МВД России
Санкт-Петербургский университет

И.Н. Васильева, О.Г. Смирнова

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Санкт-Петербург
2017

План 2017, поз. 26

УДК 004.732.056 (075.8)
ББК 32.973.2-018.2я73
О68

О68 Основы информационной безопасности в органах внутренних дел: учебное пособие / О.Г. Смирнова, И.Н. Васильева. СПб.: Изд-во СПб ун-та МВД России, 2017. – 148 с.

В учебном пособии представлены базовые понятия информационной безопасности, основные концепциями и принципы организации современных систем защиты информации, их правовое обоснование и организационная поддержка, а также направления и методы обеспечения информационной безопасности с учетом того, что возможности, которые в себе несут компьютерные и информационные технологии, значительно усиливают ущерб от их преступного применения. Основной целью издания является формирование кругозора в сфере правовых, организационных и инженерно-технических методов защиты информации.

Предназначено для обучающихся Санкт-Петербургского университета МВД России.

УДК 004.732.056 (075.8)
ББК 32.973.2-018.2я73

Рецензенты:
А.Н. Бабкин, кандидат технических наук, доцент
(Воронежский институт МВД России);
А.В. Костюк, кандидат технических наук, доцент
(Санкт-Петербургский военный институт войск национальной гвардии Российской Федерации)

Оглавление

ВВЕДЕНИЕ

Современное общество и то, как в нем живет человек, все в большей степени зависят от информации и знания людей. Информатизация дает определенные преимущества современному человеку, снижает его затраты и повышает полезность его действий. Вместе с тем зависимость людей от информации определяет и их уязвимость, связанную с недостатками в методах и недостатками технической среды информационных процессов: технические сбои, нарушения при передаче информации, человеческие ошибки при вводе информации, логические – в программах ее обработки. Угрозы могут исходить от случайных причин, а могут определяться преднамеренными действиями каких-либо заинтересованных людей и сообществ. В любом случае существуют способы снизить риски этих угроз, а также их вредные последствия. Некоторые информационные процессы и отношения, которые в них возникают, являются предметом информационного права. Законодательство является частью среды, в которой проходят информационные процессы, и оказывает на них преднамеренное влияние.

Эта область права – одна из самых быстроразвивающихся. Изменения, которые происходят в компьютерной технике и средствах связи, доступность информации – все это обнаруживает неочевидные и невидимые ранее противоречия в информационном праве. Возникающие правовые вопросы часто требуют определенных познаний в области информатики, техники, средств связи, которые не входят в круг компетенции, например, суда и следователя. Однако в соответствии со ст. 11 федерального закона «О полиции»:

1. В своей деятельности полиция обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру.

2. Полиция в порядке, установленном законодательством Российской Федерации, *применяет электронные формы приема и регистрации документов,* уведомления о ходе предоставления государственных услуг, взаимодействия с другими правоохранительными органами, государственными и муниципальными органами, общественными объединениями и организациями.

3. Полиция использует технические средства, включая средства аудио-, фото- и видеофиксации, при документировании обстоятельств совершения преступлений, административных правонарушений, обстоятельств происшествий, в том числе в общественных местах, а

также для фиксирования действий сотрудников полиции, выполняющих возложенные на них обязанности.

При этом, согласно закону, федеральный орган исполнительной власти в сфере внутренних дел обеспечивает полиции возможность использования информационно-телекоммуникационной сети Интернет, автоматизированных информационных систем, интегрированных банков данных (ст.11 п. 4).

Поэтому сотруднику полиции необходимо владеть навыками по использованию технических и электронных средств в информационной сфере. Использование информационно-телекоммуника-ционной сети Интернет в служебной деятельности обеспечивает возможность быстрого поиска и обработки необходимой информации, в том числе и конфиденциальной.

На основании п. 32 и 33 ст. 13 сотрудник полиции имеет право:

– получать, учитывать, хранить, классифицировать, использовать, выдавать и уничтожать в соответствии с законодательством Российской Федерации дактилоскопическую информацию и геномную информацию;

– вести видеобанки и видеотеки лиц, проходивших (проходящих) по делам и материалам проверок полиции;

– формировать, вести и использовать банки данных оперативно-справочной, криминалистической, экспертно-криминалистической, розыскной и иной информации о лицах, предметах и фактах;

– использовать банки данных других государственных органов и организаций, в том числе персональные данные граждан, если федеральным законом не установлено иное.

Для реализации данного права необходимым становится не только создание условий для данной деятельности, но и своевременное обнаружение, и устранение угроз информационной безопасности.

В соответствии со ст. 17 полиция имеет право обрабатывать данные о гражданах, необходимые для выполнения возложенных на нее обязанностей, с последующим внесением полученной информации в банки данных о гражданах. Автоматически данная информация становиться ограниченной к доступу и подлежит защите в соответствии с законодательством. В соответствии с п. 4 данной статьи полиция *обеспечивает защиту информации*, содержащейся в банках данных, от неправомерного и случайного доступа, уничтожения, копирования, распространения и иных неправомерных действий. Обработка персональных данных осуществляется в соответствии с требованиями, установленными законодательством Российской Федерации в области персональных данных.

Реализуя данную норму, полицейский обязан обладать навыками по созданию и ведению электронных банков данных. Информация, содержащаяся в банках, носит *конфиденциальный характер* и имеет *статус служебной тайны***.** Поэтому п. 4, 7, 8 данной статьи возлагают на сотрудника полиции ответственность за обеспечение защиты данной информации от неправомерного и случайного доступа, уничтожения, копирования, распространения и иных неправомерных действий.

Для обеспечения защиты государственной тайны, конфиденциальной информации полицейский должен обладать знаниями в области современных информационных технологий, использовать на практике достижения современной науки и техники, а также современную информационно-телекоммуникационную инфраструктуру.

Целью настоящего пособия является формирование представлений о вопросах информационной безопасности у специалистов-гуманитариев, которые с этими вопросами могут сталкиваться в практической деятельности.

Глава 1. ПОНЯТИЕ И СУЩНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Понятия информационной безопасности

Безопасность – такое состояние системы, когда действие внешних и внутренних факторов не приводит к ее ухудшению, к невозможности ее функционирования и развития. В соответствии с этим под информационной безопасностью можно понимать такое ее состояние, когда никакие факторы не снижают ее ценности для собственника или владельца и не ограничивают использования этой ценности.

В зависимости от того, кто является собственником, встречаются, например, такие определения:

– *информационная безопасность организации* – состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в организации;

– *информационная безопасность государства* – состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере.

Рассмотрение условий утраты ценности информации приводит к модели информационной безопасности, включающей три категории, которые называют критериями безопасности:

– *конфиденциальность*, то есть доступность информации только определенному кругу лиц;

– *целостность*, сохранность информация в определенном необходимом собственнику виде;

– *доступность*, возможность использования информации собственником при необходимости.

Таким образом, б*езопасность информации* – состояние защищенности информации, при котором обеспечены её конфиденциальность, доступность и целостность.

В мире сложилась система концептуальных взглядов на вопросы информационной безопасности. Понятно, что обеспечить стопроцентную безопасность не могут никакие методы и средства. Примером может служить любая антивирусная программа, которая обеспечивает безопасность компьютера только от известных ей вирусов, а распознать новые она не в состоянии. Поэтому сегодня трудно представить на компьютерах у пользователей не обновляемый автоматически антивирусный программный продукт. Специалисты по информационной безопасности предлагают все новые методы и средства защиты информации, связанные с развитием информационных тех-

нологий, но обеспечить полную безопасность информации не удается. Этому способствуют многочисленные условия и факторы информационной среды.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. *Документированная информация* (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Источник информации – материальный объект, обладающий определенными сведениями (информацией), представляющими конкретный интерес для злоумышленников или конкурентов.

В общем плане, без значительной детализации можно считать источниками конфиденциальной информации следующие категории:

– людей (сотрудники, обслуживающий персонал, продавцы, клиенты и др.);

– документы самого различного характера и назначения;

– публикации (доклады, статьи, интервью, проспекты, книги и т. д.);

– технические носители информации и документов;

– технические средства обработки информации (автоматизированные средства обработки информации и средства обеспечения производственной и трудовой деятельности, в том числе и средства связи);

– выпускаемую продукцию;

– производственные и промышленные отходы.

Информацию можно структурировать и классифицировать, исходя из различных признаков:

а) по степени доступа – общедоступная информация; информация, доступ к которой не может быть ограничен; информация с ограниченным доступом; информация, не подлежащая распространению (*доступ к информации* (доступ) – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации; *доступность* (санкционированная доступность) информации – состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия);

б) по степени систематизации – систематизированная в информационных системах (каталоги, энциклопедии, рубрикаторы и т. д.) и несистематизированная информация, то есть свободная;

в) по виду носителя – на бумажном носителе, видео- и звуковая, компьютерная информация;

г) по сфере применения – массовая информация, распространяемая через СМИ, сеть Интернет, и отраслевая, предназначенная для круга лиц, связанного профессиональными интересами.

Объектом защиты информации может быть информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации, это *защищаемая информация*. К защищаемой информации относятся государственная и профессиональная тайны, коммерческая тайна, интеллектуальная собственность и другие виды информации.

Носитель защищаемой информации – это физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Под *защитой информации* понимаются любые действия, направленные на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Главным показателем при выборе средств и методов защиты информации считают ее ценность – реальную или потенциальную. Ценность информации определяется возможным ущербом от ознакомления с ней конкурентов, приносимым от нее доходом, значением, которое она имеет в обеспечении процессов.

Каждая защита тоже имеет свою степень и свою цену. Бессмысленно тратить на защиту больше, чем может стоить сама информация. Поэтому главный критерий на средства защиты информации простой: затраты на них не должны превышать ценности информации. Для конкурентов же эта ценность должна компенсировать риск, связанный с ее получением (добыванием).

Для повышения эффективности защиты информации рассматривают ее возможные *уязвимости* – характерные особенности и недостатки в защите.

Целью защиты информации является сокращение потерь, вызванных нарушением целостности или потерями данных, нарушением

их конфиденциальности или недоступностью информации для ее потребителей.

Основными задачами системы информационной безопасности являются:

– анализ источников угроз, причин, условий и уязвимостей защищаемой информации;

– разработка системы защиты, механизмов и условий оперативного реагирования на угрозы безопасности;

– разработка системы ответственности и проведение мероприятий по включению системы защиты в организации;

– создание условий для минимизации и локализации возможного ущерба, ослабления негативного влияния последствий.

Цели и задачи защиты достаточны для формирования общего взгляда на построение системы информационной безопасности. Для более детального представления необходимо знание основных принципов организации системы информационной безопасности.

1.2. Принципы организации системы информационной безопасности

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных принципах:

– соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;

– открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;

– правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

– приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подклю-

чение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Государство в процессе реализации своих *функций* по обеспечению информационной безопасности Российской Федерации:

– проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности Российской Федерации, разрабатывает меры по ее обеспечению;

– организует работу законодательных (представительных) и исполнительных органов государственной власти Российской Федерации по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации;

– поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;

– осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;

– проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории Российской Федерации и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

– способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;

– формулирует и реализует государственную информационную политику России;

– организует разработку федеральной программы обеспечения информационной безопасности Российской Федерации, объединяющей усилия государственных и негосударственных организаций в данной области;

– способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Принцип – некоторое положение, из которого исходят в какой-либо стороне действительности. Для защиты информации ее принци-

пы должны обеспечивать ее эффективность – меньшие затраты, бóльшая результативность.

Непрерывное совершенствование. Суть принципа – в постоянном выявлении слабых мест системы защиты, которые обнаруживаются или могут возникать при изменениях внутренних и внешних условий системы.

Комплексный характер. Защита использует все доступные средства, распространяется на все структурные элементы организации и на все этапы работы с информацией. Исходят из того, что злоумышленники ищут самое слабое звено в системе безопасности.

Достаточность. Если какие-либо средства обеспечивают необходимый уровень защиты в некотором направлении, то других средств в этом направлении привлекать нет необходимости.

Законность. Все меры и средства не должны выходить за рамки закона.

Подготовка сотрудников. Знания и умения, связанные с защитой информации, которые ожидаются от пользователей и сотрудников системы безопасности, должны целенаправленно формироваться некоторой систематической подготовкой.

Взаимодействие с правоохранительными органами. Не все вопросы безопасности организация может решить своими силами. Часть вопросов может быть переложена на государственную правоохранительную систему.

С позиций системного подхода можно назвать ряд требований на процесс и саму систему защиты информации, которая должна быть:

– открытой для изменения и дополнения;

– разнообразной по используемым средствам;

– эффективной экономически (как уже говорилось, затраты на систему защиты не должны превышать размеры возможного ущерба).

Наряду с основными требованиями существует ряд устоявшихся рекомендаций создателям систем информационной безопасности:

– средства защиты должны быть просты для технического обслуживания и «прозрачны» для пользователей;

– каждый пользователь должен иметь минимальный набор привилегий, необходимых для работы;

– система защиты должна быть независимой от субъектов защиты;

– разработчики должны предполагать, что пользователи имеют наихудшие намерения, что они будут совершать серьезные ошибки и искать пути обхода механизмов защиты;

– в организации информация о существовании и механизмах защиты должна быть доступна в пределах компетенции и служебных обязанностей сотрудников.

Изложенные концептуальные положения являются основой конкретных предложений по формированию политики и построению системы информационной безопасности.

1.3. Понятие политики безопасности

Политика безопасности – совокупность правил, которым должны следовать люди, программы и устройства при действиях с информацией. Этот термин чаще всего используется по отношению к организации.

Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Комплект документов может включать:

– концепцию безопасности (систематически изложенные взгляды на основные направления, условия и порядок практического решения задач защиты деятельности организации от противоправных действий и недобросовестной конкуренции – цели и задачи, принципы, объекты защиты, виды угроз, правовые основы, техническое обеспечение и т. д.);

– Положение о конфиденциальной информации (перечень, учет, хранение и использование, порядок допуска, меры по контролю, ответственность);

– Положение об использовании информационной системы;

– Положение об использовании мобильных устройств и носителей информации;

– Положение об учете, хранении и использовании ключевой информации;

– Положение об использовании программного обеспечения;

– Положение об использовании сети Интернет;

– Положение об использовании электронной почты;

– Положение об обучении сотрудников;

– Положение о системе резервного копирования (система, стратегия, порядок, организация резервного копирования, задачи, права, ответственность администратора);

– Положение об отделе информационных технологий;

– должностные инструкции (начальника отдела информационных технологий, инженера-электроника этого отдела и т. д.), определяющие требования, компетенцию, выполняемые обязанности, права и ответственность.

В документах рассматриваются две группы мероприятий – по построению (формированию) системы защиты и по использованию системы для защиты информации.

Политика информационной безопасности определяет облик системы защиты информации – правовые нормы, организационные меры, программно-технические средства, процедуры, направленные на противодействие угрозам, минимизацию возможных последствий. Для каждого вида потенциальных проблем обычно назначается ответственный исполнитель.

Контроль состояния должен получать ответы на вопросы:

– сколько компьютеров (вспомогательного оборудования) установлено в организации, сколько их на рабочих местах, сколько в ремонте, сколько в резерве;

– какие задачи и с какой целью решаются на каждом компьютере;

– можно ли узнать каждый компьютер «в лицо» и обнаружить «маскарад» оборудования, когда какой-нибудь компьютер, его часть или программное обеспечение подменены;

– есть ли уверенность в необходимости каждой единицы контролируемого оборудования и в том, что среди него нет ничего лишнего? Наличие избыточного оборудования приводит к дублированию функций, затруднению и, в конечном счете, ослаблению контроля, что может нанести урон безопасности;

– каков порядок ремонта и технической профилактики компьютеров;

– как проверяется оборудование, возвращаемое из ремонта, перед установкой на рабочее место;

– как производится изъятие и передача компьютеров в подразделения и каков порядок приема в работу нового оборудования.

Аналогичные вопросы выясняются в отношении программного обеспечения и персонала.

Другими словами, защита информации начинается с постановки и решения организационных вопросов. Практика деятельности в сфере обеспечения информационной безопасности в автоматизированных показывает, что реальный интерес к проблеме защиты информации, проявляемый на верхнем уровне управления, на уровне подраз-

делений, отвечающих за работоспособность автоматизированной системы, сменяется на резкое неприятие.

Как правило, приводятся следующие аргументы против проведения работ и принятия мер по обеспечению информационной безопасности:

– появляются дополнительные ограничения для пользователей, затрудняющие использование и эксплуатацию автоматизированной системы организации;

– как правило, дополнительные действия, которые возлагаются на пользователей, не сопровождаются дополнительной оплатой труда;

– возникают дополнительные материальные затраты как на проведение таких работ, так и на расширение штата специалистов, занимающихся информационной безопасностью.

Экономия на информационной безопасности может выражаться в различных формах, крайними из которых являются:

– принятие только организационных мер защиты информации;

– использование только технических средств защиты.

В первом случае, как правило, разрабатываются многочисленные инструкции, приказы и положения, требования которых (при отсутствии соответствующего технического обеспечения) затрудняют повседневную деятельность сотрудников организации и, как правило, не выполняются. Во втором случае приобретаются и устанавливаются дополнительные технические средства. Их применение без соответствующей организационной поддержки только усиливает существующий беспорядок.

Рассмотрим комплекс организационных мер, необходимых для реализации защиты информации в компьютерных системах. С одной стороны, эти меры должны быть направлены на обеспечение правильности функционирования механизмов защиты и выполняться администратором безопасности системы. С другой стороны, руководство организации, эксплуатирующей средства автоматизации, должно регламентировать правила автоматизированной обработки информации, включая и правила ее защиты, а также установить меру ответственности за нарушение этих правил.

По времени проведения мероприятия могут быть:

– разовые (однократные и повторяемые только при полном пересмотре принятых решений);

– периодические (через определенное время);

– проводимые при возникновении определенных условий или изменений в самой защищаемой системе или среде (по необходимости);

– постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.

К разовым мероприятиям относятся:

– общесистемные мероприятия по созданию научно-технических и методологических основ (концепции и других руководящих документов) защиты;

– мероприятия при проектировании, строительстве и оборудовании вычислительных центров и других объектов (исключение тайного проникновения в помещения, установки аппаратуры и т. п.);

– мероприятия при проектировании, разработке и вводе в эксплуатацию технических средств и программного обеспечения (проверка и сертификация используемых средств, документирование и т. п.);

– разработка и утверждение функциональных обязанностей должностных лиц службы компьютерной безопасности;

– внесение необходимых изменений и дополнений в организационно-распорядительные документы (положения о подразделениях, функциональные обязанности должностных лиц, инструкции пользователей системы и т. п.) по вопросам обеспечения безопасности программно-информационных ресурсов и действиям в случае кризисных ситуаций;

– определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к ресурсам системы;

– разработка правил управления доступом к ресурсам системы (определение перечня задач, решаемых структурными подразделениями организации с использованием компьютерных средств, а также используемых при их решении режимов доступа к данным; перечня файлов и баз данных, содержащих сведения, составляющие коммерческую и служебную тайну);

– выявление наиболее вероятных угроз для данной системы, выявление уязвимых мест обработки информации и каналов доступа к ней; оценка возможного ущерба, вызванного нарушением безопасности информации);

– организация пропускного режима;

– определение порядка учета, выдачи, использования и хранения съемных носителей информации, содержащих эталонные и резервные копии программ, архивные данные и т. п.;

– организация учета, хранения, использования и уничтожения документов и носителей с закрытой информацией;

– определение порядка проектирования, разработки, отладки, модификации, приобретения, исследования, приема в эксплуатацию, хранения и контроля целостности программных продуктов, а также порядок обновления версий используемых и установки новых системных и прикладных программ на рабочих местах защищенной системы (кто обладает правом разрешения таких действий, кто осуществляет, кто контролирует и что при этом они должны делать);

– создание отделов (служб) компьютерной безопасности или, в случае небольших организаций и подразделений, назначение нештатных ответственных, осуществляющих единое руководство, организацию и контроль за соблюдением всеми категориями должностных лиц требований по обеспечению безопасности программно-информационных ресурсов автоматизированной системы;

– определение перечня регулярно проводимых мероприятий и оперативных действий персонала по обеспечению непрерывной работы и восстановлению вычислительного процесса в критических ситуациях, возникающих из-за несанкционированного доступа, сбоев и отказов техники, ошибок в программах и действиях персонала, стихийных бедствий.

Периодически проводимые мероприятия:

– распределение и смена реквизитов разграничения доступа (паролей, ключей шифрования и т. п.);

– анализ системных журналов и принятие мер по обнаруженным нарушениям правил работы;

– анализ состояния и оценки эффективности мер и применяемых средств защиты (периодически, с привлечением сторонних специалистов);

– пересмотр состава и построения системы защиты.

Мероприятия, проводимые по необходимости:

– осуществляемые при кадровых изменениях в составе персонала системы;

– осуществляемые при ремонте и модификациях оборудования и программного обеспечения;

– по подбору и расстановке кадров (проверка принимаемых на работу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности и т. д.).

Постоянно проводимые мероприятия:

– противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности техники и носителей информации и т. п.;

– явный и скрытый контроль за работой персонала системы;

– контроль за применением мер защиты.

Все мероприятия осуществляются в соответствии с планом защиты, ревизию которого рекомендуется производить раз в год. Кроме того, существует ряд случаев, требующих внеочередного его пересмотра. К их числу относятся изменения следующих компонентов объекта:

– *люди*: пересмотр может быть вызван кадровыми изменениями, связанными с реорганизацией организационно-штатной структуры объекта, увольнением служащих, имевших доступ к конфиденциальной информации и т. д.;

– *техника*: изменение плана может быть вызвано подключением других сетей, изменением или модификацией используемых средств вычислительной техники или программного обеспечения;

– *помещения*: пересмотр плана защиты может быть вызван изменением территориального расположения компонентов объекта.

Документы, регламентирующие деятельность по защите информации, оформляются в виде различных планов, положений, инструкций, наставлений и других аналогичных документов. Для государственных учреждений комплект подобных документов регламентируется централизованно, не требует самостоятельной разработки, как для вновь создаваемых коммерческих организаций и предприятий.

1.4. Модель нарушителя безопасности информации

В документах политики безопасности часто используется понятие нарушителя.

Нарушитель – лицо, предпринявшее попытку выполнения запрещенных действий по ошибке, незнанию или осознанно и использующее для этого различные возможности, методы и средства.

Наиболее опасная форма нарушителя – *злоумышленник*, действующий намеренно, чаще всего с корыстной целью.

Для своих целей нарушитель должен затратить определенные силы, время и средства. Если его затраты из-за надежности системы защиты будут чрезмерно высоки, то он, вероятно, откажется от своего замысла. Для того чтобы представлять поведение нарушителя в определенных условиях, используют понятие «модель нарушителя».

Модель нарушителя – абстрактное (формализованное или неформализованное) описание нарушителя, которое определяет для него (или для группы нарушителей):

– возможные цели и мотивы;

– возможный количественный состав и квалификацию;

– используемые инструменты, оснащение, оружие и т. д.;

– типовые сценарии возможных действий, способы и алгоритмы.

Модель нарушителей отражает систему принятых руководством организации взглядов на контингент потенциальных нарушителей, может иметь разную степень детализации. Например, может включать математическую модель для количественных оценок угроз – вероятности и ущерба.

Нарушителями могут быть как лица, имеющие постоянный или разовый доступ в *контролируемую зону* (ограниченная территория с обозначенным периметром, на которой принимаются меры по защите информации), так и не имеющие такого доступа.

Простая модель может подразделять нарушителей по их возможностям при работе со средствами вычислительной техники. Например, в качестве потенциального нарушителя отдельно описываются:

1) разработчик;

2) обслуживающий персонал (системный администратор, сотрудники обеспечения ИБ);

3) пользователи;

4) сторонние лица.

Так, оператор или программист автоматизированной банковской системы может нанести несравненно больший ущерб, чем обычный пользователь, тем более недостаточно знакомый с информационными технологиями.

Пользователи различных категорий различаются не только по степени по месту действия, но и по тому, какому элементу системы они угрожают больше всего – внутренним и внешним данным, прикладным или системным программам, оборудованию и элементам компьютера, а также по характеру угроз – уничтожение, модификация, блокирование, а также компрометация (раскрытие) информации.

Из сказанного может возникнуть впечатление, что работа на современных компьютерах невозможна вообще из-за многочисленных различных угроз. На самом деле такой вывод также неверен, как и вывод, вытекающий из чрезмерного оптимизма или обычной небрежности.

В отношении возможных нарушений следует придерживаться принципа «золотой середины». Например, существует вероятность ядерного конфликта, но очень мало людей строят бомбоубежища, запасаются продуктами и водой, так как эта вероятность слишком мала. В то же время, каждый человек стремится обезопасить свою квартиру, машину, сбережения: ущерб меньше, чем при ядерной войне, но ощутим, а возможность более значительна.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика. Каждый вид нарушителя должен быть охарактеризован значениями характеристик, приведенных выше.

Правильно построенная модель нарушителя, в которой отражаются его практические возможности, априорные знания, время и место действия и т. п. характеристики – важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

1.5. Основные причины нарушений персонала в автоматизированных системах

Можно выделить три основные группы причин нарушений, которые допускают сотрудники: безответственность, самоутверждение, корыстный интерес пользователей (персонала).

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные, тем не менее, со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности. Маловероятно, чтобы разработчики системы защиты могли предусмотреть все такие ситуации. Более того, во многих случаях система в принципе не может предотвратить подобные нарушения (например, случайное уничтожение своих данных).

Некоторые пользователи считают получение дополнительного, не предусмотренного политикой безопасности доступа к информации значимым успехом, который позволяет самоутвердиться и в собственных глазах, и в глазах коллег. Хотя намерения могут быть и безвредными, результатом может быть снижение защищенности автоматизированной системы.

Нарушение безопасности может быть вызвано и корыстным интересом пользователя системы. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к информации.

Как показывает практика, ущерб от каждого вида нарушений обратно пропорционален его частоте: чаще всего встречаются нарушения, от которых он незначителен и легко восполняется. Например, ошибочно уничтоженные данные можно восстановить, если сразу заметить ошибку: если информация имеет существенное значение, то для нее хранят регулярно обновляемую резервную копию. Напротив, редкие нарушения, которые определяются умыслом (из-за обиды, неудовлетворенности своим служебным или материальным положением или по указанию других лиц) и связаны с целенаправленным доступом, модификацией, блокированием и уничтожением, дают, как правило, значительный ущерб. Например, для банков это может быть модификация счетов с уничтожением журнала транзакций (логических операций).

Для организации защиты необходимо понимать, от каких именно нарушений важнее всего избавиться. А способы предотвращения нарушений вытекают из природы их побудительных мотивов – это соответствующая подготовка пользователей, а также поддержание здорового рабочего климата в коллективе, подбор персонала, своевременное обнаружение потенциальных злоумышленников и принятие соответствующих мер. То есть задачи и руководства, и администрации, и сотрудников системы безопасности, и коллектива в целом.

1.6. Криминалистическая характеристика компьютерной преступности в России[1]

Криминалистическая характеристика преступлений – один из элементов частной криминалистической методики, представляющий собой систему сведений о типичных криминалистически значимых признаках преступлений и связях между ними. Такие знания помогают в выдвижении наиболее вероятных версий о различных сторонах совершенного преступления, соответственно – позволяют экономить время и повышать эффективность правоохранительной системы.

[1] По оценкам специалистов, уровень латентности компьютерных преступлений определяется в настоящее время в 90%. А из 10% выявленных компьютерных преступлений раскрывается только 1%.

Перед правоохранительными органами при расследовании компьютерных преступлений возникают криминалистические проблемы, характеризующие одновременно и специфику компьютерной преступности, которая определяется сложностью:

– в установлении факта компьютерного преступления и решении вопроса о возбуждении уголовного дела;

– подготовке и проведении отдельных следственных действий;

– выборе и назначения необходимых судебных экспертиз, в формулировании к ним вопросов, которые находятся в компетенции экспертов;

– использовании компьютерной техники в расследовании преступлений данной категории;

– из-за отсутствия методик расследования компьютерных преступлений и недостатка специалистов.

Ниже приводится криминалистическая характеристика компьютерных преступлений, позволяющая более эффективно их расследовать.

