Национальный исследовательский университет «Высшая школа экономики»
Институт проблем безопасности

Шульц В.Л., Рудченко А.Д., Юрченко А.В.

Комплексное противодействие атакам на информационные ресурсы

Пособие для обучения на майноре

Раздел IV. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Глава 20. Угрозы в области информационной безопасности

Угроза разглашения защищаемой информации
Угроза перехвата каналов связи и компрометации шифров
Угроза осуществления промышленного шпионажа
Угроза нарушения нормальной жизнедеятельности предприятия

Глава 21. Защита персональных данных

21.1. Право личности на защиту персональных данных
21.2. Система защиты персональных данных в Российской Федерации
21.3. Защита персональных данных на предприятии
21.4. Ответственность за нарушение правил защиты персональных данных

Глава 22. Защита конфиденциальной информации

22.1. Система защиты конфиденциальной информации в Российской Федерации
22.2. Коммерческая тайна
22.3. Налоговая тайна
22.4. Банковская тайна
22.5. Ведомственная тайна

Глава 23. Защита государственной тайны

23.1. Понятие и виды государственной тайны
23.2. Система защиты государственной тайны

Глава 24. Безопасность электронных ресурсов, систем и процессов

24.1. Электронные информационные ресурсы, системы и процессы
24.2. Типовые угрозы кибернетической безопасности предприятия
24.3. Архитектура стандартов кибернетической безопасности
24.4. Превентивная защита информации на автоматизированных рабочих местах, в корпоративных сетях и банках данных, при передаче с использованием Интернета, при функционировании систем электронных финансов
24.5. Расследование кибернетических инцидентов

Глава 25. Взаимодействие частных и государственных институтов

6.1. Нормативно-правовая база в сфере информационной безопасности
6.2. Участие государства в обеспечении информационной безопасности
6.3. Информационные инциденты, требующие взаимодействия с государством

Раздел IV. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Глава 20. Угрозы в области информационной безопасности

В результате изучения главы студент должен **знать** основы теории информации и основные угрозы в области информационной безопасности предприятия; о преднамеренной деятельности государств и транснациональных корпораций по хищению охраняемой информации в процессе промышленного шпионажа; об умышленном и непреднамеренном разрушении системы передачи информации в целях управления, что может привести к нарушению нормальной жизнедеятельности предприятия; **уметь** использовать признаки несанкционированного доступа к информации в местах ее хранения, в процессе ее передачи от одного пользователя к другому путем перехвата каналов связи и компрометации шифров; **владеть** методами выявления рисков и угроз в области информационной безопасности предприятия.

20.1. Элементы системы информационной безопасности

Под термином *информация* традиционно принято понимать сведения о предметах и лицах, событиях и фактах, процессах и явлениях вне зависимости от формы их восприятия. В современной науке существует устойчивое мнение рассматривать информацию, опираясь на философские категории отражения и различия (разнообразия). Информация не может существовать без отражения, как и отражение не может быть без информации.

Свойство отражения представляет собой способность любого объекта воссоздавать определенные особенности влияющих на него объектов. В то же время, применение одной лишь категории отражения будет недостаточно для определения понятия информации. Информация появляется лишь в том случае, когда в определенном тождестве существует некоторое различие. Выделяют четыре вида отражения: неживая естественная природа (элементарное отражение), живая природа (биологическое отражение), общество (социальное отражение) и искусственная природа. К данным видам отражения относят следующие виды информации:

- Элементарную информацию (в неживой природе);
- Биологическую информацию (в объектах живой природы);
- Социальную информацию (в обществе);
- Технико-кибернетическую информацию (в автоматизированных устройствах).

К особенностям информации относится невозможность представления ее без определенной материальной основы, так как эта основа является свойством материи и не может быть отделима от нее. Даже в случае отражения информации сознанием человека, она не может существовать без единства с определенными нейрофизиологическими процессами, то есть имеет собственный материальный носитель. В свою очередь, идеалистическое представление допускает самостоятельное существование информации, то есть без материального носителя. В конце 1950-х годов Н. Винер, один из основоположников кибернетики, дал следующее определение понятию информация - **определение содержания, которое получено из внешнего мира в процессе адаптации человека к нему и адаптации к внешнему миру чувств человека. Процесс получения и использования информации является процессом адаптации человека к непроизвольностям внешней среды и жизнедеятельности человека в этой среде*.**

Развитие информационных технологий провоцирует собой интенсивное совершенствование законодательной базы, а также введения в юридическую сферу понятий, которые ранее применялись в кибернетике и информатике. Так, например, всякая информация выступает в качестве объекта гражданских прав. Отсюда следует, что *правовой режим информации* представляет собой нормативно установленные правила, которые определяются степенью открытости, порядком документирования, доступностью, хранением, распространением и защитой информации, а также исключительностью права на информацию. В Российской Федерации вопросы информации, информационных технологий и защиты информации регламентированы законодательно.

Уровень развития современных информационных технологий обуславливает почти безграничные возможности личности, общества и государства в отношении получения и использования информации. Как результат, информация стала важнейшим ресурсом по сравнению с другими основными ресурсами, к которым, в свою очередь, относятся природные, экономические, трудовые, материальные ресурсы. Для правового регулирования информацией необходимо наличие в ней соответствующих свойств, присущих только данному объекту познания.

К таким свойствам информации можно отнести:

- Физическую неотчуждаемость, так как информация неотделима от материального носителя;
- Обособленность, то есть включение информации в гражданский оборот в форме знаков и символов, обособив ее, таким образом, от производителя и предав ей отдельное существование;

**Винер Н.* Кибернетика и общество. Творец и Будущее. М.: АСТ, 2003. С. 19

- Двуединство информации и носителя, которое определено в самом понятии «информация» как вещь на материальном носителе;
- Распространяемость (тиражируемость), которая проявляется в возможности неограниченного распространения экземпляров информации без изменения ее содержания;
- Организационная форма информации, которой является документ;
- Экземплярность, то есть наличие информации на отдельном материальном носителе.

В данном контексте понятию «информация» придается универсальность, так как под информацией имеются в виду любые данные, которые получаются из любого источника в любой форме: устной, письменной, визуальной и др. При этом понятие *данные* рассматривается в качестве реальных объектов социальной жизни: лица и предметы, факты и события, явления и процессы. В свою очередь, данные могут выступать как объектами познания, так и ресурсами пополнения информационной базы, полученные как в результате исследования окружающей среды и приобщения ее к существующей объективной системе знаний о мире, так и в результате поиска конкретного потребителя для достижения собственных целей.

Существует четыре вида информации:

Контрольно-измерительная информация представляет информацию, связанную с постоянным техническим контролем на производстве и получаемую в результате естественнонаучных исследований. Данный вид информации регистрируется приборами и первичными учетными документами (таблицами, перфокартами) и используется при регуляции процессов.

Учетно-статистическая информация заключает в себе данные, поступающие, в основном, в цифровом виде и отражающие развитие экономики, образования, культуры, здравоохранения и др. Так, для разрешении комплексных задач в области государственного и хозяйственного управления относительно природопользования находят широкое применение разного рода кадастров, реестров и регистров в сфере водного, рыбного и лесного хозяйства, гидрометеорологии, экологии и геологии, геодезии и картографии, землепользования и землеустройства, а также данных государственного учета ресурсов растительного и животного мира. В свою очередь, отображать статистическую информацию лучше всего в специфических отчетах, которые применяются в сфере управления.

К научно-технической информации относятся разного рода данные, которые характеризуют состояние наук. Данная информация находит отражение в специальной литературе по различным отраслям науки, сельскохозяйственного и промышленного производства, а также используется в основном небольшим кругом специалистов этих отраслей.

Общественно-политическую информацию представляют сведения, которые получаются в повседневной политической, экономической и культурной общественной жизни.

По степени организованности (упорядоченности) информация также делится на два вида – документированная и недокументированная. В широком смысле документ – это материальный объект, который фиксирует информацию в виде изображения, текста, звукозаписи и предназначенный для передачи в целях хранения и общественного использования во времени и пространстве.

Изучение проблем создания, передачи, обработки, и хранения информации показало, что функция защиты информации на всех стадиях методологически может быть представлена тремя этапами: начальный, развитый и комплексный. Для первых двух этапов характерны экстенсивные подходы к решению проблем защиты информации, основное содержание которых проявляется в осмыслении важности и необходимости проблемы, накоплении и анализе статистической информации, внедрении в практику эффективных методов и средств защиты. Последний, современный этап, характеризуется разработкой и внедрением принципиально новых научных подходов, которые реализуют системные принципы.

Под *правами доступа к информации* понимается совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и её носителям, установленных собственником (владельцем) информации или правовыми документами. Согласно этому определению, права доступа к информации определяют набор действий (например, чтение, запись, выполнение), разрешённых для выполнения субъектам над информацией. Таким образом, возникает необходимость в некой упорядоченной системе для предоставления субъектам различных прав доступа к информации. Указанные функции реализуются на практике с использованием системы информационной безопасности. Под *системой информационной безопасности* понимается **организованная совокупность специальных органов, средств, служб, методов и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке.** Системы информационной безопасности призваны обеспечивать информационную безопасность на различных уровнях. Соответственно, на государственном уровне под *информационной безопасностью государства* понимается состояние сохранения целостности информационных ресурсов государства и защищённости прав общества и личности в информационной сфере. На уровне организации *информационной безопасности организации* это представляется как состояние защиты интересов (целей) организации в условиях существующей информационной сферы (рис. № 50).

Рис. № 50. Структура информационной сферы организации по Курило А.П.

Под информационной сферой представляется совокупность информации, субъектов, информационной инфраструктуры, которая осуществляет сбор, формирование, использование, распространение и хранение информации*. При этом должны обеспечиваться конфиденциальность, целостность и доступность информации. В международных стандартах информационной безопасности указанные свойства образуют *AIC-триаду* (от английских слов: Availability - доступность, Integrity - целостность, Confidentiality - конфиденциальность). Уровень безопасности, необходимый для реализации этих свойств, отличается в различных компаниях. Защитные меры и механизмы безопасности внедряются для реализации одного (нескольких) из указанных свойств, также как и все риски измеряются по их потенциальной способности нарушения свойств AIC - триады.

*Обеспечение информационной безопасности бизнеса. *Под редакцией Курило А.П.* М.: Альпина, 2011. С 38

Доступность – свойство системы (среды, средств и технологии обработки), обеспечивающее своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность всех служб к обслуживанию поступающих запросов. *Уровень доступности информации* является одним из важнейших показателей правовой культуры общества.

Целостность – существование информации в некотором неискаженном виде (фиксированном относительно определенного состояния). Пользователи, как правило, влияют на целостность систем или данных в результате ошибок (хотя внутренние пользователи также могут совершать мошеннические или злоумышленные действия). Например, случайное удаление конфигурационных файлов, ввод ошибочной суммы операции и т.д.

Конфиденциальность – субъективно определяемая характеристика, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации. Это свойство обеспечивается способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий доступа к ней. Конфиденциальность должна обеспечиваться как при хранении информации, так и в процессе ее передачи.

В течение тысячелетий под обеспечением безопасности информации подразумевалось обеспечение ее конфиденциальности. Для этого использовались различные способы: тайнопись, иностранные языки, тайные знаки и др. Позже человечество изобрело криптографию, которая до сих пор широко используется в прикладной математике. Новую эпоху в передаче информации открыло радио. Сразу возникла возможность передавать в эфире значительные объемы конфиденциальной информации. Это породило сразу два направления деятельности: по созданию эффективных шифров и, естественно, алгоритмов их взлома (рис. № 56).

Уязвимость информационной системы является свойством информационной системы, которое определяет возможность реализации угроз безопасности информации, обрабатываемой в ней. Другими словами уязвимостью является слабость или отсутствие защитных мер. Уязвимостью может стать служба, которая была запущена на сервере, низкий уровень физической безопасности, которая позволяет каждому войти в серверную комнату, неограниченный открытый порт на межсетевом экране, неуправляемость паролями на серверах и рабочих станциях. В широком смысле помехи (шумы) на приведенном ниже рисунке являются своеобразными уязвимостями изображенного канала связи, которые могут привести к тому, что используемые в кодировании криптографические шифры могут быть скомпрометированы, а декодирование потеряет смысл. Поэтому и защиту от помех необходимо трактовать в широком смысле.

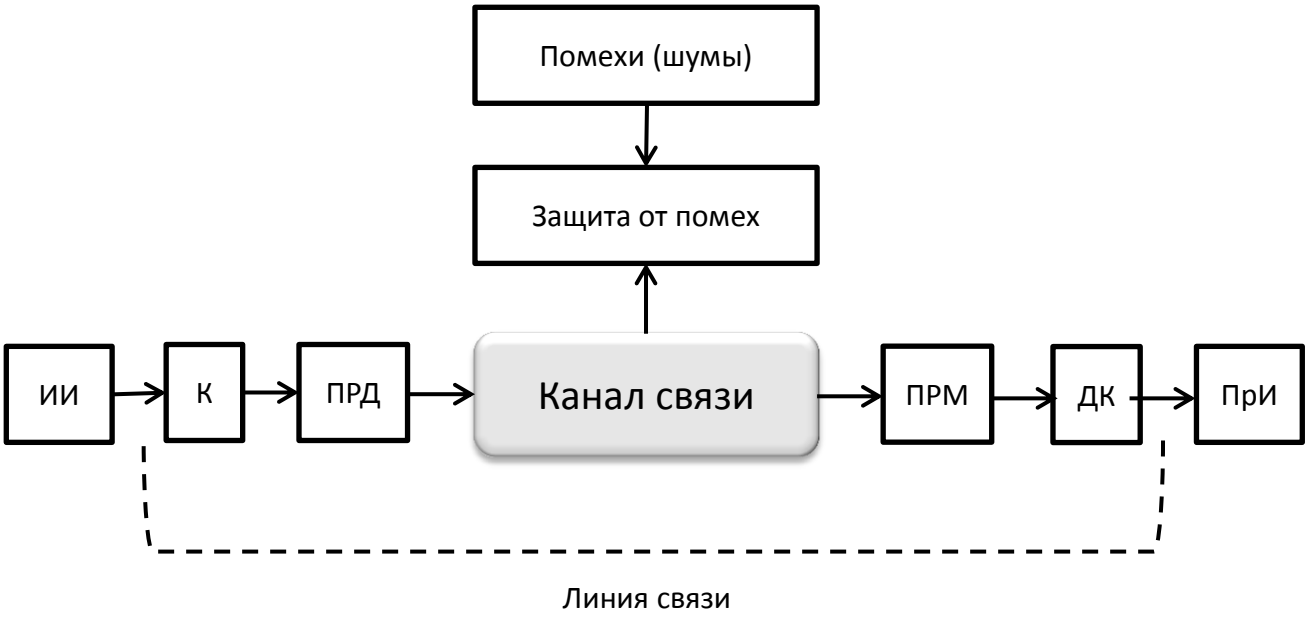

Рис. 51. Общая схема передачи информации по Белову В.М. и др.

На приведенном выше рисунке используются следующие сокращения: ИИ – источник информации, К – кодер, ПРД – передатчик информации, ПРМ – приемник информации, ДК – декодер, ПрИ – приемник информации*.

Риски в области информационной безопасности, согласно современной классификации предпринимательских рисков, относятся к области *операционных рисков*. Они могут быть природно-естественного, техногенного и политического характера, являться следствием целенаправленных или неумышленных действий людей, носить потенциальный или реальный характер. В случае, если защитные меры не позволили предотвратить наступление неблагоприятных факторов, возникает угроза перехода риска из состояния потенциального (реального) в состояние *реализованного риска*.

Угрозы реализации рисков в области информационной безопасности могут наступить в качестве следствия ряда причин. К ним относятся: риски информационного противоборства с внешними субъектами; риски злоумышленной активности персонала; риски получения неполной, недостоверной и несвоевременной информации; риски несовершенства организационной, функциональной и информационной сферы организации; риски несовершенства ролей и слабости менеджмента в критичных областях; риски технологической слабости в противостоянии негативным факторам.

**Белов В.М., Новиков С.Н., Солонская О.И.* Теория информации. М.: Телеком, 2012. С 55

20.2. Угроза разглашения защищаемой информации

Под разглашением защищаемой информации понимается противоправное предание огласке сведений ограниченного доступа посторонним лицом. При этом посторонним лицом считается любое лицо, которое по характеру служебных обязанностей или выполняемой работы не имеет доступа к защищаемой информации. Субъектом разглашение сведений ограниченного доступа является физическое лицо - владелец охраняемых секретов. Разглашение сведений ограниченного доступа может осуществляться в двух вариантах: путем непреднамеренного разглашения либо путем преднамеренного разглашения. Непреднамеренное разглашение, как правило, происходит по невнимательности или халатности лица, допущенного к закрытой информации. Обычно это случается на служебных совещаниях, при проведении деловых встреч, при передаче информации по открытым каналам связи (почта, телефон, телеграф, электронные каналы), на обучающих и научных мероприятиях, во время выставок. Информация может быть преднамеренно передана заинтересованной стороне одним из субъектов, допущенных к закрытой информации либо получившим ее при определенных обстоятельствах.

Кейс № 21. Торговля секретами в автопроме

В 2007 г. суд г. Модена (Италия), где расположена штаб-квартира Ferrari, признал двух бывших работников этой компании виновными в промышленном шпионаже. По словам представителя обвинения, сотрудники Ferrari Анджело Сантини и Мауро Яккони, уволившись из фирмы в 2002 г., перешли на работу в компанию Toyota. Однако перед своим увольнением они скачали файлы с конфиденциальной информацией о разработках Ferrari в области проектирования болидов Формулы-1, которые впоследствии были переданы представителям японского автопроизводителя. Полученные данные были использованы японцами при создании болида Toyota FT103y. В 2009 г. полиция США арестовала бывшего инженера компании Ford, которого подозревали в промышленном шпионаже в пользу Китая. Мужчине по имени Майк Юя, который является выходцем из Китая, предъявлены обвинения в том, что во время работы на компанию Ford Motor он похищал информацию, проникал в защищенную компьютерную сеть и проводил прочую шпионскую деятельность с 1997 по 2007 год. По данным полиции, непосредственно перед своим увольнением инженер скопировал с компьютера около 4000 файлов, которые относятся главным образом к дизайну новых моделей и концепт-каров. Какие китайские компании получали от шпиона секретную информацию пока неизвестно. Возможно, речь идет об очень крупных и известных китайских автопроизводителях*.

*Сайт автомобильных новостей [Электронный ресурс] // auto.mail.ru: информ.-справочный портал. М. URL: https://auto.mail.ru/news?id=22216 & https://auto.mail.ru/article/29908-ford_poimal (дата обращения: 27.01.2015)

Современные исследования компании PWC позволили выделить основные группы факторов и предпосылок, которые влияют на разглашение сведений ограниченного доступа, и определить их средние значения в процентах:

- Излишняя болтливость сотрудников компании – 32 %;
- Попытка сотрудников заработать любой ценой и любым способом– 24 %;
- Отсутствие службы безопасности компании – 14 %;
- Привычка сотрудников рассказывать друг другу новости компании – 12 %;
- Бесконтрольное использование информационных систем в компании – 10 %;
- Предпосылки возникновения конфликтных ситуаций в среде сотрудников компании (отсутствие работы по сплочению коллектива компании или случайный подбор кадров) – 8 %.

Исследования показали также, что наиболее часто разглашается информация о персональных данных сотрудников компаний, а также клиентов по бизнесу и учащихся. При этом упрощенный подход к проблеме неприемлем. Особенно в тех случаях, когда доступ к этим сведениям получают те лица, которые не являются конфидентами (надлежащими хранителями информации). Вот несколько примеров:

a. Работодатель, узнав, что соискатель в прошлом году четыре месяца провел на больничном, отказал ему в приеме на работу.
b. Человек уволился после того, как увидел, сколько получает его коллега.
c. В банке взяли кредит на реального человека, предоставив все паспортные данные и расписавшись похожей подписью.
d. Группа черных риелторов «освобождала» квартиры от людей, оставшихся без попечения родственников.

Таким образом, паспортные данные, сведения о заработной плате, о состоянии здоровья, о составе семьи, - все это конфиденциальная информация. Ее нельзя предоставлять по телефону и без личного согласия человека запрещается передавать третьим лицам. Даже данные о годе рождения могут навредить человеку, по тем или иным причинам не желающему, чтобы коллеги знали его настоящий возраст. Конечно, здесь важно не дойти до абсурда - в одном из вузов даже информация о книгах, которые берут студенты в библиотеке, была объявлена «закрытой», - но все же лучше перестраховаться, чем потом столкнуться с последствиями.

20.3. Угроза перехвата каналов связи и компрометации шифров

В соответствии с действующими российскими стандартами, **перехват информации – это неправомерное получение данных с использованием технических средств, которое осуществляет поиск, прием и обработку информативных сигналов, то есть,**

сигналов, по параметрам которых можно восстановить защищаемую информацию. В свою очередь, неконтролируемое носителем защищаемой информации распространение информации через физическую среду до технического устройства, которое осуществляет перехват информации, называется *утечкой* информации по техническому каналу.

Средствами бесконтрольного переноса конфиденциальной информации выступают акустические, электромагнитные, визуально-оптические и другие каналы*.

Рис. 52. Информационные физические поля по Меньшакову Ю.К.

Канал утечки информации – это физический путь от источника защищенной информации к правонарушителю, по которому возможно осуществление утечки или несанкционированное получение охраняемых данных. Для установления канала утечки информации необходимы некоторые временные, пространственные и энергетические условия, а также технические средства фиксации данных.

На практике информационные физические поля являются объектами проникновения для следующих технических видов разведки:

- Оптической разведки (визуально-оптическая, фотографическая);
- Оптико-электронной разведки (инфракрасная, телевизионная, лазерная);
- Радиоэлектронной разведки (радио, радиотехническая, радиолокационная, радиотепловая);
- Компьютерной разведки;

**Меньшаков Ю.К.* Теоретические основы технических разведок. М.: МГТУ им. Баумана, 2008. С. 10

- Гидроакустической разведки (активная, сигнальная, пассивная);
- Акустической разведки (речевая, сигнальная);
- Химической разведки (контактная, дистанционная);
- Радиационной разведки;
- Сейсмической разведки;
- Магнитометрической разведки;
- Измерительно-сигнатурной разведки.

Техническая разведка объектов военного и гражданского назначения имеет значительный опыт, который был принципиально усовершенствован в XX веке. Комплекс данных, полученных в результате применения этого вида разведки, с большой вероятностью позволит установить тип вооружения, профиль воинских частей и соединений, характер промышленного предприятия и номенклатуру выпускаемой им продукции. Однако не всегда перехват одного из физических излучений предоставлял возможность получения требуемой информации. Иногда перехват радиоканалов связи свидетельствовал о том, что стороны обмениваются зашифрованной информацией. Для того, чтобы расшифровать такую информацию, требовалось овладеть применяемым шифром. В этой связи криптографическая защита информации и попытки преодоления защитных мер известны достаточно давно. Долгое время эта сфера деятельности была прерогативой спецслужб.

Кейс № 22. Из опыта британских спецслужб

В мемуарах Питера Райта, бывшего английского контрразведчика, рассказывается про британские спецслужбы и его личные знакомства с агентами контрразведки, которые работали в посольстве Чехословакии в Лондоне и осуществляли операции проникновения в шифровальное бюро этого представительства с целью изъятия оттуда шифродокументов. В свою очередь, слепки с ключей от сейфов они добывали от других своих агентов. Похищенные шифры позволяли английской разведке изучать зашифрованную чехословацкую переписку. Однако через 6 месяцев шифры на документах были заменены, а английские агенты были уволены из посольства Чехословакии. Можно предположить, что это было сделано не случайно, а по причине раскрытия английских агентов чехословацкими спецслужбами.

