Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

1/2011

Журнал зарегистрирован
Федеральной службой по надзору
в сфере связи, информационных технологий
и массовых коммуникаций.
Свидетельство **ПИ № ФС77-44941** от 05.05.2011
Адрес редакции: Россия, 454080,
г. Челябинск, пр. Ленина, д. 76.
Тел./факс **(351) 267-90-65, 267-97-01.**
Электронная версия журнала
в Интернете
www.info-secure.ru
E-mail **i-secur@mail.ru**

В номере

In this issue

Конец двадцатого века в России был ознаменован высоким скачком развития информационных технологий, электронных коммуникаций, компьютеризацией всех структур государства и общества. Двадцать первый век характеризуется тотальной компьютеризацией и интернетизацией всей страны. И, видимо, недалек тот день, когда компьютер и Интернет будут в каждой семье. Президентом поставлена задача создания «электронного правительства». А закон «О персональных данных», принятый в 2006 году, всех граждан России включает в электронный информационный оборот.

Интернет стал универсальным средством получения и обмена информацией, благом и пользой для гражданина, общества и бизнеса. Но в то же время Интернет превратился в опасный инструмент противоправных деяний против государства и личности, если его используют хакеры, криминальные группы, националисты или террористы. Возросли риски и угрозы информационной безопасности.

Недавний пример тому — скандальная история с сайтом Вики Ликс.

Поэтому построение современного информационного общества, в котором важнейшими ценностями являются информация и знания, невозможно без обеспечения информационной безопасности. А развитое информационное общество является важнейшей предпосылкой построения правового государства.

Коллеги, считаю создание журнала в Уральском федеральном округе «Безопасность в информационной сфере» велением времени.

Отмечу, что само название журнала адресует нас к Доктрине информационной безопасности Российской Федерации. Очевидным будет и формирование контента журнала в соответствии с положениями Доктрины. В любом случае общие направления работы редакционного совета будут базироваться на методах обеспечения информационной безопасности страны: правовых, организационно-технических и экономических. Они подсказывают рубрикацию журнала и иерархию построения рубрик.

Приглашаю коллег к сотрудничеству.

Ваши предложения по формированию тематических планов выпусков, рубрик и ваши творческие идеи помогут в становлении журнала «Вестник УрФО. Безопасность в информационной сфере».

В. И. МАЙОРОВ,
ответственный редактор журнала,
д. ю. н., проф., проректор ЮУрГУ,
руководитель Челябинской секции
Координационного совета по подготовке
(переподготовке) и повышению квалификации
кадров по защите информации
в Уральском федеральном округе.

Уважаемые читатели!

Этой статьей я открываю первый номер журнала, который в дальнейшем, надеюсь, приобретет популярность среди студентов, аспирантов, специалистов и людей, интересующихся информационной безопасностью.

Выражаю надежду на успешное и плодотворное развитие журнала, стимулирующего исследования по информационной безопасности, рад приветствовать его читателей и желаю им новых творческих успехов, новых достижений на благо безопасности информационного пространства Урала и России!

А. И. БОЛГАРСКИЙ,
руководитель Управления Федеральной службы
по техническому и экспортному контролю России
по УрФО

УДК 32:316:002
ББК 66.2с51

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК СОСТАВЛЯЮЩАЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

В статье рассмотрены место и роль информационной безопасности в системе национальной безопасности, закрепленные в «Стратегии национальной безопасности Российской Федерации до 2020 года», а также определены задачи ФСТЭК России как объекта отечественной системы обеспечения информационной безопасности.

***Ключевые слова**: информационная безопасность, национальная безопасность, стратегия.*

Protection of constitutional rights of citizens in the domain of information security

The article describes the position and role of the information security in the National Security System stipulated in the «National Security Strategy of the Russian Federation until 2020», as well as the objectives of the Federal Agency for Technical and Export Control of Russia as an object of domestic information security system.

***Key words:** information security, national security, strategy.*

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность России существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет только возрастать.

Согласно «Стратегии национальной безопасности Российской Федерации до 2020 года» (далее — «Стратегия…»), национальная безопасность — состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права,

свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие России, оборону и безопасность государства.

Важнейшую роль в системе обеспечения национальной безопасности играет информационная безопасность. Это подтверждается анализом положений «Стратегии...», согласно которым, с целью разработки и реализации комплекса оперативных и долговременных мер по предотвращению угроз национальной безопасности, предполагаются разработка и внедрение технологий информационной безопасности в системах государственного и военного управления, системах управления экологически опасными производствами и критически важными объектами, а также обеспечение условий для гармонизации национальной информационной инфраструктуры с глобальными информационными сетями и системами. Угрозы информационной безопасности предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в России, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности.

Информационная безопасность представляет собой самостоятельную составляющую национальной безопасности, роль и значение которой с каждым годом неуклонно возрастает. Угрозы информационной безопасности возникают со стороны человеческого общества и могут состоять в воздействии на экономику, государство, личность. Глобализация дает средства для информационного и финансового воздействия на партнеров и конкурентов в локальном, региональном и глобальном масштабах. Целью таких воздействий является изменение распределения произведенных благ в пользу тех, кто разрабатывает, имеет и применяет соответствующие технологии для таких воздействий. Воздействия на экономику могут осуществляться, например, путем информационных атак против национальных валют и фондовых рынков (волна которых прокатилась по миру в конце 90-х гг. прошлого века). Целенаправленные информационные воздействия могут иметь далеко идущие деструктивные последствия, как для отдельной личности, общества, государства, так и для самого существования цивилизации. Так, например, ежегодный размер убытков в мире от компьютерной преступности оценивается в 500 миллиардов долларов. Процесс информатизации мирового сообщества развивается столь стремительно и зачастую непредсказуемо, что не всегда своевременно удается оценить реальность проблемы информационной безопасности, многообразие ее проявлений и недопустимость недооценки рисков, которые несет глобальная информатизация жизни человеческого общества. Наряду с этим, серьезную опасность для России, как отмечается в «Стратегии...», представляют стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним. Информационный взрыв, вызванный научно-техническим прогрессом в области средств информатизации и коммуникации, резко увеличил возможности ведения информационной борьбы и привел к появлению новых категорий «информационная война» и «информационное оружие».

В современных условиях политического и социально-экономического развития обостряются противоречия между потребностями в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение. Тенденция к увеличению открытости общества, повышение интенсивности информационного обмена, широкое использование передовых технологий сбора и обработки информации создают предпосылки для возможных противоправных действий в отношении информации и ее пользователей. Поэтому наряду с информационной открытостью должна быть обеспечена также реализация конституционных прав человека, общества и государства на защиту информации с ограниченным доступом. Защита информации — это комплекс мероприятий, проводимых собственником информации по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих доступ к засекреченной информации и ее носителям.

Вопросы защиты государственной тайны приобрели в России особую значимость на

рубеже прошлого и нынешнего веков — в период глубоких социально-экономических преобразований, когда, с одной стороны, появляются новые угрозы безопасности государства, а, с другой — сложившиеся режимы защиты государственной тайны перестали срабатывать должным образом. Объективные требования быть более открытым и доступным исходят из потребности развития современного общества. Тенденция увеличения степени открытости государства перед обществом диктует необходимость максимально возможного сокращения числа сведений, относимых к государственной тайне, открытости общего перечня относимых к ней категорий сведений, механизмов засекречивания и условий рассекречивания. Обязанность государства — взять на себя формирование взвешенного механизма защиты различных видов информации и установления рамок действия институтов тайн. Такие требования исходят, с одной стороны, из потребности современного общества быть более открытым и доступным, а, с другой — диктуются необходимостью обеспечения безопасности личности, общества и государства.

Руководствуясь положениями «Стратегии...», можно сделать вывод, что обеспечение информационной безопасности России должно быть направлено на защиту конституционных прав и свобод личности, информационное обеспечение государственной политики, обеспечение безопасности информационных ресурсов и надежное функционирование информационных и телекоммуникационных систем. При этом одной из требующих решения задач по обеспечению информационной безопасности России является развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны.

В июне 2000 г. Совет Безопасности Российской Федерации принял, а 9 сентября того же года Президент Российской Федерации В. В. Путин подписал «Доктрину информационной безопасности Российской Федерации», которая развивает общие положения о национальной безопасности применительно к информационной сфере и служит основой для формирования государственной политики в области обеспечения информационной безопасности России.

Принятие этого документа на столь высоком уровне является безусловным свидетельством признания значимости проблемы информационной безопасности в жизни современного российского общества и знаменует включение информационной безопасности в число важнейших государственных проблем.

В частности, данный документ определил такие основополагающие понятия, как:

— национальные интересы Российской Федерации в информационной сфере и их обеспечение;

— виды и источники угроз информационной безопасности;

— основные задачи по обеспечению информационной безопасности;

— методы и особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни;

— основные положения государственной политики обеспечения информационной безопасности Российской Федерации;

— основные функции системы обеспечения информационной безопасности;

— основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации.

В этой связи необходимо отметить, что Федеральная служба по техническому и экспортному контролю (далее — ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1) обеспечения безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства (далее — КСИИ);

2) противодействия иностранным техническим разведкам на территории Российской Федерации (далее — ПД ИТР);

3) обеспечения защиты информации, содержащей сведения, составляющие государственную тайну (далее — ТЗИ);

4) обеспечения безопасности персональных данных;

5) осуществления экспортного контроля.

ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации.

ФСТЭК России и ее территориальные органы входят в состав государственных органов обеспечения безопасности.

Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации.

В пределах Уральского федерального округа вышеуказанные задачи, в рамках сво-

ей компетенции, решаются нашим Управлением.

В заключение считаю своим долгом напомнить, что Федеральной службой по техническому и экспортному контролю разработаны, а приказом Минздравсоцразвития России от 22 апреля 2009 г. № 205 утверждены «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации», в соответствии с которыми современный специалист по защите информации должен уметь определять состав защищаемой информации, степень уязвимости, рассчитывать ущерб от возможной утраты информации, оценивать эффективность различных методов и средств защиты, проводить специальные исследования и сертификацию различных технических средств обработки и защиты информации, уметь проектировать и внедрять системы защиты информации, знать и использовать зарубежный опыт.

Полноценное профессиональное становление защитника информации требует от него больших усилий по овладению самыми разными знаниями, но оно принципиально невозможно без творческого подхода к быстро меняющемуся миру информационных технологий. Не только умение познавать и применять имеющееся знание, но и создавать новое — вот отличительная черта истинного профессионала.

А. И. Болгарский

BOLGARSKIY A. I., Head of the Department of Federal Agency for Technical and Export Control of Russia for Ural Federal District.

КОНСТИТУЦИОННЫЕ ПРАВА ГРАЖДАН И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 347.157:004.7 + 004.7:347.157
ББК Х401.114 + Х400.32

М. И. Гришанков

Ребенок в Интернете: проблемы и решения

В статье рассмотрена проблема защиты детей от негативного влияния вредной информации, функционирующей в Интернете; охарактеризованы пути ее решения негосударственными организациями, органами исполнительной и законодательной властей; обоснована необходимость разработки и реализации государственной политики формирования в России культуры кибербезопасности.

Ключевые слова: *кибербезопасность, вредная информация, защита детей, культура безопасности.*

M. I. Grishankov

Child Surfing on the Internet: Problems and Solutions

The article is devoted to the problem of protection of children against the adverse effect of harmful Internet content. The article describes the solutions to this problem developed for non-government organizations, executive and legislative bodies, and justifies the need for development and implementation of national policy aiming at formation of cyber safety culture in Russia.

Key words: *cyber safety, harmful content, protection of children, safety culture.*

Сегодня в ряду многочисленных проблем, связанных с обеспечением безопасности Интернета, выделяется задача защиты детей от тлетворного влияния вала гуляющей по Интернету вредной информации. Мы в Комитете Государственной Думы по безопасности занимаемся этими вопросами постоянно. Под эгидой Комитета проводятся соответствующие исследования в рамках созданных нами экспертных рабочих групп.

Хочу подчеркнуть, что интернет-сообщество оперативно реагирует на возникающие новые угрозы в упомянутой сфере. Развёрнута работа горячих линий, создаются новые средства фильтрации информации, налаживается обучение детей, родителей и педагогов, организуется пропаганда «чистого» Интернета. К этой работе присоединяются и те представители интернет-бизнеса, которые прежде не соотносили свою деятельность с содержанием информации, например, операторы связи. В прошлом году был принят ряд документов, закрепляющих осознанное стремление профессионального интернет-сообщества максимально защитить детей-пользователей. Практически все это делается негосударственными организациями.

Нельзя сказать, что государство безучастно к проблемам «чистого» Интернета. Конечно, и исполнительная, и законодательная власти предпринимают определенные шаги в деле очищения сети от противоправной информации. В конце прошлого года был принят Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию». Мы усилили уголовную ответственность за развратные действия сексуального характера по отношению к несовершеннолетним и иные подобные преступления. Однако приходится констатировать, что эта деятельность пока осуществляется недостаточно системно.

Защиту детей и подростков как самой уязвимой части общества от компьютерной преступности и вредоносной информации нельзя отрывать от формирования в целом

устойчивой культуры кибербезопасности. Как нам кажется, пришла пора разработать основы целостной государственной политики формирования в России культуры кибербезопасности.

Ребенок, особенно школьник, должен уметь работать с информацией: искать ее, эффективно отсеивать ненужную, обрабатывать, анализировать, оценивать достоверность и актуальность и так далее. Но одновременно он должен обладать знаниями и навыками защиты информации персонального характера, должен уметь защитить используемые средства коммуникации и плюс к этому — защитить себя самого от негативной информации, которую обрушивает на него эпоха передовых информационных технологий. В этом ему, конечно, должны помогать взрослые, в первую очередь родители и педагоги.

Сегодня на этом фоне серьезную тревогу вызывает низкий уровень медиаграмотности и культуры кибербезопасности подрастающего поколения при наличии развитых навыков пользования информационно-коммуникационными технологиями. Это создаёт у молодых пользователей сети иллюзию вседозволенности и безнаказанности, усиливает правовой нигилизм, делает их легкой добычей преступников всех мастей. Эти проблемы мы не раз обсуждали в рамках мероприятий Национального форума информационной безопасности (Инфофорума), который успешно работает в нашей стране вот уже более десяти лет.

На Евразийском Инфофоруме 2010 года участниками заседания на тему «“Чистый Интернет”: новые возможности в развитии интеграционных процессов электронного взаимодействия и социальная ответственность в Интернете» была принята резолюция, направленная на формирование безопасной и этичной интернет-среды. Участники сочли крайне важным усилить поддержку полезных общественных инициатив и стимулировать их дальнейшее развитие. В целях координации этой работы и обеспечения концептуального единства общих и отраслевых принципов деятельности в сети предложено сформировать Общественный совет по координации общественных инициатив с участием представителей органов государственной власти, бизнес-сообщества, институтов гражданского общества и традиционных конфессий. Пока окончательные решения по механизмам формирования Общественного совета не приняты. Но ряд организаций уже двигаются в данном направлении.

Проблемы формирования культуры кибербезопасности носят глобальный характер, поэтому нам придется создавать национальные и межгосударственные механизмы для формирования, развития и внедрения устойчивой глобальной культуры кибербезопасности. Именно к этому призывает нас соответствующая резолюция, принятая на 66 заседании Генеральной Ассамблеи Организации Объединенных Наций.

Представляется, что обсуждение в рамках Инфофорума целесообразно в приоритетном порядке ориентировать на выработку общественно-государственных механизмов взаимодействия в деле формирования культуры кибербезопасности, в том числе путем создания необходимых технологических решений, организационных структур, развития образования и подготовки кадров. Уверен в том, что это позволит в конечном счете существенно понизить степень угроз, которые несет глобализация инфокоммуникационных технологий, и усилить эффективность их применения во всех сферах жизнедеятельности.

Перед нами, законодателями, все еще стоят серьезные задачи по правовому регулированию обеспечения безопасности детей и юношества в Интернете, совершенствованию норм ответственности за нарушение законодательства, созданию более эффективных механизмов противодействия экстремизму и терроризму с использованием сети, обеспечению однозначной идентификации лица, разместившего в сети антиобщественные материалы, владельца домена, под которым они опубликованы, а также лица, предоставившего технические средства для их размещения. И все это надо делать в рамках гармонизации национальных и международных подходов.

Еще одна важнейшая для всех нас задача состоит в том, чтобы создавать в Интернете позитивный контент. Его задача — отвлекать внимание детей и подростков от вредной по содержанию информации, циркулирующей в Интернете. Здесь должен сработать эффект замещения объекта внимания. Действительно, добро в Интернете обязано вытеснять зло. Пусть медленно, постепенно, но комплексные усилия интернет-сообщества и государства, я убежден, дадут положительный эффект.

ГРИШАНКОВ Михаил Игнатьевич, первый заместитель председателя Комитета Госдумы РФ по безопасности.

GRISHANKOV Mikhail Ignatievich, First Deputy Chairman of the Defense Committee of RF State Duma.

УДК 351.746 + 004.056.5:347
ББК Х401.132

А. А. Скоробогатов, О. Р. Уторов

Проблемы правового регулирования обращения и защиты государственной тайны

Статья посвящена научному осмыслению проблем правового регулирования обращения и защиты государственной тайны в современных условиях. Выявлены положения, которые в ближайшей перспективе потребуют принципиальной перестройки отношений, связанных с государственной тайной.

***Ключевые слова**: государственная безопасность, государственная тайна, ФСБ, правовое регулирование.*

A. A. Skorobogatov, O. R. Utorov

Problems of Legal Regulation of Circulation and Protection of State Secret

The article is devoted to the scientific understanding of problems connected with the legal regulation of circulation and protection of state secret in the present-day conditions. The article contains regulations that will require a fundamental alteration in relations connected with the state secret in the near future.

***Key words:** national security, state secret, Federal Security Service, legal regulation.*

Обеспечение национальной безопасности государства и его устойчивого функционирования неразрывно связано с деятельностью органов федеральной службы безопасности по защите сведений, составляющих государственную тайну.

В современной России, как и во всем мире, государственная тайна остается важнейшим инструментом защиты оборонных, экономических, политических и других важнейших интересов страны.

Сегодня ряд вопросов защиты государственной тайны получают новую трактовку в контексте прав и свобод человека. Преодолеваются сложившиеся ранее стереотипы культа секретности, ликвидируются информационные барьеры, изживаются методы административно-командного управления информационными процессами. Вместе с тем, чрезмерная информационная открытость ориентирует иностранные спецслужбы и организации на добывание и интегрирование данных из всех возможных источников, а соответственно усиливает интерес к нашей стране как объекту разведки.

Размеры ущерба от посягательств на государственную тайну делают проблему ее сохранности значимой для государства и общества. В то же время государство и общественность по вопросу государственной тайны в оценках далеко не всегда едины.

Необходимость трансформации института обращения и защиты государственной тайны вызвана, на наш взгляд, следующими актуальными проблемами:

— трудностью обеспечения баланса между правом на свободу доступа к информации и столь же правомерными основаниями на ограничение в доступе к ней;

— резким возрастанием информационных ресурсов и отставанием технологии их анализа;

— несовершенством процедур своевременного рассекречивания с целью их вклю-

чения в ресурсы экономического роста государства;

— распространением части сведений, составляющих государственную тайну, в средствах массовой информации.

При построении оптимальной модели правовой охраны государственных секретов важно правильно поставить задачу. По нашему мнению, усилия должны быть направлены не только на улучшение существующего правового режима защиты имеющихся секретов. Необходимо оценить весь цикл обращения сведений, которые объективно нуждаются в охране как государственная тайна.

В настоящее время объем сведений, отнесенных к государственной тайне и подлежащих защите, явно избыточен. Это влечет значительные затраты как для государства, так и для отдельных предприятий. Тормозится развитие отношений собственности, в том числе интеллектуальной. Из-за необоснованного засекречивания информации затрудняется информационный обмен. Затрудняется внешний контроль за деятельностью ведомств, поскольку информация об их деятельности нередко засекречивается необоснованно. В то же время значимая и чрезвычайно ценная для общества и государства информация нередко остается без внимания и не охраняется режимом государственной тайны.

На наш взгляд, это объясняется отсутствием объективных критериев отнесения сведений к государственной тайне. Действующие нормативные правовые акты еще не сложились в стройную систему и не в полной мере соответствуют друг другу.

На концептуальном уровне требуется осмыслить целый ряд вопросов. Прежде всего к ним относятся следующие:

— понятие государственной тайны как комплексного правового института;

— ее соотношение с другими видами защищаемой информации;

— взаимосвязь правового регулирования обращения государственной тайны и отношений собственности, в том числе интеллектуальной;

— правоотношения, возникающие в процессе обращения государственной тайны;

— правовые механизмы обеспечения сохранности государственной тайны во всех сферах общественной жизни и на всех этапах ее оборота;

— объем правоограничений для секретоносителей;

— виды и условия ответственности за нарушения сохранности государственной тайны.

В зависимости от научно обоснованных ответов на эти вопросы можно будет вести речь о перспективном правовом регулировании обращения государственной тайны, базирующемся на комплексе взаимно увязанных интересов личности, общества и государства.

Научное осмысление вопросов правового регулирования обращения государственной тайны позволяет сформулировать следующие основные положения:

1. Государственная тайна — это часть информации, изъятая из свободного оборота. Она ограничивает конституционные права граждан, интересы в научной, экономической и иных сферах. Это нередко приводит к конфликту, в котором приоритет отдается интересам безопасности государства. Поэтому недопустим произвольно расширительный подход к определению понятия государственной тайны и круга относимых к ней сведений. Критерии государственной тайны должны быть осязаемыми и объективными, а потому понятными и приемлемыми не только для государства, но и для гражданина и общества. Это — условие достижения баланса интересов.

2. Государственная тайна является особым видом защищаемой государством информации. Ее сохранность не может быть обеспечена в должной мере механизмами защиты тайны следствия, коммерческой тайны и прочих тайн. В то же время не следует объявлять государственной тайной те секреты, которые более эффективно могут охраняться их обладателями иными способами.

3. Основным объективным (материальным) критерием отнесения сведений к государственной тайне в законе должно быть наличие реальной угрозы причинения существенного вреда безопасности государства, а также жизненно важным интересам общества и личности в случае их распространения. По данному критерию, в частности, выделяются те области общественной жизни, в которых государственная тайна может обращаться: военная, внешнеполитическая, экономическая, разведывательная, контрразведывательная и оперативно-розыскная. Речь идет об уточнении объема государственной тайны с учетом, во-первых, областей, в которых она обращается, и, во-вторых, возможности существенного, а не любого вреда названным интересам. Такое уточнение повлечет изменение структуры государственной тайны, но вряд ли позволит ограничить ее объем (в связи с тем, что потребуется засекречивать данные, которые ныне государством не охраняются).

4. Государственная тайна — это межотраслевой правовой институт. Поэтому правовое регулирование оборота государственной тайны должно быть комплексным, то есть осуществляться нормами различных отраслей права. Дальнейшее регулирование ее оборота исключительно в административно-правовой сфере малоэффективно. Объектом внимания должно стать также гражданское, уголовное, гражданское процессуальное, арбитражное и уголовно-процессуальное законодательство.

Перечисленные положения требуют достаточно принципиальной для нашей страны перестройки отношений, связанных с государственной тайной. Уже в ближайшей перспективе возможна реализация ряда мер. Они, по нашему мнению, будут способствовать решению наиболее острых проблем правового регулирования оборота государственной тайны. Эти проблемы, часть которых уже была обозначена ранее, таковы:

1. Проблема недостаточной системности правового регулирования оборота государственной тайны.

В настоящее время нормативно-правовая база в сфере обращения государственной тайны представляет собой громоздкую и противоречивую конструкцию, состоящую из более чем двухсот правовых актов. Регулирование обращения государственной тайны ныне фактически свелось к административно-правовому режиму защиты государственной тайны с распространением действия административно-правовых норм на правовые отношения, относящиеся к другим отраслям права.

Для решения этой проблемы необходимо:

— усилить системообразующую роль Закона РФ «О государственной тайне»;

— провести систематизацию действующего законодательства с целью устранения противоречий между различными нормативно-правовыми актами;

— начать не декларативную, а реальную дифференциацию регулирования оборота государственной тайны путем создания процедурных механизмов в отраслевом законодательстве.

2. Проблема критериев отнесения соответствующих сведений к государственной тайне. Критерии должны быть четкими и соответствовать друг другу. Без этого нельзя определить оптимальный объем сведений, составляющих государственную тайну.

Согласно статье 2 Закона «О государственной тайне» общие критерии относимости сведений к государственной тайне обусловлены, в частности, возможным ущербом безопасности РФ. В связи с этим следует иметь в виду, что институт государственной тайны должен защищать не только безопасность Российской Федерации, но и жизненно важные интересы общества и личности (например, в области оперативно-розыскной деятельности). Кроме того, правильнее было бы говорить не о возможном ущербе безопасности Российской Федерации, а о создании угрозы его наступления.

Например, предание огласке сведений о конфиденциальном сотрудничестве лица с правоохранительным органом сразу же создает реальную и вполне доказуемую угрозу наступления ущерба: от угрозы для жизни этого лица до срыва всех планируемых мероприятий. Нередко точный размер ущерба установить, а, самое главное, доказать представляется невозможным.

Необходимо продолжить работу по уточнению и, особенно, детализации перечней сведений, составляющих государственную тайну, а также критериев засекречивания информации.

В настоящее время избыточный объем сведений с грифом «секретно» девальвирует понятие государственной тайны и порождает недостаточно ответственное отношение к ее сохранности.

Сказанное свидетельствует о необходимости установления эффективного контроля за обоснованностью засекречивания и рассекречивания информации. В настоящее время различные ведомства засекречивают и рассекречивают информацию, и они же и контролируют обоснованность этого. Понятно, что эффективным такой механизм быть не может. Государство в лице специально уполномоченного органа обязано проверять все ведомства на предмет обоснованности засекречивания или рассекречивания, ведь речь идет не о тайне ведомства, а о тайне государства.

В то же время принцип максимального ограничения доступа к сведениям, составляющим государственную тайну, в данной норме сочетается с принципом отраслевой, ведомственной или программно-целевой принадлежности, декларированном в статье 9 Закона РФ «О государственной тайне». Однако практическая реализация нормы сопряжена с определенными трудностями. Дело в том, что в Перечне сведений, отнесенных к государственной тайне, в ряде случаев сразу несколько ведомств являются полномочными органами по распоряжению одними и теми же сведениями. Например, сведениями о балансовых запасах в недрах

страны, добыче (производстве), передаче или потреблении стратегических видов полезных ископаемых в целом по Российской Федерации и ее субъектам распоряжаются Минприроды России, Минпромторг России, Минэкономразвития, Минэнерго России. Каждое из них правомочно передать такие сведения без согласования с другими распорядителями. Очевидно, что интересы безопасности государства требуют проведения единой политики в данном вопросе, а следовательно, максимального ограничения числа органов, имеющих право распоряжения теми или иными категориями сведений.

Многие проблемы административно-правового регулирования государственной тайны также требует своего решения.

Во-первых, новый Кодекс Российской Федерации об административных правонарушениях так или иначе урегулировал вопросы административной ответственности юридических и должностных лиц, но упустил обычных граждан.

Во-вторых, «Инструкция по обеспечению режима секретности в Российской Федерации», утвержденная постановлением Правительства РФ от 5 января 2004 года № 3-1, требует приведения в соответствие с ней ведомственных нормативных актов.

В-четвертых, Закон «О государственной тайне» предусматривает указание на носителе информации срока ее засекречивания. Исходя из этого, рассекречивание сведений, составляющих государственную тайну, должно осуществляться по истечении указанных сроков засекречивания. Однако на практике указать срок засекречивания достаточно сложно.

В-пятых, не предусмотрена персонификация ответственности за правильность установления грифа секретности в отношении исполнителя, фактически засекречивающего сведения.

Нами поставлены далеко не все проблемы современного правового регулирования обращения государственной тайны. Их решение может быть реализовано в новом Законе «О государственной тайне» либо в его новой редакции, а также в отраслевом законодательстве.

СКОРОБОГАТОВ Андрей Александрович, сотрудник Южно-Уральского государственного университета.

SKOROBOGATOV Andrey Aleksandrovich, employee of the Southern Ural State University.

УТОРОВ Олег Равильевич, сотрудник Южно-Уральского государственного университета.

UTOROV Oleg Ravilievich, employee of the Southern Ural State University.

УДК 343.63 + 004.738.5.056.53
ББК Х404.06 + Х401.114

З. В. Макарова, А. А. Сильченко

Защита от диффамации в рамках сети Интернет

В статье рассмотрены проблемы защиты личности от диффамации в сети Интернет — правонарушений в виде распространения информации, не соответствующей действительности и порочащей честь, достоинство или деловую репутацию личности. Выявлены признаки диффамации, регулирующие проблему нормативные акты, особенности диффамации через интернет-коммуникации, даны рекомендации по решению проблемы диффамации.

***Ключевые слова**: диффамация, ложная информация, клевета, угроза, честь, достоинство личности.*

Z. V. Makarova, A. A. Silchenko

Protection against Defamation in the Internet

The article describes the problems of protection of individuals against defamation in the Internet (law violations in the form of distribution of false statements that affect the honor, dignity or goodwill of an individual). The article also contains the signs of defamation, regulations governing this problem, peculiar features of defamation via the Internet communication means and recommendations to solve the defamation problem.

***Key words:** defamation, false information, libel, threat, honor, dignity of individual.*

Актуальность вопроса информационной безопасности как отдельной личности, так и элементов общества в целом, подчеркивается мощным развитием информационного поля, в том числе благодаря интернет-технологиям. Современный человек подвержен значительным воздействиям разного рода со стороны направляемой на него информации, а значит, он нуждается в защите от возможного негативного воздействия со стороны общества и социальной среды. Основа такой безопасности для личности или организации — правовые нормы, регулирующие такие воздействия.

Рассмотрим такое понятие, как диффамация. Данный юридический термин, являющийся общепринятым во многих странах мира, означает правонарушение в виде распространения информации (устно или в публикациях), не соответствующей действительности и порочащей честь, достоинство или деловую репутацию физических и юридических лиц. Понятие имеет латинское происхождение — diffanatio (*англ.* defame — порочить)[1].

В качестве диффамации принято выделять как распространение заведомо ложных сведений, порочащих репутацию (умышленная недостоверная диффамация, или клевета), так и неумышленное распространение таких сведений (неумышленная недостоверная диффамация).

Заведомость ложных сведений означает, что виновный осознает несоответствие или возможность несоответствия действительности сообщаемых им о другом человеке сведений. Предположение о том, что распространяемые сведения могут оказаться правдивыми (значит, возможно, и ложными), следует считать одним из проявлений заведомости и предполагает уголовную ответственность за клевету (статья 129 УК РФ)[2].

Обязательными признаками диффамации являются:

1. Факт публичного распространения сведений, причем истцу, защищающему свои честь, достоинство и деловую репутацию, достаточно доказать только данный признак.

2. Распространяемые сведения не соответствуют действительности. Доказывание соответствия сведений действительности возлагается на ответчика. Кроме того, важным моментом является признание экспертами, что эти сведения содержатся именно

в фактах и утверждениях, а не являются домыслами, мнениями либо оценочными суждениями.

3. Сведения порочат честь, достоинство, деловую репутацию. Порочащими сведения являются в случае, если их распространение влечет умаление репутации лица в глазах правильно мыслящих членов общества или побуждает их остерегаться или избегать его.

Основополагающими нормативными актами, регулирующими обозначенную проблему, являются сразу несколько правовых источников. При злоупотреблении свободой слова и массовой информацией в Конституции Российской Федерации предусмотрено право на защиту своей чести и доброго имени (ст. 23 и 46)[3]. Помимо этого, в ст. 152 Гражданского кодекса Российской Федерации предусмотрено право на судебную защиту чести, достоинства и деловой репутации от распространения не соответствующих действительности порочащих сведений[4]. Таким образом, суть любого диффамационного спора заключается в нахождении золотой середины между правом на защиту чести, достоинства, деловой репутации и правом на свободу слова и массовой информации.

Некоторые разъяснения по этому поводу даются в Постановлении Пленума Верховного Суда РФ от 24 февраля 2005 г. № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» (далее — Постановление): «Гражданин или организация, в отношении которых распространены сведения, порочащие его честь, достоинство или деловую репутацию, вправе наряду с опровержением таких сведений требовать возмещения убытков и морального вреда, причиненных их распространением»[5].

Теперь рассмотрим явление диффамации как угрозу информационной безопасности личности через призму интернет-коммуникаций. Легкость, с которой в Интернете можно опубликовать какое-то сообщение на весь мир, послать послание друзьям, врагам или третьим лицам, вводит в соблазн множество людей. Но использование открывающихся новых возможностей далеко не всегда регулируется принятыми в обществе нормами вежливости и корректности.

На сегодняшний день данные явления в сети Интернет привлекают к себе все больше и больше внимания. Блоги, социальные сети, форумы, комментарии — все это удобная площадка для выражения собственного мнения. Однако некая свобода и неявная вседозволенность в сети довольно часто порождает и диффамацию.

Представим такую ситуацию: некий пользователь оставил негативный отзыв о качестве услуг на странице сайта, где размещена информация о какой-либо компании.

По постановлению, надлежащими ответчиками по искам о защите чести, достоинства и деловой репутации являются авторы не соответствующих действительности порочащих сведений, а также лица, распространившие эти сведения[6]. Это значит, что по закону ответственность могут понести как автор данного сообщения, так и администратор Интернет-ресурса (а именно владелец домена).