Обстановка совершения преступления

Под *обстановкой совершения преступления* понимается система различного рода взаимодействующих между собой до и в момент преступления объектов, явлений и процессов, характеризующих место, время, вещественные, природно-климатические, производственные, бытовые и иные условия среды, особенности поведения непрямых участников противоправного события, психологические связи между ними и другие факторы объективной реальности, определяющие возможность, условия, обстоятельства совершения преступления.

Обстановка преступлений, связанных с неправомерным доступом к компьютерной информации, характеризуется рядом существенных факторов. Чаще всего эти преступления совершаются в области профессиональной деятельности. Преступники, как правило, владеют не только специальными навыками в управлении компьютером и его устройствами, но и специальными знаниями в области обработки информации, в информационных системах в целом. Иногда – в зависимости от сферы преступления – преступникам необходимы специальные познания в финансовых, банковских и других информационных технологиях.

Для преступлений, связанных с созданием и распространения вредоносных программ, требуются специальные знания в узкой профессиональной области программного обеспечения.

Во всех этих преступлениях злоумышленник нарушает порядок своей служебной деятельности, это доказывает умысел в этих действиях.

Криминалистической проблемой является характерное для большинства случаев «разнесение» в пространстве и во времени факта совершения действия и факта наступления его общественно-опасных последствий. Например, преступник и объект преступления могут находиться в разных странах. В силу этого может возникнуть и проблема доказательства причинной связи между действиями лица и наступившим результатом.

Свойства личности субъекта преступления

В ЭКЦ МВД России был проведен классификационный анализ лиц, замешанных в применении компьютеров для совершения противоправных деяний.

Обобщенный портрет отечественного злонамеренного хакера, созданный на основе уголовного преследования такого рода личностей, выглядит примерно так:

– это мужчина в возрасте от 15 до 45 лет, либо имеющий многолетний опыт работы на компьютере, либо почти не обладающий таким опытом;

– в прошлом к уголовной ответственности не привлекался;

– является яркой, мыслящей личностью, способной принимать ответственные решения;

– хороший, добросовестный работник, по характеру нетерпимый к насмешкам и к потере своего социального статуса в рамках группы окружающих его людей;

– любит уединенную работу; приходит на службу первым и уходит последним;

– часто задерживается на работе после окончания рабочего дня и очень редко использует отпуска и отгулы.

Профессиональные хакеры обычно работают только после тщательной предварительной подготовки. Они снимают квартиру на подставное лицо, подкупают сотрудников организации, знакомых с деталями электронных платежей и паролями, работников телефонной станции, чтобы обезопаситься на случай поступления запроса от служб безопасности. Нанимают охрану из бывших сотрудников правоохранительных органов. Чаще всего атака компьютерной сети осуществляется рано утром, когда внимание и бдительность дежурного администратора ослаблены, а вызов помощи затруднен.

Опыт борьбы с преступностью свидетельствует о том, что одним из приоритетных направлений противодействия ей является активное использование различных мер профилактического характера. Предупредить компьютерное преступление всегда легче, чем его расследовать. Выделяются три основные группы методов предупреждения компьютерных преступлений, составляющие в своей совокупности целостную систему борьбы с этим явлением.

К *правовым* методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности.

Отечественное уголовное законодательство приведено в соответствие с общепринятыми международными правовыми нормами развитых стран. Уголовно-процессуальное законодательство, в свою очередь, регламентирует возможные следственные действия и механизм их осуществления.

Однако есть проблемы, затрудняющие предупреждение и расследование компьютерных преступлений, которые включают в себя:

– дефицит специалистов в правоохранительных органах;

– отсутствие наработок (методических рекомендаций по изъятию, обыску, осмотру места происшествия и т. п.);

– незавершенность УПК РФ и некоторые другие.

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:

– создание и совершенствование системы обеспечения информационной безопасности;

– усиление правоприменительной деятельности органов исполнительной власти, включая предупреждение и пресечение правонарушений в информационной сфере, а также привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;

– разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, повышение надежности специального программного обеспечения;

– создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации;

– сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

– контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности;

– формирование системы мониторинга показателей и характеристик информационной безопасности в наиболее важных сферах жизни и деятельности общества и государства и др.

Ввиду того, что компьютерные преступления имеют транснациональный характер, усиливается международное сотрудничество в этой области. Разрабатывается порядок взаимодействия правоохранительных органов и заинтересованных министерств и ведомств Российской Федерации, а также международного обмена информацией в борьбе с использованием высоких технологий в преступных целях. Обобщается следственная практика и на этой основе разрабатываются методические рекомендации. Организуются и проводятся научно-практические конференции с участием иностранных специалистов и практических работников по проблемам выявления, пресечения и расследования преступлений в сфере высоких технологий. В составе экспертно-криминалистических учреждений создаются подразделения для производства компьютерно-технических экспертиз. Разрабатываются программы подготовки кадров для работы в сфере высоких технологий, в вузах вводятся соответствующие курсы лекций и организуется обучение сотрудников.

По публикациям в российских журналах и на сайтах организаций, связанных с защитой информации, можно сделать вывод, что основными условиями, способствующими компьютерным преступлениям, являются:

– отсутствие должностного лица, отвечающего за режим секретности;

– отсутствие должностного лица, отвечающего за конфиденциальность информации и ее безопасность;

– отсутствие категорий допуска (определяются соответствующими положениями) сотрудников к конфиденциальной информации;

– отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации;

– отсутствие контроля за доступом сотрудников к управлению компьютера;

– беспечность обслуживающего персонала, которая позволяет преступнику свободно использовать ЭВМ в качестве орудия преступления;

– недостатки программного обеспечения, которое не имеет контрольной защиты, проверки соответствия и правильности вводимой информации;

– недостатки парольной системы защиты от несанкционированного доступа.

Зарубежный опыт показывает, что эффективной защитой организации от компьютерных преступлений является введение в ней должности специалиста по компьютерной безопасности (администратора по защите информации), либо создание специальных служб безопасности. Наличие такой службы в организации снижает вероятность совершения компьютерных преступлений вдвое. Кроме того, настоятельно рекомендуются следующие организационные меры:

– для всех лиц, имеющих право доступа к средствам компьютерной техники (СКТ), должны быть определены категории доступа;

– определена ответственность за сохранность информационных ресурсов;

– налажен периодический контроль за качеством защиты информации;

– проведена классификация информации в соответствии с ее важностью, дифференциация на основе этого мер защиты;

– организация физической защиты СКТ.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

– разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;

– совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Защита информации в компьютерных системах обеспечивается созданием *комплексной системы защиты***,** включающей:

– методы защиты от случайных угроз;

– методы защиты от традиционного шпионажа и диверсий;

– методы защиты от электромагнитных излучений и наводок;

– методы защиты от несанкционированного доступа;

– криптографические методы защиты;

– методы защиты от компьютерных вирусов.

Среди методов защиты имеются и универсальные, которые являются базовыми при создании любой системы защиты.

Методы *защиты от случайных угроз* разрабатываются и внедряются на этапах проектирования, создания, внедрения и эксплуатации компьютерных систем, к числу которых относятся:

– создание высокой надёжности компьютерных систем;

– создание отказоустойчивых компьютерных систем;

– блокировка ошибочных операций;

– оптимизация взаимодействия пользователей и обслуживающего персонала с компьютерной системой;

– минимизация ущерба от аварий и стихийных бедствий;

– дублирование информации.

При защите информации в компьютерных системах от *традиционного шпионажа и диверсий* используются те же средства и методы защиты, что и для защиты других объектов, на которых не используются компьютерные системы. К их числу относятся:

– создание системы охраны объекта;

– организация работ с конфиденциальными информационными ресурсами;

– противодействие наблюдению и подслушиванию;

– защита от злоумышленных действий персонала.

Все методы *защиты от электромагнитных излучений и наводок* можно разделить на пассивные и активные: пассивные методы обеспечивают уменьшение уровня опасного сигнала или снижение информативности сигналов, активные – направлены на создание помех в каналах побочных электромагнитных излучений и наводок, затрудняющих приём и выделение полезной информации из перехваченных злоумышленником сигналов. На электронные блоки и магнитные запоминающие устройства могут воздействовать мощные внешние электромагнитные импульсы и высокочастотные излучения. Эти воздействия могут приводить к неисправности электронных блоков и стирать информацию с магнитных носителей информации. Для блокирования угрозы такого воздействия используется экранирование защищаемых средств.

Для защиты информации от *несанкционированного доступа* создаются:

– система разграничения доступа к информации;

– система защиты от исследования и копирования программных средств.

Под *криптографической защитой* информации понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий. По виду воздействия на исходную информацию методы криптографического преобразования информации разделяются на следующие группы:

– шифрование;

– стеганография;

– кодирование;

– сжатие.

Наряду с методами защиты информации необходимо обратить внимание и на порядок и правила применения определенных принципов и средств защиты информации

1. Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами[1].

2. Защита информации от несанкционированного воздействия – защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

3. Защита информации от непреднамеренного воздействия – защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

4. Защита информации от разглашения – защита информации, направленная на предотвращение несанкционированного доведения

[1] Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

5. *Защита информации от несанкционированного доступа* – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

6. *Защита информации от преднамеренного воздействия* – защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

7. *Защита информации от [иностранной] разведки* – защита информации, направленная на предотвращение получения защищаемой информации [иностранной] разведкой.

Выделение типовых моделей разных категорий преступников, знание их основных черт позволяет оптимизировать процесс выявления круга лиц, среди которых целесообразно вести поиск преступника и точнее определить способы установления и изобличения конкретного правонарушителя. Уголовный кодекс разделил «компьютерных преступников» на следующие категории:

– лица, осуществляющие неправомерный доступ к компьютерной информации;

– лица, осуществляющие неправомерный доступ к компьютерной информации в группе по предварительному сговору или организованной группой;

– лица, осуществляющие неправомерный доступ к компьютерной информации с использованием своего служебного положения;

– лица, имеющие доступ к ЭВМ, но осуществляющие неправомерный доступ к компьютерной информации или нарушающие правила эксплуатации ЭВМ;

– лица, создающие, использующие и распространяющие вредоносные программы.

Напомним, что уголовной ответственности по УК РФ за преступления рассматриваемого вида подлежат вменяемые лица, достигшие 16 лет.

Зарубежный опыт свидетельствует, что сам факт появления компьютерной преступности в обществе многие исследователи отождествляют с появлением так называемых «хакеров» (англ., «*hack*» –

рубить, кромсать) – пользователей вычислительной системы, занимающихся поиском незаконных способов получения несанкционированного доступа к данным.

По свидетельству экспертов из правоохранительных органов, самым привлекательным сектором российской экономики для преступников является кредитно-банковская сфера. Анализ совершаемых здесь преступных деяний с использованием компьютерных технологий, а также опросы представителей банковских учреждений позволяют выделить следующие наиболее типичные способы совершения компьютерных преступлений против банков и других финансовых учреждений.

Во-первых, все более распространенными становятся компьютерные преступления, совершаемые путем несанкционированного доступа к банковским базам данных посредством телекоммуникационных сетей. Основной результат – незаконный перевод денежных средств.

Во-вторых, за последнее время не отмечено практически ни одного компьютерного преступления, которое было бы совершено одиночкой. Более того, известны случаи, когда организованными преступными группировками нанимались бригады из десятков хакеров, которым предоставлялось отдельное охраняемое помещение, оборудованное по последнему слову вычислительной техники, с тем, чтобы они осуществляли хищение крупных денежных средств путем нелегального проникновения в компьютерные сети крупных коммерческих банков.

В-третьих, большинство компьютерных преступлений в банковской сфере совершается при непосредственном участии самих служащих коммерческих банков[1]. Например, преступники оформляют проводку фиктивного платежа с помощью удаленного доступа к банковскому компьютеру через модем, введя пароль и идентификационные данные, которые им передают сообщники из персонала филиала банка. Далее похищенные деньги переводятся в соседний банк, где преступники снимают их со счета, оформив поддельное платежное поручение.

В-четвертых, все большее число компьютерных преступлений совершается в России с использованием возможностей, которые

[1] Результаты исследований, проведенных с привлечением банковского персонала, показывают, что доля таких преступлений приближается к отметке 70%.

предоставляет своим пользователям глобальная компьютерная сеть Интернет.

1.7. Доктрина информационной безопасности

Концептуальные основы обеспечения информационной безопасности нашей страны определены Доктриной информационной безопасности Российской Федерации (утв. указом Президента РФ 05.12.2016 №646). По характеристике самого документа Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере, где под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

В настоящей Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учётом стратегических национальных приоритетов Российской Федерации.

Документ служит:

– для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;

– подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;

– разработки целевых программ обеспечения информационной безопасности Российской Федерации.

В Доктрине отмечается, что информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Фе-

дерации. Национальными интересами в информационной сфере являются:

– обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

– обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее – критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

– развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

– доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и её официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;

– содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнёрства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

В данном документе определены ключевые проблемы обеспечения информационной безопасности, а также соответствующие угрозы, методы предотвращения и нейтрализации этих угроз, основные

положения государственной политики обеспечения информационной безопасности Российской Федерации.

Информационная безопасность Российской Федерации – состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Интересы *личности* в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы *общества* в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы *государства* в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Доктрина выделяет *четыре основные составляющие национальных интересов Российской Федерации* в информационной сфере, а именно:

– соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;

– информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государствен-

ной политике России, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;

– развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечения накопления, сохранности и эффективного использования отечественных информационных ресурсов;

– защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

Также в Доктрине содержатся основные виды и источники угроз безопасности. В частности, в качестве основных видов угроз указаны:

– возможности трансграничного оборота информации, которые всё чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности;

– наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях;

– наращивание информационного воздействия на население России, в первую очередь на молодёжь, в целях размывания традиционных российских духовно-нравственных ценностей;

– использование механизмов информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряжённости, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников;

– возрастающие масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличение преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий;

– увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации;

– высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран;

– недостаточная эффективность научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомлённостью граждан в вопросах обеспечения личной информационной безопасности;

– стремление отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве.

По аналогии с понятием информационной безопасности Российской Федерации соответствующее понятие для органов внутренних дел можно определить следующим образом: под *информационной безопасностью органов внутренних дел* следует понимать состояние защищенности интересов последних в информационной сфере в соответствии с возложенными на них задачами.

Так же по аналогии можно установить основные элементы информационной сферы органов внутренних дел, а именно:

– ведомственная информация и информационные ресурсы;

– ведомственная информационная инфраструктура – средства и системы информатизации;

– субъекты осуществления информационной деятельности – сотрудники органов внутренних дел;

– система нормативно-правового регулирования этой деятельности.

К наиболее важным объектам обеспечения информационной безопасности в правоохранительной и судебной сферах Доктрина относит:

– информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

– информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

– информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах, являются:

– разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;

– деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

– нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;

– недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

– отсутствие единой методологии сбора, обработки и хранения информации оперативно-розыскного, справочного, криминалистического и статистического характера;

– отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

– преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.

В качестве основных задач органов внутренних дел в информационной сфере рассматриваются: эффективная реализация функций по *добыванию, обработке* и *использованию* оперативно-розыскной информации в целях защиты личности, ее прав и свобод, обеспечения безопасности общества и государства от преступных посягательств и обеспечение безопасности ведомственной информации, информационных ресурсов, а также средств и систем информатизации.

Соответственно, к числу основных угроз, возникающих в сфере информационно-аналитического обеспечения оперативно-розыскной деятельности органов внутренних дел, следует относить угрозы, возникающие в процессе добывания, обработки и использования оперативно-розыскной информации, а также угрозы, связанные с нарушением безопасности информации и средств информатизации.

Отдельно можно выделить следующие угрозы, возникающие в процессе реализации субъектами оперативно-розыскной деятельности своих функциональных обязанностей.

К *угрозам по добыванию, обработке и использованию оперативно-розыскной информации можно отнести:*

– несовершенство действующего законодательства в сфере борьбы с преступностью;

– несовершенство нормативно-правового обеспечения оперативно-розыскной деятельности;

– нарушение установленного порядка добывания, обработки и использования оперативно-розыскной информации;

– противодействие, в том числе техническое, оказываемое организованными преступными группами правоохранительным органам;

– относительная известность средств и тактики оперативно-розыскной деятельности криминальным структурам;

– недостаточный уровень профессиональной подготовки оперативных сотрудников;

– недостаточное ресурсное обеспечение оперативно-розыскной деятельности;

– недостаточный уровень информационного взаимодействия подразделений по борьбе с организованной преступностью с иными службами органов внутренних дел, другими правоохранительными органами, специальными службами;

– коррупционные проявления в органах внутренних дел.

Угрозы безопасности информации и средствам информатизации:

– неконтролируемое распространение (утечка) защищаемой информации в результате разглашения, несанкционированного доступа, ведения агентурной и технической разведок;

– несанкционированные воздействия на информационные ресурсы, средства и системы информатизации;

– нарушение установленного порядка обработки и использования защищаемой информации;

– недостаточное ресурсное обеспечение формирования инфраструктуры и эксплуатации средств информатизации оперативных подразделений;

– отказы в работе технических средств и систем информатизации;

– широкое применение средств и систем информатизации зарубежного производства.

Угрозы негативных информационно-психологических воздействий:

– шантаж оперативных работников, целенаправленно осуществляемый организованными преступными группами;

– формирование средствами массовой информации искаженного представления о деятельности органов внутренних дел;

– девальвация нравственных ценностей общества;

– отсутствие реальной социальной защиты оперативных сотрудников и членов их семей.

Основными факторами, препятствующими эффективному добыванию, обработке и использованию оперативно-розыскной информации, по мнению практических работников, являются:

1. Активное противодействие (в самых различных формах) правоохранительным органам со стороны уголовно-преступного мира, включая противодействие технической разведке органов внутренних дел с помощью специальных средств защиты информации.

2. Широкое использование криминальными структурами средств и тактики оперативно-розыскной деятельности.

Причины утечки информации о силах, средствах, тактике и методах оперативно-розыскной деятельности могут быть самыми различными. Например, несоблюдение установленного порядка обращения с секретной информацией (постоянная сменяемость кадров в правоохранительных органах, связанная в основном с уходом сотрудников в коммерческие структуры), нелегальный оборот технических средств разведывательного назначения.

3. Недостаточное ресурсное обеспечение оперативно-розыскной деятельности.

4. Несовершенство законодательства, главным образом в сфере борьбы с организованной и международной преступностью, коррупцией и незаконным оборотом наркотиков.

Определенные неточности и противоречивость характерны для ведомственных подзаконных актов.

Кроме того, в части, касающейся правового статуса персональных и иных данных ограниченного доступа, используемых в аналитической деятельности, нормативная правовая база, связанная добыванием и обработкой оперативно-розыскной информации, развита пока недостаточно.

Актуальность проблемы обеспечения информационной безопасности органов внутренних дел определяется рядом взаимосвязанных факторов, многие из которых являются следствием процесса информатизации современного общества. Например, применение новейших информационных технологий высокой сложности в правоохранительной деятельности, высокая уязвимость инфраструктуры из-за сложности используемых систем, стремительный прогресс в развитии технических средств разведывательного назначения и т. д.

Необходимо учитывать, что значительная многочисленность имеющихся нормативных актов ослабляет правоприменительную деятельность в данной области.

Объем подзаконного уровня регламентации оперативно-розыскной работы тоже достаточно велик, так как множество нормативных актов систематизируется на ведомственном и межведомственном уровнях.

Характерной особенностью правоотношений, возникающих в сфере обеспечения информационной безопасности при осуществлении оперативно-розыскной деятельности, является то обстоятельство, что её объекты и субъекты вступают в активное взаимодействие с объектами и субъектами информационной безопасности.

Следует напомнить, что в качестве основных объектов национальной безопасности Российской Федерации, включая и ее информационную составляющую, рассматриваются *личность* – ее права и свободы; *общество* – его материальные и духовные ценности; и, наконец, само *государство* – его конституционный строй, суверенитет и территориальная целостность.

При исполнении своих профессиональных обязанностей сотрудники органов внутренних дел, решая возложенные на них задачи, нередко затрагивают частную жизнь отдельных граждан, что полно-

стью нарушает конституционный принцип о неприкосновенности частной жизни, личной и семейной тайны. Во-первых, подобная информация поступает к ним в ходе непосредственных контактов с их собственниками (например, при осуществлении оперативно-розыскных мероприятий), во-вторых – через посредников, (например при наведении справок). Поэтому важно, чтобы данный процесс всегда протекал в правовом русле, строго соответствуя целям и задачам заданных мероприятий.

В тех случаях, когда субъекты органов внутренних дел после получения конфиденциальной информации обретают статус ее пользователей, данная информация превращается в *служебную тайну,* и их основная задача заключается в *обеспечении защиты* этих сведений от дальнейшего неправомерного доступа к ним.

Гарантами соблюдения законности в этих случаях являются судебные инстанции, прокуратура, а также ведомственный контроль. Нарушения требований конституционного и федерального законодательства в области защиты частной жизни граждан при осуществлении указанных видов деятельности влекут строгую юридическую ответственность.

Например, *отказ* в предоставлении гражданину собранных в установленном порядке документов и материалов, непосредственно затрагивающих его права и свободы, либо *несвоевременное* предоставление таких документов и материалов, а также предоставление *неполной или заведомо ложной* информации предусматривает наступление административной ответственности по ст. 5.39 КоАП РФ. В том случае, если подобные деяния причинили вред правам и законным интересам гражданина, то они образуют состав преступления и преследуются уже в уголовном порядке по ст. 140 УК РФ. Ответственность за незаконное проникновение в жилище, совершенное против воли проживающего в нем лица, предусматривается ч. 1 ст. 139 УК РФ. Незаконным проникновением следует считать не только вхождение в жилище, но и *размещение* в нем *специальных технических средств* для аудиовизуального наблюдения в отсутствие владельца или пользователя жилища.

Разглашение или утрата сведений, составляющих служебную тайну, не угрожают напрямую безопасности государства, однако при определенных условиях эти действия могут причинить существенный вред его охраняемым интересам. Поэтому соблюдение правового режима служебной тайны в ходе осуществления оперативно-розыскных мероприятий в полной мере отвечает интересам обеспече-

ния информационной безопасности не только отдельных граждан и общества, но и государства в целом.

К государственной тайне относятся различные категории сведений оперативно-розыскного характера, в том числе и обретаемые в ходе осуществления оперативно-розыскных мероприятий. Основные их виды определяются положениями нормативных правовых актов высших органов государственной власти, а различные категории такой информации, образующейся непосредственно в ходе оперативно-служебной деятельности органов внутренних дел, конкретизируются в соответствующих перечнях, разрабатываемых и согласовываемых в соответствии с определенными правилами. Особое место в них занимают результаты оперативно-розыскной деятельности. За разглашение таких сведений либо утрату документов, содержащих государственную тайну, предусмотрена уголовная ответственность.

Полномочия по защите государственной тайны в различных сферах деятельности МВД России, включая и оперативно-розыскную деятельность, нашли отражение в Положении о Министерстве внутренних дел Российской Федерации. Они самым тесным образом связаны с требованиями Инструкции по обеспечению режима секретности в органах внутренних дел Российской Федерации, отражающими основные меры организационного характера в рассматриваемой сфере деятельности. Эти меры, помимо всего прочего, предполагают также введение особого порядка допуска субъектов оперативно-розыскной деятельности к работе с секретными документами, предусмотренного дополнительной инструкцией.

Что касается обеспечения организационно-правовой защиты средств и систем информатизации, используемых в правоохранительной сфере, то техническая защита информации ограниченного доступа определяется аттестацией защищаемого объекта информатизации, что включает в себя категорирование этого объекта и его техническую паспортизацию.

В органах внутренних дел встречается три основных вида категорируемых объектов информации, различающихся по своему составу:

1) объект информатизации, в состав которого входит только выделенное помещение, в котором циркулирует (обрабатывается) речевая информация ограниченного доступа;

2) объект информатизации, включающий в свой состав только основные технические средства, предназначенные для обработки информации ограниченного доступа;

3) объект информатизации, в состав которого входят и выделенное помещение, и основные технические средства и системы.

При категорировании автоматизированной системы (как правило, локальной вычислительной сети) в техническом паспорте отражается ее топологическая схема, которая должна отражать все информационные потоки и механизм их обработки.

В типовой перечень работ (мероприятий) по технической защите информации категорированных объектов информатизации в органах внутренних дел включаются:

– специальные исследования;

– специальные проверки;

– специальное обследование;

– установка и настройка средств защиты информации;

– проведение контрольных измерений для оценки эффективности установленной защиты;

– оформление предписания на эксплуатацию;

– проведение аттестационных испытаний с оформлением аттестата соответствия объекта информатизации требованиям по безопасности информации.

Подразделения системы МВД России, осуществляющие указанные работы, или привлекаемые для этого сторонние организации должны обладать соответствующей государственной лицензией (лицензиями), подтверждающей право на их выполнение:

– для проведения специальных исследований – лицензией ФСТЭК;

– специальных проверок – лицензией ФСБ;

– установкой и настройкой средств защиты информации без использования криптографических средств – лицензией ФСТЭК;

– установкой и настройкой средств защиты информации с использованием криптографических средств – лицензией ФСБ;

– контрольных измерений для оценки эффективности установленной защиты – лицензией ФСТЭК (измерений шифраппаратуры – лицензией ФСБ);

– аттестационных испытаний с оформлением аттестата соответствия объекта информатизации требованиям по безопасности информации – органов по аттестации объектов информатизации, аккредитованных ФСТЭК.

На применяемые средства защиты информации (в номенклатуру средств защиты информации входят собственно средства защиты информации; средства информатизации, в которых эти средства за-

щиты информации реализованы (или средства информатизации в специальном защищенном исполнении), а также средства контроля эффективности защиты информации – контрольно-измерительная аппаратура и тестирующие средства) должны быть оформлены государственные сертификаты на соответствие этих средств требованиям по безопасности информации:

– на средства, не содержащие криптографического преобразования – сертификат ФСТЭК;

– на средства, содержащие криптографическое преобразование, – сертификат ФСБ.

В отдельных случаях, например, когда средство защиты от несанкционированного доступа по системе классификации ФСТЭК содержат элементы криптографического преобразования, требуются одновременно сертификаты и ФСТЭК, и ФСБ.

Сертификаты на средства защиты информации, оформленные в системе сертификации Министерства обороны России или других ведомств для применения в их узковедомственных интересах, не могут применяться в системе МВД России, если это обстоятельство не согласовано с ФСТЭК и (или) ФСБ.

В ходе принятия решения о применении тех или иных средств защиты информации (средств информатизации в специальном защищенном исполнении) необходимо руководствоваться данными из государственного реестра сертифицированных средств защиты информации. Информация о сертифицированных средствах имеется в Управлении информационно-телекоммуникационных технологий и связи Департамента тыла МВД России.

Таким образом, поддержание уровня организационно-правового обеспечения безопасности ведомственной информации, информационных ресурсов, средств и систем информатизации в правоохранительной деятельности целиком зависит от степени соблюдения законности всеми заинтересованными субъектами.

1.8. Угрозы информационной безопасности и методы их реализации

Под угрозой обычно понимают возможную опасность. В дальнейшем изложении *угрозой информационной безопасности автоматизированной системы (АС)* будем называть возможность воздействия на информацию, обрабатываемую в АС, приводящего к ее модификации, уничтожению, копированию, блокированию, а также возможность воздействия на компоненты АС, приводящего к утрате,

уничтожению или сбою технических устройств и носителей информации.

Определение возможных угроз информационной безопасности проводится с целью задания полного перечня требований к разрабатываемой системе защиты АС. Эффективный анализ угроз возможен на основе их классификации по ряду признаков. При этом каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. Как следствие, для защищаемой системы определяют не полный перечень угроз, а перечень *классов угроз*.

Классификация возможных угроз информационной безопасности АС может быть проведена по ряду базовых признаков.

1. По природе возникновения:

– естественные угрозы – угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, не зависящих от человека;

– искусственные угрозы – угрозы, вызванные деятельностью человека.

2. По степени преднамеренности проявления:

– угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала. Например: проявление ошибок программно-аппаратных средств АС; некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности; неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т. п.); неправомерное включение оборудования или изменение режимов работы устройств и программ; неумышленная порча носителей информации; пересылка данных по ошибочному адресу абонента (устройства); ввод ошибочных данных; неумышленное повреждение каналов связи;

– угрозы преднамеренного действия (например, угрозы действий злоумышленника для хищения информации).