Кроме того, в мемуарах П. Райта также приводится другой случай операции британских спецслужб в египетском посольстве, который произошел перед Суэцкой войной Великобритании, Франции и Израиля против Египта. Пользуясь войной, британские спецслужбы добывали информацию из шифрпереписки египетских правящих кругов, которая была направлена против стран-противников Египта. При этом британские спецслужбы также читали переписку Египта с посольством в Лондоне, в Москве и других мировых столицах. Это позволило Великобритании оказаться в курсе советско-египетских отношений в данный период.

Однако наибольшим успехом британских спецслужб, по мнению автора, было вскрытие французских шифров, осуществленное по новому методу перехвата линий коммуникаций, которое получило кодовое название «Стокэйд» или по-русски «перехватчик». С помощью этого метода можно было раскрыть шифр по перехваченным излучениям шифровальных машин при зашифровке или расшифровке телеграфных сообщений. Используя метод «Стокэйд», британские спецслужбы успешно читали шифрованную переписку посольства Франции в Лондоне в течение 1960-1963 годов. Пользуясь, этим же методом АНБ США получало доступ к чтению шифротелеграмм посольства Франции в Вашингтоне. Однако вскоре французские спецслужбы обнаружили слабую защищенность своих шифромашин и усилили экранизацию их излучения. Питер Райт, в свою очередь, рассказал, что британские спецслужбы, используя метод "Стокэйд", добыли секреты шифров многих других государств, чьи шифровальные машины не были защищены надежными экранами.

Вопрос: сообщите ваше мнение о возможности аналогичных действий в наше время.

С появлением компьютеров и их внедрением в повседневную деятельность государственных институтов, участников предпринимательской деятельности и других лиц, начался новый этап совершенствования мер криптографической защиты информации и попыток дешифрования в различных целях. В 1977 г. Национальное бюро стандартов США выбрало стандарт шифрования данных DES, разработанный корпорацией IBM. Данный метод был основан на принципе использования одного ключа, предназначенного как для шифрования, так и для дешифрования сообщения*. Этот 56-битовый ключ в тот период обеспечивал исключительную стойкость. В такой системе и отправитель, и получатель обязаны применять защиту шифра от компрометации - хранить ключ в секрете. Распределение таких ключей является существенной проблемой, особенно в том случае, если один и тот же ключ необходим более чем двум абонентам. Двухключевая система шифрования была разработана в качестве ответа на данную проблему. Такая система с открытым ключом позволяет избегать трудностей в распределении ключей – они напечатаны в справочнике для шифровальщика. Секретность обеспечивается вторым ключом – для расшифровывания. В обеих системах криптографии одной из общих проблем является установление подлинности (аутентификация) отправителя или получателя, верности подписей на договоре, переданном на дальнее расстояние. Особенно это актуально в наше время, когда с помощью Интернета многие люди получили доступ к средствам связи. Они должны быть уверены, что люди (абоненты), с которыми они обмениваются информацией, действительно являются теми, за кого себя выдают. Поэтому в современные процедуры по обеспечению безопасности входят цифровые подписи, сертификаты и органы по сертификации. Еще одна из важных обеспечительных мер –

**Риксон Ф.Б.* Коды, шифры, сигналы и тайная передача информации. М.: АСТ, 2011. С. 260

автоматическая генерация случайных ключей для каждого сообщения, которая активно применяется в последнее время для защиты системы «банк – клиент».

При передаче информации по компьютерным сетям недружественные помехи носят более сложный характер и выходят за пределы простого перехвата канала связи и расшифровки передаваемой по нему информации (рис. № 58)*.

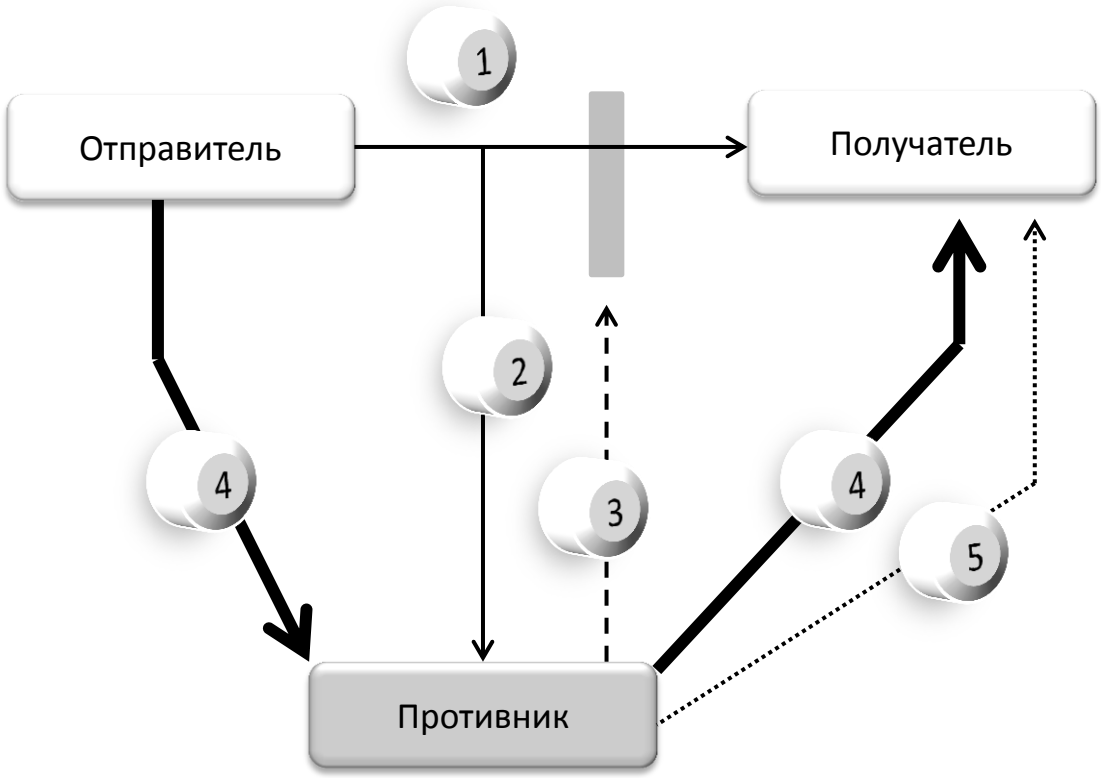

Рис. 53. Классификация помех в виде сетевых атак по Лапониной О.Р.

На изображенном выше рисунке цифрами обозначены следующие режимы передачи информации и типовые сетевые атаки на каналы передачи (связи):

1. Штатный информационный поток между абонентами (отправитель-получатель);
2. Пассивная атака – простой съем информации;
3. Активная атака – отказ в обслуживании (DoS-атака, Denial of Service);
4. Активная атака – модификация потока данных (man in the middle);
5. Активная атака – создание ложного потока данных (фальсификация).

**Лапонина О.Р.* Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. М.: Бином, 2011. С. 14-16

В качестве разновидности сетевых атак также применяется прием, называемый *повторное использование,* что означает пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа (replay – атака).

20.4. Угроза осуществления промышленного шпионажа

Современные рыночные отношения невозможно представить без конкуренции. Известно два ее типа: *добросовестная* и *недобросовестная* конкуренция. Предпосылками появления недобросовестной конкуренции являются жесткие условия существования компании. При этом одним из самых важных факторов успешного ведения бизнеса является наличие актуальной информации. К способам получения информации следует отнести: покупку, сбор из легальных источников, хищение.

С развитием постиндустриальной экономики возрастает и ценность информации как предпринимательского ресурса. Вместе с этим возрастает и опасность завладения со стороны конкурентов секретами производства, управленческими и маркетинговыми разработками, клиентскими базами. Данные виды промышленного шпионажа могут серьезно навредить компании и даже привести ее к краху. В свою очередь, овладение этими секретами предоставляет исключительные преимущества в борьбе за лидерство на рынке. В то же время, являясь инструментом недобросовестной конкуренции, шпионаж заставляет компанию, с одной стороны, принимать меры по защите своих секретов, а с другой – самой заниматься шпионажем, чтобы выжить в рыночной среде. В ряде случаев промышленный шпионаж осуществляется государственными спецслужбами в интересах оказания помощи национальному бизнесу.

Промышленный шпионаж — **это форма недобросовестной конкуренции, базирующаяся на незаконном получении, использовании и разглашении данных, которые составляют коммерческую, служебную или другую охраняемую законом тайну с целью получения преимуществ для осуществления предпринимательской деятельности.** Основным предназначением промышленного шпионажа является экономия средств и времени, которые требуется затратить, чтобы догнать конкурирующую компанию, занимающую лидирующее положение, а также, чтобы расширить свою активность за счет выхода на новые рынки.

История промышленного шпионажа уходит глубоко в древность. Самым известным примером можно назвать раскрытие секретов производства шелка и фарфора в Китае. В свое время промышленный шпионаж стал причиной появления целого комплекса

мер по защите интеллектуальной собственности и изобретения патента (от лат. patens — открытый, ясный, очевидный). Промышленный шпионаж, как любой вид деятельности, имеет объект, предмет, субъектов, адресат и способ совершения (рис. № 54).

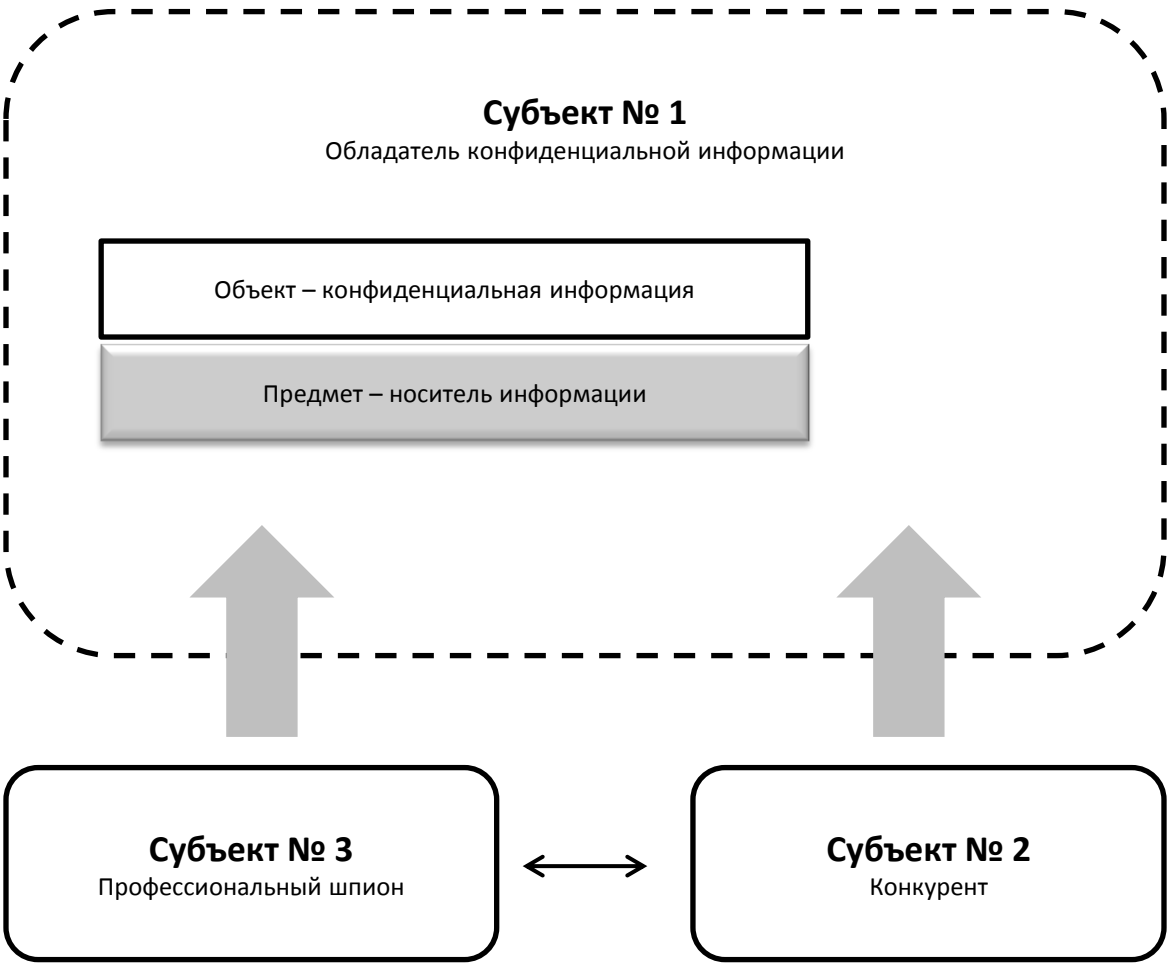

Рис. 54. Принципиальная схема промышленного шпионажа

Объектом промышленного шпионажа является конфиденциальная информация, которая, как правило, содержится в предмете (носителе информации). Информация может быть представлена образцами продукции, инженерными чертежами или схемами на любых известных носителях (включая электронные). Правообладателем информации (субъект № 1), в зависимости от ее вида, может быть государство, уполномоченные органы власти, предприятия и организации, физические лица. Правообладатели хранят информацию в специально определенных местах (адрес хранения) и могут применять меры по защите охраняемой информации от утечки, несанкционированного доступа и разглашения. Конкуренты, уполномоченные государственные органы или профессиональные промышленные шпионы (субъекты №№ 2 и 3) могут принимать меры

для неправомерного завладения чужими производственными или иными секретами. Способы и методы похищения секретов могут быть разными, они зависят от характера самих секретов, предмета и места их хранения, а также от защитных мер.

Из истории известно, что для получения необходимой конфиденциальной информации заинтересованные стороны не гнушались любыми методами, изобретенными человечеством в процессе тайных и явных войн: шантаж; подкуп лица, которое имеет доступ к данным, относящимся к коммерческой, служебной или другой охраняемой законом тайне; незаконный доступ к защищаемой информации с помощью технических средств (прослушивание телефонов, незаконное проникновение в компьютерные сети и т. п.); похищение носителей защищенной информации; внедрение агента в компанию или в страну конкурента с целью получения доступа к информации или продукции, составляющей предмет коммерческой или иной охраняемой законом тайны.

Кейс № 23. Японские будни промышленного шпионажа

В скандалах и конфликтах, связанных с промышленным шпионажем, японские компании долгое время выступали в роли ответчиков. Одним из наиболее известных примеров стало дело 1982 года, когда сотрудники компании Hitachi были обвинены в краже интеллектуальной собственности у корпорации IBM. Однако на современном этапе развития японские компании заняли доминирующие позиции в промышленном производстве, и поэтому чаще всего сегодня именно они выступают в качестве жертв промышленных шпионов. Так, корпорация Sharp, для тщательной охраны собственных технологических разработок, разместила свой суперсовременный завод по производству жидкокристаллических панелей в местечке Камеяма, которое находится в глухой горной местности вдали от посторонних взглядов. Однако и это не защищает гиганта электронной промышленности от шпионажа. Так, в определенный момент тревогу сотрудников Sharp стал вызывать таинственный автомобиль, который примерно раз в месяц объезжает вокруг секретного объекта корпорации. По мнению представителей Sharp, эта подозрительная машина может принадлежать агенту конкурирующей корпорации, которая надеется выведать важные детали чужого ноу-хау. «Утечка технологий из Японии снижает конкурентоспособность страны и приводит к сокращению занятости, – утверждает директор Агентства по защите интеллектуальной собственности при Министерстве экономики, торговли и промышленности Японии (МЭТП) Йосинори Комия, – Мы признаем, что некоторые технологии подлежат передаче за границу; но сейчас часто передаются и те технологии, которые руководители компаний стремятся сохранить в тайне».

По данным МЭТП, большинство корпораций, которые стали жертвами промышленного шпионажа, стремятся сохранить это в тайне и не раздувать скандал, поскольку виновными в этом становятся их собственные сотрудники, а не посторонние агенты. По признанию вице-президент Matsushita Йокио Сотоку, в японском бизнесе до сих пор сохраняются нарушения со стороны «пятой колонны», например со стороны сотрудников, которые работают в конкурирующих компаниях по выходным. Исследования МЭТП также показали, что одним из каналов утечки информации являются бывшие сотрудники японских компаний,

которые устраиваются на работу в других азиатских странах и уносят с собой ноу-хау своих прежних работодателей. Основными путями утечки защищенной информации японских корпораций к конкурентам МЭТП выделила следующие: нарушение партнером-поставщиком соглашения о сохранении тайны; копирование защищенной информации сотрудниками компании в нерабочее время; создание совместной корпорации с зарубежной компанией в условиях недостаточной проработки политики информационной безопасности; работа сотрудников компании по совместительству в конкурирующих компаниях.

Вопрос: сообщите об иных каналах утечки конфиденциальной информации.

Промышленный шпионаж является неотъемлемой составной частью рыночных отношений, как за рубежом, так и у нас в стране. В связи с постоянным развитием технических средств разведки, а также совершенствованием информационных технологий, появляются все новые методы шпионажа и области его применения. Чтобы сохранить свои конкурентные преимущества, предприятию необходимо постоянно совершенствовать систему защиты своей конфиденциальной информации, как в части внедрения современных технических средств и организационных мер противодействия техническим разведкам, так и в части мероприятий кадровой безопасности.

20.5. Угроза нарушения нормальной жизнедеятельности предприятия

В последние годы изобретены и стали быстро распространяться специальные средства, действие которых значительно выходит за рамки реализации отдельных угроз информационной безопасности. Такие средства обладают свойствами существенно влиять через киберпространство на бизнес-процессы компаний, приводя к нарушениям жизнедеятельности предприятий (рис. № 60). Учитывая эту специфику, их стали называть средствами кибернетического воздействия на управление бизнесом, а в ряде случаев – средствами кибернетического нападения.

В настоящее время более 140 стран мира, по оценке экспертов, разрабатывают такие средства. При этом результаты их воздействия на деятельность предприятий и госструктур отличаются экономической эффективностью и скрытностью. Поэтому количество операций по воздействию на бизнес компаний в киберпространстве постоянно растёт. Ежедневно фиксируется более тысячи атак, которые направлены на нарушение работы объектов экономической и государственной инфраструктур разных стран.

Исходя из этого, было сформировано специальное понятие *кибернетические угрозы*, которые представляют собой действия, явления, факторы, условия, являющиеся опасными для инфраструктуры управления, информации управления, порядка управления

и субъектов управления. При этом опасность состоит в возможном нарушении свойств одного или нескольких элементов, что, в конце концов, может привести к нарушению процессов управления и нормальной жизнедеятельности компании.

В сфере кибернетических угроз наблюдается две тенденции. Первая связана с профессиональным созданием мощных вирусных программ, способных парализовать работу крупных предприятий. Вторую тенденцию представляет традиционное мошенничество, связанное с размещением в Интернете заведомо ложной информации, имеющей внешние признаки бизнеса.

По результатам совместного исследования «Лаборатории Касперского» и компании B2B International по киберпреступности за 2014 год, каждая кибератака на сети крупных российских компаний за указанный период наносит финансовый ущерб в среднем на сумму в 695 тыс. долларов. В свою очередь, на сети компаний среднего и малого бизнеса – на сумму около 4 тыс. долларов. Что же касается кибератак в среднем по миру, то для крупных компаний ликвидация последствий обходится в сумму 109 тыс. долларов, для среднего и малого бизнеса – в 13 тыс. долларов.

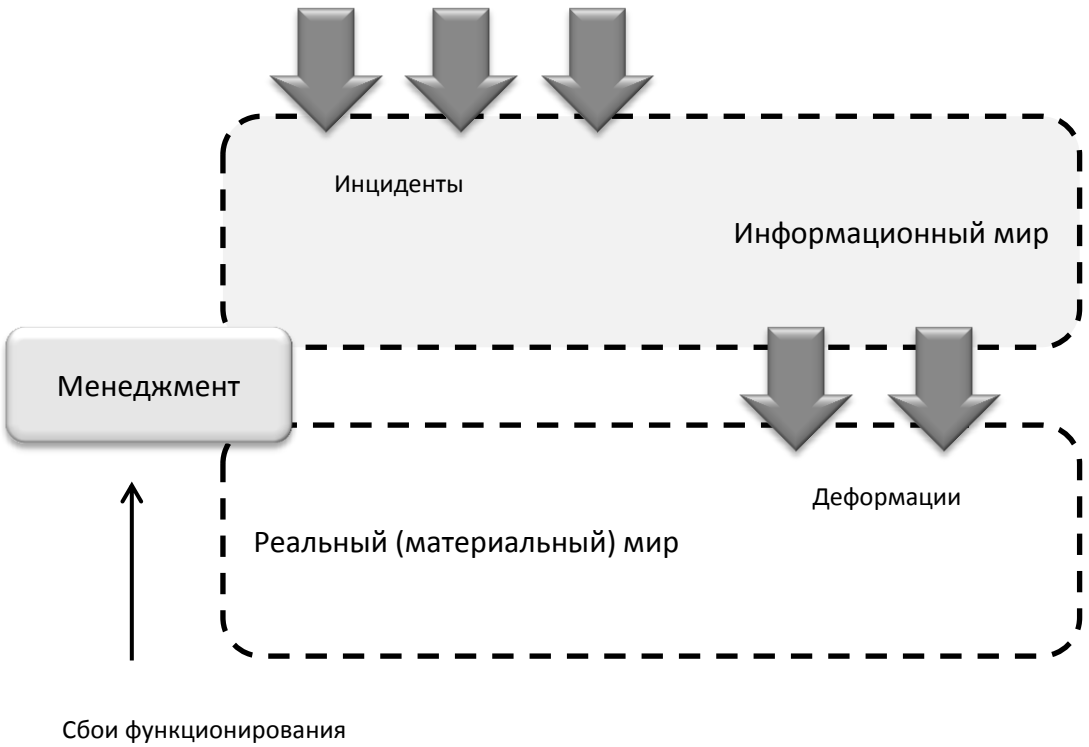

Рис. 55. Деформация бизнеса через инциденты в информационной сфере информационного мира

Согласно результатам отчета «Global Cyber Executive Briefing» для компании «Делойт Туш Томацу Лимитед», обеспечение надежности необходимо начать с изучения слабых сторон прикладных программ и усиления цифровой инфраструктуры. Поэтому компании, которые желают вовремя обнаруживать кибератаки, должны проявлять максимальную бдительность в этом процессе. На основе материалов отчета можно сформулировать основные угрозы для компаний в рассматриваемой области. При этом указанные угрозы могут быть сгруппированы по отраслям производства:

a) Компании, работающие в области высоких технологий, постоянно являются целью кибератак, которые представляют собой угрозы крупнейших потерь интеллектуальной собственности. Кроме того, как показал анализ специфики этих атак, они наиболее подвержены хактивизму. Угрозы для данного класса компаний также зачастую используются как средство атаки и заражения других компаний.

b) Кибератаки на онлайн-медиа компании наиболее часто проводятся с целью нанесения ущерба их репутации. Угрозы также представляет использование первой волны атак как средство для новых атак и заражения других компаний.

c) Телекоммуникационные компании чаще остальных подвергаются сложным с технической точки зрения атакам, числе которых также находятся атаки правительственных агентств, которые используют целенаправленные угрозы с целью установления скрытой слежки на длительный период. Еще одной угрозой в области телекоммуникаций является атака на арендуемое техническое оборудование, одним из которых является домашний маршрутизатор интернет провайдеров.

d) В области электронной коммерции имеют место преимущественно взломы баз данных (то есть потеря данных о клиентах). Чаще всего подвергаются атакам такие уязвимые области, как системы проведения онлайн-платежей с помощью атаки, которая называется вызов ответа системы «Отказ в обслуживании». Данный тип атаки часто используется хактивистами, которые стремятся нарушить работу компании наименее заметным способом.

e) Компании, работающие в области страхового бизнеса, как правило, имеют дело с большим количеством чувствительных данных, которые требуют защиты. К сожалению, данный сектор подвержен частым кибератакам, которые возрастают в геометрической прогрессии. Причиной тому является и переход страховых компаний на цифровые каналы обслуживания. В свою очередь, атаки все более усложняются в техническом плане, комбинируя усовершенствованное вредоносное программное обеспечение и другие технологии, среди которых психологическая атака. В свою очередь, текущие атаки являются краткосрочными, однако в перспективе прогнозируется возможный рост долгосрочных атак, которые еще не привлекают особого внимания.

f) Вектор атак на компании обрабатывающей промышленности в основном склоняется в сторону хакеров и киберпреступников, а также в область корпоративного шпионажа. При этом типы кибератак на указанные компании варьируются от фишинга до использования усовершенствованного вредоносного программного обеспечения и нацелены не только на IT-системы, но и на связанные с ними системы промышленного контроля.

g) В секторе ретейла в современных условиях сложилась ситуация, при которой для преступников и хакеров главной целью стали данные кредитных карт как новой валюты. При этом резко возрастает угроза утечки инсайдерской информации, а это способствует формированию нового типа

преступников, целью которых становится кража информации, в частности ценных данных о держателях карты, которыми обмениваются потребители и ритейлера.