Несмотря на то что, если форма отправки сообщения может не предусматривать наличие никакой контактной информации о лице, являющемся автором данного сообщения, это лицо все же можно в некоторых случаях идентифицировать по IP-адресу. Для этого делается запрос провайдеру интернет-услуг о предоставлении информации об абоненте. Но в ряде случаев при использовании автором диффамационного материала прокси-серверов, подменяющих IP-адрес, лицо установить все же не удается.

В постановлении по этому поводу указывается: «Судебная защита чести, достоинства и деловой репутации лица, в отношении которого распространены не соответствующие действительности порочащие сведения, не исключается также в случае, когда невозможно установить лицо, распространившее такие сведения (например, при направлении анонимных писем в адрес граждан и организаций либо распространении сведений в сети Интернет лицом, которое невозможно идентифицировать)». В соответствии с п. 6 ст. 152 Гражданского кодекса Российской Федерации суд в указанном случае вправе по заявлению заинтересованного лица признать распространенные в отношении него сведения не соответствующими действительности порочащими сведениями. Такое заявление рассматривается в порядке особого производства[7].

Однако в этом случае вполне резонно в качестве лица, распространившего диффамационные материалы, считать администратора сайта. С одной стороны, это логично: ведь администратор сайта распространил данную информацию с помощью специализированного программного обеспечения, которое позволило опубликовать отзыв автора, и теперь владелец интернет-ресурса в случае доказательства его вины должен понести ответственность. Но в то же время, каким об-

разом владельцу популярного сайта, на котором публикуются несколько тысяч сообщений в сутки, отследить все опубликованные сообщения? Использовать предварительную модерацию? Для большинства проектов в сети это могло бы стать гибельным явлением, поскольку будет отнимать слишком много времени. Тем не менее, законодатель предоставляет администратору возможность разрешить данную проблему. В статье 57 Закона Российской Федерации «О средствах массовой информации»[8] предусматривается освобождение ответственности редакции средств массовой информации, если материалы содержатся в авторских произведениях, идущих в эфир без предварительной записи, либо в текстах, не подлежащих редактированию в соответствии с настоящим Законом, что в среде интернет-ресурсов можно трактовать как публикацию сообщений и комментариев на сайте без предварительной модерации. Таким образом, выходом для владельцев интернет-площадок может быть регистрация сайта в качестве средства массовой информации.

В интернет-среде многие сайты практикуют пользовательские соглашения, в которых упоминается, что администрация сайта не несет ответственности за публикуемые на ресурсе материалы. Данная мера является юридически неверной и не дает владельцу сайта какой-либо правовой защиты.

В качестве рекомендаций администраторам интернет-ресурсов, не зарегистрированных в качестве средств массовой информации, можно предложить обязательное указание контактных данных при регистрации пользователей с аутентификацией через мобильные сервисы (подтверждение регистрации с помощью СМС и мобильного телефона). Данная мера будет направлена на повышение ответственности зарегистрированных пользователей при публикации различного рода сообщений и позволит уменьшить диффамационную составляющую в публикуемой информации.

Таким образом, защита от диффамационного воздействия, в том числе и в среде Интернета, требует юридически грамотного отношения как со стороны владельцев сайтов, так и со стороны обычных рядовых пользователей. Необходимо быть ответственным за свои слова и поступки, соблюдать правовые нормы и рамки юридической и моральной дозволенности. Только при таком подходе, когда правовым нормам будут следовать все участники отношений в данной сфере, возможно осуществление права на защиту чести, достоинства, репутации с соблюдением свободы слова и мнений.

Примечания

[1] *Потапенко С. В.* Диффамация и российская судебная практика в контексте опыта Европейского Суда по правам человека // www.medialaw.ru/article10/7/15.htm.
[2] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. № 63-ФЗ // СЗ РФ. — 1996. — № 25. — Ст. 2954.
[3] Конституция РФ от 12 декабря 1993 г. М. : НОРМА М., 2006.
[4] Гражданский кодекс Российской Федерации (часть первая): Федеральный закон от 30 ноября 1994 г. № 51 // Российская газета. — 2008. — 24 марта.
[5] Постановление Пленума Верховного Суда РФ от 24 февраля 2005 г. № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» // Российская газета. — 2005. — 15 марта.
[6] Там же.
[7] Гражданский кодекс Российской Федерации (часть первая)…
[8] Закон РФ от 27 декабря 1991 г. № 2124-I «О средствах массовой информации» (с изменениями от 27 июля 2006 г.) // Российская газета. — 2007. — 28 ноября.

МАКАРОВА З. В., д. ю. н., профессор, засл. юрист РФ.

MAKAROVA Z. V., Doctor of Law, Professor, Honored Jurist of the Russian Federation.

СИЛЬЧЕНКО А. А., аспирант кафедры конституционного и административного права Южно-Уральского государственного университета.

SILCHENKO A. A., Postgraduate Student of the Chair "Constitutional and Administrative Law", South Ural State University.

УДК 346 + 004.056.53
ББК Х401.114 + Ч231.3

А. В. Минбалеев

Понятие и признаки инсайдерской информации как особого вида информации ограниченного доступа

В статье рассматриваются понятие и признаки нового для российского информационного права вида информации — инсайдерской информации. Автором выделяется ряд признаков инсайдерской информации, что дает основание говорить о самостоятельном правовом режиме, закрепляемом законодателем для защиты инсайдерской информации.

Ключевые слова: *инсайдер, инсайдерская информация, информация ограниченного доступа, конфиденциальность, ценные бумаги.*

A. V. Minbaleev

Definition and Features of Insider Information as a Peculiar Type of Restricted Information

The article contains the definition and features of insider information as a new type of information for Russian information law. The author describes a range of features of insider information giving evidence of autonomous legal regime formalized by lawmaker to protect the insider information.

Key words: *insider, insider information, restricted information, confidentiality, securities.*

Инсайдерская информация как особый вид информации ограниченного доступа длительный период времени в нашей стране был только предметом многочисленных обсуждений с позиции зарубежного опыта защиты и возможностей внедрения данного института в Российской Федерации. Необходимость защиты инсайдерской информации от несанкционированного разглашения или использования традиционно связывается с защитой инвесторов, которые лишаются преимущества на финансовом рынке «из-за лиц, которые используют публично не раскрытую информацию для себя или третьих лиц»[1]. С принятием и вступлением в силу Федерального закона «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее — Закон об инсайдерской информации)[2] мы можем говорить о появлении принципиально нового вида информации в сфере информационной безопасности.

Попытки принятия закона об инсайдерской информации в России ведутся с 2003 года, когда в Государственной Думе Российской Федерации рассматривался законопроект «Об инсайдерской информации». С того времени многое изменилось, в том числе и само понимание инсайдерской информации. Последнее значительно расширилось. Так, изначально под инсайдерской информацией понималась «любая информация об эмиссионных ценных бумагах и сделках с ними, а также об эмитенте этих ценных бумаг и осуществляемой им деятельности, не известная третьим лицам, раскрытие которой может оказать существенное влияние на рыночную цену этих ценных бумаг». В качестве альтернативы данному понятию в российском законодательстве длительное время использовался термин «служебная информация на рынке ценных бумаг». Однако данный термин не в полной мере отражал потребности экономики в защите информации о финансовых инструментах.

Закон об инсайдерской информации понимает под ней «точную и конкретную информацию, которая не была распространена или предоставлена (в том числе сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну), распространение или предоставление которой

может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров (в том числе сведения, касающиеся одного или нескольких эмитентов эмиссионных ценных бумаг, одной или нескольких управляющих компаний инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, одного или нескольких хозяйствующих субъектов, указанных в Законе об инсайдерской информации (п. 2 ст. 4), либо одного или нескольких финансовых инструментов, иностранной валюты и (или) товаров) и которая относится к информации, включенной в соответствующий перечень инсайдерской информации, указанный в Законе об инсайдерской информации (ст. 3). Из данного определения явно прослеживается расширение толкования российским законодателем понятия «инсайдерская информация» за счет включения в ее содержание информации, распространение или предоставление которой может оказать существенное влияние на цены иностранной валюты и (или) товаров.

Из законодательного определения, а также ряда норм Закона об инсайдерской информации можно выделить ряд признаков, которые характеризуют инсайдерскую информацию как особый вид информации ограниченного доступа:

1) к инсайдерской информации относятся сведения, охраняемые в режиме той или иной тайны (кроме государственной и налоговой тайн). Таким образом, инсайдерская информация относится к вторичной информации ограниченного доступа (наряду с кредитными историями, персональными данными), конфиденциальность которой строится на основе мер по ее обеспечению, устанавливаемых законом для соответствующего вида охраняемой законом тайны, а также собственных мер, определенных Законом об инсайдерской информации и другими нормативными правовыми актами (так, на Федеральную службу по финансовым рынкам возложена задача по принятию ряда актов, устанавливающих как перечень инсайдерской информации, так и определенные меры по ее защите);

2) распространение или предоставление этой информации может оказать существенное влияние на цены финансовых инструментов (ценные бумаги или производные финансовые инструменты), иностранной валюты и (или) товаров (вещи, за исключением ценных бумаг, которые допущены к торговле на организованных торгах на территории Российской Федерации или в отношении которых подана заявка о допуске к торговле на указанных торгах);

3) сведения, которые подпадают под вышеуказанные признаки, должны также относиться к информации, включенной в соответствующий перечень инсайдерской информации, указанный в Законе об инсайдерской информации (ст. 3). Таким образом, законодатель изначально определяет некоторый перечень, под который могут подпадать охраняемая инсайдерская информация (в некоторой степени можно видеть аналогию с перечнем сведений, составляющих государственную тайну. Согласно Закону Российской Федерации «О государственной тайне» отнесение сведений к государственной тайне и их засекречивание должно осуществляться в строгом соответствии в том числе и с перечнем сведений, составляющих государственную тайну, закрепленным в ст. 5).

К инсайдерской информации инсайдеров, указанных в пунктах 1—4, 11 и 12 ст. 4 Закона об инсайдерской информации, относится информация, исчерпывающий перечень которой утверждается нормативным правовым актом федерального органа исполнительной власти в области финансовых рынков. Лица, указанные в настоящей части, обязаны утвердить собственные перечни инсайдерской информации.

К инсайдерской информации органов и организаций, указанных в п. 9 ст. 4 Закона об инсайдерской информации, Банка России относится:

— информация о принятых ими решениях об итогах торгов (тендеров);

— информация, полученная ими в ходе проводимых проверок, а также информация о результатах таких проверок;

— информация о принятых ими решениях в отношении лиц, указанных в пунктах 1—4, 11 и 12 ст. 4 Закона об инсайдерской информации, о выдаче, приостановлении действия или об аннулировании (отзыве) лицензий (разрешений, аккредитаций) на осуществление определенных видов деятельности, а также иных разрешений;

— информация о принятых ими решениях о привлечении к административной ответственности лиц, указанных в пунктах 1—4, 11—13 ст. 4 Закона об инсайдерской информации, а также о применении к указанным лицам иных санкций;

— иная инсайдерская информация, определенная их нормативными актами.

Органы и организации, указанные в п. 9 ст. 4 Закона об инсайдерской информации, Банк России обязаны утвердить нормативные акты, содержащие исчерпывающие перечни инсайдерской информации, в соответствии с методическими рекомендациями

федерального органа исполнительной власти в области финансовых рынков.

Также необходимо учитывать, что к инсайдерской информации не относятся: сведения, ставшие доступными неограниченному кругу лиц, в том числе в результате их распространения; осуществленные на основе общедоступной информации исследования, прогнозы и оценки в отношении финансовых инструментов, иностранной валюты и (или) товаров, а также рекомендации и (или) предложения об осуществлении операций с финансовыми инструментами, иностранной валютой и (или) товарами;

4) данная информация должна быть точной (достоверной) и конкретной;

5) ранее она не была распространена или предоставлена третьим лицам (неизвестность третьим лицам, которые не имеют доступа к такой информации);

6) к субъектам — обладателям инсайдерской информации (инсайдерам) относятся:

— эмитенты и управляющие компании;

— хозяйствующие субъекты, включенные в предусмотренный ст. 23 Федерального закона от 26 июля 2006 года № 135-ФЗ «О защите конкуренции» реестр и занимающие доминирующее положение на рынке определенного товара в географических границах Российской Федерации;

— организаторы торговли, клиринговые организации, а также депозитарии и кредитные организации, осуществляющие расчеты по результатам сделок, совершенных через организаторов торговли;

— профессиональные участники рынка ценных бумаг и иные лица, осуществляющие в интересах клиентов операции с финансовыми инструментами, иностранной валютой и (или) товарами, получившие инсайдерскую информацию от клиентов;

— лица, имеющие доступ к инсайдерской информации вышеуказанных лиц на основании договоров, заключенных с соответствующими лицами, в том числе аудиторы (аудиторские организации), оценщики (юридические лица, с которыми оценщики заключили трудовые договоры), профессиональные участники рынка ценных бумаг, кредитные организации, страховые организации;

— лица, которые владеют не менее чем 25 процентами голосов в высшем органе управления лиц, вышеуказанных (за исключением предшествующего данному пункта), а также лица, которые в силу владения акциями (долями) в уставном капитале указанных лиц имеют доступ к инсайдерской информации на основании федеральных законов или учредительных документов;

— члены совета директоров (наблюдательного совета), члены коллегиального исполнительного органа, лицо, осуществляющее функции единоличного исполнительного органа (в том числе управляющая организация, управляющий либо временный единоличный исполнительный орган), члены ревизионной комиссии юридических лиц, указанных в Законе об инсайдерской информации, управляющих организаций;

— лица, имеющие доступ к информации о направлении добровольного, обязательного или конкурирующего предложения о приобретении акций в соответствии с законодательством Российской Федерации об акционерных обществах, в том числе лица, направившие в акционерное общество добровольные или конкурирующие предложения, кредитная организация, предоставившая банковскую гарантию, оценщик (юридические лица, с которыми оценщики заключили трудовые договоры);

— федеральные органы исполнительной власти, исполнительные органы государственной власти субъектов Российской Федерации, органы местного самоуправления, иные осуществляющие функции указанных органов органы или организации, органы управления государственных внебюджетных фондов, имеющих в соответствии с федеральными законами и иными нормативными правовыми актами Российской Федерации право размещать временно свободные средства в финансовые инструменты (далее — органы управления государственных внебюджетных фондов), Банк России;

— имеющие доступ к инсайдерской информации руководители федеральных органов исполнительной власти, имеющие доступ к инсайдерской информации руководители исполнительных органов государственной власти субъектов Российской Федерации, имеющие доступ к инсайдерской информации выборные должностные лица местного самоуправления, имеющие доступ к инсайдерской информации государственные служащие и муниципальные служащие органов, указанных в предыдущем пункте, имеющие доступ к инсайдерской информации работники органов и организаций, осуществляющих функции органов, указанных в предыдущем пункте, имеющие доступ к инсайдерской информации работники органов управления государственных внебюджетных фондов, имеющие доступ к инсайдерской информации служащие (работники) Банка России, члены Национального банковского совета;

— информационные агентства, осуществляющие раскрытие или предоставление информации лиц, указанных в пунктах 1—4 ст. 4 Закона об инсайдерской информации, органов и организаций, указанных в п. 9 ст. 4 Закона об инсайдерской информации, Банка России;

— лица, осуществляющие присвоение рейтингов лицам, указанным в пунктах 1—4 ст. 4 Закона об инсайдерской информации, а также ценным бумагам (рейтинговые агентства);

— физические лица, имеющие доступ к инсайдерской информации лиц, указанных в пунктах 1—8, 11 и 12 ст. 4 Закона об инсайдерской информации, на основании трудовых и (или) гражданско-правовых договоров, заключенных с соответствующими лицами;

7) правовой режим инсайдерской информации предполагает осуществление инсайдерами ряда мер по защите инсайдерской информации, в том числе:

— ведение списка инсайдеров;

— уведомления в порядке, установленном нормативным правовым актом федерального органа исполнительной власти в области финансовых рынков (Федеральная служба по финансовым рынкам), лиц, включенных в список инсайдеров, об их включении в такой список и исключении из него, информировать указанных лиц о требованиях Закона об инсайдерской информации;

— осуществление передачи в порядке, установленном нормативным правовым актом федерального органа исполнительной власти в области финансовых рынков (Федеральная служба по финансовым рынкам), список инсайдеров организаторам торговли, через которых совершаются операции с финансовыми инструментами, иностранной валютой и (или) товаром. Данное требование не распространяется на органы и организации, указанные в п. 9 ст. 4 Закона об инсайдерской информации, а также на Банк России;

— осуществление передачи списка инсайдеров в уполномоченный федеральный орган исполнительной власти в области финансовых рынков по его требованию;

— уведомление инсайдерами о совершенных ими операциях в соответствии со ст. 10 Закона об инсайдерской информации. Например, инсайдеры, включенные в список инсайдеров эмитента или управляющей компании, обязаны уведомлять указанные организации, а также федеральный орган исполнительной власти в области финансовых рынков об осуществленных ими операциях с ценными бумагами этого эмитента или управляющей компании и о заключении договоров, являющихся производными финансовыми инструментами, цена которых зависит от таких ценных бумаг;

— осуществление мер по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации и (или) манипулирования рынком, в том числе:

а) разработать и утвердить порядок доступа к инсайдерской информации, правила охраны ее конфиденциальности и контроля за соблюдением требований настоящего Федерального закона и принятых в соответствии с ним нормативных правовых актов;

б) создать (определить, назначить) структурное подразделение (должностное лицо), в обязанности которого входит осуществление контроля за соблюдением требований настоящего Федерального закона и принятых в соответствии с ним нормативных правовых актов и которое подотчетно совету директоров (наблюдательному совету), а в случае его отсутствия высшему органу управления юридического лица;

в) обеспечить условия для беспрепятственного и эффективного осуществления вышеуказанным структурным подразделением (должностным лицом) своих функций;

— осуществление контроля за операциями с финансовыми инструментами, иностранной валютой и (или) товарами, осуществляемыми на организованных торгах.

Указанные признаки в целом характеризуют инсайдерскую информацию как принципиально новый вид информации ограниченного доступа, для которой характерен собственный механизм обеспечения конфиденциальности, а, значит, самостоятельный правовой режим.

Примечания

[1] *Карпович О. Г.* Борьба с распространением инсайдерской информации на фондовом рынке в России // Юридический мир. — 2011. — № 4. — С. 16.

[2] Федеральный закон Российской Федерации «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» от 27.07.2010 г. № 224-ФЗ // СЗ РФ. — 2010. — № 31. — Ст. 4193.

МИНБАЛЕЕВ Алексей Владимирович, к. ю. н., доцент кафедры предпринимательского и коммерческого права, доцент кафедры конституционного и административного права ЮУрГУ.

MINBALEEV Aleksey Vladimirovich, Candidate of Legal Sciences, Associate Professor, Associate Professor of the Chair «Entrepreneurial and Commercial Law», Associate Professor of the Chair «Constitutional and Administrative Law», South Ural State University.

УДК 342.738:621.39 + 004.056 + 025:004
ББК Х401.132 + Ч231.5

П. А. Новоструев, А. В. Новоструев

Легитимность использования Data Leak Prevention (DLP) систем при перлюстрации электронной корреспонденции

В работе рассматриваются законодательные аспекты использования компьютерных систем предотвращения утечки информации и вопросы легитимности перлюстрации электронной корреспонденции.

Ключевые слова: *DLP-система, перлюстрация, тайна связи, инсайдер. Problems of Data Leak/Loss Prevention systems.*

P. A. Novostruev, A. V. Novostruev

legislative aspects of usage of soft hardware complexes that prevent the loss of information

This article is devoted to the problem of legitimacy of censorship of e-mail. The article discloses legislative aspects of usage of soft hardware complexes that prevent the loss of information.

Key words: *DLP-system perusal, secret of communications, an insider.*

Введение

Информация, необходимая для работы современного предприятия, как правило, включает в себя технологии, ноу-хау, базы клиентов и поставщиков, персональные данные и другую информацию, являющуюся конфиденциальной. Вся эта информация находится под постоянной угрозой со стороны конкурентов и недобросовестных сотрудников.

Некоторые действия, например, непреднамеренное разглашение коммерческой тайны, отправка корреспонденции ошибочному адресату, некорректное ведение переписки, даже будучи произведенные без злого умысла, могут серьезно навредить компании и ее имиджу.

Периметр информационной безопасности организации находится под постоянной угрозой по многим причинам. В частности:

1) угроза конфиденциальной информации (коммерческой тайне, персональным данным и т. д.) в результате действий инсайдеров, шпионских программ, вторжений в локальную сеть и беспечного отношения сотрудников;

2) действия сотрудников, использующих компьютеры компании для посторонних нужд, не связанных с выполнением трудовых обязанностей и рискующих тем самым разгласить конфиденциальные данные или подвергнуть компьютер заражению вредоносными и шпионскими программами.

Одним из способов защиты конфиденциальной информации может стать использование DLP-систем в сети компании.

Data Leak Prevention (DLP) переводится с английского языка как «предотвращение утечек информации».

DLP-система — это:

1) продукт, который на основе централизованных политик осуществляет идентификацию, мониторинг и защиту данных во время их использования, передачи и/или хранения;

2) комплекс мер по защите от утечек информации, являющейся собственностью организации.

В настоящее время самыми распространенными корпоративными системами передачи данных являются электронная почта, системы обмена мгновенными сообщениями, IP-телефония, веб-ресурсы, сетевые файловые хранилища и другое. Вся информация, обрабатываемая вышеописанными службами, передается по каналам локальной сети организации, проходит через корпоративные сервера и шлюзы.

Для осуществления наблюдения за электронной корреспонденцией достаточно

установить на одном из промежуточных узлов (или узлах) компонент DLP-системы, регистрирующий весь проходящий трафик. Использование этой системы поможет лучше разобраться в структуре и содержании сетевого трафика, входящих и исходящих потоков данных, а также дает руководству возможность получить больше информации о том, что читают, загружают, отсылают, смотрят и слушают сотрудники организации.

Анализ корреспонденции может помочь оценить эффективность принимаемых мер информационной безопасности, а также обнаружить «слабые места» в системе защиты конфиденциальной информации.

Если злоумышленнику удалось обойти систему защиты корпоративной информации и воздействовать на данные, то при использовании DLP-системы вероятность его нахождения и поимки по «горячим следам» значительно возрастает. А сама перехваченная и восстановленная сессия может использоваться в качестве доказательства в суде при условии, если возможность перлюстрации почтовой корреспонденции закреплена в трудовом договоре и имеется письменное согласие сотрудника.

Именно поэтому системы, осуществляющие перлюстрацию электронной корреспонденции, могут быть весьма полезны сотрудникам службы информационной безопасности организации или лицам, выполняющим эту функцию. Они, в свою очередь, могут представлять отчеты кадровой службе и руководству компании.

Данные, перехваченные и сохраненные DLP-системой, также могут быть использованы контролирующими и проверяющими органами, судебными представителями, органами правопорядка и др.

Законодательное регулирование систем перлюстрации электронной корреспонденции

Пункт. 2 ст. 23 действующей Конституции Российской Федерации гласит «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения».

Никаких исключений, кроме судебного решения, Конституция не подразумевает. Именно суд относится к числу тех гарантов, которые препятствуют необоснованным ограничениям указанного права человека и гражданина.

Законодательство разрешает ограничение на тайну переписки и говорит, что ограничение возможно только при выполнении двух основных условий:

1) ограничение должно быть прямо установлено федеральным законодательством;

2) ограничение должно быть подтверждено решением суда.

На сегодняшний день в России действует несколько законов, разрешающих ограничивать право на тайну переписки.

Статья. 8 Федерального закона «Об оперативно-розыскной деятельности» от 12.08.95 № 144-ФЗ: «Проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища допускается на основании судебного решения».

Статья. 13 УПК РФ: «Ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения».

Подпункт 8 п. 2 ст. 29 УПК РФ: «Только суд, в том числе в ходе досудебного производства, правомочен принимать решения: … о наложении ареста на корреспонденцию, разрешении на ее осмотр и выемку в учреждениях связи».

В то же время действующее гражданско-процессуальное законодательство не регулирует порядок ограничения конституционного права на тайну переговоров при производстве по гражданскому делу. Однако, в соответствии с требованиями Конституции РФ и ГК, право на тайну переписки может быть обойдено только с разрешения суда.

Если отправитель и получатель, а также их уполномоченные представители не дали своего законного согласия на проведение мониторинга своей электронной корреспонденции, то перлюстрация является уголовно наказуемым деянием.

Резюмируя вышесказанное можно заключить, что руководство, служба ИБ, системные администраторы и другие служащие предприятия не имеют законного права самостоятельно вмешиваться в переписку своих сотрудников. В соответствии со ст. 138 УК РФ эти деяния классифицируются как отягчающие, так как выполняются с использованием служебного положения.

Выход из создавшегося положения дает использование работодателем электронных средств перлюстрации, в частности DLP-систем, так как само по себе средство мониторинга и контроля электронной кор-

респонденции не может стать субъектом уголовного или административного разбирательства. Виновным может быть признан только человек, который лично занимается перлюстрацией потоков данных.

Легитимность перлюстрации и право работодателя на охрану информации компании

Разработчики DLP-систем утверждают, что схема, при которой сотрудники службы информационной безопасности выполняют поиск конкретной информации в базе данных и знакомятся с искомым результатом, вполне легитимна и не нарушает закона, так как реального сообщения никто не читает.

Законодательство РФ дает работодателям возможность применения систем, обеспечивающих перлюстрацию электронной корреспонденции работников (пользователей) в процессе их трудовой деятельности, о чем говорят следующие статьи трудового кодекса РФ.

Статья. 15 ТК РФ: «Трудовые отношения — отношения, основанные на соглашении между работником и работодателем о личном выполнении работником за плату трудовой функции ..., подчинении работника правилам внутреннего трудового распорядка при обеспечении работодателем условий труда, предусмотренных трудовым законодательством и иными нормативными правовыми актами, содержащими нормы трудового права, коллективным договором, соглашениями, локальными нормативными актами, трудовым договором».

Статья. 189 ТК РФ: «Правила внутреннего трудового распорядка — локальный нормативный акт, регламентирующий ... порядок приема и увольнения работников, основные права, обязанности и ответственность сторон трудового договора, режим работы, время отдыха, применяемые к работникам меры поощрения и взыскания, а также иные вопросы регулирования трудовых отношений у данного работодателя».

В соответствии со ст. 21 ТК РФ работник обязан исполнять свои трудовые обязанности, возложенные на него трудовым договором, соблюдать правила внутреннего трудового распорядка организации и трудовую дисциплину.

Вышеприведенные обязанности перекликаются с правами работодателя, содержащимися в ст. 22 ТК РФ. — правом требовать от работников исполнения ими трудовых обязанностей и бережного отношения к имуществу работодателя и других работников, соблюдения правил внутреннего трудового распорядка организации.

Необходимость наблюдения за электронной корреспонденцией ставит перед собой задачи обеспечить исполнение работником возложенных на него трудовых обязанностей и сохранить конфиденциальные данные компании. При этом все действия работника должны быть направлены исключительно на выполнение его трудовых обязанностей .

Использование электронных средств коммуникации для целей, не связанных с исполнением трудовых обязанностей, является противоречащим существу трудовых правоотношений и противоречит такой обязанности работника, как добросовестное исполнение возложенных на него трудовых обязанностей. Кроме того, оно ставит под угрозу сохранность конфиденциальных данных, принадлежащих предприятию. Работник, работающей с закрытой информацией, принадлежащей компании и составляющей ее коммерческую тайну, может отправить ее по электронным каналам связи. Подпункты 1—3 ст. 183 УК РФ определяют ответственность за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

В свою очередь, п. 1 ст. 272 УК РФ содержится определение «неправомерный доступ к охраняемой законом компьютерной информации»: «Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию, либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети». Следовательно, факт использования работодателем систем, осуществляющих перлюстрацию электронной корреспонденции, может рассматриваться как направленный на сохранение конфиденциальности информации, улучшение трудовых показателей и соблюдение работниками трудовой дисциплины в организации.

Еще одним выходом для компаний является отчуждение прав пользователей от всей корреспонденции, отправленной ими с рабочих компьютеров, и передачу работодателю права на нее. Этот факт также должен быть отражен в трудовом договоре.

Этические аспекты перлюстрации

С моральной точки зрения слежка за электронной корреспонденцией пользователей может показаться неэтичной.

Тем не менее, в случае работы сотрудников с конфиденциальной информацией службе безопасности вменено в обязанность проведение мероприятий в целях предотвращения утечек информации. К таким мероприятиям, в частности, относится внедрение систем, осуществляющих мониторинг и перлюстрацию электронной корреспонденции. Эти системы решают следующие задачи: определение состава защищаемой информации, определение источников и потребителей защищаемой информации, разработка инструкций, регламентирующих процедуры обращения с защищаемой информацией, обнаружение факта уже свершившейся утечки и т. п.

Сотрудники, работающие с конфиденциальной информацией, будучи осведомленными о просмотре электронной корреспонденции, практически гарантированно воздержатся от совершения противоправных действий, нарушения политики безопасности компании и станут эффективнее расходовать рабочее время. Но если нарушение все же произойдет, оно будет раскрыто по горячим следам благодаря информации, сохраненной системой мониторинга.

Использование систем, предназначенных для перлюстрации электронной корреспонденции, должно служить в целях обеспечения сохранения конфиденциальных данных, с которыми работают сотрудники, а не для получения информации, касающейся их частной жизни.

Для того чтобы у руководителей компании не возникло проблем с законом в вопросах организации ИБ, рекомендуется:

1. Создать перечень сведений, которые составляют конфиденциальную информацию (коммерческую тайну предприятия, персональные данные и т. д.), которая не подлежит разглашению, и ознакомить с данным документом всех сотрудников организации под роспись.

2. Включить в трудовой договор пункт, запрещающий использование предоставляемых сотруднику рабочих ресурсов организации в личных целях.

3. Заключить с каждым сотрудником организации «Обязательство о неразглашении конфиденциальной информации», в котором закрепить возможность перлюстрации корреспонденции работодателем.

4. Ознакомить сотрудников предприятия с процедурами обжалования действий, контролирующих подразделений компании.

Примечания

[1] Конституция Российской Федерации. Текст и справочные материалы. — М. : Эксмо, 2009.
[2] Уголовно-процессуальный кодекс. — М. : Эксмо, 2010.
[3] Уголовный кодекс. — М. : Эксмо, 2010.
[4] Трудовой кодекс РФ с комментариями. — М. : Проспект, 2010.
[5] Информационная безопасность систем организационного управления. Теоретические основы : в 2 т. — Т. 2. — М. : Наука, 2006.
[6] *Родичев Ю.* Информационная безопасность: нормативно-правовые аспекты. СПб. : Питер, 2007.

НОВОСТРУЕВ Андрей Викторович, ст. преподаватель ГОУ ВПО «Курганский государственный университет». E-mail: bigus2@yandex.ru

NOVOSTRUEV Andrey Viktorovich, Head Lecturer of State Educational Institution of Higher Professional Education (GOU VPO) "Kurgan State University".
E-mail: bigus2@yandex.ru

НОВОСТРУЕВ Павел Андреевич, студент ГОУ ВПО «Курганский государственный университет». E-mail: admin@nv-trade.ru

NOVOSTRUEV Pavel Andreevich, Student of GOU VPO "Kurgan State University". E-mail: admin@nv-trade.ru

ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ

УДК 004.056 + 06.08:004.056
ББК Ч23

Л. В. Астахова

Проблема оценки HR-уязвимости объекта защиты информации

В статье обосновывается проблема недостаточной изученности угроз и уязвимостей объекта защиты информации, связанных с человеческими ресурсами, и методологии их оценки в процессе создания системы защиты информации. Анализируются стандарты и методические документы по информационной безопасности, выявляется гуманитарно-антропоцентрический характер нового поколения банковских стандартов по информационной безопасности, аргументируется необходимость применения компетентностного подхода к моделированию и оценке компетенций персонала на объектах защиты на всех этапах его работы.

Ключевые слова: *человеческие ресурсы, информационные угрозы, уязвимости информации, оценка, кадровая безопасность.*

L. V. Astakhova

Problems of Review HR-Vulnerability of Information Protection Object

The article justifies the problem of insufficient understanding of threats and vulnerabilities of information protection object connected with human resources and the method for their review when creating an information protection system. The author analyzes standards and guideline documents related to the information security, describes the humanitarian anthropocentric nature of new-generation bank standards for information security and justifies the need for using a competence approach to simulate and assess the competences of personnel of protection object through all the stages of its work.

Key words: *human resources, information threats, information vulnerability, review, personnel security.*

Стратегический курс на интенсивное информационное и инновационное развитие России с каждым днем все больше обостряет проблему информационной безопасности в организациях всех отраслей и форм собственности. Сфера высоких технологий дает мощное невидимое оружие в руки не только тех, кто защищает информацию, но и тех, кто стоит «по другую сторону баррикад». В Управлении «К» МВД России отмечают, что в преступном киберсообществе усиливается специализация и разделение ролевых функций, улучшается координация и расширяется география деятельности злоумышленников. При этом сами преступления становятся все масштабнее и изощреннее, а их количество растет из года в год. В целом за первые 9 месяцев 2010 года сотрудниками подразделений «К» МВД России было возбуждено **более 5 тыс.** уголовных дел, выявлено почти 7,5 тыс. преступлений.

Среди противоправных действий в сфере ИТ по величине ущерба лидирует неправомерный доступ к компьютерной информации, а также создание, использование и распространение вредоносных программ. На их долю приходится **более 60 % всех инцидентов**, поскольку именно завладение кодами и паролями, блокирование компьютерных систем служат своего рода ключом к совершению других преступлений, в том числе электронному мошенничеству [5].

