Министерство образования и науки Российской Федерации
Байкальский государственный университет экономики и права

Д.И. Сачков
И.Г. Смирнова

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВЛАСТИ

Учебное пособие

Иркутск
Издательство БГУЭП
2015

УДК 343.98(075.8)
ББК 67.408.135я7
С22

Печатается по решению редакционно-издательского совета
Байкальского государственного университета экономики и права

Издается при финансовой поддержке проекта «Повышение эффективности уголовного судопроизводства по делам о киберпреступлениях для обеспечения национальной безопасности», выполняемого в рамках гранта Президента Российской Федерации для государственной поддержки молодых российских ученых – докторов наук (конкурс МД-2014) на 2014–2015 годы (договор № 14.Z56.14.2691-МД).

Рецензенты канд. физ.-мат. наук, доц. В.В. Братищенко
д-р юрид. наук, проф. А.А. Протасевич

Сачков Д.И.
С22 Обеспечение информационной безопасности в органах власти : учеб. пособие / Д.И. Сачков, И.Г. Смирнова. – Иркутск : Изд-во БГУЭП, 2015. – 122 с.

ISBN 978-5-7253-2807-3

Анализируется правовая и техническая характеристики основ обеспечения информационной безопасности в современном обществе, а также теория защиты информации. Раскрывается понятие информационной безопасности, дается классификация нормативно-правовых актов, регулирующих общественные отношения в сфере обеспечения информационной безопасности, и описание компьютерных преступлений и проблем производства по уголовным делам о киберпреступлениях.

Для научных сотрудников, преподавателей, учителей, аспирантов, студентов магистратуры и бакалавриата, школьников, интересующихся проблемами информационной безопасности.

УДК 343.98(075.8)
ББК 67.408.135я7

ISBN 978-5-7253-2807-3

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Широкое распространение и относительная дешевизна средств вычислительной техники и сведений о методах добычи информации привели к тому, что угроза в отношении конфиденциальной информации со стороны отдельных злоумышленников и организованных преступных группировок к настоящему времени уже может быть сравнима с угрозой информации, составляющей государственную тайну, со стороны иностранных технических разведок.

Стремительное развитие и внедрение информационных технологий оказывают возрастающее влияние на все стороны жизни государства и общества. Социальная, политическая, экономическая и военная сферы находятся в прямой зависимости от работы вычислительных и информационных сетей, систем связи, управления и разведки, составляющих техническую базу информационного пространства России.

Вместе с тем по мере развития этой базы повышается и уязвимость информационного пространства. Главными причинами этого являются широкое использование для обработки информации средств вычислительной техники с программным обеспечением, позволяющим сравнительно легко модифицировать, копировать и разрушать обрабатываемую информацию, а также легкость доступа к современным открытым информационно-телекоммуникационным системам.

В этой связи в последнее время во всем мире, и в частности в России, растет число преступлений, связанных с применением компьютерной техники. Информационное пространство России включает в себя федеральный и региональный компоненты. Причем эти компоненты взаимосвязаны самым тесным образом и построены зачастую с использованием сходных технических средств.

Широкое использование современных информационных технологий для обработки конфиденциальной информации создает серьезный источник угроз региональной информационной безопасности. Так, для преступных сообществ большой интерес представляет информация правоохранительных органов и финансовых структур. Специфической особенностью здесь является то, что во многих случаях невозможно обеспечить выполнение строгих режимных и организационных мер.

В связи с этим задача по защите конфиденциальной информации очень важна и требует высокой квалификации и значительного опыта. К сожалению, это часто недооценивается, что приводит к напрасным тратам, а порой и к негативным последствиям.

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Понятие информационной безопасности и ее составляющие в Российской Федерации

Информационная безопасность (ИБ) является неотъемлемой составной частью общей проблемы безопасности, роль и значимость которой во всех сферах жизни и деятельности общества и государства на современном этапе неуклонно возрастают. С повышением значимости и ценности информации растет и важность ее защиты. Обеспечение ИБ, безопасности информации и защиты информации – это стратегические сферы интересов любого развитого общества.

Анализ положения дел в рассматриваемой области сегодня позволяет сделать вывод о том, что в настоящее время одними из главных стратегических национальных ресурсов, основой экономической и оборонной мощи России являются информация и передовые ИТ, ценность которых порой превышает стоимость информационно-телекоммуникационных систем, где они обрабатываются. Распределение, использование и защита информации стали функциями нашего государства.

В то же время в России усиливается интенсификация процессов информатизации различных сфер деятельности в связи с тем, что информационные ресурсы, ИТ и информационная инфраструктура в совокупности образуют глобальную информационную среду нашего общества. Вопросы безопасности информации представляют собой важную часть процесса внедрения новых ИТ во все сферы жизни общества.

Кроме того, широкомасштабное использование вычислительной техники и телекоммуникационных систем в рамках территориально распределенных информационных систем, переход на этой основе к безбумажной технологии, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости [13]. Повышается роль самой информации и, соответственно, ее безопасности в эффективном обеспечении жизнедеятельности личности, общества и государства, реализуемая в процессах информатизации и информационного управления, так как информационный сектор экономики (т.е. информация, знания, информационные услуги) большинства стран растет в целом быстрее, чем экономика.

Отказ от традиционных бумажных технологий и переход к автоматизированным (безбумажным) технологиям обработки информации способствуют повышению производительности труда и т.д., но в то же время увеличивают информационные риски. Эти риски не связаны с конкретными угрозами информации. Развитие технологий, расширение покрытия телекоммуникационных сетей порождают все новые виды угроз.

Развитие информационных технологий изменило объем и важность информации, обрабатываемой в технических средствах обработки и передачи, что в свою очередь приводит к росту рисков нарушения ее целостности, конфиденциальности и доступности. Повсеместное внедрение информационных технологий (ИТ) в основные сферы деятельности государства увеличило число внутренних и внешних угроз безопасности сраны. Расширился спектр нетрадиционных каналов утечки информации и несанкционированного доступа к ней.

Помимо роста видов возможных угроз увеличился и размер причиненного ущерба субъектам информационных отношений при использовании ИТ, обеспечивающих хранение, передачу и защиту обрабатываемой в них информации.

В связи с ухудшающейся ситуацией международной обстановки следует ожидать рост деятельности разведывательных служб иностранных государств в отношении РФ в целях получения информации.

В настоящий момент наблюдается рост несанкционированного доступа к информации населения вследствие доступности ему средств вычислительной техники и отсутствия грамотности в области пользования информационными технологиями.

Статистика деятельности Управления ФСТЭК России в области контроля состояния защиты информации органов власти субъектов РФ показывает, что большинство современных ИТ, используемых органами власти, достаточно уязвимы ввиду недостаточности применяемых методов защиты информации. Как показывают исследования, более 80 % угроз исходят от пользователей-сотрудников, значит, для снижения рисков информационных угроз необходимо повышать их грамотность в области информационных технологий.

Необходимо рассмотреть базисные понятия в области информационной безопасности. Понятие «информация» в латинском языке (informatio) означает «разъяснение, изложение, сведения», передаваемые людьми устно, письменно или другим способом (с помощью условных сигналов, технических средств и т.д.).

В словаре русского языка С.И. Ожегова информация – это «сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством» [30].

В Федеральном законе РФ «Об информации, информационных технологиях и о защите информации» информация толкуется следующим образом: «сведения (сообщения, данные) независимо от формы их представления».

Согласно ГОСТ 7.0-99 под информацией понимаются сведения, воспринимаемые человеком и (или) специальными устройствами, как отражение фактов материального или духовного мира в процессе коммуникации.

Информация – сведения и сообщения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Сведения – форма существования информации, представляющая собой результат отражения в организме человека движения объектов материального мира. Сведения – основной инструмент познания человеком окружающей действительности.

Сообщения – форма существования информации, обладающая свойством (-вами) материальности, объективности, уничтожимости, статичности, ограниченной воспроизводимости, копируемости, представляющая собой упорядоченную совокупность знаков, с помощью которых сведения передаются от одного человека другому во времени и пространстве.

1.2. Угрозы безопасности информации и общие подходы к их классификации

Под ***угрозой безопасности информации*** будем понимать возникновение такого явления или события, следствием которого могут быть негативные воздействия на информацию: нарушение физической целостности, логической структуры, несанкционированная модификация, несанкционированное получение, несанкционированное размножение.

Классически считалось, что обеспечение безопасности информации складывается из трех составляющих:

– конфиденциальности;

– целостности;

– доступности.

Точками приложения процесса защиты информации к информационной системе являются аппаратное обеспечение, программное обеспечение и обеспечение связи (коммуникации). Сами процедуры (механизмы) защиты разделяются на защиту физического уровня, защиту персонала и организационный уровень.

В Российской Федерации к **нормативно-правовым актам в области информационной безопасности** относятся:

– акты федерального законодательства;

– международные договоры РФ;

– Конституция РФ;

– законы федерального уровня (включая федеральные конституционные законы, кодексы);

– указы Президента РФ;

– постановления правительства РФ;

– нормативные правовые акты федеральных министерств и ведомств;

– нормативные правовые акты субъектов РФ, органов местного самоуправления и т.д.

К **нормативно-методическим документам государственных органов России** можно отнести:

– Доктрину информационной безопасности РФ;

– руководящие документы ФСТЭК (Гостехкомиссии России);

– приказы ФСБ;

– стандарты информационной безопасности, из которых выделяют: международные стандарты; государственные (национальные) стандарты РФ; рекомендации по стандартизации; методические указания.

В зависимости от приложения деятельности в области защиты информации (в рамках государственных органов власти или коммерческих организаций) сама деятельность организуется специальными государственными органами (подразделениями) либо отделами (службами) предприятия.

Государственные органы РФ, контролирующие деятельность в области защиты информации:

– комитет Государственной Думы по безопасности;

– Совет безопасности России;

– Федеральная служба по техническому и экспортному контролю (ФСТЭК России);

– Федеральная служба безопасности Российской Федерации (ФСБ России);

– Служба внешней разведки Российской Федерации (СВР России);

– Министерство обороны Российской Федерации (Минобороны России);

– Министерство внутренних дел Российской Федерации (МВД России);

– Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Службы, организующие защиту информации на уровне предприятия:

– служба экономической безопасности;

– служба безопасности персонала (режимный отдел);

– отдел кадров;

– служба информационной безопасности.

Группы информационных угроз:

– хищение носителей;

– запоминание или копирование информации;

– несанкционированное подключение к аппаратуре;

– несанкционированный доступ к ресурсам системы;

– перехват побочных излучений и наводок.

Три типа средств:

– человек;

– аппаратура;

– программа.

К группе угроз, в реализации которых основную роль играет ***человек***, относятся:

– хищение носителей;

– чтение информации с экрана дисплея;

– чтение информации с распечаток.

К группе, где основным средством выступает ***аппаратура***, – подключение к устройствам и перехват излучений.

К группе, где основное средство – ***программа***:

– несанкционированный программный доступ;

– программное дешифрование зашифрованных данных;

– программное копирование информации с носителей.

Выделяется **четыре способа хищения информации**:

– по каналам побочных электромагнитных излучений;

– посредством негласного копирования, причем выделено две разновидности копирования: ручное (печать с экрана на принтер или

вывод из памяти на принтер или экран) и вирусное (вывод из памяти на принтер, на экран или передача информации с помощью встроенной в компьютер радиозакладки);

– хищение носителей информации;

– хищение персонального компьютера.

1.3. Классификация угроз безопасности информации по способам их возможного негативного воздействия

Информационные угрозы реализуются в виде:

– нарушения адресности и своевременности информационного обмена, противозаконного сбора и использования информации;

– осуществления несанкционированного доступа к информационным ресурсам и их противоправного использования;

– хищения информационных ресурсов из банков и баз данных;

– нарушения технологии обработки информации.

Программно-математические угрозы реализуются в виде:

– внедрения в аппаратные и программные изделия компонентов, реализующих функции, не описанные в документации на эти изделия;

– разработки и распространения программ, нарушающих нормальное функционирование информационных систем или систем защиты информации.

Физические угрозы реализуются в виде:

– уничтожения, повреждения, радиоэлектронного подавления или разрушения средств и систем обработки информации, телекоммуникации и связи;

– уничтожения, повреждения, разрушения или хищения машинных и других носителей информации;

– хищения программных или аппаратных ключей и средств криптографической защиты информации;

– перехвата информации в технических каналах связи и телекоммуникационных системах;

– внедрения электронных устройств перехвата информации в технические средства связи и телекоммуникационные системы, а также в служебные помещения;

– перехвата, дешифрования и навязывания ложной информации в сетях передачи данных и линиях связи;

– воздействия на парольно-ключевые системы защиты средств обработки и передачи информации.

Организационные угрозы реализуются в виде:

– невыполнения требований законодательства в информационной сфере;

– противоправной закупки несовершенных или устаревших информационных технологий, средств информатизации, телекоммуникации и связи.

1.4. Нарушители безопасности информации

В руководящем документе Гостехкомиссии России введено понятие модели *нарушителя* в автоматизированной системе обработки данных, причем в качестве нарушителя здесь рассматривается субъект, имеющий доступ к работе со штатными средствами системы.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами. В документе выделяются четыре уровня этих возможностей:

– самый низкий: возможности запуска задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции обработки информации;

– первый промежуточный: дополнительно к предыдущему предусматривает возможности создания и запуска собственных программ с новыми функциями обработки информации;

– второй промежуточный: дополнительно к предыдущему предполагает возможности управления функционированием системы, т.е. воздействия на базовое программное обеспечение и на состав и конфигурацию ее оборудования;

– самый высокий: определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств системы, вплоть до включения в состав системы собственных технических средств с новыми функциями обработки информации.

Предполагается, что нарушитель на своем уровне является специалистом высшей квалификации, знает все о системе, в том числе и о средствах защиты.

1.5. Происхождение угроз безопасности информации

Выделяется два значения данного параметра: случайное и преднамеренное. При этом под *случайным* понимается такое происхожде-

ние угроз, которое обусловливается спонтанными и не зависящими от воли людей обстоятельствами.

Наиболее известными событиями данного плана являются отказы, сбои, ошибки, стихийные бедствия и побочные влияния. Сущность перечисленных событий (кроме стихийных бедствий, сущность которых ясна) определяется следующим образом:

а) отказ – нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им своих основных функций;

б) сбой – временное нарушение работоспособности какого-либо элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции;

в) ошибка – неправильное (разовое или систематическое) выполнение элементом одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния;

г) побочное влияние – негативное воздействие на систему в целом или отдельные ее элементы, оказываемое какими-либо явлениями, происходящими внутри системы или во внешней среде.

Преднамеренное происхождение угрозы обусловливается злоумышленными действиями людей.

Выделяют две разновидности **предпосылок появления угроз:** объективные (количественная или качественная недостаточность элементов системы) и субъективные (деятельность разведорганов иностранных государств, промышленный шпионаж, деятельность уголовных элементов, преднамеренные или непреднамеренные действия недобросовестных сотрудников).

Перечисленные разновидности предпосылок интерпретируются следующим образом:

а) количественная недостаточность – физическая нехватка одного или нескольких элементов системы, вызывающая нарушения технологического процесса обработки информации и (или) перегрузку имеющихся элементов;

б) качественная недостаточность – несовершенство организации системы, в силу чего могут появляться возможности случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию;

в) деятельность разведорганов иностранных государств – специально организуемая деятельность государственных органов, профес-

сионально ориентированных на добывание необходимой информации всеми доступными способами и средствами.

К основным видам разведки относятся агентурная (несанкционированная деятельность профессиональных разведчиков, завербованных агентов и так называемых доброжелателей) и техническая, включающая радиоразведку (перехват радиосредствами информации, циркулирующей в радиоканалах систем связи), радиотехническую (регистрацию спецсредствами сигналов, излучаемых техническими системами) и космическую (использование космических кораблей и искусственных спутников для наблюдения за территорией, ее фотографирования, регистрации радиосигналов и получения полезной информации другими доступными способами);

г) промышленный шпионаж – негласная деятельность организации (ее представителей) по добыванию информации, специально охраняемой от несанкционированной утечки или хищения, а также по созданию для себя благоприятных условий в целях получения максимальных выгод (недобросовестная конкуренция);

д) злоумышленные действия уголовных элементов – хищение информации или компьютерных программ в целях наживы или их разрушение в интересах конкурентов;

е) действия недобросовестных сотрудников – хищение (копирование) или уничтожение информационных массивов и (или) программ по эгоистическим или корыстным мотивам, а также в результате несоблюдения установленных правил работы.

2. ТЕОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Сущность теории защиты информации, ее основные составляющие и задачи

Теория защиты информации определяется как система основных идей, относящихся к защите информации в современных системах ее обработки, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся и развивающаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

В более развернутом виде ***теория защиты*** должна:

– предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты;

– полно и адекватно отображать структуру и содержание взаимосвязей с родственными и смежными областями знаний;

– аккумулировать опыт предшествующих исследований, разработок и практического решения задач защиты информации;

– ориентировать в направлении наиболее эффективного решения основных задач защиты и предоставлять необходимые для этого научно-методологические и инструментальные средства;

– формировать научно обоснованные перспективные направления развития теории и практики защиты информации.

Сформулированным целевым назначением теории защиты предопределяется ее состав и общее содержание. Составляющими частями ее должны быть:

– полные и систематизированные сведения о происхождении, сущности и содержании проблемы защиты;

– систематизированные результаты ретроспективного анализа развития теоретических исследований и разработок, а также опыта практического решения задач защиты, полно и адекватно отображающие наиболее устойчивые тенденции в этом развитии;

– научно обоснованная постановка задачи защиты информации, полно и адекватно учитывающая текущие и перспективные концепции построения систем и технологий обработки, потребности в защите информации и объективные предпосылки их удовлетворения;

– общие стратегические установки на организацию защиты информации, учитывающие все многообразие потенциально возможных условий защиты;

– методы, необходимые для наиболее эффективного решения всех задач защиты и содержащие как общеметодологические подходы к решению, так и конкретные приложения;

– методологическая и инструментальная база, содержащая необходимые методы и инструментальные средства решения любой совокупности задач защиты в рамках любой выбранной стратегической установки;

– научно обоснованные предложения по организации и обеспечению работ по защите информации;

– научно обоснованный прогноз перспективных направлений развития теории и практики защиты информации.

2.2. Моделирование процессов защиты информации

Модели процессов защиты информации являются одним из основных элементов научно-методологического базиса защиты. Следует отметить, что так как процессы защиты информации в значительной степени определяются случайными факторами, то применяемые для их анализа и прогнозирования модели неминуемо должны иметь стохастический характер.

На сегодняшний день проблема моделирования систем и процессов защиты информации нашла довольно серьезное отражение в ряде учебных и научных изданий. В соответствии с упомянутым назначением рассматриваемой модели в ней отражаются те процессы, которые должны осуществляться в самой системе защиты. Центральным решением стратегического характера является оценка объема ресурсов, необходимых для обеспечения требуемого уровня защиты, и оптимальное их распределение, определяющими в этой модели должны быть именно процессы распределения ресурсов. Основой для ее построения являются общие цели (задачи) защиты информации и условия, в которых осуществляется защита.

Цели защиты информации в самом общем виде могут быть сформулированы как построение оптимальных систем защиты информации и организация оптимального их функционирования.

При этом понятие оптимальности интерпретируется в соответствии с общими постановками оптимизационных задач: при заданных

ресурсах обеспечить достижение максимального результата или обеспечить достижение заданного результата при минимальном расходовании ресурсов.

Таким образом, в любом случае речь идет о наиболее рациональном использовании ресурсов, выделяемых или необходимых для защиты информации.

Защищенность информации определяется некоторыми показателями, которые в свою очередь определяются параметрами системы и внешней среды. Всю совокупность параметров, определяющих значения показателей защищенности информации, в самом общем случае можно разделить на три вида:

1) управляемые параметры, т.е. такие, значения которых полностью формируются системой защиты информации;

2) параметры, недоступные для такого однозначного и прямого управления, как параметры первого вида, но на которые система защиты может оказывать некоторое воздействие;

3) параметры внешней среды, на которые система защиты информации никаким образом воздействовать не может.

2.3. Стратегии защиты информации

Стратегия – это общая, рассчитанная на перспективу руководящая установка при организации и обеспечении соответствующего вида деятельности, направленная на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов.

Стратегическая установка на защиту информации: вся совокупность мероприятий по защите информации должна быть такой, чтобы во все время функционирования системы уровень защиты соответствовал требуемому, а выделяемые для этих целей ресурсы расходовались бы наиболее рациональным способом.

Организация защиты информации в самом общем виде может быть определена как поиск оптимального компромисса между потребностями в защите и необходимыми для этих целей ресурсами.

Потребности в защите обусловливаются прежде всего важностью и объемами защищаемой информации, а также условиями ее хранения, обработки и использования. Эти условия определяются уровнем (качеством) структурно-организационного построения защищаемой системы или объекта, уровнем организации технологиче-

ских схем обработки информации, местом и условиями расположения компонентов системы, а также некоторыми другими параметрами.

Размер ресурсов на защиту информации может быть ограничен определенным пределом либо определяться условием обязательного достижения требуемого уровня защиты.

В первом случае защита должна быть организована так, чтобы при выделенных ресурсах обеспечивался максимально возможный уровень защиты, а во втором – так, чтобы требуемый уровень защиты обеспечивался при минимальном расходовании ресурсов.

В целях обоснования числа и содержания необходимых стратегий используем два критерия – *требуемый уровень защиты* и *степень свободы действий при организации защиты*.

Множество угроз, относительно которых должна быть обеспечена защита:

– защита от уже известных (ранее проявлявшихся) угроз;

– защита от наиболее опасных потенциально возможных угроз;

– защита от всех потенциально возможных угроз.

Для защиты от известных угроз, очевидно, необходимо организовать регулярный сбор и обработку данных о проявлениях угроз и их последствиях и иметь арсенал проверенных средств эффективной нейтрализации каждой из угроз.

Защита от всех потенциально возможных угроз возможна только в случае знания всего их множества. Формирование этого множества представляет собой достаточно сложную научно-техническую и организационную проблему.

Общая интерпретация второго критерия (степени свободы действий при организации защиты) сводится к тому, что организаторы и исполнители процессов защиты имеют относительно полную свободу распоряжаться методами и средствами защиты и некоторую степень свободы вмешательства в архитектурное построение защищаемой системы или объекта, а также в организацию и обеспечение технологии их функционирования.

По этому последнему аспекту удобно выделить три различных степени свободы следующего содержания:

– никакое вмешательство в систему не допускается;

– к архитектурному построению системы и технологии ее функционирования допускается предъявлять требования неконцептуального характера;

– требования любого уровня, обусловливаемые потребностями защиты информации, принимаются в качестве обязательных условий при построении системы, организации и обеспечении ее функционирования.

На основе анализа всех стратегических подходов могут быть выделены три основных стратегии защиты: оборонительная, наступательная и упреждающая.

Анализ сущности условий, способствующих эффективной реализации различных стратегий защиты, приводит к следующему выводу: кардинальное повышение эффективности защиты информации (равно как и эффективности обеспечения качества информации и информационной безопасности) не может быть достигнуто в рамках существующих концепций автоматизированной обработки информации.

Необходимы принципиально иные концепции, построение которых требует существенного видоизменения постановки задач развития и использования вычислительной техники, а также в целом взглядов на процесс совершенствования информационного обеспечения различных сфер деятельности.

3. ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

3.1. Киберпреступления: характеристика и особенности

Термин «компьютерная преступность» впервые появился в США в начале 60-х гг. вследствие первых преступлений с использованием информационных технологий.

Одно из первых крупных компьютерных преступлений было совершено в США в конце 70-х гг. прошлого столетия. Некто Стэнли Рифкин, специалист по обслуживанию ЭВМ, расшифровал код, управляющий системой банка в Лос-Анджелесе, и дал команду ЭВМ на перевод 70 млн дол. на его текущий счет.

Страной, впервые предусмотревшей ответственность за компьютерные преступления, была Швеция (1973 г.). В 1979 г. на конференции Американской ассоциации адвокатов в г. Далласе были сформулированы составы компьютерных преступлений, воспроизведенные в последующем в уголовных кодексах штатов.

В конце 80-х и начале 90-х гг. прошлого столетия ответственность за компьютерные преступления была предусмотрена во многих государствах мира.

Компьютерная преступность (преступление с использованием компьютера) представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом компьютерная информация является предметом или средством совершения преступления. Структура и динамика компьютерной преступности в разных странах существенно отличаются друг от друга.

Основные признаки компьютерных преступлений были сформулированы в 1974 г. на конференции Американской ассоциации адвокатов. Тогда были выделены три направления компьютерных преступлений:

1) использование или попытка использования компьютера, вычислительной системы или сети компьютеров с целью получения денег, собственности или услуг;

2) преднамеренное несанкционированное действие, имеющее целью изменение, повреждение, уничтожение или похищение компьютера, вычислительной системы, сети компьютеров или содержащихся в них систем математического обеспечения, программ или информации;

3) преднамеренное несанкционированное нарушение связи между компьютерами, вычислительными системами или сетями компьютеров.

За последние 10 лет количество подобных инцидентов в мире увеличилось в 23 раза. Но эта статистика раскрывает только зарегистрированные случаи. А, как известно, большинство компаний не стремится сообщать о проблемах.

Проблемы информационной безопасности, защиты персональных данных, обеспечения сохранности сведений, образующих охраняемую законом тайну, и иные аналогичные вопросы вызывают серьезную озабоченность всего мирового сообщества. Указанные явления самым непосредственным образом угрожают национальной безопасности государств.