Как свидетельствует практика, основными целями подобных атак являются следующие категории объектов:

1) *Офисы управления компаний*. Часто аппаратура в этих подразделениях слабо защищается от физического повреждения (например, со стороны персонала по уборке или техническому обслуживанию помещений).

2) *Подразделения, работающие в области НИОКР*. Обычно эти структуры требуют наиболее высокого уровня защиты, однако защищаются на уровне других департаментов.

3) *Центры обработки данных*. Эти подразделение представляют собой надежную область для размещения частного облака. Проблема состоит в обеспечении безопасного функционирования многочисленных серверов и приложений, которые работают на них.

4) *Сеть поставщиков*. Из-за расширяющегося применения сетевых решений при работе с поставщиками зачастую возникают риски, связанные с недостаточной защищенностью небольших компаний-поставщиков.

5) *Облачные вычисления и сервисы*. По своей сути использовать внешнее облако безопасно. Проблема возникает на уровне защиты данных, которая зависит от законодательства стран размещения серверов, при этом возникает угроза доступа со стороны спецслужб.

6) *Производство*. Объединение старых специализированных систем в сети вызывают проблему отслеживания и контроля их работы. В свою очередь, атаки злоумышленников могут привести к производственным потерям или даже к краху компании.

7) *Базы данных* обеспечивают безопасное хранение важной информации, в свою очередь, в качестве «инструментов» для проникновения в базы данных взломщики могут использовать самих администраторов этих баз.

8) *Конечная продукция* активизируется с помощью информационных технологий, что облегчает проведение кибератак. В свою очередь, дистанционный контроль устройства пользователей с целью провоцирования поломок, может быть использован хакерами как возможность незаконного доступа к конфиденциальной информации. В результате компании могут потерять репутацию и получить иски от пользователей, которые станут жертвами мошенничества.

9) *Офисные сети* предусматривают объединение всех систем компании в единую систему, что дает возможность хакерам богатые возможности при условии проникновения в сеть.

10) *Продажи*. Утечка данных о ценах, клиентской базе и маркетинговых планов вызовет подрыв репутации компании, и лишить ее конкурентных преимуществ.

11) *Мобильные устройства*. Современные смартфоны являются доступным средством для получения хакерами конфиденциальных данных с их карты памяти. Поэтому сотрудникам компании для решения производственных задач или для управления бизнес-процессами не стоит использовать собственные мобильные устройства.

12) *Интернет-магазины*. В последние годы хакеры часто используют личные данные клиентов или их реквизиты кредитных карт для незаконного доступа под видом реально существующих покупателей и совершения мошеннических действий.

13) Телефонные звонки. Злоумышленники могут использовать телефонные звонки как способ легкого получения нужной информации, используя готовность людей помогать друг другу.

Таким образом, с изменением среды ведения бизнеса переходом его в область мобильных устройств и технологий с виртуализацией вычислений и облачных технологии, при одновременном использовании совместной работы многих пользователей, происходит количественная и качественная трансформация угроз процессам управления бизнесом. При этом, как показывают исследования консалтинговой компании в области экспертизы информационной безопасности «NSS LABS», можно выделить следующие основные направления их эволюции:

- Создаваемые вирусы для кибератак намного эффективнее лучших антивирусов и WEB-шлюзы, которые иногда не могут им противостоять;
- Современные вредоносные программы и шпионское ПО воруют не только ссылки на посещаемые сайты, но и реквизиты доступа к ним;
- WEB и социальные сети часто являются рассадниками вредоносных программ и инструментом разведки злоумышленников;
- Для своих действий вредоносные программы используют неизвестные уязвимости.

Одновремено с этим происходит эволюция тактики реализации киберугроз:

- В первую очередь – это использование массового заражения объектов нападения. Причем злоумышленников не интересует известность и слава – им нужна финансовая выгода от реализации угроз.
- Все больший вес начинает приобретать полиморфизм угроз – современные угрозы постоянно меняются, чтобы не дать возможности средствам защиты отследить их изменение поведения, адреса серверов управления и т.д.
- В большинстве случаев фокус делается на конкретную жертву, т.е. угрозы разрабатываются специально под атаку на объект, учитывая его инфраструктуру и встраиваясь в него, что делает невозможным применение специальных методов анализа.
- Для реализации угроз широко используются передовые и тайные средства (типа Advanced Persistent Threat). При этом угрозы становятся модульными, самовосстанавливающимися, устойчивыми к отказам и обнаружениям.

Однако угрозу представляют не только программные вирусы и вредоносное программное обеспечение (ПО), но и намеренно модифицируемые в процессе производства микросхемы, на которые также возможны кибератаки. Практически любой современный чип может хранить множество скрытых внутренних функций, к которым у пользователей нет прямого доступа. Хорошо спланированная кибератака может спровоцировать экономический коллапс, парализовав собой важнейшие структуры армии или правительства.

Кейс № 24. Необдуманные действия сотрудника

Клиника Stalwart (США) была основана в 1909 г. С 1956 г. она стала универсальным лечебным заведением и стала специализироваться на лечении пороков сердца. В последние годы она входила в список 100 лучших клиник США, занимающихся лечением сердечно-сосудистых заболеваний. Ее врачи каждый год делали до 800 операций на открытом сердце и более 9 000 катеризаций сердца*.

Однажды утром, сотрудник регистратуры отделения интенсивной терапии Шин Макрэй приехал на работу и рядом со своим автомобилем обнаружил броскую серебристую карту памяти USB, которую он подобрал и положил в карман. Перед завершением смены Макрэй освободился от текучки и вспомнил о «флэшке». Вставив устройство в гнездо своего служебного компьютера, сотрудник просмотрел карту памяти. В ней не было ничего необычного – несколько графических таблиц и файлов со статистическими отчетами. Просмотрев карту, Макрэй вынул ее из компьютера и выбросил в мусорное ведро. Сорок восемь часов спустя клиника была «поставлена на колени» вредоносным вирусом. Электронные истории болезней стали недоступными, пациентов срочно переправили в ближайшие клиники. Администрация пригласила внешнего консультанта, приняла меры для установления причин инцидента и обеспечила сохранность улик (приняв меры физической защиты всех компьютеров). По результатам экспресс анализа клиника обратилась в группу по борьбе с компьютерной преступностью ФБР (NCCS FBI). В это время хакер по имени Энтони Бэйкер с гордостью смотрел передачу телевизионного канала CNN о результатах своей атаки на клинику. Как показало следствие, преступник гордился своей изобретательностью в части выбора способа совершения атаки. Однако через 11 месяцев окружной суд вынес приговор по его делу.

Вопросы:

1. Оцените действия сотрудника клиники Шина Макрэя;
2. Сообщите свое мнение о действиях администрации клиники по факту выявленного инцидента в компьютерной сети.

В современном мире доминирующими в области компьютерных технологий являются ведущие корпорации США, а основной архитектурной линией в проектировании современных ключевых микропроцессорных компонентов служит архитектура x86, которая продвигается корпорациями, такими как «Intel», «AMD» и другими. В свою очередь, правительство США рассматривают доминирующее положение американских корпораций на мировом рынке микропроцессорной техники как важнейший фактор, который обеспечивает стратегическое превосходство и позволяет при необходимости оказывать экономическое, политическое и военное давление на другие мировые страны.

Глобализация приводит к социально-политической и экономической прозрачности государств, размыванию барьеров между странами. Глобальная безопасность связана с миграцией не только населения (человеческого капитала), но и финансового капитала,

*Компьютерное мошенничество. *Под редакцией Дж.Т. Уэллса.* М.: Маросейка, 2010. С. 25-32

созданием новых его центров. В этих условиях выживают и развиваются организации, в максимальной степени использующие возможности быстрых перемен для укрепления собственной безопасности. При этом необходимо учитывать, что наиболее полную информацию об угрозах и рисках имеют руководители, непосредственно работающие на местах, в городе или регионе. Они же располагают оперативными возможностями для последовательной минимизации рисков и устранения угроз. В результате выигрывают организации, которые обеспечивают максимальное использование возможностей своих сотрудников на местах для повышения безопасности в условиях быстрых перемен. Для этого применяются прогрессивные адаптивные механизмы безопасности, разработкой которых занимаются исследователи.

Вопросы и задания для самоконтроля

1. Дайте определение понятия «информационная безопасность».
2. Дайте определение понятия «промышленный шпионаж».
3. Сообщите об основных угрозах в области защиты охраняемой информации от несанкционированного доступа.
4. Расскажите об основных угрозах в сфере защиты вычислительных систем, сетей и телекоммуникаций.
5. Сообщите о возможных угрозах совершения уголовно наказуемых деяний в сфере информационной безопасности предприятия.

Глава 21. Защита персональных данных

В результате изучения главы студент должен **знать** какие сведения отнесены к персональным данным; историю и современное состояние защиты персональных данных в Российской Федерации и за рубежом; **уметь** определять обязанности предприятия по защите персональных данных своих работников, клиентов и контрагентов; **владеть** практической информацией об уполномоченных государственных органах и мерах по привлечению к ответственности за нарушение правил защиты персональных данных.

21.1. Право личности на защиту персональных данных

К конфиденциальной информации, доступ к которой ограничен действующим законодательством, относятся и персональные данные. *Персональные данные* – **это любые данные, которые относятся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).**

Они включают фамилию, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другую информацию о лице.

В данной области деятельности существуют следующие понятия:

- *Оператор* - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующего и (или) осуществляющего обработку персональных данных, а также определяющего цели обработки персональных данных, которые подлежат обработке, действия (операции), совершаемые с персональными данными;
- *Обработка персональных данных* - любое действие или операция, либо совокупность действий или операций, которые совершаются при использовании средств автоматизации или без использования подобных средств с персональными данными, включая запись, сбор, хранение, систематизацию, уточнение накопление (обновление, изменение), использование, извлечение, передачу (распространение, предоставление, доступ), блокирование, обезличивание, удаление, уничтожение персональных данных;
- *Автоматизированная обработка персональных данных* - обработку персональных данных с помощью средств вычислительной техники;
- *Распространение персональных данных* - действия, которые направлены на раскрытие персональных данных неопределенному кругу лиц;
- *Предоставление персональных данных* - действия, которые направлены на раскрытие персональных данных определенному лицу;
- *Блокирование персональных данных* - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Не допускается обработка специальных категорий персональных данных, которые касаются политических взглядов, расовой или национальной принадлежности, состояния здоровья, религиозных или философских убеждений, интимной жизни, за исключением специально предусмотренных случаев законодательством. Субъект имеет право дать согласие оператору на обработку его персональных данных, может отказать в предоставлении этих данных или отозвать ранее представленные данные (рис. № 56).

Субъект также вправе официально запросить у оператора:

- Подтверждение факта обработки персональных данных;
- Предоставить цели и правовые основания обработки персональных данных;
- Раскрыть цели и способы обработки персональных данных, применяемых оператором;
- Назвать место нахождения и наименование оператора, а также предоставить сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым они могут быть раскрыты, основываясь на договор с оператором или федеральный закон;
- Назвать наименование или персональные данные (фамилия, имя, отчество и адрес) оператора, который осуществляет обработку персональных данных;

- Охарактеризовать порядок осуществления субъектом персональных данных прав, который предусмотренный настоящим федеральным законом;
- Предоставить информацию об осуществленной или о предполагаемой трансграничной передаче персональных данных;
- Назвать сроки обработки персональных данных, в том числе и сроки их хранения;
- Перечислить обрабатываемые персональные данные, которые относятся к соответствующему субъекту персональных данных и источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
- Иные сведения, предусмотренные настоящим федеральным законом или другими федеральными законами.

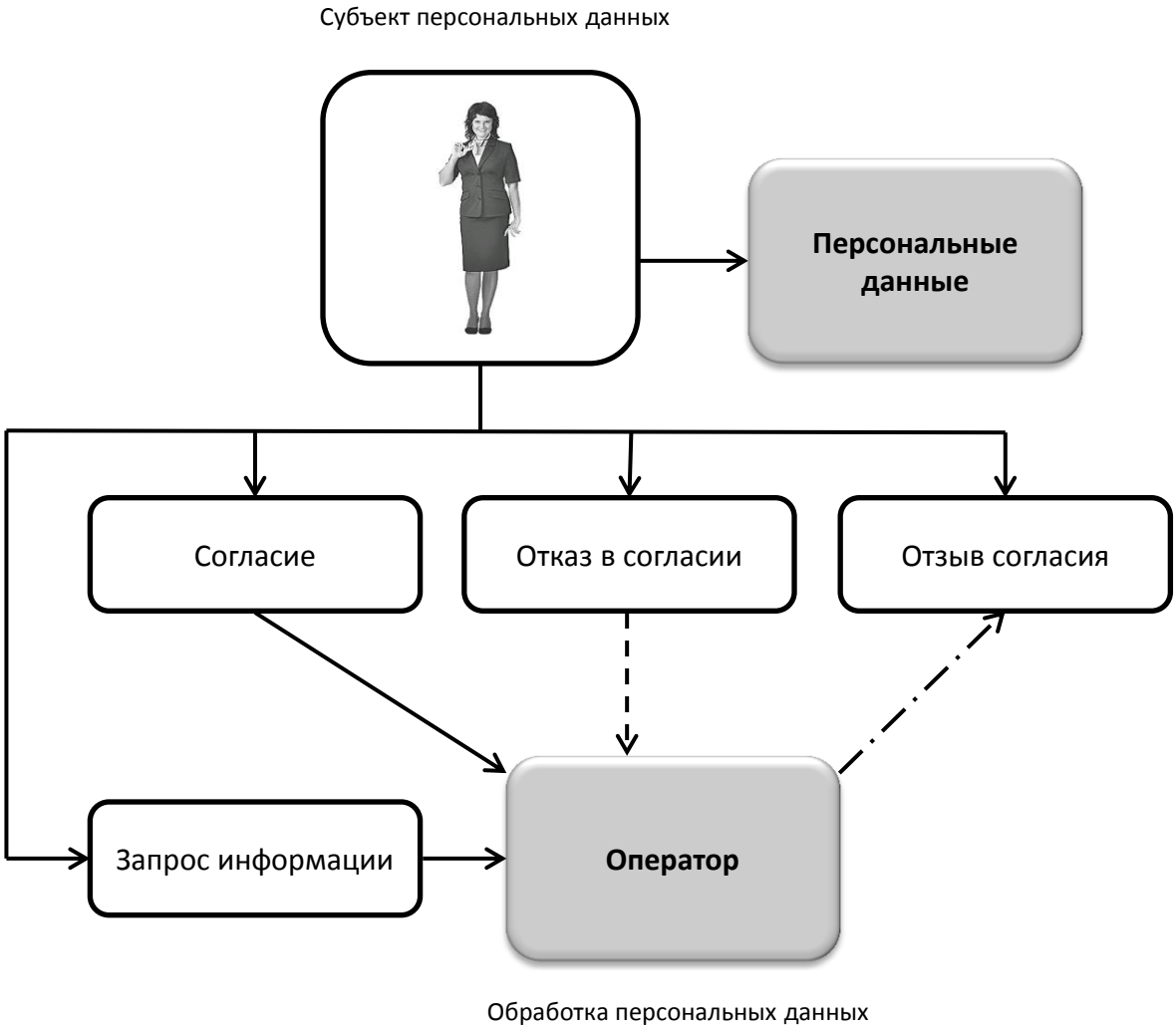

Рис. 56. Права субъекта персональных данных

При обработке персональных данных оператор обязан руководствоваться рядом принципов. В частности, оператор обязан придерживаться принципа законность целей и способов обработки персональных данных, добросовестность. Цели обработки

персональных данных должны соответствовать целям, которые заранее определены и заявлены при сборе персональных данных, а также полномочиям оператора. Объем и характер обрабатываемых персональных данных, способы обработки персональных данных должны соответствовать целям обработки персональных данных. Оператор должен обеспечить достоверность персональных данных, их достаточность для целей обработки, недопустимость обработки персональных данных, избыточных по отношению к целям, которые заявлены при сборе персональных данных. Кроме этого, оператор должен понимать недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных. Хранение персональных данных осуществляется в форме, которая позволяет определять субъект персональных данных в короткие сроки, при этом по истечению сроков хранения персональные данные подлежат уничтожению.

В свою очередь, операторы и третьи лица, которые получили доступ к персональным данным, должна обеспечивать конфиденциальность этих данных, за исключением следующих случаев:

- Обезличивание персональных данных;
- Общедоступность персональных данных.

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных при условии письменного согласия субъекта персональных данных могут быть включены фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные субъекта. Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных законодательством.

21.3. Система защиты персональных данных в Российской Федерации

Федеральное законодательство по вопросам защиты персональных данных действует в нашей стране с 2005 г. после ратификации соответствующей конвенции Совета Европы*. Закон устанавливает основные принципы обработки персональных данных:

1) Обработка персональных данных осуществляется на законной и справедливой основе;
2) Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, которые несовместимы с целями сбора персональных данных;
3) Не допускается объединение баз данных, которые содержат персональные данные и обработка которых возможна только в целях, несовместимых между собой;
4) Допускается обработка только тех персональных данных, которые отвечают ее целям;
5) Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
6) При обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры по удалению или уточнению неполных или неточных данных;
7) Хранения персональных данных обеспечивается в форме, которая позволит определить субъект персональных данных, однако не дольше сроков, установленных целями обработки персональных данных. По достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом, обрабатываемые персональные данные подлежат уничтожению либо обезличиванию.

С учетом требований трудового законодательства работодатель может обрабатывать только те персональные данные сотрудников, которые необходимы в связи с трудовыми отношениями и смежными с ними отношениями (например, по социальному и медицинскому страхованию, пенсионному обеспечению, допуску к секретам). Целями обработки для работодателя могут служить исключительно:

- Обеспечение соблюдения законодательства;
- Содействие работникам в трудоустройстве;
- Содействие в обучении и продвижении по службе;
- Обеспечение личной безопасности работников;
- Контроль количества и качества выполняемой работы;
- Обеспечения сохранности имущества.

**Горохова Д.И.* Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. Журнал «Национальная безопасность/nota bene» № 1. М.: 2013. С 165-170

По общему правилу обработка персональных данных (включая их получение) может осуществляться только с согласия субъекта персональных данных (работника). Закон устанавливает обязательные требования к содержанию письменного согласия субъекта персональных данных на их обработку. Оператор (работодатель) должен обеспечить конфиденциальность персональных данных в соответствии с требованиями безопасности и условиями хранения, которые устанавливаются Правительством России. Исключение составляют только обезличенные и общедоступные персональные данные.

Закон разрешает в целях информационного обеспечения создание общедоступных источников персональных данных (справочников, телефонных и адресных книг). В такие источники с письменного согласия субъекта персональных данных может включаться фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных. При этом такие сведения могут быть исключены из общедоступных источников по требованию субъекта персональных данных. Закон вводит специальные категории персональных данных, обработка которых по общему правилу не допускается. К таким категориям отнесены сведения, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Обработка таких данных допускается только с согласия субъекта персональных данных или в случаях, предусмотренных законом.

Уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). В данной данном органе исполнительной власти для выполнения названных функций создано подразделение по защите прав субъектов персональных данных. Надзор и контроль соблюдения установленных требований безопасности при обработке персональных данных осуществляет ФСБ России.

В 2008 г. были выпущены методические документы Роскомнадзора:

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»,
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»,
- «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных».

Имеются также методические документы ФСБ России:

- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации».

Роскомнадзор в своей деятельности по защите прав субъектов персональных данных реализует ряд основных полномочий. В частности, он вправе запрашивать и безвозмездно получать требуемую информацию у юридических и физических лиц; осуществлять проверки собственными силами или с привлечением других органов; требовать от оператора выполнения предусмотренных законом действий; принимать меры по приостановлению или прекращению обработки персональных данных; обращаться в суд с исковыми заявлениями в защиту прав неопределенного числа лиц; направлять заявление в регулирующий орган оператора о приостановлении или отзыве лицензии; направлять в правоохранительные органы материалы для возбуждения уголовных дел; вносить предложения в Правительство Российской Федерации; привлекать виновных лиц к административной ответственности.

21.3. Защита персональных данных на предприятии

Эксперты в области защиты информации выделяют следующие основные этапы построения системы обеспечения безопасности персональных данных на предприятии. На **первом этапе** издаётся нормативный документ об организации работ по созданию системы защиты персональных данных в компании. В данном приказе (распоряжении) содержатся следующие позиции:

- Назначается ответственный сотрудник компании за осуществление мероприятий, направленных на защиту персональных данных;
- Дается указание о разработке локальной документации, которая имеет отношение к защите персональных данных;
- Создается комиссии по контролю за обработкой персональных данных;
- Утверждается и вводится в действие положение по защите и обработке персональных данных в компании.

На **втором этапе** проводится обследование и аудит информационных систем персональных данных компании. Целью данного этапа является определение статуса

компании и принятия решения относительно предоставления ей полномочий оператора обработки персональных данных. После этого проводится процедура определения класса информационной системы персональных данных в компании. В результате реализации данного этапа должны быть разработаны и утверждены следующие документы:

- Приказ (распоряжение) о создании комиссии по классификации информационных систем персональных данных;
- Отчет об обследовании информационных систем персональных данных;
- Акт классификации типовой информационной системы персональных данных;
- Положению о защите и обработке персональных данных в организации:
- Примерная модель угроз безопасности данных, обрабатываемых в информационных системах персональных данных.

Третий этап предполагает направление уведомления об обработке (или о намерении осуществить обработку) персональных данных в территориальное подразделение Роскомнадзора. **Четвертый этап** целесообразно отвести под разработку, утверждение и применение следующих документов: «Согласие на обработку персональных данных» и «Отзыв согласия на обработку персональных данных».

Пятый этап – это начало непосредственного внедрения системы защиты персональных данных. В организационном плане этот этап обязательно включает в себя следующие основные мероприятия:

- Перечня лиц, которые будут допущены к обработке персональных данных; составление и утверждение
- Создание и утверждение перечень персональных данных, которые обрабатываются в компании;
- Создание и утверждение положение об обработке и защите персональных данных в организации, а также типового обязательства об обеспечении конфиденциальности персональных данных сотрудниками предприятия;
- Создание и утверждение описания системы защиты персональных данных при их обработке в информационных системах организации. К Описанию обычно прикрепляют: «Инструкцию пользователя по соблюдению режима защиты информации при работе в информационных системах персональных данных»; «Инструкцию администратора безопасности информационных систем персональных данных организации»; «Инструкцию по резервному копированию и восстановлению данных в информационных системах персональных данных предприятия»; «Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных в организации».

На **шестом этапе** требуется определить технические средства защиты персональных данных.

На заключительном **седьмом этапе** разрабатывается и утверждается заключение о соответствии системы защиты персональных данных, обрабатываемых в информационных системах организации предъявляемым требованиям.

