Д.И. Сачков,
И.Г. Смирнова,
В.Н. Быкова

ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИЯХ

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

Д.И. Сачков,
И.Г. Смирнова,
В.Н. Быкова

ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИЯХ

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

Издано 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. техн. наук, доц. В.В. Братищенко
д-р юрид. наук., проф. А.А. Протасевич

Сачков Д.И.
С22 Оценка уровня защищенности персональных данных в организациях / Д.И. Сачков, И.Г. Смирнова, В.Н. Быкова. – Иркутск : Изд-во БГУЭП, 2015. – 150 с.

ISBN 978-5-7253-2867-7

В работе раскрывается понятие информационной безопасности, содержится анализ теории защиты информации, дается классификация нормативно-правовых актов, регулирующих общественные отношения в сфере обеспечения информационной безопасности. Положения и выводы данной монографии могут быть использованы в качестве практической основы для решения задач эффективного обеспечения защиты персональных данных в организациях различных сфер деятельности.

Предназначено для научных сотрудников, преподавателей, аспирантов, магистрантов, бакалавров, интересующихся проблемами защищенности персональных данных.

УДК 43.98(075.8)
ББК 67.408.135я7

ISBN 978-5-7253-2867-7

ОГЛАВЛЕНИЕ

Список сокращений

NIST – National Institute of Standards and Technology;
ИСПДн – информационная система, обрабатывающая персональные данные;
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;
ИСПДн-О – информационная система, обрабатывающие общедоступные категории персональных данных (если данные в информационной системе получены только из общедоступных источников);
ИСПДн-С – информационная система, обрабатывающая специальные категории персональных данных (например, данные о расовой, национальной принадлежности, интимной жизни, политические взгляды, философские убеждения);
НСД – несанкционированный доступ;
ПДн – персональные данные;
ТЗКИ – техническая защита конфиденциальной информации;
УЗ – уровень защиты;
ФСБ – Федеральная служба безопасности;
ФСТЭК – Федеральная служба по техническому и экспортному контролю.

ВВЕДЕНИЕ

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, используемых сегодня. Это 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 др.).

Государство на законодательном уровне четко определило, что сбор, хранение и распространение информации о частной жизни лица без его согласия не допускаются, в связи с чем требует от организаций и индивидуальных предпринимателей, обрабатывающих персональные данные, обеспечить их защиту. Активная деятельность по защите персональных данных 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 5359 дел в суд на общую сумму 8,9 млн р., а в 2013 г. 9709 физических лиц

пожаловались на нарушение их прав и 4125 дел было передано в суд на сумму более 6,5 млн р.[1]

Помимо простого невыполнения законодательства в области защиты персональных данных, имеет место быть неквалифицированное применение требований закона. А самые негативные последствия влечет за собой формальное применение закона, только на бумаге, без включения реальных 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 закона. В настоящее время требования законодательства 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: не подготовили документацию, отвечающую требованиям закона, а также не внедрили средства защиты.

[1] Отчеты о деятельности Уполномоченного органа по защите прав субъектов персональных данных [Электронный ресурс]. URL: http://rkn.gov.ru.

1. ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1. 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[1], что в 2,2 % выше аналогичного показателя 2012 г. А по данным компании SafeNet[2] 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[3], 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 свершимся 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 пре-

---

[1] Аналитический отчет «Безопасность информации в корпоративных информационных системах. Внутренние угрозы» [Электронный ресурс]. URL: http://www.infowatch.ru/ analytics.

[2] Аналитический отчет «Количество утечек данных в 2014 году значительно увеличилось» [Электронный ресурс]. URL: http://ru.safenet-inc.com/About_SafeNet/ News_and_ Media/News_and_Media_Items/2014/ Количество_утечек_данных_в_2014_году_значительно_увеличилось;_за_первые_три_месяца_года_было_похищено_200_ миллионов_ записей.

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

жде всего с нормой в законодательстве этих стран, поэтому компании предпочитают выстраивать эффективную защиту не на бумаге, а на деле[1, 2].

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 2014 г. распределились поровну (рис. 1).

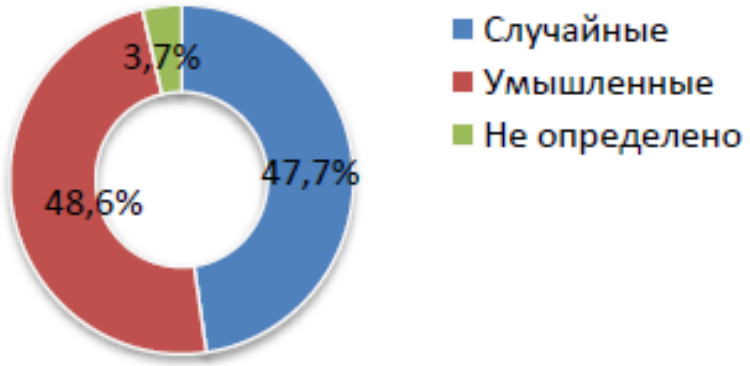

Рис. 1. Распределение случайных и умышленных утечек в 2014 г.

По данным аналитического центра компании InfoWatch[3], выявлено не большое число актуальных каналов утечки (рис. 2):

бумажные документы (ксерокопии паспортов, выброшенные договора, формы, заявки и прочее);

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

голосовой канал.

[1] Информационная безопасность в России и мире [Электронный ресурс]. URL: http://80na20.blogspot.ru.

[2] Полезная аналитика про утечки информации [Электронный ресурс]. URL: http://80na20.blogspot.ru/2014/06/blog-post_10.html.

[3] Глобальное исследование утечек конфиденциальной информации из компаний среднего и малого бизнеса в 2013 г. [Электронный ресурс] : аналит. отчет. URL: http://www.infowatch.ru/analytics.

Рис. 2. Распределение случайных и умышленных утечек по отраслям

Также сотрудниками аналитического центра компании InfoWatch выявлено, что в 2014 г. 19 % утечек персональных данных пришлись на государственные органы, а более 66 % всех утечек происходит на долю малых и средних компаний (рис. 3)[1].

Таким образом, авторы данного исследования 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, изменить ситуацию возможно лишь в том случае, если операторы ПДн начнут отвечать за утечки персо-

[1] Утечки конфиденциальной информации. Итоги 2013 года [Электронный ресурс] : аналит. отчет. URL: http://www.zecurion.ru/press/analytics.

нальных данных рублем и репутацией, только в этом случае у них появиться стимул обеспечивать безопасность ПДн на должном уровне.

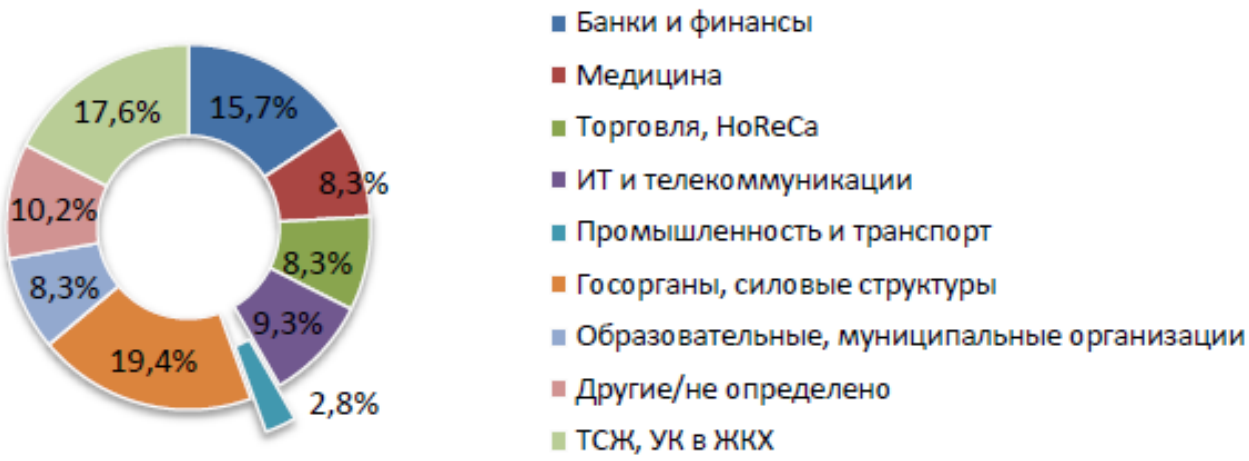

Рис. 3. Распределение утечек по отраслям

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

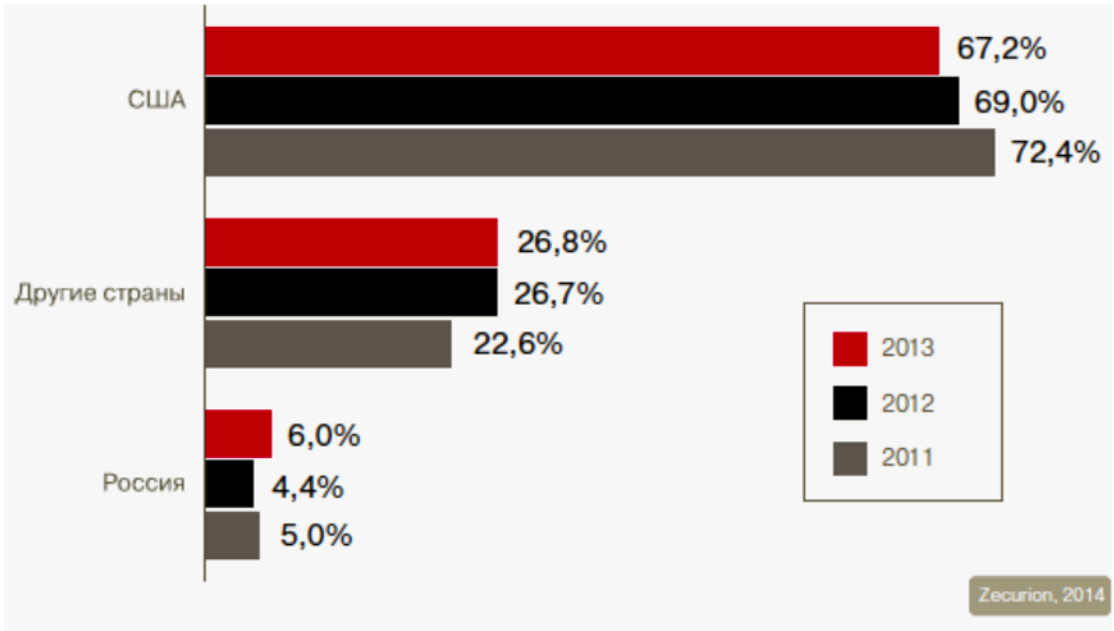

Рис. 4. Доля утечек по странам

[1] Информационная безопасность в России и мире [Электронный ресурс]. URL: http://80na20.blogspot.ru.

Как и в России, в странах Европы умышленные и случайные утечки распределились поровну. По данным аналитиков, выявлено не большое число актуальных каналов утечки (рис. 5)[1].

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

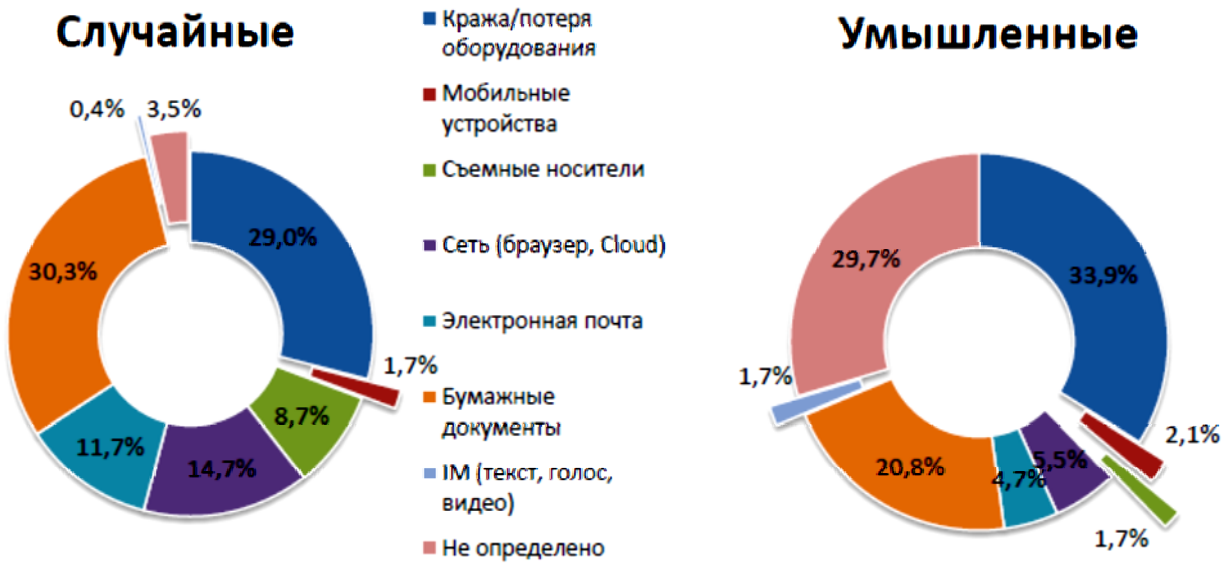

Рис. 5. Актуальные каналы утечки конфиденциальной информации

Аналитики компаний констатируют, что наибольшее количество утечек персональных данных в зарубежных странах также приходиться на государственные структуры.

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, который может привести компании к выплате многомиллионных штрафов и компенсаций пострадавшим.

[1] Количество утечек данных в 2014 году значительно увеличилось [Электронный ресурс] : аналит. отчет. URL: http://ru.safenet-inc.com/About_SafeNet/News_and_Media/News_and_Media_Items/2014/Количество_утечек_данных_в_2014_ году_ значительно_ увеличилось;_за_первые_три_месяца_года_было_похищено_200_миллионов_записей.

Наиболее громкими публичными утечками 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 банк. Среди утилизированных бумаг оказались заявления на выдачу пластиковых карт, подписанные договора банковского обслуживания, заявления на выдачу кредитов. Было инициировано служебное расследование, результаты которого в открытый доступ не обнародовали[1].

1.2. Обеспечение информационной безопасности: технический анализ

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, используемых 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 ин-

[1] Утечки конфиденциальной информации. Итоги 2013 года [Электронный ресурс] : аналит. отчет. URL: http://www.zecurion.ru/press/analytics.

формации (так называемый промышленный шпионаж), так и на организацию собственной информационной безопасности (коммерческая тайна, персональные данные, информация о клиентах и поставщиках и другая информация).

Еще больше ситуация усложняется с колосальным ростом количества утечек информации. Так по данным аналитического центра компании InfoWatch в рамках глобального исследования утечек конфиденциальной информации за 2014 год. число утечек информации в мире выросло на 22 %, в России – на 73 % по сравнению с 2013 г.[1] В I полугодии 2015 года в мире обнародовано (в СМИ и иных источниках) и зарегистрировано Аналитическим центром InfoWatch 723 случая утечки конфиденциальной информации, что на 10 % превышает количество утечек, зарегистрированных за аналогичный период 2014 года. Что говорит о постоянном росте количества утечек информации.

Особое внимание необходимо обратить на внешние атаки в РФ, в первом полугодии 2015 г. они составили 32 % утечек данных[2]. Доля таких утечек выросла на 9 пунктов по сравнению с показателем I полугодия 2014 года.

Так исходя из отчета аналитического центра, за 2014 год, 90 % утечек связаны с компрометацией персональных данных, скомпрометированы более 262 млн записей, в том числе платежная информация.

Также зафиксированы 8 крупных утечек информации, итогом стали скомпрометированы более 10 млн персональных данных. На такие утечки пришлось 83 % всех скомпрометированных записей. Основными виновниками остаются сотрудники, порядка 58 % случаев, что говорит о низком уровне образования персонала компаний в рамках информационной безопасности и информационных технологиях[3]. В 1 % случаев – высшие руководители организаций стали причиной разглашения информации. По итогу 2014 г. Россия заняла второе место по числу утечек, ставших достоянием общественности.

---

[1] В России две трети утечек информации происходят в СМБ-компаниях [Электронный ресурс] : ст. URL: https://www.infowatch.ru/presscenter/news/6696.

[2] Исследование утечек информации за первое полугодие 2015 года [Электронный ресурс] : аналит. отчет InfoWatch. URL: https://www.infowatch.ru/analytics/reports/16340.

[3] Там же.

Наиболее часто скомпрометированными оказываются персональные данные, по данным компании SafeNet[1] 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[2], 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 свершимся 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[3].

Для получения представления об истинных причинах ухудшения положения в области защиты информации, необходимо рассмотреть основные каналы утечки в России.

Так в первом полугодии 2015 г. зарегистрирована 471 (65 %) утечка информации, причиной которой стал внутренний нарушитель. В 233 (32 %) случаях утечка информации произошла из-за внешнего воздействия, 2,6 % не определено (рис. 6).

