов, контроль текущей системной конфигурации на предмет соблюдения этих условий и адаптация параметров безопасности.

Наличие в СУИБ аппарата критериев безопасности позволяет сформировать некую область безопасности, в которую входят управляемые активы и множество параметров, обеспечивающих безопасность информационной системы. СЗИ, их рабочая среда, как и информационная система в целом, изменяются в ходе эксплуатации и реализации угроз безопасности. Поэтому условия служат индикаторами безопасности, и их нарушение является признаком отклонений в конфигурации системы, требующих вмешательства со стороны СУИБ с целью предотвращения эскалации угроз. При этом проверка условий должна быть периодичной.

Для реализации управления необходимы требования моделирования процессов, происходящих в управляемых системах, в части описания механизмом функционирования средств защиты, воздействия параметров системы, влияния внутренней и внешней среды на конфиденциальность, целостность и доступность информационных ресурсов.

СУИБ должна также включать механизм адаптации управляемых систем. Для обеспечения согласованности параметров СЗИ и условий реализации заданных условий функционирования и безопасности требования, предъявляемые к СУИБ, должны затрагивать функционал управления безопасностью, срабатывающий в случае возникновения нарушений. Воздействие, как и контроль, должно выполняться посредством направленного влияния на параметры безопасности информационных систем.

Таким образом, являясь средством сопровождения информационной безопасности, которое обеспечивает не только анализ безопасности, но и позволяет воздействовать на параметры управляемых защищенных систем с целью достижения ими стационарности, СУИБ нуждаются в построении системы сертификационных требований, отражающих эту специфику систем управления.

Зегжда Д.П., Калинин М.О., Москвин Д.А.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ЦЕЛОСТНОСТЬ ПОСТОЯННЫХ И ИЗМЕНЯЮЩИХСЯ КОМПОНЕНТОВ ПРОГРАММНОЙ СРЕДЫ
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ**

Для любой современной информационно-телекоммуникационной системы (ИТКС) характерно непрерывное изменение и усложнение структуры программной среды, включающей системное, прикладное программное обеспечение и средства защиты.

Развитие информационных технологий с одной стороны позволяет повысить функциональный потенциал использования программной среды ИТКС, предоставляя новые возможности и эффективные средства по их реализации. С другой стороны, подобная вариативность решений открывает для внешних и внутренних злоумышленников новые возможности по нарушению информационной безопасности (ИБ) за счет возникновения новых уязвимостей.

Безопасность программной среды ИТКС обеспечивается включением в ее состав средств защиты, таких как антивирусное программное обеспечение, межсетевые экраны, системы обнаружения атак, системы аутентификации и разграничения доступа.

Все программные компоненты ИТКС можно разделить на две группы: постоянные и изменяющиеся. К постоянным относятся компоненты программной среды, состав и содержимое которых не изменяется на всем протяжении эксплуатации ИТКС. Целостность таких компонентов может контролироваться "традиционным" методом контрольного суммирования. К изменяющимся относятся компоненты программной среды, состав и содержимое которых может изменяться во

время эксплуатации ИТКС. Изменения могут быть обусловлены установками различных обновлений, дополнений, исправлений и новых версий системного, прикладного программного обеспечения и средств защиты, их конфигурированием и установлением функциональной совместимости. Наличие таких изменений не позволяет контролировать целостность программной среды с помощью криптографических методов (контрольного суммирования, подсчета ЭЦП, хэшей). Поэтому необходим более гибкий механизм контроля и обеспечения целостности, который позволял бы обеспечивать и контролировать согласованность параметров функционирования и безопасности системного, прикладного программного обеспечения (ПО) и средств защиты с характеристиками программной среды ИТКС.

Функционирование программной среды ИТКС должно быть согласовано со следующими ее характеристиками, а также связями между ними:

- особенности конкретной программной среды ИТКС;
- условия эксплуатации средств защиты;
- назначение и состав используемого системного и прикладного ПО;
- актуальные угрозы безопасности.

Таким образом, целостность программной среды ИТКС – это состояние взаимного соответствия конфигурационных параметров системного, прикладного ПО и средств защиты. Следовательно, задача обеспечения целостности программной среды ИТКС представляется как достижение взаимоувязанности и единства используемых средств защиты и характеристик программной среды ИТКС. Обеспечение целостности программной среды ИТКС осложняется наличием ряда факторов, таких как:

- применение разнообразного ПО с множеством функциональных свойств и настроек, предназначенного для обработки разнородной информации, поступающей из различных источников;
- гетерогенность вычислительных сетей ИТКС, в которых взаимодействуют компьютеры под управлением ОС различных семейств (MS Windows, UNIX/Linux и пр.);
- необходимость оперативной передачи информации между территориально удаленными подразделениями;
- необходимость учитывать изменения программной среды ИТКС, связанные с обновлением ПО, установкой различных обновлений и функциональных дополнений, изменением пользовательского состава;
- необходимость контроля, предупреждения и предотвращения нарушений ИБ.

В этой связи механизм обеспечения целостности основывается на следующих принципах:

- принцип моделирования поведения средств защиты (необходимо использование логической модели, описывающей и предсказывающей поведение средств защиты с учетом характеристик программной среды ИТКС);
- принцип эквивалентности состояний программной среды (задание отношений эквивалентности между состояниями программной среды ИТКС в виде простых критериев. Под состоянием программной среды понимается множество всех настроек и конфигурационных параметров безопасности (ПБ) системного, прикладного ПО и средств защиты, зафиксированное в некоторый момент времени);
- принцип допустимых отклонений (формирование с помощью критериев области, в которой допустимы отклонения для изменяемых ПБ и в которой методы контрольного суммирования имеют ограниченную применимость).

Указанные принципы позволяют контролировать целостность программной среды ИТКС с учетом ее изменений, которые не нарушают цельность совокупности свойств и характеристик среды, связей между ними и внешними факторами. В соответствии с изложенными принципами авторами разработана технология обеспечения целостности программной среды, в основе которой лежит концепция области эквивалентности конфигурационных ПБ.

Область эквивалентности представляет собой объединение подмножеств конфигурационных ПБ системного, прикладного ПО и средств защиты, которые удовлетворяют требованиям безопасности и функционирования программной среды ИТКС. Любые сочетания конфигурационных ПБ программных компонентов, которые принадлежат области эквивалентности, удовлетворяют требованиям согласованности параметров функционирования и безопасности программных компонентов с характеристиками программной среды ИТКС. Если изменение состояния программной среды приводит к отклонению конфигурационных параметров программных компонентов, не выходящих за границы области эквивалентности, то целостность программной среды ИТКС сохраняется.

Данная технология позволяет автоматизировать решение задачи контроля целостности программных сред ИТКС и реализовать следующие функции:

1. Контроль соответствия программной среды требованиям безопасности и регламентам эксплуатации.

2. Контроль соответствия программной среды назначению ИТКС и текущим задачам ее применения.
3. Контроль инвариантности программной среды по всем компонентам ИТКС.
4. Оценка интегральных характеристик программной среды.
5. Вычисление нормализованного представления безопасности конфигурации.

Применение данной технологии позволяет оперативно, целенаправленно и эффективно реагировать на негативные изменения, происходящие в программной среде ИТКС в процессе ее эксплуатации, и тем самым поддерживать интегральную информационную устойчивость функционирования ИТКС, предотвращая недоступность ресурсов, отказы сервисов, сбои и нарушения безопасного функционирования элементов программной среды ИТКС. Применение данной технологии также позволяет оптимизировать управление ИБ, повысить эффективность эксплуатации инфраструктуры ИТКС, и при этом понизить требования к квалификации персонала.

Ивашук И.Ю.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

ПОДХОД К СОЗДАНИЮ БАЗОВОГО ФУНКЦИОНАЛЬНОГО ПАКЕТА СЕМЕЙСТВА ПРОФИЛЕЙ ЗАЩИТЫ ДЛЯ БЕСПРОВОДНОЙ СЕТИ

Профиль защиты (ПЗ) предназначен для сертификации средств защиты информации продуктов и систем ИТ и получения сопоставимых оценок их безопасности. Профили защиты служат также основой для разработки разделов требований безопасности информации (заданий по безопасности) на конкретные изделия ИТ. Тип изделий ИТ характеризуется общими функциональными требованиями безопасности (ФТБ). ФТБ, общие для всех изделий ИТ одного типа составляют базовый функциональный пакет (БФП) семейства ПЗ.

Как видно из определения, основной задачей для получения БФП семейства является исследование множества объектов оценки (ОО) и получение общего для него набора ФТБ.

В качестве ОО при разработке ПЗ беспроводной сети (БС) рассматривается вся сеть, а не отдельные ее сегменты. Разработка профилей защиты для беспроводных сетей позволит аттестовать их в соответствии с международным стандартом ISO 15408.

Суммируя знания по существующим ныне стандартам в мире БС, был выделен ряд критериев для проведения анализа, а впоследствии и оценки защищенности беспроводной сети.

Было выделено две основные группы критериев, в соответствии с которыми и происходит оценка сети:

- Криптографические критерии
- Критерии аутентификации.

Каждая группа включает в себя ряд компонентов.

Криптографические критерии:

1. Криптографические алгоритмы
2. Длина используемого ключа
3. Использование динамических или статических ключей
4. Технология проверки целостности сообщений (MIC, CCMP)

Критерии аутентификации

1. Протокол
2. Наличие сервера аутентификации
3. Взаимная аутентификация
4. Использование цифровых сертификатов

В соответствии с этими критериями были проранжированы средства защиты информации БС. В ходе работы был получен набор семейств и компонентов ФТБ, которые должны быть включены во все ПЗ семейства (БФП) и являются основополагающими при их построении.

Игнатьев М.Б.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

БЕЗОПАСНОСТЬ И ПОДДЕРЖКА УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ НА ОСНОВЕ МОДЕЛИРОВАНИЯ

Неправильные управленческие решения подрывают безопасность как отдельных предприятий и регионов, так и государства в целом. Выработка правильных решений в сложном меняющемся мире – трудная задача, в решении которой может помочь компьютерное моделирование. С помощью моделирования можно оценить последствия принимаемых решений в краткосрочной, среднесрочной и долгосрочной перспективе и выбрать наилучшее в рамках заданных ограничений. К сожалению в планах по созданию так называемого электронного правительства не предусмотрено формирование блока моделирования последствий от принимаемых решений, что критиковалось Президентом России Д.А.Медведевым.

В докладе рассматривается лингво-комбинаторное моделирование слабо формализованных систем применительно к моделированию городов и региона Балтийского моря. Это моделирование осуществляется на основе выделения ключевых слов, которые определяют основные переменные модели, и на основе формирования матрицы структурированной неопределенности, что позволяет подстраивать модель к неизвестным заранее параметрам. Крупноблочная модель формируется на основе ключевых слов «население», «пассионарность населения», «территория», «производство», «экология и безопасность», «финансы», «внешние связи», каждая из этих переменных имеет вектор характеристик. Например, переменная «население» имеет характеристики «занятость», «здоровье», «образование». Число блоков может быть увеличено. Формируются компьютерные структуры для поддержки управленческих решений и анализируется опыт их использования.

В докладе утверждается, что наибольшие адаптационные возможности систем имеются в зоне адаптационного максимума, откуда вытекает стратегия управления сложными системами в потоке перемен – сложные системы должны управляться так, чтобы удерживать систему в зоне адаптационного максимума путем наложения и снятия ограничений, путем объединения в коллективы или выхода из коллектива и др. В условиях кризиса особенно важно удерживать системы в зоне адаптационного максимума, да и сам кризис той или иной системы определяется удалением от зоны адаптационного максимума.

Казаков А.А.

Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
КЛАССИФИКАЦИЯ МЕТОДОВ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК В INTERNET

В докладе рассматриваются следующие вопросы:

- Определение угроз безопасности узлов Internet и их классификация.
- Существующие подходы к защите узлов Internet от рассмотренных угроз.
- Анализ и классификация методов защиты узлов Internet.

Угрозы безопасности узлов Internet могут быть подразделены на два типа:

1) Вызванные атаками, использующими уязвимость в реализации программного обеспечения узла.

Как правило, данные атаки не требуют отправки больших объемов данных, достаточно нескольких пакетов специального для используемой уязвимости содержания существуют исключительные ситуации, например, когда уязвимость атакуется отправкой нескольких очередей пакетов, когда резкие всплески интенсивности обрабатываемых данных вызывают сбой.

2) Вызванные большими объемами трафика предназначенного для атакуемого узла, что ведет к поглощению ресурсов самого узла (процессорное время, память), а также монополизировать канал. Последствием данной атаки является не возможность атакуемого узла обрабатывать запросы реальных пользователей.

Наиболее существенной угрозой безопасности для систем, предоставляющих прикладные сервисы для пользователя является распределенный отказ в обслуживании, большинство рассмотренных методов защиты в данном докладе посвящены защите от распределенного отказа в обслуживании.

Существующие подходы к защите узлов Internet можно поделить на два типа:

1) Защита средствами сетевого узла. Методы данного типа целиком реализуют механизмы защиты непосредственно на защищаемом узле.

В качестве примеров данного типа выступают: Методы определения отправителя, в данном случае отдельный сетевой узел пытается, основываясь на различных критериях установить аутентичность источника трафика, например в Hop Count Filtering (метод проверки аутентичности отправителя) это сопоставление значения TTL и адреса источника, TCP/IP proxy (метод защиты узла от уязвимостей в реализации TCP/IP) решения, которые являются посредником между клиентом и штатной реализацией протоколов, что предостерегает узел от известных уязвимостей.

2) Защита средствами маршрутизации. Данные подходы работают как динамические механизмы маршрутизации, тем самым создается Overlay Network (множество доверенных узлов создающих сеть), где при передаче сообщений от клиента путь их прохождения выбирается динамически. Например сети компании Akamai, технология MONET руководствуются данным принципом.

Приведена классификация методов защиты узлов Internet рассмотренных в данном материале, основываясь на различных признаках, например: тип угрозы, от которой обеспечивается защита, условия реализации атаки, которой способен противостоять рассматриваемый метод защиты, например количество атакующих узлов в заданной топологии сети, количество и специфика ложных срабатываний, применимость метода в сетях Internet и так далее.

На основе проведенной классификации сформулированы требования к методам защиты узлов Internet от сетевых угроз и сделано предположение о комплексном подходе к защите от отказа в обслуживании.

Карташов В., Рычагов А.Ю.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики
О ПРОТИВОДЕЙСТВИИ ROOTKIT

В последнее время всё большее распространение получают так называемые RootKit-технологии. Термин RootKit (Руткит) впервые появился в Unix-системах, где означает набор утилит, устанавливаемых взломщиком для получения первоначального доступа к машине. В Windows же под ним понимается программа, внедряющаяся в систему и перехватывающая системные функции или производящая замену системных библиотек. Руткит позволяет взломщику закрепиться в системе, скрывая следы своего присутствия. Эта технология получила большое распространение в создании botnet сетей.

Как правило, Руткиты классифицируют на работающие в режиме пользователя и в режиме ядра, так же встречаются классификации по принципу действия и постоянству существования.

Из-за многочисленных уязвимостей операционных систем существуют разнообразные методы реализации Руткита; особенно успешно эта технология проявляет себя в операционных системах семейства Windows, которые распространены больше других. Хотя в Windows переписывание системных файлов затруднено, есть возможность модификации памяти. Руткит использует методы перехвата системных функций Windows API, изменение системных структур данных, модификацию MBR и загрузку до ядра операционной системы. Данный вид вредоносных кодов давно известен в мире Windows и с начала 90-х годов прошлого столетия носит название Stels-вируса. Кроме того, Руткиту нужно как-то поставить себя на автозапуск, а в Windows для этого существуют и другие способы, помимо «стандартных».

Для противостояния злоумышленнику необходимо знать принципы вызова функций, размещенных в DLL. Не смотря на то, что для рядового пользователя обнаружить Руткит в системе достаточно проблемно, для человека более опытного это не представляется задачей нереальной, как несовершенны методы защиты, так нет и идеальных методов атак и заражения, следовательно, можно предложить вполне реализуемые методики обнаружения Руткитов.

Основные методики перехвата функций, поясняющие принципы работы Руткитов сегодня описаны. Однако разработчики RootKit-технологий не стоят на месте: постоянно появляются новые разработки, подходы и методы. Поэтому также должны развиваться и средства защиты, а главное культура пользователей, которые в первую очередь и должны следить за безопасностью своей машины. Заражённый компьютер весьма тяжело освободить от «порабощения» злоумышленником.

Корт С.С.

Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
МОДЕЛЬ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ СИСТЕМЫ РАСПОЗНАВАНИЯ ОБРАЗОВ

В настоящем докладе рассматриваются основные модели систем обнаружения вторжений, описанные в литературе, а также предлагается модель системы обнаружения вторжений как системы распознавания образов.

В работе Denning D. «An intrusion-detection model» рассматривается классическая модель системы обнаружения вторжений CIDF. Вследствие ее популярности подробно рассматриваться она не будет. Критика данной модели приводится в работе Корт С.С., Рудина Е.А. «Архитектура универсального ядра систем мониторинга и защиты от вторжений».

В работе P. Helman, G. Liepins «Statistical foundations of audit trail analysis for the detection of computer misuse» была сформулирована модель COB (Системы обнаружения вторжения), описывающая процесс обнаружения вторжений и атак с точки зрения теории Байеса. В данной работе функционирование COB рассматривается как оценка параметров случайного процесса, сформированного из данных, принадлежащих нормальному и аномальному поведению. После этого описываются вероятности того, что некоторое действие принадлежит нормальному или аномальному процессу N. Детектор, предложенный в работе, функционирует в соответствии с выражением, оценивающим байесовскую вероятность того, что действие принадлежит нормальному или аномальному процессу.

В работе G. Di Crescenzo, A. Ghosh, R. Talpade «Towards a Theory of Intrusion Detection» была сформулирована модель COB, объединяющая в едином формализме методы обнаружения вторжений, основанные на выявлении аномалий и поиске сигнатур. Требования к системе обнаружения вторжений в рамках модели основываются на понятиях теории сложности и криптографических понятиях. При этом используются понятия вычислительной различимости и различимости для одиночного образца распределения, определяющие чувствительность системы к обнаружению вторжений.

В работе Guofei Gu, Prahlaad Fogla, David Dagon, Wenke Lee and Boris Skoric «Towards an Information-Theoretic Framework for Analyzing Intrusion Detection Systems» была представлена модель COB, предназначенная для оценки количества информации, передаваемой между компонентами COB. В предлагаемой модели система обнаружения вторжений описывается как кортеж, описывающий структуры

данных и алгоритмы, используемые в системе обнаружения вторжений. В модели достаточно полно описаны процедуры преобразования данных в процессе обнаружения вторжений.

Таким образом, на основании проведенного анализа можно сделать следующие выводы.

1) Модель CIDF является первой моделью систем обнаружения вторжений и предлагает общую структуру данных систем. К недостаткам модели CIDF можно отнести то, что она не учитывает процессов, происходящих в модуле сбора данных и в модуле анализа, а также не отражает самого процесса обнаружения вторжений.

2) Достоинством Байесовской модели системы обнаружения вторжений является то, что она впервые ввела понятие вероятности в алгоритм обнаружения вторжений. К недостаткам можно отнести недостаточную выразительность байесовских алгоритмов.

3) Достоинством криптографической модели является то, что она опирается на хорошо разработанную криптографическую теорию. К недостаткам можно отнести отсутствие в модели характеристик алгоритмов, используемых для обнаружения вторжений, в том числе вопросов, связанных с формулировкой безопасного и небезопасного поведения.

4) Информационная модель впервые отражает алгоритмы и структуры данных, используемые на различных этапах работы системы обнаружения вторжений. К сожалению, авторы модели использовали ее только для получения единой метрики, описывающей ошибки системы обнаружения вторжений.

Постановка проблемы обнаружения вторжений как задачи распознавания образов позволяет:

1) Описать математическую постановку задачи обнаружения вторжений как задачу распознавания образов.

2) Использовать разработанный аппарат задач распознавания образов и обучения для решения задачи обнаружения вторжений.

3) Исследовать и характеризовать трансформации, обеспечивающие преобразование данных к виду, удобному для обнаружения вторжений.

4) Разработать формальные конструкции для описания алгоритмов, используемых системами обнаружения вторжений.

5) Выявить ограничения, присущие различным методам обнаружения вторжений.

6) Разработать систематические методы автоматического выбора алгоритма обнаружения вторжений для конкретной системы.

Для того, чтобы рассматривать систему обнаружения вторжений как систему распознавания образов, необходимо учесть специфику данной области. Это, в частности, связано со следующими фундаментальными результатами теории обучения и распознавания образов:

1) Не существует свободных от контекста и проблемно-независимых критериев, показывающих предпочтение одного метода обучения или классификации перед другими. Преимущества алгоритма или множества алгоритмов могут выявиться вследствие природы исследуемой проблемы или распределения данных.

2) Не существует предпочтительного набора признаков для представления шаблонов.

Таким образом, при описании модели системы обнаружения вторжений как системы распознавания образов необходимо отделять понятия, описывающие предметную область от понятий, применяющихся в теории обучения и распознавания образов. Как следствие данного положения вводится множество аксиом, используемых в системе обнаружения вторжений. Под аксиомами понимается использование в системе некоторого подмножества эвристик, описывающих предметную область, истинность которых не ставится под сомнение. В качестве примеров аксиом можно ввести следующие положения:

- статистические характеристики множества данных, описывающего атаки, существенно отличаются от статистических характеристик данных, представляющих нормальное поведение (аномальность редких событий, малая плотность в пространстве аномальных событий и т.д.);

- поведение пользователя стационарно;

- в системе, в которой используется система обнаружения вторжений введена нормативная политика безопасности.

Анализ аксиоматики, используемой системой обнаружения вторжений, может показать ее ограничения, связанные с невозможностью обеспечения истинности аксиом в конкретной вычислительной системе.

Предлагаемая модель имеет следующие преимущества:

1). Позволяет ввести в модель положения аксиоматики предметной области и положения теории систем обнаружения вторжений.

2). Дает возможность сравнивать на уровне модели системы обнаружения вторжений, построенные на основании различных принципах обнаружения.

3). Предоставляет математический аппарат для перенесения фундаментальных результатов, полученных в рамках одних методов обнаружения для использования в рамках других методов обнаружения вторжений.

Костин А.А., Молдовян Н.А., Фаль А.М.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
Украина, Киев, Институт кибернетики им. В.М. Глушкова НАН Украины
О РЕАЛИЗАЦИИ ПРОТОКОЛОВ СЛЕПОЙ И КОЛЛЕКТИВНОЙ ПОДПИСИ
НА ОСНОВЕ СТАНДАРТОВ ЦИФРОВОЙ ПОДПИСИ**

Новым типом криптографических протоколов являются протоколы слепой коллективной электронной цифровой подписи (ЭЦП), которые имеют перспективы практического использования для обеспечения анонимности в системах тайного электронного голосования или в системах электронных денег. Ввиду того, что в настоящее время отсутствуют официально рекомендованные стандарты на реализацию протоколов слепой подписи, коллективной подписи и слепой коллективной подписи, возникает актуальная для практики задача разработки протоколов таких типов на основе имеющихся стандартов ЭЦП.

В настоящей работе выполнено исследование возможности реализации протоколов слепой коллективной подписи на основе известных стандартов ЭЦП. В случае американских стандартов DSA и ECDSA и корейского стандарта KCDSA не удалось найти подходов к построению приемлемых вариантов протоколов слепой подписи и протоколов коллективной подписи. Это обусловлено спецификой применяемых уравнений генерации и проверки ЭЦП в этих стандартах, которые не позволили расширить функциональность этих стандартов без внесения изменений в их базовую схему построения алгоритмов ЭЦП. Стандарты России ГОСТ Р 34.10–94 и ГОСТ Р 34.10–2001, стандарт Украины ДСТУ 4145–2002 и стандарт Беларуси СТБ 1176.2–99 оказались подходящими для реализации упоминавшихся типов протоколов, включая протокол слепой коллективной подписи. Протоколы коллективной ЭЦП были построены на основе механизма свертки индивидуальных параметров генерируемых каждым пользователем, участвующим в формировании общей разделяемой ЭЦП. При этом для каждого из стандартов, используемых для задания базовой схемы формирования ЭЦП, можно показать, что стойкость протокола сводится к стойкости используемого стандарта ЭЦП, поэтому предлагаемые варианты протоколов представляются безопасными.

Реализация протоколов слепой подписи на основе стандартов ГОСТ Р 34.10–94, ГОСТ Р 34.10–2001, ДСТУ 4145–2002 и СТБ 1176.2–99 имеет существенные отличия, включая отличия по числу генерируемых случайных чисел, используемых для задания «ослепляющих» множителей. В случае стандарта СТБ 1176.2–99 реализация протокола слепой подписи потребовала использования двух случайных чисел и оказалась весьма близкой к общей схеме построения слепой подписи на основе алгоритма ЭЦП Шнора. В случае российских стандартов реализация протокола слепой подписи, обеспечивающего надежную анонимность, потребовала использования четырех случайных значений и существенно другого подхода к построению протокола. Все стандарты, допускающие реализацию слепой подписи и коллективной подписи, позволили также реализовать и протокол слепой коллективной подписи. Протоколы последнего типа ранее не предлагались.

Результаты выполненного исследования показали принципиальную возможность расширения функциональности ряда национальных стандартов ЭЦП, что представляет интерес для практической информатики.

Работа поддержана грантом РФФИ № 08–07–00096–а.

Костина А.А., Молдовян Д.Н., Савчук М.Н.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
Украина, Киев, Институт кибернетики им. В.М. Глушкова НАН Украины
О ПОСТРОЕНИИ СХЕМ ОТКРЫТОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ И КОММУТАТИВНЫХ
ШИФРОВ НА ОСНОВЕ НЕКОММУТАТИВНЫХ КОНЕЧНЫХ ГРУПП**

Ряд криптографических протоколов используют коммутативные функции шифрования. Наиболее широко известные коммутативные функции шифрования задаются криптосистемой RSA, в которой вычисления ведутся по модулю, равному произведению двух больших простых чисел, и алгоритмом Полига-Хеллмана (патент США № 4 424 414), в котором вычисления ведутся по простому модулю. При этом в приложениях, существенно использующих свойство коммутативности, в случае криптосистемы RSA потребуется использовать одно и то же значения модуля, по которому выполняются операции возведения в степень, что ведет к тому, что каждый пользователь должен держать в секрете как экспоненту расшифрования, так и экспоненту зашифрования. Это приводит к тому, что RSA становится идентичной алгоритму Полига-Хеллмана. Для обеих функций коммутативного шифрования достаточная криптостойкость обеспечивается при длине модуля, равной 1024 бит и более.

В настоящем сообщении предлагается построение алгоритмов коммутативного шифрования, основанных на вычислениях в некоммутативных группах, где задача дискретного логарифмирования в ее циклических подгруппах имеет предположительно экспоненциальную сложность. При этом имеется возможность использования трудной вычислительной задачи, имеющей сложность более высокую, чем сложность задачи дискретного логарифмирования в

циклической подгруппе. В случае схем открытого распределения ключей это достигается тем, что открытый ключ формируется как произведение степеней двух заданных некоммутативных элементов G и Z , обладающих большим значением порядка, причем, таких, что порядок каждого из них делится на достаточно большое простое число q . Секретным ключом являются степени x и w , в которые возводятся элементы G и Z . Открытый ключ вычисляется по формуле $Y = XU/X$, где $X = G^x$ и $U = Z^w$. Значение x задает автоморфизм, отображающий циклическую подгруппу, генерируемую элементом Z в другую циклическую подгруппу с тем же значением порядка. При этом из подгруппы-образа известным является только один элемент, а именно, элемент Y . Поэтому условия задачи дискретного логарифмирования в подгруппе-образе связаны с выбором значения x , что не позволяет свести вычисление секретного ключа, представляющего собой пару чисел (x, w) , к традиционной задаче дискретного логарифмирования. Коммутативный шифр на основе некоммутативных конечных групп предлагается строить на основе формулы шифрования вида $C = X(M^w)/X$, где $X = G^x$, M – шифруемое сообщение. Секретным ключом является пара чисел (x, w) . Достоинством такого шифра является достаточно высокое быстродействие, а недостатком – необходимость представления сообщений в виде элементов некоммутативной группы. В качестве некоммутативных групп могут быть использованы конечные группы матриц и конечные группы векторов над конечным полем.

Работа поддержана грантом РФФИ № 08–07–00096–а.

Котенко И.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПОСТРОЕНИЕ И ПОДДЕРЖКА ФУНКЦИОНИРОВАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ
ЗАЩИТЫ ИНФОРМАЦИИ**

Используемым в настоящее время подходам к защите присущ целый ряд недостатков и, как показывают исследования, они оказываются не в состоянии эффективно решать задачу противодействия современным сетевым атакам и вредоносному ПО. Эти недостатки обусловлены, в том числе, неразвитыми механизмами противодействия защитным средствам злоумышленников, недостаточными возможностями по обнаружению вредоносных проявлений и прогнозированию развития ситуации, неадекватными механизмами определения уязвимостей, анализа рисков и определения уровня защищенности, слабыми возможностями по мониторингу состояния компьютерных сетей и систем, негибкостью механизмов управления защитой и адаптацией к изменению условий функционирования.

В соответствии с современными представлениями перспективная система защиты распределенных компьютерных систем должна представлять собой взаимосвязанную, многоэшелонированную и непрерывно контролируемую систему, способную оперативно реагировать на удаленные и локальные компьютерные атаки и несанкционированные действия (НСД), накапливать знания о способах противодействия, обнаружения и реагирования на атаки и НСД и использовать их для усиления защиты.

Поэтому одним из центральных вопросов исследований в области защиты информации должна быть разработка эффективных моделей и методов построения и поддержки функционирования интеллектуальных систем защиты информации, в том числе моделей и методов проактивной защиты, обеспечивающих сбор необходимой информации, анализ защищенности, мониторинг состояния сети, обнаружение атак, противодействие их реализации, введение злоумышленника в заблуждение, а также интегральной оценки состояния сети, управления защитными механизмами и адаптации политик безопасности и компонентов защиты. Предполагается, что проактивное обнаружение и реагирование против сетевых атак и вредоносного программного обеспечения (ПО) основывается на автоматических механизмах, которые используют информацию об “истории” анализируемых сетевых событий и прогнозе будущих событий, а также автоматической подстройке параметров защиты к текущему состоянию конфигурации сети.

