Министерство науки и высшего образования Российской Федерации
Байкальский государственный университет

М.М. Бусько

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие

Иркутск
Издательский дом БГУ
2022

УДК 004.056(075.8)
ББК 32.973я7
Б92

Издается по решению редакционно-издательского совета
Байкальского государственного университета

Рецензенты
канд. техн. наук, доц. А.В. Сорокин
(Байкальский государственный университет)

канд. физ.-мат. наук, доц. Т.И. Белых (Иркутский институт
(филиал) ВГУЮ (РПА Минюста России))

Бусько, М.М.

Б92 Информационная безопасность и защита информации : учеб. пособие / М.М. Бусько. — Иркутск : Изд. дом БГУ, 2022. — 224 с.

ISBN 978-5-7253-3094-6.

В пособии дано введение в общие проблемы информационной безопасности, рассмотрены правовые и организационные вопросы, связанные с построением комплексной системы защиты информации, вопросы защиты информации в автоматизированных системах обработки данных, криптографические методы защиты информации, компьютерные вирусы и защита от них, средства и методы инженерно-технической защиты.

Для студентов, изучающих дисциплины «Информационная безопасность» и «Защита информации».

УДК 004.056(075.8)
ББК 32.973я7

ISBN 978-5-7253-3094-6

© Бусько М.М., 2022
© ФГБОУ ВО «БГУ», 2022

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Реалии современного информационного общества показывают, что ни одна сфера деятельности в цивилизованном государстве не может эффективно функционировать без развитой информационной инфраструктуры, широкого применения аппаратно-программных средств и сетевых технологий обработки и обмена информации. По мере возрастания ценности информации, развития и усложнения средств ее обработки и обмена безопасность общества все в большей степени зависит от безопасности используемых информационных технологий. Информационная безопасность — это состояние защищенности, которое достижимо при помощи комплекса мероприятий по защите информации.

Информационная безопасность — многогранная область деятельности, в которой успех может принести только систематический, комплексный подход. Для решения данной проблемы необходимы меры законодательного, административного, процедурного и технического уровня.

Цель настоящего учебного пособия — научить выполнять основные этапы решения задач по обеспечению информационной безопасности, правильно проводить анализ угроз информационной безопасности, принимать меры и внедрять средства для нейтрализации актуальных угроз.

В пособии рассмотрены свойства информации как предмета защиты, методы нарушения конфиденциальности, целостности и доступности информации, определены закономерности создания комплексной системы защиты информации в организации, раскрыты принципы обеспечения информационной безопасности, уделено внимание информационным угрозам и рискам. Дан краткий анализ систем аутентификации, моделей и политик безопасности (разграничения доступа) в компьютерных системах, а также описаны применяемые меры для обеспечения безопасности информации при межсетевом взаимодействии. Отдельные главы посвящены методам криптографической, инженерно-технической защиты информации.

Пособие будет полезно для студентов, изучающих дисциплины «Информационная безопасность» и «Защита информации», а также для специалистов, связанных с современными информационными технологиями.

1. ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

1.1. Основные понятия

Доктрина информационной безопасности Российской Федерации [1] (далее — Доктрина ИБ) ставит информационную сферу в разряд стратегических национальных приоритетов Российской Федерации. В частности, Доктрина гласит: «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».

Предпосылками принятия нового документа, в 2016 г. пришедшего на смену версии 2000 г., послужили изменения во внешнеполитической ситуации, а именно:

– стало все четче ощущаться противостояние России другим государствам;

– публикации западных СМИ начали смещаться в сторону антипропаганды России;

– в стратегиях кибербезопасности зарубежных стран присутствует неявная агрессия по отношению к России;

– сейчас практически 100 % документов хранятся в электронном виде, что влечет за собой потребность в дополнительных способах защиты;

– появились новые вирусы и киберугрозы, направленные на государственные устои;

– возникла техническая возможность подвергать целевым атакам не только компьютерные сети, но и системы управления автоматизированными процессами (АСУ ТП);

– появление социальных сетей и других многочисленных интернет-ресурсов, предназначенных для общения, делает возможным их использование для пропаганды политики какого-либо государства и организации массовых беспорядков на территории других стран.

В связи с этим «информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации» [1].

«Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации» [1].

Информационная безопасность Российской Федерации (далее — информационная безопасность) — состояние защищенности 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 [1].

Это понятие информационной безопасности в широком смысле на уровне государства. Есть и более узкая трактовка безопасности информации уровня отдельного субъекта — организации, предприятия и даже человека.

Безопасность информации — состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами [2]. Соответственно, формирование безопасной информационной среды требует принятия определенных защитных мер в отношении информации. Для поддержания состояния защищенности необходима защита информации. Таким образом, предметом защиты является информация.

Для того чтобы лучше разобраться с предметом защиты, обратимся к нормативным документам, выполняющим правовое регулирование в информационной сфере. По определению **«информация** — сведения (сообщения, данные) независимо от формы их представления» [3]. Данное определение не является исчерпывающим. Понятие «информация» не имеет пока строго научного однозначного определения и имеет в разных сферах деятельности различное смысловое наполнение. Дискутировать на эту тему выходит за рамки дисциплин «Защита информации» и «Информационная безопасность». Обратимся лучше к ряду особенностей информации, которыми она обладает:

– она нематериальна;

– информация хранится и передается с помощью материальных носителей;

– любой материальный объект может содержать информацию о самом себе или других объектах.

Исходя из этих особенностей, нематериальная информация может храниться, передаваться, обрабатываться, если она содержится на материальном носителе. Так как с помощью материальных средств можно защищать только материальный объект, то объектами защиты являются материальные носители информации.

Объект защиты — вся совокупность носителей информации, которая представляет собой комплекс физических, аппаратных, программных и документальных средств. Важно помнить, что под объектом защиты понимаются не только информационные ресурсы, аппаратные и программные средства, но и обслуживающий персонал, пользователи, помещения, здания, а также прилегающая к зданиям территория. В широком смысле любой материальный объект является носителем информации хотя бы в виде значений его признаков. Соответственно, элементом защиты информации является и непосредственный физический доступ к объекту.

Наиболее важным свойством информации является ее **ценность (значимость)**. Ценность информации определяется степенью ее полезности для обладателя. Обладание истинной (достоверной) информацией дает определенные преимущества. Истинной, или достоверной, информацией является информация, которая с достаточной для обладателя точностью отражает объекты и процессы окружающего мира в определенных временных и пространственных рамках. Однако ценность или полезность информации — это понятие субъективное. Один человек получает много полезной информации из определенного источника, другой нет. Это возможно только в том случае, если исходные априорные совокупности признаков (значений характеристик) двух человек различаются на величину разности изменений их признаков после получения этой информации.

Оценка ценности информации нужна для того, чтобы знать, какие потери мог бы понести ее обладатель в случае потери полезной информации. Соответственно, затраты сил и средств на защиту информации не должны превышать возможные потери. В зависимости от вида информации можно использовать различные единицы для определения ценности информации. Далеко не всегда возможно и нужно давать денежную оценку информации. Например, оценка личной информации, политической информации или военной информации не всегда разумна в денежном исчислении. В этом случае возможны экспертные оценки в качественной шкале.

Если информация ценна для ее обладателя, то необходимо разобраться, кто такой обладатель с правовой точки зрения.

Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [3]. В соответствии с требованиями ФЗ-149 «Об информации, информационных технологиях и о защите информации» «обладатель информации вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа» [3]. Кроме своих прав в отношении информации обладатель имеет и обязанности. Согласно ФЗ-149, «обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами» [3].

Таким образом, «информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)» [3].

К **общедоступной информации** относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя [3]. Одной из обязанностей обладателя информации является ее защита. Рассмотрим определения защиты информации, имеющиеся в нормативных документах.

Защита информации (ЗИ) — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [4].

Согласно ГОСТ Р 50922-2006, различают следующие виды защиты информации.

Правовая защита информации — защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Техническая защита информации (ТЗИ) **—** защита информации, заключающаяся в обеспечении не криптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Криптографическая защита информации — защита информации с помощью ее криптографического преобразования.

Физическая защита информации — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Если поразмыслить над этими терминами, то очевидно, что криптографическая защита информации является частью технической защиты. В настоящее время все шифрование осуществляется с помощью программных или программно-аппаратных средств. Физическая защита — это опять же применение технических средств, препятствующих доступу к объектам защиты, и режимные регламенты, то есть технические меры в совокупности с организационными.

Согласно ФЗ № 149, **защита информации** представляет собой принятие правовых, организационных и технических мер, направленных:

– на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

– соблюдение конфиденциальности информации ограниченного доступа;

– реализацию права на доступ к информации [3].

Таким образом, правильнее выделять три вида защиты информации: правовая, организационная и техническая. Эти три вида прослеживаются и в нормативно-методических документах регуляторов в области защиты информации. Исходя из определения, изложенного в ФЗ-149, можно сделать вывод, что защита информации — это принятие правовых, организационных и технических мер, направленных на обеспечение целостности, конфиденциальности и доступности (рис. 1.1).

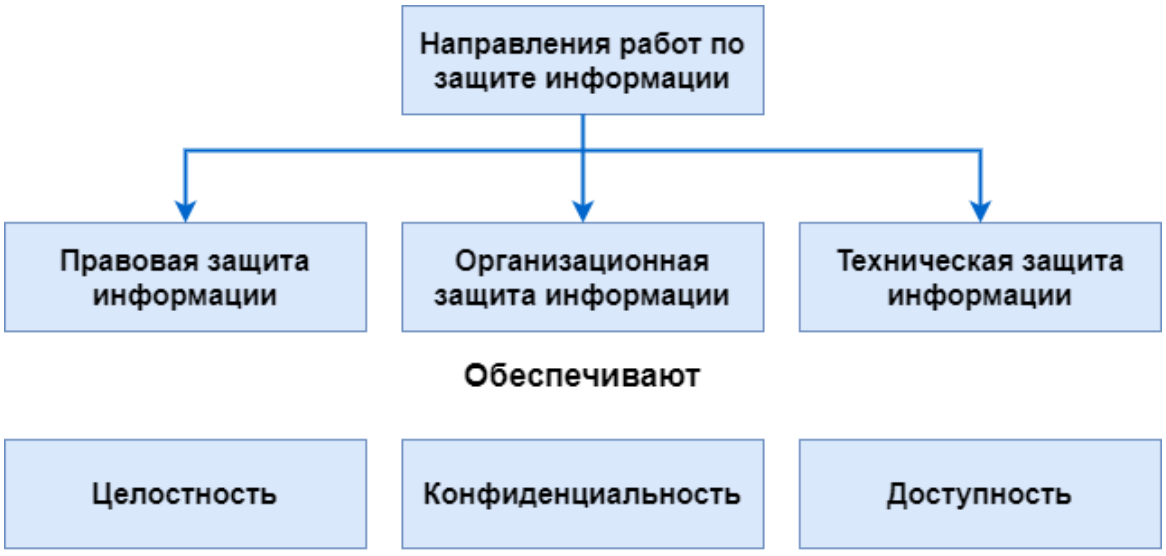


Рис. 1.1. Виды защиты информации и обеспечиваемые свойства

Итак, дадим более простые толкования видам защиты информации.

Правовые меры защиты информации включают действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

Организационные меры защиты информации заключаются в регламентации взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка, несанкционированный доступ и воздействие на информацию становятся невозможными или будут существенно затруднены за счет проведения организационных мероприятий.

Технические меры защиты информации — это обеспечение безопасности информации (данных) с применением инженерных конструкций, средств аппаратной защиты, технических, программных и программно-технических средств.

Все эти меры защиты информации направленны на обеспечение свойств информации:

– конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);

– целостности информации (исключение неправомерного уничтожения или модифицирования информации);

– доступности информации (исключение неправомерного блокирования информации).

Конфиденциальность информации — это свойство, указывающее на необходимость введения ограничений на доступ к ней определенного круга пользователей. Другими словами, это свойство, позволяющее не давать права на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам.

Целостность информации — свойство, при выполнении которого информация сохраняет заранее определенные вид и качество. Целостность информации заключается в ее существовании в неискаженном виде, неизменном по отношению к некоторому ее исходному состоянию.

Доступность информации — это свойство, характеризующее ее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным. Доступность заключается в отсутствии препятствия доступа к информации и законному ее использованию обладателем или уполномоченными лицами. Другими словами, возможность за приемлемое время получить требуемую информационную услугу.

Приведем определения этих понятий, представленные в официальных нормативных документах.

Конфиденциальность — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [3].

Целостность — состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право [5].

Доступность — возможность реализации беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия [6].

1.2. Направления развития

Приоритетность задачи, связанной с защитой информации, нашла свое отражение и в государственной программе «Цифровая экономика». Реализация этой программы идет по пяти базовым направлениям, и одним из них является информационная безопасность. Национальная программа «Цифровая экономика Российской Федерации» принята в соответствии с указом Президента России «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» от 7 мая 2018 г. № 204, утверждена 24 декабря 2018 г. на заседании президиума Совета при Президенте России по стратегическому развитию и национальным проектам и к базовым направлениям относит информационную безопасность [7].

Целью направления, касающегося информационной безопасности, является достижение состояния защищенности 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 и устойчивое социально-экономическое развитие Российской Федерации в условиях цифровой экономики, что предполагает:

– обеспечение единства, устойчивости и безопасности информационно-телекоммуникационной инфраструктуры Российской Федерации на всех уровнях информационного пространства;

– обеспечение организационной и правовой защиты личности, бизнеса и государственных интересов при взаимодействии в условиях цифровой экономики;

– создание условий для лидирующих позиций России в области экспорта услуг и технологий информационной безопасности, а также учет национальных интересов в международных документах по вопросам информационной безопасности.

Разработка и реализация мероприятий Программы базируется на основополагающих принципах информационной безопасности, включающих:

– использование российских технологий обеспечения целостности, конфиденциальности, аутентификации и доступности передаваемой информации и процессов ее обработки;

– преимущественное использование отечественного программного обеспечения и оборудования;

– применение технологий защиты информации с использованием российских криптографических стандартов.

Мероприятия федерального проекта «Информационная безопасность» направлены на реализацию четырех ключевых направлений:

– повышение уровня защищенности личности, информационной безопасности и устойчивости сетей связи общего пользования;

– создание новых сервисов (услуг) для граждан, гарантирующих защиту их персональных данных;

– профилактика и выявление правонарушений с использованием информационных технологий против общества и бизнеса;

– разработка новых механизмов поддержки отечественных разработчиков программного обеспечения и компьютерного оборудования в сфере информационной безопасности.

1.3. Государственная система защиты информации РФ

Проблема безопасности информации с точки зрения государственных интересов в последние годы приобрела остроактуальный характер и рассматривается как одна из приоритетных государственных задач, как важный элемент национальной безопасности. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации [3].

Государственная система защиты информации — совокупность федеральных органов власти, местного самоуправления, предприятий, организаций и учреждений, а также система правовых, организационных, технических и иных мер, направленных на обеспечение информационной безопасности Российской Федерации, сохранение государственной и других видов тайн, информационных ресурсов, систем, технологий и средств их обеспечения.

Основные задачи государственной системы защиты информации:

– обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

– оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

– планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

– организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-розыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

– выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

Структура государственной системы защиты информации представлена на рис. 1.2.

Рис. 1.2. Структура государственной системы защиты информации

Межведомственная комиссия по защите государственной тайны действует на основании Положения [8]. Межведомственная комиссия — коллегиальный орган, основной функций которого является координация деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных правовых актов и методических документов, обеспечивающих реализацию федерального законодательства о государственной тайне [8].

Руководство деятельностью Межведомственной комиссии осуществляет Президент Российской Федерации, а ее полномочия [8]:

– координация деятельности органов государственной власти, органов местного самоуправления и организаций по вопросам реализации федерального законодательства в области государственной тайны;

– рассмотрение и представление в установленном порядке Президенту Российской Федерации и в Правительство Российской Федерации предложений по правовому регулированию вопросов защиты государственной тайны и совершенствованию системы защиты государственной тайны в Российской Федерации, а также предложений по организации разработки и выполнения государственных программ, нормативных правовых актов и методических документов, обеспечивающих реализацию федерального законодательства о государственной тайне;

– формирование перечня сведений, отнесенных к государственной тайне;

– разработка и представление в Правительство Российской Федерации предложений по правилам отнесения сведений, составляющих государственную тайну, к различным степеням секретности;

– координация работы по техническому регулированию в отношении продукции (работ, услуг), сведения о которых составляют государственную тайну, а также работы по организации сертификации средств защиты информации;

– координация проведения 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;

– координация деятельности в области подготовки, переподготовки и (или) повышения квалификации специалистов по вопросам защиты государственной тайны.

Федеральная служба по техническому и экспортному контролю России (ФСТЭК) осуществляет общую организацию и координацию работ в стране по защите информации, обрабатываемой техническими средствами, действует на основании Положения [9]. ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности. Полномочия ФСТЭК [9]:

– обеспечение безопасности информации в ключевых системах информационной инфраструктуры;

– противодействие иностранным техническим разведкам на территории Российской Федерации;

– обеспечение защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращение 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;

– защита информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

– осуществление экспортного контроля.

ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля. ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею. Приказы, распоряжения и указания ФСТЭК России, изданные в пределах ее компетенции, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, предприятиями, учреждениями и организациями. Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации, сама же служба подведомственна Министерству обороны России. В своей работе по организации и координации деятельности по защите информации ФСТЭК России активно взаимодействует с Федеральной службой безопасности России (ФСБ) и Федеральной службой охраны (ФСО).

Федеральная служба безопасности России является федеральным органом исполнительной власти, обеспечивающим, в пределах своих полномочий, информационную безопасность Российской Федерации, действует на основании Положения [10]. Президент Российской Федерации руководит деятельностью ФСБ России, утверждает Положение о Федеральной службе безопасности Российской Федерации и структуру органов федеральной службы безопасности. Правительство Российской Федерации в соответствии с Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, указами и распоряжениями Президента Российской Федерации координирует деятельность ФСБ России в части, касающейся взаимодействия ФСБ России с федеральными органами исполнительной власти. При ФСБ России действует Академия криптографии Российской Федерации.

Задачи ФСБ в области защиты информации [10]:

– обеспечение в пределах своих полномочий защиты сведений, составляющих государственную тайну, и противодействия иностранным организациям, осуществляющим техническую разведку;

– формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности;

– организация в пределах своих полномочий обеспечения криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за рубежом.

Функции ФСБ [10]:

– разрабатывает меры по защите сведений, составляющих государственную тайну, осуществляет контроль за обеспечением сохранности сведений, составляющих государственную тайну, осуществляет меры, связанные с допуском граждан к сведениям, составляющим государственную тайну, а также с допуском предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации и с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны;

– разрабатывает и утверждает нормативные и методические документы по вопросам обеспечения информационной безопасности информационно-телекоммуникационных систем и сетей критически важных объектов, а также организует и осуществляет контроль за обеспечением информационной безопасности указанных систем и сетей;

– осуществляет и организует сертификацию средств защиты информации, средств, используемых для выявления электронных устройств, предназначенных для негласного получения информации, специальных технических средств, предназначенных для негласного получения информации, технических средств обеспечения безопасности и (или) защиты информации; определяет основные направления деятельности органов федеральной службы безопасности в этих областях;

– осуществляет регулирование в области разработки, производства, реализации, эксплуатации, ввоза в Российскую Федерацию и вывоза из Российской Федерации шифровальных средств и защищенных с использованием шифровальных средств систем и комплексов телекоммуникаций, а также в области предоставления на территории Российской Федерации услуг по шифрованию информации и выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах;

– обеспечивает в пределах своих полномочий защиту сведений, составляющих государственную тайну, и противодействие иностранным организациям, осуществляющим техническую разведку;

– формирует и реализует в пределах своих полномочий государственную и научно-техническую политики в области обеспечения информационной безопасности;

– организует в пределах своих полномочий обеспечение криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за рубежом.

Федеральная служба охраны (ФСО) осуществляет выработку государственной политики, нормативно-правовое регулирование, контроль и надзор в сфере президентской, правительственной и иных видов специальной связи, а также функции по информационно-технологическому и информационно-аналитическому обеспечению деятельности государственных органов, от-

несены к компетенции Федеральной службы охраны Российской Федерации. ФСО РФ действует на основании Положения [11].

В число задач ФСО входят [11]:

– обеспечение организации и функционирования федеральных информационных систем, находящихся во владении или пользовании органов государственной охраны (далее — федеральные информационные системы);

– участие в пределах своих полномочий в обеспечении информационной безопасности Российской Федерации;

– обеспечение защиты персональных данных объектов государственной охраны и членов их семей.

Функции ФСО РФ [11]:

– осуществляет эксплуатацию, организует и проводит мероприятия по совершенствованию, обеспечению безопасности и надежности систем специальной связи на территории Российской Федерации, а также международной правительственной и иных видов специальной международной связи;

– обеспечивает защиту категорированных помещений, организует и проводит мероприятия по предотвращению утечки информации по техническим каналам в системах специальной связи, по предотвращению несанкционированного доступа к указанным системам;

– участвует в разработке, создании и развитии средств защиты информации, включая системы специальных технических средств, а также в разработке нормативно-технической документации по вопросам защиты информации в системах специальной связи.

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

– определяют перечень охраняемых сведений;

– обеспечивают разработку и осуществление технически и экономически обоснованных мер по защите информации на подведомственных предприятиях;

– организуют и координируют проведение научно-исследовательских и опытно-конструкторских работ (НИОКР) в области защиты информации в соответствии с государственными (отраслевыми) программами;

– разрабатывают по согласованию с ФСТЭК России отраслевые документы по защите информации;

– контролируют выполнение на предприятиях отрасли установленных норм и требований по защите информации;

– создают отраслевые центры по защите информации и контролю эффективности принимаемых мер;

– организуют подготовку и повышение квалификации специалистов по защите информации.

Государственными органы исполнительной власти, работающие в области защиты информации, следующие.

Служба внешней разведки Российской Федерации (СВР России) — основной орган внешней разведки Российской Федерации.

Министерство обороны Российской Федерации (Минобороны России) — федеральный орган исполнительной власти (федеральное министерство), проводящий государственную политику и осуществляющий государственное управление в области обороны, а также координирующий деятельность федеральных министерств, иных федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по вопросам обороны. Является центром сертификации средств защиты информации.

Министерство внутренних дел Российской Федерации (МВД России) — федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, а также по выработке государственной политики в сфере миграции.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) — федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы.

Государственная система защиты информации подразумевает необходимость разделения прав и обязанностей между субъектами обеспечения защищенности информации: государством, предприятиями, их объединениями, учреждениями и организациями, а также отдельными должностными лицами. Для проведения работ по защите информации могут привлекаться на договорной основе специализированные предприятия, имеющие лицензии на право проведения работ в области защиты информации.

Кроме того, в отраслях промышленности и в регионах страны создаются и функционируют лицензионные центры, осуществляющие организацию и контроль за деятельностью в области оказания услуг по защите информации, органы сертификации средств вычислительной техники и средств связи, испытательные центры по сертификации конкретных видов продукции по требованиям безопасности информации, органы аттестации объектов информатизации. Если продолжать перечень, то можно выделить следующие органы:

– структурные подразделения по защите информации федеральных органов исполнительной власти, других органов государственной власти и организаций Российской Федерации;

– предприятия, проводящие работы с использованием сведений, отнесенных к информации ограниченного доступа, и их подразделения по защите информации;

– научно-исследовательские организации по проблемам защиты информации;

– организации-разработчики средств защиты информации, защищенных технических средств и средств контроля эффективности защиты информации;

– предприятия, оказывающие услуги в области защиты информации;

– организации Федерального агентства по техническому регулированию и метрологии (бывшего Госстандарта России), выполняющие работы по стандартизации в области защиты информации;

– органы системы лицензирования деятельности в области защиты информации;

– органы системы сертификации средств защиты информации;

– органы системы аттестации объектов защиты по требованиям безопасности информации.

1.4. Угрозы информационной безопасности

Защита информации направлена на выполнение пяти задач:

– предупреждение угроз как превентивных мер по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;

– выявление угроз, которое выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;

– обнаружение угроз, целью которого является определение реальных угроз и конкретных преступных действий;

– локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;

– ликвидацию последствий угроз и преступных действий и восстановление статус-кво.

Угроза (безопасности информации) — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [4]. Чаще всего угроза является следствием наличия уязвимых мест в защите информации (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении). Уязвимость (информационной системы), брешь — свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации [4].

Уязвимость — это слабое место в системе защиты, которое может привести к нарушению безопасности путем реализации некоторой угрозы.

Свойствами угрозы являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость. Оценка угроз безопасности информации проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях с заданной архитектурой и в условиях их функционирования — актуальных угроз безопасности информации. Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются:

а) определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;

б) инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;

в) определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;

г) оценка способов реализации (возникновения) угроз безопасности информации;

д) оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;

е) оценка сценариев реализации угроз безопасности информации в системах и сетях.

Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия, способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным последствиям:

$$УБИ_j = [нарушитель\ (источник\ угрозы);\ объекты\ воздействия;\ способы\ реализации\ угрозы;\ негативные\ последствия]$$

По результатам оценки должны быть выявлены актуальные угрозы безопасности информации, реализация (возникновение) которых может привести к нарушению безопасности обрабатываемой в системах и сетях информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования систем и сетей [13]. Актуальные угрозы безопасности информации включаются в модель угроз безопасности информации. Модель угроз безопасности информации, учитывая особенности информационной системы, используемые в ней программные, программно-технические, технические средства и процессы обработки информации, дает описание угроз безопасности, которым подвержена информационная система.

Сведения о возможных угрозах, а также об уязвимых местах, через которые эти угрозы могут быть реализованы, необходимы, с одной стороны, для того чтобы выработать требования к создаваемой системе защиты информации, с другой стороны, для того чтобы выбрать наиболее экономичные средства обеспечения безопасности.

Модель угроз (безопасности информации) — физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации [12].

Примечание — видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ [12].

Модель угроз — это документ, определяющий перечень и характеристики основных (актуальных) угроз безопасности и уязвимостей, которые должны учитываться в процессе организации защиты информации, проектирования и разработки систем защиты информации, проведения проверок (контроля) защищенности объекта информатизации. Цель разработки модели угроз — опре-

деление актуальных угроз безопасности, источников угроз и уязвимостей. Результаты моделирования должны использоваться в качестве исходных данных для выработки требований ИБ к разрабатываемой системе защиты.

Основным классификационным признаком угроз безопасности информации является ее источник. В зависимости от источника различают антропогенные, техногенные и стихийные угрозы.

Угрозы, обусловленные действиями субъекта (антропогенные угрозы). Действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия этим угрозам управляемы и зависят от организации защиты информации.

Угрозы, обусловленные техническими средствами (техногенные угрозы). Угрозы менее прогнозируемые, напрямую зависящие от свойств техники и поэтому требующие особого внимания.

Угрозы, обусловленные стихийными источниками (стихийные угрозы). Угрозы не поддаются прогнозированию, и поэтому меры их противодействия должны применяться всегда.

Субъектами антропогенных угроз могут быть как внешние (криминальные структуры, потенциальные преступники, недобросовестные партнеры, конкуренты, политические противники), так и внутренние (персонал учреждения, персонал филиалов, специально внедренные агенты). Реализация антропогенных угроз может привести к таким нежелательным последствиям:

– кража: технических средств (винчестеров, ноутбуков, системных блоков), носителей информации (бумажных, магнитных, оптических и пр.), информации (чтение и несанкционированное копирование), средств доступа (ключи, пароли, ключевая документация и пр.);

– подмена (модификация): операционных систем, систем управления базами данных, прикладных программ, информации (данных), отрицание факта отправки сообщений, паролей и правил доступа;

– уничтожение (разрушение): технических средств (винчестеров, ноутбуков, системных блоков), носителей информации (бумажных, магнитных, оптических и пр.), программного обеспечения (ОС, СУБД, прикладного ПО), информации (файлов, данных), паролей и ключевой информации;

– нарушение нормальной работы (прерывание): скорости обработки информации, пропускной способности каналов связи, объемов свободной оперативной памяти, объемов свободного дискового пространства, электропитания технических средств;

– ошибки: при инсталляции ПО, ОС, СУБД, при написании прикладного ПО, при эксплуатации ПО, при эксплуатации технических средств;

– перехват информации (несанкционированный): за счет ПЭМИ от технических средств, за счет наводок по линиям электропитания, за счет наводок по посторонним проводникам, по акустическому каналу от средств вывода, по акустическому каналу при обсуждении вопросов, при подключении к каналам передачи информации, за счет нарушения установленных правил доступа (взлом).

Техногенные угрозы также могут быть внутренними (некачественные технические средства обработки информации, некачественные программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства) и внешними (средства связи, близко расположенные опасные производства, сети инженерных коммуникаций (энерго-, водоснабжения, канализации), транспорт). Последствия, к которым могут привести техногенные угрозы это:

– нарушение режима работы: нарушение работоспособности системы обработки информации, нарушение работоспособности связи и телекоммуникаций, старение носителей информации и средств ее обработки, нарушение установленных правил доступа, электромагнитное воздействие на технические средства;

– уничтожение (разрушение): программного обеспечения, ОС, СУБД, средств обработки информации (броски напряжений, протечки), информации (размагничивание, радиация, протечки и пр.);

– модификация (изменение): программного обеспечения, ОС, СУБД, информации при передаче по каналам связи и телекоммуникациям.

Стихийные источники всегда являются внешними (пожары, землетрясения, наводнения, ураганы, другие форс-мажорные обстоятельства). Их последствия — это в первую очередь уничтожение (разрушение) технических средств обработки информации, носителей информации, программного обеспечения (ОС, СУБД, прикладного ПО), информации (файлов, данных), помещений, персонала.

Еще одним важным признаком классификации возможных угроз является степень преднамеренности проявления. Здесь различают случайные, или непреднамеренные, угрозы и преднамеренные (рис. 1.3). К первому типу относятся угрозы, вызванные ошибками или халатностью персонала, например некомпетентное использование средств защиты, ввод ошибочных данных и т.п. Ко второму — угрозы преднамеренного действия, например действия злоумышленников. Преднамеренные угрозы всегда являются антропогенными.

Еще одним важным параметром классификации угроз является вид несанкционированных действий, осуществляемых с информацией:

– угрозы, приводящие к нарушению конфиденциальности (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;

– угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется ее изменение или уничтожение;

– угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы, в результате которого осуществляется блокирование информации.

Рис. 1.3. Классификация угроз по степени преднамеренности проявления

Кроме этого, есть еще менее важные критерии классификации возможных угроз, которые, тем не менее, могут помочь в их идентификации.

По положению источника угроз:

– вне контролируемой зоны. Например, перехват данных, передаваемых по каналам связи, перехват побочных электромагнитных, акустических и других излучений устройств;

– в пределах контролируемой зоны (например, применение подслушивающих устройств, хищение распечаток, записей, носителей информации и т.п.);

– непосредственно в информационной системе (например, некорректное использование ресурсов информационной системы).

По степени зависимости от активности информационной системы:

– независимо от активности ИС (например, вскрытие шифров криптозащиты информации);

– только в процессе обработки данных (например, угрозы выполнения и распространения программных вирусов).

По степени воздействия на ИС:

– пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании ИС (например, угроза копирования секретных данных);

– активные угрозы, которые при воздействии вносят изменения в структуру и содержание ИС (например, внедрение троянских коней и вирусов).

По этапам доступа пользователей или программ к ресурсам:

– угрозы, проявляющиеся на этапе доступа к ресурсам ИС (например, угрозы несанкционированного доступа в ИС);

– угрозы, проявляющиеся после разрешения доступа к ресурсам ИС (например, угрозы несанкционированного или некорректного использования ресурсов ИС).

По способу доступа к ресурсам ИС:

– угрозы, осуществляемые с использованием стандартного пути доступа к ресурсам ИС;

– угрозы, осуществляемые с использованием скрытого нестандартного пути доступа к ресурсам ИС (например, несанкционированный доступ к ресурсам ИС путем использования недокументированных возможностей ОС).

По текущему месту расположения информации, хранимой и обрабатываемой в ИС:

– угрозы доступа к информации, находящейся на внешних запоминающих устройствах (например, несанкционированное копирование секретной информации с жесткого диска);

– угрозы доступа к информации, находящейся в оперативной памяти (например, чтение остаточной информации из оперативной памяти, доступ к системной области оперативной памяти со стороны прикладных программ);

– угрозы доступа к информации, циркулирующей в линиях связи (например, незаконное подключение к линиям связи с последующим вводом ложных сообщений или модификацией передаваемых сообщений, незаконное подключение к линиям связи с целью прямой подмены законного пользователя с последующим вводом дезинформации и навязыванием ложных сообщений);

– угрозы доступа к информации, отображаемой на мониторе или печатаемой на принтере (например, запись отображаемой информации на скрытую видеокамеру).

Вопросы для самоконтроля

1. Дайте определение информации и носителя информации.
2. Дайте определение понятия информационная безопасность.
3. Что такое информация и каковы уровни ее представления?
4. Перечислите основные носители информации, особенности их использования и защиты.
5. Какими свойствами определяется ценность информации?

6. Какие критерии оценки ценности информации вы можете предложить?

7. Приведите примеры различной зависимости ценности информации от времени.

8. Что понимается под информационными ресурсами?

9. Какие основные составляющие информационной безопасности?

10. Значение составляющих информационной безопасности для субъектов информационных отношений.

11. Информационная безопасность в системе национальной безопасности.

12. Источники угроз информационной безопасности РФ и их классификация.

13. Основные методы обеспечения информационной безопасности РФ.

14. Примеры угроз, которые являются нарушением целостности, конфиденциальности и доступности.

15. Примеры непредумышленных угроз.

16. Антропогенные информационные уязвимости.

17. Техногенные информационные уязвимости.

18. На примере нескольких различных угроз покажите, что их осуществление приведет к изменению одного из основных свойств защищаемой информации (конфиденциальности, целостности, доступности).

19. Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.

20. Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?

21. В каких системах на первом месте стоит обеспечение доступности информации?

22. В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?

23. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.

2. ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ

2.1. Структура правовой базы в области информационной безопасности

Согласно федеральному закону «Об информации, информационных технологиях и о защите информации», защита информации представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение целостности, доступности и конфиденциальности для информации ограниченного доступа. Предметом правового обеспечения является правовой режим информации (степень конфиденциальности, собственность, средства и формы защиты информации, которые можно использовать), правовой статус участников информационного взаимодействия, порядок отношения субъектов с учетом их правового статуса.

К правовым методам относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности в Российской Федерации. Цель нормативного правового обеспечения информационной безопасности Российской Федерации — создание правовых условий для эффективной деятельности субъектов системы обеспечения информационной безопасности по противодействию внешним и внутренним угрозам национальным интересам Российской Федерации в информационной сфере. Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

– свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

– установление ограничений доступа к информации только федеральными законами;

– открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

– равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

– обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите, содержащейся в них информации;

– достоверность информации и своевременность ее предоставления;

– неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

– недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Структура правовой базы в области информационной безопасности представлена на рис. 2.1.

Рис. 2.1. Структура правовой базы в области информационной безопасности

2.2. Международные нормы

Международные правовые нормы включают в себя конвенции, резолюции ООН, декларации. Наиболее значимым из них является следующий документ: Конвенция об обеспечении международной информационной безопасности (концепция) (2011 г.). Это инициатива России и представителей Шанхайской организации сотрудничества (ШОС), направленная на формирование глобального режима обеспечения безопасности информационного пространства. Данный документ:

– претендует на всеобъемлющий характер и полное урегулирование проблематики международной информационной безопасности;

– должен через механизм ООН получить глобальный охват, распространившись на все международное сообщество; предполагает юридически обязывающий характер, не ограничиваясь декларативными заявлениями и формулированием общих принципов поведения государств в информационном пространстве;

– позиционируется как почти завершенный механизм, который, с точки зрения его авторов и сторонников, после соответствующей доработки может превратиться в действующий международно-правовой инструмент ООН уже в ближайшие годы [14].

Второй документ, который заслуживает внимания, — это Конвенция о защите персональных данных физических лиц при их автоматизированной обработке 1981 г. В декабре 2005 г. Российская Федерация ратифицировала данную Конвенцию Совета Европы, взяв на себя тем самым обязательства привести национальное законодательство в соответствие с этой Конвенцией. В рамках данных обязательств был принят федеральный закон «О персональных данных», который закрепляет общие принципы их охраны, а также ряд подзаконных актов [14].

Также в качестве примера можно привести такие документы, как:

– Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.);

– Окинавская хартия глобального информационного общества 2000 г.