---

[1] Количество утечек данных в 2014 году значительно увеличилось [Электронный ресурс] : аналит. отчет. URL: http://ru.safenet-inc.com/About_SafeNet/News_and_Media/News_and_Media_Items/2014/Количество_утечек_данных_в_2014_году_значительно_увеличилось;_за_первые_три_месяца_года_было_похищено_200_миллионов_записей.

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

[3] Информационная безопасность в России и мире [Электронный ресурс]. URL: http://80na20.blogspot.ru.

Рис. 6. Распределение утечек по вектору воздействия
в первом полугодии 2015 г.
(по данным Аналитического центра InfoWatch, 2015 г.)

Из схемы видно, что из года в год внутренний нарушитель представляет наибольшую опасность, так как пользователь, имеющий широкий спектр прав доступа, может нанести наибольший ущерб.

На одну утечку в среднем приходится 0,36 млн скомпрометированных записей. Общий объем скомпрометированных персональных данных за первое полугодие 2015 г. составил 262 млн записей[1].

На основе этих данных, рост доли утечек персональных данных не позволяет говорить о их качественной защите. На наш взгляд это является следствием отсутствия корректно работающих нормативно-правовых документов.

В первом полугодии 2015 г. Доля утечек под воздействием внешнего злоумышленника выросла на 9 п. п. и составила 32 %. Доля случаев, когда виновника не удалось определить, по сравнению с показателем I полугодия 2014 года снизилась на 2 п. п. и составила 6 % (рис. 7).

[1] Исследование утечек информации за первое полугодие 2015 года [Электронный ресурс] : аналит. отчет InfoWatch. URL: https://www.infowatch.ru/ analytics/reports/16340.

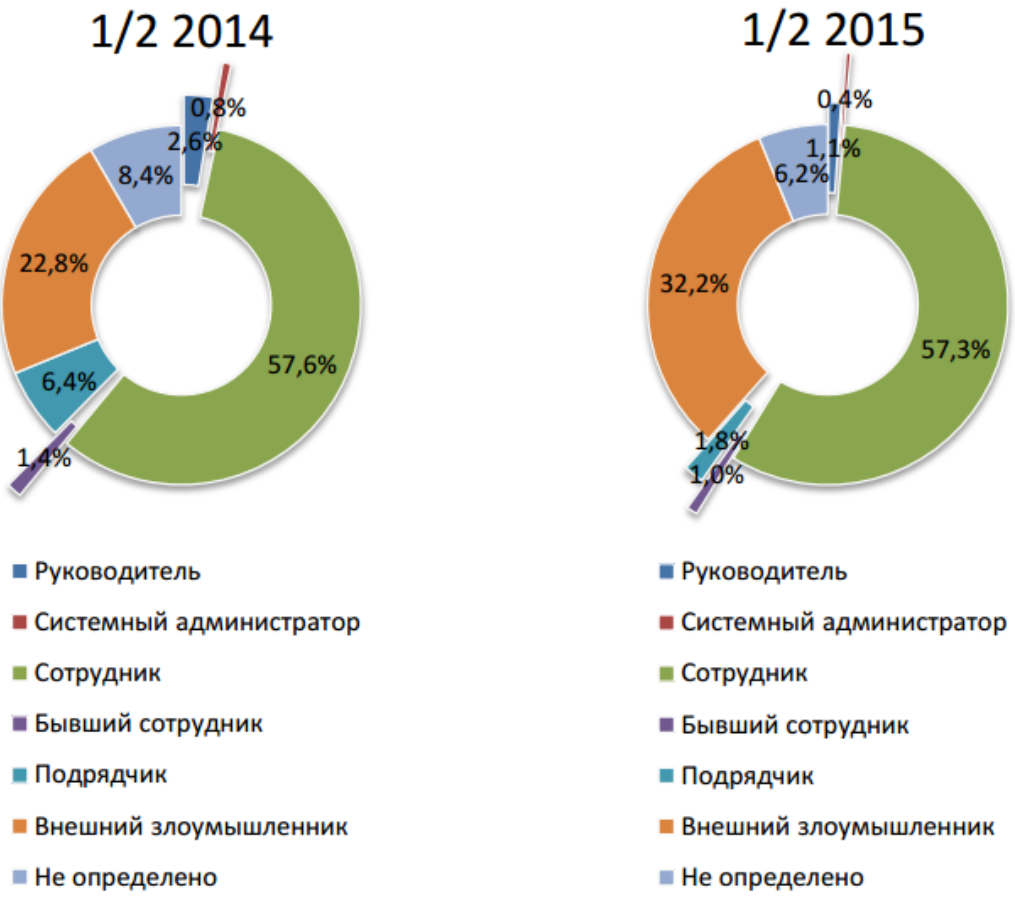

Рис. 7. Распределение утечек по источнику (виновнику),
I полугодие 2014 – I полугодие 2015 г.
(по данным Аналитического центра InfoWatch, 2015 г.)

Данный график говорит в первую очередь о безграмотности сотрудников в области информационных технологий и технологий защиты информации. Более половины всех угроз составляют рядовые сотрудники. Подтверждением служит крайне малый процент скомпрометированных данных системными администраторами, всего 0,4 %.

Доля утечек персональных и платежных данных осталась на уровне 2014 года – 90 %. Незначительно подросли утечки информации, составляющей государственную и коммерческую тайну. Доли таких утечек – 3 и 5 % соответственно (рис.8)

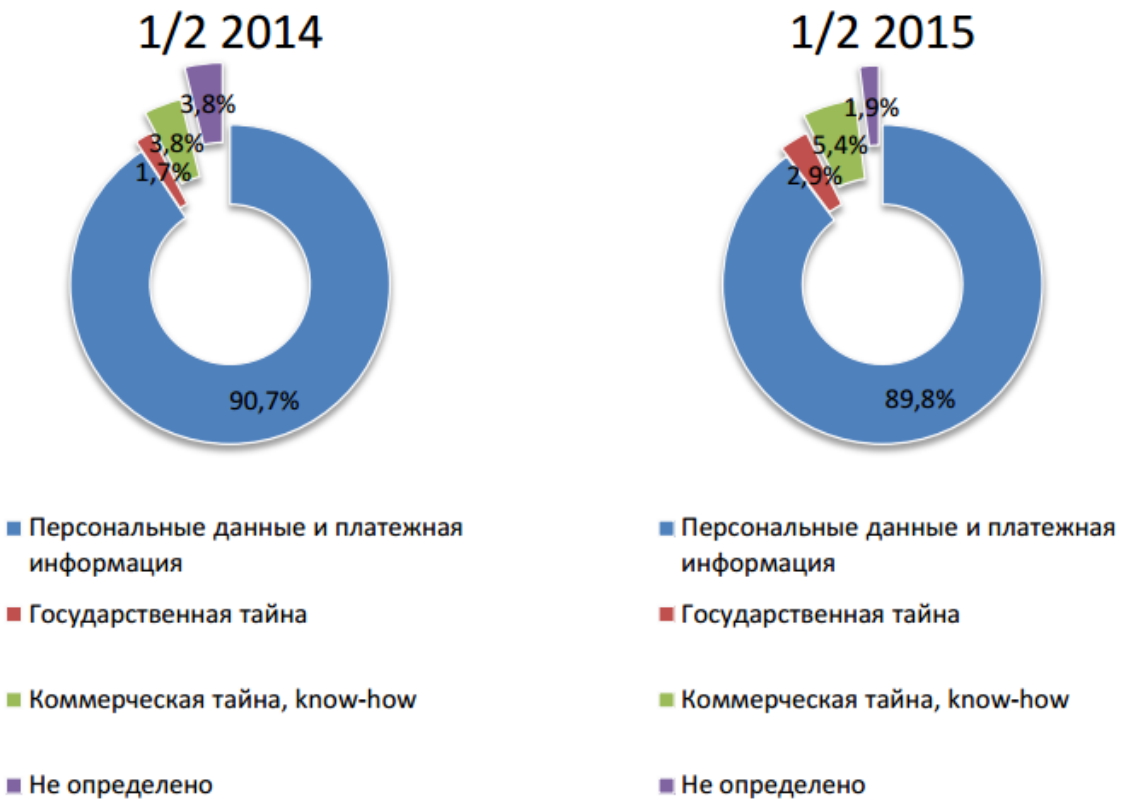

Рис. 8. Распределение утечек по типам данных,
первое полугодие 2014–2015 г.
(по данным Аналитического центра InfoWatch, 2015 г.)

Наибольшее количество утечек информации, связанных с использованием персональных данных в целях мошенничества – являются преступления, известные как «кража личности» (identity theft). Преступление, характеризуется незаконным использованием персональных данных человека с целью получения материальной выгоды. «Кражи личности» получили широкое распространение в США во второй половине XX в. Это было связано с широким внедрением услуг, предоставляемых удаленно без личного присутствия, в том числе с использованием информационно-телекоммуникационных технологий. Наибольшее количество было связано с выпуском кредитных карт, получения кредитов и т.д. Также преступления связывают с широким распространением SSN (Social Security number) в качестве идентификатора личности. Для подтверждения личности по телефону организации запрашивают номер SSN. В Британии для «краж личности» используют страховые идентификаторы NINO (National Insurance number) и NHS (National Health Service number).

Внутренние и внешние злоумышленники пытаются любым способом получить доступ к базам с персональными данными клиентов и сотрудников компаний, используют эти данные при проведении мошеннических финансовых операций, например при оформлении электронных требований на возврат налогов.

По данным CioWorld, приобрести персональную информацию не составит большого труда, так стоимость на черном рынке США набор информации для кражи личности, включающий адрес и SSN, стоит от 16 до 30 дол. Вероятность стать жертвой кражи личности оценивается в 2 % для среднего жителя США.

По данным TrendMicro, скан паспорта, водительских прав, счетов стоит от 10 до 25 дол. Кредитная история обойдется в 25 дол. Аккаунты PayPayl и eBay с транзакциями за полгода-год – по 300 дол. каждый. Цена информации о банковских счетах колеблется от 200 до 500 дол. А те самые ПДн (имя, адрес, дата рождения, SSN) стоят около 1 дол.[1]

Исходя из этого, можно сделать вывод о растущем спросе на данный вид информации. Эксперты зафиксировали рост мошенничества с персональными данными интернет-пользователей. Кража, связанная с финансовыми махинациями, выросла на 12 %. В Великобритании более половины всех выявленных случаев мошенничества с информацией о пользователях сети приходится на кражу денег.

Число похищений персональных данных, связанных с текущими счетами, за 2014 г. выросло на 20 %. Мошенники используют данные жертв еще и для взятия кредита без ведома последних. На 79 % увеличилось число заявок на получение банковских карт от чужого имени. А вот брать автокредиты на чужое имя у мошенников не популярно. Как показывает статистика, их доля составляет 12 % от числа зафиксированных фиктивных займов от чужого имени.

Но есть и мошенники, которые действуют под собственным именем. В частности, при открытии ипотечного кредита. Почти девять из десяти мошеннических попыток взять деньги под ипотеку – это предоставление заемщиком неверных сведений в заявке на кредит.

Впрочем, по сравнению с аналогичным периодом 2014 г., в 2015 г. доля утечек данных, сопряженных с последующим исполь-

[1] The price of your identity in the Dark Web? No more than a dollar http://www.zdnet.com/article/the-price-of-your-identity-in-the-dark-web-no-more-than-a-dollar/#ftag=RSSbaffb68.

зованием скомпрометированной информации в целях мошенничества (как правило, банковский фрод – вид мошенничества в области информационных технологий, в частности, несанкционированные действия и неправомочное пользование ресурсами и услугами в сетях связи) снизилась и составила 11 % (рис. 9).

Рис. 9. Распределение утечек по характеру, I полугодие 2015 г. (по данным Аналитического центра InfoWatch, 2015 г.)

Мошенничество с помощью кредитных карт (кардинг, включает в себя кражу данных карты в интернете (фишинг), копирование информации, содержащейся на магнитной полосе карты (скимминг), а также мошенничество при оплате при физическом отсутствии карты (Card not present transaction).

Большинство банков публикуют списки фродоопасных стран на своем сайте. И если клиент посещает такую страну, банк отслеживает операции с его пластиковой карточкой и предлагает перевыпустить её за счет банка или клиента[1].

Также фроду относятся операции, касающиеся поддельных банковских карт. С использованием гибридной карты (чип и магнитная полоса), производится копирование информации её магнитной полосы и переносятся на другую карту с магнитной поло-

[1] Голдовский И. Ещё раз о фроде. Очередные шаги международных платёжных систем, направленные на повышение безопасности карточных транзакций // ПЛАС. 2009. № 2 (142). С. 3–5.

сой или на гибридную с нерабочим чипом. Операции могут успешно выполняться: в режиме онлайн (в устройствах читающих магнитную полосу), в режиме оффлайн (подлимитные операции) или в режиме fallback (при невозможности читать чип устройство проводит операцию по магнитной полосе). Ответственность за такой фрод ложится на эмитента карточки или на эквайрера.

В настоящее время наблюдается стабилизация распределения угроз. Наиболее значимым является увеличение доли утечек данных под воздействием внешних атак и, соответствующее увеличение доли внешнего злоумышленника в распределении по критерию «виновник утечки». Что говорит о росте угрозы со стороны не простого персонала, а высококвалифицированных специалистов в области защиты информации, занимающихся не законными способами обогащения. Введение новых нормативов, законодательных актов, использование программно-технических средств защиты не позволяет снизить риски, возникшие по вине внутреннего нарушителя (случайные и намеренные). Такие факты утечек в настоящий момент принимают обыденное явление и с каждым годом увеличивают свою долю. Широко распространенные средства контроля и ограничения доступа, не оказывают системного влияния на снижение утечек данных. Что в свою очередь, говорит о необходимости обновления нормативно-законодательных актов, направленных на снижение подобных рисков, как показывает практика одним внедрением программно-технических комплексов недостаточно для существенной минимизации внутренних угроз.

Также стоит отметить рост доли утечек вследствие злоупотребления (превышения) правами доступа. Данный вид угрозы также относится к внутренним угрозам. С минимизацией которых, на наш взгляд, наиболее эффективно стоит бороться с помощью нормативно правовых актов, изменением внутренней политики организации. В настоящий момент подобные угрозы будут усиливаться, осложняющаяся экономическая ситуацией в стране: сокращение штата, снижение уровня заработной платы, недобросовестная конкуренция. Все эти факторы будут способствовать увеличению внутренних угроз.

Помимо этих угроз набирает силу угрозы, произошедшие вследствие внешних атак. На их долю приходиться наиболее крупных и заметных инцидентов. Именно внешние атаки на сегодня

являются основным фактором, который оказывает решающее воздействие на формирование картины утечек данных.

В разрезе каналов утечек, в первом полугодии 2015 года наблюдается тенденция сокращения доли утечек по каналам «потеря оборудования», «электронная почта», «бумажные документы». Это каналы, которые можно контролировать с помощью технических средств защиты. Это обусловлено ростом использования программно-технических средств защиты. Доли утечек через съемные носители, через мобильные устройства, текстовые и видеосообщения остались на уровне I полугодия 2014 г. (рис. 10).

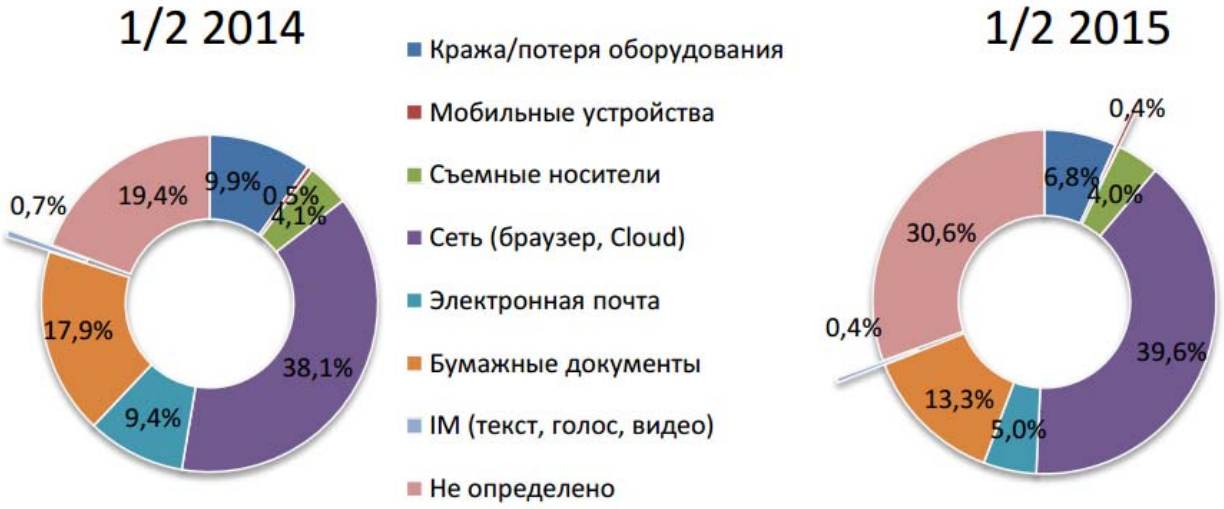

Рис. 10. Распределение утечек по каналам,
I полугодие 2014 – I полугодие 2015 гг.
(по данным Аналитического центра InfoWatch, 2015 г.)