3. По непосредственному источнику угроз:

– угрозы, источником которых является человек. Например: внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность); вербовка (путем подкупа, шантажа и т. п.) персонала или отдельных пользователей, имеющих определенные полномочия; угроза несанкционированного копирования секретных данных пользователем АС;

разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т. п.);

– угрозы, источником которых являются санкционированные программно-аппаратные средства. Например: запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т. п.); возникновение отказа в работе операционной системы;

– у грозы, источником которых являются несанкционированные программно-аппаратные средства. Например: нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях), заражение компьютера вирусами с деструктивными функциями;

– угрозы, непосредственным источником которых является природная среда (стихийные бедствия, магнитные бури, радиоактивное излучение и т. п.).

4. По положению источника угроз:

– угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС. Например: перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т. п.); перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему; дистанционная фото- и видеосъемка;

– угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится АС. Например: хищение производственных отходов (распечаток, записей, списанных носителей информации и т. п.); отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т. д.); применение подслушивающих устройств;

– угрозы, источник которых имеет доступ к периферийным устройствам АС (терминалам);

– угрозы, источник которых расположен в АС. Например: проектирование архитектуры системы и технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и безопасности информации; некорректное использование ресурсов АС.

5. По степени зависимости от активности АС:

– угрозы, которые могут проявляться независимо от активности АС. Например: вскрытие шифров криптозащиты информации; хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем);

– угрозы, которые могут проявляться только в процессе автоматизированной обработки данных. Например: угрозы выполнения и распространения программных вирусов, снятие передаваемых данных.

6. По степени воздействия на АС:

– пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС. Например, угроза копирования секретных данных);

– активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС. Например: внедрение аппаратных вложений, программных «закладок» и «вирусов», то есть таких участков программ, которые не нужны для выполнения заявленных функций, но позволяют преодолеть систему защиты, скрытно и незаконно осуществить доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы; действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т. п.); угроза умышленной модификации информации.

7. По этапам доступа пользователей или программ к ресурсам АС:

– угрозы на этапе запрета доступа к ресурсам АС;

– угрозы при разрешенном доступе к ресурсам АС.

8. По способу доступа к ресурсам АС:

– угрозы с использованием прямого стандартного пути доступа к ресурсам АС. Например: незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, подбором, имитацией интерфейса системы

и т. д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»); несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т. п.;

– угрозы скрытого нестандартного пути доступа к ресурсам АС. Например: вход в систему в обход средств защиты (загрузка посторонней операционной системы (ОС) со сменных магнитных носителей и т. п.); угроза несанкционированного доступа к ресурсам АС путем использования недокументированных возможностей ОС.

9. По месту расположения информации в АС:

– угрозы доступа к информации на внешних запоминающих устройствах. Например: угроза несанкционированного копирования секретной информации с жесткого диска;

– угрозы доступа к информации в оперативной памяти. Например: чтение остаточной информации из оперативной памяти; чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, используя недостатки мультизадачных АС и систем программирования; угроза доступа к системной области оперативной памяти со стороны прикладных программ;

– угрозы доступа к информации, циркулирующей в линиях связи. Например: незаконное подключение к линиям связи, использование пауз в действиях законного пользователя для действий от его имени или после его физического отключения; модификация передаваемых сообщений; перехват всего потока данных с целью его дальнейшего анализа;

– угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере. Например: угроза записи отображаемой информации на скрытую видеокамеру.

Вне зависимости от конкретных видов угроз, АС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются следующие свойства информации и систем ее обработки, которые кратко рассматривались раньше:

– *конфиденциальность* информации – субъективно определяемая (приписываемая) характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы и среды сохранять указанную информацию в тайне от

субъектов, не имеющих полномочий доступа к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты их законных интересов от других субъектов информационных отношений;

– *целостность* информации – существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию или каким-либо требованиям). Точнее говоря, субъектов интересует обеспечение более широкого свойства – достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, то есть ее неискаженности;

– *доступность* информации – свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Таким образом, в соответствии с существующими подходами, принято считать, что информационная безопасность АС обеспечена в случае если для любых информационных ресурсов в системе поддерживается определенный уровень конфиденциальности (невозможности несанкционированного получения какой-либо информации), целостности (невозможности несанкционированной или случайной ее модификации) и доступности (возможности за разумное время получить требуемую информацию).

Соответственно для АС можно рассматривать три основных вида угроз:

– угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой;

– угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нару-

шена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных);

– угроза отказа служб возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

Описанные выше угрозы были сформулированы в 60-х годах прошлого столетия для открытых *Unix*-подобных систем, где не предпринимались меры по защите информации. На современном этапе информационных технологий подсистемы или функции защиты являются неотъемлемой частью комплексов по обработке информации. Информация не представляется «в чистом виде», на пути к ней имеется хотя бы какая-нибудь система защиты, и поэтому, чтобы угрожать, скажем, нарушением конфиденциальности, атакующая сторона должна преодолеть эту систему. Однако не существует абсолютной системы защиты, вопрос лишь во времени и средствах, требующихся на ее преодоление.

К числу основных методов реализации угроз информационной безопасности АС относятся:

– определение злоумышленником типа и параметров носителей информации;

– получение злоумышленником информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения;

– получение злоумышленником детальной информации о функциях, выполняемых АС;

– получение злоумышленником данных о применяемых системах защиты;

– определение способа представления информации;

– определение злоумышленником содержания данных, обрабатываемых в АС, на качественном уровне (применяется для мониторинга АС и для расшифровывания сообщений);

– хищение (копирование) машинных носителей информации, содержащих конфиденциальные данные;

– использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок (ПЭМИН) – конфиденциальные данные перехватываются злоумышленником путем выделения информативных сигналов из электромагнитного излучения и наводок по цепям питания средств вычислительной техники, входящей в АС;

– уничтожение средств вычислительной техники и носителей информации;

– хищение (копирование) носителей информации;

– несанкционированный доступ пользователя к ресурсам АС в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов;

– несанкционированное превышение пользователем своих полномочий;

– несанкционированное копирование программного обеспечения;

– перехват данных, передаваемых по каналам связи;

– визуальное наблюдение – конфиденциальные данные считываются с экранов терминалов, распечаток в процессе их печати и т. п.;

– раскрытие представления информации (расшифровывание данных);

– внесение пользователем несанкционированных изменений в программно-аппаратные компоненты АС и обрабатываемые данные;

– установка и использование нештатного аппаратного и / или программного обеспечения;

– заражение программными вирусами;

– внесение искажений в представление данных, уничтожение данных на уровне представления, искажение информации при передаче по линиям связи;

– внедрение дезинформации;

– выведение из строя машинных носителей информации без уничтожения информации – выведение из строя электронных блоков накопителей на жестких дисках и т. п.;

– проявление ошибок проектирования и разработки аппаратных и программных компонентов АС;

– обход (отключение) механизмов защиты – загрузка злоумышленником нештатной операционной системы на собственном носителе, использование отладочных режимов программно-аппаратных компонентов АС и т. п.;

– запрет на использование информации – имеющаяся информация по каким-либо причинам не может быть использована.

Вопросы для самоконтроля

1. Каковы основные критерии информационной безопасности?
2. Что является объектом защиты информации?
3. Каковы основные цели и задачи системы защиты информации?
4. Каковы основные принципы построения системы защиты информации?
5. Что понимается под политикой информационной безопасности организации?
6. Каковы основные организационные меры и мероприятия по обеспечению информационной безопасности?
7. Что понимается под нарушителем и моделью нарушителя информационной безопасности?
8. Каковы основные особенности компьютерных преступлений?
9. Какие группы методов применяются для обеспечения информационной безопасности?
10. Каковы национальные интересы Российской Федерации в информационной сфере?
11. Как понимается информационная безопасность Российской Федерации?
12. Каковы основные виды и источники угроз безопасности Российской Федерации в информационной сфере?
13. Каковы основные угрозы информационной безопасности в правоохранительной и судебной сферах?
14. Каковы основные меры организационно-правовой защиты объектов информатизации в правоохранительной сфере?
15. Какие требования предъявляются к средствам технической защиты информации (средств информатизации в специальном защищенном исполнении), применяемым в системе МВД России?
16. По каким признакам может быть проведена классификация угроз информационной безопасности?

Глава 2. ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Правовой режим информации

В современном мире возрастает общественная значимость информационных отношений: информация все в большей степени становится товаром, от наличия и сохранности которого зависит благополучие как отдельных граждан и организаций, так и общества в целом.

При этом информация является особым объектом, у которого может быть, а может и не быть материального носителя, информация может иметь разную достоверность, обладать различной ценностью и т. д. Это определяет необходимость целого комплекса правовых норм, которые определили бы правовой режим информации.

В самом общем виде *правовой режим информации* следует понимать, как совокупность норм, определяющих:

– права собственности, владения и распоряжения информацией;

– степень открытости информации, необходимость или возможность ее отнесения к категории ограниченного доступа;

– порядок отнесения информации к категории ограниченного доступа и уполномоченных на это лиц;

– порядок документирования, доступа, хранения, контроля и распространения информации;

– применение различных средств и методов обеспечения информационной безопасности;

– порядок привлечения к ответственности и меры наказания за нарушение установленных норм и правил в области информационных отношений.

Комплексное изучение установленных норм и правил в конкретной прикладной области всегда является обязательным элементом культуры работающего в этой области специалиста.

В целом проблема обеспечения информационной безопасности в достаточной степени противоречива. С одной стороны, в соответствии со ст. 29 Конституции РФ, *«Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом»*. С другой стороны, ст. 23 Конституции России провозглашает права

граждан на *«неприкосновенность частной жизни, личную и семейную тайну»*.

Все многообразие нормативных актов, затрагивающих вопросы обеспечения информационной безопасности, может быть *классифицировано* по группам регламентируемых ими вопросов. При этом можно выделить законодательные нормы, которые определяют:

– разделение информации на категории открытого и ограниченного доступа, причем информация ограниченного доступа по условиям ее правового режима подразделяется на отнесенную к государственной тайне и конфиденциальную, включающую в себя служебную и коммерческую тайну;

– правовой режим защиты информации, неправомерное обращение с которой может нанести ущерб обладателю этой информации;

– организацию работ по защите информации, структуру и основные функции государственной системы защиты информации (ГСЗИ), государственные органы управления в области информационной безопасности, их права и обязанности;

– государственное лицензирование деятельности в области защиты информации;

– обязательность и порядок сертификации технических и программных средств, применяемых в информационных объектах для обработки защищаемой информации;

– обязательность и порядок аттестации информационных объектов, обрабатывающих информацию с ограниченным доступом;

– необходимость и порядок создания специальных служб, обеспечивающих защиту информации с ограниченным доступом на информационных объектах;

– порядок контроля защищенности информации с принятием мер по приостановке обработки информации в случае невыполнения требований по защите информации;

– права и ответственность должностных лиц за охрану и защиту информации;

– ответственность за противоправные действия в области информационных отношений.

Данная классификация определяет группы вопросов, требующих нормативного регулирования в области информационных отношений. Однако дать четкую привязку отдельных законодательных актов к конкретным группам вопросов достаточно сложно, так как большинство законов содержит правовые нормы для решения различных групп вопросов.

В Российской Федерации к нормативно-правовым актам федерального законодательства в области информационной безопасности относятся: международные договоры; конституция; федеральные законы; указы президента; постановления правительства. Нормативные документы государственных органов России в области информационной безопасности: Доктрина информационной безопасности Российской Федерации; руководящие документы ФСТЭК; приказы ФСБ России.

Стандарты информационной безопасности, из которых выделяют:

– международные стандарты;

– государственные (национальные) стандарты Российской Федерации;

– рекомендации по стандартизации;

– методические указания.

Непосредственно российское законодательство в области информатизации начало формироваться с 1991 года.

К наиболее важным сегодня следует отнести следующие нормативно-правовые акты: закон РФ от 21.07.1993 № 5485-I «О государственной тайне» и федеральные законы:

– от 29.12.1994 № 77 «Об обязательном экземпляре документов»;

– от 22.10.2004 № 125 «Об архивном деле в Российской Федерации»;

– от 29.07.2004 № 98 «О коммерческой тайне»;

– от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации»;

– от 27.07.2006 №152 «О персональных данных»;

– от 06.04.2011 № 63 «Об электронной подписи».

При решении организационно-правовых вопросов обеспечения информационной безопасности исходят из того, что информация подпадает под нормы вещного права, это дает возможность применять к информации нормы уголовного и гражданского права в полном объеме.

Впервые в правовой практике России информация как объект права была определена в ч. 1 ст. 128 ГК РФ: «К объектам гражданских прав относятся … информация; результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность) …». Данная статья дает возможность квалифицировать посягательства на сохранность и целостность информа-

ции как преступления против собственности, при этом собственнику предоставляется право самостоятельно в пределах своей компетенции устанавливать режим защиты информационных ресурсов и доступа к ним.

Рассмотрим правовой режим общедоступной информации**,** неправомерное обращение с которой может нанести ущерб собственнику этой информации.

Для обеспечения применения к информации норм вещного права в законе «Об информации, информационных технологиях и о защите информации» вводится понятие *документированная информация* (ч. 11 ст. 2) – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель. Разрешение различных конфликтов в области информационных отношений на базе действующего законодательства возможно только для документированной информации. Этим же законом введено понятие *обладателя* информации в информационной области (ст. 2 п. 5).

Обладатель информации вправе:

– разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

– использовать информацию, в том числе распространять ее по своему усмотрению;

– передавать информацию другим лицам по договору или на ином установленном законом основании;

– защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами.

С правом *собственности*, *владения* и *распоряжения* информацией тесно связано понятие авторского права и сопутствующее этому понятию нарушение в форме «пиратства». Понятие авторского права впервые сформулировано и закреплено законом в Великобритании в 1709 году, когда английский парламент принимает Статут королевы Анны. В нем изложены основные принципы авторского права, не устаревшие до настоящего времени. В 1787 году, вскоре после провозглашения независимости, американская Конституция наделяет Конгресс властью «содействовать прогрессу науки и полезных ремесел, гарантируя на определенное время авторам и изобретателям исключительное право на их произведения». Программное обеспечение (ПО) пополнило список объектов интеллектуальной собственности, и

еще в 1964 году США признали необходимым регистрировать его наравне с литературными произведениями в соответствии с Законом об авторском праве. В 1980 году Закон уже явно защищает компьютерные программы от любых форм самовольного использования, а в декабре 1990 года Конгресс США вынужден ужесточить меры наказания за нарушения авторского права создателей программного обеспечения. Запрещается дублирование программного обеспечения для прибыли, перекачивание копий из сети или «бескорыстное» предоставление неправомочной копии другому индивидууму (единственное исключение − право пользователя на одну резервную архивную копию). Названные действия квалифицируются в США как федеральное преступление, подлежащее наказанию значительным штрафом и сроком тюремного заключения. С 1993 года не менее 45 стран пересматривали законодательство об авторском праве, повышая уголовную ответственность за нарушения и предоставляя соответствующие полномочия суду и исполнительным органам. Специально созданный союз *BSA* (*Business Software Alliance*) представляет интересы почти 20 компаний-производителей ПО: способствует продвижению продукции ПО на мировом рынке и координирует свои действия по защите авторского права в международном масштабе. В 1988 году США принимают решительные меры по защите своей информационной системы (ИС) в других странах. Комиссия по торговле следит за соблюдением закона и составляет перечень из трех списков:

– страны, где допускаются самые грубые нарушения (именно в этом списке находиится Россия);

– страны, где возможны нарушения;

– страны, где достаточно простого наблюдения.

В отношении стран, фигурирующих в первом списке, США могут применять различные санкции (увеличение пошлин, отмена льгот и т. п.), вынуждая совершенствовать национальную систему охраны интеллектуальной собственности, и не только чужой, но и отечественной.

Первый российский закон об авторском праве принят в начале XIX века, затем указом Николая I в середине века был увеличен срок охраны авторского права до 50 лет после смерти автора. Появление этого указа связывают с ходатайством вдовы А.С. Пушкина Натальи Николаевны.

Восстановление института авторского права в России, начиная с 1992 года, знаменовалось принятием ряда известных законов, унифицированных с аналогичными законами европейских стран (ЕЭС),

США и Японии, что позволило России в 1994−1995 годах присоединиться к важным международным соглашениям в этой области − Бернской конвенции и Римской конвенции.

Сегодня вопросы защиты прав на интеллектуальную собственность регулируются гражданским законодательством.

Авторское право и регулируемые им имущественные и личные неимущественные отношения связаны с созданием и использованием произведений литературы, науки и искусства.

Авторское право как самостоятельный институт решает конкретные задачи, которые включают всемирную охрану:

– имущественных, личных неимущественных прав и законных интересов авторов;

– обеспечение правовыми средствами наиболее благоприятных условий для создания научных и художественных произведений;

– широкое использование их обществом.

Произведения, пользующиеся охраной

1. Литературные произведения – особенность их в том, что мысли, чувства, идеи и образы выражаются посредством слова в оригинальной композиции и оригинальном изложении.

2. Музыкальные произведения выражаются в сочетании звуков, образующих мелодию и связанных ритмом и гармонией. Музыкальное произведение может фиксироваться также на аудионосителях (кассеты, компакт-диски и т. п.).

3. Литературная обработка – представляет собой музыкальную или литературную обработку произведений авторов, которые в силу некоторых причин (отсутствие навыков и др.) не в состоянии сами привести свое произведение в законченный вид (произведения неизвестных авторов и народные).

4. Хореографические произведения или пантомимы − произведения искусства, создаваемые при помощи пластических движений человеческого тела. Эти произведения довольно сложно закрепить с помощью каких-то особых знаков на бумаге, поэтому для этих целей, как правило, используют фото-, кино- и видеозапись.

5. Произведения изобразительного искусства − это произведения живописи, графики, скульптуры, декоративно-прикладного искусства и т. п.

6. Архитектурные произведения (проекты) представляют собой синтез инженерного искусства, бионики, живописи, скульптуры,

науки, архитектуры. На основе архитектурного проекта строятся здания, сооружения, комплексы и т. п.

7. Аудиовизуальные произведения − категория, охватывающая многообразные произведения для кино, телевидения, радио, интерактивных сетей и т. п.: сценарии, сценарные планы, тексты песен, кинофильмы, телепередачи, радиопередачи, заставки и многое другое.

8. Программные продукты для средств вычислительной техники могут представлять собой как отдельные прикладные программы (текстовые редакторы, компиляторы и т. п.), так и базы данных, энциклопедии, программы мультимедиа. Кроме того, особенность этой категории заключается в том, что в программах для ЭВМ может иметь место использование других объектов авторского права, это могут быть произведения литературы, музыкальные произведения, произведения изобразительного искусства, кинематографии, а также многое другое.

Основное отличие авторского права от режима правовой охраны других результатов интеллектуальной деятельности состоит в том, что произведение литературы, науки и искусства становится объектом авторского права в силу самого факта его создания автором без какой-либо регистрации, оформления или соблюдения иных формальностей.

Свободно распространяемая информация

Согласно федеральному закону «Об информации, информационных технологиях и о защите информации» к общедоступной относится общеизвестная и иная информация, доступ к которой не ограничен (ст. 7). Такая информация может использоваться ее получателями свободно, по своему усмотрению, если только для ее использования не установлены специальные ограничения.

По общему правилу, открытой является информация о деятельности государственных органов и органов местного самоуправления – если иное не установлено федеральными законами (ст. 3).

Развивая это правило, законодатель говорит о том, что любой гражданин вправе получать от государственных органов, органов местного самоуправления, их должностных лиц информацию, непосредственно затрагивающую его права и свободы (ст. 8). Отказ в предоставлении такой информации, при условии соблюдения гражданином порядка обращения за получением информации, является неправомерным и может быть оспорен гражданином в суде.

В соответствии с п. 4 ст. 8 указанного закона не может быть ограничен доступ:

1) к нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Следует отметить, что – при необходимости гражданин вправе в письменном заявлении на имя руководителя государственного, муниципального органа, организации просить также выдачи копий документов, необходимых для решения вопросов, касающихся его прав и законных интересов.

Закон гарантирует бесплатность предоставления информации в следующих случаях:

– если информация о деятельности государственных и муниципальных органов размещается такими органами в информационно-телекоммуникационных сетях (Интернет);

– если информация затрагивает права и обязанности заинтересованного лица.

Установление государственным органом, либо органом местного самоуправления, их должностными лицами платы за предоставление информации возможно только в случаях и на условиях, которые установлены федеральным законом.

Следует отметить, что действующее законодательство об информации предоставляет широкие полномочия её обладателю – он вправе, в частности, разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа. При этом данное право обладателя информации не может нарушать прямо предусмотренное федеральным законом право гражданина на доступ к той или иной информации. Это означает, что установление произвольных ограничений, запретов на доступ к информации неправомерно (ч. 4

ст. 29, ч. 3 ст. 55 Конституции РФ, постановление Конституционного суда РФ от 18.02.2000 № 3-П).

Ограничение доступа к информации

Ограничение доступа к информации, а также условия отнесения информации к сведениям, составляющим коммерческую, служебную и иную тайну определяется федеральным законодательством. Информация, полученная при исполнении должностными лицами профессиональных обязанностей или при осуществлении организациями определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица (организации) федеральным законодательством возложены обязанности по соблюдению конфиденциальности такой информации.

Важное требование к обладателям информации ограниченного доступа, которым она стала известна в связи с исполнением должностных обязанностей, – соблюдение её конфиденциальности (то есть она не может передаваться третьи лицам).

Конфиденциальная информация – это документированная информация, то есть зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать, доступ к которой ограничивается в соответствии с законодательством. Законом охраняется государственная, служебная, банковская, военная, коммерческая тайна. Часть коммерческой информации составляет особый блок и может быть отнесена к коммерческой тайне.

Особой категорией охраняемой законом информации являются *персональные данные* – любая информация, относящаяся к определенному или определяемому на основании такой информации гражданину, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая соответствующая информация (ст. 3 федерального закона «О персональных данных»). Такая информация, по общему правилу, должна оставаться конфиденциальной для третьих лиц (ч. 1 и 2 ст. 7), за исключением случаев, когда:

1) сам гражданин – субъект персональных данных – дает согласие на ее разглашение, в том числе для определенных (ограниченных) целей использования (например, включение данных о сотрудниках организации в общедоступные справочники);

2) законом установлены обязательные требования для предоставления персональных данных (например, обнародование государственными служащими сведений о своих доходах и имуществе);

3) информация о гражданине обезличивается, то есть не позволяет достоверно установить его и, по существу, теряет характер персональных данных (например, гражданин Б., сотрудник коммерческой фирмы).

Также, по общему правилу, не допускаются любые действия по обработке персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни (ст. 10 федерального закона «О персональных данных»). Исключение из этого правила закон устанавливает, в частности, для целей отправления правосудия, оказания медицинской помощи, безопасности, оперативно-розыскной деятельности.

Наконец, в ряде случаев закон устанавливает запрет на распространение информации. Так, федеральным законом «Об информации…» (ст. 10) установлен запрет на распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти или вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Предпринимательская тайна отождествляется с коммерческой тайной.

Коммерческая тайна – это охраняемое законом право предпринимателя на засекречивание сведений, не являющихся государственными секретами о деятельности предприятия, связанные с производством, технологией, управлением, финансами, разглашение которых могло бы нанести ущерб его интересам. В соответствии с ГК РФ коммерческой тайной является информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель принимает меры к охране ее конфиденциальности. Следовательно, коммерческая тайна не может быть общеизвестной и общедоступной информацией, открытое ее использование несет угрозу экономической безопасности предпринимательской деятельности, в связи с чем предприниматель осуществляет меры по сохранению ее конфиденциальности и защите от незаконного использования.

Отнесение тех или иных сведений к коммерческой тайне должно удовлетворять следующим требованиям:

– их открытое использование может причинить ущерб;

– фирма может обеспечить сохранение их конфиденциальности;

– эти сведения нуждаются в защите, так как они не являются государственной тайной и не защищены патентом;

– их сокрытие не наносит вред обществу.

При определении информации, относящейся к категории коммерческой тайны, предприниматель должен учитывать, что по степени конфиденциальности вся имеющаяся информация может быть распределена по следующим группам:

– информация высшей степени конфиденциальности. Данная информация является ключевой в деятельности фирмы, основой ее нормального функционирования. Утрата или разглашение этой информации нанесет непоправимый ущерб деятельности фирмы. Это угроза высокой степени, и ее реализация может привести к ликвидации фирмы;

– строго конфиденциальная информация. Утечка этой информации может вызвать значительные по тяжести последствия. Это информация о стратегических планах фирмы, о перспективных соглашениях и т. п.;

– конфиденциальная информация – ее разглашение наносит фирме ущерб, сопоставимый с текущими затратами фирмы, но он может быть преодолен в сравнительно короткие сроки;

– информация ограниченного доступа – ее утечка оказывает незначительное негативное воздействие на экономическое положение фирмы (должностные инструкции, структура управления);

– открытая информация. Ее распространение не представляет угрозы для экономической безопасности фирмы. Наоборот, отсутствие данной информации может оказать негативное воздействие на экономическое положение фирмы.

Каким же образом можно осуществить разграничение информации открытой и той, которая нуждается в защите?

Для этого следует использовать следующие критерии.

Во-первых, это вероятность угрозы экономической безопасности фирмы. В случае получения этой информации конкурентами фирма понесет экономический ущерб. Так, широко известный напиток «кока-кола» производится на основе секретной формулы, являющейся коммерческой тайной, и обеспечивает процветание фирмы. В случае разглашения этой информации фирму ожидают серьезные экономические трудности.

Во-вторых, это возможность защиты информации. Если, например, информация не входит в обязательный перечень открытого характера, то следует определить, существует ли возможность ее защиты с помощью общих либо специальных мер защиты.

В-третьих, это экономическая целесообразность защиты информации. Только в том случае, если разглашение или утечка информации может нанести существенный экономический ущерб фирме, следует организовывать ее защиту.

Однако не вся информация, которой располагает предприниматель, может быть отнесена к категории коммерческой тайны. Постановлением Правительства РФ от 5 декабря 1991 г. № 35 утвержден перечень сведений, которые не могут составлять коммерческую тайну.

К ним относятся:

– учредительные документы (устав, учредительный договор); документы, дающие право заниматься предпринимательской деятельностью (регистрационное удостоверение, свидетельство о регистрации, лицензии, сертификаты, патенты);

– сведения по установленным формам отчетности о финансово-хозяйственной деятельности, необходимые для проверки правильно-

сти исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РФ); документы о платежеспособности;

– сведения о численности работающих, их составе, заработной плате, условиях работы, наличии свободных рабочих мест; документы об уплате налогов и обязательных платежей; сведения о соблюдении установленных правил охраны труда; сведения о соблюдении установленных норм охраны окружающей среды;

– сведения о нарушении антимонопольного законодательства; сведения о реализации продукции, причинившей вред здоровью населения;

– сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, акционерных обществах и других организациях, занимающихся предпринимательской деятельностью.

Так, *не может быть признана коммерческой тайной* такая социально значимая информация, как*:*

– о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

– о численности и составе работников предприятия, о системе оплаты и об условиях труда, об охране труда, показателях производственного травматизма и профессиональной заболеваемости, о наличии свободных рабочих мест;

– о загрязнении предприятием окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и населения в целом;

– сведения, содержащиеся в документах, дающих право на осуществление предпринимательской деятельности (ст. 5 федерального закона «О коммерческой тайне»).

В плане защиты наиболее важной информации предприниматель должен решить сложную проблему.

С одной стороны, он должен предоставить максимум информации о своей деятельности потребителям, контрагентам, кредиторам и т. п. для того, чтобы они сделали выбор в его пользу. Реклама привлекает покупателей, деловые связи, патенты и лицензии, ноу-хау – контрагентов, финансовое положение – инвесторов.

С другой стороны, предприниматель должен оградить названные группы лиц, а также своих конкурентов от информации, утечка

или разглашение которой может представлять угрозу его экономической безопасности. В выборе «золотой середины», то есть определении того оптимального количества информации, которого будет достаточно для внешних пользователей и разглашение которой не будет представлять угроз экономической безопасности, и состоит первый шаг предпринимателя в процессе защиты информации, составляющей коммерческую тайну.