Первое место среди виновников утечек информации уверенно занимают инсайдеры. В 2010 году их доля составила 39,3 %. При этом сократилась доля хакеров (23 %, что на 15,1 % меньше, чем в 2009 году), что связано с тем, что многие компании после

ряда громких инцидентов усилили защиту своих сетей против внешних угроз, однако не смогли предотвратить внутренние утечки, обезопасить себя от которых в разы сложнее [6]. Таким образом, устойчивой тенденцией является тот факт, что более двух третей ущербов, имеющих злонамеренный характер, исходит от персонала предприятия, или — от HR (Human Resources — человеческих ресурсов) . Логично предположить, что уже сам факт наличия этой тенденции свидетельствует о том, что угрозы, исходящие от человека, должны быть дифференцированы в отдельный вид угроз безопасности информации — HR-угрозы, а уязвимости — в HR-уязвимости объектов защиты информации.

Взяв за основу определения угроз и уязвимостей информационной безопасности, приведенные в Стандарте ЦБ РФ СТО БР ИББС-1.0-2010 «Обеспечение ИБ организаций банковской системы РФ. Общие положения», сформулируем определения HR-угроз и HR-уязвимостей информационной безопасности:

HR-угроза информационной безопасности — это угроза нарушения свойств ИБ — доступности, целостности или конфиденциальности информационных активов организации, исходящая от ее персонала.

HR-уязвимость информационной безопасности — слабое место в кадровом обеспечении информационной инфраструктуры организации, включая СОИБ, которое может быть использовано для реализации или способствовать реализации HR-угрозы ИБ.

Нельзя сказать, что угрозам и уязвимостям, связанным с персоналом, совсем не уделяется внимания, однако упоминание о них носит большей частью декларативный характер.

Так, в ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности» на руководство возложена ответственность по обеспечению подготовки, осведомленности и квалификации персонала: определение требуемого уровня сотрудников и навыков для персонала, который выполняет работу, влияющую на СМИБ; организация обучения персонала; оценка результативности предпринятых действий; ведение записей об образовании, подготовке, навыках, опыте и квалификации. В Приложении А «Цели и меры управления» в разделе А8 описаны правила безопасности, связанные с персоналом в различные периоды: перед трудоустройством (документирование функций и обязанностей, проверка, определение и документирование условий трудового договора); в период работы по трудовому договору (ознакомление с правилами и процедурами обеспечения ИБ, обучение и переподготовка по ИБ, применение дисциплинарной практики); в период увольнения и/или изменения трудового договора (установление ответственности по окончании действия трудового договора, возврат активов, аннулирование прав доступа).

ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» также содержит вопросы безопасности, связанные с персоналом: учет вопросов безопасности в должностных обязанностях и при найме персонала; включение вопросов ИБ в должностные обязанности; проверка персонала при найме и соответствующая политика; соглашения о конфиденциальности; условия трудового соглашения; обучение пользователей; обучение и подготовка в области ИБ.

В ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности» в кратком обзоре классов и семейств доверия к безопасности в процессе характеристики семейства «Безопасность разработки» указывается, что оно содержит требования не только к физической безопасности местоположения разработки, но и к контролю за отбором и наймом персонала разработчиков. В стандарте есть также характеристика компонентов доверия к руководствам администратора и пользователей, однако описание компонентов доверия к самим администратору и пользователям отсутствует.

В ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» в число активов — ценностей, которые должны иметь гарантированную защиту, включены не только материальные и нематериальные ресурсы, информационные активы и программное обеспечение, но и люди (п. 3.2.). Связанные с активами уязвимости включают в себя: слабости физических носителей, организации, процедур, управления, администрирования, информации, программно-аппаратного обеспечения и персонала (п.3.4.).

В ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4.

Выбор защитных мер» в число защитных мер в категории «Персонал» вошли: проверка и соглашение о соблюдении правил конфиденциальности для штатного персонала, обязательство о соблюдении правил конфиденциальности — для нанятых по контракту; инструктаж по вопросам обеспечения безопасности, обеспечение материалами и специальное обучение — в разделе «Обучение и осведомленность о мерах безопасности»; и обеспечение исполнительской дисциплины (п. 8.1.4.).

В документах Федеральной службы по техническому и экспортному контролю России по защите персональных данных («Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных») вопросы HR-уязвимостей совсем не нашли отражения. Исходная защищенность ИСПДн, согласно Методике, определяется по нескольким признакам: по территориальному размещению, по наличию соединения с сетями общего пользования, по встроенным (легальным) операциям с записями баз персональных данных, по разграничению доступа к персональным данным, по наличию соединений с другими базами ПДн иных ИСПДн, по уровню обобщения (обезличивания) ПДн, по объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки. Признаки, так или иначе связанные с обслуживаемым эту информационную систему персоналом, в данном перечне отсутствуют.

В числе уязвимостей ИСПДн в «Базовой модели» названы: уязвимости ПО; уязвимости ИСПДн, вызванные наличием программно-аппаратной закладки; уязвимости, связанные с реализацией протоколов сетевого взаимодействия каналов передачи данных; уязвимости, вызванные недостатками организации ТЗИ от НСД; уязвимости СЗИ; уязвимости программно-аппаратных средств ИСПДн в результате сбоев в работе, отказов этих средств; наличие технических каналов утечки информации. Люди рассматриваются в документе в качестве источника угроз безопасности, однако HR-уязвимости ИСПДн не упоминаются.

Что касается защитных мер, то, как правило, подробно описываются технические меры защиты ИСПДн. Работа с персоналом организации в процессе создания системы защиты персональных данных также не затрагивается.

Полагаем, что проблема нормативной недооценки HR-угроз и уязвимостей связана, во-первых, с существованием весьма «живучего» стереотипа о приоритетности технических мер защиты информации, доставшегося нам от эпохи технократизма индустриального общества, как правило, страдающего, по словам О. Тоффлера, «технической болезнью» [3; 9]; во-вторых, с известной сложностью формализации процессов в гуманитарной сфере, каковой является работа с персоналом организации; в-третьих, неразработанностью методологических проблем организационной защиты информации в новых условиях — формирования и развития информационного общества, структурной гуманитарной революции, захвативших все сферы жизнедеятельности человека в XXI веке; и, наконец, в-четвертых, — с закрытостью тематики кадровых проверок в сфере защиты гостайны, накопившей уникальный опыт в этой области.

При этом классификация угроз информационной безопасности постоянно выступает объектом изучения в современной теории и практике. Так, одну из наиболее полных, многоаспектных классификаций угроз разработал А. И. Алексенцев, положив в основу источники угроз. При этом главным источником были названы люди [2]. Попытки специалистов компании Digital Security использовать разные классификации для описания по возможности большего количества угроз показали, что во многих случаях реальные угрозы либо не подходили ни под один из классификационных признаков, либо, наоборот, удовлетворяли нескольким (4). Поэтому ими была предложена классификации угроз, которая описывает все существующие угрозы информационной безопасности, по которой каждая из угроз подпадает только под один классификационный признак, и которая, таким образом, наиболее применима для анализа рисков реальных информационных систем. По характеру угрозы информационной безопасности были разделены на технологические и организационные. Технологические угрозы информационной безопасности по виду воздействия они разделили на физические и программные (логические), а организационные угрозы — на воздействие на персонал и действия персонала.

Воздействие на персонал может быть физическим и психологическим. Как физическое, так и психологическое воздействия на персонал направлены на сотрудников компании с целью получения информации или нарушения непрерывности ведения бизнеса.

Причинами действий персонала, способных вызвать угрозы информационной безопасности, могут быть умышленные или неумышленные действия. И те и другие угрозы могут быть направлены на информацию или на непрерывность ведения бизнеса.

Очевидно, что в основе этой классификации угроз информационной безопасности лежат несколько оснований: характер угрозы, виды воздействия, причины и объекты угрозы.

Большой вклад в развитие теории HR-угроз и уязвимостей и методологии их оценки внес ЦБ РФ, разработав систему отраслевых стандартов по информационной безопасности. В Стандарте ЦБ РФ СТО БР ИББС-1.0-2010 «Обеспечение ИБ организаций банковской системы РФ. Общие положения» выделены источники угроз природного, техногенного и антропогенного характера. Указано при этом, что источники угроз антропогенного характера могут быть как злоумышленные, так и незлоумышленные.

Примечательно, что в основу исходной концептуальной схемы ИБ организаций БС РФ положено противоборство собственника и злоумышленника с целью получения контроля над информационными активами. Однако другие, незлоумышленные, действия или источники угроз также лежат в сфере рассмотрения настоящего стандарта, поскольку под злоумышленником в стандарте понимается лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий (п. 5.2).

Приоритетность антропогенных источников угроз стандарт подчеркивает в п. 5.4, который гласит, что «наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является прямое нецелевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами либо нерегламентированная деятельность для получения контроля над активами. При этом он будет стремиться к сокрытию следов своей деятельности».

Новый стандарт отличается наличием наиболее полных на сегодняшний день требований к СИБ для области назначения и распределения ролей и обеспечения доверия к персоналу. К числу таких требований относятся принципы: «знать своего клиента» (Know your Customer) — принцип, используемый регулирующими органами для выражения отношения к финансовым организациям с точки зрения знания деятельности их клиентов; «знать своего служащего» (Know your Employee) — принцип, демонстрирующий озабоченность организации по поводу отношения служащих к своим обязанностям и возможных проблем, таких, как злоупотребление имуществом, аферы или финансовые трудности, которые могут приводить к проблемам с безопасностью, и др.

Также в п. 7.2. в числе общих требований по обеспечению информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу названы: выделение и документальное определение роли работников; персонификация и установление ответственности; в рамках одной роли не совмещать следующие функции: разработки и сопровождения системы/ПО, их разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора ИБ, выполнения операций в системе и контроля их выполнения; документальное определение процедуры приема на работу, влияющую на обеспечение ИБ (проверка подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов; проверка в части профессиональных навыков и оценка профессиональной пригодности); регулярная проверка (с документальной фиксацией результатов) в части профессиональных навыков и оценки профессиональной пригодности работников, а также внеплановой проверки (с документальной фиксацией результатов) — при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии; письменное обязательство работников о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов.

Столь пристальный интерес разработчиков стандарта к персоналу как антропогенной угрозе информационной безопасности не мог не сказаться и на новой методике оценки последней. Вполне закономерно, что в стандарте ЦБ РФ СТО БР ИББС-1.2-2010 «Обеспечение ИБ организаций банковской системы РФ. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0» в качестве одного из показателей информационной безопасности назван групповой показатель М1 «Обеспечение информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу». Дается характеристика частных показателей, соот-

ветствующих вышеназванным требованиям, обозначены обязательность их выполнения и коэффициенты значимости каждого из показателей. Так, показатель М.1.1 — определение в документах организации роли ее работников — имеет коэффициент значимости 0,0581; М.1.3 — персонификация ролей в организации с установлением ответственности за их выполнение — 0,0502; М.1.4 —документальная фиксация в должностных инструкциях ответственности за выполнение ролей — 0,0461; М.1.5 — отсутствие в организации ролей, совмещающих функции разработки и сопровождения системы/ПО — 0,0522; М.1.6 — отсутствие в организации ролей, совмещающих функции разработки и эксплуатации системы/ПО — 0,0610; М1.7 — отсутствие в организации ролей, совмещающих функции сопровождения и эксплуатации — 0,0522; М1.8 — отсутствие в организации ролей, совмещающих функции администратора системы и администратора информационной безопасности — 0,0661; М1.9 — отсутствие в организации ролей, совмещающих функции по выполнению операций в системе и контроля их выполнения — 0,0661; М1.10 — выполнение процедур контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющих получить контроль над защищаемым информационным активом организации — 0,1001; М1.11 — определение в документах организации процедуры приема на работу, влияющей на обеспечение ИБ (проверка подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов; проверка в части профессиональных навыков и оценка профессиональной пригодности) — 0,0513; М1.12 — указание в частном показателе М1.11 процедуры документальной фиксации результатов проводимых проверок — 0,0371.

Заметим, что частные показатели М.1.5 — М.1.9 являются не обязательными, а рекомендуемыми, и потому, вероятно, имеют высокие коэффициенты значимости — от 0,0522 до 0,0661. Между тем совершенно очевидно, что некоторые обязательные частные показатели (например, М.1.11) должны иметь гораздо большие коэффициенты значимости, поскольку качественно реализованные защитные меры, содержащиеся в них, могут обеспечить эффективную безопасность информационных ресурсов без дополнительных (рекомендуемых стандартом) защитных мер.

В число показателей ИБ, кроме показателя, связанного с доверием персоналу, в стандарт включен и групповой показатель М18 «Разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ», содержащий более традиционные защитные меры, способные предупредить HR-уязвимости активов организации. К ним относятся:

- организованная и документально оформленная работа с персоналом организации в направлении повышения осведомленности и обучения в области ИБ, включая разработку и реализацию планов и программ обучения и повышения осведомленности в области ИБ и контроля результатов выполнения указанных планов; утверждение руководством указанной работы (0,1898);
- установление в планах обучения и повышения осведомленности требования к периодичности обучения и повышения осведомленности (0,1378);
- включение в программы обучения и повышения осведомленности информации: по существующим политикам ИБ; по применяемым в организации защитным мерам; по правильному использованию защитных мер в соответствии с внутренними документами организации; о значимости и важности деятельности работников для обеспечения ИБ организации (0,1536);
- определение в организации перечня документов, являющихся свидетельством выполнения программ обучения и повышения осведомленности в области ИБ, в частности: документы (журналы), подтверждающие прохождение руководителями и работниками организации обучения в области ИБ с указанием уровня образования, навыков, опыта и квалификации обучаемых; документы, содержащие результаты проверок обучения работников организации; документы, содержащие результаты проверок осведомленности в области ИБ в организации (0,1184);
- организация для работника, получившего новую роль, обучения или инструктажа в области ИБ, соответствующего полученной роли (0,1396);
- определение в документах организации роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов (0,1290);
- назначение ответственных за выполнение ролей по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов (0,1338).

Соотношение коэффициентов значимости перечисленных показателей также

весьма спорно, однако сам факт их наличия в стандарте говорит о том, что направление деятельности по оценке HR-угроз и уязвимостей объектов информатизации начинает развиваться более интенсивно, поскольку вышло на новый, нормативный уровень. А это значит, что внимание к методологии и методике обеспечения кадровой безопасности организаций уже в ближайшем будущем будет более пристальным.

«Человеческое лицо» имеет и РС БР ИББС-2.4-2010 «Обеспечение ИБ организаций банковской системы РФ. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах ПД организаций банков банковской системы РФ». В п. 6.2. перечислены основные источники угроз безопасности ПДн: неблагоприятные события природного и техногенного характера; террористы, криминальные элементы; компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе использование компьютерных вирусов и других типов вредоносных кодов и атак; поставщики программно-технических средств, расходных материалов, услуг и т. п.; подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования и его ремонт; сотрудники организации БС РФ, являющиеся легальными участниками процессов в ИСПДн и действующие вне рамок предоставленных полномочий; сотрудники организации БС РФ, являющиеся легальными участниками процессов в ИСПДн и действующие в рамках предоставленных полномочий. Каждому из названных источников угроз, подавляющая часть которых имеет антропогенный характер, соответствуют уровни информационной инфраструктуры, на которых возможна реализация названных угроз: физический уровень; сетевой уровень; уровень сетевых приложений и сервисов; уровень операционных систем; уровень систем управления базами данных; уровень банковских технологических процессов и приложений.

К сожалению, другие стандарты ЦБ нового поколения (РС БР ИББС-2.3-2010 «Обеспечение ИБ организаций банковской системы РФ. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы РФ»), а также Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях БС РФ, разработанные совместно Банком России, АРБ и Ассоциацией региональных банков России (Ассоциацией «Россия») дополнительной информации о требованиях к персоналу и соответствующей им методологии и методики защиты от HR-угроз и уязвимостей не дают.

Последовавшая за структурными гуманитарными изменениями в обществе революция в российском образовании, связанная с переходом на уровневую систему, позволяет утверждать, что одним из главных методологических подходов в процессе разработки системы работы с персоналом организации для защиты информации от HR-угроз и уязвимостей должен стать компетентностный подход. Для построения эффективной защиты от HR-угроз необходимо разработать:

A. Базовую модель компетенций персонала на объектах защиты информации, которая должна быть применима к любой деятельности в организации;

B. Частную модель компетенций персонала на разных должностях на конкретном объекте защиты информации;

C. Базовую модель HR-угроз безопасности объекта защиты информации;

D. Частную модель HR-угроз безопасности объекта защиты информации;

E. Методику оценки HR-угроз безопасности объекта защиты информации;

F. Правила принятия кадровых решений по итогам оценки HR-угроз безопасности объекта защиты.

Еще сравнительно недавно понятия компетенции в отечественной кадровой практике и уж тем более — в кадровых аспектах деятельности по защите информации — не существовало. Применялся термин «профессионально важные качества», которым обозначались особенности человека (психофизиологические, психологические и даже физические), способствующие профессиональной успешности. Наряду с ними нередко указывали особенности человека, нежелательные для профессии, или противопоказания к ней. Например, в специалисты по защите информации не возьмут судимого. Сегодня для профессионально важных качеств используют понятие «компетенции», а для нежелательных свойств — «антикомпетенции». Правда, последний термин употребляется редко — чаще составляются перечни противопоказаний, связанных с физическим состоянием работника, его моральными качествами (социальным статусом) или образованием.

Чтобы модель компетенций была разработана корректно, следует понимать, что представляет собой компетенция — набор полезных для работы качеств, способности, знания, умения или совокупность

всех этих понятий. В американской практике используется термин «KSAO»: знания (Knowledge); умения (Skills); способности (Abilities, Attitudes); иные характеристики (Other – физические кондиции, поведение) [1]. Сегодня в отечественной практике под компетенциями принято понимать не только личностные качества, но и опыт человека (знания и умения), а также иные полезные качества (например, рост и даже внешность). Компетенция — это способность применять знания, умения и личностные качества для успешной деятельности в определенной области; компетентность — это совокупность компетенций.

Компетенции следует отличать от требований должности. Как известно, должность не обладает компетенциями — это атрибут человека. Однако она предъявляет требования к работнику и его качествам — компетенциям. Соответственно, компетенции — это качества работника, которые соответствуют требованиям должности. Поэтому термины «требования должности» и «требуемые компетенции» можно употреблять как синонимы.

Методология построения системы требуемых компетенций в организации предполагает два основных подхода. Первый подход — целостный — подразумевает способность человека действовать в соответствии со стандартами. Если можно удостовериться в том, что кандидат способен выполнять данную работу, он считается пригодным к ней. При этом не принимаются в расчет отдельные качества человека (например, уровень его образования, опыт, психофизические качества и др.). Второй подход — компетентностный — предполагает поиск характеристик человека, позволяющих ему добиваться результатов в работе.

Применение целостного подхода нуждается в специализированном инструментарии оценки, ведь здесь не используется профиль требуемых компетенций и не ставится вопрос, за счет каких качеств работник достигает успеха. В оценке акцент смещается на средства диагностики, на их пригодность определять способность человека быть успешным в определенных условиях.

Чтобы подобрать средства оценки персонала на основе компетентностного подхода, нужно понять, каков предмет оценки, т. е. какие компетенции предстоит оценивать. Для разработки профиля требуемых компетенций (профиля должности) применяют средства анализа работ (job analysis), а именно метод описания должности (job description) и метод описания требований должности (job specification). В мировой практике существует целый ряд универсальных методик описания работ, позволяющих составлять профили требуемых компетенций, — от опросников CMQ, PAQ, FJA до различных оценочных шкал. В организациях могут использоваться как готовые модели компетенций, опубликованные в специальной литературе [8], так и разработанные собственными силами (или сторонними специалистами) с учетом специфики организации. В. Чемеков приводит примеры нескольких таких моделей, наиболее известных и часто применяемых [13].

Одной из первых стала использоваться модель Д. Мак-Клелланда [11], которая содержит три устойчивые и прогностически значимые для диагностики эффективности параметры: мотивацию достижения, мотивацию аффилиации [11] и мотивацию доминирования. В последние годы стала популярной модель компетенций «Большая пятерка» (Big Five), вытеснившая более раннюю модель «Большая девятка» [15]. Она включает в себя: экстраверсию / социальную активность; дружелюбие / согласие; самоконтроль / добросовестность; эмоциональную устойчивость; интеллект / открытость опыту.

Существует практика использования иных фиксированных наборов компетенций в оценке персонала и разработке тестов. Так, SHL применяет модель из восьми компетенций [7]: потребности во власти и контроле; потребности в согласии; мотивации достижений; экстраверсии; общего интеллекта; открытости новому; обязательности; эмоциональной стабильности.

Мы согласны с мнением В. Чемекова о том, что модель компетенций, удовлетворяющая требованиям системности, должна иметь как минимум три уровня и охватывать все работы, производимые в организации. Первый уровень — базовые или корпоративные требования — обобщенные понятия, свойственные всем сотрудникам компании, поэтому присутствующие в профилях требуемых компетенций для любой должности в неизменном виде. Второй уровень — профильные требования, у руководителей и подчиненных или работников с разными функциями они будут различными. Однако они не зависят от опыта сотрудников, не описывают требования к знаниям и умениям работника на конкретной должности, для этого существуют специальные требования. Специальные требования самые «подвижные»: они отражают требуемый опыт работы, необходимый уровень образования, знание конкретных документов, в том числе

и корпоративных. Их аналогом может служить спецификация (или специализация) к должностной инструкции: для позиций с одинаковыми наименованиями может применяться одна и та же должностная инструкция, но если они отличаются по содержанию работ, то это отражается в спецификации.

Если организация разрабатывает собственный профиль компетенций, то общая схема построения модели компетенций такова:

1) определение нужд организации, ее целей, корпоративной культуры, ценностей;

2) определение основных требуемых компетенций;

3) описание индикаторов;

4) составление инструмента профилирования — единого списка требований с индикаторами;

5) апробация полученного инструмента [13].

Таким образом, в современной теории и практике защиты информации сложилась парадоксальная ситуация: с одной стороны, более 60 % нарушений информационной безопасности исходит от персонала организации, с другой стороны, существует проблема недооценки HR-угроз и уязвимостей информационной системы: они отсутствуют в классификациях угроз и уязвимостей, недостаточно обоснованы в нормативных документах (стандартах, методических документах). Организационные защитные меры, связанные с персоналом, как правило, не затрагивают сущности угрозы — требований к компетенциям персонала, в состав которых входят требования не только к знаниям, но и к его личностным качествам, которые позволяют успешно осуществлять профессиональную деятельность без ущерба информационной безопасности организации. В связи с этим специальным объектом исследований должны стать HR-угрозы и уязвимости на основе компетентностного подхода. Активное использование достижений теории отечественной и зарубежной педагогики позволит создать адекватную методологию моделирования HR-угроз и уязвимостей с последующим внесением изменений в действующие стандарты и методические рекомендации по обеспечению информационной безопасности организаций.

Примечания

[1] *Harvey R. J.* Job analysis // M. D. Dunnette & L. Hough (eds.). Handbook of Industrial and Organizational Psychology. Palo Alto: Consulting Psychologists Press, 1991.

[2] *Алексенцев А. И.* Понятие и структура угроз защищаемой информации // Безопасность информационных технологий. — 2000. — № 3.

[3] *Астахова Л. В.* Информационная безопасность: герменевтический подход : монография. — М. : РАН, 2010. — 185 с.

[4] Классификация угроз Digital Security (Digital Security Classification of Threats) (Электронный ресурс) // http://www.dsec.ru/products/grif/fulldesc/classification/

[5] Министерство внутренних дел Российской Федерации: Официальный сайт. (Электронный ресурс) // http://www.mvd.ru/userfiles/yanvar_dekabr_2010.pdf

[6] Отчет SECURIT Analytics об утечках информации за 2010 год (Электронный ресурс)//http://www.securit.ru/docs/securit_research_2010.pdf

[7] *Скирманов В.* Восемь компетенций SHL // Кадровый менеджмент. — 2006. — № 1.

[8] *Спенсер Л. М., Спенсер С. М.* Компетенции на работе / пер. с англ. — М. : ГИППО, 2005.

[9] *Тоффлер О.* Третья волна. — М. : АСТ, 2002. — 698 с.

[10] *Уиддет С., Холлифорд С.* Руководство по компетенциям / пер. с англ. — М. : ГИППО, 2008.

[11] *Хекхаузен Х.* Мотивация и деятельность. — Т. 2. — М. : Педагогика, 1986.

[12] *Хьюзлид М. А., Беккер Б. Е., Битти Р. У.* Оценка персонала: как управлять человеческим капиталом, чтобы реализовать стратегию / пер. с англ. — М. : ИД «Вильямс», 2007. — 432 с.

[13] *Чемеков В. П.* Диагностика компетенций в системе оценки персонала // Кадровик. RU. — 2011. — № 4.

[14] *Чемеков В. П.* Грейдинг: построение системы управления персоналом. — М. : Вершина, 2007.

[15] *Шмелев А. Г.* Психодиагностика личностных черт. — СПб. : Речь, 2002.

АСТАХОВА Людмила Викторовна, д. п. н., профессор, зав. кафедрой «Информационная безопасность» ЮУрГУ.

ASTAKHOVA Lyudmila Viktorovna, Doctor of Education, Professor. South Ural State University.

УДК 004.032.26
ББК Ч231.3

Т. Ю. Зырянова, В. С. Ковалев

Использование аппарата искусственных нейронных сетей для анализа информационных рисков

В статье раскрываются основные проблемы, связанные с оценкой информационных рисков организации. Подробно рассматриваются основные методики оценки информационного риска, а также возможность применения нейросетевых технологий для проведения анализа риска. В заключение сделан вывод о целесообразности применения нейронных сетей для проведения анализа информационных рисков.

Ключевые слова: *информационная безопасность, анализ риска, нечеткие множества, нейронные сети.*

T. Yu. Zyryanova, V. S. Kovalev

Using artificial neural network technology for information risk analysis

This article describes the main problems associated with information risks assessing of the organization. The basic methodology for information risks assessing examines here in detail, and the possibility of using neural network technology to conduct a risk analysis considers. The conclusion of the expediency of using neural networks to analyze the information risks is considered in final chapter.

Key words: *information security, risk analysis, fuzzy sets, neural networks.*

1. Введение

Любая форма человеческой деятельности связана с определенным риском, т. к. на исход решений, принимаемых людьми, влияет множество условий и факторов. Зачастую все эти факторы невозможно учесть, что представляет собой основную проблему при попытке оценить уровень риска. С развитием науки, промышленности, экономики возрастает необходимость в научно обоснованных и эффективных методах оценки рисков. В таких областях, как ядерная промышленность, авиапромышленность, медицина и, конечно, финансы, невозможно обойтись без тщательной оценки предполагаемых последствий, связанных с тем или иным решением. Выгоды от применения риск-менеджмента доказаны многолетней практикой крупнейших организаций по всему миру[1].

На сегодняшний момент информация является таким же ценным активом организации, как оборудование, рабочая сила, финансы и т. д. Утечка конфиденциальной информации третьим лицам или нарушение ее доступности или целостности приводит к потере конкурентоспособности предприятия на рынке, снижению прибыли, потере репутации и, как следствие, серьезным финансовым убыткам вплоть до банкротства предприятия. По данным мировой статистики, в 2010 году зафиксировано 1014 утечек ценной информации, при этом средний ущерб от одной утечки в 2010 году составил 3 793 725 долларов США[2]. О важности информационных ресурсов также свидетельствует и то внимание государства, которое последнее время уделяется регулированию отношений в информационной сфере.

Под влиянием процессов глобализации в экономике и обществе, новых идей развития бизнеса, технологий непрерывно растут сложность и распределенность информационных систем, что в свою очередь снижает управляемость и защищенность таких систем. Между тем существует большое количество дестабилизирующих факторов, воздействующих на информацию и информационные системы, как внешних, так и внутренних. В связи с этим является актуальным внедрение процедур управления рисками нарушения информационной безопасности (информационными рисками) в систему менеджмента любой современной организации.

Основная цель статьи состоит в раскрытии содержания проблемы управления информационными рисками предприятия и в описании механизма оценки информационных рисков предприятия с помощью нейросетевых технологий.

Методологическую основу исследования составили концепции и взгляды отечественных и зарубежных специалистов по информационной безопасности, журнальные статьи, материалы научных семинаров и конференций, связанные с проблемами риска.

2. Описание процессов управления информационными рисками

Управление информационными рисками является составной частью общей системы управления организацией и играет основную роль в построении комплексной системы защиты информации.

В общем случае риск — это сочетание вероятности и последствий наступления неблагоприятного события. В информационной безопасности риск определяется как функция трех переменных:

1. Вероятность существования угрозы нарушения информационной безопасности.

2. Вероятность существования незащищённости (уязвимости).

3. Величина ущерба от потенциального воздействия.

Если любая из этих переменных приближается к нулю, полный риск приближается к нулю.

Управление информационными рисками представляет собой непрерывный циклический процесс, включающий в себя анализ информационных рисков, а также разработку и применение мер, направленных на снижение информационного риска до приемлемого уровня. В свою очередь анализ информационных рисков состоит из шагов, представленных на рис. 1[3].

Анализ информационных рисков является довольно сложной задачей по следующим причинам:

- На информационный риск влияет множество факторов, которые с трудом поддаются количественному описанию и формализации;
- Сложно подобрать исходные данные для анализа информационных рисков, т. к. собственная статистика у предприятия может отсутствовать, а чужая статистика может не соответствовать условиям функционирования предприятия;
- Неотъемлемой частью анализа информационных рисков является процесс принятия решений человеком, т. е. результат зависит от уровня знаний и опыта специалистов, проводящих анализ;
- Процесс анализа информационных рисков требует использования нелинейных методов моделирования.

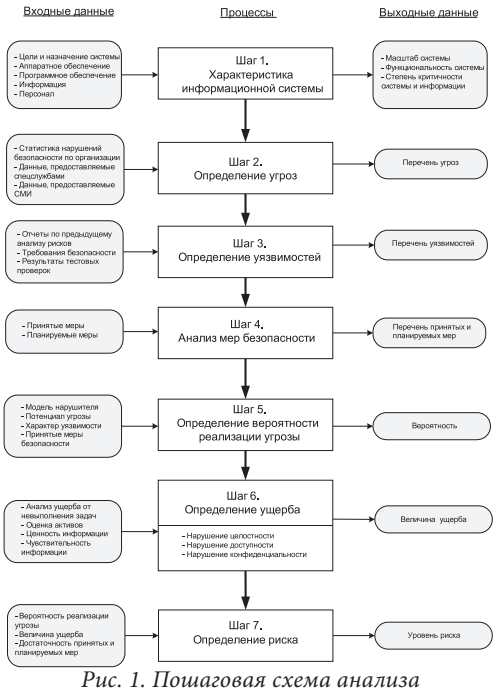

Рис. 1. Пошаговая схема анализа информационных рисков

Для задач оценки вероятности реализации угрозы и предполагаемого ущерба нет однозначного решения, т. к. на конечный результат влияет случайная составляющая, тем не менее существуют различные методы, позволяющие выполнить данные процессы с некоторой степенью точности. К таким методикам относятся:

- Структурированные интервью с экспертами в области информационной безопасности;
- Вероятностно-статистические методы;
- Методы статистики нечисловых данных, в том числе интервальной статистики и интервальной математики, а также методы теории нечеткости.

Сложность и затраты исследований увеличиваются в диапазоне от качественного, полуколичественного до количественного анализа. Качественный анализ проводится на начальном этапе идентификации рисков и определяет необходимость более детального анализа. Такой анализ также часто проводится в случаях, если уровень риска не оправдывает времени и затрат для его более детального изучения.

Вероятность и последствия появления риска могут также оцениваться на основе количественного анализа. Количественный

анализ предназначен для оценки последствий на основе моделирования результатов явлений или данных, взятых наблюдений.

3. Обзор традиционных методов анализа информационных рисков

3.1. Анализ информационных рисков методом экспертного оценивания

Методы экспертных оценок информационных рисков являются комплексами математических процедур получения от специалистов-экспертов информации о рисках, ее анализа и обобщения (консолидации) с целью выработки рациональных рисковых решений[4]. Ниже рассмотрен распространенный метод прямого оценивания.

Исходные данные: число специалистов-экспертов, из которых формируется экспертная группа, — n, число ранжируемых факторов рисковой ситуации — k (в данном случае угроз информационной безопасности).

Каждому i-му эксперту (i = 1, 2, … n) предлагается определить риск реализации каждой угрозы r_{ij} из предварительно составленной матрицы угроз, то есть предлагается установить r_{ij} — j-го фактора, j = 1, 2, … k.

В результате получается матрица-строка мнений каждого i-го эксперта относительно каждой угрозы информационной безопасности (по отдельности для каждой угрозы):

$$| r_i | = | r_{i1}, r_{i2}, \dots r_{ik} |. \qquad (1)$$

Пример результатов экспертного оценивания представлен в табл. 1.

Таблица 1

Результат экспертного оценивания

		Угроза (j)			
		1	2	…	k
Эксперт 1 (i)	Уровень риска (r)	0	0,5	…	r_{1k}
Эксперт 2	Уровень риска	0	0,6	…	r_{2k}
Эксперт ...	Уровень риска	…	…	…	…
Эксперт n	Уровень риска	0	0,7	…	r_{nk}

Далее нужно определить среднее значение модуля $| r_j |$ оценки j-го фактора по всем экспертам:

$$\frac{| r_j |= \sum_{i=1}^{r} r_{ij}}{n}. \qquad (2)$$

Для данного метода оценки необходимо определить пороговое значение, при котором результат экспертизы признается истинным. Необходимо «отсеять» тех экспертов, мнение которых значительно отходит от среднего мнения группы, т. е. превышает порог расхождения мнений.