Но наблюдается значительный рост количества сетевых угроз. На наш взгляд, это связано ростом количества инцидентов с участием внешних злоумышленников.

Рост числа случаев, когда невозможно точно определить, по какому каналу «ушла» информация, можно обосновать значительной долей утечек с помощью внутренних нарушителей. Доля таких утечек составила 31 %, рост к данным 2014 г. – 10 %.

Стоит отметить, что потери на прямую не связаны с количеством утечек по конкретному каналу. Может быть достаточно одного случая утечки критически важной информации по любому из каналов, чтобы у организации возникли серьезные проблемы.

По данным аналитического центра InfoWatch, доля умышленных утечек на каналах «кража/потеря оборудования», через мобильные устройства, съемные носители, электронную почту, бумажные документы, текстовые и видеосообщения год от года все более незначительны. Распределение умышленных утечек по каналам не отличается однородностью. В основном информация уходит через сеть (рис. 11).

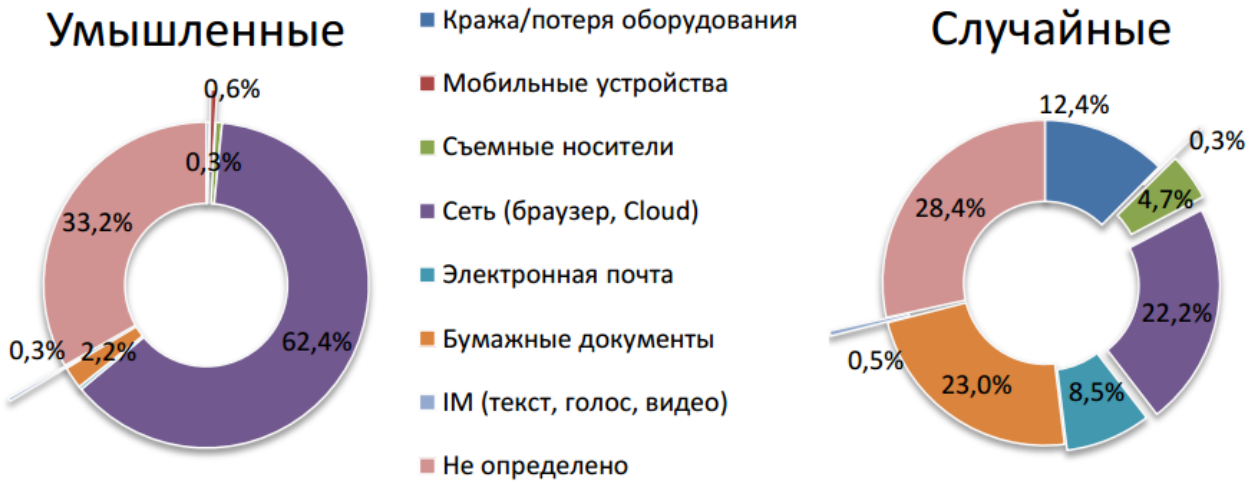

Рис. 11. Распределение утечек по каналам,
первое полугодие 2014–2015 гг.
(по данным Аналитического центра InfoWatch, 2015 г.)

Стоит отметить, что рост скомпрометированных данных через сетевые каналы неуклонно растет. В концепции защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа 1992 г., в качестве нарушителя рассматривается субъект, имеющий доступ к работе с штатными средствами автоматизированных систем и средств вычислительной техники как части автоматизированной системы. А также в своем уровне нарушитель является специалистом высшей квалификации, знает все о автоматизированных системах и, в частности, о системе и средствах ее защиты. Это говорит о том, что в большинстве случаев внешним нарушителем является высококвалифицированный специалист в области информационных технологий.

В рамках «Доктрины информационной безопасности РФ» от 9 сентября 2000 г. № Пр-1895, предусмотрено совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации.

Сегодня вопрос подготовки специалистов в этой области как никогда актуален и является важной задачей государственного уровня для организационно-правового обеспечения формирования и реализации государственной политики в этой области. В связи с развитием информационно-телекоммуникационных технологий, информационного права, формированием информационного общества, созданием электронного правительства особое значение приобретает подготовка специалистов, ориентированных на профессиональную деятельность в сфере организационно-правового обеспечения информационной безопасности. На долю таких специалистов отводится получения компетенций в рамках способов построения комплексных систем защиты информации, применения аппаратно-программных средств защиты. Данные компетенции становятся приоритетными для поддержания нормального функционирования как коммерческих, так и государственных структур.

Однако, как мы отмечали ранее, в настоящее время наблюдается острый дефицит высококвалифицированных специалистов в области обеспечения информационной безопасности. Причем такое положение характерно не только для России, но и для всего мира, поскольку проблемы обеспечения информационной безопасности в настоящее время приобретают трансграничный характер.

В связи с этим, первоочередной задачей в рамках обеспечения безопасности становится необходимость разработки таких методик учебно-воспитательной работы, в которых бы сочеталось обучение современным информационным технологиям с формированием высоких нравственных качеств для выработки не только иммунитета к совершаемым компьютерным преступлениям, но и к правовому просвещению и воспитанию киберкультуры [1].

Еще одним фактором подготовки кадров является количество утечек, и объем скомпрометированных данных чрез сетевой канал. Если рассматривать внутренних нарушителей, то в первую очередь компрометация данных происходит через сохранение конфиденциальной информации в облаках, а также использование бесплатных почтовых сервисов.

Большая часть (62 %) утечек персональных данных (конкретно – платежной информации) приходится на сетевой канал (рис. 12).

---

[1] Полякова Т.А., Химченко А.И. Особенности подготовки кадров в области организационно-правового обеспечения информационной безопасности // Информационное право. 2013. № 3.

В «Доктрине информационной безопасности РФ» от 09 сентября 2000 г., № Пр-1895 указано, что проблемы информационной безопасности перестали в настоящее время быть областью исключительной компетенции специальных служб (государства), они все больше становятся предметом внимания общества и личности. Объясняется это следующими обстоятельствами[1]:

1. Информация все больше становится таким атрибутом, от которого в решающей степени зависит эффективность жизнедеятельности всех сфер современного общества.

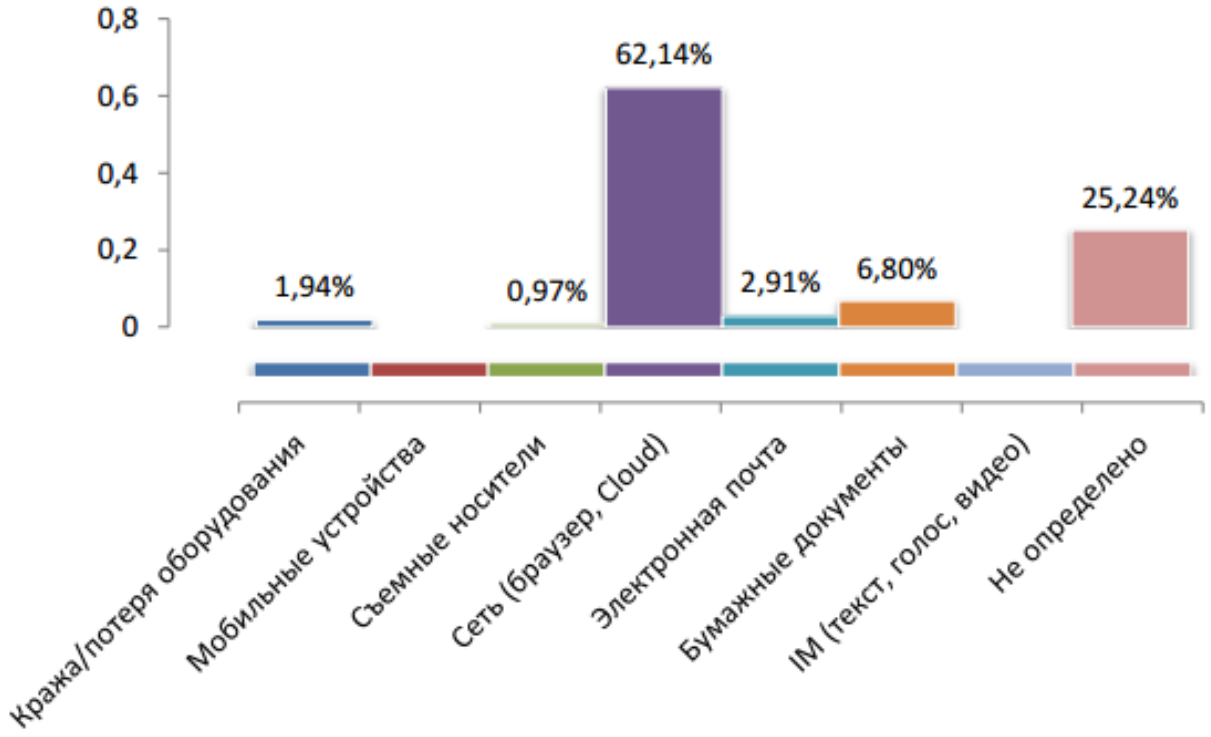

Рис. 12. Утечки платежных данных, распределение по каналам, первое полугодие 2015 г.
(по данным Аналитического центра InfoWatch, 2015 г.)

2. Происходящие в последние годы в стране изменения, переход к более открытому обществу, создают в то же время благоприятную обстановку для несанкционированного доступа к информации, в том числе конфиденциальной.

[1] Коваленко А.П., Белов Е.Б. Концепция подготовки кадров в области обеспечения информационной безопасности (проблемы, анализ, подходы) // Научные и методологические проблемы информационной безопасности / под ред. В. П. Шерстюка. М., 2004.

3. Всеобщая компьютеризация основных сфер деятельности привела к появлению широкого спектра нетрадиционных каналов утечки информации и несанкционированного доступа к ней.

Последнее обстоятельство таит в себе реальную угрозу несанкционированного контроля над информационными процессами. Это особо опасно в связи с тем, что программно-техническая база информатизации в России практически целиком основана на продукции зарубежных фирм. В то же время развитие информационных технологий уже в недалеком будущем способно привести к появлению качественно новых информационных форм борьбы, так называемых информационных войн.

Изучение утечек в разрезе каналов, по которым уходит информация, имеет практическое значение. В зависимости от частоты утечек по тому или иному каналу, можно разрабатывать модели угроз (отраслевые, региональные, применительно к конкретным типам данных), осуществлять внедрение средств защиты в компании или в отрасли, определить, каким каналам следует уделить повышенное внимание. По причине всё большего распространения смартфонов, мы полагаем, что этот канал утечек также является одним из важнейших. Однако средства контроля смартфонов, по сути, отсутствуют сегодня на рынке. Очевидно, с этим связана низкая доля утечек, зафиксированных по этому каналу.

С каждым годом ситуация в области защиты информации ухудшается, ежегодно только в РФ компрометируются более 260 млн записей[1]. Внешние атаки с целью хищения данных, платежной информации занимают первое место. В результате воздействия внешнего злоумышленника скомпрометировано 230 млн записей о персональных данных – 87 % от общего объема «утекших» персональных данных.

В настоящий момент мы наблюдаем формирование информационного общества в РФ. Нарастающая информатизация общества с использованием телефонии, радио, телевидения, сети Интернет, а также традиционных и электронных СМИ. Создание глобального информационного пространства, обеспечивающего: эффективное информационное взаимодействие людей; их доступ к мировым информационным ресурсам; удовлетворение их потребностей в

[1] Исследование утечек информации за первое полугодие 2015 года [Электронный ресурс] : аналит. отчет InfoWatch // URL https://www.infowatch.ru/analytics/reports/16340.

информационных продуктах и услугах. Помимо социальной значимости стоит отметить бурное развитие информационной экономики, цифровых рынков, электронных социальных и хозяйствующих сетей.

Но помимо пользы от пользования данными ресурсами, каждый участник несет значительные риски. С ростом осведомленности нарушителей о применении технических средств контроля каналов, растет уровень квалификации нарушителя, который более изощрённо совершает преступления. Это подтверждается увеличением роста утечки информации из неопределенных каналов. Это все влияет на рост числа внешних атак и ущерба от них, по средствам сетевых каналов.

Если в крупных компаниях сетевые каналы имеют наибольшую защиту, то в организации среднего и малого бизнеса не могут позволить использовать дорогостоящие системы защиты. Что подтверждается ростом скомпрометированных записей в средних компаниях.

Таким образом, наиболее целесообразным способом повышения уровня защищенности информации в Российской Федерации, в настоящий момент, является целенаправленная подготовка высококвалифицированных специалистов в специализированных учебных заведениях, а также непрерывный процесс развития общих навыков грамотности, культуры при обращении со служебной и личной информацией (особое место занимают персональные данные).

Не маловажным фактором должна стать пропаганда политики безопасности в обществе, это особенно актуально в условиях отсутствия границ для кибератак. В настоящий момент информационная безопасность становится одной из важнейших составляющих обеспечения как национальной безопасности государств, так и международной информационной безопасности в целом.

1.3. 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]. И сбор, распространение информации о частной жизни лица без его согласия запрещены[2].

До недавнего времени вопрос о частной жизни и персональных данных граждан не стоял так остро, но с развитием современных технологий, увеличения мошенничества, киберпреступлений, а также преступлений, направленных против человека – этот вопрос стал одним из ключевых элементов 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 конвенцию о защите прав и свобод человека, то, государство принимает на себя международное понятие «частной жизни»[3].

Под понятие «частная жизнь» попадает область жизнедеятельности человека, которая имеет отношение к нему, касается только его и не подлежит контролю со стороны государства, если она не носит противоправного характера[4]. 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 возможность доверить свои тайны священнику, врачу, адвокату без опасения их разглашений[5].

Право на обеспечение персональных данных возникает у гражданина с момента рождения и является тайной частной жизни[6]. 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

---

[1] Статья 23 Конституции РФ.

[2] Статья 24 Конституции РФ.

[3] Статья 15 Конституции РФ.

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

[5] Фролова О.С. Частная жизнь в свете Конвенции о защите прав человека и основных свобод // Журнал Российского права. 2008. № 10. С. 119.

[6] Статья 2 Федерального закона «О персональных данных» от 26.07.2006 г. № 152-ФЗ.

параллельно с информатизацией общества. Как следствие, институт защиты ПДн достаточно развит.

Обзоры зарубежной нормативной базы выполняются достаточно редко, и как правило не являются общедоступными. 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)[1], 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;

[1] Конвенция о защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс]. URL: http://base.garant.ru/2559798/1/#block_9999.

– 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[1], 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 нарушения/разглашение персональной информации.

В декабре 1997 г. тот же Европейский парламент и Совет Европейского Союза принимают директиву 97/66/ЕС[2], 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[3] 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 наличие

---

[1] Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных» [Электронный ресурс]. URL: http://32.rkn.gov.ru/personal-data/p2309.

[2] Директива 97/66/ЕС Европейского Парламента и Совета Европейского Союза от 15 декабря 1997 г. «О использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций» [Электронный ресурс]. URL: http://32.rkn.gov.ru/personal-data/p2309.

[3] ISO/IEC 27001:2005 «Системы менеджмента информационной безопасности. Требования» [Электронный ресурс]. URL: https://dominder.com/iso27001.ru.

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[1]. Предусматривается административная и уголовная ответственность за утечку персональной информации и передачу ее третьим лицам.

Действительно, 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 образуют угрозу национальной безопасности государств.

Так, по данным Главного информационного центра МВД России, в 2004 году было совершено 13723 компьютерных правонарушений, что почти в два раза больше по сравнению с 2003 годом – 7053, и их количество неуклонно растет. По словам руководителя Бюро специальных технических мероприятий МВД России А. Мошкова в сфере высоких технологий именно мошенничества являются самыми распространенными преступлениями в IT-среде и их количество растет с каждым годом. Если в 2010 году было возбуждено 736 таких уголовных дел, то за 9 месяцев 2011 года их число уже превысило 1 тысячу, при том, что у этих преступлений весьма высокий уровень латентности.

Не менее тревожные тенденции характеризуют состояние преступности и в странах АТР. В частности, в Японии рекордное количество преступлений, связанных с интернетом и другими компьютерными сетями, зафиксировано за прошедший год. Их количество увеличилось почти на треть и составило около 5 500 преступлений, среди которых большинство связано с присвоением денег в результате аукционных покупок по интернету.

---

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

В соответствии с утвержденной Указом Президента РФ «Стратегией национальной безопасности Российской Федерации до 2020 года» национальной безопасностью является состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства. В свою очередь, под угрозой национальной безопасности следует понимать прямую или косвенную возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию государства, его обороне и безопасности.

Совершение киберпреступлений самым непосредственным образом влияет на состояние защищенности жизненно важных интересов субъектов охраны.

В этой связи необходимо отметить, что в соответствии со ст. 2 Конституции РФ права и свободы человека и гражданина являются высшей ценностью в государстве. К таковым относятся неприкосновенность личности, неприкосновенность жилища и, наконец, тайна (неприкосновенность) частной жизни.