Международное сотрудничество в области информационной безопасности также представлено рядом резолюций ООН:

– Резолюция Генеральной Ассамблеи Организации Объединенных Наций «Роль науки и техники в контексте международной безопасности и разоружения» A/RES/55/29 от 20 ноября 2000 г.;

– Резолюция Генеральной Ассамблеи Организация Объединенных Наций «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур» A/RES/64/211 от 21 декабря 2009 г.;

– Резолюция Генеральной Ассамблеи Организации Объединенных Наций «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности» A/RES/65/41 от 8 декабря 2010 г.

2.3. Внутригосударственное право

Начальным этапом формирования правовой защиты информации являются нормы, закрепленные в Конституции РФ, которая является основным источником права в области обеспечения информационной безопасности в России. Конституция Российской Федерации (принята всенародным голосованием 12декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) содержит следующие статьи, касающиеся сферы информационной безопасности [16]:

– ст. 23 «Личная, семейная тайны охраняются в режиме тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограни-

чение права на этот вид информационной тайны допускается только на основании судебного решения»;

– ст. 24, п. 1 «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются»;

– ст. 24, п. 2 «Органы государственной власти и органы местного самоуправления обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом»;

– ст. 29 «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом»;

– ст. 42 «Каждый имеет право на достоверную информацию о состоянии окружающей среды»;

– ст. 46, ч. 3 «Ответственность должностных лиц за сокрытие фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, в соответствии с федеральными законами».

Составляющие национальных интересов Российской Федерации в информационной сфере определены в Доктрине информационной безопасности Российской Федерации (утверждена указом Президента РФ № 646 от 5 декабря 2016 г). Они заключаются в следующем:

– 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 устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры РФ и единой сети электросвязи;

– развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности по разработке, производству и эксплуатации средств обеспечения информационной безопасности;

– доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации;

– содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности.

К основным общим законам относятся:

– Федеральный закон «О безопасности» от 28 декабря 2010 г. № 390-ФЗ (ред. от 5 октября 2015 г.);

– Федеральный закон от «Об информации, информационных технологиях и о защите информации» 27 июля 2006 г. № 149-ФЗ (ред. от 29 июля 2017 г.);

– «Гражданский кодекс Российской Федерации» от 30 ноября 1994 г. № 51-ФЗ (ред. от 29 июля 2017 г.) (с изм. и доп., вступ. в силу с 6 августа 2017 г.);

– «Кодекс Российской Федерации об административных правонарушениях» от 30 декабря 2001 г. № 195-ФЗ (ред. от 29 июля 2017 г.) (с изм. и доп., вступ. в силу с 10 августа 2017 г.);

– «Трудовой кодекс Российской Федерации» от 30 декабря 2001 г. № 197-ФЗ (ред. от 29 июля 2017 г.);

– «Уголовный кодекс Российской Федерации» от 13 июня 1996 г. № 63-ФЗ (ред. от 29 июля 2017 г.) (с изм. и доп., вступ. в силу с 26августа 2017 г.);

Федеральный закон «О безопасности» от 28 декабря 2010 г. № 390-ФЗ:

– закрепляет правовые основы обеспечения безопасности личности, общества и государства;

– определяет систему безопасности и ее функции;

– устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

Одним из принципов обеспечения безопасности является: системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности.

Закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-Ф регулирует отношения, возникающие при:

– осуществлении права на поиск, получение, передачу, производство и распространение информации;

– применении информационных технологий;

– обеспечении защиты информации.

Гражданский кодекс Российской Федерации, Административный кодекс Российской Федерации, Трудовой кодекс Российской Федерации, Уголовный кодекс Российской Федерации устанавливают ответственность за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации: дисциплинарную, гражданско-правовую, материальную, административную, уголовную.

Специальные законы:

– Закон РФ «О государственной тайне» от 21июля 1993 г. № 5485-1 (ред. от 8 марта 2015 г.);

– Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ (ред. от 12 марта 2014 г.);

– Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ (ред. от 29 июля 2017 г.);

– Федеральный закон «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ (ред. от 23 июня 2016 г.).

Указы Президента РФ:

– «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188;

– «Об утверждении Доктрины информационной безопасности Российской Федерации» от 5 декабря 2016 г. № 646;

– «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» от 12 апреля 2021 г. № 213;

– «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17 марта 2008 г. № 351;

– «Вопросы Федеральной службы безопасности Российской Федерации» от 11 июля 2003 года № 960;

– «Вопросы Межведомственной комиссии по защите государственной тайны» от 6 октября 2004 г. № 1286;

– «Вопросы Федеральной службы по техническому и экспортному контролю» (выписка) от 16 августа 2004 г. № 1085 (ред. от 31 декабря 2015 г.).

Постановления правительства РФ:

– «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. № 1233;

– «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. № 333;

– «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687;

– «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» от 21 марта 2012 г. № 211;

– «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119;

– «О лицензировании деятельности по технической защите конфиденциальной информации» от 3 февраля 2012 г. № 79.

2.4. Документы уполномоченных органов

ФСТЭК является основным государственными ведомством, ведающим вопросами защиты информации, разработки методик и стратегий такой работы и закреплением данных механизмов и критериев на законодательном уровне. Именно постановления, приказы и руководящие документы ФСТЭК берутся за основу при проектировании и исполнении информационных систем, защищенных от НСД на различных уровнях. Примеры таких документов:

– приказ ФСТЭК России «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 г. № 17 (ред. от 15 февраля 2017 г.);

– «Методический документ. Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11 февраля 2014 г.);

– приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. № 21;

– Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30 августа 2002 г. № 282;

– «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 5 февраля 2021 г.).

Кроме документов ФСТЭК обязательными для исполнения являются документы ФСБ при использовании криптографических средств либо если имеет место защита государственной тайны. Примером такого документа является приказ ФСБ России «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» от 9 февраля 2005 г. № 66. Есть совместные документы, например приказ ФСБ России № 416, ФСТЭК № 489 от 31 августа 2010 г. «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования». В области криптографии есть документ ФАПСИ «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 г. № 152.

2.5. Стандарты в области информационной безопасности

Стандартизация — деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг [17]. Обязательность применения документов по стандартизации установлена в отношении

объектов стандартизации, включенных в определенный Правительством Российской Федерации перечень. Объекты в области информационной безопасности рассматриваются только косвенно, когда речь касается оборонной продукции, защиты сведений, составляющих государственную тайну, в отношении продукции, для которой устанавливаются требования, связанные с обеспечением безопасности в области использования атомной энергии, обязательное применение которых обеспечивает безопасность дорожного движения и т.д.

Государственные стандарты:

1. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России.

2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Госстандарт России.

3. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России.

4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России.

5. ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России.

6. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

7. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

8. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.

9. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

10. ГОСТ РО 0043-001-2010 Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Термины и определения.

11. ГОСТ РО 0043-002-2012 Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Система документов. Общие положения. Для служебного пользования.

12. ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения. Национальный стандарт Российской Федерации, ограниченного распространения.

13. ГОСТ РО 0043–004–2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний.

2.6. Правовой статус защищаемой информации

Статья 5 ФЗ № 149 гласит: «Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)».

Классификация информации на основании ее правового статуса представлена на рис. 2.2.

Рис. 2.2. Предметные направления защиты информации

Информация в зависимости от порядка ее предоставления или распространения подразделяется на [3]:

– информацию, свободно распространяемую;

– информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

– информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

– информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Рассмотрим сначала общедоступную информацию. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к

которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации. Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Есть еще отдельный правовой статус информации, предусмотренный законодательством, — это информация, распространение которой в Российской Федерации запрещается. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Рассмотрим теперь различные виды информации, доступ к которой ограничивается законодательством, и первый такой вид — это государственная тайна. Правовой режим государственной тайны установлен первым в истории российского государства Законом «О государственной тайне», который вступил в действие 21 сентября 1993 г. (новая редакция закона была принята в 1997 г.) [18].

Государственная тайна (ГТ) — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Закон содержит восемь разделов, в которых определены следующие основные вопросы:

– полномочия органов всех ветвей государственной власти и должностных лиц в вопросе отнесения сведений к ГТ;

– сведения, относимые к ГТ;

– порядок отнесения сведений к ГТ;

– принципы и порядок засекречивания информации;

– сведения, не подлежащие засекречиванию;

– степени секретности сведений и грифы секретности носителей этих сведений;

– порядок рассекречивания сведений;

– передача сведений, составляющих ГТ, в связи с выполнением совместных и других работ, а также другим государствам;

– структура органов защиты ГТ;

– порядок допуска должностных лиц и граждан к ГТ;

– ответственность за нарушение законодательства Российской Федерации о ГТ;

– порядок сертификации средств защиты информации.

Перечень сведений, составляющих государственную тайну, приводится в законе и конкретизируется указом Президента РФ «Об утверждении Перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. № 1203 (ред. от 28 февраля 2016 г.). Кроме того, указ определяет ведомства, ответственные за тот или иной вид сведений, он включает четыре раздела:

I. Сведения в военной области.

II. Сведения в области экономики, науки и техники.

III. Сведения в области внешней политики и экономики.

IV. Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, в области противодействия терроризму и обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.

Не вдаваясь в подробное описание перечня, нельзя не упомянуть того факта, что к государственной тайне относятся сведения:

– раскрывающие методы, способы или средства защиты информации, содержащей сведения, составляющие государственную тайну, планируемые и (или) проводимые мероприятия по защите информации от несанкционированного доступа, иностранных технических разведок и утечки по техническим каналам, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

– об организации или о фактическом состоянии защиты государственной тайны;

– раскрывающие методы, средства, организационные, технические или иные меры, направленные на обеспечение режима секретности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения [18].

Данные факты говорят о том, методы и способы защиты государственной тайны, а также используемые средства являются секретными.

Основными нормативными документами в области защиты государственной тайны являются:

– Закон РФ «О государственной тайне» от 21 июля 1993 г. № 5485-1 (ред. от 8 марта 2015 г.);

– указ Президента РФ «Об утверждении Перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. № 1203 (ред. от 5 июля 2017 г.);

– указ Президента РФ «Вопросы Межведомственной комиссии по защите государственной тайны» от 6 октября 2004 г. № 1286 (ред. от 11 августа 2014 г.);

– указ Президента РФ «Об утверждении состава Межведомственной комиссии по защите государственной тайны» от 10 октября 2016 г. № 535 (ред. от 16 мая 2017 г.);

– распоряжение Президента РФ «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне» от 16 апреля 2005 г. № 151-рп (ред. от 5 июля 2017 г.);

– постановление Правительства РФ «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. № 870 (ред. от 18 марта 2016 г.);

– постановление Правительства РФ «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» от 6 февраля 2010 г. № 63 (ред. от 29 декабря 2016 г.);

– постановление Правительства РФ «Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне» от 22 августа 1998 г. № 1003 (ред. от 18 марта 2016 г.).

Указом Президента от 6 марта 1997 г. № 188 был закреплен перечень сведений конфиденциального характера, таких как персональные данные, тайна судопроизводства, коммерческая тайна и т.д. В этом документе только прозвучали, но не были раскрыты другие понятия конфиденциальной информации, не являющейся государственной тайной. Указ Президента РФ от 6 марта 1997 г. № 188 (ред. от 13 июля 2015 г.) «Об утверждении Перечня сведений конфиденциального характера» включает семь пунктов [19]:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с федеральными законами «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» от 20 апреля 1995 г. № 45-ФЗ и «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» от 20 августа 2004 г. № 119-ФЗ, другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом «Об исполнительном производстве» от 2 октября 2007 г. № 229-ФЗ.

Согласно представленной схеме на рис. 2.2, определим поочередно виды конфиденциальной информации.

Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [20].

Статья 19 Федерального закона «О персональных данных» от 27 июля 2006 г. № 152-ФЗ (действующая редакция от 2июля 2021 г.) предписывает оператору применять меры по обеспечению безопасности персональных данных при их обработке, а именно: «оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных». При этом обеспечение безопасности персональных данных достигается:

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

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Нормативные правовые документы, регулирующие обращение персональных данных:

– Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ (действующая редакция от 2 июля 2021 г.);

– постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119;

– постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687;

– постановление Правительства РФ «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» от 6 июля 2008 г. № 512 (ред. от 27 декабря 2012 г.);

– постановление Правительства РФ «Об утверждении Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» от 21 марта 2012 г. № 211;

– распоряжение Правительства РФ «О плане подготовки проектов нормативных актов, необходимых для реализации Федерального закона «О персональных данных» от 15 августа 2007 г. №1055-р.

Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах [20].

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные, или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю. Имеются и соответствующие документы уполномоченных органов:

– приказ ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных

данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. № 21;

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 г.;

– приказ Роскомнадзора «Об утверждении образца формы уведомления об обработке персональных данных» (вместе с «Рекомендациями по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных») от 16 июля 2010 г. № 482 (ред. от 19 августа 2011 г.);

– разъяснения Роскомнадзора «О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки» (публикация 13 сентября 2013 г.)»;

– приказ ФСБ «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10 июля 2014 г. № 378;

– «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31 марта 2015 г.).

Законодательством определено четыре категории персональных данных, к которым предъявляются различные требования по их защите [20]:

1. Общедоступные персональные данные — персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных.

Статья 8 ФЗ-152 поясняет, какие источники являются общедоступными. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта

персональных данных либо по решению суда или иных уполномоченных государственных органов.

2. Специальные категории персональных данных — касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

3. Биометрические персональные данные — сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

4. Иные категории персональных данных — персональные данные не являющиеся общедоступными, специальными и биометрическими.

Коммерческая тайна — режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду [21].

Информация, составляющая коммерческую тайну, — сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений федерального закона «О коммерческой тайне».

Нормативные документы:

– Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ (ред. от 12 марта 2014 г.);

– «Гражданский кодекс Российской Федерации (часть вторая)» от 26 января 1996 г. № 14-ФЗ (ред. от 28 марта 2017 г.), ст. 727 «Конфиденциальность полученной сторонами информации»;

– «Гражданский кодекс Российской Федерации (часть четвертая)» от 18 декабря 2006 г. № 230-ФЗ (ред. от 1 июля 2017 г.), ст. 1465 «Секрет производства (ноу-хау)»;

– постановление Правительства РСФСР «О перечне сведений, которые не могут составлять коммерческую тайну» от 5 декабря 1991 г. № 35 (ред. от 3 октября 2002 г.).

Меры по охране конфиденциальности информации, составляющей коммерческую тайну принимаемые ее обладателем, должны включать в себя [21]:

1. Определение перечня информации, составляющей коммерческую тайну.

2. Ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.

3. Учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана.

4. Регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров.

5. Нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц — полное наименование и место нахождения, для индивидуальных предпринимателей — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

В законе (98-ФЗ) есть небольшой перечень сведений, которые не могут составлять коммерческую тайну, это сведения:

– содержащиеся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

– содержащиеся в документах, дающих право на осуществление предпринимательской деятельности;

– о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

– о 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 безопасности населения в целом;

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

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

– о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

– об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

– о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда

их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

– о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

– обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами;

– составляющие информацию о состоянии окружающей среды (экологическую информацию) [22].

Профессиональная тайна — сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и различными федеральными законами. Примерами таких тайн являются:

– тайна переписки, телефонных, телеграфных и иных сообщений, иными словами, «тайна связи» (ст. 63 Федерального закона «О связи» от 7 июля 2003 г. № 126-ФЗ);

– банковская тайна (ст. 26 Федерального закона «О банках и банковской деятельности» от 2 декабря 1990 г. № 395-1);

– налоговая тайна (ст. 102 Налогового кодекса РФ);

– тайна страхования (ст. 946 Гражданского кодекса РФ);

– адвокатская и нотариальная тайна (ст. 8 Федерального закона «Об адвокатской деятельности и адвокатуре Российской Федерации» от 31 мая 2002 г. № 63-ФЗ и ст. 5 «Основ законодательства Российской Федерации о нотариате» от 11 февраля 1993 г. № 4462-1);

– журналистская тайна (ст. 49 Федерального закона «О средствах массовой информации» от 27 декабря 1991 г. № 2124-1);

– аудиторская тайна (ст. 9 Федерального закона «Об аудиторской деятельности» от 30 декабря 2008 г. № 307-ФЗ);

– тайна следствия, дознания (ст. 161 Уголовно-процессуального кодекса РФ) и судопроизводства (ст. 194 ГПК, ст. 298, 341 УПК);

– врачебная тайна (ст. 13, 92 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» от 21 ноября 2011 г. № 323-ФЗ);

– тайна исповеди (ст. 3 Федерального закона «О свободе совести и о религиозных объединениях» от 26 сентября 1997 г. № 125-ФЗ);

– и др.

Служебная тайна — вид конфиденциальной информации, который до сих пор не определен на уровне федерального закона. Имеется только постановление Правительства РФ «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» от 3 ноября 1994 г. № 1233 (ред. от 6 августа 2020 г.).

К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также по-

ступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами [22].

Руководитель федерального органа исполнительной власти, уполномоченного органа управления использованием атомной энергии, уполномоченного органа по космической деятельности в пределах своей компетенции определяет категории должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения.

Должностные лица, принявшие решение об отнесении служебной информации к разряду ограниченного распространения, несут персональную ответственность за обоснованность принятого решения и за соблюдение ограничений. Не могут быть отнесены к служебной информации ограниченного распространения:

– акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

– сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

– описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

– порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;

– решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;

– сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;

– документы, накапливаемые в открытых фондах библиотек, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан;

– информация, содержащаяся в архивных документах архивных фондов (за исключением сведений и документов, доступ к которым ограничен законодательством Российской Федерации).

Имеется проект Федерального закона «О служебной тайне» № 124871-4 (внесен в Государственную Думу ФС РФ 24 декабря 2004 г., 5 апреля 2006 г. повторно внесен в Государственную Думу ФС РФ, 2 ноября 2011 г. отклонен Государственной Думой ФС РФ).

Есть нормативные документы уполномоченных органов:

1. Приказ ФСТЭК России «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11февраля 2013 г. № 17 (ред. от 15 февраля 2017 г.). В документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, со-

ставляющие государственную тайну, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в государственных информационных системах.

Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

– формирование требований к защите информации, содержащейся в информационной системе;

– разработка системы защиты информации информационной системы;

– внедрение системы защиты информации информационной системы;

– аттестация информационной системы по требованиям защиты информации и ввод ее в действие;

– обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

– обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

2. «Методический документ. Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11 февраля 2014 г.). Детализирует организационные и технические меры защиты информации, принимаемые в государственных информационных системах в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17, а также определяет содержание мер защиты информации и правила их реализации.

Справочная информация: «Перечень нормативных актов, относящих сведения к категории ограниченного доступа», подготовленный специалистами «КонсультантПлюс», доступен в сети по адресу: http://www.consultant.ru/document/cons_doc_LAW_93980.

Вопросы для самоконтроля

1. Каковы основные предметные направления ЗИ?

2. Что такое государственная тайна?

3. Основные нормативные акты в области защиты государственной тайны РФ.

4. Что называется коммерческой тайной?

5. Нормативные акты в области защиты коммерческой тайны РФ.

6. Что такое служебная тайна?

7. Что представляет собой профессиональная тайна?

8. Что такое персональные данные?

9. Каковы источники права на доступ к информации?

10. Каковы уровни доступа к информации с точки зрения законодательства?

11. Что такое информация ограниченного распространения?

12. Каковы виды доступа к информации?

13. В чем может заключаться ответственность за нарушение законодательства в информационной сфере?

14. Что не разрешается относить к информации ограниченного доступа?

15. Что понимается под конфиденциальной информацией?

16. Какие существуют виды тайны?

17. Какое назначение имеет перечень конфиденциальных сведений предприятия?

18. Каковы интересы РФ в информационной сфере?

19. Основные проблемы международного сотрудничества в сфере информационной безопасности.

20. Основные документы в области международной информационной безопасности.

3. ОРГАНИЗАЦИОННАЯ ЗАЩИТА ИНФОРМАЦИИ

3.1. Общие принципы организационного обеспечения

Организационная защита информации — составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационная защита информации — заключается в регламентации производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию. Основные направления организационной защиты представлены на рис. 3.1.

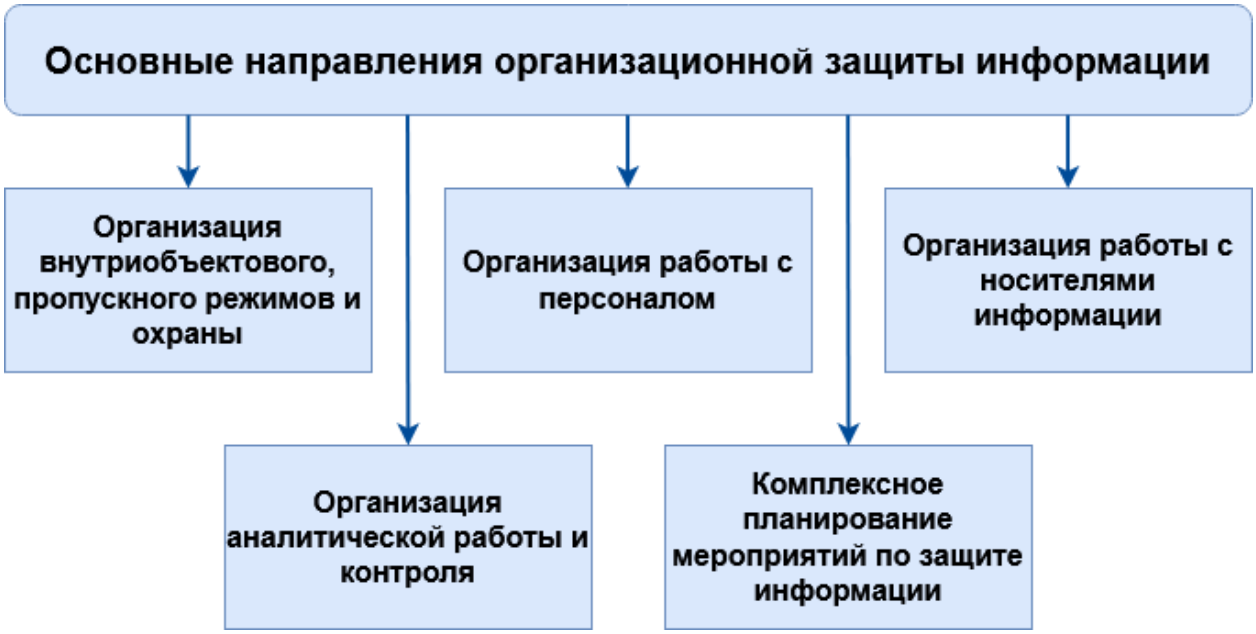


Рис. 3.1. Организационное обеспечение

Организационное обеспечение состоит из таких компонентов, как:

- подбор сотрудников и службы безопасности;
- оборудование служебных помещений;
- организация режимно-пропускной службы;
- организация хранения документов;
- организация системы делопроизводства;
- эксплуатация технических средств;
- создание охраняемых зон.

Организационные методы защиты информации включают меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе работы с информацией для обеспечения заданного уровня ее безопасности. Организационные методы защиты информации тесно связаны с правовым регулированием в области безопасности информации.

На организационном уровне должны решаться следующие задачи:

– организация работ по разработке системы защиты информации;
– ограничение доступа на объект и к ресурсам информации;
– разграничение доступа к ресурсам информации;
– планирование мероприятий;
– разработка документации;
– воспитание и обучение обслуживающего персонала и пользователей;
– сертификация средств защиты информации;
– лицензирование деятельности по защите информации;
– аттестация объектов защиты;
– совершенствование системы защиты информации;
– оценка эффективности функционирования системы защиты информации;
– контроль выполнения установленных правил работы в компьютерных системах.

Организационная защита информации — это комплекс направлений и методов управленческого, ограничительного и технологического характера, определяющих основы и содержание системы защиты, побуждающих персонал соблюдать правила защиты конфиденциальной информации. С помощью организационных методов возможно объединение на правовой основе технических, программных и криптографических средств защиты информации в единую комплексную систему.

Виды объектов защиты:

– руководящие работники и производственный персонал, владеющий информацией ограниченного пользования;
– финансовые средства и документы;
– материальные ценности;
– средства производства и производственные ресурсы;
– серийно выпускаемая продукция и опытные образцы;
– информационные ресурсы с ограниченным доступом, составляющие конфиденциальную информацию;
– средства и автоматизированные системы обработки информатизации;
– технические, программно-аппаратные средства защиты информации и различные системы охраны и защиты материальных и информационных ресурсов.

Организационную основу защиты информации в организации составляют мероприятия двух уровней:

1. Высший уровень (административный) — политика безопасности организации.

2. Низший уровень (процедурный) — регламентация действий сотрудников и структурных подразделений.

3.2. Административный уровень

К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые руководством организации. Административный уровень является основой практического построения комплексной системы, определяющей генеральное направление работ по обеспечению безопасности информации

Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения. Программа представляет официальную политику безопасности. Практические мероприятия включают следующие этапы:

1. Проведение анализа рисков.
2. Разработка политики безопасности.

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая (пере-) оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения уровень риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимые места), а также величины возможного ущерба.

Риск информационной безопасности (information security risk) — возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации (Примечание: он измеряется исходя из комбинации вероятности события и его последствия). Определение взято из ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности [23].

Управление рисками (или их анализ) рассматривается на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Для оценки рисков, кроме вероятности осуществления угрозы, важен размер ожидаемых потерь. В общем случае риск рассчитываются по следующей формуле:

$$E = P \cdot V,$$

где P — вероятностная оценка риска проявления угрозы; V — ущерб при реализации угрозы.

Данный расчет риска информационной безопасности проводится по каждому объекту защиты (носителю информации) для каждого информационного ресурса с учетом каждой идентифицированной угрозы. При этом величина риска рассчитывается с учетом нарушения любого из свойств информационной безопасности. Алгоритм представлен на рис. 3.2. На основании определения риска разрабатывается политика информационной безопасности.

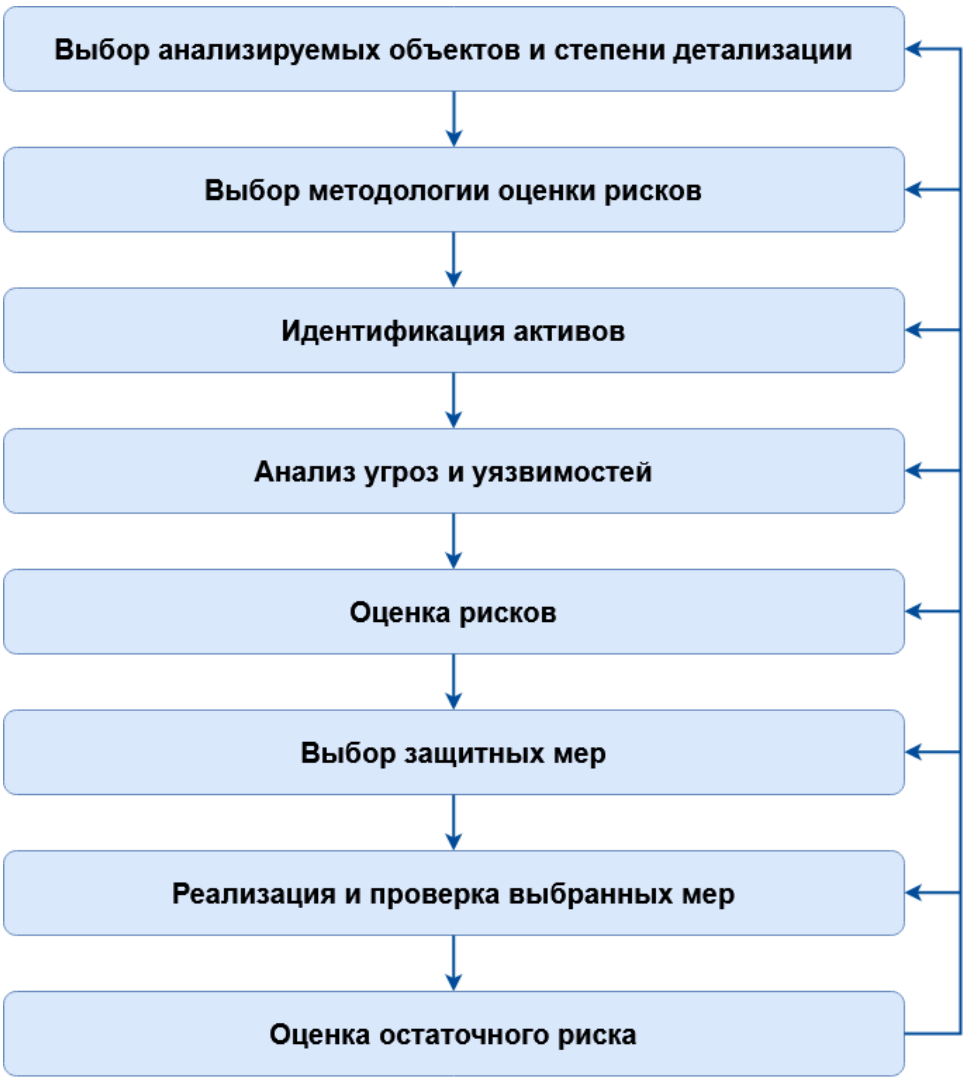


Рис. 3.2. Алгоритм анализа рисков

ГОСТ Р ИСО/МЭК 15408-1-2008 дает определение понятия «**политика безопасности организации**» — это одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности [24].

ГОСТ Р ИСО/МЭК 27002-2012 трактует данное понятие немного по-другому: **политика безопасности организации** — соответствие мер государственным законодательным и нормативным актам в области безопасности, ответственность руководства, координация работ подразделений, организацию контроля безопасности организации, планирование процессов безопасности, аудита безопасности [25].

Говоря проще, политика безопасности — это совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов. Политика безопасности отражает подход организации к защите своих информационных активов. Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации.

3.3. Процедурный уровень

Практические мероприятия включают следующие этапы:

– планирование обеспечения информационной безопасности;

– планирование действий в чрезвычайных ситуациях;

– подбор механизмов и средств обеспечения информационной безопасности.

На процедурном уровне можно выделить следующие классы мер:

– управление персоналом;

– физическая защита;

– поддержание работоспособности;

– реагирование на нарушения режима безопасности;

– планирование восстановительных работ.

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше — с составления описания должности. Уже на данном этапе желательно подключить к работе специалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существует два общих принципа, которые следует иметь в виду:

– разделение обязанностей;

– минимизация привилегий.

Принцип разделения обязанностей предписывает, как распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс. Например, можно искусственно создать дублирование действий, т.е. «двойное управление». Тогда критически важные действия смогут выполняться только вдвоем, что снижает вероятность ошибок и злоупотреблений.

Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно: уменьшить ущерб от случайных или умышленных некорректных действий.

Есть и другие особенности работы с персоналом:

– проведение усложненных аналитических процедур при приеме и увольнении сотрудников;

– документирование добровольного согласия лица не разглашать конфиденциальные сведения и соблюдать правила обеспечения безопасности информации;

– инструктирование и обучение сотрудников практическим действиям по защите информации;

– контроль за выполнением персоналом требований по защите информации, стимулирование ответственного отношения к сохранению конфиденциальных сведений;

– особенности увольнения сотрудников, владеющих конфиденциальной информацией.

Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как «непрерывность защиты в пространстве и времени». Направления физической защиты:

– физическое управление доступом;
– противопожарные меры;
– защита поддерживающей инфраструктуры;
– защита от перехвата данных.

Направления повседневной деятельности для поддержания работоспособности:

– поддержка пользователей;
– поддержка программного обеспечения;
– конфигурационное управление;
– резервное копирование;
– управление носителями;
– документирование;
– регламентные работы.

Реакция на нарушения режима безопасности преследует три главные цели:

– локализация инцидента и уменьшение наносимого вреда;
– выявление нарушителя;
– предупреждение повторных нарушений.

Процесс планирования восстановительных работ можно разделить на следующие этапы:

– выявление критически важных функций организации, установление приоритетов;
– идентификация ресурсов, необходимых для выполнения критически важных функций;
– определение перечня возможных аварий;
– разработка стратегии восстановительных работ;
– подготовка к реализации выбранной стратегии;
– проверка стратегии.

3.4. Организация службы безопасности предприятия

Организационная структура, численность и состав службы безопасности (СБ) определяются реальными потребностями предприятия и степенью конфиденциальности ее информации. В зависимости от масштабов и мощности организации ее безопасность и защита информации могут быть обеспечены по-разному: от абонементного обслуживания силами аутсорсинговых структур до развертывания собственной службы и системы безопасности с развитой структурой и штатной численностью. Организационная структура службы безопасности может быть следующей:

1. Отдел режима и охраны, в составе сектор режима и сектор охраны.
2. Специальный отдел.

3. Инженерно-техническая группа.

4. Группа безопасности внешней деятельности.

Функции сектора режима:

– организация и обеспечение пропускного и внутриобъектового режима: выдача пропусков (постоянных, временных, разовых), порядок посещения, учет посетителей;

– определение выделенных помещений, проведение их паспортизации, обеспечение их защиты совместно с группой инженерно-технической защиты информации;

– учет сотрудников, допущенных к работе с документами и материалами, содержащими сведения, составляющие конфиденциальную информацию.

Функции сектора охраны:

– реализует учет, контроль и наблюдение за охраняемыми зонами, помещениями, хранилищами;

– осуществляет прием под охрану и сдачу в эксплуатацию охраняемых помещений, проверяя при этом надежное срабатывание средств охраны, делая соответствующую запись в журнале приема и сдачи под охрану;

– принимает меры по ликвидации возможных пожаров и других аварийных ситуаций;

– осуществляет личную охрану руководящего состава.

Функции специального отдела:

– обработка поступающей и отправляемой корреспонденции, доставка ее по назначению;

– осуществление контроля за сроками исполнения документов;

– организация работы по регистрации, учету и хранению документальных материалов текущего пользования;

– разработка номенклатуры дел, осуществление контроля за правильным формированием дел в подразделениях и подготовкой материалов к своевременной сдаче в архив;

– разработка и внедрение предложений по совершенствованию системы делопроизводства;

– печатание и размножение секретных документов и документов с грифом.

Функции инженерно-технической группы:

– определение границ охраняемой (контролируемой) территории (зоны) с учетом возможностей технических средств, наблюдения за злоумышленниками;

– определение технических средств, используемых для передачи, приема и обработки конфиденциальной информации, в пределах охраняемой (контролируемой) территории (зоны);

– определение опасных технических средств с точки зрения возможности образования каналов утечки;

– локализация возможных каналов утечки информационно-организационными, организационно-техническими или техническими средствами и мероприятиями;

– организация наблюдения за возможным неконтролируемым излучением за счет ПЭМИН (побочных электромагнитных излучений и наводок);

– организация контроля наличия, проноса каких-либо предметов (устройств, средств, механизмов) в контролируемую зону, способных представлять собой технические средства несанкционированного получения конфиденциальной информации.

Функции группы безопасности внешней деятельности:

– изучение торгово-конъюнктурных ситуаций в пространстве деятельности учредителей, партнеров, клиентов и потенциально возможных конкурентов;

– ситуационный анализ текущего состояния финансово-торговой деятельности с точки зрения прогнозирования возможных последствий, могущих привести к неправомерным действиям со стороны конкурирующих организаций и предприятий;

– выявление платежеспособности юридических и физических лиц, их возможности по своевременному выполнению платежных обязательств;

– установление антагонистических конкурентов, выявление их методов ведения конкурентной борьбы и способов достижения своих целей;

– определение возможных направлений и характера злоумышленных действий со стороны специальных служб промышленного шпионажа против предприятия, его партнеров и клиентов.

3.5. Организация конфиденциального делопроизводства

Если в организации имеется информация ограниченного доступа, то целесообразно предпринимать меры по организации оборота документов, содержащих конфиденциальную информацию. Для этого необходимо выполнить следующие рекомендуемые мероприятия:

– разработать перечень конфиденциальной документированной информации;

– организовать учет бумажных и электронных носителей конфиденциальной информации;

– организовать учет на стадии проектов конфиденциальной документированной информации;

– организовать учет выполненных копировальных работ;

– организовать уничтожение конфиденциальных документов, в том числе черновиков, в машинках для уничтожения бумаг (шредерах) в присутствии нескольких человек и с проставлением соответствующих пометок в журналах уничтожения конфиденциальных документов;

– разработать регламент уничтожения конфиденциальных документов на машинных носителях, включающий организацию комиссии с соответствующими пометками об исполнении;

– запрет на вынос из контролируемой территории конфиденциальных документов;

– разработка разрешительной системы допуска и доступа к конфиденциальной информации.

Гриф ограничения доступа к документу — реквизит, свидетельствующий об особом характере информации документа и ограничивающий доступ к нему [26].

Гриф секретности — реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него [18].

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно» [18].

Нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» [21].

На документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования» [22].

В случаях, когда законодательством не установлена форма грифа (пометки) ограничения доступа к документам, содержащим конфиденциальную информацию, собственник или пользователь информации может принимать решения о применении какого-либо грифа. При этом чаще всего используется гриф «Конфиденциально».

3.6. Алгоритм разработки и внедрения комплексной системы защиты информации

Этап 1. На начальном этапе необходимо собрать и проанализировать информацию о предприятии. В этот этап входит процесс изучения информационных потоков. Необходимо определить, какая информация подлежит защите, какая является конфиденциальной, а какая открытой. Для этого производится категорирования информации. Составляются «перечни сведений», в том числе и составляющих конфиденциальную информацию предприятия.

Этап 2. На основе этого списка определяют и представляют на согласование необходимые к защите объекты (оборудование для обработки и обращения информации, программное обеспечение, коммуникации для передачи конфиденциальных данных, носители информации, персонал, допущенный к работе с использованием коммерческой и иной тайны).

Этап 3. Так как большинство предприятий чаще всего уже имеют некоторые средства защиты, то, с целью максимально эффективного использования имеющихся средств, необходимо собрать все информацию о них и заблаговременно оценить их роль в планирующейся КСЗИ. Анализируются существующие меры защиты соответствующих объектов, определяется степень их недостаточности, неэффективности, физического и морального износа.

Этап 4. Изучив и проанализировав текущее состояние предприятия необходимо определить возможных нарушителей ИБ и актуальные угрозы при помощи нормативных документов. Изучаются зафиксированные случаи попыток несанкционированного доступа к охраняемым информационным ресурсам и разглашения информации. На основе опыта предприятия, а также используя метод моделирования ситуаций, группа специалистов выявляет возможные пути несанкционированных действий по уничтожению информации, ее копированию, модификации, искажению, использованию и т. п. Угрозы ранжируются по степени значимости и классифицируются по видам воздействия. Строится модель угроз безопасности информации.

Этап 5. На основе собранных данных оценивается возможный ущерб предприятия от каждого вида угроз, который становится определяющим фактором для категорирования сведений в «Перечне» по степени важности, например для служебного пользования (3), важно (2), особо важно (1). Определяется риск нарушения информационной безопасности — мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы. На этом заканчивается этап сбора и анализа информации о предприятии и начинается этап проектирования КСЗИ.

Этап 6. На этапе проектирования важным шагом является определение требований нормативных документов к КСЗИ. К ним относятся федеральные законы в области ИБ, приказы ФСТЭК, ФСБ, постановления правительства, указы президента. Законодательство регламентирует минимальный (базовый) набор мер по защите информации (рис. 3.3). Далее необходимо определить меры, нейтрализующие актуальные угрозы. К ним относятся внедрение программно-аппаратных, инженерно-технических средств, а также разработка внутриорганизационной документации. Далее необходимо составить адаптивный набор мер, который включает в себя базовый набор и набор мер, нейтрализующий актуальные угроз.

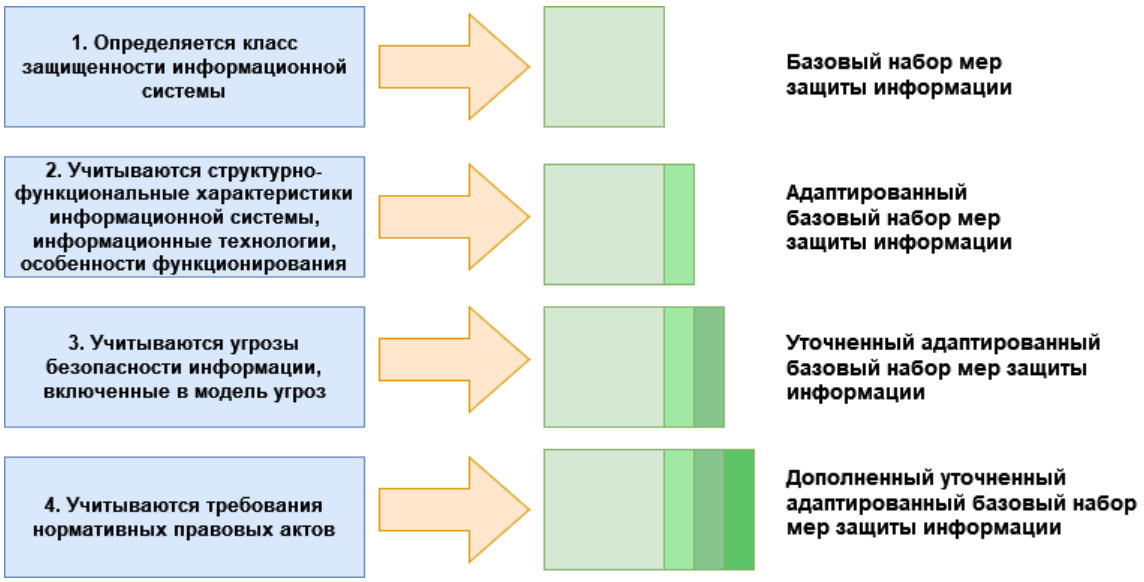


Рис. 3.3. Порядок действий по выбору мер защиты

Этап 7. Следующим шагом является выбор и внедрение средств защиты. Это должно быть комплексным процессом, так как необходимо заранее продумать всю систему так, чтобы средства дополняли друг друга и их функционал использовался на 100 %, так выполняется принцип превентивности.

Меры аппаратной и программной защиты (для компьютерного оборудования информационных систем и сетей). Включают в себя разные по принципу действия и по техническому исполнению устройства и программные средства, которые реализуют защиту от несанкционированного доступа к источникам информации.

Меры физической защиты. Включают в себя установление определенного режима деятельности, соблюдение которого обязательно для всех сотрудников, посетителей и клиентов. Это ограничение доступа, создание соответствующего пропускного режима, контроль за посетителями.

Меры технической защиты. Включают в себя защиту компьютерной техники, помещений и всех коммуникаций от устройств съема, и передачи информации, используя различные технические решения.

Этап 8. Проводится финансовая экспертиза затрат на предложенные меры защиты. Программа обеспечивается необходимыми кадровыми ресурсами. Приказами руководителя предприятия внедряются утвержденные меры защиты, выстраивается система комплексного обеспечения безопасности информации. Проводится постоянный контроль и мониторинг работоспособности системы. Корректируются внедренные меры защиты.

Алгоритм разработки и внедрения комплексной системы защиты информации является непрерывным, т.е. циклически замкнутым (рис. 3.4).

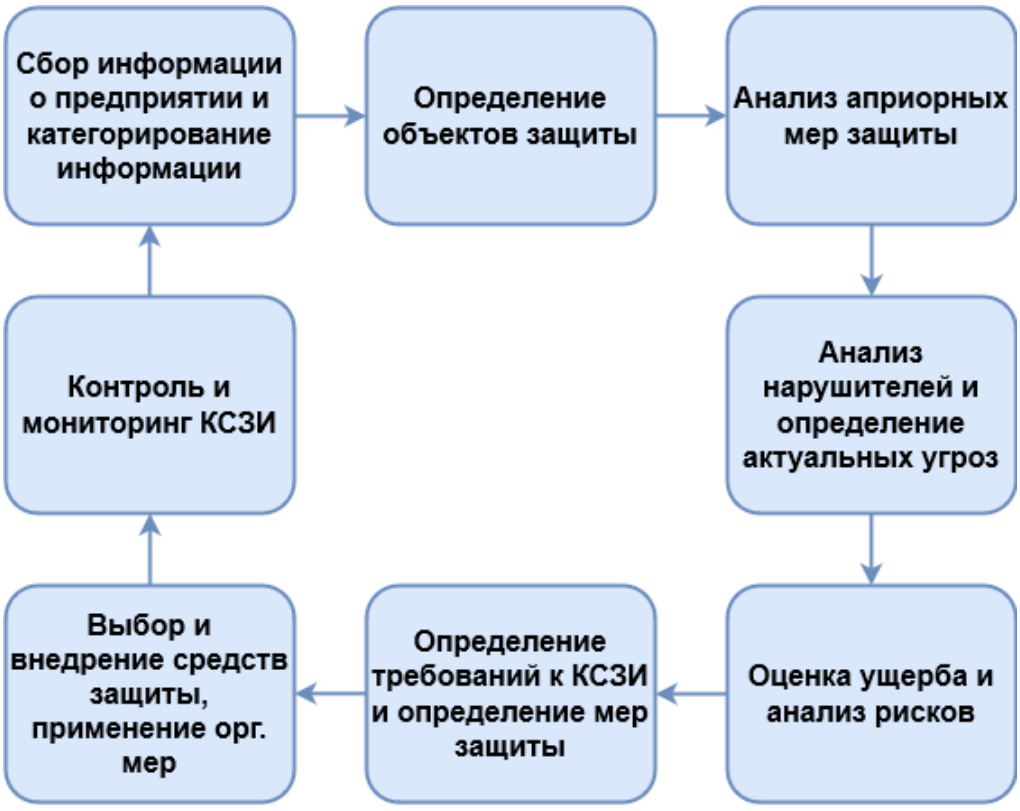


Рис. 3.4. Цикл создания КСЗИ

Вопросы для самоконтроля

1. Основные элементы организационной основы системы обеспечения информационной безопасности.
2. Общая характеристика организационных методов.
3. Требования к построению системы безопасности.
4. Основные направления организационной защиты.
5. Каким требованиям должна удвлетворять система защиты информации на предприятии?
6. Какие мероприятия проводятся на административном уровне организационной защиты информации?
7. Какие мероприятия проводятся на процедурном уровне организационной защиты информации?
8. Организационная структура службы безопасности.
9. Организация внутриобъектового режима на предприятии.
10. Организация работы с конфиденциальными документами.
11. Что такое гриф ограничения доступа к информации?
12. Какие грифы ограничения доступа к документу регламентированы нормативными документами?
13. Организационная структура службы.
14. Особенности увольнения сотрудников, владеющих конфиденциальной информацией.
15. Что такое политика безопасности, кто ее разрабатывает и где она применяется?
16. Каковы основные этапы проектирования системы защиты информации?
17. Основные принципы по управлению персоналом для снижения угроз информации.

4. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

4.1. Нормативная база

Если учитывать положения 149-ФЗ [3], то третьей составляющей применяемых мер по защите информации является техническое обеспечение. Это достаточно обширный перечень мер, который включает в себя внедрение различных технических средств для обеспечения целостности, доступности и (или) конфиденциальности информации. Разнообразие применяемых технических средств, в том числе и для автоматизированной обработки информации, различающихся объектами защиты, физическим и логическим принципом действия, требует условного выделения нескольких направлений технической защиты. В настоящем разделе будет рассматриваться программно-аппаратная защита информации, обрабатываемой с применением средств автоматизации. Далее отдельными направлениями будет рассмотрена криптографическая, антивирусная и инженерно-техническая защита.

Первым национальным стандартом безопасности компьютерных систем явился документ под названием Руководящий документ Гостехкомиссии России (от 30 марта 1992 г.) «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Данный документ имеет статус руководящего документа, однако он создавался на базе международного стандарта, берущего свои истоки из самого первого стандарта в области информационной безопасности «Оранжевой книги». Более подробно развитие стандартизации международной и отечественной в сфере защиты информации будет рассматриваться далее.

Руководящий документ (РД) распространяется на все действующие и проектируемые автоматизированные системы (АС) учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию. Согласно документу, устанавливается девять классов защищенности АС от несанкционированного доступа (НСД) к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, различающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС [27].

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса — 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса — 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфи-

денциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов — 1Д, 1Г, 1В, 1Б и 1А.

В общем случае комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

Второй документ, требующий внимания и принятый одновременно с первым, — это Руководящий документ Гостехкомиссии (от 30 марта 1992 г.) «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Показатели защищенности средств вычислительной техники (СВТ) применяются к общесистемным программным средствам и операционным системам (с учетом архитектуры ЭВМ). Требования к показателям реализуются с помощью программно-технических средств. Совокупность всех средств защиты составляет комплекс средств защиты (КСЗ). Документация КСЗ должна быть неотъемлемой частью конструкторской документации на СВТ [28].

Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс — седьмой, самый высокий — первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один — седьмой — класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность СВТ оказалась ниже уровня требований шестого класса. Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

Наконец, третий документ от той же даты, что и первые два, — это Руководящий документ Гостехкомиссии «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (от 30 марта 1992 г.). Документ устанавливает классификацию программного обеспечения (ПО) (как отечественного, так и импортного произ-

водства) средств защиты информации (СЗИ), в том числе и встроенных в общесистемное и прикладное ПО, по уровню контроля отсутствия в нем недекларированных возможностей.

Недекларированные возможности — функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации [29].

Реализацией недекларированных возможностей, в частности, являются программные закладки. Программные закладки — внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации. Функциональный объект — элемент программы, осуществляющий выполнение действий по реализации законченного фрагмента алгоритма программы. В качестве функциональных объектов могут выступать процедуры, функции, ветви, операторы и т.п. Классификация распространяется на ПО, предназначенное для защиты информации ограниченного доступа.

Устанавливается четыре уровня контроля отсутствия недекларированных возможностей. Каждый уровень характеризуется определенной минимальной совокупностью требований. Для ПО, используемого при защите информации, отнесенной к государственной тайне, должен быть обеспечен уровень контроля не ниже третьего. Самый высокий уровень контроля — первый, достаточен для ПО, используемого при защите информации с грифом «ОВ». Второй уровень контроля достаточен для ПО, используемого при защите информации с грифом «СС». Третий уровень контроля достаточен для ПО, используемого при защите информации с грифом «С». Самый низкий уровень контроля — четвертый, достаточен для ПО, используемого при защите конфиденциальной информации.

Рассмотренные документы устанавливают классификацию системного и прикладного программного обеспечения по обеспечению защиты информации и отсутствию недекларированных возможностей. Кроме этого, для целей сертификации средств защиты Гостехкомиссией были утверждены три части руководящего документа «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (утв. Гостехкомиссией России 19 июня 2002 г.).

Безопасность автоматизированной системы — это состояние АС, определяющее защищенность обрабатываемой информации и ресурсов от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность АС выполнять предписанные функции без нанесения неприемлемого ущерба объектам и субъектам информационных отношений [30]. Руководящий документ содержит систематизированный каталог требований к безопасности информационных технологий (ИТ), порядок и методические рекомендации по его использованию при задании требований, разработке, оценке и сертификации продуктов и систем информационных технологий по требованиям безопасности информации. Название и текст документа полностью соответствуют международному стандарту ГОСТ Р ИСО/МЭК

15408, и создание полной копии потребовалось только для того, чтобы закрепить юридический статус критериев оценки.

Есть еще один полезный документ для разработчиков системы защиты информации — это Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30 августа 2002 г. № 282. Требования имеют гриф «Для служебного пользования», однако по мотивированному запросу от организации их можно получить в бумажном виде. Документ устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты конфиденциальной информации. Там определены следующие основные вопросы защиты информации:

– организация работ по защите информации, в том числе при разработке и модернизации объектов информатизации и их систем защиты информации;

– состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;

– требования и рекомендации по защите речевой информации при осуществлении переговоров, в том числе с использованием технических средств;

– требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;

– порядок обеспечения защиты информации при эксплуатации объектов информатизации;

– особенности защиты информации при разработке и эксплуатации автоматизированных систем, использующих различные типы средств вычислительной техники и информационные технологии;

– порядок обеспечения защиты информации при взаимодействии абонентов с информационными сетями общего пользования [2].

Обобщив все изложенное в вышеперечисленных документах, можно выделить базовый состав мер защиты информации, содержащейся в информационной системе. Перечислим их и дадим краткую характеристику:

1. Идентификация и аутентификация субъектов доступа и объектов доступа — должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

2. Управление доступом субъектов доступа к объектам доступа — должно обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

3. Ограничение программной среды — должно обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) за-

пуска запрещенного к использованию в информационной системе программного обеспечения.

4. Защита машинных носителей информации — должна исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

5. Регистрация событий безопасности — должна обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

6. Антивирусная защита — должна обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

7. Обнаружение (предотвращение) вторжений — должно обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

8. Контроль (анализ) защищенности информации — должен обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

9. Обеспечение целостности информационной системы и информации — должно обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

10. Обеспечение доступности информации — должно обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

11. Защита среды виртуализации — должна исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

12. Защита технических средств — должна исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее — средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, обеспечивать защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

13. Защита информационной системы, ее средств, систем связи и передачи данных — должна обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

4.2. Технологии идентификации и аутентификации

Целью идентификации и аутентификации при доступе субъекта доступа к объекту доступа является опознавание субъекта доступа с необходимой уверенностью в том, что он является именно тем, за кого себя выдает. При этом степень достижения цели идентификации и аутентификации определяется уровнем доверия к результатам идентификации и аутентификации [31]. Базовая схема представлена на рис. 4.1.

Идентификация (Identification) — действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Это процедура распознавания пользователя по его идентификатору (имени), который используется при идентификации и однозначно определяет (указывает) соотнесенную с ними идентификационную информацию.

Аутентификация (Authentication) — действия по проверке подлинности субъекта доступа и (или) объекта доступа, а также по проверке принадлежности субъекту доступа и (или) объекту доступа предъявленного идентификатора доступа и аутентификационной информации.

Это процедура проверки подлинности заявленного пользователя, процесса или устройства. Аутентификация рассматривается применительно к конкретному субъекту доступа и (или) конкретному объекту доступа.

За процедурами идентификации и аутентификации следуют еще две процедуры, касающиеся уже непосредственно управления доступом.

Авторизация (Authorization) — процедура предоставления субъекту определенных полномочий и ресурсов в данной системе.

Авторизация устанавливает сферу действий субъекта и доступные ему ресурсы.

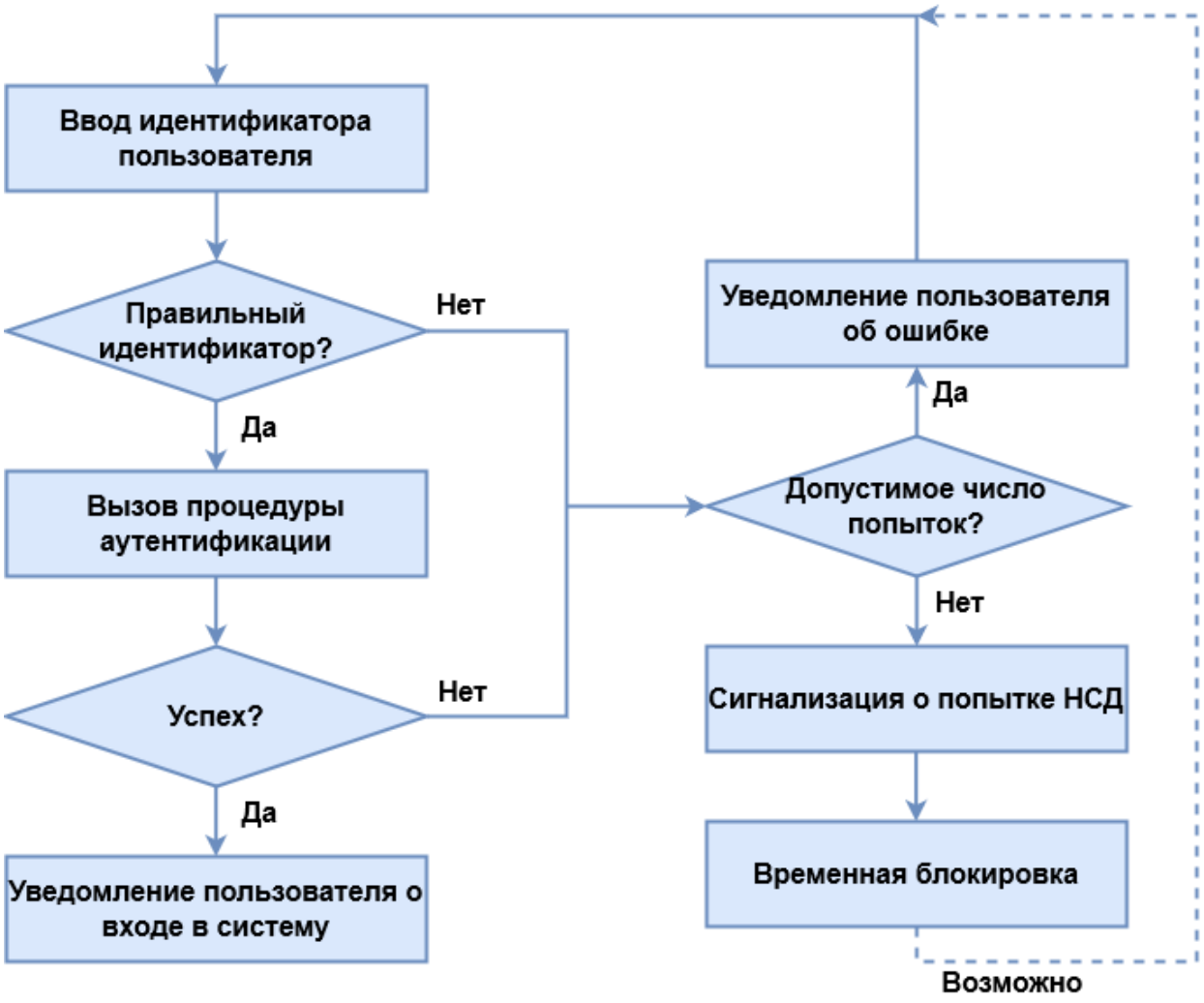


Рис. 4.1. Базовая схема идентификации и аутентификации

Администрирование (Accounting) — регистрация действий пользователя в сети, включая его попытки доступа к ресурсам.

Администрирование — учет действий пользователя в системе.

При защите каналов передачи данных должна выполняться взаимная аутентификация субъектов, т.е. взаимное подтверждение подлинности субъектов, связывающихся между собой по линиям связи. Взаимная аутентификация — обоюдная аутентификация, обеспечивающая каждому из участников процесса аутентификации (и субъекту доступа, и объекту доступа) уверенность в том, что другой участник процесса аутентификации является тем, за кого себя выдает.

В процессе аутентификации применяются следующие факторы:

1. Фактор знания: субъект доступа должен знать определенную информацию. При аутентификации с применением фактора знания может использоваться как аутентификационная информация, непосредственно известная пользователю, например пароль, графический пароль, изображение, так и информация, позволяющая получить доступ к аутентификационной информации, например одноразовый пароль или PIN-код.

2. Фактор владения: субъект доступа должен обладать определенным предметом, содержащим аутентификационную информацию. При аутентификации с применением фактора владения может использоваться, например, устройство аутентификации или механизм, приспособление, вещь, которые содержат аутентификационную информацию.

3. Биометрический фактор: субъекту доступа должен быть свойственен определенный признак (характеристика), информация о котором (которой) используется при аутентификации. Биометрический фактор применяется при аутентификации субъектов доступа, ассоциированных с физическими лицами. При аутентификации с применением биометрического фактора могут использоваться, например, биометрические данные физического лица или шаблон его поведения.

Примером использования фактора знания является парольная аутентификация (рис. 4.2). **Пароль** — конфиденциальная аутентификационная информация, обычно состоящая из строки знаков [31]. Пароль — это то, что знает пользователь и другой участник взаимодействия.

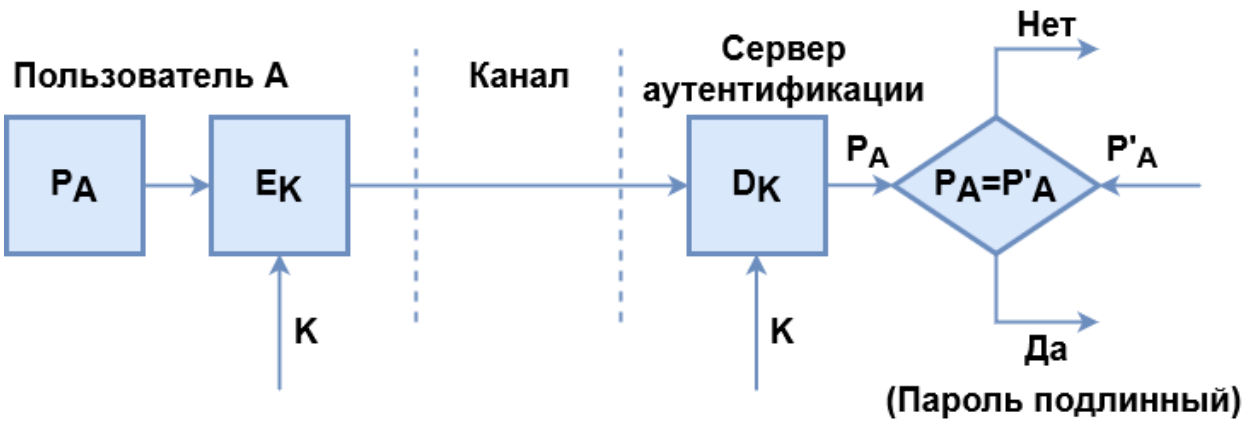


Рис. 4.2. Простая аутентификация с использованием пароля

Причинами широкого распространения парольной защиты является относительная простота реализации и традиционность. Относительная простота реализации заключается в том, что обычно не требует привлечения дополнительных аппаратных средств. Традиционность состоит в том, что механизмы парольной защиты являются привычными для большинства пользователей автоматизированных систем и не вызывают психологического отторжения, в отличие, например, от сканеров рисунка сетчатки глаза.

Однако стойкие пароли мало пригодны для использования человеком. Стойкость пароля возникает по мере его усложнения; но чем сложнее пароль, тем труднее его запомнить, и у пользователя появляется искушение записать неудобный пароль, что создает дополнительные каналы для его дискредитации.

Угрозы безопасности парольных систем:

1. За счет использования слабостей человеческого фактора (подглядывание, подслушивание, шантаж, угрозы, использование чужих учетных записей с разрешения их законных владельцев).

2. Путем подбора. При этом используются следующие методы:

– полный перебор: данный метод позволяет подобрать любой пароль вне зависимости от его сложности;

– подбор по словарю: значительная часть используемых на практике паролей представляет собой осмысленные слова или выражения;

– подбор с использованием сведений о пользователе: в подавляющем большинстве случаев в качестве пароля будет выбрана некая персональная информация, связанная с пользователем.

3. За счет использования недостатков реализации парольных систем (эксплуатируемые уязвимости сетевых сервисов, недекларированные возможности соответствующего программного или аппаратного обеспечения).

Рекомендации по практической реализации парольных систем:

1. Установление минимальной длины пароля — затрудняет реализацию подбора пароля путем полного перебора.

2. Увеличение мощности алфавита паролей — также усложняется полный перебор.

3. Проверка и отбраковка паролей по словарю. Данный механизм позволяет затруднить подбор паролей по словарю за счет отбраковки заведомо легко подбираемых паролей.

4. Установка максимального срока действия пароля. Срок действия пароля ограничивает промежуток времени, который злоумышленник может затратить на подбор пароля. Тем самым сокращение срока действия пароля уменьшает вероятность его успешного подбора.

5. Установка минимального срока действия пароля. Данный механизм предотвращает попытки пользователя незамедлительно сменить новый пароль на предыдущий.

6. Отбраковка по журналу истории паролей. Механизм предотвращает повторное использование паролей, возможно ранее скомпрометированных.

7. Ограничение числа попыток ввода пароля. Соответствующий механизм затрудняет интерактивный подбор паролей.

8. Принудительная смена пароля при первом входе пользователя в систему. В случае если первичную генерацию паролей для всех пользователь осуществляет администратор, пользователю может быть предложено сменить первоначальный пароль при первом же входе в систему, в этом случае новый пароль не будет известен администратору.

9. Задержка при вводе неправильного пароля. Механизм препятствует интерактивному подбору паролей.

10. Запрет на выбор пароля пользователем и автоматическая генерация пароля. Данный механизм позволяет гарантировать стойкость сгенерированных паролей — однако у пользователей возникнут проблемы с запоминанием паролей.

Наиболее надежным является динамический (одноразовый) пароль — это пароль, который после однократного применения никогда больше не используется. Суть схемы одноразовых паролей — использование различных паролей при каждом новом запросе на предоставление доступа. Динамический меха-

низм задания пароля — один из лучших способов защиты процесса аутентификации от угроз извне. Возможность использования для аутентификации одноразового пароля прекращается (исключается) при наступлении события получения доступа субъектом доступа или события отказа субъектом доступа и получения доступа, или события отказа объектом доступа в предоставлении доступа.

Примером использования фактора владения является предъявление пользователем **аппаратных систем аутентификации**. Под этим понимаются аппаратно-программные системы идентификации и аутентификации (СИА) или устройства ввода идентификационных признаков. В состав СИА входят аппаратные идентификаторы, устройства ввода-вывода (считыватели, контактные устройства, адаптеры, разъемы системной платы и др.) и соответствующее ПО. Классификация аппаратных систем идентификации и аутентификации представлена на рис. 4.3. Идентификаторы предназначены для хранения уникальных идентификационных признаков. Кроме этого, они могут хранить и обрабатывать конфиденциальные данные. Устройства ввода-вывода и ПО осуществляют обмен данными между идентификатором и защищаемой системой.

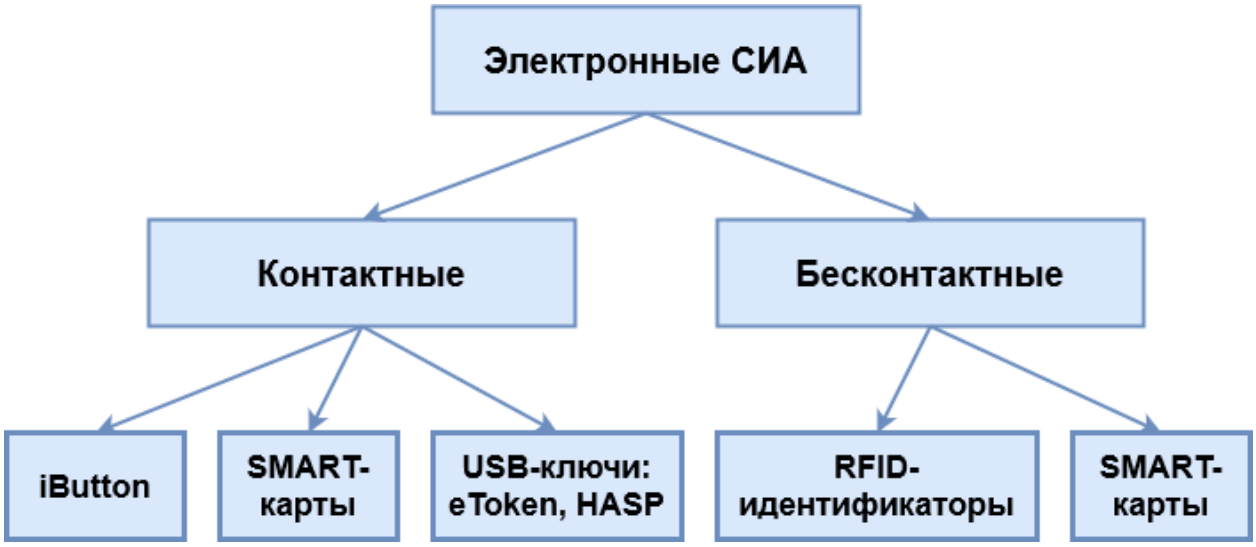


Рис. 4.3. Классификация электронных СИА

Распространенным методом аутентификации держателя пластиковой карты и смарт-карты является ввод секретного числа PIN-кода. Персональный идентификационный номер PIN (Personal Identification Number). Различают алгоритмические и неалгоритмические методы. Неалгоритмический способ проверки PIN-кода не требует применения специальных алгоритмов. Алгоритмический способ проверки PIN-кода заключается в том, что введенный клиентом PIN-код преобразуют по определенному алгоритму с использованием секретного ключа и затем сравнивают со значением PIN-кода, хранящимся в определенной форме на карте.

Биометрические факторы разделяются на статические и динамические методы. Статические методы биометрической аутентификации основываются

на физиологической (статической) характеристике человека, т.е. уникальной характеристике, данной ему от рождения и неотъемлемой от него. Динамические методы основаны на анализе особенностей поведения, т.е. характерных черт, подсознательно демонстрируемых человеком в процессе воспроизведения какого-либо обыденного действия.

Эффективность биометрической аутентификационной системы характеризуется двумя параметрами:

– коэффициентом ошибочных отказов FRR (false-reject rate);

– коэффициентом ошибочных подтверждений FAR (false-alarm rate).

Ошибочный отказ возникает, когда система не подтверждает личность законного пользователя (типичные значения FRR — порядка одной ошибки на 100). Ошибочное подтверждение происходит в случае подтверждения личности незаконного пользователя (типичные значения FAR — порядка одной ошибки на 10 000).

Биометрические факторы аутентификации:

– отпечаток пальца;
– геометрия руки;
– сетчатка глаза;
– радужная оболочка глаза;
– геометрия лица;
– рисунок вен;
– голосовая аутентификация;
– клавиатурный почерк;
– собственноручная подпись.

4.3. Управление доступом

Под политикой управления доступом (УД) понимается совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое (а иногда и достаточное) условие безопасности системы. Для строгого и однозначного толкования норм и правил политики управления доступом обычно дается ее формализованное описание в виде соответствующей модели.

Основная цель такого описания — это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Все существующие в настоящее время модели управления доступом основаны на следующих базовых представлениях:

– компьютерная система является совокупностью взаимодействующих сущностей — субъектов и объектов;

– все взаимодействия в системе моделируются установлением отношений определенного типа между субъектами и объектами;

– все операции между субъектами и объектами, контролируемые монитором взаимодействий, либо запрещаются, либо разрешаются в соответствии с правилами политики безопасности;

– политика безопасности задается в виде правил, определяющих все взаимодействия между субъектами и объектами;

– совокупность множеств субъектов, объектов и отношений между ними (установившихся взаимодействий) определяет состояние системы.

Основной элемент модели безопасности — это доказательство того, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние при соблюдении всех установленных правил и ограничений.

Политика управления доступом — совокупность правил, подлежащих реализации средством защиты информации и регламентирующих предоставление доступа между компонентами среды функционирования этого средства защиты информации [32].

В качестве компонента среды функционирования средства защиты информации, как правило, рассматривается объект или субъект доступа. При этом доступом между компонентами среды функционирования средства защиты информации является доступ субъекта доступа к субъекту или объекту доступа.

Существует четыре основных способа разграничения доступа субъектов к совместно используемым объектам:

– физический — субъекты обращаются к физически различным объектам (однотипным устройствам, наборам данных на разных носителях и т.д.);

– временной — субъекты получают доступ к объекту в различные промежутки времени;

– логический — субъекты получают доступ к объектам в рамках единой операционной среды, но под контролем средств разграничения доступа;

– криптографический — все объекты хранятся в зашифрованном виде, права доступа определяются знаниями ключа для расшифрования объекта.

На практике основными способами разграничения доступа являются логический и криптографический. Среди моделей политики управления доступом можно выделить два основных типа: дискреционные (произвольные), мандатные (нормативные). Есть также дополнение в виде ролевой модели. В основе этих моделей лежат, соответственно, дискреционное управление доступом (Discretionary Access Control — DAC), мандатное управление доступом (Mandatory Access Control — MAC) и ролевое управление доступом (Role-Based Access Control — RAC).

Дискреционное (произвольное, матричное, разграничительное) УД, дискреционный доступ (Discretionary Access Control — DAC) — разграничение доступа между поименованными субъектами и поименованными объектами. Он основан на задании владельцем объекта или другим полномочным лицом прав доступа других субъектов (пользователей) к этому объекту. Каждый объект объявляется собственностью соответствующего субъекта (владельца). Причем в конкретный момент времени у объекта может быть только один владелец, но с

течением времени они могут меняться. Владелец имеет все права доступа к объекту, и он определяет права доступа других субъектов к этому объекту.

В рамках этой модели система обработки информации представляется в виде совокупности активных сущностей — субъектов (множество S — пользователи, процессы и т.д.), которые осуществляют доступ к информации, пассивных сущностей — объектов (множество O — файлы, каталоги, процессы и т.д.), содержащих информацию, и конечного множества прав доступа $R = \{r_1, ..., r_n\}$, означающих полномочия на выполнение соответствующих действий (например, чтение (Read — R), запись (Write — W), выполнение (Execute — E), удаление (Delete — D), владение (Ownership — O) и т.д.).

Политика дискреционного управления доступом — это политика, при реализации которой задается матрица доступов, строки которой соответствуют субъектам доступа (учетным записям пользователей), столбцы — объектам или субъектам доступа, ячейки — множеству прав доступа соответствующего строке субъекта доступа к соответствующему столбцу объекту или другому субъекту доступа, субъект доступа может получить доступ к объекту или другому субъекту доступа только в случае, когда выполняется следующее правило: в ячейке матрицы доступов, соответствующей субъекту доступа и объекту или другому субъекту доступа, содержится соответствующее право доступа. Матрица доступов может быть задана эквивалентными способами: списки контроля доступа, списки привилегий, граф прав доступа или другие способы [32]. Пример матрицы доступа представлен в табл. 4.1.