Следует отметить, что кроме вышеописанного метода существуют и другие методы экспертного оценивания рисков, например «Медиана Кемени» или метод «большинства».

3.2. Корреляционно-регрессионный анализ информационных рисков

Корреляционно-регрессионный анализ является одним из основных методов определения значимых факторов, оказывающих влияние на уровень риска с использованием статистики.

Корреляционный анализ позволяет определить закономерности для массовых наблюдений, когда заданным значениям зависимой переменной соответствует некоторый ряд вероятных значений независимой переменной. Задачи регрессионного анализа лежат в сфере установления формы зависимости, определения функции регрессии, использования уравнения для оценки неизвестных значений зависимой переменной.

Можно выделить два основных типа связей между уровнем риска и факторами, воздействующими на риск[5]: функциональная (жестко детерминированная) и статистическая (случайная). При функциональной связи каждому значению фактора признака соответствуют строго определенные значения результативного признака. При статистической связи с изменением значения факторного признака значения результативного признака могут варьировать в определенных пределах, т. е. принимать любые значения в этих пределах с некоторыми вероятностями.

Рассмотрим механизм оценки информационного риска с помощью корреляционно-регрессионного анализа.

Пусть на уровень риска y влияет некоторый случайный фактор x. Зная статистику, по данной зависимости можно найти линию регрессии. На практике линия регрессии чаще всего ищется в виде линейной функции:

$$y = a + bx, \qquad (3)$$

где a, b — коэффициенты пропорциональности уравнения.

Чтобы построить линию регрессии, необходимо определить коэффициенты a и b. Для этого можно использовать метод наименьших квадратов, в котором минимизируется сумма квадратов отклонений реально наблюдаемых значений y от их проекций на искомую прямую линию регрессии — y':

$$\sum_{i=1}^{M}(y_i - y_i^{'})^2 = \sum_{i=1}^{M}(a + b + y_i^{'})^2 \to \min, \quad (4)$$

где M — объем выборки.

На рис. 2 показано, как располагаются наблюдаемые значения относительно предполагаемой линии регрессии.

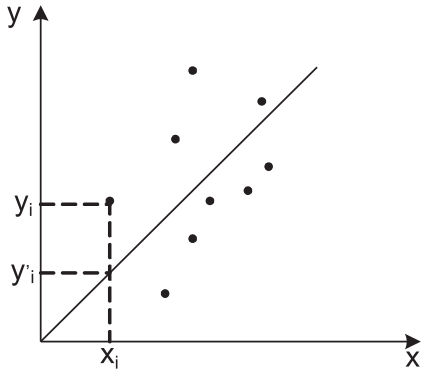

Рис. 2. Линия регрессии

Исследуя на экстремум функцию (4) с помощью производных, можно доказать, что функция принимает минимальное значение, если коэффициенты *a* и *b* являются решениями системы:

$$\begin{cases} a\sum_{i=1}^{M} x_i + b\sum_{i=1}^{M} x_i^2 = \sum_{i=1}^{M} x_i y_i \\ Ma + b\sum_{i=1}^{M} x_i = \sum_{i=1}^{M} y_i \end{cases} \quad (5)$$

Разделив обе части нормальных уравнений на M, получим:

$$\begin{cases} a\dfrac{\sum_{i=1}^{M} x_i}{M} + b\dfrac{\sum_{i=1}^{M} x_i^2}{M} = \dfrac{\sum_{i=1}^{M} x_i y_i}{M} \\ a + b\dfrac{\sum_{i=1}^{M} x_i}{M} = \dfrac{\sum_{i=1}^{M} y_i}{M} \end{cases} \quad (6)$$

Введем средние значения:

$$\frac{\sum_{i=1}^{M} x_i}{M} = \bar{x}, \ \frac{\sum_{i=1}^{M} y_i}{M} = \bar{y}, \quad (7)$$

$$\frac{\sum_{i=1}^{M} x_i^2}{M} = \overline{x^2}, \ \frac{\sum_{i=1}^{M} x_i y_i}{M} = \overline{xy}$$

где $\bar{x}$ — среднее значение переменной *x*,

$\bar{y}$ — среднее значение переменной *y*.

Получаем систему уравнений:

$$\begin{cases} a\bar{x} + b\overline{x^2} = \overline{xy} \\ a + b\bar{x} = \bar{y} \end{cases} \quad (8)$$

Выразим из системы уравнений значения *a* и *b*:

$$b = \frac{\overline{xy} - \bar{x}\cdot\bar{y}}{\overline{x^2} - \bar{x}^2}, \quad (9)$$

$$a = \frac{\overline{x^2}\cdot\bar{y} - \bar{x}\cdot\overline{xy}}{\overline{x^2} - \bar{x}^2}. \quad (10)$$

Построив линию регрессии с использованием выведенных значений, можно спрогнозировать изменение уровня информационного риска при определенном значении фактора риска.

Следует отметить, что для прогнозирования риска корреляционно-регрессионным методом необходимо иметь значительный объем статистических данных, взятых либо из предыдущего анализа рисков, либо у сторонних организаций, что в большинстве случаев крайне проблематично. По мнению автора, данный метод целесообразно использовать для прогнозирования ущерба от реализации угроз безопасности.

3.3. Анализ информационных рисков на основе теории нечетких множеств

Применение нечёткой логики наиболее математически адекватно для решения проблемы оценки информационных рисков. Теория нечёткой логики позволяет оперировать лингвистическими переменными при обработке недетерминированных данных, связанных с риском, что наиболее естественно для человеческого понимания[6].

Процесс оценки рисков на основе теории нечетких множеств представлен ниже.

Для начала необходимо определить входные и выходные параметры нечеткой логической системы, а также определить значения, которые могут принимать эти лингвистические переменные. Для примера рассмотрим нечеткую систему со следующими входными параметрами:

$$A = \{ A_1, A_2, A_3 \} , \quad (11)$$

где A — множество вероятности реализации угрозы,

$$B = \{ B_1, B_2, B_3 \} , \quad (12)$$

где B — множество возможного ущерба от реализации угрозы.

В качестве выходного параметра будет выступать множество уровней информационного риска C:

$$C = \{ C_1, C_2, C_3 \} . \quad (13)$$

Данные лингвистические переменные могут принимать, например, такие значения, как: низкий, средний и высокий и т. д. Для перевода лингвистических переменных на математический язык и дальнейшего применения метода нечетких множеств введем понятие функции принадлежности. Функцией принадлежности $\mu A(X)$ является некая математическая функция, задающая степень или уверенность, с которой элементы некоторого числового множества X принадлежат заданному нечеткому множеству A. Сама функция принадлежности строится на основе экспертных оценок. Пример функций принадлежности представлен на рис. 3.

Задачей нечеткого вывода в данном случае является определение числового значения для выходной переменной С. Для этого, экспертами должны быть разработаны правила нечеткого вывода, которые представляют собой формальное представление эмпирических знаний экспертов в той или иной проблемной области. Наиболее часто база правил имеет вид структурированного текста:

- Правило 1: если «условие A_1» и «условие B_1», то «следствие C_1»;
- Правило 2: если «Условие A_2» и «условие B_2», то «следствие C_2»;
- …
- Правило n: если «условие A_n» и «условие B_n», то «следствие C_n».

Построив функции принадлежности для каждого входного параметра нечеткой системы и сформулировав необходимые правила нечеткого вывода, необходимо провести агрегирование. Целью данного этапа является определение степени истинности каждого из подзаключений по каждому из правил систем нечеткого вывода. Это приводит к одному нечеткому множеству, которое

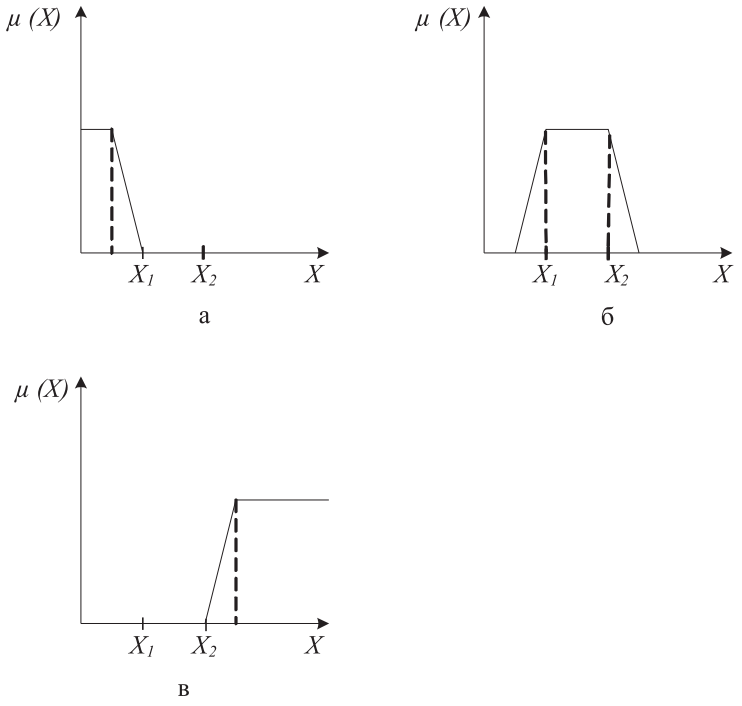

Рис. 3. Функция принадлежности числовых значений к нечеткому множеству А: а) для низкой вероятности реализации угрозы; б) для средней вероятности реализации угрозы; в) для высокой вероятности реализации угрозы

будет назначено каждой выходной переменной для каждого правила. В качестве правил логического вывода обычно используются операции минимума или умножения.

На следующем этапе проводится активизация подусловий в нечетких правилах.

Нечеткие подмножества, назначенные для каждой выходной переменной, объединяются вместе, чтобы сформировать одно нечеткое подмножество для каждой переменной.

Далее полученные результаты всех выходных переменных на предыдущих этапах нечеткого вывода преобразуются в обычные количественные значения каждой из выходных переменных. Формально это выглядит так:

$$c_i = \frac{\int_{\underline{x}}^{\bar{x}} x \cdot \mu A(x)}{\int_{\underline{x}}^{\bar{x}} x \cdot \mu A(x) dx}, \qquad (14)$$

где c_i — значение выходной переменной;

$\bar{x}$, $\underline{x}$ — границы числовых значений нечетких переменных.

Т. о., составив такую нечеткую логическую систему, можно определить количественное значение уровня информационного риска на основе значений лингвистических переменных.

Следует отметить, что при использовании данного метода анализа информационных рисков существует субъективность в выборе функций принадлежности и формировании правил нечеткого ввода.

4. Применение аппарата искусственных нейронных сетей для анализа информационных рисков

4.1. Преимущества и недостатки нейросетевых технологий

Одним из перспективных подходов к управлению информационными рисками является применение аппарата нейронных сетей для классификации и прогнозирования рисков.

Искусственные нейронные сети представляют собой набор взаимосвязанных искусственных нейронов, функционирующих по принципам биологических нейронов — нервных клеток живого организма. Каждый искусственный нейрон представляет собой довольно простой процессор, тем не менее, будучи соединёнными в масштабную сеть с управляемым взаимодействием, такие локально простые процессоры вместе способны выполнять сложные задачи[7]. Искусственные нейронные сети демонстрируют такие возможности, как способность к неформальному обучению, способность к обобщению и кластеризации неклассифицированной информации.

Нейронные сети широко применяются в различных сферах человеческой деятельности, в том числе и для анализа финансовых рисков[8, 9], однако эта область науки все еще находится в динамическом развитии.

Нейросетевые технологии используются в случаях, когда формализация процесса решения трудна или вообще невозможна. Линейное моделирование долгое время являлось основным в большинстве областей, поскольку для него существует большое число методов оптимизации. Однако в задачах анализа информационных рисков методы линейного моделирования в подавляющем большинстве случаев неприменимы.

Искусственные нейронные сети являются очень мощным инструментом моделирования, т. к. нелинейные по своей природе. Следует отметить, что для нейронных сетей не существует проблемы «проклятия размерности», не позволяющей моделировать линейные зависимости от большого числа переменных.

Нейронная сеть применяется в первую очередь тогда, когда входные данные становятся неопределёнными, но между тем влияют на результаты решения. Если между входными и выходными данными существует какая-то зависимость, пусть даже не обнаруживаемая традиционными корреляционными методами, нейронная сеть способна настроиться на нее с заданной степенью точности. При этом сама зависимость будет выведена в процессе обучения нейронной сети. По сравнению с традиционными технологиями нейронные сети обладают следующими достоинствами[10]:

- Универсальность. Нейронные сети не зависят от свойств входных данных, для них не существует требования к определенному типу распределения исходных данных, либо требования к линейности целевых функций.
- Простота. Использование нейронных сетей не требует специальной подготовки, для практического применения нет необходимости глубоко вникать во внутренние механизмы работы сети, в отличие от статистических методов, требующих фундаментальных знаний из области теории вероятностей и математической статистики.
- Не существует проблемы «проклятия размерности». Они способны моделировать зависимости в случае большого числа переменных.
- Адаптивность нейронных сетей позволяет работать в среде с изменяющимися параметрами. Т. е. нейронная сеть легко под-

страивается и переучивается под изменяющуюся статистику.

• Ускоряют процесс нахождения зависимости за счет одновременной обработки данных всеми нейронами[11].

Однако следует отметить, что нейронные сети обладают рядом серьезных недостатков:

• Сложность построения архитектуры сети для конкретной задачи. Для подавляющего большинства реальных задач не разработано стандартных схем, в результате в каждом случае конструирование приходится начинать «с нуля».

• Сложность обучения. Особенности построения нейронной сети будут рассмотрены дальше. Пока же можно отметить, что значения параметров элементов сети почти всегда невозможно объяснить в терминах решаемой задачи, в результате нейронная сеть остается «черным ящиком» не только для пользователей, но отчасти и для разработчиков. Кроме того, для обучения нейронной сети требуется большое количество исторических данных, которое в некоторых случаях недоступно.

• Требуются значительные затраты по времени и аппаратным ресурсам для построения удовлетворительной модели.

4.2. Математическая модель искусственной нейронной сети

Искусственный нейрон имитирует в первом приближении свойства биологического нейрона. На рис. 4 показана схема нейрона[12]. Хотя сетевые парадигмы весьма разнообразны, в основе почти всех их лежит эта конфигурация.

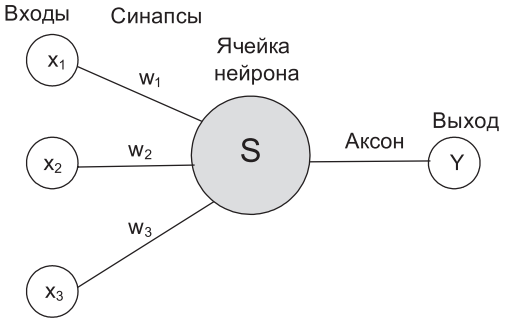

Рис. 4. Функциональная схема нейрона

Искусственный нейрон, так же, как и живой, состоит из синапсов, связывающих входы нейрона с ядром, ядра нейрона, которое осуществляет обработку входных сигналов и аксона, который связывает нейрон с нейронами следующего слоя. На входы искусственного нейрона — x_i поступает некоторое множество сигналов, которые по синапсам поступают в ядро нейрона. Каждый синапс имеет вес w_i, который определяет, насколько соответствующий вход нейрона влияет на его состояние. В ячейке нейрона вычисляется взвешенная сумма входов:

$$S = \sum_{i=1}^{n} x_i \cdot w \qquad (15)$$

где S — взвешенная сумма входов.

Далее полученная сумма сравнивается с пороговым значением активации нейрона *Q*. Если

$$S > Q\ , \qquad (16)$$

то нейрон активируется с определенной величиной активации, равной разности *S* и *Q*. Пороговое значение активации нейрона обычно устанавливается равным нулю.

Сигнал активации преобразуется с помощью функции активации (или передаточной функции) и в результате получается выходной сигнал нейрона:

$$Y = F(S) \qquad (17)$$

Активационная функция нейрона определяет преобразование (линейное либо нелинейное), осуществляемое нейроном. Существует множество видов активационных функций, но более всего распространены следующие[13]:

1. Пороговая функция (рис. 5, а):

$$F(S) = \begin{cases} 1, S > Q \\ 0, S \le Q \end{cases}. \qquad (18)$$

2. Линейная функция (рис. 5, б):

$$F(S) = \begin{cases} S, S > Q \\ 0, S \le Q \end{cases}. \qquad (19)$$

3. Сигмоидальная функция (рис. 5, в):

$$F(S) = \frac{1}{1 + exp(-(S - Q)}. \qquad (20)$$

Отдельные нейроны могут быть объединены в сети путем замыкания выходов одних нейронов на входы других[14]. Группы нейронов со схожими функциями образуют слои

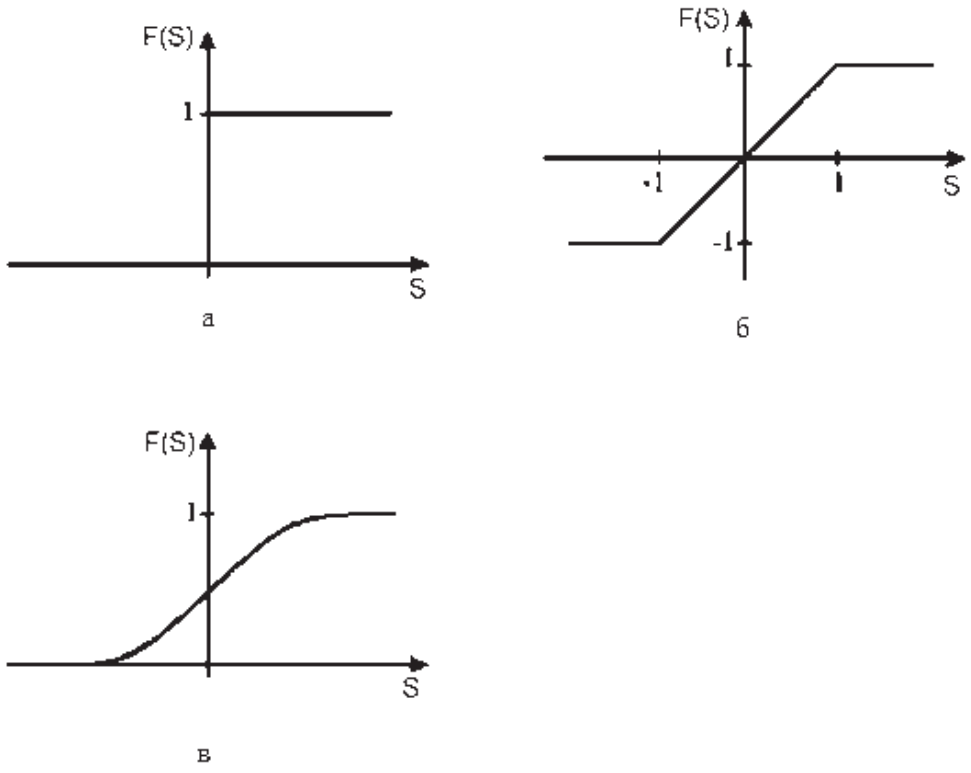

Рис. 5. Типы активационных функций: а) пороговая; б) линейная; в) сигмоидальная

(рис. 6). При работе сети во входные элементы подаются значения входных переменных, затем последовательно отрабатывают нейроны промежуточных и выходного слоев. Каждый из них вычисляет свое значение активации, беря взвешенную сумму выходов элементов предыдущего слоя и вычитая из нее пороговое значение. На рис. 6 показана нейронная сеть, в которой каждый из скрытых и выходных нейронов соединен со всеми элементами предыдущего слоя. Данная схема сети с полной системой связей типична для решения большинства задач, хотя возможны варианты сетей, в которых нейроны связаны только с некоторыми из нейронов предыдущего слоя.

Важнейшим свойством нейронных сетей является их способность обучаться на основе исторических данных — обучающего множества. В процессе обучения экспериментальным способом определяются значения для весов и порогов сети, которые бы минимизировали ошибку результата, выдаваемого нейронной сетью. По сути, этот процесс представляет собой подгонку модели сети к имеющимся обучающим данным.

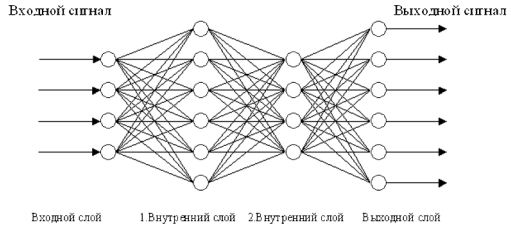

Рис. 6. Схема нейронной сети типа «многослойный персептрон»

4.3. Описание механизма анализа информационных рисков с использованием нейростевых технологий

Построение нейронной сети для анализа информационных рисков следует начинать с определения факторов, влияющих на уровень риска. Необходимо собрать статистику по каждым факторам. Упорядоченная статистика будет служить в качестве набора обучающих данных для нейронной сети.

На следующем этапе необходимо выбрать подходящую топологию нейронной сети. Определение оптимальных значений таких параметров нейронной сети, как количество слоев, количество входных и выходных нейронов в каждом слое, связи между нейронами, определяется экспериментальным путем исходя из условий задачи. Количество нейронов во входном слое будет определяться количеством факторов, воздействующих на уровень информационного риска, единствен-

ный нейрон выходного слоя должен выдавать уровень информационного риска.

Важным этапом построения нейронной сети является выбор активационной функции нейронов. По мнению автора, для задачи анализа информационных рисков следует использовать сигмоидальную функцию активации, т. к. данная функция нелинейная. Кроме того, сигмоидальная функция дифференцируема, что положительно сказывается на способности сети к обучению.

В качестве алгоритма обучения автором предлагается использовать алгоритм обратного распространения ошибки. Данный алгоритм хорошо изучен и достаточно эффективен[15].

Схема обучения нейронной сети представлена на рис. 7.

Основной задачей в процессе обучения является нахождение значений для весов и порогов сети, которые бы минимизировали ошибку результата, выдаваемого нейронной сетью. В процессе обучения с использованием собранных исторических данных веса и пороговые значения корректируются с целью минимизировать эту ошибку.

При обучении вычисляется вектор градиента поверхности ошибок. Этот вектор указывает направление кратчайшего спуска по поверхности из данной точки, поэтому если «немного» продвинуться по нему, ошибка уменьшится. Последовательность таких шагов (замедляющаяся по мере приближения к дну) в конце концов приведет к минимуму. Определенную трудность здесь представляет вопрос о том, какую нужно брать длину шагов. При большой длине шага сходимость будет более быстрой, но имеется опасность «перепрыгнуть» через решение или уйти в неправильном направлении. Напротив, при маленьком шаге, вероятно, будет схвачено верное направление, однако при этом потребуется большое количество итераций. На практике величина шага берется пропорциональной крутизне склона (так что алгоритм замедляет ход вблизи минимума) с некоторой константой, которая называется скоростью обучения. Правильный выбор скорости обучения зависит от конкретной задачи и обычно осуществляется опытным путем.

Обученная нейронная сеть подлежит тщательной проверке с помощью специального тестирующего множества для того чтобы окончательно убедиться в адекватности выдаваемого сетью результата.

Следует отметить, что нейронные сети можно строить с использованием теории нечетких множеств. Поскольку нечеткие множества описываются функциями принадлежности, можно представить нечеткие логические рассуждения в виде нейронной сети. Для этого функции принадлежности надо интерпретировать как функции активации нейронов. Нейронные сети, построенные таким образом, будут сочетать в себе преимущества обоих методов.

Заключение

Таким образом, объединение методов экспертного оценивания, теории нечетких множеств и нейросетевых технологий для анализа информационных рисков позволит значительно усовершенствовать имеющиеся на сегодняшний день подходы к проблемам принятия решений при работе с информационными рисками.

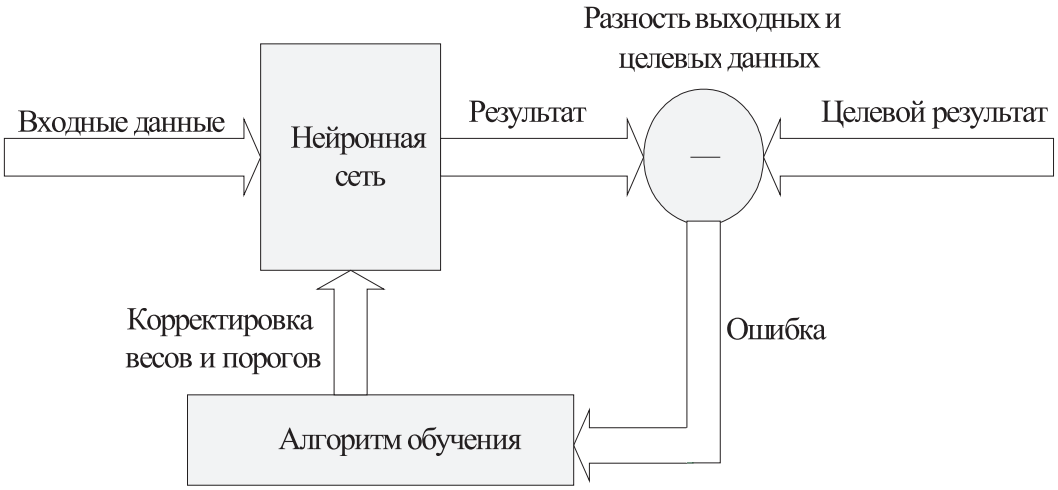

Рис. 7. Функциональная схема обучения нейронной сети

Появляется прямая возможность повысить точность и оперативность оценки информационного риска путём построения модели искусственной нейронной сети. При этом, благодаря гибкости метода, степень точности решения может быть согласована с требованиями задачи и точностью имеющихся статистических данных.

Развитие нейросетевых технологий вызвало немало энтузиазма и критики. Во многих областях нейронные сети зарекомендовали себя как наиболее рациональное решение, однако для полноценного применения данного метода для анализа информационных рисков требуются дальнейшие исследования в данной области.

Примечания

[1] *Поваляева О. Н.* Системное управление рисками как необходимое условие успешности современной коммерческой организации. Государственное управление // Электронный вестник — 2010. — № 25. — С. 7—11. — URL: http://e-journal.spa.msu.ru/images/File/2010/25/ Povaliaeva.pdf (дата обращения: 05.04.2011).

[2] *Ковалев А.* Отчет SECURIT Analytics об утечках информации за 2010 год // 2011. — URL: http://www.securit.ru/docs/securit_research_2010.pdf (дата обращения: 05.04.2011).

[3] *Stoneburner G., Goguen A., Feringa A.* Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology / National Institute of Standards and Technology — 2002.

[4] *Марцынковский Д. А.* Экспертные оценки / 2011. — URL: http: // www. regcon. ru/jo/images/stories/ risk_men_4.pdf (дата обращения: 06.04.2011).

[5] *Севрук В. Т.* Риски финансового сектора Российской Федерации : практическое пособие / под ред. В. Т. Севрук. — М. : Финстатинформ, 2001.

[6] *Абдулаева З. И., Недосекин А. О.* Анализ рисков предприятия на основе методов нечёткой логики / URL: http://www.kpilib.ru/article.php? page= 57 (дата обращения: 07.04.2011).

[7] *Callan R.* The Essence of Neural Networks First Edition / Prentice Hall, 1998.

[8] *Ежов А. А, Шумский С. А.* Нейрокомпьютинг и его применение в экономике и бизнесе. — М. : МИФИ, 1998.

[9] *Angelini E., di Tollo G., Roli A.* A neural network approach for credit risk evaluation // The Quarterly Review of Economics and Finance. — 2007. — URL: http://www.sci.unich.it/~ditollo/works/qref.pdf (дата обращения: 07.04.2011).

[10] *Haykin S.* Neural Networks: A Comprehensive Foundation / MacMillan College Publishing, 1994.

[11] *Hertza A., Krogh R. G., Palmer L.* Introduction to the Theory of Neural Computation / Addison-Wesley Reading, 1991.

[12] *Macculloch W., Pitts W.* A logical Calculus of Ideas Immanent in Nervous Activity // Mathematical Biophysics / Bull, 1943. — Vol. 5. — p. 115—133.

[13] *Laurene F.* Fundamentals of Neural Networks: Architectures, Algorithms And Applications / Prentice Hall, 1993. — p. 17—19.

[14] *Ротштейн А.* П. Интеллектуальные технологии идентификации. — Винница : Универсум, 1999.

[15] *Орлов А.* Обратное распространение ошибки / 2010. (дата обращения: 11.04.2011).

ЗЫРЯНОВА Татьяна Юрьевна, к. т. н., заведующая кафедрой «Системы и технологии защиты информации» Уральского государственного университета путей сообщения. E-mail TZyryanova@zi.usurt.ru

ZYRYANOVA Tatiana Yurievna, Candidate of Engineering Sciences, Head of the Chair «Systems and Technologies of Information Protection», Ural State University of Communications. E-mail: TZyryanova@zi.usurt.ru

КОВАЛЕВ Виктор Сергеевич, аспирант, ассистент кафедры «Системы и технологии защиты информации», Уральский государственный университет путей сообщения. E-mail: vkovalev@gammaural.ru

KOVALYOV Viktor Sergeevich, Postgraduate Student, Assistant of the Chair «Systems and Technologies of Information Protection», Ural State University of Communications. E-mail vkovalev@gammaural.ru

УДК 004.056
ББК Х401.114

Н. А. Гайдамакин

«Краткий курс» истории исследований в сфере компьютерной безопасности

Приводится типология основных событий по исследованиям в сфере компьютерной безопасности. По критерию соотнесенности с историей развития компьютерных информационных технологий (IT) выделены четыре периода в истории исследований компьютерной безопасности. Материал статьи призван способствовать формированию у молодых (начинающих) специалистов исторически-ретроспективного понимания основных направлений развития компьютерной безопасности и их истоков, осознания причастности к важной для развития современного общества профессиональной сфере.

Ключевые слова: *компьютерная безопасность, история, исследования, события, этапы.*

N. A. Gaydamakin

Brief History of Computer Security Studies

The article contains a typology of key events occurred in the domain of computer security studies. Basing on the criterion of relatedness to the IT development history, the author breaks down the history of computer security studies into four periods. This article oriented towards new (beginning) specialists aims to form their historical retrospective understanding of key directions in computer security development and their sources and awareness of their belonging to the professional sphere which is important for development of today's society.

Key words: *computer security, history, studies, events, stages.*

Безопасность, понимаемая в широком смысле как отсутствие опасностей, угроз, препятствий в существовании и развитии, всегда была частью цивилизации, являясь не просто обеспечивающей сферой человеческой жизни и деятельности, но и ее постоянной составляющей. При этом с самого зарождения цивилизации все новое, что обеспечивало выживание человеческих сообществ, их развитие, было связано, в том числе, с новыми или специфическими знаниями и сведениями, их сбором, хранением, передачей и обменом такими знаниями и сведениями.

Поэтому исследования в сфере защиты информации, прежде всего в сфере обеспечения сохранности в тайне определенных знаний, сведений и сообщений, разработка специальных организационно-процедурных механизмов и приемов работы с конфиденциальной информацией, ее сбора, хранения и передачи, возникли одновременно с самой цивилизацией. С древних времен известны технологии тайнописи (предтечи современной криптографии), парольные механизмы идентификации/аутентификации в процессах передачи тайных (секретных, «закрытых») знаний, сведений и сообщений. Одновременно, следуя диалектике развития, накапливались специальные знания о методах и способах, создавались механизмы добывания таких тайных знаний, сведений и [перехвата] сообщений.

Это двуединство средств, технологий защиты и нападения являлось постоянным источником развития и сферы защиты информации, и сферы ее «добывания», закручивая их в спираль событий, явлений и изобретений на протяжении многих веков и технологических инноваций. Однако следует заметить, что всегда сфера защиты секретных знаний, сведений, сообщений, их передачи, с одной стороны, сфера их добывания, перехвата — с другой стороны, сами были тайными, «закрытыми», уделом специальных структур, создаваемых властными ин-

ститутами, государством или их внутренними и внешними противниками.

С наступлением компьютерной эры, с развитием и повсеместным внедрением новых информационных технологий, основанных на вычислительной технике, роль и значимость безопасности информации еще более возросла, превратив ее защиту в обязательную составляющую функциональности любых IT-продуктов и систем. Массовый и всеобъемлющий характер процессов, связанных с IT-технологиями, обусловил возникновение целого ряда новых теоретических и практических задач и, кроме того, вывел, если так можно выразиться, некоторые из известных к этому времени способов защиты информации «из тени» «в мир».

В результате история исследований в сфере компьютерной безопасности, во-первых, связана с массовым применением компьютерной техники для сбора, накопления, обработки, хранения, передачи и использования разнообразной, в т. ч. конфиденциальной (секретной, закрытой, критической), информации. Во-вторых, эта «новая» история неотделима от истории развития самой компьютерной (вычислительной) техники.

Поэтому характеристику исследований в сфере компьютерной безопасности трудно оторвать от основных событий и рубежей в развитии самих компьютерных систем. Отталкиваясь от принципа «типизации», выделим четыре этапа в этой истории по критерию «вовлечения» компьютерной техники в процессы обработки информации.