Так, по данным главного информационного центра МВД России, в 2004 г. было совершено 13 723 компьютерных правонарушения, что почти в 2 раза больше по сравнению с 2003 г. – 7 053, и их количество неуклонно растет. По словам руководителя Бюро специальных технических мероприятий МВД России А. Мошкова, в сфере высоких технологий именно мошенничество является самым распространенным преступлением в IT-среде и его количество растет с каждым годом. Если в 2010 г. было возбуждено 736 таких уголовных дел, то за 9 месяцев 2011 г. их число уже превысило 1 000, при том что у этих преступлений весьма высокий уровень латентности.

Мировое сообщество в целом обеспокоено проблемами, связанными с таким явлением, как киберпреступность, а также с разработкой системы адекватных ответных мер со стороны всего мирового сообщества. В частности, в феврале 2013 г. в Вене группой экспертов был подготовлен итоговый документ, резюмирующий основные проблемы в сфере борьбы с киберпреступностью в различных государствах на всех пяти континентах. Условно их можно разделить на три основные группы:

1. Проблемы законодательного характера:

– отсутствие единого, универсального определения киберпреступности. В целом предлагают следующую типологизацию компьютерных преступлений:

1) сетевая атака и повреждение компьютерной системы,

2) сетевое мошенничество,

3) хищение денежных средств из финансовых учреждений путем несанкционированного доступа к компьютерным системам,

4) азартные игры в онлайновой среде и реклама услуг сексуального характера в интернете,

5) посягательства на авторские и смежные права, преступления против интеллектуальной собственности,

6) хищение информации, составляющей государственную тайну, – угроза государственной безопасности,

7) распространение информации;

– различный подход государств к определению круга составов преступлений, охватываемых понятием киберпреступности. Так, в Уголовном кодексе КНР было предусмотрено пять статей, оговаривающих уголовную ответственность за компьютерные преступления. Постановлением Постоянного комитета ВСНП КНР об охране компьютерных сетей, принятом в 2000 г., установлена уголовная ответственность уже за 15 видов компьютерных преступлений;

– несмотря на возросшую за последнее десятилетие активность в принятии международных и региональных документов, направленных на противодействие киберпреступности (выделяют пять основных групп таких документов: Совета Европы и Европейского Союза, СНГ или Шанхайской организации сотрудничества, межправительственных африканских организаций, Лиги арабских государств и ООН), во многих из них отсутствуют основные положения и имеются существенные расхождения;

– многие страны Азии считают свое действующее уголовно-процессуальное законодательство частично достаточным или недостаточным для расследования киберпреступлений.

2. Проблемы уголовно-процессуального характера:

– отсутствие четкого определения диапазона специальных следственных полномочий в сфере международного сотрудничества при производстве по данной категории уголовных дел;

– все страны Африки, а также треть иных стран отмечают недостаточность уровня подготовки прокуроров для работы с электронными доказательствами и отстаивания своей процессуальной и правовой позиции в суде. Аналогичным образом только в каждой десятой стране существуют специализированные судебные службы. Например, 19 мая 2014 г. премьер-министр Японии Синдзо Абэ на заседании правительственного комитета по информационной безопасности отметил, что в связи с ростом угроз киберпространству одной из ответных мер станет превращение нынешнего комитета по информационной безопасности в комитет по кибербезопасности с придани-

ем ему дополнительных функций, а также будет учреждена должность чиновника по кибербезопасности при правительстве в статусе заместителя министра. Он должен будет координировать действия и информацию между государственными структурами, частными компаниями, а также с другими государствами [2]. В свою очередь, в Китае для борьбы с компьютерной преступностью созданы специальные отряды интернет-полиции.

3. Проблемы криминалистического характера:

– преимущественно организованный характер совершаемых киберпреступлений. Одно из самых распространенных явлений в интернете – фишинг представляет собой охоту за персональными данными клиентов в интернете. Как правило, киберпреступники используют ложную электронную почту и сайты, чтобы обмануть пользователя и заполучить его личную информацию. Чтобы не попасться на удочку мошенников, пользователям интернета советуется почаще менять пароли и идентификационные коды.

Можно упомянуть также необычную форму кибернетической преступности со стороны Китайской Народной Республики. Продукция, поступающая с китайских заводов, в большинстве случаев начиняется шпионскими приспособлениями, а если речь идет об электронике, то в большинстве случаев она изначально заражена вредоносным программным обеспечением или так называемыми вирусными программами. Все чаще и чаще внутри китайской продукции находят подозрительные комплектующие. При этом продукция, в которой были найдены шпионские устройства, варьируется от флеш-карт и мелкой бытовой техники, например блендеров и чайников, и до крупной домашней электроники, такой как телевизоры, домашние кинотеатры и компьютеры [5].

Организованный характер киберугроз подтверждается также выступлением генерала Сон Юн Кын, занимающегося в вооруженных силах Республики Корея вопросами национальной безопасности, в котором генерал утверждает, что северокорейские компьютерные взломщики уже активно проникают в южнокорейские компьютерные сети. Особенно хакеров из КНДР привлекают сети государственных ведомств, из которых разведчики пытаются красть секретные сведения [6];

– необходимость развития нетрадиционных методов работы правоохранительных органов, органов уголовного преследования по делам о киберпреступлениях (например производство удаленной компьютерно-технической экспертизы);

– потребность создания специализированных структур для расследования киберпреступлений.

Многогранность существующих проблем требует незамедлительной реакции государств на вызовы преступного мира в виртуальном пространстве. И такая реакция должна носить унифицированный, системный, единообразный, адекватный характер.

Основные виды компьютерных преступлений

Как уже было отмечено нами ранее, одной из проблем обеспечения информационной безопасности является различный подход государств к определению круга составов преступлений, охватываемых понятием киберпреступности. В частности, в целом к основным видам компьютерных преступлений могут быть отнесены:

1. Несанкционированный доступ к информации, хранящейся в компьютере.

Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

2. Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

«Временная бомба» – разновидность «логической бомбы», которая срабатывает по достижении определенного момента времени. Способ «троянский конь» состоит в тайном введении в чужую программу таких команд, которые позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

3. Разработка и распространение компьютерных вирусов.

Компьютерные вирусы типа «Червь» обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание. Выявляется вирус не сразу: первое время компьютер «вынашивает инфекцию», поскольку для маскировки вирус нередко используется в комбинации с «логической бомбой» или «временной бомбой». Вирус наблюдает за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации.

4. Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.

Проблема неосторожности в области компьютерной техники сродни неосторожной вине при использовании любого другого вида техники, транспорта и т.п.

Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти не достижима.

5. Подделка компьютерной информации.

Этот вид компьютерной преступности является одним из наиболее свежих. Он является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик, причем имеющий достаточно высокую квалификацию.

Преступление состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосования, референдумов и т.п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы. Естественно, что подделка информации может преследовать и другие цели.

6. Хищение компьютерной информации.

Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться.

В соответствии с национальным законодательством – Уголовным кодексом РФ (далее – УК РФ) – в настоящее время криминализировано только три деяния, образующих самостоятельные составы преступления:

Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст. 272 УК РФ).

Более тяжким преступлением считается аналогичное деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а также если деяние повлекло тяжкие последствия или создало угрозу их наступления.

Особо следует обратить внимание, что законодатель применительно к преступлениям, совершенным в сфере компьютерной информации, крупным ущербом признает ущерб, сумма которого превышает 1 млн р.

Далее, самостоятельный состав преступлений образует **создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)**. Данное деяние, заключающееся в создании, распространении или использовании компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, наказывается ограничением свободы на срок до четырех лет либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до 200 тыс. р. или в размере заработной платы или иного дохода осужденного за период до 18 месяцев.

Более тяжким считается то же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившее крупный ущерб или совершенное из корыстной заинтересованности, или повлекшее тяжкие последствия, или создавшее угрозу их наступления.

Наконец, ст. 274 УК РФ предусматривает уголовную ответственность за **нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям**, повлекшее уничтожение, блокиро-

вание, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

3.2. Характеристика личности киберпреступника

С распространением компьютеров у обывателей появилось новое понятие – хакер, вызывающее у пользователей эмоции от интереса до панического страха.

Слово «хакер» имеет несколько определений:

1) человек, который любит исследовать и вытягивать максимум возможностей программируемых систем в отличие от большинства пользователей, не лезущих глубже необходимого минимума;

2) тот, кто программирует увлеченно, даже одержимо, или наслаждается процессом разработки больше, чем теориями программирования;

3) человек, способный быстро схватить суть явления;

4) человек, способный к быстрой разработке программ;

5) эксперт по определенной системе, как правило, часто использующий ее;

6) эксперт или энтузиаст любого рода;

7) тот, кто испытывает интеллектуальное наслаждение от творческого преодоления или обхода ограничений;

8) злоумышленник, который пробует обнаружить необходимую информацию (к примеру, пароль) с помощью записи в адрес машины.

Первые шесть достаточно близки, позволяют создать некую картину. Седьмое определение отвечает на вопрос: «Почему хакеры ломают?» И естественно, чем выше стена, тем интересней через нее перелезать. «Счастье в борьбе». А что если стены нет? Хакер просто проигнорирует такую систему.

Хакеров можно условно разделить на три группы.

Кракеры. Ломают программные защиты от серийных номеров до аппаратных ключей. Основные инструменты – отладчик и дизассемблер (к примеру, Soft-Ice и IDA PRO).

Фрикеры. Занимаются телефонией. К примеру, создан сотовый телефон, за который не надо платить. Существуют вечные телефонные карты. Устройства для телефонного междугороднего разговора с оплатой как по городу и т.д.

Сетевые хакеры. Цель – глобальные и локальные сети. Во времена популярности BBS нередко ломали и их. Вообще понятие взлом

часто используется без понимания и требует пояснения. Взлом – несанкционированный доступ. Есть некоторые предусмотренные методы использования ПО, сетей. Если же улучшить Shareware программу, убрав рекламу из нее, или зайти в сеть не с парадного, а с черного входа (или просто не под своим паролем) – это уже взлом.

Кевин Митник. Родился в 1963 г. в Калифорнии. Уже в возрасте 12 лет мальчик заинтересовался информационной безопасностью и социальной инженерией. Это привело Кевина к тому, что в будущем он, задавая определенные наводящие вопросы, смог получать доступ к электронным ящикам различных пользователей и к их компьютерам. Такие простые, казалось бы, методы помогли хакеру взломать карточную систему, принятую в Лос-Анджелесе. Первоначально же Митник вместе со своей подругой занимался взломом телефонных сетей, развлекаясь бесплатными международными разговорами. В 1979 г. телефоны и АТС были для хакера пройденным этапом. В результате он стал специализироваться на взломе компьютерных сетей, начав со своей родной школы. В итоге за годы своей деятельности Митник взломал системы таких компаний, как Нокиа, Моторола, Фуджитсу Сименс и Digital Equipment Corporation. За поимку знаменитого киберпреступника была объявлена высокая награда. В 1994 г. Митник заинтересовался сотовой телефонией, а в 1995 г. он был арестован. Прокурор огласил, что преступник нанес ущерба на 80 млн дол.! Однако адвокаты сумели снять большую часть обвинений, и после четырехлетнего заключения Кевин вышел на свободу. Сейчас он занимается законопослушной деятельностью: у него своя компания по организации сетевой безопасности, он является автором ряда книг о жизни хакеров. О самой же жизни и деятельности самого известного хакера был даже снят фильм «Взлом».

Адриан Ламо. Получил прозвище «Бездомный хакер». Родился он в 1981 г. в Бостоне, а свою кличку получил за то, что постоянно менял места своих действий. Уже в детстве Адриан взломал отцовский Commodore 64, чтобы играть по своим сценариям. В 17 лет Ламо остался без опеки родителей: те переехали, оставив сына одного. Он уже хорошо разбирался в компьютерах, подрабатывая в различных компаниях. Вскоре Ламо начал путешествовать по стране с одним лишь ноутбуком, комплектом одежды да одеялом. Хакер выходил в интернет из кафе и библиотек, других публичных мест. Ламо исследовал системы безопасности крупнейших компаний, взламывая их затем. Список его жертв впечатляет – Microsoft, NY Times, Yahoo, Bank

of America. Мелкие сайты, вроде сайтов знакомств, его попросту не интересовали. При этом хакер не просто взламывал системы защиты, но и сообщал о найденных уязвимостях. Именно поэтому ФБР долго не объявляло охоту на такого «помощника». В сентябре 2003 г. преступник сдался властям, признавшись в содеянных взломах. Его приговорили к условному сроку и штрафу в 65 тыс. дол. В 2007 г. испытательный срок прошел, ныне Ламо является журналистом. В 2010 г. Адриан отметился тем, что выдал властям доверившегося ему Брэдли Мэннинга, который снабжал конфиденциальными материалами известный Wikileaks.

Владимир Левин. Стал первым известным российским хакером. О нем заговорили в 90-е, когда он попытался взломать российский «Ситибанк». Родился преступник в 1967 г. в семье интеллигентов и получил образование микробиолога. Компьютеры были для Левина всегда только хобби. Полноценным хакером его трудно назвать, ведь для взлома он использовал человеческий фактор, а не машинный. В 1994 г. Левин смог получить доступ к корпоративным счетам клиентам Ситибанка и попытался вывести около 12 млн дол. в различные страны. Хакер был арестован в 1995 г. в лондонском аэропорту. Воспользоваться сворованными средствами ему так и не удалось. Правда, администрация банка так и не смогла вернуть обратно все средства – 400 тысяч так и остались ненайденными. В 1997 г. Левин был доставлен в США, где на суде признался в краже почти 4 миллионов. Процесс привлек к себе большое внимание: еще никогда хакер не попадался на краже таких больших сумм. Преступника посадили на три года, любопытно, что английский он начал изучать только в самой тюрьме, до этого Левин знал его только в рамках компьютерных терминов. Сам «Ситибанк» вынужден был пересмотреть свою систему безопасности. Эта история оставила много вопросов. Так и осталось непонятным, были ли у Левина сообщники и куда делись деньги?

Нейшон Ивен-Чейм. Появился на свет в Австралии в 1971 г. Он стал одним из самых высококвалифицированных специалистов группировки «Сфера», сам же выступал под прозвищем «Феникс». В 1988 г. полиция Австралии с помощью своих агентов и информаторов начала разработку этого незаконного объединения. Для своих преступных действий Нейшон использовал сначала компьютерную сеть X25, работающую на основе телефонных сетей, а затем и интернет. В итоге полиция стала прослушивать модем юного хакера. В апреле

1990 г. состоялся арест, Ивен-Чейму было предъявлено обвинение по 48 мошенническим действиям. В их число вошли взлом нескольких американских университетов и даже НАСА. Это дело стало первым в Австралии такого рода. Хакеру грозило десять лет тюрьмы, но он решил сотрудничать с полицией, получив в итоге 500 ч общественных работ и год заключения условно. Мотивацию своих действий Нейшон так и не смог объяснить. Сейчас знаменитый хакер работает в сфере IT, предпочитая уклоняться от интервью и обсуждать свою былую карьеру.

3.3. Спаминг, фишинг, кардинг

Кроме хакерства, существует также кардинг, крекинг, фишинг, нюкинг и спаминг. Давайте разберем каждый из этих компонентов по отдельности.

Кардинг – это похищение реквизитов, идентифицирующих пользователей в сети интернет как владельцев банковских кредитных карт, с их возможным последующим использованием для совершения незаконных финансовых операций (покупка товаров либо отмывание денег).

Крекинг – снятие защиты с программного обеспечения для последующего бесплатного использования (защита обычно устанавливается на так называемые «shareware/demo/trial»-продукты). Сюда же можно отнести пиратское распространение законно купленных копий программного обеспечения.

Крекинг карается ст. 146 «Нарушение авторских и смежных прав (незаконное использование объектов авторского права или смежных прав, а равно присвоение авторства, если эти деяния причинили крупный ущерб)» и ст. 273 «Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами».

Фишинг. Незаконное получение и использование чужих учетных данных для пользования сетью интернет. То есть деятельность энергичных молодых людей, которые завладели логином и паролем друго-

го человека или организации, карается ст. 165 «Причинение имущественного ущерба путем обмана или злоупотребления доверием».

Нюкинг, или d.o.s. – это атаки (Denial of Service), действия, вызывающие отказ в обслуживании (d.o.s.) удаленным компьютером, подключенным к сети. То есть деятельность, направленная на стимулирование массового зависания компьютеров. Эта группа тесно связана с первой, поскольку одним из методов взлома интернет-сайтов является d.o.s.-атака с последующим запуском программного кода на удаленном сетевом компьютере с правами администратора.

Это, наверное, наиболее вредоносное преступление, и наказание за него предусмотрено тремя статьями: ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание и распространение вредоносных программ для ЭВМ», ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред».

Спаминг – это массовая несанкционированная рассылка электронных сообщений рекламного или иного характера. Со спамом сталкивался почти каждый пользователь интернета. Американская статистика говорит о том, что в 2011 г. спамерами был нанесен ущерб: американским организациям – 9 млрд дол., европейским – 2,5 млрд дол. Примечательно, что дотошные американцы высчитали эти цифры на основе оценок уменьшения производительности труда за счет того, что в среднем каждый работник тратит 4,5 секунды на удаление письма. В Соединенных Штатах, Англии и в континентальных европейских странах уже давно борются со спамерами путем применения уголовной или административной ответственности. В США совсем недавно принят специальный закон о борьбе со спамом. Однако даже уголовное наказание в виде лишения свободы или административная ответственность в виде штрафа в 5 000 фунтов (в Англии) никоим образом не снижает количество рассылаемых писем. Российский законодатель упорно молчит. По нашему уголовному законодательству можно привлечь за спаминг только в том случае, если кто-либо вышлет столько писем, что их количество приведет к отключению почтового ящика (ст. 274).

Наравне с хакерством (хакинг) эти кибернарушения являются структурными компонентами компьютерных преступлений.

3.4. Защита от виртуальных мошенников

Интернет-мошенничество представляет собой одну из разновидностей киберпреступности. Новые технологии рождают новые замыслы в головах злоумышленников.

Основной целью интернет-мошенничества является обман пользователей глобальной паутины и кража конфиденциальной информации, которая после используется в личных целях преступника. В результате такой деятельности миллионы людей во всем мире несут значительные убытки каждый год.

Существует большое количество различных видов интернет-мошенничества: фишинг, нигерийские письма счастья, вишинг и др. Но всех их объединяет одно: успех всех этих методов напрямую зависит от степени доверчивости и безалаберности пользователя.

Для того чтобы не попасться на удочку интернет-мошенников, необходимо выполнять несколько простых правил:

1) не доверять всем непонятным сообщениям, в которых содержится просьба предоставить личные данные;

2) игнорировать спам;

3) не открывать все маломальские подозрительные письма, приходящие на ваш ящик;

4) никогда не сообщать ваши персональные данные личностям, в чистоте намерений которых вы не уверены;

5) быть аккуратными при совершении онлайн-покупок, выбирать для этого сайты, обеспечивающие безопасность сделок и конфиденциальность личных данных.

Кроме того, необходимо пользоваться многоуровневой системой безопасности. Для этого нужно установить и регулярно обновлять программы для обеспечения безопасности компьютера (антивирус, файервол и многое другое).

Самые громкие киберпреступления современности

Одну из первых громких хакерских атак совершил в 1983 г. американский студент и один из самых известных в будущем хакеров **Кевин Митник**. Используя один из университетских компьютеров, он проник в глобальную сеть ARPANet, являющуюся предшественницей Internet, и сумел войти в компьютеры Пентагона. Он получил доступ ко всем файлам министерства обороны США. Митника арестовали прямо на территории университета. Он был осужден и отбыл

свое первое настоящее наказание, проведя полгода в исправительном центре для молодежи.

Ущерб более чем в 300 млн дол. нанес компании Dassault Systemes **58-летний хакер из Греции**. В январе 2008 г. он был арестован местной полицией за незаконное вторжение в серверы компании и кражу программного обеспечения, которое впоследствии вор продал в интернете. Хакер был арестован в собственном доме в Афинах.

Ущерб почти в 25 млн дол. причинили американским банкам **два хакера из России**. В ноябре 2000 г. в США ФБР поймало хакеров из Челябинска: 20-летнего Алексея Иванова и 25-летнего Василия Горшкова. Россиянам удалось взломать компьютерные системы нескольких компаний и украсть номера кредитных карт, в частности они похитили 15,7 тыс. номеров кредитных карт из Western Union. В 2002 г. Горшков был приговорен к трем годам заключения, а Иванов был осужден на четыре года.

12 млн дол. попытался похитить гражданин России **Владимир Левин**. В марте 1995 г. он был арестован в Лондоне. Служба безопасности американского «Ситибанка» обвинила Левина в том, что в июне – октябре 1994 г. он взломал центральный сервер банка и попытался обчистить счета клиентов. Суд Нью-Йорка осудил Левина на 36 месяцев тюрьмы и депортировал в Россию.

Ущерб в 1,7 млн дол. нанес НАСА в 1999 г. 16-летний хакер **Джонатан Джеймс**. Джеймс осуществил первый в истории взлом сервера НАСА и украл несколько файлов, включая исходный код международной орбитальной станции. Однако ему удалось избежать тюрьмы, так как на момент преступления он был несовершеннолетним. Ему грозило около десяти лет тюрьмы.

Несколько миллионов долларов сумел украсть из иностранных банков одессит **Дмитрий Голубов**. С помощью созданного им сайта Carderplanet.com примерно 7 тыс. мошенников-кардеров продавали друг другу краденые данные о банковских счетах по всему миру. Преступник был задержан 7 июля 2005 г. и провел в тюрьме шесть месяцев.

1,5 млн дол. выкрал из электронных «карманов» американцев из списка Forbes 24-летний москвич **Игорь Клопов** вместе с нанятыми четырьмя гражданами США. 15 мая 2007 г. он был задержан в Нью-Йорке.

Еще одну хакерскую атаку на НАСА предпринял в 2001–2002 гг. хакер из Великобритании **Гари Мак-Киннон**. Ему удалось проник-

нуть в компьютеры, принадлежащие армии, НАСА, ВМС, министерству обороны, ВВС и Пентагону. В общей сложности Мак-Киннон получил несанкционированный доступ к 97 компьютерам, каждый раз он искал в них информацию о летающих тарелках. Он был арестован в 2002 г., но за недостаточностью улик был отпущен.

Громкую атаку осуществил в 2002 г. хакер **Адриан Ламо**. Ему удалось получить доступ во внутреннюю сеть редакции газеты New York Times, где он начал модифицировать важные файлы. Ламо менял конфиденциальные базы данных, в одну из которых, содержащую список сотрудничающих с газетой экспертов, он добавил свое собственное имя. В августе 2003 г. Адриана Ламо арестовали, приговорили к двум годам испытательного срока и назначили выплатить Times 65 тыс. дол. в качестве компенсации.

3.5. Расследование киберпреступлений

Случается, что даже несмотря на действующие в политике сферы безопасности, подкрепленные современными техническими решениями, организации сталкиваются с утечками информации, хакерскими атаками и иными неприятными инцидентами. Сейчас вопрос «Как защищать?» уже не столь актуален. Этой теме посвящено большое количество трудов, разработано множество теорий. Но вот другая тема – «Что делать, если произошел инцидент или он происходит в данный момент?» – настоящая головная боль руководителей и специалистов.

Правительства развитых стран быстро осознали, что компьютерные преступления – серьезная угроза для национальной и экономической безопасности. Поэтому начиная с 70-х гг. в структурах органов внутренних дел ведущих государств мира начали формироваться специальные подразделения по борьбе с компьютерной преступностью, высшие учебные заведения ввели в курсы криминалистики методики расследования информационных преступлений, активизировалась научная работа.

Благодаря масштабным правительственным инвестициям в исследование вопросов компьютерной криминалистики, а также законодательной поддержке в таких странах, как Германия и США, отделы по борьбе с киберпреступлениями и кибертерроризмом вели и ведут эффективную работу.

Отдельно стоит затронуть правовые аспекты. Поскольку речь идет о преступлениях, нарушениях и инцидентах, то, естественно, подобные события должны корректно оформляться в юридическом отношении, не говоря уже о наказании за такие действия. Поэтому одновременно с созданием подразделений на государственном законодательном уровне шла работа по созданию юридической базы. И действия законодательной власти были скоординированы настолько, что соответствующие законы появились достаточно быстро и сразу же начали работать.

Рынок расследований компьютерных преступлений

А что делать, если расследование нужно произвести незамедлительно, или недопустимо афишировать инцидент, произошедший в компании? Тогда на помощь могут прийти организации, которые занимаются расследованием компьютерных преступлений на коммерческой основе.

На Западе такие компании давно заняли свой сегмент на рынке безопасности, но в России ситуация выглядит несколько иначе. Пока гораздо выгоднее внедрять системы безопасности и получать гарантированные деньги, чем заниматься деятельностью, которая может и не принести результат. Ведь деятельность эта требует огромных усилий с научно-исследовательской точки зрения.

По сути, штат подобных организаций должен состоять из людей, знания и навыки которых аналогичны знаниям и навыкам людей, совершающих компьютерные преступления. Что, например, делать, если расследование зашло в тупик? Становится непонятно, каким образом рассчитывать сумму затрат на работы. А главное, когда дело касается расследования сути преступления, то речь уже идет о контакте не с образом злоумышленника, о котором идет речь при оценке рисков, а о контакте с конкретным преступником (нарушителем, злоумышленником) или группе таковых. А для этого нужна специальная подготовка.