В зависимости от оснований появления, все существующие и имеющие правовое значение тайны можно классифицировать следующим образом:

I. Государственная тайна.

II. Конфиденциальная информация:

1. Личная.
2. Семейная.
3. Профессиональная.
4. Коммерческая.
5. Служебная.

И если во многих сферах государственной деятельности конфликт частных и публичных интересов неизбежен, то в случае совершения преступлений в сфере компьютерной информации, в одинаковой степени страдают и частные интересы, и государственные, и общественные.

Именно поэтому международно-правовое регулирование вопросов борьбы с киберпреступностью отличается разносторонностью и

вариативностью. В этой связи уместно вспомнить следующие нормативные акты международного характера:

– Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 года[1]. Несмотря на то, что Российская Федерация не присоединилась к данной Конвенции, с точки зрения особенностей правового регулирования она представляет определенный интерес, поскольку устанавливает перечень преступлений, которые европейским сообществом отнесены к категории компьютерных. Так, к правонарушениям в сфере компьютерной информации отнесены: противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование устройств, подлог с использованием компьютерных технологий, мошенничество с использованием компьютерных технологий, правонарушения, связанные с детской порнографией, правонарушения, связанные с нарушением авторского права и смежных прав. Как видно из приведенного перечня в отличие от УК РФ понятие компьютерных преступлений в данном акте толкуется расширительно.

– Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем от 28 января 2003 года[2]. Данный акт еще более расширяет сферу совершения компьютерных преступлений, относя к ним: распространение расистских и ксенофобских материалов посредством компьютерных систем, Мотивированную угрозу расизма и ксенофобии, расистское и ксенофобское мотивированное оскорбление, отрицание, чрезвычайную минимизацию, одобрение или оправдание геноцида или преступлений против человечества посредством использования компьютерных систем.

– Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 года[3]. Данный документ по причине того, что Российская Федерация является его участницей представляет для нас повышенный интерес. В целях оптимизации

---

[1] Документ опубликован не был.

[2] Convention Committee on Cybercrime [Электронный ресурс]. URL : http://conventions.coe.int/Treaty/RUS/Treaties/Html/189.htm.

[3] Собрание законодательства РФ. 2009. № 13. Ст. 1460.

борьбы с киберпреступностью стороны договорились о том, что признают в соответствии с национальным законодательством в качестве уголовно-наказуемых следующие деяния, совершенные умышленно:

а) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;

б) создание, использование или распространение вредоносных программ;

в) 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 или тяжкие последствия;

г) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб[1].

– Communication from the Commission to the European Parliament, the Council and the Committee of the Regions of 22 May 2007 «Towards a general policy on the fight against cyber crime»[2].

– Communication from the Commission to the European Parliament, the Council and the Committee of the Regions on Critical Information Infrastructure Protection «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience» of 30 march 2009[3].

Особо следует подчеркнуть, что 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 года в Вене группой экспертов был подготовлен итоговый документ, резюмирующий основные проблемы в сфере борьбы с кибер-

[1] Определение понятий «существенный вред», «тяжкие последствия» и «существенный ущерб» относится к компетенции Сторон.

[2] Сообщение Европейской комиссии «На пути к общей политике по борьбе с киберпреступностью» от 22 мая 2007 г.

[3] Сообщение Европейской комиссии «Защита Европы от крупномасштабных кибератак и сбоев: повышение готовности, безопасности и устойчивости» от 30 марта 2009 г.

преступностью 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, например, 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 году, 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 года 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 приданием 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[1]. 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, кибер-преступники 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 кото-

[1] РИА новости [Электронный ресурс]. URL: http://rian.com.ua/world_news/20140519/349471767.html?utm_source=twitterfeed&utm_meium=twitter.

рой 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[1].

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[2];

– 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

Обзор нормативной базы в США. Вопрос по защите персональных данных в США начал развиваться с конца 60-х годов XX в. Нормативные документы применялись как на федеральном уровне, так и на уровне штатов[3].

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 пра-

[1] China modern [Электронный ресурс]. URL : http://www.chinamodern.ru/?p=13939.

[2] Центр исследования компьютерной преступности [Электронный ресурс]. URL: http://www.chinamodern.ru/?p=13939.

[3] Волчинская Е.К. Защита персональных данных. М. : Галерея, 2001. 236 с.

воохранительных органов[1] 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 носит только рекомендательный характер[2], 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 другие.

В руководстве по защите персональных данных «SP 800-122»[3], 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.

---

[1] The Freedom of Information Act [Электронный ресурс]. URL: http://www.justice.gov /oip/foia_updates /Vol_XVII_4/page2.htm.

[2] Медведев В. О защите и о «защите» персональных данных [Электронный ресурс]. URL: http://polit.ru/article/2013/01/18/data.

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

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, авторизация и идентификация пользователей, маркировка и хранение носителей и другое.

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[1]). 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[2].

---

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

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

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, встроенные 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[1]. Затем в 1977 г. был принят федеральный закон, основной целью которого 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 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

[1] Волчинская Е.К. Защита персональных данных. М. : Галерея, 2001. 236 с.

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[1].

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 частные компании[2]. 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 другие).

Кроме данного закона можно выделить еще так называемое семейство добровольных стандартов BS 7799, которые помогают организациям 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 (финансовую, кадровую, информацию о контрагентах и другую). 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 началась много позднее, чем в странах Европейского союза. Поэтому законодательство по защите персональной информации, развитие прав и свобод граждан началось

[1] Волчинская Е.К. Защита персональных данных. М. : Галерея, 2001. 236 с.

[2] Там же.

намного позже. Этот период можно отнести к 90-ым годам 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 правого режима использования персональных данных и функций их держателей[1].

В Конституциях этих стран гарантирована неприкосновенность частной жизни[2]. Положения, прописанные в Конституциях, совпадают с принципами, провозглашенными Советом Европы. Так, например, 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 Республики 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»[3]. В данном законе персональные данные определяются как первичные статические данные о конкретном респонденте, сбор которых осуществляется при проведении переписи населения.

---

[1] Модельный закон «О персональных данных» [Электронный ресурс]. URL: http://www.russianlaw.net/law/civil_rights/pd/t20.

[2] Конституции стран СНГ [Электронный ресурс]. URL: http://www.new.medialaw.ru/law_CIS_Baltic/texts.

[3] О регистре населения [Электронный ресурс] : закон Республики Беларусь от 21.06.2008 г. № 418-З. URL: http://pravo.by.

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 персональные данные, органичен[1], регулирует, что сбор, обработка, хранение информации о частной жизни лица, осуществляются с согласия физического лица[2]. 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 в Республике Казахстан официально вступил в действие закон «О персональных данных и их защите»[3]. Основной целью, прописанной в статье 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[4], лишения свободы,

---

[1] Статья 17 закона «Об информации, информатизации и защите информации» Республики Беларусь.

[2] Там же, ст. 18.

[3] О персональных данных и их защите [Электронный ресурс] : закон Республики Казахстан. URL: http://online.zakon.kz/Document/?doc_id=31396226.

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

либо лишения права занимать определенные должности или заниматься определенной деятельностью[1].

Также разработаны Правила осуществления собственником и (или) оператором[2], 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 другие.

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»[3], 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 в персональных данных, перечисленных в п. 4. ст. 5 Закона.

Согласно закона 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[4] и уголовная ответственности[1]).

---

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

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

[3] О защите персональных данных [Электронный ресурс] : закон Украины от 01.01.2011 г. № 2297-VI. URL: http://www..medialaw.kiev.ua/ru/laws/laws_local/115.

[4] Ст. 182 Уголовного кодекса Украины.

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 защите физических лиц при автоматизированной обработке персональных данных в 2005 г[2].

Основываясь на ст. 23 и ст. 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].

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 от невозможности выполнить требования ст. 25.3 Закона. В результате он претерпел

---

[1] Кодекс Украины об административных правонарушениях от 07.12.1984 г. № 8073-X [Электронный ресурс]. URL: http://www.nibu.factor.ua/info/Zak_basa/Kodeksy/KUoAP.

[2] О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных : федер. закон от 19 дек. 2005 г. № 160-ФЗ // Рос. газ. 2005. 22 дек. (№ 3957).

[3] Ст. 2 федерального закона «О персональных данных» № 152-ФЗ.

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 № 55/86/20 «О утверждении порядка проведения классификации информационных систем персональных данных» (в настоящее время документ утратил свою силу с 11 марта 2014 года на основании совместного приказа ФСТЭК России, ФСБ России и Минкомсвязи России от 31 декабря 2013 года № 151/786/461).

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработанная ФСТЭК России[1].

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработанных ФСТЭК России[2].

Все эти документы были разработаны с целью помочь операторам организовать защиту 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 от № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»[3].

---

[1] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15 февраля 2008 г. // СПС «Консультант плюс».

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

[3] Собрание законодательства РФ. 2009. № 21. Ст. 2573.

2012 год – Постановление Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[1].

2013 год – Приказ № 21 ФСТЭК России «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»[2].

Замечу, что в настоящее время, в Государственной Думе рассматриваются несколько законопроектов, касающихся увеличения штрафов за невыполнение требований по защите ПДн, а также внесения изменений в ст. 10 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»[3], 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).

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 безопасно-

---

[1] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства от 1 нояб. 2012 г. № 1119 // Собрание законодательства РФ. 2012. № 45. Ст. 6257.

[2] 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 // Рос. газ. 2013. № 107.

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

сти, 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 развиться достаточно давно, к настоящему времени проработана нормативная база: разработаны не только законы, в которых прописана 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[1].

[1] О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3451.

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	Кол-во утечек конф. инфор., в т.ч. ПДн за 2012[1]	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	Административные (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	

[1] Отчет аналитического центра InfoWatch [Электронный ресурс]. URL: http://www.infowatch.ru/analytics/panels/2580.

1.4. 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 связана 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 выполнят 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 к требованиям законодательства;

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

– несоизмеримость штрафов и затраты 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[1] (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, вероис-

[1] Пункт 1 ст. 3 Федерального закона «О персональных данных» от 27.06.2006 г. № 152-ФЗ.

поведание, 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 другие[1].

Трудовой кодекс РФ[2] под персональными данными работника подразумевает информацию, относящуюся к работникам, выполняющим обязанности, прописанные трудовым договором. К таким данным относят: табельный номер, дата трудового договора, документы воинского учета, фотографии, образование, квалификация, занимаемая должность, наличие детей, приказы, заявления, сведения о здоровье, оклад и другие.

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 прочие; либо физические носители: съемные, жесткие диски)[3].

Итак, определив понятие «персональные данных» и кому они могут принадлежать, можно начинать построение системы защиты персональных данных. Опираясь на постановление[4], операторы ПДн должны определить актуальные угрозы безопасности, определить вы-

---

[1] Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования : федер. закон от 1 апр. 1996 г. Ст. 6 [Электронный ресурс] // СПС «Контур-Норматив».

[2] Глава 14 Трудового Кодекса РФ от 30 дек. 2001 г.

[3] Просвирин Ю.Г. Защита персональных данных // Вестник БГУ. 2008. № 1. С. 174–188.

[4] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства от 1 нояб. 2012 г. № 1119 // Собрание законодательства РФ. 2012. № 45. Ст. 6257.

бор 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[1].

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, становиться 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 части 3 статьи 6 закона содержится норма включать в поручение оператора требование обеспечивать безопасность персональных данных при их обработке, а также ука-

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

зать 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 аутсерсерам, выполняющим данные услуги по договору?

Еще один интересный факт, вытекает из постановления[1] пункт 13. В этом пункте обозначено требование наличия защиты контролируемой зоны при обработке ПДн (т.е. зоны, в которую запрещен доступ посторонних). Например, выносная точка продаж sim-карт в торговом центре: при продаже карты клиент указывает свои персональные данные (фамилия, имя, отчество, паспортные данные и другие) 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 запрещен или выносная точка продажи должна быть оборудована сигнализацией, сейфом и другими устройствами, а также должна быть огорожена[2].

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 существует 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 – это оставить все как есть и ждать проверки со стороны регулятора, выплатив по их результатам штрафы.

---

[1] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства от 1 нояб. 2012 г. № 1119 // Собрание законодательства РФ. 2012. №45. Ст.6257.

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

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.

1.5. Теоретические основы защиты персональных данных

В рамках рассматриваемого вопроса 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 поднимается вопрос выбора средств защиты персональных данных, обрабатываемых в информационных системах, на основе оценки их защищенности[1]. 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 то, 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, неправильный выбор средств защиты, который приведет к наложению штрафа Регулятором и непредусмотренным затратами по переоснащению средствами защиты.

---

[1] Голембиовская О.М. Автоматизация выбора средств защиты персональных данных на основе анализа их защищенности : дис. канд. техн. наук : 05.13.19. Брянск, 2013. 167 с.

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 разработана методика оценки защищенности персональных данных, позволяющая в соответствии 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. В работе *Е. С. Волокитиной* поднимается вопрос об обезличивании персональных данных с последующей невозможность по остаточным данным его идентифицировать[1]. 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, повышения 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[2], И.Ю. Кучина[3].

---

[1] Волокитина Е.С. Метод и алгоритмы гарантированного обезличивания и реидентификации субъекта персональных данных в автоматизированных информационных системах : автореф. дис. … канд. техн. наук : 05.13.19. Санкт-Петербург, 2013. 24 с.

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

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

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.

2. ОЦЕНКА ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. 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.

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 приведению защиты персональных данных[1]. 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 другие);

– 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 возникнут (например, угроза загрузки с внешних носителей информации; выявление уязвимостей, связанных с ошибками в конфигурации программного

[1] 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 // Рос. газ. 2013. № 107.

обеспечения информационной системы; угроза несанкционированного доступа и другие).

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 затрать денежные средства на внедрения/установку аппаратных средств защиты ПДн (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 прочие).

На рис. 13 представлена схема приведения ИСПДн в соответствие требованиям законодательства.

Выполнение каждого этапа связано с трудоемким процессом: изучением законодательства, подготовкой организационно-распорядительной документации, обучение сотрудников, связанных с обработкой персональных данных, внедрение технических средств защиты, настройки программно-аппаратных средств защиты.

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 т.ч. 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.

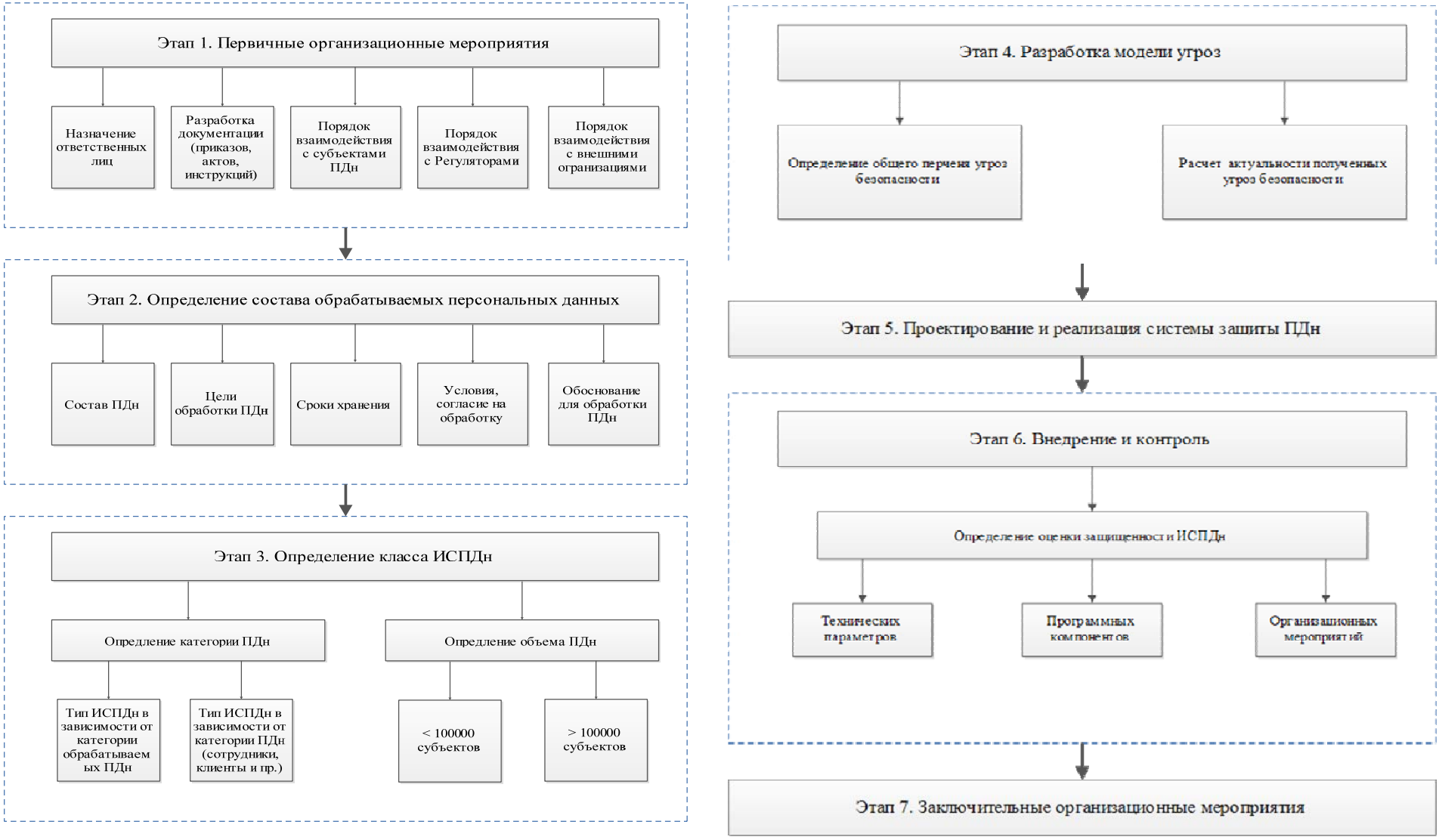

Рис. 13. Схема приведения ИСПДн

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, оказание услуг, продажа товаров и другие);

– сроки хранения персональных данных (для различных целей обработки ПДн устанавливаются различные сроки хранения и 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[1]);

– 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.