40-е — середина 60-х гг. XX века

Начальный (или, как выразились бы программисты, — нулевой) этап можно отнести к периоду 40-х — середине 60-х годов XX века, когда собственно и были изобретены компьютеры (электронно-вычислительные машины — ЭВМ), которые сразу же стали интенсивно применяться в сфере криптоаналитики, для вычислений, связанных с созданием ядерного оружия, ракетной техники и других вооружений, т. е. в специальной сфере открытого (явного) и скрытого противостояния стран и их спецслужб. Исследования в сфере защиты информации этого периода целиком связаны с криптоанализом, с разработкой криптографических алгоритмов шифрования данных, которые могли бы успешно и эффективно реализовываться средствами вычислительной техники.

Середина 60-х — начало 70-х гг. XX века

Следующий этап развития компьютерных технологий (следуя нашей типологии, будем называть его первым) охарактеризовался разработкой ЭВМ т. н. «третьего поколения» (приблизительно 1964 г. — БЭСМ-4, БЭСМ-6 в СССР и IBM-360 в США). Архитектура и операционные системы компьютеров третьего поколения предусматривали многозадачный режим функционирования с разделением ресурсов процессора на «кванты» для разных задач (процессов) и наличие «внешних» (долговременных) устройств памяти. Это обеспечивало возможности коллективной работы с дорогостоящими по тем временам ЭВМ, а также возможности длительного и отдельного от ЭВМ хранения программ и данных. Вероятно, именно это послужило инициализирующей потребностью в исследованиях, посвященных собственно компьютерной безопасности.

Постепенно начали формироваться и выделяться направления этих исследований:

— исследования и разработка формальных моделей безопасности компьютерных систем, сердцевиной которых являлись и являются модели безопасности компьютерных данных, основанные на парадигме «конфиденциальность» — «целостность» — доступность»;

— исследования и разработка механизмов идентификации/аутентификации, являющихся архитектурными и инфраструктурными основами создания защищенных компьютерных систем;

— исследования и разработка алгоритмов криптографической защиты компьютерных данных при передаче их в сетях;

— исследования и разработка методов противодействия в сфере вредоносного программного обеспечения, компьютерных атак;

— исследования в сфере методов анализа и оценивания безопасности (защищенности) компьютерных систем.

Потребности в разработке механизмов защиты компьютерной информации усиливались еще и тем, что именно в этот период ЭВМ, хотя еще и весьма дорогостоящие, стали доступными крупным «гражданским» компаниям и организациям. Появились потребности в программных средствах, предназначенных не только для вычислений, но и для накопления, хранения, обработки, использования разнообразных данных в компьютерной форме. В середине 60-х годов компания IBM совместно с фирмой NAA (ныне Rockwell International) создали первую иерархическую систему управления базами данных (СУБД IMS — Information Management System).

Примерно в те же годы компания General Electric разработала СУБД IDS (Integrated Data Store). В 1965 г. на конференции

CODASYL (Conference on Data Systems Languages) была сформирована исследовательская рабочая группа «List Processing Task Force», переименованная в 1967 году в группу «Data Base Task Group» (DBTG) для разработки спецификаций и стандартов СУБД с сетевой моделью организации данных.

В этом же ряду событий весьма показательным является приобретение в 1967 г. информационным агентством «Рейтер» компьютера IBM-360 для накопления, хранения и обработки новостных сообщений.

В результате информация, накапливаемая в процессах деятельности крупных, и не только военных («закрытых») организаций, но и предприятий «гражданской» сферы, включая сведения конфиденциального характера («ноу-хау», персональные данные, данные о финансовом положении и т. д.), стала переводиться в электронную компьютерную форму. Добавим на примере агентства «Рейтер», что в некоторых случаях основной результат деятельности предприятий, организаций стал выражаться и воплощаться в форме компьютерной базы данных.

Другим фактором из сферы компьютерных IT-технологий этого периода, также непосредственно связанным с исследованиями в сфере защиты информации, точнее передаваемых сообщений, является развертывание в конце 60-х годов в США проекта «ARPANET» (Advanced Research Projects Agency Network), направленного на разработку принципов создания и устойчивого функционирования компьютерных сетей передачи данных, охватывающих основные центры (города) сначала в рамках национальной военной и управленческой, а впоследствии и международной научно-образовательной инфраструктуры.

Отмеченные факторы развития компьютерных технологий этого периода инициализировали исследования, в т. ч. и в сфере компьютерной безопасности. Появились первые теоретические работы и публикации по проблемам защиты компьютерной информации, в частности публикация в 1969 г. Вайссманом (C. Weissmann) результатов разработки первой дискреционной модели безопасности АДЕПТ-50, включающей парольную аутентификацию, рабочие группы пользователей и др.

Кроме того, государства и их соответствующие структуры стали осознавать необходимость «открытия» для «гражданской» сферы хотя бы части криптографических технологий, которые можно было бы использовать в компьютерных сетях передачи данных. В результате к исследованиям в сфере криптографии стал постепенно подключаться многочисленный отряд «гражданских» специалистов, стали прорабатываться идеи создания и организовываться исследования по разработке отдельных элементов компьютерных сетей сугубо «гражданской» направленности, в частности, компьютерных сетей межбанковских коммуникаций (платежей), явно требовавших криптографических механизмов защиты передаваемой информации.

Начало 70-х — начало 80-х гг. XX века

Второй этап в истории развития компьютерных информационных технологий и, соответственно, исследований в сфере компьютерной безопасности можно очертить рамками начала 1970-х — начала 1980-х гг. XX века.

В начале 70-х годов появились первые мини- и микро-ЭВМ, доступные и потребные не только крупным, но и средним предприятиям и организациям. Соответственно, внедрение вычислительной техники в информационное обеспечение и технологические процессы различных предприятий и организаций существенно расширилось и стало приобретать массовый характер.

Логическим продолжением этих процессов, базирующихся на миниатюризации электронной элементной базы, с одной стороны, а, с другой, — на стремлении предприятий и организаций, их работников к «персонализации» своих «отношений» со средствами вычислительной техники, явилось создание в 1975 г. в США первого т. н. «персонального компьютера»[1]. В 1976 г. компания «Apple» разработала и выпустила «в свет» свой первый персональный компьютер. Чрезвычайно важно отметить, что программное обеспечение «эппловского» компьютера включало т. н. «табличный процессор» (программное средство для создания и работы с табличными данными, включая разнообразные вычислительные функции финансового и экономического характера). Поэтому своих потребителей «эппловский» компьютер нашел не только в среде профессиональных программистов, ученых и инженеров, для которых был необходим («под рукой» и не обязательно «мощный») персональный электронный вычислитель, но и в среде многочисленных работников финансово-экономической сферы теперь уже не только крупных, средних, но и мелких предприятий. В результате еще бóльшие массивы самой разнообразной информации, включая «конфиденциальные» данные, стали переводиться в электронную компьютерную форму.

Кульминацией этого массового и грандиозного по масштабам инновационного про-

цесса стал выпуск «в свет» в США в 1981 г. персонального компьютера компании IBM (IBM PC). Помимо табличного редактора он включал и простейший текстовый редактор, при помощи которого стало возможным разрабатывать на ПЭВМ несложные служебные документы разнообразного характера, используемые в документообороте предприятий и организаций. Появилась существенно более «продвинутая» альтернатива пишущей машинки, которую в США, начиная с 1902 г., многие десятилетия подряд выпускала та же компания IBM. Соответственно, круг потребителей такого рода инструментария (персональных компьютеров) стал поистине всеобъемлющим, что, в свою очередь, еще более интенсифицировало перевод процессов обработки и хранения разнообразной информации в компьютерную форму.

Параллельно «компьютерной персонализации» в этот период продолжались не менее значимые процессы в сфере создания СУБД для «больших» ЭВМ. Именно в этот период был развернут ряд исследовательских проектов (проект «System R» фирмы IBM по созданию СУБД DB2, 1975—1979 гг.; проект разработки СУБД «Ingres» университета Беркли, 1975—1980 гг.), результатом которых стало появление на рынке новых программных средств обработки данных — реляционных СУБД. Начался массовый процесс создания предприятиями и организациями автоматизированных систем в различных сферах деятельности (в управленческой, технологической; в сферах обеспечения деятельности). В результате организационно-управленческая и организационно-технологическая сферы крупных и средних предприятий, организаций стали стремительно «компьютеризироваться».

Важно также отметить еще одно направление развития информационных технологий этого периода. К концу семидесятых годов проект «ARPANET» из военно-исследовательского перешел в фазу создания международной компьютерной сети передачи данных, которая связала электронными компьютерными коммуникациями правительственные структуры, крупные исследовательские государственные и частные центры, университеты США, Канады и стран Западной Европы. К началу 1980-х гг. стал возникать прообраз глобальной информационной инфраструктуры «общегражданского» назначения.

Таким образом, основные события и инновации в сфере компьютерных информационных технологий в период начала 70-х — начала 80-х гг. XX века явились мощным потребным аспектом разработки и создания механизмов защиты компьютерной информации, исследований в различных направлениях компьютерной безопасности.

Начало этого (второго) периода характеризуется интенсивными теоретическими исследованиями в сфере формальных моделей безопасности компьютерных систем. В это время были опубликованы результаты по таким формальным моделям безопасности, как «система с полным перекрытием [угроз]» (Хоффман и др., 1970—1974 гг.), «пятимерное пространство безопасности» (Хартсон, 1975 г.), дискреционная модель «распространения прав доступа» (модель Харрисона, Руззо, Ульмана — т. н. модель HRU, 1975 г.), теоретико-графовая модель «TAKE-GRANT» (Джонс, Липтон, Шнайдер, 1976 г.).

Для понимания логики исследований в сфере формальных моделей безопасности того периода важно отметить следующее. Результаты исследований по двум последним моделям безопасности (модели HRU и TAKE-GRANT), которые были созданы для исследования процессов передачи прав доступа в рамках дискреционной политики безопасности[2], привели к обескураживающим результатам — при отсутствии ограничений на передачу прав доступа на какие-либо объекты от владельцев этих объектов другим пользователям нет теоретических гарантий невозможности ознакомления какого-либо субъекта-пользователя с определенным (конфиденциальным) объектом, т. е., по сути, нет гарантий безопасности. Введение же ограничений, при которых такие гарантии могут быть обоснованы, приводит к существенной потере функциональности компьютерных систем.

Данные результаты в середине 70-х годов привели к некоему «теоретическому кризису» в области формальных моделей безопасности и тем самым стимулировали поиски новых методов и принципов организации доступа к [информационным] объектам в компьютерных системах.

В 1973—1975 гг. сотрудники MITRE Corporation (организации, проводящей исследования в интересах Министерства обороны США) Дж. Белл и Л. ЛаПадула (J. E. Bell и L. J. LaPadula) разработали альтернативную дискреционному подходу т. н. «мандатную» модель безопасности компьютерных систем. Как и многое другое в технологиях защиты компьютерной информации, основы и принципы данной модели были «подсмотрены» во внекомпьютерной сфере — в сфере работы с «бумажными» секретными документами. Белл и ЛаПадула в рамках своей модели, которую впоследствии стали называть по их именам (модель Белла — ЛаПадулы), на основе теоретико-множественной формализации

методологии и правил доступа к секретным документам сотрудников военных и других «закрытых» организаций математически доказали безопасность функционирования компьютерной системы, воспроизводящей эти правила. Было строго доказано, что с точки зрения утечки секретных данных от доверенного пользователя (или из секретного файла) к недоверенному пользователю (в несекретный файл) компьютерная система, удовлетворяющая условиям модели Белла — ЛаПадулы, функционирует безопасно[3].

Модель Белла — ЛаПадулы сыграла (и во многом играет до сих пор) огромную методологическую роль в теории компьютерной безопасности. С одной стороны, была продемонстрирована возможность создания компьютерных систем, в которых безопасность математически доказана, а с другой — возможность воспроизведения в архитектуре компьютерных систем и в алгоритмах доступа к компьютерным данным тех правил, которые установлены нормативными регламентациями в «бумажной» сфере.

Как это часто бывает в отношении неких новаторских фундаментальных результатов, модель Белла — ЛаПадулы на протяжении второй половины 70-х — первой половины 80-х годов подверглась тщательному и всестороннему анализу (или, как говорят в компьютерной сфере, — атакам). Одним из исследователей, который внес наиболее существенный вклад в развитие модели Белла — ЛаПадулы, был Дж. МакЛин (J. McLean). Его работы снизили некоторую «схоластичность» модели Белла — ЛаПадулы, приблизив ее к различным аспектам практической реализации в компьютерных системах.

Другим заметным результатом в разработке новых подходов и формальных моделей в конце второго периода развития компьютерных IT-технологий стала «автоматная модель» Гогена и Мессигера (J. Goguen, J. Messeguer, 1982 г., — GM-модель). Она сыграла важную методологическую роль в поисках теоретических подходов к перекрытию т. н. «скрытых» каналов утечки информации[4], о существовании которых в рамках исследований дискреционных и мандатных моделей было много обсуждений во второй половине 70-х годов. Кроме того, GM-модель предоставила разработчикам защищенных КС ряд важных принципов (правил) для разработки интерфейса пользователя в контексте безопасности компьютерной информации.

Исследования в области компьютерной безопасности в этот период проводились и крупными «гражданскими» организациями из IT-сферы. В конце 70-х годов та же корпорация IBM провела исследовательский проект по тематике организации коллективного доступа пользователей к сложноорганизованным данным в компьютерных системах. Одним из результатов этого исследовательского проекта стало появление «ролевого» подхода к организации доступа. В развитие идей ролевого доступа и других теоретико-прикладных результатов, накопленных к концу этого периода, появилась т. н. MMS-модель (модель системы военных сообщений — Security Models for Military Message System), опубликованная в 1984 г. К. Лендвером, К. Гайтмейером и Дж. МакЛином (C. E. Lendwehr, C. L. Heitmeyer, J. McLean), в которой были объединены элементы дискреционного, мандатного и ролевого доступа.

Другое направление исследований и разработок в сфере компьютерной безопасности в 70-х годах XX века связано с криптографическими механизмами обеспечения конфиденциальности и целостности компьютерных данных. Их инициализирующей основой, как уже отмечалось, являлись потребности в защите передаваемых данных по «гражданским» информационно-телекоммуникационным сетям, процессы создания которых активно развивались в то время.

В 1973 г. национальным бюро стандартов США был объявлен конкурс на разработку алгоритма шифрования данных, который мог бы быть эффективно реализован в текущих и перспективных параметрах электронной элементной базы, применяемой в компьютерных системах и сетях передачи данных. Алгоритм Lucifer, представленный IBM, основанный на более раннем алгоритме Хорста Фейстеля, был признан победителем. Агентство национальной безопасности (АНБ) США «помогло усовершенствовать» алгоритм, и в 1977 г. он был утвержден правительством США как официальный стандарт алгоритма симметричного шифрования данных под наименованием DES (Data Encryption Standard).

Трудно переоценить значение опубликования алгоритма DES для развития современной криптографии. По сути, это был первый в истории случай следования т. н. принципу Керкхофа[5], в результате которого в сферу анализа стойкости и создания новых криптоалгоритмов было вовлечено огромное количество «гражданских» математиков всего мира.

Однако применение в компьютерных сетях таких «быстрых» и надежных (по тем временам) алгоритмов шифрования данных, как DES, натолкнулось на неразрешимую проблему. Абонентами сетей является большое количество пользователей, разделенных

территориально. Для реализации в таких сетях симметричных криптоалгоритмов шифрования данных необходимо для каждой пары абонентов разделить (доставить обоим абонентам) общий секретный ключ шифрования.

Способ разрешения этой теоретико-прикладной проблемы предложили в 1975 г. американские математики У. Диффи и М. Хелманн на основе выдвинутого ими предположения (и не доказанного строго до сих пор) о существовании т. н. «односторонних функций»[6]. Несмотря на отсутствие строгого доказательства «односторонности» каких-либо конкретных функций, рассматривались различные виды функций, «претендующих» на такую «односторонность», например, функции модульного экспоненцирования[7] ($y = e^x \bmod p$). В 1976 г. У. Диффи и М. Хелманн с учетом работ Р. Меркля (Ralph Merkle) предложили алгоритм для получения двумя абонентами общего секретного ключа через незащищенный канал связи[8].

Так было положено начало новой т. н. «асимметричной» криптографии.

Однако при всех своих новаторских достоинствах алгоритм Диффи — Хелманна — Меркля обладал весьма существенным для практического использования недостатком — он был не защищен от злоумышленника, способного в канале связи перехватывать и подменять обмен сообщениями.

После внимательного изучения данного алгоритма Р. Райвест (Ronald Linn Rivest), А. Шамир (Adi Shamir) и Л. Адлеман (Leonard Adleman) из Массачусетского технологического института в 1977 г. предложили алгоритм шифрования данных, который был предназначен для организации безопасной передачи по незащищенным каналам связи секретных сообщений, в первую очередь, секретных ключей к алгоритмам симметричного шифрования. Алгоритм, получивший по первым буквам фамилий его разработчиков название RSA, основывался также на использовании «односторонности» функции модульного экспоненцирования, и, кроме того, на «односторонности» функции произведения двух больших простых целых чисел[9].

Создание и публикация алгоритма RSA[10] сыграло без преувеличения революционную роль в развитии современной криптографии (не зря АНБ США много лет пыталось воспрепятствовать использованию алгоритма RSA неправительственными организациями). Однако значение изобретения и публикации алгоритма RSA заключалось не только в возможности создания компьютерных сетей с большим количеством пользователей, которые могут обмениваться шифрованными сообщениями. Идеи криптографии с открытым ключом были положены в основу создания технологий электронной цифровой подписи (ЭЦП), которые обеспечивают целостность передаваемых по сетям компьютерных данных и подлинность авторства передаваемых сообщений.

Возможность создания алгоритма цифровой подписи была высказана в 1975—1976 гг. теми же У. Диффи и М. Хелманном. Р. Райвест, А. Шамир и Л. Адлеман предложили для получения простых ЭЦП, передаваемых по сетям сообщений, использовать их алгоритм RSA, только, если так можно выразиться, «наоборот»[11].

Таким образом, к концу 70-х — началу 80-х гг. были разработаны доступные в «гражданской» сфере эффективные криптографические механизмы защиты информации, на основе которых стало возможным создавать защищенные компьютерные сети передачи данных.

Кроме бурных событий в сфере криптографических технологий, в определенном смысле символичным завершением второго периода развития IT-технологий и компьютерной безопасности стало опубликование в 1983 г. разработанного Национальным центром компьютерной безопасности Министерства обороны США (DoD Computer Security Center) совместно с Национальным бюро стандартов США (NBS) первого стандарта в сфере требований к защищенным компьютерным системам.

Документ, названный «Критериями оценки безопасности (надежности) компьютерных систем» (Trusted Computer System Evaluation Criteria, TCSEC), впервые в нормативно-методическом плане закрепил используемую в теоретических исследованиях и практических разработках еще с начала 70-х гг. парадигму понятия компьютерной безопасности как триады «конфиденциальность — целостность — доступность», с перечислением соответствующих требований к организации доступа к компьютерным данным, к архитектуре и механизмам функционирования компьютерных систем. Но, может быть, еще большее теоретическое и методологическое значение этого документа заключается в том, что впервые была введена порядковая шкала измерения (оценивания) безопасности компьютерных систем, используемая в оценочных стандартах безопасности и поныне.

Таким образом, к завершению второго периода истории исследований в сфере компьютерной безопасности (начало 70-х — начало 80-х гг. XX века) был создан теоретический, методический и технико-

технологический фундамент разработки и функционирования защищенных компьютерных систем и сетей передачи данных.

Середина 80-х — конец 90-х гг. XX века

Выделение четвертого этапа истории исследований в сфере компьютерной безопасности обусловлено грандиозными по масштабам IT-процессами, охватившими в этот период человеческую деятельность и человеческое общежитие[12].

С середины 80-х гг. компьютерные IT-технологии стали внедряться и применяться повсеместно. По сути, человечество «по-настоящему» стало переходить в компьютерную эру. Стремительно и практически весь объем, весь оборот информации (данных) приобрел электронную компьютерную форму, хотя хранение и оборот «бумажных» документов сохранился и применяется (чаще всего параллельно электронному) во многих учреждениях до сих пор.

В 1983г. IEEE (Институт инженеров по электротехнике и радиоэлектронике) по предложению консорциума компаний Digital, Intel и Xerox утвердил разработанный еще в 1973 г. Робертом Меткалфом из Xerox «10-Мбитный» стандарт Ethernet, предназначенный для соединения в локальные вычислительные (информационные) сети компьютеров на основе идеологии 7-уровневой модели взаимодействия открытых систем (OSI). В результате всевозможные предприятия и организации не просто «компьютеризировались», а повсеместно перешли к созданию своих внутренних (локальных) компьютерных информационных инфраструктур, в которых стал обращаться в электронной форме практически весь объем внутрикорпоративных данных, включая конфиденциальные.

Таким образом, к концу 80-х — началу 90-х гг. практически все «секреты» (и государственные, и частные) перешли в электронную компьютерную форму.

Но процесс развития IT-сферы пошел еще дальше. Можно сказать (несмотря на пафос выражения), что где-то в начале 90-х гг. XX века человечество «однажды проснулось» в новой — интернетовской — эре. «Последние мили» были преодолены, и технологии «всемирной паутины» («старые» и новые) стали доступными «обычным» людям. Этому способствовало несколько, как сказали бы раньше, «изобретений», а ныне — «инноваций».

Одним из них является гипертекст (идея о котором была высказана еще в 1945 г. советником президента Рузвельта Ваневаром Бушем, а сам термин введен в 1965 г. Теодором Нельсоном), заключающийся в снабжении обычного текста специальными отметками-отсылками по каким-либо смысловым связям или ассоциациям к другим частям данного текста или к другим текстам.

В развитии идеи гипертекста с учетом работ, проводившихся Теодором Нельсоном по созданию гипертекстовой системы Xanadu, в 1989 г. Тим Бернес-Ли из лаборатории ЦЕРН (Швейцария) написал первый в мире веб-сервер и первый веб-браузер, названный «WordWideWeb». Так было положено начало созданию «всемирной паутины».

Постепенно возникала «критическая масса» коммуникаций, программных средств представления компьютерных данных различного типа и удаленного доступа к ним. Результатом «неуправляемого» процесса развития этой «критической массы» и стала всемирная глобальная информационная инфраструктура — Интернет. В определенном смысле (в информационно-коммуникационном) расстояния между людьми перестали играть существенную роль.

С середины 90-х годов через Интернет предприятия и организации стали создавать территориально-распределенные информационно-телекоммуникационные и автоматизированные системы, в массовом порядке подключать к Интернету свои локальные сети и отдельные компьютеры. В результате через Интернет (или, как говорят в некоторых кругах, — через неконтролируемую территорию) стал передаваться и циркулировать огромный массив самых разнообразных компьютерных данных. Через Интернет появилась возможность удаленно — из другого здания, города, страны — получать доступ к данным, размещаемым во внутренних сетях и компьютерах предприятий и организаций.

Как это происходит практически всегда, с появлением новых технологий, новых средств деятельности и человеческого общежития вместе с новыми возможностями, с повышением эффективности соответствующих видов деятельности возникают и новые угрозы.

В сфере IT появились явления, относящиеся к новым видам угроз компьютерной безопасности, — компьютерные вирусы и компьютерные атаки.

Возникший первоначально еще в 1973 г. в «фантастических» фильмах термин «компьютерный вирус» официально был введен в научный и практический оборот в 1984 г. Ф. Коэном. Из «игрушек» программистов к концу 80-х гг. компьютерные программы, способные к самораспространению без ведома пользователей (посредством присоеди-

нения к каким-либо полезным программам и данным при их копирования на компьютер, через сетевые соединения) и способные производить различные деструктивные действия, превратились в одну из серьезных проблем компьютерной безопасности (вирус Jerusalem, 1987 г., «сетевой червь Мориса», 1988 г., и т. д., и т. д., и т. д.).

Массовое подключение к Интернету локальных и корпоративных сетей предприятий и организаций привело, помимо прочего, к нелегальному (незаконному, мошенническому и т. д.) доступу к их данным, ресурсам, осуществлению несанкционированных и без ведома их владельцев различных действий над ними. Одним из наиболее известных в ряду подобных событий можно назвать многочисленные нелегальные проникновения (с разными целями) во внутренние сети организаций в конце 80-х, начале 90-х годов Кевина Митника, которого ФБР США все-таки удалось в 1994 г. взять «с поличным» и привлечь к уголовной ответственности.

Примерно в эти годы появились специальные наименования для тех, кто занимается таким «неблагородным» делом, — «хакеры», появился термин «хакерские [компьютерные] атаки».

Массовое создание и распространение в 90-е годы компьютерных сетей банковских коммуникаций и услуг быстро привело на это «поле» технократов, самостоятельно либо в сообществе с теми же банковскими служащими, занимающихся, по сути, обычным мошенничеством, кражами и воровством. В этом ряду отметились и наши соотечественники в лице Владимира Левина и других ему подобных, но менее известных.

Соответственно исследования в сфере компьютерной безопасности помимо традиционных направлений, связанных с дальнейшим развитием формальных моделей безопасности, криптографических алгоритмов, стали направляться в т. ч. на «антивирусный фронт» и на теоретические основы, практические механизмы и создание систем противодействия компьютерным атакам.

В начале 90-х годов появились первые теоретические работы по анализу деструктивного программного обеспечения (по «разрушающим программным воздействиям»). В этом отношении можно отметить работы наших соотечественников С. П. Расторгуева и А. Ю. Щербакова. Были разработаны и быстро вошли в состав обязательного программного обеспечения компьютеров различные антивирусные средства, функциональность которых в большинстве случаев заключается в анализе всех программ и данных с активными элементами, установленных на компьютере, на предмет наличия в них т. н. «сигнатур», однозначно идентифицирующих вирусы и другие программы деструктивного характера.

С середины 90-гг. стали активно проводиться исследования в направлениях создания формальных моделей компьютерных атак и т. н. «вторжений» в компьютерные системы, стали разрабатываться программные инструменты их обнаружения и противодействия им — «системы обнаружения компьютерных атак (вторжений)», или иначе — «системы активного аудита».

Теоретические исследования и практические разработки в этом направлении активно проводятся в настоящее время, но можно выделить два основных подхода в этих исследованиях и, соответственно, два вида систем обнаружения компьютерных атак: исследования и системы, основанные на развитии «сигнатурного» подхода; исследования и системы на основе обнаружения т. н. «аномалий» в функционировании компьютерных сетей и систем.

Первое направление основывается на анализе журналов аудита компьютерных систем, в которых осуществляется поиск сигнатур известных атак. Соответственно, компаниями-разработчиками таких систем или независимыми организациями создаются и постоянно уточняются, пополняются банки (сигнатуры) компьютерных атак, которые периодически рассылаются организациям-«подписчикам», применяющим для защиты своих сетей системы активного аудита.

Второй подход, в свою очередь, развивается сразу по нескольким направлениям:

— на основе статистического анализа параметров (трафика, активности приложений и т. д.) функционирования компьютерной сети (для этого подобные системы развертывают в узловых элементах сети специальные программные сенсоры, называемые иногда «агентами»);

— на основе аппарата нечеткой логики, тех или иных направлений интеллектуального анализа данных (искусственного интеллекта) и т. д.

В 90-е годы продолжались исследования и в традиционных направлениях теоретических основ компьютерной безопасности — в разработке и совершенствовании моделей безопасности компьютерных систем. В частности, были развиты дискретные модели распространения прав доступа (модель TAM — типизованной матрицы доступа, R. S. Sandhu, 1992 г.), расширенная модель TAKE-GRANT (eXtended TAKE-GRANT, 1996 г., J. Frank, M. Bishop).

Последняя из упомянутых моделей посвящена в т. ч. давней и «трудной» проблеме в сфере компьютерной безопасности — «скрытым»[13] каналам утечки информации.

Еще одно направление в развитии теоретических основ компьютерной безопасности в этот период связано с расширением трактовки информационных потоков в сторону перехода от детерминированного процесса передачи символов данных к использованию теоретико-вероятностной интерпретации информации.

Были представлены теоретические работы по моделям «информационной невыводимости» и «информационного невмешательства», идеи по которым высказывались еще в работах Гогена и Мессигера. Данные модели во многих источниках относят к классу моделей безопасности информационных потоков, в которых информационные потоки трактуются как изменение вероятности состояния каких-либо объектов компьютерных систем, из чего можно «вывести» определенные конфиденциальные данные о системе или осуществить определенное воздействие («вмешательство») в функционирование системы.

В 90-е гг. к теоретическим исследованиям в сфере компьютерной безопасности присоединились отечественные специалисты, среди которых помимо упомянутых С. П. Расторгуева и А. Ю. Щербакова можно отметить А. А. Грушо, П. Д. Зегжду и многих других, «продвинувших» компьютерную безопасность в специальных областях.

И опять-таки в определенном смысле символическим окончанием обсуждаемого этапа истории исследований в сфере компьютерной безопасности можно считать принятие в 1999 г. международного стандарта ИСО/МЭК 15408-1999, посвященного критериям оценки безопасности информационных технологий (в профессиональном обиходе называемом «Общими критериями» — ОК). В этом фундаментальном нормативно-методическом документе «энциклопедически» сведены все известные на тот момент требования (механизмы) к обеспечению безопасности во всевозможных продуктах и системах IT, представлена новая концепция формирования требований безопасности к конкретным IT-продуктам — ОК — профиль защиты (ПЗ) — задание по безопасности (ЗБ); введено понятие градуированного доверия к реализации требований ЗБ (7 уровней).

Завершая «краткий курс истории» исследований в сфере компьютерной безопасности, отметим, что к концу 4-го периода (конец 90-х гг.) компьютерная безопасность обрела разработанный теоретический фундамент, превратилась в динамично развивающееся научное направление и практическую сферу деятельности.

Отметим также, что «история» компьютерной безопасности («краткая» или иная) «привязана» к развитию IT-сферы и поэтому не имеет окончания. Многочисленные ее теоретические и практические задачи «ждут» новых исследователей, разработчиков и решений.

Примечания

[1] В нашей стране закрепился термин-словосочетание — «персональная электронно-вычислительная машина» — ПЭВМ.

[2] Права доступа субъектов (пользователей) к объектам компьютерных систем задаются непосредственно путем «прописывания» разрешенных операций (прав доступа) в специальной информационной конструкции, которой математически соответствует т. н. матрица доступа на основе дискреционного принципа — для каждого субъекта (строка матрицы доступа) к каждому объекту (столбец матрицы) по каждому виду доступа (чтение, запись, выполнение); содержание ячейки матрицы доступа — права доступа соответствующего субъекта к соответствующему объекту.

[3] Изъяны безопасности в КС могут возникнуть только в результате ошибок программно-технической реализации правил модели.

[4] Скрытый канал утечки информации — механизм получения (извлечения) из защищенной КС (защищенного сегмента КС) определенных конфиденциальных данных в обход (без явного нарушения) установленных правил и процедур доступа к конфиденциальным данным.

[5] В XIX веке голландец Август Керкхоф сформулировал фундаментальное требование, предъявляемое к криптосистемам и сегодня: секретность шифра (иначе — стойкость шифрования) должна базироваться не на секретности алгоритма, а на секретности ключа шифрования.

[6] Односторонняя функция — функция, значение которой от конкретного аргумента вычисляется относительно «легко», т. е. с приемлемыми вычислительными затратами (с приемлемой сложностью), а обратная функция, вычисляющая значение аргумента по известному значению функции, характеризуется существенно большими вычислительными затратами. В литературе можно

также встретить альтернативные названия — «необратимая функция», «однонаправленная функция».

[7] Значением функции $y = e^x \bmod p$ является модуль остатка значения $y = e^x$ от p (модуль разности $|e^x - p|$, где p — некоторое целое число). На сегодняшний день иного алгоритма вычисления x при известных y и p, кроме перебора прямых подстановок, не известно.

[8] Алгоритм основывался на использовании абонентами двух чисел, например, g и p (возможно, известных злоумышленникам), генерации абонентами больших чисел — a (на стороне первого абонента) и b (на стороне второго абонента) и обменом по незащищенному каналу значениями $A = g^a \bmod p$ и $B = g^b \bmod p$, соответственно. Общим секретным ключом для шифрпереписки абонентов по какому-либо симметричному алгоритму является число $K = g^{ab} \bmod p$, которое вычисляется на первой стороне канала связи как $B^a \bmod p = g^{ab} \bmod p$, а на второй стороне как $A^b \bmod p = g^{ab} \bmod p$. Злоумышленник, знающий g и p, A и B (но не знающий чисел a и b, хранимых абонентами в секрете), при вычислении секретного ключа $K = g^{ab} \bmod p$ сталкивается с практически неразрешимой вычислительной проблемой нахождения числа a по известным A, g и p и числа b по известным B, g и p.

[9] На сегодняшний день другого алгоритма, кроме прямого перебора различных пар простых целых чисел, вычисления их произведения и соответствующей проверки (для получения значений двух простых чисел по известному их произведению), не известно.

[10] Алгоритм RSA предусматривает наличие у абонента сети пары чисел (например, e и d), которые в отношении использования их в качестве аргументов функции модульного экспоненцирования являются взаимно-обратимыми $(T^e \bmod n)^d \bmod n = T$, где T — сообщение, n — т. н. база алгоритма). Одно число из пары соответствующих чисел (например, e) публикуется (т. е. должно быть известно заинтересованным в отправлении соответствующему абоненту шифрованных сообщений) и называется «открытым» ключом. Другое число пары (d) называется «закрытым» ключом, которое абонент должен хранить втайне. Для направления этому абоненту зашифрованного сообщения необходимо отправляемое ему сообщение зашифровать на его открытом ключе $(T^e \bmod n)$. В силу односторонности функции модульного экспоненцирования злоумышленники, зная значение зашифрованного сообщения $(T^e \bmod n)$ и открытый ключ шифрования (e), при попытке получить исходное сообщение наталкиваются на непреодолимую вычислительную преграду (при вычислении d или самого сообщения T). Для расшифровки полученного шифрсообщения $T_ш = (T^e \bmod n)^d$ абоненту необходимо применить свой закрытый ключ d ($T = T_ш^d \bmod n$), отсюда название — криптоалгоритмы с «открытым ключом».