Основными направлениями рынка расследования компьютерных преступлений в России и в мире являются:

1) реагирование на инциденты (Incident response);
2) расследование инцидентов (eDiscovery);
3) компьютерная криминалистика (Digital Forensic);
4) мониторинг инцидентов;
5) юридическое сопровождение инцидентов.

Направление расследования инцидентов (компьютерных преступлений) позволяет ответить на следующие вопросы: является ли инцидент внутренним или внешним, как он произошел и почему, что делать сейчас и кто может быть причастен к случившемуся?

Реагирование на инциденты и их мониторинг позволяют в момент совершения инцидента в режиме реального времени минимизировать ущерб, правильно собрать доказательства и не сделать лишнего. Кроме того, в рамках этого направления ведутся мониторинг и обнаружение инцидентов. Компьютерная криминалистика – это прежде всего анализ доказательств, изучение улик и скомпрометированных информационных систем. Лаборатория компьютерной криминалистики отвечает за восстановление хронометража событий инцидента, поиск доказательств на носителях информации, восстановление данных и многое другое, связанное с компьютерной криминалистикой.

Юридическое сопровождение всех работ обязательно. Поскольку все инциденты так или иначе могут быть тесно связаны с компьютерными преступлениями, важно выполнять и оформлять работы в соответствии с действующим законодательством, подключать правоохранительные органы и участвовать в оперативной, следственной и судебной стадиях работ.

Расследования – это не только поиск и обнаружение злоумышленников. Во многом это тонкий, особенный аудит скомпрометированных систем. Ведь нужно разобраться, почему инцидент произошел! Кроме определения лиц, причастных к инциденту, заказчик должен получать еще и рекомендации по улучшению систем ИБ. И эти рекомендации должны носить практический, так называемый постинцидентный характер.

Отрадно, что сегодня руководителей организаций чаще всего уже не приходится убеждать в необходимости изменений системы информационной безопасности.

В части правоприменительной практики на территории РФ следует констатировать, что государство признает исключительно один способ реагирования на факт совершения деяний, закрепленных в УК РФ, – это уголовное судопроизводство, возбуждение уголовного дела, расследование преступления и привлечение виновного (виновных) к уголовной ответственности.

Реализация предоставляемых действующим российским уголовно-процессуальным законодательством возможностей собирания доказательств при расследовании преступлений в сфере компьютерной

информации и компьютерных сетей сталкивается с рядом существенных трудностей и проблем, настоятельно требующих своего решения.

Не претендуя на полноту их выявления, тем не менее целесообразно отметить наиболее существенные и сложные из них. На наш взгляд, такими проблемами являются следующие.

Проблема розыска компьютерной информации. При раскрытии и расследовании преступлений в сфере компьютерной информации зачастую возникает необходимость в поисковой деятельности, направленной на установление (и лишь затем изъятие) компьютерной информации при наличии достаточных оснований полагать, что она имеет существенное значение для установления истины по уголовному делу.

Информация по своим качественным характеристикам не совпадает ни с одним из объектов розыска. Коренное отличие состоит в ее нематериальной природе, в то время как все остальные объекты розыска материальны. Фиксируя информацию на материальном носителе, следователь изменяет форму, в которой она закреплена, но содержание остается неизменным. Следовательно, сами по себе носители не отражают никаких следов преступления и лишь с того момента, как следователь запечатлел на них искомую информацию, приобретают процессуальную значимость. Таким образом, доказательственное значение при расследовании конкретного уголовного дела будет иметь сама информация, запечатленная на соответствующих носителях. Тем более, что согласно действующему уголовно-процессуальному законодательству, следователь при производстве отдельных следственных действий может применять несколько различных способов фиксации доказательственной информации.

Бурное развитие техники и использование правоохранительными органами в процессе расследования возможности высоких технологий технически позволяет проходить в глобальных сетях по следам сообщений, передаваемых по сетям электросвязи последовательно от сервера к серверу, от компьютера к компьютеру для их отыскания и изъятия.

Также остаются неурегулированными вопросы, касающиеся прав и законных интересов человека и гражданина при определении пределов использования разыскной деятельности сотовых систем связи, сети интернет, спутниковой навигации, микропроцессорных устройств и других возможностей высоких технологий.

Обыск в компьютерных сетях. Сейчас компьютеры широко используются в целях обработки и хранения различного рода информа-

ции. Используются они и в преступной деятельности. В связи с этим при производстве обысков по различным категориям уголовных дел и прежде всего при расследовании преступлений в сфере компьютерной информации можно выделить принципиально новый объект исследования – средства компьютерной техники, а также объект поиска – информацию, хранящуюся в памяти компьютера или на внешних носителях – дисках, USB флэш-накопителях и т.п.

Не редкость, когда искомым объектом является компьютерная информация, физическое местонахождение носителей которой, по существу, не имеет какого-либо значения для следствия. В то же время имеются достаточные основания полагать, что в определенном удаленном массиве компьютерной информации на таком носителе находится требуемая, доступ к которой возможен с использованием сетевых технологий в условиях, когда любая задержка с ее копированием может повлечь за собой ее утрату в результате действий иных лиц, а равно иные вредные последствия. В таких условиях производство выемки компьютерной информации фактически невозможно.

В связи с этим возникает новая, на сегодняшний день законодательно не урегулированная проблема ее изъятия, а по существу – обыска в компьютерных сетях (или в среде для хранения компьютерных данных) с целью изъятия искомой компьютерной информации. Обыск должен проводиться при условии, когда примерное место ее нахождения известно. Именно это должно определять регулирование правового режима такого обыска. Учитывая особенности компьютерного пространства, настоятельно требуется отдельная уголовно-процессуальная регламентация такой деятельности.

Следы в сфере компьютерной информации. Следы совершения преступления в сфере компьютерной информации в силу специфики рассматриваемого вида преступлений редко остаются в виде изменений внешней среды. Они в основном не рассматриваются современной трасологией, поскольку в большинстве случаев носят информационный характер, т.е. представляют собой те или иные изменения в компьютерной информации, имеющие форму ее уничтожения, модификации, копирования, блокирования. Как справедливо отмечает А.В. Касаткин, «при современном развитии вычислительной техники и информационных технологий «компьютерные следы» преступной деятельности имеют широкое распространение. Это должно учитываться следователями и оперативными работниками в их деятельно-

сти по собиранию доказательств наряду с поиском уже ставших традиционными следов».

Как известно, Р.С. Белкин выделяет два вида следа: след как отпечаток какого-либо объекта на другом объекте – след-отображение и след как признак некоего события – след преступления.

Специфика механизма образования компьютерных следов определяется киберсредой, следообразующим объектом – программно-техническим средством, следовоспринимающим объектом – компьютерной информацией. Компьютерная информация хранится на носителях в определенной форме и может обрабатываться и преобразовываться в форму, понятную человеку, только специальными средствами компьютерной техники. В этом плане она неотделима от своего носителя.

Соответственно, следы в сфере компьютерной информации можно разделить на два типа: традиционные следы (следы-отображения, рассматриваемые трасологией, а также следы-вещества и следы-предметы) и нетрадиционные – информационные следы.

К первому типу относятся материальные следы. Ими могут являться какие-либо рукописные записи, распечатки и т.п., свидетельствующие о приготовлении и совершении преступления. Материальные следы могут остаться и на самой вычислительной технике (следы пальцев рук, микрочастицы на клавиатуре, дисководах, принтере и т.д.), а также на магнитных носителях и CD-ROM дисках.

Местонахождение информационных следов обусловлено местом совершения преступления. В этой связи можно выделить следующие следы:

1. На носителях компьютерной информации в месте использования преступником технических средств для неправомерного доступа (рабочее место преступника). Следы здесь обычно представлены в виде записей, которые заносятся в журналы операционной системой. Записи могут существовать как текстовые файлы или базы данных, совместимые с ODBC. Путем анализа данных следов (записей) можно получить информацию о регистрации доступа и работе пользователей, сервера, прикладных программ.

2. На промежуточных носителях компьютерной информации, посредством которых преступник осуществлял связь с компьютерной системой, подвергшейся нападению (сетевые кабели, промежуточные серверы и т.п.). Следы здесь представлены специальными техническими файлами регистрации сообщений, полиформатными записями

журналов регистрации сетевых устройств и требуют специального программного обеспечения для доступа и чтения.

3. На носителях компьютерной информации, где непосредственно наступил результат неправомерного доступа (ЭВМ, подвергшаяся нападению). Обычно представлены нештатными изменениями компьютерной информации, запуском посторонних программ и процессов и т.п.

На практике серьезные проблемы могут вызвать обнаружение, изъятие и фиксация материально фиксированных следов. Это связано с тем, что в большинстве случаев одним персональным компьютером может пользоваться неограниченное число пользователей. Это обстоятельство является причиной того, что на различных частях компьютера можно обнаружить большое количество отпечатков пальцев, принадлежащих нескольким людям. Как показал проведенный анализ специальной криминалистической литературы и практического опыта работников правоохранительных органов, к числу таких специфических свойств в первую очередь следует отнести:

– трудности в определении места происшествия и установлении его границ (в рамках которых должен проходить следственный осмотр), а также в реализации тактических рекомендаций по проведению следственного осмотра;

– необходимость активного использования специальных знаний при подготовке и проведении следственного осмотра;

– необходимость подготовки и использования специальных аппаратных и программных средств, позволяющих выявить, извлечь и зафиксировать виртуальные следы (уголовно-релевантную компьютерную информацию).

Ввиду отсутствия специализированных криминалистических средств выявления и изъятия следов неправомерного доступа к компьютерной информации в повседневной деятельности правоохранительных органов используется достаточно широкий набор стандартных программных средств общего применения, которые условно можно разделить на два основных класса: универсальные (многоцелевые) и специализированные (выполняющие определенный круг задач) программные средства.

Обозначенные проблемы требуют разработки и внесения соответствующих дополнений в действующее уголовно-процессуальное законодательство.

Одним из возможных подходов к решению этой задачи могло бы явиться включение в раздел о доказательствах УПК РФ нормы, регламентирующей порядок закрепления и изъятия следов в сфере компьютерной информации.

Подводя некоторые итоги, можно сделать выводы о том, что сложность компьютерной техники, неоднозначность квалификации, а также трудность сбора доказательственной информации не приведет в ближайшее время к появлению большого числа уголовных дел, возбужденных по ст. 272–274 УК РФ. Разработка проблемы компьютерной преступности и поиск методов борьбы с нею являются чрезвычайно важным элементом. Несмотря на то что информационная безопасность и бюджеты на нее в России развиваются в геометрической прогрессии, количество компьютерных преступлений и инцидентов информационной безопасности растет еще более стремительно. Остается надеяться, что законодатель будет шагать в ногу со временем и научно-техническим прогрессом, а российские криминалисты внесут свой вклад в решение проблем, касающихся преступлений в сфере компьютерной информации.

4. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Анализ канала утечек конфиденциальной информации

Персональные данные отнесены к категории конфиденциальной информации, доступ к которой ограничен законодательством. Однако все чаще в СМИ появляется информация об утечках персональных данных клиентов, сотрудников. Уже никого не удивляют сообщения о краже паспортных данных сотрудниками банка для совершения мошеннических действий.

Так, по данным аналитического центра InfoWatch, в России за 2013 г. обнародовано 109 случаев утечки данных [55–57], что в 2,2 % выше аналогичного показателя 2012 г. А по данным компании SafeNet [58], количество утечек в первом квартале 2014 г. увеличилось на 233 % по сравнению с аналогичным периодом прошлого года.

По данным исследования, которое было проведено компанией Perimetrix [63], более половины компаний в России обрабатывают персональные данные и их утечка – это далеко не локальный инцидент, так как в группу риска входит большое количество граждан и причиненный им ущерб может измеряться не только в денежном эквиваленте, но также и в репутационном ущербе для компаний, допустивших такой инцидент.

В России регистрация инцидентов, связанных с утечкой персональных данных, началась только в 2010–2012 гг. с принятием закона, но организации не спешат оповещать своих клиентов, сотрудников о свершившемся факте, пытаясь зачастую скрыть неприятный инцидент. В свою очередь, в других странах (например США, Великобритания) компании обязаны сообщать общественности, информировать своих пострадавших клиентов. И связано это прежде всего с нормой в законодательстве этих стран, поэтому компании предпочитают выстраивать эффективную защиту не на бумаге, а на деле [61; 64].

Обзор основных каналов утечки в России. В настоящее время рост доли утечек персональных данных не позволяет говорить о их качественной защите. Умышленные и случайные утечки ПДн в 2013 г. распределились поровну (рис. 1).

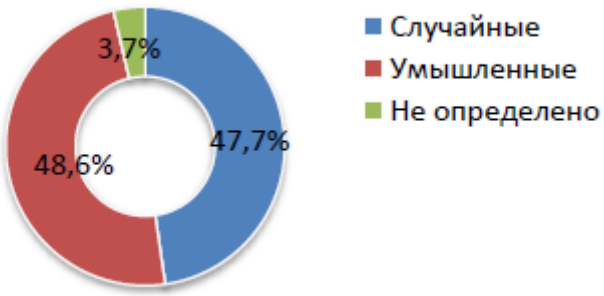

Рис. 1. Распределение случайных и умышленных утечек в 2013 г.

По данным аналитического центра компании InfoWatch [57], выявлено небольшое число актуальных каналов утечки (рис. 2):

– бумажные документы (ксерокопии паспортов, выброшенные договоры, формы, заявки и пр.);

– электронные документы, опубликованные на веб-сайтах, отправленные через электронную почту;

– голосовой канал.

Рис. 2. Распределение случайных и умышленных утечек по отраслям

Также сотрудниками аналитического центра компании InfoWatch [55; 59] выявлено, что в 2013 г. 19 % утечек персональных данных пришлись на государственные органы, а более 66 % всех утечек – на долю малых и средних компаний (рис. 3).

Таким образом, авторы данного исследования [55–57; 59] вынуждены констатировать тот факт, что в России степень защищенности персональных данных критически низкая, и связано это прежде всего со следующими факторами:

– формальным выполнением требований только на бумаге;

– замалчиванием фактов утечки персональных данных;

– мизерными суммами штрафов за нарушение требований;

– отсутствием исков к компании со стороны пострадавших клиентов;

– низкой активностью регуляторов в плане проведения плановых и внеплановых проверок;

– низкой компетенцией сотрудников, руководителей в защите ПДн;

– отсутствием обучения, семинаров, активной пропаганды о необходимости защиты.

По мнению авторов [55–57; 59], изменить ситуацию возможно лишь в том случае, если операторы ПДн начнут отвечать за утечки персональных данных рублем и репутацией, только в этом случае у них появится стимул обеспечивать безопасность ПДн на должном уровне.

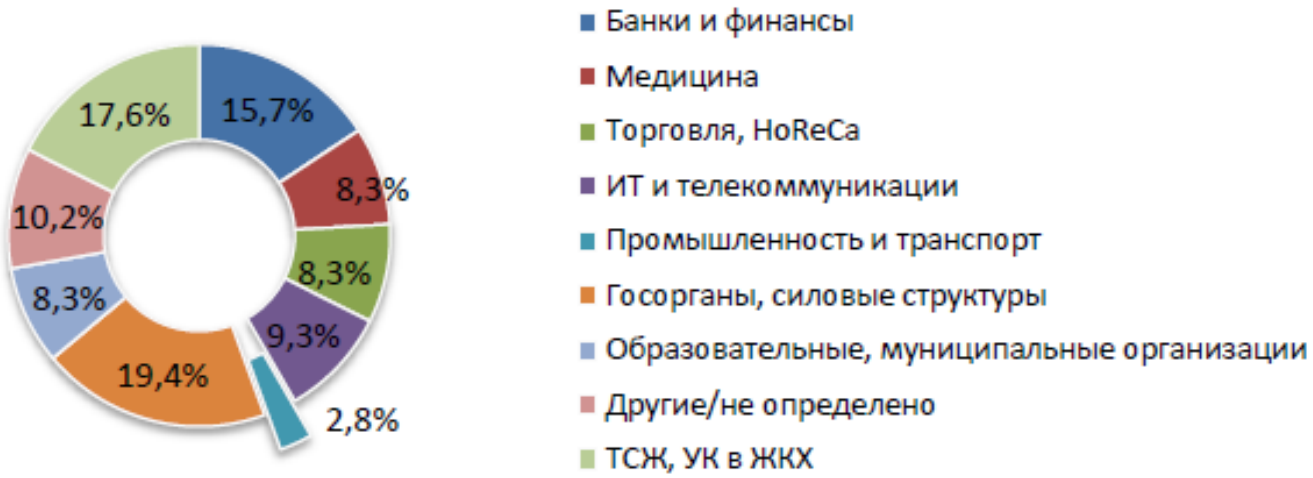

Рис. 3. Распределение утечек по отраслям

Зарубежная аналитика по утечкам информации. Если рассматривать глобальную статистику утечек, то англосакские страны занимают лидирующие позиции (США – 1-е место, Великобритания – 3-е место) и на них приходится до 78 % общемирового числа утечек данных (рис. 4) [61].

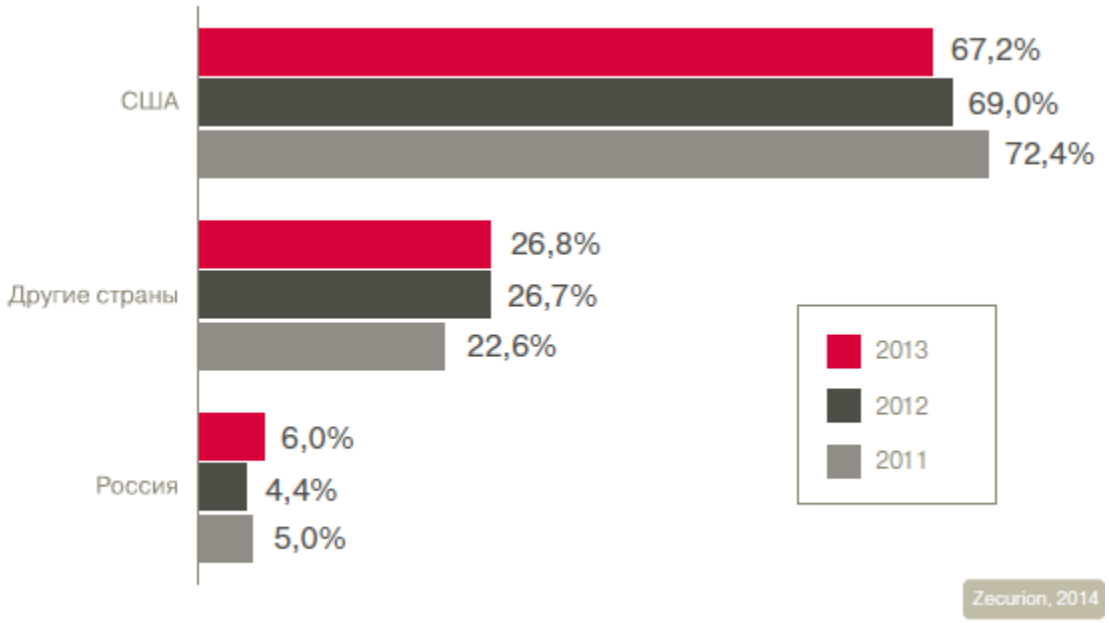

Рис. 4. Доля утечек по странам

Как и в России, в странах Европы умышленные и случайные утечки распределились поровну. По данным аналитиков, выявлено небольшое число актуальных каналов утечки (рис. 5) [57; 59]:

– кража, потеря оборудования;
– использование мобильных устройств;
– использование съемных носителей;
– веб-сервисы, электронная почта;
– бумажные документы;
– прочие.

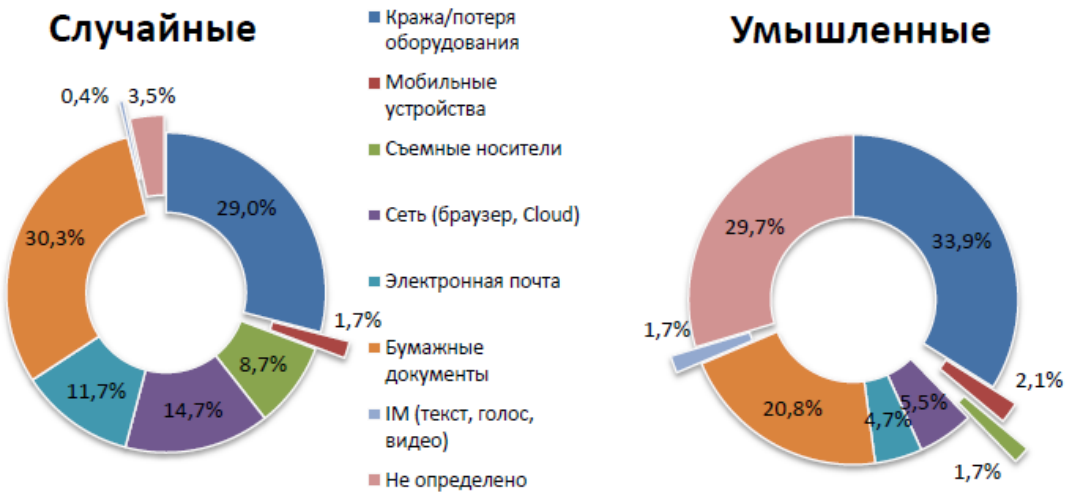

Рис. 5. Актуальные каналы утечки конфиденциальной информации

Аналитики компаний констатируют, что наибольшее количество утечек персональных данных в зарубежных странах также приходится на государственные структуры [55–59].

Используя аналитические данные известных российских компаний в сфере защиты конфиденциальной информации, можно сделать вывод, что для всех стран мира вопрос защиты персональной информации является наиболее ключевым, так как утечка данных может привести компании к выплате многомиллионных штрафов и компенсаций пострадавшим [57–59].

Наиболее громкие публичные утечки персональных данных в 2013 г. в России были выявлены в финансовой и телекоммуникационных сферах. Резонансное дело произошло весной 2013 г., когда жители города Зеленограда обнаружили банковские документы, раздуваемые ветром по дворам. Как выяснилось позже, это были документы Сбербанка России, выброшенные в мусорный бак. Среди утилизированных бумаг оказались заявления на выдачу пластиковых карт, подписанные договоры банковского обслуживания, заявления на выдачу кредитов. Было инициировано служебное расследование, результаты которого в открытый доступ не обнародовали [59].

4.2. Обзор зарубежного и отечественного законодательства в области защиты персональных данных

Частная жизнь человека, использующего информационные технологии на работе, в личных целях, становится уязвимой. Каждый гражданин РФ имеет право на неприкосновенность частной жизни, личную и семейную тайну, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений [1, ст. 23]. И сбор, распространение информации о частной жизни лица без его согласия запрещены [1, ст. 24].

До недавнего времени вопрос о частной жизни и персональных данных граждан не стоял так остро, но с развитием современных технологий, увеличением количества мошенничеств, киберпреступлений, а также преступлений, направленных против человека, этот вопрос стал одним из ключевых моментов по защите прав и свобод граждан.

В Российском законодательстве нет четкого определения частной жизни, но поскольку Россия ратифицировала международные договоры о гражданских и политических правах, Европейскую конвен-

цию о защите прав и свобод человека, то государство принимает на себя международное понятие частной жизни [1, ст. 15].

Под понятие «частная жизнь» подпадает область жизнедеятельности человека, которая имеет отношение к нему, касается только его и не подлежит контролю со стороны государства, если она не носит противоправного характера [38]. Таким образом, понятие «частная жизнь» охватывает многочисленные аспекты жизнедеятельности человека: от бытовых, семейных, интимных отношений, тайны усыновления, трудовых отношений до тайны переписки, покупки товаров, свободы высказываний, а также возможности доверить свои тайны священнику, врачу, адвокату без опасения их разглашения [52].

Право на обеспечение персональных данных возникает у гражданина с момента рождения и является тайной частной жизни [52, ст. 2]. Следовательно, защита персональных данных гражданина является составляющим права на неприкосновенность частной жизни, которая закреплена в Конституции РФ.

В европейских странах и в США переход к автоматизированным системам обработки информации начался ранее, чем в России, и, следовательно, вопрос защиты персональной информации развивался параллельно с информатизацией общества. Как следствие, институт защиты ПДн достаточно развит.

Обзоры зарубежной нормативной базы выполняются достаточно редко и, как правило, не являются общедоступными. Обзор, приведенный в данной работе, не претендует на полноту, мы анализируем только те источники, в которых имеется интересная, по мнению автора, к рассмотрению информация по теме исследования. Для удобства восприятия рассматриваемые документы расположены в хронологическом порядке по мере их публикации [43].

Под зарубежным законодательством понимаются нормативные документы различных стран в области права, технического регулирования процесса по защите персональных данных как обязательных к исполнению, так и носящих рекомендательный характер.

История вопроса по защите персональных данных в странах Европы начинается с 1981 г., в котором была подписана Конвенция Совета Европы «О защите личности в связи с автоматической обработкой персональных данных» (далее – Конвенция) [71], главной целью которой является обеспечение прав и свобод каждого человека на неприкосновенность частной жизни.

На сегодняшний день в Конвенции (с изменениями от 1999 г.) отсутствует понятие «информационная система обработки данных», но выделены следующие понятия: «автоматизированная база данных» и «автоматическая обработка».

Под автоматизированной базой данных понимается любой набор данных, подвергающихся автоматизированной обработке.

Под автоматической обработкой следует понимать операции, осуществляемые полностью или частично с помощью автоматизированных средств: хранение данных, осуществление логических и (или) арифметических операций с этими данными, их изменение, уничтожение, поиск или распространение.