Одним из самых трудоемких этапов – это «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

[1] Пункт 2 ст. 5 Федерального закона «О персональных данных» от 27.06.2006 г. № 152-ФЗ.

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, политические взгляды, философские убеждения);

– ИСПДн-О – информационная система, 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 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 100000).

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 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, пре-

доставление, распространение персональных данных, а также иные неправомерные действия[1].

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» типа актуальны для информационной системы, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном 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 моделирования 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[2]:

— 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.

---

[1] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства от 1 нояб. 2012 г. № 1119 // Собрание законодательства РФ. 2012. №45. Ст. 6257.

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

При обработке персональных данных в информационных системах выделяются четыре уровня защищенности персональных данных[1].

— 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-го типа (более подробное описание угроз, описано в табл. 2);

— 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 типа 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, обеспечивающий 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.

[1] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства от 1 нояб. 2012 г. № 1119 // Собрание законодательства РФ. 2012. №45. Ст. 6257.

Таблица 2

Соответствие типа ИСПДн и актуальных угроз

Тип ИСПДн	Сотрудники оператора	Кол-во субъектов	Тип актуальных угроз		
			1	2	3
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)[1], оператор ПДн может юридически доказать минимизацию используемых средств защиты, и как следствие, затрат на их приобретение[2]. 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[3].

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

---

[1] 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 // Рос. газ. 2013. № 107.

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

[3] 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 // Рос. газ. 2013. № 107.

1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа. Эти меры должны обеспечивать присвоение 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 систе-

ме, 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 и (или) воздействие на них, 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.

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, защиту технических средств от

внешних воздействий, а также защиту персональных данных, представленных 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.

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 разработка методических материалов, в которых описываются действия сотрудников по регистрации утечек персональных данных и ликвидации их последствий.

Таблица 3

Соответствие типов угроз и необходимым требованиям

УЗ ПДн	Обоснование о необходимости обеспечения УЗ	Организационно-технические меры	Требования по использованию сертифицированных средств защиты
4-ый 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 100000 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
3-ий уровень	а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников	Выполнение требований для 4-го уровня защищенности, а также назначение должностного лица	а) средства вычислительной техники не ниже 5-го класса; б) системы обнаружения вторжений и

УЗ ПДн	Обоснование о необходимости обеспечения УЗ	Организационно-технические меры	Требования по использованию сертифицированных средств защиты
	оператора или общедоступные персональные данные менее чем 100000 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 100000 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 100000 субъектов персональных данных, не являющихся сотрудниками оператора; г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные; д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора	(работник), ответственного за обеспечение безопасности персональных данных в информационной системе	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 информационно-телекоммуникационными сетями международного информационного обмена
2-ой 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 100000 субъ-	Необходимо выполнение требований для 3-ого, 4-ого уровней защищенности, а также организовать доступ к содержанию электронного журнала сообщений был возможен исключительно для	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 клас-

УЗ ПДн	Обоснование о необходимости обеспечения УЗ	Организационно-технические меры	Требования по использованию сертифицированных средств защиты
	ектов 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 100000 субъектов ПДн, не являющихся сотрудниками оператора; д) для ИС актуальны угрозы 2-го типа и ИС обрабатывает иные категории персональных данных более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора; е) для ИС актуальны угрозы 3-го типа и ИС обрабатывает специальные категории персональных данных более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора	должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей	са 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
1-ый 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 100000 субъектов персональных данных, не являющихся сотрудниками оператора	Необходимо выполнение требований для 2-ого, 3-ого, 4-ого 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	

2.2. 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 требований 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, план работ, журналы 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[1].

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;

---

[1] Сачков Д.И., Быкова В.Н. Использование информационных систем для защиты персональных данных // Известия Иркутской государственной экономической академии. 2014. № 3. С. 203–210.

– 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).

Сравнительный анализ систем защиты информации от НСД выполнен на основе.

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.

В табл. 4 приведен сравнительный анализ СЗИ по некоторым мерам безопасности ПДн, описанных в приказе № 21 ФСТЭК России. В анализируемом программном обеспечении, предназначенном для защиты информации от несанкционированного доступа, реализовано большинство мер, описанных в приказе ФСТЭК России[1].

[1] 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 // Рос. газ. 2013. № 107.

Таблица 4

Сравнительный анализ СЗИ от НСД

№ п/п	Меры по обеспечению безопасности ПДн	Secret Net 7.0[1]	Dallas Lock 8.0[2]
1	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 пользователей с использованием аппаратной поддержки ПАК «Соболь» и Secret Net Card	Обеспечивает идентификацию и аутентификацию локальных, доменных, терминальных и удаленных пользователей на этапе входа в операционную систему. Осуществляет работу с различными типами аппаратных идентификаторов
2	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 прочие)

[1] Официальный сайт «ООО «Код безопасности» [Электронный ресурс]. URL: http://www.securitycode.ru/products/secret_net/scope_auto_edition.

[2] Официальный сайт «ООО «Кондидент» [Электронный ресурс]. URL: http://www.dallaslock.ru/sub-doc.html.

№ п/п	Меры по обеспечению безопасности ПДн	Secret Net 7.0[1]	Dallas Lock 8.0[2]
3	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
4	Защита машинных носителей информации	Поддерживается контроль следующих устройств: Основные параметры рабочей станции (процессор, память). Диски (физические, оптические, сменные и виртуальные). Сетевые интерфейсы (Ethernet, 1394 FireWire, Bluetooth, IrDA, Wi-Fi). USB-устройства	Предотвращает утечки информации с использованием сменных накопителей (таких как CD-диск, USB-Flash-диск, внешний жесткий диск и прочие) система позволяет разграничивать доступ, как к отдельным типам накопителей, так и к конкретным экземплярам
5	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)
8	Выявление инцидентов и реагирование на них	Реализована возможность обнаружения, идентификации и регистрации инцидентов, с последующим информированием ответственных лиц	
9	Техническая поддержка	Предоставляется	Предоставляется
10	Язык программы	Русский	Русский
11	Сертификат ФСТЭК	Сертификат ФСТЭК России № 2707 от 07.09.2012	Сертификат ФСТЭК России № 2945 от 16.08.2013 г
12	Стоимость на 1 раб. Место	от 6750 р.	от 6000

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 приведен в табл. 5.

Таблица 5

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 рабочего места	от 5750 руб	От 5500 руб

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[1] 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 систем) 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

[1] Шабанов И. Тест антивирусов на лечение активного заражения (октябрь 2012) [Электронный ресурс]. URL: http://www.anti-malware.ru/malware_ treatment_test_2012.

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.

Таблица 6

Сравнительные характеристики межсетевых экранов

Сравнительные характеристики	VipNet Personal Firewall	АПКШ «Континент»	ИКС
Наличие сертификата ФСТЭК	+	+	+
Операционная система	Windows	Windows, Linux	Windows
Уровень защищенности:			
УЗ1	—	+	—
УЗ2	+	+	
УЗ3	+	+	+
УЗ4	+	+	+
Класс ИСПДн:	К2	К1	К2
Класс МЭ	МЭ 4	МЭ 2	МЭ 4
Стоимость	Предоставляется по запросу		14000 р. до 10 станций

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, другие факторов).

Группа «DLP-решения». DLP-системы – это программные продукты, защищающие организации от утечек конфиденциальной информации, основная задача которых создание защищенный цифровой «периметр», анализируя исходящую и входящую документацию (электронную почту, распечатка документов, передача через Bluetooth, копирование информации на цифровой носитель).

Перехват сообщений основывается на построении «правил безопасности», которые базируется 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 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, позволяющие блокировать передаваемую информацию;

б) с пассивным контролем действий пользователя, позволяющие 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 другие) уже воспользовались возможностями DLP – решений. В результате использования данных решений обеспечили надежную защиту своих интересов и конфиденциальной информации своих клиентов.

Группа «Программа для проведение 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

Наименование DLP-решения	Falcongaze SecureTower[1]	InfoWatch Traffic Monitor[2]	Zecurion DLP[3]
Разработчик	Falcongaze, РФ, г. Москва	ЗАО «ИнфоВотч»	ООО «Зекурион Рус»
Наличие сертификата/ Класс ИСПДн	ИСПДн до 2 класса включительно	ИСПДн до 1 класса включительно	ИСПДн до 1класса 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, «циф-

[1] Возможности SecureTower [Электронный ресурс]. URL: http://falcongaze.ru/products/secure-tower/opportunities.html.

[2] Возможности InfoWatch Traffic Monitor [Электронный ресурс]. URL: http://www.infowatch.ru/products/traffic_monitor_enterprise.

[3] Возможности [Электронный ресурс]. URL: http://www.zecurion.ru/products/zgate.

Наименование DLP-решения	Falcongaze SecureTower[1]	InfoWatch Traffic Monitor[2]	Zecurion DLP[3]
			ровых отпечатков», 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 отсутствие 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 требованиям законодательства, предупреждения возникновения инцидентов информационной безопасности, повышения культуры информационной безопасности, оптимизацией расходов на обеспечение информационной безопасности.

Таблица 8

Критерии сравнения	Программный продукт							
	RA2	vsRisk	Risk Watch	Callio Secura	CRAMM	COBRA	Method Ware	Риск Менеджер
Разработчик	AEXIS Security Consultants	IT Governance Ltd	RiskWatch International	Callio Technologies	(CCTA - Central Computer and Tele-communica-tions Agency	Corporate Risk Associates Ltd	MethodWare	Институт системного анализа РАН
Сайт	–	http://www.itgovernance.co.uk/	http://riskwatch.com/	–	–	http://www.corporateriskassociates.com/	http://methodware.biz/	http://www.sriskss.ru/
Интерфейс	Англ.	Англ.	Англ.	Англ.	Англ.	Англ.	Англ.	Русский
Простота использо-вания	+	+	+	+	Требуются высокая квалификация специалиста в области ИБ			
Количественная оценка	+	-	+	+	+	+	–	+
Качественная оценка	+	+	–	–	+	–	+	–
Тех. поддержка	–	+	+	–	–	–	–	
Поддерживаемые стандарты ИБ	ISO 17799/ IEC 27001	ISO 27001 ISO 27005	ISO 17799 NIST SP 800-30	BS 7799/ ISO17799	BS 7799 ISO 17799	BS7799 ISO 17799	AS/NZS 4360:1999 ISO 17799 BS7799	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	–	–	–	–	+	+	+	+

2.3. Выявление уровня выполнения требований законодательства ПДн на территории Иркутской области

Выявление уровня выполнения требований законодательства ПДн на территории Иркутской области проведено анкетирование среди организаций, относящихся к среднему и малому бизнесу, государственному сектору, а также индивидуальных предпринимателей. Основной задачей данного анкетирования узнать:

– знакомы ли руководители и сотрудники с законом «О персональных данных»;

– проведены ли организационные мероприятия (назначены ответственные лица, подготовлены инструкции, приказы и другие необходимые документы, проведено обучение и инструктаж персонала);

– проведена ли классификация ИСПДн;

– используемые категории персональных данных;

– внедрены ли технические средства защиты.

Всего в анкетировании приняли участие 89 организаций, находящихся на территории Иркутской области (г. Иркутск, г. Ангарск, г. Усолье-Сибирское, пос. Мегет).

Рис. 14. Результаты анкетирования

В результате анкетирования выявлено, что 61 % от общего числа опрошенных руководителей и специалистов организаций знают о существовании данного закона и его требований, 31 % – что-то слышали, но в чем суть даже не пытались разобраться, 8 % – вообще не знают, что персональные данные необходимо защищать (см. рис. 14). В табл. 9 представлены результаты опроса.

Таблица 9

Результаты опроса

Организация / Вопросы	Гос. учреждения	Ком. организации	ИП
Всего участие в анкетировании приняли	37	40	12
1. Назначен ли у Вас ответственный за обработку ПДн?	37 (100 %)	25 (62,5 %)	5 (41,7)
2. Объем обрабатываемых ПДн			
до 1000	16	26	7
до 100000	18	4	
Свыше 100000	3	-	
Не знаю		10	5
3. Выполненные мероприятия по ПДн			
Обследование ИСПДн	23	2	
Закупка и установка СЗИ	25	14	1
Аттестация ИСПДн	19	0	
Сопровождение ТСО	9	5	
Переаттестация ИСПДн	4	0	
Другое	12	2	
Ни какие мероприятия не выполнялись	0	24	11
4. Режим обработки ПДн			
Однопользовательский	5	6	7
Многопользовательский	30	33	3
Затрудняюсь ответить	2	1	2
5. Есть ли разграничение прав доступа к ИСПДн			
Да	33	28	3
Нет	1	10	7
Затрудняюсь ответить	3	2	2
6. Подключен ли интернет к ПК, на которых ведется обработка ПДн?			
Да	37 (100 %)	40 (100 %)	12 (100 %)
Нет			
7. Какие используете средства защиты ИСПДн?			

Организация / Вопросы	Гос. учреждения	Ком. организации	ИП
Антивирусная защита	37	40	9
Межсетевой экран	21	12	
Средства от НСД	21	5	
Средства контроля над ресурсами Интернет	19	2	
Шифрование	6		
Усиленная аутентификация	2		
Средства от утечки по тех. каналам	7		
Затрудняюсь ответить			3
8. Имеется охранно-пожарная сигнализация в кабинетах, в которых обрабатываются ПДн?			
Да	37	32	6
Нет		8	6
9. Проводилось ли у Вас обучение персонала по защите ПДн?			
Да	31	1	1
Нет	7	39	10
Затрудняюсь ответить			1
10. Проводилась ли у Вас проверка РОСКОМНАДЗОРа?			
Да	6		
Нет	27	40	12
Затрудняюсь ответить	4		

Исходя из полученных данных, можно сделать следующий вывод, что учреждения, относящиеся к государственному сектору (больницы, школы, органы власти и прочие) в большей степени выполнили требования законодательства по защите персональных данных: провели обследование информационной системы, установили и настроили средства защиты информации от несанкционированного доступа, провели аттестацию информационной системы, а самое главное, провели обучение персонала, ответственного за обработку персональных данных.

Организации, относящиеся к малому и среднему бизнесу, а также индивидуальные предприниматели проигнорировали требования законодательства и в большей части не выполнили мероприятия по защите, начиная от организационных (назначение ответственных лиц) и заканчивая настройкой технических мер (настройка межсетевых экранов и прочее).

Самое главное в этих организациях не проведено обучение сотрудников, занимающихся обработкой персональных данных. Не проведены инструктажа, что делать в случае утечки данных, как реагировать и какие возможны последствия.

В проведенном анкетировании стояла задача узнать какие категории персональных данных обрабатываются в организациях. На рис. 15 представлены основные категории ПДн, которые обрабатывают организации, принявшие участие в опросе.