Служебная и профессиональная тайна

Служебная тайна – это охраняемая законом информация о деятельности сотрудников государственных органов, а также полученные ими на законных основаниях конфиденциальные сведения.

Информацию, отнесенную к категории служебной тайны, можно условно разделить на два блока:

1. Информация с грифом *«Для служебного пользования»* о деятельности государственных или муниципальных органов (например, тайна следствия (данные предварительного расследования), военная тайна, тайна совещания судей и прочие виды судебной тайны и т. д.).

2. Сведения, ставшие известными госслужащим в ходе исполнения непосредственных обязанностей (например, информация о частной жизни гражданина (данные об имущественном положении, вероисповедании, добытые в процессе расследования уголовного дела), сведения о секретах производства или антиконкурентной политике предприятия и т. д.).

Следует отметить, что сегодня в российском законодательстве не имеется чёткого и конкретного определения *профессиональной тайны*, однако наличествуют прямые указания Декларации прав и свобод человека и гражданина, направленные на ограничение всеобщего доступа к информации в целях сохранения конфиденциальности.

Виды профессиональной тайны

Банковская тайна. Понятие банковской тайны, в соответствии со ст. 857 ГК РФ, охватывает сведения о банковском счете, вкладе, операциях по счету, а также сведения о клиентах банка. Банковская тайна защищает конфиденциальную информацию клиента или коммерческую информацию корреспондента. Федеральный закон «О банках и банковской деятельности» гласит, что Банк России не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций,

полученные им в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Нотариальная тайна. Тайна является специфическим правилом нотариальных действий. В соответствии со ст. 5 Основ законодательства Российской Федерации о нотариате, нотариусу при исполнении служебных обязанностей, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий или увольнения, за исключением случаев, предусмотренных Основами. (Обязанность хранить профессиональную тайну включена в текст присяги нотариуса.)

Врачебная тайна. Согласно ст. 61 Основ законодательства Российской Федерации об охране здоровья граждан информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну.

Адвокатская тайна. В соответствии с Федеральным законом «Об адвокатской деятельности и адвокатуре в Российской Федерации» адвокат, помощник адвоката и стажер адвоката не вправе разглашать сведения, сообщенные доверителем в связи с оказанием ему юридической помощи. Причем доверительные сведения, полученные адвокатом, могут быть как в виде документов, так и в устном виде. Законом установлены гарантии независимости адвоката. В частности, адвокат не может быть допрошен в качестве свидетеля об обстоятельствах, которые стали ему известны в связи с исполнением им обязанностей защитника или представителя.

Тайна страхования. Институт страховой тайны во многих отношениях схож с институтом банковской тайны. Тайну страхования, в соответствии со ст. 946 ГК РФ, составляют полученные страховщиком в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с российским законодательством.

Тайна связи. Тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, охраняется Конституцией Российской Федерации.

Тайна усыновления. Институт тайны усыновления связан с интересами охраны семейной жизни и выражается в установлении гражданской и уголовной ответственности за разглашение тайны усыновления (удочерения). Согласно ст. 155 УК РФ тайна усыновления может быть двух разновидностей. Первой обладают лица, которые обязаны хранить факт усыновления как служебную или профессиональную тайну (судьи, работники местных администраций, органов опеки и попечительства и прочие лица, указанные в ч. 1 ст. 139 СК РФ). Второй – все другие лица, если установлены их корыстные или иные низменные побуждения при разглашении тайны усыновления без согласия обоих усыновителей.

Тайна исповеди. Обеспечение тайны исповеди является внутренним делом священника, юридической ответственности за ее разглашение он не несет. Согласно ч. 2 ст. 51 Конституции РФ, а также ч. 7 ст. 3 федерального закона «О свободе совести и религиозных объединениях» священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали ему известны из исповеди.

Сведения можно отнести к профессиональной тайне, если они удовлетворяют таким требованиям:

– информация, о которой идёт речь, получена держателем вследствие его профессиональной деятельности;

– она не есть государственная тайна или служебная;

– держатель не является работником муниципальным и не состоит на госслужбе;

– засекреченность необходимо соблюсти, как этого требует законодательство, чтобы не нанести ущерба доверителю.

Понятие *«государственная тайна»* является одним из важнейших в системе защиты государственных секретов в любой стране. От ее правильного определения зависит и политика руководства страны в области защиты секретов. Определение этого понятия дано в законе «О государственной тайне»: «Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации».

В этом определении указываются категории сведений, которые защищаются государством, и сообщается, что *распространение этих сведений может нанести ущерб интересам государственной безопасности.*

Модель определения государственных секретов обычно включает в себя следующие *существенные признаки***:**

– предметы, явления, события, области деятельности, составляющие государственную тайну;

– противник (данный или потенциальный), от которого в основном осуществляется защита государственной тайны;

– указание в законе, перечне, инструкции сведений, составляющих государственную тайну;

– наносимый ущерб обороне, внешней политике, экономике, научно-техническому прогрессу страны и т. п. в случае разглашения (утечки) сведений, составляющих государственную тайну.

Сведения, которые относятся к государственной тайне (указаны лишь разделы):

– в военной области;

– о внешнеполитической и внешнеэкономической деятельности;

– в области экономики, науки и техники;

– в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

Нельзя засекречивать информацию в качестве государственной тайны:

– если ее утечка (разглашение и т. п.) не влечет ущерба национальной безопасности страны;

– в нарушение действующих законов;

– если сокрытие информации будет нарушать конституционные и законодательные права граждан;

– для сокрытия деятельности, наносящей ущерб окружающей природной среде, угрожающей жизни и здоровью граждан.

Подробнее этот перечень содержится в ст. 7 закона РФ «О государственной тайне».

Важным *признаком* государственной тайны является *степень секретности* сведений, отнесенных к ней.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений*: «особой важности», «совершенно секретно»* и *«секретно»*.

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством Российской Федерации.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

В зависимости от вида, содержания и размеров ущерба можно выделить *группы некоторых видов ущерба* при утечке (или возможной утечке) сведений, составляющих государственную тайну.

1. Политический ущерб наступает при утечке сведений политического и внешнеполитического характера, о разведывательной деятельности спецслужб государства и др. Выражаться в следующем: в результате утечки информации могут произойти серьезные изменения в международной обстановке не в пользу Российской Федерации; утрата страной политических приоритетов в каких-то областях; ухудшение отношений с какой-либо страной или группой стран и т. д.

2. Экономический ущерб наступает при утечке сведений любого содержания: политического, экономического, военного, научно-технического и т. д. и выражается прежде всего в денежном исчислении.

Экономические потери от утечки информации могут быть *прямые и косвенные.* Прямые потери могут наступить в результате утечки секретной информации о системах вооружения, обороне страны, которые в результате этого практически потеряли или утратили свою эффективность и требуют крупных затрат на их замену или переналадку. Косвенные потери чаще всего выражаются в виде размера упущенной выгоды: срыв переговоров с иностранными фирмами, о выгодных сделках с которыми ранее была договоренность; утрата приоритета в научном исследовании, в результате чего соперник быстрее довел свои исследования до завершения и запатентовал их и т. д.

3. Моральный ущерб, как правило, неимущественного характера, наступает от утечки информации, вызвавшей или инициировавшей противоправную государству пропагандистскую кампанию, подрывающую репутацию страны. Выражается, например, в выдворении из государств наших дипломатов, разведчиков, действовавших под дипломатическим прикрытием, и т. п.

2.2. Понятие утечки информации ограниченного доступа по техническим каналам

Согласно ГОСТу 50922-2006 «Защита информации. Основные термины и определения», под *утечкой* понимают неконтролируемое распространение защищаемой информации.

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Итак, из определения можно сделать вывод, что основными причинами утечки являются:

– её разглашение;

– нарушение заинтересованными лицами установленных правил доступа к защищаемой информации (несанкционированный доступ);

– целенаправленная деятельность разведок, в том числе с помощью технических средств.

Информация может передаваться за пределы контролируемой зоны или полем, или веществом. Человек же является источником или субъектом отношений. В зависимости от природы сигналы распространяются в определенных физических средах. Средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые (грунт) среды. Физические процессы, происходящие в средствах вычислительной техники, создают в окружающей среде побочные электромагнитные, акустические и другие волны (колебания), которые в той или иной степени связаны с обработкой и передачей информации.

Подобные излучения могут обнаруживаться на довольно значительных расстояниях (до сотен метров) и использоваться злоумышленниками, пытающимися получить доступ к информации ограниченного доступа. Поэтому мероприятия по защите информации, циркулирующей в информационных технических системах, направлены прежде всего на снижение уровней таких излучений.

Источниками излучения колебаний являются разнообразные технические средства, в которых циркулирует информация с ограниченным доступом.

Такими средствами могут быть:

– электронно-вычислительная техника и компьютерные сети;

– электронные средства оргтехники;
– сети электропитания и линии заземления;
– системы телеграфной, факсимильной и сотовой связи;
– автоматические сети телефонной связи;
– средства громкоговорящей связи;
– средства звуко- и видеозаписи и воспроизведения;
– системы звукоусиления речи и т. д.

Как правило, технические средства излучающие сигналы (волны) улавливают за счет антенных или микрофонных свойств существующие в непосредственной близости от них электромагнитные или акустические излучения. Такие технические средства могут преобразовывать принятые излучения в электрические сигналы и передавать их по своим линиям связи за территорией объекта на значительные расстояния, что повышает опасность утечки информации.

Каналом утечки информации, как правило, называют физический путь от источника информации к злоумышленнику. Для возникновения такого канала необходимы определенные условия и факторы, которые позволили бы злоумышленнику при наличии специальных технических средств получить конфиденциальную информацию. Анализ современных технических средств позволяет говорить о следующей классификации технических каналов утечки информации:

– электромагнитные каналы (утечка за счет побочного или паразитного электромагнитного излучения разных диапазонов);

– акустические каналы (утечка за счет распространения звуковых колебаний в любом звукопроводящем материале);

– электрические каналы (утечка по токоведущим линиям, сетям питания или заземления, по линиям охранной и других видов сигнализаций и т. д.);

– визуально-оптические каналы (утечка за счет электромагнитных излучений в инфракрасной, видимой и ультрафиолетовой части спектра);

– материально-вещественные каналы (утечка информации на материальных носителях: бумага, фото, магнитные носители, отходы (жидкие, твердые, газообразные) и т. д.

Электромагнитные каналы утечки информации

Одной из наиболее вероятных угроз перехвата информации в системах обработки данных считается утечка за счет перехвата побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами.

Электромагнитные излучения технических средств передачи информации (ТСПИ). Носителем информации в ТСПИ является электрический ток. При прохождении электрического тока по токоведущим элементам ТСПИ вокруг них (в окружающей среде) возникает электромагнитное поле, поэтому элементы ТСПИ рассматриваются как излучатели электромагнитных волн. К электромагнитному излучению ТСПИ относят:

– *электромагнитные излучения на частотах работы высокочастотных (ВЧ) генераторов ТСПИ и вспомогательных технических средств и систем (ВТСС)*. К таким устройствам можно отнести: генераторы тактовой частоты, генераторы измерительных приборов, задающие генераторы, и т. д.;

– *электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.* Самовозбуждение УНЧ ТСПИ (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи т. п.) возможно за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радиоразведкии радиотехнической разведки, размещенными вне контролируемой зоны.

Побочные электромагнитные излучения возникают вследствие непредусмотренной схемой или конструкцией рассматриваемого технической системы передачи информации по паразитным связям напряжения, тока, заряда или магнитного поля.

Под паразитной связью понимают связь по электрическим или магнитным цепям, появляющуюся независимо от желания конструктора.

Экранирование технических средств обработки информации и помещений, в которых происходит прием, передача и обработка конфиденциальной информации, позволяет снизить уровни электромагнитных излучений до заданных величин.

Акустические каналы

Источником образования акустического канала утечки информации являются механические колебательные системы, преобразующие акустические сигналы в электрические, и обратно. К колебательным системам можно отнести: человеческую речь, движущиеся элементы машин, телефонные аппараты, звукоусилительные системы и т. д.

Акустические каналы утечки информации образуются за счет:

– распространение акустических колебаний в свободном воздушном пространстве;

– воздействия звуковых колебаний на элементы и конструкции зданий;

– воздействия звуковых колебаний на технические средства обработки информации.

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются высокочувствительные микрофоны и специальные направленные микрофоны. Они предназначены для прослушивания акустической информации с определенного направления и с больших расстояний.

Миниатюрные микрофоны соединяются с портативными звукозаписывающими устройствами (диктофонами) или передатчиками. Автономные устройства, конструкционно объединяющие миниатюрные микрофоны и передатчики, называют закладными устройствами перехвата речевой информации, или просто акустическими закладками «жучками».

Радиомикрофоны – «жучки»

Прием информации осуществляется на специальные приемные устройства, работающие в соответствующем диапазоне длин волн. Закладные устройства, прием информации с которых можно осуществлять с обычного телефонного аппарата, устанавливаются как непосредственно в корпусе телефонного аппарата, находящегося в контролируемой зоне, так и подключаются к телефонной линии, чаще всего в телефонную розетку. Подобное устройство конструкционно объединяет миниатюрный микрофон и специальный блок коммутации и часто называется *«телефонным ухом».*

В вибрационных технических каналах утечки информации средой распространения акустических сигналов являются конструкции

зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твердые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы). Стетоскопы – это устройства, преобразующие упругие механические колебания твердых физических сред в акустический сигнал. Они применяются для прослушивания соседних помещений через стены, потолки, пол или через трубы центрального отопления. Стетоскопические датчики часто дооборудуются радиопередатчиком, что позволяет прослушивать перехваченную информацию на сканирующий приемник, как от обычной радиозакладки. Лазерные стетоскопы считывают лазерным лучом вибрацию с различных предметов, обычно это оконные стекла. Современные лазерные стетоскопы хорошо работают на дальности до 300 *м*.

Электронный стетоскоп *Лазерные стетоскопы*

Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС, обладающих «микрофонным эффектом».

Чтобы обеспечить защиту от несанкционированного прослушивания используют средства виброакустического зашумления, которые обеспечивают высокую эффективность при относительно небольших материальных затратах и несложности установки. Наиболее простое устройство акустического шума для защиты от прослушивания в замкнутых пространствах (тамбур, салон автомобиля, небольшие кабинеты) представляет собой генератор «белого» шума. Он обеспечивает снижение разборчивости речевой информации после записи или передачи по каналу связи. Самым простым методом получения «белого» шума является использование шумящих электронных элементов (транзисторов, различных диодов, а ранее и электронных ламп) с усилением напряжения шума.

Для защиты от узконаправленных микрофонов рекомендуются следующие меры:

– при проведении совещаний следует обязательно закрывать окна и двери (лучше всего, чтобы комната для совещаний представляла собой изолированное помещение);

– для проведения переговоров нужно выбирать помещения, стены которых не являются внешними стенами здания;

– необходимо обеспечить контроль помещений, находящихся на одном этаже с комнатой для совещаний, а также помещений, находящихся на смежных этажах.

Электрические каналы утечки информации

Электрический канал перехвата информации – это прямое (непосредственное) подключение к линиям связи. Самый простой способ – это непосредственное параллельное подключение к линии связи. Но данный факт легко обнаруживается, так как приводит к изменению характеристик линии связи за счет падения напряжения. Поэтому злоумышленнику необходимо подключаются через согласующее устройство, несколько снижающее падение напряжения. Электрический канал часто используется для перехвата телефонных разговоров. Информация записываться на диктофон или передается злоумышленнику, при этом время передачи неограниченно. Элементы, цепи, тракты, соединительные провода и линии связи любых электронных систем и схем постоянно находятся под воздействием собственных (внутренних) и сторонних (внешних) электромагнитных полей различного происхождения, индуцирующих или наводящих в них значительные напряжения. Такое воздействие называют *электромагнитным влиянием или просто влиянием на элементы цепи*. Такое влияние образует паразитные связи.

Основными видами паразитных связей в схемах радиоэлектронного оборудования являются емкостные, индуктивные, электромагнитные, электромеханические связи и связи через источник питания и заземления.

Заземление – это устройство, состоящее из заземлителей и проводников, соединяющих заземлители с электронными и электрическими устройствами, приборами и т. д. *Заземлителем* называют проводники, выполненные из проводящего материала и находящиеся в непосредственном соприкосновении с грунтом. В основном они выполняют защитную функцию и предназначаются для соединения с землей приборов.

Для защиты объекта обычно используется экранирование информационных линий связи между устройствами технических средств передачи информации (ТСПИ).

Защита линей связи от наводок, обычно связана с необходимостью разместить линию связи в экранирующую оплетку или фольгу.

Для уменьшения магнитной и электрической связи между проводами необходимо сделать следующее:

– уменьшить напряжение источника сигнала или тока;

– уменьшить площадь петли;

– максимально разнести цепи;

– передавать сигналы постоянным током или на низких частотах;

– использовать провод в магнитном экране с высокой проницаемостью;

– включить в цепь дифференциальный усилитель.

Визуально-оптические каналы утечки информации

Основой визуально-оптического канала является оптическое излучение, или свет. По диапазону излучения визуально-оптические каналы утечки информации могут быть образованы:

– в видимой (λ от 10 *нм* до 1 *мм*),

– инфракрасной (от 1 *мм* до 770 *нм*),

– ультрафиолетовой (от 380 до 10 *нм*) областях спектра.

Получение видовых характеристик объекта является результатом решения трех задач:

– обнаружение – зрительное восприятие объекта;

– различение – определение крупных деталей объекта;

– опознавание (идентификация) – различение мелких деталей объекта.

Для получение видовых характеристик используются различные технические устройства и приборы: бинокли, приборы ночного видения, тепловизоры и т. д.

Для защиты объекта от утечки информации по оптико-визуальному каналу необходимо:

– располагать объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника;

– уменьшить отражательные свойства объекта защиты;

– уменьшить освещенность объекта защиты;

– использовать средства преграждения или значительного ослабления отраженного света (ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды);

– применять средства маскировки, имитации и др.

Материально-вещественные каналы утечки информации

Особенность материально-вещественного канала, в сравнении с другими каналами, обусловлена спецификой источников и носителей, добываемой по нему информации. Источниками и носителями информации в данном случае являются субъекты (люди) и материальные объекты (макро- и микрочастицы), которые имеют четкие пространственные границы локализации (за исключением излучений радиоактивных веществ). Утечка информации по материально-вещественным каналам сопровождается физическим перемещением людей и материальных тел с информацией за пределы защищаемого объекта.

Основными источниками информации материально-вещественного канала утечки информации являются:

– черновики различных документов;

– отходы делопроизводства и издательской деятельности в организации, в том числе использованная копировальная бумага, забракованные при оформлении и размножении документов листы;

– вышедшие из строя магнитные и иные носители информации ЭВМ, на которых во время эксплуатации содержалась информация с ограниченным доступом.

Основные направления инженерно-технической защиты информации от утечки

Защита информации от технических средств разведки представляет собой совокупность организационных и технических мероприятий, проводимых с целью исключения (существенного затруднения) добывания злоумышленником информации об объекте защиты с помощью технических средств.

Защита должна проводиться своевременно, активно, разнообразно, непрерывно, рационально, комплексно, планово.

Одним из основных требований является своевременность принятия решения на организацию защиты информации. Ускорение процесса выработки решения необходимо, во-первых, для того чтобы своевременно решить возникшие проблемы и не давать им разрастись

до такого состояния, когда решение их станет невозможным или бесполезным, во-вторых, для того чтобы подчиненные имели достаточно времени для выполнения поставленных перед ними задач.

Активность противодействия прежде всего предусматривает наступательный, активный характер противодействия, основанный на анализе складывающейся обстановки, умении сделать правильные выводы о возможных действиях потенциального противника, позволяющие упредить их и настойчиво осуществлять эффективные меры противодействия.

Разнообразие противодействия направлено на исключение шаблона в организации и проведении мероприятий и подразумевает творческий подход к его организации и осуществлению.

Комплексность предусматривает проведение комплекса мероприятий, направленных на своевременное закрытие всех возможных каналов утечки информации об объекте. Недопустимо применять отдельные технические средства или методы, направленные на защиту только некоторых, из общего числа возможных, каналов утечки информации.

Непрерывность противодействия предусматривает проведение мероприятий по комплексной защите объекта информатизации на всех этапах жизненного цикла разработки и существования специальной продукции или обеспечения производственной деятельности объекта защиты.

Плановость проведения мероприятий предусматривает прежде всего разработанные заранее, еще на стадии проектирования и строительства объекта, мероприятия, направленные на защиту информации.

Технические средства защиты территории и объектов

Для управления доступом в помещения широкое распространение получили замки с кодовым набором. Кроме того, для защиты помещений широко используются датчики, которые могут быть разделены на три группы:

– датчики для обнаружения попыток проникновения на территорию объекта или в контролируемое помещение;

– датчики для обнаружения присутствия человека в помещении;

– датчики для обнаружения перемещения охраняемого предмета.

а) *б)* *в)* *г)* *д)*

Датчики охранных сигнализаций:

а) датчик движения; б) датчик дыма; в) датчик газа; г) датчик открытия окон, дверей и т. д; д) датчик разбития оконных стекол

Проведение специальных проверок объектов информатизации

Специальная проверка – проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

Специальное исследование (объекта защиты информации) – исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации.

Цель проведения комплексных специальных проверок помещений заключается в пресечении (предотвращении) получения злоумышленником (противником) защищаемой информации из этих помещений с помощью средств несанкционированного съема информации (НСИ). Тем самым предотвращается ущерб, который может быть нанесён собственнику, владельцу, пользователю защищаемой информации в случае использования злоумышленником (противником) этой информации в своих интересах.

Комплексные специальные проверки помещений занимают заметное место в общей системе мероприятий по защите информации. Они проводятся: при аттестации помещений; периодически (в соответствии с заранее разработанным планом-графиком); после проведения в помещениях каких-либо работ (ремонта, монтажа оборудования, изменения интерьера и т. д.); неконтролируемого посещения посторонними лицами; во всех случаях, когда возникает подозрение в утечке информации через возможно внедрённые средства НСИ.

2.3. Классификация компьютерных преступлений

Современные компьютерные технологии в настоящее время охватывают практически все сферы социальной жизни общества.

Внедрение современных компьютерных технологий привело к новым видам преступлений, связанных с ЭВМ, получившим распространенное название – киберпреступления.

Киберпреступления приобретают сегодня все более изощренный (кибертерроризм) и иногда трудноопределимый (компьютерное мошенничество) характер. Сегодня киберпреступления можно смело сравнивать с оружием массового поражения. Киберпреступность – это нарастающая угроза безопасности общества и государства, а в целом и мирового сообщества.

Безопасность в сфере информационных технологий – основная проблема государств всего мира. Конвенция Совета Европы о киберпреступности была открыта для подписания в 2001 году, а вступила в силу 1 июля 2004 года. Сегодня Конвенцию подписали 46 государств – членов Совета, а также Канада, Япония, ЮАР и США. Конвенция стала первым документом, в котором содержится классификация киберпреступлений. Конвенция Совета Европы о киберпреступности называет четыре вида так называемых «чистых» компьютерных преступлений, определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

– незаконный доступ – ст. 2 (противоправный умышленный доступ к компьютерной системе либо ее части);

– незаконный перехват – ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);

– вмешательство в данные – ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);

– вмешательство в систему – ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

Эти преступления являются компьютерными. Именно на свойства конфиденциальности, целостности и доступности данных направлена защита компьютерной информации в целом. Но есть и другая группа преступлений, которые непосредственно связаны с компьютером или совершаются с его помощью. К ним можно отнести электронные кражи, мошенничество, нарушение авторских прав, распространение призывов в сети Интернет к межнациональной розни и т. д.

В настоящее время наиболее приемлемой классификацией компьютерных преступлений с учетом развития научно-технического прогресса является классификация, выделяющая следующие виды киберпреступлений:

– насильственные или иные потенциально опасные киберпреступления, посягающие на физическую безопасность, жизнь и здоровье человека;

– преступления, посягающие на конфиденциальность информации (незаконный доступ к компьютерам или компьютерным системам без причинения ущерба информации);

– деструктивные киберпреступления, заключающиеся в повреждении данных и посягающие на целостность данных и безопасность функционирования компьютерных систем (такие преступления также могут причинить имущественный ущерб, но они не связаны с хищением информации, данных, денежных средств);

– преступления, посягающие на имущество, имущественные права, а также на право собственности на информацию и авторские права;

– преступления, посягающие на общественную нравственность;

– преступления, посягающие на общественную безопасность;

– иные киберпреступления, совершаемые посредством компьютерных сетей и посягающие на различные охраняемые законом объекты.

Анализ совершенных за последнее время преступных деяний с использованием компьютерных технологий позволяют выделить следующие наиболее типичные способы совершения компьютерных преступлений*:*

– «хакинг» – взлом интернет-сайтов) с последующим «дефейсом» (изменение содержания сайта, в частности, заглавной странички) или без него;

– «кардинг» – похищение реквизитов, идентифицирующих пользователей в сети Интернет как владельцев банковских кредитных карт с их возможным последующим использованием для совершения незаконных финансовых операций (покупка товаров либо банальное «отмывание» денег);

– «крекинг» – снятие защиты с программного обеспечения для последующего бесплатного использования, защита обычно устанавливается на так называемые «shareware»-продукты (программы с ограниченным сроком бесплатного пользования, по истечении которого необходима покупка продукта у компании-производителя). Сю-

да же можно отнести пиратское распространение законно купленных копий программного обеспечения;

– незаконное получение и использование чужих учетных данных для пользования сетью Интернет;

– «нюкинг», или «d.o.s.»-атаки (Denial of Service) – действия, вызывающие «отказ в обслуживании» (d.o.s.) удаленным компьютером, подключенным к сети (так называемое «зависание» ПК). Эта группа тесно связана с первой, поскольку одним из методов взлома интернет-сайтов является «d.o.s.»-атака с последующим запуском программного кода на удаленном сетевом компьютере с правами администратора;

– «спамминг» – массовая несанкционированная рассылка электронных сообщений рекламного или иного характера, либо «захламление» электронного почтового адреса (адресов) множеством сообщений;

– чтение чужих электронных сообщений.

В российском законодательстве такой вид преступлений, как компьютерные преступления был криминализирован лишь в 1996 году, когда в УК РФ была введена глава 28 «Преступления в сфере компьютерной информации». Она состоит всего лишь из трех статей: неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273), нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274). Глобализация информационных процессов в обществе привела к открытию новых глобальных угроз безопасности, перед которыми все мировое сообщество оказалось бессильно. Приведенная выше классификация киберпреступлений требует качественного пересмотра уголовного законодательства в этой сфере.

Сегодня все чаще и чаще мы встречаемся еще с одним проявлением киберпреступности – это мошенничество в информационной сфере.

Социальная инженерия

Социальная инженерия – метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Цель социальной инженерии – получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам. Термин «социальная инженерия» появился не так давно, но первые социальные инженеры начали свою деятельность еще в конце 90-х годов прошлого столетия. Примером может стать Кевин Митник, который сегодня знаменит именно тем, что читает

лекции об информационной безопасности и созданию превентивных мер по борьбе с кибермошенничеством, потому что сотрудники различных ведомств и корпораций, чтобы получить желаемую информацию, сами того не подозревая, используют методы социальной инженерии.

Чтобы не стать жертвой социальной инженерии, необходимо понять, как она работает. Рассмотрим основные типы социальной инженерии и методы защиты от них.

Претекстинг – это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Чаще всего данный вид атаки предполагает использование голосовых средств, таких как Skype, телефон и т. п. Сначала злоумышленник собирает некоторую информацию о жертве (имя сотрудника; должность; название проектов, с которыми он работает; дату рождения), потом использует реальные запросы с именем сотрудников компании и, после того как войдет в доверие, получает необходимую ему информацию.

Фишинг – интернет-мошенничество, направленное на получение конфиденциальной информации пользователей, например, авторизационных данных различных систем. Фишинговая атака – это поддельное письмо, отправленное жертве по электронной почте, которое выглядит как официальное письмо от платежной системы или банка. В письме могут содержаться сведения о дополнительных элементах безопасности и форма для ввода персональных данных (пин-кодов, логина и пароля и т. п.) или ссылка на web-страницу, где располагается такая форма. Причины доверия жертвы подобным страницам могут быть разные: блокировка аккаунта, поломка в системе, утеря данных и прочее.