Согласно данной Конвенции ПДн должны отвечать следующим требованиям:

– ПДн должны быть получены и обработаны добросовестным и законным образом;

– ПДн должны накапливаться для точно определенных и законных целей и не использоваться в противоречии с этими целями;

– ПДн должны быть адекватными, относящимися к делу и не быть избыточными применительно к целям, для которых они накапливаются;

– ПДн должны быть точными и в случае необходимости обновляться;

– ПДн должны храниться в такой форме, которая позволяет идентифицировать субъектов данных не дольше, чем этого требует цель, для которой эти данные накапливаются.

В дальнейшем институт защиты персональных данных стал развиваться стремительней. В октябре 1995 г. Европейский парламент и Совет Европейского Союза принимают директиву 95/46/ЕС [72], касающуюся защиты прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных. Основной целью данной директивы является возможность обработки персональных данных при наличии однозначного согласия субъекта персональных данных, даны определения основных понятий, прав и свобод частных лиц, определена ответственность за нарушение/разглашение персональной информации.

В декабре 1997 г. тот же Европейский парламент и Совет Европейского Союза принимают директиву 97/66/ЕС [72], касающуюся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций.

Выбор конкретных мер защиты, технических решений, стандартов, которыми необходимо руководствоваться, архитектур информационной системы остается в компетенции оператора персональных данных, но Европейский Союз рекомендует проведение сертификации по ISO27001 [73] к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы.

В Европейском Союзе реализованы комплексные механизмы защиты персональных данных, которые основываются на наличии общеевропейской нормативной базы, а также национальных законов, регламентирующих деятельность по защите персональных данных.

В странах Европы (например Норвегии, Исландии, государстве Лихтенштейн) создаются специализированные уполномоченные органы персональных данных, отвечающие за соблюдение безопасности в области их защиты. Это свидетельствует о том, что институт по защите персональных данных становится неотъемлемой частью национальных правовых систем [54]. Предусматривается административная и уголовная ответственность за утечку персональной информации и передачу ее третьим лицам.

Обзор нормативной базы в США. Вопрос по защите персональных данных в США начал развиваться в конце 60-х гг. XX в. Нормативные документы применялись как на федеральном уровне, так и на уровне штатов [18].

Основой информационных свобод граждан США является закон об информации (The Freedom of Information Act), который был принят в 1966 г. По данному федеральному закону США собранные федеральными органами власти персональные данные доступны всем желающим, кроме материалов, имеющих отношение к национальной безопасности, личным и финансовым документам, и материалов правоохранительных органов [74] для обеспечения безопасности граждан США, членов их семей, а также имущества.

В 1974 г. в США принимается закон «О защите конфиденциальности» (The Privacy Act), основной целью которого становится защита персональных данных граждан США от злоупотреблений со стороны государства. Данный закон стал одним из первых в мире законов о защите персональных данных в мире.

Как это ни странно, но нормативные документы регламентируют работу и являются обязательными только для государственных структур, для частных компаний выполнение данных требований но-

сит только рекомендательный характер [75], и дополнительно к основным законам в США применяются документы Национального института стандартов и технологий (NIST – National Institute of Standards and Technology). Основная задача института – это содействие повышению инновационной и индустриальной конкурентоспособности США путем развития наук с целью повышения экономической безопасности и улучшения качества жизни. NIST – неправительственная некоммерческая организация, которая не разрабатывает стандарты, а утверждает стандарты, разработанные авторитетными организациями, такими как Американское общество по испытаниям и материалам, Американское общество по контролю качества, Американское общество инженеров-механиков и др.

В руководстве по защите персональных данных «SP 800-122» [76], выпущенном NIST в 2009 г., содержатся организационные, технические, юридические рекомендации, а также примеры, которыми организации могут воспользоваться.

В данном документе рассмотрены требования, предъявляемые к защите ПДн. Ключевым требованием является систематическое обучение сотрудников нормам безопасной работы с персональными данными. Данный подход позволяет понять ценность информации, к которой сотрудник имеет доступ, оценить свою персональную ответственность за утечку такой информации, а также знать, как поступить, если обнаружил нарушения, связанные с обработкой данных.

Вторым требованием, описанным NIST, является обезличивание персональных данных. Обезличивание – это процесс обработки персональных данных таким образом, при котором нет возможности идентифицировать субъекта персональных данных. Логика этого требования такова, что если нет субъекта персональных данных, то и защищать его данные нет смысла. Следовательно, нет необходимости использовать дорогостоящие программные продукты по защите от несанкционированного доступа (далее НСД), можно минимизировать расходы на информационную безопасность, а также уменьшить риски.

Следующим шагом регламентируется создание политики безопасности в области защиты персональных данных, которая должна содержать в себе порядок доступа к ПДн, правила хранения ПДн, ограничения по работе с ПДн, а также порядок реагирования на инциденты и устранение их последствий.

После выполнения описанных выше требований в руководстве идут меры по защите управления доступом, авторизации и идентификации пользователей, маркировки и хранения носителей и др.

Таким образом, этапы по защите персональной информации сводятся к следующему: обезличить данные —> описать процедуры их обработки —> внедрить меры по защите.

Кроме федеральных законов, в различных штатах принимаются региональные законы по защите персональных данных, в основном это связано с тем, что наблюдается всплеск активности граждан по защите своих персональных данных.

Тем не менее, по оценкам Федеральной торговой комиссии США, которая отмечает, что каждая четвертая семья так или иначе столкнулась с проблемой утечки персональных данных (более 10 млн чел. – около 3,25 % населения [76]. В связи с этим сенатором-демократом Джеем Рокфеллером был представлен законопроект о запрете отслеживания личных данных и предпочтений в сети, внесенный в Сенат США, что позволит пользователям интернета блокировать отслеживание сбора информации об их деятельности в интернете [77].

Таким образом, в США законодатели, разрабатывая новые нормативные документы, пытаются защитить граждан от утечки их персональной информации, обеспечить их безопасность в сети интернет. Если учесть, что защита персональных данных – это комплекс организационных, технических и юридических мер, встроенных в отлаженный механизм защиты субъектов ПДн, то необходимо констатировать, что такая защита обеспечивается в США лишь частично.

Обзор нормативной базы в Германии. Первые шаги по разработке и внедрению закона по защите персональных данных Германия сделала в 1970 г., причем следует отметить, что данный закон был принят на региональном уровне [18]. Затем в 1977 г. был принят федеральный закон, основной целью которого было защитить индивидуума от посягательств на неприкосновенность его частной жизни.

Кроме этого закона, в каждом регионе страны действуют региональные законы по защите персональных данных, которые распространяются на государственные учреждения.

Закон о защите персональных данных (Federal Data Protection Act of December 20, 1990 г. (BGBl.I 1990 S.2954), amended by law of September 14, 1994 г. (BGBl. I S. 2325)) является весьма развернутым, в нем содержится 44 раздела, и все они посвящены персональным

данным, описан порядок их сбора, хранения, распространения, обработки и удаления.

В 1996 г. принимается постановление о защите персональных данных, передаваемых по телекоммуникационным каналам связи. За исполнением законодательства в области защиты персональных данных следит Федеральная комиссия персональных данных, а также соответствующие региональные комиссии, которые обеспечивают исполнение местного законодательства.

Законодательство распространяется как на государственные, так и на коммерческие организации. Сотрудники учреждений подписывают соглашения о неразглашении персональной информации, которая стала доступна им в ходе выполнения служебных обязанностей. Соглашение о нераспространении продолжает действовать и после перехода на другую работу.

Германия ратифицировала Конвенцию о защите частных лиц в отношении автоматической обработки персональных данных (ETS No. 108), а также Европейскую конвенцию о защите прав и основных свобод человека.

В настоящее время правительство Германии разрабатывает поправки к закону с целью приведения последнего к Директиве ЕС 97/66/ЕС.

Обзор нормативной базы в Великобритании. Великобритания входит в Организацию по экономическому сотрудничеству и развитию, ратифицировала Директиву ОЭСР о защите неприкосновенности частной жизни и международных обменов персональными данными, Конвенцию о защите частных лиц в отношении автоматической обработки персональных данных (ETS No. 108) вместе с Европейской конвенцией о защите прав и основных свобод человека [18].

Как такового закона о защите персональных данных в Великобритании нет, но есть Закон о защите информации, принятый в 1998 г. и составленный в соответствии с Директивой Европейского Союза. Действие закона распространяется как на государственные структуры, так и на частные компании [18]. В соответствии с данным законом все юридические лица должны регистрироваться в Комиссариате по защите информации, а также соблюдать требования закона на использование персональной информации (обработку, хранение, распространение и др.).

Кроме данного закона можно выделить еще так называемое семейство добровольных стандартов BS 7799, которые помогают орга-

низациям и учреждениям сформировать свои программы безопасности по защите конфиденциальной и персональной информации.

Несмотря на то, что данные стандарты являются добровольными, компании в Великобритании активно пользуются ими, чтобы обеспечить полноценную защиту любых видов информации (финансовой, кадровой, информации о контрагентах и др.). Следует особо отметить, что на практике данными стандартами стали пользоваться компании различных стран мира, так как благодаря им в организации можно построить полноценную и эффективную систему информационной безопасности.

Обзор нормативной базы стран СНГ. Развитие вычислительной техники в странах СНГ началось много позднее, чем в странах Европейского Союза. Поэтому законодательство по защите персональной информации, развитие прав и свобод граждан началось намного позже. Этот период можно отнести к 90-м гг. прошлого столетия, когда страны приобрели независимость. Поэтому институт защиты персональных данных в странах СНГ развит не столь качественно, как в западных странах и США.

Законодательства стран СНГ во многом схожи и опираются на принятый в 1999 г. на 14-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ Модельный закон «О персональных данных». Основной целью данного закона является защита прав человека в отношении его персональных данных и операций над ними, определение правового режима использования персональных данных и функций их держателей [78].

В конституциях этих стран гарантирована неприкосновенность частной жизни [79]. Положения, прописанные в конституциях, совпадают с принципами, провозглашенными Советом Европы. Так, в Конституции Республики Беларусь (ст. 28) и Конституции Кыргызской Республики (ст. 29) устанавливается, что «…каждый имеет право на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство».

Правовой механизм защиты персональных данных состоит из нескольких составляющих: во-первых, это специализированное законодательство в области защиты персональных данных; во-вторых, законодательство, обеспечивающее правовые нормы на неприкосновенность частной жизни; в-третьих, нормативные акты, регламентирующие сферу информации и защиты информации.

В Республике Беларусь как такового закона о защите персональных данных нет, в связи с чем отсутствует понятие «персональные данные». Такое понятие вводится в закон «О переписи населения» [80]. В данном законе персональные данные определяются как первичные статические данные о конкретном респонденте, сбор которых осуществляется при проведении переписи населения.

В законодательстве отсутствует классификация персональных данных, нет ответственности за разглашение и утечку персональных данных, а также за передачу их третьим лицам.

В законе «Об информации, информатизации и защите информации» также не определен статус понятия «персональные данные», но определено, что доступ к информации о частной жизни физического лица и персональным данным органичен [81], регулирует, что сбор, обработка, хранение информации о частной жизни лица осуществляются с согласия физического лица [81, ст. 18]. А также что никто не вправе требовать от физического лица информацию о его частной жизни, включая информацию о состоянии его здоровья, тайну телефонных переговоров, почтовых и иных сообщений.

Таким образом, в Республике Беларусь институт защиты персональных данных находится в зачаточном состоянии, что естественно вызывает много вопросов как у рядовых граждан, так и у экспертов по защите информации.

В ноябре 2013 г. в Республике Казахстан официально вступил в действие закон «О персональных данных и их защите» [82]. Основной целью, прописанной в ст. 2 данного закона, является обеспечение защиты прав и свобод человека и гражданина при сборе и обработке его персональных данных.

Закон призван регулировать процедуры сбора, хранения, обработки персональной информации, права и обязанности операторов по обработке такой информации, регламентирует государственное регулирование. Помимо закона «О защите персональных данных и их защите» вносятся изменения в Кодекс Республики Казахстан об административных правонарушениях и в Уголовный кодекс Республики Казахстан. В этих документах вводится административная ответственность за нарушение порядка обработки персональных данных в виде штрафа для физических и юридических лиц [83], лишения свободы либо лишения права занимать определенные должности или заниматься определенной деятельностью [84].

Также разработаны Правила осуществления собственником и (или) оператором [85], а также третьим лицом мер по защите персональных данных, которые описывают требования законодательства по выполнению организационных, технических мер, устанавливают порядок хранения носителей, определения ответственных лиц, процедуры обезличивания, уничтожения и др.

Таким образом, в Республике Казахстан также обеспокоены защитой персональных данных граждан, которые являются основой свобод и прав граждан, гарантированных Конституцией Республики.

В ст. 32 Конституции Украины определяется, что «…никто не может подвергаться вмешательству в его личную и семейную жизнь...». В связи с чем в 2011 г. был принят закон Украины «О защите персональных данных» [86], который регулирует отношения, связанные с защитой персональных данных при их обработке. В законе определено понятие персональных данных и указано, что персональные данные, кроме обезличенных, являются информацией с ограниченным доступом, кроме персональных данных, перечисленных в п. 4 ст. 5 Закона.

Согласно закону Украины все персональные данные, кроме обезличенных и указанных в п. 4 ст. 5, являются конфиденциальными. В законе прописаны права субъектов персональных данных, порядок сбора, обработки, хранения, распространения и других действий с персональными данными. Устанавливает ответственность за несоблюдение требований законодательства (установлена административная [87, ст. 182] и уголовная ответственности [88]).

Рассматривая нормативную базу различных государств по защите персональных данных, становится ясно, что для стран Европы, входящих в Европейский Союз или кандидатов на вступление в Европейский Союз, этот вопрос является приоритетной задачей, требующей серьезного отношения. Для стран СНГ институт защиты персональных данных достаточно молод, законодательные акты в большинстве своем требуют доработки, которые должны быть согласованы с экспертами в области информационной безопасности, а также необходимо использовать опыт других государств, у которых данный институт достаточно развит.

Обзор российского законодательства. История развития законодательства в странах Европы в области защиты информации насчитывает уже не одно десятилетие, в то время как в России данный вопрос начал бурно развиваться после ратификации Конвенции о защи-

те физических лиц при автоматизированной обработке персональных данных в 2005 г. [89].

Основываясь на ст. 23 и 24 Конституции РФ, которые гарантируют право на неприкосновенность частной жизни, личную и семейную тайну, а также запрет на сбор, хранение и распространение информации о частной жизни лица без его согласия, был принят Федеральный закон № 152-ФЗ «О персональных данных» в 2006 г.

Целью данного закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав «…на неприкосновенность частной жизни, личную и семейную тайну» [3, ст. 2].

Сфера деятельности закона – это регулирование отношений, связанных с обработкой персональных данных с использованием или без использования средств автоматизации.

Вступление закона в силу откладывалось до 2011 г., в основном это было связано с тем, что вызвало множество вопросов у экспертов в области информационной безопасности, а также невозможность выполнить требования ст. 25.3 Закона. В результате он претерпел серьезные изменения, которые были направлены на уменьшение и упрощение процедур. За это время было разработано множество нормативных актов, которые должны были помочь операторам организовать защиту персональных данных в своих автоматизированных системах.

В ст. 19 Закона говорится об организационных, правовых и технических требованиях к защите персональных данных, относящихся к различному уровню защищенности, а требования эти обеспечивают ФСБ России и ФСТЭК России.

В связи с чем только в 2008 г. появляются документы:

1. Так называемый «Закон трех» – это приказ ФСТЭК России, ФСБ России и Министерства информационных технологий и связи Российской Федерации от 13.02.2008 г. № 55/86/20 «О утверждении порядка проведения классификации информационных систем персональных данных».

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработанная ФСТЭК России [12].

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработанных ФСТЭК России [13].

Все эти документы были разработаны с целью организовать защиту информации в соответствии с требованиями законодательства. Количество документов, регламентирующих защиту персональных данных, увеличивается с каждым годом. Стоить выделить обязательные документы, с которыми должны быть знакомы все операторы ПДн:

2010 г. – приказ ФСБ России и ФСТЭК России № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

2012 г. – постановление Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [5].

2013 г. – приказ № 21 ФСТЭК России «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [10].

Замечу, что в настоящее время в Государственной Думе рассматривается несколько законопроектов, касающихся увеличения штрафов за невыполнение требований по защите ПДн, а также внесение изменений в ст. 10 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» [90], в ч. 4 ст. 12 Закона № 152-ФЗ «О персональных данных» про трансграничную передачу ПДн.

Законодательством определены регуляторы, осуществляющие контроль за исполнением закона. К таким регуляторам относятся:

– РОСКОМНАДЗОР – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (контроль за исполнением юридических требований закона, осуществление документального контроля);

– ФСТЭК – Федеральная служба по техническому и экспортному контролю (контроль за состоянием информационных систем и средств их защиты, осуществление технического контроля);

– ФСБ – Федеральная служба безопасности (контроль средств защиты информации при необходимости ее шифрования).

Таблица 1

Сравнение требований по защите ПДн в различных странах

Страна	Дата принятия закона о ПДн	Дата подписания/ратификации Директивы ЕС	Нормативные документы, в которых есть упоминание о защите ПДн	Обязательность выполнения	Количество утечек конфиденц. информ., в том числе ПДн за 2012 г.[91]	Ответственность за невыполнение требований	Адекватно защищают ПДн
США	2009	–	The Freedom of Information Act 1966) The Privacy Act (1974) SP 800-122 (2009)	Только государственные учреждения	576	Административная (очень высокие штрафы) Уголовная	–
Германия	1990	1981/1985	Federal Data Protection Act	На все организации	4		+
Англия	–	1981/1987	Закон о защите информации (1998) Стандарты BS 7799	На все организации	94		+
Белоруссия	–	–	Конституция Об информации, информатизации и защите информации	–	–	–	–
Казахстан	2013	–	Конституция О персональных данных и их защите КоАп, УК	На все организации	–	Административная Уголовная	–
Украина	2011	2005/2010	Конституция, О персональных данных и их защите, КоАп, УК	На все организации	6	Административная Уголовная	+
Россия	2006	2001/2013	Конституция, О защите ПДн, КоАп, УК, документы ФСТЭК, ФСБ, РОСКОМНАДЗОР	На все организации	75	Административная Уголовная	+

Государство, таким образом, более серьезно обеспокоилось о защите персональных данных граждан. Роль государства не ограничивается только законотворческой деятельностью, а предоставляет гражданам гарантии, что их персональные данные будут в безопасности, оставляя за собой право осуществлять контроль за выполнением всех требований.

В связи с вышесказанным защита персональных данных является актуальной задачей, а порядок защиты персональных данных остается серьезным вопросом, требующим внимательного к себе отношения не только со стороны государственных структур, учреждений и организаций, обрабатывающих персональные данные, но и самих граждан.

Как видно из табл. 1, в странах Европы и США институт защиты персональных данных начал развиваться достаточно давно, к настоящему времени проработана нормативная база: разработаны не только законы, в которых прописаны обязанность защищать персональные данные и ответственность за невыполнение этих требований, но и разработаны национальные и международные стандарты, в которых приводятся конкретные примеры по реализации необходимой защиты.

Также стоит отметить, что некоторые страны, по версии РОСКОМНАДЗОРа, не обеспечивают полноценную защиту персональных данных не только своих граждан, но и граждан других стран. Поэтому трансграничная передача персональных данных с этими странами должна соответствовать требованиям российского законодательства [2; 62].

4.3. Проблемы применения нормативно-правовых актов в сфере ПДн

Серьезность вопроса защиты персональных данных не вызывает сомнения, и именно поэтому государство поставило этот вопрос под контроль. Но с чем же связаны проблема его реализации, негативное восприятие со стороны экспертного сообщества и руководителей организаций?

Как отмечалось выше, требования закона выполнили государственные, муниципальные учреждения, а также организации, относящиеся к сегменту крупного бизнеса. Большая же часть компаний среднего и малого бизнеса, индивидуальные предприниматели проигнорировали закон. Основными причинами, по которым компании

не выполняют требования законодательства и не спешат выполнять их являются:

– постоянно меняющиеся нормативные акты, запутанность терминологии, юридические коллизии;

– отсутствие в штате квалифицированного юриста, владеющего знаниями, касающимися персональных данных;

– отсутствие технических работников (программистов, системных администраторов), которые могут настроить автоматизированную систему в соответствии с требованиями законодательства;

– высокая стоимость услуг сторонних организаций (аутсорсинг) по приведению документации и технических средств в соответствие с требованиями законодательства;

– высокая стоимость аппаратно-программных средств, обеспечивающих качественную защиту персональных данных;

– несоизмеримость штрафов и затрат на подготовку и внедрение системы защиты персональных данных.

Существуют проблемы, связанные с толкованием понятий. С введением закона понятие «персональные данные» получило более общее определение и толкование. В законе под персональными данными понимается любая информация, относящаяся к определенному лицу или определяемому физическому лицу [3, п. 1 ст. 3] (к такой информации можно отнести: фамилию, имя, отчество, дату рождения, место рождения, адрес, номера мобильных и домашних телефонов, адрес электронной почты, семейное положение, образование, доходы, вероисповедание, национальность и другие данные). В других законодательных актах в зависимости от цели правового применения понятие «персональные данные» может быть конкретизировано.

Например, в Федеральном законе «Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования» от 1 апреля 1996 г. к персональным данным застрахованного лица относят фамилию, имя, отчество, пол, дату и место рождения, страховой номер, паспортные данные, адрес постоянного места жительства, гражданство, стаж, сумма дохода и др. [92, ст. 6].

Трудовой кодекс РФ [2, гл. 14] под персональными данными работника подразумевает информацию, относящуюся к работникам, выполняющим обязанности, прописанные трудовым договором. К таким данным относят табельный номер, дату трудового договора, документы воинского учета, фотографии, образование, квалификацию,

занимаемую должность, наличие детей, приказы, заявления, сведения о здоровье, оклад и др. [14; 19; 20; 36].

Для различных целей обработки персональных данных само понятие «персональные данные» может включать в себя множество атрибутов, которые характеризуют конкретного человека и могут по каким-либо признакам идентифицировать личность.

Понятие «персональные данные» должно обладать двумя признаками: во-первых, оно должно относиться к конкретному физическому лицу, что позволило бы его идентифицировать, а во-вторых, такая информация должна быть зафиксирована на материальном носителе (бумажные документы: личные дела, заявления, приказы и пр.; физические носители: съемные, жесткие диски) [93].

Итак, определив понятие «персональные данные» и кому они могут принадлежать, можно начинать построение системы защиты персональных данных. Опираясь на [5], операторы ПДн должны определить актуальные угрозы безопасности, определить выбор средств защиты, определить уровень защищенности информационной системы и тип информационной системы (обрабатывающая специальные категории ПДн, обрабатывающая биометрические данные ПДн, обрабатывающая общедоступные категории ПДн), в которой обрабатываются персональные данные *сотрудника* оператора ПДн. У операторов ПДн мгновенно возникает вопрос: «Кто такой сотрудник оператора ПДн?» Ведь в Трудовом кодексе РФ не определено понятие «сотрудник», существует понятие «работник». А раз такого понятия не определено, следовательно, действие данного документа не распространяется на большинство юридических лиц, являющихся работодателем [94].

Таким образом, юридическая коллизия на лицо. Регуляторы считают, что действие должно распространяться на всех работодателей, а те, в свою очередь, считают иначе, и ситуация с юридической точки зрения по-прежнему висит в воздухе.

В настоящее время развернулась в экспертном сообществе дискуссия о необходимости лицензирования ПДн в области деятельности по технической защите конфиденциальной информации, к которой персональные данные относятся.

Позиция ФТЭК России: лицензия на деятельность по технической защите конфиденциальной информации (далее – ТЗКИ) нужна только в трех случаях:

– организация извлекает прибыль из деятельности по ТЗКИ;

– деятельность организации по ТЗКИ прописана в уставных документах организации;

– защита конфиденциальной информации в явной форме поручена ее обладателем организации.

В этом случае становится ясно, что для операторов ПДн, обрабатывающих персональные данные для собственных нужд, лицензия на ТЗКИ не нужна. Тогда как быть с операторами ПДн, которые их обрабатывают по договору? В п. 3 требований Постановления также говорится, что «…договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе», а в ч. 3 ст. 6 закона содержится норма включать в поручение оператора требование обеспечивать безопасность персональных данных при их обработке, а также указать требования к защите обрабатываемых персональных данных в соответствии со ст. 19 закона.

Исходя из вышесказанного возникает вопрос. Если оператор ПДн явно передал третьей стороне право обрабатывать данные, то требуется ли лицензия на ТЗКИ аутсорсерам, выполняющим данные услуги по договору?

Еще один интересный факт вытекает из [5]. В п. 13 обозначено требование наличия защиты контролируемой зоны при обработке ПДн (т.е. зоны, в которую запрещен доступ посторонних). Например, выносная точка продаж сим-карт в торговом центре: при продаже карты клиент указывает свои персональные данные (фамилия, имя, отчество, паспортные данные и др.) в договоре, один экземпляр которого остается у продавца. По логике закона получается, что посторонние лица не могут находиться в помещениях, в которых обрабатываются ПДн. И получается, что доступ покупателей в торговый центр должен быть запрещен или выносная точка продажи должна быть оборудована сигнализацией, сейфом и другими устройствами, а также должна быть огорожена [95].

Таких спорных вопросов большое количество, и в них разбираются специалисты информационной безопасности, юристы, эксперты. А что делать небольшим организациям и индивидуальным предпринимателям, которые не могут позволить себе иметь в штате таких специалистов?