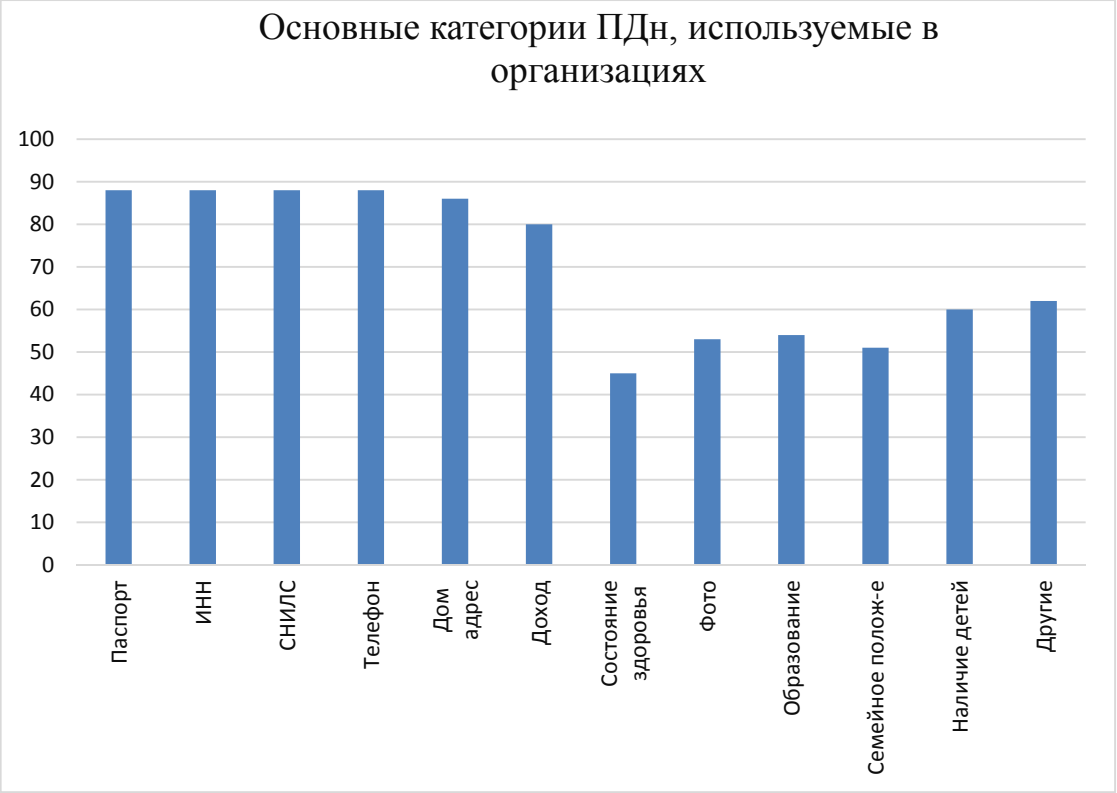

Рис. 15. Основные категории ПДн

Из анализа видно, что организации для своей работы используют данные, которые можно отнести к следующим информационным системам:

– ИСПДн – Б – по наличию фотографий;

– ИСПДн-О – по наличию общедоступных категорий ПДн;

– ИСПДн-С – по наличию специальных категорий ПДн (например, состояние здоровья);

– ИСПДн-И – по наличию других категорий ПДн (например, судимости, наличие автомобиля, заграничного паспорта и других).

Таким образом, анализируя полученные результаты, можно сделать следующие выводы, что организации, оперируя персональными данными, при утечки которых, у субъекта ПДн могут возникнут различные последствия, практически не решили ни технических, ни организационных задач. Не обеспечивают защиту должным образом, ограничиваются только установкой антивирусных программ.

2.4. Обзор существующих методик оценки защищенности ИСПДн

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

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

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

– Проанализированы 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 с это прежде всего тем, что это облачные приложения и пользователю нет необходимости устанавливать обновления у себя на компьютере. Разработ-

чики в кратчайшие сроки изменять 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:

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

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

– «непрозрачность» механизма отнесения к типу ИСПДн;

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

В табл. 10 представлена сравнительная характеристика автоматизированных систем, позволяющих провести оценку защищенности информационных систем.

Таблица 10

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	–	+	+	–

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
Определение уровня защищенности	–	+	+	+
Определение контролируемой зоны	–	–	+	+
Определение угроз безопасности	–	+	+	+
Разработка ТЗ на проектирование системы защиты	–	–	+	+
Оценка эффективности принимаемых мер	–	–	+	+
Техническая поддержка	+	+	+	–
Соответствие законодательству	+	?	+	–
Стоимость на 1 год	От 6000 до 20000 р.	От 7800 до 49000 р.	От 9900 до 89900 р.	Не массовый продукт

Из сравнительных характеристик программных видно, что некоторые автоматизированные системы уже не соответствуют требованиям текущего законодательства, например, «АС ИСПДн» – разрабатывалась по старые требования и не соответствуют[1], 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 10).

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

[1] Голембиовская О.М. Автоматизация выбора средств защиты персональных данных на основе анализа их защищенности : дис. … канд. техн. наук : 05.13.19. Брянск, 2013. 167 с.

В работе «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[1]. Существенным недостатком данной работы служит то, что автоматизированная система разрабатывалась под старые требования законодательства и нуждается в модернизации.

[1] Голембиовская О.М. Автоматизация выбора средств защиты персональных данных на основе анализа их защищенности : дис. … канд. техн. наук : 05.13.19. Брянск, 2013. 167 с.

3. МЕТОДИКА ОЦЕНКИ ЗАЩИЩЕННОСТИ ПДН

3.1. Алгоритм определение класса ИСПДн

Для определения класса информационной системы, необходимо выполнение двух требований: определить категории ПДн и количество субъектов ПДн. Процедура категорирования персональных данных является трудно формализованной задачей, так как в нормативных документах отсутствует точный перечень персональных данных. Исходя из имеющихся нормативно-правовых документов, я разбила персональные данные на 4 категории: О – общедоступные данные; И – иные категории персональных данных; Б – биометрические персональные данные; С – специальные персональные данные. Результат категорирования представлен в табл. 11.

Таблица 11

Категорирование персональных данных

№	Персональные данные	Категория
a	Фамилия Имя Отчество	О
b	Паспортные данные	И
c	Дата и место рождения	И
d	ИНН, СНИЛС	И
e	Телефоны (домашний, мобильный)	О
f	Адрес (фактический, по прописке)	И
g	Электронная почта	О
h	Военный билет, паспорт моряка, временное удостоверение	И
j	№ водительского удостоверения	И
k	Сведения о доходе, № банковских карт, финансовое состояние	И
l	Семейное положение, наличие детей	И
m	Фотография	Б
n	Состояние здоровья/сведения об инвалидности	С
o	Информация о национальности, расовой принадлежности	С
p	Информация о политических взглядах	С
q	Данные о религиозных убеждениях	С
r	Данные об интимной жизни	С
s	Другие данные: образование, повышение квалификации, курсы, льготы, прочие	И

В проанализированных работах[1], методиках на предмет категорирования персональных данных не существует единой точки зрения на однозначное определение категории.

Для идентификации субъекта необходимо определить соответствующие признаки. Для этого разобьем имеющие персональные данные на несколько групп:

A – общедоступные данные, которые включают в себя множество A = {a, e, o}. По данным признакам идентифицировать однозначно невозможно.

B – иные категории персональных данных, по которым можно однозначно идентифицировать субъекта персональных данных, содержит множество B = {b, d, h, j}.

C – биометрические персональные данные, по котором можно опознать человека содержатся в множестве C = {m}.

D – специальные категории персональных данных (информацию о расовой, национальной принадлежности, политических взглядов, религиозных убеждений, состоянии здоровья, интимной жизни), но не позволяющих однозначно идентифицировать гражданина. Содержится в множестве D = {n, o, p, q, r, s}.

E – иные категории персональных данных, но не позволяющих однозначно идентифицировать гражданина. Содержится в множестве E = {c, k, l, s}.

Для определения категории персональных данных их необходимо определить в соответствующие множества. Результат процесса представлен на рис. 16.

[1] Голеомбиовская О.М., Терехов М.В. Разработка автоматизированной системы аудита и построения модели объекта защиты с использованием технологии 3D-прототипирования // Региональные проблемы защиты персональных данных : материалы 2-й регион. науч.-практ. конф. Брянск : БГТУ, 2010. С. 47–49.

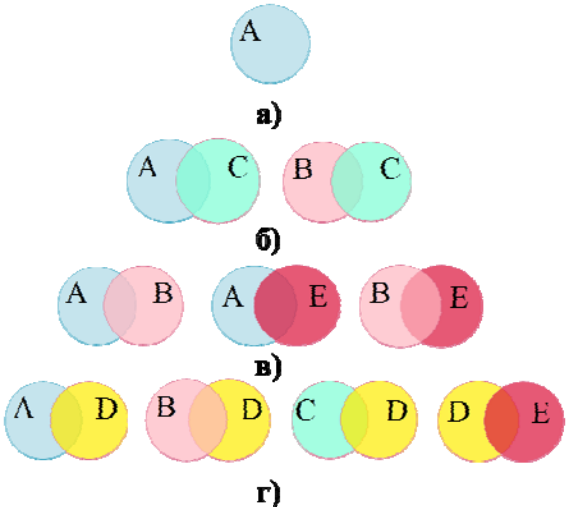

Рис. 16. Определение типа ИСПДн

Таким образом, определилось несколько классов ИСПДн, в которые попадают различные категории персональных данных:

– ИСПДн-О – это множество A (см. рис. 16*а*);

– ИСПДн-Б – это множества: A ∪ C и C ∪ B (см. рис. 16*б*);

– ИСПДН-И – это множества: A ∪ B; A ∪ E; E ∪ B (см. рис. 16*в*);

– ИСПДн-С – это множества: A ∪ D, D ∪ B, C ∪ D; E ∪ D (см. рис. 16*г*).

На основе данного категорирования разработан алгоритм, позволяющий сэкономить время оператора ПДн при определении класса ИСПДн (см. рис. 17). Данный алгоритм также позволяет определить уровень защищенности информационной системы (УЗ4 – УЗ1) и позволит в дальнейшем быстро перейти на следующий этап, который определяет тип угроз и уязвимостей информационной системы.

3.2. Оценка уровня защищенности

Методика оценки уровня защищенности персональных данных в основном рассчитана на организации малого и среднего бизнеса, а также индивидуальных предпринимателей. Предназначена для того, чтобы руководители и специалисты компании могли без дополнительных материальных и временных затрат выполнить требования законодательства по защите персональных данных.

На рис. 18 представлена сетевая модель процесса оценки защищенности ИСПДн. На основе этой модели разрабатывалась методика оценки уровня защищенности персональных данных.

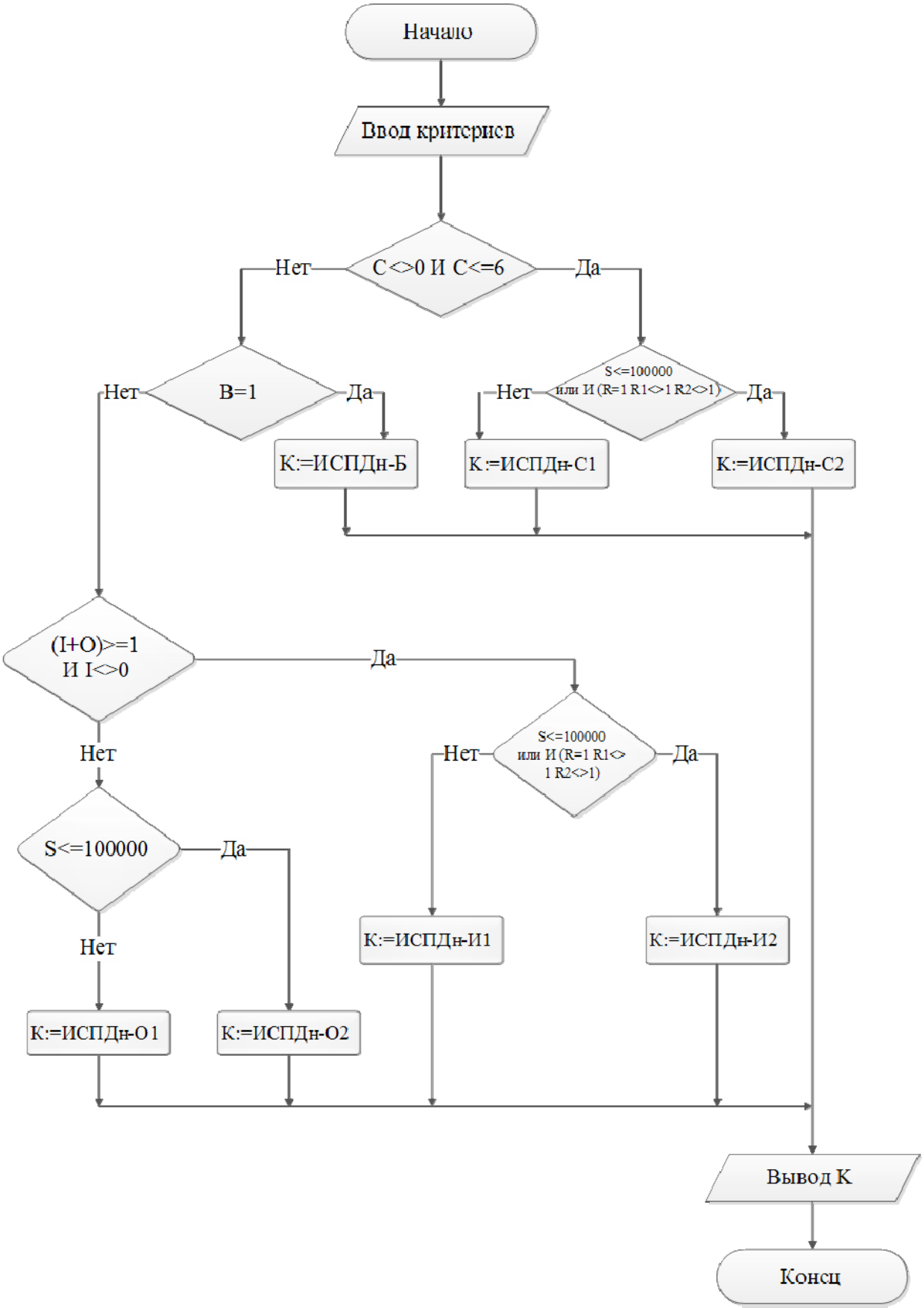

Рис. 17. Алгоритм определения типа ИСПДн

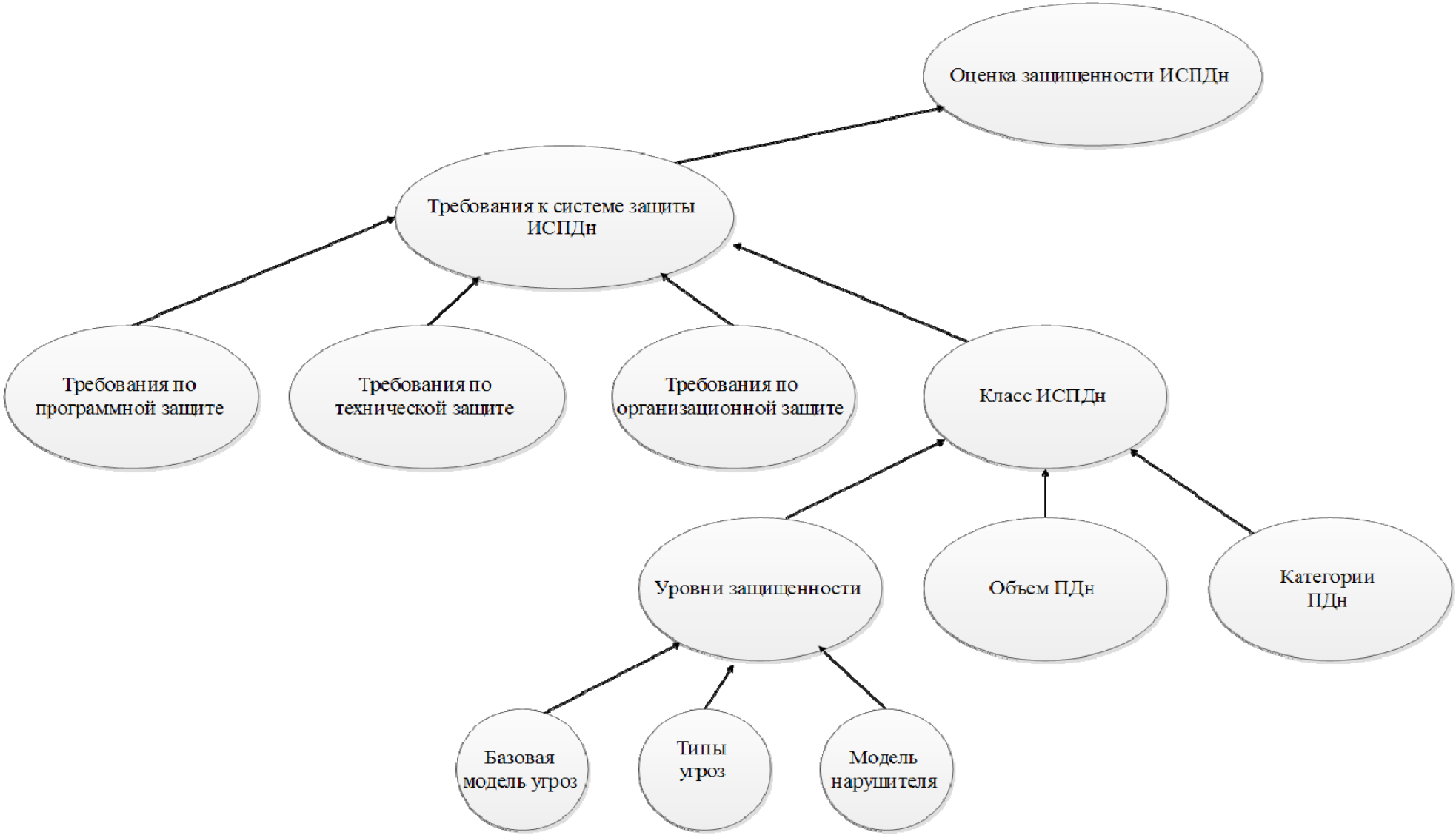

Рис. 18. Сетевая модель процесса оценки защищенности ИСПДн

Методика построена на процессе интервьюирования различных специалистов (руководителей, бухгалтеров, системных администраторов, других специалистов) и состоит из опросного листа, который, в свою очередь, разбит на группы, позволяющих оценить уровень защищенности персональных данных:

– требования по организационной защите;

– требования по технической защите (утечки по техническим каналам; угрозы несанкционированного доступа);

– требования по программной защите;

– класс ИСПДн (категории ПДн, объем ПДн);

– уровень защищенности (модель нарушителя; типы угроз; базовые модели угроз).