Троянский конь – эта техника основывается на любопытстве, страхе или других эмоциях пользователей. Злоумышленник отправляет письмо жертве посредством электронной почты, во вложении которого находится, например, «обновление» антивируса, компромат на сотрудника, или видео с вечеринки. На самом же деле во вложении находится вредоносная программа, которая после того, как пользователь запустит ее на своем компьютере, будет использоваться для сбора или изменение информации злоумышленником.

Кви про кво (услуга за услугу) – данная технология предполагает обращение злоумышленника к пользователю по электронной почте или корпоративному телефону. Злоумышленник может представить-

ся, например, сотрудником технической поддержки и информировать о возникновении возможных технических неполадок в рабочие время и возможные варианты их устранения. В разговоре злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое программное обеспечение на компьютере жертвы.

Дорожное яблоко – адаптация троянского коня, которая состоит в использовании физических носителей (CD, флэш-накопителей). Атакующий обычно подбрасывает такой носитель в общедоступных местах на территории организации (парковки, столовые, рабочие места сотрудников, туалеты). На носителе делают вызывающую интерес у сотрудников надпись (например, премия к новому году, заработная плата руководителей или отчет для налоговой инспекции и т. п.). Интерес прочтения такой информации заставляет забыть об осторожности. При запуске диска «яблоко» автоматически активируется и запускает вредоносный код

Обратная социальная инженерия – данный вид атаки направлен на создание такой ситуации, при которой жертва будет вынуждена сама обратиться к злоумышленнику за «помощью». Например, злоумышленник может выслать письмо с телефонами и контактами «службы поддержки» и через некоторое время создать обратимые неполадки в компьютере жертвы. Пользователь в таком случае позвонит или свяжется по электронной почте со злоумышленником, а в процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные.

Защита от социальной инженерии

Основные рекомендации для усиления безопасности компьютерных систем организации:

– привлечение внимания к вопросам безопасности, необходимость осознания серьезности проблемы и причин принятия политики безопасности организации;

– проверка личности и встречные звонки любому, кто просит сообщить персональную или конфиденциальную информацию;

– реализация программы обучения пользователей в области безопасности;

– назначение ответственных за техническую поддержку, обязательность личного знакомства с ответственным за техническую поддержку и обращения за помощью исключительно к нему;

– создание системы оповещения об угрозах (атакующие знают, что, даже если их обнаружат, у служащего нет возможности предупредить других сотрудников об атаках, в результате этого атака может быть продолжена с минимальными изменениями и после компрометации; по существу, компрометация только улучшит атаку, так как атакующие узнают, что именно не срабатывает);

– создание политики безопасности применительно к различным опасным направлениям (например, определив правила корректного использования телефонов, компьютеров и т. д.).

Социальная инженерия является единственным подходящим методом проверки эффективности политики безопасности. Хотя многие тесты проверяют физические и электронные уязвимые места, но лишь некоторые анализы безопасности исследуют бреши, создаваемые людьми.

Тестирование системы защиты – это метод выявления недостатков безопасности с точки зрения постороннего человека (взломщика). Он позволяет протестировать схему действий, которая раскрывает и предотвращает внутренние и внешние попытки проникновения и сообщает о них. Используя этот метод, можно обнаружить даже те недостатки защиты, которые не были учтены в самом начале при разработке политики безопасности. Тест должен разрешить два основных вопроса:

– все ли пункты политики безопасности достигают своих целей и используются так, как это было задумано;

– существует ли что-либо, не отраженное в политике безопасности, что может быть использовано для осуществления целей злоумышленника.

Необходимо свести к минимуму количество людей, знающих о проведении эксперимента. При тестировании могут быть затронуты деликатные вопросы частной жизни сотрудников и безопасности организации, поэтому желательно получить предварительное разрешение на проведение такой акции. (Непосредственное начальство обязательно должно быть в курсе происходящего.)

Профессионалам в области безопасности при проведении теста необходимо иметь такое же положение, как и у потенциального злоумышленника: в их распоряжении должны быть время, терпение и максимальное количество технических средств, которые могут быть использованы взломщиком. Более того, проверяющим следует расценить это как вызов своему профессионализму, а значит, проявить

столько же рвения, сколько и взломщик, иначе тесты могут не достичь необходимого результата.

Таким образом, были рассмотрены основные вопросы информационной безопасности, которыми должен владеть руководитель подразделения, отдела, учреждения и т. п. для постановки задачи защиты информации.

2.4. Ответственность за компьютерные преступления

В УК РФ «компьютерные преступники» разделены на следующие категории:

– лица, осуществляющие неправомерный доступ к компьютерной информации;

– лица, осуществляющие неправомерный доступ к компьютерной информации в группе по предварительному сговору или организованной группой;

– лица, осуществляющие неправомерный доступ к компьютерной информации с использованием своего служебного положения;

– лица, имеющие доступ к ЭВМ, но осуществляющие неправомерный доступ к компьютерной информации или нарушающие правила эксплуатации ЭВМ;

– лица, создающие, использующие и распространяющие вредоносные программы.

Важнейшим и определяющим элементом криминалистической характеристики любого, в том числе и компьютерного, преступления является совокупность данных, характеризующих способ его совершения.

Под способом совершения преступления обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющего различного рода характерные следы, позволяющие помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и соответственно определить наиболее оптимальные методы решения задач раскрытия преступления.

Составы компьютерных преступлений (то есть перечень признаков, характеризующих общественно опасное деяние как конкретное преступление) приведены в главе 28 УК РФ «Преступления в сфере компьютерной информации», которая содержит три статьи: «Непра-

вомерный доступ к компьютерной информации» (ст. 272), «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273) и «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (ст. 274).

Неправомерный доступ к компьютерной информации (ст. 272)

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, –

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо арестом на срок до шести месяцев, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, –

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок до семи лет.

Общественная опасность неправомерного доступа к компьютерной информации состоит в нарушении соответствующего закону и другим нормативным актам порядка эксплуатации компьютерных систем, а также использования и распространения содержащейся в них информации лицами, не являющимися собственниками или законными владельцами этих систем.

Совершение преступления, предусмотренного ст. 272, ставит под угрозу или причиняет ущерб также имущественным и иным законным правам и интересам собственников или владельцев компьютерных систем и компьютерной информации (в том числе их праву на владение информацией).

Предметом данного деяния следует рассматривать компьютерную информацию.

Следы совершения неправомерного доступа делят на две части: вещественные и интеллектуальные.

Вещественные в свою очередь подразделяются:

1) на остающиеся на средствах защиты информации (электронные карточки, электронные ключи доступа к ПК, устройства идентификации пользователя (отпечаток пальца, руки и т п.), устройства опознания по почерку);

2) остающиеся на средствах компьютерной техники (отпечатки пальцев, микрочастицы).

Интеллектуальные следы:

1) указывающие на изменения в файловой структуре (переименование каталогов и файлов, изменение размеров и содержимого файла, изменение стандартных реквизитов файла, появление новых файлов или каталогов);

3) изменение в конфигурации компьютера (изменение картинки и цвета экрана, порядка взаимодействия с периферийным устройством и т. д.);

4) необычные проявления в работе (зависание, замедление при загрузке, появление на экране нестандартных символов и т. п.).

Первая часть статьи 272 предусматривает уголовную ответственность за неправомерный доступ к компьютерной информации (информации на машинном носителе, в ЭВМ или сети ЭВМ), если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы вычислительных систем.

Электронно-вычислительная машина (ЭВМ) – устройство или система, способная выполнять заданную, четко определенную последовательность операций по преобразованию или обработке данных.

Система ЭВМ – это программный комплекс, предназначенный для решения конкретной прикладной задачи или спектра задач на общих данных, алгоритмах, действиях.

Понятия системы ЭВМ и ЭВМ (компьютер) являются в информатике взаимозаменяемыми.

Сеть ЭВМ – это объединенные общими линиями связи ряд программно-совместимых компьютеров. Линии связи – это внешние по отношению к конкретной ЭВМ каналы передачи информации и общения между ЭВМ и внешней средой – отдельными пользователями, технологическими процессами, другими ЭВМ.

В соответствии с российским законодательством любая информация может находиться в собственности физических и юридических лиц, или государства. Ее правовой режим определяется нормами, устанавливающими категорию информации по уровню доступа к ней, а также правом собственности на отдельные документы, массивы документов, базы данных и т. д.

Авторское право распространяется на любые программы для ЭВМ и базы данных – как выпущенные, так и не выпущенные в свет.

Базы данных – это объективная форма представления и организации данных, систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Базы данных могут включать конфиденциальные сведения, составляющие личную, семейную, коммерческую, банковскую тайну, использование которых регулируется соответствующим законодательством.

Объективная сторона рассматриваемого деяния выражается:

– в неправомерном доступе к охраняемой законом компьютерной информации;

– последствиях в виде (альтернативно) уничтожения, блокирования, модификации либо копирования информации; нарушении работы ЭВМ;

– причинной связи между неправомерным доступом и наступившими преступными последствиями.

Неправомерный доступ – это несанкционированное владельцем информации ознакомление с данными, содержащимися на машинных носителях или в ЭВМ лицом, не имеющим соответствующего допуска. Незапланированный просмотр чужой информации совершается в результате проникновения в компьютерную систему, которое может быть пассивным или активным. Как правило, преступное деяние выражается в проникновении в компьютерную систему путем использо-

вания специальных технических или программных средств, позволяющих преодолеть установленные системы защиты; незаконного применения действующих паролей или маскировки под видом законного пользователя.

Пассивное проникновение – подключение к линиям связи или сбор электромагнитных излучений этих линий в любой точке системы лицом, не являющимся пользователем ЭВМ.

Активное проникновение – это непосредственное считывание информации из файлов, хранящихся в ЭВМ.

Важным является наличие причинной связи между несанкционированным доступом и наступлением предусмотренных ст. 272 последствий, поэтому простое временное совпадение момента сбоя в компьютерной системе, которое может быть вызвано неисправностями или программными ошибками не содержит признака и неправомерного доступа не влечет уголовной ответственности.

Неправомерный доступ признается оконченным с момента наступления указанных в диспозиции последствий, то есть (альтернативно) уничтожения, блокирования, копирования информации, либо нарушения работы ЭВМ, системы ЭВМ или их сети.

Уничтожение информации представляет собой удаление ее с физических носителей, а также несанкционированные изменения составляющих ее данных, кардинально меняющие ее содержание (например, введение ложной информации, добавление, изменение, удаление записей).

Модификация информации – это изменение логической и физической организации базы данных, за исключением изменений, обеспечивающих ее функционирование под управлением конкретных программ пользователя.

Копирование – изготовление второго и последующих экземпляров базы данных, файлов в любой материальной форме, а также их запись в память ЭВМ. Как копирование следует рассматривать и распространение информации, то есть предоставление доступа к воспроизведенной в любой материальной форме базе данных (в т. ч. сетевыми способами, а также путем сдачи внаем, продажи, проката, предоставления взаймы носителей информации).

Блокирование представляет собой создание условий (в т. ч. и с помощью специальных программ), исключающих пользование (ознакомление, передачу, внесение изменений и т. д.) компьютерной информацией ее законным владельцем.

Нарушение работы ЭВМ означает повреждение ЭВМ или системы ЭВМ, то есть приведение их в состояние, требующее обязательного восстановления ЭВМ, системы ЭВМ или их сети для дальнейшего использования.

Обязательным признаком анализируемого деяния является причинная связь между неправомерным доступом к компьютерной информации и наступившими вредными последствиями. Если уничтожение, блокирование информации, нарушение работы ЭВМ и т. д. не является результатом несанкционированного проникновения в ЭВМ, а происходит вследствие других причин (например, нарушения правил эксплуатации ЭВМ), содеянное не содержит признаков преступления, предусмотренного ст. 272.

Неправомерный доступ признается оконченным с момента наступления указанных в диспозиции последствий, то есть (альтернативно) уничтожения, блокирования, копирования информации, либо нарушения работы ЭВМ, системы ЭВМ или их сети.

Деяние, предусмотренное ст. 272, может быть совершено только умышленно. Виновный осознает, что неправомерно получает доступ к компьютерной информации, предвидит, что в результате совершенных им действий возможно (либо неизбежно) наступление указанных в норме последствий, и желает этого либо относится к этому безразлично.

Мотивы и цели данного преступления могут быть любыми, что позволяет применять ст. 272 УК РФ к всевозможным компьютерным посягательствам. Это и корыстный мотив, цель получить какую-либо информацию, желание причинить вред, желание проверить свои профессиональные способности.

Субъект – общий, то есть вменяемое лицо, достигшее на момент совершения преступления возраста 16 лет и не наделенное со стороны законного владельца или пользователя правом доступа к ЭВМ и заложенной в ней информации.

Часть вторая ст. 272 – то же деяние, причинившее крупный ущерб[1] или совершенное из корыстной заинтересованности, –

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы

[1] Крупным ущербом в статьях главы 28 УК РФ признается ущерб, сумма которого превышает один миллион рублей.

на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо арестом на срок до шести месяцев, либо лишением свободы на тот же срок.

Часть третья ст. 272 предусматривает в качестве признаков, усиливающих уголовную ответственность, совершение его группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Таким образом, признаки квалифицированного состава рассматриваемого преступления характеризуют либо объективную сторону посягательства, либо субъекта преступления.

Согласно ч. 2 ст. 35 УК РФ преступление признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении преступления. Это может касаться времени, места, способа совершения преступления и т. д. Для признания неправомерного доступа к компьютерной информации, совершенного по предварительному сговору группой лиц, не обязательно, чтобы все соисполнители в полном объеме принимали участие в посягательстве на объект уголовно-правовой охраны. Для признания соисполнителем преступления по ч.2 ст. 272 УК РФ, достаточно совершения любого действия, которое было бы непосредственно направлено на достижение общей преступной цели. Например, один взламывает закрытую компьютерную систему и передает управление другому, который производит поиск и уничтожение (блокирование, копирование, модификацию) информации.

Неправомерный доступ к охраняемой законом компьютерной информации признается совершенным организованной группой, если он совершен устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений.

Определяющим критерием организованной группы является признак устойчивости (стабильность состава, тесная связь между ее членами, согласованность действий, постоянство форм и методов преступных действий), что отличает его от предыдущего квалифицирующего признака.

Организованной группой, как правило, руководит организатор, который осуществляет подбор участников преступления, планирует слаженную деятельность, распределяет роли между ними, устанавливает дисциплину и т. д. Неправомерный доступ к компьютерной информации, совершенной организованной группой, квалифицируется

независимо от того, какую роль сыграл тот или иной участник преступления. Например, одни выполняли роль непосредственных исполнителей, другие – руководителей группы, третьи – создавали условия для совершения преступления.

Привлечь к уголовной ответственности по ч. 3 ст. 272 УК РФ можно вменяемое лицо, достигшее шестнадцатилетнего возраста, которое использовало для реализации преступных целей свое служебное положение. Получение неправомерного доступа к компьютерной информации лицом с использованием своего служебного положения имеет место в случаях, когда виновный использует предоставленные ему законом, договором или трудовым соглашением права и полномочия на совершение четко определенных действий с компьютерной информацией.

Исходя из смысла ст. 272, виновный может совершать действия как в пределах, так и выходящие за пределы его компетенции (например, неправомерно получает доступ к информации ограниченного пользования путем просмотра чужих файлов). К таким лицам относят не только субъектов, занимающих руководящие должности в организации, но и специалистов (операторов, программистов, референтов и т. д.). Таким образом, субъект квалифицированного состава – специальный. Надо сказать, что таких как раз большинство (до 75%).

И, наконец, норма данной статьи предусматривает ответственность лиц, имеющих доступ к ЭВМ, системе ЭВМ или их сети. К таким лицам следует отнести законных пользователей информации (операторов ЭВМ, программистов, абонентов системы коллективного пользования, имеющих развитую сеть терминалов, например, Интернет), а также лиц, по характеру своей деятельности имеющих доступ к ЭВМ, системе ЭВМ или их сети (наладчиков оборудования; иной технический персонал, обслуживающий ЭВМ). В этом случае неправомерный доступ к охраняемой законом компьютерной информации осуществляется посредством превышения таким лицом своей компетенции, специально оговоренной законом, трудовым соглашением или иным нормативным актом.

Мотивы и цели, так же как и в ч.1 ст. 272 УК РФ, могут быть различными, а преступное деяние совершено умышленно.

Однако следует отметить, что ст. 272 не регулирует ситуацию, когда неправомерный доступ осуществляется в результате неосторожных действий, что, в принципе, отсекает огромный пласт возможных посягательств и даже те действия, которые действительно

совершались умышленно, так как при расследовании обстоятельств доступа будет крайне трудно доказать умысел компьютерного преступника.

Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273)

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок до семи лет.

Статья состоит из трех частей.

Первая часть предусматривает уголовную ответственность за создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию ин-

формации, нарушению работы ЭВМ, системы ЭВМ или их сетей, а равно использование либо распространение таких программ или машинных носителей с такими программами.

Программа для ЭВМ – это объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата. Под программами для ЭВМ подразумеваются также подготовленные материалы, полученные в ходе ее разработки и порождаемые ею аудиовизуальные отображения.

Вредоносная программа для ЭВМ – это программное средство, приводящее к несанкционированному уничтожению, блокированию, копированию или модификации программ для ЭВМ или информации, выводящее из строя материальные носители, информационное оборудование или нарушающее систему защиты. Эти программы для ЭВМ способны самопроизвольно присоединяться к другим программам и при запуске таких измененных программ выполнять нежелательные действия.

Наиболее распространенными видами вредоносных программ являются широко известные компьютерные вирусы и логические бомбы.

Создание программ – это целенаправленная разработка программ, приводящих к несанкционированному пользователем уничтожению, блокированию, копированию, модификации информации, нарушению работы ЭВМ, системы ЭВМ или их сети. В информатике такие программы получили название «компьютерных вирусов». Внесение изменений в существующие программы означает внесение изменений вирусного характера, то есть запись «вируса» на программы пользователя с носителей информации и с сетей связи, содержащих компьютерный вирус (вредоносную программу для ЭВМ).

Распространение вредоносных программ (компьютерного вируса) – воспроизведение таких программ в любой материальной форме, передача ее сетевыми способами, а также продажа, прокат, сдача внаем, предоставление взаймы носителей информации, содержащие такие программы.

Использование – применение при эксплуатации ЭВМ физических носителей информации, заведомо для лица содержащих программу, приводящую к нарушению работы ЭВМ, системы ЭВМ и их сети, либо к несанкционированным манипуляциям с информацией.

Объективная сторона преступления, предусмотренного ст. 273, состоит в совершении одного из следующих действий:

– создание вредоносных программ для ЭВМ либо внесение подобных изменений в существующие программы;

– использование или распространение таких программ или машинных носителей с такими программами.

Преступление признается оконченным с момента совершения хотя бы одного из перечисленных в диспозиции действий. При этом не имеет значения, была ли нарушена работа ЭВМ, уничтожена, блокирована, скопирована информация. Достаточно совершения одного из указанных в диспозиции действий. Например, лицо создает вредоносную программу для утверждения своего имиджа, предполагая только демонстрацию ее в кругу студентов группы.

Субъект преступления – общий, то есть любое вменяемое лицо, достигшее 16-летнего возраста.

Создание вредоносных программ для ЭВМ, их использование и распространение совершается только умышленно. Виновный сознает, что создает, использует либо распространяет вредоносные программы для ЭВМ или вносит опасные для информации изменения в существующие программы и желает совершить эти действия.

Мотивы и цели могут быть самые разнообразные: хулиганство, корысть, зависть, неприязнь, а также самые благородные побуждения (например, борьба за экологическую чистоту планеты и т. д.). Они не оказывают влияния на квалификацию преступления, но влияют на назначение наказания.

Следует учитывать, что в ряде случаев использование подобных программ не будет являться уголовно наказуемым. Это относится к деятельности организаций, осуществляющих разработку антивирусных программ и имеющих соответствующую лицензию (например, лаборатория Касперского).

При совершении преступления, предусмотренного рассматриваемой статьей, лицо сознает, что создает вредоносную программу, использует либо распространяет такую программу или ее носители и либо предвидит возможность наступления тяжких последствий, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение, либо не предвидит этих последствий, хотя при необходимой внимательности и предусмотрительности должно и могло их предусмотреть.

Преступление окончено с момента наступления указанных в законе последствий. Обязательным признаком является также причинная связь между созданием, распространением и использованием вредоносных программ и наступившими тяжкими последствиями.

Мотивы и цели могут быть различными, так как не оказывают влияния на квалификацию преступления, но, как и в первой части данной статьи, влияют на степень наказания (например, на одном автомобильном заводе нашей страны был изобличен программист, который из мести к руководству предприятия умышленно внес изменения в программу ЭВМ, управлявшей подачей деталей на конвейер, в результате чего заводу был причинен существенный материальный ущерб – не сошло с конвейера свыше сотни автомобилей).

Если сбой «зараженной» программы повлек за собой гибель людей либо причинение вреда их здоровью, действия виновного должны квалифицироваться по совокупности ст. 273 и соответствующей статьи УК РФ, предусматривающей ответственность за преступление против личности.

Данная норма закономерна, поскольку разработка вредоносных программ доступна только квалифицированным программистам, которые в силу своей профессиональной подготовки должны предвидеть потенциально возможные последствия использования этих программ, которые могут быть весьма многообразными: смерть человека, вред здоровью, возникновение реальной опасности военной или иной катастрофы, нарушение функционирования транспортных систем..

Если же в действиях лица содержатся не только признаки преступления, предусмотренного ст. 273 УК РФ, но и признаки другого преступления (убийства, уничтожения имущества), виновный будет нести ответственность по совокупности совершенных преступлений.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274)

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, –

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на

срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, –

наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

Общественная опасность преступления заключается в нарушении регламентированного нормативными актами (законом, ведомственными положениями, а также правилами, установленными в конкретной организации) порядка пользования компьютерными системами и компьютерной информацией. Во многих случаях этим деянием может быть причинен вред имущественным и иным охраняемым законом правам и интересам граждан, организаций, государства.

Объективная сторона этого преступления заключается:

– в нарушении правил эксплуатации ЭВМ;

– уничтожении, блокировании или модификации охраняемой законом информации, причинивших существенный вред;

– причинной связи между нарушением правил и наступившим вредным результатом.

Норма состоит из двух частей.

Первая часть устанавливает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред.

Данная уголовная норма, естественно, не содержит конкретных технических требований и отсылает к ведомственным инструкциям и правилам, определяющим порядок работы, которые должны устанавливаться специально уполномоченным лицом и доводиться до пользователей.

Правила эксплуатации ЭВМ вырабатываются в каждой организации самостоятельно, иногда на базе предложенных рекомендаций. Однако практически все они включают разделы, посвященные обработке, хранению, обеспечению безопасности системы ЭВМ или их сети и содержат юридические, организационные, аппаратные и программные меры предотвращения неправомерного доступа к аппаратуре и информации.

Нарушение правил может быть совершено как действием, так и бездействием. В последнем случае виновный не выполняет предписанные правилами действия. Правила нарушаются, например, в случае, когда вопреки требованию инструкции не используется система «замков и ключей» (определенным участкам памяти не присваиваются идентификационные номера, а зарегистрированным пользователям - числовые коды: «ключи»), что создает возможность доступа к информации, содержащейся в памяти, любому лицу.

В соответствии с диспозицией ст. 274, уголовная ответственность возможна лишь в том случае, когда нарушение правил повлекло модификацию, блокирование и уничтожение информации, что, в свою очередь, причинило крупный ущерб. Однако при всех условиях между действиями лица, допустившего нарушение, и наступившим результатом должна быть установлена причинная связь.

Так как вред должен быть причинен в результате нарушения правил, ст. 274 не может быть применена в том случае, когда правила были нарушены, но вред произошел не в результате их нарушения, а в силу каких-либо других причин. Например, хотя и была применена «система кодирования», но лицо в процессе несанкционированного пользования системой сумело подобрать код и блокировало информацию в сегменте памяти; лицо не произвело проверку машинных и ручных протоколов выполнения работ со стороны пользователя, однако информация, содержащаяся в запоминающем устройстве, была уничтожена из-за неопытности оператора.

Преступление признается оконченным с момента причинения существенного вреда.

Субъектом анализируемого преступления может быть только лицо, на которое возложено (его функциональными обязанностями) соблюдение правил эксплуатации ЭВМ.

Субъективная сторона преступления, предусмотренного ч. 1 ст. 274, характеризуется умышленной виной. Виновный осознает, что нарушает правила эксплуатации ЭВМ, предвидит возможность уничтожения, блокирования или модификации компьютерной информации с причинением существенного вреда владельцу, желает либо допускает наступление этих последствий или безразлично к ним относится.

Мотивы и цели содеянного не влияют на квалификацию преступления.

Применение данной статьи невозможно для сети Интернет, ее действие распространяется только на локальные сети организаций.

Наиболее строгое наказание за данную норму – ограничение свободы до двух лет.

Ответственность за деяния, повлекшие тяжкие последствия, предусматривается ч. 2 ст. 274. Тяжкие последствия, в смысле этой нормы, включают имущественный ущерб и иные тяжкие последствия. Под имущественным ущербом, причиненным владельцу информации или ЭВМ, понимают как прямой (реальный) имущественный ущерб, так и ущерб в форме упущенной выгоды.

Величина причиненного ущерба во многом зависит от важности информации. По этому признаку можно выделить следующие уровни информации:

– жизненно важная – незаменимая информация, наличие которой обеспечивает функционирование организации;

– важная – информация, которая может быть заменена или восстановлена, но этот процесс связан с большими затратами и серьезными трудностями;

– полезная – информация, которая приносит очевидную пользу и которую трудно восстановить, хотя в принципе организация может вполне нормально функционировать и без нее.

Уничтожение, блокирование либо модификация жизненно важной или важной информации, безусловно, влечет наступление тяжких последствий.

К иным тяжким последствиям могут быть отнесены, например, такие как:

– дезорганизация технологического процесса на предприятии,

– длительная остановка работы организации;

– крупная авария;

– утрата данных, необходимых для проведения научных исследований;

– утрата данных, содержащих сведения о здоровье большой группы людей и собираемых в течение нескольких лет;

– утрата данных об основных параметрах и формулы изобретений (открытий);

– причинение тяжкого вреда здоровью людей.

Субъективная сторона – нарушение правил эксплуатации, повлекшее наступление тяжких последствий, характеризуется неосторожной виной или умышленной.

Субъект либо не предвидел возможности наступления таких последствий своих действий, хотя при необходимой внимательности или предусмотрительности мог и должен был их предвидеть, либо

предвидел возможность наступления тяжких последствий в результате нарушения правил эксплуатации, однако самонадеянно рассчитывал на их предотвращение (например, действия специалиста по обслуживанию системы управления транспортом, установившего инфицированную программу без антивирусной проверки, повлекшее серьезную транспортную аварию).

Подводя некоторые итоги, можно сделать вывод о том, что сложность компьютерной техники, неоднозначность квалификации, а также трудность сбора доказательной информации не приведет в ближайшее время к появлению большого числа уголовных дел, возбужденных по ст. 272 – 274 УК РФ.

Предусмотренные составы компьютерных преступлений не охватывают полностью всех видов совершения посягательств в этой сфере. В ряде случаев могут быть использованы другие статьи УК РФ, предусматривающие наказание за информационные преступления. Так, к разряду преступлений против конституционных прав и свобод человека и гражданина УК РФ относит такие преступления, как:

– нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (ч. 1 ст. 138);

– незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации (ч. 3 ст. 138);

– предоставление гражданину должностным лицом неполной или заведомо ложной информации, если этим причинен вред правам и законным интересам граждан (ст. 140);

– незаконное использование объектов авторского права или смежных прав, присвоение авторства (ч. 1 ст. 146);

– нарушение авторских прав группой лиц (ч. 2 ст. 146);

– незаконное использование изобретения, полезной модели, промышленного образца, разглашение их сущности без согласия автора или заявителя до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству (ст. 147).