Проблема отсутствия специализированных работников становится достаточно актуальной. В небольших городах, поселках суще-

ствует проблема нехватки специалистов по информационной безопасности. Небольшим компаниям приходится выбирать между несколькими вариантами решения проблемы: первый – выполнить требования законодательства своими силами; второй – привлечь на выполнение этих работ специализированную фирму; третий – оставить все как есть и ждать проверки со стороны регулятора, выплатив по их результатам штрафы.

Стоимость привлечения сторонних организаций на выполнение услуг, покупку технических и аппаратных средств защиты в настоящее время намного выше штрафных санкций, поэтому многие руководители организаций осознанно выбирают либо формальное выполнение требований законодательства, либо оплату штрафа.

4.4. Теоретические основы защиты персональных данных

Рассматриваемому вопросу по защите персональных данных с научной точки зрения уделяется много внимания. Связано это в основном с тем, что проблема актуальна и требует пристального изучения.

Работы, посвященные этому вопросу, нашли отражение в трудах ряда российских специалистов. Причем в этих вопросах рассматриваются различные проблемы: от вопроса по категорированию ПДн, обезличиванию ПДн до вопросов оценки рисков безопасности, разрабатываются новые методики, методы и модели, а также различные алгоритмы. Например, в работе *О.М. Голембиовской* [19] поднимается вопрос выбора средств защиты персональных данных, обрабатываемых в информационных системах, на основе оценки их защищенности. Основной целью работы является снижение трудоемкости и повышение эффективности защиты персональных данных посредством разработки универсальных методов и методик категорирования ПДн, определения уровня защищенности и выбора средств защиты ПДн, обрабатываемых в информационных системах.

В своей работе автор акцентирует внимание на том, что операторам ПДн, которые решили самостоятельно привести ИСПДн в соответствие требованиям законодательства, порой сложно вникнуть в суть проблемы из-за недостаточной компетенции в сфере информационной безопасности. Операторы ПДн могут совершить ряд распространенных ошибок: от определения типа информационной системы до формирования актуальных угроз и, как следствие, неправильного выбора средств защиты, который приведет к наложению штрафа ре-

гулятором и непредусмотренным затратам по переоснащению средствами защиты.

Результатами работы О.М. Голембиовской явились разработки методик по определению категории персональных данных, позволяющих однозначно определять каждую категорию ПДн и исключать неоднозначность определения категорий, а также методика оценки защищенности персональных данных, позволяющая в соответствии с нормативно-правовой базой объективно оценить уровень защищенности ИСПДн.

Вопросы по построению систем защиты персональных данных нашли свое отражение в работах В.И. Аверченкова, Е.К. Волчинской. *Е.С. Волокитина* [17] поднимает вопрос об обезличивании персональных данных с последующей невозможностью по остаточным данным их идентифицировать. Этот вопрос также является актуальным. По нормативным документам данное требование является обязательным для государственных и муниципальных операторов ПДн. Поэтому разработка алгоритмов и методов по обезличиванию, повышению их надежности и эффективности является приоритетной задачей, что и явилось целью работы Е.С. Волокитиной.

Автор разработал и внедрил математическую модель обезличивания персональных данных и проверку невозможности реидентификации субъекта по обезличенным персональным данным. Разработанная модель позволяет более продуктивно исследовать особенности моделируемого процесса обезличивания, более эффективно строить информационные системы, разработан алгоритм обезличивания персональных данных с применением хеширования данных и алгоритм реидентификации субъекта ПДн. Данная проблема рассматривалась в работах Р.В. Шередина [96], И.Ю. Кучина [97].

Большое количество научных работ посвящено юридической стороне вопроса, анализу правового регулирования персональных данных, правам и обязанностям оператора персональных данных.

Изучив научные труды, литературу по вопросам защиты персональных данных, можно выделить несколько типов вопросов, на которые ученые, эксперты в области информационной безопасности пытаются найти ответы:

– правовые исследования российского и зарубежного законодательства;

– развитие правового института персональных данных в России;

– исследования информационных систем персональных данных в конкретной отрасли или регионе (например в здравоохранении, пенсионном фонде или в государственных учреждениях г. Москвы);

– методы и алгоритмы построения информационной системы персональных данных;

– построение системы защиты методом обезличивания;

– разработка автоматизированных систем для выбора средств защиты персональных данных;

– оценка защищенности информационных систем.

5. ОЦЕНКА ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Этапы построения системы защиты

Для более эффективного подхода к построению информационной системы персональных данных, для устранения неточностей в формулировках приняты дополнительные постановления Правительства, приказы, рекомендации Регуляторов, помогающие операторам связи выполнить все требования по защите персональных данных [5; 10–13].

При построении информационной системы, обрабатывающей персональные данные, необходимо руководствоваться документами, которые регламентируют следующие вопросы:

– порядок проведения классификации информационных систем персональных данных;

– требования к материальным носителям;

– требования к хранению персональных данных вне информационных систем персональных данных;

– построение базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– методы и способы защиты информации в информационных системах персональных данных;

– определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– порядок определения уровней защищенности ИСПДн.

Анализируя методические рекомендации контролирующих органов (ФСТЭК, ФСБ, РОСКОМНАДЗОР) в области защищенной обработки персональных данных, можно сделать вывод, что выполнить требования законодательства можно при условии деления этих требований на несколько этапов.

ФСТЭК России утвердила состав и содержание мер для выполнения требований закона, документ позволяет выделить несколько этапов по проведению защиты персональных данных [5; 10]. Ниже приведены обобщенные этапы реализации требований:

– **организационные мероприятия.** Целью данного этапа является назначение ответственного лица, в обязанности которого входят взаимодействие с субъектами ПДн; обработка ПДн; взаимодействие с

третьими лицами по вопросам передачи и получения ПДн; взаимодействие с регулирующими органами; обеспечение безопасности ПДн. Результатом выполнения данного этапа служат внутренние документы компании (например, приказ о назначении ответственного за организацию работ по защите ПДн, приказ о назначении администратора безопасности ИСПДн и др.);

– **определение класса информационной системы персональных данных (ИСПДн).** На этом этапе в зависимости от структуры информационной системы, категорий и объема обрабатываемых персональных данных определяется класс информационной системы. Результатом данного этапа является сформированный акт классификации информационной системы персональных данных, в котором отражены категория, объем и класс ИСПДн, а также характеристики ИСПДн;

– **формирование модели угроз.** Обеспечение безопасности ПДн достигается, в частности, определением угроз безопасности ПДн при их обработке в ИСПДн и формированием на их основе моделей угроз с целью их последующей нейтрализации. Для формирования требований к системе защиты ПДн необходимо построить частные модели угроз безопасности ПДн для каждой из выделенных в компании ИСПДн. Результат этапа – документы «Частные модели угроз» и «Модели нарушителя безопасности ПДн»;

– **техническая реализация требований по защите ПДн.** На этом этапе особое внимание удаляется внедрению аппаратно-программных средств, позволяющих нейтрализовать актуальные угрозы. При проектировании системы безопасности требуется рассмотреть различные угрозы, которые могут возникнуть (например, угроза загрузки с внешних носителей информации; выявление уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы; угроза несанкционированного доступа и др.).

Стоит заметить, что для организации защиты персональных данных первые три пункта методических рекомендаций требуют только организационных решений без затрат на материальные ресурсы. В последнем, четвертом пункте в рамках реализации технических требований по защите ПДн необходимо будет затратить денежные средства на внедрение/установку аппаратных средств защиты ПДн (например, Secret Net, который поддерживает процедуры идентификации и аутентификации; электронный замок «Соболь»), программ-

ных средств (например, средства антивирусной защиты, защиты от вторжений и средств имитации, межсетевые экраны и пр.).

На рис. 6 представлена схема приведения ИСПДн в соответствие требованиям законодательства. Выполнение каждого этапа связано с трудоемким процессом: изучением законодательства, подготовкой организационно-распорядительной документации, обучением сотрудников, связанных с обработкой персональных данных, внедрением технических средств защиты, настройкой программно-аппаратных средств защиты.

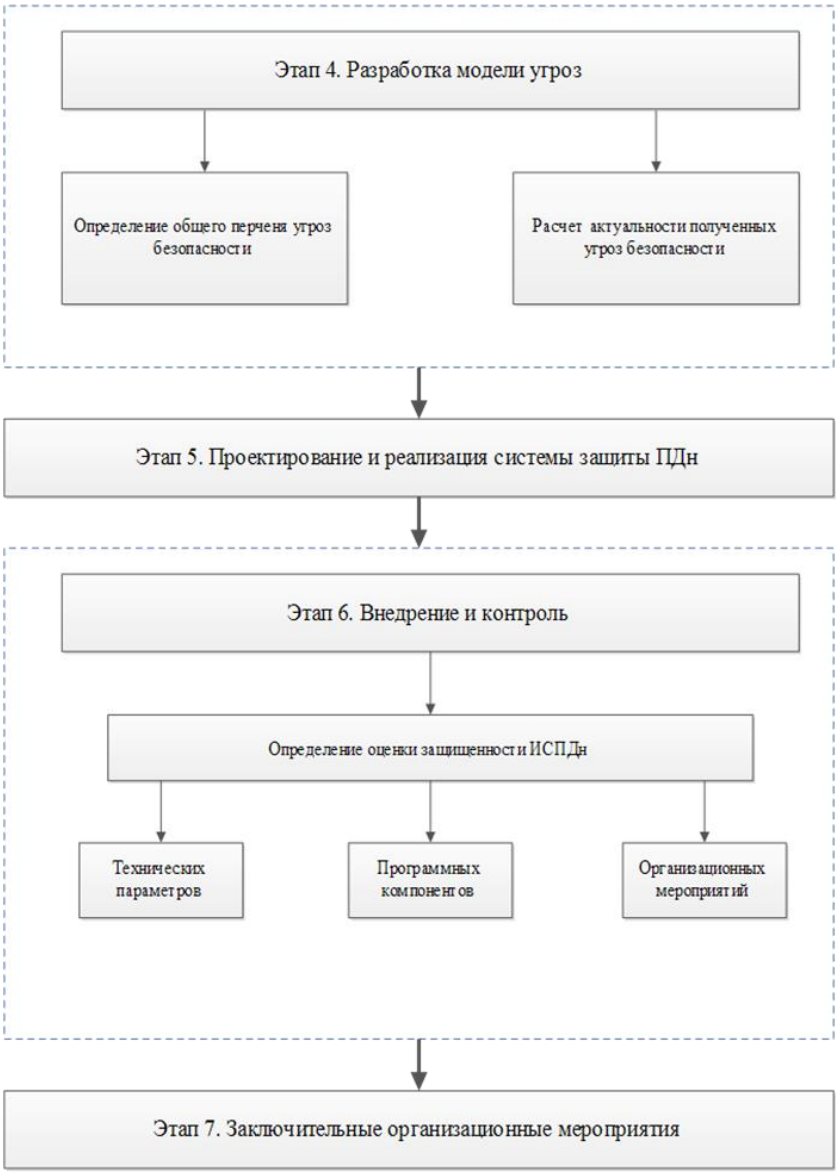

Рис. 6. Схема приведения ИСПДн

При выполнении первого этапа **«Первичные организационные мероприятия»** следует подробно изучить законодательство, определить ответственных лиц, отвечающих за сохранность персональных данных, взаимодействие между организацией, субъектами ПДн, Регуляторами, определить порядок передачи ПДн третьим лицам, в том числе трансграничную передачу. Подготовить приказы о назначении ответственных лиц, порядок допуска работников к персональным данным, порядок устранения инцидентов, связанных с утечкой персональных данных, разработать форму согласия субъекта ПДн с обработкой его данных, должностные инструкции для работников, в обязанности которых входит обработка ПДн.

Второй этап **«Определение состава обрабатываемых персональных данных»** необходим для определения следующих данных:

– состав персональных данных: необходимо определить, какие виды персональных данных будут использоваться и в каких бизнес-процессах, пути миграции ПДн в структуре информационной системы;

– цели обработки ПДн необходимо установить в соответствии с требованиями п. 2 ст. 5 закона (для выполнения трудового договора, оказания услуг, продажи товаров и др.);

– сроки хранения персональных данных (для различных целей обработки ПДн устанавливаются различные сроки хранения, и оно должно осуществляться не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в их достижении [3, п. 2 ст. 5]);

– условия обработки ПДн вытекают из установленных целей обработки;

– основание для обработки ПДн является критичным условием для обработки ПДн в организации. Необходимо получить письменно разрешение субъекта ПДн во избежание негативных последствий для оператора ПДн. Основной целью этого этапа является документирование всех правил обработки и защиты ПДн, в том числе для повышения осведомленности конечных пользователей.

Один из самых трудоемких этапов – **«Определение класса ИСПДн»**. Данный этап состоит из двух составляющих:

– определение объема ПДн (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);

– определение категории ПДн.

Именно последняя составляющая является затруднительной, так как отсутствуют поясняющие комментарии к термину «идентификация». Сложность задачи заключается в определении состава ПДн, который позволяет идентифицировать субъекта ПДн.

На этом этапе необходимо изучить бизнес-процессы, связанные с обработкой ПДн, а также определить программные и аппаратные средства, с помощью которых ведется их обработка. Как правило, на этом этапе, в зависимости от целей обработки ПДн, выделяют несколько ИСПДн, для которых важно определить ее тип:

– ИСПДн-С – информационная система, обрабатывающая специальные категории персональных данных (например, данные о расовой, национальной принадлежности, интимной жизни, политических взглядах, философских убеждениях);

– ИСПДн-О – информационные системы, обрабатывающие общедоступные категории персональных данных (если данные в информационной системы получены только из общедоступных источников);

– ИСПДн-Б – информационная система, обрабатывающая биометрические персональные данные (если в ней обрабатываются сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить личность человека);

– ИСПДн-И – информационная система, обрабатывающая иные категории персональных данных;

– информационная система, обрабатывающая только данные сотрудников оператора ПДн.

Данная классификация введена с [5] взамен классификации, которая разбивала ИСПДн на классы от К4 (информационная система обрабатывает общедоступные персональные данные) до К1 (информационная система обрабатывает специальные категории персональных данных и субъектов ПДн более чем 100 000).

Согласно данному подходу система защиты персональных данных, включающая в себя организационные и (или) технические меры, определяется с учетом актуальных угроз безопасности персональных данных и информационных технологий.

Актуальные угрозы необходимо определить на четвертом этапе **«Разработка моделей угроз».**

В соответствии с п. 6 [5] под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

В данном документе выявлено три типа угроз:

– «угрозы 1-го типа» актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе;

– «угрозы 2-го типа» актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в при-

кладном программном обеспечении, используемом в информационной системе;

– «угрозы 3-го типа» актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Оценка актуальности угроз безопасности ПДн проводится при моделировании действий различных групп нарушителей, использующих те или иные уязвимости, характерные для анализируемой ИСПДн.

Наличие формализованного описания актуальных угроз безопасности ПДн дает возможность подразделениям организаций и лицам, ответственным за безопасность персональных данных [98]:

– адекватно оценить необходимость реализации тех или иных мероприятий по обеспечению безопасности ПДн, исходя из состояния защищенности ИСПДн на текущий момент;

– спрогнозировать развитие ИСПДн на краткосрочную и среднесрочную перспективу, провести оптимизацию бюджетов соответствующих подразделений, выставить приоритеты по принимаемым мерам по обеспечению безопасности ПДн.

При обработке персональных данных в информационных системах выделяются четыре уровня защищенности персональных данных [5]:

– **для обеспечения 4-го уровня защищенности** устанавливаются требования об организации режима безопасности помещений, в котором обрабатываются ПДн, обеспечение сохранности носителей персональных данных, определения перечня лиц, имеющих доступ к ПДн, использование сертифицированных средств защиты, если применение таких средств необходимо для нейтрализации актуальных угроз. Для данного уровня защищенности актуальны угрозы 3-ого типа (более подробное описание угроз, описано в табл. 3);

– **для обеспечения 3-го уровня защищенности** устанавливаются следующие требования: выполнение требований, актуальных для обеспечения 4-го уровня защищенности, а также назначение должностного лица, ответственного за обеспечение безопасности персональных данных. Для данного уровня защищенности актуальны угрозы 3-го или 2-го типа;

– **для обеспечения 2-го уровня защищенности** устанавливаются следующие требования: выполнение требований, актуальных для обеспечения 3-го уровня защищенности, а также ведение электронного

журнала сообщений и ограничение доступа к данному журналу. Для этого типа защищенности характерны угрозы 2-го или 3-го типа;

– **для обеспечения 1-го уровня защищенности** устанавливаются следующие условия: выполнение требований, актуальных для обеспечения 3-го уровня защищенности, а также создание структурного подразделения, обеспечивающего безопасность персональных данных и ведение электронного журнала безопасности и фиксации в нем изменений полномочий сотрудника оператора по доступу к персональным данным. Для данного уровня защищенности характерны угрозы 1-го или 2-го типа. В табл. 2 приведена новая классификация ИСПДн с уровнями защищенности для каждого из типов.

Таблица 2

Соответствие типа ИСПДн и актуальных угроз

Тип ИСПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			1-й	2-й	3-й
ИСПДн-С	Нет	> 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100 000	УЗ-1	УЗ-2	УЗ-3
	Да	–			
ИСПДн-Б	–	–	УЗ-1	УЗ-2	УЗ-3
ИСПДн-И	Нет	> 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да	–			
ИСПДн-О	Нет	> 100 000	УЗ-2	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4

Определив уровень защищенности ИСПДн (УЗ ИСПДн) [10], оператор ПДн может юридически доказать минимизацию используемых средств защиты и, как следствие, затрат на их приобретение [22; 24]. Например, при выборе УЗ ИСПДн 4-го уровня защищенности возникает необходимость использования 27 мер по защите, а при 1-м уровне защищенности количество мер по защите возрастает до 69 [10].

Пятый этап **«Проектирование и реализация системы защиты ПДн»** тоже достаточно трудоемкий. Он включает в себя работы по консолидации уже собранной информации.

Помимо типов угроз, указанных [5], операторам ПДн при построении комплексной защиты информационной системы необходимо руководствоваться приказом ФСТЭК России [10]. Данный документ направлен на реализацию нормы ч. 4 ст. 19 закона «О персональных данных», определяет 15 мер и дает их детальное содержание:

1. **Меры по идентификации и аутентификации субъектов доступа и объектов доступа.** Эти меры должны обеспечивать присвое-

ние субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

2. **Меры по управлению доступом субъектов доступа к объектам доступа** должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

3. **Меры по ограничению программной среды** должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

4. **Меры по защите машинных носителей персональных данных** (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

5. **Меры по регистрации событий безопасности** должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

6. **Меры по антивирусной защите** должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

7. **Меры по обнаружению (предотвращению) вторжений** должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и

блокирования доступа к персональным данным, а также реагирование на эти действия.

8. **Меры по контролю (анализу) защищенности персональных данных** должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

9. **Меры по обеспечению целостности информационной системы и персональных данных** должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

10. **Меры по обеспечению доступности персональных данных** должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

11. **Меры по защите среды виртуализации** должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям и (или) воздействие на них.

12. **Меры по защите технических средств** должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, а также защищать технические средства от внешних воздействий, а также персональные данные, представленные в виде информативных электрических сигналов и физических полей.

13. **Меры по защите информационной системы, ее средств, систем связи и передачи данных** должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

14. **Меры по выявлению инцидентов и реагированию на них** должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

15. **Меры по управлению конфигурацией информационной системы и системы защиты персональных данных** должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Документ конкретизирует реализацию мер для каждого уровня защищенности ПДн. В нижеприведенной табл. 3 собраны воедино требования по обеспечению безопасности для различных уровней защищенности [5; 10].

На шестом этапе – **«Внедрение и контроль»** – осуществляется внедрение средств защиты, организационных мероприятий и программного обеспечения, которые соответствуют уровню защищенности системы персональных данных, определенного на предыдущем этапе.

Последний этап – **«Заключительные организационные мероприятия»** – включает в себя подготовку документов, таких как уведомление в уполномоченный орган по защите прав субъектов ПДн, приказы на прохождение обучения сотрудников (работников) оператора ПДн, с целью ознакомить последних с правилами работы в информационной системе персональных данных для минимизации потерь (утечек) персональных данных, а также разработку методических материалов, в которых описываются действия сотрудников по регистрации утечек персональных данных и ликвидации их последствий.

Таблица 3

Соответствие типов угроз необходимым требованиям

УЗ ПДн	Обоснование необходимости обеспечения УЗ	Организационно-технические меры	Требования по использованию сертифицированных средств защиты
4-й уровень	а) для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает общедоступные персональные данные; б) для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора	а) организация режима обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения; б) обеспечение сохранности носителей персональных данных; в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей; г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	а) средства вычислительной техники не ниже 6-го класса; б) системы обнаружения вторжений и средства антивирусной защиты не ниже 5-го класса; в) межсетевые экраны 5-го класса

УЗ ПДн	Обоснование необходимости обеспечения УЗ	Организационно-технические меры	Требования по использованию сертифицированных средств защиты
3-й уровень	а) для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора; б) для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора; в) для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора; г) для информационной системы актуальны угрозы 3-го типа, и информаци-	Выполнение требований для 4-го уровня защищенности, а также назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе	а) средства вычислительной техники не ниже 5-го класса; б) системы обнаружения вторжений и средства антивирусной защиты не ниже 4-го класса защиты в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и системы обнаружения вторжений и средства антивирусной защиты не ниже 5-го класса защиты в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена; в) межсетевые экраны не ниже 3-го класса в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4-го класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с

УЗ ПДн	Обоснование необходимости обеспечения УЗ	Организационно-технические меры	Требования по использованию сертифицированных средств защиты
	онная система обрабатывает биометрические персональные данные; д) для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора		информационно-телекоммуникационными сетями международного информационного обмена
2-й уровень	а) для ИС актуальны угрозы 1-го типа, и ИС обрабатывает общедоступные ПДн; б) для ИС актуальны угрозы 2-го типа, и ИС обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора; в) для ИС актуальны угрозы 2-го типа, и ИС обрабатывает биометрические ПДн; г) для ИС актуальны угрозы 2-го типа, и ИС обрабатывает общедоступные персональные данные более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора; д) для ИС актуальны угрозы 2-го типа, и ИС обрабатывает иные катего-	Необходимо выполнение требований для 3-го, 4-го уровней защищенности, а также организация доступа к содержанию электронного журнала сообщений, который был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей	а) средства вычислительной техники не ниже 5-го класса; б) системы обнаружения вторжений и средства антивирусной защиты не ниже 4-го класса; в) межсетевые экраны не ниже 3-го класса в случае актуальности угроз 1-го или 2-го типов или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4-го класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена

УЗ ПДн	Обоснование необходимости обеспечения УЗ	Организационно-технические меры	Требования по использованию сертифицированных средств защиты
	рии персональных данных более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора; е) для ИС актуальны угрозы 3-го типа, и ИС обрабатывает специальные категории персональных данных более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора		
1-й уровень	а) для ИС актуальны угрозы 1-го типа, и ИС обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных; б) для ИС актуальны угрозы 2-го типа, и ИС обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора	Необходимо выполнение требований для 2-го, 3-го, 4-го уровней защищенности, а также: а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе; б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности	

5.2. Анализ возможностей программных продуктов по защите конфиденциальной информации

Принятие закона № 152-ФЗ «О персональных данных» повлияло на то, что многие компании, разрабатывающие программное обеспечение, начали разработку и внедрение программных продуктов (решений), позволяющих компаниям при небольших денежных и временных затратах выполнить требования законодательства (по сравнению с услугами, которые оказывают компании – интеграторы по защите информации).

Разработчики программ для защиты персональных данных предлагают различный функционал, от которого зависит уровень защищенности ИСПДн. В некоторых решениях – это только скрытие и (или) блокировка файлов и папок или разработка полного комплекта документов, регламентирующих выполнение требований закона; у других – это полноценное шифрование, у третьих – от разработки организационно-распорядительных документов до настройки, внедрения и страхования финансовых рисков.

Программное обеспечение, обеспечивающее безопасность информационных систем персональных данных, обязано пройти сертификацию на соответствие требованиям закона и получить сертификат соответствия ФСТЭК России.

Программные решения, которые обеспечивают выполнение требований законодательства, можно разделить на следующие группы:

– документированные: подобные решения позволяют подготовить организационно-распорядительную документацию, которую запрашивает регулятор (РОСКОМНАДЗОР) при документарной проверке. Как правило, это веб-сервисы, позволяющие пользователю в режиме онлайн решить вопрос подготовки документации. Такие сервисы реализованы по принципу анкетирования с дальнейшим формированием перечня необходимых документов (приказов, положений, планов работ, журналов учета и т.д.);

– программно-аппаратные: позволяют подготовить не только необходимую документацию, а также рекомендуют аппаратно-программные средства для защиты персональных данных, исходя из особенностей ИСПДн. Функционал автоматизированных систем данной группы, значительно отличается от функционала веб-решений первой группы. Данные системы, работающие также по принципу анкетирования, разрабатывают комплект документов, регламентирую-

щих вопросы обработки и защиты персональных данных, но кроме этого и формируют рекомендации по выбору аппаратно-технических средств защиты информации;

– комплексные: позволяют выполнить технические требования законодательства для ИСПДн любого класса. Следует отметить, что данные решения имеют обязательную сертификацию ФСТЭК России или ФСБ России. И здесь функционал различных аппаратно-программных комплексов существенно различается в зависимости от целей и задач [44–46].

Если с программными решениями, относящимися к первым двум группам, все понятно, и их использование рассчитано на пользователей, не обладающих высокими компетенциями в области информационной безопасности. Тогда как решения третьей группы необходимо детально проанализировать.