В докладе рассматривается целостная концепция построения и поддержки функционирования интеллектуальных систем защиты информации и несколько групп подзадач разработки отдельных компонентов такой системы, необходимых для реализации эффективного противодействия современным сетевым атакам и вредоносному ПО: гибридном многоагентном моделировании компьютерного противоборства, реализации адаптивного управления верифицированными политиками безопасности, анализе защищенности ресурсов компьютерных сетей и систем, а также проактивном мониторинге состояния и поведения защищаемых ресурсов на базе интеграции различных методов интеллектуального анализа данных.

Работа выполнена при финансовой поддержке РФФИ (проект №07–01–0547), программы фундаментальных исследований ОИТ РАН (контракт №3.2/03), Фонда содействия отечественной науке и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST (контракт № 021186–2) и других проектов.

Кузнецов И.В., Примакин А.И.

Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД

России, Санкт-Петербургский университет МВД России

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ АКУСТИЧЕСКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ОБЕСПЕЧЕНИИ ЗАЩИТЫ ОБЪЕКТОВ РАЗЛИЧНОГО НАЗНАЧЕНИЯ

В настоящее время развитие акустических информационных технологий сформировало техническую базу для прорыва в задаче обнаружения объектов из различных твердых материалов в укрывающих средах. Другой составляющей этого процесса стали достижения в понимании механизмов согласования акустических сигналов со слуховым анализатором человека (САЧ). По существу, задача акустической информационной технологии заключается в исследовании новых моделей сигналов, каналов, помех, правил излучения и обработки сигналов. Она из задач сугубо научных трансформировалась в задачи технические. Действительно, последние достижения акустических технологий практически позволили эффективно использовать слуховой аппарат человека, созданный природой, который до настоящего времени не имеет, и по мнению ученых акустиков, не будет иметь технического аналога.

В настоящее время поставлена и решена научно-техническая задача по разработке методов согласования сигналов от поискового элемента со слуховым анализатором человека. В основе существующего метода обнаружения объектов из различных твердых материалов в укрывающих средах положен метода синхронного детектирования с разверткой, выход которого подключается к слуховому анализатору человека. Повышение помехоустойчивости метода обнаружения решается в согласовании, с одной стороны, увеличения времени интегрирования, с другой стороны, согласования со слухом человека.

Разработанный метод согласования САЧ со слуховым каналом показал:

- для повышения эффективности метода синхронного детектирования в поисковых системах, целесообразно применять специальные модулирующие сигналы, позволяющие получить более полную (в широком диапазоне частот) информацию о признаках объекта поиска и более полного учета среды;
- для повышения эффективности поисковых систем предлагается сигналы с выхода синхронного детектора представлять согласованными с областью эффективного приема САЧ. Для реализации процедуры согласования предлагается вместе с операцией гетеродинирования применять операцию транспонирования низкочастотных сигналов;
- проведена оценка эффективности САЧ при обнаружении на фоне шумовой помехи сигналов эллиптического и гиперболического типов;
- акустический эксперимент, проведенный для оценки области эффективного приема САЧ, показал, что область эффективного приема при восприятии частотно-модулированных сигналов гиперболического типа лежит в диапазон количество волн сигнала от 32 до 64;
- расчеты показали, что процедура согласования сигналов с областью эффективного приема позволит поднять помехоустойчивость системы обнаружения.

В целом, разработанные акустические технологии обеспечивают получение информационного превосходства акустических средств нового поколения по обнаружению объектов в укрывающих средах.

Все это позволяет повысить эффективность поисковых приборов по обнаружению объектов из различных твердых материалов в укрывающих средах.

Лаврентьева Ю.И.

**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»
ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ В ЗАЩИТЕ ИНФОРМАЦИИ**

В последнее время вирусные атаки стали слишком интенсивными, и никто не может чувствовать себя в безопасности; страдают как физические лица, так и целые организации. Использование антивирусов не всегда решает проблему, – если вы администрируете локальную сеть крупной организации, персонально для вас может быть написан специальный вирус, проходящий сквозь антивирусные заслоны. Кроме того, стоит отметить, что основная масса современных вирусов проникает через глобальную сеть в целевые компьютеры самостоятельно, не требуя никаких действий со стороны пользователя. В связи с этим, было бы очень полезно не просто давать отпор вирусам, а изучать принципы их распространения с тем, чтобы уметь прогнозировать их поведение.

Ежедневно в глобальной сети появляется большое количество новых вирусов, в то время как производители антивирусного программного обеспечения (ПО) всегда находятся на шаг позади и вынуждены бороться с уже существующими вирусами. Однако, владея знанием о принципах распространения вирусов и умея прогнозировать их поведение, можно будет предотвращать не последствия неизвестной вирусной атаки, а непосредственно сам факт проникновения неизвестного нового вируса на компьютер.

От вирусной атаки не защищен никто. Они способны навредить не только физическим лицам, которые рискуют потерять со своего персонального компьютера личную информацию, но и огромные корпорации, рискующие не просто большими финансовыми средствами, но даже собственным банкротством.

Использование статистических методов при имитационном моделировании сети интернет позволит спрогнозировать влияние того или иного вируса на различные сегменты глобальной сети, что в, свою очередь, может помочь как разработчикам антивирусного ПО, так и простым администраторам корпоративных сетей защищать наиболее уязвимые с точки зрения статистики места.

В докладе представлены методы имитационного моделирования, позволяющие улучшить способы защиты от вирусной атаки.

Марков Я.А., Калинин М.О.

Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ОБНАРУЖЕНИЕ МОДИФИЦИРОВАННЫХ АТАК НА ОСНОВЕ АЛГОРИТМА СРАВНЕНИЯ
ГЕНЕТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Защищаемая информационная система представляется как множество взаимодействующих сущностей. Взаимодействие называется информационным, если его целью и основным содержанием является изменение имеющейся информации хотя бы у одной из них. Информационное взаимодействие осуществляется в результате разрешения и выполнения т.н. команд, составляющих множество C . Множество возможных взаимодействий в дискретных системах конечно и определяется семантикой системы и заданным уровнем абстракции (например, на системном уровне ОС Unix определены взаимодействия "чтение", "запись" и "исполнение"). Команды выполняются при истинности заданных в системе условий доступа (например, когда в ячейке матрицы доступа соответствующей данным субъекту и объекту разрешен данный вид взаимодействия). При срабатывании условий и выполнении команд в результате информационного взаимодействия система выполняет переход из одного состояния в другое. Таким образом, зная, что в интервале времени $[t_1, t_2]$ выполнялись команды $C_1, C_2, \dots, C_n, C_i \in C, i \in \mathbb{Z}^+$, указанной последовательности, можно определить траекторию системы. Траектория является небезопасной, если при выполнении последовательности команд система становится небезопасной в терминах заданных условий при выполнении некоторой команды $C' \in C$. Атака, т.е. негативное воздействие на защищаемую систему, которое выводит ее из безопасного состояния вследствие реализации небезопасной траектории, всегда является элементом небезопасной последовательности команд. Задача обнаружения атаки состоит в том, чтобы, анализируя цепочку выполняющихся команд, выявить, присутствуют ли в ней последовательность команд, характерная для той или иной атаки.

Современным методом обнаружения атак является сопоставление текущей последовательности команд с имеющимися образцами атак (сигнатурный метод). Его недостатками являются:

- неограниченный рост базы сигнатур. Размер базы сигнатур определяется количеством атак, которое в последние годы растет экспоненциально, что определяет будущую неэффективность данного метода;
- защита от ограниченного множества атак. Система защищена только от тех атак, которые указаны в базе сигнатур;
- защита от известного множества атак. Система защищена от атак, которые проанализированы и занесены в актуальную базу. Для этого необходимы постоянный мониторинг нарушений и распространение обновленных баз;
- неэффективность при модифицированных атаках, команды которых совпадают с точностью до последовательности, но отличаются количеством команд.

Для устранения указанных недостатков авторами предлагается применять для обнаружения атак метод сравнения последовательностей, используемый в биоинформатике для сравнения ДНК. Метод заключается в определении схожих участков у нескольких последовательностей путем применения алгоритма выравнивания. Растягивая последовательности относительно друг друга и вставляя в них пустые участки, становится возможным получить оптимальное расположение последовательностей по отношению друг к другу, при котором их сходство максимально. В зависимости от особенностей разделяют локальное и глобальное выравнивания. Глобальное выравнивание растягивает меньшую последовательность вдоль большей. Локальное выравнивание, более известное как алгоритм Смита-Уотермана, применяется, когда длина одной последовательности значительно меньше, чем длина другой. Для обнаружения атак наиболее применим локальный метод, поскольку текущая последовательность команд значительно превышает длину последовательности команд атаки.

Применение алгоритма Смита-Уотермана для решения задачи обнаружения атак, позволяет не только обнаруживать атаки, которые отсутствуют в базе сигнатур, но и модифицированные сигнатурные атаки. Также становится возможным формировать приоритеты команд, встречающихся в

последовательностях, и указывать, какие из них являются более опасными, какие не оказывают влияния на безопасность системы, что облегчает задачу построения вариативных программных датчиков атак в системах управления информационной безопасностью.

Маховенко Е.Б., Павлов Д.С.

Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
СПОСОБЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ЖУРНАЛОВ В БАНКОВСКИХ ПРИЛОЖЕНИЯХ

Журналы работы приложения в процессинговом центре банка могут содержать персональные данные о клиентах, их счетах, объемах транзакций и другую информацию, которая может позволить злоумышленникам подделать карту клиента или иным образом завладеть чужими финансовыми средствами.

Шифрование журналов приложений позволяет защитить информацию от утечки и модификации. Шифрование предлагается производить не как шифрование абстрактного байтового потока данных (файла), а с учетом структуры и характера информации.

Записываемый журнал приложения предлагается разбить на записи (сообщения журнала), каждая из которых будет обладать набором полей в зависимости от типа приложения. Такими полями могут быть текст сообщения, подробный текст, время, ассоциированные данные и т.д. Для каждого типа поля определяются правила преобразования в бинарные данные. Перед записью в журнал сообщение преобразуется в последовательность байтов, например, при помощи схемы тэг (определяет тип поля) – длина – значение.

Для обеспечения большей криптостойкости следует применить алгоритм сжатия данных. Для журналов приложения достаточно использовать простейший алгоритм сжатия, предполагающий исключение одинаковых значений поля для записей, идущих подряд. Так, например, одна и та же дата сообщения может повторяться в журнале большое количество раз. Такой подход при использовании схемы тэг–длина–значение можно реализовать за счет использования нулевой длины значения или отсутствия значения в записи.

Кроме применения алгоритмов сжатия следует также сохранять поля записи в нефиксированном порядке, так как в противном случае возможно повторение первого байта (тэга первого поля) для множества записей.

Применение ассиметричного шифрования позволяет защитить ранее зашифрованные журналы от раскрытия в случае получения доступа к серверу. В этом случае не произойдет и компрометация закрытых ключей, так как на сервере хранятся только открытые компоненты ключей. Зашифрование данных производится на открытых ключах авторизованных для доступа к данным журналов сотрудников банка и, возможно, службы поддержки поставщика программного обеспечения. Использование ключа службы поддержки позволит решить проблему безопасной передачи журналов в службу поддержки для разрешения проблем в работе ПО.

Ассиметричное шифрование предлагается использовать в комбинации с симметричным алгоритмом, который будет шифровать непосредственно данные журнала. Ключ шифрования симметричного алгоритма вырабатывается случайным образом и подлежит зашифрованию под каждым из ключей шифрования пользователей.

Такая схема позволяет защитить информацию журнала от неавторизованного просмотра, как сотрудниками банка, так и сервисными службами, в которые, возможно, попадает носитель информации при ремонте ЭВМ.

Для защиты от модификации данных журнала предлагается использовать код аутентичности сообщения с использованием случайного ключа, значение которого зашифровано совместно с ключом шифрования данных. Таким образом, авторизованные пользователи будут иметь возможность проверить целостность данных журнала, а изменение содержимого записи без знания ключа кода аутентичности сообщения будет невозможно. С использованием такого подхода возможно также разделить и полномочия пользователей в модификации данных после записи журнала.

Кроме того, для защиты от вставки записи в середину следует применить схему, аналогичную гаммированию в шифрах, при которой значение кода аутентичности сообщения для предыдущей записи учитывается в вычислении кода для текущего сообщения журнала. Для этих же целей следует использовать симметричный шифр в режиме гаммирования.

Для защиты от угрозы подмены открытого ключа шифрования журналов и от добавления ключа злоумышленника к конфигурации приложения используются сертификаты с электронной цифровой подписью, которые выдаются для каждого ключа шифрования журналов. Возможно использовать два подхода, как по отдельности, так и совместно. Первый подразумевает использование удостоверяющего центра (СА) внутри банка. Второй заключается в том, что сертификаты ключам выдаются поставщиком программного обеспечения, а модуль, ведущий записи журналов, содержит внутри кода значение открытого ключа подписи поставщика ПО.

Атака при использовании первого подхода возможна только в случае подмены в конфигурации приложения адреса СА и организации злоумышленником своего СА, что много сложнее подмены

ключа, а кроме того, может быть обнаружено в сети при помощи системы обнаружения вторжений. Нарушение безопасности при использовании второго подхода возможно только при нарушении целостности ПО, ведущего записи журналов, что равносильно внедрению в ПО вредоносного модуля, передающего все данные приложения злоумышленнику.

Если вышестоящим ключом в цепочке сертификатов ключа шифрования сотрудника банка является ключ поставщика ПО, то создание и обновление ключей шифрования журналов будет достаточно сложной процедурой, так как потребуются совместная работа двух организаций. Поэтому в цепочку сертификатов удобно ввести и промежуточный сертификат, выдаваемый службой банка авторизованным сотрудникам. Тогда создание, обновление и отзыв ключей пользователей будет производится в рамках одной организации без привлечения поставщика ПО.

Недостатками предлагаемого метода записи журналов является невозможность дописывать данные в конец ранее закрытого приложением журнала, требуется создание нового файла, а также необходимость чтения журнала только от начала к концу (случайный доступ невозможен) вследствие использования MAC-chaining, гаммирования и сжатия. Однако необходимости в такой функциональности, как запись в конец закрытого журнала, в сложных системах обычно нет.

Применение такого подхода позволяет защитить журналы от несанкционированного доступа как извне, так и со стороны сотрудников банка. Выполняются следующие требования стандарта PCI-DSS: о приведении к нечитаемому виду номеров карт клиентов; о защите от внесения изменений в журналы регистрации событий; о разрешении просмотра журналов регистрации событий только тем сотрудникам, которым это необходимо.

Появляется возможность для безопасной передачи журналов в службу поддержки поставщика ПО, а также (в соответствии с требованием о ежедневном просмотре журналов событий для всех компонентов) в систему сбора и анализа событий. Упрощается и разработка ПО для контроля целостности и генерации предупреждений в случае нарушения целостности журналов.

Мельник И.А., Примакин А.И.

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

ОСНОВЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ОПАСНОСТИ ЕЕ УТЕЧКИ ПО КАНАЛАМ ПОБОЧНЫХ ИЗЛУЧЕНИЙ И НАВОДОК

Методы проникновения в сеть и последующей кражи информации достаточно хорошо известны. Наиболее действенным является внедрение в систему программы-закладки. В зависимости от поставленных целей программа-закладка может, например, перехватывать пароли пользователей или по определенному критерию находить необходимую информацию на жестких дисках. В дальнейшем собранная информация отправляется по электронной почте на заранее обусловленный адрес. Соответственно, все системные администраторы принимают определенные меры по пресечению подобных попыток. Это заставляет взломщиков придумывать новые методы проникновения в сеть или усовершенствовать известные. Есть два самых трудных для взломщика момента: установка программы-закладки («троянского коня») и передача разведанной информации. В эти моменты разведывательную деятельность проще всего обнаружить. Причем, чем больше объем внедряемой программы или объем передаваемых такой программой данных, тем выше вероятность того, что разведывательная деятельность будет обнаружена и пресечена. Необходимость скрывать факт передачи сообщения неминуемо приводит к внедрению злоумышленниками методов стеганографии (скрытной передачи данных).

Давно известно, что утечка информации может происходить и по каналам ПЭМИН – побочных электромагнитных излучений и наводок. Эти каналы неудобны только тем, что они неуправляемы. Ученым Кембриджа пришла идея использовать в качестве канала передачи данных побочные излучения компьютера, но только сделать этот канал управляемым. Работа над этой идеей привела к рождению технологии Soft Tempest – технологии скрытой передачи данных по каналу побочных электромагнитных излучений с помощью программных средств.

Soft Tempest атака позволяет с помощью специальной программы-закладки, внедряемой с использованием стандартной техники применения «вирусов», «червей» и «троянцев», искать необходимую информацию в компьютере и передавать ее путем модуляции изображения монитора. Принимая побочные излучения монитора можно выделить полезный сигнал и таким образом получить секретную информацию, хранящуюся в компьютере – пароли, письма, документы. Эта технология получила и второе название: ПЭМИН-вирус.

Однако самый лучший метод скрытой передачи информации – это передавать ее по каналу, который не охвачен контролем. В этом плане конечно лучше всего передавать разведанную информацию по радио излучениям компьютера. Но существуют и более простые способы управления излучением компьютера, чем вывод информации на монитор. Проведенный нами анализ показал, что обращение к любому устройству и даже к любому незадействованному порту вызывает появление побочных излучений на определенных, характерных для данного порта, частотах и с определенной

мощностью. Поэтому «ПЭМИН-вирусы» могут существовать во множестве вариантов, в зависимости от того, какое конкретно устройство компьютера выбрано для управления излучением.

Был проведен эксперимент с программой-закладкой, имитирующей передачу данных в последовательный порт, который демонстрирует, что возможности метода передачи информации путем управления излучением портов компьютера по скрытию факта ее передачи значительно шире, чем просто использование неконтролируемого канала связи.

Современные методы разведки с использованием управления побочными излучениями компьютера позволяют разведать всю информацию, хранящуюся или обрабатываемую в компьютере и скрытно передать ее, не оставляя следов о местонахождении разведчика. Единственный метод защиты от утечки информации по каналам ПЭМИН – это применение компьютеров в защищенном исполнении. Причем качество защиты обязательно должно быть подтверждено лабораторией, имеющей соответствующий сертификат на право выполнения таких работ.

Мирин А.Ю., Заболотный А.П., Молдовян У.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПРОТОКОЛ КОЛЛЕКТИВНОЙ ПОДПИСИ НА ОСНОВЕ СЛОЖНОСТИ ЗАДАЧИ ФАКТОРИЗАЦИИ**

Протоколы, в которых формируемая электронная цифровая подпись (ЭЦП) относится к нескольким субъектам, подписавшим документ, известны как схемы мультиподписи (multisignature schemes). Для построения таких протоколов используются вычислительно сложные задачи факторизации чисел специального вида и нахождения дискретного логарифма в конечных группах большого простого порядка. Недостатком многих известных протоколов является то, что в них подпись формируется последовательно, что приводит к тому, что на промежуточных этапах генерации (также и при проверке подлинности) возникают цифровые подписи, относящиеся к урезанному подмножеству подписывающих. Это делает потенциально возможной реализацию некоторых специфических атак на такие протоколы. Вариантом схем мультиподписи являются протоколы коллективной подписи [Автоматика и телемеханика. 2008. № 7. С.157–169], основанные на сложности задачи дискретного логарифмирования. Достоинством схем коллективной подписи является параллельность формирования коллективной ЭЦП и ее внутренняя целостность, которая означает практическую невозможность манипуляций с коллективной подписью и с промежуточными результатами вычислений, которые являются доступными более чем одному пользователю, участвующему в протоколе. Эти свойства коллективной ЭЦП устраняют ряд типов потенциальных атак, а их применение для подписания контрактов предоставляет собой удобный и простой способ решения проблемы одновременного подписания контракта. Вариант коллективной подписи, названный композиционной подписью, позволяет решить проблему одновременного подписания пакета контрактов для случая, когда различные контракты подписываются различными множествами подписывающих.

В настоящем сообщении предлагается построение схем коллективной подписи, обладающей внутренней целостностью и параллельностью формирования, на основе сложности задачи факторизации. Это расширяет класс примитивов, которые могут быть использованы для построения схем коллективной ЭЦП, а также протоколов коллективной ЭЦП, взлом которых требует одновременного решения двух независимых вычислительно трудных задач, которые предложены в работе [Безопасность информационных технологий. 2008, № 2, стр. 79–85]. Предполагается, что в протоколе участвует доверительный центр, генерирующий число n , равное произведению двух больших простых чисел, и значение степени k , которое является сравнительно малым простым числом и используется для вычисления открытого ключа путем возведения в эту степень личного секретного ключа. При этом после формирования числа n его делители уничтожаются, а само это число используется как параметр схемы коллективной ЭЦП, которая строится по аналогии со схемами, основанными на сложности вычисления корней степени дискретного логарифмирования [Вестник СПбГУ. Сер. 10, 2008. Вып. 1. С. 100–105]. k , по модулю, равному $p = N(k^2) + 1$, где N – четное число.

Работа поддержана грантом РФФИ № 08–07–00096–а.

Морозова Е.В., Молдовян Д.Н., Пилькевич С.В.

**Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Вектор»,
Военно-космическая академия им. А.Ф. Можайского
ВАРИАНТЫ РЕАЛИЗАЦИИ КОММУТАТИВНОГО ШИФРОВАНИЯ**

В ряде криптографических протоколов, имеющих значение для практической информатики, применяются алгоритмы коммутативного шифрования, обеспечивающих достаточную производительность, простоту аппаратной реализации и высокую стойкость. Этим требованиям в достаточной степени удовлетворяет алгоритм Полига-Хеллмана (патент США № 4 424 414), однако практика для ряда приложений выдвигает требования повышения производительности криптографических протоколов, основанных на коммутативном шифровании.

В настоящем сообщении рассматриваются различные варианты реализации алгоритмов коммутативного шифрования, построенные по аналогии с алгоритмом Полига-Хеллмана и отличающиеся применением конечных полей различного типа. Показано, что использование векторных конечных полей позволяет получить наиболее высокое значение производительности коммутативного шифрования.

Предложенный недавно способ задания расширенных конечных полей, в которых операция умножения может быть эффективно распараллелена основан на идее представления элементов поля в векторной форме, т. е. в виде упорядоченного набора координат, значения которых являются элементами некоторого конечного поля (называемого базовым полем), и задания операции умножения с помощью процедуры, в которой каждая координата результирующего вектора вычисляется независимо. Последнее определяет возможность эффективного распараллеливания операции умножения. Поля с возможностью эффективного распараллеливания операции умножения можно назвать векторными полями. Векторные конечные поля представляют интерес для реализации алгоритмов эллиптической криптографии, алгоритмов электронной цифровой подписи, заданных над конечными группами невырожденных квадратных матриц, а также для реализации производительных алгоритмов коммутативного шифрования.

По сравнению с конечными полями других типов (простыми полями и полями многочленов) при заданном размере порядка Ω поля операция умножения в векторном поле имеет наиболее низкую временную сложность для широкого спектра различных типов вычислительных устройств, а также как при реализации умножения по модулю с помощью операций арифметического умножения и арифметического деления, так и при реализации умножения по способу Монтгомери. Кроме того, векторные поля обеспечивают возможность наиболее эффективной (по показателю, равному отношению производительности к затрачиваемым аппаратным ресурсам) параллельной реализации. Сформулированы требования к выбору характеристики p векторного поля для заданного значения размерности векторов. Показано, что нужные простые числа могут быть достаточно легко сгенерированы. При заданном размере Ω наличие простого делителя $q|\Omega$ максимального размера обеспечивается выбором значения p и степени расширения.

Работа поддержана грантом РФФИ № 08–07–00096–а.

Никитенков К.С.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
информационных технологий, механики и оптики
АСПЕКТЫ ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА**

Внедрение системы электронного документооборота (СЭД), многократно облегчает процесс обработки и хранения информации, а значит, повышает КПД бюрократической системы компании. Выгоду от применения такой системы подчеркивает использование её самым инертным к новшествам и самым мощным холдингом нашей страны – госсектором, который вышел на это поле с русским размахом, обеспечив существенную долю спроса. С другой стороны, СЭД создает новые риски; недостаточный уровень защиты обязательно приведет к новым угрозам конфиденциальности — желающих полазить в чужих документах достаточно.

Зачастую применение абстрактных средств защиты, непосредственно не связанных с основным процессом обмена документами, не обеспечивает достаточного уровня защиты. Различные изолированные инструменты безопасности, такие как шифрование данных или аутентификация пользователей создают возможность обеспечить определенный уровень защиты, но применение их отдельно от основных процессов документооборота существенно понижает этот уровень.

Устройства и алгоритмы защиты нужно полностью синхронизировать с документооборотом компании. В пользу этого говорит высокий уровень (в последнее время рост) внутренних угроз, связанных с хищениями информации персоналом компании. Само по себе обеспечение пользователей средствами защиты не является достаточным условием, необходим тщательный контроль использования этих средств. Со стороны внутренней безопасности конфиденциальный документ не является достаточно защищенным, а значит должны контролироваться и действия пользователей с ними. Если сопоставить два этих тезиса, то представить себе идеализированную систему защиты становится не так сложно: она должна вести контроль над любыми действиями пользователей с документами и обеспечивать конкретные механизмы безопасности в зависимости от конкретности случая. А значит, она должна быть ориентирована на документы.

В докладе акцентируется внимание на платформе IBM Lotus Notes и Domino, поскольку данный инструмент для групповой работы используется уже более полутора десятилетий. При правильной настройке системы безопасности он никогда не становился жертвой крупных атак и в практике применения никогда не демонстрировал существенных слабых мест. Об организации этого инструмента обеспечения групповой работы и заложенных в нем механизмах обеспечения безопасности имеется много публикаций.

В докладе анализируются: модель безопасности Notes/Domino; аутентификация и управление доступом к серверу; контроль доступа к базам данных (Access Control List);

– управление доступом к отдельным документам, система шифрования и управление настройками безопасности. Обсуждаются: безопасность почтовой системы; уязвимость LDAP-сервера Domino; вопросы безопасности Web-сервера Domino;

– настройка мониторинга событий, связанных с безопасностью и некоторые уязвимости Domino.

Новиков В.А., Дулин А.В.

**Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского
СРЕДСТВА СЕРТИФИКАЦИИ ПРОГРАММ С ИНТЕЛЕКТУАЛЬНЫМИ СВОЙСТВАМИ**

В условиях широкого применения и использования в защищённых информационных системах сетевых операционных систем, микрокода в аппаратной части средств защиты информации и общего программного обеспечения, стало недостаточным решение вопроса защиты от несанкционированного доступа, без решения вопроса защиты от воздействий на информацию с целью ее уничтожения, искажения и блокирования со стороны недеklarированных возможностей программ (НДВ).

Основная трудность состоит в том, что планируемые к внедрению и эксплуатируемые автоматизированные системы сбора, обработки и доведения информации сопряжены на разных логических уровнях с программным обеспечением (ПО) не прошедшим сертификационные испытания на отсутствие недеklarированных возможностей, к которым чаще всего относиться ПО импортного производства.

Специфика сертификации импортного ПО является отсутствие исходных текстов и сопровождающей документации. Наличие недеklarированных возможностей в таком ПО порождает уязвимости, от которых зависит надежность, производительность и безопасность функционирования систем в целом.

В докладе рассматривается подход поиска НДВ программ при отсутствии их исходных текстов и программной документации, основанный на обнаруженных SLD признаках недеklarированных программ.

Новизна предлагаемого подхода заключается в применении многомодельного исследования дизассемблированного кода. Многомодельное исследование построено, с учётом известных в разделах теоретического программирования состояний программ (статика, имитация, динамика), их свойств (структура, логика, вычислительные действия) и наиболее эффективного к применению математического аппарата (графы, схемы, сети) описывающего семантику программ на разных уровнях абстракции.

Указанный подход реализован в программном комплексе позволяющем выполнять имитационное моделирование дизассемблированного кода на различных уровнях абстракции позволяющем обнаруживать найденные и выявлять новые SLD признаки НДВ программ.

Пилькевич С.В.

**Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского
СОВРЕМЕННЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ**

Современный этап развития общества напрямую связан с ростом ценности информации, циркулирующей в цифровых системах связи и передачи данных. Наиболее действенным средством обеспечения конфиденциальности, целостности и аутентичности, передаваемых по каналам связи данных, являются криптографические протоколы.

Для выполнения возложенных на криптографический протокол функций, он должен отвечать набору обязательных требований, в число которых входят корректность, непротиворечивость, однозначность, полнота и ряд других.

К сожалению, используемые протоколы информационного взаимодействия очень редко удовлетворяют всем перечисленным требованиям. Поэтому любой недостаток протокола представляет собой уязвимость, наличие которой может использоваться для несанкционированного доступа к информации в компьютерной или телекоммуникационной сети.

В докладе предлагается классификация уязвимостей криптографических протоколов по следующему типу: криптографическая, алгоритмическая и программная уязвимости.

Криптографические уязвимости выявляются путем применения известного математического аппарата (математический анализ, теория чисел, теория вероятностей, теория сложности и др.), которым располагает криптология. Устранение алгоритмических уязвимостей предполагает задействование формальных методов анализа криптографических протоколов, включающих в себя такие направления как специализированные языки и средства испытаний, экспертные системы, применение формальных логик, а также анализ криптографических протоколов на основе изучения их алгебраических свойств. В результате, разработанные и отлаженные правила обмена

последовательностями сообщений, их формат, правила обмена и ключевые параметры обязательно отражаются в спецификации протокола информационного взаимодействия.

Необходимо отметить, что применение формальных методов анализа производится на абстрактном уровне этапов проектирования, разработки и совершенствования криптографического протокола и не предусматривает выявления ошибок конкретной реализации, т.е. программных уязвимостей. Фактически, минимизация дефектов криптографических алгоритмов и логики их применения, в рамках того или иного криптографического протокола, осуществляется в рамках таких мероприятий разработки как спецификация и последующая верификация.

Для выявления программных уязвимостей, традиционно, применяется тестирование свойств безопасности криптографического протокола, основной целью которого является верификация корректности реализации по отношению к спецификациям. При этом основной акцент делается на тестировании реализации на соответствие её функциональным спецификациям.

Таким образом, для выявления программных уязвимостей криптографических протоколов, видится целесообразным дополнительно:

1) использовать методы эвристического анализа протоколов, позволяющих на абстрактном уровне оценить меру риска применяемых защитных мер;

2) осуществлять тестирование конкретных реализаций протоколов по отношению к конфликтным ситуациям, возникающим при обработке измененных, по какой-либо причине, последовательностей сообщений протоколов.