Таблица 4.1

Пример матрицы доступа

		O_1	O_2	O_3	O_4	O_5
M =	S_1		R			
	S_2		RW	R		
	S_3					RW
	S_4	Own	Own	Own	Own	Own

Достоинства дискреционного УД:

– гибкость — позволяет независимо управлять правами для любой пары «субъект — объект»;

– не требует никаких сложных алгоритмов реализации.

Недостатки дискреционного УД:

– в реальных системах процедуры по обслуживанию и поддержанию в адекватном состоянии матриц доступа оказываются весьма трудоемкими;

– сложный контроль за распространением прав доступа;

– дискреционные модели уязвимы по отношению к атаке с помощью «троянского коня».

Пример утечки права. Пусть в начальном состоянии в системе имеются три субъекта: *o*, *s* и *t*; *s* обладает правом записи по отношению к *t*, а *t* обладает некоторым правом *a* (которое может представлять собой либо *r*, либо *w*) по от-

ношению к *o*. Субъект *s* может получить право доступа *a* по отношению к субъекту *o*. Схема представлена на рис. 4.4.

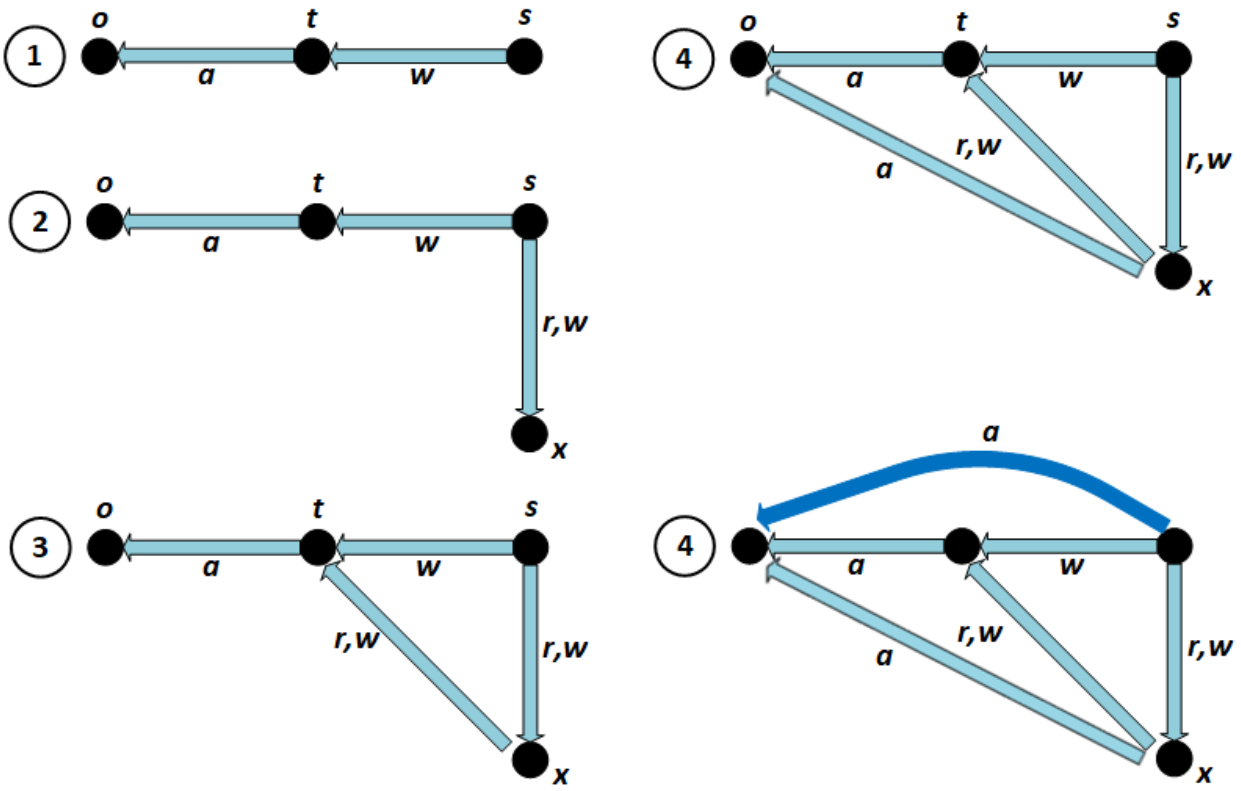


Рис. 4.4. Утечка права *a*

1. Система находится в начальном состоянии.
2. Субъект *s* создает новый субъект *x*, по отношению к которому автоматически получает права чтения и записи.
3. Субъект *s* передает субъекту *t* права чтения и записи по отношению к *x*.
4. Субъект *t* передает субъекту *x* право доступа *a* по отношению к *o*.
5. Субъект *s* получает от субъекта *x* право доступа *a* по отношению к *o*.

Мандатное (принудительное) управление доступом (Mandatory Access Control — MAC) — разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности. Оно основано на сопоставлении атрибутов безопасности субъекта (уровня допуска пользователя) и объекта (грифа секретности информации). Мандатная модель доступа основана на правилах конфиденциального документооборота, принятых в государственных и правительственных учреждениях многих стран. Основным положением данной модели, взятой из реальной жизни, является назначение всем участникам процесса обработки информации и документам, в которых она содержится, специальной метки, получившей название уровень безопасности (метка безопасности). Метка субъекта описывает его благонадежность, а метка объекта — степень закрытости, содержащейся в нем информации.

Политика мандатного управления доступом — это политика, при реализации которой задаются классификационные метки (уровни конфиденциальности, уровни доступа): каждому объекту доступа присваивается уровень конфиденциальности, каждому субъекту доступа присваивается уровень доступа (являющийся элементом множества уровней конфиденциальности), субъект доступа может получить доступ к объекту или другому субъекту доступа только в случае, когда выполняются следующие правила [32]:

– при получении доступа на чтение к объекту доступа уровень доступа субъекта доступа должен быть не ниже уровня конфиденциальности объекта доступа;

– при получении доступа на запись к объекту доступа уровень доступа субъекта доступа должен быть не выше уровня конфиденциальности объекта доступа;

– доступ субъекта доступа к объекту доступа или другому субъекту доступа не приводит к возникновению скрытого канала от объекта доступа к другому объекту доступа, первый из которых обладает не сравнимым или более высоким уровнем конфиденциальности, чем у второго объекта доступа.

Уровень конфиденциальности объекта доступа, как правило, отражает степень конфиденциальности, содержащейся в нем информации. Уровень доступа субъекта доступа, как правило, соответствует степени его полномочий по доступу к объектам доступа в зависимости от их уровней конфиденциальности. Классификационные метки могут быть несравнимы друг с другом, например при использовании для их задания неиерархических категорий. Уровни секретности, поддерживаемые системой, образуют множество, упорядоченное с помощью отношения доминирования. Такое множество может выглядеть следующим образом: совершенно секретно, секретно, конфиденциально, несекретно и т.д. Система в мандатной модели представляется в виде множеств субъектов S, объектов O, решетки уровней безопасности L (табл. 4.2) и матрицы доступа M (табл. 4.3).

Таблица 4.2

Решетка уровней безопасности

Уровень безопасности	Субъекты	Объекты	R	W
Совершенно секретно	S_1, S_2	O_5		
Секретно	S_3	O_1, O_2		
Конфиденциально	S_4	O_4		
Несекретно	S_5, S_6	O_3, O_6		

Таблица 4.3

Матрица доступа

	O_1	O_2	O_3	O_4	O_5	O_6
S_1	R	R	R	R	RW	R
S_2	R	R	R	R	RW	R
S_3	RW	RW	R	R	W	R
S_4	W	W	R	RW	W	R
S_5	W	W	RW	W	W	RW

S_6	W	W	RW	W	W	RW

Достоинства мандатного УД:

– экономия памяти, так как элементы матрицы доступа не хранятся, а динамически вычисляются при попытке доступа для конкретной пары «субъект — объект» на основе их меток;

– удобство корректировки базы данных защиты, т.е. модификации меток;

– принудительное УД хорошо согласуется с работой государственных, правительственных и военных организаций, так как переносит общепринятые и хорошо отработанные принципы обращения с бумажными секретами на современную основу работы с документами.

Недостатки мандатного УД:

– затруднено задание прав доступа конкретного субъекта к конкретному объекту;

– каждый субъект и объект должен быть помечен и при любых операциях с данными метки должны оставаться правильными. В особенности это относится к экспорту и импорту данных. Например, печатный документ должен открываться заголовком, содержащим текстовое и (или) графическое представление метки безопасности. Аналогично при передаче файла по каналу связи должна передаваться и ассоциированная с ним метка, причем в таком виде, чтобы удаленная система могла ее правильно трактовать, несмотря на возможные различия в уровнях секретности и наборе категорий.

Принципиальное различие между дискреционным и мандатным разграничением доступа состоит в следующем:

– при дискреционном разграничении доступа права на доступ к ресурсу для пользователей определяет его владелец;

– при мандатном разграничении доступа уровни секретности задаются извне, и владелец ресурса не может оказать на них влияния.

Сам термин «мандатное» является неудачным переводом слова mandatory — «обязательный». Тем самым мандатное разграничение доступа следует понимать как принудительное.

Ролевое управление доступом (Role-Based Access Control — RAC) — универсальная надстройка (каркас), применяемая с дискреционным и мандатным УД и предназначенная для упрощения функций администрирования систем с большим количеством субъектов и объектов. Между пользователями и их правами доступа к объектам появляются промежуточные сущности — роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права доступа к объекту, и, наоборот, несколько пользователей могут выступать в одной роли по отношению к одному объекту.

Политика ролевого управления доступом — это политика, при реализации которой задаются роли, каждая из которых представляет собой поименованное множество прав доступа к объектам доступа или субъектам доступа; каждому субъекту доступа ставится в соответствие множество разрешенных для него ролей; субъект доступа может получить доступ к объекту или другому

субъекту доступа только в случае, когда выполняется следующее правило: во множестве соответствующих субъекту доступа ролей имеется роль, во множестве прав доступа к объектам или субъектам доступа которой содержится соответствующее право доступа к объекту или субъекту доступа (рис. 4.5).

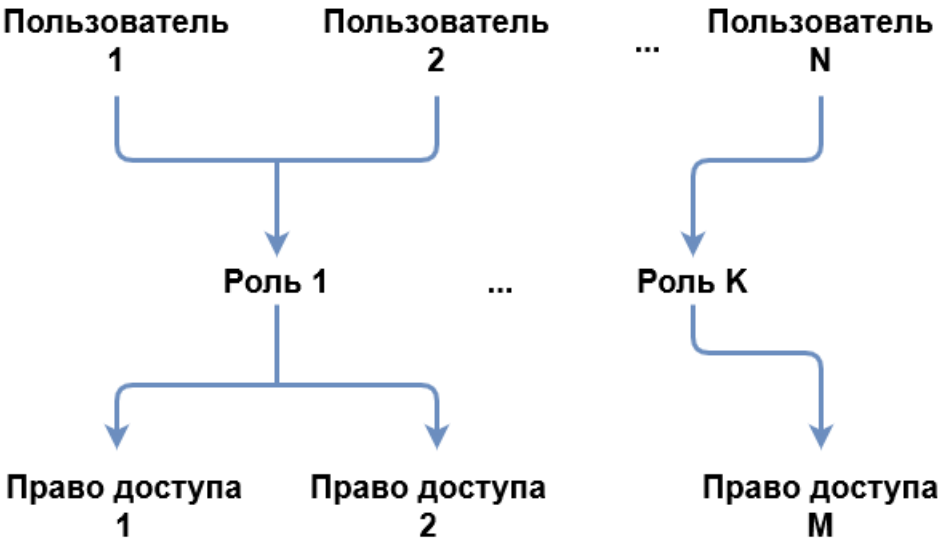


Рис. 4.5. Пользователи, объекты и роли

Можно сформировать иерархию ролей, начиная с минимума прав (и максимума пользователей), с постепенным уточнением состава пользователей и добавлением прав, в соответствии с принципом минимизации привилегий (рис. 4.6).

Рис. 4.6. Фрагмент иерархии ролей

Пример применения ролевой политики управления доступом представлен на рис. 4.7.

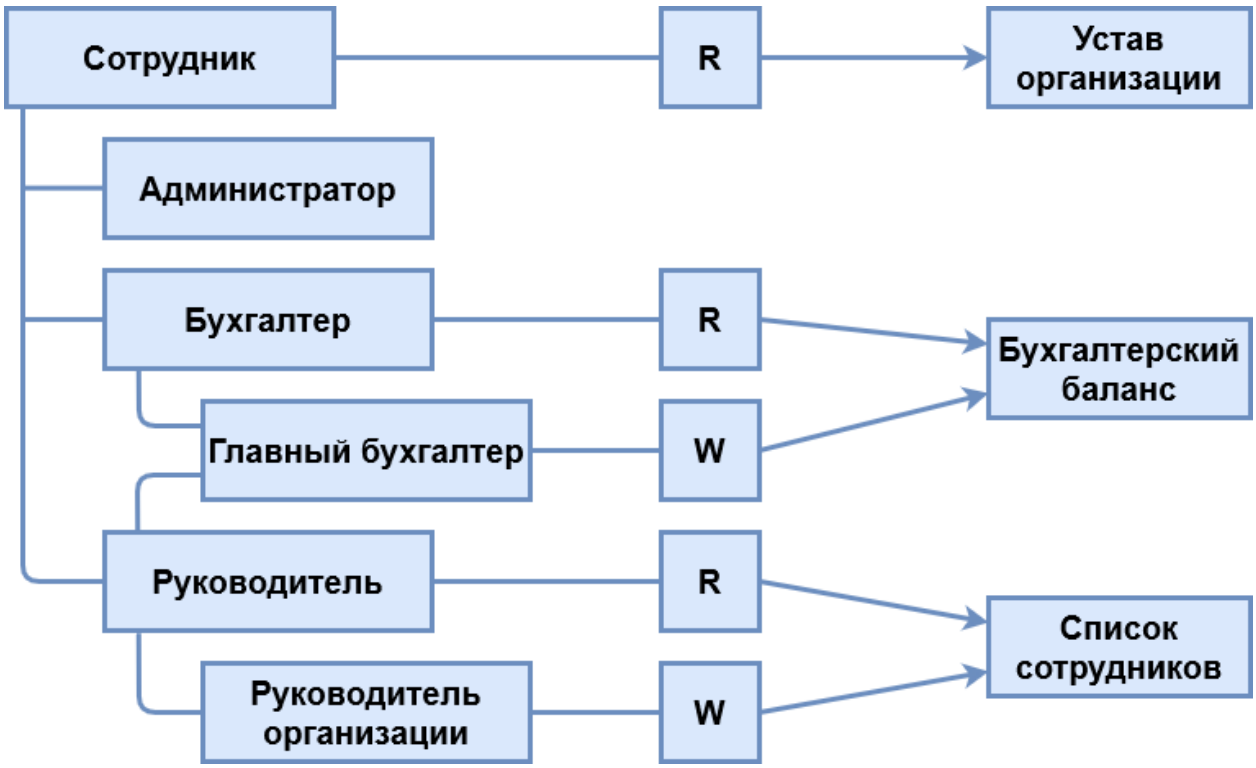


Рис. 4.7. Политика ролевого управления доступом

4.4. Обеспечение безопасности операционных систем

Значительная часть состава **организационных** и **технических мер** защиты информации, реализуемых в информационной системе, который рассматривался в разд. 4.1, может быть исполнена средствами операционной системы. Любая операционная система имеет ряд штатных средств, позволяющих активировать следующие меры:

– идентификацию и аутентификацию;
– управление доступом;
– ограничение программной среды;
– защиту машинных носителей информации;
– регистрацию событий безопасности;
– частично защиту информационной системы, ее средств, систем связи и передачи данных;
– частично и другие.

Угрозы безопасности операционных систем (ОС) существенно зависят от условий эксплуатации системы, от того, какая информация хранится и обрабатывается. Информационная безопасность ОС обеспечивается: программными средствами защиты информации, сетевым оборудованием, средствами физической защиты и организационными процедурами. Под безопасностью ОС понимают такое состояние ОС, при котором невозможно случайное или преднамеренное нарушение функционирования ОС, а также нарушение безопасности находящихся под управлением ОС ресурсов системы. Операционную систему называют защищенной, если она предусматривает средства защиты от основ-

ных классов угроз. Существуют два основных подхода к созданию защищенных ОС: фрагментарный и комплексный.

При фрагментарном подходе вначале организуется защита от одной угрозы, затем от другой и т.д.

При комплексном подходе защитные функции вносятся в ОС на этапе проектирования архитектуры ОС и являются ее неотъемлемой частью.

Организация эффективной и надежной защиты операционной системы невозможна с помощью одних только программно-аппаратных средств. Эти средства обязательно должны дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже самая надежная программно-аппаратная защита оборачивается фикцией. Необходим постоянный контроль корректности функционирования операционной системы, особенно ее подсистемы защиты. Такой контроль наиболее удобно организовать, если операционная система поддерживает регистрацию событий (event logging). В этом случае операционная система автоматически регистрирует в специальном журнале (или нескольких журналах) наиболее важные события, произошедшие в процессе функционирования системы.

Административные меры защиты включают:

1. Организацию и поддержание адекватной политики безопасности. Политика безопасности должна постоянно корректироваться, оперативно реагируя на изменения в конфигурации операционной системы, установку, удаление и изменение конфигурации прикладных программных продуктов и расширений операционной системы, попытки злоумышленников преодолеть защиту операционной системы и т.д.

2. Инструктирование пользователей операционной системы о необходимости соблюдения мер безопасности при работе с операционной системой и контроль за соблюдением этих мер.

3. Регулярное создание и обновление резервных копий программ и данных операционной системы.

4. Постоянный контроль изменений в конфигурационных данных и политике безопасности операционной системы. Информацию об этих изменениях целесообразно хранить на неэлектронных носителях информации для того, чтобы злоумышленнику, преодолевшему защиту операционной системы, было труднее замаскировать свои несанкционированные действия.

Однако достижение какого-то уровня защищенности операционной системы должно быть обосновано как минимум наличием угроз. Чем лучше операционная система защищена, тем труднее с ней работать пользователям и администраторам. Это обусловлено рядом факторов:

1. Система защиты не всегда способна определить, является ли некоторое действие пользователя злонамеренным. Поэтому система защиты либо не пресекает некоторые виды несанкционированного доступа, либо запрещает некоторые вполне легальные действия пользователей. Например, если некоторому пользователю запрещено создавать файлы на жестком диске, этот пользователь не сможет запустить ни одну программу, которой для нормального функционирования необходимо создавать временные файлы. Просто в данной политике

безопасности класс несанкционированных действий настолько широк, что это препятствует нормальной работе пользователей с операционной системой.

2. Любая система, в которой предусмотрены функции защиты информации, требует от администраторов определенных усилий, направленных на поддержание адекватной политики безопасности. Чем больше в операционной системе защитных функций, тем больше времени и средств нужно тратить на поддержание защиты.

3. Подсистема защиты операционной системы, как и любой другой программный пакет, потребляет аппаратные ресурсы компьютера. В отдельных случаях подсистема защиты операционной системы может потреблять более половины аппаратных ресурсов компьютера.

4. Поддержание слишком жесткой политики безопасности может негативно сказаться на надежности функционирования операционной системы. Если запретить псевдопользователю SISTEM, от имени которого выполняются системные процессы, доступ к исполняемым файлам системных процессов, операционная система, как и следовало ожидать, не сможет загрузиться.

При определении адекватной политики безопасности не следует пытаться достигнуть максимально возможного уровня защищенности операционной системы. Оптимальная адекватная политика безопасности — это такая политика безопасности, которая не только не позволяет злоумышленникам выполнять несанкционированные действия, но и не приводит к вышеописанным негативным эффектам. Не существует единой адекватной политики безопасности на все случаи жизни. То, какая политика безопасности будет адекватной, определяется не только архитектурой операционной системы, но и ее конфигурацией, установленными прикладными программами и т.д.

Большинство современных операционных систем достаточно универсальны и могут применяться для решения самых различных задач. Угрозы безопасности для всех применений операционной системы совершенно различны, и, следовательно, адекватная политика безопасности в каждом случае будет своя.

Для оценки защищенности операционных систем используется методический документ «Требования безопасности информации к операционным системам» (утв. ФСТЭК), которые вступили в силу с 1 июня 2017 г. Требования применяются к операционным системам, используемым в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, и иной информации ограниченного доступа при ее обработке в информационных системах (автоматизированных системах управления). В соответствии с Требованиями выделяются следующие типы операционных систем [33]:

– операционная система общего назначения (тип «А») — операционная система, предназначенная для функционирования на средствах вычислительной техники общего назначения (автоматизированные рабочие места, серверы, смартфоны, планшеты, телефоны и иные);

– встраиваемая операционная система (тип «Б») — операционная система, встроенная (прошитая) в специализированные технические устройства, предназначенные для решения заранее определенного набора задач;

– операционная система реального времени (тип «В») — операционная система, предназначенная для обеспечения реагирования на события в рамках заданных временных ограничений при заданном уровне функциональности.

Для дифференциации требований к функциям безопасности операционных систем выделяются шесть классов защиты операционных систем. Самый низкий класс — 6-й, самый высокий — 1-й. Операционные системы, соответствующие 6-му классу защиты, применяются в государственных информационных системах 3-го и 4-го классов защищенности, в автоматизированных системах управления производственными и технологическими процессами 3-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3-го и 4-го уровней защищенности персональных данных. Операционные системы, соответствующие 5-му классу защиты, применяются в государственных информационных системах 2-го класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2-го уровня защищенности персональных данных. Операционные системы, соответствующие 4-му классу защиты, применяются в государственных информационных системах 1-го класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1-го уровня защищенности персональных данных, в информационных системах общего пользования II класса.

Операционные системы, соответствующие 1, 2 и 3-му классам защиты, применяются в информационных (автоматизированных) системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

В настоящее время к защищенным ОС семейства Windows, имеющим сертификат ФСБ, можно отнести клиентские версии [34]:

– Microsoft Windows 7 Professional Service Pack 1;
– Microsoft Windows 7 Enterprise Service Pack 1;
– Microsoft Windows 7 Ultimate Service Pack 1;
– Microsoft Windows 8.1 Enterprise 32/64-bit;
– Microsoft Windows 10 Pro 32/64-bit;
– Microsoft Windows 10 Enterprise 32/64-bit.

Со встроенными и дополнительно интегрируемыми механизмами обеспечения безопасности, реализуемыми средством защиты информации Secure Pack Rus версия 3.0.

Серверные операционные системы:

– Microsoft Windows Server 2012 R2 VL Standard/Datacenter Service Pack 1 64-bit;

– Microsoft Windows Server 2012 VL Standard/Datacenter Service Pack 1 64-bit;

– Microsoft Windows Server 2016 R2 VL Standard/Datacenter;

– Microsoft Windows Server 2016 VL Standard/Datacenter.

Также при наличии встроенных и дополнительно интегрируемых механизмов обеспечения безопасности, реализуемых средством защиты информации Secure Pack Rus версия 3.0. Secure Pack Rus — средство защиты информации. Secure Pack Rus версия 3.0 (СЗИ SPR 3.0) является сервисным пакетом для операционных систем семейства Microsoft Windows и позволяет обеспечить выполнение требований ФСБ России по защите конфиденциальной информации по классу АК2 и АК3 (разработчик ООО «СиЭйЭн»). Эти же версии операционных систем имеют также сертификат ФСТЭК [35].

Кроме продуктов компании Microsoft к защищенным ОС с сертификатом ФСБ относятся:

– защищенная операционная система QP ОС («Криптософт»);

– Astra Linux Special Edition (версия 1.2);

– Astra Linux Special Edition (версия 1.4) («Русские базовые информационные технологии»);

– защищенная операционная система «Синтез» (Red Hat);

– защищенная мобильная операционная система общего назначения на базе Sailfish Mobile OS (Jolla, Открытая мобильная платформа).

Операционные системы, имеющие сертификат ФСТЭК, дополнительно к системам Windows [35]:

– доверенная операционная система «Циркон 10С» (на базе ОС Solaris 10 Update 4 с установленным Solaris Trusted Extensions);

– операционная система «Циркон 36К» (на базе ОС CentOS GNU/Linux 6.5);

– операционная система «Атликс 2» и «Атликс-3» (ядро Linux версии 2.6.32, на базе CentOS Linux);

– операционная система «Альт Линукс СПТ 6.0»;

– операционная система специального назначения Astra Linux Special Edition;

– операционная система SUSE Linux EnterpriseServer 11 ServicePack 1;

– операционная система типового дистрибутива «Автоматизированная информационная система ФССП» (Гослинукс);

– операционная система Red Hat Enterprise Linux Server 5.3 и Red Hat Enterprise Linux Advanced Server release 4 (Nahant Update 4);

– операционная система IBM AIX 6.1 и IBM AIX 7 с компонентом IBM Virtual I/O Server v.2 (UNIX-подобная операционная система);

– операционная система РОСА SX «ХРОМ» 1.0 и РОСА SX «КОБАЛЬТ» 1.0;

– операционная система CentOS 5.5;

– операционная система «Операционная система «Oracle Enterprise Linux 5 Update 5»;

– серверная операционная система с интегрированными серверными службами МСВ «Сфера 6.3 Сервер»;

– клиентская операционная система с интегрированными пользовательскими приложениями МСВ «Сфера 6.3 АРМ»;

– защищенная операционная система реального времени «QNX» КПДА.00002-01;

– защищенная операционная система реального времени «Нейтрино»;

– операционная система с открытым программным кодом «Синергия»;

– операционная система Samsung Tizen 2.x;

– операционная система EMIAS OS 1.0 автоматизированной информационной системы города Москвы «Единая медицинская информационно-аналитическая система города Москвы» (на платформе ОС openSuSe 42.3, пятого класса защиты);

– операционная система «РЕД ОС» (операционная система на основе ядра Linux);

– операционная система общего назначения «Стрелец» (ядро Linux);

– операционная система общего назначения (ОСОН) «Основа» (на базе ядра Linux, АО «НППКТ»);

– защищенная операционная система «Арамид» для супер-ЭВМ (второго класса защиты, ядро Linux);

– операционная система «Аврора» (новая версия Sailfish Mobile OS RUS).

4.5. Технологии межсетевого экранирования

Подсистема защиты внешнего периметра автоматизированной системы обычно включает в себя два основных механизма: средства межсетевого экранирования и средства обнаружения вторжений. Решая родственные задачи, эти механизмы часто реализуются в рамках одного продукта и функционируют в качестве единого целого. В то же время каждый из механизмов является самодостаточным и заслуживает отдельного рассмотрения.

Межсетевой экран (МЭ) — это специализированный комплекс межсетевой защиты, называемый также брандмауэром или системой firewall. МЭ позволяет разделить общую сеть на две части (или более) и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Типовая схема подключения представлена на рис. 4.8.

Задачи межсетевого экрана:

– ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи, хакер и даже сотрудники самой компании, пытающиеся получить доступ к ресурсам, защищаемых МЭ;

– разграничение доступа пользователей защищаемой сети к внешним ресурсам, т.е. регулирование доступа к серверам, не требующимся для выполнения служебных обязанностей.

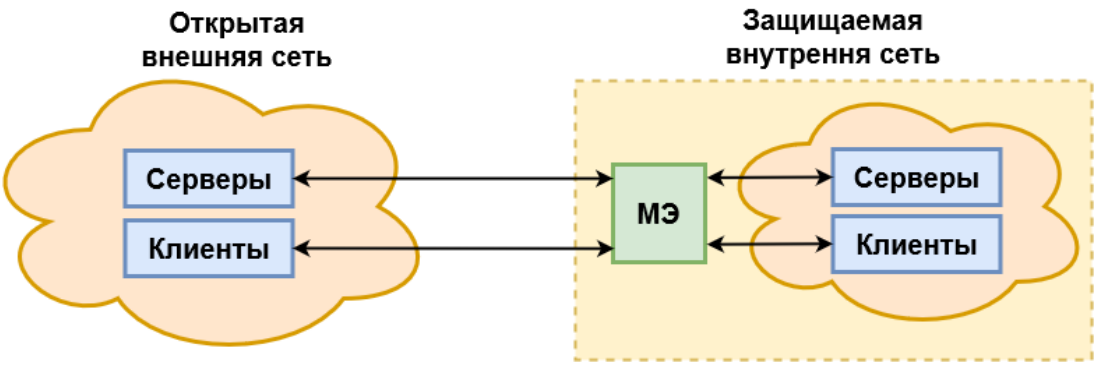


Рис. 4.8. Типовая схема подключения межсетевого экрана

Межсетевые экраны выполняют две основные функции: фильтрации трафика и посредничества. Естественно, любой брандмауэр может быть оснащен и дополнительным функционалом.

Фильтрация трафика состоит в выборочном пропускании данных через экран, возможно, с выполнением некоторых преобразований. Фильтрация осуществляется на основе набора предварительно загруженных в МЭ правил, соответствующих принятой политике безопасности. Поэтому МЭ удобно представлять как последовательность фильтров, обрабатывающих информационный поток. Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем:

– анализа информации по заданным в интерпретируемых правилах критериям, например по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена;

– принятия на основе интерпретируемых правил одного из следующих решений:

- не пропустить данные;
- обработать данные от имени получателя и возвратить результат отправителю;
- передать данные на следующий фильтр для продолжения анализа;
- пропустить данные, игнорируя следующие фильтры (рис. 4.9).

Функции посредничества осуществляются с помощью специальных программ, называемых экранирующими агентами или программами-посредниками. Эти программы являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетью. При необходимости доступа из внутренней сети во внешнюю сеть или наоборот вначале должно быть установлено логическое соединение с программой-посредником, функционирующей на компьютере с МЭ. Программа-посредник проверяет допустимость запрошенного межсетевого взаимодействия и при его разрешении сама устанавливает отдельное соединение с требуемым компьютером. Далее обмен информацией между компьютерами внутренней и внешней сети осу-

ществляется через программного посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять другие защитные функции.

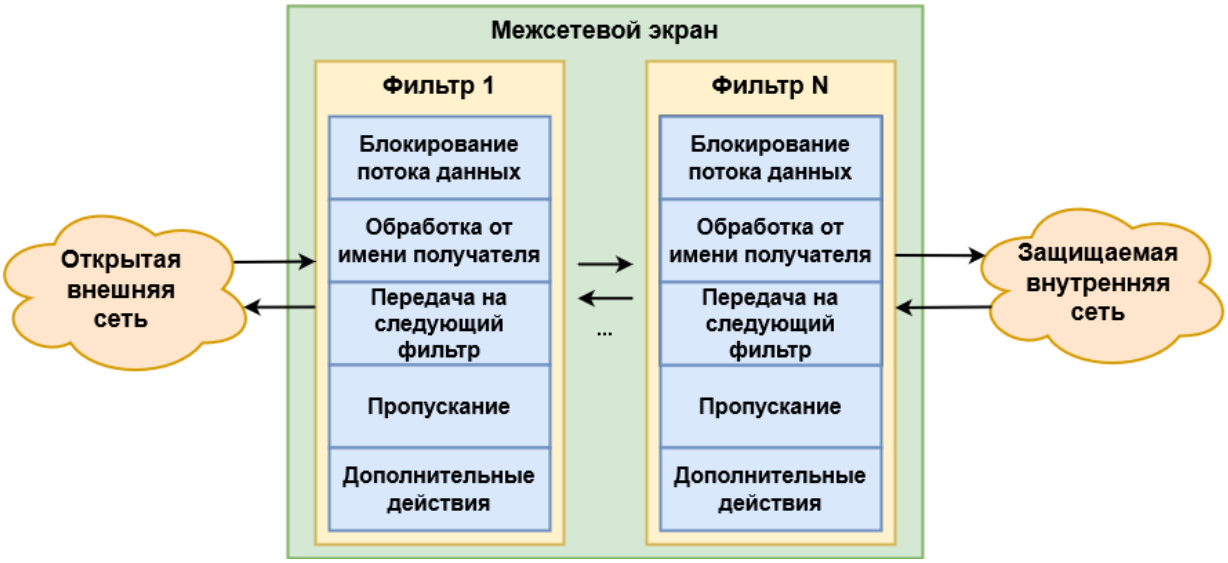
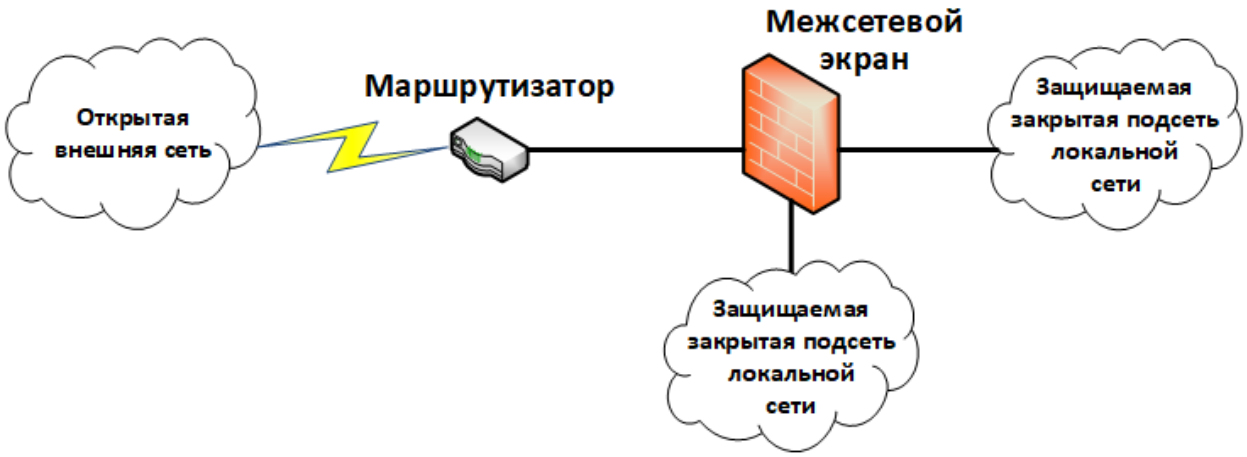


Рис. 4.9. Фильтрация трафика

Разделение общей сети на части называется сегментированием и может осуществляться разными способами. Наиболее простые варианты показаны на рис. 4.10 (а, б).

а)



б)

Рис. 4.10. Варианты сегментирования сети

Особенностью функционирования МЭ является то, что они поддерживают безопасность межсетевого взаимодействия на различных уровнях модели OSI (рис. 4.11). При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Поэтому комплексный МЭ удобно представить в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI. Чаще всего комплексный экран функционирует на сетевом, сеансовом и прикладном уровнях эталонной модели.

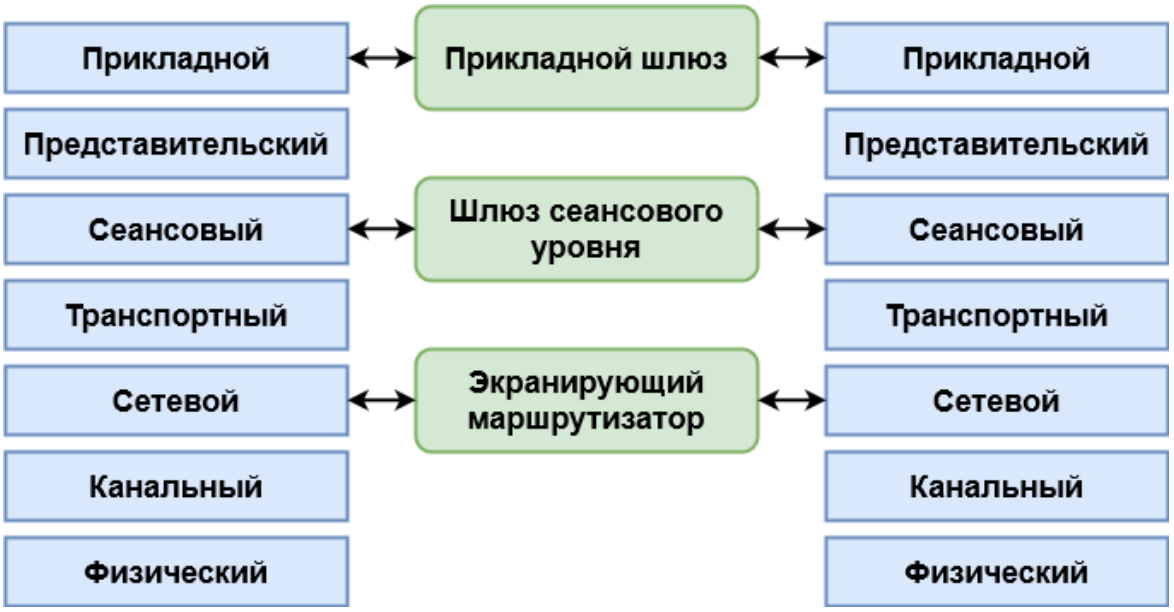


Рис. 4.11. Функционирование МЭ на различных уровнях OSI

Пакетные фильтры (packet filter) — это одни из первых и самые распространенные межсетевые экраны, которые функционируют на третьем, сетевом уровне и принимают решение о разрешении прохождения трафика в сеть на основании информации, находящейся в заголовке пакета (рис. 4.12). По-другому такие межсетевые экраны называют экранирующими маршрутизаторами (рис. 4.13).