В данном исследовании анализ проведен по нескольким группам программного обеспечения:

– средства защиты от несанкционированного доступа;

– средств антивирусной защиты;

– межсетевые экраны;

– программы для проведения аудита информационной безопасности.

Ниже представлен обзор специализированного программного обеспечения, позволяющего обеспечить надежную защиту конфиденциальной информации. Данный обзор разбит на несколько групп:

– **защита от НСД.** В эту группу входит программное обеспечение, позволяющее обеспечить: разграничение доступа пользователей к информации и ресурсам автоматизированной системы; контроль утечек и каналов распространения конфиденциальной информации; аутентификация пользователей;

– **антивирусная защита** – это программное обеспечение позволяет обнаружить и лечить наиболее сложные активные заражения компьютера, когда вредоносная программа уже была ранее запущена и установлена и, более того, маскирует свое присутствие в системе;

– **межсетевые экраны** осуществляют блокировку неавторизованных сетевых коммуникаций, подразделяемых на внутренние и внешние;

– **DLP-решения**, позволяющие распознавать и классифицировать информацию, записанную в объекте (например, в сообщении электронной почты, файле, приложении), и динамически применять к

этим объектам разные правила, начиная от передачи уведомлений и заканчивая блокировкой;

– **программы для проведения аудита безопасности.**

Группа «Средства защиты от несанкционированного доступа». Анализ наиболее распространенных систем защиты информации от НСД и утечки информации: Secret Net 7.0 (разработчик ООО «Код безопасности», г. Москва), Dallas Lock 8.0 (разработчик ООО «Конфидент», г. Санкт-Петербург) (табл. 4).

Сравнительный анализ систем защиты информации от НСД выполнен на основе [10].

Кроме основных мер по обеспечению безопасности персональных данных, взяты еще следующие параметры: наличие сертификатов ФСТЭК, количество клиентов, среда функционирования, техническая поддержка.

Данные средства защиты имеют все необходимые лицензии ФСТЭК России, которые позволяют использовать их для защиты информации в автоматизированных системах класса до 1Б включительно и в ИСПДн до первого класса включительно.

Secret Net 7.0 и Dallas Lock 8.0 могут функционировать на любом компьютере под управлением операционных систем семейства Windows, поддерживают 32- и 64-битные версии операционных систем. Средства защиты информации (далее – СЗИ) могут функционировать в двух режимах: автономный и сетевой режимы, обеспечивая защиту от несанкционированного доступа через локальный, сетевой и терминальный входы.

Таблица 4

Сравнительный анализ СЗИ от НСД

Меры по обеспечению безопасности ПДн	Secret Net 7.0 [99]	Dallas Lock 8.0 [100]
Идентификация и аутентификация субъектов доступа и объектов доступа	Реализован механизм парольной аутентификации пользователей средствами СЗИ. Идентификация и аутентификация пользователя совместно с ОС Windows с помощью программно-аппаратных средств (iButton; eToken Pro, eToken PRO Java (USB, смарт-карты); Rutoken, Rutoken ЭЦП и Rutoken Lite), а также усиленная аутентификация пользова-	Обеспечивает идентификацию и аутентификацию локальных, доменных, терминальных и удаленных пользователей на этапе входа в операционную систему. Осуществляет работу с различными типами аппаратных идентификаторов

Меры по обеспечению безопасности ПДн	Secret Net 7.0 [99]	Dallas Lock 8.0 [100]
	телей с использованием аппаратной поддержки ПАК «Соболь» и Secret Net Card	
Управление доступом субъектов доступа к объектам доступа	Каждому информационному ресурсу назначается один из трех уровней конфиденциальности: «неконфиденциально», «конфиденциально», «строго конфиденциально», а каждому пользователю – уровень допуска. Доступ осуществляется по результатам сравнения уровня допуска с категорией конфиденциальности информации. Реализован контроль подключения и изменения устройств, а также разграничения доступа к устройствам, отслеживается неизменность (целостность) аппаратной конфигурации компьютера и контролируется использование отчуждаемых носителей	Возможно ограничение круга доступных для пользователя объектов файловой системы (дисков, папок и файлов под FAT и NTFS). Применяется полностью независимый от ОС механизм. Используются два принципа контроля доступа: **мандатный** – каждому пользователю присваивается уровень доступа. Пользователь будет иметь доступ к объектам, уровень доступа которых не превышает его собственный; **дискреционный** – обеспечивает доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа). В соответствии с содержимым списка вычисляются права на доступ к объекту для каждого пользователя (чтение, запись, выполнение и пр.)
Ограничение программной среды	Для каждого пользователя компьютера формируется определенный перечень программ, разрешенных для запуска. Он может быть задан как индивидуально для каждого пользователя, так и определен на уровне групп пользователей	Существует механизм «замкнутой программной среды» (ЗПС), который позволяет явно указать, с какими программами пользователь может работать
Защита машинных носителей информации	Поддерживается контроль следующих устройств: Основные параметры рабочей станции (процессор, память). Диски (физические, оптические, сменные и виртуальные). Сетевые интерфейсы (Ether-	Предотвращает утечки информации с использованием сменных накопителей (CD-диск, USB-Flash-диск, внешний жесткий диск и пр.), система позволяет разграничивать доступ как к отдельным

Меры по обеспечению безопасности ПДн	Secret Net 7.0 [99]	Dallas Lock 8.0 [100]
	net, 1394 FireWire, Bluetooth, IrDA, Wi-Fi). USB-устройства	типам накопителей, так и к конкретным экземплярам
Регистрация событий безопасности	Регистрирует все события, происходящие на компьютере: включение/выключение компьютера, вход/выход пользователей, события НСД, запуск приложений, обращения к конфиденциальной информации, контроль вывода конфиденциальной информации на печать и отчуждаемые носители и т.п.	Реализовано ведение 6 электронных журналов (журнал входов; журнал доступа к ресурсам; журнал запуска процессов; журнал управления политиками безопасности; журнал управления учетными записями; журнал печати)
Выявление инцидентов и реагирование на них	Реализована возможность обнаружения, идентификации и регистрации инцидентов с последующим информированием ответственных лиц	
Техническая поддержка	Предоставляется	Предоставляется
Язык программы	Русский	Русский
Сертификат ФСТЭК	Сертификат ФСТЭК России № 2707 от 07.09.2012 г.	Сертификат ФСТЭК России № 2945 от 16.08.2013 г.
Стоимость на 1 рабочее место	от 6 750 р.	от 6 000 р.

Группа «Антивирусная защита». Анализ наиболее распространенных антивирусных решений: Антивирус Касперского (разработчик ЗАО «Лаборатория Касперского», г. Москва), ESET 32 (дистрибьютор в России ООО «ИСС Дистрибьюшн», г. Москва). Сравнительный анализ выполнен [5; 10] и приведен в табл. 5.

Таблица 5

Сравнительный анализ антивирусов

Базовый функционал	«Kaspersky Security Center 10»	ESET NOD 32
Класс ИСПДн	До К1	До К1
Реализация антивирусной защиты	+	+
Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+
Наличие сертификата ФСТЭК	+	+
Операционная система	Windows	Windows
Стоимость 1-го рабочего места	От 5 750 р.	От 5 500 р.

В каждом антивирусном решении присутствуют дополнительные функции, и пользователь самостоятельно выберет антивирус, который будет соответствовать его целям и задачам при построении комплексной защиты ИСПДн.

В независимом аналитическом центре Anti-Malware [101] ежегодно проводятся тесты антивирусов, позволяющие оценить качество того или иного антивируса, увидеть динамику развития и работоспособность. Так, по результатам проведенного исследования антивирусов в 2012 г. на способность успешно (не нарушая работоспособности операционной системы) обнаруживать и удалять уже проникшие на компьютер вредоносные программы в их активном состоянии лидирующие позиции занимают следующие программы: Kaspersky Internet Security, Dr.Web Security Space Pro.

Группа «Межсетевые экраны». В табл. 6 представлен анализ наиболее распространенных межсетевых экранов: VipNet Personal Firewall (разработчик ОАО «ИнфоТеКС», г. Москва), АПКШ «Континент» (разработчик ООО «Код Безопасности», г. Москва), ИКС (разработчик ООО «Информационные технологии в бизнесе», г. Санкт-Петербург). Сертифицированные межсетевые экраны бывают пяти классов: от МЭ1 до МЭ5, в информационных системах для обеспечения 4-го уровня защищенности используются межсетевые экраны 5-го класса, а для обеспечения 1-го или 2-го уровня защищенности используются межсетевые экраны не ниже 3-го класса.

Анализ существующих решений (автоматизированных систем) показывает, что для создания комплексной защиты ПДн есть все необходимые инструменты, позволяющие обеспечить безопасность информации на высоком уровне. А выбор в пользу того или иного СЗИ зависит от ценовой политики компании, от требований заказчика и частных особенностей объекта (персональных компьютеров, сети, здания, мобильных и периферийных устройств, других факторов).

Таблица 6

Сравнительные характеристики межсетевых экранов

Сравнительные характеристики	VipNet Personal Firewall	АПКШ «Континент»	ИКС
Наличие сертификата ФСТЭК	+	+	+
Операционная система	Windows	Windows, Linux	Windows

Сравнительные характеристики	VipNet Personal Firewall	АПКШ «Континент»	ИКС
Уровень защищенности: УЗ1	–	+	–
УЗ2	+	+	+
УЗ3	+	+	+
УЗ4	+	+	+
Класс ИСПДн	К2	К1	К2
Класс МЭ	МЭ 4	МЭ 2	МЭ 4
Стоимость	Предоставляется по запросу		14 000 р. до 10 станций

Группа «DLP-решения». DLP-системы – это программные продукты, защищающие организации от утечек конфиденциальной информации, основная задача которых создание защищенного цифрового «периметра», анализ исходящей и входящей документации (электронная почта, распечатка документов, передача через Bluetooth, копирование информации на цифровой носитель).

Перехват сообщений основывается на построении «правил безопасности» либо путем анализа специальных маркеров документа, либо путем анализа содержимого документа. На практике чаще всего используется второй вариант, поскольку он более устойчив перед модификациями, вносимыми в документ перед отправкой, кроме того, это позволяет легко расширять число конфиденциальных документов, с которыми может работать система.

Дополнительная задача, которую осуществляют данные решения, – это контроль за деятельностью персонала, например, контроль за использованием рабочего времени или мониторинг общения персонала с целью «подковерной игры», способной нанести вред организации. DLP-системы можно разбить на несколько классов:

– **по способу блокирования конфиденциальной информации:**

а) с активным контролем действий пользователя, позволяющим блокировать передаваемую информацию,

б) с пассивным контролем действий пользователя, позволяющим более эффективно бороться с систематическими утечками;

– **по различию сетевой архитектуры:**

а) шлюзовые работают на промежуточных серверах,

б) хостовые – непосредственно на рабочих станциях пользователей.

В табл. 7 представлены сравнительные характеристики DLP-решений, наиболее распространенных в России. Сегодня многие

крупные компании (ОАО Сбербанк, ВТБ, Страховая группа СОГАЗ и др.) уже воспользовались возможностями DLP-решений. В результате использования данных решений обеспечили надежную защиту своих интересов и конфиденциальной информации своих клиентов.

Группа «Программа для проведения аудита безопасности». Существуют программные продукты, позволяющие оценить уровень защищенности информационной системы. Оценка уровня защищенности производится на основе международных стандартов: ISO 17799:2000, ISO 17799:2005, ISO 27001, которые, к сожалению, не поддерживают российское законодательство в области информационной безопасности.

Таблица 7

Сравнительная характеристика DLP-решений

DLP-решение	Falcongaze SecureTower [102]	InfoWatch Traffic Monitor [103]	Zecurion DLP [104]
Разработчик	Falcongaze, РФ, г. Москва	ЗАО «Инфо-Вотч»	ООО «Зекурион Рус»
Наличие сертификата/Класс ИСПДн	ИСПДн до 2-го класса включительно	ИСПДн до 1-го класса включительно	ИСПДн до 1-го класса включительнон
Определение подключения съемных носителей	–	+	–
Снимки экрана монитора	+	+	–
Перехват сообщений (ICQ)	+	+	+
Контроль мобильных рабочих мест	+	+	–
Перехват и анализ трафика	+	+	+
Установка и удаление программ	–	–	–
Учет распечатываемых подключений	+	+	+
Формирование статистики	+	+	+
Контроль Skype	+	+	+
Поиск по критериям	+	+	+
Блокирование действий на агенте	–	–	+
Средства анализа перехваченного контента на предмет утечек данных	Контекстный и контентный анализ (ключевые слова и выражения с учетом русской морфологии, регулярные выражения, цифровые отпечатки документов и БД)		Гибридный анализ перехваченных данных (эффективность более 95 %) с использованием морфологии, «цифровых от-

DLP-решение	Falcongaze SecureTower [102]	InfoWatch Traffic Monitor [103]	Zecurion DLP [104]
			печатков», регулярных выражений, OCR и собственной технологии SmartID
Расследование инцидентов	–	+	–
Стоимость	В зависимости от размера и конфигурации сети		

В сравнительном анализе использованы следующие программы, предназначенные для оценки и управления рисками информационной безопасности: RA2 art of Risk, vsRisk, RiskWatch, Callio Secura, CRAMM, COBRA, MethodWare, РискМенеджер. В табл. 8 приведены сравнительные характеристики.

В результате проведенного анализа автоматизированных систем для оценки уровня защищенности информационных систем и оценки рисков можно сделать следующие выводы:

– большинство программ поставляется на английском языке, что не позволяет российским специалистам использовать их в своей деятельности;

– большинство программ не сопровождается специалистами технической и экспертной поддержки, нет возможности настроить программы под конкретную организацию, а также отсутствует пополнение баз по угрозам;

– все выше перечисленные программы, кроме «РискМенеджер», в качестве стандартов используют зарубежные нормативные акты, что не позволяет оценить построение информационной системы на соответствие российскому законодательству в области защиты персональных данных.

Затраты от внедрения системы менеджмента информационной безопасности должны быть соотнесены между рисками и затратами на обеспечение безопасности и должны достигаться за счет обеспечения требований законодательства, предупреждения возникновения инцидентов информационной безопасности, повышения культуры информационной безопасности, оптимизации расходов на обеспечение информационной безопасности.

Таблица 8

Сравнительные характеристики ПО по защите персональных данных

Критерий сравнения	Программный продукт							
	RA2	vsRisk	Risk Watch	Callio Secura	CRAMM	COBRA	Method Ware	РискМенеджер
Разработчик	AEXIS Security Consultants	IT Governance Ltd	Risk Watch Interna-tional	Callio Techno-logies	CCTA – Central Computer and Telecommunica-tions Agency	Corporate Risk Associates Ltd	MethodWare	Институт системного анализа РАН
Сайт	–	www.itgovern ance.co.uk	riskwatch. com	–	–	www.corporater iskassociates. com	methodware.biz	www.srisks.ru
Интерфейс	Англ.	Англ.	Англ.	Англ.	Англ.	Англ.	Англ.	Русский
Простота использо-вания	+	+	+	+	– Требуются высокая квалификация специалиста в области ИБ			
Количественная оценка	+	–	+	+	+	+	–	+
Качественная оцен-ка	+	+	–	–	+	–	+	–
Техподдержка	–	+	+	–	–	–	–	+
Поддерживаемые стандарты ИБ	ISO 17799/ IEC 27001	ISO 27001 ISO 27005	ISO 17799 NIST SP 800-30	BS 7799/ ISO 17799	BS 7799 ISO 17799	BS 7799 ISO 17799	AS/NZS 4360:1999 ISO 17799 BS 7799	ГОСТ Р ИСО/МЭК 15408-2002 ISO 17799 ISO/IEC 27001:2005 СТО БР ИББС-1.1-2007
Обновляемая база знаний по угрозам	–	+	–	–	–	–	–	–
Возможность под-стройки параметров	–	–	–	–	+	+	+	+

5.3. Обзор существующих методик оценки защищенности ИСПДн

В данном разделе приведен анализ уже существующих методик, позволяющих провести оценку защищенности информационной системы, обрабатывающей персональные данные. Данные методики можно разделить на две группы:

– **документарные**, которые содержатся в различных инструкциях (приказах ФСТЭК, ГОСТах, международных стандартах, методических рекомендациях фирм, занимающихся защитой конфиденциальной информации (являются интеллектуальной собственностью и не раскрываются);

– **автоматизированные**, которые, как правило, реализованы в виде автоматизированных систем, веб-решений и позволяют в кратчайшие сроки проверить уровень защищенности своей информационной системы. Но реализованные методики в этих решениях являются интеллектуальной собственностью разработчика программного продукта и не раскрываются.

В процессе работы над пособием автор проанализировал автоматизированные методики на основе их описания на официальных сайтах компаний разработчиков, демонстрационных версий. Данные методики имеют ряд преимуществ:

– **простота работы.** Не обладая знаниями в области информационной безопасности, защиты персональных данных, пользователи данных решений могут в кратчайшие сроки определить тип своей ИСПДн. Работа в сервисах основана на методах интервьюирования;

– **соответствие законодательству.** Многие программы быстро адаптируются к изменениям законодательства. Связано это прежде всего с тем, что это облачные приложения, и пользователю нет необходимости устанавливать обновления у себя на компьютере. Разработчики в кратчайшие сроки изменяют программу под новые требования законов, нормативных актов;

– **экспертная поддержка.** Данные сервисы разрабатываются крупными интеграторами, имеющими колоссальный опыт в области защиты информации, поэтому пользователи данных программ получают индивидуальные консультации;

– **формирование документов.** Позволяют сформировать полный комплект организационно-распорядительной документации;

– **наличие доступных комментариев на каждом этапе**, что позволяет пользователю познакомиться с нормативными документами в данной сфере.

К недостаткам данных веб-решений можно отнести:

– **высокую стоимость программных продуктов**, которая зачастую может превышать месячный бюджет небольшой фирмы;

– **«базовый подход» ко всем компаниям.** Специфика бизнеса компаний не учитывается, не определяются актуальные угрозы;

– **«непрозрачность» механизма отнесения к типу ИСПДн**;

– **отсутствие рекомендаций по защите ПДн** (не во всех решениях).

В табл. 9 представлена сравнительная характеристика автоматизированных систем, позволяющих провести оценку защищенности информационных систем.

Таблица 9

Сравнительные характеристики программ

Характеристика	152.kontur.ru	b-152.ru	152 онлайн	АС ИСПДн
Разработчик	ЗАО «ПФ «СКБ Контур» г. Екатеринбург	ООО «Б152» г. Москва	ООО Центр безопасности данных «Айдеко» г. Тольятти	ФГБОУ ВПО «БГТУ» О.М. Голембиовская
Веб-решение	+	+	+	–
Организационные мероприятия	+	+	+	+
Правовые мероприятия	+	+	+	+
Разработка регламентов	–	+	+	–
Определение уровня защищенности	–	+	+	+
Определение контролируемой зоны	–	–	+	+
Определение угроз безопасности	–	+	+	+
Разработка ТЗ на проектирование системы защиты	–	–	+	+
Оценка эффективности принимаемых мер	–	–	+	+
Техподдержка	+	+	+	–
Соответствие законодательству	+	?	+	–
Стоимость на 1 год	От 6 000 до 20 000 р.	От 7 800 до 49 000 р.	От 9 900 до 89 900 р.	Не массовый продукт

Из сравнительных характеристик программных продуктов видно, что некоторые автоматизированные системы уже не соответствуют требованиям текущего законодательства, например «АС ИСПДн» разрабатывалась по старым требованиям и не соответствует новым [19], продукт «152 онлайн» на данный момент является наиболее функциональным и позволяет пользователям выполнить все требования законодательства в полном объеме, но его стоимость достаточно высока (приведенная в таблице стоимость тарифа действительна при количестве компьютеров не более десяти).

Реализованные методики в этих решениях являются интеллектуальной собственностью разработчика программного продукта и не раскрываются.

В работе [19] «АС ИСПДн» можно выделить ряд достоинств, позволяющих использовать данную методику в организациях различных сфер деятельности, например, формирование матрицы доступа для различных категорий персонала, формирование актуальных угроз, выдача рекомендаций по установке средств защиты. Существенным недостатком данной работы служит то, что автоматизированная система разрабатывалась под старые требования законодательства и нуждается в модернизации.

5.4. Проблемы реализации закона о персональных данных в РФ

Прошлое столетие характеризуется бурным развитием информационных технологий. В настоящее время информационное пространство с применением компьютерных систем, позволяющих упростить ежедневный быт, основательно вошло в повседневную жизнь рядового человека. Но вместе с этим появились негативные факторы, связанные с безопасностью данных. Использование персональных данных в информационных системах, начиная с социальных сетей заканчивая простой поликлиникой, носят в себе опасность разгласить персональные данные. В рамках решения этих проблем был принят Федеральный закон № 152-ФЗ «О персональных данных».

Стремительное развитие телекоммуникационных и информационных технологий, а также повсеместное применение вычислительной техники привели к тому, что интернет прочно вошел в жизнь современного человека. Социальные сети, интернет-магазины, развлекательные игры, портал государственных услуг, интернет-банкинг – вот далеко не полный перечень информационных продуктов, исполь-

зуемых сегодня. Эта сторона медали, позволяющая современному человеку экономить время при оплате товаров и услуг, получать образование, не выходя из дома, а также находить информацию, необходимую в процессе его жизнедеятельности, с помощью нескольких щелчков мыши.

Как известно, есть и другая сторона медали – это информационная безопасность человека, использующего телекоммуникационные технологии. Регистрируясь на различных информационных ресурсах, пользователи вводят данные о себе (паспортные данные, номера банковских счетов и другие персональные данные). Попадая в руки злоумышленников, эти данные могут нанести вред владельцу персональных данных.

В настоящее время информация – это очень дорогой продукт, и компании тратят огромные денежные средства как на поиск информации (так называемый промышленный шпионаж), так и на организацию собственной информационной безопасности (коммерческая тайна, персональные данные, информация о клиентах и поставщиках и другая информация).

И государство на законодательном уровне четко определило, что сбор, хранение и распространение информации о частной жизни лица без его согласия не допускается. В связи с чем требует от организаций и индивидуальных предпринимателей, обрабатывающих персональные данные, обеспечить их защиту. Активная деятельность по защите информации началась с принятия Федерального закона № 152-ФЗ «О персональных данных» и продолжается до сих пор.

Стоить отметить, что далеко не все организации в полной мере обеспокоились необходимостью применения закона, это подтверждается результатами проверок в 2012 г. Роскомнадзор передал 5 359 дел в суд на общую сумму 8,9 млн р.

Помимо простого невыполнения законодательства в области защиты персональных данных, имеет место неквалифицированное применение требований закона. А самые негативные последствия влечет за собой формальное применение ФЗ, только на бумаге без включения механизмов защиты в деятельность организации.

В связи с этим защита персональных данных является актуальной задачей, а порядок защиты персональных данных остается серьезным вопросом, требующим внимательного к себе отношения.

В России более 7 млн юридических лиц и индивидуальных предпринимателей, на которых распространяется действие Федераль-

ного закона № 152-ФЗ «О персональных данных». Требования законодательства сейчас практически полностью выполнили организации, относящиеся к крупному бизнесу, а также государственные, муниципальные учреждения (больницы, школы, учреждения социальной защиты и пр.). Большая часть компаний, относящихся к среднему и малому бизнесу, до сих пор серьезно не задумались о выполнении данного закона и не подготовили документацию, отвечающую требованиям закона.

Основными причинами, по которым компании не выполняют требования законодательства и не спешат выполнять их, являются:

1. Постоянно меняющиеся нормативные акты, запутанность терминологии, юридические коллизии.
2. Отсутствие в штате квалифицированного юриста, владеющего знаниями, касающимися персональных данных.
3. Отсутствие технических работников (программистов, системных администраторов), которые могут настроить автоматизированную систему в соответствии с требованиями законодательства.
4. Высокая стоимость услуг сторонних организаций (аутсорсинг) по приведению документации и технических средств по всем требованиям законодательства.
5. Высокая стоимость аппаратно-программных средств, обеспечивающих качественную защиту персональных данных.
6. Несоизмеримость штрафов и затрат на подготовку и внедрение системы защиты персональных данных.

Федеральный закон № 152-ФЗ «О персональных данных» был принят в 2006 г., но его вступление в силу откладывалось до 2011 г. За это время было разработано множество нормативных актов, которые должны были помочь операторам организовать защиту персональных данных (ПДн) в своих автоматизированных системах. Только в 2008 г. появляются следующие документы:

1. Так называемый «Закон трех» – это приказ ФСТЭК России, ФСБ России и Министерства информационных технологий и связи Российской Федерации от 13.02.2008 г. № 55/86/20 «О утверждении порядка проведения классификации информационных систем персональных данных».
2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России.

Количество документов, регламентирующих защиту персональных данных, увеличивается с каждым годом. Стоить выделить обязательные документы, с которыми должны быть знакомы все операторы ПДн:

2010 г. – приказ ФСБ России и ФСТЭК России № 416/489;

2012 г. – постановление Правительства РФ № 1119, Разъяснения Роскомнадзора;

2013 г. – постановление Правительства РФ № 1119, Разъяснения Роскомнадзора, приказ № 21 ФСТЭК России, приказ Роскомнадзора № 274, Федеральный закон № 99-ФЗ, Разъяснения Роскомнадзора, Информационное сообщение ФСТЭК России, приказ Роскомнадзора № 996.

В 2014 г. планируется принятие новых нормативных документов (проект изменений в ФЗ «О персональных данных» и в Кодексе об административных правонарушениях), ужесточение требований закона, а также увеличение максимального размера штрафа до 700 000 р. за невыполнение требований закона «О персональных данных».