Платонов А.А.

**Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского
К ВОПРОСУ РАСПОЗНАВАНИЯ ПРИЗНАКОВ МОДИФИКАЦИИ ИСПОЛНЯЕМОГО
КОДА ПРОГРАММ В ПРОЦЕССЕ ИХ ФУНКЦИОНИРОВАНИЯ**

На современном информационно-вычислительном этапе человеческой деятельности, который характеризуется компьютеризацией процессов добыwania, обработки и хранения информации, остро встает вопрос о защите программного кода, являющегося основой любого исполняемого процесса. Процессы вычислений протекают на любом автоматизированном рабочем месте локальной вычислительной сети государственного или частного характера, что обуславливает важную роль, поставленного вопроса.

При рассмотрении этого вопроса необходимо отметить существующие в настоящее время уязвимости и угрозы, которые преднамеренно или случайно могут влиять на структуру исполняемого кода и недостатки средств контроля функциональной целостности программ.

Все существующие методы контроля целостности ориентированы на два состояния, в котором может находиться исполняемая программа: непосредственное выполнение программы (динамика) и хранение в файловой системе (статика). Первые методы направлены на контроль доступа к адресному пространству процесса, что обуславливает большую зависимость от окружающей вычислительной среды (функции операционной системы). Методы контроля статического положения программы основаны на эталонировании с помощью контрольных сумм. К недостаткам контрольных сумм можно отнести:

- невозможность контроля быстро изменяемого во времени исполняемого кода программ;
- отсутствие семантической составляющей в процессе контроля, что не дает анализировать вид искажения;
- теоретически существует возможность нахождения коллизий, несмотря на сложность используемой хеш-функции.

Таким образом, можно говорить о том, что в настоящее время существует проблемная ситуация, состоящая в противоречии между потребностью различных органов управления в корректном функционировании критически важных программных комплексов и отсутствием эффективных методов по распознаванию признаков нарушения функциональной целостности программ.

При разрешении этого противоречия необходимо построение методики, лишенной вышеуказанных недостатков. В этом случае методика должна быть универсальной, то есть независимой от состояния программы (выполнение или хранение).

В качестве основы такой методики предлагается использование структурированной модели взаимодополняющих семантик. Она включает в себя денотационный, аксиоматический и операционный уровень представления программы. Этот вид представления программы имеет несомненные достоинства в сравнение с битовыми блоками, используемыми для вычисления контрольных сумм. Такая модель позволяет независимо от окружающей вычислительной среды, а также от постоянно меняющихся данных в процессе функционирования программы, контролировать потоки управления и потоки данных. Эти свойства, предлагаемой модели, позволяют снизить риск незаметного изменения исполняемого кода.

Платонов В.В., Цвилик Н.В., Цвилик А.С.

Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
АНАЛИЗ АЛГОРИТМОВ ОБУЧЕНИЯ И ТИПОВ НЕЙРОННЫХ СЕТЕЙ ДЛЯ
ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ

Рассматриваются возможности применения технологии нейронных сетей (НС) в системах обнаружения вторжений (СОВ), а также дается оценка преимуществ и недостатков данной технологии.

Одним из важных узлов СОВ является модуль анализатора событий, который может быть реализован множеством различных способов. В работе рассматривается представление модуля анализатора в виде многослойной нейронной сети. Такой подход имеет ряд важных преимуществ перед другими типами анализаторов:

- возможность анализа искаженных или неполных данных;
- возможность анализа, классификации и кластеризации данных, которые встречаются впервые;
- возможность обрабатывать данные в нелинейном режиме;
- быстрота обработки данных и реакции нейронной сети;
- возможность прогнозирования событий;
- самообучение.

Эксперименты показали, что указанные преимущества нейронных сетей во многом нивелируют их недостатки. Для решения задачи синтеза нейронной сети для реализации функций анализатора был выбран ряд наиболее часто используемых типов сетевых протоколов: IP, ICMP, TCP, UDP, HTTP. Для каждого из выбранных протоколов был сформирован набор параметров, на основе которого нейронная сеть должна проводить анализ сетевого трафика. Сформированный набор обладал некоторой избыточностью, которая использовалась для работы других модулей СОВ.

Такой подход значительно усложнил процесс первичного построения сети и замедлил процесс обучения.

Для проведения экспериментов потребовалось разработать модуль подготовки исходных данных для преобразования их к виду, который удобен для восприятия сетью. Параметр считался пригодным только в том случае, если среди данных, представленных в обучающей выборке, присутствуют минимум два уникальных значения для данного параметра. Эксперименты показали, что для адекватного процесса обучения (на выходе нейронная сеть правильно распознавала от 92 до 100% атак) необходимо, чтобы обучающие данные содержали приблизительно 10% аномальных пакетов от их общего числа.

Поскольку не существует формальных обоснований того, какой тип нейронных сетей должен быть положен в основу реализации СОВ, поэтому различные типы нейронных сетей проверялись экспериментально. Тестирование различных конфигураций нейронных сетей проводилось с использованием программы NeuroShell 2.0, на стандартных настройках которой проверялась эффективность различных типов нейронных сетей. В результате была выбрана архитектура многослойного перцептрона. В результате обучения нейронной сети типа многослойный перцептрон с помощью алгоритма обратного распространения ошибки были получены достаточно хорошие результаты, например, погрешность по обучающей выборке статистических значений составила 0,00; погрешность по тестовой статистической выборке - 0,017 (1.7%); погрешность по обучающей выборке значений полей - 0,00; погрешность по тестовой выборке, содержащей данные о значениях полей: 0,02 (2%).

Для обнаружения атак отказа в обслуживании (DoS атаки, удаленное сканирование) были построены отдельные модули, входными параметрами для которых были вычисляемые значения параметров сетевого трафика. В результате экспериментов было выявлено "золотое" соотношение количества атак к общему количеству данных в обучающем множестве.

В настоящее время осуществляется разработка программного прототипа модульной СОВ с использованием аппарата нейронных сетей.

Попов А.А.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
информационных технологий, механики и оптики
МНОВЕНДОРНЫЕ СИЛЫ АНТИВИРУСНОЙ ОБОРОНЫ

Каждый день в мире появляются десятки новых вредоносных кодов, но их образцы попадают к разработчикам разных антивирусных программ в разное время. Соответственно, и средства борьбы с этими новыми вирусами добавляются в соответствующие вирусные базы программ в разное время. Более того, какое-то время требуется еще и на доставку новых сигнатур непосредственно на компьютеры конечных пользователей антивирусов. Наконец, некоторые корпоративного уровня пользователи антивирусов зачастую проводят собственные тесты новых версий вирусных баз до того, как включить новые программные модули в производственные процессы. В итоге, на каком-то компьютере в какой-то момент времени какой-то новый вирус вполне может и обмануть защиту

какого-то конкретного антивируса, проникнуть на компьютер или в сеть и, соответственно, осуществить какое-то вредоносное действие — нанести ущерб владельцу компьютера или сети. В настоящее время — это серьезная проблема всей антивирусной индустрии.

Одно из решений, которым в последнее время достаточно часто пользуются многие корпорации для повышения уровня своей антивирусной защиты — это применение многовендорных и мультиядерных антивирусных решений. Одной из первых стала поставлять в рамках своего антивируса Antigen сразу несколько антивирусных ядер ("движков") американская компания Sybari. Сегодня на рынке представлено уже 8 ядер — от английской компании Sophos, шведской компании Norman, американской компании Computer Associates (два ядра — Inoculate израильского производства и Vet австралийского производства), венгерской компании Virus Buster, российской компании Kaspersky Lab, американской компании Authentium и корейской компании Ahnlab. Благодаря плотному "покрытию" временных зон, где работают разработчики разных ядер, гарантируются быстрая реакция и высокая эффективность противодействия всем новым вирусам, исходящими из любой точки мира.

Многовендорные решения существенно повышают вирусостойкость — против атак новых вирусов, сигнатуры которых пока не попали в вирусную базу конкретного антивируса. Если какому-то новому вирусу и удастся "прорвать" защитные редуты одного или даже двух антивирусов, то он обязательно будет обезврежен третьим, пятым или восьмым антивирусом.

Среди преимуществ антивирусных решений Sybari были отмечены также: легкость интеграции напрямую с Exchange Server, что устраняет необходимость выделять отдельные машины для вирусного сканирования; способность справляться с задачами по нейтрализации вирусов даже при максимальных нагрузках, а также и в неожиданных ситуациях, например, при перезагрузке компьютера для обновления ПО; масштабируемость для целей защиты сетевых шлюзов; способность эффективно бороться с вирусами, спрятанными в zip-файлах вложений в электронные сообщения; наличие поддержки всех возможных кодировок сообщений, которые могут встретиться в реальной ситуации и др.

В течение 8 месяцев производственного использования решений от Sybari, например, в компании Microsoft не было зафиксировано ни одного случая, чтобы какой-либо вирус, червь или троян смог бы "пробить" эту супернадёжную оборону. Есть и другие примеры успешных мультиядерных антивирусных решений.

В настоящее время все чаще под термином "антивирусная защита" понимается совокупность таких средств противодействия атакам вредоносных кодов как антивирусы, персональные межсетевые экраны, антиспамовые продукты, системы предотвращения вторжений, антишпионские программы и другие. Однако заметим, что если "системы предотвращения вторжений" (IPS, Intrusion Prevention Systems) включают в такое обобщенное понимание термина "антивирусная защита", то "системы обнаружения вторжений" (IDS, Intrusion Detection Systems) — нет.

Важную роль в деле укрепления антивирусной защиты корпоративных сетей призваны сыграть промышленные инициативы Network Admissions Control (NAC) и Network Access Protection (NAP), которые ведут соответственно компании Cisco и Microsoft, — для обеспечения доступа в корпоративную сеть только тех удаленных компьютеров, у которых, во-первых, имеются все обновления соответствующих (политике предприятия) антивирусов и, во-вторых, которые уже были проверены свежими версиями этих антивирусов и на которых не было обнаружено каких-либо признаков вредоносных кодов.

Резник С.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
КОМБИНИРОВАННЫЕ ПОДХОДЫ К ВЕРИФИКАЦИИ ПРОТОКОЛОВ БЕЗОПАСНОСТИ**

Представляемая работа посвящена анализу существующих методов верификации протоколов безопасности и разработке подходов, комбинирующих их сильные стороны.

В работе рассматриваются различные методы верификации, анализируются их сильные и слабые стороны. Данный анализ производится на примерах как существующих протоколов безопасности, так и entrusting-протокола, разработанного в рамках проекта RE-TRUST. Выделяются наиболее развитые реализации разных методов:

- AVISPA, как средство, ориентированное на автоматическую верификацию набора классических свойств протоколов безопасности (аутентификации, конфиденциальности);
- Isabelle, как универсальное средство автоматизированного доказательства теорем, одной из областей применения которого может являться задача доказательства свойств протоколов безопасности.

Демонстрируется семантический разрыв между моделями, с которыми работают средства верификации с конечной задачей обоснования корректности протокола.

В работе предлагаются следующие варианты комбинированного использования подходов к верификации протоколов безопасности:

- использование разных подходов для верификации разных свойств. В этом случае подходы, реализованные в AVISPA, используются для доказательства классических свойств протоколов

безопасности, а более гибкие подходы, основанные на использовании Isabelle, применяются для доказательства более тонких свойств;

- использование подходов, основанных на использовании Isabelle, для экстраполяции результатов, полученных с помощью подходов, реализованных в AVISPA, на модель, соответствующую задаче обоснования безопасности системы в целом. Другими словами, Isabelle используется для доказательства того, что неизбежные допущения, сделанные при создании AVISPA-модели не умаляют общности полученного результата;

- использование AVISPA-модели для генерирования скелета доказательства с использованием Isabelle. AVISPA-модель применяется для удобного описания такой модели системы, а Isabelle – для исчерпывающего обоснования надежности системы.

Все варианты имеют целью совместить удобство AVISPA-модели с гибкостью, предлагаемой Isabelle. Общей идеей, по-разному воплощаемой в каждом из вариантов, является использование AVISPA-модели в той мере, в какой это возможно, и переход к верификации с помощью Isabelle только там, где без этого не обойтись.

Предлагаемые варианты комбинированного использования подходов к верификации протоколов безопасности рассматриваются на примере entrusting-протокола.

В дальнейшем предполагается развитие и дальнейшее исследование описанных вариантов комбинирования, а также их применение в новых областях – таких как верификация протоколов поддержки сервисно-ориентированной архитектуры и динамическая генерация протоколов безопасности.

Работа выполнена при финансовой поддержке РФФИ (проект №07–01–00547), программы фундаментальных исследований ОНИТ РАН (контракт №3.2/03) и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST (контракт № 021186–2) и других проектов.

Романовский Р.С.

Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ПРОГРАМНО-АППАРАТНОГО КОМПЛЕКСА ТЕСТИРОВАНИЯ ЦИФРОВЫХ УСТРОЙСТВ

1. Создание безопасных систем требует применения высоконадежной и достоверной аппаратуры, при разработке которой необходимо комплексное тестирование цифровых устройств на расширенных тестах в широком диапазоне изменения условий. Такие проверки должны быть выполнены системами входного/выходного контроля, которые в настоящее время являются громоздкими и неэффективными, либо в них не определяется запас параметрической устойчивости, напрямую влияющий на надежность и достоверность разрабатываемых систем. В докладе рассматривается система, которая позволяет осуществлять функциональное и параметрическое тестирование цифровых устройств на рабочих частотах и имеет преимущества перед аналогами по функциональности и мобильности.

2. На архитектурном уровне система представляет собой набор из двух плат – Модуля Цифрового Тестера (МЦТ) и Модуля Цифрового Осциллографа (МЦО) – размещенных на материнской плате содержащей модуль управления питанием, двунаправленный буфер с раздельным питанием портов и контактирующее устройство для подключения тестируемого объекта. Управление логическими уровнями сигналов осуществляется путем управления питанием буферов, включенных между источником тестирующих сигналов и испытуемой микросхемой. Система позволяет проводить тестирование цифровых устройств на частотах до 50 МГц, имея полосу пропускания аналоговых цепей МЦО до 300 МГц.

3. Одной из важных задач при параметрическом тестировании является оценка входных/выходных сопротивлений тестируемого объекта. Для проведения такой оценки обычно используют остановку тестов и коммутацию на измеритель тока. Но с учетом специфики решаемых системой задач, такой подход приведет к существенному увеличению размеров системы и снижению полосы пропускания аналоговых трактов МЦО.

4. Предлагается методика оценки, состоящая в использовании свойств, применяемых буферов, а именно выходном сопротивлении в установившемся режиме. Таким образом, эквивалентная схема цепи представляет собой делитель напряжения, состоящий из выходного сопротивления буфера и входного/выходного сопротивления канала тестируемого объекта. Измеряя напряжение на выводе тестируемой микросхемы можно оценить сопротивление тестируемой микросхемы. Измерение проводится в определенные моменты времени после уравнивания уровней на линии (из-за схемы динамической подтяжки буферов).

5. При работе с тестирующим оборудованием одним из основных параметров является длина непрерывно выдающегося теста. В связи с ограниченностью некоторых систем, в данном решении предложена система хранения тестов в сжатом виде, что позволило на порядок увеличить длину непрерывно выдаваемых тестовых последовательностей.

6. Разработанная система в полной мере удовлетворяет поставленным требованиям и показывает эффективность применения двунаправленных буферов с отдельным питанием как средств управления логическими уровнями сигналов, сохраняя такой важный параметр как компактность системы. В настоящее время направление работы связано с разработкой форматов параметрического тестирования, встроенного ПО и разработкой программных модулей сопряжения со стандартными средствами разработки и тестирования.

Рудакова С.А.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
информационных технологий, механики и оптики
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ**

27 июля 2006 года Президент РФ Путин В.В. подписал закон N152–ФЗ «О персональных данных». Закон требует, чтобы каждая организация, владеющая персональными данными своих сотрудников, клиентов, партнеров и т.д., обеспечила конфиденциальность всей этой информации. Информационные системы персональных данных, созданные до дня вступления в силу этого Федерального закона, должны быть приведены в соответствие с его требованиями не позднее 1 января 2010 года.

Представляется, что существует опасность того, что в свете реализации норм Закона «О персональных данных» может появиться дополнительный инструмент у недобросовестных конкурентов. Что мешает, например, подать заявление от лица субъекта персональных данных (конкретного гражданина) о нарушении его прав компанией, которой он сообщил личную информацию? Предприятие ждет еще одна проверка, отвлекающая силы от основного бизнеса. Поэтому задача построения защиты персональных данных выходит далеко за рамки полномочий департамента информационной безопасности. Ведь невыполнение требований закона несет угрозу не просто информационным ресурсам или интересам отдельных клиентов – возникает угроза для нормального функционирования самого бизнеса. Именно поэтому все ключевые решения по проекту «Построение защиты персональных данных» должны приниматься на уровне высшего менеджмента организации.

Подавляющее большинство организаций до сих пор не запустило проекты по приведению информационных систем в соответствие с положениями закона. Промедление связано, прежде всего, с тем, что лишь совсем недавно появился полный массив нормативных актов регуляторов. Вторая причина в том, что организациям очень непросто решиться на серьезные траты и реорганизацию ряда бизнес-процессов.

В соответствии с законом «О персональных данных», в орбиту процессов, связанных с защитой персональных данных, вовлечены три органа государственной власти: ФСБ, ФСТЭК и Роскомнадзор Министерства связи и массовых коммуникаций. В УК РФ уже внесены изменения (статья 137), ужесточающие ответственность за нарушения, затрагивающие неприкосновенность частной жизни. Они вступят в силу с 1 января 2010 года.

В октябре 2006 года вступил в силу федеральный закон от 30.06.2006 N 90–ФЗ «О внесении изменений в Трудовой кодекс РФ». Этот нормативный акт вносит в ТК самые многочисленные изменения за весь период действия Кодекса. Прежде всего, новый закон приравнял разглашение персональных данных другого работника, ставших известными в связи с исполнением служебных обязанностей, к разглашению охраняемой законом тайны.

Закон «О персональных данных» предполагает, что оператор персональных данных применяет специализированное программное и аппаратное обеспечение в процессах сбора, обработки, передачи и хранения персональных данных. Средства защиты персональных данных должны обладать сертификатами ФСТЭК или ФСБ.

Вполне реальна ситуация, когда в реестре сертифицированного программного и аппаратного обеспечения упоминается средство, аналогичное тому, что уже установлено в компании, но не прошло процедуры сертификации. Если так, то это средство не будет рассматриваться проверяющим как надлежащий механизм защиты персональных данных. Выходов в такой ситуации два: или переходить на использование сертифицированных средств или подавать на сертификацию уже применяемые. Но сертификация – очень непростая процедура. Кроме того, это может потребовать ощутимых расходов и займет не менее 6 месяцев.

Семьянов П.В.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
ОРГАНИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ ВЫЧИСЛЕНИЙ НА ГРАФИЧЕСКИХ ПРОЦЕССОРАХ**

Графические процессоры (*GPU*) в последнее время стали опережать центральные процессоры по производительности (1000 гигафлопс против 200), во многом за счет того, что они предлагают высокопараллельные вычисления. Более того, кроме использовавшихся недавно только узкоспециализированных вычислений для вывода графики появились и активно развиваются технологии вычислений общего назначения на GPU (*GPGPU*): технология CUDA от NVIDIA, ATI

Stream от AMD и общий стандарт OpenCL. За счет этих технологий появилась возможность ускорять различные алгоритмы, допускающие параллельную обработку, в пределах от 4-8 до 100-150 раз.

Криптографические алгоритмы также возможно реализовывать на GPU, получая существенное ускорение в том случае, если возможно параллельное исполнение, то есть:

- 1) в задачах перебора ключей или паролей;
- 2) при шифровании или хешировании больших объемов открытого текста.

К сожалению, многие криптографические алгоритмы плохо подходят для реализации второй задачи, т.к. шифрование или хеширование части данных зависит от предыдущих данных и не может быть сделано одновременно. В настоящее время разрабатываются новые алгоритмы, которые будут допускать параллельную обработку данных.

В рамках данного исследования был реализован перебор ключей/хешей с помощью технологии CUDA для следующих алгоритмов: MD5, SHA-1, RC4, AES. Были сомнения, что некоторые алгоритмы, если их и удастся реализовать на CUDA, дадут прирост скорости, однако эти сомнения успешно разрешились. Все они, особенно хеши семейства MD, подходят для реализации на GPU и дают существенное ускорение.

Необходимо заметить, что переделка исходного текста криптофункций с языка C на язык CUDA была минимальна, однако для получения максимальной скорости сам код необходимо было оптимизировать, что не всегда было тривиальным. В таблице представлены результаты сравнения оптимизированных версии алгоритмов под CPU (SSE2-код) и GPU, что дает реальные значения ускорения.

Таким образом, использование технологии параллельных вычислений на GPU дает существенный эффект для многих существующих криптографических алгоритмов, причем достижение этого эффекта является недорогим с точки зрения разработки.

Харинов М.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПРИМЕНЕНИЕ СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЙ С СОХРАНЕНИЕМ ЗРИТЕЛЬНОГО ОБРАЗА**

В задачах, связанных с автоматизированным анализом и распознаванием, сегментация является характерной стадией первоначальной обработки сигнала, в результате которой элементы сигнала («пиксели» изображения, «сэмплы» аудиосигнала и т. п.) группируются в составные сегменты, рассматриваемые вместо отдельных исходных элементов сигнала при продолжении обработки. В настоящее время известны тысячи алгоритмов сегментации, которые применяются в различных приложениях, но не хватает алгоритмов сегментации, применимых для различных задач, сигналов различного содержания, а также сигналов различной природы, например, изображений и аудиосигналов. Для разработки подобных алгоритмов необходима научная интерпретация понятия сегментации.

В докладе сегментация формализуется как один из двух основных процессов преобразования информации — процесса ее формирования при записи в сигнал некоторого «сообщения» и процесса фильтрации информации при ее извлечении в виде упрощенного (сегментированного) сигнала для дальнейшего анализа и распознавания. Для указанных процессов устанавливаются общие алгебраические свойства преобразования информации. Первое свойство состоит в идемпотентности преобразования сигнала, которая в приложении к сегментации означает, что повторная сегментация не меняет однажды сегментированный сигнал. Второе свойство состоит в том, что сегментация сохраняется также при преобразовании сигнала в некоторое инвариантное представление, которое не зависит от предусмотренных линейных и нелинейных преобразований сигнала.

В рамках установленных условий предлагается алгоритм сегментации, который не требует указания параметров, по скорости превосходит известные алгоритмы, так называемой, «адаптивной иерархической сегментации» и применим к изображениям, а также к аудиосигналам независимо от их конкретного смыслового содержания.

Результаты обработки демонстрируются на примере изображений лиц, дистанционных снимков, графических изображений и других, для которых алгоритм обеспечивает выраженную сегментацию с сохранением зрительного образа, что проявляется наглядно и выражается в сохранении целостности воспринимаемого образа изображения, а также образов объектов. Рассматриваются приложения сегментации изображений с сохранением зрительного образа к задаче защиты денежных знаков, в которой при минимальных затратах обеспечивается защита каждая купюры от подделки, задаче распознавания с обучением без накопления эталонов или иных описаний объектов по прототипу, в системных редакторах изображений и других.

В заключение анализируются известные подходы к проблеме сегментации изображений с сохранением зрительного образа, которая в англоязычных источниках именуется как «perceptual segmentation» и связывается с моделированием, так называемой, «подпороговой» («preattentive») стадии процесса восприятия информации живыми организмами, в частности, человеком. Наряду с теоретическим обсуждением недостатков известных подходов к сегментации сигналов в качестве практического обоснования преимуществ предлагаемого решения проводится сравнительный анализ экспериментальных результатов.

Цехановский В.В., Захаров Д.В., Дернова Е.С., Гортинская Л.В.

Россия, Санкт-Петербург Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

ПРОТОКОЛЫ СЛЕПОЙ ПОДПИСИ, ОСНОВАННЫЕ НА ДВУХ НЕЗАВИСИМЫХ ТРУДНЫХ ЗАДАЧАХ

Системы электронных денег и тайного электронного голосования используют криптографические протоколы, известные как схемы слепой электронной цифровой подписи (ЭЦП). Данный тип протоколов применяется для решения задачи обеспечения анонимности. Протоколы такого типа позволяют подписать электронное сообщение таким образом, что подписывающий не может ознакомиться с содержанием сообщения в процессе генерации ЭЦП, а в будущем при получении сообщения и соответствующей подписи не может идентифицировать однозначно пользователя, который предоставлял ему это сообщение для подписи. Известные протоколы слепой подписи основаны на вычислительной сложности задачи факторизации составных чисел вида $n = qr$, где q и r – два больших простых числа или на трудности нахождения дискретного логарифма в конечной группе большого простого порядка. В случае «обычных» ЭЦП для повышения безопасности предложены протоколы, взлом которых требует одновременного решения двух различных трудных вычислительных задач [Вопросы защиты информации. 2008. №1. С. 22–26]. Эти протоколы обеспечивают безопасность ЭЦП в случае прорывного успеха в решении одной трудной задачи. Вероятность события появления двух прорывных решений независимых трудных задач значительно меньше, что повышает уровень безопасности ЭЦП.

В докладе рассматриваются схемы построения протоколов слепой подписи, основанных на двух независимых трудных вычислительных задачах. Предложены две конструкции таких протоколов. Первая конструкция основана на объединении двух различных рандомизированных схем ЭЦП, путем использования единого для обеих схем параметра рандомизации, что позволяет сократить размер подписи по сравнению с формированием вслепую подписей для двух независимых схем ЭЦП. Такой способ позволяет комбинировать задачи дискретного логарифмирования, заданные в конечных группах различного типа (числовых мультипликативных группах, группах матриц, группах векторов, группах точек эллиптической кривой). Однако этот не предоставляет удобных решений по построению протоколов слепой подписи, комбинирующих задачи дискретного логарифмирования и факторизации. Для решения последней задачи предложен второй способ, в котором используется конечная числовая группа с операцией умножения по модулю p , имеющему структуру вида $p = 2n + 1$, где $n = qr$, q и r – большие простые числа размером $|q| \approx |r| \geq 512$ бит. При этом одно из двух больших простых чисел, например q , служит порядком числа α , используемому в алгоритме ЭЦП. Открытым ключом является четверка чисел (p, y, α, λ) , где λ – длина секретного значения q ; $y = \alpha^x \bmod p$; где x – секретный ключ. Подпись представляет собой пару чисел (s, e) , где $|s| \approx |q|$ и $|e| \geq 160$ бит. При проверке подлинности ЭЦП в качестве одного из шагов процедуры проверяется выполнимость соотношения $|s| \leq \lambda + 1$.

Излагаются проблемы построения протоколов слепой коллективной ЭЦП, основанных на двух трудных задачах. Работа поддержана грантом РФФИ № 08–07–00096–а.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Алексеев О.Б.

Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»

ВОПРОСЫ ФОРМИРОВАНИЯ ФУНКЦИОНАЛЬНОЙ АРХИТЕКТУРЫ ПОДСИСТЕМ

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Перспективные телекоммуникационные сети специального назначения (ТКС СН) и системы управления ими все больше интегрируются с компьютерными сетями соответствующих органов и пунктов управления, превращаясь в информационно-телекоммуникационные системы, обеспечивающие использование в интересах пользователей важнейших разнородных информационных ресурсов, обеспечение безопасности которых становится актуальнейшей задачей.

Учитывая сложность задачи обеспечения безопасности информационных ресурсов автоматизированных систем управления (АСУ) ТКС СН для ее решения целесообразно создание специальной подсистемы управления информационной безопасностью АСУ ТКС СН. Такая подсистема должна быть направлена на предотвращение самих предпосылок реализации компьютерных атак.

Для обеспечения функциональной полноты, основными элементами подсистемы управления информационной безопасностью АСУ ТКС СН должны стать:

- средства управления инцидентами;
- средства управления рисками;
- средства управления политиками безопасности;
- средства аудита безопасности и тестирования подсистемы;
- средства управления восстановлением функционирования АСУ и подсистемы обеспечения информационной безопасности АСУ;
- средства поддержки принимаемых решений;
- имитационные модели сети и компьютерных атак;
- средства управления.

Следует подчеркнуть, что подсистема управления информационной безопасностью АСУ ТКС СН должна создаваться адаптивной. Адаптация заключается в различных формах реагирования, которые могут включать:

- отправление уведомления системам сетевого управления по протоколу SNMP, по электронной почте или на пейджер дежурному офицеру;
- автоматическое завершение сеанса связи с атакующим узлом или пользователем, реконфигурацию межсетевых экранов или иных сетевых устройств (например, маршрутизаторов);
- выработку рекомендаций дежурному офицеру, позволяющих своевременно устранить обнаруженные уязвимости в сетях, приложениях или иных компонентах АСУ ТКС СН.

Использование модели адаптивной безопасности АСУ позволит контролировать практически все угрозы и своевременно реагировать на них способами, позволяющими не только устранить уязвимости, которые могут привести к реализации угрозы, но и проанализировать условия, приводящие к появлению таких уязвимостей.

Бабкова М.И., Привалов А.А., Романова К.Н.

Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»

ОБОБЩЕННАЯ МОДЕЛЬ ПРОЦЕССА ПЕРЕДАЧИ ДАННЫХ ПО ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ПРОТИВНИКА

Особенностью телекоммуникационных сетей специального назначения (ТКС СН) является, с одной стороны, предъявление жестких требований по своевременности, достоверности и безопасности информационного обмена между пользователями, а с другой – их использование в условиях воздействия множества антагонистических факторов. Существующие модели не позволяют определить значение показателей эффективности функционирования ТКС СН в динамике радиоэлектронного конфликта и предъявить требования к длительности и структуре цикла управления ею.

В докладе рассматривается динамическая обобщенная модель процесса передачи данных по ТКС СН в условиях деструктивных воздействий противника, состоящая из моделей: процессов передачи данных от приложения-клиента к приложению-серверу, от приложения-сервера к приложению-серверу, от приложения-сервера к приложению-клиенту, тракта обмена сообщениями в IP-сети, процессов реализации воздействий на сетевые элементы ТКС СН, а также восстановления работоспособности и передачи данных.