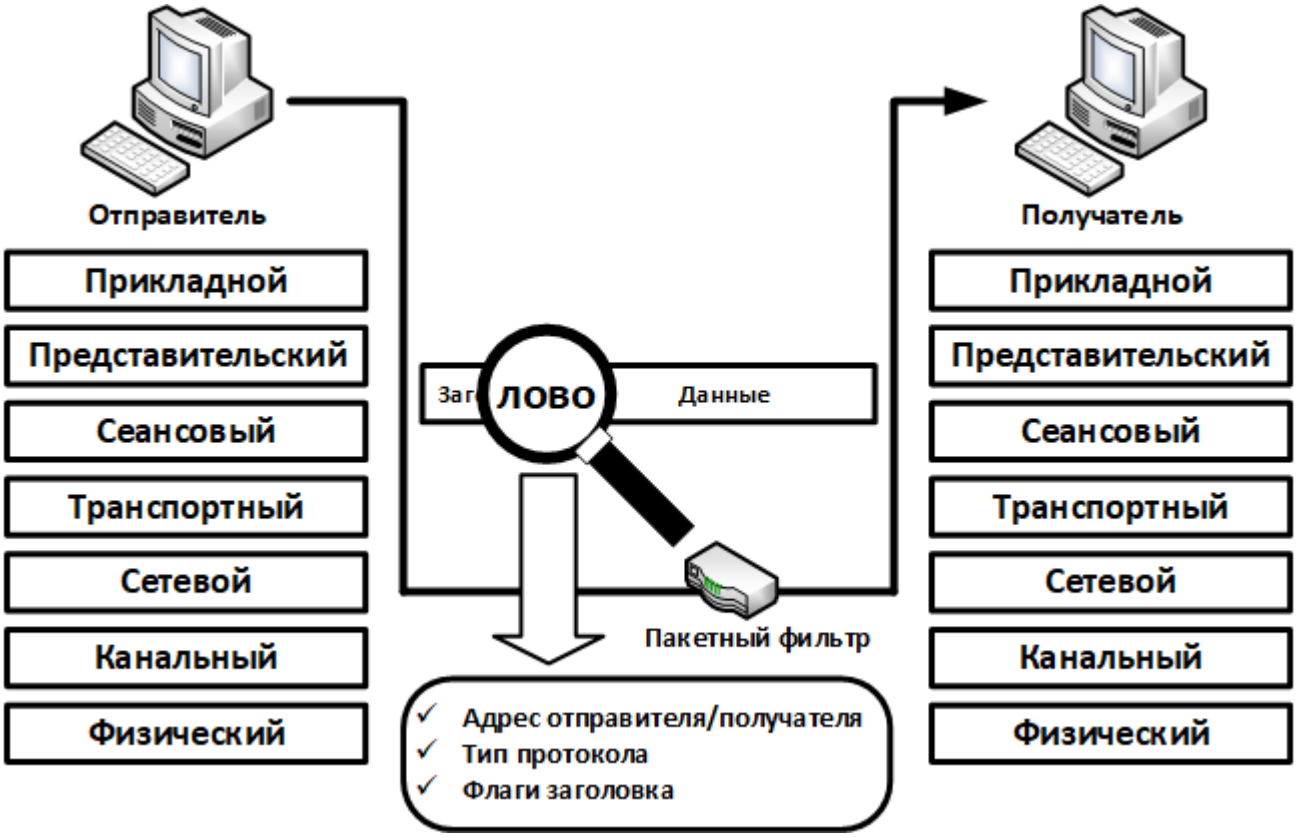


Рис. 4.12. Пакетные фильтры

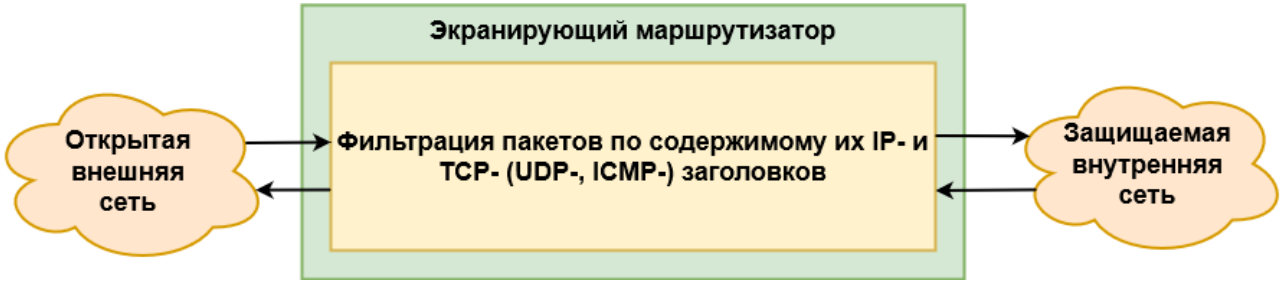


Рис. 4.13. Фильтрация пакетов экранирующим маршрутизатором

Шлюз сеансового уровня — исключает прямое взаимодействие двух узлов, выступая в качестве так называемого посредника (proxy), который перехватывает все запросы одного узла на доступ к другому и, после проверки допустимости таких запросов, устанавливает соединение. После этого шлюз сеансового уровня просто копирует пакеты, передаваемые в рамках одной сессии, между двумя узлами, не осуществляя дополнительной фильтрации. Как только авторизованное соединение установлено, шлюз помещает в специальную таблицу соединений соответствующую информацию (адреса отправителя и получателя, состояние соединения, информация о номере последовательности и т.д.). Как только сеанс связи завершается, запись о нем удаляется из этой таблицы. Все последующие пакеты, которые могут быть сформированы злоумышленником и «как бы относятся» к уже завершенному соединению, отбрасываются (рис. 4.14).

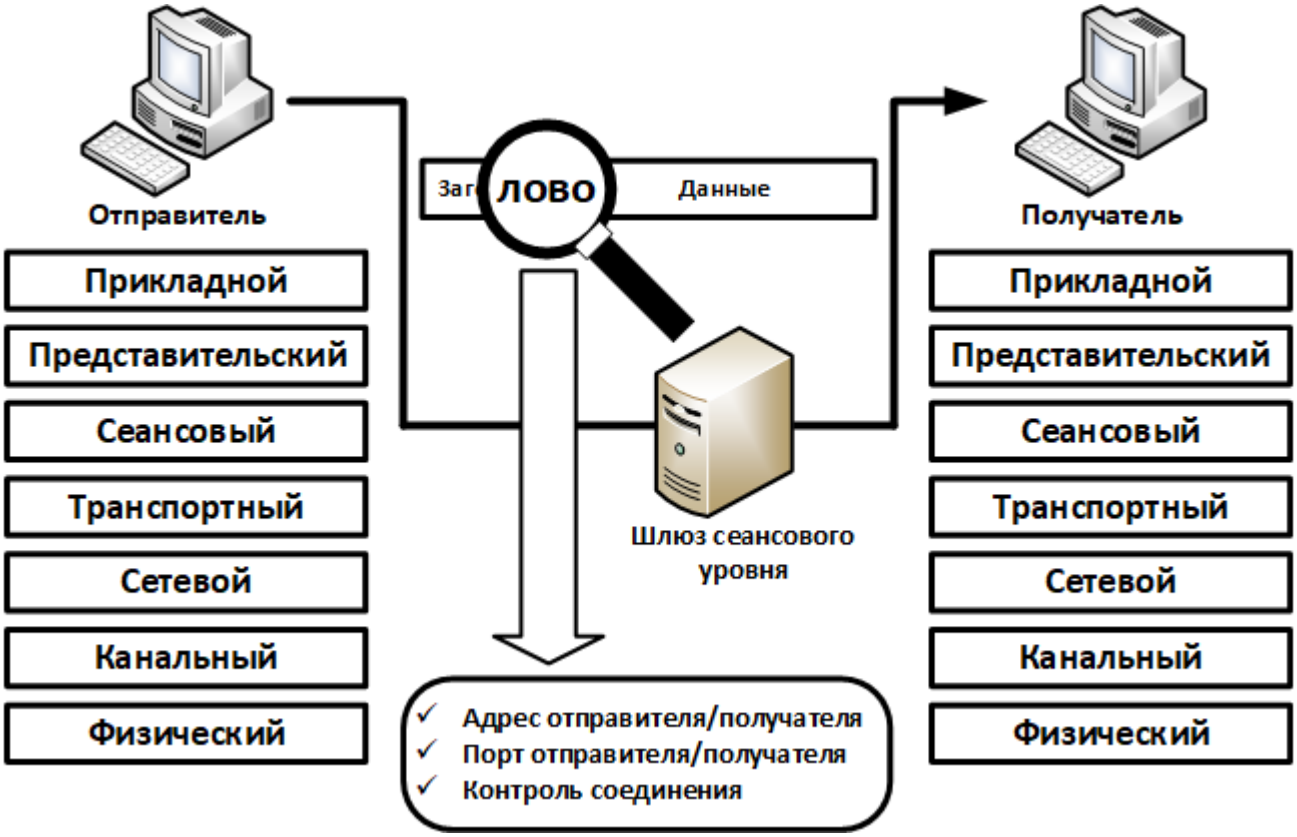


Рис. 4.14. Шлюз сеансового уровня

Работа посредника на сеансовом уровне показана на рис. 4.15.

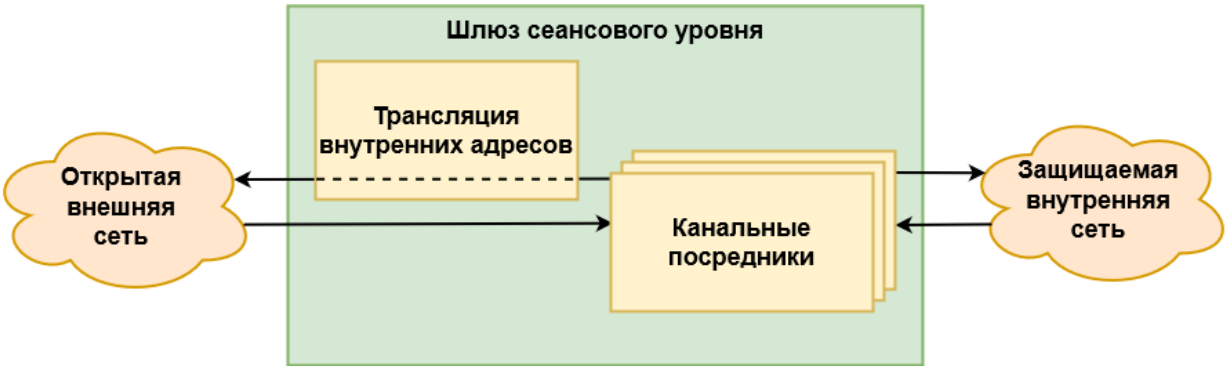


Рис. 4.15. Шлюз сеансового уровня

Посредники прикладного уровня, они осуществляют посредническую функцию между двумя узлами, исключая их непосредственное взаимодействие, но позволяют проникать в контекст передаваемого трафика, так как функционируют на прикладном уровне. Межсетевые экраны, построенные по этой технологии, содержат так называемых посредников приложений (application proxy), которые, «зная» как функционирует то или иное приложение, могут обрабатывать сгенерированный ими трафик. Еще одно отличие от шлюзов сеансового уровня — возможность фильтрации каждого пакета (рис. 4.16, 4.17).

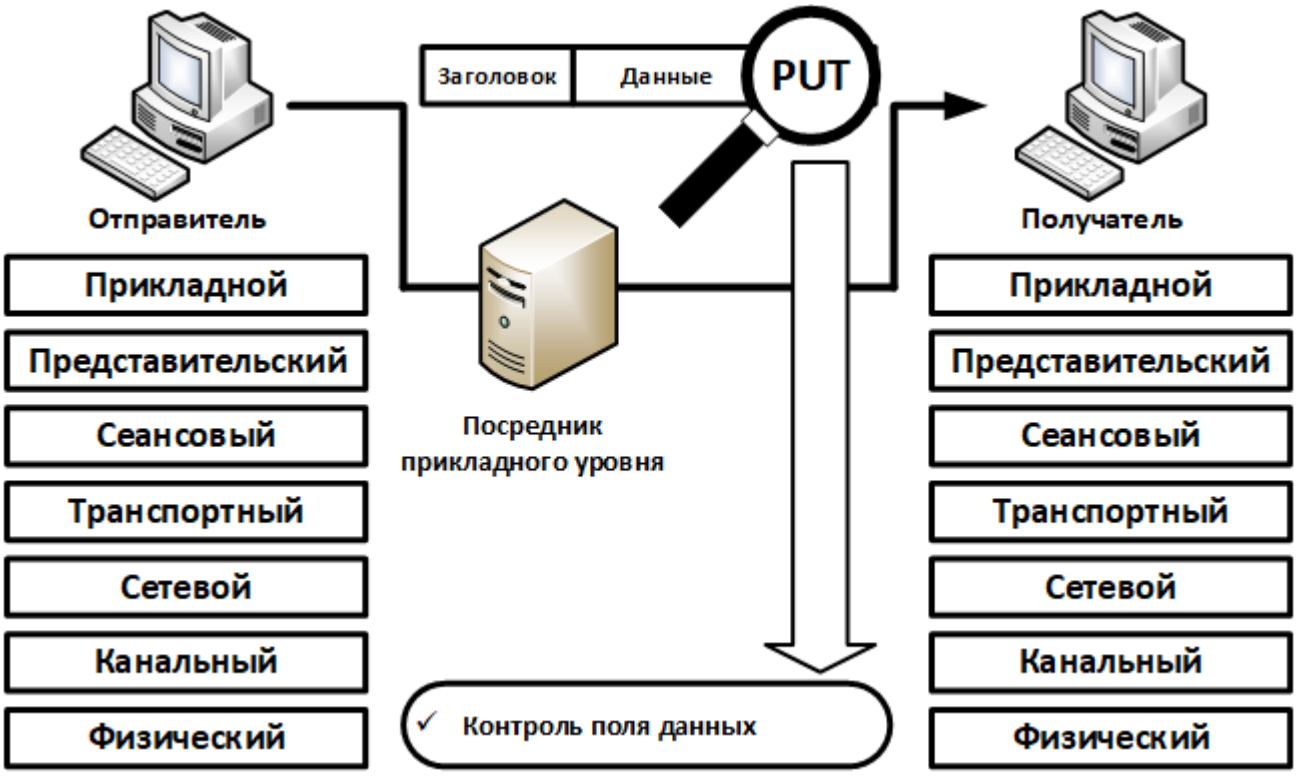


Рис. 4.16. Посредники прикладного уровня

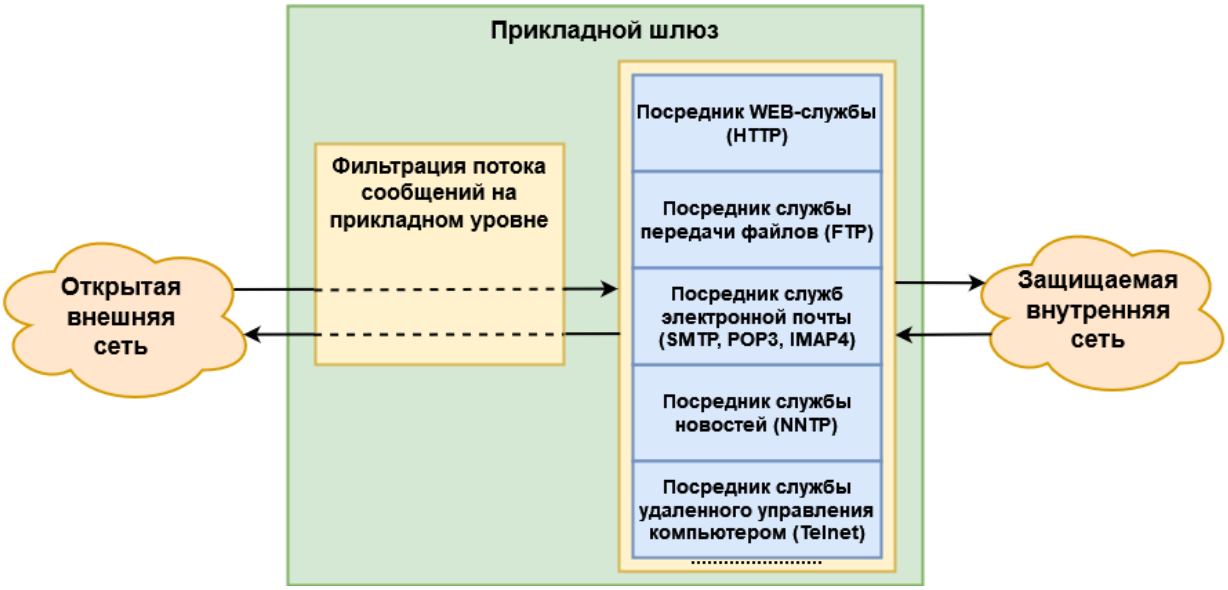


Рис. 4.17. Прикладной шлюз

Как говорилось ранее, межсетевые экраны могут обладать дополнительными возможностями, к которым относятся:

– идентификация и аутентификация пользователей (рис. 4.18);
– трансляция сетевых адресов (рис. 4.19);
– администрирование, регистрация событий и генерация отчетов.

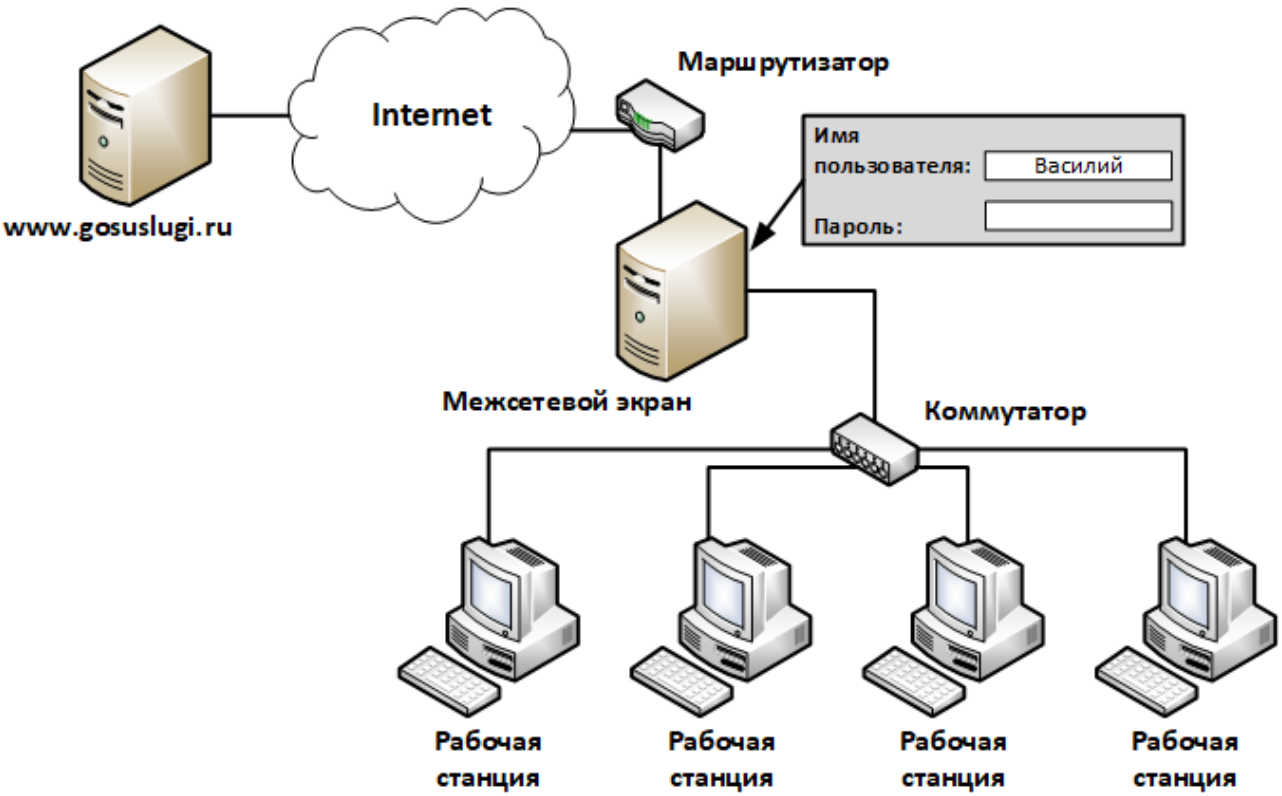


Рис. 4.18. Идентификация и аутентификация пользователей

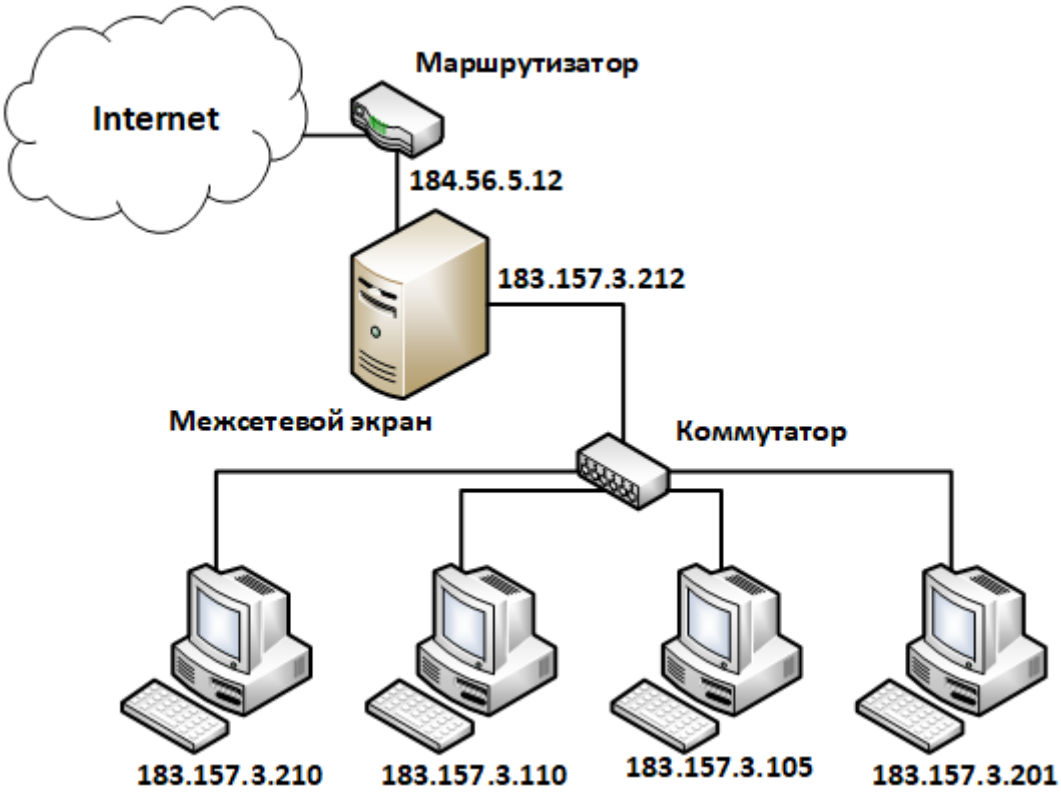


Рис. 4.19. Трансляция сетевых адресов

Требования к межсетевым экранам как средствам защиты информации, изложены в РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации».

Согласно этому документу, устанавливается пять классов защищенности МЭ. Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации. Самый низкий класс защищенности — пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый — для 1Г, третий — 1В, второй — 1Б, самый высокий — первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой.

Кроме простейшего контроля периметра сети, как это показано на рис. 4.20, существуют следующие базовые схемы построения МЭ (могут быть модифицированы в другие варианты конфигурации) на основе:

- фильтрующего маршрутизатора;
- двудомного узла (узла с двумя сетевыми интерфейсами);
- экранирующего узла;
- экранирующей сети.

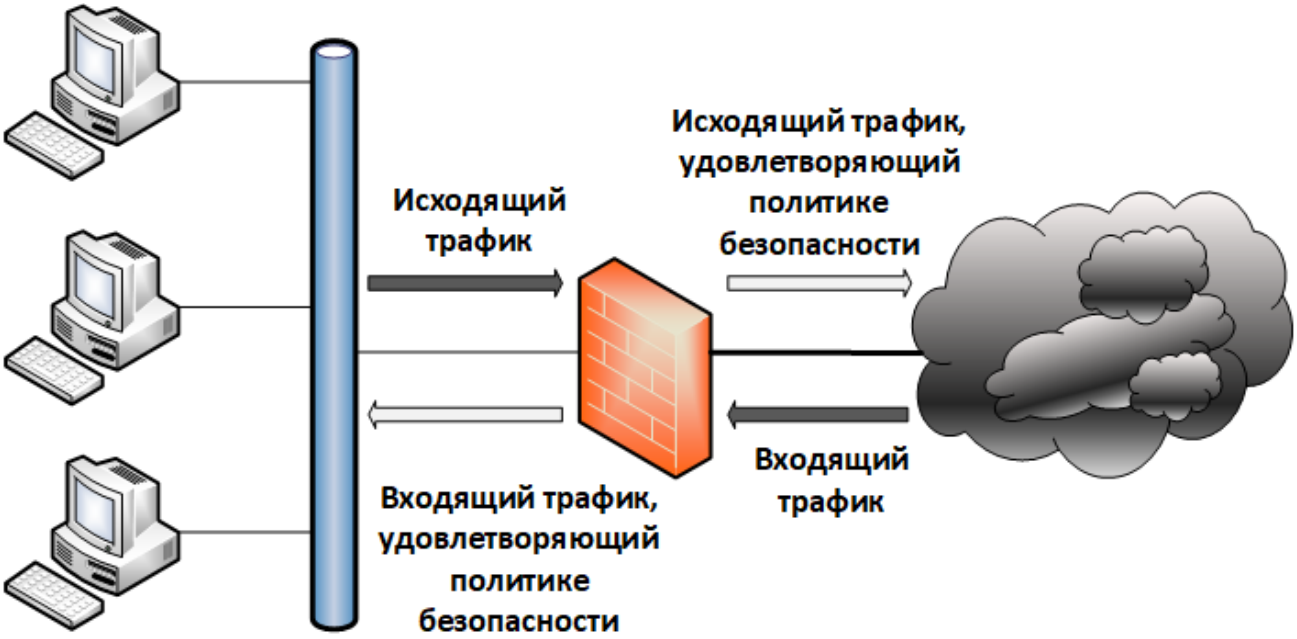


Рис. 4.20. Контроль периметра сети

МЭ на основе фильтрующего маршрутизатора представляет собой аппаратный или программный маршрутизатор на периметре защищаемой сети, в котором определен набор правил, устанавливающих разрешенные сетевые сервисы (рис. 4.21). Каждый сетевой пакет перед принятием решения о его маршрутизации проверяется на принадлежность к разрешенному типу трафика. Достоинства и недостатки данной схемы МЭ определяются возможностями функционирующего на маршрутизаторе пакетного фильтра.

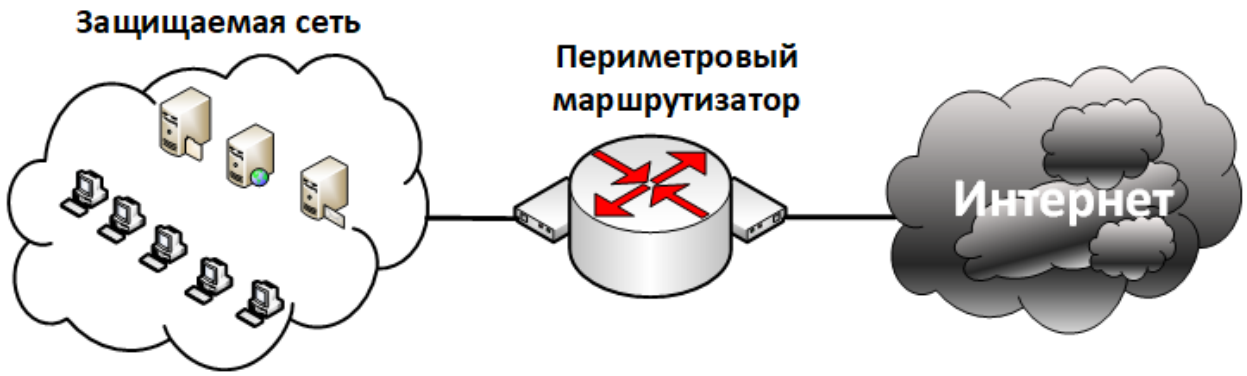


Рис. 4.21. МЭ на основе фильтрующего маршрутизатора

МЭ на основе двудомного узла представляет собой компьютер с двумя сетевыми интерфейсами, один из которых подключен к защищаемой внутренней сети, а второй — к внешней (рис. 4.22). Стандартная служба маршрутизации сетевых пакетов в ОС двудомного узла отключается для того, чтобы непосредственное взаимодействие между узлами внутренней и внешней сети было невозможным. Межсетевое взаимодействие в рамках разрешенных сервисов обеспечивается прокси-сервером, функционирующим на двудомном узле. Схема по сравнению с предыдущей характеризуется большей степенью безопасности, но предоставляемый пользователям сети набор сервисов ограничен и определяется программным обеспечением прокси-сервера.

Рис. 4.22. МЭ на основе двудомного узла

МЭ на основе экранирующего узла представляет собой комбинацию предыдущих схем (рис. 4.23): в состав его входят фильтрующий маршрутизатор на периметре и прокси-сервер, функционирующий на узле-бастионе с одним интерфейсом, во внутренней сети. Пакетный фильтр на маршрутизаторе конфигурируется таким образом, что разрешенный входящий и выходящий сетевой трафик обязательно проходит через узел-бастион. Схема характеризуется большей гибкостью по сравнению со схемой МЭ на основе двудомного узла, так как сервис, не поддерживаемый прокси-сервером, может быть разрешен напрямую через маршрутизатор.

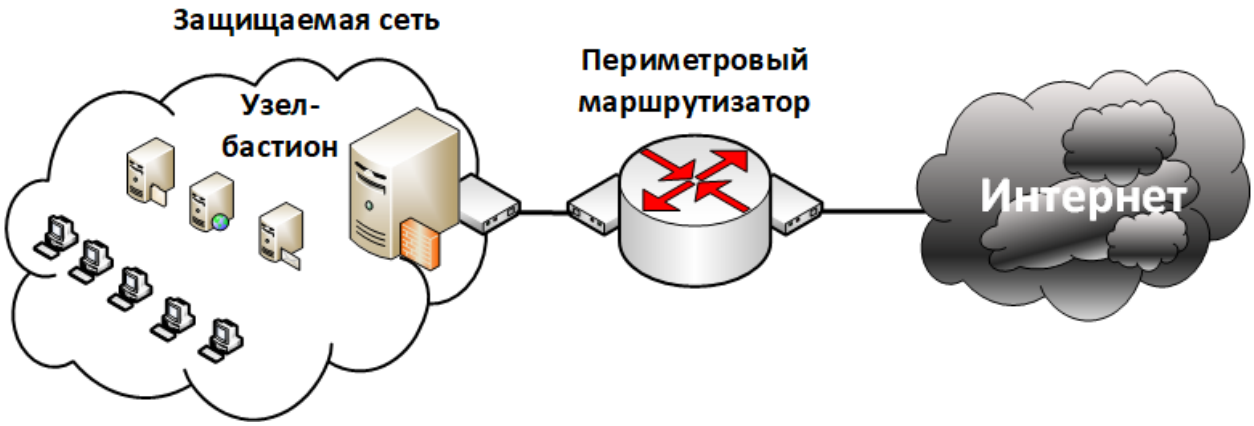


Рис. 4.23. МЭ на основе экранирующего узла

Схема МЭ на основе экранирующей сети представляет собой развитие предыдущей схемы и отличается от нее наличием дополнительного маршрутизатора (рис. 4.24). Между внешним и внутренним фильтрующими маршрутизаторами создается «менее защищаемая» сеть, называемая периметровой сетью или демилитаризованной зоной (DMZ), которая «экранирует» защищаемую сеть от внешнего мира. Как правило, в периметровой сети устанавливаются узлы с прокси-сервером и серверами открытых сервисов.

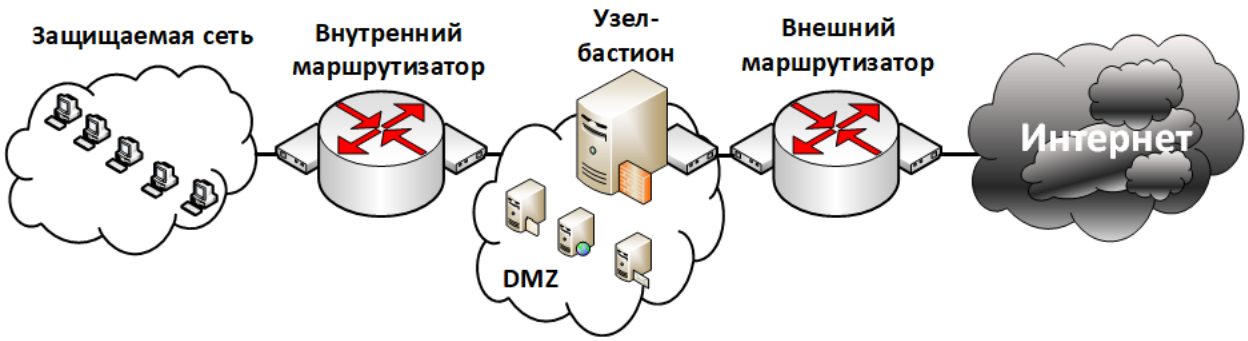


Рис. 4.24. МЭ на основе экранирующей сети

Линейка межсетевых экранов, имеющих сертификаты ФСТЭК России, включает следующие модели [35]:

– межсетевой экран с расширенной функциональностью, коммуникационный центр «ИВК Кольчуга»;

– программный комплекс «Межсетевой экран «ЗАСТАВА М» для ОС МСВС 3.0;

– специальное программное обеспечение межсетевой экран «Z-2», версия 2.6;

– межсетевой экран Cisco PIX Firewall PIX-515E ver. 7.0(6) для защиты информации, не составляющей гостайну;

– программно-аппаратный комплекс межсетевой экран WatchGuard Firebox с программным обеспечением Fireware OS для защиты информации, не составляющей гостайну;

– межсетевой экран ССПТ-2;

– межсетевой экран Checkpoint UTM-1 Edge N;

– программный межсетевой экран «Интернет Контроль Сервер»;

– межсетевой экран Altell NEO;

– межсетевой экран Vyatta с программным обеспечением Vyatta Core;

– программно-аппаратный комплекс «Межсетевой экран D-Link DFL-260E с установленным программным обеспечением «D-Link Firewall;

– межсетевой экран Juniper NetScreen-ISG 2000 с установленным программным обеспечением ScreenOS;

– межсетевой экран и система обнаружения вторжений «Рубикон-К»;

– межсетевой экран Kerio Control;

– межсетевой экран «Киберсейф: Межсетевой экран»;

– межсетевой экран StoneGate Firewall;

– межсетевой экран «Виток-МЭ3» с установленным ПО NS_FW;

– межсетевой экран «З-Экран».

4.6. Технологии обнаружения вторжений

Анализ защищенности — это поиск уязвимых мест в сети. Средства анализа защищенности — сканеры безопасности (security scanners). Обнаружение атак является процессом оценки подозрительных действий, которые происходят в корпоративной сети. Реализуется посредством анализа, или журналов регистрации ОС и приложений, или сетевого трафика в реальном времени.