21.4. Ответственность за нарушение правил защиты персональных данных

Ответственность за нарушение правил защиты персональных данных в Российской Федерации установлена нормами действующего законодательства.

Согласно требованиям трудового законодательства лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, привлекаются к материальной и дисциплинарной ответственности в порядке, который установлен кодексом и иными федеральными законами, а также привлекаются к административной, гражданско-правовой и уголовной ответственности в порядке, который установлен федеральными законами. Согласно действующему законодательству об административных правонарушениях, нарушение установленного законом порядка сбора, хранения, использования или распространения данных о гражданах и их персональных данных, влечет предупреждение или наложение административного штрафа на граждан в размере от 300 до 500 рублей, на должностных лиц - от 500 до 1 тысячи рублей, на юридических лиц - от 5 до 10 тысяч рублей.

Уголовным законодательством предусмотрена ответственность *за нарушение неприкосновенности приватной жизни*, которая выражается в незаконном собирании или распространении сведений про приватную жизнь лица, составляющих его личную или семейную тайну, без его согласия либо распространении этих сведений публично. Ответственность также предусмотрена при *неправомерном отказе должностного лица в предоставлении собранных в установленном порядке документов и материалов, которые непосредственно затрагивают права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан*. Данный состав преступления предусматривает наказание в виде штрафа, либо в форме лишения права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет.

Ответственность также наступает за *неправомерный доступ к охраняемой законом компьютерной информации*, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло

уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Кейс № 25. Вопросы защиты персональных данных в судебной практике

В 2012 г. Ярославский областной суд вынес апелляционное определение по жалобам коммерческого банка «Юниаструм Банк» и коллекторского агентства «Морган энд Страут» на решение Фрунзенского районного суда г. Ярославля*. Суд первой инстанции признал незаконным действия банка по передаче персональных данных гражданина «Григорьева» коллекторскому агентству «Морган энд Стаут», обязал коллектора уничтожить персональные данные истца, взыскал с банка и коллектора денежные средства в целях возмещения морального ущерба, нанесенного гражданину «Григорьеву». В апелляционной жалобе «Юниаструм банк» поставил вопрос об отмене решения районного суда и направлении дела на новое рассмотрение.

Ярославский областной суд, рассмотрев апелляционные жалобы банка и коллекторского агентства на решение Фрунзенского районного суда г. Ярославля, в удовлетворении жалобы отказал. Областной суд исходил из того, что банк предоставил «Григорьеву» потребительский кредит на основании соответствующего договора. В связи с тем, что клиент перестал регулярно выполнять свои обязательства по кредитному договору, банк передал его персональные данные в коллекторское агентство для организации взыскания задолженности. При этом в кредитном договоре не было прописано условие о передаче персональных данных заемщика третьему лицу в случае ненадлежащего исполнения им своих обязанностей по данному договору. Банк также не запросил согласие «Григорьева» на передачу его персональных данных, а осуществил передачу самостоятельно. При этом судом также установлено, что передача прав требования от банка «Морган энд Страут» не было оформлено в порядке, предусмотренном законодательством.

Вопрос: каким образом, по вашему мнению, банк мог избежать нарушения законодательства.

Вопросы и задания для самоконтроля

Расскажите об основных конституционных правах личности в нашей стране.
Дайте определение понятия «персональные данные».
Сообщите об основных стандартах защиты персональных данных в Российской Федерации.
Расскажите об основных сферах и задачах защиты персональных данных на предприятии.
Сообщите об ответственности юридических и физических лиц за совершение правонарушений в сфере защиты персональных данных.

Глава 22. Защита конфиденциальной информации

*Ярославский областной суд. Апелляционное определение от 05.03.2012 г. по делу № 33-939/2012. Информационный ресурс www/consultant.ru (дата обращения 02.02.2015).

В результате изучения главы студент должен **знать** существующую в нашей стране систему защиты конфиденциальной информации, получит сведения об их взаимных правах и обязанностях субъектов права, а также об ответственности за получение незаконного доступа к защищаемой информации; **уметь** распознавать виды конфиденциальной информации (коммерческая тайна, налоговая тайна, банковская тайна, ведомственная тайна) и особенности их защиты; **владеть** основными методами защиты информации в зависимости от ее особенностей.

22.1. Система защиты конфиденциальной информации в Российской Федерации

В современных условиях развития рыночных отношений все большую значимость приобретают вопросы защиты конфиденциальной информации. Однако существующие нормативные акты правового регулирования в сфере защиты информации требуют дальнейшей разработки, а поэтому создают определенные сложности для компаний, которые стремятся создать собственную систему защиты конфиденциальной информации.

Данные специализированных изданий показывают, что Российские государственные и коммерческие компании осознают всю тяжесть отрицательных последствий разглашения конфиденциальной информации. Среди них: прямые финансовые убытки (46%), удар по репутации (42,3%) и потеря клиентов (36,9%). По мнению специалистов, утрата 20% информации, которые составляют коммерческую тайну, в 60% случаях из 100% может привести к банкротству компании. В случае же утраты конфиденциальной информации в результате шпионажа конкурентов, составляют 30% от ущерба в мировой банковской системе.

В нашей стране **конфиденциальной считается информация ограниченного доступа, признанная такой в соответствии с законодательством, разглашение (утечка) которой могут нанести ущерб охраняемым интересам личности, предприятия (организации), общества или государства.** К такой информации относятся сведения, являющиеся персональными данными, коммерческой (банковской) и налоговой тайной, служебной и государственной тайной (рис. № 57).

Как следует из рисунка, только физические лица на правах собственности обладают персональными данными, могут также обладать сведениями, составляющими банковскую и налоговую тайну, в части их касающейся. Учреждения и организации, вне зависимости от формы собственности и организационной структуры, являются правообладателями сведений, составляющих банковскую, коммерческую, налоговую и служебную тайну.

Рис. 57. Виды конфиденциальной информации (сокращения: У – учреждения, П – предприятия, Г – государство)

Такими же правами обладают и предприятия, вне зависимости от формы собственности и организационно-правовой формы. Специальными субъектами, обязанными обеспечивать сохранность налоговой тайны, являются налоговые и правоохранительные органы. Сведения, составляющие государственную тайну, относятся к исключительной компетенции государства. В соответствии с действующим законодательством определены полномочия физических и юридических лиц по правилам допуска и работы со сведениями, правообладателями которых они не являются. Все эти данные отнесены к информации, защита которой осуществляется на основании и в соответствии с нормами права.

В российском законодательстве определено содержание указанной информации, нормативные акты, определяющие работу с ней, а также виды ответственности за её разглашение. В определенном смысле совокупность сведений, представленных в указанной таблице, образуют вербальную модель системы защиты конфиденциальной информации в РФ, которой необходимо руководствоваться при организации системы защиты информации на предприятии. При этом крайне важно использовать принципы системного подхода, максимально учитывая все виды конфиденциальной информации. В свою очередь создание и внедрение такой системы будет подразумевать реализацию ряда ограничений – так называемых режимных мер, принимаемых владельцем информации. Комплекс таких мер должен, как минимум, включать следующие виды мероприятий:

- Комплексную организацию мероприятий относительно определения порядка доступа сотрудников компании к защищаемой информации и определения меры ответственности при ее утере (разглашении);
- Техническую защиту и оборудование помещений для работы с данными, доступ к которым может иметь лишь ограниченный круг лиц;
- Организацию специального делопроизводства;
- Защиту данных, которые обрабатываются техническими средствами, представленными в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптико-магнитной и иной основе.

В свою очередь, лишь защита данных, которые обрабатываются техническими средствами, определяется нормативно-методическим документом «Специальные требования и рекомендации по технической защите конфиденциальной информации», который утвержден в установленном порядке. Его требования, в свою очередь, носят лишь рекомендательный характер при проведении работ относительно защиты негосударственных информационных ресурсов, которые составляют коммерческую тайну, банковскую тайну и др. В данном документе рассмотрена система защиты данных только применительно к техническим каналам утечки конфиденциальной информации. При этом подчеркивается необходимость разработки соответствующей разрешительной системы доступа сотрудников к сведениям ограниченного доступа.

Разработанное в компании *положение о защите конфиденциальной информации* позволит организовать систему мер по защите информации, не подлежащей разглашению. В положении должны быть определены принципы формирования перечня сведений, которые содержат конфиденциальную информацию компании. Законодательно также определены сведения, которые не могут быть отнесены к конфиденциальным.

Данный перечень составляется специалистами всех подразделений предприятия с привлечением юристов и специалистов по защите информации и режимным мерам. В положении о защите конфиденциальной информации должен определяться порядок допуска должностных лиц к конфиденциальным данным и их обязанности, порядок проведения совещаний с использованием вопросов, которые содержат конфиденциальную информацию, порядок присвоения грифа конфиденциальности, требования к помещениям, которые предназначены для работы с носителями конфиденциальной информации. Статья 10 Федерального закона «О коммерческой тайне» также рекомендуется закрепить в данном положении следующие меры по обеспечению конфиденциальности данных:

- Регулирование отношений по использованию информации, которые составляют коммерческую тайну, сотрудниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- Нанесение на материальные носители, которые содержат данные, относящиеся к коммерческой тайне, соответствующего грифа с указанием обладателя этих данных (для юридических лиц следует указывать полное наименование и адрес, для индивидуальных предпринимателей – фамилию, имя, отчество гражданина и его место жительства).

Система защиты конфиденциальных данных в компании всегда должна строиться от реальных и потенциальных угроз, также как и в других областях обеспечения корпоративной безопасности.

22.2. Коммерческая тайна

В соответствии с нормами гражданского законодательства России, коммерческая тайна включена в число объектов интеллектуальной собственности как секрет производства (ноу-хау). Действующее законодательство определяет:

- *Коммерческую тайну* как режим конфиденциальности данных, при котором позволяется ее владельцу при существующих или возможных обстоятельствах увеличивать доходы, избегать неоправданных расходов, сохранять положение на рынке товаров, услуг или работ, получать иную коммерческую выгоду;

- *Информацию, которая составляет коммерческую тайну (секрет производства),* как данные всякого характера (производственные, экономические, технические, организационные), в том числе результаты интеллектуальной деятельности в научно-технической сфере; данные про способы осуществления профессиональной деятельности, которые носят потенциальную или действительную коммерческую ценность по причине неизвестности е третьим лицам, не имеющим свободного доступа к ней на законном основании и в отношении которых действует режим коммерческой тайны;

- *Обладателя информации, которая составляет коммерческую тайну*, как лицо, владеющее данными, которые составляют коммерческую тайну, на законном основании, ограничившее доступ к этим данным, а также установившее в отношении нее режим коммерческой тайны;
- *Доступ к информации, которая составляет коммерческую тайну*, как возможность ознакомления определенными лицами с этими данными с согласия ее владельца или на ином законном основании при условии сохранения конфиденциальности этих данных;
- *Передачу информации, которая составляет коммерческую тайну*, как возможность передачи этих данных, которые зафиксированы на материальном носителе, ее владельцем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, в том числе включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

При этом лишь обладатель информации (предприятие, организация), которая относится к коммерческой тайне, имеет право на отнесение этих данных к данным, составляющим коммерческую тайну, и на определение перечня и состава таких данных.

В законодательстве о коммерческой тайне дается перечень информации, которая относится к коммерческой тайне. Поэтому фирмы, как правило, ограничивают доступ ещё к двум видам информации, выделяя их в отдельные блоки. Сведения о частной жизни работников (местожительство, семейное положение, другая частная информация) охраняются Конституцией Российской Федерации, а правила распространения таких сведений очень жестко прописаны в действующем Трудовом кодексе. Предприятия должны соблюдать неприкосновенность частной жизни, так как, в противном случае, её работники, разгласившие указанную информацию, несут уголовную ответственность. Кроме того, многие виды информации, хотя и не могут составлять коммерческую тайну предприятия, тем не менее, не могут свободно распространяться без ущерба для предприятия. Поэтому такие сведения открыты для фискальных органов, контрольных и надзорных организаций, но имеют ограниченный характер распространения для всех остальных возможных потребителей информации.

В соответствии с действующим законодательством нельзя относить к коммерческой тайне сведения, которые содержатся:

- В учредительных документах юридического лица и документах, которые подтверждают факт внесения записей об индивидуальных предпринимателях и о юридических лицах в соответствующие государственные реестры;
- В документах, которые дают право на осуществление предпринимательской деятельности;
- В документах о составе имущества государственной или муниципальной унитарной организации, государственного учреждения и об использовании ими средств соответствующих бюджетов;

- В документах о загрязнении окружающей среды, состоянии санитарно-эпидемиологической, противопожарной безопасности и радиационной обстановке, безопасности пищевых продуктов и других факторах, которые оказывают негативное воздействие на обеспечение безопасности каждого гражданина, безопасного функционирования производственных объектов и безопасности населения в целом;
- В документах о составе и численности работников, об условиях труда, в том числе об охране труда, о системе оплаты труда, о наличии свободных рабочих мест, о показателях производственного травматизма и профессиональной заболеваемости;
- В документах о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;
- В документах о нарушениях законодательства РФ и фактах привлечения к ответственности за совершение этих нарушений;
- В документах про условия аукционов или конкурсов по приватизации объектов государственной или муниципальной собственности.

Рис. 58. Порядок допуска работников к конфиденциальной информации

Эффективная организация работы по защите коммерческих данных на предприятии предполагает разработку и утверждение положения о коммерческую тайну. Это положение (иные нормативные документы) должно основывается на действующем законодательстве, и отражать специфику данного субъекта предпринимательства; содержать перечень данных, которые составляют коммерческую тайну; предусматривать степень конфиденциальности данных, порядок доступа к данным и круг сотрудников компании, которые имеют доступ к данным определенной степени конфиденциальности.

Защита коммерческой тайны как части деятельности по обеспечению безопасности предпринимательства предусматривает, что возможные противозаконные посягательства на коммерческие данные могут иметь различную направленность. Поэтому эффективный механизм защиты предполагает:

- Правовое обеспечение коммерческой тайны;
- Внедрение организационной защиты;
- Осуществление инженерно-технической защиты;
- Мотивацию сотрудников, от поведения которых зависит утечка информации;
- Ответственность за разглашение конфиденциальных сведений.

Разные страны мира выделяют собственные приоритетные меры защиты коммерческих данных. В Российской Федерации отдается предпочтение следующим способам защиты данных:

- Законодательная защита, основанная на соблюдении тех прав предпринимателя на конфиденциальные данные, которые закреплены в законодательстве. При нарушении прав предпринимателя как пользователя, владельца или собственника данных он может обратиться в соответствующие государственные органы с целью возмещения убытков и восстановления нарушенных прав;
- Физическая защита, включающая охрану, пропускной режим в компании, использование закрывающихся сейфов, специальные карточки для посторонних;
- Организационная защита**,** включающая:
    a. создания службы или введение должности, которые будут ответственны за отнесение определенных данных к категории конфиденциальных и соблюдение правил доступа и использования этих данных;
    b. разделение данных по степени конфиденциальности и организация допуска к конфиденциальным данным только в соответствии с разрешения руководства или должностью;
    c. соблюдение установленных правил пользования данными; а также наличие постоянно действующей системы контроля по соблюдению правил доступа и пользования данными (при этом контроль может быть документальный, визуальный и т.п.);

- Техническая защита, предусматривающая использование таких средств зашиты и контроля, как видеокамеры, сигнализирующие устройства, средства идентификации, микрофоны, а также программные средства защиты компьютерных систем от несанкционированного доступа;
- Работа с кадрами, предполагающая активную работу кадровой службы компании по проверке, набору, обучению, продвижению, стимулированию персонала, расстановке. Это направление деятельности компании предполагает регулярные инструктажи персонала про необходимость соблюдения правил пользования конфиденциальными данными и об ответственности за их нарушение.

По исследованиям зарубежных специалистов относительно проблемы обеспечения безопасности компании считается, что сохранность конфиденциальных данных на 80% зависит от правильного подбора, воспитания и расстановки персонала предприятия.

22.3. Налоговая тайна

В соответствии с действующим налоговым законодательством *налоговую тайну* представляют собой всякие полученные налоговыми органами, таможенными органами, органами государственного внебюджетного фонда и органами внутренних дел данные о налогоплательщике, за исключением:

- Сведений открытых налогоплательщиком лично или по его согласию;
- Сведений про идентификационный номер налогоплательщика;
- Сведений о нарушении законодательства про налоги и сборы, а также меры ответственности за подобные нарушения;
- Сведения правоохранительным или налоговым (таможенным) органам других стран, предоставляемых в соответствии с международными соглашениями или договорами; при этом РФ также выступает одной из сторон соглашения про взаимное сотрудничество между правоохранительными или налоговыми (таможенными) органами;
- Сведения, предоставляемые избирательным комиссиям по законодательству о выборах, которые были получены в результате проверок налоговым органом данных про размер и источники доходов кандидата и его супруги (ее супруга), про имущество, которое принадлежит кандидату и его супругу (ее супругу) на праве собственности.

Институт налоговой тайны представляет собой комплексный раздел, который включает в себя нормы налогового, административного, информационного, уголовного и прочих отраслей права.

Согласно законодательству, налоговые сведения по форме могут быть различными. По содержанию данные могут включать сведения, которые непосредственно связаны с вопросами налогообложения, или другую информацию, правовая охрана которой предусмотрена различными нормативно-правовыми актами.

Основным отличительным признаком данных, которые составляют налоговую тайну, является возможность получения налоговым органом данных о налогоплательщике только при исполнении своих полномочий. В свою очередь, данные, которые были получены должностным лицом вне осуществления им своих полномочий, не могут считаться налоговой тайной. Причиной этому является отсутствие основания отнесения этих данных к налоговой тайне, так как в таком случае всякое третье лицо может таким же способом получить подобные данные о налогоплательщике без особых препятствий.

Получение налоговым органом данных о налогоплательщике может осуществляться в рамках правоотношений, которые возникли в силу Налогового Кодекса Российской Федерации, имеют публично-правовой характер и основаны на властном подчинении одной стороны другой. Данные правоотношения в соответствии с действующим законодательством отводят властное полномочие истребовать необходимые данные налоговому органу, а налогоплательщику – обязанность ее предоставить. В свою очередь, несоблюдение налогоплательщиком данной обязанности влечет применение к нему мер ответственности, установленных Налоговым кодексом.

Налоговый контроль должен осуществляться должностными лицами налогового органа в рамках своих полномочий путем проведения налоговых проверок, получения объяснений от налогоплательщиков, налоговых агентов и плательщиков сборов, осмотра помещений и территорий, проверки данных учета и отчетности, а также в других формах, которые предусмотрены законодательством. Данные формы налогового контроля предусматривают получение налоговыми органами разных сведений о налогоплательщике. В свою очередь, всякие данные, которые были получены должностными лицами налоговых органов в рамках реализации полномочий по налоговому контролю, выступают объектом налоговой тайны.

Согласно действующему законодательству устанавливается обязанность определенных физических лиц и организаций предоставлять данные о налогоплательщике, доступные им. Эта обязанность устанавливается за банковскими организациями, налоговыми агентами, свидетелями (см. Рис. 59). Воспрепятствование в представлении налоговым органам указанных данных предусматривает ответственность. Данные, которые предоставляют лица в налоговые органы, охраняются в режиме налоговой тайны, но только в той части, где она касается непосредственно отдельно взятого налогоплательщика. Доступ к налоговой тайне имеют суды, что им необходимо для рассмотрения гражданских, административных и уголовных дел.

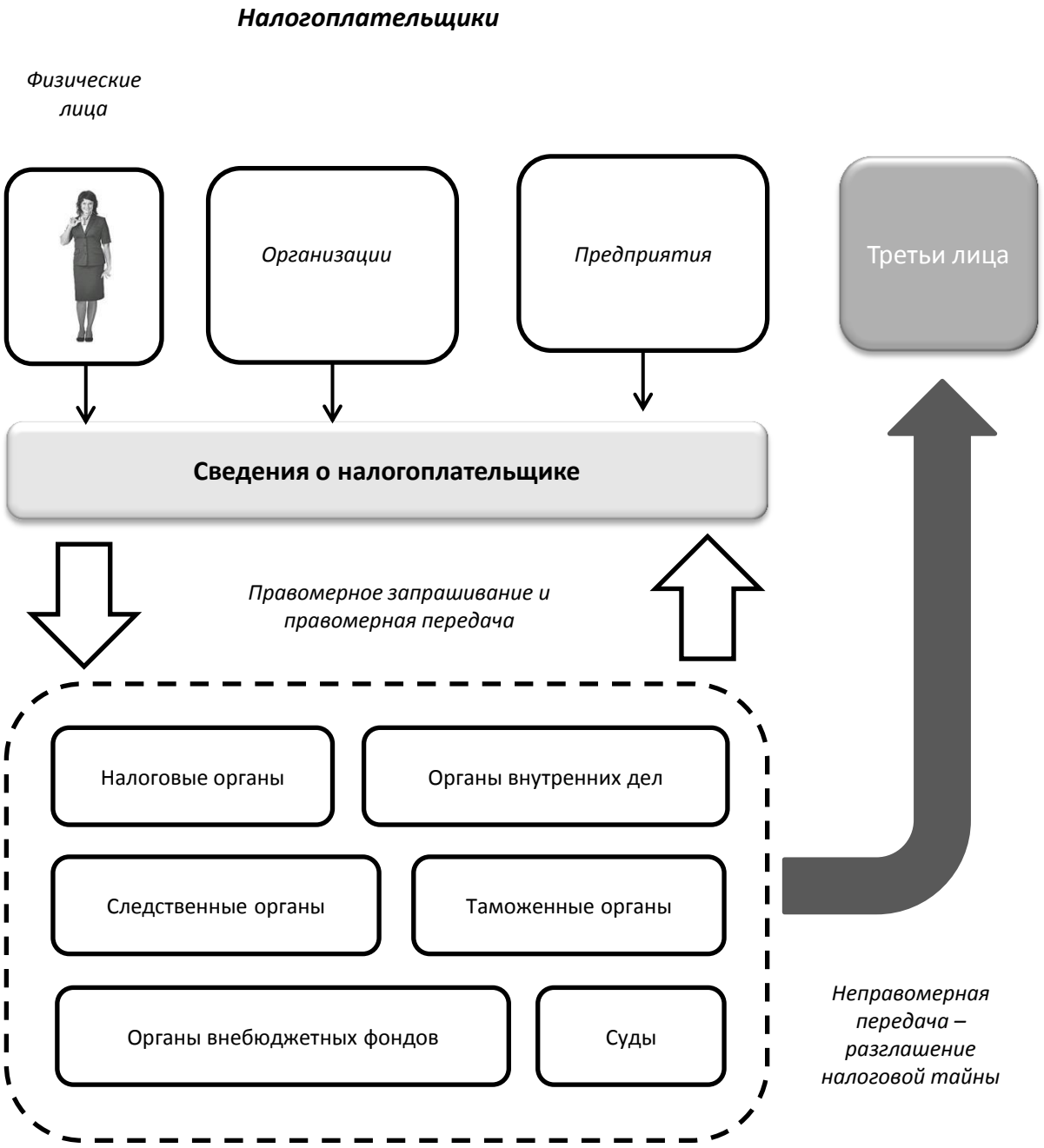

Рис. 59. Обращение сведений, составляющих налоговую тайну

Суды также рассматривают жалобы налогоплательщиков на решения и действия (бездействия) налоговых органов и должностных лиц, а также в связи с оспариванием ненормативных актов; при проведении производства по делам об административных правонарушениях может возникнуть потребность в данных о налогоплательщике в качестве доказательств. Такие материалы о налогоплательщике предоставляются налоговым органом в суд по мотивированному письменному запросу судьи.