К разряду преступлений в сфере экономической деятельности отнесены:

– незаконное использование чужого товарного знака, знака обслуживания, наименования места происхождения товара или сходных с ним обозначений для однородных товаров (ч. 1 ст. 180);

– незаконное использование предупредительной маркировки (ч. 2 ст. 180);

– использование в рекламе заведомо ложной информации относительно товаров, работ или услуг, а также их изготовителей, исполнителей, продавцов (ст. 182);

– собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз, а также иным незаконным способом (ч. 1 ст. 183);

– незаконное разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца (ч. 2 ст. 183);

– незаконный экспорт технологий, научно-технической информации и услуг в сфере вооружения и военной техники (ст. 189).

2.5. Органы, обеспечивающие информационную безопасность

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

Государственные органы РФ, контролирующие деятельность в области защиты информации:

– Совет Безопасности России;

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

– Федеральная служба безопасности (ФСБ России);

– Министерство внутренних дел (МВД России);

– Федеральная служба охраны (ФСО России);

– Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия (Россвязьохранкультуры);

– Межведомственная комиссия по защите государственной тайны.

Службы, организующие защиту информации на уровне предприятия:

– служба экономической безопасности;

– служба безопасности персонала (режимный отдел);

– отдел кадров;

– служба информационной безопасности.

Рассмотрим более подробно статус основных служб, контролирующих деятельность в области защиты информации.

Совет Безопасности Российской Федерации

Совет Безопасности Российской Федерации является конституционным совещательным органом, осуществляющим подготовку решений Президента Российской Федерации по вопросам обеспечения безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации (далее – национальная безопасность), организации обороны, военного строительства, оборонного производства, военного и военно-технического сотрудничества Российской Федерации с иностранными государствами, по иным вопросам, связанным с защитой конституционного строя, суверенитета, независимости и территориальной целостности Российской Федерации, а также по вопросам международного сотрудничества в области обеспечения безопасности.

Правовую основу деятельности Совета Безопасности составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности», другие федеральные законы, указы и распоряжения Президента Российской Федерации.

Совет Безопасности формируется и возглавляется Президентом Российской Федерации.

Положение о Совете Безопасности Российской Федерации утверждается Президентом Российской Федерации.

В целях реализации задач и функций Совета Безопасности Президентом Российской Федерации могут создаваться рабочие органы Совета Безопасности и аппарат Совета Безопасности.

Основными задачами Совета Безопасности являются:

1) обеспечение условий для осуществления Президентом Российской Федерации полномочий в области обеспечения безопасности;

2) формирование государственной политики в области обеспечения безопасности и контроль за ее реализацией;

3) прогнозирование, выявление, анализ и оценка угроз безопасности, оценка военной опасности и военной угрозы, выработка мер по их нейтрализации;

4) подготовка предложений Президенту Российской Федерации:

а) о мерах по предупреждению и ликвидации чрезвычайных ситуаций и преодолению их последствий;

б) о применении специальных экономических мер в целях обеспечения безопасности;

в) о введении, продлении и об отмене чрезвычайного положения;

5) координация деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по реализации принятых Президентом Российской Федерации решений в области обеспечения безопасности;

6) оценка эффективности деятельности федеральных органов исполнительной власти в области обеспечения безопасности.

Основными функциями Совета Безопасности являются:

1) рассмотрение вопросов обеспечения безопасности, организации обороны, военного строительства, оборонного производства, военно-технического сотрудничества Российской Федерации с иностранными государствами, иных вопросов, связанных с защитой конституционного строя, суверенитета, независимости и территориальной целостности Российской Федерации, а также вопросов международного сотрудничества в области обеспечения безопасности;

2) анализ информации о реализации основных направлений государственной политики в области обеспечения безопасности, о социально-политической и об экономической ситуации в стране, о соблюдении прав и свобод человека и гражданина;

3) разработка и уточнение стратегии национальной безопасности Российской Федерации, иных концептуальных и доктринальных документов, а также критериев и показателей обеспечения национальной безопасности;

4) осуществление стратегического планирования в области обеспечения безопасности;

5) рассмотрение проектов законодательных и иных нормативных правовых актов Российской Федерации по вопросам, отнесенным к ведению Совета Безопасности;

6) подготовка проектов нормативных правовых актов Президента Российской Федерации по вопросам обеспечения безопасности и осуществления контроля деятельности федеральных органов исполнительной власти в области обеспечения безопасности;

7) организация работы по подготовке федеральных программ в области обеспечения безопасности и осуществление контроля за их реализацией;

8) организация научных исследований по вопросам, отнесенным к ведению Совета Безопасности.

Федеральная служба по техническому и экспортному контролю

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) создана в соответствии с указом Президента РФ от 09 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти» вместо существовавшей ранее Государственной технической комиссии при Президенте Российской Федерации и является головным органом по защите информации.

ФСТЭК России является федеральным органом исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1) обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;

2) противодействия иностранным техническим разведкам на территории Российской Федерации;

3) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

4) осуществления экспортного контроля.

Деятельность ФСТЭК России обеспечивают Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России (головная научная организация по проблемам защиты информации), а также другие подведомственные ФСТЭК России организации. ФСТЭК России осуществляет свою деятельность во взаимодействии с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления и организациями.

Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации. ФСТЭК России подведомственна Минобороны России.

Основные полномочия ФСТЭК России:

– разрабатывает стратегию и определяет приоритетные направления деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации;

– разрабатывает и вносит в установленном порядке Президенту РФ и в Правительство РФ проекты законодательных и иных нормативных правовых актов по вопросам своей деятельности;

– издает нормативные правовые акты по вопросам своей деятельности;

– разрабатывает и утверждает в пределах своей компетенции методические документы, организует их издание за счет средств, выделяемых из федерального бюджета ФСТЭК России на эти цели;

– организует и финансирует работы по изучению излучений различной физической природы, возникающих при использовании неинформационных излучающих комплексов, систем и устройств;

– осуществляет межотраслевую координацию деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления и организациях;

– осуществляет в пределах своей компетенции контроль за состоянием работ по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации;

– осуществляет в пределах своей компетенции межведомственный контроль за обеспечением защиты государственной тайны, контроль за соблюдением лицензионных требований и условий, а также рассмотрение дел об административных правонарушениях;

– вносит в установленном порядке представления о применении мер ответственности за нарушения законодательства Российской Федерации по вопросам своей деятельности;

– выдает предписания на приостановление работ на объектах федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления и организаций в случае выявления в ходе осуществления контроля нарушений норм и требований, касающихся противодействия техническим разведкам и технической защиты информации;

– организует радиоконтроль за соблюдением установленного порядка передачи служебной информации должностными лицами организаций, выполняющих работы, связанные со сведениями, составляющими государственную и (или) служебную тайну, при использовании открытых каналов радиолиний, радиорелейных, тропосферных, спутниковых и других линий и сетей радиосвязи, доступных для радиоразведки, подготавливает предложения, направленные на предотвращение утечки информации по указанным каналам;

– организует и проводит лицензирование деятельности по осуществлению мероприятий и (или) оказанию услуг в области защиты государственной тайны (в части, касающейся противодействия техническим разведкам и (или) технической защиты информации), по созданию средств защиты информации, содержащей сведения, составляющие государственную тайну, по технической защите конфиденциальной информации, по разработке и (или) производству средств защиты конфиденциальной информации, а также лицензирование иных видов деятельности в соответствии с законодательством Российской Федерации;

– организует в соответствии с законодательством Российской Федерации проведение работ по оценке соответствия (включая работы по сертификации) средств противодействия техническим разведкам, технической защиты информации, обеспечения безопасности информационных технологий, применяемых для формирования государственных информационных ресурсов, а также объектов информатизации и ключевых систем информационной инфраструктуры;

– участвует совместно с ФСБ России в проведении специальных экспертиз по допуску организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, а также принимает участие в проведении государственной аттестации руководителей организаций, ответственных за защиту указанных сведений;

– организует разработку программ стандартизации, технических регламентов и национальных стандартов в области обеспечения безопасности информации в ключевых системах информационной ин-

фраструктуры, обеспечения безопасности применяемых информационных технологий, а также в области противодействия техническим разведкам и технической защиты информации;

– организует и проводит в установленном порядке государственную экспертизу внешнеэкономических сделок в отношении товаров (работ, услуг), информации, результатов интеллектуальной деятельности, которые могут быть использованы при создании оружия массового поражения, средств его доставки, иных видов вооружения и военной техники;

– организует в соответствии с законодательством Российской Федерации государственную аккредитацию организаций, создавших внутрифирменные программы экспортного контроля, и выдает им свидетельства о государственной аккредитации;

– осуществляет в пределах своей компетенции нетарифное регулирование внешнеторговой деятельности, в том числе выдает лицензии на осуществление операций по экспорту и (или) импорту товаров (работ, услуг), информации, результатов интеллектуальной деятельности в случаях, предусмотренных законодательством Российской Федерации;

– осуществляет иные функции в установленной сфере деятельности в соответствии с федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации.

В Российской Федерации коммерческая деятельность, связанная с использованием *криптографических средств*, подлежит обязательному лицензированию. С 22 января 2008 года действует постановление Правительства РФ от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами», которым приняты Положения о лицензировании деятельности:

– по распространению шифровальных (криптографических) средств;

– техническому обслуживанию шифровальных (криптографических) средств;

– предоставлению услуг в области шифрования информации;

– разработке, производству шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

В настоящее время действует также приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производ-

стве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение пкз-2005)», который определяет порядок разработки и эксплуатации криптографических средств. В частности, согласно приказу, средства криптографии реализуются «юридическим лицом или индивидуальным предпринимателем, имеющим право на осуществление данного вида деятельности, связанного с шифровальными (криптографическими) средствами … вместе с правилами пользования ими, согласованными с ФСБ России».

Федеральная служба безопасности Российской Федерации

Обеспечение информационной безопасности − деятельность органов ФСБ России, осуществляемая ими в пределах своих полномочий:

– при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;

– при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в России и ее учреждениях, находящихся за пределами России.

Федеральная служба охраны

Основными задачами органов государственной охраны являются:

1) прогнозирование и выявление угрозы безопасности объектов государственной охраны, осуществление комплекса мер по предотвращению этой угрозы;

2) обеспечение безопасности объектов государственной охраны;

3) обеспечение в пределах своих полномочий организации и функционирования связи для нужд органов государственной власти;

4) участие в пределах своих полномочий в борьбе с терроризмом;

5) обеспечение защиты охраняемых объектов;

6) выявление, предупреждение и пресечение преступлений и иных правонарушений на охраняемых объектах и на трассах проезда (передвижения) объектов государственной охраны;

7) обеспечение организации и функционирования федеральных информационных систем, находящихся во владении или в пользовании органов государственной охраны;

8) участие в пределах своих полномочий в обеспечении информационной безопасности Российской Федерации.

Межведомственная комиссия по защите государственной тайны

Межведомственная комиссия по защите государственной тайны:

– осуществляет следующие основные полномочия в области информационной безопасности:

– координирует деятельность органов государственной власти, органов местного самоуправления и организаций по вопросам реализации федерального законодательства в области государственной тайны;

– рассматривает и представляет в установленном порядке Президенту Российской Федерации и в Правительство Российской Федерации предложения по правовому регулированию вопросов защиты государственной тайны и совершенствованию системы защиты государственной тайны в Российской Федерации, а также предложения по организации разработки и выполнения государственных программ, нормативных правовых актов и методических документов, обеспечивающих реализацию федерального законодательства о государственной тайне;

– формирует перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне;

– формирует перечень сведений, отнесенных к государственной тайне;

– формирует в установленном порядке перечень особорежимных объектов Российской Федерации и представляет его в Правительство Российской Федерации;

– определяет порядок рассекречивания носителей сведений, составляющих государственную тайну, в случае ликвидации организации-фондообразователя и отсутствия ее правопреемника;

– рассматривает вопросы о возможности передачи сведений, составляющих государственную тайну, другим государствам и международным организациям и представляет в установленном порядке в Правительство Российской Федерации соответствующие экспертные заключения;

– организует разработку и представляет в установленном порядке в Правительство Российской Федерации предложения о порядке определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого организациям и гражданам в связи с засекречиванием информации, находящейся в их собственности;

– организует разработку и представляет в установленном порядке в Правительство Российской Федерации предложения по правилам отнесения сведений, составляющих государственную тайну, к различным степеням секретности;

– рассматривает по поручениям Президента Российской Федерации и Правительства Российской Федерации проекты международных договоров Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну, организует разработку соответствующих предложений и экспертных заключений, участвует в международном сотрудничестве по этим вопросам;

– координирует в установленном порядке работы по техническому регулированию в отношении продукции (работ, услуг), сведения о которых составляют государственную тайну, а также работы по организации сертификации средств защиты информации;

– координирует в установленном порядке проведение работ по лицензированию деятельности организаций, связанной с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны;

– координирует деятельность в области подготовки, переподготовки и (или) повышения квалификации специалистов по вопросам защиты государственной тайны;

– осуществляет разработку методических рекомендаций по организации и проведению государственной аттестации руководителей организаций, ответственных за защиту сведений, составляющих государственную тайну, определяет перечень учебных заведений, свидетельство об окончании которых дает право на освобождение указанных руководителей от государственной аттестации;

– осуществляет иные полномочия в соответствии с федеральным законодательством о государственной тайне.

Бюро специальных технических мероприятий МВД России (Управление «К» МВД)

В ведение данного ведомства входят:

1. Борьба с преступлениями в сфере компьютерной информации:

– выявление и пресечение фактов неправомерного доступа к компьютерной информации;

– борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ;

– противодействие мошенническим действиям с использованием возможностей электронных платежных систем;

– борьба с распространением порнографических материалов с участием несовершеннолетних через сеть Интернет.

2. Пресечение противоправных действий в информационно-телекоммуникационных сетях, включая сеть Интернет:

– выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи;

– противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет;

– противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.

3. Борьба с незаконным оборотом радиоэлектронных и специальных технических средств.

4. Выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий.

5. Борьба с международными преступлениями в сфере информационных технологий:

– противодействие преступлениям в сфере информационных технологий, носящим международный характер;

– взаимодействие с национальными контактными пунктами зарубежных государств.

6. Международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий.

Обязательность и порядок сертификации технических и программных средств для обработки защищаемой информации

Основным нормативным правовым актом в области подтверждения соответствия вообще и сертификации в частности является федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

Посредством сертификации подтверждается соответствие продукции, процессов производства, эксплуатации, работ, услуг или иных объектов установленным требованиям (техническим регламентам, стандартам). Осуществляет процедуру сертификации независимая от изготовителя (продавца, исполнителя) и потребителя (покупателя) организация − орган по сертификации.

Органы сертификации, осуществляющие обязательную сертификацию, должны быть аккредитованы в порядке, устанавливаемом Правительством РФ. Документом, подтверждающим соответствие продукции установленным требованиям, является сертификат соответствия, выдаваемый на срок, установленный соответствующим техническим регламентом.

К средствам защиты информации отнесены технические, криптографические, программные и другие средства, а также средства, в которых они реализованы, и средства контроля эффективности защиты информации. Криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных ФСБ России.

Органы государственного контроля могут приостанавливать или отменять действие сертификата в случае, если его требования не соответствуют реальной ситуации.

В случае выявления лицензирующими органами неоднократных или грубых нарушений лицензионных требований и условий, лицензирующие органы вправе приостанавливать действие лицензии. Лицензирующий орган обязан установить срок устранения лицензиатом нарушений, повлекших за собой приостановление действия лицензии. Указанный срок не может превышать шести месяцев. В случае если в установленный срок лицензиат не устранил указанные нарушения, лицензирующий орган обязан обратиться в суд с заявлением об аннулировании лицензии.

Кодекс Российской Федерации об административных правонарушениях содержит ряд соответствующих статей, устанавливающих ответственность за нарушения в области сертификации и лицензирования:

– ст. 13.6 – за использование несертифицированных средств связи либо предоставление несертифицированных услуг связи, если законом предусмотрена их обязательная сертификация;

– ст. 13.11 − за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);

– ст. 13.12 — за нарушение правил защиты информации, а именно: нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации; использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, подлежащих обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну); нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, и осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну;

– ст. 13.13 − за незаконную деятельность в области защиты информации, проявившуюся в виде: занятия видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке обязательной лицензии; занятия видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, представляющей государственную тайну, и осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии;

– ст. 19.19 – за нарушение обязательных требований государственных стандартов, правил обязательной сертификации, нарушение требований нормативных документов по обеспечению единства измерений.

Вопросы для самоконтроля

1. Что понимается под правовым режимом информации?
2. Каковы основные нормативно-правовые акты и федеральные законы РФ в сфере обеспечения информационной безопасности?
3. Что, согласно действующему законодательству РФ, понимается под общедоступной информацией и информацией ограниченного доступа?
4. Каковы основные виды информации ограниченного доступа?
5. Каковы основные характеристики правового режима коммерческой тайны?
6. Каковы основные характеристики правового режима государственной тайны?

7. Что понимается под утечкой информации ограниченного доступа? Каковы основные технические каналы утечки информации?

8. Каковы основные виды компьютерных преступлений?

9. Какие деяния отнесены к преступлениям в сфере компьютерной информации согласно УК РФ?

10. Какие государственные органы РФ осуществляют контроль деятельности в сфере защиты информации? Каковы их основные функции и полномочия?

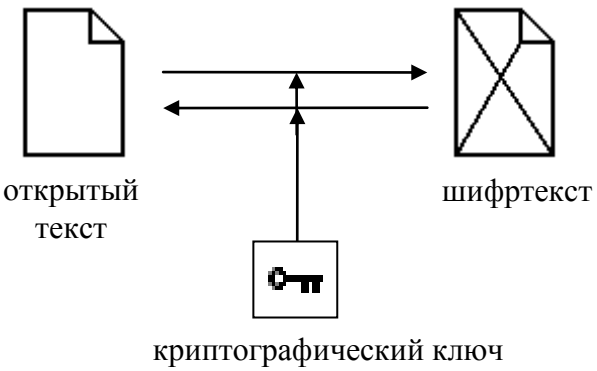
Глава 3. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Основные понятия классической криптографии

Криптография (от др.-греч. *криптос* − скрытый и *графи* − пишу) – это наука о методах и алгоритмах шифрования. Основной целью криптографии является обеспечение конфиденциальности информации при ее хранении и передаче путем шифрования содержания сообщений. Однако криптографические методы и средства также широко используются для обеспечения других качеств защищенной информации: целостности (неизменности), аутентичности (подлинности автора, отправителя сообщения) и неотрекаемости (невозможности отказа от авторства).

Криптографические алгоритмы охватывают шифрование, выработку имитовставки (криптографической контрольной суммы, кода аутентификации), хэширования (выработку контрольной суммы), цифровой подписи, а также различные вспомогательные алгоритмы, например, алгоритмы выработки ключевой информации.

В традиционном понимании *криптографическое преобразование информации* – взаимно-однозначное математическое преобразование, зависящее от секретного параметра – *ключа*, ставящее в соответствие открытой информации, представленной в некоторой цифровой кодировке, зашифрованную информацию (шифртекст), также в цифровой кодировке.



Криптографическое преобразование

Шифрованием называется зависящее от ключа преобразование открытого текста в кажущуюся случайной последовательность символов, называемую *криптограммой* или *шифртекстом*, с целью сделать непонятным его смысл для посторонних. Расшифрованием

называется извлечение открытого текста из криптограммы при условии знания секретного ключа.

Классическим *шифром* или *криптографической системой* (криптосистемой) называется семейство взаимно-однозначных отображений множества возможных сообщений X во множество криптограмм Y, проиндексированное элементами k из множества ключей:

$$\{F_k : X \to Y, k \in K\}.$$

Считается, что на стороне отправителя (А) имеются два источника информации – источник сообщений и источник ключей. Выбранный для шифрования ключ k передается отправителю (А) и получателю (В) по *защищенному* (закрытому) каналу, то есть перехватить его невозможно. Предполагается, что канал передачи ключей абсолютно надежен и недоступен для других.

В то же время основной канал обмена является *открытым*, это значит, что противник (Е) может перехватывать передаваемые зашифрованные сообщения. При этом предполагается, что противнику известно о криптосистеме все, кроме использованного для шифрования секретного ключа k. Противник может знать шифрующий алгоритм, вероятности выбора различных ключей и открытых текстов, но не знает, какой именно ключ был выбран на этот раз. Таким образом, секретность шифра обеспечивается только секретностью ключа.

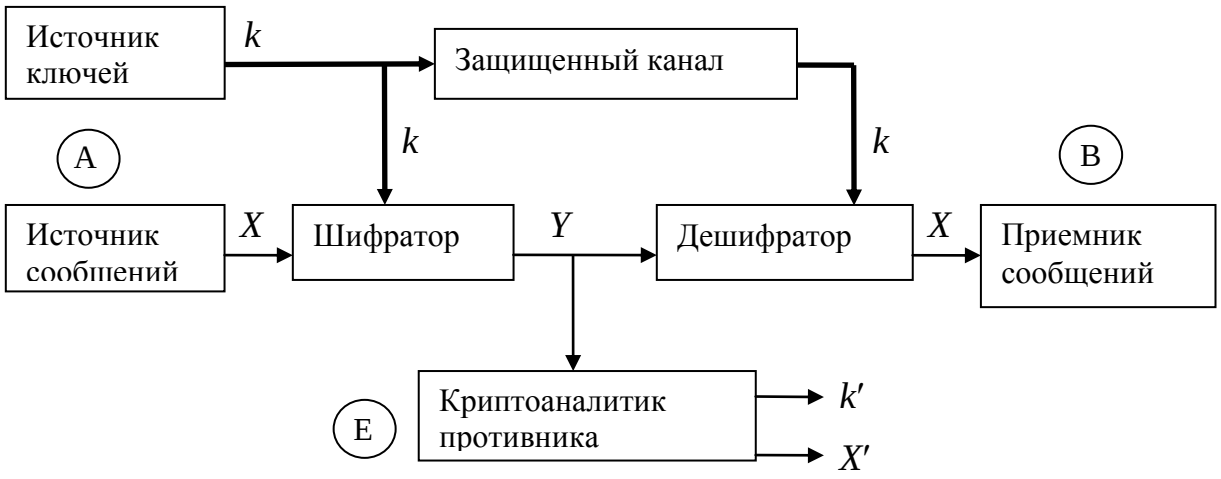


Схема традиционной криптосистемы

Целью противника является определение содержания скрывающегося за шифртекстом сообщения или нахождение использованного ключа, с помощью которого можно расшифровать криптограмму. Попытка определения открытого текста или нахождения ключа шиф-

рования называется *криптоаналитической атакой*. Успешная криптоаналитическая атака называется взломом, или *вскрытием шифра.*

Степень гарантий того, что криптосистема не будет взломана, называется ее *стойкостью*. Показано существование абсолютно стойких шифров, невозможность вскрытия которых может быть теоретически доказана. Однако на практике использование таких криптосистем оказывается затруднительным. Стойкость подавляющего большинства практически применимых шифров базируется на вычислительной сложности методов криптоанализа, то есть теоретически они могут быть взломаны, но на практике это оказывается слишком сложной задачей. Успех вскрытия вычислительно стойких шифров зависит от наличия у криптоаналитика определенного объема перехваченных сообщений, доступных временных и вычислительных ресурсов.

Кроме *пассивных атак*, связанных с прослушиванием канала связи, перехватом и последующим криптоанализом передаваемых зашифрованных сообщений, существуют и *активные атаки*, предполагающие активное вмешательство противника с процесс обмена зашифрованными сообщениями: подмена криптограмм, блокирование их передачи, повторная передача или навязывание ложных сообщений, подмена отправителя сообщения или его переадресация другому абоненту. Для противодействия активным угрозам используют *методы имитозащиты* (добавление к сообщениям имитовставки, кодов аутентификации, регистрационных номеров, отметок времени) и *цифровую подпись* сообщений.

Традиционные шифры используют и для шифрования, и для расшифровывания один и тот же секретный ключ и называются *симметричными*.

В зависимости от числа и типа используемых секретных параметров (ключей) криптографические алгоритмы делятся на бесключевые, одноключевые и двухключевые. Кроме того, существуют специальные криптографические протоколы (схемы разделения секрета), которые позволяют использовать более двух ключей, то есть являются многоключевыми.

К *одноключевым* относятся симметричные криптосистемы. Подавляющее большинство современных симметричных криптосистем являются блочными композиционными шифрами, то есть объединяют разнотипные преобразования информации в рамках одного раунда, шифрование производится в несколько раундов. К шифрам такого типа относятся алгоритмы «Магма» и «Кузнечик» отечественного

криптографического стандарта ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации. Блочные шифры», американский стандарт AES (Advanced Encryption Standard, FIPS 197) и TDEA (SP 800-67), алгоритмы международного стандарта ISO/IEC 18033-3:2010: TDEA, MISTY1, CAST-128, HIGHT, AES, Camellia, SEED.

Симметричные блочные шифры допускают различные режимы работы, позволяющие использовать их, в том числе и как потоковые шифры, и в качестве имитовставки (кода аутентификации). В России принят стандарт ГОСТ Р 34.13–2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров», определяющий шесть режимов работы, применимых для произвольных симметричных блочных шифров, в том числе и описанных в стандарте ГОСТ Р 34.12–2015.

Основными достоинствами симметричных криптосистем является высокая эффективность и стойкость, однако существуют проблемы, связанные с необходимостью надежной передачи секретных ключей между абонентами до начала шифрования.

Эта проблема решена в *асимметричных* криптосистемах, использующих пару ключей: свой личный ключ (privat key) каждый из абонентов держит в секрете, а второй ключ пары – открытый (public key) может публиковаться открыто. Асимметричные криптосистемы называют также криптосистемами *с открытым ключом*, они являются *двухключевыми*. Наиболее известным асимметричным шифром являются шифр RSA (IEEE P1363, PKCS 1), стандартизированный в международной организации ISO (ISO/IEC 18033-2:2006). В России стандарт шифрования с открытым ключом не принят.

К асимметричным криптосистемам относятся также система распределения ключей Диффи-Хеллмана (NIST SP 800-56A, IEEE P1363, X9.42) и системы цифровой подписи DSA, ECDSA (американские стандарты FIPS 186, NIST SP 800-56B, X9.62, международный стандарт ISO/IEC 14888 в трех частях). Российский стандарт цифровой подписи ГОСТ Р 34.10–2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» реализует алгоритм, подобный ECDSA.

Наряду с асимметричными криптосистемами технология цифровой подписи использует *бесключевые* хэш-функции. В США приняты алгоритмы хэш-функций SHA-2 (FIPS 180) и SHA-3 (FIPS 202, SP 800-185). Международный стандарт ISO/IEC 10118-3 наряду с алго-

ритмами SHA-2 определяет хэш-функции RIPEMD и WHIRLPOOL. Отечественный алгоритм цифровой подписи используется совместно с хэш-функциями, описанными стандартом ГОСТ Р 34.11–2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

Для лучшего понимания строения современных криптосистем рассмотрим сначала примеры простых классических шифров.

3.2. Традиционные симметричные криптосистемы

Шифрование используется для защиты конфиденциальной информации с глубокой древности, история криптографии насчитывает не менее четырех тысяч лет, что подтверждается историческими документами таких древних цивилизаций, как Месопотамия, Египет, Индия, Китай и др. Несмотря на долгую историю, математическое обоснование классической криптографии было дано лишь в середине XX века Клодом Шенноном в его работе «Теория связи в секретных системах». Он показал, что все исторические шифры сводятся к двум основным преобразованиям: *замене* (подстановке) и *перестановке* символов шифруемого текста.

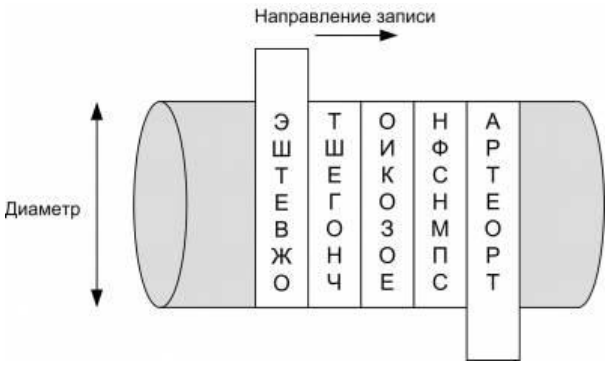
Шифры замены выполняют замену символов текста на другие символы по какому-то определенному правилу. Символы исходного текста могут заменяться, например, на символы другого языка, пиктограммы (как в рассказе А. Конан Дойла «Пляшущие человечки»), числа или на другие символы того же самого языка. Шифры перестановки изменяют порядок следования символов в тексте, переставляя с одних позиций на другие, но не заменяя их.