Основной в обобщенной модели является модель тракта обмена сообщениями в IP-сети. Она основана на формализованном представлении ТКС СН в виде многофазной сети массового обслуживания, определении первых четырех центральных моментов времени доставки данных с последующей аппроксимацией функции распределения с использованием семейства распределений Пирсона. В качестве элементов ТКС СН рассматриваются сервера отправителя и получателя, а также оборудование связи транспортной системы. Каждая фаза сети массового обслуживания представляется в виде системы массового обслуживания, которая отображает процесс обслуживания заявок на элементе сети, задействованным в траектории передачи данных. Исходными данными являются параметры, определяемые из моделей процессов передачи данных от приложения-клиента к приложению-серверу, от приложения-сервера к приложению-серверу, от приложения-сервера к приложению-клиенту, включающие частные модели процессов установления соединения «клиент-сервер», «сервер-сервер», «сервер-клиент», процессов передачи данных и последующего завершения соединения, а также оказания воздействий на элементы ТКС СН. Подход к моделированию основан на представлении указанных процессов в виде укрупненных смешанных стохастических сетей с последующим определением функции распределения времени реализации соответствующих процессов.

Результатом моделирования процесса передачи данных по ТКС СН в условиях воздействия противника является определение функции и поверхности распределения времени передачи данных в течение времени функционирования, а также вычисление среднего времени безотказной работы и интенсивности перехода ТКС СН в состояние отказа предоставления услуг пользователям.

Реализуемый в модели метод анализа результатов позволяет определить наиболее существенные для ТКС СН угрозы, определить требования к длительности цикла управления ТКС СН в условиях антагонистических воздействий, а также осуществлять обоснованный выбор управляющих воздействий на ТКС СН, обеспечивающих заданную эффективность её функционирования.

Буренин А.Н.

**Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»
КОМПЛЕКСЫ СРЕДСТВ ПРЕДУПРЕЖДЕНИЯ И ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК НА
СИСТЕМЫ УПРАВЛЕНИЯ СОВРЕМЕННЫХ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ**

В современных условиях информационного противодействия все чаще объектом информационного воздействия становятся системы управления телекоммуникационных сетей, что позволяет в значительной степени дезорганизовать работу этих сетей.

Перечень задач управления и структура систем управления перспективных защищенных телекоммуникационных сетей позволяют на основе предполагаемых угроз программно-аппаратных атак уточнить уязвимые места для этих воздействий и как-то классифицировать сами воздействия. При этом следует выявить критически важные элементы систем управления (включая задачи управления), программно-аппаратные атаки на которые могут привести наибольший вред и наибольшие разрушительные последствия.

Критически важными функциональными подсистемами, которые соответствуют этим уровням архитектуры систем управления перспективных телекоммуникационных сетей назначения, по мере убывания важности являются:

- подсистема оперативно-технического управления;
- подсистема технологического управления.

Для обеспечения требуемого уровня информационной безопасности в состав системы комплексной безопасности необходимо включать средства предупреждения и обнаружения программно-аппаратных атак на системы управления телекоммуникационных сетей.

В состав средств предупреждения программно-аппаратных воздействий на средства подсистем управления входят программно-аппаратные комплексы традиционных средств обеспечения безопасности, комплексы средств, генерирующих ложные информационные объекты, и программно-аппаратные средства, осуществляющие безопасное применение стандартных протоколов управления (протокол SNMP).

В состав средств обнаружения программно-аппаратных атак на средства подсистем управления входят средства контроля регистрационной информации о несанкционированных действиях, о случайных и аварийных ситуациях, система обнаружения атак, специальные средства подсистемы технологического управления системы управления телекоммуникационной сети,

специальное программное обеспечение обработки комплексной информации и адаптивная имитационная модель.

Рассмотренные выше различные компоненты комплексов предупреждения и обнаружения атак имеют свои достоинства и недостатки, связанные со спецификой их организации и построения. Они строятся так, чтобы взаимно добавлять возможности по своевременному обнаружению и гарантированному предупреждению атак нарушителя на системы управления перспективных защищенных телекоммуникационных сетей, т.е. рассмотренные комплексы должны работать в едином процессе функционирования системы комплексной безопасности.

Буренин А.Н.

Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»

МЕТОД ПОВЫШЕНИЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЗАЩИЩЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ IP-СЕТИ

Безопасность информационного взаимодействия пользователей современной телекоммуникационной сети приобретает в настоящее время наиболее важное значение, так как процессы передачи информации в IP-сети с применением стандартных протоколов управления и маршрутизации не обеспечивают требуемый уровень информационной безопасности.

Традиционное объединение локальных сетей пользователей через слабо защищенную внешнюю среду передачи информации в единую виртуальную сеть с образованием защищенной виртуальной сети, в которой каналы связи интерпретируются с помощью каналов связи реальной сети, не защищают от несанкционированных воздействий через протоколы маршрутизации и управления.

Известны методы снижения возможности несанкционированных воздействий на сеть при использовании в ней простого протокола сетевого управления SNMP.

Можно предложить способ снижения возможности несанкционированных воздействий на сетевом уровне при использовании в IP-сети наиболее часто применяемых протоколов маршрутизации RIP и OSPF.

В целом протокол OSPF и многие другие (IGRP, EIGRP, EGP, BGP, IGMP, DVMRP, MOSPF, PIM) подходят для современных больших, динамически изменяющихся сетей. Однако, ориентировка этих протоколов на открытую сеть типа Интернет, предполагающая фактически знание на каждом маршрутизаторе всей структуры сети и возможность влияния на процессы маршрутизации извне, являются существенными недостатками. Поэтому применение их в защищенных телекоммуникационных сетях нежелательно по причинам невозможности обеспечения требований по информационной безопасности.

Поэтому может быть предложен метод, основанный на изменении формирования метрики при составлении матрицы маршрутов в маршрутизаторе. Причем процедуры формирования метрики можно распространить на каждый из доменов маршрутизации, что позволит организовать псевдоключевые зоны на сетевом уровне IP-сети. Эти алгоритмы должны быть встроены в стандартные протоколы маршрутизации (RIP и OSPF). Процедуры формирования метрики могут носить различный характер, определяемый степенью ее адекватности реальным процессам распределения информации в сети. Важно только то, чтобы они существенно отличались от применяемых в протоколах. При этом могут быть рекомендованы достаточно простые известные методы управления и формирования метрики.

Буренин В.А., Винниченко А.В.

Россия, Санкт-Петербург, ЗАО «ВСС», ФГУП «Научно-исследовательский институт «Рубин»

ВАРИАНТЫ ПОСТРОЕНИЯ ПОДСИСТЕМЫ УПРАВЛЕНИЯ ОБОРУДОВАНИЕМ СОВРЕМЕННОЙ ЗАЩИЩЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Исторически работы в области создания систем автоматизированного управления современными защищенными телекоммуникационными сетями велись отдельно от работ обеспечения безопасности процедур управления, хотя в настоящее время понятия управление сетью, безопасность сети, безопасность собственно управления сетью пересекаются.

Потенциальные возможности коммутационного и серверного оборудования современных защищенных телекоммуникационных сетей по их мониторингу и управлению в целом позволяют разработать и предложить решения по управлению оборудованием узлов, включая их безопасность.

Принимаемые решения по созданию средств автоматизированного управления сетями и их оборудованием необходимо соотносить с уровнями, предусмотренными концепцией управления телекоммуникациями (TMN):

- управление сетевыми элементами - технологическое управление;
- управление сетями и услугами - оперативно-техническое.

С учетом вышеизложенного, архитектура и принципы построения подсистемы технологического управления предусматривают двухуровневое ее построение. При этом возможны два основных

варианта построения подсистемы технологического управления на каждом узле защищенной телекоммуникационной сети.

В первом, предусматривается применение так называемых интеллектуальных менеджеров, управляющих определенным типом сетевого оборудования, в функции которых наряду с обработкой информации мониторинга состояния управляемого оборудования, выработкой управляющих воздействий по поддержанию требуемого уровня эффективности его функционирования, входят задачи по адаптации оборудования к стандартным протоколам управления, что во многих случаях практического применения разнородного оборудования различных производителей вырастает в достаточно сложную проблему, решение которой приводит к существенному усложнению менеджеров. Однако такой вариант обеспечивает высокий уровень информационной безопасности процессов технологического управления оборудованием, так как менеджеры, как правило, встраиваются в опечатанные стойки оборудования.

Во втором варианте менеджеры осуществляют только реализацию протокола SNMP и пересылку всех данных MIB в единый на узле сервер технологического управления, что повышает гибкость, но снижает безопасность управления

Воронков К.Л., Шерстюк М.Ю.

Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

МЕТОДИКА СИНТЕЗА ВИТРИНЫ РАЗНОРОДНЫХ ДАННЫХ НАРУШЕНИЙ БЕЗОПАСНОСТИ

В современной автоматизированной системе управления связью (АСУС) потенциальными объектами компьютерных атак (КА) являются как средства вычислительных сетей (в т.ч. самой АСУС), так и сети и средства телекоммуникаций. В связи с этим комплексная защита от КА в АСУС предполагает в том числе информационную интеграцию принципиально разнородных детекторов КА.

Осуществление информационной интеграции с применением технологий хранилищ и витрин данных требует решения задачи синтеза структуры информационного хранилища, обеспечивающего консолидированное хранение семантически разнородных, но логически связанных данных.

Предлагаемая методика синтеза структуры подобного информационного хранилища, рассматриваемого как витрина данных о выявленных нарушениях безопасности, обнаруженных КА и предпринятых действиях по противодействию КА, минимизации их последствий предполагает выполнение следующих действий:

- определение групп синтаксически эквивалентных классов событий для сообщений, формируемых детекторами атак – источниками первичных данных (ИПД);
- разработка структуры буферных таблиц для сообщений, формируемых ИПД, и установление их соответствия классам первичных событий;
- определение групп синтаксически эквивалентных классов событий для сообщений, формируемых ИПД;
- разработка структуры таблиц хранения консолидированных данных – таблиц фактов, измерений и консольных таблиц.

Данная методика базируется на следующих основных положениях:

- разделение таблиц информационного хранилища на буферные таблицы и таблицы хранения данных;
- определение понятия семантической эквивалентности параметров событий, самих событий и таблиц информационного хранилища, и семантического покрытия групп событий.

Собственно синтез структуры таблиц хранения может быть осуществлен как процесс построения остова графа семантического покрытия, что обеспечивает получение минимально допустимого состава таблиц хранения данных.

Котылевский А.С.

Россия, Санкт-Петербург, ООО «НеоБИТ»

РАСПРЕДЕЛЕННЫЙ КОНТРОЛЬ ПОТОКОВ ДАННЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННЫХ СИСТЕМАХ

Идея реализации функций контроля и управления доступом на уровне инфраструктуры сети является аналогией сетей шифрованной связи. Создание технических средств, позволяющих строить сети связи с контролируемым и управляемым доступом, обеспечит в информационно-телекоммуникационных системах (ИТКС) надежную защиту от внутреннего нарушителя подобно тому, как сети шифрованной связи обеспечивают защиту от внешнего нарушителя.

Задача распределенного контроля потоков данных в ИТКС состоит в мониторинге и управлении передачей информации между территориально распределенными узлами системы, объединенными сетью связи. Под потоком данных понимается одно- или двунаправленный обмен данными между двумя узлами сети ограниченный по времени. В общем случае действующие в ИТКС приложения и сервисы могут требовать обмена данными между узлами сети по различным схемам – напрямую, либо через центральный узел, либо по какой-то иной схеме. Таким образом, множество узлов ИТКС,

осуществляя обмен данными посредством передачи потоков данных по определенной схеме, образуют сеансы связи. Информация, циркулирующая в пределах сеансов связи, рассматривается как объект доступа.

Задача распределенного контроля потоков данных в ИТКС может быть решена различными методами. Идентификация узлов связи может быть выполнена на основе сетевого адреса, либо с привлечением средств идентификации и аутентификации пользователей. Отнесение потоков данных к сеансам связи может быть выполнено на основе анализа пересылаемых данных, маркировки данных перед отправкой приложениями, либо по указанию от пользователя узла связи. Механизмы мониторинга и управления передачей информации могут быть реализованы на узлах связи, либо в сети на основе шлюзовых технологий; в случае, если все сеансы связи организуются через единый сервер связи, механизмы управления передачей потоков данных могут располагаться на этом сервере.

Применение концепции сетей связи с разграничением доступа (ССРД) позволяет решить задачу распределенного контроля потоков данных без необходимости модификации приложений и сервисов ИТКС. Другим существенным преимуществом предлагаемого подхода является существенное снижение сложности сертификационных исследований ИТКС на основе ССРД. Точно также как применение сертифицированных потоковых шифраторов снимает необходимость реализации и последующей сертификации подсистем криптографической защиты каналов связи, применение ССРД снимет необходимость разработки и последующей сертификации подсистем контроля и управления доступом, регистрации и учета событий.

Построение ССРД на практике связано с множеством трудностей. Так в одной ИТКС, как правило, функционирует множество приложений, каждое из которых использует свои протоколы связи. Существует также служебный трафик, такой как ARP, ICMP, DHCP, DNS и пр. Большой объем протоколов связи усложняет детектирующие механизмы сети связи. Также необходимо определить будет ли применяемая политика безопасности единой для всех приложений, или для каждого приложения будет отдельная политика. Одним из самых серьезных вопросов разработки сетей связи с разграничением доступа является механизм интеграции с целевой ИТКС. От этого зависят подсистемы идентификации, аутентификации, детектирования и др.

Вопросы разработки сетей связи с разграничением доступа достаточно актуальны. И по мере того, как будут усложняться ИТКС, актуальность этих вопросов будет возрастать, поскольку на сегодняшний день не существует иных способов снижения трудоемкости процесса сертификации, кроме использования готовых сертифицированных компонентов при построении ИТКС.

Кочубинский А.И., Мирин А.Ю.

Украина, Киев, Институт кибернетики им. В.М. Глушкова НАН Украины,

Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПЕРЕДАЧА СООБЩЕНИЙ ПО НЕЗАЩИЩЕННОМУ КАНАЛУ СВЯЗИ С ГАРАНТИРОВАННЫМ
ПОДТВЕРЖДЕНИЕМ ПОЛУЧЕНИЯ

Предлагается протокол передачи сообщений по незащищенному каналу связи с гарантированным подтверждением факта его получения и санкционированным доступом к его содержанию. Сообщение передается таким образом, чтобы отправитель был уверен в том, что документ дошел до получателя в исходном виде, получатель и только получатель получил доступ к содержанию документа и не мог оспорить факта знакомства с содержанием сообщения. Получатель уверен в подлинности документа и его аутентичности и в том, что отправитель не может оспорить своего авторства. Весь информационный обмен идет по незащищенному каналу связи, в частности, возможны незаконные действия законного участника информационного обмена с целью получения каких-либо преимуществ. Протокол обеспечивает конфиденциальность, неоспоримость, целостность, явную аутентичность сообщений и аутентичность источника сообщений. Особенность предлагаемого метода состоит в том, что получатель документа получает физический доступ к документу только после подтверждения его получения, причем в дальнейшем это можно доказать. Протокол строится на комбинированном использовании симметричных алгоритмов шифрования и криптографических алгоритмов с открытыми ключами, основанных на криптографических преобразованиях в якобианах эллиптических кривых, определенных над конечными полями. Протокол трехшаговый, на всех этапах его выполнения передается только несекретная аутентифицированная информация.

Курносов В.И., Хузин В.З.

Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННО-
ПОИСКОВОЙ СИСТЕМЫ, ОБЕСПЕЧИВАЮЩЕЙ РЕШЕНИЕ ЗАДАЧ ИНТЕГРАЛЬНОЙ
БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ СВЯЗИ

Актуальность данной темы определяется тем, что в настоящее время во всем мире идет стремительное развитие телекоммуникационных систем, сетей и их интеграция с вычислительными системами, что непосредственно связано с возрастающими потребностями общества во всех видах

информации. Постоянно растущий объем передаваемой информации, повышение уровня требований к скорости передачи данных, достоверности и безопасности передаваемой информации стимулируют внедрение в телекоммуникационные системы новых сетевых и информационных технологий. Все это приводит к значительному усложнению создаваемых информационно-поисковых систем (ИПС) для специалистов-разработчиков телекоммуникационных систем, сетей, комплексов технических средств.

Военно-политическая обстановка в современном мире требует дальнейшего повышение эффективности работы предприятий связи оборонно-промышленного комплекса (ПС ОПК) по обеспечению информационной безопасности на достойном уровне. Эта работа остается приоритетным направлением нашей экономики и политики.

ПС ОПК являются важнейшей составляющей российской экономики. Они существуют, функционируют и развиваются в условиях, в которых живет вся наша страна.

Объем финансирования государственного оборонного заказа составил в 2009 году свыше 1 трлн. рублей. В условиях глобального мирового кризиса принимаются меры для своевременного и ритмичного финансирования научно-исследовательского сектора и подготовки высококвалифицированных кадров.

Необходимо учесть, что эффективность работы ПС ОПК по всем направлениям их деятельности, включая и обеспечение информационной безопасности, зависит от их устойчивости и надежности.

Существующие автоматизированные ИПС ПС, основанные на традиционных технологиях управления, ориентированные в основном на позадачный подход, не могут удовлетворить современным требованиям.

В данном проекте рассматриваются новые концепция и принципы реализации ИПС ПС, построенные на перспективных информационных технологиях, в частности, на базе методов искусственного интеллекта. Предложенный модельный подход позволяет строить автоматизированные ИПС ПС с учетом обеспечения интегральной безопасности предприятия связи.

Представленные решения построения АИПС ПС являются весьма гибкими, учитывают большое число факторов, позволяют оптимальным образом планировать и обеспечивать своевременность выдачи большого числа вариантов ответов на вопросы специалистов, обращающихся к разработанной АИПС.

Материалы, изложенные в настоящей работе, могут послужить основой для дальнейшего совершенствования предложенной АИПС ПС и создания автоматизированных систем информационной и вычислительной поддержки многих процессов, с которыми на практике встречаются ведущие специалисты-разработчики новых информационных технологий.

Следует также подчеркнуть, что предложенные методы и подходы имеют более широкое значение и могут быть использованы при построении других автоматизированных систем управления связью.

В работе решались задачи:

- 1) анализ использования АИС на предприятии связи;
- 2) разработка структурной модели АИС ПС;
- 3) обоснование выбранной аппаратно-программной основы АИС ПС;
- 4) определение аспектов организации хранения и поиска документов при использовании заданных ресурсов АИС ПС.

По виду выполняемых задач разработанная структурная модель АИПС ПС относится к АСУ ПС, основная цель которой – решение задач организации управления и автоматизация работы отделов предприятия связи: бухгалтерии, планового, кадрового, снабжения, сбыта и т. д.

Современный подход к проектированию АИПС ПС предполагает решение задач на всех этапах жизненного цикла, включающего этапы анализа и выбора АПС, а также реализации принятых решений с учетом существующей топологии сети ПС, разработанной структуры БД и форм документов для решения задач АИПС ПС на последующих этапах внедрения, сопровождения и развития представленной АИПС ПС.

До внедрения разработанной системы на ПС отсутствовала локальная сеть, требовалось большое количество периферийного оборудования для обеспечения функционирования предприятия.

Большая часть программно-аппаратной составляющей АИПС ПС требует переоснащения. В связи с невысокой ее производительностью необходима работа по объединению компьютеров и периферийных устройств в локальную сеть.

Внедрение разработанной системы на ПС позволит повысить производительность труда, сократить эксплуатационные расходы.

Информационное обеспечение ПС будет представлять собой единое информационное пространство, с конечным числом пользователей, обладающих правами доступа в соответствии с занимаемой должностью.

Разработанная АИПС ПС имеет клиент-серверную архитектуру, которая позволяет делать запросы непосредственно к серверу, снижая нагрузку на локальную машину, так как все операции по

обработке данных осуществляются на сервере. За счет выполнения операций на сервере значительно уменьшается трафик сети.

Локальная сеть ПС построена по топологии «звезда», которая является наиболее надежной, так как выход из строя одной машины не сказывается на работе других пользователей.

В работе представлена структура локальной сети ПС. В каждом отделе ПС в соответствии с потребностями установлено АРМ. Сегменты сети соединены с помощью коммутаторов D-LINK. Маршрутизация осуществляется в сети NetGear.

Соединение между сегментами сети и коммутационным оборудованием произведено при помощи кабеля «витая пара». В качестве сервера используется HP Proliant DL360R05 E5405 с установленной ОС MS Windows Server 2003, поддерживающей технологию NET, которая позволяет организовать обмен информацией между абонентами в локальной сети. На сервере также установлен программный пакет MS Office 2003.

Выбор ПО компании Microsoft обусловлен идеальной совместимостью и согласованностью работы между различными компонентами, поддержкой основных приложений и сравнительно невысокой ценой.

Курносов В.И., Хузин В.З.

Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»

НЕКОТОРЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ПРОДУКЦИИ ПРЕДПРИЯТИЯ СВЯЗИ В КРИТИЧЕСКИХ УСЛОВИЯХ ФУНКЦИОНИРОВАНИЯ

На сегодняшний день большинство специалистов-разработчиков на предприятии связи (ПС) приходят к мысли, что система менеджмента качества (СМК) не заменяет, а дополняет другие организационные и технические формы обеспечения качества промышленной продукции. ПС оборонно-промышленного комплекса (ОПК) не безразличны к общим и весьма сложным проблемам, с которыми они сталкиваются при исполнении ГОЗ. Предлагается рассмотреть наиболее существенные и важные системные вопросы, влияющие на качество продукции, производимой по ГОЗ, когда они определяют роль и место СМК.

Установлено, что:

1) неустойчивые по годам объемы заказов не позволяют обеспечить достаточно четкий ритм производства по всей технологической цепочке. Это приводит к образованию узких мест, а иногда и к разрыву устоявшихся связей, к росту цен на сырье и комплектующие изделия. При этом установлено, что введение 100 процентного входного контроля на многих головных предприятиях не решает проблемы повышения качества;

2) низкий уровень подготовки производства на многих ПС приводит к невозможности выявить скрытые производственные и конструкторские дефекты. Ныне коэффициент сменяемости технологического оборудования составляет 1-2%, в то время: как во времена СССР он составлял 5-10%, а ведущих странах мира – 15-20%.

По большинству видов продукции специальных программ и целевых инвестиций на технологическую подготовку производства в настоящее время нет. Заказчик на эти цели средств не имеет, поэтому специализированные ПС ОПК остаются один на один с решением проблемы повышения своего социально-экономического положения. Более того, эта проблема осложняется еще двумя факторами, которые связаны:

- с формальным конкурсным размещением заказов, не гарантирующих выполнение устойчивой долгосрочной программы социально-экономического развития ПС. Это, безусловно, не стимулирует интерес ПС к технологическому перевооружению;

- с наличием в технологической цепочке создания, например, промышленного пакета прикладных программ различных видов собственности на технологическое обеспечение. Конечно, такое положение усложняет выделение целевых инвестиций на развитие ПС;

3) практика работы ПС ОПК в условиях реализации Федерального закона (ФЗ) №94 2005 год показала неоправданно низкий уровень законодательной базы и нормативного регулирования отношений, связанных с реализацией и размещением заказов на поставки товаров и выполнение работ в интересах различных заказчиков федерального, регионального и местного уровня. Особенно следует обратить внимание на то, что при выполнении ГОЗ неоднократно изменялась редакция ФЗ № 94: в 2006 № 102, в 2007 г. № 53, № 218 и № 257; в 2008 г. № 160, № 225, № 308 и № 323. Разобраться в таком изобилии документов трудно и особенно когда мы имеем дело с конкурентным механизмом рыночной экономики. Всем ясно, что соревноваться с возможностями государства ни одна структура негосударственного уровня не может;

4) сокращение профессионального аппарата государственного заказчика и его представительства на местах существенно снизило возможности представителей заказчика по обеспечению требуемого уровня качества контроля выпускаемой продукции на ПС. Особенно это относится к вопросам прямого влияния на отработку технологической документации и технологических процессов на предприятиях;

5) существенное ослабление системы нормативного регулирования по всему жизненному циклу создания ВБТ в части обеспечения общими и специальными стандартами. По этому вопросу следует отметить наибольшее количество недостатков, число которых особенно возросло после принятия ФЗ «О техническом регулировании». Авторы этого закона стали отождествлять понятия обязательных стандартов и регламентов, что, понятно каждому является недопустимым. Регламенты устанавливают обязательные требования, прежде всего, по безопасности (экологии, здоровья и т. д.), а стандарты всегда устанавливали требования как общие, так и специальные с учетом потребительских качеств продукции. В этих условиях за последние годы появилось несоответствие существующих требований, которые хорошо известны специалистам ПС ОПК, и методик оценки качества продукции в условиях малых объемов заказа, приведенных в ГОСТах;

6) появление потребности централизованного регулирования развития базовых и критических технологий. Эта проблема многоплановая. Она вынуждает создавать унифицированные комплектующие изделия и компонентную базу важнейших образцов ВБТ. Сегодня большинство ПС ОПК вынуждены уделять достаточно серьезное внимание системному подходу, сохранению развития корпоративных связей по технологическим процессам. Но объективно для многих ПС ОПК эта проблема остается болезненной и трудно преодолимой.

В докладе не ставилась задача дать рекомендации по их решению, так как все перечисленные выше проблемы многоплановые, достаточно сложные и требуют дополнительной проработки.

В заключении хотелось подчеркнуть, что в условиях современного глобального мирового кризиса значение и роль СМК предприятий связи ОПК только возрастает. СМК разработки и производства и обучения специалистов ПС существенно дополняет систему контроля качества продукции государственного заказчика и показывает необходимость постоянного совершенствования обучения специалистов-разработчиков. В этих условиях сертификат соответствия ПС ОПК по СМК мог бы стать одним из главных условий принятия решения по размещению ГОЗ и оценке способности ПС выполнять заказ по каждому из видов ВБТ.

Левин И.И., Яковлев В.А.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

телекоммуникаций им. проф. М.А. Бонч-Бруевича

МЕТОД ОТСЛЕЖИВАНИЯ ИСТОЧНИКОВ РАСПРЕДЕЛЕННЫХ СЕТЕВЫХ АТАК С ВНЕСЕНИЕМ МЕТОК ПЕРЕМЕННОЙ ДЛИНЫ

В настоящее время активно развиваются методы отслеживания источников распределенных сетевых атак на основе внесения меток маршрутизаторов в заголовок IP-пакета. Под меткой будем понимать короткую цепочку бит, соответствующую значению хеш-кода от IP-адреса маршрутизатора, через который проходит пакет. Для хранения меток применяются малоиспользуемые поля IP-заголовка, такие как: поле идентификации длиной 16 бит и неиспользуемое поле флагов длиной 1 бит и др. Для оптимального использования свободного пространства в заголовке IP-пакетов можно ввести механизм маркировки, который бы позволял маршрутизаторам вносить в пакеты метки оптимальной длины. Так как каждый маршрутизатор в сети соединен с различным количеством соседей, то не всегда метка фиксированной длины является для него оптимальной. Например, если длина метки установлена равной 2 битам, а маршрутизатор соединен с двумя соседними маршрутизаторами, для различения которых нам достаточно в принципе 1 бита. Следовательно, второй бит фактически не используется. Обратная ситуация будет складываться, когда маршрутизатор соединен с пятью и более маршрутизаторами. Двухбитной метки будет не хватать для того, чтобы однозначно идентифицировать один соседний маршрутизатор. В этом случае можно было бы использовать метку длиной 3 бита, которая позволит однозначно идентифицировать до 8 соседних маршрутизаторов.

Так как каждый маршрутизатор знает сколько у него соседей, то он сам может установить длину метки, которая позволит ему однозначно идентифицировать один из соседних маршрутизаторов.. Маршрутизатор должен сообщить всем своим соседям длину необходимой ему метки n , чтобы в случае отслеживания атаки он мог однозначно определить от кого из них пришел данный пакет. В итоге у каждого маршрутизатора для каждого сетевого интерфейса устанавливается определенное значение длины метки, которую маршрутизатор должен сгенерировать при посылке пакета конкретному соседу. При этом данная метка является минимально-необходимой.

Каждый маршрутизатор знает IP-адреса соседних маршрутизаторов, так же он знает хеш-функции, используемые при метке пакетов. Следовательно, маршрутизатор может заранее вычислить для каждого из соседей значения его меток для каждой из набора хеш-функций и узнать, какие из них будут совпадать. Если обнаружались коллизии, то маршрутизатор вырабатывает поправочный коэффициент, при прибавлении которого ко всем IP-адресам соседей, они бы давали различные хеш-коды. Введение поправочных коэффициентов исключает возможность коллизии хеш-кодов от разных маршрутизаторов, а использование меток переменной длины позволяет наиболее эффективно использовать имеющееся свободное пространство в IP-заголовке.

Олимпиев А.А.

Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

ОБЪЕКТНАЯ МОДЕЛЬ КАК СРЕДСТВО ВЫЯВЛЕНИЯ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ РЕСУРСОВ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

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.

Данные мониторинга, поступающие от средств технологического управления (например, SNMP-менеджеров), позволяют создавать объекты, соответствующие реально существующим трактам передачи, направлениям обмена и т.д., а также определять фактические значения параметров функционирования объектов, соответствующих средствам телекоммуникаций – маршрутизаторам, мультиплексорам, коммутаторам.

Тем самым, появляется возможность сопоставления требуемого (планируемого) и фактического состояния телекоммуникационной сети на предмет их совпадения. Очевидно, что расхождения в данном случае могут быть обусловлены несоответствием настроек конфигурации оборудования – как объективно обусловленным следствием деятельности персонала, так и преднамеренных действий (в том числе воздействий со стороны незащищенной телекоммуникационной платформы). Так, например, достаточно простыми воздействиями на агентов управления первичных мультиплексоров может быть создан тракт передачи, не предусмотренный планом связи – за счет перераспределения использования канальных интервалов между интерфейсными модулями.

Задача сопоставления планируемого и фактического состояния сети связи может решаться в автоматическом режиме с формированием соответствующих диагностических сообщений – посредством сопоставления перечней динамически создаваемых объектов и значений параметров функционирования статических объектов, критических с позиций корректности использования ресурсов имеющихся средств телекоммуникаций.

Никитин В.Н., Юркин Д.В.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

телекоммуникаций им. проф. М.А. Бонч-Бруевича

АНАЛИЗ БЕЗОПАСНОСТИ СЕТЕЙ ШИРОКОПОЛОСНОГО РАДИОДОСТУПА

Защита передаваемых данных является необходимым условием функционирования как офисных так и городских сетей широкополосного радиодоступа.

В стандартах IEEE 802.1х механизмы защиты основаны на использовании криптографических алгоритмов и функционально замкнуты на канальном уровне модели OSI.