В свою очередь, данные о налогоплательщике, которые необходимы для принудительного исполнения взыскания, предоставляются непосредственно судебным приставам-исполнителям. При отсутствии данных про должника, которые необходимы для принудительного исполнения, судебный пристав-исполнитель должен направить мотивированный письменный запрос в налоговый орган про ИНН, про номера счетов, про наименование и место нахождения банков и кредитных организаций, которые располагают счетами должника. Данный вид информации также является объектом налоговой тайны. В свою очередь, запрошенные судебным приставом-исполнителем данные должны быть предоставлены налоговым органом в трехдневный срок.

Федеральное законодательство предусматривает другие случаи предоставления данных, которые составляют налоговую тайну, со стороны налоговых органов по запросу Счетной палаты Российской Федерации, таможенных органов, Государственной Думы и Совета Федерации Федерального собрания. При этом получение данной информации влечет обязанность получателя по соблюдению и сохранению налоговой тайны.

Однако европейская практика наряду, с обязанностью налоговых органов и их должностных лиц по неразглашению данных про налогоплательщиков, законодательно закрепила возможность публикации некоторых налоговых данных, создав, таким образом, дополнительно практику налоговой публичности. Налоговая публичность широко применяется в таких европейских странах, как Италия, Франция, Норвегия, Швеция. Правовой основой налоговой публичности является конституционное право каждого гражданина на ознакомление с документами и материалами органов государственной власти, которые непосредственно затрагивают права и свободы гражданина. Основным критерием, от которого отталкивается практика налоговой публичности, является публичный характер обязанности по уплате налогов. Поэтому некоторые налоговые данные, перечень которых строго регламентирован, признаны в этих странах общедоступными и предоставляют право каждому налогоплательщику контролировать исполнение налоговой повинности всеми гражданами страны.

Режим правовой защиты данных подразумевает ответственность в случае нарушения налоговой тайны. Законодательно определено два основных вида *нарушения режима налоговой тайны*: утрату документов, имеющих данные, представляющие собой налоговою тайну, и собственно разглашение налоговой тайны. За нарушение режима налоговой тайны лицо привлекается к ответственности в том случае, если оно, обязано было его соблюдать в соответствии с действующим законодательством.

Под разглашением понимают передачу или использование другим лицом коммерческой или производственной тайны налогоплательщиков, которая стала известна должностному лицу налогового органа, органу государственного внебюджетного фонда, органу внутренних дел или таможенному органу при исполнении ими своих должностных обязанностей. Однако современная наука видит ряд изъянов в этом определении понятия *разглашение,* среди которых: включение в понятие «налоговая тайна» не только сведений, которые составляют налоговую, коммерческую и производственную тайны, но прочих данных о налогоплательщике; проявления разглашения не только в использовании и передаче данных, но и в придании их огласке (к примеру, публикация в СМИ).

Однако в справочно-правовых системах отсутствует судебная практика о наказании лиц по вопросу разглашения данных, которые составляют налоговую тайну. Вместе с тем, имеется ряд фактов принятия судебных решений в целях недопущения разглашения сведений, отнесенных к данной категории охраняемой информации.

Кейс № 26. Судебное решение об отказе в предоставлении информации

Федеральный арбитражный суд Восточно-Сибирского округа 25.04.2014 г. принял решение по делу N А19-12085/2013. Отказывая в признании недействительным требования налогового органа о представлении документов (информации), суд отклонил доводы о том, что оспариваемое требование не соответствует положениям ст. 93.1 Налогового кодекса, так как были истребованы документы за 2013 год, а камеральная проверка проводилась в отношении отчетности за 2012 год. Суд исходил из того, что контрагент проверяемого налогоплательщика не вправе оценивать относимость истребуемых документов к проверяемому периоду, поскольку такая оценка находится в компетенции налогового органа, осуществляющего проверку. Налоговые органы не обязаны отчитываться перед контрагентом проверяемого лица о причинах, по которым они посчитали истребуемую информацию (документы) относящейся к проверяемому периоду; иной вывод привел бы к незаконному разглашению налоговой тайны о проверяемом лице его контрагенту (ст. 102 НК РФ). Кроме того, суд пришел к выводу о том, что нормами не установлено ограничений по периоду времени, за который могут быть истребованы документы (информация), касающиеся деятельности проверяемого налогоплательщика (плательщика сбора, налогового агента).*

Вопрос: считаете ли вы, что контрагент мог запросить данную информацию у налогоплательщика.

Вместе с тем, нормы налогового, гражданского, административного и уголовного права предусматривают ответственность должностных лиц за разглашение сведений, составляющих различные виды конфиденциальной информации. Данные нормы позволяют применять различные режимы защиты налоговой тайны.

*Федеральный арбитражный суд Восточно-Сибирского округа. Решение по делу № А19-12085/2013. Информационный ресурс www/consultant.ru (дата обращения 05.02.2015)

22.4. Банковская тайна

Банковская тайна – это юридический принцип в законодательствах определенных стран мира, по которому банки и иные кредитные организации получают возможность защищать данные о вкладах и счетах своих клиентов и корреспондентов, банковские операции по счетам и сделкам в интересах клиентов, а также сведения клиентов, разглашение которых нарушает их право на неприкосновенность приватной жизни. В действующем законодательстве **под банковской тайной понимается сохранение уполномоченными лицами и организациями тайны об операциях, о счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.**

Статья 26 ФЗ «О банках и банковской деятельности» является прямой нормой права и содержит исчерпывающий перечень положений, в соответствии с которыми сведения, составляющие банковскую тайну, могут быть выданы третьим лицам (рис. № 60). В соответствии с этой нормой получить сведения, составляющие банковскую тайну, об юридических лицах и частных предпринимателях могут только суды (общей юрисдикции, арбитражные и мировые), Счетная палата Российской Федерации, Федеральная налоговая служба и ее органы, Федеральная служба финансового мониторинга и ее органы, Пенсионный фонд Российской Федерации и его органы, Фонд социального страхования Российского Федерации и его органы, Федеральная служба судебных приставов и ее органы, уполномоченный федеральный орган по страхованию вкладов. Органы предварительного следствия вправе запрашивать в банках информацию о юридических лицах и частных предпринимателях только по возбужденным уголовным делам и при наличии согласия руководителя следственного органа. Органы внутренних дел (полиция) вправе запрашивать указанную информацию только при проведении оперативно-розыскной деятельности по выполнению своих функций по выявлению, предупреждению и пресечению налоговых преступлений.

В соответствии с названной нормой сведения, составляющие банковскую тайну, о физических лицах, могут быть раскрыты только перед уполномоченным федеральным органом по страхованию вкладов (выплата компенсаций физическим лицам при банкротстве банков), судам и судебным приставам. Органы предварительного следствия вправе получить информацию, составляющую банковскую тайну физических лиц, в порядке, предусмотренном в предыдущем абзаце (при наличии возбужденного уголовного дела и санкции руководителя следственного органа).

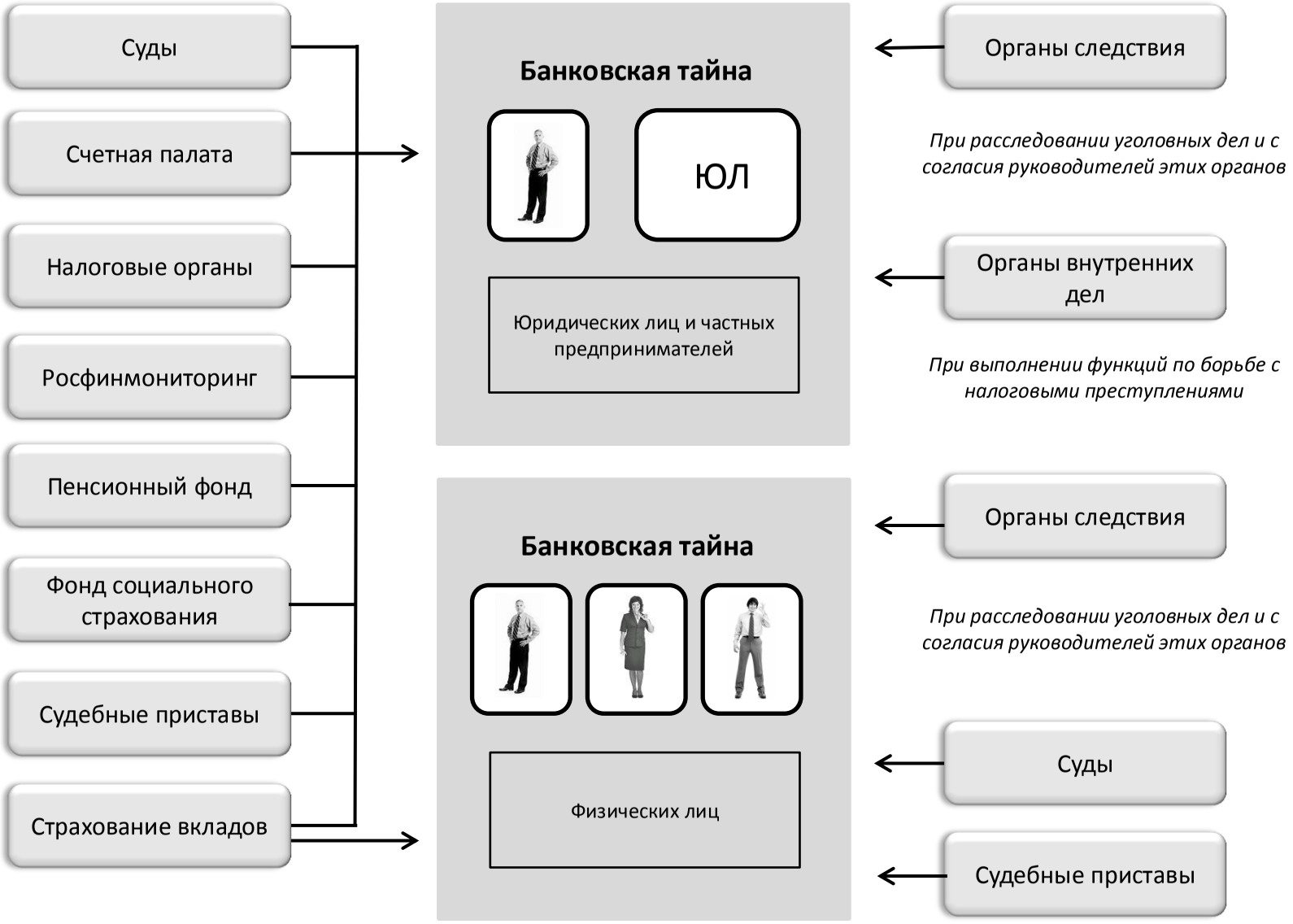

Рис. 60. Режим раскрытия сведений, составляющих банковскую тайну

Кейс № 27. Отказ банка в раскрытии информации

В 2007 г. в один из банков, расположенных в г. Санкт-Петербурге, поступил запрос из отдела экономической безопасности Управления МВД России по Центральному административному району. В запросе, подписанным начальником отдела, содержалась информация о том, что органами внутренних дел рассматривается вопрос о возбуждении уголовного дела в отношении гражданина «Петрова Ивана Сидоровича». Как сообщалось, полиция располагала сведениями о том, что названное физическое лицо является клиентом банка. Отдел экономической безопасностит просил, на основании полномочий, предоставленных ФЗ «Об оперативно-розыскной деятельности», сообщить о наличии у подозреваемого счетов, вкладов и движении денежных средств по ним за весь период.

Рассмотрев указанный запрос, управление безопасности банка сообщило сотрудникам полиции, что не вправе предоставить требуемую информацию.

Вопрос: обоснуйте отказ банка полиции в предоставлении информации, составляющей банковскую тайну физического лица.

С принятием ФЗ «О противодействии коррупции», в указанную статью также внесены дополнения, связанные с проверкой информации о доходах и расходах физических лиц, занимающих или претендующих на замещение должностей государственной и муниципальной службы, а также работы в учреждениях, предприятиях и организациях, принадлежащих государству. К указанным категориям отнесены:

1) Граждане, претендующие на замещение государственных должностей Российской Федерации;
2) Граждане, претендующие на замещение должности судьи;
3) Граждане, претендующие на замещение государственных должностей субъектов Российской Федерации, должностей глав муниципальных образований, муниципальных должностей, замещаемых на постоянной основе;
4) Граждане, претендующие на замещение должностей федеральной государственной службы, должностей государственной гражданской службы субъектов Российской Федерации, должностей муниципальной службы;
5) Граждане, претендующие на замещение должностей руководителя (единоличного исполнительного органа), заместителей руководителя, членов правления (коллегиального исполнительного органа), исполнение обязанностей по которым осуществляется на постоянной основе в государственной корпорации, Пенсионном фонде Российской Федерации, Фонде социального страхования Российской Федерации, Федеральном фонде обязательного медицинского страхования, иных организациях, создаваемых Российской Федерацией на основании федеральных законов;
6) Граждане, претендующие на замещение отдельных должностей на основании трудового договора в организациях, создаваемых для выполнения задач, поставленных перед федеральными государственными органами и др.

В случае нарушения требований, виновные в разглашении информации, составляющей банковскую тайну, могут быть привлечены к ответственности.

22.5. Служебная тайна

Служебная тайна – **это конфиденциальная информация, которая защищается законом и является собственностью органов государственного и муниципального управления, государственных учреждений и предприятий.** Она формируется на законных основаниях, содержащая служебную тайну информация применяется представителями государства для исполнения своих служебных обязанностей. В свою очередь, доступ к служебной информации о деятельности государственных органов ограничивается федеральными законами или в силу служебной необходимости.
В виду того, что служебная тайна представляет собой вид конфиденциальной информации, она выступает самостоятельным объектом права. Правовая охрана и защита служебной тайны осуществляется с помощью специального ФЗ «О служебной тайне». Данным нормативным актом предусмотрены следующие виды служебной тайны:

- Служебная информация о деятельности федеральных государственных органов, доступ к которой ограничивается федеральными законами с целью защиты государственных интересов;
- Тайна следствия (данные предварительного следствия); судебные тайны (тайны совещаний судей, содержания дискуссий и результатов голосования закрытого совещания, материалы закрытых судебных заседаний, тайны совещаний присяжных заседателей или в силу служебной необходимости, порядки выработки и принятия решений, организации внутренней работы);
- Конфиденциальная информация, которая стала известной в результате исполнения служебных обязанностей должностным лицам государственных и муниципальных органов управления (банковская тайна, коммерческая тайна, информация о приватной жизни лица, профессиональная тайна).
- Действующим законодательством также определен перечень сведений, которые не могут быть отнесены к категории служебной тайны:
- Акты законодательства, которые устанавливают правовой статус государственных органов, общественных объединений, организаций и права, свободы и обязанности граждан, а также порядок их реализации;
- Описание структуры, функций, направлений и форм деятельности органа исполнительной власти, а также его адрес;
- Сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах; гидрометеорологические, экологические, гидрогеологические, санитарно-эпидемиологические, демографические и другие данные, которые необходимы для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

В случае нарушения требований, виновные в разглашении информации, составляющей банковскую тайну, могут быть привлечены к ответственности.

22.5. Служебная тайна

Служебная тайна – **это конфиденциальная информация, которая защищается законом и является собственностью органов государственного и муниципального управления, государственных учреждений и предприятий.** Она формируется на законных основаниях, содержащая служебную тайну информация применяется представителями государства для исполнения своих служебных обязанностей. В свою очередь, доступ к служебной информации о деятельности государственных органов ограничивается федеральными законами или в силу служебной необходимости.

В виду того, что служебная тайна представляет собой вид конфиденциальной информации, она выступает самостоятельным объектом права. Правовая охрана и защита служебной тайны осуществляется с помощью специального ФЗ «О служебной тайне». Данным нормативным актом предусмотрены следующие виды служебной тайны:

- Служебная информация о деятельности федеральных государственных органов, доступ к которой ограничивается федеральными законами с целью защиты государственных интересов;
- Тайна следствия (данные предварительного следствия); судебные тайны (тайны совещаний судей, содержания дискуссий и результатов голосования закрытого совещания, материалы закрытых судебных заседаний, тайны совещаний присяжных заседателей или в силу служебной необходимости, порядки выработки и принятия решений, организации внутренней работы);
- Конфиденциальная информация, которая стала известной в результате исполнения служебных обязанностей должностным лицам государственных и муниципальных органов управления (банковская тайна, коммерческая тайна, информация о приватной жизни лица, профессиональная тайна).

Действующим законодательством также определен перечень сведений, которые не могут быть отнесены к категории служебной тайны:

- Акты законодательства, которые устанавливают правовой статус государственных органов, общественных объединений, организаций и права, свободы и обязанности граждан, а также порядок их реализации;
- Описание структуры, функций, направлений и форм деятельности органа исполнительной власти, а также его адрес;
- Сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах; гидрометеорологические, экологические, гидрогеологические, санитарно-эпидемиологические, демографические и другие данные, которые необходимы для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

- Порядок рассмотрения и разрешения заявлений, в том числе юридических лиц, которые рассматриваются в установленном порядке;
- Данные про исполнение бюджета и использования других государственных ресурсов, про состояние экономики и потребностей населения;
- Документы, которые накапливаются в открытых фондах библиотек и архивов, а также информационных системах организаций, которые необходимы для реализации прав, свобод и обязанностей граждан.

Рис. 61. Обращение сведений, составляющих служебную тайну

Особенность правоотношений в области функционирования государственной и муниципальной власти, государственных учреждений и предприятий состоит в том, что они обязаны защищать конфиденциальную информацию, принадлежащую иным лицам (коммерческая, налоговая и банковская тайны, а также персональные данные). В процессе своей деятельности указанные органы также создают собственную конфиденциальную информацию, которая отнесена к категории *служебной тайны* и входит в специальные ведомственные перечни, если она не является государственной тайной.

Вопросы и задания для самоконтроля

1. Дайте определение понятия «конфиденциальная информация».
2. Расскажите о возможных мерах по защите коммерческой тайны на предприятии.
3. Сообщите об основных отличиях в сферах защиты сведений, составляющих коммерческую и налоговую тайну.
4. Сообщите об условиях предоставления банками сведений, составляющих банковскую тайну, сторонним организациям, учреждениям и предприятиям.
5. Сообщите о правовом статусе сведений, составляющих ведомственную тайну.

Глава 23. Защита государственной тайны

В результате изучения главы студент должен **знать** основные понятия и виды государственной тайны в Российской Федерации, формы и методы ее защиты, порядок допуска лиц к сведениям, составляющим государственную тайну; угрозы, существующие в данной области, и ответственность за умышленное и неумышленное разглашение государственной тайны; **уметь** определять формы взаимодействия государства и предприятий (в целесообразных случаях) в области обеспечения сохранности сведений, составляющих государственную тайну; **владеть** методикой распознавания информации, отнесенной к государственной тайне, и общими методами ее защиты.

23.1. Понятие и виды государственной тайны

Федеральное законодательство регулирует отношения, которые возникают в связи с отнесением данных к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах осуществления безопасности государства.

Государственная тайна представляет собой сведения в области военной, экономической, внешнеполитической, разведывательной, оперативно-розыскной и контрразведывательной деятельности, которые защищаются государством, и разглашение которых может нанести вред безопасности страны. Особый правовой статус этих сведений обуславливает их характер и выражается в процедуре засекречивания и рассекречивания, а также доступе к ним (Рис. № 62).

Рис. 62. Структура сведений, составляющих государственную тайну

В соответствии с действующим законодательством, отнесение данных к государственной тайне и их засекречивание определяется как введение ограничений на доступ к ним и их распространение. Существует перечень сведений, которые не подлежат ограничениям, и не могут быть отнесены к государственной тайне:

1) О чрезвычайных происшествиях и катастрофах, а также стихийных бедствиях, которые угрожают безопасности и здоровью граждан;

2) О состоянии экологии, санитарии, здравоохранения, образования, демографии, сельского хозяйства, культуры, а также о ситуации с преступностью;

3) О привилегиях, льготах и компенсациях, которые предоставляются государством гражданам, предприятиям, должностным лицам, учреждениям и организациям;

4) О размерах золотого запаса и государственных валютных резервах РФ; о состоянии здоровья высших должностных лиц РФ;

5) О фактах нарушения законности органами государственной власти и их должностными лицами.

Согласно нормативным требованиям степень секретности данных, которые составляют государственную тайну, равен размеру вреда, который может быть нанесен национальной безопасности вследствие их распространения. Закон устанавливает три степени секретности данных, которые составляют государственную тайну, и определяет грифы секретности для носителей указанных данных: «особой важности»; «совершенно секретно» и «секретно». Должностные лица допускаются к сведениям, составляющим государственную тайну, на основании следующих принципов:

- Ограниченность (возможность ознакомления должностного лица или гражданина только с теми данными и в таких объемах, которые необходимы для выполнения должностных обязанностей);
- Добровольность (осуществления допуска должностных лиц и граждан к государственной тайне в добровольном порядке);
- Согласие на временные и частные ограничения прав;
- Наложение дополнительных обязанностей (принятие на себя обязательств перед государством относительно неразглашения доверенных данных, которые составляют государственную тайну);
- Повышение ответственности (граждане и должностные лица, виновные в нарушении законодательства о государственной тайне, несут административную, уголовную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством).

23.2. Система защиты государственной тайны.

В соответствии с действующим законодательством Российской Федерации *система защиты государственной тайны* определяется как **совокупность органов защиты государственной тайны, которые осуществляют свою деятельность в координации и взаимодействии согласно предоставленной законодательством компетенции, а также используют формы, методы и средства защиты данных, которые составляют государственную тайну, и их носителей.** Соответствующие органы по защите государственной тайны создаются и осуществляют свою деятельность в соответствии с реальными и потенциальными рисками нанесения ущерба интересам национальной безопасности нашего государства.

Сведения, которые требуют отнесения к сведениям, составляющим государственную тайну, определяются органами государственной власти и учреждениями, которые получают (обрабатывают) эти данные. Указ Президента РФ № 90 от 11.02.2006 «О перечне сведений, отнесенных к государственной тайне» утверждает перечень этих органов, среди которых: Администрация Президента, Аппарат Правительства, Министерство обороны, Министерство внутренних дел, Министерство юстиции, Министерство здравоохранения, Министерство энергетики, Министерство по чрезвычайным ситуациям и вопросам гражданской обороны, Федеральная служба охраны, Служба внешней разведки, Федеральная служба безопасности, Росатом, Роскосмос и др.

Доступ граждан к сведениям, которые составляют государственную тайну, разрешен только в случае наличии у них допуска к государственной тайне, оформленном в соответствующей форме. При этом обладателям допуска более высокой степени секретности, автоматически разрешается допуск и к данным более низкой степени секретности. Допуск граждан к государственной тайне оформляется по месту работы или службы. В учреждениях, организациях и на предприятиях, имеющих отношение к работе со сведениями, составляющими государственную тайну, существуют *номенклатуры должностей лиц, подлежащих допуску к секретам*. Номенклатуры состоят из перечня должностей, перечня секретов, к которым допускаются работники, и разделены на группы по формам допуска. При этом тщательность проверки кандидата зависит от формы допуска к тайне. Так, допуск по третьей форме оформляется без проведения органами безопасности проверочных мероприятий, а решение принимается на основании анкетных данных гражданина. Исключением является оформление допусков сотрудникам подразделений, которые связанны с защитой государственной тайны, а также руководителям организаций, в отношении которых обязательны проверочные мероприятия. В допуске может быть отказано по следующим причинам:

- Наличие у гражданина медицинских противопоказаний для работы с использованием данных, которые составляют государственную тайну;
- Признание судом недееспособности гражданина (ограничено дееспособным), наличие у гражданина неснятой судимости за преступления в области разглашения государственной тайны, рецидивистом, нахождение его под судом или следствием за государственные или иные тяжкие преступления;
- Уклонение гражданина от проверочных мероприятий и (или) сообщение ним заведомо ложных анкетных сведений;

- Постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными гражданами документов для выезда на постоянное место жительства в другие государства;
- Выявление в результате проведения проверочных мероприятий действий гражданина, которые создают угрозу безопасности страны.