По размеру преобразуемой информации шифры делятся на *блочные* и *потоковые*. Блочные шифры осуществляют преобразование информации блоками фиксированной длины, составленными из подряд идущих символов сообщения. В блочных шифрах результат шифрования фактически зависит от всех исходных символов блока. Поскольку перестановка символов всегда производится в пределах некоторого фрагмента текста, все перестановочные шифры являются блочными.

В потоковых алгоритмах каждый символ открытого текста зашифровывается (и расшифровывается) независимо от других. Большинство классических шифров замены преобразуют символы сообщения по очереди, один за другим, и являются потоковыми.

Рассмотрим некоторые примеры исторических шифров замены и перестановки.

Сцитала – одно из первых шифровальных приспособлений, шифр использовался в Спарте в V–IV веках до н. э. Сцитала представляла собой жезл цилиндрической формы, на который наматывалась лента пергамента. Кроме жезла могли использоваться рукоятки мечей, кинжалов копий и пр. Изготавливались две копии устройства, одна оставалась у отправителя сообщений, другая передавалась получателю. Лента была столь узкой, что поперек нее мог быть записан только один символ. Вдоль оси цилиндра на пергамент, намотанный на сциталу, построчно записывался текст, предназначенный для передачи. После записи текста лента сматывалась с жезла, теперь символы на ней были написаны вразнобой и текст невозможно было прочитать, не намотав предварительно пергамент на точно такую же сциталу. Очевидно, что сцитала осуществляла перестановку букв сообщения, а ключом шифра был диаметр сциталы.



Принцип использования сциталы

Интересно, что метод вскрытия этого шифра принадлежит Аристотелю. Аристотель предлагал заточить на конус длинный брус и, обернув вокруг него ленту, начать сдвигать ее по конусу от большего диаметра до самого малого. В том месте, где диаметр конуса совпадал с диаметром, сциталы, буквы текста сочетались в слоги и слова. После этого оставалось лишь изготовить цилиндр нужного диаметра.

По сути, шифр сциталы был простейшим вариантом шифрующих (перестановочных) таблиц.

Шифрующие таблицы являются одним из самых примитивных шифров перестановки, для которой ключом служит размер таблицы. Сообщение вписывается в таблицу определенного размера в одном направлении (например, по строкам), а считывается в другом (например, по столбцам).

Запишем фразу «система защиты информации» в таблицу размером 5×5 по строкам, последние две клетки таблицы заполним произвольным символом, например, буквой «ж». Выписав текст из таблицы по столбцам, получим «смифциатоисзыритаимжещнаж».

	→ Направление записи				
↓ Направление чтения	с	и	с	т	е
	м	а	з	а	щ
	и	т	ы	и	н
	ф	о	р	м	а
	ц	и	и	ж	ж

Пример шифрующей таблицы

Отправитель и получатель сообщения должны заранее условиться о ключе (размере таблицы). На практике обычно размер таблицы задается заранее. Пусть таблица содержит n столбцов и m строк. Тогда в нее может вместиться не более $n \times m$ символов. Если длина сообщения $L > n \times m$, то исходный текст делится на несколько блоков, каждый из которых шифруется одинаковым образом.

Этот шифр может быть несколько усилен, например, столбцы могут быть переставлены в некоторой последовательности, определяемой ключом. Возможна двойная перестановка – столбцов и строк.

Шифр Цезаря. Одним из наиболее известных шифров древнего Рима (I век до н. э.) был шифр Цезаря. Шифр Цезаря является вариантом шифра *простой замены*. В этом шифре каждая буква открытого текста заменяется третьей после нее буквой в алфавите, то есть «A» заменяется на «D», «B» – на «E», «C» – на «F» и т. д. При этом считается, что алфавит шифрования циклически сдвинут относительно исходного на 3 позиции, то есть написан по кругу, и после буквы «Z», последней буквы латинского алфавита, следует буква «A».

порядковый № символа	0	1	2	3	4	…	23	24	25
нормативный алфавит	**A**	**B**	**C**	**D**	**E**		**X**	**Y**	**Z**
	↓	↓	↓	↓	↓	…	↓	↓	↓
алфавит шифрования	**D**	**E**	**F**	**G**	**H**		**A**	**B**	**C**
порядковый № символа	3	4	5	6	7		0	1	2

Шифрующая система Цезаря

Например, результат применения шифра Цезаря к слову RIM имеет вид ULP. При расшифровании надо сделать обратную замену символов (то есть «D» заменить на «A», «E» – на «B» и т. д.).

Цезарь использовал сдвиг равный 3, но можно использовать и какое-либо другое значение сдвига (S), главное, чтобы получатель зашифрованного сообщения, знал величину сдвига. Используемое значение сдвига является ключом криптосистемы Цезаря. Число возможных ключей здесь равно числу букв алфавита (N) минус единица, например, всего 25 для латинского и 32 для русского алфавита. Поскольку число вариантов ключа невелико, стойкость такого шифра невысока.

С математической точки зрения шифр Цезаря описывается операциями сложения и вычитания по модулю с величиной фиксированного сдвига S исходного алфавита, символы алфавита нумеруются числами от 0 до N–1, где N – число различных символов алфавита:

$y_i = (x_i + S) \bmod N$ – для шифрования

$x_i = (y_i - S) \bmod N$ – для расшифрования,

где: $\{x_n\}$ – последовательность символов исходного текста в числовой кодировке, $0 \le x_i \le N-1$, $\{y_n\}$ – последовательность символов криптограммы в числовой кодировке, $0 \le y_i \le N-1$, $i = 0,\ldots, n$.

Кроме шифрующей системы Цезаря существуют и другие варианты шифров *простой замены*. Самым легким способом описать такой шифр – задать соответствие между символами (алфавитом) исходного текста и символами шифртекста (шифралфавитом) с помощью таблицы. Основная особенность шифров *простой замены* заключается в том, что это соответствие не изменяется на протяжении всего процесса шифрования.

Шифр простой (табличной) замены. Ключ этого шифра – таблица соответствия между исходным алфавитом и алфавитом шифрования.

нормативный алфавит	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	…
алфавит шифрования	Л	Я	С	П	И	Р	Х	Э	О	Б	У	Ь	А	Щ	З	Г	Ю	Ф	Ж	М	Е	К	…

Пример табличной замены

В процессе шифрования буква текста ищется в первой строке и заменяется соответствующей буквой из второй строки. Например, если зашифровать слово «БЕРЕГ» шифром простой замены, приведенным в таблице, то получим «ЯРЮРП». Для расшифрования букву криптограммы надо найти во второй строке таблицы замен и подставить вместо нее соответствующую букву из первой строки.

Если алфавит шифрования в таблице замен представляет собой случайным образом перемешанный исходный алфавит, можно получить достаточно большое число вариантов ключа ($26! = 4 \cdot 10^{26}$ для латинского алфавита и $33! = 8{,}6 \cdot 10^{36}$ – для русского), полный перебор вариантов ключа в этом случае практически неосуществим.

Однако следует отметить, что шифр простой замены не меняет статистических характеристик шифруемого текста. Например, в открытом тексте «БЕРЕГ» имеются повторяющиеся буквы «Е», а в соответствующей криптограмме – повторяющиеся буквы «Р», стоящие в тех же позициях. Эта особенность позволяет легко вскрывать длинные тексты, зашифрованные шифром простой замены, не прибегая к перебору вариантов ключа.

Вскрытие шифра простой замены осуществляется с помощью частотного анализа. Поскольку символы в текстах на естественном языке встречаются с разной вероятностью, а частоты появления отдельных символов совпадают в исходном сообщении и в криптограмме шифра простой замены, можно сопоставить частоты конкретных символов шифртекста с частотами символов языка сообщения. Частотные таблицы языка рассчитываются по корпусу текстов естественного языка (объемному набору текстов, представительному для языка в целом) и приводятся в справочной литературе, например, в орфографических словарях.

Символ	*Относительная частота*	*Символ*	*Относительная частота*	*Символ*	*Относительная частота*	*Символ*	*Относительная частота*
А	0,080	И	0,074	Р	0,047	Ш	0,007
Б	0,016	Й	0,012	С	0,055	Щ	0,004
В	0,045	К	0,035	Т	0,063	ъ	0,000
Г	0,017	Л	0,043	У	0,026	Ы	0,019
Д	0,030	М	0,032	Ф	0,003	Ь	0,017
Е, Ё	0,085	Н	0,067	Х	0,010	Э	0,003
Ж	0,009	О	0,110	Ц	0,005	Ю	0,006
З	0,016	П	0,028	Ч	0,015	Я	0,020

Частоты встречаемости символов русского языка

Следует, однако, иметь в виду, что частоты появления символов в конкретном тексте могут существенно отличаться от табличных, причем обычно отличия проявляются сильнее для коротких сообщений. Например, в фразе «Четыре черненьких чернявеньких чертенка чертили черными чернилами чертеж» буква «Ч» встречается почти в 10 раз чаще (0,123), чем в среднем по языку (0,015), а такая популяр-

ная буква, как «О» (самая часто встречающаяся в естественном языке) вообще отсутствует, всего же в этом тексте встречается лишь половина (16) букв русского алфавита. Поэтому частотный анализ длинных сообщений обычно легче, чем коротких.

К. Шеннон показал, что существует определенная граничная длина шифртекста, ниже которой невозможно однозначное дешифрование текста. Эту длину он назвал *расстоянием единственности шифра*. Теоретическая оценка расстояния единственности шифра простой замены для текстов на английском языке составляет 27 символов.

Частотный анализ шифра простой замены начинается с подсчета частот появления символов в криптограмме. Затем полученное распределение частот сравнивается с распределением частот в естественном языке и наиболее часто встречающиеся символы криптограммы заменяются наиболее часто используемыми символами языка. После каждой замены текст анализируется, и, если не выявлено никаких противоречий, предположения о соответствии символов считаются верными. Криптоанализ существенно облегчается, если учитываются характерные особенности текста на естественном языке – вероятные слова и сочетания букв. Например, для русского языка может помочь поиск:

– сдвоенных букв: «НН», «СС» (в середине слов, перед окончанием); «ИИ», «ЕЕ», «ММ» (как в середине слов, так и окончание), «ОО» (только в середине слов), «ВВ» (в начале или в середине слов);

– коротких (однобуквенных, двухбуквенных) слов – такие слова, как правило, являются служебными (местоимения, союзы, предлоги) и часто встречаются в текстах;

– слов с дефисом;

– слов-палиндромов (слова, читающиеся одинаково как слева направо, так и справа налево);

– вероятных окончаний (например, для прилагательных «ИЙ», «ОЙ», «АЯ», «ОГО», «ИМИ» и др.) и сочетаний букв (например, сочетание двух подряд идущих согласных менее вероятно, чем чередование согласной и гласной буквы).

Частотный анализ может быть применен к простым перестановочным шифрам. В этом случае принимаются во внимание закономерности сочетаний букв и чередования гласных и согласных.

Как правило, частотный анализ простых шифров не представляет особого труда для носителя языка и может быть осуществлен «вручную». Поэтому естественным развитием криптографии стало

изобретение шифров сложной замены, устойчивых к частотному анализу.

Если в шифре простой замены соответствие между символами естественного языка и символами криптограммы не меняется на всем протяжении шифрования сообщения, то в шифре *сложной замены* к каждому символу сообщения может быть применена своя замена. Фактически в шифрах сложной (многоалфавитной) замены в процессе шифрования постоянно осуществляется переход от одного алфавита замены к другому, то есть применяются различные простые шифры замены. Поэтому одной и той же букве открытого текста в криптограмме могут соответствовать разные символы, более того, один и тот же символ криптограммы может обозначать разные буквы. Примером сложной замены служит шифр Виженера.

Шифр Виженера. Шифр был описан французом Блезом Виженером в «Трактате о шифрах», вышедшем в 1585 году. Для шифрования используется «таблица Виженера» – квадратная таблица с числом элементов $N \times N$, где N – число различных символов алфавита. В заголовке таблицы записывают буквы в порядке их очередности в исходном алфавите, в первой строке – ту же последовательность букв, но с циклическим сдвигом влево на одну позицию, во второй – со сдвигом на две позиции и т. д. Фактически, каждая строка таблицы Виженера представляет шифр Цезаря со сдвигом, равным номеру строки.

Для шифрования текста выбирают ключ, представляющий собой некоторое слово, если оно короче шифруемого текста, то его циклически повторяют, пока не будет зашифровано все сообщение. Далее из таблицы Виженера получают матрицу шифрования, включающую первую строку и строки матрицы, начальными буквами которых являются буквы ключа. Так, если выбрать ключ «сталь», то матрица шифрования примет показанный ниже вид. В процессе шифрования под каждой буквой шифруемого текста записывают буквы ключа. Затем шифруемый текст по матрице шифрования заменяют буквами, расположенными на пересечениях линий, соединяющих буквы текста первой строки таблицы и буквы ключа, находящейся под ней.

*	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
С	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
Т	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
А	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
Л	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
Ь	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ

Матрица шифрования для ключа «сталь»

Исходный текст	З	А	Щ	И	Т	А		И	Н	Ф	О	Р	М	А	Ц	И	И
Ключ	С	Т	А	Л	Ь	С		Т	А	Л	Ь	С	Т	А	Л	Ь	С
Шифр	Ш	Т	Щ	У	М	С		Ь	Н	Я	И	Б	Ю	А	Б	В	Ш

Процесс шифрования с ключом «сталь»

Расшифрование криптограммы, зашифрованной шифром Виженера, выполняется следующим образом: под буквами зашифрованного текста последовательно записывают буквы ключа, повторяя ключ требуемое число раз, затем в строке матрицы шифрования для каждой буквы ключа отыскивается буква, соответствующая знаку шифрованного текста. Заголовок столбца с найденной буквой и будет знаком расшифрованного текста.

Таким образом, к каждому символу открытого текста фактически применяется свой шифр Цезаря, величина циклического сдвига в котором определяется символом ключевой последовательности. Это позволяет записать шифрующее преобразование Виженера с помощью математических формул, приведенных для шифра Цезаря, с той лишь разницей, что величина сдвига будет переменной.

Шифр Виженера описывается следующими операциями (символы алфавита закодированы числами от 0 до N–1):

$y_i = (x_i + k_i) \bmod N$ – для шифрования,

$x_i = (y_i - k_i) \bmod N$ – для расшифрования,

где $\{x_n\}$ – последовательность символов исходного текста, $\{y_n\}$ – последовательность символов крипторамы, а $\{k_n\}$ – ключевая последовательность, $0 \le x_i, k_i, y_i \le N-1$, $i = 0, \ldots, n$, n – длина шифруемого текста.

Шифр Виженера, как и другие многоалфавитные замены, достаточно хорошо маскирует естественные частоты появления символов в тексте, и, как следствие, значительно труднее поддается «ручному» криптоанализу. Однако при неслучайных ключах и ключах, длина

которых короче сообщения, к нему также применим статистический анализ.

Одноразовый шифровальный блокнот. Шифр гаммирования. В конце первой мировой войны американским инженером Гилбертом Вернамом был предложен шифр, фактически являющийся вариантом шифра Виженера с рядом ограничений на использование ключа шифрования:

– ключ является случайной равномерно распределенной последовательностью символов, то есть появление каждого из символов алфавита в ключе случайно и равновероятно;

– длина ключа не короче длины шифруемого сообщения;

– ключ используется однократно (каждое сообщение шифруется своим ключом).

Этот шифр получил название «одноразовый шифровальный блокнот». Можно показать, что этот шифр является принципиально невзламываемым, то есть теоретически стойким. Однако применение шифра на практике оказалось не слишком удобным, что вызвано прежде всего необходимостью генерации и надежной передачи большого объема ключевой информации.

Вариант шифра Вернама, использующий двоичный алфавит, состоящий из символов 0 и 1 и операцию сложения / вычитания по модулю 2, получил название *шифра гаммирования*. Шифруемый текст и ключ представляются в двоичном виде, а криптограмма представляет собой наложение ключа (гаммы) на открытый текст с помощью логической функции исключающего ИЛИ. При этом обычно предполагается, что гамма является непредсказуемой (случайной или псевдослучайной равномерно распределенной) последовательностью бит.

Логическая операция исключающего ИЛИ (XOR) эквивалентна по модулю 2 и обычно обозначается значком $\oplus$.

Двоичный разряд исходного текста	0	0	1	1
Двоичный разряд ключа	0	1	0	1
Двоичный разряд шифртекста	0	1	1	0

Основной особенностью этой операции является то, что она обратна сама себе, то есть сложение и вычитание по модулю 2 эквивалентны, поэтому $y \oplus x \oplus x = y$, а значит для расшифрования шифртекста необходимо наложить на него ту же самую гамма-последовательность.

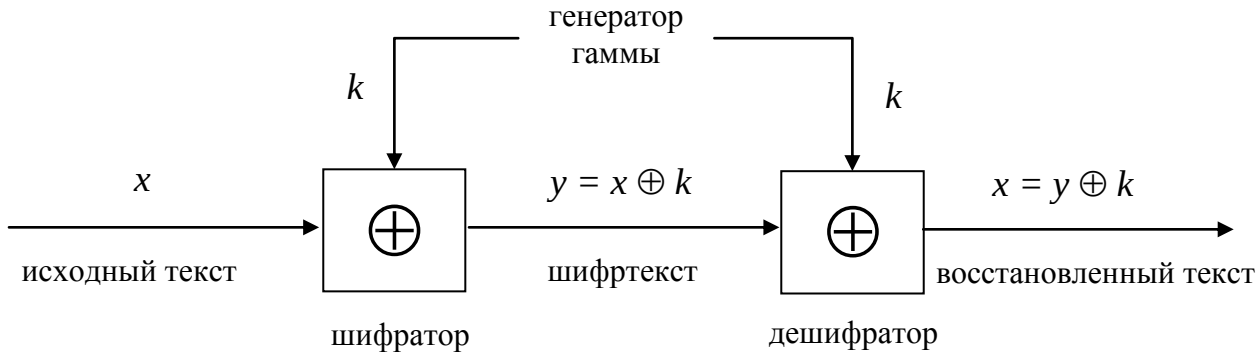


Схема шифра гаммирования

В настоящее время гаммирование применяется как одна из операций раунда симметричных блочных шифров для наложения раундового ключа. Кроме того, современные симметричные потоковые шифры также являются шифром гаммирования и различаются лишь способом выработки гаммы. При этом обычно гамма не передается между абонентами, а вырабатывается каждой из сторон самостоятельно на основе некоторой инициализационной информации, синхронизирующей генераторы гаммы отправителя и получателя зашифрованного сообщения.

Потоковые шифры высокоэффективны, однако их стойкость во многом определяется качеством метода выработки гаммы. Поэтому наряду с гаммированием в настоящее время широко применяются блочные шифры, по сути, являющиеся композицией элементарных шифрующих преобразований.

3.3. Современные симметричные криптосистемы

Стремление использовать короткие ключи, конфиденциальность которых легче обеспечить при хранении и передаче, а также требование обеспечения вычислительной стойкости криптосистемы, привели к созданию современных симметричных блочных шифров. Такие шифры преобразуют исходную информацию блоками одинаковой длины (64, 128, 256 бит и т. д.) с использованием одного и того же ключа. К. Шеннон сформулировал общие принципы, которые определили основной путь синтеза блочных шифров. В алгоритме вычислительно стойкого блочного шифра необходимо использовать операции подстановки (замены) и перестановки символов в блоках, причем делать это многократно и с разными ключами.

Такие шифры являются *композиционными*, поскольку заключаются в многократном последовательном выполнении разнотипных элементарных криптографических преобразований.

Операции подстановки (замены) обычно представляют собой нелинейные преобразования битовых блоков в блоки такой же длины, задаваемые фиксированной таблицей – *таблицей замен*, *S-блоком*. Нелинейность замен позволяет сделать как можно более сложной зависимость между ключом и шифртекстом, что затрудняет применение статистического анализа. Как правило, таблицы замен применяются не целиком к входному блоку, а к его подблокам гораздо меньшей длины.

Для устранения зависимости между символами разных подблоков, которая может присутствовать в исходном сообщении, используются преобразования перестановок. Перестановка – преобразование, которое показывает, на какую позицию в выходном блоке должен попасть стоящий на определенной позиции символ входной последовательности. Перестановки могут задаваться в виде таблицы (P-блок), содержащей номера бит входного текста, сводится к операции циклического сдвига битов блока, использовать линейные регистры сдвига с обратной связью и т. п.

Для наложения материала раундового ключа обычно используется гаммирование (побитовое сложение с битами ключа операцией исключающего ИЛИ), однако может использоваться и другие приемы, например сложение по модулю 2^n, где n – длина раундового ключа.

Многократно повторяющийся набор элементарных криптографических операций называется *раундом шифрования*, а используемый для каждого набора ключ k_i – *раундовым ключом*, $i = 1, \ldots, r$. При этом выходные данные раунда считаются входными для следующего. Чем больше раундов шифрования, тем выше вычислительная стойкость криптосистемы, но ниже скорость работы (эффективность) композиционного шифра.

Основное ограничение при построении композиционного шифра заключается в запрете на использование подряд идущих однотипных операций как в рамках одного раунда, так и на границах раундов, так как любое количество подряд выполняющихся однотипных операций можно заменить одной эквивалентной. Если на границе соседних раундов оказались два однотипных преобразования, между ними вставляют другое простое преобразование (буфер), разрушающее эту однотипность.

Обычно все раундовые ключи получаются из исходного ключа k с помощью алгоритма выработки раундовых ключей (при этом размер исходного ключа k существенно меньше суммарного размера всех раундовых ключей). Процедура генерации раундовых ключей из исходного часто называется *процедурой расширения ключа*. Порядок генерации и использования раундовых ключей называется *расписанием использования ключа шифрования*. Как правило, при расшифровании используются те же самые раундовые ключи, но в обратном порядке.

На практике чаще всего используется два вида структур блочных шифров: шифры на основе схемы Фейстеля и подстановочно-перестановочные шифры.

Блочные шифры на основе сети Фейстеля являются наиболее изученными. Основным достоинством схемы Фейстеля является то, что даже если функция раундового преобразования $f(\cdot)$ необратима, преобразование сети Фейстеля обратимо. Следовательно, для расшифрования в схеме Фейстеля можно использовать ту же функцию $f(\cdot)$, но с обратным порядком следования раундовых ключей.

Схема Фейстеля основана на следующих принципах:

– каждый входной блок делится на две равные части – левую L_i и правую R_i, где i – номер раунда;

– способ формирования половин выходного блока раунда выполняется следующим образом:

$L_i = R_{i-1}$,

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$.

Обе половины блока постоянно меняются местами, поэтому, несмотря на кажущуюся несимметричность, обе половины блока шифруются с одинаковой стойкостью.

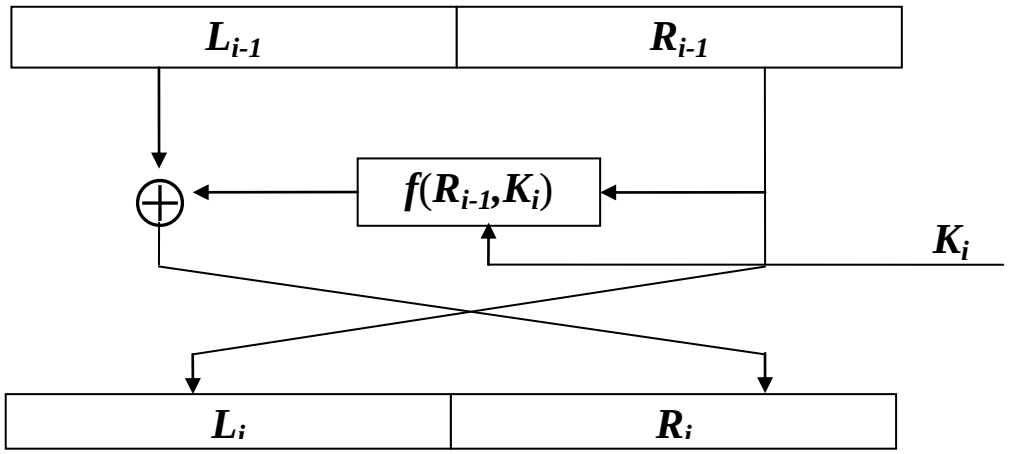


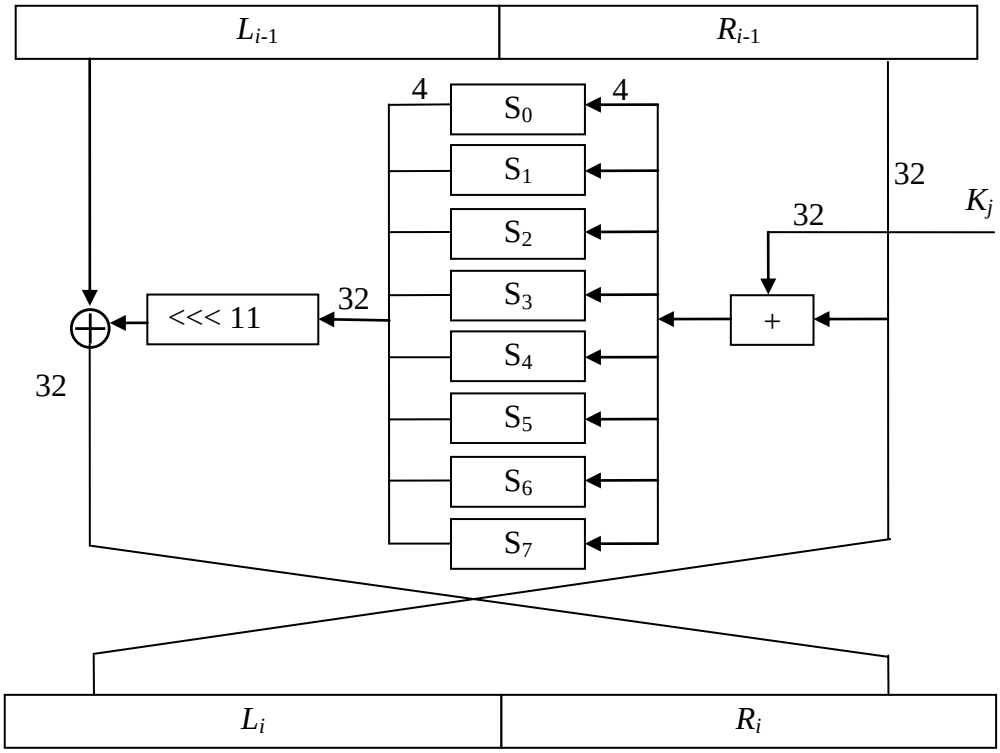
Схема Фейстеля

Существует достаточно много вариантов блочных шифров на основе схемы Фейстеля, различающихся видом нелинейной функции $f(\cdot)$,

числом раундов, размерами блока шифрования и способом выработки раундовых ключей из исходного ключа. В частности, на схеме Фейстеля построены алгоритм старого американского стандарта шифрования DES, шифра «Магма» отечественного стандарта ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры», шифры RC5, Blowfish, TEA, CAST-128 и др.

Шифр «Магма» является действующим российским стандартом симметричного шифрования, фактически это еще советский шифр ГОСТ 28147-89, но с фиксированными таблицами замен. Алгоритм ГОСТ 28147-89 обладает достаточной стойкостью (на сегодняшний день лучшая из предложенных атак требует выполнения порядка 2^{192} тестовых операций шифрования и практически неосуществима) и показывает хорошую скорость работы для ряда платформ, в частности допускает эффективные реализации для низкоресурсной криптографии. Поэтому шифр был включен в действующий российский криптографический стандарт ГОСТ Р 34.12-2015.

Алгоритм построен на сети Фейстеля, имеет размер блока 64 бит, 256-битный раундовый ключ и выполняет 32 раунда шифрования. Структура раунда алгоритма достаточно проста, что обеспечивает неплохие скоростные характеристики шифра даже при достаточно большом числе раундов.