Таким образом, каждый оператор ПДн обязан соблюдать требования законодательства и отслеживать соответствующие изменения. Вполне логично, что не каждое предприятие среднего и малого бизнеса, а также индивидуальные предприниматели могут позволить себе отдельного юриста, который занимался бы вопросами защиты персональных данных работников и клиентов компании.

Анализируя методические рекомендации контролирующих органов (ФСТЭК, ФСБ, РОСКОМНАДЗОРА) в области защищенной обработки персональных данных, можно сделать вывод, что выполнить требования законодательства можно лишь разбив эти требования на несколько этапов. В соответствии с приказом № 21 от 18.02.2013 г. ФСТЭК России утвердила «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Документ позволяет выделить несколько этапов по приведению защиты персональных данных к требованиям законодательства.

1. Организационные мероприятия. Целью данного этапа является назначение ответственного лица, в обязанности которого входят взаимодействие с субъектами ПДн; обработка ПДн; взаимодействие с

третьими лицами по вопросам передачи и получения ПДн; взаимодействие с регулирующими органами; обеспечение безопасности ПДн. Результатом выполнения данного этапа служат внутренние документы компании (например, приказ о назначении ответственного за организацию работ по защите ПДн, приказ о назначении администратора безопасности ИСПДн и др.).

2. Определение класса информационной системы персональных данных (ИСПДн). На этом этапе в зависимости от структуры информационной системы, категорий и объема обрабатываемых персональных данных определяется класс информационной системы. Результатом данного этапа является сформированный акт классификации информационной системы персональных данных, в котором отражены категория, объем и класс ИСПДн, а также характеристики ИСПДн.

3. Формирование модели угроз. Обеспечение безопасности ПДн достигается, в частности, определением угроз безопасности ПДн при их обработке в ИСПДн и формированием на их основе моделей угроз с целью их последующей нейтрализации. Для формирования требований к системе защиты ПДн необходимо построить частные модели угроз безопасности ПДн для каждой из выделенных в компании ИСПДн. Результат этапа – документы «Частные модели угроз» и «Модели нарушителя безопасности ПДн».

4. Техническая реализация требований по защите ПДн. На этом этапе особое внимание уделяется внедрению аппаратно-программных средств, позволяющих нейтрализовать актуальные угрозы. При проектировании системы безопасности требуется рассмотреть различные угрозы, которые могут возникнуть (например, угроза загрузки с внешних носителей информации; выявление уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы; угроза несанкционированного доступа и др.).

Стоит заметить, что для организации защиты персональных данных первые три пункта методических рекомендаций требуют только организационных решений, без затрат на материальные ресурсы. Что нельзя сказать о четвертом пункте в рамках технической реализации требований по защите ПДн. Таким образом, определяется целесообразность внедрения/установки аппаратных средств защиты ПНд (например, Secret Net, который поддерживает процедуры идентификации и аутентификации; электронный замок «Соболь»), программных средств (например, средства антивирусной защиты, защиты от вторжений и средств имитации, межсетевые экраны и пр.).

Принятие закона № 152-ФЗ «О персональных данных» повлияло на то, что многие компании, разрабатывающие программное обеспечение, начали разработку и внедрение программных продуктов (решений), позволяющих компаниям при небольших денежных и временных затратах выполнить требования законодательства (по сравнению с услугами, которые оказывают компании – лицензиаты по защите информации).

Разработчики программ для защиты персональных данных предлагают различный функционал, от которого зависит уровень защищенности ИСПДн. В некоторых решениях это только скрытие и (или) блокировка файлов и папок или разработка полного комплекта документов, регламентирующих выполнение требований закона; у других – это полноценное шифрование; у третьих – от разработки организационно-распорядительных документов до настройки, внедрения и страхования финансовых рисков.

Программное обеспечение, обеспечивающее безопасность информационных систем персональных данных, обязано пройти сертификацию на соответствие требованиям закона № 152-ФЗ «О персональных данных» и получить сертификат соответствия ФСТЭК России.

Программные решения, которые обеспечивают выполнение требований законодательства, можно разделить на следующие группы:

1. Решения, позволяющие подготовиться к проверке Роскомнадзора. Такие решения позволяют подготовить организационно-распорядительную документацию, которую запрашивает регулятор (Роскомнадзор) при документарной проверке.
2. Решения не только позволяют подготовить необходимую документацию, но и рекомендуют аппаратно-программные средства для защиты персональных данных, исходя из особенностей ИСПДн.
3. Решения, позволяющие закрыть все требования законодательства для ИСПДн любого класса.

Для создания комплексной защиты ПДн есть все необходимые инструменты, позволяющие обеспечить безопасность информации на высоком уровне. Использование автоматизированных систем позволяет лучшим образом определять структуру и решения защиты ПДн и технического обеспечения, которые будут способствовать снижению бизнес-рисков (потеря репутации организации, финансовые риски, приостановление деятельности). От организации зависит будут ли реализованы все требования законодательства, или все это будет формальный подход – только подготовка необходимой документации.

6. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕХАНИЗМЕ МЕСТНОГО САМОУПРАВЛЕНИЯ

Основными стратегическими задачами органов местного самоуправления (ОМСУ) в системе экономики региона традиционно являются создание условий для стабильного экономического развития хозяйствующих субъектов, действующих на территории, поддержание необходимого (достаточного) уровня жизни и социального обеспечения населения, решение экологических проблем, а также активизация инновационных процессов.

От эффективности, скоординированности и обоснованности принимаемых решений по социально-экономическому развитию субъектов местного самоуправления во многом зависят уровень экономического развития (и, соответственно, уровень жизни населения), состояние социальной сферы.

Неоспоримо важной задачей в проводимых реформах, имеющих свои особенности в каждой стране, является повышение эффективности и качества деятельности государственных органов власти, предоставляющих услуги населению.

В Российской Федерации в настоящее время инструментом реализации инноваций в сфере ИКТ деятельности ОМСУ в РФ служит поэтапное внедрение проекта «Электронное правительство».

В настоящее время достижение целей, определенных в концепции «Электронное правительство», будет способствовать логическому завершению преобразований в муниципалитетах всех уровней. А процедуру контроля за результативностью органов государственной власти необходимо усилить, используя механизм оценки деятельности органов государственной власти.

Для выявления потребности в информационном обеспечении в рамках выяснения мнения населения МО о деятельности органов муниципальной власти целесообразно проводить соцопросы. Однако проведение соцопросов не позволяет поддерживать актуальность данных из-за трудности сбора информации и ее обработки, и информативность и спектр срезов крайне узок.

На наш взгляд, для решения данных задач необходимо создание соцопросов посредством ИКТ ЭМ (информационно-коммуникационные технологии электронного муниципалитета). Они должны содержать новые технологии проведения соцопроса, основанные на технологиях и возможностях: интернета (интернет-беседки, созданные на базе муни-

ципалитета или коммерческих организаций на основе субсидирования); сотовой и телефонной связи (горячая линия, SMS); телевидения; радио и других технологий. Но, в свою очередь, применение подобных средств связи порождает угрозы информационной безопасности систем.

В настоящее время наблюдается широкое распространение новых ИТ, многие типовые задачи сменяются мобильными «разовыми» решениями, задачи могут различаться по масштабам, темпам изменений и времени. На наш взгляд, для решения данных задач в наибольшей степени подходят сетевые технологии, а именно системы интернет-технологий в государственном управлении. Данные технологии можно использовать при предоставлении услуг населению через систему электронного правительства.

Эти системы, получившие название «e-government», используются в подавляющем большинстве стран и подразумевают использование компьютерных технологий в государственном управлении. Электронный муниципалитет – это преобразование внутренних и внешних отношений государственных организаций на основе использования возможностей ИКТ с целью оптимизации предоставляемых услуг, повышения уровня участия общества в вопросах государственного управления и совершенствования внутренних процессов местного самоуправления.

Сегодня уже многие развитые страны получили ощутимые социально-экономические результаты от проектов, основанных на преимуществах интернета. Успех подобных проектов объясняется следующими их особенностями: учетом индивидуальных интересов каждого гражданина; стимулированием роста персональных навыков работающего населения; ускорением развития новых экономических проектов при облегчении процедур отчетности, уплаты налогов и т.д.; снятием барьеров для коммуникации с населением и выработкой новых совместных инициатив как с бизнесом, так и с гражданами.

Однако необходимо иметь в виду, что сетевые технологии порождают и новые задачи для управления. Прежде всего, это вопросы эффективности и информационной безопасности.

В настоящее время в муниципалитетах наблюдается ситуация по использованию информационных систем в работе муниципалитетов в основном для механизации процесса формирования документов. Не используются возможности автоматизации механизма управления муниципалитетом.

На современном этапе развития МО одной из главных задач является повышение эффективности и качества решений, принимаемых ОМСУ. Выполнение данной задачи в настоящее время сводится к осмыслению и выработке инновационных механизмов управления МО. На наш взгляд, основными направлениями совершенствования МО, с применением современных ИКТ, должны стать вовлечение населения в механизм управления МО; контроль населением деятельности ОМСУ.

Деятельность ОМСУ в аспекте информирования направлена на информационную поддержку осуществления принципов народовластия, обеспечения государственных гарантий гласности, а так же правовой, экономической, финансовой и социальной деятельности на территории МО и обеспечения непосредственного участия граждан в самоуправлении.

Одной из характерных черт современного управления МО является инновационный тип управления, при котором в конечном продукте постоянно увеличивается доля знаний как основного ресурса. Именно такой тип управления сегодня является эффективным. Он позволяет в процессе планирования, организации, мотивации и контроля максимально быстро при минимальном количестве затрат достигать наибольшего экономического, управленческого и социального эффекта, обеспечивая постоянное поступательное развитие муниципального образования и повышение уровня и качества жизни населения. Одним из передовых направлений инновационного типа развития всех сфер деятельности в настоящее время является использование ИКТ.

Классификация ИКТ, представленная в табл. 10, отражает, что наиболее эффективными инструментами с точки зрения применения органами государственной власти с целью управления социально-экономическим развитием и повышением уровня и качества жизни населения являются электронно-вычислительные технологии. В табл. 10 столбец «Свойства и характеристики ресурса ИКТ в целях управления МО» отображает информацию по назначению информационных продуктов. На наш взгляд, целесообразно выделить балльную градацию эффективности свойств и характеристик ресурсов ИКТ в целях использования в управлении МО: 1 – низкоэффективные; 2 – среднеэффективные; 3 – высокоэффективные; 4 – наиболее эффективные. Такие информационные продукты, как почта и телеграф, по нашему мнению, обладают низкой эффективностью, так как только отчасти являются системами ИКТ, однако и их использование неотъемлемо.

Таблица 10

Классификация ИКТ и их эффективность при использовании в механизме управления МО

Информационный продукт	Общая характеристика ИКТ	Виды производных продуктов	Степень охвата населения, %	Скорость передачи информации	Соцэффект*	Свойства и характеристики ресурса ИКТ в целях управления МО	Эффективность для ОМСУ**	Искажение информации***
Почта, телеграф	Механические, электронные (проводные)	Пешая, конная, курьерская, автомобильная, морская, речная, железнодорожная, авиационная, электронная	85	Низкая	1	Рассылка уведомлений, писем, квитанций, предупреждений с очень низкой скоростью доставки и высокой степенью угроз утери информации	1	1
Печатные издания	Механические	Официальные газетные издания, специализированные журналы, научные издания	40	Низкая	2	Оповещение, ознакомление	1	1
		Листовки, желтая пресса, брошюры, буклеты	60	Низкая		Представление информации для всех слоев населения	1	3
Телефон	Электронные (проводные)	Средство передачи информации	70	Средняя	3	Прямое общение с населением, с подразделениями в целях управления, низкая эффективность дозвона	2	2
Радио, телевидение	Электронные (проводные, беспроводные)	Средства представления информации	70	Средняя	4	Оповещение, выборы, праздники, новости, ЧС, уровень СЭР, стратегия СЭР	3	1

Информационный продукт	Общая характеристика ИКТ	Виды производных продуктов	Степень охвата населения, %	Скорость передачи информации	Соцэффект*	Свойства и характеристики ресурса ИКТ в целях управления МО	Эффективность для ОМСУ**	Искажение информации***
Сотовая связь	Электронно-вычислительные	Телефон	55	Средняя	4	Мобильность, высокая эффективность дозвона	2	2
		Иинтернет	55	Высокая		Универсальное средство информирования, установление двусторонней связи	3	3
		SMS	55	Низкая		Ограниченные объемы информации	2	3
ЭВМ	Электронно-вычислительные	Операции обработки данных	45	Высокая	5	Устройство автоматической обработки, вывода и представления данных с возможностью использования передовых технологий коммуникации	4	1
Интернет	Электронно-вычислительные	Электронная почта	25	Высокая	6	Универсальное средство информирования, установление двусторонней связи	3	1
		Системы обмена сообщениями	25	Низкая		Универсальное средство информирования, установление двусторонней связи;	3	3

Информационный продукт	Общая характеристика ИКТ	Виды производных продуктов	Степень охвата населения, %	Скорость передачи информации	Соцэффект*	Свойства и характеристики ресурса ИКТ в целях управления МО	Эффективность для ОМСУ**	Искажение информации***
						ограниченный объем информации		
		Сетевые порталы с личной электронной подписью	10	Высокая		Средство информирования, установление двусторонней связи	3	1
		Финансовые операционные программы	5	Высокая		Средство осуществления финансовых операций	3	1
		Дистанционные курсы повышения квалификации и обучения	15	Высокая		Средство обучения и контроля, возможности удаленного обучения, консультирования	3	1
		Электронное правительство	25	Высокая		Средство информирования, установление двусторонней связи, возможность общения с органами власти посредством ЭВМ	3	1
Спутниковая связь	Электронно-вычислительные	Спутниковая связь	5	Высокая	7	Абсолютная мобильность, высококачественное соединение	4	1
		Спутниковая навигация	10	Высокая		Абсолютная мобильность, высо-	4	1

Информационный продукт	Общая характеристика ИКТ	Виды производных продуктов	Степень охвата населения, %	Скорость передачи информации	Соцэффект*	Свойства и характеристики ресурса ИКТ в целях управления МО	Эффективность для ОМСУ**	Искажение информации***
						кая эффективность соединений, возможность определение местоположения		

* Уровень и качество жизни, которому соответствует ИКТ, при ее постепенном использовании в процессе повышения покупательной способности граждан: 1 – минимальный, 2 – ниже среднего, 3 – средний, 4 – выше среднего, 5 – высокий, 6 – очень высокий, 7 – наивысший.

** Эффективность свойств и характеристик ИКТ при использовании в ОМСУ: 1 – низкоэффективные, 2 – среднеэффективные, 3 – высокоэффективные, 4 – наиболее эффективные.

*** Вероятность искажения информации: 1 – низкая, 2 – средняя, 3 – высокая.

Кроме того, мы вводим балльную градацию вероятности искажения информации, состоящую из трех степеней: 1 – низкая; 2 – средняя; 3 – высокая.

В классификации эффективности использования ИКТ в механизме управления МО выделен показатель социального эффекта, который заключается в соответствии уровню и качеству жизни каждой конкретной информационной технологии при их постепенном приобретении в процессе повышения покупательной способности граждан от почты до спутниковых ИКТ. Данный показатель целесообразно разделить на семь категорий: 1 – минимальный уровень и качество жизни; 2 – ниже среднего уровень и качество жизни; 3 – средний уровень и качество жизни; 4 – выше среднего уровень и качество жизни; 5 – высокий уровень и качество жизни; 6 – очень высокий уровень и качество жизни; 7 – наивысший уровень и качество жизни.

Современные технологии связи и информационного оповещения за счет комбинирования различных функций технических устройств могут обладать характеристиками различных информационно-коммуникационных технологий. Так, сотовая связь позволяет получать доступ в интернет, к электронной почте, пользоваться навигацией и другими информационными услугами, при этом само устройство может являться мини-ЭВМ, телефоном, телевизором, радио и другими устройствами одновременно (рис. 7).

Из всего представленного перечня ИКТ, по оптимистичным прогнозам, используется не более 40 % технических средств автоматизации при управлении МО. В основном последние разработки используются в силовых ведомствах и органах по предупреждению и предотвращению чрезвычайных ситуаций и устранению их последствий в части навигационного оборудования и средств связи.

В настоящее время даже наиболее доступные ИКТ, такие как телевидение, радио и сотовая связь, достаточно редко и несистемно используются ОМСУ в целях управления МО. Как правило, это связано с политическими мероприятиями при реализации выборного права жителей МО; с оповещением населения о социально-экономическом и экологическом состоянии территории посредством новостной информации, что в индивидуальном порядке доступно далеко не всем МО; с социальной рекламой, что происходит очень редко и не всегда учитывает специфику отдельных МО; с отдельными тематическими аналитическими программами.

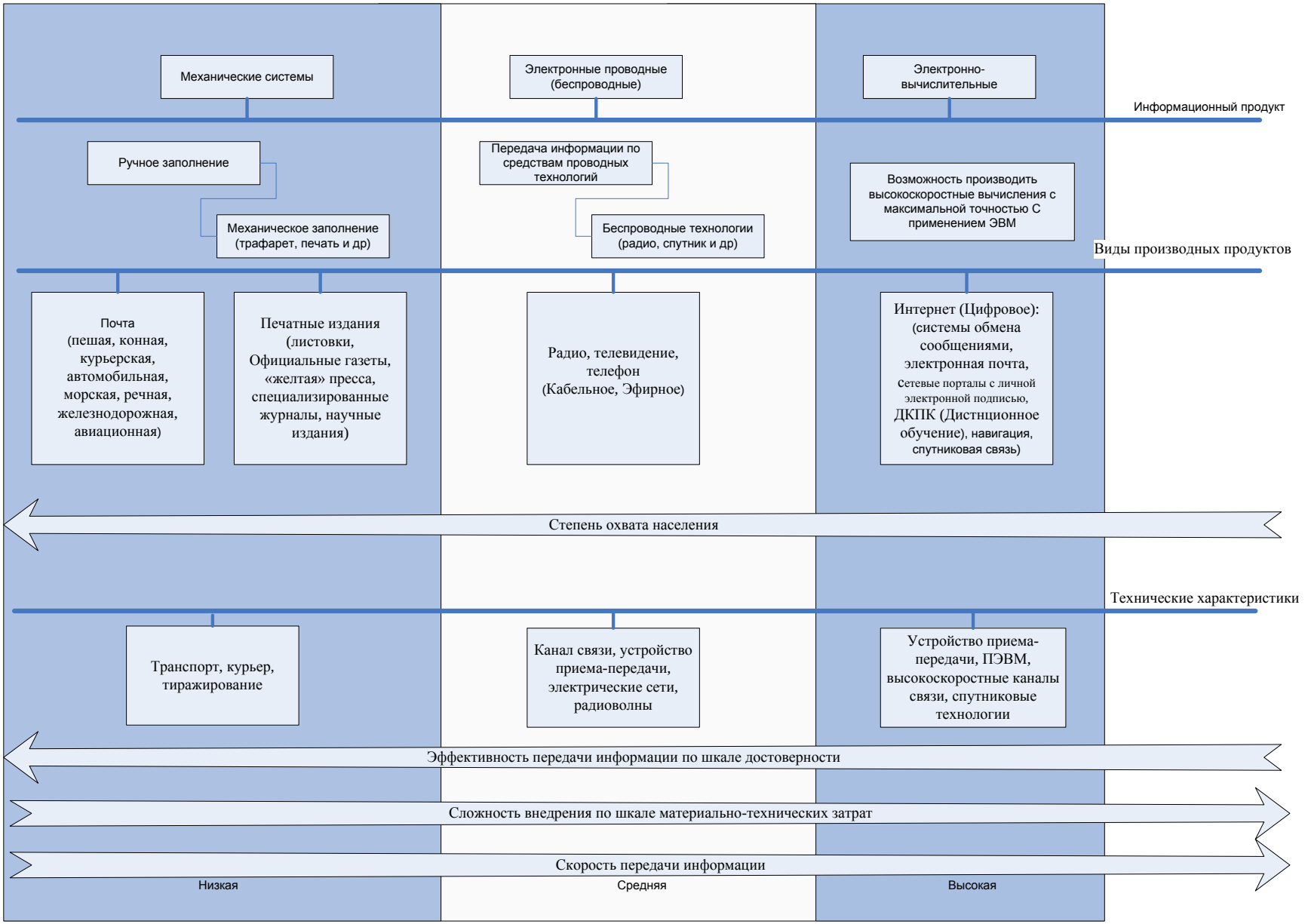

Рис. 7. Характеристика основных инструментов информационного обеспечения населения МО

Кроме того, практически все телевизионные и радиопрограммы, за исключением предвыборных мероприятий, создаются и транслируются в основном частными организациями, преследующими собственные коммерческие цели.

В этой связи считаем необходимым более активно использовать и разрабатывать индивидуальные механизмы информационного обеспечения жителей каждого МО на основе общедоступных ИКТ, прежде всего, в направлении усиления социальной рекламы, кадровой политики, образования, здравоохранения, досуга, правопорядка, экологической ответственности.

Информационные, коммуникационные, вычислительные и комбинированные системы и программы управления используются в деятельности ОМСУ так же редко и несистемно, что значительно замедляет развитие МО и делает сомнительным скорый переход на модель информационного общества и инновационного устойчивого социально-экономического развития МО.

Внедрение систем информатизации в ОМСУ в настоящее время производится в следующих направлениях совершенствования управления МО:

1. При информатизации организационно-правовой деятельности ОМСУ необходимо внедрять ИКТ по следующим направлениям: 1) поддержка нормативно-правового обеспечения МО; 2) обеспечение процесса подготовки и ведения базы данных нормативно-правовых актов МО и контроля их исполнения; 3) обеспечение делопроизводства МО – развитие систем документооборота, в том числе обработка и контроль обращений граждан в МО; 4) поддержка и обеспечение эффективности процесса принятия управленческих решений должностными лицами ОМСУ (электронное правительство – мониторинг и прогнозирование социально-экономического развития МО); 5) обеспечение эффективного противодействия коррупции в ОМСУ (видео- и аудиофиксация служебной деятельности в рабочее время); 6) ведение баз данных «Структура органов власти и управления»; 7) обеспечение взаимодействия власти, населения и бизнес-структур, создание на базе интернет-кафе или отдельных специально отведенных мест – информационныех социальных беседок, в которых с помощью специальных сотрудников каждый житель МО, предприниматель и организация в интерактивном режиме (по интернету) сможет задать вопросы, получить ответы, сообщить информацию, высказать мнение, оформить за-

явки и получить консультации от сотрудников ОМСУ по всем социально-экономическим аспектам жизни МО.

2. При информатизации финансово-кредитной деятельности МО ИКТ необходимо внедрять по следующим направлениям: 1) формирование, распределение и контроль целевого использования бюджетных и внебюджетных средств; 2) разработка и внедрение информационно-вычислительных программ по обеспечению эффективного налогообложения юридических и физических лиц; 3) разработка и внедрение информационно-вычислительных программ по обеспечению эффективного использования финансовых ресурсов; 4) подготовка, реализация, мониторинг и контроль за реализацией планов и программ социально-экономического развития; 5) формирование и мониторинг балансов использования финансовых, трудовых, земельных ресурсов, роста денежных доходов населения.

3. При обеспечении информатизации процесса управления муниципальным имуществом ИКТ необходимо внедрять по следующим направлениям: 1) ведение реестра предприятий и учреждений; 2) ведение договоров аренды муниципального имущества.

4. При информационной поддержке управления потребительским рынком города ИКТ необходимо внедрять по следующим направлениям: 1) расчет минимального потребительского бюджета населения; 2) формирование муниципального заказа по обеспечению населения города товарами и услугами и организация контроля его исполнения; 3) формирование региональных нормативов на использование городских ресурсов и социально-экономического паспорта города; 4) ведение баз данных по ценам на товары и услуги; 5) учет, контроль и анализ наличия товарных ресурсов; 6) оперативное выявление спроса на товары и услуги.

5. При информатизации процессов социального развития территории города ИКТ необходимо внедрять по следующим направлениям: 1) ведение базы данных о малообеспеченных слоях населения; 2) учет, контроль и анализ оказания помощи малообеспеченным слоям населения; 3) ведение баз данных по объектам системы образования; 4) дистанционное обучение граждан с ограничениями опорно-двигательного аппарата – инвалидов; 5) дистанционное обучение и переподготовка кадров граждан, потерявших работу по сокращению, и иных нетрудоустроенных; 6) ведение базы данных по объектам системы здравоохранения; 7) дистанционное диагностирование и консультирование при лечении и проведении сложных хирургических

операций; 8) ведение базы данных по объектам культуры; 9) перевод информации с бумажных носителей в библиотеках на электронный носитель – электронная библиотека; 10) ведение базы данных по объектам физической культуры и спорта.

6. При информатизации процессов градостроительства и землепользования необходимо внедрять ИКТ и геоинформационные технологии по следующим направлениям: 1) поддержка системы ведения городских кадастров; 2) ведение Генерального плана (схемы развития) города; 3) планирование капитального строительства и контроль исполнения; 4) предоставление земельных участков; 5) ведение земельных кадастров; 6) ведение базы данных по использованию земельных ресурсов города; 7) разработка планов оптимального использования земельных ресурсов.