Отдельные категории граждан освобождены от необходимости оформления допуска к сведениям, составляющим государственную тайну. К ним отнесены депутаты Государственной Думы и члены Совета Федерации Федерального Собрания, судьи на период исполнения своих полномочий, а также адвокаты, которые участвуют в качестве защитников в уголовном судопроизводстве по делам, которые связаны со сведениями, составляющими государственную тайну.

Получив доступ к сведениям, которые являются государственной тайной, указанные лица предупреждаются об обязанности неразглашения государственной тайны, которая станет им известной в связи с исполнением своих полномочий, а также о привлечении их к ответственности в случае разглашения. Предусматривается уголовная, административная, дисциплинарная и гражданско-правовая ответственность за нарушение законодательства о государственной тайне. В качестве дополнительного наказания может применяться также право лишение возможности занимать некоторые должности. На практике, привлечение к уголовной ответственности гражданина по указанным выше статьям практически лишает его возможности дальнейшего карьерного роста.

Кейс № 27. О лишении военнослужащего допуска к секретам

Судебная коллегия по делам военнослужащих Верховного суда Российской Федерации 18.11.2014 г. рассмотрела в судебном заседании гражданское дело по апелляционной жалобе на решение Северо-Кавказского окружного военного суда от 15.08.2014 г. по заявлению майора Агаларова А.М. об оспаривании действий командира войсковой части, связанных с прекращением допуска к государственной тайне.

Судебная коллегия установила, что решение суда первой инстанции основано на правильном применении норм материального права, а выводы, изложенные в решении, соответствуют фактическим обстоятельствам дела, установленным в ходе судебного разбирательства. Майор Агаларов А.М. был допущен командиром части к государственной тайне по форме № 3. Приказом командира части ему был прекращен допуск к государственной тайне. Основанием послужили выявленные случаи невыполнения военнослужащим требований законодательства о государственной тайне и соблюдении режима секретности. В нарушение установленного порядка Агаларов А.М. передавал свою рабочую тетрадь с грифом «секретно» другим лицам. Он жэе нарушил порядок оформления допуска и скрыл наличие постоянно проживающих за границей родственников, аннулирование паспорта гражданина РФ и оформление вида ни жительство в нашей стране, не устранил нарушения после привлечения к дисциплинарной ответственности и

предостережения, объявленного военным прокурором. В соответствии с заключенным контрактом, майор Агаларов А.М. исполнял общие, должностные и специальные обязанности по службе, работал с документами с грифом «секретно». На основании изложенного судебная коллегия оставила без изменений решение Северо-Кавказского окружного военного суда по заявлению Агаларова А.М. об оспаривании действий командира войсковой части, связанных с прекращением допуска к государственной тайне, а жалобу заявителя – без удовлетворения*.

Вопрос: сможет ли по вашему мнению Агаларов А.М. продолжить военную службу.

Отдельное место в системе защиты государственной тайны занимают вопросы регулирования отношений в области науки и производства. В соответствии с перечнем данных, которые отнесены к государственной тайн, предусматривает 87 типов данных, конкретное содержание которых определяют ведомственные перечни федеральных органов исполнительной власти. В свою очередь, в практической деятельности лишь часть из этих данных находятся под защитой в рыночных условиях. К этим сведениям относятся лишь те сведения, с которыми работают компании, среди них:

- Данные в военной области о режимах объектов на различных стадиях жизненного цикла, технологиях двойного назначения, НИОКР;
- Данные о внешнеполитической1 и внешнеэкономической деятельность в области информации об импорте и экспорте военной техники и вооружения, государственном оборонном заказе в рамках военно-технического сотрудничества;
- Данные в области науки, экономики и техники, которые касаются оборонных научно-исследовательских и опытно-конструкторских работ (НИОКР), запасов, производства, себестоимости редких, драгоценных и цветных металлов, стратегических запасов и мобилизационных мощностей.

Содержание защищаемой информации имеет значение для исполнителей работ, т.к. это влияет на возможность регулярного исполнения государственного заказа, объемы производства в интересах военно-технического сотрудничества с зарубежными странами, а также меры, связанные с защитой секретов. При этом предприятия оборонно-промышленного комплекса (ОПК) не всегда обладают собственными исчерпывающими возможностями по защите секретов, в связи с чем вынуждены использовать аутсорсинг, специально сертифицированный уполномоченными государственными органами. К таким организациям относятся: интеграторы средств и систем защиты информации (аттестационные центры); испытательные лаборатории систем сертификации; производители средств защиты информации от утечки по техническим каналам;

*Решение судебной коллегии Верховного суда РФ по делам военнослужащих от 18.11.2014 г. № 205-АПГ14-12. Информационно-справочный портал Консультант плюс (электронный ресурс). www.konsultant.ru. М. (дата обращения: 06.02.2015)

лицензионные центры и центры проведения специальных экспертиз; производители средств защиты от несанкционированного доступа в компьютерных сетях.

Рынок названных услуг характеризуется невысокой средней доходностью. В свою очередь, финансовые издержки входа в рынок составляют 50-100 тыс. долл. США. Значительно выше приходятся нематериальные барьеры, к которым относятся репутационные и лицензионные препятствия. При этом издержки выхода из рынка превышают издержки входа из-за узкой специализации и низкой востребованности на других рынках. Эта особенность определяет относительную стабильность состава участников. Сегмент находится на стадии замедления роста и растет на 15-20% в год, в основном за счет государственного оборонного заказа, в то же время, ведущие участники рынка ежегодно увеличивают свои обороты на 50-100%. На рынке появляется мало новых сильных игроков в сегменте интеграции систем защиты информации — аттестации объектов информатизации. Конкуренция среди 8-10 ведущих интеграторов обостряется. Потребности заказчиков в сегменте государственной тайны стабильны. Существует четкая тенденция увеличения количества заказчиков, требующих комплексного (10-15 видов работ) оказания услуг. Маркетинговая активность участников рынка низкая. В отрасли практически повсеместно все мощности загружены полностью, у нескольких ведущих организаций формируются очереди на исполнение заказов. В продуктах (средства защиты информации и услуги) не существует значительных функциональных отличий, но существуют серьезные отличия в ценах, имидже, поддержке.

Регионально основные участники рынка распределены следующим образом. 70% объемов рынка сосредоточиваются в Центральном (ЦФО) и Северо-Западном федеральных округах (СЗФО) России. В свою очередь, темпы роста рынка в регионах превышают темпы роста в СЗФО и ЦФО. Тем не менее, в регионах практически отсутствуют компании, которые дифференцированы в области информационной безопасности. Основные разработчики и производители средств защиты информации расположены в Москве и Санкт-Петербурге. К основным организациям-разработчикам средств защиты информации, которые способные организовать массовое производство относятся: «Информзащита», «Инфосистемы Джет», «Инфотекс», «Маском», «Элвис+», «Спектр», «Нелк», «Анна», «ОКБ САПР», «Гамма». Существует значительное количество организаций, которые в силу опыта работы или условий своего основания занимают прочные технологические или рыночные «ниши» и в силу этого в меньшей степени подвержены конкурентному влиянию.

Вопросы и задания для самоконтроля

1. Дайте определение понятия «государственная тайна».
2. Сообщите о видах государственной тайны в Российской Федерации.
3. Расскажите об основных мерах по защите информации, составляющей государственную тайну, в нашей стране.
4. Расскажите об особенностях защиты информации, составляющей государственную тайну, на предприятии оборонно-промышленного комплекса.
5. Сообщите о мерах ответственности в случае нарушения правил защиты информации, составляющей государственную тайну.

Глава 24. Безопасность электронных ресурсов, систем и процессов

В результате изучения главы студент должен **знать** об особенностях электронных ресурсов, систем и процессов, используемых в реальном секторе экономики и типовых угрозах информационной безопасности предприятия в данной области; **уметь** определять принципы применения предупредительных мер защиты электронных ресурсов, систем и процессов; **владеть** основами применения рекомендаций по современным стандартам кибернетической безопасности, их архитектуре и способах их внедрения в деятельность компании; **владеть** правилами расследования многообразных кибернетических инцидентов о нарушений при пользовании компьютером, вплоть до сбора процессуальных доказательств в совершенных уголовных преступлениях в данной области.

24.1. Электронные информационные ресурсы, системы и процессы

В результате перехода от индустриальной к постиндустриальной эпохе изменилась значимость отдельных факторов производства, в результате чего произошло смещение в интенсивности использования различных ресурсов. Современное производственное предприятие или организация в процессе своего функционирования потребляет следующие виды ресурсов: материальные, трудовые, информационные (интеллектуальные), финансовые. Главная характеристика этих ресурсов (кроме информационных ресурсов) ограниченность или одноразовость в использовании. В свою очередь, информационные ресурсы являются многоразовыми и не подлежат физической амортизации. Однако они также имеют свойство устаревать, терять свою актуальность как отражение реального мира.

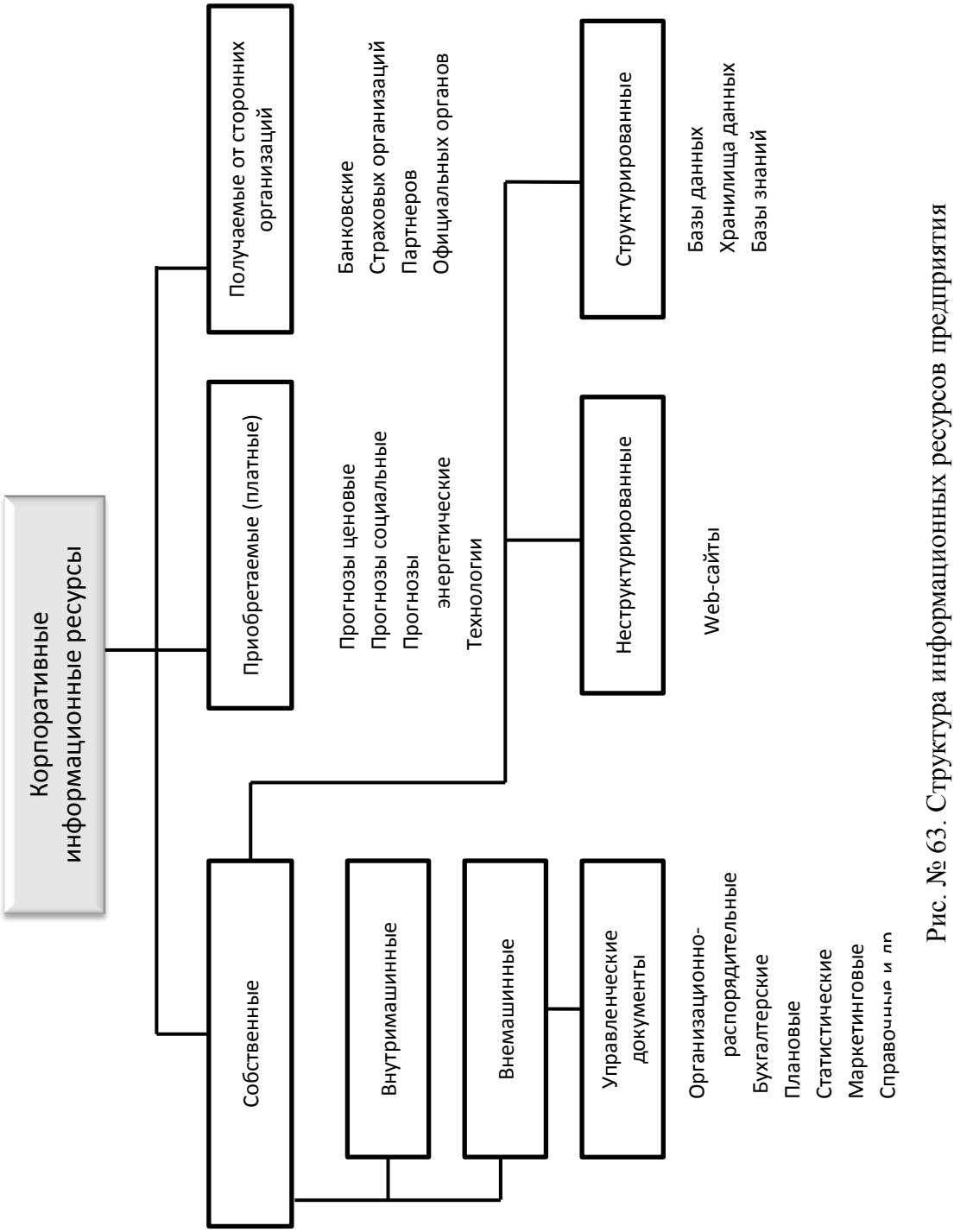

Рис. № 63. Структура информационных ресурсов предприятия

Согласно данным Европейской комиссии по стратегическим исследованиям, доля участия информационных ресурсов в процессе производства за последние 20 лет возросла в среднем на 17%. Этому способствует возрастающее значение знаний (информационного ресурса) как части капитала организации в производстве. Согласно действующему законодательству **информационные ресурсы представляют собой информацию, которая зафиксирована на материальном носителе и хранится в информационных**

системах: архивах, библиотеках, фондах и других информационных системах. Все информационные ресурсы (ИР), которые используются в организации, предназначены для обеспечения ее деятельности. По источнику приобретения информационные ресурсы делятся на внешние и внутренние. Обобщенная классификация ИР предприятия по источнику возникновения представлена выше (рис. № 63). Под *информационным ресурсом предприятия* понимают совокупность нематериальных активов, документов, имеющих важное стратегическое значение для функционирования организации. Информационные ресурсы служат инструментами стимулирования производственно-коммерческой деятельности, принятия управленческих решений и обучения.

С повышением значимости информационных ресурсов для ведения бизнеса компании все более актуальной проблемой становится обеспечение их защиты от чужого вторжения. При деятельности компании на международных рынках возникает постоянная потребность в использовании глобальных информационных ресурсов (рис. № 64).

Рис. № 64. Обобщенная структура глобальных информационных ресурсов

Популярное во всем мире справочное издание «Gale Directory of Databases», издаваемое дважды в год в виде двух томов фирмой «Gale Research, Inc», помогает ориентироваться в гигантском объеме мировых информационных ресурсов. К наиболее крупным информационным ресурсам относятся: принадлежащая Всемирному банку World Banke-Library (www.worldbank.org), включающая более 1400 наименований

финансовой информации; Организация экономического сотрудничества и развития (OECD, www.oecd.org), включающая 34 статистические базы данных по 30 странам-членам OECD и 70 странам дополнительно; библиотека ООН (UNCDB), включающая данные 435 статистических рядов. Различные информационные агентства предоставляют доступ к мировым информационным статистическим ресурсам, что позволяет получать данные, кроме всех основных субъектов российского информационного рынка, в таких крупнейших международных информационных центрах, как DIAIOG (США), EURUSTART (Европейское Экономическое Сообщество), DATE-STAR (Швейцария), TRADSTAT (Швейцария), Dun & Bradstreet (США) и другие. Кроме того, с целью эффективного ведения внутриэкономической деятельности организации широко используются *государственные и региональные информационные ресурсы*.

Виды государственных ИР по функциональному назначению: государственная система научно-технической информации, архивный фонд, государственная система статистики, библиотечная сеть, ИР органов государственной власти и местного самоуправления, ИР социальной сферы, государственная система правовой информации, ИР в сфере финансов и внешнеэкономической деятельности, ИР о природных ресурсах, явлениях и процессах. *Региональные (городские, муниципальные) информационные ресурсы* предназначаются для управления территориальным образованием, среди которых: региональные и муниципальные органы статистики, органы юстиции, страховые компании, налоговые органы, медицинские учреждения. При этом вся первичная информация для региональных информационных ресурсов создается на муниципальном уровне, а базовыми среди информационных ресурсов считаются: регистры, реестры, кадастры. *Информационным ресурсом* предприятия или организации подразумевает совокупность собственных, приобретаемых и поставляемых извне данных и знаний, которые зафиксированы на бумажных и электронных носителях.

Процесс управления информационными ресурсами подразумевает комплексное решение следующей совокупности задач:

- Оценка информационных потребностей в рамках каждой функции управления и на каждом уровне;
- Преодоление проблемы несовместимости типов данных;
- Стандартизация и унификация форм и типов документов; типизация данных; рационализация и изучения документооборота организации;
- Создание системы управления данными.

Для решения вышеуказанных задач ИР используют информационные системы. *Информационная система* (ИС) – коммуникационная система по сбору, передаче, переработке и хранению данных об объекте, который снабжает сотрудников различного ранга данными с целью реализации ими функций управления. Информационная система организации представляет совокупность информационного контура, а также средств сбора, передачи, обработки и хранения данных.

Известны следующие основные виды информационных систем:

- Локальные АРМ (автоматизированное рабочее место) – это программно-технический комплекс, который предназначен для реализации управленческих функций на отдельном рабочем месте и информационно связанный с другими ИС (АРМ);
- Комплекс функционально и информационно связанных АРМ, которые реализуются в полном объеме функции управления;
- Компьютерная сеть АРМ на единой информационной базе, которая обеспечивает интеграцию функций управления в масштабе организации или группы бизнес-единиц;
- Корпоративная ИС, которая обеспечивает полнофункциональное распределенное управление крупномасштабной организаций (понятие КИС тождественно определению ERP-системы).

Другим классификационным признаком для информационной системы является степень сложности и формализации (структурированности) алгоритмов обработки информации функциональных компонентов и соответствующих информационных технологий. В этом смысле применяется система поддержки и принятия решений DSS (Decision Support Systems) и система оперативной обработки данных – OLTP-системы (On-Line Transaction Processing). OLTP-системы предполагают сильную защиту баз данных от несанкционированного доступа, а также программных и аппаратных сбоев в работе информационной системы. При этом имеется жесткая регламентация формы выходных и входных документов, а также схемы документооборота. С целью повышения эффективности функционирования ИС рекомендуется использовать компьютерные сети с архитектурой «клиент-сервер». В свою очередь, система поддержки и принятия решений ориентирована на реализацию сложных бизнес-процессов, которые требуют аналитической обработки данных и формирования новых знаний. При этом анализ информации должен определяться целевой ориентацией, например, финансовом анализом предприятия, аудитом бухгалтерского учета.

Хранилище данных является основой создания подмножества данных, среди которых применяются OLAP-кубы. Они представляют собой многомерные иерархические структуры данных, которые содержат следующие признаки:

- Дату/время (период времени, к которому относятся данные);
- Сферу деятельности (бизнес-сфера, результат), к которой относятся данные;
- Уровень управления (структурное подразделение), которому соответствуют данные;
- Вид ресурса;
- Субъект управления (лицо, принимающее решение).

Данные признаки позволяют агрегировать информацию путем вычисления статистических оценок и произвольного сочетания признаков. В результате этого анализа информации создается новое знание, полезное для целей управления. Содержательный анализ данных основан на применении инструментальных средств OLAP-технологий. Действие любой информационной системы осуществляется путем реализации совокупности информационных процессов. Таким образом, исходя из сущности информационной системы, можно определить понятие информационного процесса как процесса получения, создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

Результатом исполнения информационных процессов является осуществление информационных прав и свобод, выполнение обязанностей соответствующими структурами вводить в обращение и производить данные, которые затрагивают права и интересы граждан, а также решение вопроса защиты личности, общества и государства от ложных данных и дезинформации, защиты информации и информационных ресурсов ограниченного доступа от несанкционированного доступа.

24.2. Типовые угрозы кибернетической безопасности предприятия

В последнее время происходит постепенное осознание большей значимости информационного воздействия на бизнес-процесс (управление им), чем материального или финансового воздействия, что, в свою очередь, превращает информационное противоборство в главный инструмент выживания и конкурентной борьбы. В этом случае информационная безопасность выходит на первый план в развитии бизнеса. В повседневной жизни приходится часто соприкасаться с такими терминами, как «киберпространство», «киберпреступность», «кибертерроризм», «кибернетическая безопасность» и тому подобные. Согласно принятому в июле 2012 года стандарту ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity дается четкое понимание связи кибербезопасности с сетевой безопасностью, прикладной безопасностью, Интернет-безопасностью и безопасностью критичных информационных инфраструктур.

Исследования кибернетических угроз, ежегодно проводимые Лабораторией Касперского (ЛК), позволили выделить пять наиболее опасных для будущего категорий киберугроз на государственном уровне: цифровые войны, социальные сети, Интернет-зависимость подрастающего поколения, хакеры, отсутствие приватности.

За последние два года на корпоративном уровне наблюдается обострение кибератак, жертвами которых все чаще становятся коммерческие компании.

По результатам опроса «Лаборатории Касперского» и аналитической компанией «B2B International», 91% опрошенных организаций в мире хотя бы один раз в течение года подверглись кибератаке, 9% компаний стали мишенью целевых атак. Основные типы кибератак указаны ниже (рис. № 65)*.

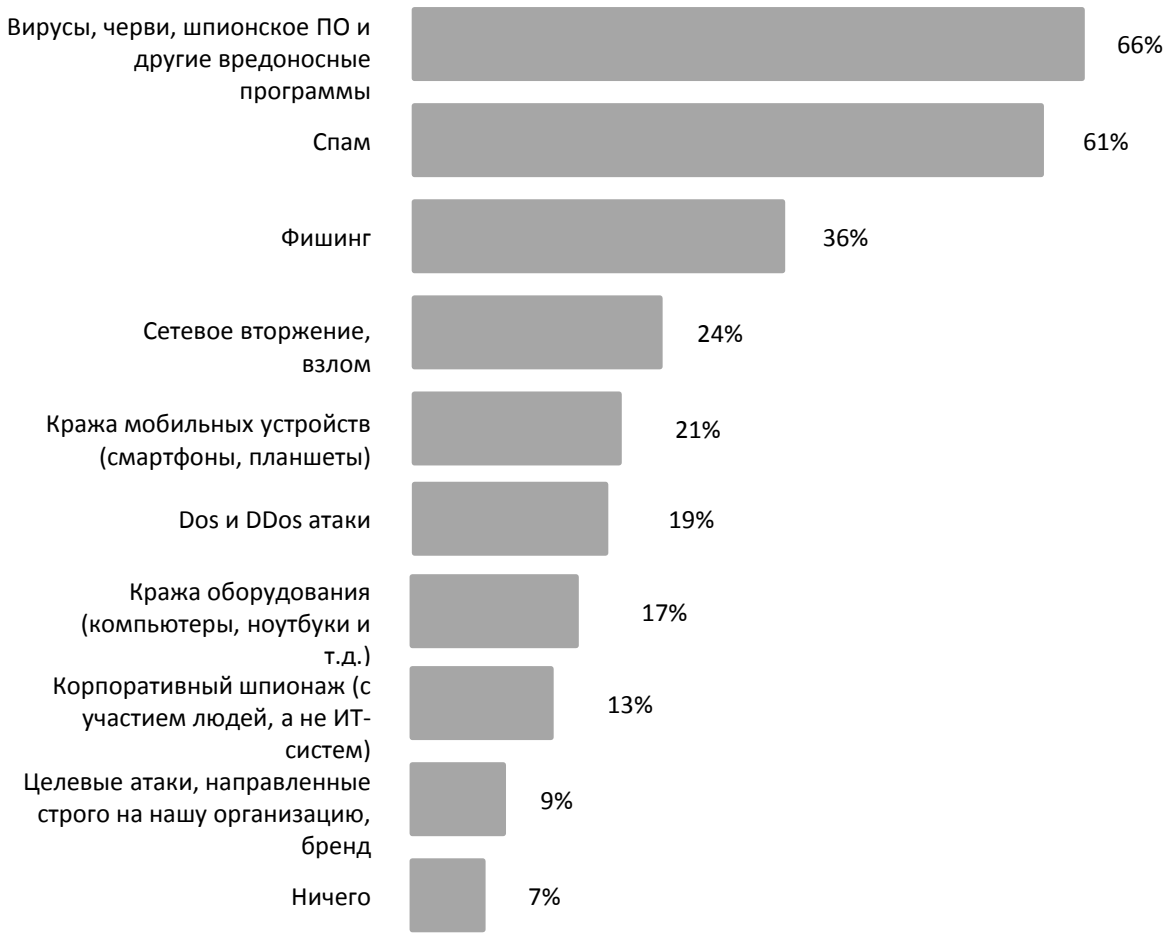

Рис. 65. Основные виды кибернетических атак на корпоративном уровне

Основой успешного применения злоумышленниками вредоносного программного обеспечения для кражи корпоративных данных и коммерческого шпионажа является

*Kaspersky Security Bulletin. Корпоративные угрозы. М.: ЗАО «Лаборатория Касперского». 2013. С. 24. Электронный ресурс: http://media.kaspersky.com/pdf/KSB_2013_RU.pdf. (дата обращения 12.02.2015).