Система обнаружения вторжений (СОВ) (англ. Intrusion Detection System (IDS)) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть. IDS являются необходимым дополнением инфраструктуры сетевой безопасности к межсетевым экранам (firewall). IDS служат механизмами мониторинга и наблюдения подозрительной активности. Они могут обнаружить атакующих, которые обошли firewall, и выдать отчет для дальнейших шагов по предотвращению атаки. Использование IDS помогает достичь нескольких целей:

– обнаружить вторжение или сетевую атаку;

– спрогнозировать возможные будущие атаки и выявить уязвимости для предотвращения их дальнейшего развития;

– выполнить документирование существующих угроз;

– обеспечить контроль качества администрирования с точки зрения безопасности, особенно в больших и сложных сетях;

– получить полезную информацию о проникновениях, которые имели место, для восстановления и корректирования вызвавших проникновение факторов;

– определить расположение источника атаки по отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов в сети.

Структурная схема системы обнаружения вторжений показана на рис. 4.25.

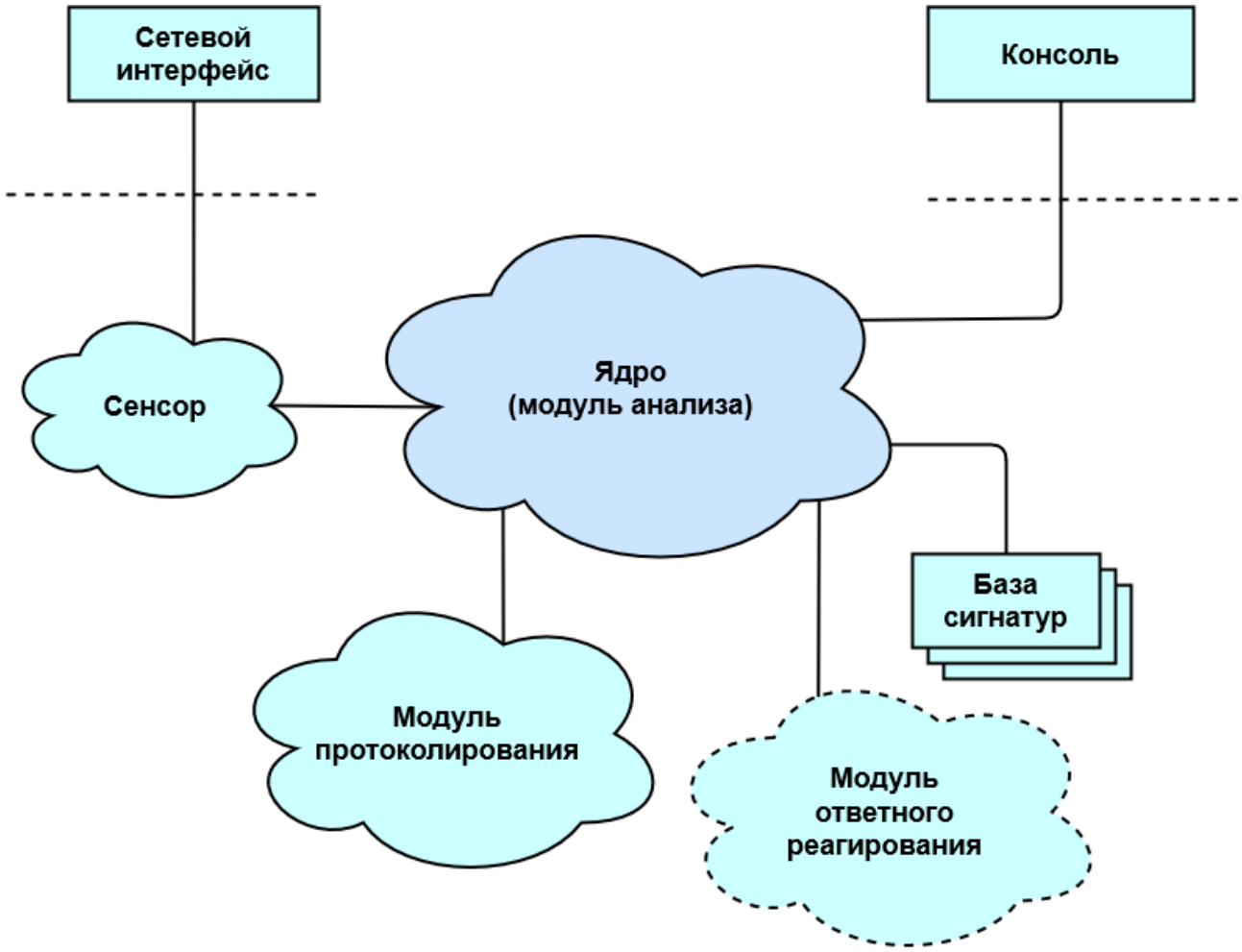


Рис. 4.25. Структурная схема IDS

Архитектура IDS обычно включает:

– сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой сети или системы;

– подсистему анализа, предназначенную для выявления сетевых атак и подозрительных действий;

– хранилище, в котором накапливаются первичные события и результаты анализа;

– консоль управления, позволяющая конфигурировать IDS, наблюдать за состоянием защищаемой системы и IDS, просматривать выявленные подсистемой анализа инциденты.

По способам мониторинга IDS системы подразделяются на:

– network-based (NIDS) — система обнаружения вторжений сетевого уровня;

– host-based (HIDS) — система обнаружения вторжений системного (хостового) уровня.

Основными коммерческими IDS являются network-based. Эти IDS определяют атаки, захватывая и анализируя сетевые пакеты. Слушая сетевой сегмент, NIDS может просматривать сетевой трафик от нескольких хостов, которые присоединены к сетевому сегменту, и таким образом защищать эти хосты.

Преимущества NIDS:

1. Большое покрытие для мониторинга и в связи с этим централизованное управление. Несколько оптимально расположенных NIDS могут просматривать большую сеть.

2. Не влияют на производительность и топологию сети. NIDS обычно являются пассивными устройствами, которые прослушивают сегменты сети без воздействия на ее нормальное функционирование. Таким образом, обычно бывает легко модифицировать топологию сети для размещения таких IDS.

Недостатки NIDS:

1. Обладают высокой ресурсоемкостью. Для NIDS может быть трудно обрабатывать все пакеты в большой или занятой сети, и, следовательно, они могут пропустить распознавание атаки, которая началась при большом трафике.

2. Требуют дополнительной настройки и функциональности сетевых устройств. Многие коммутаторы, не предоставляют универсального мониторинга портов, и это ограничивает диапазон мониторинга сенсора NIDS только одним хостом. Даже когда коммутаторы предоставляют такой мониторинг портов, часто единственный порт не может охватить весь трафик, передаваемый коммутатором.

3. Не могут анализировать зашифрованную информацию. Эта проблема возрастает, чем больше организации (и атакующие) используют VPN.

4. Не могут распознать результат атаки. NIDS не могут сказать была ли атака успешной, они могут только определить, что атака была начата. Администратор должен вручную исследовать каждый атакованный хост для определения, происходило ли реальное проникновение.

5. Некоторые NIDS имеют проблемы с определением сетевых атак, которые включают фрагментированные пакеты. Такие фрагментированные пакеты могут привести к тому, что IDS будет функционировать нестабильно.

Системы обнаружения вторжений системного (хостового) уровня (Host-based IDS) имеют дело с информацией, собранной внутри единственного компьютера. Такое расположение позволяет HIDS анализировать деятельность с большой достоверностью и точностью, определяя только те процессы и пользователей, которые имеют отношение к конкретной атаке в ОС. HIDS обычно используют информационные источники двух типов: результаты аудита ОС и системные логи.

Преимущества HIDS:

1. Имеют возможностью следить за событиями локально относительно хоста, могут определять атаки, которые не могут видеть NIDS.

2. Могут функционировать в окружении, в котором сетевой трафик зашифрован. Это становится возможным, когда host-based источники информации создаются до того, как данные шифруются, и (или) после того, как данные расшифровываются на хосте назначения.

3. Не требуют дополнительной функциональности сетевых устройств. Например, на функционирование HIDS не влияет наличие в сети коммутаторов.

Недостатки HIDS:

1. Не имеют централизованного управления. HIDS более трудны в управлении, так как они должны быть сконфигурированы и управляться для каждого целевого хоста.

2. Могут быть блокированы некоторыми DDoS-атаками или даже запрещены. Так как источники информации (сенсоры) или часть средств анализа для HIDS расположены на том же хосте, который является целью атаки, то IDS может быть атакована и запрещена.

3. Обладают высокой ресурсоемкостью. HIDS используют вычислительные ресурсы хостов, за которыми они наблюдают, что влияет на производительность наблюдаемой системы.

4. Малое покрытие для мониторинга. HIDS не полностью соответствуют возможности определения сканирования сети или других аналогичных исследований, когда целью является вся сеть, так как IDS наблюдает только за сетевыми пакетами, получаемыми конкретным хостом.

По способам определения вредоносного трафика IDS системы подразделяются на:

– signature-based (сигнатурного метода);
– anomaly-based (метода аномалий);
– policy-based (метода, основанного на политике).

Преимущества сигнатурного метода:

1. Эффективное определение атак и отсутствие большого числа ложных сообщений.

2. Надежная диагностика использования конкретного инструментального средства или технологии атаки. Это позволяет администраторам, независимо от уровня их квалификации в области безопасности, начать процедуры обработки инцидента, а также скорректировать меры обеспечения безопасности.

Метод аномалий состоит в определении ненормального (необычного) поведения на хосте или в сети. Детекторы аномалий предполагают, что атаки отличаются от «нормальной» (законной) деятельности и могут, следовательно, быть определены системой, которая умеет отслеживать эти отличия. Детекторы аномалий создают профили, представляющие собой нормальное поведение пользователей, хостов или сетевых соединений. Эти профили создаются, исходя из данных истории, собранных в период нормального функционирования. Затем детекторы собирают данные о событиях и используют различные метрики для определения того, что анализируемая деятельность отклоняется от нормальной.

Преимущества метода аномалий:

1. Определение атаки без знания конкретных деталей (сигнатуры).

2. Детекторы аномалий могут создавать информацию, которая в дальнейшем будет использоваться для определения сигнатур атак.

Недостатки метода аномалий:

1. Большое количество ложных сигналов при непредсказуемом поведении пользователей и непредсказуемой сетевой активности.

2. Временные затраты на этапе обучения системы, во время которого определяются характеристики нормального поведения.

Метод, основанный на политике (*policy-based*), заключается в написании правил сетевой безопасности в терминах распределения доступа (например, какие сети могут взаимодействовать друг с другом и какие протоколы при этом могут использоваться).

Преимущество метода политик: способен обнаруживать новые (неизвестные) атаки.

Недостаток метода политик: трудоемкость создания базы политик.

Алгоритм функционирования системы IDS основанной на сигнатурном методе определения атак приведен на рис. 4.26.

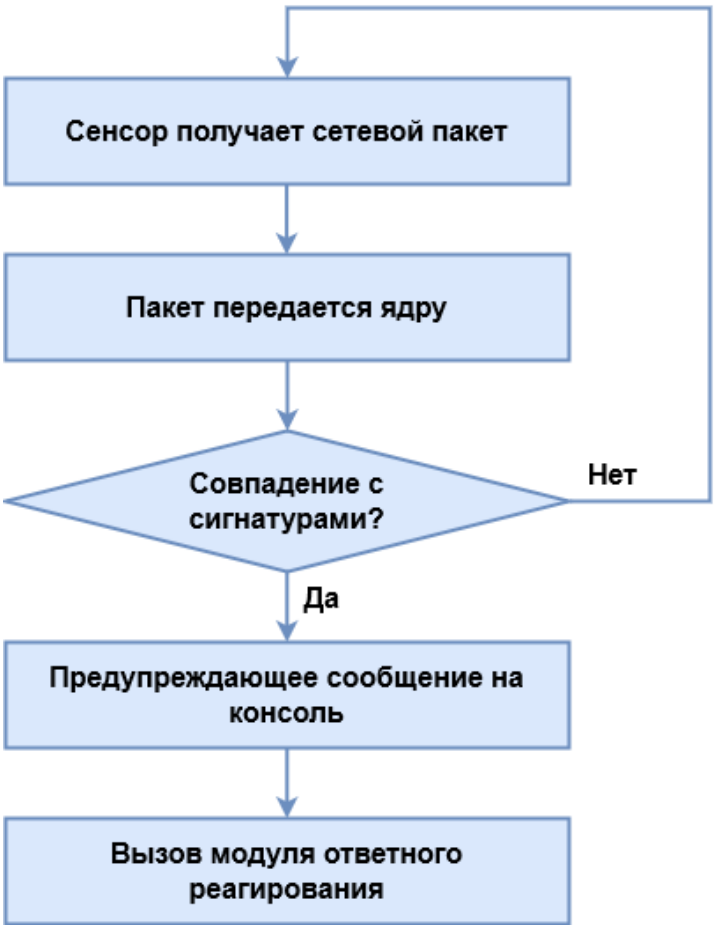


Рис. 4.26. Алгоритм функционирования IDS

Типичная схема защиты локальных сетей на базе IDS Snort представлена на рис. 4.27.

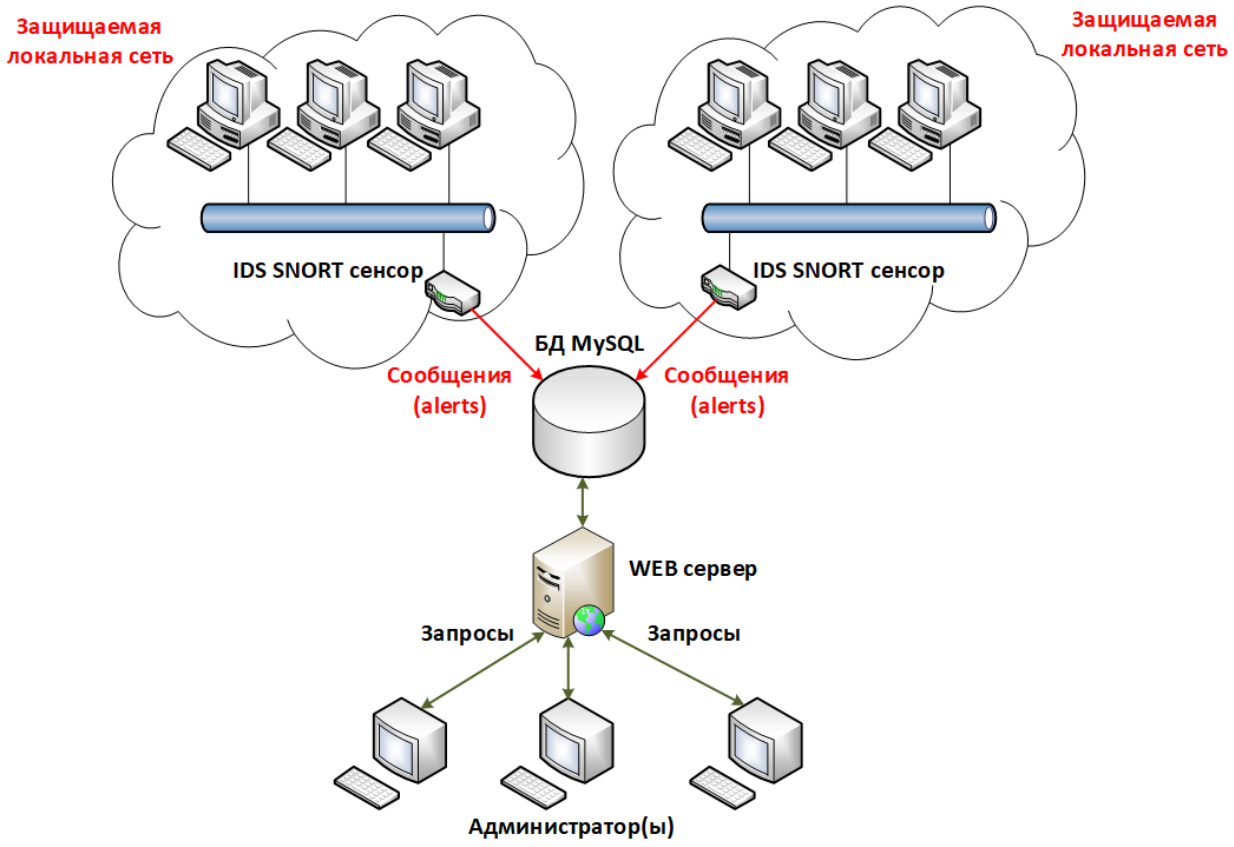


Рис. 4.27. Система обнаружения сетевых атак на базе IDS Snort

Установленные на периметре межсетевые экраны (firewall) и системы обнаружения вторжений (IDS) имеют свои недостатки. МЭ пропускали трафик через себя, но не «заглядывали» внутрь пересылаемых данных, фокусируясь только на заголовке IP-пакета. Системы IDS (Intrusion Detection System) анализировали то, что упускалось из виду межсетевыми экранами, но не были способны блокировать атаки, так как трафик через них не проходил.

Модуль ответного реагирования представляет собой опциональный компонент, который может быть использован для оперативного блокирования угрозы: например, может быть сформировано правило для межсетевого экрана, блокирующее источник нападения. Поэтому на стыке двух технологий родился новый класс защитных средств — системы предотвращения вторжений (IPS).

Система предотвращения вторжений (англ. Intrusion Prevention System (IPS)) — программное или аппаратное средство, которое осуществляет мониторинг сети или компьютерной системы в реальном времени с целью выявления, предотвращения или блокировки вредоносной активности. IPS по классификации и своим функциям аналогичны IDS. Отличие состоит в том, что они функционируют в реальном времени и могут в автоматическом режиме блокировать сетевые атаки. Каждая IPS включает в себя модуль IDS. Правиль-

ное размещение систем IDS/IPS в сети не оказывает влияния на ее топологию, но зато имеет огромное значение для оптимального мониторинга и достижения максимального эффекта от ее защиты.

Типичные примеры развертывания систем обнаружения и систем предотвращения вторжений представлены на рис. 4.28–4.30.

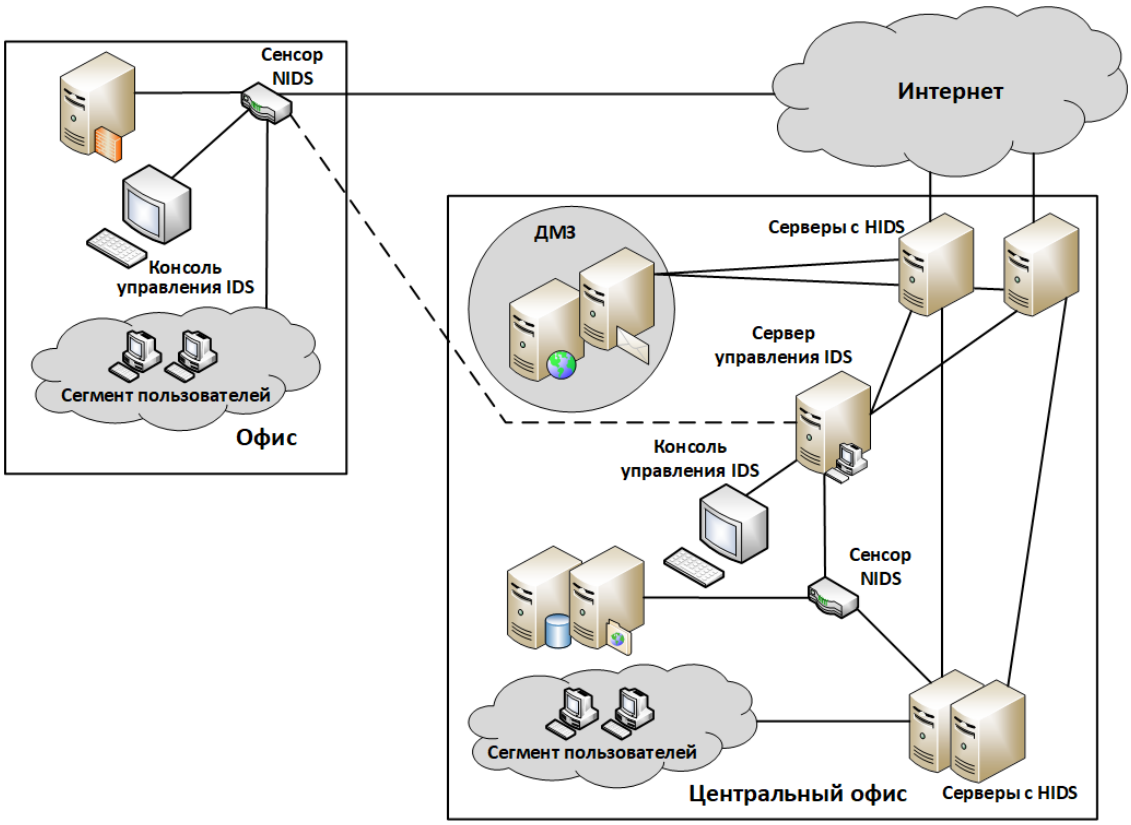


Рис. 4.28. Подсистема обнаружения вторжений сетевого уровня

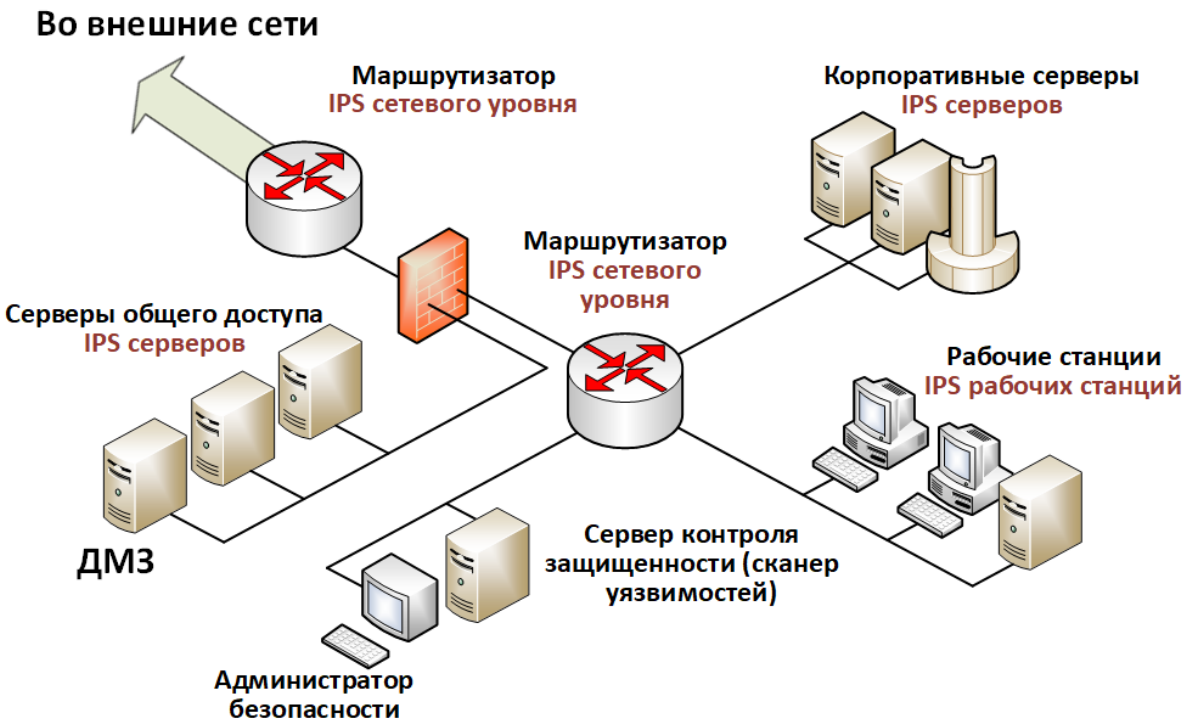


Рис. 4.29. Пример развертывания системы предотвращения вторжений

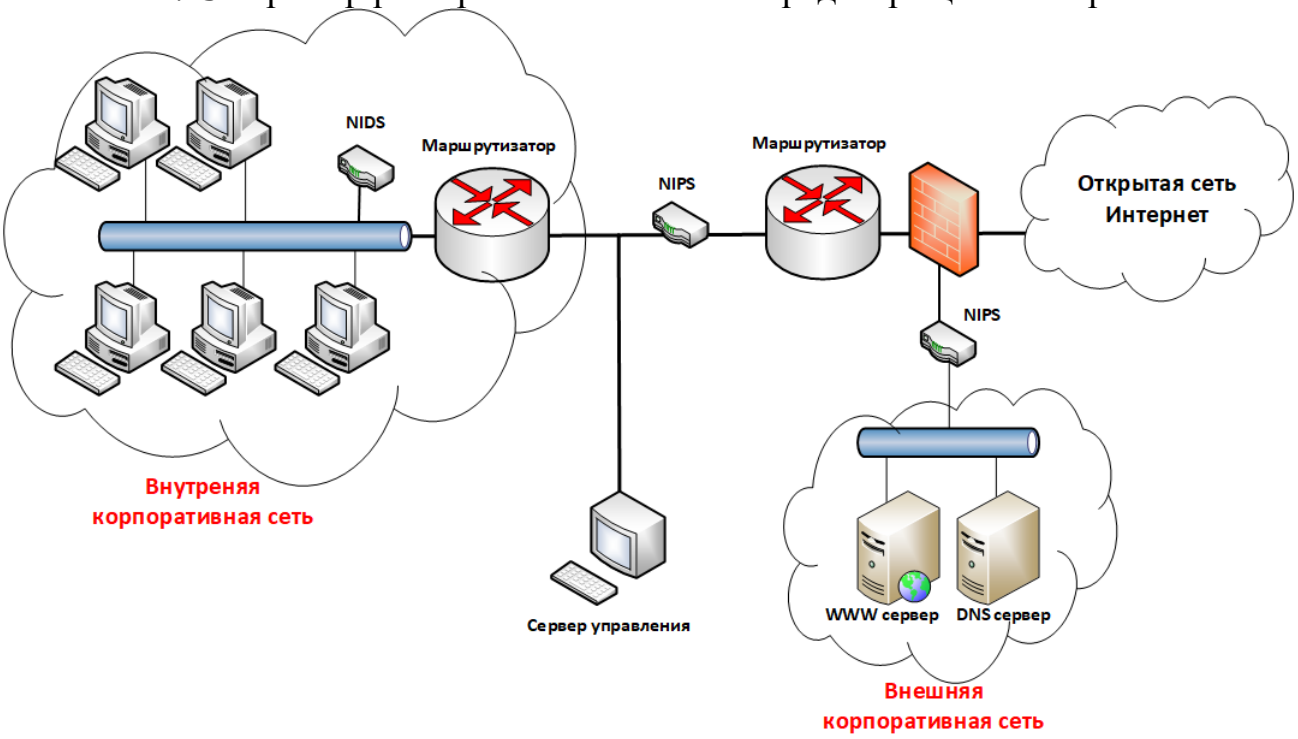


Рис. 4.30. Типичное развертывание систем NIDS и NIPS

Различия в поведении систем обнаружения и систем предотвращения вторжений показаны на рис. 4.31.

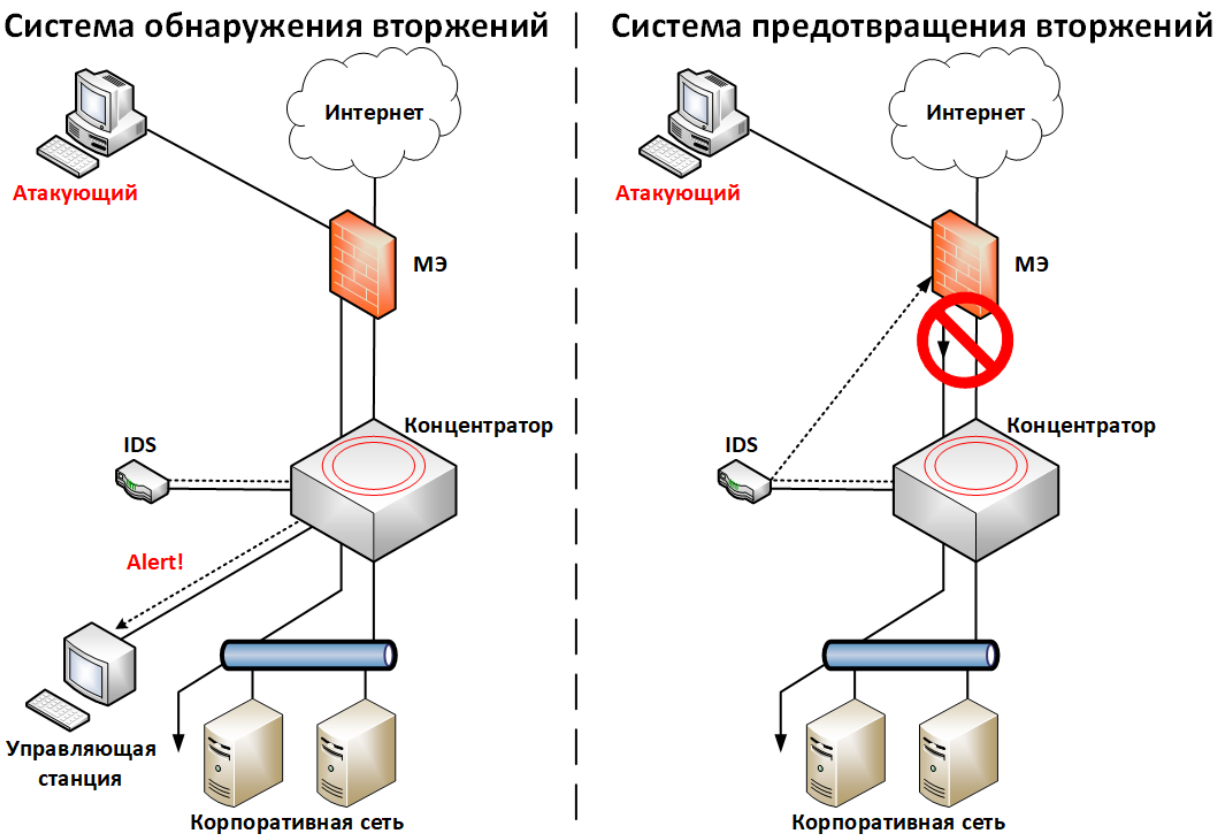


Рис. 4.31. Поведение систем обнаружения и предотвращения вторжений

4.7. Виртуальные защищенные сети (VPN)

При подключении корпоративной локальной сети к открытой сети возникают угрозы безопасности двух основных типов:

– несанкционированный доступ к внутренним ресурсам корпоративной локальной сети, получаемый злоумышленником в результате несанкционированного входа в эту сеть;

– несанкционированный доступ к корпоративным данным в процессе их передачи по открытой сети.

Обеспечение безопасности информационного взаимодействия локальных сетей и отдельных компьютеров через открытые сети, в частности через сеть Интернет, возможно путем эффективного решения следующих задач:

– защита подключенных к открытым каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды;

– защита информации в процессе ее передачи по открытым каналам связи.

Защита локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды обеспечивается межсетевым экранированием. Защита информации в процессе ее передачи по открытым каналам основана на использовании виртуальных защищенных сетей VPN.

В основе концепции построения виртуальных сетей VPN лежит идея: если в глобальной сети имеются два узла, которым нужно обменяться информацией, то между этими двумя узлами необходимо построить виртуальный защищенный туннель для обеспечения конфиденциальности и целостности информации, передаваемой через открытые сети. Доступ к этому виртуальному туннелю должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям.

Виртуальной защищенной сетью VPN (Virtual Private Network) называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных. Создаются виртуальные защищенные каналы связи туннели VPN. Туннель VPN представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети. Защита информации в процессе ее передачи по туннелю VPN основана:

– на аутентификации взаимодействующих сторон;
– криптографическом закрытии (шифровании) передаваемых данных;
– проверке подлинности и целостности доставляемой информации.

Для этих функций характерна взаимосвязь друг с другом. При их реализации используются криптографические методы защиты информации. Эффективность такой защиты обеспечивается за счет совместного использования симметричных и асимметричных алгоритмов шифрования. Туннель VPN, формируемый устройствами VPN, обладает свойствами защищенной выделенной линии, которая развертывается в рамках общедоступной сети, например Интернета. Устройства VPN могут играть в виртуальных частных сетях роль VPN-клиента, VPN-сервера или шлюза безопасности VPN. Исходя из этого можно различить соединения типа сеть-сеть (рис. 4.32) и хост-сеть (рис. 4.33).

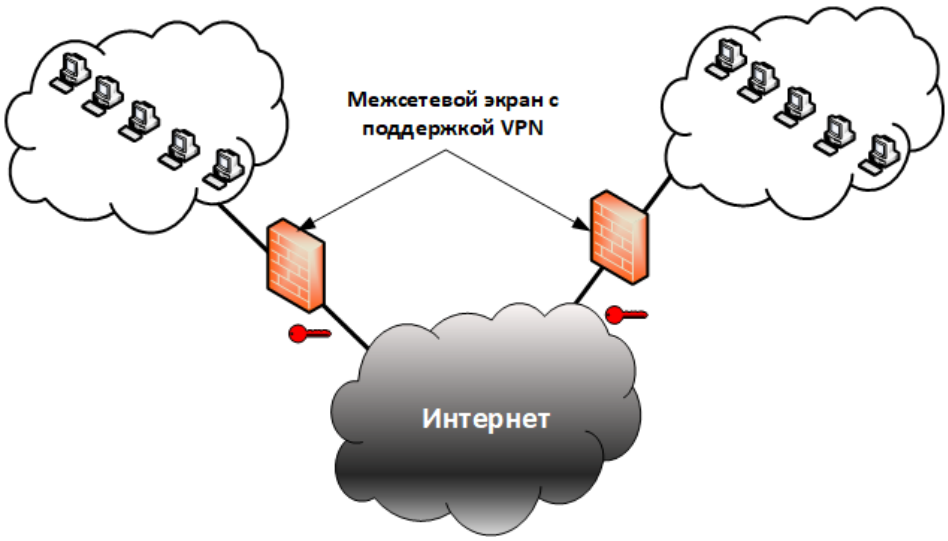


Рис. 4.32. VPN-соединение типа сеть-сеть

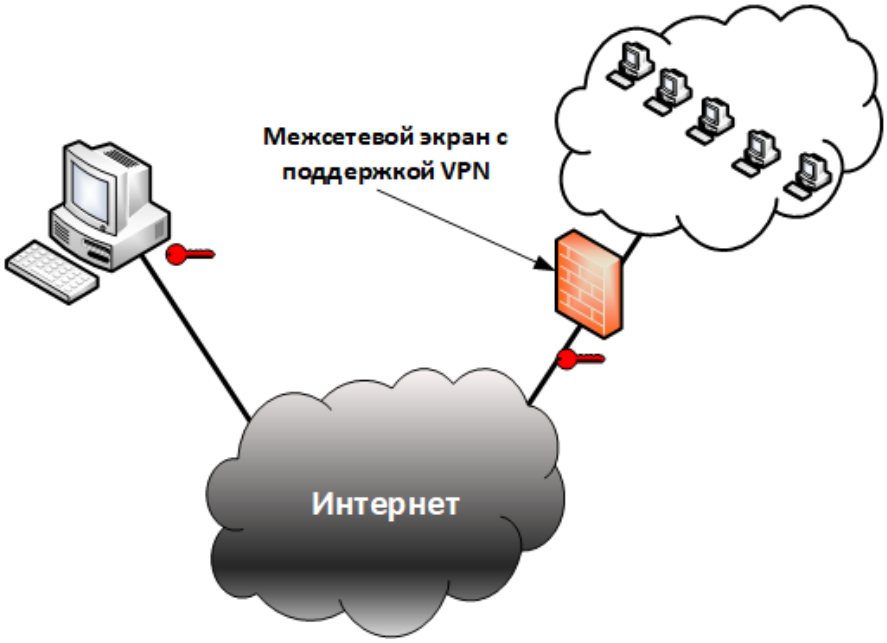


Рис. 4.33. VPN-соединение типа хост-сеть

В общем виде виртуальную защищенную сеть можно представить схематично, как это изображено на рис. 4.34.

VPN-клиент представляет собой программный или программно-аппаратный комплекс, выполняемый обычно на базе персонального компьютера. Обычно реализация VPN-клиента представляет собой программное решение, дополняющее стандартную ОС.

VPN-сервер представляет собой программный или программно-аппаратный комплекс, устанавливаемый на компьютере, выполняющем функции сервера.