В первых версиях механизмы защиты были реализованы в протоколе WEP, однако в следствие отсутствия в нем механизмов удостоверения подлинности и целостности сообщений, слабой односторонней аутентификации корреспондентов и недостаточно стойкого шифрования он не обеспечивал должную безопасность беспроводных сетей.

В протоколе PKM, разработанном для сетей широкополосного радиодоступа городского масштаба стандарта IEEE 802.16, применены протоколы односторонней аутентификации с использованием асимметричной криптографии на цифровых сертификатах обладающие большей вычислительной стойкостью. В дополнение к усиленной аутентификации и автоматическому распределению ключевой информации PKM предполагает использование более стойких, чем RC4 в протоколе WEP, алгоритмов шифрования DES и AES.

Вместе с тем, ассоциации безопасности PKMv1 присущи недостатки, связанные с недостаточной защищенностью от криптоатак, основанных на методах повторной передачи сообщений и подмены корреспондентов, что послужило поводом к дальнейшему совершенствованию механизмов защиты в стандартах IEEE 802.1х, включая разработку протокола PKMv2 в стандарте IEEE 802.16e и разделению стандарта IEEE 802.11 на две ассоциации безопасности: pre-robust security network association, реализованной протоколом шифрования WEP или появившимся позднее протоколом TKIP (в котором добавлена функция контроля целостности сообщения MIC) с протоколом односторонней аутентификации «Запрос-ответ», и robust security network association, реализующей протокол шифрования и контроля целостности данных CCM и протокол аутентификации EAP.

Анализ реализованных протоколов показывает, что механизмы защиты, реализуемые в рамках ассоциации безопасности robust security network association стандарта IEEE 802.11i 2007 года будут обладать лучшей защищенностью и, в то же время, обеспечивают простоту предоставления телекоммуникационных услуг в сетях фиксированной связи. Вместе с тем следует

подчеркнуть, что данные механизмы защиты замкнуты на уровне радиоканала одной базовой станции и не обеспечивают не обеспечивают разграничения доступа пользователей к ресурсам сети связи оператора в целом.

Таким образом, для сетей широкополосного радиодоступа с глубокой интеграцией в современные телекоммуникационные системы, обеспечивающих мобильность пользователей и разграничение прав доступа к телекоммуникационным и информационным ресурсам, механизмов защиты канального уровня недостаточно и, как следствие, необходимо создание централизованной (в рамках телекоммуникационной системы оператора) подсистемы защиты сетевого уровня, требующее подключения всех БС к серверам аутентификации типа RADIUS или Active Directory.

Никифоров О.Г.

**Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»
О ПОДХОДЕ К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД
НА ОБЪЕКТАХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ**

Современные системы защиты информации на объектах телекоммуникационных систем от НСД, как правило, являются сложными и многопараметрическими. При этом каждый параметр системы оказывает влияние на эффективность ее функционирования в целом. При системном подходе к построению системы защиты информации на объектах телекоммуникационных систем необходимо построение методики, учитывающей все возможные факторы, оказывающие влияние на эффективность ее функционирования в различных возможных на практике условиях.

В докладе рассматривается подход к построению комплексной методики оценивания эффективности системы защиты информации от НСД, учитывающий следующие основные практически важные аспекты, характеризующие технические средства защиты и условия их функционирования на объектах:

- скрытность технических средств защиты от средств разведки нарушителя, определяющая возможности нарушителя по выявлению функциональных характеристик средств защиты;
- возможные способы обхода средств защиты, предпринимаемые нарушителем;
- возможности технических средств защиты выполнять свои задачи в условиях попыток их обхода;
- техническая надежность средств защиты;
- возможности сил реагирования по ликвидации физических и информационных угроз объекту.

Комплексная методика базируется на модели процесса защиты от НСД, построенной на основе математических методов анализа сетей, которая позволяет получить комплексную оценку эффективности системы защиты в зависимости от скрытности технических средств защиты, их возможностей противостоять обходу со стороны нарушителя, их технической надежности, а также от возможностей сил реагирования по ликвидации возникших угроз. Она содержит следующую совокупность частных методик:

- методику оценивания скрытности технических средств защиты информации от технических средств разведки, основанную на анализе демаскирующих признаков средств защиты и имитационной статистической модели для решения задачи их распознавания;
- методику прогнозирования характеристик средств защиты для случая попытки их обхода нарушителем которая представляет собой методический аппарат для решения сложной слабо формализуемой задачи прогноза технических характеристик средств защиты, базирующийся на теории экспертных оценок;
- методику оценивания технической надежности систем защиты, разработанную на основе классических методов и моделей теории надежности и основанную на анализе надежности различных практически возможных структур систем защиты;
- методику оценки возможностей систем защиты по ликвидации физических и информационных угроз, выполненную на основе модели конфликта между нарушителем и силами защиты.

Орлов К. М

**Россия, Санкт-Петербург, 24 Центральный НИИ Министерства обороны Российской Федерации
АНАЛИЗ КРИТЕРИЕВ КАЧЕСТВА ВИЗУАЛИЗАЦИИ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ
СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**

Задача построения эффективных систем управления различного назначения, максимально реализующих возможности современных информационных технологий, является традиционной и всегда актуальной. Пожалуй, в первую очередь это относится к подсистемам интеллектуальной, аналитической и информационной поддержки действий оператора в процессе оценки обстановки (наиболее «интеллектуально ёмкого» и сложного этапа аналитического обеспечения систем управления), выработки вариантов действий и непосредственного принятия решений.

Одним из «неисчерпанных» резервов в этой части, по мнению автора, являются возможности автоматизированной комплексной визуальной обработки и многомерного отображения массива информации, который поступает на автоматизированное рабочее место (АРМ) оператора.

Качество подсистем визуализации информации (ПВИ) современных автоматизированных систем в защищенном исполнении (АСЗИ) традиционно оценивается рядом частных критериев типа: технические показатели ПВИ (характеризующие размеры мониторов, их разрешение, динамичность, цветовые и графические возможности (в том числе, 3D-график) устройств отображения, вычислительные ресурсы коммуникационных средств АСЗИ); алгоритмические и функциональные показатели (характеризующие потоки входных и выходных сообщений ПВИ, особенности программных средств и информационно-справочных сегментов АСЗИ).

При этом, крайне редко используются «сугубо информационные» критерии и показатели качества АСЗИ и ПВИ типа: оперативность (своевременность) отображения данных, ценность и достоверность представляемой информации (её актуальность, точность, безошибочность), устойчивость, скрытность и непрерывность (полнота, безизбыточность) данных, степень защищенности данных (конфиденциальность (разграничение доступа, степень ознакомления), доступность, целостность), наглядность данных (многомерность, латентность и т.п.), а также «классические» (по В.И. Корогодину) показатели качества (фиксируемость (инвариантность, бренность, изменчивость, транслируемость, размножаемость, мультипликативность), действенность (семантика, полиплетность, полезность, истинность) и информации).

Наконец, практически не используются интегральные (сводные, обобщённые) критерии и показатели качества отображаемых в ПВИ АСЗИ данных типа ценность информации (например, по критериям А.А. Харкевича, И.И. Когана и др.), информационная эффективность, информационно-техническая избыточность и т.п.

На основе выполненного анализа критериев качества визуализации информации в АСЗИ специального назначения предложена «пилотная» система критериев и показателей оценки качества ПВИ АСЗИ (систем отображения информации АСУ), которая, по мнению автора, позволяет перейти к квалиметрическому анализу действующих и разрабатываемых АСЗИ, обоснованию требований и оптимизации параметров перспективных средств и систем визуализации АСЗИ с учётом специфики информационных преобразований.

Именно подобный подход, позволяет, как показывает анализ, количественно обосновывать требования к качеству ПВИ АСЗИ, и, следовательно, аргументировано решать многовариантные задачи синтеза и оптимизации проектных решений сложных комплексов и систем при возрастании объёма собираемых, распределяемых, обрабатываемых и отображаемых данных.

Восприятие разнородной информации оператором АСУ в процессе функционирования системы «оператор - отображение информации» имеет ряд важных особенностей, которые также учитываются в представленном подходе и могут быть использованы для наращивания возможностей современных (при их модернизации) и разрабатываемых ПВИ АСЗИ.

Перминов С.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ИСПОЛЬЗОВАНИЕ ОНТОЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ ПОИСКА
ИНФОРМАЦИОННЫХ АНОМАЛИЙ ЧЕРЕЗ WEB**

Под аномалией понимается отклонение от нормы. Поиск аномалии сводится к нахождению совокупности данных, свидетельствующих о том, что существует отклонение от нормы. Под поиском через web подразумевается уточнение, что информация, в которой осуществляется поиск, должна быть представлена в виде множества web-документов (в форматах данных HTML, XML и производных от XML).

Рассмотрим применимость существующих поисковых технологий в web для обнаружения информационных аномалий в web-документах. Поиск информации в глобальной сети в том виде, в котором он существует сейчас, не является совершенным. Можно выделить, по крайней мере, три распространенные проблемы поисковых машин:

1. Нерелевантность поиска.

2. Большое разнообразие способов представления и организации данных в глобальной сети web.

3. Неполнота поиска.

Нерелевантность можно определить как несоответствие результата поиска ожиданиям пользователя. При поиске информационных аномалий это может определяться непредставительной совокупностью данных, выбранной пользователем для описания информационной аномалии, что тесно связано с проблемой отсутствия единообразия данных в web.

Неполнота поиска информационных аномалий связана с возможностью различным образом представить одно и то же отклонение от нормы, другими словами возможностью описать семантику аномалии множеством синтаксических конструкций.

Для того, чтобы осуществить попытку смыслового поиска в существующих web-документах, необходим предварительный семантический анализ их содержимого, его основная цель – улучшить структурирование информации в документах. Семантический анализ развивает идею распознавания образов, другими словами чрезвычайно сжатых представлений документов, в которых не учитывается ни их конкретное содержание, ни лексика. Можно сказать, что семантический поиск – это поиск по ключевым понятиям, а семантическое представление документа – это множество присутствующих в нем понятий или семантических категорий.

Один из подходов к семантическому анализу заключается в использовании онтологического моделирования для описания предметной области, в рамках которой производится поиск аномалий в web-документах. Согласно распространенному определению онтология в информационной системе – это точная спецификация концептуализации. Согласно формальному определению онтология состоит из трех множеств: множества сущностей, множества отношений между сущностями и множества правил вывода над отношениями.

В докладе предлагается подход к поиску информационных аномалий, где основной задачей является не сам статистический алгоритм поиска, а онтологическое моделирование, посредством которого осуществляется предварительная обработка и формализация базы данных web-документов. В частности рассматривается использование при моделировании справочной онтологии на языке OWL, которая построена на базе описания семантических классов русского языка, предложенных Тузовым В.А.

Рожнов М.Д., Шерстюк Ю.М.

Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

НАЗНАЧЕНИЕ ПРАВ И ПОЛНОМОЧИЙ В СИСТЕМЕ ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ СРЕДСТВАМИ ТЕЛЕКОММУНИКАЦИЙ

Технологическое управление (ТУ) инфотелекоммуникациями рассматривается как управление сетевыми элементами (СЭ) без учета их взаимодействий (сопряжений). В инфотелекоммуникационной сети к качеству СЭ могут выступать любые программные и технические средства, образующие эту сеть – мультиплексоры, коммутаторы, серверы телематических и информационных служб и т.д., имеющие в своем составе агентов управления.

Для осуществления ТУ создается служба технологического управления (СТУ) – как совокупность средств автоматизации ТУ, используемых соответствующими должностными лицами (ДЛ) – пользователями этой службы, имеющими определенные права и полномочия.

При использовании определенного подхода СТУ создается на каждом узле связи (УС) сети и включает в свой состав сервер ТУ, менеджеры ТУ и приложения пользователей (ПП) ТУ (клиентские приложения). Совокупность всех СТУ УС сети при условии возможности обмена данными между ними образует сетевую службу технологического управления. Одной из особенностей указанного выше подхода является наличие механизма проксирования – ПП имеют возможность обращения только к одному («локальному») серверу ТУ – для дистанционного (удаленного) ТУ ПП посылает запросы локальному серверу ТУ, который авторизуется от имени пользователя у сервера ТУ корреспондирующего УС и передает ему данный запрос, получает результаты его выполнения и передает их ПП.

Наличие такого механизма дает возможность определить понятие прав на технологическое управление как прав доступа пользователя к локальной и, возможно, удаленным СТУ.

Полномочия ДЛ определяют его возможности по получению сведений о состоянии СЭ и изменению этого состояния посредством выдачи управляющих воздействий, в конечном итоге представляющих собой команды на изменение значений параметров MIB, поступающие к соответствующему агенту управления.

Наличие в СТУ механизма поддержки назначения и контроля прав и полномочий позволяет в потенциально полносвязной сетевой СТУ организовывать различные варианты ее использования с позиций предоставления возможностей ТУ ДЛ различных УС.

Если добавить в СТУ механизм интегральной оценки состояния ОМУ и внести в сервер ТУ функциональность агента управления, то становится возможным строить иерархические сети СТУ, в которых СТУ узла видна для СТУ старшего по отношению к ней уровня в виде СЭ, состояние которого интегрально отражает состояние всех СЭ подчиненной СТУ. Данное решение открывает ряд новых возможностей по организации сетевой СТУ как сочетания одноранговых и иерархических сетей, но существенно усложняет решение задачи назначения прав и полномочий в масштабах сети. В связи с этим целесообразна разработка средств автоматизированного решения указанной задачи – как части решения общей задачи планирования сети связи. Задача назначения прав и полномочий хорошо формализуема и имеет алгоритмическое решение, основывающееся на различных критериях наблюдаемости объектов технологического управления.

Салко Н.В.

**Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского
К ВОПРОСУ ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В
БЕСПРОВОДНЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ**

Среди разнообразных технологий беспроводной передачи данных необходимо выделить технологию WIMAX. WIMAX (Worldwide Interoperability for Microwave Access) стандартизирован институтом IEEE технологий как широкополосная беспроводная связь, дополняющая линии DSL и кабельные технологии в качестве альтернативного решения проблемы "последней мили" на больших расстояниях. Учитывая эти характеристики необходимо сказать о большой привлекательности технологии WIMAX для пользователей. Технология позволяет эффективно использовать такие услуги, как передача мультимедиа данных с высокими скоростями на относительно большие расстояния, а также IP телефония, видеотелефония и т.д.

С ростом популярности стандарта возникает необходимость обеспечения безопасности данных передаваемых в сетях WIMAX. Учитывая то, что WIMAX это технология беспроводной связи, существует потенциальная возможность перехвата нарушителем передаваемых данных. Соответственно вопросу обеспечения безопасности в стандарте WIMAX уделено особое внимание. Существует, так называемый, «Подуровень Безопасности», который функционирует на канальном уровне (если рассматривать технологию с точки зрения модели OSI) и отвечает за авторизацию и аутентификацию.

Аутентификация реализуется путем использования протокола обмена открытыми ключами, при этом обеспечивается не только аутентификация, но и создание ключей шифрования. В стандарт WIMAX 802.16e–2005 определен протокол управления (PKM – Privacy Key Management), поддерживающий три типа аутентификации: основанная на RSA – цифровые сертификаты X.509 и RSA шифрование; основанная на EAP (опционально); основанная на RSA после EAP. Базовая станция (БС) сравнивает Абонентскую Станцию (АС) и подписчика услуги, и, соответственно, определяет список сервисов, к которым подписчику разрешен доступ. Таким образом, через обмен ключей аутентификации (АК), БС определяет подписчика и доступные для него сервисы.

По завершению аутентификации, АС отправляет запрос на авторизацию БС. Этот запрос, также называют запросом Ассоциации безопасности (SAID). Запрос на идентификацию включает сертификат X.509 БС, алгоритм шифрования и криптографический ID. В ответ БС проводит необходимую процедуру подтверждения доступа (запрашивая сервер Аутентификации Авторизации и Билингации (AAA) в сети) и отправляет обратно ответ авторизации, который содержит АК, зашифрованный открытым ключом АС, ключ времени жизни и SAID. После прохождения стадии авторизации, AAA посредством БС периодически проводит процедуру повторной инициализации АС. В стандарте 802.16e–2005 определено, что весь трафик, проходящий в сетях WIMAX, должен быть зашифрован с использованием алгоритма блочного шифрования AES. Необходимо отметить, что на сегодняшний день не существует эффективных методов получения несанкционированного доступа к информации зашифрованной алгоритмом шифрования AES.

Резюмируя вышеизложенное можно сделать выводы:

- 1) стремление операторов к тому чтобы пользователи и устройства, подключенные к их сетям действительно были теми, за кого себя выдают, а также, что они получают доступ к тем услугам, за которые они заплатили, обеспечивается применением процедур аутентификации и авторизации;
- 2) требование пользователей к конфиденциальности передаваемой информации обеспечивается применением алгоритма блочного шифрования.

Сидельникова Е.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ВЕРИФИКАЦИЯ ПРАВИЛ ФИЛЬТРАЦИИ ПОЛИТИКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ
СЕТИ НА ОСНОВЕ ИСЧИСЛЕНИЯ СОБЫТИЙ И АБДУКТИВНОГО ВЫВОДА**

Представляемая работа посвящена разработке автоматизированной методики верификации правил фильтрации политики безопасности компьютерной сети на основе исчисления событий и абдуктивного вывода.

В работе рассмотрено моделирование поведения межсетевого экрана (МЭ) при помощи исчисления событий. Приведена предметно-независимая аксиоматика исчисления событий, а также модификация аксиоматики для решения рассматриваемой задачи. Рассмотрена предметно-зависимая аксиоматика исчисления событий, используемая для формализации правил МЭ, а также пример работы конкретного МЭ в терминах исчисления событий.

Таблица доступа для межсетевого экрана состоит из упорядоченных правил, разрешающих или запрещающих пересылку пакетов с определенным адресом и портом источника и получателя для заданного протокола. Аномалия в таблице доступа МЭ возникает, если условия двух или более правил пересекаются. В работе представлена классификация аномалий по типу пересечения условий правил, и рассмотрены возможные стратегии разрешения для каждого типа аномалий. Предложена

модель межсетевых аномалий в правилах фильтрации межсетевых экранов на языке исчисления событий.

В работе разработаны алгоритмы поиска и разрешения аномалий в правилах фильтрации политики безопасности компьютерной сети при помощи абдуктивного вывода. Один из алгоритмов нахождения и разрешения аномалий в правилах фильтрации использует стратегию, которая заключается в разбиении условий правил МЭ на непересекающиеся части и удалении затененных частей (стратегия разбиения). Данная стратегия может применяться ко всем типам аномалий и ее применение не меняет поведение МЭ.

Также в работе предложен алгоритм нахождения аномалий всех типов, и нахождение аномалий только одного определенного типа. Рассмотрены алгоритмы применения всех типов стратегий разрешения аномалий и проведен их сравнительный анализ с точки зрения количества введения новых правил МЭ, возможных изменений работы МЭ, проведен анализ временной эффективности предложенных алгоритмов.

Проведены эксперименты, оценивающие эффективность применения предложенной методики верификации правил фильтрации политики безопасности компьютерной сети. В работе представлены итоги экспериментов.

Программный прототип данного подхода для анализа и верификации политик фильтрации реализован на языке Java на основе использования CIFF, библиотеки для SICStus Prolog, реализующей алгоритм абдуктивного вывода.

Работа выполнена при финансовой поддержке РФФИ (проект №07–01–00547), программы фундаментальных исследований ОНИТ РАН (контракт №3.2/03) и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST (контракт № 021186–2) и других проектов.

Сорокин И.В., Копыльцов А.В.

Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ОСНОВНЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ ЗОМБИ-СЕТЕЙ

Описаны основные подходы для противодействия одной из самых серьезных киберугроз за последние 10 лет – зомби-сети. Зомби-сеть или ботнет обозначает сеть компьютеров, зараженных вредоносным программным обеспечением называемым бот-агентом. С помощью подобных бот-агентов злоумышленник может использовать ресурсы зараженного компьютера для решения различного рода криминальных задач: от рассылки спама до атак на государственные сети. Для выявления самого факта существования бот-сети используются различные методы анализа сетевой активности. Анализ может быть как вертикальным, т.е. выявлять конкретные зараженные компьютеры, так и горизонтальным, позволяющим оценить группы машин входящих в бот-сеть. Для этого используются различные методы и алгоритмы из теории машинного обучения. Так решение задач классификации и кластеризации при анализе сетевого трафика позволяет выявлять не только сами зараженные машины, но и различные характеристики всей бот-сети: масштаб, мощность, тип и направление атак и т.п. Полученная информация может использоваться как для противодействия, так и для прогнозирования угроз осуществляемых с помощью бот-сетей. На сегодняшний день разработка систем подобных описанным в данной работе является одной из актуальных проблем в антивирусной индустрии.

Суворов А.А.

Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
АРХИТЕКТУРА СЕТЕЙ СВЯЗИ С РАЗГРАНИЧЕНИЕМ ДОСТУПА НА ОСНОВЕ
ШЛЮЗОВ КОНТРОЛЯ ДОСТУПА

В сетях связи с разграничением доступа, существует проблема распределенного контроля потоков данных между узлами сети, состоящая в контроле и мониторинге установления сеансов связи по одной из трех возможных схем: «точка-точка», «звезда» или «каждый с каждым», в рамках которых осуществляется одно- или двусторонний обмен данными между двумя или несколькими узлами сети. Для решения этой проблемы предлагается архитектура сетей связи с разграничением доступа, основанная на использовании шлюзовых технологий, объектом доступа в которой является информация, циркулирующая в пределах сеансов связи.

Для организации защиты сети связи с разграничением доступа должны быть добавлены следующие компоненты: шлюзы контроля доступа (ШКД), центр управления доступом (ЦУД) и Пульты Управления (ПУ). Шлюзы контроля доступа обеспечивают распределенную защиту узлов сети и производят непосредственный контроль над установлением сеансов связи. Каждый оконечный узел системы подключается к сети связи через ШКД. Центр управления доступом используется как рабочее место администратора сети, обеспечивающее автоматизированное централизованное принятие решений о возможности установления сеансов связи между конечными узлами сети, отправляя на соответствующие ШКД управляющие команды. Пульты управления предназначены для

инициации сеансов связи абонентами системы: создание новых сеансов, подключение и выход из установленных, и отклонение, при необходимости, входящих запросов на установление сеанса. Также ПУ предоставляет абоненту информацию о текущем состоянии и список пользователей сети и сеансов, к которым возможно подключение.

Центр управления доступом принимает решение о доступе основываясь на гибкой политике безопасности и текущем состоянии системы. В качестве модели контроля доступа используются мандатный и дискреционный контроль доступа. Шлюзы контроля доступа решают задачу контроля потоков данных путем осуществления коммутации соединений между узлами и сетью передачи данных. В состоянии бездействия все соединения между узлами запрещены. В момент создания сеанса связи абонент указывает участников сеанса, используя пульт управления. Центр управления доступом проверяет легитимность запрашиваемого сеанса связи и отправляет на ШКД команды, разрешающие создать между участниками сеанса каналы связи, по которым будет передаваться информация.

Предлагаемая архитектура накладывает несколько ограничений: требуется сеть шифрованной связи, возможно использование только одного приложения в сети связи и за оконечным узлом сети может работать только один абонент. Таким образом, решение может быть использовано для построения защищенных информационно-технических каналов связи, таких как VoIP и видеоконференцсвязь. При этом обеспечивается автоматизация принятия решений распределенного контроля доступа к потокам данных, основывающаяся не только на используемой модели контроля доступа, но и на состоянии системы. Используемое централизованное управление предоставляет администратору возможность контролировать все происходящие в системе события в режиме реального времени. Применение пультов предоставляет пользователю два основных преимущества: возможность отказа от установления сеанса связи и возможность отслеживания состояний установленных с ним сеансов связи. Также важным преимуществом решения является его прозрачность для всего оборудования и программного обеспечения сети связи. Предложенное решение показывает возможность применения шлюзовых технологий для решения проблемы распределенного контроля потоков данных в сетях связи с разграничением доступа.

Таран В.В., Шерстюк Ю.М.

Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»,

ЗАО «Институт инфотелекоммуникаций»

СРЕДСТВА СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ PYTHON-ПРОГРАММ

Программное обеспечение (ПО) является неотъемлемой частью любой автоматизированной системы (АС), во многом определяющей ее функциональные возможности и потребительские свойства, существенно влияющей на конечную эффективность всей автоматизированной системы.

К АС, в процессе функционирования которых осуществляется хранение, обработка и передача информации ограниченного доступа, предъявляется ряд специальных требований по обеспечению информационной безопасности. Одним из таких требований является отсутствие недеklarированных возможностей (НДВ) в их ПО.

Проверка ПО на отсутствие НДВ имеет целью подтверждение выполнения двух основных требований:

- соответствие между программной документацией, исходными текстами и исполняемыми модулями программ;
- безопасность программ с позиций их возможности нарушить (способствовать нарушению) конфиденциальность, целостность или доступность информации в той вычислительной среде, в которой они выполняются.

Нормативные требования по отсутствию НДВ определены в соответствующих нормативных документах.

Проведение испытаний ПО на отсутствие НДВ невозможно без использования ряда инструментальных средств – программ, автоматизирующих выполнение соответствующих операций. Исходя из содержания статических и динамических проверок, таких программных инструментальных должно быть по крайней мере три:

- программа статического анализа текстов испытываемых программ;
- программа расстановки маркеров в текстах испытываемых программ;
- программа обработки результатов выполнения программ в ходе их динамического анализа, получение которых обеспечивается размещенными в программах маркерами.

Указанные инструментальные программные средства могут представлять собой как отдельные программы (наборы программ), так и программные комплексы, ориентированные на применение с учетом характера сертифицируемого ПО, использованных языков программирования, требуемого уровня контроля НДВ.

С учетом роста объема ПО, разрабатываемого с использованием языка программирования Python, был разработан набор инструментальных программ анализа python-приложений,

позволяющих решать задачи статических и динамических сертификационных испытаний программных комплексов, функционирующих в операционной среде МСВС. Имеющийся в настоящее время опыт применения этих программ показал их состоятельность и эффективность как средств поддержки проведения сертификационных испытаний современного ПО – в частности, для средств управления телекоммуникациями с повышенными требованиями к безопасности.

Хейстонен Д.П.

Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»
АНАЛИЗ ВЛИЯНИЯ ЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ НА РАБОТУ
ИНФОКОММУНИКАЦИОННОЙ СЕТИ

Рост потребительского спроса на инфокоммуникационные ресурсы (т.е. на информационные и телекоммуникационные службы и услуги) приводит к необходимости их анализа и оптимизации. Введение в инфокоммуникационную сеть централизованной системы управления позволит своевременно обнаруживать «слабые» места и оперативно принимать решения по их устранению, например путем регулирования пропускных способностей отдельных участков сети, распределения и перенаправления потоков информации и т.д.

Отлаженная работа системы управления способствует повышению надежности передачи трафика и улучшению контроля за передаваемыми данными для пользователя и наиболее эффективно используется оборудования для поставщика служб и услуг.

Для оценки влияния системы управления на работу инфокоммуникационной сети необходимо решить следующие задачи:

- построить математическую модель сети;
- определить ее вероятностно-временные характеристики (ВВХ);
- сравнить полученные ВВХ с характеристиками сети в которой есть централизованная система управления.

При сравнении характеристик не стоит забывать о возможных функциях по управлению безопасностью, реализованных в централизованной системе управления, которые довольно трудно оценить количественной характеристикой.

В докладе раскрываются пути решения данных задач.

Хейстонен Д.П.

Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин»
ПОВЫШЕНИЕ ОТКАЗОУСТОЙЧИВОСТИ ЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ

Удаленные системы управления строятся по принципу «менеджер-агент» (клиент-серверная архитектура). Менеджер представляет собой процесс, формирующий и отправляющий команды управления и принимающий уведомления на них. Агентом называется процесс, который управляет соответствующими объектами. При централизованном управлении на устройстве, в котором реализован менеджер, накапливается значительное количество управляющей и статистической информации, собранной агентами со всей сети. Для уменьшения вероятности потери накопленных статистических данных и оставлении инфокоммуникационной сети без системы управления необходимо предусмотреть резервную систему управления.

Введение резерва в централизованную систему управления повысит ее отказоустойчивость, но вместе с тем возрастет объем служебного трафика, связанный с синхронизацией баз управления между основным и резервным менеджерами. Рост объемов служебного трафика несомненно скажется на ухудшении ВВХ передачи пользовательских сообщений, т.к. информация управления, в связи со своим предназначением, должна иметь более высокий приоритет, чем пользовательский трафик.

Для снижения нагрузок на инфокоммуникационную сеть, связанных с увеличением количества служебной информации, необходимо расположить основную и резервную системы управления на менее загруженных участках сети. Выявить самые мало загруженные участки сети можно с помощью предлагаемых в докладе моделей и соответствующих им методик расчета. Проведя математический расчет и выполнив условия политики безопасности, достигается оптимальное решение по критерию «эффективность-безопасность».

Хвостунов Ю.С.

Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»
АВТОМАТИЗИРОВАННЫЙ КОМПЛЕКС СРЕДСТВ СКОРОСТНОЙ АДАПТИВНОЙ
ПОМЕХОЗАЩИЩЕННОЙ СИСТЕМЫ РАДИОСВЯЗИ

1. Перспективные автоматизированные системы радиосвязи дециметрового диапазона должны удовлетворять следующим требованиям:

- обеспечивать устойчивую (с надежностью не хуже 0,99) многоканальную связь при воздействии различных дестабилизирующих факторов (помехи, сдвиг рабочих частот, многолучевость и т.д.);

- обеспечивать одновременную передачу и прием данных, обмен речевой информацией на расстоянии до 3000 км на трассах с стационарными и подвижными объектами;

- обеспечивать работу с существующим парком систем радиосвязи

2. Предлагаемый комплекс средств скоростной адаптивной помехозащищенной системы связи декаметрового диапазона удовлетворяет всем предъявляемым требованиям. Данный комплекс обеспечивает:

- передачу и прием информации по радиоканалам декаметрового диапазона (диапазон рабочих частот 1,6–30 МГц) в адаптивном режиме с псевдослучайной перестройкой рабочей частоты при работе со скоростями до 64 Кбит/с с реализацией алгоритма исправления ошибок;

- ведение радиосвязи с адаптацией (в зависимости от качества канала связи) по частоте, скорости приема/передачи, помехоустойчивому коду, виду модуляции, длине пакета;

- обеспечение одновременной работы (включая речь) с несколькими корреспондентами через один комплект аппаратуры (с суммарной скоростью работы до 64 Кбит/с);

- сопряжение с установленным и перспективным оборудованием передачи данных по интерфейсам информационного обмена, выдаваемого заказчиком;

- устойчивую работу при воздействии различных дестабилизирующих факторов;

- дуплексный (при условии разнесения передающего и приемного АФУ), полудуплексный или симплексный обмен информацией между различными абонентами сети по каналам связи на дальности связи до 3000 км в условиях внешних воздействий;

- высокий коэффициент готовности предоставляемого канала связи в организованной сети (более 0,99).