Группа «1. Требования по организационной защите», в которой основной акцент сделан на выполнение требований по организационной защите в соответствии с требованиями ст. 18, 19 Закона «О персональных данных». В табл. 12 представлен перечень вопросов, относящихся к данной группе.

Таблица 12

Опросный лист «Требования по организационной защите»

№ критерия	Описание критерия	Значение критерия
1.1.	Назначен ли ответственный сотрудник за организацию обработки персональных данных в компании?	
1.2.	Назначен ли сотрудник за обеспечение безопасности персональных данных?	
1.3.	Имеется ли в компании системный администратор?	
1.4.	Есть ли у Вас приказ о назначении ответственных лиц?	
1.5.	Есть ли у Вас приказ об обработке персональных данных?	
1.6.	Проводилось ли у Вас обучение по защите персональных данных?	
1.7.	Есть ли у Вас приказ о допуске работников, допущенных к обработке персональных данных?	
1.8.	Есть ли у Вас положение о допуске сотрудников и посетителей в рабочее и нерабочее время?	
1.9.	Внесены ли изменения в должностные инструкции?	
1.10.	Разработаны ли инструкции по устранению последствий утечки информации?	
1.11.	Разработаны ли регламенты по передачи ПДн третьим лицам?	

Значение уровня защищенности для каждого критерия вычисляется по формуле:

$$Y = \frac{Y1+Y2}{20}, \quad (1)$$

где Y1 – степень исходной защищенности ИСПДн:

$$Y1=\begin{cases} 0 - \text{ высокий уровень защищенности} \\ 10 - \text{низкий уровень защищенности} \end{cases};$$

Y2 – степень критичности требований законодательства:

$$Y2=\begin{cases} 0 - \text{ критичное требование} \\ 10 - \text{некритичное требование} \end{cases}$$

Далее вычисляется итоговый уровень защищенности для данной группы:

а) ИСПДн имеет «Высокий» уровень исходной защищенности, если не менее 70 % критериев соответствуют уровню «Высокий»;

б) ИСПДн имеет «Средний» уровень исходной защищенности, если не менее 50 % критериев соответствуют уровню «Высокий»;

в) ИСПДн имеет «Низкий» уровень исходной защищенности, если не выполняются пункты *а* и *б*.

Группа «2. Оценка защищенности ИСПДн от угрозы утечки акустической информации». Данная группа предназначена для определения уровня защищенности информационной системы от утечек по акустическому каналу. В табл. 13 представлен опросный лист.

Таблица 13

Опросный лист «Выполнение требований по технической защите от утечек по акустическому каналу»

№ критерия	Описание критерия	Значение критерия
2.1.	Какие средства защиты акустического сигнала вы используете:	
	Не используются	
	средства защиты акустического канала информации, обеспечивающие зашумление помещения	
	средства защиты акустического канала информации, обеспечивающие глушение акустических сигналов	
	средства защиты акустического канала информации, обеспечивающие звукопоглощение акустической волны	
2.2.	Какие двери у Вас установлены	

№ критерия	Описание критерия	Значение критерия
	Не установлены (или стеклянные перегородки)	
	Обычные деревянные (до 32 Дб)	
	Обычные деревянные с уплотняющими прокладками (до 36 Дб)	
	Металлическая дверь (до 32 Дб)	
	Металлическая дверь с обивкой или уплотняющими прокладками (До 36Дб)	
	Имеется тамбур перед дверью	
	Двойная дверь или с повышенной звукоизоляцией	
2.3.	Какой степени звукоизоляции установлены окна:	
	Одинарное остекление или двойное остекление (деревянные окна)	
	Пластиковые окна 3 класса	
	Пластиковые окна 4 класса	
	Пластиковые окна 5 класса	
	Пластиковые окна 6 класса	
2.4.	Какие виды жалюзи установлены на окнах	
	Не установлены	
	Тканевые (или плотные шторы)	
	Пластиковые	
	Алюминиевые	
2.5.	Разрешено ли в Вашем учреждении использование личных мобильных телефонов?	
	Нет	
	Да	

Значение уровня защищенности для каждого критерия вычисляется по формуле (1),

где Y1 –степень исходной защищенности ИСПДн:

$$Y1=\begin{cases} 0 - \text{высокий уровень защищенности} \\ 10 - \text{низкий уровень защищенности} \end{cases}$$

Y2 –вероятность возникновения угрозы:

$$Y2=\begin{cases} 0 - \text{реализация угрозы низкая} \\ 5 - \text{реализация угрозы средняя} \\ 10 - \text{реализация угрозы высокая} \end{cases}$$

Далее вычисляется итоговый уровень защищенности для данной группы:

а) ИСПДн имеет «Высокий» уровень исходной защищенности, если не менее 70 % критериев соответствуют уровню «Высокий»;

б) ИСПДн имеет «Средний» уровень исходной защищенности, если не менее 50 % критериев соответствуют сумме уровней («Высокий» + «Средний»);

в) ИСПДн имеет «Низкий» уровень исходной защищенности, если не выполняются пункты *а* и *б*.

Группа «3. Оценка защищенности ИСПДн от угрозы утечки визуальной информации». Данная группа предназначена для определения уровня защищенности информационной системы от утечек визуальной информации. В табл. 14 представлен опросный лист.

Таблица 14

Опросный лист «Выполнение требований по технической защите от утечек визуальной информации»

№ критерия	Описание критерия	Значение критерия
3.1.	В Вашей организации используется пропускной режим?	
	Не используется	
	Пропускной пункт с охраной	
	Контроль доступа	
3.2.	Посетители могут видеть визуальную информацию от монитора?	
	Да	
	Нет	
3.3.	Покидая рабочее место, Вы оставляете ПК:	
	В активном режиме	
	В спящем режиме	
	Выключаете	
3.4.	Бумажные документы, в которых содержаться персональные данные, хранятся:	
	В открытом доступе, в ящиках стола/ шкафу, не закрывающимся на замок	
	В ящиках стола/ шкафу, закрывающимся на замок	
	В сейфе	
3.5.	Имеется ли у Вас устройства для уничтожения бумажных копий (например, шредер?)	
	Нет	
	Да	
3.6.	Где Вы храните архив (дела уволенных сотрудников, старые договора и другие?)	
	У нас нет архива	

№ критерия	Описание критерия	Значение критерия
	Выбрасываем документы	
	Передаем на хранение в архив	
3.7.	Доступ в архив имеют:	
	Все сотрудники	
	Специалисты (бухгалтера, кадровые работники, менеджеры)	
	Только руководитель	

Значение уровня защищенности для каждого критерия вычисляется по формуле (1),

где Y1 – степень исходной защищенности ИСПДн:

$$Y1=\begin{cases} 0 - \text{высокий уровень защищенности} \\ 10 - \text{низкий уровень защищенности} \end{cases}$$

Y2 – вероятность возникновения угрозы:

$$Y2=\begin{cases} 0 - \text{реализация угрозы низкая} \\ 5 - \text{реализация угрозы средняя} \\ 10 - \text{реализация угрозы высокая} \end{cases}$$

Далее вычисляется итоговый уровень защищенности для данной группы:

– ИСПДн имеет «Высокий» уровень исходной защищенности, если не менее 70 % критериев соответствуют уровню «Высокий»;

– ИСПДн имеет «Средний» уровень исходной защищенности, если не менее 50 % критериев соответствуют сумме уровней («Высокий» + «Средний»);

– ИСПДн имеет «Низкий» уровень исходной защищенности, если не выполняются пункты *а* и *б*.

Группа «4. Оценка защищенности ИСПДн от угроз уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн». Данная группа предназначена для определения уровня защищенности информационной системы от угроз уничтожения, хищения аппаратных средств ИСПДн. В табл. 15 представлен опросный лист.

Таблица 15

Опросный лист «Выполнение требований по технической защите от угроз хищения носителей информации»

№ критерия	Описание критерия	Значение критерия
4.1.	Установлена ли у Вас охранно-пожарная сигнализация в помещениях, где происходит обработка и хранение персональных данных?	
	Нет	
	Да	
4.2.	Установлена ли у Вас решетки на окнах?	
	Нет	
	Да	
4.3.	Установлены ли у Вас видеокамеры в помещениях, где происходит обработка и хранение персональных данных?	
	Нет	
	Да	
4.4.	Ведется ли у Вас журнал посетителей в помещениях, где происходит обработка и хранение персональных данных?	
	Нет	
	Да	

Значение уровня защищенности для каждого критерия вычисляется по формуле (1),

где Y1 – это степень исходной защищенности ИСПДн:

$$Y1=\begin{cases} 0 - \text{ высокий уровень защищенности} \\ 10 - \text{низкий уровень защищенности} \end{cases}$$

Y2 – это вероятность возникновения угрозы:

$$Y2=\begin{cases} 0 - \text{ реализация угрозы низкая} \\ 5 - \text{ реализация угрозы средняя} \\ 10 - \text{реализация угрозы высокая} \end{cases}$$

Далее вычисляется итоговый уровень защищенности для данной группы:

– ИСПДн имеет «Высокий» уровень исходной защищенности, если не менее 70 % критериев соответствуют уровню «Высокий»;

– ИСПДн имеет «Средний» уровень исходной защищенности, если не менее 50 % критериев соответствуют сумме уровней («Высокий» + «Средний»);

– ИСПДн имеет «Низкий» уровень исходной защищенности, если не выполняются пункты *а* и *б*.

Группа «5. Оценка защищенности ИСПДн от угроз несанкционированного доступа». В табл. 16 представлен опросный лист.

Таблица 16

Опросный лист «Выполнение требований по технической защите от несанкционированного доступа»

№ критерия	Описание критерия	Значение критерия
5.1.	Установлена ли антивирусная защита на ПК, обрабатывающих ПДн?	
	Нет	
	Да	
5.2.	Как часто Вы проверяете свой ПК на наличие вирусов?	
	Не проверяю	
	Ежемесячно	
	Еженедельно	
	Ежедневно	
5.3.	Установлен ли у Вас межсетевой экран?	
	Нет	
	Да	
5.4.	Утверждены ли в организации правила работы с Интернет?	
	Нет	
	Да	
5.5.	Утверждены ли в организации инструкции по антивирусной защите?	
	Нет	
	Да	
5.6.	Используете ли Вы в программы для отслеживания утечек конфиденциальной информации?	
	Нет	
	Да	

Значение уровня защищенности для каждого критерия вычисляется по формуле (1):

Y1 – степень исходной защищенности ИСПДн:

$$Y1=\begin{cases} 0 - \text{ высокий уровень защищенности} \\ 10 - \text{низкий уровень защищенности} \end{cases}$$

Y2 – вероятность возникновения угрозы:

$$Y2=\begin{cases} 0 - \text{ реализация угрозы низкая} \\ 5 - \text{ реализация угрозы средняя} \\ 10 - \text{реализация угрозы высокая} \end{cases}$$

Далее вычисляется итоговый уровень защищенности для данной группы:

– ИСПДн имеет «Высокий» уровень исходной защищенности, если не менее 70 % критериев соответствуют уровню «Высокий»;

– ИСПДн имеет «Средний» уровень исходной защищенности, если не менее 50 % критериев соответствуют сумме уровней («Высокий» + «Средний»);

– ИСПДн имеет «Низкий» уровень исходной защищенности, если не выполняются пункты *а* и *б*.

Группа «6. Оценка защищенности ИСПДн по выполнению технических требований». Опросный лист по выполнению требований по технической защите представлен в табл. 17.

Таблица 17

Опросный лист «Выполнение требований по технической защите»

№ критерия	Описание критерия	Значение критерия
6.1.	ИСПДн территориально распределена:	
	распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом	
	городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	
	корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	
	локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	
	локальная ИСПДн, развернутая в пределах одного здания	
6.2.	Соединения с сетями общего пользования	
	ИСПДн, имеющая многоточечный выход в сеть общего пользования;	
	ИСПДн, имеющая одноточечный выход в сеть общего пользования;	
	ИСПДн, физически отделенная от сети общего пользования	
6.3.	По встроенным (легальным) операциям с записями баз	

№ критерия	Описание критерия	Значение критерия
	персональных данных:	
	модификация, передача	
	запись, удаление, сортировка	
	чтение, поиск	
6.4.	По разграничению доступа к персональным данным:	
	ИСПДн с открытым доступом	
	ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	
	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	
6.5.	По наличию соединений с другими базами ПДн иных ИСПДн:	
	интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	
	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	
6.6.	По уровню обобщения (обезличивания) ПДн:	
	ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	
	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	
	ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	
6.7.	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:	
	ИСПДн, предоставляющая всю базу данных с ПДн;	
	ИСПДн, предоставляющая часть ПДн;	
	ИСПДн, не предоставляющая никакой информации	
6.8.	Разрешается ли установка программного обеспечения	
	Да, всем пользователям	
	Пользователям с определенными правами, если это ПО является разрешенным	
	Только системному администратору	

№ критерия	Описание критерия	Значение критерия
6.9.	Ведется ли учет машинных носителей и контроль перемещения их за пределы контролируемой зоны?	
	Нет	
	Да	
6.10.	Ведется ли журнал событий ИСПДн?	
	Нет	
	Да	
6.11.	Проводятся ли работы по резервному копированию баз данных ПДн?	
	Нет	
	Ежемесячно	
	Еженедельно	
	Ежедневно	
6.12.	Разрешено ли удаленное администрирование ПО лицам, не являющимся работниками оператора ПДн	
	Нет	
	Да	
6.13.	Используется ли в организации источники бесперебойного питания?	
	Нет	
	Да	

Значение уровня защищенности для каждого критерия вычисляется по степени исходной защищенности ИСПДн, которая может принимать значения:

$$Y1=\begin{cases} 0 - \text{высокий уровень защищенности} \\ 10 - \text{низкий уровень защищенности} \end{cases}$$

Далее вычисляется итоговый уровень защищенности для данной группы:

– ИСПДн имеет «Высокий» уровень исходной защищенности, если не менее 70 % критериев соответствуют уровню «Высокий»;

– ИСПДн имеет «Средний» уровень исходной защищенности, если не менее 50 % критериев соответствуют сумме уровней («Высокий» + «Средний»);

– ИСПДн имеет «Низкий» уровень исходной защищенности, если не выполняются пункты *а* и *б*.

Группа «7. Оценка уровня защищенности по выполнению программных требований». Вопросы из опросного листа по выполнению

требований по программной защите от недекларированных возможностей представлены в табл. 18.

Таблица 18

Опросный лист «Выполнение требований по программной защите»

№ критерия	Описание критерия	Значение критерия
7.1.	Вы используете:	
	не лицензионную ОС	
	лицензионную ОС	
7.2.	Вы используете ОС версии:	
	XP SP2	
	XP SP3	
	Windows 7	
	Windows 8	
	Другую ОС	
7.2.	Прикладное программное обеспечение	
	не лицензионное	
	частично лицензионное	
	полностью лицензионное	
7.3.	Используете ли вы облачные технологии?	
	Нет	
	Да	
7.4.	Разрешено ли использование социальных сетей	
	Нет	
	Да	
7.5.	Разрешено ли использование Skype, ICQ?	
	Нет	
	Да	
7.6.	Разрешено ли скачивание файлов из сети Интернет?	
	Нет	
	Да	

Значение уровня защищенности для каждого критерия вычисляется по степени исходной защищенности ИСПДн, которая может принимать следующие значения:

$$Y1=\begin{cases} 0 - \text{ высокий уровень защищенности} \\ 10 - \text{низкий уровень защищенности} \end{cases}$$

Далее вычисляется итоговый уровень защищенности для данной группы:

– ИСПДн имеет «Высокий» уровень исходной защищенности, если не менее 70 % критериев соответствуют уровню «Высокий»;

– ИСПДн имеет «Средний» уровень исходной защищенности, если не менее 50 % критериев соответствуют сумме уровней («Высокий» + «Средний»);

– ИСПДн имеет «Низкий» уровень исходной защищенности, если не выполняются пункты *а* и *б*.

Группа «8. Разработка моделей нарушителя». Модель нарушителя представляет собой описание типов злоумышленников, которые своими действиями или бездействиями, намеренно или случайно способны нанести ущерб информационной системе. Модель нарушителя должна быть составлена, чтобы в последствии определить меры для недопущения возникновения инцидентов[1].

Обычно составляют следующую модель нарушителя:

– внутренние (конечные пользователи системы, персонал обслуживающий технические средства, программное обеспечение, руководители, сотрудники службы безопасности, вспомогательный персонал);

– внешние (технический персонал по обслуживанию вычислительной техники, клиенты/посетители, представители конкурирующих предприятий, специалисты, обслуживающие специализированное программное обеспечение).