использование компьютеров и других цифровых устройств во всех бизнес-процессах. Это открыло новую эпоху в развитии вредоносных программ, которые в ближайшем будущем смогут полностью заменить инсайдерскую разведку. В свою очередь, зависимость успешности бизнеса от надежности работы компьютеров и каналов связи между ними, предоставляет злоумышленникам все основание для использования различных программ деструктивного действия. К основным направлениям киберугроз относят*:

- *Кражу информации*. Цель – хищение коммерческой тайны, персональных данных или ценных корпоративных данных сотрудников и клиентов компании, мониторинг ее деятельности компании со стороны конкурирующих бизнесменов, которые обращаются к услугам киберпреступников для проникновения в корпоративные сети конкурентов;
- *Уничтожение данных или блокирование работы инфраструктуры*. Некоторые вредоносные программы используются для своего рода диверсий, задача которых состоит в уничтожении важных данных или нарушении работы инфраструктуры компании (троянские программы Wiper и Shamoon);
- *Кражу денег,* которая осуществляется посредством заражения специализированными троянскими программами, похищающими финансовые средства через системы дистанционного банковского обслуживания (ДБО), а также целевые атаки на внутренние ресурсы процессинговых и финансовых центров;
- *Удар по репутации компании*. Успешность бизнеса и очень высокая посещаемость официальных сайтов компаний, особенно работающих в сфере интернет-услуг, привлекает злоумышленников. Взлом корпоративного сайта с последующим внедрением ссылок, направляющих посетителей на вредоносные ресурсы, вставка вредоносного рекламного баннера или размещение политически ориентированного сообщения на взломанном ресурсе наносит существенный урон отношению клиентов к компании;
- *Кражу цифровых сертификатов IT-компаний*. В отдельных случаях, например для компаний, имеющих свои публичные центры сертификации, потеря сертификатов или проникновение в инфраструктуру цифровой подписи может привести к полному уничтожению доверия к компании и последующему закрытию бизнеса;
- *Финансовый ущерб*. Одним из популярных способов нанесения прямого вреда компаниям и организациям являются DDoS-атаки. Киберпреступники разрабатывают новые способы проведения таких атак. В результате DDoS-атак порой на несколько дней выводятся из строя внешние веб-ресурсы компаний. В таких случаях клиенты не только не могут воспользоваться услугами атакованной компании, что наносит ей прямой финансовый ущерб, но и нередко совсем отказываются от них в пользу более надежной компании, что ведет к уменьшению базы клиентов и долгосрочным финансовым потерям.

В качестве основных целевых категорий компаний для организации кибератак в последнее время стали предприятия нефтяной индустрии, телекоммуникационные компании, научно-исследовательские центры и компании, занятые в аэрокосмической, судостроительной и других отраслях, связанных с разработкой высоких технологий.

*Там же. С 25

Исследования показывают, что происходит постоянная эволюция киберугроз. На стратегическом уровне фиксируется переход от применения простых вирусов к использованию эксплойтов к неизвестным уязвимостям в программном обеспечении. При этом на тактическом уровне модификация вирусов такова, что даже лучшие антивирусы и Web-шлюзы не могут их отследить, а вредоносные программы воруют уже не ссылки на посещаемые сайты, а реквизиты доступа к ним. Изменяется и тактика реализации угроз: от массового заражения к фокусу на конкретную жертву. При этом сами угрозы становятся модульными, самовосстанавливающимися, устойчивыми к отказам и обнаружению. Необходимо отметить новую тенденцию в сфере киберугроз – это появление новой категории атакующих, которую ЛК назвала «кибернаемники». Это организованные группы хакеров с очень высоким уровнем подготовки, которые могут быть наняты правительствами и частными компаниями для организации и проведения сложных эффективных целевых атак на частные компании с целью кражи информации, уничтожения данных или инфраструктуры. В ближайшей перспективе ожидается наиболее значительное увеличение количества угроз, связанных с экономическим и внутригосударственным кибершпионажем.

Обеспечит увеличение числа подобных атак перепрофилирование части киберпреступников, которые сейчас заняты атаками на пользователей, в кибернаемников-кибердетективов. Кроме того, весьма возможно, что услуги кибернаемников станут оказывать и те IT-специалисты, которые ранее никогда не занимались криминальной деятельностью. Этому будет способствовать ореол легитимности, который создадут работе «кибердетективов» заказы со стороны солидных компаний.

24.3. Архитектура стандартов кибернетической безопасности

Обобщенная архитектура стандартов обеспечения информационной и кибернетической безопасности организации, которая сформировалась к настоящему времени на международном уровне, представлена на ниже (рис. № 66)*.

В системе обеспечения информационной безопасности (ИБ) выделяют несколько тематических разделов. Прежде всего, это «Менеджмент ИБ» к которому относятся стандарты менеджмента идентификационными атрибутами и стандарты обеспечения безопасности личности в электронном мире.

*Стандарт ISO/IES 27032: 2012, Каталог стандартов ISO

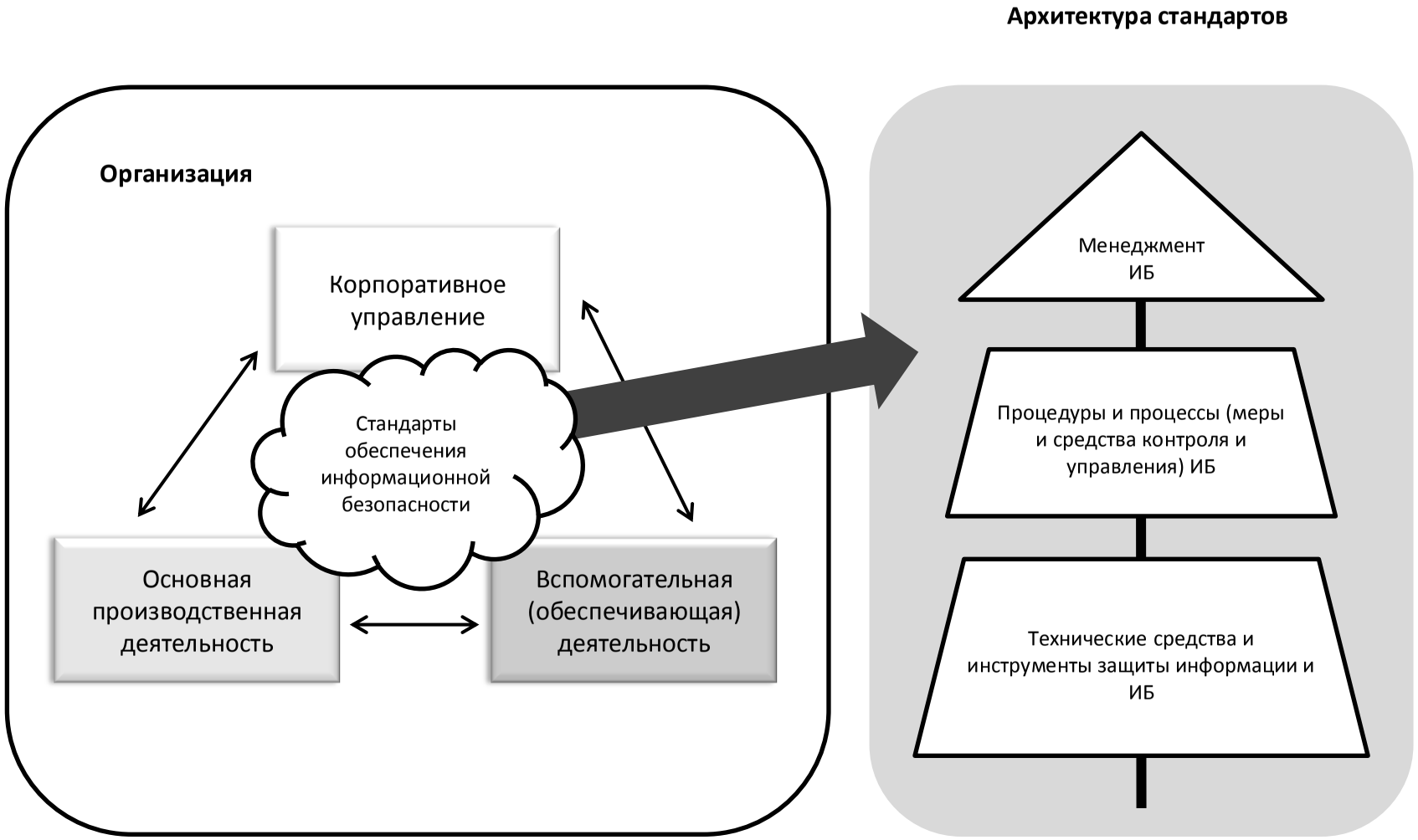

Рис. № 66. Обобщенная архитектура стандартов обеспечения информационной безопасности по Курило А.П.

К следующей категории, «Процедуры и процессы, меры и средства контроля и управления ИБ», относятся стандарты для следующих объектов и аспектов стандартизации:

- Менеджмент инцидентов информационной безопасности;
- Безопасность сетей информационных технологий;
- Обнаружение вторжений, выбора и поставки систем обнаружения вторжений;
- Управление и пользование услуг третьей доверенной стороны;
- Восстановление информационных технологий после бедствий и аварий.

К последней категории, «Технические средства и инструменты защиты информации и информационной безопасности», относятся стандарты на алгоритмы криптографических преобразований, критерии оценки безопасности информационных технологий и т. п. В области кибербезопасности основополагающим является стандарт ISO / IEC 27032: 2012, принятый в июле 2012 г. Указанный стандарт не только описывает понятие кибербезопасности, но и объясняет его связь с другими областями информационной безопасности, такими как сетевая безопасность, интернет безопасность, а также защита особо важной информационной инфраструктуры (рис. № 66). Он также определяет его взаимосвязи со стандартами, регулирующими деятельность в этих областях. В области кибербезопасности основополагающим является стандарт ISO / IEC 27032: 2012, принятый в июле 2012 г. Указанный стандарт не только описывает понятие кибербезопасности, но и объясняет его связь с другими областями информационной безопасности, такими как сетевая безопасность, интернет безопасность, а также защита особо важной информационной инфраструктуры (рис. № 67). Он также определяет его взаимосвязи со стандартами, регулирующими деятельность в этих областях.

24.4. Превентивная защита информации на автоматизированных рабочих местах, в корпоративных сетях и банках данных, при передаче с использованием Интернета, при функционировании систем электронных финансов

Российский и зарубежный опыт в области обеспечения информационной и кибернетической безопасности, а также защиты интеллектуальной собственности и государственных секретов показывает, что наибольший эффект достигается на основе использования системного подхода, когда осуществляется комплексная защита информации, включающая в себя: техническую защиту информационных ресурсов предприятия, правовую защиту на основе нормативных документов, организационную сферу, включающую в себя комплекс мероприятий, препятствующих утечке информации и использованию ее неуполномоченными лицами.

Основные объекты воздействия информационно-ударных группировок сил и средств информационного противоборства

- Программное и информационное обеспечение
- Программно-аппаратные, телекоммуникационные и другие средства информации и управления
- Каналы связи, обеспечивающие циркуляцию информационных потоков и интеграцию системы управления
- Интеллект человека и массовое сознание

С тенденцией автоматизации основных бизнес-процессов техническая защита стала одной из главных мер. В комплексную защиту информации входит использование аппаратных и программных пакетов, гарантирующих сохранность и восстановление данных. К ним относятся специальные средства администрирования, антивирусные программы, модули резервного копирования и восстановления, системы шифрования и управления доступом. Функции защиты данных все больше автоматизируются.

Представленный выше анализ угроз показывает, что традиционные средства защиты (антивирусы, файерволлы и т.д.) на сегодняшний день не способны эффективно противостоять современным киберпреступникам. Для защиты информационной системы организации требуются подходы, сочетающие несколько рубежей защиты с применением разных технологий безопасности.

Основные перспективные *технические направления* защиты.

Наиболее популярным способом защиты от внешних угроз считается система предотвращения вторжений на уровне хоста, получившая название Host-based Intrusion Prevention System (HIPS). Его правильно настроенная система даёт беспрецедентный уровень защищённости, приближенный к 100%. Грамотно выработанная политика безопасности, применение совместно с HIPS других средств защиты (например, антивирусного пакета) предоставляют очень высокий уровень безопасности. Организация получает защиту практически от всех типов вредоносного ПО, значительно затрудняет работу хакера, который решил попробовать пробить информационную защиту предприятия, сохраняет интеллектуальную собственность и важные данные организации.

Защита от *атак общей направленности.*

Рекомендации по части защиты операционных систем:

- Необходимость установления всех исправлений безопасности вне зависимости от используемых операционных систем;
- Недопущения работы сотрудников компании с административными привилегиями на системе, так как чем выше привилегии у пользователя ОС, тем больше вероятность проникновения вредоносного ПО на систему;
- Постоянное использование логина/пароля для локального входа в систему;
- Постоянное использование брендмауэра (встроенного или стороннего производителя);
- Постоянное использование антивируса известного производителя для защиты от обычных вредоносных приложений. При этом для защиты от вирусов подойдет как платный, так и бесплатный

антивирусник, в частности продукты от Лаборатории Касперского, Trend Micro, Symantec, Eset, Panda Software;

- Закрытие доступа пользователям к службам и документам, которые не требуются.
- Рекомендации в части защиты паролей:
- Использование разных логинов/паролей для доступа к разным ресурсам;
- Использование менеджеров паролей для хранения паролей, то есть приложений, умеющих безопасно сохранять пароли для доступа к разным ресурсам;

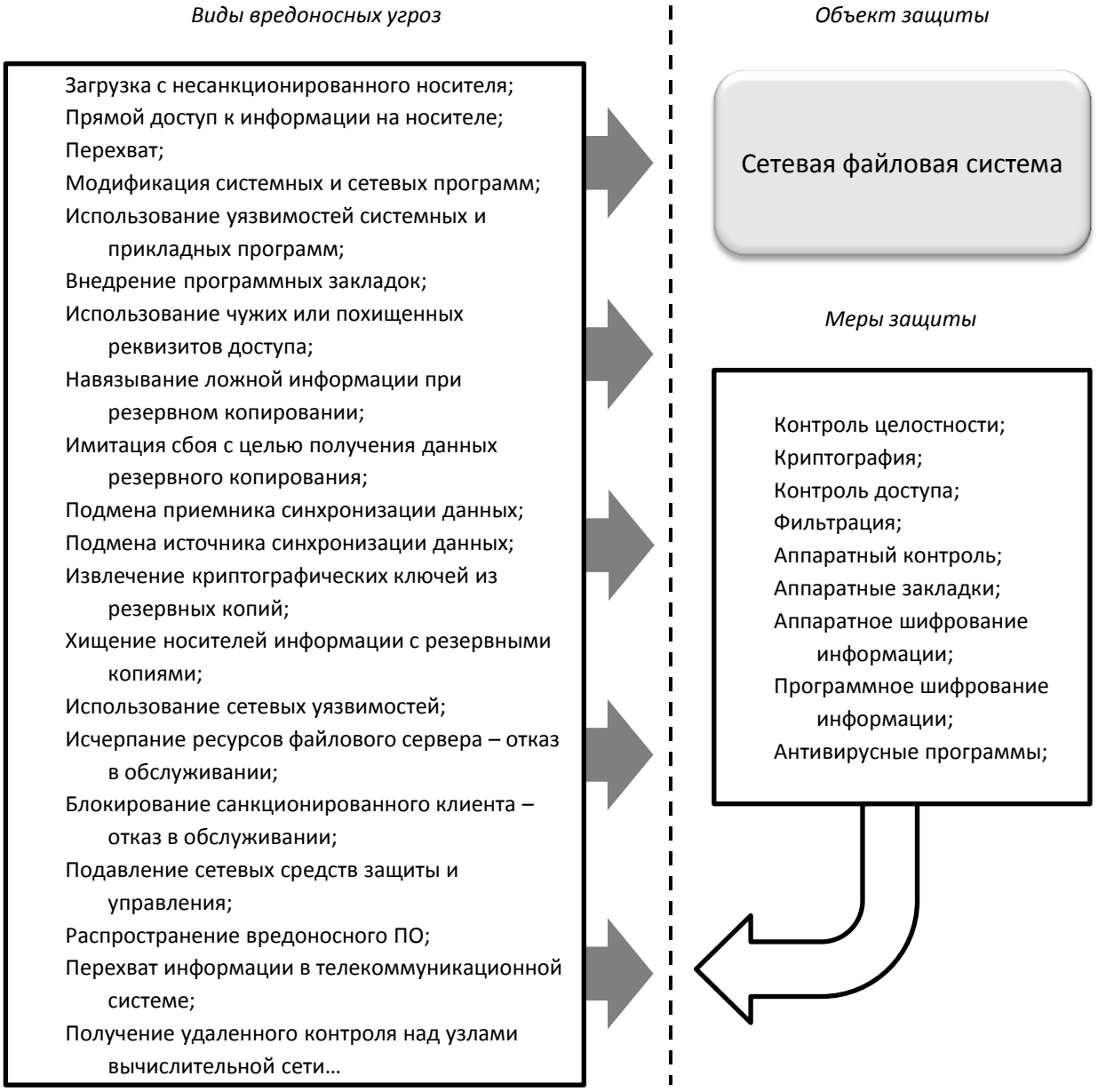

Рис. 68. Комплекс угроз в области защиты сетевой файловой системы

- Недопущение сохранения паролей в браузерах, так как современные браузеры не могут обеспечить надежную защиту учетных данных.
- Рекомендации в части защиты приложений:
    - постоянное установление исправления безопасности, направленное на защиту от функционального автоматического обновления большинство производителей программного обеспечения;
    - изолируйте важные приложения.

Безопасность автоматизированных корпоративных систем осуществляется комплексно по нескольким направлениям. К важнейшим направлениям защиты относятся: *сетевая файловая система*; *электронная почта и документооборот*; *сетевые приложения и базы данных*; *телекоммуникационные системы*. Рассмотрим защиту от типичных вредоносных угроз на примере сетевой файловой системы (рис. № 68)*.

Для доступа к банковским счетам или платежным online системам целесообразно использовать отдельные компьютеры или виртуальную операционную систему с ограниченным доступом к сети на рабочем месте и к сети Интернет. После окончания работы с банковским приложением, вы останавливаете работу Virtual PC. Если на основной системе присутствуют вредоносные приложения, они не смогут получить доступ к виртуальной системе и похитить потенциально важные данные. Кроме того, многие вредоносные приложения преднамеренно не запускаются в виртуальной среде. Это объясняется тем, что виртуальные системы используются аналитиками антивирусных компаний для изучения поведения вредоносного программного обеспечения.

Рекомендации по защите данных на АРМ:

- Избегать использования бесплатных почтовых сервисов (yandex.ru, mail.ru, gmail.com) для обмена электронными сообщениями, которые содержат конфиденциальную информацию;
- Избегать использования социальных сетей для хранения коммерческих сведений;
- Избегать пересылки конфиденциальной информации через ICQ, Jabber и др. потому что, например, QIP сохраняет всю историю переписки своих пользователей на своих серверах. Поэтому в случае компрометации ресурса, потенциально важные данные могут оказаться у ваших конкурентов;
- Избегать использования общедоступных сетей, Интернет кафе для доступа к корпоративным ресурсам;
- Защищать паролем доступ в беспроводную сеть компании;
- Шифровать конфиденциальные данные, которые сохраняются на ноутбуках сотрудников компании и выносятся ими за пределы офиса, чтобы в случае кражи ноутбука, злоумышленники не могли получить доступ к этим данным;

**Чипига А.Ф.* Информационная безопасность автоматизированных систем. М.: Гелиос АРВ, 2010. С 18-21

- Постоянно напоминать сотрудникам компании о том, какая информация является конфиденциальной и о том, что ее не следует распространять.

Рекомендации по защите от *целенаправленных атак:*

После выполнения всех рекомендаций по защите от атак общей направленности, можно приступить к защите от целенаправленных атак. При этом следует понимать, что от подобных атак полностью защититься невозможно. Существует возможность лишь максимально увеличить расходы атакующего на проведение самой атаки и тем самым сделать эту атаку нерентабельной. Никто не будет тратить десятки тысяч долларов для того, чтобы получить информацию, которая этих денег не стоит.

Для защиты от утечки данных в индустрии информационной безопасности создаются разнообразные системы защиты, традиционно обозначаемых аббревиатурой DLP (от англ. Data Leakage Prevention - предотвращение утечки данных). Как правило, это сложнейшие программные комплексы, имеющие широкий функционал по предотвращению злоумышленной или случайной утечки секретной информации. Особенностью таких систем является то, что для корректной их работы требуется строго отлаженная структура внутреннего оборота информации и документов, поскольку анализ безопасности всех действий с информацией строится на работе с базами данных. Этим объясняется высокая стоимость установки профессиональных DLP-решений: ещё перед непосредственным внедрением, компании-клиенту приходится приобретать систему управления базами данных (как правило, Oracle или SQL), заказывать дорогостоящий анализ и аудит структуры оборота информации, вырабатывать новую политику безопасности. Обычной является ситуация, когда в компании не структурировано более 80% информации, что даёт зрительное представление о масштабе подготовительных мероприятий. Разумеется, сама DLP-система тоже стоит немалых денег. Неудивительно, что профессиональную систему могут себе позволить только крупные компании, готовые тратить значительные средства на обеспечение своей информационной безопасности.

Далеко не всем компаниям требуется дорогостоящая система (типа DLP), дающая неплохие результаты по защите информационной среды предприятия от утечек, но требующая сложнейшей процедуры внедрения и пересмотра текущих механизмов документооборота. Оптимальным выбором для большинства организаций малого и среднего бизнеса станет введение функционала защиты от утечек данных, контроле документооборота и мониторинг действий пользователей локальной сети организации.

Такое решение является недорогим, простым в развёртывании и эксплуатации, но весьма эффективным инструментом внутренней безопасности.

Оптимальная защита от внутренних угроз также потребует реализации в компании целого ряда мероприятий правового и организационного характера, связанных с разработкой и внедрением должных политик информационной безопасности, введением чёткой организационной структуры, назначением ответственных за информационную безопасность сотрудников, контроле документооборота и др.

Когда намеченные меры приняты, а рекомендации реализованы, необходимо проверить их действенность. Такая проверка называется *тестирование на проникновение*. Цель – предоставление гарантий того, что для неавторизованного пользователя не существует простых путей обойти механизмы защиты. Один из возможных способов аттестации безопасности системы – приглашение независимых экспертов для осуществления попытки взлома без предварительного уведомления персонала сети. Наряду с таким способом используются программные средства тестирования.

Завершается комплекс превентивных мероприятий составлением плана защиты, вводящим в действие систему защиты информации, который утверждается руководителем предприятия (организации).