Рассматриваемый комплекс базируется на использовании технологии псевдослучайной перестройки рабочей частоты во всем используемом диапазоне радиочастот:

- время работы на одной рабочей частоте 50 мс и менее;

- период псевдослучайной последовательности перестройки рабочей частоты существенно больший периода функционирования системы (равен $2^{128}-1$);

- применяется синхронно перестраиваемый пассивный узкополосный преселектор (полоса пропускания ~3%), что исключает блокирование мощной помехой радиоприемного тракта.

Комплекс не требует использования систем единого времени, зондирования радиозфира, а также не использует в процессе обмена информацией специальные сигналы или кодограммы синхронизации.

В настоящее время:

- проработаны функциональные блоки аппаратуры быстродействующей телекодовой связи, проведены испытания;

- разработан и изготовлен наземный комплекс управления (высокоскоростной модем), проведены испытания комплекса;

- разработаны, и изготовлены макеты передатчиков и приемников, проведены испытания;

- разработаны и изготовлены макеты широкополосных АФУ различного вида (в том числе с возможностью размещения на самолете), проведены испытания.

В процессе испытаний проведены:

- всесторонние лабораторные испытания всех составляющих адаптивной системы радиосвязи с псевдослучайной перестройкой рабочей частотой на имитаторах КВ радиоканала, и с использованием реальных радиосредств;

- проведены длительные трассовые испытания, которые подтвердили все заявленные характеристики.

Чечулин А.А.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОБНАРУЖЕНИЕ И ПРОТИВОДЕЙСТВИЕ СЕТЕВЫМ АТАКАМ НА ОСНОВЕ КОМБИНИРОВАННЫХ
МЕХАНИЗМОВ АНАЛИЗА ТРАФИКА**

Разнообразие угроз, подстерегающих пользователя, работающего в сети, огромно. Часть из них является платой за использование сложных информационных технологий, уязвимых к внешним воздействиям, другая часть сопряжена с деятельностью людей. Поэтому, актуальной задачей в области обеспечения безопасности информационных ресурсов является защита от сетевых атак. Существующие средства защиты не всегда справляются с новыми видами атак, поэтому важным направлением исследований и разработок является создание систем защиты, способных защищать не от конкретных атак, а от целых классов атак. В данной работе рассматриваются методы

обнаружения и противодействия сетевым атакам, основанным на протоколах транспортного и сетевого уровней стека TCP/IP.

Существующие сетевые атаки можно разделить на четыре основных класса: сбор информации, основанный на анализе результата обработки пакетов; атаки, базирующиеся на ошибках в обработке пакетов; сканирование хостов и сетей за счет использования ошибок в обработке сессий; сканирование, основанное на корректном установлении соединений. Для каждого класса атак предлагается использовать свои механизмы защиты (методы фильтрации и нормализации отдельных пакетов, методы анализа сессий, методы анализа сетевого взаимодействия).

В докладе предлагается подход к многоуровневому комбинированию алгоритмов в виде системы базовых классификаторов, обрабатывающих данные о трафике, и мета-классификатора, осуществляющего выбор весовых коэффициентов для каждого алгоритма, что позволяет объединить достоинства отдельных методов и уменьшить их недостатки. Выбор весовых коэффициентов может осуществляться отдельно для каждого узла сети, что позволит учесть особенности работающих сетевых приложений на каждом хосте.

Общий механизм обнаружения и противодействия сетевым атакам можно представить как совокупность следующих компонентов: сенсор – анализатор сетевого трафика; детектор – механизм обнаружения, принимающий на вход данные от анализаторов сетевого трафика и дающий на выходе правила фильтрации; мета-классификатор – модуль, принимающий на вход правила фильтрации от детекторов и дающий на выходе итоговые правила фильтрации, учитывающие вычисленные на основе данных от анализаторов весовые коэффициенты каждого детектора; фильтр – компонент блокирования, модификации или сдерживания трафика на основе правил, полученных от мета-классификатора.

Работа выполнена при финансовой поддержке РФФИ (проект №07–1–00547), программы фундаментальных исследований ОИТВС РАН (контракт №3.2/03), Фонда содействия отечественной науке и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST (контракт № 021186–2).

Шерстюк К.Ю.

Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

МОНИТОРИНГ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ НА СРЕДСТВА ТЕЛЕКОММУНИКАЦИЙ

Телекоммуникационные сети (ТКС) и их сетевые элементы (СЭ) могут быть такими же объектами программных атак (ПА), как и серверы и рабочие станции вычислительных сетей. Фактически любой СЭ ТКС, имеющий в своем составе вычислительную среду с выполняемым в ней программным обеспечением и с возможностью сетевого доступа к ней потенциально является объектом ПА.

Цели ПА на СЭ ТКС достаточно очевидны – частичное или полное нарушение функционирования, сбор данных (вскрытие структуры сети, системы адресования и др.), нелегитимное использование телекоммуникационного ресурса и т.д. Можно считать, что цель ПА – это получение значений параметров функционирования СЭ и/или их изменение, т.е. получение сведений о свойствах и состоянии СЭ и/или перевод СЭ в состояние, соответствующее цели ПА.

В то же время средства управления связью в конечном итоге решают ту же задачу – сбор сведений о состоянии объектов мониторинга и управления (ОМУ), поддержание ОМУ в требуемом состоянии, а при необходимости – перевод ОМУ в новое (требуемое) состояние. Таким образом, средства управления телекоммуникациями и средства осуществления ПА как наступательных информационных операций решают задачи, диаметрально противоположные по цели и во многом схожие по объектам воздействия.

Противодействие ПА предполагает создание и применение соответствующих средств информационной защиты (СИЗ), обеспечивающих предупреждение и обнаружение ПА, минимизацию их последствий, а возможно – и активное (в т.ч. превентивное) воздействие на источники атак.

Более того, возможности СЭ современных ТКС по их мониторингу и управлению, существующие решения по созданию средств автоматизации управления связью позволяют реализовывать комплексные решения по управлению ТКС, включая их безопасность, и рассматривать СИЗ как элементы средств и сетей телекоммуникаций.

Опыт выполненных работ показал, что средства технологического управления ТКС при соответствующей доработке могут выступать в качестве:

- средства обнаружения атак (детектора атак) определенных разновидностей на СЭ;
- средства управления СИЗ;
- средства, обеспечивающего изменение состояния ОМУ как реакцию на обнаруженные ПА.

Таким образом, средства ТУ могут сыграть существенную роль в обеспечении безопасности и устойчивости ТКС – особенно для средств телекоммуникаций, для которых, в отличие от вычислительных сетей, проблема ПА является не менее актуальной, а средства ее решения не столь очевидными.

Шоров А.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АНАЛИЗ БИОЛОГИЧЕСКИХ ПОДХОДОВ ДЛЯ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ
ОТ ИНФРАСТРУКТУРНЫХ АТАК**

Данная работа посвящена исследованию биологической метафоры для защиты от инфраструктурных атак на компьютерные сети.

Для построения новых средств защиты предлагается метафора, основанная на применении биологических подходов. В работе рассматриваются несколько возможных механизмов защиты от инфраструктурных атак на основе биологических подходов: механизмов, созданных по аналогии с живыми клетками; механизмов, базирующихся на подходе «нервная система сети»; механизмов, основанных на иммунных системах.

Основу систем, созданных по аналогии с живыми клетками, составляют клетки, как активные элементы нижнего уровня биосистемы, которые могут получать и принимать данные, самовоспроизводиться делением, что дает возможность поддерживать работоспособность системы в случае её повреждения. Передача данных может происходить от клетки к клетке или с помощью потока крови, сигнал попадает на рецептор и приводит к какому-либо ответному действию соседних клеток. В компьютерной сети предлагается подобный механизм работы. Монитор (сканирующий трафик) отправляет собранные данные на IDS, которая, после получения и обработки этих данных, вносит новые правила в межсетевые экраны.

Механизмы защиты, базирующихся на подходе «нервная система сети», обычно предполагают создание распределенного механизма обнаружения вторжений и организации противодействия различного рода атакам. В каждой подсети выделяется специальный компонент, который, с точки зрения биологического подхода, играет роль «сомы» в нейроне (сوما является центральной частью нейрона). Этот компонент реализует большую часть процессов обработки и анализа информации, а также координацию действий близлежащих сетевых устройств. Функцию «дендритов» нейрона выполняют другие сетевые устройства (например, маршрутизаторы). Они передают большую часть информации о состоянии сети соме. Сомы связаны между собой с помощью виртуальной частной сети (VPN), которая играет роль «аксона» и передает обработанную информацию о состоянии данного сегмента сети (нейрона) другим сомам, находящимся в удаленных сегментах сетей, а также получает информацию о состоянии других нейронов (сетей).

На основе иммунных систем предлагаются подходы для обнаружения атак и выработки соответствующей реакции на них. В качестве примера механизмов, основанных на иммунных системах, рассматривается подход, основанный на алгоритме отрицательного отбора (Negative Selection Algorithm). При построении модели исследователи разделяют все пространства объектов и (или) событий на две части: «свой» (self) и «чужие» (nonself). Для того чтобы система могла точно определить, где свой, а где чужой, используются детекторы, которые реагируют только на «чужие» элементы. Сгенерированный детектор тестируют, проверяя «правильный» набор данных. Если детектор срабатывает, его удаляют и генерируют новый. Таким образом, создается набор детекторов, которые не обнаруживают «легитимные» события. При этом возникает проблема «дыр». Детекторы, натренированные на одном типе данных, могут пропускать данные, похожие на те, на которых производилось обучение. Для устранения данной проблемы необходимо использовать различные типы наборов данных для генерации детекторов.

Работа выполнена при финансовой поддержке РФФИ (проект №07–01–00547), программы фундаментальных исследований ОНИТ РАН (контракт №3.2/03) и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST (контракт № 021186–2) и других проектов.

Штубов А.С.

**Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс»
ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ АВИАЦИОННОЙ ЭЛЕКТРОСВЯЗИ**

Модернизация единой системы организации воздушного движения на базе укрупненных районных центров предусматривает решение ряда задач по планированию информационной загруженности и безопасности телекоммуникационных систем. Решение этих задач предусматривает рассмотрение методов повышения достоверности, применяемых в теории массового обслуживания и применение имитационного моделирования для анализа потока ошибок в каналах связи.

К вопросам планирования загруженности следует отнести исследование тупиковых ситуаций при использовании метода блокировок и ситуаций приостановления выполнения транзакций с целью выявления их влияния на работоспособность телекоммуникационных систем. Процесс укрупнения районных центров связан с параллельным доступом многих пользователей к общим данным, и затрагивает вопросы обеспечения достоверности и целостности информации, а значит, распределения ресурсов системы при возрастании общего трафика.

В докладе анализируются сформулированные проблемы, и предлагается ряд рекомендаций по их разрешению.

Явно Д.М.

Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет
УСТАНОВЛЕНИЕ ПОДЛИННОГО IP-АДРЕСА ИСТОЧНИКА АТАКИ В СЕТИ ИНТЕРНЕТ

В настоящее время при проведении атак в сети Интернет многие злоумышленники стараются скрыть свои личные данные, чтобы максимально затруднить их поиск и минимизировать вероятность поимки.

Необходимы отработанные подходы, позволяющие находить злоумышленника для того, чтобы можно было привлечь его к ответственности.

При навигации в сети пользователь оставляет на сайтах свой IP-адрес, данные о системе и об используемом интернет-обозревателе, а также списки страниц, которые он посетил в рамках этого сайта, и прочую служебную информацию. Эти данные записываются в журналы протоколов на удаленном сервере, где хранятся некоторое время. Такие действия в первую очередь обусловлены необходимостью каждого сайта собирать информацию об активности посетителей в тех или иных разделах или составлять статистику. Чтобы избежать появления своих данных в подобных журналах, злоумышленник может воспользоваться одним из следующих приемов:

- анонимными прокси-серверами;
- веб-прокси;
- предварительно взломанными компьютерами.

Способы установления истинного IP-адреса, применимые в каждой ситуации, зависят от того, какие способы скрытия применял нарушитель. В общем случае существуют следующие возможности:

- получение журналов протоколов непосредственно у владельца промежуточного сервера (обычно применимо только к прокси-серверам);
- получение журналов протоколов у поставщика услуг связи и последующий анализ интенсивности потоков данных;
- если злоумышленник использует контролируемые пользовательские компьютеры, то можно попытаться отследить не саму цепочку, а адрес, с которого проводился захват контроля. Большинство злоумышленников не проводят такие операции напрямую со своего компьютера, но чаще всего такая цепочка будет значительно короче и может состоять всего из одного узла;
- также в отдельных случаях нарушитель может выдать свою личность, например, используя почтовый ящик, который он указывал где-то еще, или оставляя другие следы, ведущие к реальным данным. В этом случае необходим тщательный анализ всех данных, оставленных на сайтах злоумышленником, и выявление информации, способной раскрыть его личность в обход анализа цепочки промежуточных серверов.

Первый и второй из приведенных способов являются применимыми независимо от предпринятых злоумышленником мер. Последний способ дает результаты только в том случае, если злоумышленник был небрежен и оставил следы.

Для отслеживания нарушителя, использующего цепочку разнородных серверов, требуется последовательно посылать запросы владельцам каждого сервера с целью установления следующего звена в цепочке. Если в процессе отслеживания нарушителя расследование выходит за пределы одного государства, то официальное взаимодействие необходимо проводить с привлечением международных правоохранительных организаций. Это замедляет процесс и уменьшает вероятность того, что владелец прокси-сервера сможет предоставить информацию о том, кем этот адрес был использован на момент атаки. Кроме того, такое расследование может вообще не дать результата в силу конфликтов в законодательстве разных государств.

Таким образом, вероятность того, что грамотно действующего нарушителя удастся отследить, является достаточно низкой. Даже в случае использования цепочки из шести-семи серверов, расположенных на территории разных государств, расследование занимает не менее нескольких месяцев. За это время информация, на основании которой возможно установление личности злоумышленника, может быть удалена из-за истечения срока давности.

Яковлев С.А., Буренин В.А.

Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», ЗАО «Бизнес Компьютер Центр»
ВЫБОР ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ КОММУТАЦИОННОГО ОБОРУДОВАНИЯ
СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ
КОМПЬЮТЕРНЫХ АТАК

Процесс выбора показателей эффективности функционирования коммутационного оборудования современных защищенных телекоммуникационных сетей осуществляется с учетом целевых показателей сети, показателей эффективности всей сети, при условии, что сеть подвергается воздействию преднамеренных компьютерных атак, специально запланированных и продуманных нарушителем на основе предварительной разведки сети и априорных знаний о структуре сети, применяемых технологиях и протоколах управления.

Нередки случаи, когда показатели эффективности коммутационного оборудования не всегда удается строго определить исходя из показателей эффективности сети, и выбор их осуществляется эмпирически (на основе здравого смысла). Естественно, что выбранные показатели эффективности алгоритмов управления коммутационным оборудованием сети – определенные существенные свойства его и, в принципе, они могут быть различными для различных изделий из состава коммутационного оборудования. Поэтому на практике выделяют такие общие свойства коммутационного оборудования, которые характеризуют однотипные показатели эффективности коммутационного оборудования.

Для снижения вероятности существенных последствий компьютерных атак, коммутационное оборудование современной телекоммуникационной сети, наряду с другим оборудованием сети, охватывается контуром средств предотвращения и обнаружения компьютерных атак, состав которых может в значительной степени варьироваться от примитивных средств обнаружения атак, до сложных комплексов, включающих средства обнаружения атак, средства поиска уязвимостей, средства ложных информационных объектов, средства анализа трафика, средства обработки различной комплексной информации, средства локализации воздействий, средства восстановления функционирования.

Для оценки степени (уровня) достаточности средств защиты коммутационного оборудования современной телекоммуникационной сети от компьютерных атак необходимо выбрать определенные показатели, характеризующие защищенность объектов коммутационной техники от этих воздействий.

Обоснованный выбор таких показателей является достаточно сложной и неоднозначной научно-технической задачей, т.к. выбор традиционных для оценки эффективности вероятностно-временных показателей не приемлем для оценки защищенности в силу того, что в условиях неопределенности как характера, локализации, так и интенсивности компьютерных атак, получить адекватные и однозначные выражения и соотношения для них едва ли осуществимо.

Поэтому может быть предложен следующий подход. Пусть имеется оценка показателей эффективности функционирования коммутационного оборудования сети в условиях отсутствия компьютерных атак. Под воздействием той или иной компьютерной атаки снижается эффективность функционирования оборудования, при этом степень снижения эффективности, которую требуется определить, может служить показателем защищенности и основой для выработки критерия защищенности.

Яковлев В.А., Шутый Р.С.

Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

телекоммуникаций им. проф. М.А. Бонч-Бруевича

ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА «ЗАБЫВЧИВАЯ ПЕРЕДАЧА» ДЛЯ КОНФИДЕНЦИАЛЬНЫХ МНОГОСТОРОННИХ ВЫЧИСЛЕНИЙ С БАЗАМИ ДАННЫХ В КОМПЬЮТЕРНЫХ СЕТЯХ

Развитие Интернета предоставило огромные возможности для многосторонних вычислений, в которых участники выполняют совместные вычислительные задачи, основываясь на конфиденциальных входных данных, имеющихся у каждого участника. Например, пользователям необходимо сравнить конфиденциальные числовые данные, хранящиеся в базах данных, не раскрывая самих данных. С помощью конфиденциальных многосторонних вычислений (КМВ) решаются и многие задачи конфиденциальных геометрических вычислений, интеллектуальный анализ баз данных, электронные аукционы, а также задачи обнаружения вторжений, сбор статистической информации, биометрической аутентификации, когда пользователи не могут раскрыть своих данных другим пользователям.

В докладе рассматривается задача сравнения столбцов баз данных, содержащих числовую информацию, нахождение часто встречающихся записей, вычисление статистической информации по объединенным таблицам без их раскрытия. Данным задачам соответствуют математические задачи конфиденциального сравнения векторов и конфиденциального вычисления скалярного произведения. Эти задачи решаются с помощью базовых протоколов конфиденциального сравнения чисел и конфиденциального умножения чисел, в которых пользователи совместно вычисляют результат, без раскрытия своих данных. Для решения данных задач необходимо использовать протокол «Забывчивая передача». Основная суть этого протокола состоит в способе «передачи» двух последовательностей (секретов) от отправителя А получателю В, который может выбрать только одну последовательность. Задача состоит в том, чтобы участник А не узнал какую из последовательностей выбрал получатель В, а участник В не узнал второй секрет. Для реализации данного протокола используется двоичный симметричный канал с ошибками (ДСК), позволяющий обеспечить безусловную стойкость протокола КМВ. Для решения задачи конфиденциального вычислений с таблицами баз данных у пользователей должно быть программное обеспечение, выполняющее вычисления и защищенный канал, по которому они обмениваются данными с программно-аппаратным средством, реализующим протокол «Забывчивая передача» и включающее в себя канал с ошибками. Для протоколов конфиденциального сравнения столбцов, вычисления скалярного произведения и для базовых протоколов разработаны методики, позволяющие выбрать параметры этих протоколов, провести их оптимизацию и выведены соотношения для их расчета. По этим методикам проведен анализ протоколов и построены зависимости объема данных, передаваемых по ДСК от количества записей в столбцах, количества разрядов чисел, хранящихся в записях и количества столбцов в таблицах.



ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Алексеев А.В.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
МЕТОДИКА ПРОВЕДЕНИЯ ДЕЛОВЫХ ИГР ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ
ПО КОМПЛЕКСНОЙ ЗАЩИТЕ ИНФОРМАЦИИ**

Одной из важнейших задач подготовки и переподготовки кадров в области обеспечения информационной безопасности (ОИБ) сегодня является формирование знаний, навыков и способностей разрабатывать и обосновывать эффективные и оптимальные проектные и управленческие решения (ПУР), основанные на многоальтернативном и многокритериальном количественном анализе и синтезе сложных систем ОИБ.

Особая актуальность компетенций обучаемых в этой области обусловлена проблемой нетрадиционно большого объема разнородной и разнокачественной информации, с которой специалистам приходится работать в поиске эффективных ПУР, а также сложностью выбора при создании систем безопасности и, особенно, систем комплексной защиты информации (СКЗИ) предпочтительных, а тем более оптимальных ПУР.

Одним из перспективных направлений решения данной проблемы, в том числе для объектов морской инфраструктуры, сложных автоматизированных комплексов и систем специального назначения, является использование при подготовке специалистов по ОИБ такой формы практических занятий, как деловые игры (ДИ). Среди апробированных тем: «Тендер на получение специального заказа», «Доклад Главному конструктору проекта по выбору оптимальной архитектуры и основных характеристик СКЗИ», «Аналитическая справка по базовым IS-технологиям для Объединённой судостроительной корпорации», «Презентация продукции Компании на международном IS-форуме» и т.п.

Опыт проведения ряда подобных ДИ при подготовке морских инженеров специальности «Системотехника объектов морской инфраструктуры» по дисциплине «Основы проектирования систем защиты информации» в Санкт-Петербургском государственном морском техническом университете подтверждает их высокую результативность, особую активность обучаемых при подготовке и в ходе ДИ, их стремление к использованию строгой и обоснованной аргументации, формирование навыков и этики публичных выступлений, приобретение определённого опыта оперативного ориентирования и принятия ответственных ПУР в сложных динамических ситуациях, воспитание определённого чувства коллективной ответственности, стремление обучаемых к «профессиональному самовыражению», поиску нестандартных решений, обоснованию и «реализации ПУР» в ходе ДИ, особую активность в «ускоренном» изучении (при подготовке к ДИ) и системном «осмыслении» теоретической части дисциплины, полноты изучения рекомендованных учебно-методических материалов (см. Алексеев А.В. Основы проектирования систем защиты информации: Методические указания. – СПб.: СПбГМТУ, 2008. – 71 с.; Алексеев А.В. Сертификация систем обработки информации: Учебное пособие. – СПб.: СПбГМТУ, 2009. – 160 с.)

При этом, следует особо подчеркнуть важность качественной подготовки ДИ преподавателем и её проведения, максимально полного использования в ходе ДИ лекционного материала по всем изученным темам, а также действующих нормативных документов (например, федеральных законов, Государственного реестра сертифицированных средств защиты информации ФСТЭК, перечня БИЗКТ и других).

Особый динамизм, как показывает практика, в проведение ДИ вносят такие элементы её организации, как смена интересов участников ДИ, формирование новых (по вводным) групповых целей (например, сговор групп участников ДИ), условие мотивированности отдельных участников и их групп, смена (по вводной) руководителя ДИ и другие.

Блажко А.В., Гуцин А.Н.

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

**ОСОБЕННОСТИ ПОДГОТОВКИ РАЗРАБОТЧИКОВ ЛИЧНОСТНО-ОРИЕНТИРОВАННЫХ
ИНФОРМАЦИОННЫХ СИСТЕМ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**

Обеспечение информационной безопасности является одной из неотъемлемых задач на любом этапе жизненного цикла информационных систем. Исходя из этого, подготовка в области методов и средств обеспечения информационной безопасности является немаловажной не только

для специалистов по защите информации в эксплуатирующихся информационных системах, но и для их разработчиков. При этом, объем и содержание подготовки разработчиков может существенно различаться в зависимости от вида от ролей в процессе разработки и предназначения разрабатываемых ими информационных систем.

Одной из основных особенностей личностно-ориентированных информационных систем является наличие ряда взаимозависимых и частично взаимоисключающих свойств: во-первых, пользователь такой системы может иметь крайне ограниченный уровень общекомпьютерной подготовки (и тем более, не иметь никакой специальной подготовки в области защиты информации); во-вторых, личностно-ориентированные информационные системы, в основном, должны состоять из полностью подконтрольных информационных ресурсов; в-третьих, они могут хранить в себе или использоваться для передачи информации, имеющей существенную (или даже критическую в случае утраты или нарушения её конфиденциальности) ценность для пользователя (например, реквизиты платежных средств); и в-четвертых, они могут использовать внешние каналы передачи информации или вообще частично располагаться на в целом подконтрольных, частично подконтрольных или слабоподконтрольных пользователю ресурсах, когда, несмотря на любые заверения владельцев этих ресурсов, всегда есть опасность попадания конфиденциальной информации в руки некоего третьего лица. Противоречивость данных свойств (особенно первого со вторым) делает затруднительным использование хорошо регламентированных способов обеспечения информационной безопасности через разграничение специально подготовленного персонала, разрабатывающего, применяющего и совершенствующего политики безопасности и «конечных пользователей». Поэтому, можно выделить два основных направления в подготовке разработчиков личностно-ориентированных систем: во-первых, подготовка в области разработки и интеграции таких средств информационной безопасности, которые бы практически не требовали эксплуатации квалифицированным персоналом, обеспечивали необходимую степень защиты и при этом соответствовали понятию полностью подконтрольного информационного ресурса; во-вторых, подготовка в области документирования используемых решений и разработки эксплуатационной документации, одновременно способной удовлетворить как «начинающего пользователя» (или пользователя, который при решении своих личных задач склонен рассматривать подсистему защиты информации как «черный ящик» или, по возможности, вообще не замечать), так и пользователя, склонного в достаточной мере разбираться во всем, что работает с его информацией («энтузиаста», по навыкам сопоставимого с профессионалом).

Блашков В.И.

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

О КОНТРПРОДУКТИВНОМ ИСПОЛЬЗОВАНИИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПРОВЕРКЕ ЗНАНИЙ УЧАЩИХСЯ

В информационном обществе существует потребность в правильной количественной оценке любого параметра, существующего в жизни общества. В сфере образования необходимо объективно оценивать уровень знаний, умений, навыков обучаемых.

Несомненно, лучшим образом можно судить об уровне подготовленности обучаемого при помощи тестирования его знаний. Так, например, традиционный экзамен в ВУЗах, по сути, является игрой без правил, с наибольшей степенью субъективизма, с предельно низкой степенью оценки градации знаний (применяется практически трехбалльная система оценки), отсутствует возможность корректировать оценку в зависимости от общего состояния знаний в группе.

Тестирование же во многом лишено этих недостатков, но Россия по уровню тестовой культуры отстает от наиболее развитых, в тестовом отношении, стран: это Нидерланды, США, Англия, Япония, Дания, Франция, Израиль, Финляндия, Канада, Австралия, Новая Зеландия и др.

Кроме качества самого теста, способа обработки результатов существуют и другие обстоятельства, способные значительно исказить результаты тестовых замеров. Так, цели проверяющих знания (преподавателей) и проверяемых (учащихся) объективно находятся в состоянии противоречия, поскольку значительная доля проверяемых желала бы получить завышенную оценку своих знаний. На современном этапе, буквально в последние несколько лет, в России это противоречие стало приобретать новые черты в связи с бурным развитием информационных и коммуникационных технологий для портативных устройств.

Если не обращать внимания на происходящие процессы, то ситуация в конце конца выйдет из-под контроля, и государственные свидетельства о высшем образовании будут обесцениваться. Россия, как это делают многие страны, должна включиться в борьбу с подобными явлениями в сфере образования.

Можно выделить несколько вариантов контрпродуктивного использования современных средств информационного обмена, ведущего к неадекватности оценки знаний обучаемых:

1. Подмена исполнителя при дистанционной проверке знаний (или при домашнем исполнении проверочной работы).
2. Выставление в сети Интернет тестовых заданий, накануне официальной даты проведения теста («утечка» материалов тестов).

3. Передача материалов тестов «в пространстве и во времени», благодаря большому числу часовых поясов на территории России.
4. Использование студентами, школьниками готовых, выполненных заданий, лабораторных работ, компьютерных программ, размещенных в сети Интернет.
5. Плагиат студенческих работ, благодаря широкому использованию Интернет.
6. Неконтролируемое использование коммуникационных возможностей портативных технических устройств в ходе проверки знаний.
7. Неконтролируемое использование информационных возможностей портативных технических устройств.

Как минимум, в ВУЗах и школах следует тщательно прописывать правила поведения учащихся в аудитории, исключая применение подобных приемов.

Это потребует от преподавателей квалифицированного анализа возможных ситуаций и даже учета правовых аспектов определенных запретов и ограничений.

Бобонец С.А.

**Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России
ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ**

Важнейшая роль в развитии современного общества, бесспорно, принадлежит информатизации. Информатизация подразумевает всеобщий социальный процесс производства и повсеместного использования информации как общественного ресурса, обеспечивающего интенсификацию развития экономики, ускорение научно-технического прогресса и процесса интеллектуализации общества. Она предусматривает массовое внедрение средств и методов сбора, обработки, передачи и хранения информации на базе современной вычислительной техники и средств коммуникаций.

Развитие информатизации находится в прямой зависимости от развития компьютерных сетей. Бурное развитие сетевых технологий, наблюдаемое в последнее время, обусловило широкую интеграцию крупных информационных систем, основанных на территориально-распределенных корпоративных сетях, с глобальной информационной сетью Интернет.

Появление многочисленных сетевых услуг, которые предоставляет Интернет (электронная почта, сетевая реклама, оперативное получение информационных новостей, доступ к современным информационным ресурсам и т.п.), становится жизненной необходимостью. На этом фоне осуществляются регулярные попытки нарушения безопасности в Интернете и через него, которые приносят государственным и коммерческим компаниям ущерб в десятки и сотни миллионов рублей, но этот факт не оказывает серьезного влияния на глобальную информатизацию общества.

Проблема необходимости защиты информации привела к появлению целой отрасли индустрии – разработка и производство средств защиты информации. Из арсенала государственных, военных и специальных служб средства защиты стали достоянием различных пользователей. Но, несмотря на уже имеющийся громадный арсенал разнообразных средств защиты, процесс вторжения в компьютерные системы продолжается и до настоящего времени, причем число вторжений постоянно растет.