Для формирования более актуальных угроз, данный пункт состоит из двух подпунктов: 1) «модели внутреннего и внешнего нарушителя», формирование источников угроз по типу нарушителя представлен в табл. 19; 2) «модель деятельности предприятия», описана в табл. 20.

Таблица 19

Опросный лист «*8 а)* Формирование актуальных угроз»

№ критерия	Описание критерия	Значение критерия
8.1.	В Вашей организации «большая текучка кадров»	
	Нет	
	Да	
8.2.	В Вашей компании были увольнения за последние 3-6 месяцев	

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

№ критерия	Описание критерия	Значение критерия
	Нет	
	Да	
8.3.	Уволившиеся сотрудники имели доступ к конфиденциальной информации?	
	Нет	
	Да	
8.4.	Уволившиеся сотрудники были системными администраторами?	
	Нет	
	Да	
8.5.	Уволившиеся сотрудники были специалистами (менеджерами, бухгалтерами, кадровыми работниками)?	
	Нет	
	Да	
8.6.	Уволившиеся сотрудники были руководителями подразделений, компании)?	
	Нет	
	Да	
8.7.	При увольнении были конфликты с этими сотрудниками?	
	Нет	
	Да	
8.8.	В Вашей компании официальное трудоустройство?	
	Нет	
	Да	
8.9.	В Вашей компании случаются «бунты»?	
	Нет Да	
8.10.	Вспомогательный персонал (уборщицы, электрики) работают в помещениях, где обрабатываются ПДн, во внерабочее время, выходные дни?	
	Нет	
	Да	
8.11.	Оцените уровень знаний Ваших сотрудников в области информационных технологий по 10 балльной шкале (10 – плохо, 0-отлично)	
8.12.	Обновления программного обеспечения (например, 1С, Консультант+, Гарант и др.) проводят приглашенные специалисты?	
	Нет	
	Да	

№ критерия	Описание критерия	Значение критерия
8.13.	Обновления ПО проводятся в присутствии Ваших сотрудников?	
	Нет	
	Да	
8.14.	При обновлении ПО специалист другой компании использует свои съемные носители?	
	Нет	
	Да	
8.15.	Копирует ли посторонний специалист Ваши базы?	
	Нет	
	Да	
8.16.	При использовании съемного носителя сотрудника обслуживающей компании, проводится ли антивирусная проверка?	
	Нет	
	Да	
8.17.	Часто ли Вас посещают Ваши клиенты?	
	Нет	
	Да	
8.18.	Часто ли возникают недоразумения, конфликты с Вашими клиентами?	
	Нет	
	Да	
8.19.	Копируете ли Вы Вашим клиентам какую-либо информацию?	
	Нет	
	Да	
8.20.	При использовании съемного носителя Вашего клиента, проверяете ли на наличие вирусов?	
	Нет	
	Да	

Значение уровня защищенности для каждого критерия вычисляется по степени исходной защищенности ИСПДн, которая может принимать следующие значения:

$$Y1=\begin{cases} 0 - \text{высокий уровень защищенности} \\ 10 - \text{низкий уровень защищенности} \end{cases}$$

Далее вычисляется итоговый уровень защищенности для данной группы:

– ИСПДн имеет «Высокий» уровень исходной защищенности, если не менее 70 % критериев соответствуют уровню «Высокий»;

– ИСПДн имеет «Средний» уровень исходной защищенности, если не менее 50 % критериев соответствуют сумме уровней («Высокий» + «Средний»);

– ИСПДн имеет «Низкий» уровень исходной защищенности, если не выполняются пункты *а* и *б*.

Таблица 20

«*8 б)* Модель деятельности предприятия»

№ критерия	Описание критерия	Значение критерия
8.21.	Укажите численность населения в Вашем городе	
	до 250 000 чел	3
	250 000-500 000 чел	5
	свыше 500 000 чел	10
8.22.	Укажите вид деятельности Вашего предприятия	
	медицинские услуги	10
	политические организации	10
	религиозные, философские организации	10
	услуги интимного характера (например, магазин)	10
	Органы государственной власти \ нотариальные услуги	10
	финансовые услуги\ услуги страхования	8
	образовательные услуги	8
	торговля	8
	строительные услуги	6
	посреднические услуги	6
	другие виды деятельности	4
8.23.	Укажите количество Ваших клиентов	
	до 1000 чел	3
	1000–100 000 чел	5
	Свыше 100 000 чел	10
8.24.	Укажите количество конкурентов (примерно)	
	до 10	5
	свыше 10	10
8.25.	Есть ли у Вашей компании сайт?	
	Нет	0
	Да	10

Значение уровня защищенности для каждого критерия вычисляется по степени исходной защищенности ИСПДн, которая может принимать следующие значения:

$$Y1=\begin{cases} 0-2 - \text{высокий уровень защищенности} \\ 3-5 - \text{средний уровень защищенности} \\ 6-10 - \text{низкий уровень защищенности} \end{cases}$$

Далее вычисляется итоговый уровень защищенности для данной группы:

– ИСПДн имеет «Высокий» уровень исходной защищенности, если не менее 70 % критериев соответствуют уровню «Высокий»;

– ИСПДн имеет «Средний» уровень исходной защищенности, если не менее 50 % критериев соответствуют сумме уровней («Высокий» + «Средний»);

– ИСПДн имеет «Низкий» уровень исходной защищенности, если не выполняются пункты *а* и *б*.

Оценка общего уровня защищенности ИСПДн. Следует отметить, что соблюдение всех требований, перечисленных выше, является необходимым условием для безопасного функционирования информационной системы.

Все показатели по группам оформляются в таблицу с вычисленным уровнем показателя по каждой группе и затем, оценка общего уровня защищенности ИСПДн производится по принципу:

а) ИСПДн имеет «Высокий» уровень исходной защищенности, если не менее 70 % критериев соответствуют уровню «Высокий»;

б) ИСПДн имеет «Средний» уровень исходной защищенности, если не менее 50 % критериев соответствуют сумме уровней («Высокий» + «Средний»);

в) ИСПДн имеет «Низкий» уровень исходной защищенности, если не выполняются пункты *а* и *б*.

Подводя итоги, о защищенности информационной системы можно судить, если выполняются все организационные, технические, правовые требования. Конфиденциальная информация, к которой относятся персональные данные, должна обрабатываться с помещениях с ограниченным доступом, с видеонаблюдением, с отсутствием возможности распечатки документов, несанкционированного копирования, невозможностью загрузки со сменного носителя, с надежной ан-

тивирусной системой, только совокупность этих мер приведет к высокой оценки защищенности персональных данных.

3.3. Направления совершенствования механизма защиты ПДн

Рассмотрев правовые нормативные документы, документы по технической защите персональных данных, обрабатываемых как в информационных системах, так и просто на бумажных носителях, автор предлагает следующие направления по совершенствованию механизмов защиты персональных данных.

Обучение. Во главе угла по защите персональных, по мнению автора, должно стоять обучение не только персонала оператора ПДн, но и простых граждан. Необходимо организовывать обучающие семинары, мероприятия, на которых в простой и доходчивой форме доносились основные требования закона и пути их реализации.

Проведенное исследование показало, что в государственных организациях, где проходили обучающие мероприятия, специалисты, обрабатывающие персональные данные, стали более внимательно относиться к этому вопросу.

Руководители малых, средних предприятий и индивидуальные предприниматели часто не знают о введении новых правовых нормативных документов и тем более о реализации и внедрении технических мер на рабочих местах в компании. Если бы РОСКОМНАДЗОР проводил обучающие мероприятия, семинары и приглашали руководителей и специалистов на них, уровень информативности о законе и его требованиях намного бы повысился.

Считаем, что обучением персонала компаний в большей части должно проводить государство (региональные отделения РОСКОМНАДЗОРа), как например, это делают региональные отделения Пенсионного Фонда или Налоговые инспекции в период изменения законодательства и введение новых форм отчетности.

Необходимо также разрабатывать информационные листовки, в которых бы кратко были описаны действия, которые должны выполнить руководители, специалисты компаний.

Еще одним немаловажным аспектом в обучении, считем взаимодействие представителей компании и Регулятора, при котором последний оказывал консультационные и методические услуги (может даже за символическую плату), помогал бы искать ответы на некоторые вопросы, хотя бы на этом переходном этапе. Ведь многие компа-

нии просто не в состоянии организовать обучающие курсы для своих специалистов из-за высокой стоимости (обучение одного специалиста обходится от 10000 и выше).

И наконец, обучение физических лиц, граждан, которые разглашают персональную информацию о себе, близких на просторах Интернета, оставляя свои номера телефонов в различных салонах, бутиках. Чем чаще сами граждане будут задумываться о своей безопасности, тем меньше шансов стать объектом мошенничества.

Постоянство правовых нормативных актов. Это второй по значимости шаг, который необходимо осуществить. За последние три года многие нормативные документы изменились. К моменту вступления закона «О персональных данных» в 2010 г. многие государственные учреждения, крупные коммерческие организации в полной мере осуществили требования закона: провели аттестацию ИСПДн; реализовали технические меры (покупка установка сертифицированных средств защиты); выполнили правовые организационные мероприятия (подготовили организационно-распорядительную документацию). В 2013 г. вступили в действие новые требования и организациям необходимо выполнять данную работу повторно.

В связи с чем возникает вопрос: «Если требования будут меняться часто, зачем их выполнять?».

Разработка примеров построения защиты ИСПДн. Здесь можно было бы обратиться к международному опыту. Как уже отмечалось выше, в Великобритании разработаны стандарты, а также примеры к ним, позволяющие организациям использовать их в своей работе. Являясь рекомендованными, уже многие компании в мире взяли на вооружение эти стандарты.

РОСКОМНАДЗОР выпустил методические рекомендации по обезличиванию персональных данных. Многие специалисты в области информационной безопасности, признали, что, в целом данные рекомендации являются неплохими и их можно использовать в работе.

Исходя из вышесказанного, разработав и выпустив методические рекомендации, по каждому из этапов приведения ИСПДн, многие компании могли бы ими воспользовались.

Информирование об утечках и обработка инцидентов. В нашей стране, как уже отмечалось выше, не существует практика информирования клиентов, надзорных органов о случившейся утечке. В случае, когда общественности станет известно об инциденте, компания понесет определенные риски (материальные, репутационные). Это,

конечно же, негативно скажется на самой компании. Таким образом, прописав законодательно норму об обязательном информировании об утечке, компании были бы заинтересованы выстаивать реальную защиту информационной системы, а не выполнять требования формально, только на бумаге.

Совместное использование DLP-решений, антивирусной защиты и межсетевых экранов позволит компаниям избежать неприятных моментов, связанных с утечкой информации.

Ужесточение контроля. В данном случае, эта мера должна быть реализована в последнюю очередь. Как отмечалось выше, для начала необходимо провести комплекс мер, направленных на информирование, обучение руководителей и сотрудников организаций. Разработать инструкции по работе с персональными данными, инструкции по реализации мероприятий в случае их утечки и другие.

И только в том случае, когда организация целенаправленно игнорирует выполнение требования закона, привлекать ее к административной ответственности. Если организация допускает нарушение повторно суммы штрафов должны быть увеличены. Кроме этого, необходимо разработать процедуру привлечения лица, допустившего утечку информации, содержащей персональные данные.

В вопросе защиты персональных данных должны быть заинтересованы все участники информационного обмена: оператор ПДн, физическое лицо и Регуляторы. Создание единого информационного образовательного пространства в сфере защиты Пдн, постоянство законодательных актов, их неукоснительное соблюдение и другие факторы помогут быстрее вникнуть в сложный процесс защиты и перейти к формированию цивилизованного информационного общества.

4. ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

4.1. 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 содержа-

щихся 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:

4. 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.

5. 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 отме-

тил, что в связи с ростом угроз киберпространству одной из ответных мер станет превращение нынешнего комитета по информационной безопасности в комитет по кибербезопасности с приданием 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[1]. В свою очередь, в Китае для борьбы с компьютерной преступностью созданы специальные отряды интернет-полиции.

6. 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[2].

Организованный характер киберугроз подтверждается также выступлением генерала Сон Юн Кын, занимающегося в вооруженных си-

---

[1] О персональных данных : федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

[2] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства от 1 нояб. 2012 г. № 1119 // Собрание законодательства РФ. – 2012. – № 45. – Ст. 6257.

лах 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[1];

– 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 про-

[1] О лицензировании деятельности по технической защите конфиденциальной информации : постановление Правительства от 3 февр. 2012 г. № 79 // Собрание законодательства РФ. – 2012. – № 7. – Ст. 863.

грамму 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 про-

токолы. 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, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

4.2. 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:

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

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

– человек, способный быстро схватить суть явления;

– человек, способный к быстрой разработке программ;

– эксперт по определенной системе, как правило, часто использующий ее;

– эксперт или энтузиаст любого рода;

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

– 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 пе-

релезать. «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.

4.3. 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 другого 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.

4.4. 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 проникнуть 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.

4.5. 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 эконо-

мической 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:

- реагирование на инциденты (Incident response);
- расследование инцидентов (eDiscovery);
- компьютерная криминалистика (Digital Forensic);
- мониторинг инцидентов;
- 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 информации. 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 деятельности 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.

ЗАКЛЮЧЕНИЕ

Рассмотрены вопросы, касающиеся защиты персональных данных работников, клиентов организаций, относящихся к различным сферам деятельности. В связи с многочисленными сообщениями об утечках персональных данных, их защита является приоритетным направлением не только со стороны Государства, но и со стороны организаций всех форм собственности. Зная основные каналы утечки персональных данных в различных странах, операторы ПДн, могут предотвратить их незаконное распространение, копирование и сбор.

Основной задачей, в настоящий момент, является снижение трудоемкости и повышение эффективности защиты персональных данных, обрабатываемых в информационных системах. Для достижения поставленной цели в монографии выполнен ряд задач: изучено законодательство в сфере защиты персональных данных, проанализированы основные каналы утечки ПДн, проведены исследования специализированного программного обеспечения, позволяющего построить надежную системы защиты информационных систем персональных данных.

Алгоритм категорирования персональных данных, позволяющий с минимальными временными затратами определить категорию персональных данных. Данный алгоритм поможет исключить неоднозначность определения категории ПДн, определить тип информационной системы и тип актуальных угроз. Подспорьем для алгоритма категорирования может служить методика оценки уровня защищенности персональных данных на основе нормативных документов. Она позволит объективно оценить насколько организация выполняет требования законодательства и принять меры по устранению недостатков.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

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

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

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

4. 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.

5. 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.

6. 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.

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

8. 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».

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

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

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

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

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

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

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

16. 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.

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

18. 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.

19. 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.

20. 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.

21. 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 конферен-

ции «Региональные проблемы защиты персональных данных». – Брянск : БГТУ, 2010. – С. 47–49.

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

23. 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.

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. 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.

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

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

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

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

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

35. 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.

36. 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.

37. 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.

38. 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.

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

40. Конституция Российской Федерации : принята всенар. голосованием 12 дек. 1993 г. // Российская газета. – 2009. – 21 янв.

41. 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.

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

43. 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.

44. 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.

45. 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.

46. 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.

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

48. 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.

49. 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».

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

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

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

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

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

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

56. 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.

57. 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.

58. 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.

59. О лицензировании деятельности по технической защите конфиденциальной информации : постановление Правительства РФ от 3 февр. 2012 г. № 79 // СЗ РФ. – 2012. – № 7. – Ст. 863.

60. О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ // СЗ РФ. – 2006. – № 31, ч. 1. – Ст. 3451.

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

62. 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.

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

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

65. 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.

66. 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.

67. 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.

68. 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.

69. 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.

70. Об утверждении требований и методов по обезличиванию персональных данных : приказ Роскомнадзора от 5 сент. 2013 г. № 996 // Российская газета. – 2013. – 18 сент.

71. 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.

72. 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.

73. 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.

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

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

76. 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.

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

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

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

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

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

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

83. 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.

84. 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.

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

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

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

88. 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.

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

90. 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.

91. 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.

92. 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.

93. 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.

94. 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.

95. 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.

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

97. 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.

98. 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.

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

100. 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.

101. 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.

102. Трудовой кодекс Российской Федерации : федер. закон от 30 дек. 2001 г. № 197-ФЗ // Российская газета. – 2001. – 31 дек.

103. 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.

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

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

106. 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.

107. 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.

108. 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.

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

110. 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.

Научное издание

Сачков Дмитрий Иванович
Смирнова Ирина Георгиевна
Быкова Вера Николаевна

ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИЯХ

Издается в авторской редакции

Технический редактор
А.С. Ларионова

ИД № 06318 от 26.11.01.
Подписано в печать 26.11.15. Формат 60х90 1/16. Бумага офсетная.
Печать трафаретная. Усл. печ. л. 9,4. Тираж 500 экз. Заказ .

Издательство Байкальского государственного университета
экономики и права.
664003, г. Иркутск, ул. Ленина, 11.
Отпечатано в ИПО БГУЭП.