[11] Абонент, желая цифровым образом подписать отправляемое другому абоненту сообщение, шифрует его на своем «секретном» ключе и результат шифрования добавляет в конец передаваемого [открытого] сообщения, создавая тем самым цифровую подпись передаваемого сообщения. Абонент, получивший подписанное сообщение, расшифровывает ЭЦП, находящееся в конце сообщения, на открытом ключе абонента, от которого пришло сообщение. Если результат такой расшифровки идентичен полученному сообщению, то делается два вывода: сообщение подписал тот, кто владеет соответствующим секретным ключом (подтверждение подлинности автора), и то, что сообщение при передаче по [незащищенному] каналу связи не подверглось модификации (проверка целостности полученного сообщения).

Впоследствии эта технология была дополнена предварительным «сжатием» исходного сообщения в битовую строку фиксированной длины, каждый бит которой сложным образом зависит одновременно от всей совокупности бит исходного сообщения (т. н. хэш-свертка). Шифрованию на секретном ключе для получения ЭЦП подвергалось не само сообщение, а его хэш-свертка. Соответственно, проверка ЭЦП осуществлялась по идентичности результата расшифрования ЭЦП с хэш-сверткой полученного сообщения. Далее развитие технологий ЭЦП шло как по направлению разработки новых алгоритмов, так и в направлении совершенствования функций (процедур) получения хэш-сверток.

[12] В данном случае слово «общежитие» употребляется в общефилософском смысле.

[13] В нотации eXtended TAKE-GRANT — «неявным» каналам утечки информации.

ГАЙДАМАКИН Н. А., д. т. н., проф., начальник Института повышения квалификации сотрудников ФСБ России.

УДК 004.49 + 353:004.056
ББК Х401.114

А. В. Рожков

Место и роль компьютерной безопасности в системе обеспечения информационной безопасности региона

В статье рассмотрены место и роль компьютерной безопасности в системе обеспечения информационной безопасности региона, выявлены этапы и современные проблемы обеспечения компьютерной безопасности региональной информатизации.

Ключевые слова: *компьютерная безопасность, региональная информатизация, универсальная электронная карта.*

A. V. Rozhkov

Place and Role of Computer Security in Regional Information Security System

The article describes the place and role of computer security in regional information security system, stages and today's challenges of computer security for regional informatization.

Key words: *computer security, regional informatization, multiple-purpose electronic card.*

Введение

Понятие «*компьютерная безопасность*» не имеет четко очерченного значения. Это скорее некий лозунг компьютерной революции, происходящей в последние годы; удачный рекламный ход, привлекающий молодежь в эту сферу деятельности.

В то же время понятие «*информационная безопасность*» является общепринятым как в нормативно-правовой, так и технической литературе. Информационную безопасность часто подразделяют на *организационно-правовую, программно-аппаратную* и *инженерно-техническую.*

Многие специалисты в области информационной безопасности под термином «компьютерная безопасность» понимают программно-аппаратные методы защиты информации.

Но даже в таком, более узком, смысле понятие «компьютерная безопасность» весьма обширно. Оно включает использование специальных электронных и радиоэлектронных устройств, использование информации об особенностях функционирования вычислительных и телекоммуникационных систем и сетей, их операционных систем, драйверов для обеспечения информационной безопасности. Изучаются с этой целью интерфейсы пользователей, микрокоды, встроенные ассемблеры и т. д. Кроме «железа», т. е. аппаратной части, к программно-аппаратным средствам защиты информации относятся и математические методы защиты. В частности, алгоритмы функционирования защищенных систем вместе с их программно-аппаратной реализацией, а также методы и средства кодирования в них информации, в том числе криптографические алгоритмы и криптографические системы.

Следует отметить, что информация о функционировании программно-аппаратных средств защиты информации в подавляющем большинстве случаев недостаточна из-за регламентов коммерческой или служебной тайны. И что еще хуже, подавляющая часть программно-аппаратных средств имеет зарубежное происхождение, производится с ведома и под наблюдением спецслужб.

Поэтому, обсуждая проблемы компьютерной безопасности, мы существенно сузим круг рассматриваемых тем. Ограничимся теми, которые необходимо решать на уровне отдельных организаций, учреждений и на региональном уровне. К таким относятся [1]:

- Обеспечение компьютерной безопасности региональной информатизации.
- Защита информации в системах ведомственного и межведомственного элек-

тронного документооборота программно-аппаратными средствами.

- Подготовка кадров по компьютерной безопасности.
- Внедрение и адаптация свободного программного обеспечения (СПО) в системах защиты информации.
- Математические и алгоритмические проблемы компьютерной безопасности.
- Вопросы обеспечения информационной безопасности решались на государственном уровне в несколько этапов.

1.1. Этап первый. Федеральная и региональная информатизация 1995—2009 гг.

Вопросы информационной безопасности на государственном уровне стали обсуждаться с середины 90-х годов прошлого века. В 1995 г. был принят ФЗ № 24 «Об информации, информатизации и защите информации», существенно обновленный в 2006 г. К 2000 г. из закрытых в разряд гражданских были переведены специальности высшего профессионального образования блока «информационная безопасность»; утверждена «Доктрина информационной безопасности». В 2002 г. начала осуществляться Федеральная целевая программа «Электронная Россия (2002—2010 гг.)», неоднократно корректировавшаяся. Для целей электронного обмена юридически значимой информацией между федеральными и муниципальными органами власти, а также организациями и частными лицами в 2002 г. был принят ФЗ № 1 «Об электронной цифровой подписи», действие которого заканчивается 1 июля 2012 г.

Однако, применение цифровой подписи шло весьма неспешно. Тем не менее активно нарабатывалась нормативная база в области государственных стандартов. К настоящему времени утверждены около 300 ГОСТ Р «Информационная технология» и около 100 ГОСТ Р «Автоматическая идентификация», в том числе биометрическая идентификация, карты доступа. Многие из этих гостов были обновлены в 2008—2010 гг.

Новый мощный толчок реальная информатизация получила в 2006 г. с принятием закона ФЗ № 152 «О персональных данных» и «Стратегии развития информационного общества в Российской Федерации». В 2008—2009 гг. было принято около полусотни постановлений и распоряжений Правительства Российской Федерации, определяющих направление развитие федеральной и региональной информатизации, организации безбумажного документооборота и защиты информации.

Были приняты законодательные акты об обеспечении доступа к информации о деятельности властной и судебной систем Российской Федерации (ФЗ № 8 от 09.02.2009; ФЗ № 262 от 22.12.2008). В области региональной информатизации также наработана обширная нормативно-правовая база.

В обычную хозяйственную жизнь стали вторгаться высокие технологии, электроника, компьютерное программирование и секретная ранее «криптография». Следует отметить, что современная криптография (тайнопись, наука о шифрах) основана на самых абстрактных разделах математики — полях Галуа и эллиптических кривых. При помощи эллиптических кривых в 1995 г. Э. Майлс доказал знаменитую теорему Ферма. Программисты, радиоинженеры, электронщики, специалисты по компьютерной безопасности, офицеры информационной безопасности стали востребованы повсеместно.

Проблемы подготовки специалистов-технарей были подняты на самом высоком уровне на 22-м заседании Комиссии по модернизации при Президенте Российской Федерации, проходившем в г. Магнитогорске 30 марта 2011 года, где были подведены итоги работы по поддержке инженерных специальностей и технического образования [2].

Итогом первого этапа стала подготовка нормативной базы и разработка типовых программно-аппаратных решений в сфере информатизации и защиты информации.

1.2. Этап второй. Федеральная и региональная информатизация 2010—2011 гг.

В 2010—2011 гг. произошло лавинообразное обновление и создание новой нормативной базы информатизации в Российской Федерации, что наиболее концентрированно, выразилось в принятии Государственной Программы Российской Федерации «Информационное общество (2011—2020 годы)» [3, 4], ставшей развитием Федеральной целевой программы «Электронная Россия». Упор с информатизации взаимодействия государственных и муниципальных органов власти [5—10] стал делаться на информатизацию взаимодействия граждан и властных структур [11, 12]. Были приняты ФЗ № 210 «Об организации предоставления государственных и муниципальных услуг», вступающий в силу 1 июля 2011 г., и 6 апреля 2011 г. ФЗ № 63 «Об электронной подписи». Принятие этих законов повлекло значительное изменение более тридцати федеральных законов в области налогового, пенсионного и миграционного законодательства. Многие государственные и муниципальные услуги, предоставляемые

населению, получили аналог в режиме электронного межсетевого взаимодействия. Начал работу портал государственных услуг, а также порталы кадровой, правоохранительной, правовой и иной юридически значимой информации. Министерства и федеральные ведомства, а также региональные власти издали соответствующие приказы, постановления, распоряжения и т. д., посвященные тематике безбумажного взаимодействия и информирования организаций и граждан.

На втором этапе были залажены все основные технологические и организационно-правовые условия обеспечения реальной информатизации, охватывающей весь государственный механизм Российской Федерации. Однако не был решен вопрос доведения информационных услуг до конечного потребителя — гражданина Российской Федерации.

1.3. Этап третий. Универсальная электронная карта

28 февраля 2011 г. прошло заседание Комиссии по модернизации и технологическому развитию экономики России при Президенте Российской Федерации, посвященное внедрению универсальной электронной карты (УЭК) как средства предоставления государственных и муниципальных услуг населению [13]. Правительство Российской Федерации издало документы, реализующие идею УЭИ. Была определена федеральная уполномоченная организация и региональные уполномоченные организации по предоставлению государственных и муниципальных услуг с использованием универсальной электронной карты. По заявлениям граждан карты УЭК будут выдаваться с 1 января 2012 г. Карта предоставляет большие возможности ее владельцам, о чем можно узнать на сайте Федеральной уполномоченной организации ОАО «Универсальная электронная карта», чьими акционерами являются ОАО «Сбербанк России», ОАО «УРАЛСИБ», ОАО Банк «АК БАРС».

Реализация мегапроекта УЭК и ФЗ № 210 «Об организации предоставления государственных и муниципальных услуг» существенно изменила ситуацию в информатизации Российской Федерации. Теперь на законодательном уровне не осталось никаких препятствий к выходу России на передовые рубежи в области компьютеризации и информатизации всех сторон управленческой, производственной и социальной жизни общества.

Важное значение имеет также решительный поворот государства к использованию свободного программного обеспечения (СПО) [14, 15]. Подобный переход существенно сокращает расходы на информатизацию, но и поднимает планку требований к квалификации персонала.

2. Выводы

Вместе с тем использование электронных карт и осуществление платежей с использованием открытых сетей, в том числе через Интернет, таит в себе немало опасностей. В средствах массовой информации неоднократно сообщалось, что в 2010 г. граждане Российской Федерации потеряли около триллиона рублей при осуществлении подобных платежей. Это составляет примерно тысячу рублей в месяц на каждого экономически активного гражданина. Точность подобных сумм весьма спорна, но их порядок, видимо, указан точно.

В Постановлении Правительства от 24.03.2011 № 208 указаны требования к УЭК. Электронные устройства должны соответствовать тем же ГОСТам, что и привычные банковские карточки и социальные карты, внедренные во многих регионах, в том числе и в Челябинской области. Защищенность подобных карточек давно вызывает вопросы у специалистов по компьютерной безопасности.

Развитие информатизации в Российской Федерации и, в частности, в Уральском регионе ставит много фундаментальных, прикладных и инженерно-технических проблем в области компьютерной безопасности.

Прежде всего исследование реальной практики применения и функционирования внедряемых информационных и телекоммуникационных систем.

Создание математических и программных моделей функционирования этих систем.

Мониторинг, в том числе в режиме реального времени, происходящих информационно-сетевых процессов.

Создание мобильных информационно-аналитических центров, в чем-то схожих с ситуационными центрами Роскомнадзора.

Любая, даже идеально спроектированная информационная система, требует серьезной профессиональной работы в направлении ее адаптации к потребностям конкретной организационной или производственной структуры.

Весьма важен фактор квалифицированности обслуживающего персонала и его владения техническими знаниями в области компьютерной безопасности.

Проблемы аварийного восстановления систем, резервное копирование информации, противовирусное наблюдение, защита внешнего периметра сети и т. д.

Исследование, создание технического задания и отладка программно-аппаратного продукта, обеспечивающего адекватную, а не избыточную, а поэтому дорогую, ресурсоемкую и неудобную для пользователей информационную защиту.

Работа с СПО и свободно распространяемыми операционными системами.

Южно-Уральский государственный национальный исследовательский университет, как лидер региона в области инженерно-технического образования, имеет достаточно материально-технических, интеллектуальных и кадровых возможностей для решения подобного круга задач.

Примечания

[1] Приоритетные проблемы научных исследований в области обеспечения информационной безопасности Российской Федерации, утверждена Исполняющим обязанности Секретаря Совета Безопасности Российской Федерации, председателя научного совета при Совете Безопасности Российской Федерации 7 марта 2008 г.

[2] Перечень поручений Президента Российской Федерации по итогам заседания Комиссии по модернизации и технологическому развитию экономики России, состоявшегося 30 марта 2011 года, утвержден 11.04.2011.

[3] Распоряжение Правительства РФ. «О государственной программе Российской Федерации «Информационное общество (2011—2020 годы)» от 20.10.2010 № 1815-р.

[4] Распоряжение Правительства РФ. Об определении ОАО «Ростелеком» единственным исполнителем работ в рамках мероприятий государственной программы Российской Федерации «Информационное общество (2011—2020)» от 21.03.2011 № 453-р.

[5] Постановление Правительства РФ. О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов от 24.05.2010 № 365.

[6] Постановление Правительства РФ. О единой межведомственной информационно-статистической системе от 25.05.2010 № 367 (ред. от 27.12.2010 № 1152).

[7] Постановление Правительства РФ. О единой системе межведомственного электронного взаимодействия от 08.09.2010 № 697.

[8] Постановление Правительства РФ. Об утверждении положения о системе межведомственного электронного документооборота от 22.09.2009 № 754.

[9] Постановление Правительства РФ. О единой системе информационно-справочной поддержки граждан и организаций по вопросам взаимодействия с органами исполнительной власти и органами местного самоуправления с использованием информационно-телекоммуникационной сети Интернет от 15.06.2009 № 478 (ред. от 16.06.2010 № 445).

[10] Распоряжение Правительства РФ. Об утверждении плана мероприятий по переходу федеральных органов исполнительной власти на безбумажный документооборот при организации внутренней деятельности от 12.02.2011 № 176-р.

[11] Распоряжение Правительства РФ. Об утверждении сводного перечня первоочередных государственных и муниципальных услуг, предоставляемых в электронном виде от 17.12.2009 № 1993-р (ред. от 07.09.2010 № 1506-р).

[12] Распоряжение Правительства РФ. Об утверждении перечня документов (сведений), обмен которыми между органами и организациями при оказании государственных услуг и исполнении государственных функций осуществляется в электронном виде от 17.03.2011 № 442-р.

[13] Перечень поручений Президента Российской Федерации по итогам заседания Комиссии по модернизации и технологическому развитию экономики России, состоявшегося 28 февраля 2011 года, утвержден 16.03.2011.

[14] Распоряжение Правительства РФ. О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения 2011—2015 от 17.12.2010 № 2299-р.

[15] Протокол заседания Правительственной комиссии по высоким технологиям и инновациям от 01.04.2011.

РОЖКОВ Александр Викторович, родился в 1959 году. В 1976 г. окончил математический факультет ЧелГУ, д. ф.-м. н., профессор, кафедра ЦРТС, Южно-Уральский государственный университет.

ROZHKOV Aleksandr Viktorovich, born in 1959. Graduated from Mathematics Faculty of Chelyabinsk State University in 1976. Doctor of Physico-Mathematical Sciences, Professor, Chair «Digital Radio-Technical System», South Ural State University.

УДК 004.451.64
ББК Х521

Д. И. Дик, В. М. Солодовников

Кэширующий аппаратный блокиратор записи с контролем изменений

Одной из проблем проведения компьютерно-технических экспертиз является обеспечение сохранности информации в исследуемой системе. В статье предлагается новый тип аппаратного блокиратора. Данный блокиратор позволит безопасно производить расследование компьютерных преступлений на «живых» системах, а также динамически отслеживать изменения информации в них.

Ключевые слова: *аппаратный блокиратор записи, компьютерно-техническая экспертиза.*

D. Dik, V. Solodovnikov

Caching Hardware Write Blocker Device with traking changes

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. The article describes a new type hardware write blocker device. This device will allow to preserve the state of the digital crime scene during a live analysis. Also it will allow to trace dynamically changes of the information on a hard disk.

Index Terms*: hardware write blocker device, computer crime, digital investigation, computer forensic analysis, forensic bridge.*

Процесс расследования компьютерных преступлений состоит из трех основных фаз[1]:

— консервация (сохранение состояния системы);

— поиск улик;

— реконструкция событий.

Данный процесс применяется при проведении расследований как в «живых», так и в «мертвых» системах. «Живой» анализ происходит при поиске улик с использованием операционной системы или других ресурсов исследуемого компьютера. «Мертвый» анализ происходит при поиске улик с использованием доверенного стендового компьютера. При проведении «живого» анализа существует риск получения ложной информации, потому что программы, работающие в системе, могут намеренно скрывать или искажать данные. «Мертвый» анализ надежнее, но он возможен не всегда, кроме того, «мертвый» анализ в ряде случаев сложнее «живого».

В соответствии с Федеральным законом «О государственной судебно-экспертной деятельности в Российской Федерации»[2] в первой фазе расследования эксперт должен по возможности законсервировать состояние цифрового места преступления и принять меры по минимизации возможных потерь улик в ходе расследования.

При проведении «мертвого» анализа эксперт отключает систему и, как правило, создает резервные копии всех содержащихся в системе данных. Для создания копий данных системы используются либо специальные программные средства, такие, как AccessData FTK Imager[3] производства AccessData Corporation, либо утилиты общего назначения, такие, как утилита dd, входящая в состав Unix-систем. Также для создания копий применяются специальные аппаратные средства[4].

Вместо создания копий данных эксперт может воспользоваться программными или аппаратными блокираторами записи, которые не позволяют компьютеру записывать данные на устройство хранения информации.

Программные блокираторы[5] представляют собой программу, перехватывающую обращения операционной системы к устройству хранения информации. Недостатком программных блокираторов является их недостаточная надежность и возможность их обойти, например, прямой записью через контроллер управления устройством хранения информации.

Аппаратные блокираторы[6] устраняют данную проблему и представляют собой устройство, подключенное между компью-

тером и устройством хранения информации. Аппаратный блокиратор отслеживает передаваемые устройству хранения информации команды, пропуская команды чтения информации (рис. 1) и блокируя команды, приводящие к модификации информации (рис. 2).

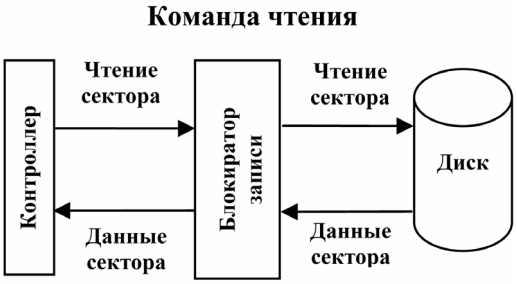

Рис. 1. Передача запроса на чтение через аппаратный блокиратор записи

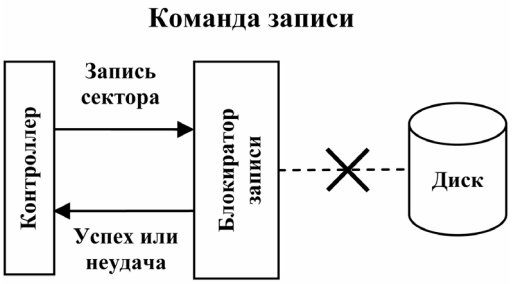

Рис. 2. Передача запроса на запись через аппаратный блокиратор записи

Блокираторы могут поддерживать разные интерфейсы передачи данных, в том числе PATA, SATA, FireWire (IEEE 1394) и USB. Группа CFTT при NIST опубликовала спецификацию тестирования аппаратных блокираторов записи[7]. В спецификации содержится классификация команд ATA. Согласно спецификации, устройство должно блокировать изменяющие команды и возвращать (не обязательно) признак успеха или неудачи.

Однако для проведения «живого» анализа применение данных средств ограничено. При создании копий информации существует возможность ее искажения. Кроме того, создание копий информации — весьма длительный процесс, что делает метод создания копий малопригодным при выполнении осмотра места компьютерного преступления. Использование аппаратных блокираторов записи в большинстве случаев приведет к ошибкам в работе операционной системы.

Для решения проблемы «живого» анализа предлагается создать кэширующий аппаратный блокиратор. Данный блокиратор должен иметь следующий алгоритм работы.

В случае поступления команды на запись кэширующий блокиратор записи просматривает имеющуюся в нем таблицу измененных секторов. Если данный сектор еще ни разу не изменялся, то блокиратор записывает его в свободную область собственного хранилища информации (диска) и добавляет в таблицу измененных секторов запись, содержащую номер сектора в исследуемом хранилище и ссылку на использованный на диске блокиратора сектор. Если сектор ранее уже изменялся, то он сохраняется на диске блокиратора по найденной ссылке на ранее сохраненный сектор (рис. 3).

При поступлении команды на чтение кэширующий блокиратор проверяет таблицу измененных секторов. В случае если в таблице содержится запись об изменении данного сектора, то сектор читается с диска блокиратора, в противном случае происходит чтение с хранилища исследуемой информации (рис. 4).

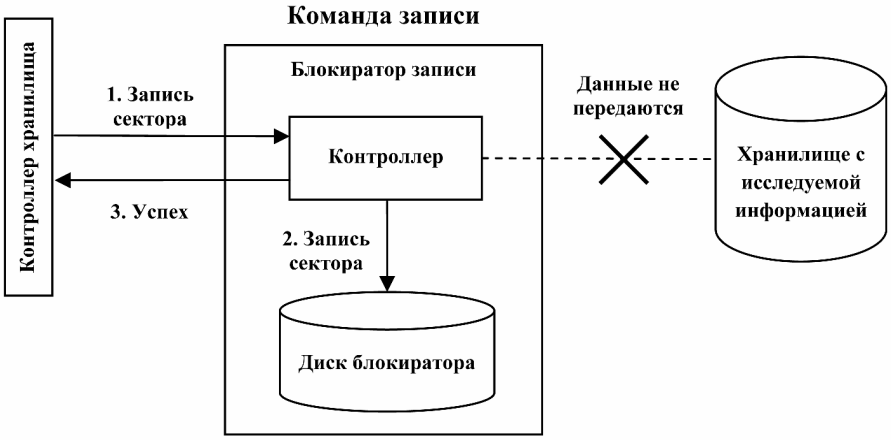

Рис. 3. Передача запроса на запись через кэширующий аппаратный блокиратор записи

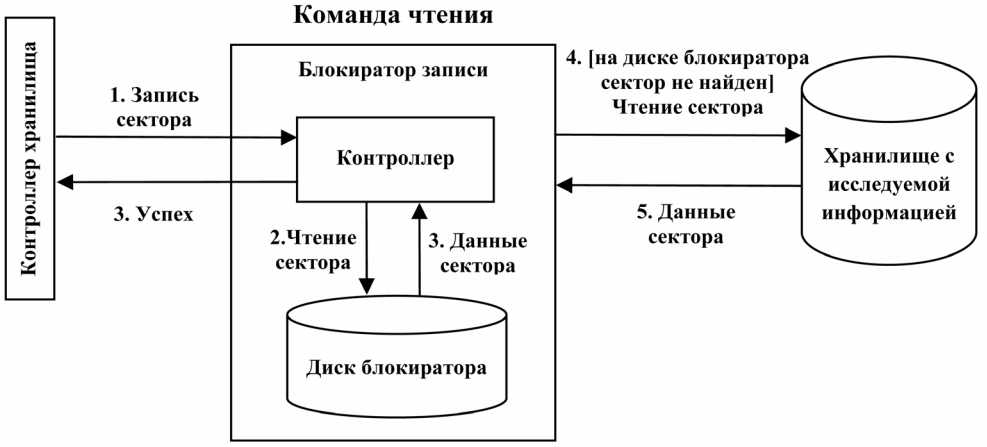

Рис. 4. Передача запроса на чтение через кэширующий аппаратный блокиратор записи

Для создания таблицы измененных секторов наиболее предпочтительным представляется использование Б-деревьев[8]. При превышении доступной оперативной памяти давно неиспользуемые узлы Б-дерева должны вытесняться на диск блокиратора. Для этого часть диска блокиратора должна выделяться для хранения узлов Б-дерева. Для отслеживания порядка использования узлов Б-дерева может использоваться список, связывающий узлы Б-дерева, загруженные в память. В данном списке узлы Б-дерева должны располагаться в порядке убывания времени обращения к ним (при обращении к узлу дерева узел переносится в начало списка; при вытеснении узла из оперативной памяти блокиратора — узел удаляется из списка; при загрузке узла дерева с диска он добавляется в список).

При наличии у блокиратора достаточно большого объема оперативной памяти часть памяти может быть использована для кэширования в ней записанных секторов.

Дополнительно предлагается оснастить блокиратор записи интерфейсом связи со стендовым компьютером эксперта. Наличие такого интерфейса позволит параллельно с «живым» анализом производить «мертвый» анализ системы, а также динамически отслеживать изменения информации в «живой» системе. Для этого контроллер блокиратора записи должен поддерживать возможность чтения данных исследуемого носителя и диска блокиратора со стендового компьютера эксперта и возможность передачи извещений на стендовый компьютер о внесенных в исследуемый носитель изменениях (рис. 5).

Стендовый компьютер эксперта должен оснащаться программным обеспечением, обеспечивающим подключение исследуемого носителя к операционной системе и позволяющим отслеживать области носителя, в которые вносятся изменения.

Применение кэширующего аппаратного блокиратора позволит безопасно производить расследование компьютерных преступлений на «живых» системах. Дополнительно данный блокиратор позволит эксперту отслеживать изменения, возникающие в исследуемом хранилище информации, что может быть полезным, например, при исследовании вредоносного программного обеспечения.

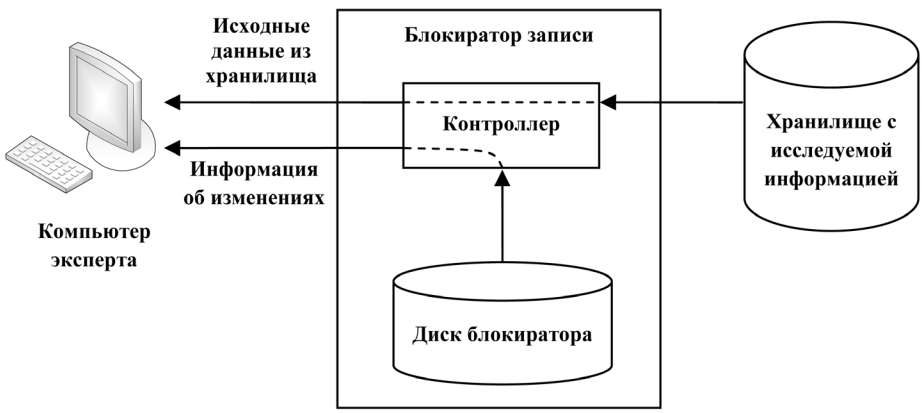

Рис. 5. Передача информации на компьютер эксперта

Примечания

[1] *Кэрриэ Б.* Криминалистический анализ файловых систем — СПб. : Питер, 2007. — С. 26—37.

[2] О государственной судебно-экспертной деятельности в Российской Федерации : федер. закон Рос. Федерации от 31 мая 2001 г. № 73-ФЗ : принят Гос. Думой 5 апреля 2001 г. : одобрен Советом Федерации 16 мая 2001 г. // Рос. газ. — 2001. — 5 июня.

[2] AccessData Product Downloads / AccessData Corporation. URL: http://www.accessdata.com/downloads.html#FTKImager (дата обращения: 24.05.2011).

[3] High Speed Drive Duplication and Forensic Acquisition / Intelligent Computer Solution. URL: http://www.ics-iq.com (дата обращения: 24.05.2011).

[4] Physical Drive BLOCKer / Digital Intelligence. URL: http://www.digitalintelligence.com/software/disoftware/pdblock/ (дата обращения: 24.05.2011).

[5] Tableau Forensic Bridges / Guidance Software Inc. URL: http://www.tableau.com/index.php?pageid=products&category=forensic_bridges (дата обращения: 24.05.2011).

[6] Hardware Write Block / National Institute of Standards and Technjlogy. URL: http://www.cftt.nist.gov/hardware_write_block.htm (дата обращения: 24.05.2011).

[7] *Т. Кормен, Ч. Лейзерсон, Р. Ривест.* Алгоритмы: построение и анализ. — М. : МЦНМО, 2001. — С. 359—375.

ДИК Дмитрий Иванович, кандидат технических наук, доцент кафедры «Безопасность информационных и автоматизированных систем» Курганского государственного университета. E-mail: ddi@kgsu.ru

DIK Dmitry Ivanovich, Candidate of Engineering Sciences, Associate Professor of the Chair «Security of Information and Automation Systems», Kurgan State University. E-mail: ddi@kgsu.ru

СОЛОДОВНИКОВ Вячеслав Михайлович, кандидат физико-математических наук, доцент, заведующий кафедрой «Безопасность информационных и автоматизированных систем» Курганского государственного университета.
E-mail: vmsolodovnikov@yandex.ru

SOLODOVNIKOV Vyacheslav Mikhailovich, Candidate of Physico-Mathematical Sciences, Associate Professor, Head of the Chair «Security of Information and Automation Systems», Kurgan State University.
E-mail: vmsolodovnikov@yandex.ru

УДК 004.056.5 + 621.39:002
ББК Ч231

Ю. Т. Карманов

Цифровые способы защиты объектов информатизации от утечек информации по каналам паразитного электромагнитного излучения

В статье анализируются перспективные способы защиты высокоскоростных систем обработки информации от утечек информации по широкополосным паразитным каналам электромагнитных излучений на основе современных достижений цифровой технологии обработки сигналов.

Ключевые слова: *утечка информации, электромагнитные излучения, цифровые технологии, обработка сигналов.*

Yu. T. Karmanov

Digital Methods for Protection of Informatization Objects against Information Leakages via Channels of Spurious Electromagnetic Emission

The author analyzes the advanced methods for protection of high-speed data processing systems against information leakages via wideband channels of spurious electromagnetic emission based on the present-day developments in the domain of signal processing digital technology.

Key words: *information leakage, electromagnetic emissions, digital technologies, signal processing.*

1. Введение

Широкое применение в системах обработки информации высокоскоростных компьютерных комплексов с использованием беспроводных технологий передачи и приема обрабатываемой информации создало проблему защиты их от утечек информации как по основным (рабочим), так и по паразитным каналам электромагнитного излучения [1, 2].

Для этих целей были разработаны организационные меры и аппаратно-программные технические средства, которые удовлетворительно защищали старое поколение систем обработки информации от утечек информации по каналам электромагнитного излучения (ЭМИ). Получили широкое применение аналоговые средства «зашумления» частотных диапазонов ЭМИ, по которым возможна утечка информации. «Зашумление» осуществляется путем генерации и излучения универсальной помехи типа «гауссовского белого шума» в защищаемом диапазоне частот. Такие устройства эффективно защищают от утечки информации по каналам паразитного излучения электромагнитных колебаний персональных компьютеров и беспроводных интерфейсов старого поколения, у которых ЭМИ сосредоточены в относительно узких частотных диапазонах, порядка нескольких сотен МГц.

Однако современные и перспективные высокоскоростные компьютерные системы и беспроводные интерфейсы работают с тактовыми частотами в десятки тысяч мегагерц, имеют высокие рабочие частоты (до 40—60тысяч мегагерц) и, соответственно, имеют очень широкие частотные диапазоны

паразитных каналов ЭМИ. Для «зашумления» таких широких частотных диапазонов ЭМИ необходимо в сотни раз расширять полосу генерируемого шума и соответственно в сотни раз увеличивать мощность излучаемой помехи. Из-за этого резко увеличиваются сложность, стоимость, габариты устройств «зашумления», резко ухудшается электромагнитная совместимость этих устройств с другими инфокоммуникационными системами, что делает их непригодными для практического использования. В связи с этим возникла необходимость разработки новых способов защиты систем обработки информации от утечек информации по паразитным каналам ЭМИ, пригодных для использования в современных и перспективных системах.

В настоящей статье описываются и анализируются перспективные способы защиты высокоскоростных систем обработки информации от утечек информации по широкополосным паразитным каналам ЭМИ на основе современных достижений цифровой технологии обработки сигналов.

2. Цифровые способы защиты систем обработки информации от утечек по каналам ЭМИ на основе цифровых устройств запоминания и воспроизведения сигналов

Маскировка («зашумление») ЭМИ используется не только в задачах защиты информации. Традиционно и широко маскировка ЭМИ применяется в радиоэлектронной борьбе (РЭБ), как способ подавления радиоэлектронных средств радиолокации, радионавигации и радиосвязи [3]. История использования этого способа в РЭБ насчитывает свыше 100 лет, и до восьмидесятых годов двадцатого века для этих целей также использовались генерация и излучение мощных широкополосных шумов [4, 5].