В сложившейся ситуации огромную роль играет процесс подготовки опытного пользователя или специалиста в области информационных технологий, осознающего реальную ответственность за неправомерные действия. Зачастую в процессе подготовки специалистов вузы или специализированные курсы повышения квалификации основной упор делают на техническую подготовку. Опытные преподаватели умело находят контакт с аудиторией, более того, если занятия организованы на курсах повышения квалификации, этот процесс взаимовыгоден как для слушателя, так и для педагога. В этот период осуществляется обмен информацией, рассматриваются реальные ситуации и совместно находятся пути решения возможных проблем. Этот процесс обучения специалистов в области информационных технологий в основном охватывает техническую подготовку слушателей и в меньшей степени затрагивает вопросы, связанные с пониманием ответственности за компьютерные преступления. Таким образом, подготовка специалистов в области информационных технологий должна в полной мере сопровождаться изучением как правовых аспектов деятельности специалиста так изучением морально-этических норм и правил работы с информационными ресурсами.

Великовская С.А.

**Россия, Углич, Московский государственный университет технологий и управления
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ УЧЕБНОГО ПРОЦЕССА**

Одной из актуальных проблем функционирования информационного пространства общеобразовательного учреждения, например, школы, является проблема информационной безопасности.

Всю информацию, наполняющую учебную сеть можно разделить на несколько категорий:

- образовательные ресурсы;
- персональная информация о сотрудниках и обучающихся;

- документация.

Одной из основных задач образовательного учреждения в части информационного обеспечения является сохранение конфиденциальности информации. Организация и хранение информации в компьютерной сети должна соответствовать ряду требований вне зависимости от размеров сети и объемов хранимой информации:

- централизация хранения;
- разграничение доступа;
- доступность информационных ресурсов с различных рабочих мест;
- регламент актуализации информации;
- защита от повреждений (вирусная безопасность, потеря данных, аппаратные повреждения);
- резервное копирование и т. д.

Рассматриваются вопросы защиты информации для общеобразовательных учреждений, современные технологии позволяют получать дополнительные сведения, участвовать в различных интернет конкурсах, форумах, дополнительных курсах и т.д. и использовать полученные знания на уроках и дополнительных занятиях.

Рассматриваемая система защиты информации опирается на систему видов собственного обеспечения, способного реализовать её функционирование не только в повседневных условиях, но и в критических ситуациях.

Верхолат А.М., Гаврилов В.А., Касаткин В.В.

Россия, Санкт-Петербург, Балтийский государственный технический университет

«ВОЕНМЕХ» им. Д.Ф. Устинова

СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СРЕДЕ КОМПЬЮТЕРНОЙ СИСТЕМЫ ОБУЧЕНИЯ

Изучение современных технологий БД невозможно без использования компьютерных систем обучения (КСО). Одним из направлений разработки КСО является создание таких систем применительно к технологиям БД, которые обеспечивают информационно-методическую поддержку процесса обучения и тестирования знаний по отдельным разделам этих технологий.

В данном докладе рассматриваются вопросы информационной безопасности при работе в среде автоматизированной системы обучения языку SQL. Разработка этой системы ведется на кафедре информационных систем и компьютерных технологий университета для информационно-методической поддержки учебных дисциплин "Базы данных" и "Управление данными".

Функционально КСО языку SQL включает две подсистемы: подсистему формирования заданий и обучения языку и подсистему аутентификации, сбора и обработки статистических данных процесса обучения. Первая подсистема предназначена для формирования уроков по изучению языка SQL, а также проведения самого процесса обучения и тестирования знаний в интерактивном режиме. Вторая подсистема обеспечивает аутентификацию пользователей системы, сбор, обработку и выдачу статистических данных индивидуального или группового процесса обучения языку SQL в интерактивном режиме.

В системе обучения языку SQL для идентификации пользователя используется уникальная пара: логин и пароль. В качестве логина используется номер зачетной книжки студента. Пароль устанавливается пользователем самостоятельно.

После прохождения процедуры аутентификации пользователю предоставляется доступ к КСО в соответствии с группой пользователя и назначенным ему набором прав. В системе предусмотрены следующие три группы пользователей с соответствующими наборами правил.

Первая группа пользователей - пользователь "Обучаемый". Пользователь этой группы может изучать уроки, проходить тесты, устанавливать пароль, просматривать информацию о своем процессе обучения. Вторая группа пользователей – пользователь "Преподаватель". Пользователь этой группы в дополнение к правам "обучаемого" может просматривать статистическую информацию процесса обучения в различных разрезах, а также восстанавливать пароли для обучаемых в случае их утери. Третья группа пользователей – пользователь "Администратор". Пользователь этой группы в дополнение к правам "Преподавателя" может создавать новые уроки, их редактировать, составлять тестовые задания текущего и итогового контроля, просматривать статистику процесса обучения всех пользователей в любом разрезе.

В КОС возможно написание любых запросов, в том числе и запросов, которые могут разрушить учебную БД системы. Учитывая, что среди студентов могут оказаться и недобросовестные личности, все тестовые запросы проходят синтаксический анализ на предмет "несанкционированных действий" обучаемых в соответствии с определенным алгоритмом. Если введенный запрос удовлетворяет критерию запроса "несанкционированного действия", то подсистема фиксирует следующую информацию: идентификатор пользователя; запрос, который пытался выполнить пользователь; время, в которое была попытка выполнить запрос "несанкционированного действия". После выявления факта запуска такого запроса пользователю возвращается код ошибки с сообщением "Запрос написан неверно".

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

Кононов О.А, Кононова О.В.

**Россия, Санкт-Петербург, Санкт-Петербургский институт управления и права
ПОДГОТОВКА ИТ-СПЕЦИАЛИСТОВ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Внедрение в сознание ИТ-специалистов необходимости соблюдения требований норм информационной безопасности и привитие навыков их применения является одной из важнейших задач системы высшего образования, как социального института «производства социального человека».

В современных государственных образовательных стандартах и учебных планах подготовки ИТ-специалистов большое внимание уделяется проблемам организации защиты информации, однако главным образом это касается технических и частично правовых аспектов. В тоже время, при решении проблем информационной безопасности большое значение имеют и такие социальные институты, определяющие систему «правил игры» в обществе, как корпоративные и этические (моральные) нормы, также затрагивающие глобальные вопросы становления информационного общества. Разъяснять и пропагандировать эти нормы необходимо в лекционных курсах информатики, информационных технологий и других информационных дисциплин.

Студенты должны понимать основные технические, правовые, социальные и этические аспекты обеспечения информационной безопасности общества. Они должны сознавать свою личную роль в процессе информатизации общества, развивать в себе способность задавать серьезные вопросы об её социальном влиянии и оценивать предлагаемые ответы на них, т.е. для обеспечения информационной безопасности общества социально-личностное развитие обучаемых имеет чрезвычайно важное значение.

Наряду со сказанным имеется необходимость включения в различные дисциплины, связанные с проектированием, внедрением и эксплуатацией информационных систем разделов, посвященных вопросам обеспечения компьютерной безопасности.

На основе вышеизложенного обосновывается необходимость системного подхода к организации образовательных курсов в части обеспечения сознательного отношения обучающихся к вопросам информационной безопасности как с точки зрения технических, так и гуманитарных аспектов.

В докладе представлены результаты введения в учебный процесс по специальности 230201 «Информационные системы и технологии» дисциплин «Физические основы защиты информации» и «Социальные и этические вопросы информационных технологий», а также включения дополнительных разделов, посвященных вопросам информационной безопасности в курсах «Введение в специальность», «Информационные технологии» и «Проектирование информационных систем» в Санкт-Петербургском институте управления и права.

Мандрик П.А.

**Беларуссия, Минск, Белорусский государственный университет
СИСТЕМА ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ И КОМПЬЮТЕРНОЙ
БЕЗОПАСНОСТИ В БЕЛОРУССКОМ ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ**

В настоящее время является общепризнанным фактом, что в современном обществе «информация» все отчетливее становится высокоценным товаром, который, как и любой товар, необходимо производить, хранить, обрабатывать, передавать и защищать. Особенно актуальными стали проблемы защиты информации в связи с мощным развитием компьютерной индустрии и интенсивным проникновением компьютерных сетей и систем связи во все области человеческой деятельности.

В Республике Беларусь (в связи с возрастающим спросом на аналитиков-программистов в области защиты информации со стороны банков, финансовых и страховых компаний, крупных фирм, медицинских учреждений, государственных организаций) в 1997 году на базе факультета прикладной математики и информатики Белорусского государственного университета (БГУ) была начата подготовка специалистов по прикладной математике с новой специализацией «Математическое и программное обеспечение криптографии и анализа данных». Основное внимание при построении учебных планов по данной специализации уделялось вопросам криптографической защиты информации, которая, как известно, заключается в специальном функциональном преобразовании информации в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования и базируется на интенсивно развивающейся в настоящее время науке «криптология».

На основе накопленного опыта подготовки студентов в рамках данной специализации, с учетом проводимых научно-исследовательских работ в области защиты информации и наличия широкого спектра соответствующих специалистов в БГУ (впервые в Беларуси) на базе двух факультетов была открыта подготовка специалистов с высшим образованием по новой специальности «Компьютерная безопасность». На факультете прикладной математики и информатики по направлению «математические методы и программные системы защиты информации» с квалификацией «Специалист по защите информации. Математик» и на факультете радиофизики и электроники по

направлению «радиофизические методы и программно-технические средства защиты информации» с квалификацией «Специалист по защите информации. Радиофизик».

Сегодня в Белорусском государственном университете создана и успешно действует система подготовки, переподготовки и повышения квалификации специалистов по информационной и компьютерной безопасности. Эта система организационно базируется на совместной, скоординированной и взаимодополняющей деятельности соответствующих факультетов (подготовка специалистов), Государственного учреждения образования «Институт технологий информатизации и управления» БГУ (повышение квалификации специалистов) и Научно-исследовательского института прикладных проблем математики и информатики БГУ (проведение научно-исследовательских работ и стажировка специалистов).

Москалёва О. И., Степанов А. Г.

**Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
аэрокосмического приборостроения
ПРОФЕССИОНАЛЬНАЯ КОМПЕТЕНТНОСТЬ ЭКОНОМИСТОВ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Обзор содержания обучения информатике студентов экономических специальностей с точки зрения современной педагогики проводится на основании формулирования требований профессиональной компетентности специалиста.

В современном обществе профессионально компетентные экономисты должны владеть знаниями и умениями в области информационной безопасности, чтобы не допустить случайных или злонамеренных действий, которые могут привести к потере информации.

Экономисту необходимо знать основные угрозы, которые могут нанести ущерб организации, в которой он работает.

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 невалифицированного 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. 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 безопасности использования вычислительной техники и предложены рекомендации по формированию требований профессиональной компетентности.

Примакина Е.И.

**Россия, Кострома, Костромская государственная сельскохозяйственная академия
ИНФОРМАЦИОННЫЕ КРИТЕРИИ ОЦЕНКИ ПСИХОМОТОРНОЙ И ИНТЕЛЛЕКТУАЛЬНОЙ
ДЕЯТЕЛЬНОСТИ ОПЕРАТОРОВ**

Для успешного обучения студентов технических специальностей в освоении ими графических и расчетных информационных технологий необходима диагностика в виде тестирования и развитие

основных профессионально важных качеств, базирующихся на соответствующем уровне психомоторики и интеллектуальных способностях.

Для решения этой задачи необходимо определить выбор тестирующих сигналов, определить меры измерения качества многоальтернативных решений приемными системами.

В данной работе восприятие зрительных и звуковых сигналов оценивалось оператором мерами Шеннона и Кульбака. Известно, мера Шеннона чувствительна к анализу ансамблей сигналов, а мера Кульбака оценивает близость той или иной гипотезы. Под качеством восприятия зрительных и звуковых сигналов понимаются выходные количественные характеристики оператора, измеренные мерами Шеннона и Кульбака. При изучении механизмов психомоторной деятельности и интеллектуальной были рассмотрены их модели, в состав которых включили физиологический шум, в связи с тем, что решения оператора носят вероятностный характер.

Выбор той или иной реакции диктуется условиями близости признаков сигналов друг к другу. Решения задачи классификации зрительных сигналов связываем с системой психомоторики оператора, а звуковые сигналы – с его системой «интеллектуальной деятельности», под которой будем понимать относительно устойчивую структуру способностей, в основе которых лежат процессы, обеспечивающие переработку разнокачественной информации о симметрии сигналов и осознанную оценку ее свойств.

Оценки мер Шеннона и Кульбака были реализованы в соответствии со следующим алгоритмом. Из банка данных (сигналов) случайным механизмом выбирался К сигнал. Оператору представлялась возможность провести выбор сигнала из К альтернатив. Накопленные данные ответов позволяли оценить матрицу ответов и с учетом соотношений, оценить меры Шеннона и меры Кульбака. Индивидуальные данные обрабатывались и консервировались в виде числовых и графических представлений.

Предлагается применить следующую последовательность оценки индивидуальных способностей классификации сигналов операторами:

- инструктаж оператора по работе с программным продуктом на ПЭВМ;
- обучение в течение часа оператора решению задачи классификации сигналов;
- фактическое проведение эксперимента.

Новые возможности проведения исследований по количественной оценке способностей достигались за счет:

- применения при формировании классов стимулов гибкой математической среды MathCAD;
- отсутствия в период проведения опыта экспериментатора, т.е. исключался субъективный фактор влияния исследователя;
- текущей оценкой надежности экспериментальных данных;
- контроля параметров стимула, оценки близости ответной траектории по отношению к предъявляемой на математическом уровне.

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

ПОДГОТОВКА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ НАПРАВЛЕНИЯ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» НА ОСНОВЕ КОМПЛЕКСНОГО ПОДХОДА

Компьютерная безопасность является одним из важных вопросов обеспечения жизненного цикла информационных систем.

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 в области информационной безопасности и должен участвовать во всех стадиях создания конечного продукта. Этим обеспечиваются высокие показатели проектируемой информационной системы и оптимальное использование ресурсов: финансовых, материальных и трудовых.

Данный подход был реализован при подготовке федерального государственного образовательного стандарта подготовки бакалавров и магистров по направлению «Информационные системы и технологии». Авторы обосновывают необходимость изложения учебного материала по вопросам информационной безопасности в рамках дисциплин «Теория информационных процессов и систем», «Информационные технологии», «Инструментальные средства информационных систем», «Инфокоммуникационные системы и сети», «Методы и средства проектирования информационных систем и технологий».

Свирский Е.А., Шалима В.Н.

Беларуссия, Минск, Институт технологий информатизации и управления Белорусского государственного университета

**ПОВЫШЕНИЕ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В РЕСПУБЛИКЕ БЕЛАРУСЬ**

Система повышения квалификации специалистов по информационной безопасности базируется на Постановлении Совета Министров Республики Беларусь от 31.05.2004г № 646 «Об обязательном повышении квалификации работников республиканских органов государственного управления и иных государственных организаций, подчиненных Правительству Республики Беларусь, в компетенцию которых входит обеспечение информационной безопасности этих органов (организаций)». В соответствии с этим постановлением в настоящее время повышение квалификации по информационной безопасности обеспечивается единственным учреждением образования, которым является ГУО «ИТИиУ» БГУ.

Специфической особенностью подготовки и переподготовки кадров и повышения квалификации в республике являются недостаточно развитая нормативно-правовая база по информационной безопасности и не сформировавшаяся инфраструктура защиты информационных ресурсов и систем.

Одной из основных своих задач при организации курсов повышения квалификации по информационной безопасности ГУО «ИТИиУ» БГУ считает формирование единого мировоззрения в области организации обеспечения информационной безопасности информационных ресурсов и систем у специалистов, обеспечивающих информационную безопасность в своих учреждениях и организациях.

По курсам повышения квалификации по информационной безопасности для специалистов разных уровней разработаны учебные планы и программы, которые согласованы с заинтересованными ведомствами. Занятия на курсах ведут в основном специалисты-практики, имеющие, как опыт разработки, внедрения и эксплуатации систем обеспечения информационной безопасности, так и навыки педагогической работы.

Для руководителей органов государственного управления организован ежегодный однодневный семинар по проблемам информационной безопасности, основными целями которого являются ознакомление с текущими проблемами информационной безопасности и рассмотрение на концептуальном уровне всего спектра вопросов, которые необходимы руководителям для организации работ по обеспечению информационной безопасности учреждений и организаций.

ГУО «ИТИиУ» БГУ важной составляющей своей работы рассматривает налаживание деловых связей с аналогичными учреждениями России и других стран в целях обмена опытом, разработки совместных учебных программ и долгосрочных проектов в сфере информационной безопасности.

В ближайших планах ГУО «ИТИиУ» БГУ создание Интернет-портала по информационной безопасности (портала знаний). Одна из целей создания портала знаний – это объединить сообщество специалистов по информационной безопасности и направить его интеллектуальный потенциал на решение насущных проблем, стоящих перед отраслью. Масштабных проблем в этой сфере деятельности достаточно много, например, создание эффективной системы управления процессами формирования общественного мнения в сфере защиты информационных ресурсов общества.

ОГЛАВЛЕНИЕ

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ	11
Болдов М.Е. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В СБЕРБАНКЕ РОССИИ: ОПТИМИЗАЦИЯ ДОКУМЕНТООБОРОТА И НОВЫЕ ВОЗМОЖНОСТИ	
	11
Демидов А.В. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК МЕРА ПРОФИЛАКТИКИ РАСПРОСТРАНЕНИЯ В РОССИИ ДЕСТРУКТИВНЫХ РЕЛИГИОЗНЫХ ОРГАНИЗАЦИЙ.....	
	11
Дианов М.М. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РОССИИ В УСЛОВИЯХ ГЛОБАЛЬНОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА.....	
	12
Дончевская Л.В. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ИНФОРМАЦИОННАЯ ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ И ЕЕ СТРУКТУРА	
	13
Дудкина О.К., Копыльцов А.В. Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена СОЗДАНИЕ ГОРОДСКОГО МОНИТОРИНГОВОГО ЦЕНТРА ЭКСТРЕМАЛЬНЫХ СИТУАЦИЙ	
	13
Иванов В.П. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ИНФОРМАЦИОННЫЕ АСПЕКТЫ КУЛЬТУРНОЙ БЕЗОПАСНОСТИ	
	14
Колин К.К. Россия, Москва, Институт проблем информатики РАН КАЧЕСТВО ЖИЗНИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ	
	15
Кононов А.А., Стиславский А.Б., Цыгичко В.Н., Черешкин Д.С. Россия, Москва, Институт системного анализа РАН АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС ОБЕСПЕЧЕНИЯ АНТИТЕРРОРИСТИЧЕСКОЙ БЕЗОПАСНОСТИ (НА ПРИМЕРЕ ТРАНСПОРТНОГО КОМПЛЕКСА)	
	16
Корт С.С. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет ОРГАНИЗАЦИЯ ДОСТУПА НАСЕЛЕНИЯ К ИНФОРМАЦИОННЫМ РЕСУРСАМ МУНИЦИПАЛЬНЫХ ОРГАНОВ.....	
	16
Кугносов В.И., Хузин В.З. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин» ПРОБЛЕМЫ РАЗВИТИЯ И СОВЕРШЕНСТВОВАНИЯ ТЕРМИНОЛОГИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА СОВРЕМЕННОМ ЭТАПЕ.....	
	17
Лясович Т.Г. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ИЗ ИСТОРИИ СОЗДАНИЯ И ФУНКЦИОНИРОВАНИЯ ОРГАНОВ ФАПСИ В РОССИИ (1991–2003г.)..	
	18

Полонский А.М., Космачев В.М. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения ПРАКТИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ КОРПОРАТИВНОЙ ПОЛИТИКИ ДОСТУПА В ИНТЕРНЕТ	19
Сальников М.А., Копыльцов А.В. Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена ПЕРСПЕКТИВЫ РАЗВИТИЯ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ В РОССИИ.....	20
Федоров А.В. Россия, Москва, Министерство юстиции Российской Федерации ГАРМОНИЗАЦИЯ И УНИФИКАЦИЯ ЗАКОНОДАТЕЛЬСТВА О ГОСУДАРСТВЕННОЙ ТАЙНЕ В ГОСУДАРСТВАХ–УЧАСТНИКАХ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ.....	21
ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	23
Агаев Р.А. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНОВ ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ, КАК ФАКТОР УЛУЧШЕНИЯ РАБОТЫ СЛЕДОВАТЕЛЯ	23
Бачило И.Л. Россия, Москва, Институт государства и права РАН О ПРАВЕ В СВЕТЕ СТАНОВЛЕНИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА	23
Бирюков В.Ю. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН АНАЛИЗ ПРОТИВОПРАВНЫХ ПРОЯВЛЕНИЙ НЕТРАДИЦИОННЫХ РЕЛИГИОЗНЫХ ОБЪЕДИНЕНИЙ КАК ОДИН ИЗ ЭЛЕМЕНТОВ ОПРЕДЕЛЕНИЯ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ	25
Гольцов В.Б. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России АКТУАЛЬНОСТЬ ИССЛЕДОВАНИЯ ЧАСТНОПРАВОВЫХ ВОПРОСОВ СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ОБЩЕСТВА И ПРЕДУПРЕЖДЕНИЕМ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ.....	26
Дементьева Н.В., Примакин А.И. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ ОВД	27
Довнар Н.Н. Беларуссия, Минск, Институт журналистики Белорусского государственного университета ДОСТУП ЖУРНАЛИСТОВ К ИНФОРМАЦИИ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ....	28
Завражина С.В. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ВЗАИМОДЕЙСТВИЕ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ С ОРГАНАМИ ВНУТРЕННИХ ДЕЛ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ	28
Иванова О.М. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России МЕСТО КОНСТИТУЦИОННОГО СУДА В СУДЕБНОЙ СИСТЕМЕ РОССИЙСКОЙ ФЕДЕРАЦИИ: ПРОБЛЕМЫ ТЕОРИИ ТОЛКОВАНИЯ ПРАВА	29
Кабанов А.А. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России КЛАССИФИКАЦИЯ ИНФОРМАЦИИ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ	30

Карпов А.М. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БОРЬБЕ С НАЛОГОВОЙ ПРЕСТУПНОСТЬЮ	31
Киикова Л.К. Россия, Санкт-Петербург, Санкт-Петербургского университета МВД России ИДЕЙНО–ПСИХОЛОГИЧЕСКИЕ ОСНОВЫ ПРЕСТУПЛЕНИЙ ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ ..	31
Кондратьев В.В., Вус М.А., Заболотский В.П. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН О РАЗРАБОТКЕ МОДЕЛЬНОГО ЗАКОНОДАТЕЛЬСТВА ГОСУДАРСТВ – УЧАСТНИКОВ СНГ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	33
Константинова Т.В. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ИСПОЛЬЗОВАНИЕ ПОТЕНЦИАЛА ТРАДИЦИОННЫХ РЕЛИГИЙ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОТИВОДЕЙСТВИИ ВНУТРИСЕМЕЙНЫМ ПРЕСТУПЛЕНИЯМ	33
Масловский В.М. Россия, Москва, Региональный учебно-научный центр «Безопасность» МГТУ им. Н.Э. Баумана КТО ОТВЕЧАЕТ ЗА ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ?	34
Мефёд А.В., Старков А.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики О ПРАВОВОМ АСПЕКТЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ПРИМЕРЕ «SKYPE»	35
Осипов Я.В. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России К ВОПРОСУ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРИМЕНЕНИЮ ПОЛИГРАФА В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ.....	35
Пономарев А.Л., Язовских А.Н. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики ПРАВОВЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ПРОТОКОЛА BITTORENT	36
Рзаев И.М. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ МОНИТОРИНГА ЗА СОСТОЯНИЕМ ПРИРОДНО-РЕСУРСНОГО КОМПЛЕКСА РОССИИ	36
Савельев А.И. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	37
Смирнова О.Г. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России СПИЦИФИКА ОБРАЩЕНИЯ С МАШИНЫМИ НОСИТЕЛЯМИ ПРИ РАССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ	38
Сухов Д.К. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ВОПРОСЫ КЛАССИФИКАЦИИ И СИСТЕМАТИЗАЦИИ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ ЭКСПЕРТИЗЫ ПО ПОИСКУ ИНФОРМАЦИИ, ОТНОСЯЩЕЙСЯ К УГОЛОВНОМУ ДЕЛУ	39
БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ	40

Александров А.М. Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс» ДЕКОМПОЗИЦИЯ ИНТЕГРАЛЬНЫХ ТРЕБОВАНИЙ ПО ВЕРОЯТНОСТИ ЛОЖНЫХ СИГНАЛОВ В МНОГОКАНАЛЬНЫХ СИСТЕМАХ КОНТРОЛЯ.....	40
Алексеев А.В., Скородумов Е.Н. Россия, Санкт-Петербург, ОАО «Научно-инженерный центр Санкт-Петербургского электротехнического университета» ОЦЕНКА ОБОБЩЁННОГО УРОВНЯ КАЧЕСТВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИХ СЕРТИФИКАЦИИ	40
Андреева Н.В., Васильев Ф.Р., Любимов А. В. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики МЕТОДЫ ИНТЕГРАЦИИ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ И СИСТЕМ ДОКУМЕНТООБОРОТА В ОРГАНИЗАЦИЯХ	41
Артамонов А.В., Васильев П.Н., Маховенко Е.Б. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет ГРУППОВАЯ ПОДПИСЬ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ НА ОСНОВЕ ТЕХНОЛОГИИ J2EE	41
Афанасьев С.В., Евневич Е.Л., Белаш Е.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО КОДА НА СТАДИИ РАЗРАБОТКИ	42
Баранюк Т.Н., Нестерук Ф.Г., Нестерук Г.Ф. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН МИНИМИЗАЦИЯ БАЗЫ ЗНАНИЙ ПРИ РАЗРАБОТКЕ АДАПТИВНОГО УРОВНЯ КЛАССИФИКАЦИИ В СОСТАВЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ	42
Блюм В.С., Заболотский В.П. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ИНДЕКС ЗДРАВООХРАНЕНИЯ КАК ФАКТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА	43
Богачева А.В. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики ОРГАНИЗАЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРА НА УРОВНЕ ФИЗИЧЕСКОГО ДОСТУПА	44
Богданов А.Г., Ростовцев А.Г. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет ГОМОМОРФИЗМЫ КОЛЕЦ И ЗАЩИЩЁННАЯ ОБРАБОТКА ДАННЫХ	45
Верхолат А.М., Гаврилов В.А. Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова К ВОПРОСУ ПОСТРОЕНИЯ БЕЗОПАСНЫХ ГЕТЕРОГЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ	45
Войцеховский С.В. Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского КОМБИНИРОВАННЫЙ МЕТОД СОГЛАСОВАНИЯ ЭКСПЕРТНЫХ ОЦЕНОК ДЛЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ВЫЧИСЛИТЕЛЬНЫХ КОМПЛЕКСОВ И СЕТЕЙ	46
Воробьев Е.Г. Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского ОПТИМИЗАЦИЯ ПРЕДСТАВЛЕНИЯ ДАННЫХ В ГЛОБАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ЕДИНОГО ИНФОРМАЦИОННОГО ПОЛЯ И КВАНТОВЫХ ТЕХНОЛОГИЙ ..	47

Вус М.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН КОМПЬЮТЕРНЫЕ ИГРЫ И ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ЮНОГО ПОКОЛЕНИЯ	48
Галанов А.И., Костина А.А., Молдовян У.А., Сухов Д.К. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ПОДГОТОВИТЕЛЬНАЯ ПРОЦЕДУРА ИССЛЕДОВАНИЯ ЦИФРОВОГО НОСИТЕЛЯ ИНФОРМАЦИИ В ПРОЦЕССЕ ЭКСПЕРТИЗЫ	48
Григорьева М.В. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики ВЕДЕНИЕ ИНФОРМАЦИОННОГО ПРОТИВОДЕЙСТВИЯ МЕЖДУ КОНКУРИРУЮЩИМИ СУБЪЕКТАМИ	49
Григорьева А.И., Колодин М.Ю. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ОСНОВНЫЕ ПРИНЦИПЫ И ПРАКТИЧЕСКИЕ ДЕЙСТВИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СВОБОДНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ	50
Домбровская Л.А. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ	50
Емелин В.И. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Вектор» ИНФОРМАЦИОННАЯ УСТОЙЧИВОСТЬ УПРАВЛЕНИЯ СОЦИАЛЬНО-ТЕХНИЧЕСКИМИ СИСТЕМАМИ	51
Зегжда Д.П. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет ВИРТУАЛИЗАЦИЯ – ОСНОВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ..	52
Зегжда Д.П., Рудина Е.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет МОДЕЛИРОВАНИЕ БЕЗОПАСНОСТИ ОБРАБОТКИ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ СИСТЕМАХ	53
Зозуля Ю. В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ОПРЕДЕЛЕНИЕ КАТЕГОРИИ ВЕБ-САЙТА ДЛЯ РЕШЕНИЯ ЗАДАЧИ РОДИТЕЛЬСКОГО КОНТРОЛЯ.....	53
Иванов С.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ПОДСИСТЕМА РАЗГРАНИЧЕНИЯ И ОБЕСПЕЧЕНИЯ ДОСТУПА В МОДЕЛИ ГРИД ПОРТАЛА САНКТ-ПЕТЕРБУРГСКОГО НАУЧНОГО ЦЕНТРА РАН	54
Калинин М.О. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет СОЗДАНИЕ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ	55
Комашинский Д.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ПОСТРОЕНИЕ МОДЕЛИ СТАТИЧЕСКОГО ДЕТЕКТИРОВАНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА БАЗЕ МЕТОДОВ DATA MINING.....	56
Конобасов А.М., Королев С.Н. Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова ДВУХКРИТЕРИАЛЬНЫЙ АЛГОРИТМ ПЕРЕДАЧИ ДАННЫХ.....	57