7. При информатизации механизмов поддержки процесса управления городским жилищным и коммунальным хозяйством ИКТ необходимо внедрять по следующим направлениям: 1) управление системой ЖКХ города, включая систему обеспечения межведомственных расчетов за коммунальные услуги; 2) внедрение геоинформационных систем ведения городских кадастров жилого и нежилого фонда; тепловых сетей; водопроводных и канализационных сетей; электрических и газопроводных сетей; 3) формирование муниципального заказа на жилищно-коммунальные услуги и организация контроля его исполнения; 4) формирование муниципального заказа на строительство и реконструкцию инженерных сетей и организация контроля его исполнения; 5) поддержка принятия управленческих решений в условиях чрезвычайных ситуаций на объектах коммунального хозяйства города.

8. При информатизации поддержки процесса управления городским транспортом и благоустройством ИКТ необходимо внедрять по следующим направлениям: 1) внедрение геоинформационных систем ведения городских кадастров улично-дорожной сети; 2) формирование муниципального заказа на перевозку пассажиров и организация контроля его исполнения; 3) внедрение геоинформационных систем формирования и организации контроля исполнения комплексной экологической программы территории города и ведения картографической базы данных природоохранных и экологически вредных объектов.

9. При создании автоматизированных систем управления технологическими процессами: 1) диспетчеризация жилищно-коммунального хозяйства города (регистрация аварийных ситуаций; разработка и внедрение автоматических систем блокировки инженерных сетей при ава-

риях; контроль и учет потребления тепла, воды, электроэнергии; функционирование лифтового хозяйства; затопляемость подвалов; блокирование доступа к чердакам и подвалам; 2) контроль и управление дорожным движением; 3) контроль и управление графиком движения общественного транспорта; 4) контроль и управление водоснабжением города (магистрали); 5) контроль и управление канализацией и очистными сооружениями; 6) контроль и управление работой котельных; 7) экологический мониторинг (внедрение ИКТ и специализированной инновационной техники по дистанционному автоматическому замеру загрязняющих выбросов в атмосферу и сбросов сточных вод (система датчиков и детекторов); обеспечение автоматического информационного оповещения населения о местах локальных и глобальных экологических, техногенных, сейсмических, климатических и т.д. аварий и катастроф, предоставление ОМСУ и населению динамической сводной информации об экологическом состоянии территории МО).

10. При информатизации органов охраны правопорядка и министерства чрезвычайных ситуаций необходимо обеспечить информационную поддержку, видео- и аудиофиксацию служебной деятельности, навигационную поддержку, внедрение специализированного технического оснащения по следующим направлениям: 1) регистрация правонарушений по средствам уличного видеонаблюдения; 2) регистрация мероприятий по задержанию правонарушителей с использованием индивидуальных средств видео- и аудиозаписи; 3) регистрация дорожно-транспортных происшествий и нарушений правил дорожного движения по средствам стационарного и передвижного видеонаблюдения; 4) информационная, навигационная мобильная поддержка сотрудников органов правопорядка (базы данных, системы глобального позиционирования и другие ИКТ).

Данный перечень необходимо принять как основу для развития информатизации ОМСУ, при этом его необходимо обновлять и дополнять с учетом специфических особенностей определенных МО.

Такой перечень направлений информатизации должен отображать не только статистические данные и справочную информацию, но и информацию по взаимодействию органов муниципальной власти и населения по всем интересующим вопросам. Также необходимо обеспечить активное развитие интернет-сайтов МО на основе многопортального подхода, позволяющих аккумулировать и рассматривать весь спектр вопросов, возникающих у жителей и организаций МО к органам исполнительной, законодательной, судебной власти.

СПИСОК ИСПОЛЬЗОВАННОЙ И РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Законодательные и нормативно-правовые акты

1. Конституция Российской Федерации : принята всенар. голосованием 12 дек. 1993 г. // Российская газета. – 2009. – 21 янв.
2. Трудовой кодекс Российской Федерации : федер. закон от 30 дек. 2001 г. № 197-ФЗ // Российская газета. – 2001. – 31 дек.
3. О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ // СЗ РФ. – 2006. – № 31, ч. 1. – Ст. 3451.
4. Об информации, информационных технологиях и о защите информации : федер. закон РФ от 27 июля 2006 г. № 149-ФЗ // СЗ РФ. – 2006. – № 31, ч. 1. – Ст. 3448.
5. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства от 1 нояб. 2012 г. № 1119 // СЗ РФ. – 2012. – № 45. – Ст. 6257.
6. О лицензировании деятельности по технической защите конфиденциальной информации : постановление Правительства РФ от 3 февр. 2012 г. № 79 // СЗ РФ. – 2012. – № 7. – Ст. 863.
7. Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных : постановление Правительства РФ от 6 июля 2008 г. № 512 // СЗ РФ. – 2008. – № 28. – Ст. 3384.
8. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации : постановление Правительства РФ от 15 сент. 2008 г. № 687 // СЗ РФ. – 2008. – № 38. – Ст. 4320.
9. Об утверждении требований и методов по обезличиванию персональных данных : приказ Роскомнадзора от 5 сент. 2013 г. № 996 // Российская газета. – 2013. – 18 сент.
10. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18 февр. 2013 г. № 21 // Российская газета. – 2013. – 25 мая.
11. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах

персональных данных от 14 февр. 2008 г. [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс».

12. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15 февраля 2008 г. [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс».

13. Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования : приказ ФСБ России и ФСТЭК РФ от 31 авг. 2010 г. № 416/489 // Российская газета. – 2010. – 22 окт.

Рекомендуемая литература

14. Аверченков В.И. Оценка рисков безопасности информационных систем персональных данных / В.И. Аверченков, М.Ю. Рытов, О.М. Голеомбиовская // Информация и безопасность. – 2012. – № 3. – С. 321–328.

15. Аверченков В.И. Оценка рисков безопасности информационных систем персональных данных / В.И. Аверченков, М.Ю. Рытов, О.М. Голеомбиовская // Информация и безопасность. – 2012. – № 3. – С. 321–328.

16. Атаманов Г.А. Азбука безопасности. Объекты и субъекты безопасности вообще и информационной безопасности в частности / Г.А. Атаманов // Защита информации. INSIDE. – 2013. – № 6. – С. 18–24.

17. Аудит информационной безопасности / под ред. А.П. Курило. – М. : Изд. группа «БДЦ-пресс», 2006. – 304 с.

18. Барышников А. Безопасность корпоративных центров обработки персональных данных / А. Барышников // Защита информации. INSIDE. – 2013. – № 6. – С. 40–41.

19. Волокитина Е.С. Метод и алгоритмы гарантированного обезличивания и реидентификации субъекта персональных данных в автоматизированных информационных системах : автореф. дис. … канд. техн. наук / Е.С. Волокитина. – СПб., 2013. – 24 с.

20. Волчинская Е.К. Защита персональных данных / Е.К. Волчинская. – М. : Галерея, 2001. – 236 с.

21. Голембиовская О.М. Автоматизация выбора средств защиты персональных данных на основе анализа их защищенности : автореф. дис. … канд. техн. наук / О.М. Голембиовская. – СПб., 2013. – 17 с.

22. Голембиовская О.М. Автоматизация выбора средств защиты персональных данных на основе анализа их защищенности : дис. … канд. техн. наук / О.М. Голембиовская. – Брянск, 2013. – 167 с.

23. Голеомбиовская О.М. Разработка автоматизированной системы аудита и построения модели объекта защиты с использованием технологии 3D-прототипирования / О.М. Голеомбиовская, М.В. Терехов // Материалы 2-й региональной научно-практической конференции «Региональные проблемы защиты персональных данных». – Брянск : БГТУ, 2010. – С. 47–49.

24. Егерева О.А. Некоторые проблемы, возникающие при расследовании преступлений в сфере компьютерной информации и компьютерных сетях: к вопросу о криминалистическом аспекте собирания доказательств / О.А. Егерева, И.Г. Смирнова // Уголовно-процессуальные и криминалистические средства обеспечения эффективности уголовного судопроизводства : материалы междунар. науч.-практ. конф. Иркутск, 25–26 сент. 2014 г. – Иркутск : Изд-во БГУЭП, 2014. – С. 337–343.

25. Ершов В.Н. Информационная защита персональных данных: доминирующий источник угрозы / В.Н. Ершов, П.Л. Смирнова // Бизнес-информатика. – 2012. – № 2. – С. 71–76.

26. Ефремов А. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн / А. Ефремов // Защита информации. INSIDE. – 2013. – № 4. – С. 12–14.

27. Жук Р.В. Классификация информационных систем персональных данных: вчера, сегодня, завтра / Р.В. Жук, А.В. Власенко // Известия Юго-Западного государственного университета. – 2013. – № 1. – С. 87–90.

28. Журавлев В. Правила игры в 21 / В. Журавлев // Защита информации. INSIDE. – 2013. – № 4. – С. 15–17.

29. Зенин Н. Защита информации от утечек: интеграция IRM- и DLP-решений / Н. Зенин // Storage News. – 2010. – № 1. – С. 26–31.

30. Капустина А. Защита государственных информационных систем выходит на новый уровень / А. Капустина // Защита информации. INSIDE. – 2013. – № 6. – С. 46–49.

31. Карпычев В.Ю. Новые подходы к опредлению актуальных угроз безопасности персональных данных / В.Ю. Карпычев // Информация и безопасность. – 2012. – № 1. – С. 93–95.

32. Кафтанникова В.М. Правовое регулирование информационных систем персональных данных / В.М. Кафтанникова // Ветсник УрФО. Безопасность в информационной сфере. – 2012. – № 2. – С. 14–19.

33. Коломинов В.В. К вопросу о формировании криминалистического знания о мошенничестве в сфере компьютерной информации / В.В. Коломинов, И.Г. Смирнова // Уголовно-процессуальные и криминалистические средства обеспечения эффективности уголовного судопроизводства : материалы междунар. науч.-практ. конф. Иркутск, 25–26 сент. 2014 г. – Иркутск : Изд-во БГУЭП, 2014. – С. 283–289.

34. Куракин А.С. Методы и алгоритмы построения информационных систем персональных данных в защищенном исполнении : автореф. дис. … канд. техн. наук / А.С. Куракин. – СПб., 2013. – 33 с.

35. Кучеренко А.В. Правовое регулирование персональных данных в Российской Федерации : автореф. дис. … канд. юрид. наук / А.В. Кучеренко. – Челябинск, 2010. – 23 с.

36. Лось А.Б. Особенности оценки рисков информационной безопасности с использованием регрессивного анализа в системе менеджмента информационной безопасности / А.Б. Лось, А.С. Кабанов // Промышленные АСУ и контроллеры. – 2014. – № 1. – С. 58–66.

37. Львович Я.Е. Модель нарушителя информационной безопасности / Я.Е. Львович, Д.С. Яковлев // Промышленные АСУ и контроллеры. – 2012. – № 2. – С. 54–56.

38. Майстренко В.А. Программный комплекс анализа информационных систем персональных данных ВУЗа / В.А. Майстренко, И.В. Аютова // Омский научный вестник. – 2012. – № 2. – С. 322–327.

39. Миронова В.Г. Модель нарушителя информационной безопасности / В.Г. Миронова, А.А. Шелупанов // Промышленные АСУ и контроллеры. – 2012. – № 3. – С. 53–56.

40. Нагорный С.И. Информационная система? Это очень просто! / С.И. Нагорный, Н.И. Дзюба // Защита информации. INSIDE. – 2013. – № 6. – С. 25–29.

41. Нагорный С.И. Вопросник от дилетанта / С.И. Нагорный, Ю.В. Клиомфас // Защита информации. INSIDE. – 2013. – № 5. – С. 12–18.

42. Новиков В.А. Понятие частной жизни и уголовно-правовая охрана ее неприкосновенности / В.А. Новиков // Уголовное право. – 2011. – № 1. – С. 43–48.

43. Петренко С.А. Инфраструктурные модели операторов персональных данных / С.А. Петренко, А.В. Зотова // Защита информации. INSIDE. – 2013. – № 6. – С. 42–45.

44. Пирбудагова Д.Ш. Проблемы защиты персональных данных в условиях глобализации / Д.Ш. Пирбудагова, И.С. Садикова // Юридический вестник ДГУ. – 2012. – № 3. – С. 69–72.

45. Попова Е.В. Повышение конкурентоспособности малых предприятий сферы услуг путем усиления информационной безопасности после принятия закона о персональных данных / Е.В. Попова // Журнал правовых и экономических исследований. – 2012. – № 3. – С. 106–110.

46. Прокушев Я.Е. Сравнительный анализ средств программно-аппаратной защиты информации, применяемых в информационных системах персональных данных / Я.Е. Прокушев, С.В. Пономаренко // Информация и безопасность. – 2012. – № 1. – С. 31–36.

47. Сабанов А.Г. Обзор иностранной нормативной базы по идентификации и аутентификации / А.Г. Сабанов // Защита информации. INSIDE. – 2013. – № 4. – С. 82–88.

48. Сачков Д.И. Использование информационных систем для защиты персональных данных / Д.И. Сачков, В.Н. Быкова // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). – 2014. – № 3. – С. 203–210.

49. Сачков Д.И. Оценка эффективности информационно-телекоммуникационных систем на основе свободного программного обеспечения / Д.И Сачков, В.В. Братищенко, З.В. Архипова. – Иркутск : Изд-во БГУЭП, 2013. – 150 с.

50. Сачков Д.И. Современные информационно-телекоммуникационные технологии в управлении социально-экономическими системами / Д.И. Сачков, З.В. Архипова, В.В. Братищенко. – Иркутск : Изд-во БГУЭП, 2013. – 196 с.

51. Сафрошкин О. Кардиохирургия. А вы защитили сердце своего бизнеса? / О. Сафрошкин // Защита информации. INSIDE. – 2013. – № 6. – С. 58–59.

52. Сковородник П. Должна ли распределяться ответственность за управление информационными рисками в организации? / П. Сковородник // Защита информации. INSIDE. – 2013. – № 6. – С. 30–33.

53. Смирнова И.Г. Киберпреступность в ряде стран Азиатско-тихоокеанского региона: сравнительно-правовой анализ / И.Г. Смирнова, В.В. Коломинов, О.А. Егерева // Евразийская парадигма России и трансформация политико-правовых институтов стран Азиатско-Тихоокеанского региона : материалы 5-й междунар. науч.-практ. конф. / под науч. ред. Ю.И. Скуратова. – Улан-Удэ : Изд-во БГУ, 2014. – С. 173–178.

54. Смирнова И.Г. К вопросу о выборе методологии исследования проблем киберпреступности / И.Г. Смирнова // Уголовно-процессуальные и криминалистические средства обеспечения эффективности уголовного судопроизводства : материалы междунар. науч.-практ. конф. Иркутск, 25–26 сент. 2014 г. – Иркутск : Изд-во БГУЭП, 2014. – С. 200–203.

55. Станкевич В.Ю. Обзор DLP-систем / В.Ю. Станкевич // Технологии безопасности. – 2011. – № 3. – С. 59–61.

56. Тищенко Е.Н. Алгоритмизация процесса формирования частной модели угроз безопасности персональных данных / Е.Н. Тищенко, Е.Ю. Шкаранда // Известия ЮФУ. Технические науки. – 2011. – № 3. – С. 32–40.

57. Федюнин А.Е. Правовая культура: роль и место конституционных прав личности в защите персональных данных сотрудника / А.Е. Федюнин, М.В. Бочкарев // Правовая культура. – 2013. – № 1. – С. 171–175.

58. Фролова О.С. Частная жизнь в свете Конвенции о защите прав человека и основных свобод / О.С. Фролова // Журнал российского права. – 2008. – № 10. – С. 119.

59. Шелестова О. Управление инцидентами безопасности: проблемы и их решения / О. Шелестова // Банковские технологии. – 2011. – № 1. – С. 28–30.

Аналитические отчеты и обзоры, статистические данные

60. Дифференцированный подход к определению периода ограничения доступа для различных тематических групп конфиденциальных персональных данных, содержащихся в архивных документах : аналит. обзор [Электронный ресурс]. – Режим доступа: http://mail.vniidad.ru/index.php?option=com_content&view=article&id=1531&Itemid=778.

61. Безопасность информации в корпоративных информационных системах. Внутренние угрозы : аналит. отчет [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/analytics.

62. Безопасность персональных данных в России в 2013 году. Статистика утечек. Отраслевые особенности : аналит. отчет [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/analytics.

63. Глобальное исследование утечек конфиденциальной информации из компаний среднего и малого бизнеса в 2013 году : аналит. отчет [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/analytics.

64. Количество утечек данных в 2014 году значительно увеличилось : аналит. отчет [Электронный ресурс]. – Режим доступа: http://ru.safenetinc.com/About_SafeNet/News_and_Media/News_and_Media_Items/2014.

65. Утечки конфиденциальной информации. Итоги 2013 года : аналит. отчет [Электронный ресурс]. – Режим доступа: http://www.zecurion.ru/press/analytics.

66. Бизнес безопасности или безопасность бизнеса? О том и о другом в одном блоге [Электронный ресурс]. – Режим доступа: http://www.lukatsky.blogspot.ru.

67. Информационная безопасность в России и мире [Электронный ресурс]. – Режим доступа: http://80na20.blogspot.ru.

68. Отчеты о деятельности Уполномоченного органа по защите прав субъектов персональных данных [Электронный ресурс]. – Режим доступа: http://rkn.gov.ru.

69. Персональные данные на практике остаются беззащитными [Электронный ресурс]. – Режим доступа: http://www.audit-it.ru/articles/soft/a115/177035.html.

70. Полезная аналитика про утечки информации [Электронный ресурс]. – Режим доступа: http://80na20.blogspot.ru/2014/06/blog-post_10.html.

Использованная литература

70. О защите личности в связи с автоматической обработкой персональных данных : Конвенция Совета Европы [Электронный ресурс]. – Режим доступа: http://base.garant.ru/2559798/1/#block_9999.

71. О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных : директива 95/46/ЕС Европ. парламента и Совета Европ. Союза от 24 окт.

1995 г. [Электронный ресурс]. – Режим доступа: http://32.rkn.gov.ru/personal-data/p2309.

72. ISO/IEC 27001:2005 «Системы менеджмента информационной безопасности. Требования» [Электронный ресурс]. – Режим доступа: https://dominder.com/iso27001.ru.

73. The Freedom of Information Act [Электронный ресурс]. – Режим доступа: http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm.

74. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/publications/PubsSPs.html.

75. США и Евросоюз: отличия законодательств по защите персональных данных [Электронный ресурс]. – Режим доступа: http://www.pdp.net.ua/ssha-i-evrosouz-otlichiya-zakonodatelstv-po-zaschite-personalnyx-dannyx.

76. Новый закон о защите персональных данных в США [Электронный ресурс]. – Режим доступа: http://www.uipdp.com/news/2011-05/27.html.

77. Модельный закон «О персональных данных» [Электронный ресурс]. – Режим доступа: http://www.russianlaw.net/law/civil_rights/pd/t20.

78. Конституции стран СНГ [Электронный ресурс]. – Режим доступа: http:// www.new.medialaw.ru/law_CIS_Baltic/texts.

79. О регистре населения : закон Респ. Беларусь от 21 июня 2008 г. № 418-З [Электронный ресурс]. – Режим доступа: http://pravo.by.

80. Об информации, информатизации и защите информации : закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З [Электронный ресурс]. – Режим доступа: http://www.pravo.by/main.aspx?guid=3871&p2=2/1552.

81. О персональных данных и их защите : закон Респ. Казахстан [Электронный ресурс]. – Режим доступа: http://online.zakon.kz/Document/?doc_id=31396226.

82. Кодекс Республики Казахстан об административных правонарушениях от 30 янв. 2001 г. № 155-II [Электронный ресурс]. – Режим доступа: http://online.zakon.kz/Document/?doc_id=1021682&sublink=84010000.

83. Уголовный кодекс Республики Казахстан от 16 июля 1997 г. № 167-I [Электронный ресурс]. – Режим доступа: http://online.zakon.kz/Document/?doc_id=1008032&sublink=1420000.

84. Об утверждении Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных : постановление Правительства Респ. Казахстан от 3 сент. 2013 г. № 909 [Электронный ресурс]. – Режим доступа: http://online.zakon.kz/Document/?doc_id=31441634.

85. О защите персональных данных : закон Украины от 1 янв. 2011 г. № 2297-VI [Электронный ресурс]. – Режим доступа: http://www.medialaw.kiev.ua/ru/laws/laws_local/115.

86. Уголовный кодекс Украины [Электронный ресурс]. – Режим доступа: http://pravoved.in.ua/section-kodeks/134-yku.html.

87. Кодекс Украины об административных правонарушениях от 7 дек. 1984 г. № 8073-X [Электронный ресурс]. – Режим доступа: http://www.nibu.factor.ua/info/Zak_basa/Kodeksy/KUoAP.

88. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных : федер. закон РФ от 19 дек. 2005 г. № 160-ФЗ [Электронный ресурс]. – Режим доступа: http://pd.rkn.gov.ru/law/p132/document172.htm?print=1.

89. Законопроект по внесению изменений в КОАП за несоблюдение требований 152-ФЗ [Электронный ресурс] // Блог «Бизнес без опасности» А. Лукацкого. – Режим доступа: http://lukatsky.blogspot.ru/2014/01/152.html.

90. Отчет аналитического центра Info Watch [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/analytics/panels/2580.

91. Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования : федер. закон РФ от 1 апр. 1996 г. [Электронный ресурс]. – Доступ из СПС «Контур-Норматив».

92. Просвирин Ю.Г. Защита персональных данных / Ю.Г. Просвирин // Вестник Воронежского государственного университета. – Сер. Право. – 2008. – № 1. – С. 174–188.

93. Лукацкий А.В. Кто такой сотрудник в контексте ПП-1119? [Электронный ресурс] / А.В. Лукацкий. – Режим доступа: http://lukatsky.blogspot.ru/2013/08/1119.html.

94. Лукацкий А.В. Очередные размышления о лицензировании деятельности по ТЗКИ [Электронный ресурс] / А.В. Лукацкий. – Режим доступа: http://lukatsky.blogspot.ru/2013/03/blog-post_6287.html.

95. Шередин Р.В. Защита персональных данных в информационных системах методом обезличивания [Электронный ресурс] / Р.В. Шередин. – Режим доступа: http://www.dissercat.com/content/zashchita-personalnykh-dannykh-v-informatsionnykh-sistemakh-metodom-obezlichivaniya#ixzz32MRjWE6v.

96. Кучин И.Ю. Обработка баз данных с персонифицированной информацией для задач обезличивания и поиска закономерностей [Электронный ресурс] / И.Ю. Кучин. – Режим доступа: http://tekhnosfera.com/obrabotka-baz-dannyh-s-personifitsirovannoy-informatsiey-dlya-zadach-obezlichivaniya-i-poiska-zakonomernostey#ixzz32MQgm9MN.

97. Рекомендации по выполнению требований Федерального закона № 152-ФЗ «О персональных данных» [Электронный ресурс]. – Режим доступа: http://www.leta.ru/library/methodological.

98. ООО «Код безопасности» [Электронный ресурс] : офиц. сайт. – Режим доступа: http://www.securitycode.ru/products/secret_net/scope_auto_edition.

99. ООО «Кондидент» [Электронный ресурс] : офиц. сайт. – Режим доступа: http://www.dallaslock.ru/sub-doc.html.

100. Шабанов И. Тест антивирусов на лечение активного заражения (октябрь 2012 г.) [Электронный ресурс] / И. Шабанов. – Режим доступа: http://www.anti-malware.ru/malware_treatment_test_2012.

101. Возможности SecureTower [Электронный ресурс]. – Режим доступа: http://falcongaze.ru/products/secure-tower/opportunities.html.

102. Возможности InfoWatch Traffic Monitor [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/products/traffic_monitor_enterprise.

103. Возможности [Электронный ресурс]. – Режим доступа: http://www.zecurion.ru/products/zgate.

104. Гуляева Л.В. Совершенствование механизма управления муниципальными образованиями / Л.В. Гуляева, А.В. Самаруха, Д.И. Сачков. – Иркутск : Изд-во БГУЭП, 2010. – 242 с.

105. Сачков Д.И. Внедрение инфокоммуникационных технологий в региональные органы власти / Д.И. Сачков // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). – 2009. – № 6. – С. 80–83.

106. Сачков Д.И. Информатизация органов местного самоуправления как основной принцип обеспечения повышения качества оказываемых услуг / Д.И. Сачков // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). – 2011. – № 2. – С. 39.

107. Самаруха А.В. Реализация модели инновационного устойчивого развития муниципального образования с использованием информационно-телекоммуникационных технологий / А.В. Самаруха, Д.И. Сачков // Экономический кризис и возможные пути его преодоления / под ред. В.И. Самарухи, Ж.-П. Гишара. – Иркутск, 2009. – С. 173–178.

108. Сачков Д.И. Модернизация системы управления на уровне муниципалитетов / Д.И. Сачков // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). – 2009. – № 2. – С. 101–105.

109. Основы предпринимательской деятельности : учеб. пособие / А.В. Самаруха, Д.И. Сачков, Л.В. Гуляева, И.В. Гущина, Е.В. Хитрова, Е.А. Стародубцева. – Иркутск : Изд-во БГУЭП, 2011. – 244 с.

Учебное издание

Сачков Дмитрий Иванович
Смирнова Ирина Георгиевна

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВЛАСТИ

Учебное пособие

Издается в авторской редакции

ИД № 06318 от 26.11.01.
Подписано в печать 18.03.15. Формат 60х90 1/16. Бумага офсетная. Печать трафаретная. Усл. печ. л. 7,6. Тираж 100 экз. Заказ .

Издательство Байкальского государственного университета экономики и права.
664003, г. Иркутск, ул. Ленина, 11.

Отпечатано в ИПО БГУЭП.