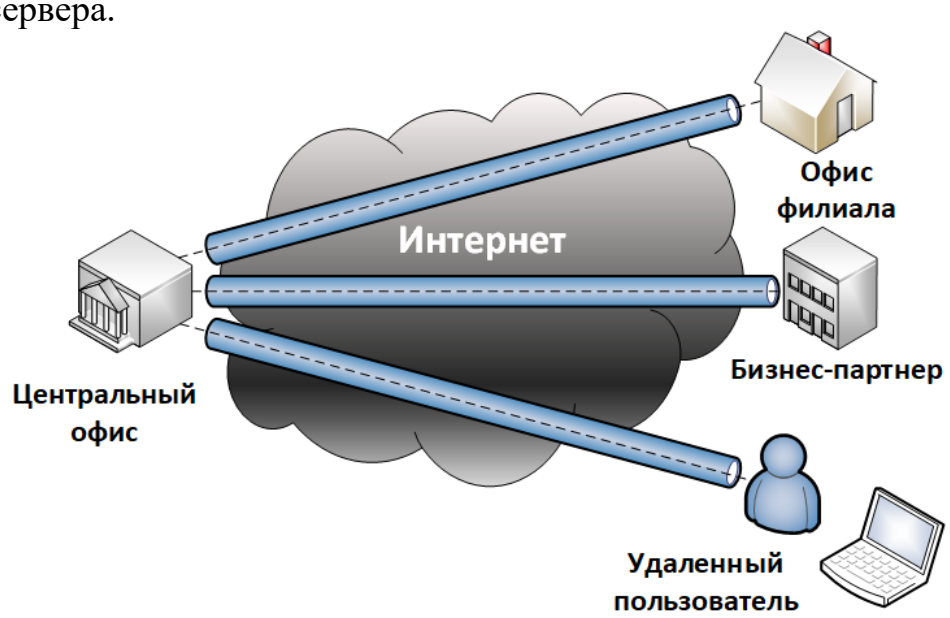


Рис. 4.34. Виртуальная защищенная сеть VPN

Шлюз безопасности VPN (security gateway) — это сетевое устройство, подключаемое к двум сетям и выполняющее функции шифрования и аутентификации для многочисленных хостов, расположенных за ним.

Размещение шлюза безопасности VPN выполняется таким образом, чтобы через него проходил весь трафик, предназначенный для внутренней корпоративной сети. Сетевое соединение прозрачно для пользователей позади шлюза, оно представляется им выделенной линией, хотя на самом деле прокладывается через открытую сеть с коммутацией пакетов. Адрес шлюза безопасности VPN указывается как внешний адрес входящего туннелируемого пакета, а внутренний адрес пакета является адресом конкретного хоста позади шлюза.

Суть туннелирования состоит в том, чтобы инкапсулировать, т.е. «упаковать», передаваемую порцию данных вместе со служебными полями в новый «конверт». При этом пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Туннелирование само по себе не защищает данные от НСД или искажения, но благодаря туннелированию появляется возможность полной криптографической защиты инкапсулируемых исходных пакетов. Чтобы обеспечить конфиденциальность передаваемых данных, отправитель шифрует исходные пакеты, упаковывает их во внешний пакет с новым IP-заголовком и отправляет по транзитной сети. Особенность технологии туннелирования в том, что она позволяет зашифровывать исходный пакет целиком, вместе с заголовком, а не только его поле данных (рис. 4.35).

Рис. 4.35. Особенность технологии туннелирования

По прибытии в конечную точку защищенного канала из внешнего пакета извлекают внутренний исходный пакет, расшифровывают его и используют его восстановленный заголовок для дальнейшей передачи по внутренней сети (рис. 4.36). Туннелирование может быть использовано для защиты не только конфиденциальности содержимого пакета, но и его целостности и аутентичности, при этом электронную цифровую подпись можно распространить на все поля пакета.

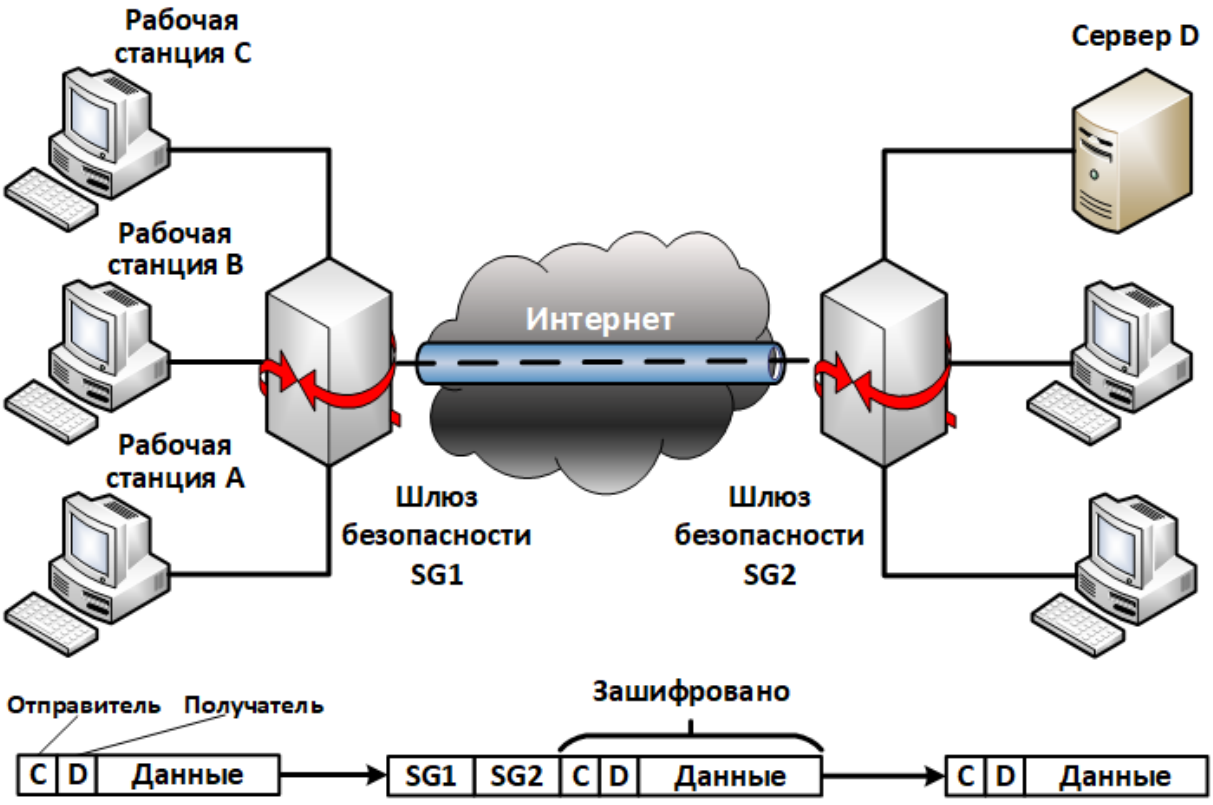


Рис. 4.36. Схема виртуального защищенного туннеля

Обычно туннель создается только на участке открытой сети, где существует угроза нарушения конфиденциальности и целостности данных, например между точкой входа в открытый Интернет и точкой входа в корпоративную сеть. Для внешних пакетов используются адреса пограничных маршрутизаторов, установленных в этих двух точках, а внутренние адреса конечных узлов содержатся во внутренних исходных пакетах в защищенном виде (рис. 4.37).

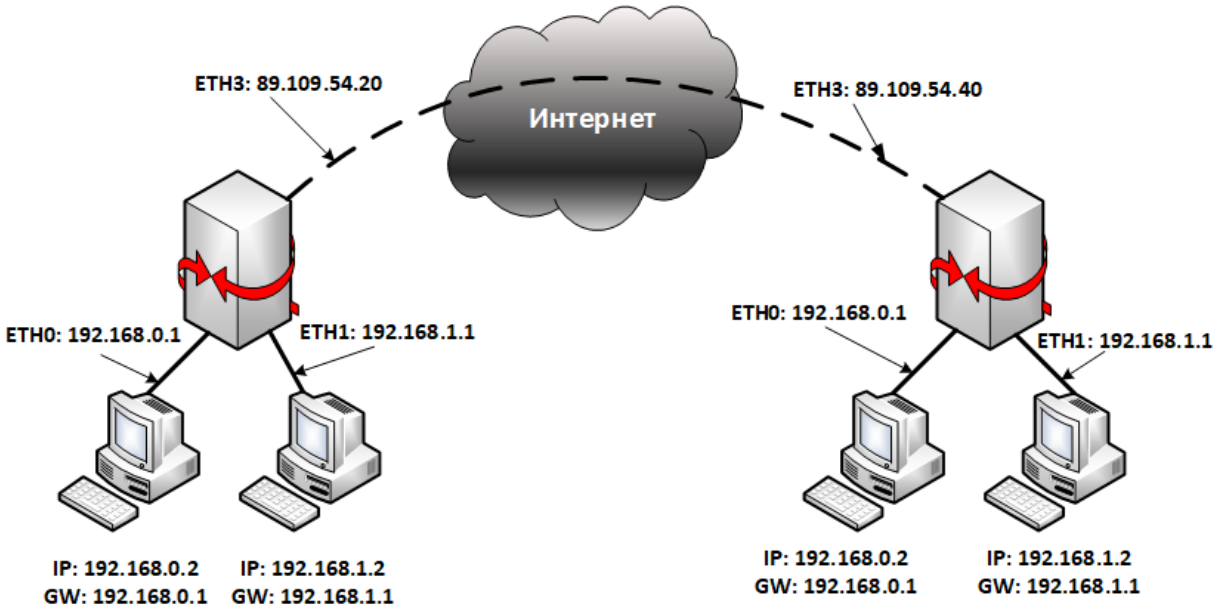


Рис. 4.37. Трансляция адресов

Существует три различные формы проверки подлинности для VPN-подключений.

Проверка подлинности на уровне пользователя по протоколу PPP (Point-to-Point Protocol). Для установления VPN-подключения VPN-сервер выполняет проверку подлинности VPN-клиента, пытающегося установить подключение, и проверяет, имеет ли VPN-клиент соответствующие разрешения на доступ. При взаимной проверке подлинности VPN-клиент также выполняет проверку подлинности VPN-сервера, что гарантирует защиту от компьютеров, выдающих себя за VPN-серверы.

Проверка подлинности на уровне компьютера по протоколу IKE (Internet Key Exchange). Чтобы установить сопоставление безопасности IPSec, VPN-клиент и VPN-сервер используют протокол IKE для обмена сертификатами компьютеров или предварительным ключом. В обоих случаях VPN-клиент и VPN-сервер выполняют взаимную проверку подлинности на уровне компьютера. Проверка подлинности на основе сертификата компьютера является одним из самых надежных способов.

Проверка подлинности источника данных и обеспечение целостности данных. Чтобы убедиться в том, что источником отправленных по VPN-подключению данных является другая сторона VPN-подключения и что они переданы в неизмененном виде, в данные включается контрольная сумма шифрования, основанная на ключе шифрования, который известен только отправителю и получателю.

Безопасность информационного обмена необходимо обеспечивать как в случае объединения локальных сетей, так и в случае доступа к локальным сетям удаленных или мобильных пользователей. При проектировании VPN обычно рассматриваются две основные схемы:

– виртуальный защищенный канал между локальными сетями (канал ЛВС — ЛВС);

– виртуальный защищенный канал между узлом и локальной сетью (канал клиент — ЛВС) (рис. 4.38).

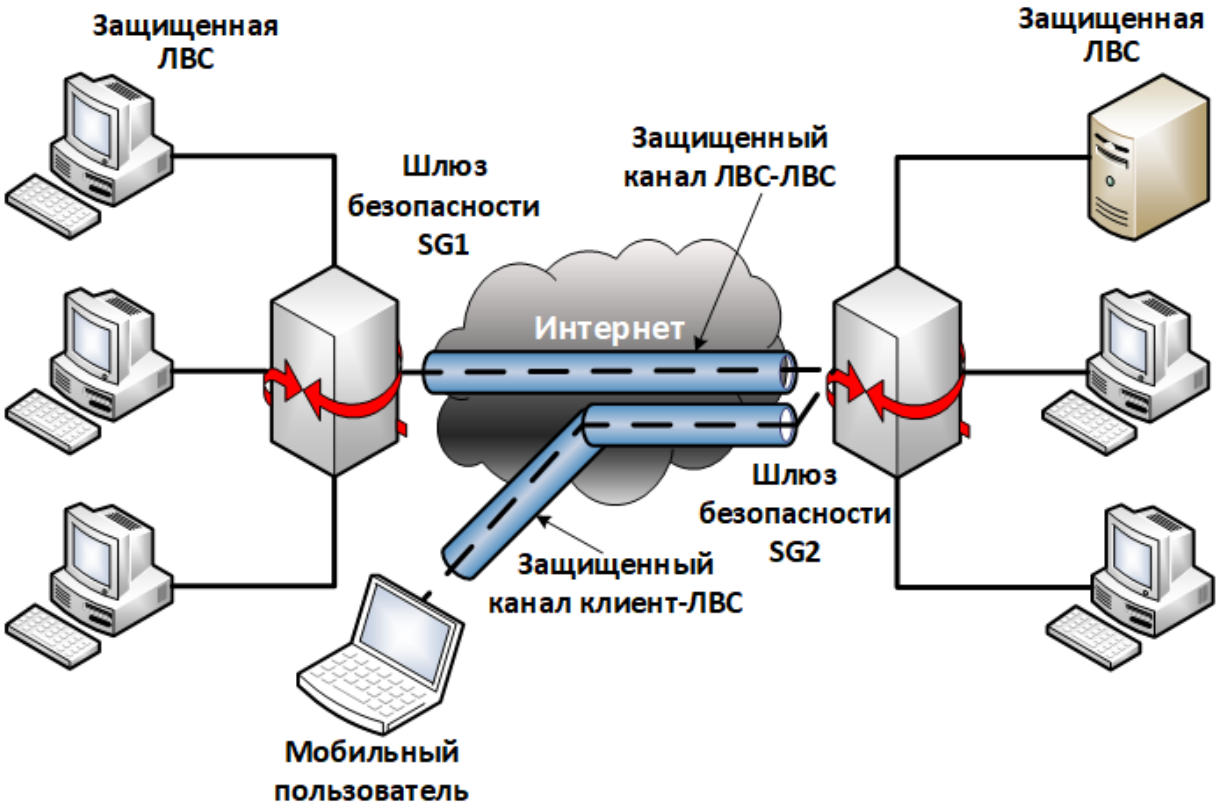


Рис. 4.38. Виртуальные защищенные каналы типа ЛВС — ЛВС и клиент — ЛВС

Существуют разные признаки классификации VPN. Наиболее часто используются:

– классификация VPN по «рабочему» уровню модели OSI;
– классификация VPN по архитектуре технического решения;
– классификация VPN по способу технической реализации.

Защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях эталонной модели взаимодействия открытых систем ISO/OSI (табл. 4.4).

В зависимости от рабочего уровня различают:

1. VPN канального уровня. Средства VPN, используемые на канальном уровне модели OSI, позволяют обеспечить инкапсуляцию различных видов трафика третьего уровня (и выше) и построение виртуальных туннелей типа «точка — точка» (от маршрутизатора к маршрутизатору или от персонального компьютера к шлюзу ЛВС).

Таблица 4.4

Влияние протоколов на функционирующих
на разных уровнях модели ISO/OSI на приложения

Протоколы защищенного доступа	Прикладной	Влияют на приложения
	Представительный	
	Сеансовый	

	Транспортный	Прозрачны для приложений
	Сетевой	
	Канальный	
	Физический	

2. VPN сетевого уровня. VPN-продукты сетевого уровня выполняют инкапсуляцию IP в IP. Одним из широко известных протоколов на этом уровне является протокол IPSec (IP Security), предназначенный для аутентификации, туннелирования и шифрования IP-пакетов. Стандартизованный консорциумом Internet Engineering Task Force (IETF) протокол IPSec входит в качестве обязательного компонента в протокол IPv6. С протоколом IPSec связан протокол IKE (Internet Key Exchange), решающий задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами. Протокол IKE автоматизирует обмен ключами и устанавливает защищенное соединение, тогда как IPSec кодирует и «подписывает» пакеты. Кроме того, IKE позволяет изменять ключ для уже установленного соединения, что повышает конфиденциальность передаваемой информации.

3. VPN сеансового уровня. Некоторые VPN используют другой подход под названием «посредники каналов» (circuit proxy). Этот метод функционирует над транспортным уровнем и ретранслирует трафик из защищенной сети в общедоступную сеть Internet для каждого порта в отдельности. Шифрование информации, передаваемой между инициатором и терминатором туннеля, часто осуществляется с помощью защиты транспортного уровня TLS (Transport Layer Security).

По архитектуре принято выделять три основных вида VPN:

1. Внутрикорпоративные сети VPN предназначены для обеспечения защищенного взаимодействия между подразделениями внутри предприятия или между группой предприятий, объединенных корпоративными сетями связи, включая выделенные линии (рис. 4.39).

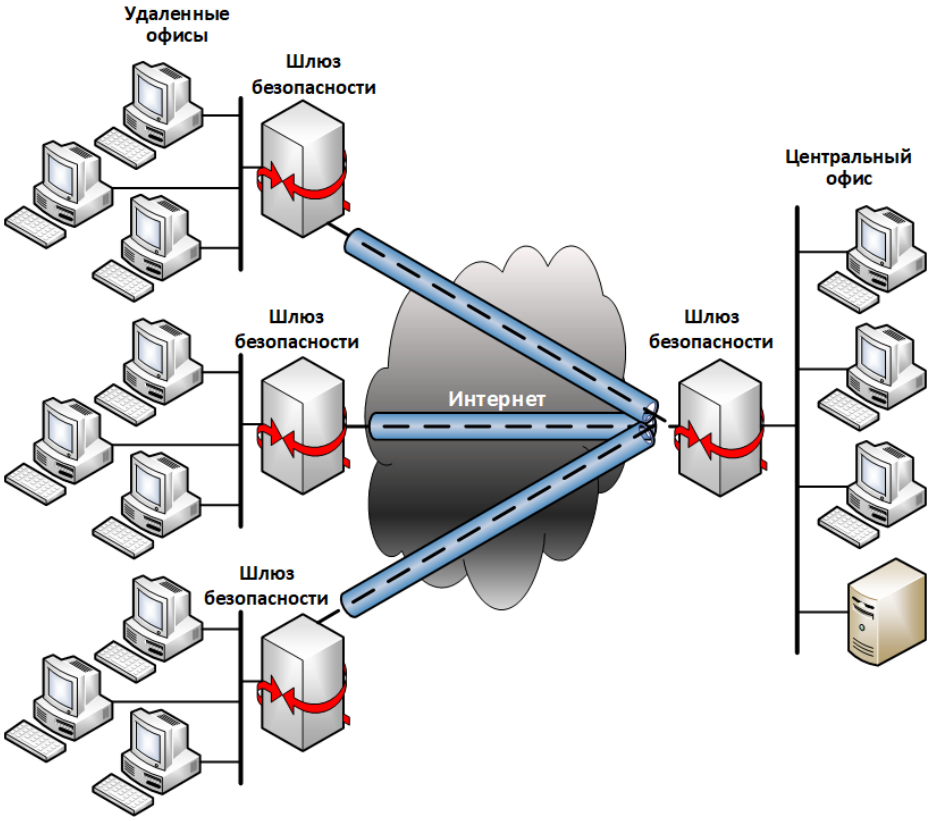


Рис. 4.39. Внутрикорпоративные VPN

2. VPN с удаленным доступом предназначены для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам мобильным и/или удаленным (home-office) сотрудникам компании (рис. 4.40).

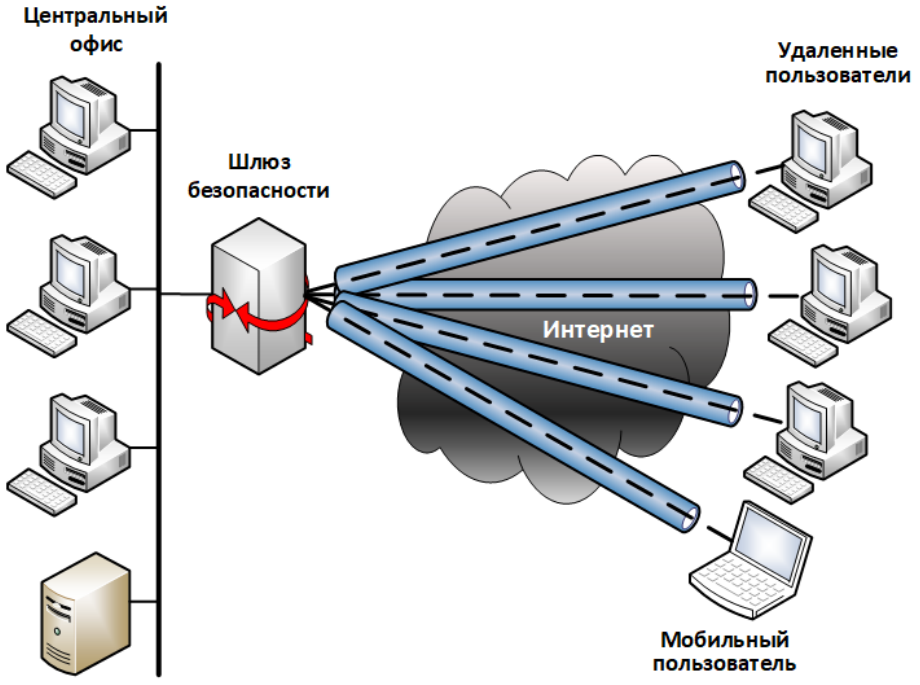


Рис. 4.40. VPN с удаленным доступом

3. Межкорпоративные сети VPN предназначены для обеспечения защищенного обмена информацией со стратегическими партнерами по бизнесу, поставщиками, крупными заказчиками, пользователями, клиентами и т.д. Extranet VPN обеспечивает прямой доступ из сети одной компании к сети другой компании и тем самым способствует повышению надежности связи, поддерживаемой в ходе делового сотрудничества (рис. 4.41).

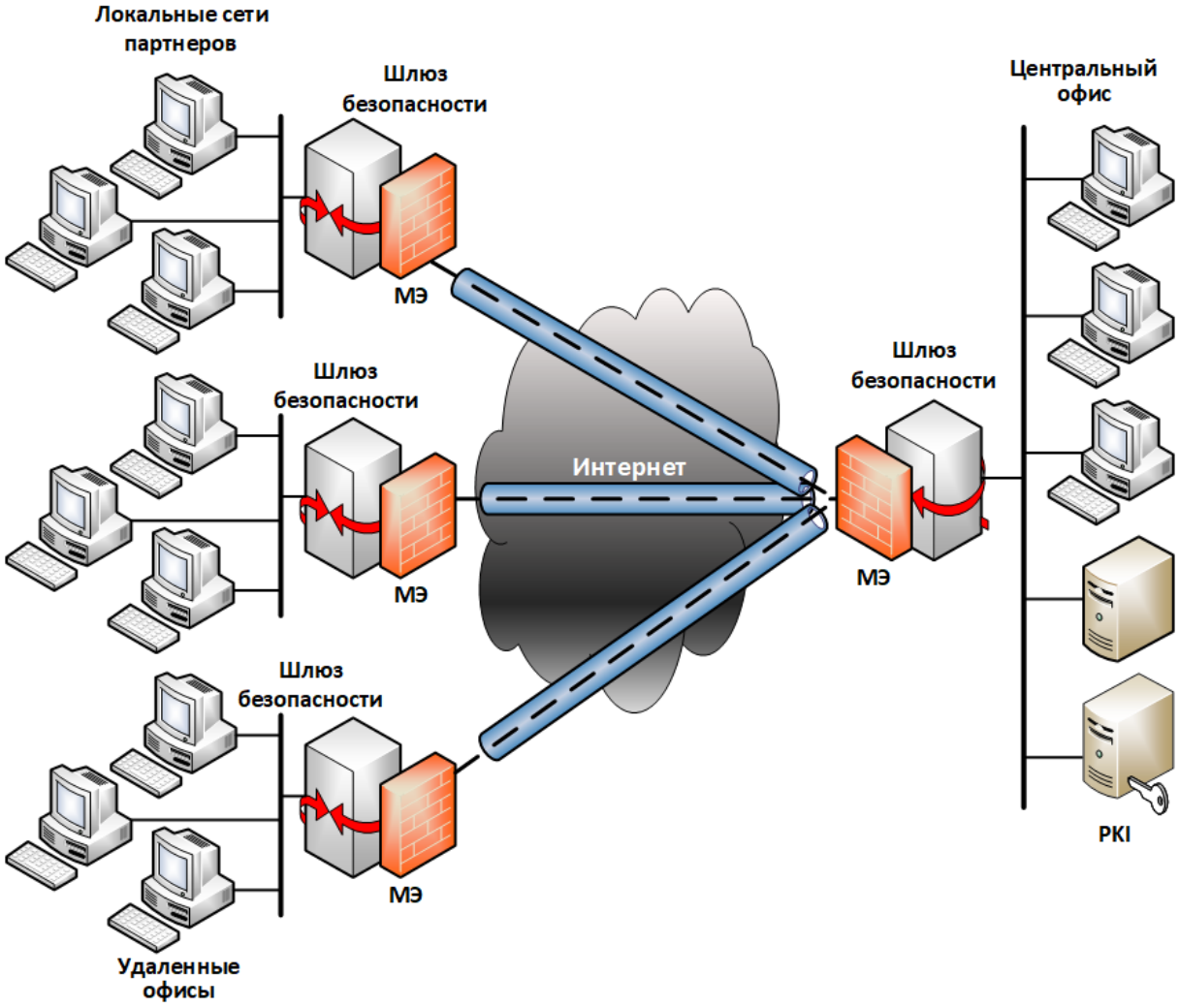


Рис. 4.41. Межкорпоративные VPN

Возможно создание комбинированной архитектуры, пример такого построения представлен на рис. 4.42.

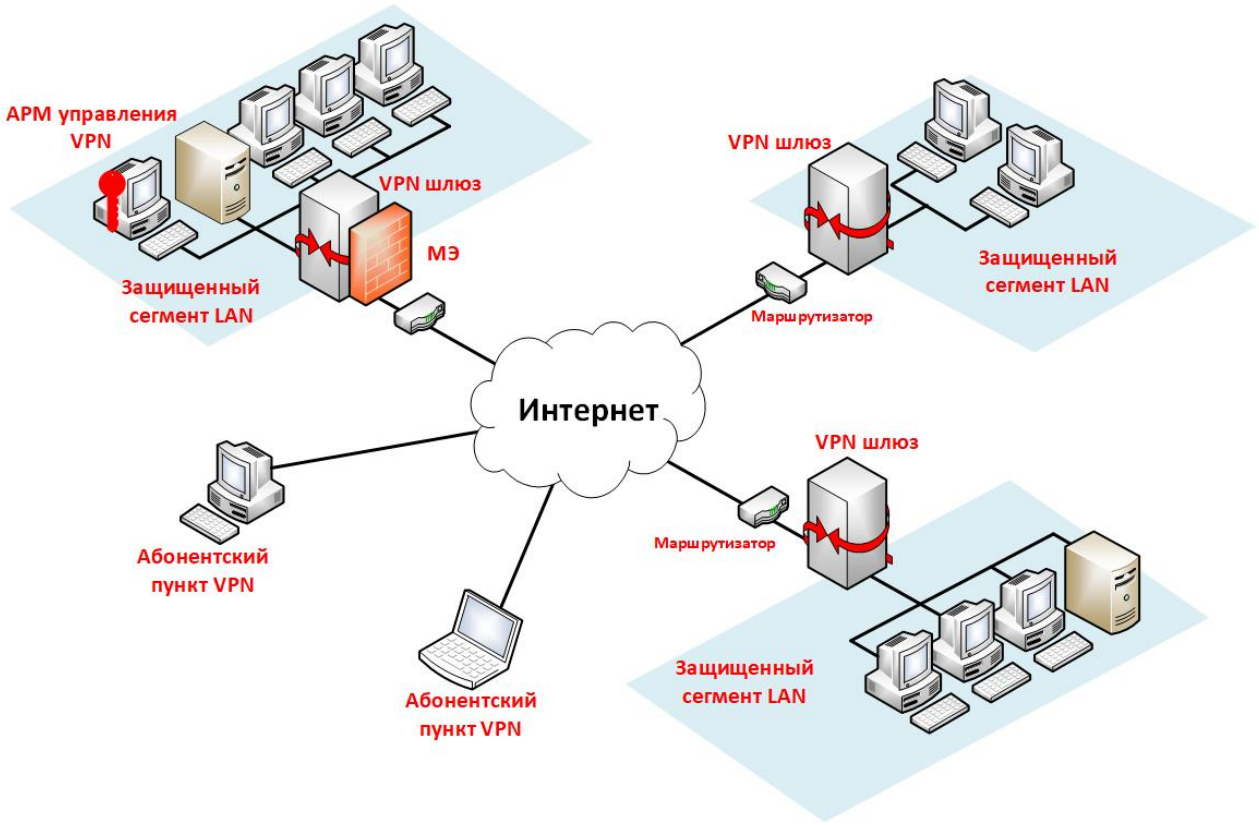


Рис. 4.42. Комбинированные структуры

По способу технической реализации различают следующие группы VPN:

1. VPN на основе маршрутизаторов. Данный способ построения VPN предполагает применение маршрутизаторов для создания защищенных каналов. Поскольку вся информация, исходящая из локальной сети, проходит через маршрутизатор, то вполне естественно возложить на него и задачи шифрования. Пример оборудования для VPN на маршрутизаторах — устройства компании Cisco Systems (рис. 4.43, 4.44).

2. VPN на основе межсетевых экранов. Межсетевые экраны большинства производителей поддерживают функции туннелирования и шифрования данных. Подобное решение подходит только для небольших сетей с относительно малым объемом передаваемой информации. Недостатками этого метода являются высокая стоимость решения в пересчете на одно рабочее место и зависимость производительности от аппаратного обеспечения, на котором работает межсетевой экран.

3. VPN на основе программного обеспечения. VPN-продукты, реализованные программным способом, с точки зрения производительности уступают специализированным устройствам, однако обладают достаточной мощностью для реализации VPN-сетей. В случае удаленного доступа требования к необходимой полосе пропускания невелики. Поэтому чисто программные продукты легко обеспечивают производительность, достаточную для удаленного доступа. Достоинством программных продуктов является гибкость и удобство в применении, а также относительно невысокая стоимость.

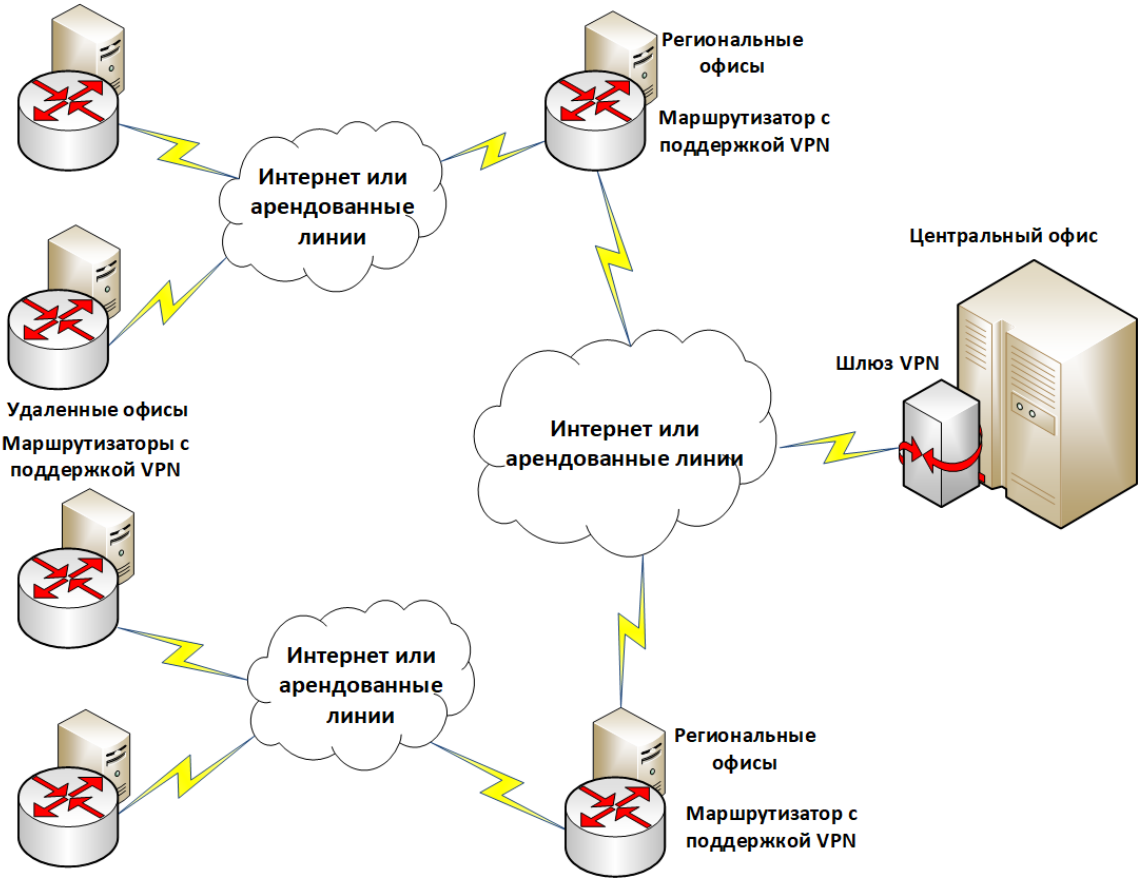


Рис. 4.43. Межсетевые взаимодействия

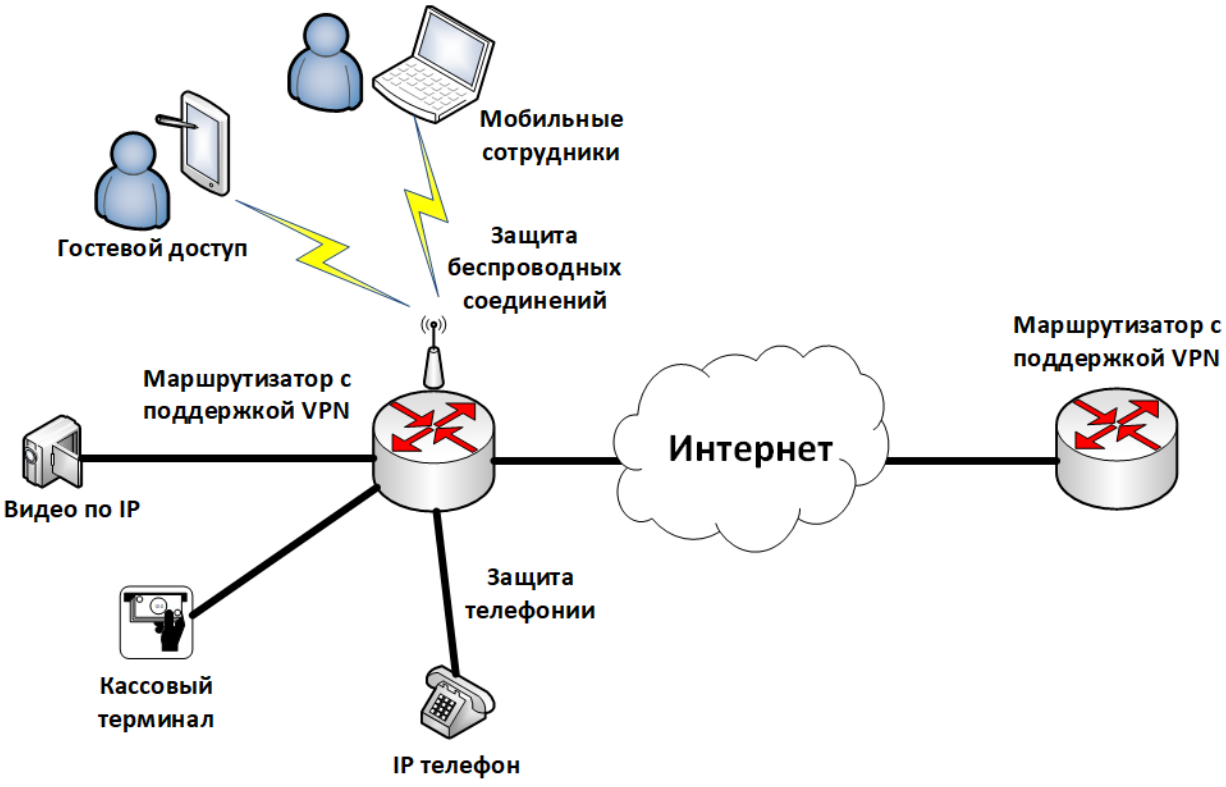


Рис. 4.44. Защита беспроводных и мультисервисных сетей

4. VPN на основе специализированных аппаратных средств со встроенными шифропроцессорами. Главным преимуществом VPN на основе специализированных аппаратных средств является их высокая производительность. Более высокое быстродействие специализированных VPN-систем обусловлено тем, что шифрование в них осуществляется специализированными микросхемами. Специализированные VPN-устройства обеспечивают высокий уровень безопасности, однако они довольно дорогие.

Далее на рис. 4.45, 4.46 представлены примеры межсетевых взаимодействий на основе VPN.