Коновалов А.М. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН МОДЕЛИРОВАНИЕ БОТНЕТОВ НА ОСНОВЕ МНОЖЕСТВА ВЗАИМОДЕЙСТВУЮЩИХ ИНТЕЛЛЕКТУАЛЬНЫХ АГЕНТОВ	58
Кононов В.О. Россия, Санкт-Петербург, Санкт-Петербургский институт управления и права ПРАКТИКА ИНТЕРНЕТ-ПРОДВИЖЕНИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ	58
Копыльцов А.В., Сорокин И.В. Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена ЭНТРОПИЙНЫЙ АНАЛИЗ ФАЙЛОВ ДЛЯ ВЫЯВЛЕНИЯ И КЛАССИФИКАЦИИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	59
Корт С.С. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет ПЕРИОДИЧНОСТЬ ОБУЧЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ	60
Корт С.С., Павличенко М.В., Рудина Е.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет АЛГОРИТМ ОБНАРУЖЕНИЯ РАСПРЕДЕЛЕННЫХ ВТОРЖЕНИЙ	61
Крыжановский О.В., Субботин Р.В. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики ИСТОРИЧЕСКИЕ АСПЕКТЫ ВОЗНИКНОВЕНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	62
Лохвицкий В.А. Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ СЕТЕВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ФОРМИРОВАНИЙ КОСМИЧЕСКИХ ВОЙСК В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА	62
Лукомский Е.А. Россия, Санкт-Петербург, ООО «НеоБИТ» ТЕХНОЛОГИЯ ВИРТУАЛИЗАЦИИ ЗАЩИТЫ ДЛЯ КОНТРОЛЯ ФУНКЦИОНИРОВАНИЯ И ВЗАИМОДЕЙСТВИЯ ПРИЛОЖЕНИЙ	63
Мамутова О.В. Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс» ВОПРОСЫ ОРГАНИЗАЦИИ ПАМЯТИ В ВЫСОКОНАДЕЖНОЙ СИСТЕМЕ	64
Мандригин И.С. Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова РОЛЬ СИСТЕМ АВТОМАТИЗАЦИИ УПРАВЛЕНЧЕСКИХ БИЗНЕС-ПРОЦЕССОВ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ	64
Мирин А.Ю., Сухов Д.К. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ВОПРОСЫ ВОССТАНОВЛЕНИЯ УДАЛЕННОЙ ИНФОРМАЦИИ ПРИ ИССЛЕДОВАНИИ ЦИФРОВЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ В ПРОЦЕССЕ ЭКСПЕРТИЗ	65
Михайлов Н.С. Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова ОРГАНИЗАЦИЯ БЕЗОПАСНОЙ МОДЕРНИЗАЦИИ ИНФОРМАЦИОННОЙ СРЕДЫ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ	65

Михайлова А.С. Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ АВТОМАТИЗИРОВАННОМ ПОСТРОЕНИИ ТЕЗАУРУСА УЧЕБНОГО ТЕКСТА	66
Некрасова Е. А., Шустиков С. В. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики РАЗРАБОТКА СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ С ПРИМЕНЕНИЕМ ФУНКЦИОНАЛЬНОЙ МОДЕЛИ.....	67
Нестерук Ф.Г., Нестерук Л.Г., Нестерук Т.Н. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН МОДЕЛИРОВАНИЕ СРЕДСТВ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ И ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ	67
Нечай А.А. Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ СЕРВЕРА В УСЛОВИЯХ РАЗРУШЕНИЯ ПРОГРАММНО- АППАРАТНОЙ СРЕДЫ	68
Никифоров В.В., Скорлышев Д.Ю., Шкиртиль В.И. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН МОДЕЛИРОВАНИЕ ЗАЩИТЫ ЦЕЛОСТНОСТИ ДАННЫХ В СИСТЕМАХ РЕАЛЬНОГО ВРЕМЕНИ	69
Ноздрачев С.О. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики IP-ТЕХНОЛОГИИ В СКУД.....	70
Ноздрачев С.О. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики IP ВИДЕОНАБЛЮДЕНИЕ С ИСПОЛЬЗОВАНИЕМ WIMAX	70
Обухов А.В. Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского ПОВЫШЕНИЕ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ОПЕРАЦИОННОЙ СРЕДЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ПРИ НАЛИЧИИ ВОЗДЕЙСТВИЯ ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	71
Пашков М.П. Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс» ИССЛЕДОВАНИЕ ПРОБЛЕМЫ РАССИНХРОНИЗАЦИИ ГРАНЕЙ В ТРОИРОВАННЫХ СИСТЕМАХ ОБРАБОТКИ И ПЕРЕДАЧИ ИНФОРМАЦИИ	73
Перервенко А.В. Россия, Санкт-Петербург, ЗАО «АСИС» ПРОБЛЕМА НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ АУТСОРСИНГА В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.....	73
Платонов В.В. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК НА ОСНОВЕ МУЛЬТИКАТЕГОРИЙНОЙ КЛАССИФИКАЦИИ	74
Платонов В.В., Поникаровский К.В. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет МОДЕЛИРОВАНИЕ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК МЕТОДОМ ОПОРНЫХ ВЕКТОРОВ	75

Потравнов А.В., Черемушкин Д.В. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики ФУНКЦИОНАЛЬНОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ СОГЛАСНО СТАНДАРТУ ISO/IEC 27005:2008.....	76
Романова К.Н., Бабкова М.И., Привалов А.А. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин» МОДЕЛЬ ПРОЦЕССОВ РЕАЛИЗАЦИИ ПРОГРАММНО-АППАРАТНЫХ ВОЗДЕЙСТВИЙ	76
Русских Я.Ю. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ ИНТЕРНЕТ-БАНКИНГА В РОССИИ	77
Савчук М. Н., Фесенко А. В., Заболотный А.П. Украина, Киев, Институт кибернетики им. В.М. Глушкова НАН Украины, Национальный технический университет Украины «КПИ», Россия, Санкт-Петербург, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН АНАЛИЗ ИСПОЛЬЗОВАНИЯ КОММУТАТИВНЫХ ШИФРОВ В КВАНТОВОЙ МОДЕЛИ ВЫЧИСЛЕНИЙ ...	77
Садченко К.И., Мироненко М.К. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики О ПРОТИВОДЕЙСТВИИ РАЗВИТИЮ БОТНЕТОВ.....	78
Суконщиков А.А., Яковлев С.А. Россия, Вологда, Вологодский государственный технический университет, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», СИТУАЦИОННОЕ МОДЕЛИРОВАНИЕ ДЛЯ ИССЛЕДОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ	78
Титов И.Е. Российская Федерация, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики КОНКУРЕНТНАЯ РАЗВЕДКА В УСЛОВИЯХ ФИНАНСОВОГО КРИЗИСА.....	79
Чистяков И.В., Орлов Д.Р. Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс» КРИПТОГРАФИЧЕСКАЯ ФАЙЛОВАЯ СИСТЕМА С ИЕРАРХИЧЕСКИМ РАЗГРАНИЧЕНИЕМ ДОСТУПА.....	80
Шишкин В.М. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ПРОБЛЕМЫ ЭКСПЕРТИЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ	80
Шустиков С. В. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики ОСНОВНЫЕ ПРОБЛЕМЫ СООТВЕТСТВИЯ РЕГУЛИРУЮЩИМ ТРЕБОВАНИЯМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	81
Щиголева М.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» РАЦИОНАЛЬНАЯ ТАКТИКА ЗАЩИТЫ ДИАГНОСТИЧЕСКИХ ДАННЫХ ПРИ ФОРМИРОВАНИИ ПРОГРАММЫ ОЗДОРОВЛЕНИЯ НАСЕЛЕНИЯ.....	82
СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ	83

Алексеев А.В. Россия, Санкт-Петербург, ОАО «Научно-инженерный центр Санкт-Петербургского электротехнического университета» РЕЙТИНГ-АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОСНОВНЫХ КЛАССОВ.....	83
Ананьев М.Ю., Баженов А. А., Галанов А.И., Щербаков В.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций, Санкт-Петербургский институт информатики и автоматизации РАН, Молдова, Кишинев, Институт математики и информатики АН Республики Молдова СТАНДАРТЫ И ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЦИФРОВОЙ ПОДПИСИ	83
Ананьев М.Ю., Доронин С.Е., Мирин А.Ю., Морозова Е.В. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций, Санкт-Петербургский институт информатики и автоматизации РАН ВАРИАНТ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ БУМАЖНЫХ ДОКУМЕНТОВ ОТ ПОДДЕЛКИ	84
Артамонов А.В., Маховенко Е.Б. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет ПРОТОКОЛЫ ГРУППОВОЙ ПОДПИСИ В СИСТЕМЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА БАЗЕ ПЛАТФОРМЫ DOCUMENTUM	85
Баженов А.А., Галанов А.И., Костин А.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций, Санкт-Петербургский институт информатики и автоматизации РАН ТЕХНОЛОГИЯ ЗАЩИТЫ БУМАЖНЫХ ДОКУМЕНТОВ ОТ ПОДДЕЛКИ НА ОСНОВЕ ЦИФРОВЫХ СЕРТИФИКАТОВ	85
Бакланов Ф.С. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики К ВОПРОСУ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ	86
Баранов Ю.А. Россия, Москва, Институт проблем информатики РАН СТАТИСТИЧЕСКИЙ МЕТОД АВТОРУБРИКАЦИИ ТЕКСТОВ ПРИ РЕАЛИЗАЦИИ МЕХАНИЗМА ТЕМАТИЧЕСКОГО РАЗГРАНИЧЕНИЯ ДОСТУПА К ТЕКСТОВЫМ ДОКУМЕНТАМ	87
Биденко С.И., Чопенко О.А., Исаенко А.Н. Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» СОДЕРЖАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ ФЛОТА	87
Борисов В.В. Россия, Санкт-Петербург, ЗАО «НПП «Системные технологии защиты информации» ЗАЩИТА СИСТЕМ УПРАВЛЕНИЯ СЕТЕВЫМИ УСТРОЙСТВАМИ	88
Верещагин В.Л. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ВОПРОСЫ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ (НА ОТСУТСТВИЕ ПРОГРАММНЫХ ЗАКЛАДОВ И НДВ) ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ОБРАБАТЫВАЮЩЕГО СВЕДЕНИЯ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ	89
Воробьев В.И., Фаткиева Р.Р., Помецко В.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ ПРОГРАММНОГО КОДА	90
Галанов А.И., Костин А.А., Молдовян У.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ПРОТОКОЛЫ СЛЕПОЙ КОЛЛЕКТИВНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ.....	90

Гаскаров В.Д. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ МОДЕЛЕЙ АБСТРАКЦИЙ	91
Гнидко К.О., Горемыкин Д.В. Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского ИССЛЕДОВАНИЕ ФРАКТАЛЬНЫХ СВОЙСТВ ВНУШАЮЩИХ ТЕКСТОВ В ИНТЕРЕСАХ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ СУГГЕСТИВНЫХ ВОЗДЕЙСТВИЙ	91
Гордеев Л.В. Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс» АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	92
Григорьева М.В. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики ПРОГРАММНЫЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ ДЛЯ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ	93
Гриняев С.Н., Довнар С.Е. Россия, Москва, Военный университет Министерства обороны Российской Федерации Беларуссия, Минск, Белорусский государственный университет О НЕКОТОРЫХ НЕДОСТАТКАХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ	93
Гурьянов Д.Ю. Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» КОНЕЧНЫЕ ГРУППЫ ДВУХМЕРНЫХ ВЕКТОРОВ: ВАРИАНТЫ ЗАДАНИЯ И СЛОЖНОСТЬ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФИМИРОВАНИЯ.....	94
Гурьянов Д.Ю., Молдовян Д.Н., Молдовяну П.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ВАРИАНТЫ РЕАЛИЗАЦИИ КОНЕЧНЫХ ГРУПП С МНОГОМЕРНОЙ ЦИКЛИЧНОСТЬЮ.....	95
Гурьянов Д.Ю., Захаров Д.В., Молдовян Н.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» СТРОЕНИЕ МУЛЬТИПЛИКАТИВНЫХ ГРУПП ВЕКТОРОВ НАД КОЛЬЦАМИ ВЫЧЕТОВ ПО МОДУЛЮ, РАВНОМУ КВАДРАТУ ПРОСТОГО ЧИСЛА	95
Дернова Е.С., Костина А.А., Синев В.Е. Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Санкт-Петербургский институт информатики и автоматизации РАН ВЫБОР ХАРАКТЕРИСТИКИ И СТЕПЕНИ РАСШИРЕНИЯ КОНЕЧНЫХ ПОЛЕЙ ДЛЯ СХЕМ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ КОНЕЧНЫХ ГРУПП МАТРИЦ	96
Дернова Е.С., Костина А.А., Синев В.Е. Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» ВЫБОР ПОРОЖДАЮЩЕГО ЭЛЕМЕНТА В СХЕМАХ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ КОНЕЧНЫХ ГРУПП МАТРИЦ И ВЕКТОРОВ	96
Десницкий В.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН КОНФИГУРИРОВАНИЕ МЕХАНИЗМА ЗАЩИТЫ ПРИ ПОМОЩИ ПОЛИТИК БЕЗОПАСНОСТИ	97
Десницкий В.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН МАСШТАБИРУЕМОСТЬ И БЕЗОПАСНОСТЬ МЕХАНИЗМА ЗАЩИТЫ НА ОСНОВЕ ПРИНЦИПА УДАЛЕННОГО ДОВЕРИЯ	98

Доронин С.Е., Молдовяну П.А., Щербаков В.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Молдова, Кишинев, Институт математики и информатики АН Республики Молдова ПОСТРОЕНИЕ СХЕМ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ КОНЕЧНЫХ ГРУПП ТРУДНОВЫЧИСЛИМОГО ПОРЯДКА.....	99
Евневич Е.Л., Белаш Е.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ПРИМЕНЕНИЕ HONEYROT ДЛЯ ЗАЩИТЫ ГРИД-СИСТЕМ	99
Егорова К.С. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики НАНОТЕХНОЛОГИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	100
Еремеев М.А., Палицын Б. А., Пономарев Ю.А. Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского К ВОПРОСУ О МЕТОДАХ ОБНАРУЖЕНИЯ ВРЕДОНОСНЫХ ВТОРЖЕНИЙ И ИХ НЕЙТРАЛИЗАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ.....	100
Замятин В.Ю., Гарбузова Т.Г. Россия, Санкт-Петербург, ГУ «Арктический и антарктический научно-исследовательский институт» ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СПЕЦИАЛИЗИРОВАННЫХ СИСТЕМ ФОНДА ДАННЫХ АРКТИЧЕСКОГО И АНТАРКТИЧЕСКОГО НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО ИНСТИТУТА (ААНИИ)	101
Захаров Д.В., Хо Нгок Зуй, Молдовян Д.Н., Молдовяну П.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет водных коммуникаций, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» СПОСОБ ЗАДАНИЯ НЕКОММУТАТИВНЫХ КОНЕЧНЫХ ГРУПП ВЕКТОРОВ ЧЕТНОЙ РАЗМЕРНОСТИ	103
Зегжда П. Д., Калинин М.О. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет ТЕХНОЛОГИЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ СРЕД ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ	103
Зегжда Д.П., Калинин М.О. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет СПЕЦИФИКА СЕРТИФИКАЦИИ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ	104
Зегжда Д.П., Калинин М.О., Москвин Д.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет ЦЕЛОСТНОСТЬ ПОСТОЯННЫХ И ИЗМЕНЯЮЩИХСЯ КОМПОНЕНТОВ ПРОГРАММНОЙ СРЕДЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ	105
Иващук И.Ю. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики ПОДХОД К СОЗДАНИЮ БАЗОВОГО ФУНКЦИОНАЛЬНОГО ПАКЕТА СЕМЕЙСТВА ПРОФИЛЕЙ ЗАЩИТЫ ДЛЯ БЕСПРОВОДНОЙ СЕТИ.....	107
Игнатьев М.Б. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения БЕЗОПАСНОСТЬ И ПОДДЕРЖКА УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ НА ОСНОВЕ МОДЕЛИРОВАНИЯ ..	107

Казаков А.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет КЛАССИФИКАЦИЯ МЕТОДОВ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК В INTERNET	108
Карташов В., Рычагов А.Ю. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики О ПРОТИВОДЕЙСТВИИ ROOTKIT	109
Корт С.С. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет МОДЕЛЬ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ СИСТЕМЫ РАСПОЗНАВАНИЯ ОБРАЗОВ.....	109
Костин А.А., Молдовян Н.А., Фаль А.М. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Украина, Киев, Институт кибернетики им. В.М. Глушкова НАН Украины О РЕАЛИЗАЦИИ ПРОТОКОЛОВ СЛЕПОЙ И КОЛЛЕКТИВНОЙ ПОДПИСИ НА ОСНОВЕ СТАНДАРТОВ ЦИФРОВОЙ ПОДПИСИ	111
Костина А.А., Молдовян Д.Н., Савчук М.Н. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Украина, Киев, Институт кибернетики им. В.М. Глушкова НАН Украины О ПОСТРОЕНИИ СХЕМ ОТКРЫТОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ И КОММУТАТИВНЫХ ШИФРОВ НА ОСНОВЕ НЕКОММУТАТИВНЫХ КОНЕЧНЫХ ГРУПП	111
Котенко И.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ПОСТРОЕНИЕ И ПОДДЕРЖКА ФУНКЦИОНИРОВАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ	112
Кузнецов И.В., Примакин А.И. Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России, Санкт-Петербургский университет МВД России К ВОПРОСУ ИСПОЛЬЗОВАНИЯ АКУСТИЧЕСКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ОБЕСПЕЧЕНИИ ЗАЩИТЫ ОБЪЕКТОВ РАЗЛИЧНОГО НАЗНАЧЕНИЯ.....	113
Лаврентьева Ю.И. Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс» ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ В ЗАЩИТЕ ИНФОРМАЦИИ	113
Марков Я.А., Калинин М.О. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет ОБНАРУЖЕНИЕ МОДИФИЦИРОВАННЫХ АТАК НА ОСНОВЕ АЛГОРИТМА СРАВНЕНИЯ ГЕНЕТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ.....	114
Маховенко Е.Б., Павлов Д.С. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет СПОСОБЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ЖУРНАЛОВ В БАНКОВСКИХ ПРИЛОЖЕНИЯХ	115
Мельник И.А., Примакин А.И. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России ОСНОВЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ОПАСНОСТИ ЕЕ УТЕЧКИ ПО КАНАЛАМ ПОБОЧНЫХ ИЗЛУЧЕНИЙ И НАВОДОК	116
Мирин А.Ю., Заболотный А.П., Молдовян У.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ПРОТОКОЛ КОЛЛЕКТИВНОЙ ПОДПИСИ НА ОСНОВЕ СЛОЖНОСТИ ЗАДАЧИ ФАКТОРИЗАЦИИ....	117

Морозова Е.В., Молдовян Д.Н., Пилькевич С.В. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Вектор», Военно-космическая академия им. А.Ф. Можайского ВАРИАНТЫ РЕАЛИЗАЦИИ КОММУТАТИВНОГО ШИФРОВАНИЯ	117
Никитенков К.С. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики АСПЕКТЫ ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА	118
Новиков В.А., Дулин А.В. Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского СРЕДСТВА СЕРТИФИКАЦИИ ПРОГРАММ С ИНТЕЛЕКТУАЛЬНЫМИ СВОЙСТВАМИ	119
Пилькевич С.В. Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского СОВРЕМЕННЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ	119
Платонов А.А. Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского К ВОПРОСУ РАСПОЗНАВАНИЯ ПРИЗНАКОВ МОДИФИКАЦИИ ИСПОЛНЯЕМОГО КОДА ПРОГРАММ В ПРОЦЕССЕ ИХ ФУНКЦИОНИРОВАНИЯ	120
Платонов В.В., Цвилик Н.В., Цвилик А.С. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет АНАЛИЗ АЛГОРИТМОВ ОБУЧЕНИЯ И ТИПОВ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ	121
Попов А.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики МНОГОВЕНДОРНЫЕ СИЛЫ АНТИВИРУСНОЙ ОБОРОНЫ	121
Резник С.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН КОМБИНИРОВАННЫЕ ПОДХОДЫ К ВЕРИФИКАЦИИ ПРОТОКОЛОВ БЕЗОПАСНОСТИ	122
Романовский Р.С. Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс» РАЗРАБОТКА И ИССЛЕДОВАНИЕ ПРОГРАМНО-АППАРАТНОГО КОМПЛЕКСА ТЕСТИРОВАНИЯ ЦИФРОВЫХ УСТРОЙСТВ	123
Рудакова С.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ	124
Семьянов П.В. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет ОРГАНИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ ВЫЧИСЛЕНИЙ НА ГРАФИЧЕСКИХ ПРОЦЕССОРАХ	124
Харинов М.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ПРИМЕНЕНИЕ СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЙ С СОХРАНЕНИЕМ ЗРИТЕЛЬНОГО ОБРАЗА	125
Цехановский В.В., Захаров Д.В., Дернова Е.С., Гортинская Л.В. Россия, Санкт-Петербург Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» ПРОТОКОЛЫ СЛЕПОЙ ПОДПИСИ, ОСНОВАННЫЕ НА ДВУХ НЕЗАВИСИМЫХ ТРУДНЫХ ЗАДАЧАХ	126

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ	127
Алексеев О.Б. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин» ВОПРОСЫ ФОРМИРОВАНИЯ ФУНКЦИОНАЛЬНОЙ АРХИТЕКТУРЫ ПОДСИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ	
	127
Бабкова М.И., Привалов А.А., Романова К.Н. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин» ОБОБЩЕННАЯ МОДЕЛЬ ПРОЦЕССА ПЕРЕДАЧИ ДАННЫХ ПО ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ПРОТИВНИКА	
	127
Буренин А.Н. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин» КОМПЛЕКСЫ СРЕДСТВ ПРЕДУПРЕЖДЕНИЯ И ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК НА СИСТЕМЫ УПРАВЛЕНИЯ СОВРЕМЕННЫХ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ	
	128
Буренин А.Н. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин» МЕТОД ПОВЫШЕНИЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЗАЩИЩЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ IP-СЕТИ	
	129
Буренин В.А., Винниченко А.В. Россия, Санкт-Петербург, ЗАО «ВСС», ФГУП «Научно-исследовательский институт «Рубин» ВАРИАНТЫ ПОСТРОЕНИЯ ПОДСИСТЕМЫ УПРАВЛЕНИЯ ОБОРУДОВАНИЕМ СОВРЕМЕННОЙ ЗАЩИЩЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ	
	129
Воронков К.Л., Шерстюк М.Ю. Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций» МЕТОДИКА СИНТЕЗА ВИТРИНЫ РАЗНОРОДНЫХ ДАННЫХ НАРУШЕНИЙ БЕЗОПАСНОСТИ	
	130
Котылевский А.С. Россия, Санкт-Петербург, ООО «НеоБИТ» РАСПРЕДЕЛЕННЫЙ КОНТРОЛЬ ПОТОКОВ ДАННЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ	
	130
Кочубинский А.И., Мирин А.Ю. Украина, Киев, Институт кибернетики им. В.М. Глушкова НАН Украины, Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ПЕРЕДАЧА СООБЩЕНИЙ ПО НЕЗАЩИЩЕННОМУ КАНАЛУ СВЯЗИ С ГАРАНТИРОВАННЫМ ПОДТВЕРЖДЕНИЕМ ПОЛУЧЕНИЯ	
	131
Курносов В.И., Хузин В.З. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин» ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННО- ПОИСКОВОЙ СИСТЕМЫ, ОБЕСПЕЧИВАЮЩЕЙ РЕШЕНИЕ ЗАДАЧ ИНТЕГРАЛЬНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ СВЯЗИ	
	131
Курносов В.И., Хузин В.З. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин» НЕКОТОРЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ПРОДУКЦИИ ПРЕДПРИЯТИЯ СВЯЗИ В КРИТИЧЕСКИХ УСЛОВИЯХ ФУНКЦИОНИРОВАНИЯ	
	133
Левин И.И., Яковлев В.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича МЕТОД ОТСЛЕЖИВАНИЯ ИСТОЧНИКОВ РАСПРЕДЕЛЕННЫХ СЕТЕВЫХ АТАК С ВНЕСЕНИЕМ МЕТОК ПЕРЕМЕННОЙ ДЛИНЫ	
	134

Олимпиев А.А. Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций» ОБЪЕКТНАЯ МОДЕЛЬ КАК СРЕДСТВО ВЫЯВЛЕНИЯ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ РЕСУРСОВ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ.....	135
Никитин В.Н., Юркин Д.В. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича АНАЛИЗ БЕЗОПАСНОСТИ СЕТЕЙ ШИРОКОПОЛОСНОГО РАДИОДОСТУПА	135
Никифоров О.Г. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин» О ПОДХОДЕ К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД НА ОБЪЕКТАХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ	136
Орлов К. М. Россия, Санкт-Петербург, 24 Центральный НИИ Министерства обороны Российской Федерации АНАЛИЗ КРИТЕРИЕВ КАЧЕСТВА ВИЗУАЛИЗАЦИИ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ.....	136
Перминов С.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ИСПОЛЬЗОВАНИЕ ОНТОЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ ПОИСКА ИНФОРМАЦИОННЫХ АНОМАЛИЙ ЧЕРЕЗ WEB	137
Рожнов М.Д., Шерстюк Ю.М. Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций» НАЗНАЧЕНИЕ ПРАВ И ПОЛНОМОЧИЙ В СИСТЕМЕ ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ СРЕДСТВАМИ ТЕЛЕКОММУНИКАЦИЙ	138
Салко Н.В. Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского К ВОПРОСУ ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БЕСПРОВОДНЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ	139
Сидельникова Е.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ВЕРИФИКАЦИЯ ПРАВИЛ ФИЛЬТРАЦИИ ПОЛИТИКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ ИСЧИСЛЕНИЯ СОБЫТИЙ И АБДУКТИВНОГО ВЫВОДА	139
Сорокин И.В., Копыльцов А.В. Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена ОСНОВНЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ ЗОМБИ-СЕТЕЙ.....	140
Суворов А.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет АРХИТЕКТУРА СЕТЕЙ СВЯЗИ С РАЗГРАНИЧЕНИЕМ ДОСТУПА НА ОСНОВЕ ШЛЮЗОВ КОНТРОЛЯ ДОСТУПА.....	140
Таран В.В., Шерстюк Ю.М. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин», ЗАО «Институт инфотелекоммуникаций» СРЕДСТВА СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ PUTHON-ПРОГРАММ.....	141
Хейстонен Д.П. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин» АНАЛИЗ ВЛИЯНИЯ ЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ НА РАБОТУ ИНФОКОММУНИКАЦИОННОЙ СЕТИ.....	142

Хейстонен Д.П. Россия, Санкт-Петербург, ФГУП «Научно-исследовательский институт «Рубин» ПОВЫШЕНИЕ ОТКАЗОУСТОЙЧИВОСТИ ЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ	142
Хвостунов Ю.С. Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс» АВТОМАТИЗИРОВАННЫЙ КОМПЛЕКС СРЕДСТВ СКОРОСТНОЙ АДАПТИВНОЙ ПОМЕХОЗАЩИЩЕННОЙ СИСТЕМЫ РАДИОСВЯЗИ	142
Чечулин А.А. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН ОБНАРУЖЕНИЕ И ПРОТИВОДЕЙСТВИЕ СЕТЕВЫМ АТАКАМ НА ОСНОВЕ КОМБИНИРОВАННЫХ МЕХАНИЗМОВ АНАЛИЗА ТРАФИКА	143
Шерстюк К.Ю. Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций» МОНИТОРИНГ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ НА СРЕДСТВА ТЕЛЕКОММУНИКАЦИЙ...	144
Шоров А.В. Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН АНАЛИЗ БИОЛОГИЧЕСКИХ ПОДХОДОВ ДЛЯ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ ОТ ИНФРАСТРУКТУРНЫХ АТАК	145
Штубов А.С. Россия, Санкт-Петербург, ФГУП «Научно-производственное объединение «Импульс» ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ АВИАЦИОННОЙ ЭЛЕКТРОСВЯЗИ	145
Явно Д.М. Россия, Санкт-Петербург, Санкт-Петербургский государственный политехнический университет УСТАНОВЛЕНИЕ ПОДЛИННОГО IP-АДРЕСА ИСТОЧНИКА АТАКИ В СЕТИ ИНТЕРНЕТ	146
Яковлев С.А., Буренин В.А. Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», ЗАО «Бизнес Компьютер Центр» ВЫБОР ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ КОММУТАЦИОННОГО ОБОРУДОВАНИЯ СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ КОМПЬЮТЕРНЫХ АТАК	146
Яковлев В.А., Шутый Р.С. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА «ЗАБЫВЧИВАЯ ПЕРЕДАЧА» ДЛЯ КОНФИДЕНЦИАЛЬНЫХ МНОГОСТОРОННИХ ВЫЧИСЛЕНИЙ С БАЗАМИ ДАННЫХ В КОМПЬЮТЕРНЫХ СЕТЯХ.....	147
ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	148
Алексеев А.В. Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет МЕТОДИКА ПРОВЕДЕНИЯ ДЕЛОВЫХ ИГР ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО КОМПЛЕКСНОЙ ЗАЩИТЕ ИНФОРМАЦИИ.....	148
Блажко А.В., Гущин А.Н. Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова ОСОБЕННОСТИ ПОДГОТОВКИ РАЗРАБОТЧИКОВ ЛИЧНОСТНО-ОРИЕНТИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	148

Блашков В.И. Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России О КОНТРПРОДУКТИВНОМ ИСПОЛЬЗОВАНИИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПРОВЕРКЕ ЗНАНИЙ УЧАЩИХСЯ	149
Бобонец С.А. Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ	150
Великовская С.А. Россия, Углич, Московский государственный университет технологий и управления ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ УЧЕБНОГО ПРОЦЕССА.....	150
Верхолат А.М., Гаврилов В.А., Касаткин В.В. Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СРЕДЕ КОМПЬЮТЕРНОЙ СИСТЕМЫ ОБУЧЕНИЯ	151
Кононов О.А, Кононова О.В. Россия, Санкт-Петербург, Санкт-Петербургский институт управления и права ПОДГОТОВКА ИТ-СПЕЦИАЛИСТОВ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ	152
Мандрик П.А. Беларуссия, Минск, Белорусский государственный университет СИСТЕМА ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ И КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ В БЕЛОРУССКОМ ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ	152
Москалёва О. И., Степанов А. Г. Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения ПРОФЕССИОНАЛЬНАЯ КОМПЕТЕНТНОСТЬ ЭКОНОМИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	153
Примакина Е.И. Россия, Кострома, Костромская государственная сельскохозяйственная академия ИНФОРМАЦИОННЫЕ КРИТЕРИИ ОЦЕНКИ ПСИХОМОТОРНОЙ И ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ОПЕРАТОРОВ.....	153
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 ПОДГТОВКА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ НАПРАВЛЕНИЯ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» НА ОСНОВЕ КОМПЛЕКСНОГО ПОДХОДА ...	154
Свирский Е.А., Шалима В.Н. Беларуссия, Минск, Институт технологий информатизации и управления Белорусского государственного университета ПОВЫШЕНИЕ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ	155
ОГЛАВЛЕНИЕ.....	156