Однако логика развития радиоэлектронных средств (РЭС), увеличение числа РЭС, их несущих частот и ширины спектра сигналов заставили вместо генерации и излучения шумов использовать для маскировки ЭМИ защищаемые радиосигналы путем цифрового запоминания их структуры, наделения их в цифровом виде дополнительными помеховыми модуляциями и излучения их после цифроаналогового преобразования [5, 6]. Тридцатилетний опыт использования в РЭБ такого способа маскирования ЭМИ показал [6, 7, 8], что:

— таким способом достигается высокое качество маскирования ЭМИ в широком диапазоне частот при использовании передатчиков помех с мощностью на порядки меньших, чем при излучении шумов;

— осуществляется автоматическая адаптация характеристик излучаемых помех к изменениям частотной и временной структуры защищаемых сигналов и характеристик каналов ЭМИ;

— современные достижения микроэлектроники и цифровой технологии обработки широкополосных радиосигналов позволяют реализовать данный способ в виде компактных устройств (специализированные большие интегральные схемы — СБИС);

— цифровой способ маскирования ЭМИ позволяет существенно повысить электромагнитную совместимость с другими средствами за счет уменьшенной (на порядки) мощности излучаемых помех, а также за счет «экономного» излучения помех только на тех частотных составляющих спектра ЭМИ, которые совпадают с частотными составляющими спектра маскирующего сигнала.

Логично и целесообразно использовать цифровой способ маскирования защищаемых сигналов в задачах защиты информационных систем от утечек информации по паразитным каналам ЭМИ.

Рассмотрим вариант использования цифрового способа защиты на примере защиты персональных ЭВМ (ЭВМ) от утечек информации по паразитным каналам ЭМИ, обусловленными работой цифровых устройств ЭВМ.

Обобщенная схема цифровой защиты ПЭВМ приведена на рис. 1.

Согласно этой схеме ЭМИ компьютеров регистрируются приемником радиосигналов, которые после усиления, преобразования, фильтрации подаются на широкополосное цифровое устройство запоминания и воспроизведения радиосигналов (ЦУЗВ). В ЦУЗВ принятые сигналы ЭМИ преобразуются в последовательность цифровых слов и запоминаются в ОЗУ. В результате формируется подробный цифровой «портрет» ЭМИ компьютеров. В цифровом модуляторе путем дополнительной модуляции цифрового портрета, разбиения его на отдельные части и их перемешивания формируется цифровая копия маскирующего сигнала, частотная и временная структура которой совпадает со структурно-временной структурой сигнала ЭМИ. Цифровая копия маскирующего сигнала преобразуется в радиосигнал в цифро-аналоговом преобразователе (ЦАП), усиливается по мощности и излучается через антенну $А_{из}$.

В результате в паразитных каналах ЭМИ присутствует смесь сигналов ЭМИ компьютеров и сформированного маскирующего сигнала. Так как по частотной и временной структуре эти сигналы практически иден-

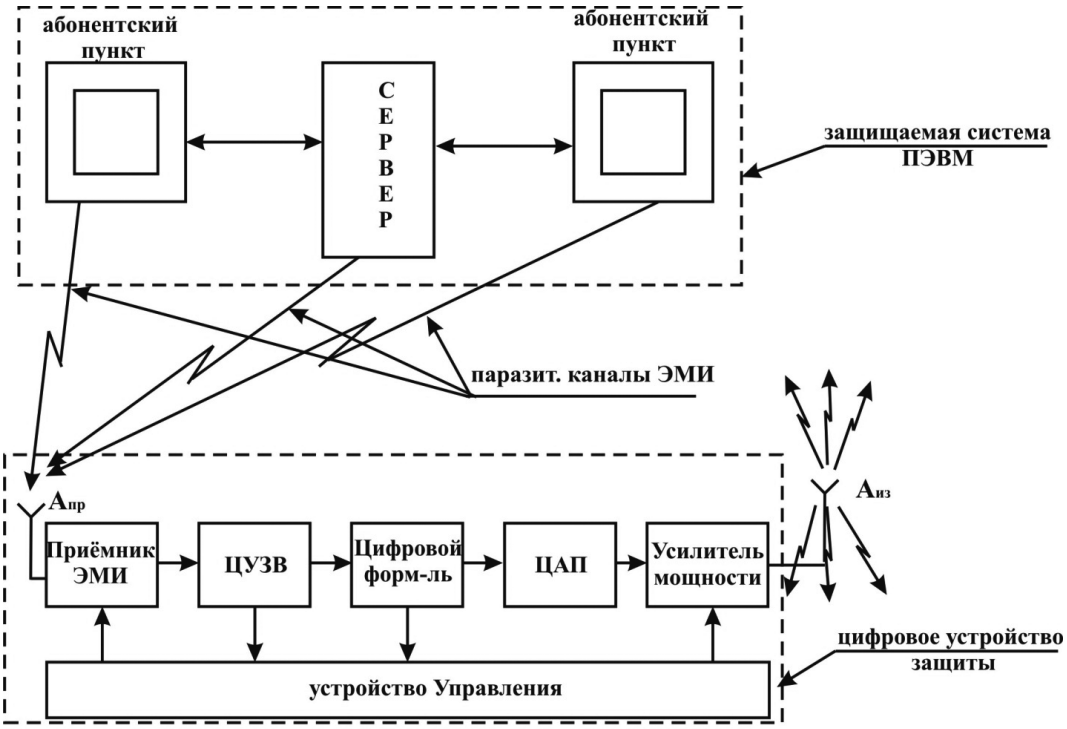

Рис. 1. Обобщенная схема цифровой защиты ПЭВМ от утечек информации по паразитным каналам

тичны, то выделить полезную информацию из этой смеси очень трудно.

Проведенные исследования показали [9], что при равенстве мощностей сигналов ЭМИ и цифрового маскирующего сигнала выделить полезную информацию из смеси невозможно.

Устройство цифровой защиты ПЭВМ периодически обновляет записанную в ОЗУ копию сигналов ЭМИ, что позволяет постоянно отслеживать изменения параметров сигналов ЭМИ и автоматически адаптировать под них частотную и временную структуру маскирующего сигнала.

На сегодняшний день на рынке интегральных схем предлагается большое разнообразие СБИС, реализующих ЦУЗВ в широком частотном диапазоне, способных производить запись сигналов ЭМИ в полосе тысяча МГц и более [8, 10].

Кроме того, на рынке предлагаются программируемые логические интегральные схемы (ПЛИС) общего назначения, на базе которых возможно создание цифровых устройств защиты с расширенным частотным диапазоном.

3. Заключение

Таким образом, на базе современных достижений микроэлектроники и цифровых технологий обработки сигналов можно создать новый класс цифровых устройств защиты систем обработки информации от утечек по паразитным каналам ЭМИ, осуществляющих маскирование сигналов ЭМИ цифровым способом на основе цифрового запоминания и воспроизведения сигналов ЭМИ.

Цифровой способ маскирования сигналов ЭМИ позволяет без увеличения габаритов и излучаемой мощности многократно увеличить полосу частот маскируемых сигналов и автоматически осуществлять адаптацию их характеристик при изменениях параметров ЭМИ защищаемой системы.

Следует отметить, что описанный цифровой метод применим для маскирования излучений не электромагнитной природы, например виброакустических излучений.

Примечания

[1] *Меньшаков Ю. К.* Защита объектов информации от технических средств разведки. — М. : Российский гос. гум. ун-т, 2002.

[2] *Куприянов А. И.* и др. Основы защиты информации. — М. : Академия, 2006.

[3] *Вакин С. А., Шустов Л. Н.* Основы радиопротиводействия и радиотехнической разведки. — М. : Сев. радио, 1968.
[4] *Любин М. Д.* Радиоэлектронная борьба в военно-воздушных силах: прошлое, настоящее и будущее // Вестник авиации и космонавтики. — 2010. — Дек.
[5] *Добыкин В. Д., Куприянов А. И., Пономарев В. Г., Шустов Л. Н.* Радиоэлектронная борьба. Цифровое запоминание и воспроизведение радиосигналов и электромагнитных волн. — М. : Вузовская книга, 2009.
[6] *Карманов Ю. Т.* 25-летний опыт применения цифровых технологий обработки радиосигналов в НИИ цифровых систем ЮУрГУ // Вестник Южно-Уральского государственного университета. Серия «Компьютерные технологии, управление, радиоэлектроника». — 2007. — Вып. 6. — № 23 (95).
[7] *Карманов Ю. Т., Рукавишников В. М.* Цифровые способы запоминания и воспроизведения радиосигналов // Цифровые радиоэлектронные системы. — 1997. — № 1. — [Электронная версия] http://www.drts.susu.ac.ru/niires/.
[8] *Карманов Ю. Т.* Проблемы цифрового запоминания и воспроизведения широкополосных СВЧ-радиосигналов // Вестник Южно-Уральского государственного университета. Серия «Компьютерные технологии, управление, радиоэлектроника». — 2004. — Вып. 3. — № 9 (38).
[9] *Карманов Ю. Т.* Маскирующая способность имитационно-шумовой помехи // Челябинский государственный технический университет : сб. научных трудов «Связь. Проблемы информационного обмена» — Челябинск, 1996.
[10] *Николаев А. Н., Лысенкова Т. А.* Компьютерная модель канала передачи и модуляции сигнала БИС 1879 ВМ3 // Цифровые радиоэлектронные системы. — 2006. — № 6. [Электронная версия] http://www.drts.susu.ac.ru/niires/.

КАРМАНОВ Юрий Трофимович, доктор технических наук, профессор, директор НИИ цифровых систем обработки и защиты информации Южно-Уральского государственного университета. E-mail: ea@drts.susu.ac.ru.

KARMANOV Yuriy Trofimovich, born in 1945, Doctor of Engineering Sciences, Professor, Director of Scientific-Research Institute of Digital Systems for Information Processing and Protection, South Ural State University. E-mail: ea@drts.susu.ac.ru.

УДК 004.7.056.5
ББК Ч231

А. С. Пономарев

Обеспечение информационной безопасности вычислительных сетей на основе имитационного подхода к их моделированию

В статье представлена виртуальная модель локальных вычислительных сетей на базе сетей Петри в совокупности с программно-аппаратной средой графического программирования LabVIEW. Данная модель позволяет определить каналы утечки информации и оценить уязвимости узлов моделируемой локально-вычислительной сети в режиме реального времени, в отличие от других моделей (OpNet), позволяющих качественно оценить параметры сети. Данная модель существенно повышает надежность всех узлов ЛВС, позволяет вести учет трафика высоконагруженных сетей в режиме реального времени.

Ключевые слова: *виртуальная модель, графическое программирование, LabVIEW, утечка информации, оценка уязвимости, учет трафика.*

A. S. Ponomaryov

Information Security of Computer Networks Based on Simulation Approach to Their Modelling

The article describes a virtual model of local area networks on the basis of Petri nets combined with firmware environment of Lab VIEW graphic programming. This model allows to detect information leakage channels and to assess vulnerability of modelled local area network on a real-time basis as opposed to other models (OpNet) allowing to efficiently evaluate the parameters of network. This model contributes to significant increase in reliability of all nodes in local area network and allows metering the traffic of highly loaded networks on a real-time basis.

Key words: *virtual model, graphic programming, Lab VIEW, information leakage, vulnerability assessment, traffic metering.*

Рост популярности интернет-технологий сопровождается ростом серьезных угроз разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т. д. Хакеры и другие злоумышленники подвергают угрозам сетевые информационные ресурсы, пытаясь получить к ним доступ с помощью специальных атак. Эти атаки становятся все более изощренными по воздействию и несложными в исполнении. Этому способствуют два основных фактора.

Во-первых, это повсеместное проникновение Интернета. К этой сети подключены миллионы компьютеров. В ближайшем будущем их число во много раз возрастет, поэтому вероятность доступа хакеров к уязвимым компьютерам и компьютерным сетям также постоянно возрастает. Во-вторых, это всеобщее распространение простых в использовании ОС и сред разработки. Этот фактор резко снижает требования к уровню знаний злоумышленника. Раньше от хакера требовались хорошие знания и навыки программирования, чтобы создавать и распространять вредоносные программы. Теперь, для того чтобы получить доступ к хакерскому сред-

ству, нужно просто знать IP-адрес нужного сайта, а для проведения атаки достаточно щелкнуть мышкой.

Проблемы обеспечения информационной безопасности в корпоративных компьютерных сетях обусловлены угрозами безопасности для локальных рабочих станций, локальных сетей и атаками на корпоративные сети, имеющими выход в общедоступные сети передачи данных.

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Одни атаки отличаются большой сложностью, другие может осуществить обычный оператор, даже не предполагающий, какие последствия будет иметь его деятельность.

Цели нарушителя, осуществляющего атаку [1]:

• нарушение конфиденциальности передаваемой информации;

• нарушение целостности и достоверности передаваемой информации;

• нарушение работоспособности всей системы или отдельных ее частей.

Распределенные системы подвержены прежде всего удаленным атакам, поскольку компоненты распределенных систем обычно используют открытые каналы передачи данных, и нарушитель может не только проводить пассивное прослушивание передаваемой информации, но и модифицировать передаваемый трафик (активное воздействие).

Трудность выявления факта проведения удаленной атаки выводит этот вид неправомерных действий на первое место по степени опасности и препятствует своевременному реагированию на осуществленную угрозу, в результате чего у нарушителя увеличиваются шансы успешной реализации атаки.

Безопасность локальной сети отличается от безопасности межсетевого взаимодействия тем, что на первое по значимости место выходят нарушения зарегистрированных пользователей, поскольку в этом случае каналы передачи данных локальной сети находятся на контролируемой территории и защита от несанкционированного подключения к которым реализуется административными методами.

На практике IP-сети уязвимы для многих способов несанкционированного вторжения в процесс обмена данными. По мере развития компьютерных и сетевых технологий (например с появлением мобильных Java-приложений и элементов ActiveX) список возможных типов сетевых атак на IP-сети постоянно расширяется.

Наиболее распространены следующие атаки:

1) подслушивание (sniffing);

2) изменение данных;

3) анализ сетевого трафика;

4) подмена доверенного субъекта;

5) посредничество;

6) посредничество в обмене незашифрованными ключами (атака man-in-the-middle);

7) перехват сеанса (session hijacking);

8) отказ в обслуживании (Denial of Service, DoS);

9) парольные атаки;

10) угадывание ключа;

11) атаки на уровне;

12) сетевая разведка;

13) злоупотребление доверием;

14) компьютерные вирусы, сетевые «черви», программа «троянский конь».

Перечисленные атаки на IP-сети возможны в результате:

1) использования общедоступных каналов передачи данных. Важнейшие данные передаются по сети в незашифрованном виде;

2) уязвимости в процедурах идентификации, реализованных в стеке TCP/IP;

3) идентифицирующая информация на уровне IP передается в открытом виде;

4) отсутствия в базовой версии стека протоколов TCP/IP механизмов, обеспечивающих конфиденциальность и целостность передаваемых сообщений;

5) аутентификации отправителя по его IP-адресу. Процедура аутентификации выполняется только на стадии установления соединения, а в дальнейшем подлинность принимаемых пакетов не проверяется;

6) отсутствия контроля за маршрутом прохождения сообщений в сети Internet, что делает удаленные сетевые атаки практически безнаказанными.

Информация, обрабатываемая в корпоративных сетях, является особенно уязвимой, чему способствуют:

1) увеличение объемов обрабатываемой, передаваемой и хранимой в компьютерах информации;

2) сосредоточение в базах данных информации различного уровня важности и конфиденциальности;

3) расширение доступа круга пользователей к информации, хранящейся в базах данных, и к ресурсам вычислительной сети;

4) увеличение числа удаленных рабочих мест;

5) широкое использование глобальной сети Internet и различных каналов связи;

6) автоматизация обмена информацией между компьютерами пользователей.

Анализ наиболее распространенных угроз, которым подвержены современные проводные корпоративные сети, показывает, что источники угроз могут изменяться от неавторизованных вторжений злоумышленников до компьютерных вирусов, при этом весьма существенной угрозой безопасности являются человеческие ошибки.

Самыми частыми и опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки пользователей, операторов и системных администраторов, обслуживающих КИС.

На втором месте по размерам ущерба располагаются кражи и подлоги. В большинстве расследованных случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и защитными мерами.

Сегодня к компьютерным сетям как к вычислительной платформе предприятия предъявляются все более жесткие требования надежности, скорости и эффективности. Сеть рассматривается как важный, иногда даже критически важный, ресурс, который должен быть использован максимально эффективно при минимальных затратах. Чаще всего к основным параметрам работы сети относят [5]:

— пропускную способность (емкость);
— скорость;
— надежность.

Высокие требования к качеству работы сети обеспечивают интерес к мониторингу и моделированию вычислительных сетей. Средства мониторинга доступны сегодня в широком ассортименте, начиная от системных консольных утилит и заканчивая программными комплексами с возможностью управления и с применением экспертных систем (*HP OpenView NNM*, *NetView* (*Tivoli*) от *IBM*, *Spectrum* от *Cabletron*). В области моделирования ВС дело обстоит иначе, поскольку здесь необходимы не только технические знания, но и понимание теоретических основ процессов передачи и обработки данных, происходящих в вычислительных сетях. К группе средств, моделирующих работу сетей, можно отнести *ComNet* от *CACI Products Company*, *OPNET* от *OPNET Technologies* (ранее — *MIL*3), *NetCracker*, *OMNeT++*, *NS-2*, *NS-3* [3]. Каждая из этих систем предназначена для решения конкретных задач разной степени абстракции. Проект *COMNET* позиционировался как система моделирования ВС с развитыми средствами визуализации и модульной структурой, позволяющей облегчить труд системных администраторов. Среди основных подсистем *COMNET* можно выделить блок стохастического моделирования, подсистему быстрого временного анализа *Predictor*, подсистему мониторинга *Enterprise Profiler*, пакет анализа производительности сети *NETWORK*. В настоящее время пакет *COMNET* не поддерживается, компания развивает симуляционный пакет *SIMPROCESS*.

Высокая стоимость, сложность внедрения и интеграции, ограниченные возможности некоторых существующих программных продуктов в совокупности с существующим спросом заставляет исследователей искать новые решения для анализа и моделирования ВС [2, 3]. Фрактальные свойства сетевого трафика исследуются в работах С. В. Ильницкого [3] и коллектива американских исследователей (M. S. Taqqu, D. V. Wilson, W. E. Leland). В Пермском государственном университете разрабатывается распределенная имитационная система Triad.Net, которая использует трехуровневое описание имитационной модели в формате M = {STR, ROUT, MES}, где STR — слой структур; ROUT — слой процедур (рутин), описывающих алгоритм взаимодействия структур, и MES — слой сообщений, которыми обмениваются структуры. Исследователи из Пензенского государственного университета (Н. П. Вашкевич, В. Н. Дубинин, С. А. Зинкин) [2] формализуют ВС с помощью языка описания сетевых моделей (ЯОСМ) и далее используют статистические методы обработки полученной модели. В ряде прочих работ используется анализ временных рядов, полученных из статистических данных о сетевом трафике, а также аппарат нейронных сетей, например, для решения задачи оптимального распределения источников трафика в корпоративной ВС.

Методология гибридного моделирования ВС на основе аналитических методов и дискретных систем подробно рассматривается в работе А. Ф. Ярославцева [4].

В настоящей статье представлен имитационный подход к моделированию ВС на базе сетей Петри, что позволяет оптимальным образом решать широкий спектр задач моделирования, используемый авторами в совокупности с программно-апаратной средой графического программирования LabVIEW.

Для решения выше обозначенных задач предлагается построение виртуальной модели, реализованной на языке графического программирования LabVIEW. Кроме того, современные вычислительные сети представляют собой достаточно громоздкую структуру, включающую не только рабочие

места пользователей, но и соединительные провода, точки доступа (концентраторы, маршрутизаторы). На крупных предприятиях количество рабочих мест может исчисляться сотнями, тысячами. Эти факторы затрудняют учет каналов утечки информации и оценки уязвимостей.

Среди основных задач, предъявляемых к информационной системе, можно выделить:

1) создание адекватных моделей ВС на основе данных трех типов:

— данные о топологии сети;

— данные о маршрутах и характеристиках потоков трафика;

— данные о вычислительных мощностях сетевых устройств;

2) аналитический расчет сетевых параметров для представленных моделей;

3) анализ полученных результатов с целью выявления «критичных» участков сети с низкой или нестабильной скоростью обработки/передачи сообщений.

Будем рассматривать вычислительную сеть, состоящую из устройств различных типов, в которой циркулируют пакеты данных. Модель вычислительной сети в общем виде можно представить в следующем виде [5] (рис. 1).

Здесь представлены основные информационные объекты и связи между ними.

Объект «Сеть» описывает реальную ВС и может включать в себя в качестве подсетей другие объекты этого типа.

Объект «Сетевое устройство» моделирует устройства, входящие в состав сети. Это абстрактный объект, функцией которого является обработка пакетов, т. е. задержка их в устройстве на некоторое время и возможная модификация пакета (например, изменение его типа). Каждый экземпляр объекта характеризуется в первую очередь значением своего параметра «тип». Типами сетевого устройства могут являться: рабочие станции, коммуникационное, периферийное оборудование, каналы передачи данных. Тип определяет конкретную структуру «Сетевого устройства».

Объект «Блок обработки пакетов» характеризует основной элемент сетевого устройства, ответственный за скорость и дисциплину обработки сетевых пакетов. Для однопроцессорных сетевых устройств «Блок обработки» моделирует работу центрального процессора и содержит данные о его мощности (в операциях в секунду). Для многопроцессорных устройств каждый «Блок обработки» характеризует один процессор. Для сетевых каналов передачи данных «Блок обработки» является виртуальным объектом и характеризует скорость передачи данных (байт(бит)/секунда). Объект «Блок приема-передачи» входят в состав «Сетевого устройства» и служит для описания входа и выхода потока сетевого трафика. Блок приема-передачи для сетевых узлов связан с их сетевыми интерфейсами. Собственно исследуемый сетевой трафик описывается объектами «Тип трафика», «Источник трафика», «Поток» и «Пакет».

Объект «Тип трафика» содержит информацию о группе потоков сообщений в сети, обладающих общими параметрами. К этим параметрам относятся:

— используемые протоколы;

— службы или приложения, создающие этот трафик (например, служебный, передача видео, ftp-трафик);

— приоритет данного типа трафика;

— коэффициент задержки, связанный с обслуживанием данного типа трафика (например, sql-запросы могут обслуживаться дольше, чем служебный трафик даже при одинаковом размере пакетов);

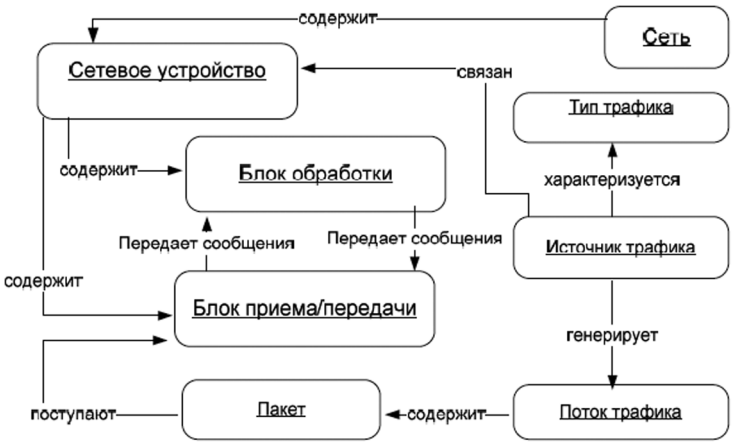

Рис. 1. Информационная модель сети

— закон распределения, характеризующий количество пакетов, сгенерированных в единицу времени;

— закон распределения, характеризующий размер пакетов, сгенерированных в единицу времени.

Объект «Источник трафика» является отправной точкой нескольких потоков однотипного трафика из одного устройства к нескольким. Источник трафика характеризуется «Блоком приема-передачи» устройства, с которым он связан, «Типом трафика» а также моментом начала генерации сообщений, который может задаваться статически или определяться в момент работы устройства. Все сообщения, сгенерированные «Источником трафика», в общем случае с различной вероятностью поступают к нескольким адресатам (если адресат один, тождественно равно 1).

Объект «Поток» служит для общего описания всех сообщений, сгенерированных одним «Источником трафика» и направленных к одному «*Блоку приема-передачи*» узла по одному маршруту, т. е. через некоторую однозначно определенную в некоторый момент времени последовательность «Сетевых устройств».

Объект «Пакет» описывает один сетевой пакет потока. Детализация до этого уровня необходима только при имитационном моделировании, поскольку ее запуск связан с отслеживанием пути каждого пакета.

Но в отличие от вышеперечисленных виртуальных (имитационных) моделей (*OPNET* от *OPNET Technologies* (ранее — *MIL*3), *NetCracker*, *OMNeT++*, *NS*-2, *NS*-3, позволяющих рассчитывать параметры сети, а затем сравнивать их с реальными физическими параметрами), предлагаемая модель оперирует параметрами реальных физических устройств, т. е. данная информационная модель работает в режиме реального времени. Данное обстоятельство позволяет существенно повысить точность измерения параметров объектов вычислительной сети.

Примечания

1. *Дубинин В. Н.* Организация и проектирование интеллектуальных распределенных вычислительных систем с групповыми взаимодействиями // Вычислительная техника в автоматизированных системах контроля и управления : межвуз. сб. науч. тр. — Пенза : ПГУ, 1999. — Вып. 26. — С. 31—38.
2. *Котов В. Е.* Сети Петри. — М. : Наука, 1984.
3. *Питерсон Дж.* Теория сетей Петри и моделирование систем. — М. : Мир, 1984.
4. *Ярославцев А. Ф.* Методы и программные средства гибридного моделирования мультисервисных сетей большой размерности : дис. … докт. техн. наук. — Новосибирск, 2006.
5. *Гудов А. М., Семехина М. В.* Имитационное моделирование процессов передачи трафика в вычислительных сетях. — Кемерово : Кемеровский государственный университет. — Управление большими системами. — Вып. 31. — 2008.

ПОНОМАРЕВ А. С., аспирант кафедры «Информационная безопасность» ЮУрГУ.

PONOMARYOV A. S., Postgraduate Student of the Chair «Information Security», South Ural State University.

УДК 342.51:004.056
ББК Х401.011.2

П. А. Мигунова

Проблемы обеспечения безопасности персональных данных в органе исполнительной власти субъекта Российской Федерации, осуществляющем переданные полномочия в области содействия занятости населения

В статье рассмотрены некоторые проблемы обеспечения безопасности персональных данных в органе исполнительной власти субъекта Российской Федерации, осуществляющем переданные полномочия в области содействия занятости населения: передачи регистров получателей, содержащих ПДн, в необезличенном виде; межведомственного взаимодействия при обработке персональных данных субъектов; классификации ИСПДн, содержащей электронные обращения и определение достоверности сведений, указанных в этих обращениях.

Ключевые слова: *персональные данные, безопасность ИСПДн, защита, занятость населения.*

P. A. Migunova

Problems of Personal Information Security in Executive Body of Constituent of the Russian Federation Exercising Powers of Population Employment Promotion

The article describes some problems of personal information security in executive body of constituent of the Russian Federation exercising powers of population employment promotion: transfer of registers of receivers containing personal information in impersonal form; interdepartmental interaction in the course of processing of personal information of subjects; classification of personal information system containing electronic references and verification of adequacy of data specified in these references.

Key words: *personal information, security of personal information system, protection, population employment.*

В связи с тем, что орган исполнительной власти субъекта Российской Федерации, осуществляющий переданные полномочия в области содействия занятости населения (далее — Главное управление), занимается оказанием государственных услуг и осуществляет подготовку сведений, необходимых для формирования регистров получателей государственных услуг в сфере занятости населения, в учреждении циркулирует большой объем информации ограниченного доступа, который согласно законодательству относится к персональным данным. В связи с этим возникает вопрос: является ли Главное управление полноценным оператором персональных данных? Согласно Федеральному закону «О персональных данных» оператором является «государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных». Цели и содержание обработки персональных данных в Главном управлении определяет заказчик (Федеральная служба по труду и занятости (далее — Роструд)). Он же ставит цели перед исполнителем и определяет содержание обработки ПДн. Главное управление получает исходные данные (ПДн по-

лучателей государственных услуг в области содействия занятости населения) от исполнителя (Государственного учреждения Центра занятости населения (далее — ГУ ЦЗН)), выполняет с ними определенные действия, предусмотренные Законом «О занятости населения в РФ», нормативными актами Правительства РФ, Министерства здравоохранения и социального развития Российской Федерации и Роструда, регламентами оказания государственных услуг, законодательством и правовыми актами региональных органов власти и управления, и передает в Росструд результаты своей работы. Оператором и исполнителем является ГУ ЦЗН, заказчиком является Роструд. Кем же является тогда Главное управление?

В европейском праве к таким исполнителям, как Главное управление, применяется термин «обработчик». Это физическое или юридическое лицо, официальный орган, агентство или иной орган, который обрабатывает персональные данные по поручению оператора. Под «третьей стороной» в европраве понимается любое лицо кроме субъекта данных, оператора, обработчика и лиц, которые уполномочены обрабатывать данные с прямой санкции оператора или обработчика. Кроме этого, введено определение «получатель», означающий любое лицо, которому раскрываются данные, при этом органы власти получателями не считаются.

Поэтому, с точки зрения европрава, Главное управление в приведенном выше примере является «третьей стороной» и обработчиком персональных данных субъектов, а значит, оператор, отдавший часть своих процессов обработчику, может не сообщать об этом субъекту ПДн в принципе и, соответственно, не брать у него никакого согласия. При этом европраво предполагает, что за все действия, приведшие к нарушению прав субъекта ПДн, совершенные обработчиком, несет ответственность именно оператор, поэтому последнему приходится серьезно потрудиться над полнотой и качеством требований, касающихся обеспечения безопасности процессов обработки и конфиденциальности ПДн.

В российском законодательстве сделана робкая попытка разделить функции «обработчика» и «оператора»: в ч. 4 ст. 6 152-ФЗ. Кроме того, в п. 10 постановления Правительства № 781 есть формулировки, позволяющие оператору на основании договора поручать обработку ПДн «уполномоченному лицу». Однако четкие определения «обработчик» и «получатель» в законодательстве, увы, отсутствуют.

Поэтому Главное управление, с одной стороны, считается «третьей стороной», а с другой — все тем же оператором ПДн, со всеми вытекающими из этого определения обязанностями.

Рассмотрим порядок получения и передачи персональных данных получателей государственных услуг в области содействия занятости населения.

Основанием для начала предоставления государственной услуги содействия в поиске подходящей работы является личное обращение гражданина в ГУ ЦЗН. При обращении в ГУ ЦЗН гражданина работник ГУ ЦЗН проверяет наличие документов и на основании заявления-анкеты и документов, представленных гражданином, осуществляет регистрацию гражданина. Регистрация граждан осуществляется в электронном виде в регистре получателей государственных услуг в сфере занятости населения (банке работников) с использованием единого программно-технологического комплекса «Система обработки информации службы занятости населения» (СОИ СЗН). Далее ГУ ЦЗН города и области передают в Главное управление сведения о получателях государственных услуг в сфере занятости населения (физических лиц и работодателей) (далее — сегменты регистров получателей) ежемесячно, в соответствии с Приказом о порядке ведения регистров получателей государственных услуг в сфере занятости населения (физических лиц и работодателей), включая порядок, сроки и форму представления в них сведений (от 8 ноября 2010 г. № 972н). Главное управление в течение 5 дней после получения сегментов регистров получателей:

1. Проводит сверку сведений, содержащихся в сегментах регистров получателей, с основными показателями государственной статистической отчетности, отражающими количество учетных записей в регистрах получателей и объем оказанных услуг;

2. Осуществляет проверку, необходимую корректировку при выявлении расхождений между сведениями, содержащимися в сегментах регистров получателей, и показателями государственной статистической отчетности, отражающими количество учетных записей в регистрах получателей и объем оказанных услуг, и проводит повторную сверку сведений;

3. Формирует сводный сегмент регистров получателей субъекта Российской Федерации (далее — региональный сегмент регистров получателей).

4. Передает ежемесячно в Роструд региональные сегменты регистров получателей.

Роструд обеспечивает на правах пользователя доступ Министерства здравоохранения и социального развития Российской Федерации к сведениям, содержащимся в регистрах получателей, в соответствии с Федеральным законом «О персональных данных».

Чтобы разобраться в схеме движения информации, содержащей персональные данные в структуре органов по труду и занятости населения, необходимо выделить ИСПДн Главного управления, их назначение и характеристики. На основании закона «О персональных данных» любая информационная система персональных данных должна быть классифицирована. В соответствии с приказом Мининформсвязи/ФСТЭК/ФСБ от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» проведенная классификация ИСПДн показала, что в Главном управлении функционируют три ИСПДн:

№	Наименование ИСПДн	Описание
1	Единый программно-технологический комплекс «Система обработки информации службы занятости населения» (СОИ СЗН)	Реализация ГУ ЦЗН и Главным управлением переданных полномочий в сфере занятости населения в соответствии с Законом «О занятости населения в РФ», нормативными актами Правительства РФ, Министерства здравоохранения и социального развития Российской Федерации и Роструда, регламентами оказания государственных услуг, законодательством и правовыми актами региональных органов власти и управления
2	АИС «Регистры получателей услуг» (Рострудконтроль)	Формирование и ведение регионального сегмента регистров получателей. Предоставление доступа к Регистрам сотрудникам Главного управления и ЦЗН. Осуществление функций надзора и контроля за осуществлением органами исполнительной власти субъектов Российской Федерации переданных им полномочий в сфере занятости населения. Анализ информации в Регистрах, поддержка принятия решений.
3	1-С: «Бухгалтерия» (8 версия)	Бюджетная бухгалтерия; Зарплата и управление персоналом; СВОД отчетов

В ИСПДн 1-С: «Бухгалтерия» меры, средства и способы, применяемые для обеспечения безопасности персональных данных, являются типичными для бухгалтерских информационных систем с использованием средств автоматизации, так как бухгалтерия ведется государственными органами, органами местного самоуправления, муниципальными органами, юридическими и физическими лицами.