24.5. Расследование кибернетических инцидентов

Рост киберпреступности, переход её в фазу индустриализации и своеобразного развития крупного бизнеса со своими бизнес-моделями и партнерами, заставляет искать ответ на вопрос: «Существует ли сила, которая могла бы помочь бороться с киберпреступностью?» Компании, занимающиеся информационной безопасностью, по большей части нацелены сейчас только на одно – на получение максимальной прибыли, в том числе и за счет сокращения внутренних издержек предприятия. Если ситуация не изменится, то мы увидим новый мир информационных технологий, который будет полностью поглощен организованной преступностью.

Тема правового и правильного проведения расследования компьютерных инцидентов побуждает персонал информационной безопасности осуществлять не только пассивную защиту, но и активно выявлять признаки киберпреступности, документировать ее деятельность и активно взаимодействовать с уполномоченными государственными органами. Глобальная задача - создать в России культуру расследований. Это поможет

повысить степень ответственности и приведет к снижению количества преступлений, увеличит эффективность отрасли информационной безопасности для бизнеса.

Если говорить о корпоративном рынке, то есть устоявшиеся мнение – корпоративная служба безопасности может все сделать сама. Зачастую, из-за отсутствия средств, технологий, инструментария, ресурсов и опыта расследования проводятся непрофессионально и не имеют юридических перспектив. Сейчас только передовые западные и российские компании готовы к проведению такого рода мероприятий. Тактика расследования компьютерных инцидентов и преступлений зависит от обстоятельств.

Область расследования компьютерных преступлений относится к сфере тесного взаимодействия предприятия, ставшего жертвой компьютерной атаки, органов следствия и дознания, а также специалистов, обладающих навыками выявления и закрепления следов преступления (будущих судебных доказательств) в виртуальной области, а также могущих провести розыскные мероприятия в среде электронных коммуникаций и обнаружить злоумышленников.

При этом необходимо учитывать, что виновник инцидента, как правило, преследует одну из целей: разрушение системы, кража денежных средств, доступ к защищаемой информации, сокрытие других действий, атаки некоего информационного ресурса. Поэтому на начальной стадии исследования нужно ответить на вопрос о том, какие ресурсы подверглись атаке и, предположительно, кем это было сделано. Для инцидентов, нанесших существенный ущерб, проводится *процессуальное дублирование* – создание резервной копии поврежденных систем.

По практике расследования подобных правонарушений в США, судебные и правоохранительные органы предпочитают, как правило, точное побитовой копирование систем, либо просто проводят полное изъятие жестких носителей информации*. При этом корпоративные интересы пострадавших не всегда позволяют применить этот метод на практике. Многие стремятся ограничиться подробным отчетом об инциденте, с указанием точного местоположения файлов и лиц, оперировавших с ними. Это позволяет предоставлять следствию не всю информацию, а только те данные, которые имеют отношение к расследуемому событию.

Однако в этом случае исходные файлы должны быть сохранены в исходном состоянии на момент происшествия.

**Просис К., Мандиа К.* Расследование компьютерных преступлений. М.: Лори, 2012. С 24

Кейс № 27. Бесшумная атака

Компания Always on Time Transportation Co (AOTC) была прибыльной транспортной компанией, имевшей филиалы не только по всей территории Канады, но в США и Мексике*. Управляя маршрутами сотен большегрузных автомобилей, AOTC полностью зависела от компьютерной сети. Несколько лет эту сеть обслуживала компания Wylan, пока ее не заменил местный конкурент, Best Service Computers. О последней фирме было известно, что она очень быстро реагирует на звонки клиентов, но ей не хватает опыта работы с компьютерными сетями. Через некоторое время в офисе AOTC в самом начале рабочего дня обнаружили, что корпоративная сеть снова не работает. Обычно это означало, что «сервер завис» и его следует перезагрузить. При перезагрузке случилось «ужасное» - после ввода идентификатора пользователя и пароля администратора появилось сообщение «пароль неверен». Это было странно, т.к. пароль не менялся годами. Тогда администратор попытался войти в систему под личным логином и паролем. Сервер снова ответил отказом. Аналогичным образом отреагировал и другой входивший в сеть компьютер.

С учетом того, что все рабочие станции сотрудников AOTC ответили отказом, администратор немедленно обратился к сервисной компании. В Best Service не сумели поставить диагноз инцидента и предложили сразу приступить к восстановлению системы. После нескольких дней подготовки плана восстановления, когда компания AOTC несла значительные убытки, Best Service демонтировала оригинальные жесткие диски и приступила к установке новых. К сожалению, резервные копии содержали только данные компании, без приложений. Это потребовало дополнительных усилий. Только через 7 дней сеть вновь заработала. Руководство AOTC, понимая, что инцидент может повториться, обратилось в подразделение полиции, отвечающее за проведение расследований и криминалистической компьютерной экспертизы. Специалисты получили оригинальные жесткие диски сервера и образ компьютера контролера. Экспресс-анализ показал точную дату вторжения, установил одновременное нападение на несколько входивших в сеть компьютеров. В ходе нападения на одну из машин также установили программу VNC viewer, которая позволяла злоумышленникам по-прежнему иметь доступ в подвергшуюся нападению сеть. По итогам были сняты образы еще нескольких компьютеров, входивших в число пораженных. Дальнейшее обследование показало, что неизвестный осуществил нападение с помощью программы, известной как «удаленный компьютер» (RDP) и вошел под идентификатором «администратор». В журнале доступа к серверу не было зафиксировано неудачных попыток ввода логина и пароля. Пароль был буквенно-цифровой, длиной 14 знаков, содержал символы в верхнем и нижнем регистрах. Все указывало на то, что взломщик хорошо знал не только саму систему, но и пароль. При этом также было установлено, что злоумышленник поэтапно удалил с сервера ряд важных файлов, а также историю работы в Интернете. После этого была отключена активная директория, что привело к фиаско с доступом в сеть. По всем признакам, вторжение было организовано профессионалом. Он был идентифицирован благодаря тому, что в системном журнале оказалось информация о непреднамеренной ошибке – нападавший случайно запустил задание печати и тут же его отменил, но компьютер неизвестного отобразился. Это был сотрудник Wylan Джозеф Дамиен.

Вопрос: не кажется ли вам, что инцидента не случилось бы, если бы сеть управлялась по принципу «двух ключей»?

*Компьютерное мошенничество. *Под редакцией Дж.Т. Уэллса*. М.: Маросейка, 2010. С 168-174

Вопросы и задания для самоконтроля

1. Дайте определение понятий «электронные информационные ресурсы, системы и процессы» и «кибернетическая безопасность».
2. Опишите основные угрозы в области кибернетической безопасности.
3. Сообщите об основных стандартах архитектуры кибернетической безопасности предприятия.
4. Расскажите о стандартах защиты информации на автоматизированных рабочих местах (АРМ), в корпоративных сетях и банках данных, при передаче с использованием Интернета, при функционировании систем электронных финансов.
5. Сообщите об основных правилах расследования кибернетических инцидентов.

Глава 25. Взаимодействие частных и государственных институтов

В результате изучения главы студент должен **знать** аспекты нормативно-правовой базы, существующей в нашей стране в области защиты информации; основы расследования информационных инцидентов силами самого предприятия, с использованием аутсорсинга (возможностей специализированных участников рынка); **уметь** устанавливать роль и место государства в обеспечении различных видов информационной безопасности; **владеть** основными правилами взаимодействия с государственными институтами в области информационной безопасности, включая вопросы участия в расследовании возбужденных уголовных дел.

25.1. Нормативно-правовая база в сфере информационной безопасности

Информация является объектом, по поводу которой возникают определенные отношения, которые имеют социальное, правовое и научное значение, нуждаются в регулировании со стороны государства и общества. Это послужило основой для формирования самостоятельной отрасли правовых отношений, которая получило название информационного права. Одной из важнейших форм реализации информационного права является защита информации. Правовая защита информации представляет собой защиту данных правовыми методами, которые включают в себя разработку законодательных и иных нормативно-правовых документов, которые регулируют отношения субъектов по защите информации, применение этих документов, а также надзор и контроль в сфере их практического исполнения. Правовая база должна обеспечивать следующие основные функции:

1. Обеспечение авторского права;
2. Разработку основных принципов отнесения данных к защищаемой информации;
3. Определение системы обеспечение информационной безопасности и порядка регулирования деятельности предприятий и организаций в этой области;
4. Создание полного комплекса нормативно-правовых и иных материалов (документов), которые регламентируют вопросы обеспечения информационной безопасности на всех уровнях;
5. Определение мер ответственности за нарушение правил защиты;
6. Определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

Объекты существуют, движутся и взаимодействуют в реальном (материальном) мире и информационном мире параллельно (рис. № 69). Частично это взаимодействие происходит в виде отдельных транзакций, а частично в виде управления и регулирования. При этом в ряде случаев действия над материальными объектами сопровождаются, а в некоторых случаях заменяются, действиями над их описаниями.

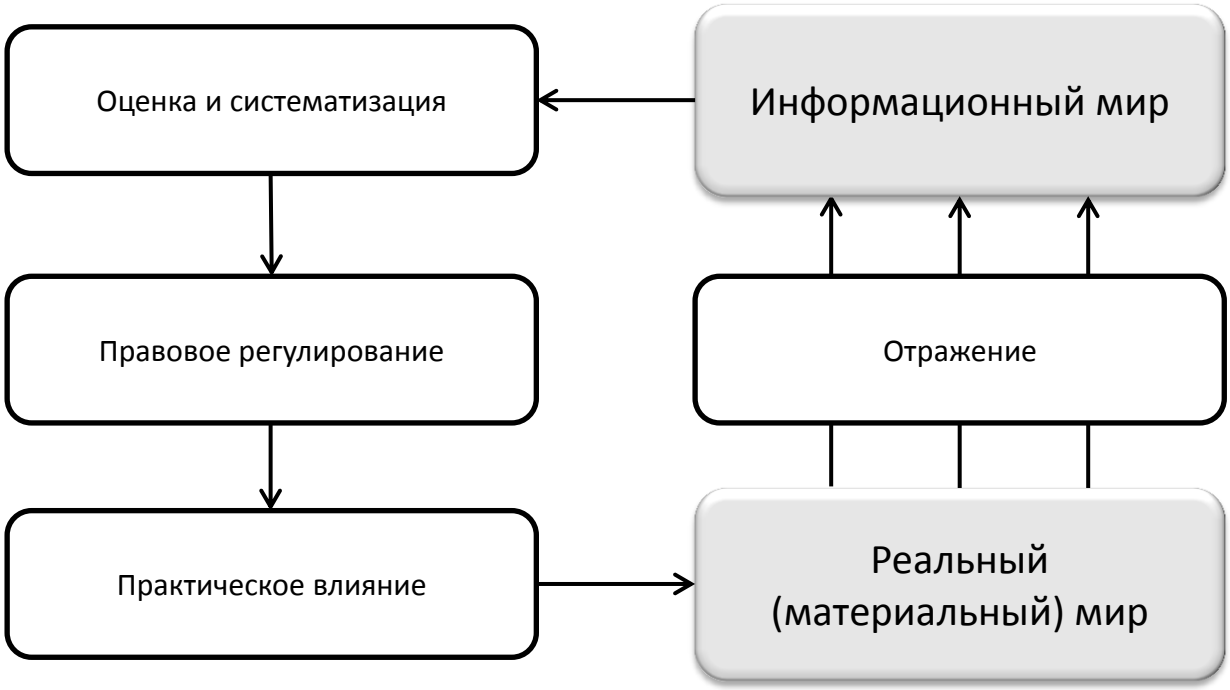

Рис. 69. Соотношение реального и информационного миров

Именно таким образом осуществляется правовое регулирование в области обеспечения информационной безопасности современного бизнеса. При этом правовые

режимы пользования конкретной информацией устанавливаются правомочными субъектами (владельцами информации) или уполномоченными органами государственной и муниципальной власти, в целях формирования однородных режимов пользования информацией при взаимодействии личности, бизнеса и государства. В Российской Федерации такие режимы обращения информации сформированы на уровне федерального законодательства, иных нормативно-правовых актов органов государственной власти и управления, органов муниципальной власти, а также в рамках полномочий субъектов предпринимательской деятельности. Ряд вопросов технического регулирования в сфере обработки и защиты информации установлены соответствующими государственными стандартами, которые обязательны для ряда субъектов права.

При этом на федеральном уровне устанавливаются категории информации, которая не может быть отнесена к разделу конфиденциальной, категории специально защищаемой информации в зависимости ее относимости и важности, субъекты правообладания и уровни осуществления полномочий по регулированию движения такой информации.

25.2. Участие государства в обеспечении информационной безопасности

Основная задача государственной системы защиты информации заключается в осуществлении единой технической политики, организации и координации работы по защите данных в экономической, оборонной, научно-технической, политической и других сферах деятельности государства. Общую организацию и координацию работы в государстве по защите данных, которые обрабатываются техническими средствами, осуществляет Федеральная служба по техническому и экспортному контролю (ФСТЭК России). Эта служба является федеральным органом исполнительной власти, который осуществляет организацию межведомственной координации и взаимодействия, реализацию государственной политики, специальные и контрольные функции в области обеспечения информационной безопасности:

1) Обеспечение безопасности данных в системах телекоммуникационной и информационной инфраструктуры, которые оказывают существенное влияние на безопасность в информационной сфере;
2) Противодействие иностранным техническим разведкам на территории Российской Федерации;
3) Обеспечение защиты данных, которые содержат сведения, составляющие государственную тайну, или других данных с ограниченным доступом, предотвращение несанкционированного доступа к

ней, ее утечки по техническим каналам, уничтожения, искажения и блокирования доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания на территории РФ;
4) Защита данных при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

Нормативные правовые акты и методические документы, которые изданы по вопросам деятельности ФСТЭК России, являются обязательными для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов РФ, органами местного самоуправления и организациями, федеральными органами исполнительной власти, органами исполнительной власти субъектов РФ. В свою очередь, ФСТЭК России осуществляет свою деятельность во взаимодействии с другими федеральными органами исполнительной власти Российской Федерации.

Одним из основных направлений деятельности Федеральной службы безопасности Российской Федерации (ФСБ России) является обеспечение информационной безопасности, которое осуществляется им в пределах своих полномочий:

- Во время формирования и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием криптографических и инженерно-технических средств;
- Во время обеспечения инженерно-техническими и криптографическими методами безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи России и ее учреждениях, которые находятся за пределами страны.

В своей деятельности Служба внешней разведки РФ может при наличии собственных органов лицензировании и сертификации приобретать, создавать, разрабатывать (за исключением криптографических средств защиты), эксплуатировать информационные системы, системы передачи данных, системы связи, средства защиты информации от утечки по техническим каналам. Министерство обороны Российской Федерации организует деятельность по защите государственной тайны в Вооруженных силах, обеспечению информационной безопасности и сертификации средств защиты информации, в установленном порядке и в пределах своей компетенции.

Другие органы государственного управления (министерства, ведомства) в пределах своей компетенции могут:

- Определять перечень охраняемых данных;

- Обеспечивать разработку и осуществление экономически и технически обоснованных мер относительно защиты данных на подведомственных организациях;
- Организовать и координировать проведение НИОКР в области защиты данных в соответствии с государственными (отраслевыми) программами;
- Разрабатывать отраслевые документы по защите данных;
- Контролировать выполнение на организациях отрасли установленных норм и требований по защите данных;
- Создавать центры по защите данных и контролю эффективности принимаемых мер;
- Организовывать подготовку и повышение квалификации специалистов по защите данных.

На предприятиях, которые выполнят оборонные и иные секретные работы, должны функционировать научно-технические подразделения защиты данных и контроля, которые призваны участвовать в разработке и реализации мер по защите данных, координировать деятельность в этом направлении производственных и научных структурных подразделений предприятия, осуществлять контроль эффективности этих мер. Кроме этого, в отраслях промышленности должны создаваться и функционировать органы по сертификации средств вычислительной техники и средств связи; лицензионные центры, которые осуществляют организацию и контроль за лицензионной деятельностью в области оказания услуг по защите данных; органы по аттестации объектов информатики; испытательные центры по сертификации конкретных видов продукции относительно требований безопасности данных.

Государственная система обеспечения информационной безопасности требует обязательной законодательной поддержки и создается для решения следующих проблем:

- Защиты персональных данных;
- Борьбы с компьютерной преступностью, прежде всего, в финансовой сфере;
- Обеспечения благоприятных условий для предпринимательской деятельности и защиты коммерческой тайны;
- Защиты государственных секретов;
- Создания системы взаимных финансовых расчетов в электронной форме с элементами цифровой подписи;
- Обеспечения безопасности АСУ потенциально опасных производств;
- Страхования данных и информационных систем;
- Контроля безопасности информационных систем; сертификации и лицензирования в области безопасности;
- Организации взаимодействия в сфере защиты информации со странами-членами СНГ и другими государствами.

При этом ключевые проблемы, которые решаются в сфере информационной безопасности при участии государства, представляют собой:

- Формирование нормативно-правовой и законодательной базы обеспечения информационной безопасности, в том числе разработка регламента информационного обмена для органов государственной власти и управления, нормативного закрепления ответственности должностных лиц и граждан по соблюдению требований информационной безопасности, реестра информационного ресурса;
- Разработка механизмов реализации прав граждан на данные;
- Формирование системы информационной безопасности, которая обеспечивает реализацию государственной политики в этой области;
- Совершенствование методов и технических средств, которые обеспечивают комплексное решение задач защиты данных;
- Разработка критериев и методов оценки эффективности систем и средств информационной безопасности;
- Исследование форм и способов цивилизованного воздействия государства на формирование общественного сознания;
- Комплексное исследование деятельности персонала информационных систем, в том числе методов морально-психологической устойчивости, социальной защищенности людей, повышения мотивации, которые работают с секретными и конфиденциальными данными.

25.3. Информационные инциденты, требующие взаимодействия с государством

В современных условиях правительства разных стран мира уделяют все больше внимания проблемам обеспечения информационной безопасности, в том числе и в национальном масштабе. В официальных заявлениях и публикациях российских правительственных организаций данный тренд находит особое отражение, что особенно четко заметно на фоне масштабных программ по развитию и внедрению информационных технологий в различные отрасли экономики РФ. Однако по-прежнему остается проблема оценки степени рисков, которые связаны с атаками компьютерных злоумышленников на компании, задействованные в отраслях, которые необходимых для нормального функционирования государства, экономики и общества.

Исследования российских и зарубежных специалистов в области компьютерной безопасности показывают, что отечественные объекты критической инфраструктуры активно подвергаются атакам со стороны компьютерных злоумышленников. При этом большинство компаний, системы которых подверглись атакам, не смогли определить успешность этих атак. Это свидетельствует о том, что уровень защиты информационных ресурсов значительно ниже, чем в других странах. Общий индекс защищенности в России составляет -7%, а в среднем по миру он равен +25%. Данная ситуация возможна потому,

что многие руководители российских компаний склонны экономить на вопросах информационной безопасности и не осознают того факта, что их организации являются объектом постоянных хакерских атак со стороны организованных киберпреступников.

Рост уровня защищенности российских предприятий напрямую зависит от скорейшего внедрения современных инструментов обеспечения информационной безопасности. При этом, в первую очередь, необходимо заботиться не только о технических решениях защиты и мониторинга, но и об организационных мерах. Например, аудит защищенности АСУ ТП (автоматические системы управления технологическими процессами) помогает увидеть слабые места в системе защиты технологических объектов и получить рекомендации по их точечному устранению. А разработка и внедрение на предприятии системы управления инцидентами информационной безопасности позволит подготовиться к реагированию на возможные внештатные ситуации и при этом не зависеть от наличия технических средств.

Учитывая все возрастающие требования со стороны регуляторов в части мониторинга информационных инцидентов, а также в целях стандартизации и оптимизации деятельности предприятий по реагированию на инциденты и управлению ими, были определены основные группы информационных инцидентов, требующих взаимодействия с правоохранительными органам, а также с государственными структурами. На самом верхнем уровне все инциденты могут быть разделены на внутренние и внешние.

Внутренний инцидент – инцидент, источником которого является нарушитель, связанный с пострадавшей стороной непосредственным образом (трудовым договором или иным способом). Среди системных событий такого типа можно выделить следующие наиболее распространенные:

- Утечка конфиденциальной информации;
- Неправомерный доступ к информации;
- Удаление информации;
- Компрометация информации;
- Саботаж;
- Мошенничество с помощью информационных технологий;
- Аномальная сетевая активность;
- Аномальное поведение бизнес-приложений;
- Использование активов компании в личных целях или в мошеннических операциях.

Внешний инцидент – инцидент, источником которого является нарушитель, не связанный с пострадавшей стороной непосредственным образом. Среди системных событий такого типа можно выделить следующие наиболее распространенные:

- мошенничество в системах дистанционного банковского обслуживания;
- атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS);
- перехват и подмена трафика;
- неправомерное использование корпоративного бренда в сети Интернет;
- фишинг;
- размещение конфиденциальной/провокационной информации в сети Интернет;
- взлом, попытка взлома, сканирование портала компании;
- сканирование сети, попытка взлома сетевых узлов;
- вирусные атаки;
- неправомерный доступ к конфиденциальной информации;
- анонимные письма (письма с угрозами).

Зачастую действия компьютерных злоумышленников вступают в противоречие с действующим уголовным законодательством и посягают на охраняемые уголовным правом общественные отношения. В настоящее время предусмотрена уголовная ответственность за такие деяния, как «неправомерный доступ к компьютерной информации», «создание, использование и распространение вредоносных программ для ЭВМ» и «нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети».

Помимо самостоятельного регулирования преступлений в сфере компьютерной информации в ряде случаев правоохранительными и судебными органами перечисленные выше статьи используются в совокупности с другими статьями УК РФ. Например, мошенничество в сети Интернет квалифицируется по статье «мошенничество в сфере компьютерной информации». Данный состав преступления имеет ряд квалифицирующих признаков: хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

В 2012 г. с целью совершенствования системы безопасности информационных сетей государственных учреждений ФСБ России создан Центр реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации «GOV-CERT.RU», основной задачей которого является предотвращение, выявление и ликвидация последствий кибератак. Основной его задачей является осуществление координации действий для предотвращения, выявления и ликвидации последствий инцидентов, в которые были вовлечены не только объекты в сегменте RSNET (Russian State Network), но и другие организации, являющиеся частью информационной инфраструктуры РФ. В настоящее время ведутся активные работы по включению в систему мониторинга и управления инцидентами также организаций банковского и промышленного секторов в интересах:

- Оказания им консультативной и методической помощи при проведении мероприятий по устранению последствий компьютерных инцидентов;
- Анализа причин и условий возникновения таких инцидентов;
- Разработки перечня рекомендаций по способам нейтрализации актуальных угроз безопасности информации;
- Реализации взаимодействия с российскими, иностранными и международными организациями, осуществляющими реагирование на компьютерные инциденты.

При выявлении компьютерных инцидентов, создающих угрозу функционированию предприятий и организаций (вне зависимости от формы собственности), подразделения информационной безопасности должны не только проводить их техническую, но и правовую оценку. Это позволит не только ставить правильный «диагноз» происшествия, но и обращаться в уполномоченные правоохранительные органы с заявлениями о выявлении признаков уголовно наказуемых деяний, что позволит привлечь виновных к ответственности и не допустить совершения ими иных преступлений в сфере компьютерной информации. Такая позиция субъектов предпринимательской деятельности позволит повысить раскрываемость киберпреступлений и обеспечить реализацию на практике принципа неотвратимости наказания.

Вопросы и задания для самоконтроля

1. Расскажите об особенностях нормативно-правовой защиты кибернетической информации в нашей стране.
2. Расскажите о мерах государственного контроля в области обеспечения безопасности кибернетической информации.
3. Сообщите об участии уполномоченных государственных органов в защите кибернетической информации в реальном секторе экономики от неправомерных посягательств.
4. Расскажите о самозащите гражданских прав предприятия в случае совершения кибернетического инцидента.
5. Сообщите об информационных инцидентах в сфере кибернетической безопасности, требующих взаимодействия с уполномоченными органами государства.