Структура раунда алгоритма «Магма»

В каждом раунде алгоритма выполняются следующие преобразования:

1. *Наложение раундового ключа*. Содержание подблока R_i складывается по модулю 2^{32} с 32-битовым раундовым ключом раунда K_j.

Раундовые ключи получаются из исходного 256-битового ключа шифрования простым делением на восемь частей: K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7. В процессе шифрования подключи K_j используются в соответствии со следующим расписанием:

– с 1 по 24 раунд – в прямой последовательности: K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, ...

– с 25 по 32 раунд – в обратной последовательности: K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0.

2. *Нелинейная замена*. После наложения ключа 32-битовый блок разбивается на 8 частей по 4 бита, значение каждой из которых по отдельности заменяется в соответствии с одной из 8 таблиц замен (S-блоком). Каждый S-блок алгоритма ГОСТ представляет собой вектор (одномерный массив) с 16 элементами, пронумерованными числами от 0 до 15.

S_0 = (12, 4, 6, 2, 10, 5, 11, 9, 14, 8, 13, 7, 0, 3, 15, 1);
S_1 = (6, 8, 2, 3, 9, 10, 5, 12, 1, 14, 4, 7, 11, 13, 0, 15);
S_2 = (11, 3, 5, 8, 2, 15, 10, 13, 14, 1, 7, 4, 12, 9, 6, 0);
S_3 = (12, 8, 2, 1, 13, 4, 15, 6, 7, 0, 10, 5, 3, 14, 9, 11);
S_4 = (7, 15, 5, 10, 8, 1, 6, 13, 0, 9, 3, 14, 11, 4, 2, 12);
S_5 = (5, 13, 15, 6, 9, 2, 12, 10, 11, 7, 8, 1, 4, 3, 14, 0);
S_6 = (8, 14, 2, 5, 6, 9, 1, 12, 15, 4, 11, 0, 13, 10, 3, 7);
S_7 = (1, 7, 14, 13, 0, 5, 8, 3, 4, 15, 10, 6, 9, 12, 11, 2).

Из таблицы S-блока извлекается элемент, порядковый номер которого совпадает с входным значением подстановки. Значениями S-блока также являются 4-битовые значения (целые числа от 0 до 15).

3. *Циклический сдвиг* битов обрабатываемого подблока влево на 11 битов.

Расшифрование осуществляется по этой же схеме, но с другим расписанием использования ключей:

– с 1 по 8 раунд – в прямой последовательности: K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7.

– с 9 по 32 раунд – в обратном порядке: K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0, …

Подстановочно-перестановочные шифры (SP-сети) преобразуют входной блок целиком, за счет чего на каждом шаге обеспечивается гораздо более быстрое перемешивание входных данных по сравне-

нию со схемой Фейстеля, поэтому современные криптосистемы на SP-сетях обеспечивают необходимую вычислительную стойкость за меньшее, по сравнению со схемой Фейстеля, число раундов. С другой стороны, для SP-сети функция расшифрования отличается от функции шифрования, то есть структуры раунда шифрования и раунда расшифрования будут различны.

На SP-сетях основаны шифры SAFER+, Serpent, действующий американский стандарт симметричного шифрования AES, а также шифр «Кузнечик» российского стандарта ГОСТ Р 34.12–2015.

Шифр «Кузнечик» имеет размер входного блока 128 бит, 256-битовый ключ и выполняет 10 раундов шифрования. Каждый раунд состоит из трех слоев: наложения ключа с помощью побитовой операции исключающего ИЛИ, нелинейной подстановки (S-блоков замен) и линейного перемешивания. В последнем, десятом раунде выполняется только наложение ключа.

Первой выполняется операция наложения ключа раунда с помощью побитового XOR: $X[k](a) = k \oplus a$, где k – раундовый ключ, a – входной блок раунда.

Затем входной 128-битовый блок a алгоритма шифрования представляется в виде последовательности 16 байтов, которые нумеруются справа налево, начиная с 0: $a = a_{15} \| a_{14} \| \ldots \| a_1 \| a_0$, где значком || обозначена операция конкатенации строк.

К каждому байту применяется нелинейная подстановка, задаваемая 256-значным массивом S, приведенным в стандарте. Элементы массива пронумерованы от 0 до 255 и имеют уникальные значения также в диапазоне от 0 до 255. Например, если входной байт $a_i = 0$ значение a_i будет заменено на нулевой элемент массива $S(0) = 252$, при $a_i = 1$ – на $S(1) = 238$ и т. д. Для входного блока в целом нелинейная подстановка может быть определена как

$$S(a) = S(a_{15} \| \ldots \| a_0) = S(a_{15}) \| \ldots \| S(a_0).$$

Линейное перемешивание L шифра «Кузнечик» использует операции над полем Галуа $GF(2^8)$ и может быть описано с помощью линейного регистра сдвига R:

1. Байты a_i представляются в виде полиномов поля Галуа $GF(2^8)$. Для простоты обозначим их также a_i.

2. Вычисляется $\ell(a_{15}, \ldots, a_0) = 148 \cdot a_{15} + 32 \cdot a_{14} + 133 \cdot a_{13} + 16 \cdot a_{12} + 194 \cdot a_{11} + 192 \cdot a_{10} + 1 \cdot a_9 + 251 \cdot a_8 + 1 \cdot a_7 + 192 \cdot a_6 + 194 \cdot a_5 + 16 \cdot a_4 + 133 \cdot a_3 + 32 \cdot a_2 + 148 \cdot a_1 + 1 \cdot a_0$,

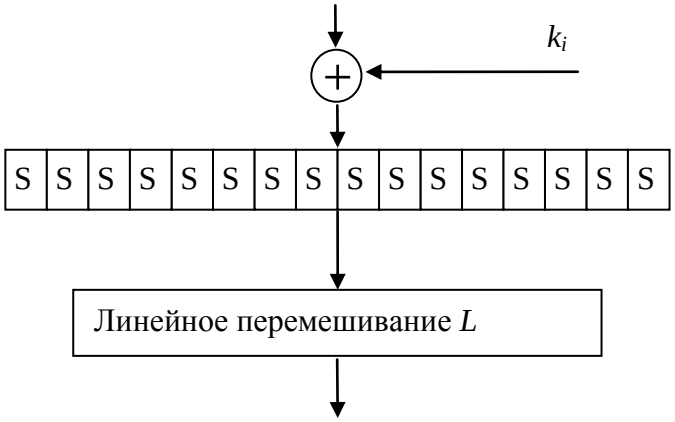
где + и • – операции сложения и умножения над полем Галуа $GF(2^8)$ с неприводимым многочленом $m(x) = x^8 + x^7 + x^6 + x + 1$. Для

выполнения вычислений числовые коэффициенты $a_i \in GF(2^8)$ могут быть представлены восьмиразрядными двоичными числами, которым соответствуют полиномы 7 степени над $GF(2^8)$. Результат операции – полином 7 степени, который может быть переведен обратно в 8 двоичных разрядов (байт).

3. Полученный на предыдущем шаге результат записывается первым в строку байтов, затем записываются все байты входной строки a, кроме младшего (последнего). Таким образом, фактически производится сдвиг строки байтов a вправо на 1 байт: $R(a) = R(a_{15} \| \ldots \| a_0) = \ell(a_{15}, \ldots, a_0) \| a_{15} \| \ldots \| a_1$,

4. Шаги 1–3 повторяются 16 раз, при этом входом каждого следующего шага является выход предыдущего: $L(a) = R^{16}(a)$.

В результате на выходе строка не содержит ни одного не преобразованного байта исходной строки.



Структура раунда шифрования алгоритма «Кузнечик»

Таким образом, шифрование 128-битного входного блока a описывается формулой $E(a) = X[K_{10}]LSX[K_9] \ \ldots \ LSX[K_2]LSX[K_1](a)$, где K_i – раундовые ключи, а $LSX[k]$ – последовательное применение операций побитового XOR с ключом k, нелинейной замены S и линейного перемешивания L.

Процедура расшифрования алгоритма «Кузнечик» может быть записана как

$$D(a) = X[K_1]S^{-1}L^{-1}X[K_2]\ldots S^{-1}L^{-1}X[K_9]S^{-1}L^{-1}X[K_{10}](a).$$

Порядок обратных операций не совпадает с порядком операций при шифровании, раундовые ключи используются в порядке, обратном шифрованию.

Операция S^{-1} – нелинейная подстановка с таблицей замен, обратной таблице замен S.

Операция L^{-1} задается как $L^{-1}(a) = (R^{-1})^{16}(a)$. В свою очередь, $R^{-1}(a) = R^{-1}(a_{15}|| \ldots ||a_0) = a_{14} \,||\, a_{13} \,||\, \ldots \,||\, a_0 \,||\, \ell(a_{14}, a_{13}, \ldots, a_0, a_{15})$.

Раундовые ключи алгоритма «Кузнечик» имеют длину 128 бит. Первые два раундовых ключа (K_1 и K_2) получаются разбиением исходного ключа K на две части.

Далее для выработки каждой пары раундовых ключей используется 8-раундовый алгоритм со структурой Фейстеля, в котором функция раундового преобразования f определяется как последовательность преобразований LSX, а в качестве раундовых ключей используются итерационные константы C_i, полученные как последовательность счетчиков, прошедшая линейное преобразование L:

$C_i = L(i)$, $i = 1, 2, \ldots, 32$, где значение i представлено в виде 128-битовой строки;

$(K_{2i+1}, K_{2i+2}) = F[C_{8(i-1)+8}] \ldots F[C_{8(i-1)+1}](K_{2i-1}, K_{2i})$, $i = 1, 2, 3, 4$,

где $F[k](A_1, A_0) = (LSX[k](A_1) \oplus A_0, A_1)$, k, A_1, A_0 являются 128-битовыми строками.

Режимы работы блочных шифров выведены в отдельный стандарт ГОСТ Р 34.13–2015, что соответствует принятой международной практике. Эти режимы применимы как к шифру «Магма», так и к шифру «Кузнечик». Всего стандарт ГОСТ Р 34.13–2015 определяет 6 режимов работы алгоритмов блочного шифрования с произвольной длиной входного блока: режим простой замены (Electronic Codebook, ECB), режим гаммирования (Counter, CTR), режим гаммирования с обратной связью по выходу (Output Feedback, OFB), режим простой замены с зацеплением (Cipher Block Chaining, CBC), режим гаммирования с обратной связью по шифртексту (Cipher Feedback, CFB), режим выработки имитовставки (Message Authentication Code algorithm, MAC).

Во всех режимах, кроме простой замены и выработки имитовставки, используется синхропосылка, обеспечение конфиденциальности которой не требуется. Значения синхропосылки для режима простой замены с зацеплением и режима гаммирования с обратной связью по шифртексту должны быть непредсказуемыми (случайными или псевдослучайными), они должны выбираться равновероятно и независимо друг от друга.

В режимах простой замены и простой замены с зацеплением длина шифруемого текста должна быть кратна длине блока n базового алгоритма блочного шифрования, поэтому, при необходимости, к последнему блоку исходного сообщения должна быть предварительно применена процедура дополнения.

В режиме простой замены ECB каждый блок шифруется и расшифровывается независимо от других, с использованием одного и того же ключа. Это наиболее простой, и в то же время наиболее уязвимый вариант работы шифра, так шифрование одинаковых блоков даст одинаковый результат. Поэтому данный режим обычно рекомендуется для коротких текстов, длина которых не превышает размера блока, например, для шифрования ключевой информации.

Режим простой замены с зацеплением (CBC) оказывается существенно более стойким, поскольку обеспечивает получение разных блоков шифра даже для одинаковых блоков открытого текста. Его использование рекомендовано для поблочная передачи данных общего назначения и аутентификации.

В режиме простой замены с зацеплением (CBC) и в режимах гаммирования используется инициируемый значением синхропосылки двоичный регистр сдвига *R*, который позволяет варьировать входные данные для базового алгоритма шифрования. Результаты шифрования содержимого *R* накладываются затем на открытый текст операцией побитового исключающего ИЛИ. При этом в режиме простой замены с зацеплением шифрование происходит блоками полной длины, а в режимах гаммирования – порциями произвольной длины s (от 1 бита до полного размера блока).

В режимах гаммирования (CTR), гаммирования с обратной связью по выходу (OFB) и гаммирования с обратной связью по шифртексту (CFB) дополнения последнего блока не требуется. Фактически в этих режимах осуществляется наложение на открытый текст гаммы шифра, которая вырабатывается блоками длины s. Разница заключается только в процедуре формирования гаммы. При расшифровании необходимо выработать ту же самую гамму и наложить ее на шифртекст, поэтому базовый алгоритм здесь используется в режиме шифрования. Эти режимы используются для потоковой передачи данных, причем режимы CTR и OFB, как не размножающие ошибок типа замена символа, могут быть рекомендованы для потоковой передачи данных по каналам с помехами (например, по спутниковой связи).

Процедура выработки имитовставки (кода аутентификации MAC) похожа на шифрование в режиме простой замены с зацеплением, она позволяет получить значение произвольной длины (до полного размера блока), зависящее от всего открытого текста, которое используют для контроля целостности передаваемого сообщения.

3.4. Асимметричные криптосистемы

Несмотря на достижения в области симметричной криптографии, к середине 1970-х годов стала остро осознаваться проблема неприменимости данных методов для решения целого ряда задач. Попытка решить проблемы симметричной криптографии, такие как взаимное доверие сторон при использовании общего секретного ключа и необходимость предварительного распределения ключей между сторонами информационного обмена, привела к созданию принципиально новых криптографических систем с открытым ключом. Эти системы базируются на формализме однонаправленных функций с секретом и характеризуются тем, что для шифрования и для расшифрования используются разные ключи, связанные между собой некоторой зависимостью. Любое сообщение, зашифрованное с использованием одного из этих ключей, может быть расшифровано только с использованием парного ему ключа. Один из ключей (например, ключ шифрования) может быть сделан общедоступным – *открытым* (public key), поэтому проблема передачи общего секретного ключа для связи отпадает.

Асимметричные криптосистемы решают задачу распределения ключей, однако имеют низкую производительность, что затрудняет их использование для шифрования сообщений в режиме реального времени. Поэтому шифрование с открытыми ключами в чистом виде обычно не применяется, а используются смешанные (гибридные) схемы, сочетающие достоинства криптосистем обоих типов. Для каждого сеанса связи аутентификация сторон и защищенная передача секретного ключа производится с помощью асимметричных криптосистем, а для шифрования сообщений применяются симметричные шифры, в конце сеанса связи секретный ключ уничтожается.

Криптосистема RSA. Примером асимметричной криптосистемы является шифр RSA, который также можно использовать для подписания сообщений. Шифр предложен в 1977 году Роном Ривестом (Ron Rivest), Ади Шамиром (Adi Shamir) и Леонардом Адлеманом (Leonard Adleman) и назван по именам своих создателей.

Каждый абонент вырабатывает свою пару ключей (личный и открытый ключ). Для этого он случайным образом генерирует два больших простых числа p и q, и вычисляет произведение $N = p \cdot q$. Затем абонент вырабатывает случайное число e, взаимно простое со значением функции Эйлера φ(N): φ(N) = $(p - 1) \cdot (q - 1)$, и находит число d из условия $e * d = 1 \pmod{\varphi(N)}$, то есть d является числом, обратным e по модулю φ(N): $d = e^{-1} \bmod \varphi(N)$. Пара ($N$, e) объявляется

открытым ключом абонента и публикуется открыто. Значение d является личным ключом абонента и держится в секрете. Числа p, q, $\varphi(N)$ после генерации ключей уничтожаются.

Шифрование производится открытым ключом получателя (N, e), при этом шифруемое сообщение представляется в виде последовательности чисел $M < N$. Криптограмма C получается как $C = M^e \bmod N$. Чтобы расшифровать полученную криптограмму получатель применяет свой личный ключ d: $M = C^d \bmod N$.

Криптосистема RSA может быть использована и для подписания сообщений.

Цифровая подпись. Задачи обеспечения целостности информации, обеспечения аутентификации сообщений и абонентов, обеспечения невозможности отказа сторон от авторства легко решаются в асимметричных криптосистемах с помощью технологии цифровой подписи (ЭЦП). Под электронной (цифровой) подписью понимается цифровой аналог собственноручной подписи абонента. Любая, в том числе и цифровая, подпись должна удовлетворять следующим требованиям:

– подлинность подписи можно проверить;

– подпись нельзя подделать (данную подпись может поставить только ее обладатель и никто другой);

– подпись является неотъемлемой частью документа и не может быть перенесена в другой документ;

– после подписания документ не подлежит никаким изменениям;

– автор подписи не может от нее отказаться.

Цифровая подпись обеспечивает те же свойства, что и обычная подпись автора сообщения, то есть гарантирует аутентичность, неотрекаемость и целостность документа (сообщения). Цифровая подпись является числом, зависящим от подписываемого сообщения и от секрета (личного ключа), известного только подписывающему субъекту. При этом подпись должна легко проверяться без знания секрета.

В криптосистеме RSA для подписания сообщения M $(M < N)$ абонент использует свой личный ключ d: $P = M^d \bmod N$. Проверить же подпись может любой субъект, воспользовавшись открытым ключом отправителя сообщения: $M' = P^d \bmod N$. Если в результате получено $M' = M$, подпись признается истинной, что подтверждает подлинность отправителя и неизменность переданного сообщения. Если же указанное равенство не выполняется, то подпись ложная.

Возможно совместное применение шифрования и подписывания сообщения. Подписывать длинные сообщения не слишком удобно, поэтому личным ключом отправителя обычно заверяется не само сообщение, а некоторое контрольное значение, однозначно характеризующее это сообщение. Для вычисления таких значений используются бесключевые хэш-функции.

Хэш-функцией называется односторонняя функция $y = h(x_1x_2\ldots x_n)$, которая строке символов (сообщению) $x = x_1x_2\ldots x_n$ произвольной длины n ставит в соответствие целое число (битовую строку) фиксированной длины. Результат y вычисления хэш-функции называется *хэш-значением* (*хэш-кодом*). Для любого сообщения может быть легко вычислен его хэш-код, однако по известному хэшу определить, каково было исходное сообщение, невозможно. Кроме того, даже незначительное изменение исходного документа должно приводить к значительному изменению его хэш-кода. Криптографические хэш-функции должны отвечать следующим требованиям:

1) для любого заданного x вычисление $h(x)$ выполняться относительно быстро;

2) для известного y практически невозможно найти x, такое, что $y = h(x)$;

3) для известного сообщения x практически невозможно найти какое-либо другое сообщение x', $x' \neq x$, такое, что $h(x') = h(x)$;

4) практически невозможно найти пару каких-либо различных сообщений x и x', $x' \neq x$, для которых $h(x') = h(x)$.

Российский стандарт функции хэширования ГОСТ Р 34.11–2012 определяет две хэш-функции с выходными значениями длиной 256 и 512 бит. Входное сообщение разделяется на блоки, которые последовательно обрабатываются итерационной конструкцией с помощью функции сжатия. В качестве функции сжатия используется 12-рандовый симметричный блочный шифр на SP-сети. Входом функции сжатия является очередной обрабатываемый блок сообщения, а в качестве ключа алгоритма выступает результат обработки предыдущего блока.

Российский стандарт цифровой подписи ГОСТ Р 34.10–2012 использует криптосистему, отличную от RSA, и фактически реализует вариант цифровой подписи Эль-Гамаля на эллиптических кривых (ECDSA). Стандарт определяет два варианта подписи с 256- или 512-битовой хэш-функцией по стандарту ГОСТ Р 34.11–2012.

Для создания надежной линии передачи сообщений методами асимметричной криптографии между отправителем и получателем

необходимо обеспечить доверенную передачу открытых ключей, поскольку в противном случае возможна реализация классической сетевой атаки «человек посередине». Подменив передаваемые ключи, злоумышленник-посредник может представить себя как отправителем подписанных данных, так и получателем зашифрованных сообщений. Для предотвращения подобных проблем применяются методы цифровой сертификации.

Цифровой сертификат – электронный документ, связывающий открытый ключ асимметричной криптосистемы с определенным пользователем или приложением. Информация сертификата подтверждает истинность открытого ключа и владельца соответствующего личного ключа. Для управления жизненным циклом цифровых сертификатов и обеспечения взаимодействия с пользователями должна быть развернута организационно-техническая структура, получившая название *инфраструктуры открытых ключей* (PKI, Public Key Infrastructure), основу которой составляют доверенные *центры сертификации*.

Нормативно-правовые основы использования криптографических средств защиты информации

Согласно п.1 ст.12 закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» лицензированию подлежат «разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

Согласно указу Президента РФ «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», для защиты государственных информа-

ционных систем требуется использование сертифицированных средств криптографической защиты информации (СКЗИ). Так, п. 2 гласит: «Запретить использование государственными организациями и предприятиями в информационно-телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата Федерального агентства правительственной связи и информации при Президенте Российской Федерации, а также размещение государственных заказов на предприятиях, в организациях, использующих указанные технические и шифровальные средства, не имеющие сертификата Федерального агентства правительственной связи и информации при Президенте Российской Федерации».

Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации[1], требуют использования сертифицированных ФСБ России СКЗИ для защиты персональных данных.

Согласно постановлению Правительства РФ «Об организации лицензирования отдельных видов деятельности», регулирующим органом, осуществляющим лицензирование видов деятельности, связанных с шифровальными (криптографическими) средствами, является ФСБ России. ФСБ России также организует систему сертификации СКЗИ, требования к СКЗИ не являются открыто распространяемыми и требуют соответствующего допуска.

Вопросы для самоконтроля

1. Какова основная цель применения криптографических методов и средств защиты информации?
2. Что понимается под криптографическим ключом, криптографической системой?
3. Какие существуют типы криптосистем по числу используемых ключей?
4. Каково основное различие между блочными и потоковыми шифрами?
5. Каково основное различие между шифрами замены и перестановки?

[1] Утв. руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144

6. Что понимается под гаммированием?

7. Почему современные композиционные шифры являются блочными? Какие преобразования они используют?

8. Каково назначение различных режимов работы блочных шифров?

9. В чем заключается основная особенность асимметричного шифрования?

10. Что такое цифровая подпись? Зачем нужны цифровые сертификаты?

11. Для чего применяются хэш-функции?

12. Какие типы криптосистем определены российскими стандартами?

ЗАКЛЮЧЕНИЕ

Информационная безопасность в настоящее время – одно из самых динамично развивающихся направлений, что обусловлено как широким распространением информационных технологий и демократизацией доступа к ним, так и обострением противодействия отдельных групп и государств в информационной сфере.

Особую важность данное направление принимает для государственных информационных систем, систем, обрабатывающих информацию ограниченного доступа.

В пособии изложены наиболее распространенные современные подходы, методы и технологии защиты информации. Выбор решений для конкретных информационных систем должен быть основан на анализе слабых и сильных сторон тех или иных методов и средств защиты, который должны провести технические специалисты.

Однако основой применения любых технических решений являются организационные процедуры и их правовая поддержка. Отправной точкой обеспечения информационной безопасности предприятия является формирование политики безопасности, создание организационных структур, координация сил и средств защиты информации. Ключевую роль при этом играет руководитель подразделения, организации, предприятия. Руководитель лучше других знает свою предметную область и может лучше других оценить возможные проблемы, связанные с угрозами безопасности информации. Поэтому и постановка задач, и политика в сфере безопасности должна быть согласована и одобрена руководством.

Все это требует владения основными представлениями и базовыми навыками обеспечения информационной безопасности. Поэтому изучение курса «Основы информационной безопасности» является закономерным шагом в эволюции и совершенствовании профессиональных знаний работника правоохранительных органов.

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ И ЛИТЕРАТУРА

Нормативные правовые акты

1. Конституция Российской Федерации.
2. Доктрина информационной безопасности Российской Федерации.
3. Концепция национальной безопасности Российской Федерации.
4. Федеральный закон от 21.07.1993 № 5485-ФЗ «О государственной тайне».
5. Федеральный закон от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов».
6. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности».
7. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
8. Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации».
9. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
10. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
11. Федеральный закон от 7.02.2011 № 3-ФЗ «О полиции».
12. Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи».
13. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».
14. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.
15. ГОСТ Р 34.10-2012. Национальный стандарт РФ «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
16. ГОСТ Р 34.11-2012. Национальный стандарт РФ «Информационная технология. Криптографическая защита информации. Функция хэширования».
17. ГОСТ Р 34.12-2015. Национальный стандарт РФ «Информационная технология. Криптографическая защита информации. Блочные шифры».
18. ГОСТ Р 34.12-2015. Национальный стандарт РФ. «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».
19. ГОСТ Р 50922-2006 Национальный стандарт РФ «Защита информации. Основные термины и определения».
20. ГОСТ Р 51275-99. Национальный стандарт РФ «Защита информации. Объект информатизации».
21. ГОСТ Р 51898-2002. О Государственном стандарте РФ «Аспекты безопасности. Правила включения в стандарты».
22. ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт РФ «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

Литература

Основная:

1. Васильева И.Н. Криптографические методы защиты информации. Учебник и практикум для академического бакалавриата. – М.: Изд-во Юрайт, 2016. – 349 с.

2. Васильева И.Н., Куватов В.И., Потехин В.С. Криптографическая защита информации: учеб. пособие. – СПб.: Изд-во СПб ун-та МВД России, 2016. – 152 с.

3. Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем: учебник для вузов. – М.: Университетская книга, 2012. – 598 с.

Дополнительная:

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. – М.: Академия, 2011. – 336 с.

2. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ Санкт-Петербург, 2000. – 384 с.

3. Аполлонский А.В., Домбровская Л.А., Примакин А.И., Смирнова О.Г. Основы информационной безопасности в ОВД: учебник для вузов. – СПб.: Изд-во СПб ун-та МВД России, 2010. – 126 с.

4. Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации – М.: Либроком, 2016. – 416 с.

5. Златопольский Д.М. Простейшие методы шифрования текста. – М.: Чистые пруды, 2007. – 30 с.

6. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации. – М.: Форум, 2012. – 254 с.

7. Кузнецов М., Симдянов И. Социальная инженерия и социальные хакеры. – СПб.: БХВ-Петербург, 2007. – 368 с.

8. Малюк А.А. Теория защиты информации. – М.: Горячая линия – Телеком, 2012. – 184 с.

9. Основы информационной безопасности: учеб. пособие / В.А. Галатенко. М.: Интернет-ун-т информ. технологий, 2006. – 208 с.

10. Партыка Т.Л., Попов И.И. Информационная безопасность: учеб. пособие. – М.: Форум: НИЦ ИНФРА-М, 2014. – 432 с.

11. Петров С.В. Информационная безопасность: учеб. пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. – М.: АРТА, 2012. – 296 с.

12. Прокопенко А.Н., Кривоухов А.А. Правовая защита информации: курс лекций / под ред. Ю.Н. Каниберга. – М.: ЦОКР МВД России, 2008. – 216 с.

13. Расторгуев С.П. Основы информационной безопасности: учеб. пособие для студентов вузов. – М.: Академия, 2007. – 192 с.

14. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. – М.: Горячая линия – Телеком, 2014. – 229 с.

15. Семененко В.А. Информационная безопасность. – М.: МГИУ, 2011. – 316 с.

16. Сёмкин С.Н., Сёмкин А.Н. Основы правового обеспечения защиты информации: учеб. пособие. – М.: Горячая линия – Телеком, 2008. – 238 с.

17. Ташков П. Защита компьютера на 100%. Сбои, ошибки и вирусы. – СПб.: Питер, 2011. – 288 с.

18. Шаньгин В.Ф. Информационная безопасность и защита информации. – М.: ДМК-Пресс, 2014. – 702 с.

19. Фаронов А.Е. Основы информационной безопасности при работе на компьютере. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 154 с.

20. Чипига А.Ф. Информационная безопасность автоматизированных систем. – М.: Гелиос АРВ, 2010. – 336 с.

Учебное издание

Васильева Ирина Николаевна
кандидат физико-математических наук, доцент
Смирнова Ольга Геннадьевна
кандидат юридических наук, доцент

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Редактор *Свикша Н.О.*
Компьютерная вёрстка *Свикша Н.О.*

Подписано в печать 16.11.2017 г. Формат 60×84 $^{1}/_{8}$
Печать цифровая. Объем 9,25 п. л. Тираж 100 экз. Заказ № 71 /17

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1