Необходимо отметить, что обработка ПДн получателей государственных услуг является автоматизированной, т. к. в Главное управление сегменты регистров получателей, содержащие персональные данные граждан, поступают исключительно в автоматизированном виде. ИСПДн является распределенной, так как информация, содержащая ПДн, поступает из подведомственных учреждений (ГУ ЦЗН), обрабатывается на серверах и АРМ Главного управления и передается в Роструд (рис. 1).

Рассмотрим проблемы обеспечения безопасности персональных данных, связанные со специфическими функциями Главного управления, а именно — переданными полномочиями в области содействия занятости населения:

1. Региональные сегменты регистров получателей до 2010 года передавались в Роструд в обезличенном виде, следовательно, ИСПДн присваивался 4 класс и меры по защите ПДн принимались минимальные. В соответствии с Приказом Минздравсоцразвития от 8 ноября 2010 г. № 972н региональные сегменты регистров получателей должны передаваться в необезличенном виде, что существенно повышает затраты на создание системы защиты ПДн. Согласно приказу обезличивание персональных данных применяется только при необходимости передачи данных, предоставляемых в регистр получателей, по незащищенным каналам связи.

2. В целях исполнения переданных полномочий в области содействия занятости населения государственным гражданским служащим Главного управления необходимо сверять базы данных Главного управления, содержащие массив ПДн, с базами данных Управления федеральной налоговой службы и базами данных Главного управления социальной защиты населения. Обмен этими базами данных никак не регламентирован, но необходим для выполнения возложенных

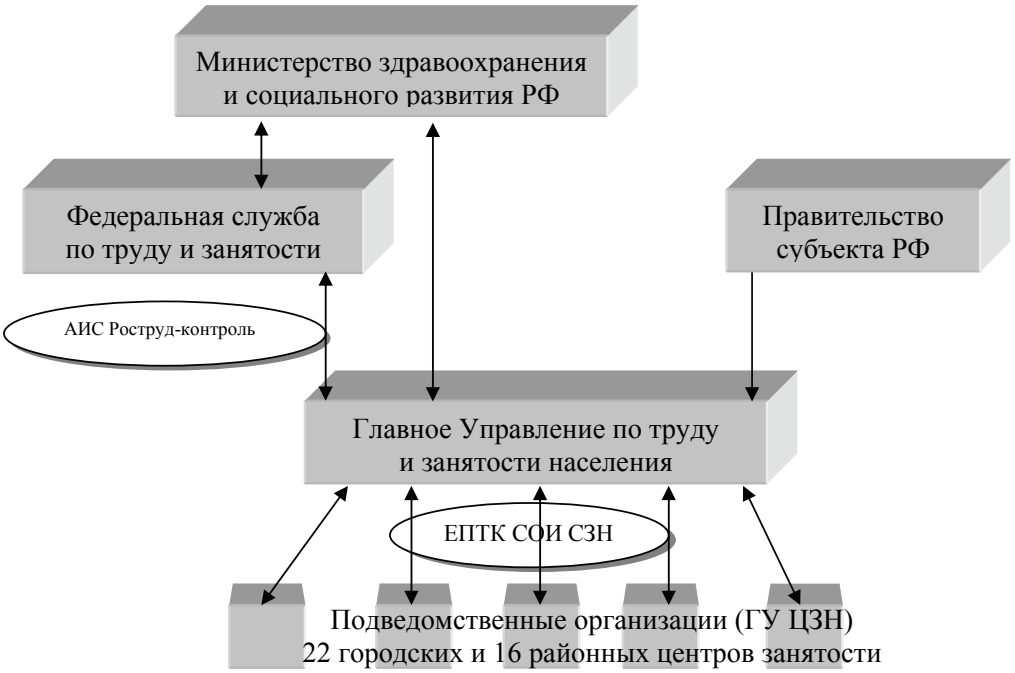

Рис. 1. Схема получения информации по каналам связи

полномочий. Из-за отсутствия регламентов, инструкций и положений об обмене информацией между этими органами возникает много проблем. В частности, несовместимость форматов баз данных из-за разного программного обеспечения (ПО), предназначенного для формирования баз данных, и различных версий этого ПО, установленного в Главном управлении, в Управлении федеральной налоговой службы и в Главном управлении социальной защиты населения.

3. Следующая проблема возникает из-за установленных в Главном управлении, Управлении Федерального казначейства и Министерстве финансов (далее — Минфин) разных версий средств защиты информации. В Федеральном казначействе и Минфине используется вторая версия средств криптозащиты, а в Главном управлении — третья версия. Так как третья версия более новая, сертификаты для третьей версии не работают на второй версии. Если же в Главное управление установить более раннюю версию, то проблемы взаимодействия будут с другими органами. Если же устанавливать более новую версию в Федеральном казначействе и Минфине, то придется переустанавливать ПО и во всех других организациях, учреждениях, предприятиях, которые взаимодействуют с этими органами, с применением этих средств криптозащиты.

4. Минздравсоцразвития посылает запросы на предоставление регистров получателей не в Роструд, а в Главное управление. Хотя в соответствии с Приказом Минздравсоцразвития от 8 ноября 2010 г. № 972н Роструд должен обеспечивать на правах пользователя доступ Министерства здравоохранения и социального развития РФ к сведениям, содержащимся в регистрах получателей.

5. Следующая проблема присуща большинству государственных органов и заключается: во-первых, в определении достоверности персональных данных, содержащихся в обращениях, так как сведения, содержащиеся в них, могут быть не подкреплены никакими документами (например, в жалобе могут быть указаны выдуманные ФИО, а могут быть указанны ФИО, паспортные данные, сведения об инвалидности, о болезнях, а также документы и материалы, содержащие эти сведения). Во-вторых, в классификации ИСПДн, содержащей обращения, ведь категория ПДн зависит от сведений, указанных субъектом в обращении, а следовательно, остается под вопросом, каким образом хранить, обрабатывать и защищать ПДн, содержащиеся в электронных обращениях, ведь эти процессы никак не регламентированы. Согласно 59-ФЗ от 02.05.2006 г. «О порядке рассмотрения обращений граждан Российской Федерации» граждане имеют право обращаться лично, а также направлять индивидуальные и коллективные обращения в Главное управление. Под обращением гражданина (далее — обращение) понимаются на-

правленные в государственный орган, орган местного самоуправления или должностному лицу в письменной форме или в форме электронного документа предложение, заявление или жалоба, а также устное обращение гражданина в государственный орган, орган местного самоуправления. Гражданин в своем обращении в обязательном порядке указывает свои фамилию, имя, отчество (последнее — при наличии), почтовый адрес, по которому должны быть направлены ответ или уведомление о переадресации обращения, излагает суть предложения, заявления или жалобы, ставит дату.

В конце хочется отметить, что Минздравсоцразвития были опубликованы Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости, включающие 26 приложений — шаблонов документов, требуемых в процессе приведения ИСПДн в соответствие с законодательством, и рекомендаций по их составлению и заполнению. Но, несмотря на это, остается много проблем в процессе создания системы защиты ПДн в Главном управлении, нами были рассмотрены только некоторые, а именно:

— проблема передачи регистров получателей, содержащих ПДн, в необезличенном виде, согласно требованиям Роструда, что существенно повышает стоимость системы защиты ПДн;

— проблема межведомственного взаимодействия при обработке персональных данных субъектов, связанная с недостаточной регламентацией передачи персональных данных и использования конкретных средств защиты;

— проблема классификации ИСПДн, содержащей электронные обращения и определение достоверности сведений, указанных в этих обращениях.

Примечания

1. «О порядке ведения регистров получателей государственных услуг в сфере занятости населения (физических лиц и работодателей), включая порядок, сроки и форму представления в них сведений»: приказ Министерства здравоохранения и социального развития Российской Федерации от 8 ноября 2010 г. № 972н.
2. Персональные данные: от Европы до России (Часть 4). [Электронный ресурс]. — Режим доступа: http://www.ispdn.info/stati/personalnie-dannie-ot-evropi-do-rossii-chast-4.html

МИГУНОВА П. А., студентка кафедры «Информационная безопасность» ЮУрГУ.

MIGUNOVA P. A., Student of the Chair «Information Security», South Ural State University.

УДК 004.056 + 368:004.056
ББК Х404.213.3 + У9(2)27:Ч23

И. И. Бухарова, В. И. Майоров

К вопросу о защите информации в страховой сфере

В статье обоснованы понятие «страхование информационных рисков», преимущества страхования как метода защиты информации, некоторые особенности деятельности по использованию этого метода на предприятиях.

Ключевые слова: *информационные риски, страхование, защита информации.*

I. I. Bukharova, V. I. Mayorov

On Information Protection in Insurance Sphere

The article justifies the concept of «insurance against information security risk», advantages of insurance as a method for information protection and some peculiarities of using this method in enterprises.

Key words: *information security risk, insurance, information protection.*

Любая предпринимательская деятельность тесно взаимосвязана с получением, накоплением, обработкой и использованием разнообразной информации. Неопределенности и риски, сопутствующие предпринимательству, являются одной из его характеризующих черт. Сегодня уровень конкурентоспособности в немалой степени зависит от умения защитить конфиденциальную информацию от хищений, несанкционированного использования, изменения или уничтожения. Опыт эксплуатации информационных систем и ресурсов в различных сферах деятельности неопровержимо показывает, что существуют различные и весьма реальные угрозы (риски) потери информации, приводящие к конкретному, материально выразимому, ущербу.

Анализ и устранение рисков невозможен без их классификации. Существуют различные виды рисков и критерии, позволяющие их классифицировать.

Традиционно выделяют внешние и внутренние риски информационной безопасности предприятия (хозяйствующего субъекта).

Из всего числа зарегистрированных и проанализированных компьютерных преступлений против банков в России 52 % было связано с хищением денежных средств, 16 % — с разрушением и уничтожением программного обеспечения компьютерной техники, 12 % — с преднамеренным искажением исходных данных, 10 % — с хищением информации и программ[1].

По оценкам экспертов, основным источником информационных угроз для банков России в начале XXI в. будет обслуживающий (в том числе и бывший) персонал (до 90 % случаев), а основными видами угроз — несанкционированный доступ и вирусы (считается, что практически все банки, без исключения, будут подвергаться вирусным атакам)[2].

Обеспечение информационной безопасности предприятия предполагает управление информационными рисками — процесс определения и использования различных контрмер, позволяющих в определенной степени прогнозировать наступление рискового события и принимать меры по снижению степени риска. Каждой разновидности рисков присущи свои методы управления.

На Западе издавна страхуются практически любые риски. По оценкам экспертов, в развитых странах Запада страхованием охвачено примерно 90—95 % всех возможных рисков, в России пока — 5—7 %. В США, например, в 1994 г. совокупная страховая премия составила огромную сумму, эквивалентную 11,4 % ВНП[3].

В России основная масса средств, выделяемых на защиту информации, тратится на выполнение мероприятий, направленных на предупреждение утечки информации. В случае же произошедшей утечки конфиденциальной информации предприятие несет материальный или моральный ущерб, при этом тратя огромные средства на локализацию последствий произошедшей утеч-

ки информации. Практика показывает, что только комплексная система защиты информации является наиболее надежной защитой секретов предприятия.

Комплексная система защиты информации должна предусматривать процедуру управления информационными рисками на предприятии. Однако методам, направленным на компенсацию ущерба при уже реализованных угрозах безопасности информации, руководителями предприятий уделяется недостаточное внимание. С другой стороны, применение методов возмещения убытков зачастую является более обоснованным с финансовой точки зрения.

Различные виды обеспечения системы защиты информации имеют свои методы и способы защиты информации. В существующих условиях развития рыночных отношений можно выделить еще один метод защиты информации в рамках финансово-экономического обеспечения системы защиты информации — *страхование информационных рисков.*

Страхование информационных рисков предприятия — это метод защиты информации в рамках финансово-экономического обеспечения системы защиты информации, основанный на выдаче страховыми обществами гарантий субъектам информационных отношений по восполнению материального ущерба в случае реализации угроз информационной безопасности.

Страхование — отношения по защите интересов физических и юридических лиц, Российской Федерации, субъектов Российской Федерации и муниципальных образований при наступлении определенных страховых случаев за счет денежных фондов, формируемых страховщиками из уплаченных страховых премий (страховых взносов), а также за счет иных средств страховщиков[4].

Правовые нормы, регулирующие страховые отношения, содержатся в нормативных актах различной отраслевой принадлежности (конституционном, административном, налоговом, экологическом и других отраслях права). Однако приоритетное значение имеют акты гражданского законодательства. Совокупность нормативных актов, содержащих страховые нормы, образует комплексное, межотраслевое по своей природе законодательство о страховании[5].

Федеральный закон «Об организации страхового дела в Российской Федерации» не содержит правил о договоре страхования[6], сохранив действие норм, регулирующих отношения, связанные с обеспечением финансовой устойчивости страховщиков и осуществлением государственных надзорных функций, за страховой деятельностью[7].

Действующий ГК РФ не предоставляет федеральному органу по надзору за страховой деятельностью прав по изданию приказов и инструкций, регламентирующих страхование. Однако эти права содержатся в Законе «Об организации страхового дела»[8]. Если орган по надзору за страховой деятельностью, действуя в пределах своих полномочий, издает акт, регламентирующий публично-правовые отношения, в которых с ним состоят страховщики, то такой акт в принципе не противоречит ГК РФ. Однако гражданско-правовые отношения в нем не могут быть закреплены.

Преимущества страхования в качестве метода защиты очевидны. Это не только способ возмещения материального ущерба. Использование страхования предполагает анализ объекта страхования, а также полный и тщательный аудит состояния системы защиты информации предприятия перед заключением договора. Причем в этом заинтересован как страхователь, которому важно не переплатить взносы, так и страховщик, который не захочет принимать на страхование «недоделанную» систему. Страхование играет и стимулирующую роль — фирма, улучшая свою систему защиты информации, получает возможность снизить свои страховые взносы.

Выигрыш от страхования информационных рисков выражается также в повышении эффективности функционирования предприятия, в результате чего возрастает доверие к нему со стороны потенциальных клиентов и партнеров. По этому параметру деятельность предприятий приближается к мировым стандартам. Кроме того, страхование информационных рисков повышает информационную прозрачность предприятий на внутреннем и внешнем рынках.

Договор страхования не только является одним из оснований возникновения страховых отношений, но и является одной из форм гражданско-правового регулирования этих отношений, отражающей основные требования законодательства о страховании.

Обычно страхование используется как дополнительная мера защиты информации. В случае если другие меры оказываются слишком дорогостоящими или непригодными, страхование используется как альтернативный метод.

После принятия решения об использовании страхования в качестве метода защиты информации специалист по защите информации (информационной безопасности) должен составить справку по объектам, подле-

жащим страхованию, рискам и возможным потерям, по вероятности реализации рисков и по размерам возможных убытков и принять решение по поводу вида страхования, типа договора, условий страхования.

Примечания

[1] ООО «Страховой Сервис» Страхование информационных рисков в кредитно-финансовой сфере деятельности [Электронный ресурс]. — Режим доступа: http://forinsurer.com/public/03/09/03/688, свободный. — Проверено 14.03.2011.
[2] Защита электронных платежей [Электронный ресурс]. — Режим доступа: http://www.lghost.ru/lib/security/kurs5/theme18_chapter03.htm, свободный. — Проверено 14.03.2011
[3] *Дьяконов Д.* Страхование информационных рисков как метод защиты информации [Электронный ресурс]. — Режим доступа: http://www.amulet-group.ru/page.htm?id=30, свободный. — Проверено 14.03.2011
[4] См. ст. 2 Федерального закона «Об организации страхового дела в РФ» от 27 ноября 1992 г. № 4015-1 // Ведомости СНД и ВС РФ. — 1993. — № 2. — С. 56.
[5] *Суханов Е. А.* Гражданское право : учебник. — Т. 2. — Полутом 1. — М. : Волтерс Клувер, 2004. — С. 347.
[6] Федеральным законом от 31 декабря 1997 г. № 157-ФЗ глава 2 ФЗ «Об организации страхового дела в РФ» от 27 ноября 1992 г. № 4015-1 исключена.
[7] См. гл. 3, 4 Федерального закона «Об организации страхового дела в РФ».
[8] См. ст. 30 Федерального закона «Об организации страхового дела в РФ».

БУХАРОВА И. И., магистр кафедры конституционного и административного права ЮУрГУ.

BUKHAROVA I. I., Master of the Chair «Constitutional and Administrative Law", South Ural State University.

МАЙОРОВ В. И., доктор юридических наук, профессор, ЮУрГУ.

MAYOROV V. I., Doctor of Law, Professor, South Ural State University

УДК 347.511:004.01.56 + 004.56.55 + 004.01.056
ББК Х404.2:Ч23

С. А. Неймышева

Основные аспекты использования электронной цифровой подписи

В современном мире все чаще используется приставка «электронный» к терминам начиная с документов и заканчивая деньгами. Все эти «электронные» составляющие нуждаются в защите от несанкционированного доступа. Развитие современных средств электронного документооборота, средств электронных платежей немыслимо без развития средств доказательства подлинности и целостности документа, которым является электронная цифровая подпись. После анализа использования электронной цифровой подписи, сделан вывод, что защита электронных документов в настоящий момент является достаточно актуальной проблемой.

Ключевые слова: *электронная цифровая подпись, электронный документооборот, защита информации, алгоритм DSA.*

S. A. Nejmysheva

The basic aspects of use of the electronic digital signature

In the modern world it is even more often used a prefix «electronic» to terms since documents and finishing money. All these «electronic» components require protection against not authorised access. Development of modern means of electronic document circulation, means of electronic payments is impossible without development of provers of authenticity and integrity of the document which the electronic digital signature is. After the analysis of use of the electronic digital signature, the conclusion is drawn, that protection of electronic documents at the moment is enough an actual problem.

Key words: *the electronic digital signature, electronic document circulation, information protection, Digital Signature Algorithm.*

Одним из средств защиты от нежелательного вмешательства является электронная цифровая подпись (ЭЦП), но не все понимают ее назначение. Слово «подпись» понятно многим: мы расписываемся на различных документах. Что же значит электронная цифровая? Это информация, преобразованная в электронный вид, передаваемая по различным сетям. Такая информация очень уязвима, а значит, нуждается в защите. Электронная цифровая подпись необходима для гарантированного подтверждения подлинности информации, содержащейся в электронном документе, а также для возможности неопровержимо доказать третьей стороне (партнеру, арбитру, суду и т. п.), что электронный документ был составлен именно конкретным лицом или по его поручению и именно в том виде, в котором он предъявлен, автору документа предлагается выбрать свое индивидуальное число (называемое обычно индивидуальным ключом [1], паролем, кодом и т. д.) и каждый раз для «цифрового подписывания» «сворачивать» (замешивать) этот свой индивидуальный ключ, хранимый в секрете от всех, с содержимым конкретного электронного документа. Результат такого «сворачивания» — другое число — может быть назван цифровой подписью данного автора под данным конкретным документом[1].

Преимущества ЭЦП:

— подпись аутентична, то есть с ее помощью получателю документа можно доказать, что она принадлежит подписывающему;

— подпись неподделываема; то есть служит доказательством, что только тот человек, чей автограф стоит на документе, мог подписать данный документ, и никто иной;

— подпись непереносима, то есть является частью документа и поэтому перенести ее на другой документ невозможно;

— документ с подписью является неизменяемым.;

— подпись неоспорима;

— любое лицо, владеющее образцом подписи, может удостовериться, что документ подписан владельцем подписи [4].

ЭЦП является таким, сохраняя основные свойства обычной подписи.

Существует несколько методов построения ЭЦП, а именно:

— шифрование электронного документа на основе симметричных алгоритмов. Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа в данной схеме является сам факт зашифрования электронного документа секретным ключом и передача его арбитру;

— использование асимметричных алгоритмов шифрования. Фактом подписания документа является зашифровка на секретном ключе отправителя;

— развитием предыдущей идеи стала наиболее распространенная схема ЭЦП — шифрование окончательного результата обработки электронного документа хэш-функцией при помощи асимметричного алгоритма [5].

Кроме перечисленных, существуют и другие методы построения схем ЭЦП: групповая подпись, неоспариваемая подпись, доверенная подпись и др. Появление этих разновидностей обусловлено разнообразием задач, решаемых с помощью электронных технологий передачи и обработки электронных документов.

Существует несколько стандартов цифровой подписи, приведем пример одного из них: алгоритм DSA.

В 1991 г. в США был опубликован проект федерального стандарта цифровой подписи — DSS (Digital Signature Standard, [DSS91], описывающий систему цифровой подписи DSA (Digital Signature Algorithm)). Одним из основных критериев при создании проекта была его патентная чистота [3].

Его надежность основана на практической неразрешимости определенного частного случая задачи вычисления дискретного логарифма. Современные методы решения этой задачи имеют приблизительно ту же эффективность, что и методы решения задачи факторизации; в связи с этим предлагается использовать ключи длиной от 512 до 1024 бит. Длина подписи в системе DSA составляет 320 бит [3].

Генерация ЭЦП в системе DSA осуществляется следующим образом.

При генерации ЭЦП используются параметры трех групп:

— общие параметры;

— секретный ключ;

— открытый ключ.

Общие параметры необходимы для функционирования системы в целом. Секретный ключ используется для формирования ЭЦП, а открытый — для проверки ЭЦП. Общими параметрами системы являются простые целые числа p, q, g, удовлетворяющие следующим условиям:

$$p: 2^{511} < p < 2^{511},$$

q: простой делитель числа (p–1), который удовлетворяет условию

$$2^{159} < q < 2^{16};$$

g: так называемый генератор, удовлетворяющий равенству

$$g = h^{\frac{p-1}{q}} \bmod p > 1.$$

Параметры p, q, g публикуются для всех участников обмена ЭД с ЭЦП. Секретный ключ x случайно выбирается из диапазона $[1, q]$ и держится в секрете.

Открытый ключ вычисляется:

$$y = g^x \bmod p.$$

Также при описании данной схемы будут использоваться следующие обозначения и дополнительные параметры: m — входное сообщение пользователя для схемы с ЭЦП; k — случайное число, удовлетворяющее условию $0 < k < q$, хранящееся в секрете и меняющееся от одной подписи к другой; H — хэш-функция, h — хэш-код сообщения.

Процесс генерации ЭЦП состоит из нескольких этапов:

1. Вычисляется хэш-код сообщения

$$m \cdot h = H(m).$$

2. Из диапазона $[1, q]$ случайным образом выбирается значение k и вычисляется

$$r = g^k \bmod.$$

3. Вычисляется $S = k^{\frac{-1}{h+xr}} \bmod q$, где k^{-1} удовлетворяет условию

$$k^{-1} \cdot k \cdot \bmod q = 1.$$

Значения r, s являются ЭЦП сообщения m и передаются вместе с ним по каналам связи [3].

Проверка ЭЦП осуществляется так.

Пусть принято сообщение m_1 и его подпись s_1, r_1.

Проверка ЭЦП происходит следующим образом:

— проверяется выполнение условий $0 < r_1 < q$, $0 < s_1 < q$, и если хотя бы одно из них нарушено, подпись отвергается.

— Вычисляются значения:

$$w = s_1^{-1} \bmod q,$$

$$u_1 = (H(m_1)w) \bmod q,$$

$$u_2 = (\frac{r_1}{w}) \bmod q,$$

$$v = ((g^{u_1} \cdot y^{u_2}) \bmod p) \bmod q,$$

— проверяется равенство $v = r_1$.

Если последнее равенство выполняется, то подпись принимается. В данном стандарте специфицируется также процедура генерации основных параметров системы и проводится доказательство того, что если $v = r_1$, то $m_1 = m$, $r_1 = r$, $s_1 = s$ [3].

Все схемы ЭЦП, известные на сегодняшний день, уязвимы.

Стойкость большинства схем ЭЦП зависит от стойкости асимметричных алгоритмов шифрования и хэш-функций.

Существует следующая классификация атак на схемы ЭЦП:

— атака с известным открытым ключом;

— атака с известными подписанными сообщениями — противник кроме открытого ключа имеет и набор подписанных сообщений;

— простая атака с выбором подписанных сообщений — противник имеет возможность выбирать сообщения, при этом открытый ключ он получает после выбора сообщения;

— направленная атака с выбором сообщения;

— адаптивная атака с выбором сообщения [2].

Каждая атака преследует определенную цель, которые можно разделить на несколько классов:

— полное раскрытие. Противник находит секретный ключ пользователя;

— универсальная подделка. Противник находит алгоритм, функционально аналогичный алгоритму генерации ЭЦП;

— селективная подделка. Подделка подписи под выбранным сообщением;

— экзистенциальная подделка. Подделка подписи хотя бы для одного случайно выбранного сообщения [2].

На практике применение ЭЦП позволяет выявить или предотвратить следующие действия нарушителя:

— отказ одного из участников авторства документа;

— модификация принятого электронного документа;

— подделка документа;

— навязывание сообщений в процессе передачи — противник перехватывает обмен сообщениями и модифицирует их;

— имитация передачи сообщения [5].

Также существуют нарушения, от которых невозможно оградить систему обмена сообщениями, — это повтор передачи сообщения и фальсификация времени отправления сообщения. Противодействие данным нарушениям может основываться на использовании временных вставок и строгом учете входящих сообщений.

Таким образом, защита электронных документов в настоящий момент является достаточно актуальной проблемой. Для того чтобы электронная цифровая подпись была доступна, а ее использование понятно каждому пользователю, который работает с электронными документами, необходимо упростить процедуру получения и использования электронной подписи. А также проинформировать каждого пользователя о такой возможности, как защита электронных документов с помощью электронной подписи, которая имеет такую же юридическую силу, как и «собственноручная» подпись. Защищенный документооборот поможет сэкономить время и денежные средства пользователей.

Примечания

1. *Анин Б. Ю.* Защита компьютерной информации. — СПб., 2001.
2. *Мамаев М. А., Петренко С.* Технологии защиты информации в Интернете: спец. справ. — СПб. : Питер, 2002.
3. *Нечаев В. И.* Элементы криптографии : Основы теории защиты информации : учеб. пособие. — М. : Высш. шк., 2001.
4. *Степанов Е. А., Корнеев И. К.* Информационная безопасность и защита информации : учеб. пособие — М. : ИНФРА-М, 2001.

5. *Хорев А. А.* Защита информации от утечки по техническим каналам : учеб. пособие. — Ч. 1 : Технические каналы утечки информации. — М. : Гостехкомиссия России, 2006.

НЕЙМЫШЕВА Светлана Александровна, аспирант, ассистент кафедры естественно-научных дисциплин, филиал УрГУПС в г. Нижний Тагил. E-mail: ksa-nt@yandex.ru

NEYMYSHEVA Svetlana Aleksandrovna, Postgraduate Student, Assistant of the Chair «Natural Science Disciplines», Branch of Ural State University of Communications, Nizhniy Tagil, E-mail: ksa-nt@yandex.ru

Правила для авторов

Редакция просит авторов при направлении статей в печать руководствоваться приведенными ниже правилами и прилагаемым образцам оформления рукописи, а также приложить к статье сведения о себе.

Структура статьи (суммарный объем статьи — не более 40 000 знаков):

1. УДК, ББК, название (не более 12—15 слов), список авторов.
2. Аннотация (не более 500 знаков, включая пробелы), список ключевых слов.
3. Основной текст работы.
4. Примечания

Объем статьи не должен превышать 40 тыс. знаков, включая пробелы, и не может быть меньше 5 страниц. Статья набирается в текстовом редакторе Microsoft Word в формате *.rtf шрифтом Times New Roman, размером 14 пунктов, в полуторном интервале. Отступ красной строки: в тексте — 10 мм, в затекстовых примечаниях (концевых сносках) отступы и выступы строк не ставятся. Точное количество знаков можно определить через меню текстового редактора Microsoft Word (Сервис — Статистика — Учитывать все сноски).

Параметры документа: верхнее и нижнее поле — 20 мм, правое — 15 мм, левое — 30 мм.

В начале статьи помещаются: инициалы и фамилия автора (авторов), название статьи, аннотация на русском языке объемом до 50 слов, ниже отдельной строкой — ключевые слова. Инициалы и фамилия автора (авторов), название статьи, аннотация и ключевые слова должны быть переведены на английский язык.

В случае непрямого цитирования источников и литературы в начале соответствующего примечания указывается «См.:».

Цитируемая литература дается не в виде подстрочных примечаний, а общим списком в конце статьи с указанием в тексте статьи ссылки порядковой надстрочной цифрой (Формат — Шрифт — Надстрочный) (например, [1]). Запятая, точка с запятой, двоеточие и точка ставятся после знака сноски, чтобы показать, что сноска относится к слову или группе слов, например: по иску собственника[1]. Вопросительный, восклицательный знак, многоточие и кавычки ставятся перед знаком сноски, чтобы показать, что сноска относится ко всему предложению, например: …все эти положения закреплены в Федеральном законе «О ветеранах»[1].

Литература дается в порядке упоминания в статье.

При подготовке рукописи автору рекомендуется использовать ГОСТ Р 7.0.5-2008 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления» (Полный текст ГОСТ Р размещен на официальном сайте Федерального агентства по техническому регулированию и метрологии).

В конце статьи должна быть надпись «*Статья публикуется впервые*», ставится дата и авторучкой подпись автора (авторов). При пересылке статьи электронной почтой подпись автора сканируется в черно-белом режиме, сохраняется в формате *.tif или *.jpg и вставляется в документ ниже затекстовых сносок.

Обязательно для заполнения: В конце статьи (в одном файле) на русском языке помещаются сведения об авторе (авторах) — ученая степень, ученое звание, должность, кафедра, вуз; рабочий адрес, электронный адрес и контактные телефоны.

В редакцию журнала статья передается качественно по электронной почте одним файлом (название файла — фамилия автора). Тема электронного письма: Информационная безопасность

Порядок прохождения рукописи

1. Все поступившие работы регистрируются, авторам сообщается ориентировочный срок выхода журнала, в макет которого помещена работа.
2. Поступившая работа проверяется на соответствие всем формальным требованиям и при отсутствии замечаний, в случае необходимости, направляется на дополнительную экспертизу.
3. Для публикации работы необходима положительная рецензия специалиста из данной или смежной области. На основании рецензии принимается решение об опубликовании статьи (рецензия без замечаний) или о возврате автору на доработку, в этом случае рукопись может проходить экспертизу повторно. При получении второй отрицательной рецензии на работу редакция принимает решение об отказе в публикации.

ОБРАЗЕЦ

УДК
ББК

А. А. Первый, Б. Б. Второй, В. В.Третий

НАЗВАНИЕ СТАТЬИ, ОТРАЖАЮЩЕЕ ЕЕ НАУЧНОЕ СОДЕРЖАНИЕ, ДЛИНОЙ НЕ БОЛЕЕ 12—15 СЛОВ

Аннотация набирается одним абзацем, отражает научное содержание статьи, содержит сведения о решаемой задаче, методах решения, результатах и выводах. Аннотация не содержит ссылок на рисунки, формулы, литературу и источники финансирования. Рекомендуемый объем аннотации — около 50 слов, максимальный — не более 500 знаков (включая пробелы).

Ключевые слова: список из нескольких ключевых слов или словосочетаний, которые характеризуют Вашу работу

Рисунки

Вставляются в документ целиком (не ссылки). Рекомендуются черно-белые рисунки с разрешением от 300 до 600 dpi. Подрисуночная подпись формируется как надпись («Вставка», затем «Надпись», без линий и заливки). Надпись и рисунок затем группируются, и устанавливается режим обтекания объекта «вокруг рамки». Размер надписей на рисунках и размер подрисуночных подписей должен соответствовать шрифту Times New Roman, 8 pt, полужирный. Точка в конце подрисуночной подписи не ставится. На все рисунки в тексте должны быть ссылки.

Все разделительные линии, указатели, оси и линии на графиках и рисунках должны иметь толщину не менее 0,5 pt и черный цвет. Эти рекомендации касаются всех графических объектов и объясняются ограниченной разрешающей способностью печатного оборудования.

Формулы

Набираются со следующими установками: стиль математический (цифры, функции и текст — прямой шрифт, переменные — курсив), основной шрифт — Times New Roman 11 pt, показатели степени 71 % и 58 %. Выключенные формулы должны быть выровнены по центру. Формулы, на которые есть ссылка в тексте, необходимо пронумеровать (сплошная нумерация). Расшифровка обозначений, принятых в формуле, производится в порядке их использования в формуле. Использование букв кириллицы в формулах не рекомендуется.

Таблицы

Создавайте таблицы, используя возможности редактора MS Word или Excel. Над таблицей пишется слово «Таблица», Times New Roman, 10 pt, полужирный, затем пробел и ее номер, выравнивание по правому краю таблицы. Далее без абзацного отступа следует таблица. На все таблицы в тексте должны быть ссылки (например, табл. 1).

Примечания

Источники располагаются в порядке цитирования и оформляются по ГОСТ 7.05-2008.

Статья публикуется впервые
Подпись, дата

ВЕСТНИК УрФО
Безопасность в информационной сфере № 1/2011

Подписано в печать 03.05.2011. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 7,35. Тираж 300 экз. Заказ 106/259.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.