Соответствие функционирования межсетевых экранов и виртуальных защищенных сетей VPN уровням эталонной модели взаимодействия открытых систем (ISO/OSI) представлено в табл. 4.5 и 4.6.

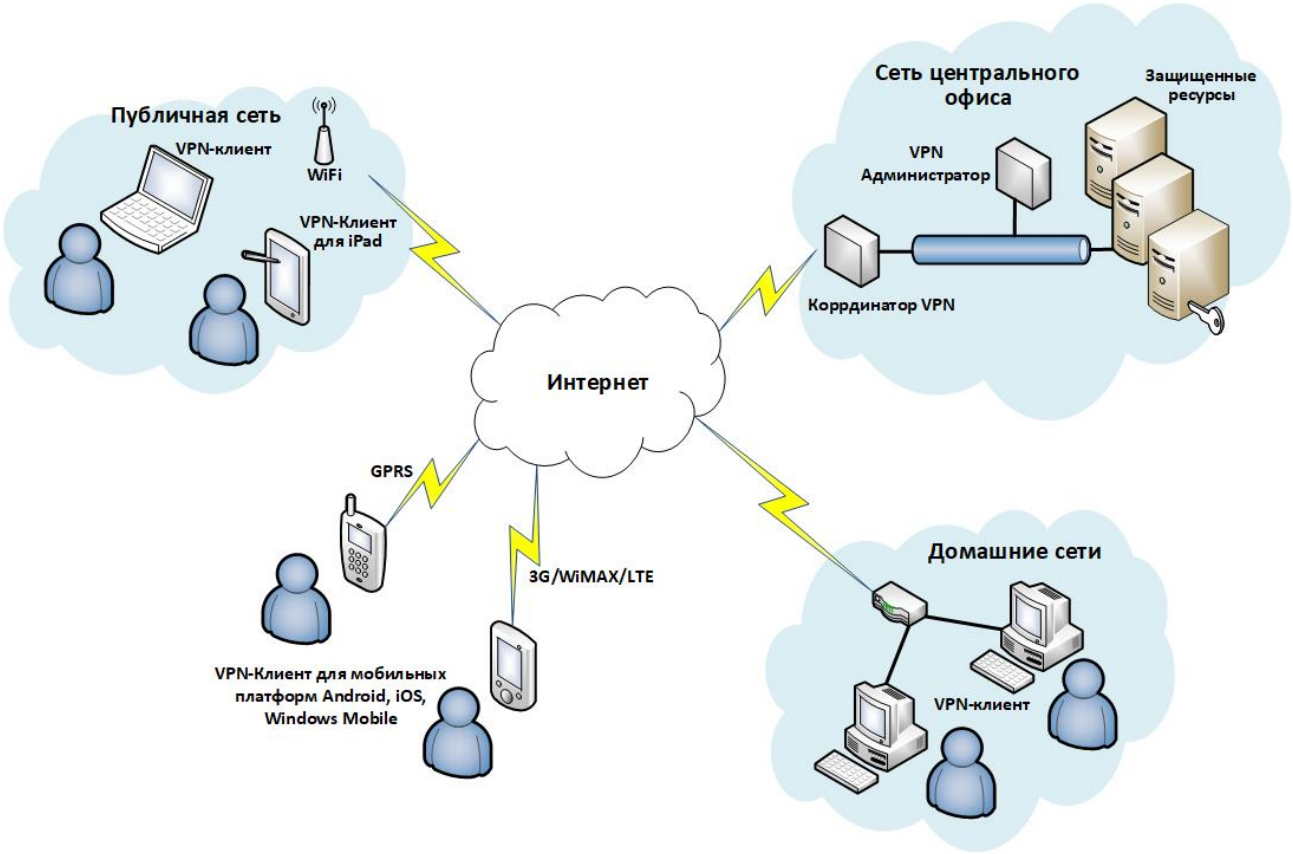


Рис. 4.45. Связь различных клиентских устройств

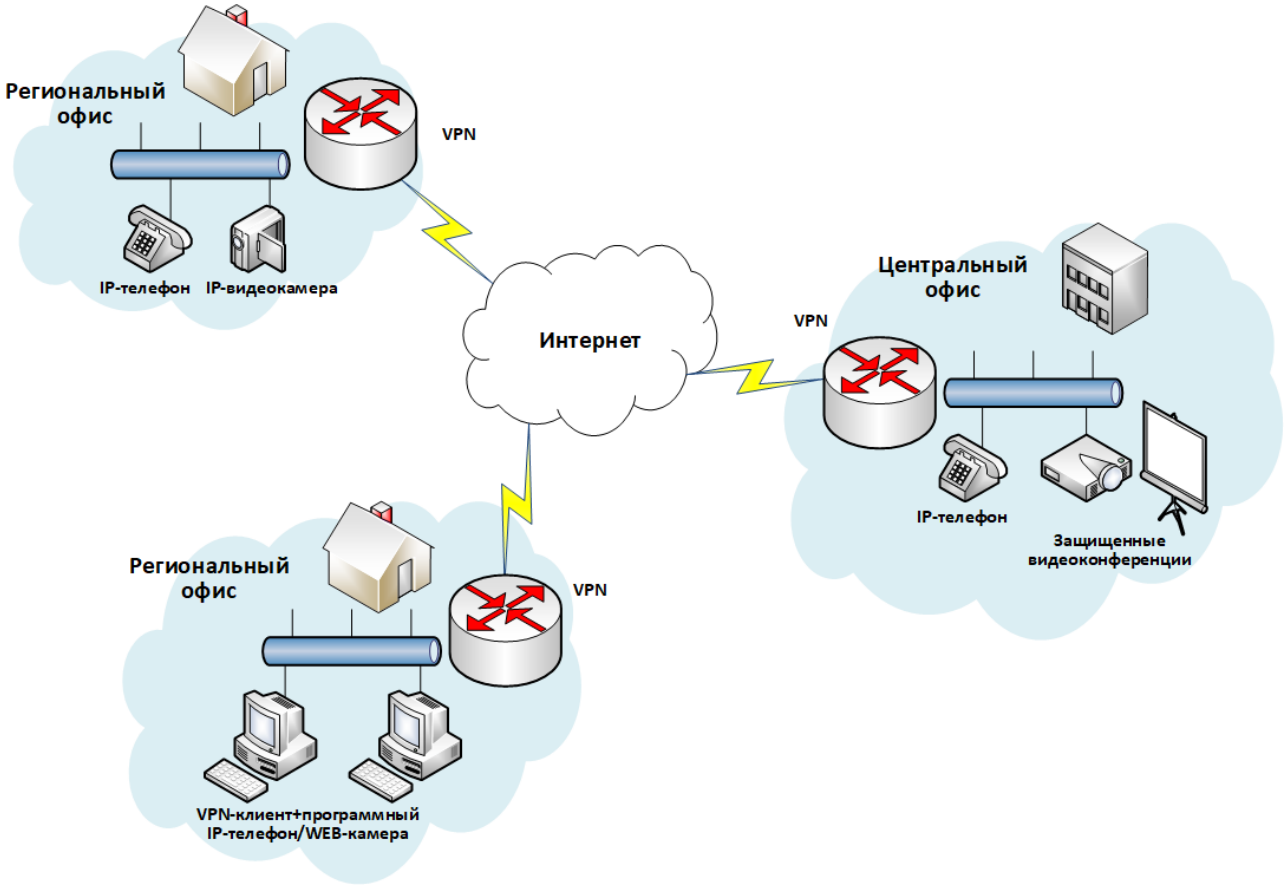


Рис. 4.46. Защищенный удаленный доступ

Таблица 4.5

Уровни функционирования МЭ

Прикладной уровень	Прикладной шлюз	Прикладной уровень
Представительский уровень		Представительский уровень
Сеансовый уровень	Шлюз сеансового уровня	Сеансовый уровень
Транспортный уровень		Транспортный уровень
Сетевой уровень	Экранирующий маршрутизатор	Сетевой уровень
Канальный уровень		Канальный уровень
Физический уровень		Физический уровень

Таблица 4.6

Уровни функционирования VPN

Прикладной уровень		Прикладной уровень
Представительский уровень		Представительский уровень
Сеансовый уровень	VPN сеансового уровня	Сеансовый уровень
Транспортный уровень		Транспортный уровень

Прикладной уровень		Прикладной уровень
Сетевой уровень	VPN сетевого уровня	Сетевой уровень
Канальный уровень	VPN канального уровня	Канальный уровень
Физический уровень		Физический уровень

4.8. Технологии резервного копирования и восстановления данных

Система резервного копирования — совокупность программного и аппаратного обеспечения, выполняющего задачу создания копии данных на носителе, предназначенном для восстановления информации в оригинальном месте их расположения в случае их повреждения или разрушения. Системы резервного копирования обеспечивают непрерывность бизнес-процессов и защиту информации от природных и техногенных катастроф, действий злоумышленников. Эти технологии активно используются в ИТ-инфраструктурах организаций самых разных отраслей и масштабов. Цель резервного копирования — понижение затрат от незапланированного уничтожения данных в нештатных ситуациях. Достигается эта путем дублирования ценных данных с рабочих машин в сторонние хранилища.

Следующие задачи определяются из целей резервного копирования:

– выделение целевых данных;

– сохранение указанных данных для последующего восстановления;

– восстановление сохраненных данных;

– обеспечение устойчивости хранимых данных к изменению и уничтожению;

– разграничение доступа к хранимым данным;

– обеспечение контроля системы и процесса резервного копирования.

Выделяют два основных метода резервного копирования — это копирование образа жесткого диска и файловое копирование.

Копирование образа жесткого диска — это создание точной копии всего жесткого диска, что позволяет восстанавливать не только данные пользователя, но и операционную систему и всю информацию о состоянии операционной системы, такую как данные системного реестра, драйверы, профили пользователей, системные настройки, программы и приложения.

Файловое копирование — это копирование файловой системы компьютера, т.е. папок и файлов, хранящихся на компьютере. Такое копирование поможет восстановить папки и файлы пользователя, но не сможет вернуть систему в рабочее состояние.

Резервное копирование информации является одним из важнейших механизмов, обеспечивающих ее доступность и целостность. Используются следующие способы резервного копирования:

1. Полное (full). В этом случае все без исключения файлы, потенциально подвергаемые резервному копированию, переносятся на резервный носитель.

2. Дифференциальное (differential). Копируются файлы, измененные с момента полного резервного копирования. Количество копируемых данных в этом случае с каждым разом возрастает.

3. Инкрементальное (incremental). Резервному копированию подвергаются только файлы, измененные с момента последнего инкрементального копирования.

На практике резервное копирование обычно осуществляется следующим образом: периодически проводится полное резервное копирование, в промежутках — инкрементальное или дифференциальное. Выбор между дифференциальным и инкрементальным резервным копированием осуществляется с учетом требуемых характеристик подсистемы резервного копирования: инкрементальное копирование выполняется быстрее, однако в случае дифференциального копирования легче восстановить оригинал по резервной копии.

По способу доступа к носителю различают:

1. Оперативное копирование (Online backup) — создание резервного архива на постоянно подключенном (напрямую или через сеть) носителе в режиме реального времени. Позволяет создавать копии файлов, каталогов и томов, не прерывая работу, без перезагрузки компьютера.

2. Автономное копирование (Offline backup) — хранение резервной копии на носителе, который перед использованием следует подключить к системе. Это может быть FTP-сервер, кассета или картридж.

Топология системы резервного копирования может соответствовать централизованной или децентрализованной схеме.

Децентрализованная схема использует общий сетевой ресурс и набор программ для резервного копирования, время от времени выгружающих информацию с серверов и рабочих станций, а также других объектов сети (например, конфигурационные файлы с маршрутизаторов) на этот ресурс. Общим ресурсом может быть общая папка или FTP-сервер. Принцип действия децентрализованной схемы представлен на рис. 4.47.

Централизованное резервное копирование использует четкую иерархическую модель, работающую по принципу «клиент — сервер». В классическом варианте на каждый компьютер устанавливаются специальные программы-агенты, а на центральный сервер — серверный модуль программного пакета (рис. 4.48).

Рис. 4.47. Децентрализованная схема резервного копирования

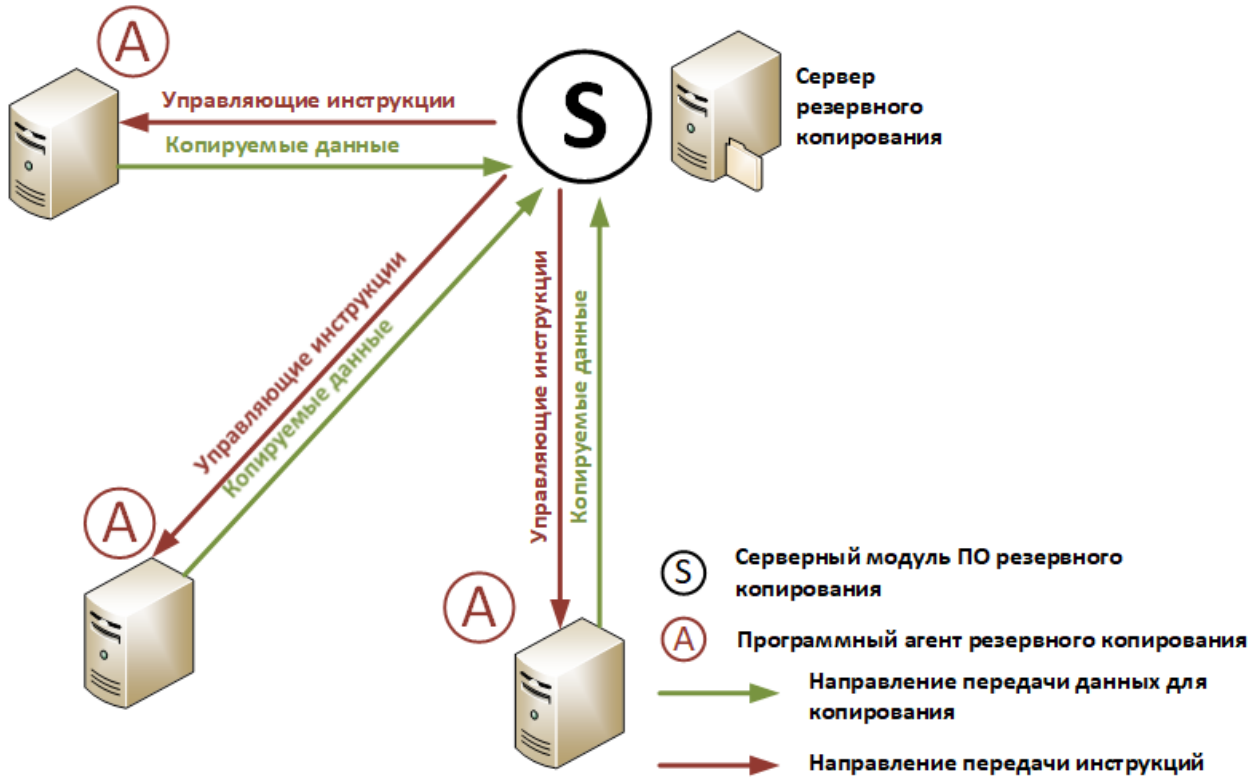


Рис. 4.48. Централизованная схема резервного копирования

Для совсем небольших организаций в некоторых случаях может использоваться упрощенный вариант централизованной схемы резервного копирования без применения программ-агентов (рис. 4.49).

Рис. 4.49. Упрощенная централизованная схема резервного копирования

Иногда организуют смешанную схему резервного копирования. Например, с серверов, для которых есть в наличии программы-агенты резервного копирования, данные собираются посредством этих агентов. Для всех остальных ресурсов используется децентрализованная схема (рис. 4.50).

Внешние системы резервного хранения данных бывают трех типов — DAS (Direct Attached Storage), SAN (Storage Area Network) и NAS (Network attached Storage), они представлены на рис. 4.51.

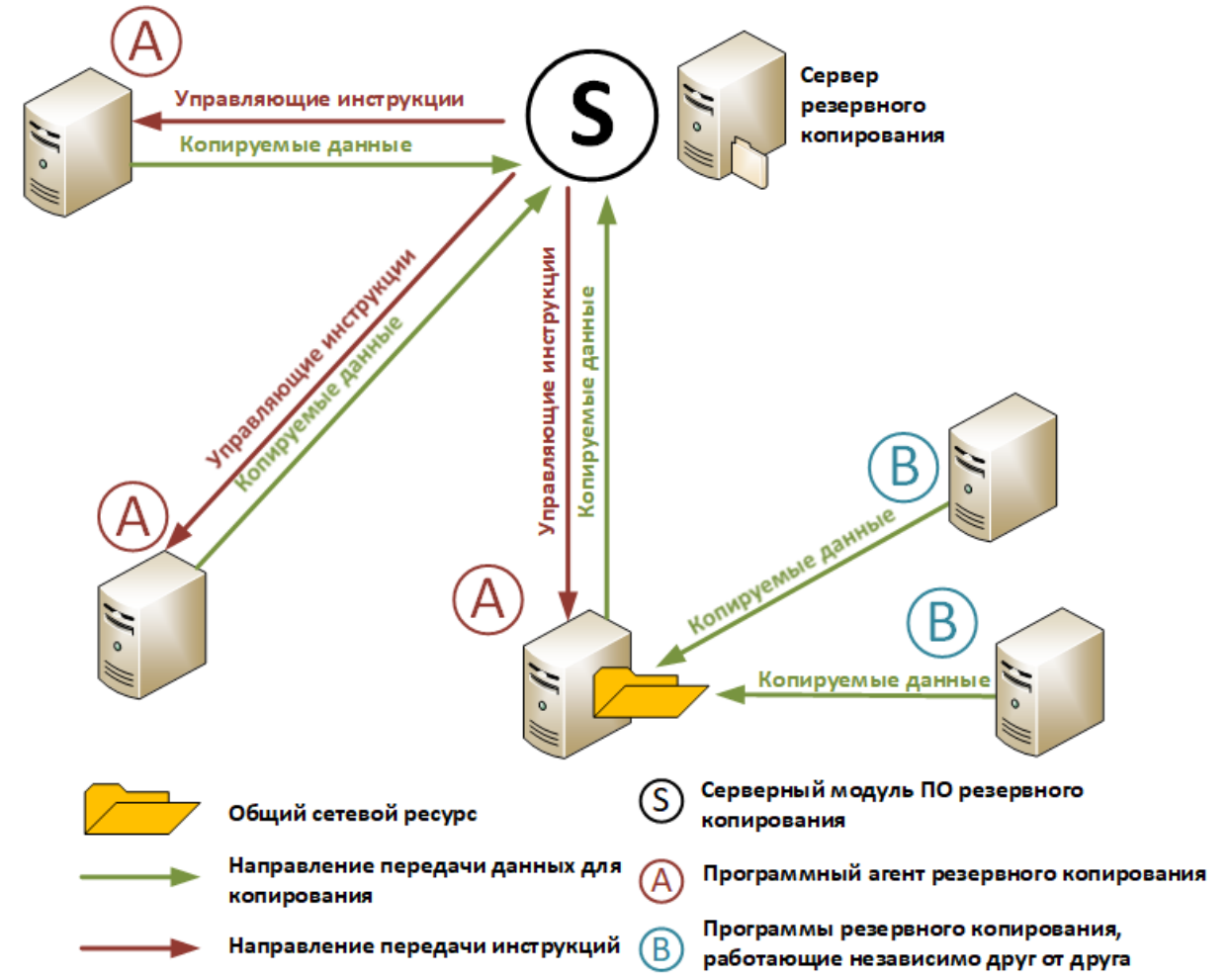


Рис. 4.50. Смешанная схема резервного копирования

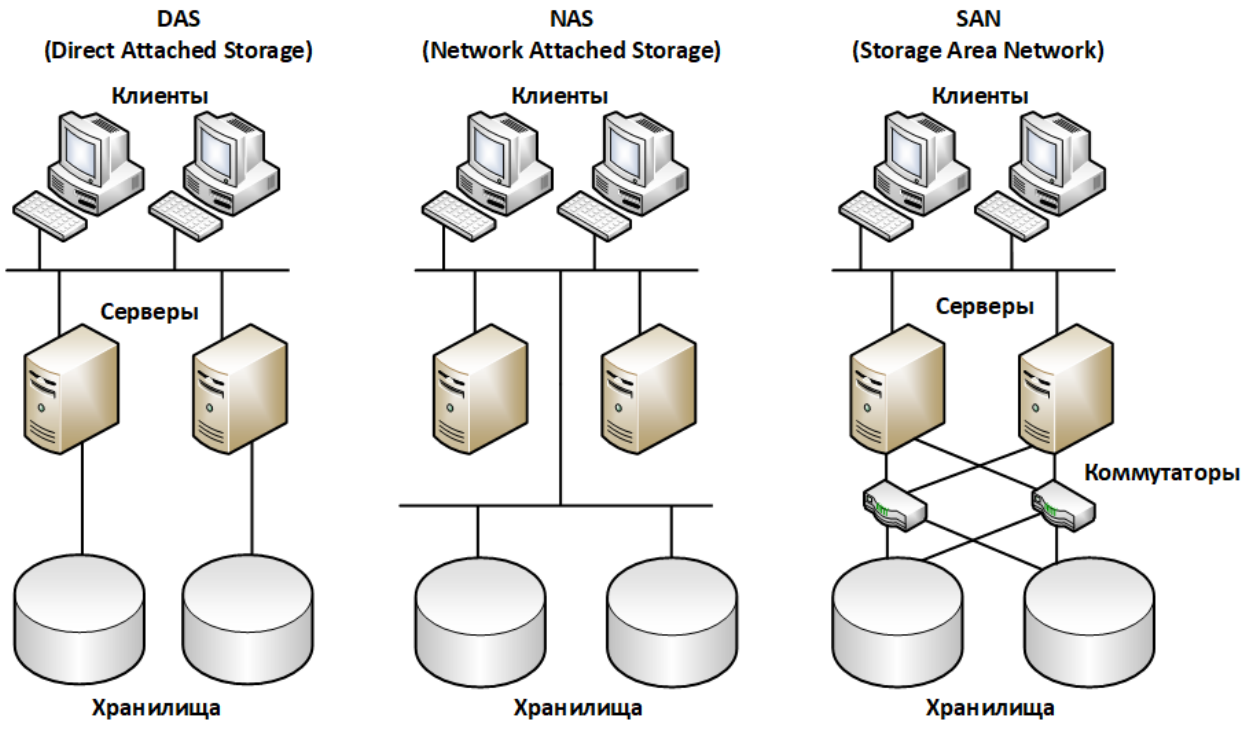


Рис. 4.51. Варианты организации хранилищ

Локальное резервное копирование и восстановление на сервере DAS (Direct Attached Storage) — устройство внешней памяти, напрямую подсоединенное к основному компьютеру и используемое только им. Простейший пример DAS — встроенный жесткий диск (рис. 4.52).

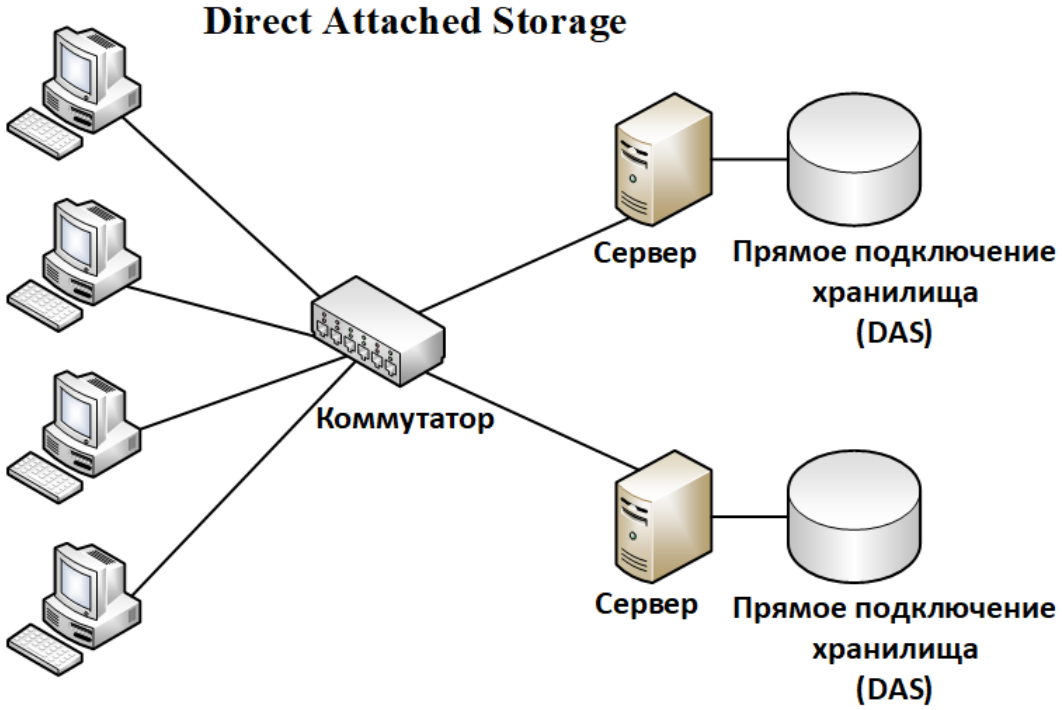


Рис. 4.52. Локальное резервное копирование

Резервное копирование и восстановление по локальной сети NAS (Network Attached Storage) обозначает сетевое устройство хранения, точнее выделенный файловый сервер, с подсоединенной к нему дисковой подсистемой (рис. 4.53).

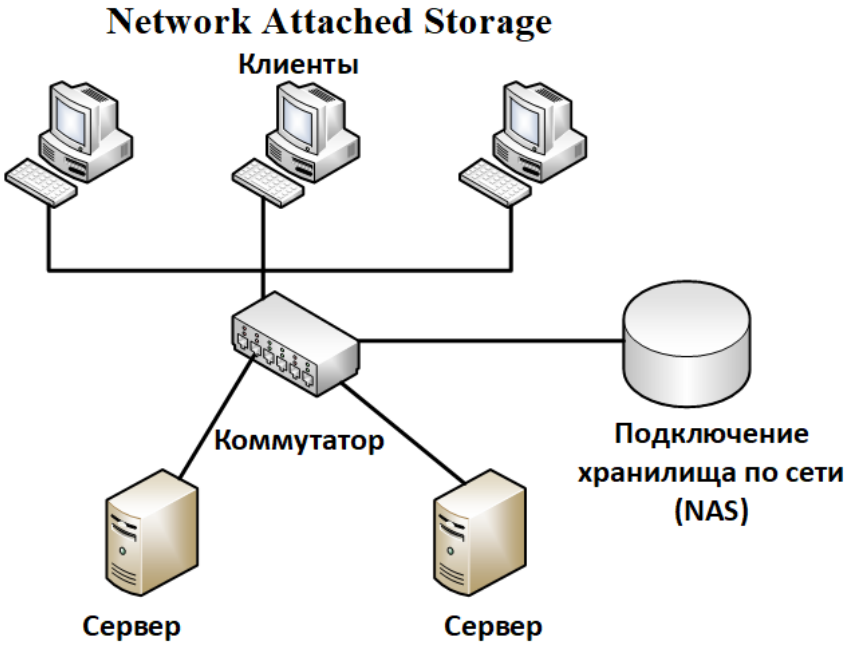


Рис. 4.53. Резервное копирование и восстановление по локальной сети

Резервное копирование и восстановление с помощью сетевых хранилищ SAN (Storage Area Network) представляет собой выделенную сеть устройств хранения, которая позволяет множеству серверов использовать совокупный ресурс внешней памяти без нагрузки на локальную сеть (рис. 4.54).

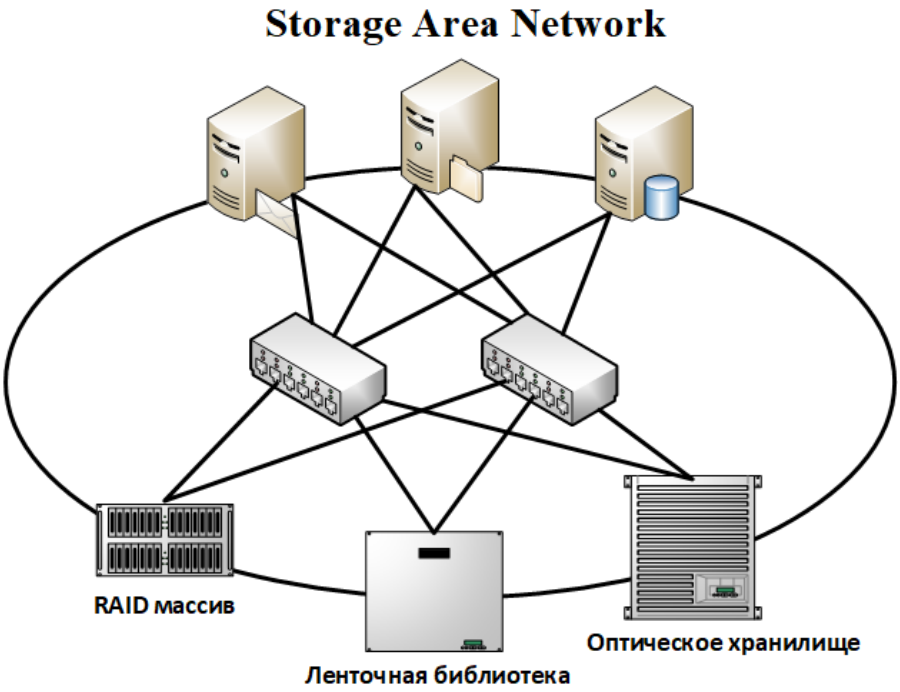


Рис. 4.54. Резервное копирование и восстановление
с помощью сетевых хранилищ

Хранение резервных копий возможно на различных носителях:

– лента стримера — запись резервных данных на магнитную ленту стримера;

– «облачный» бэкап — запись резервных данных по «облачной» технологии через онлайн-службы специальных провайдеров;

– DVD или CD — запись резервных данных на компактные диски;

– HDD — запись резервных данных на жесткий диск компьютера;

– LAN — запись резервных данных на любую машину внутри локальной сети;

– FTP — запись резервных данных на FTP-серверы;

– USB — запись резервных данных на любое USB-совместимое устройство (такое как флэш-карта или внешний жесткий диск).

Резервирование при обработке информации осуществляется путем зеркального копирования. Зеркальное копирование (способ копирования с двухсторонней синхронизацией) — этот способ предполагает, что как только на диске появляется новый файл, он тут же появляется и в копии (в режиме реального времени). Достигается такой режим в частности путем использования RAID-технологии (Redundant Array of Independed Disks — избыточный массив

независимых дисков), основанной на системе специальным образом сконфигурированных жестких дисков.

Возможны аппаратная или программная реализации RAID. Аппаратная реализация является более эффективной и основана на подключении жестких дисков через специальные RAID-контроллеры. Такой контроллер выполняет функции связи с сервером (рабочей станцией), генерации избыточной информации при записи и проверки при чтении, распределения информации по дискам в соответствии с алгоритмом функционирования. Принцип работы программной реализации состоит в следующем: на основе двух разделов, расположенных на двух разных физических дисках, создается так называемый зеркальный (отказоустойчивый) том (Mirror Volume). Ему присваивается собственная буква диска (исходные разделы дисков лишаются таковой вообще), и при выполнении каких-либо операций над данными этого тома все изменения синхронно отражаются в обоих исходных разделах.

Уровни RAID:

RAID 0 — полосование. Содержимое файла записывается одновременно на несколько дисков массива, работающих как один дисковод большой емкости. Этот уровень обеспечивает высокую скорость выполнения операций чтения (записи), но очень низкую надежность. Для реализации уровня необходимы минимум два дисковода.

RAID 1 — зеркальное отражение. Данные, записанные на одном диске, дублируются на другом, что обеспечивает высокую отказоустойчивость (при повреждении одного диска данные считываются с другого). При этом заметного повышения эффективности матрицы по сравнению с отдельным дисководом не происходит. Для реализации уровня необходимы минимум два диска.

RAID 2 — код коррекции ошибок на уровне битов. Одновременно происходит побитовое дробление данных и запись кода коррекции ошибок на нескольких дисках. Он обеспечивает высокую скорость передачи данных и достаточную надежность матрицы. В то же время для достижения хотя бы 50%-ной эффективности необходимо минимум семь дисков (4 диска с данными, 3 диска с кодами коррекции ошибок).

Зеркалирование серверов в целом аналогично зеркалированию дисковых накопителей: идентичные данные в целях защиты от сбоев оборудования записываются на два независимых сервера. Речь в данном случае идет исключительно о хранении данных. Дублирование серверов, в свою очередь, позволяет обеспечить полноценную замену сервера в случае его сбоя за счет передачи управления резервному серверу. В случае отказа основного сервера резервный сервер, постоянно синхронизирующийся с основным с использованием failover-связи, оперативно перехватит управление (рис. 4.55).

Использование кластеров позволяет наиболее эффективно обеспечить балансировку нагрузки между несколькими серверами. Кластером называется группа независимых серверов, управляемых как единая система. В отличие от механизма дублирования в данном случае все серверы являются активными и принимают полноценное участие в обслуживании запросов клиентов.

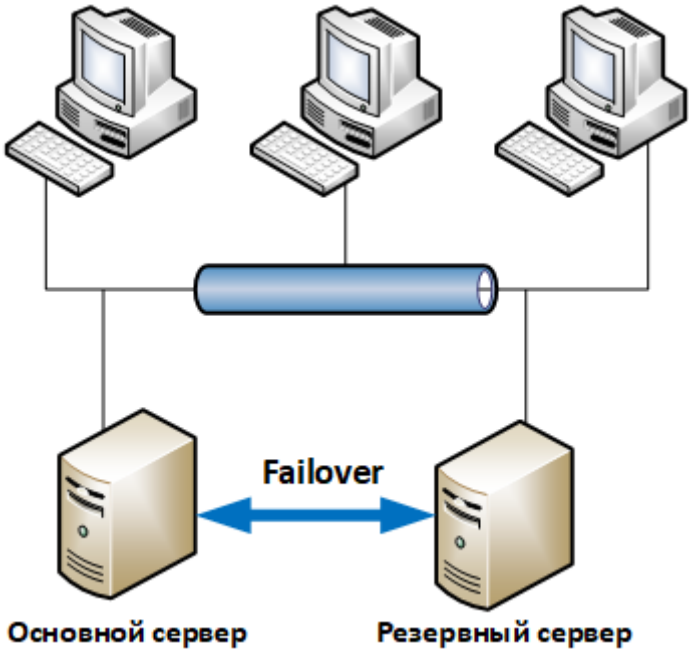


Рис. 4.55. Дублирование серверов

В качестве накопителей данных могут использоваться:

– дисковые хранилища;
– стримеры;
– магнитные картриджи.

Плотность записи на магнитных картриджах — 201 гигабит на 1 квадратный дюйм (чуть больше 31 гигабита на 1 см^2), что доводит возможный объем картриджа до 330 терабайт.

4.9. DLP-системы

DLP — Data Loss Prevention, Data Leak Prevention или Data Leakage Protection, что можно перевести на русский как «предотвращение потери данных», «предотвращение утечки данных», «защита от утечки данных». Под DLP-системами понимают программное обеспечение, предназначенное для предотвращения потери данных путем обнаружения возможных нарушений при фильтрации и отправке. Данные сервисы также осуществляют мониторинг, обнаружение и блокирование конфиденциальной информации при ее использовании, движении и хранении. DLP-системы направлены на минимизацию рисков внутренних угроз информационной безопасности, или, иными словами, на защиту корпоративной информации от инсайдеров. Первые DLP-системы возникли именно как средство предотвращения утечки ценной информации. Они были предназначены для обнаружения и блокирования сетевой передачи информации, опознаваемой по ключевым словам или выражениям и по заранее созданным цифровым «отпечаткам» конфиденциальных документов. Дальнейшее развитие DLP-систем определялось инцидентами, с одной стороны, и законодательными актами государств — с другой. После-

пенно потребности по защите от различных видов угроз привели компании к необходимости создания комплексных систем защиты. В настоящее время развитые DLP-продукты, кроме непосредственно защиты от утечки данных, обеспечивают защиту от внутренних и даже внешних угроз, учет рабочего времени сотрудников, контроль всех их действий на рабочих станциях, включая удаленную работу.

DLP-системы различают по способу обнаружения утечки данных:

– при использовании (Data-in-Use) — на рабочем месте пользователя;

– при передаче (Data-in-Motion) — в сети компании;

– при хранении (Data-at-Rest) — на серверах и рабочих станциях компании.

Компонента для рабочих станций и ноутбуков позволяет контролировать все каналы, по которым может произойти утечка. Эти каналы включают в себя копирование на USB, CD/DVD или сетевое хранилище, печать и отправку факса. Кроме того, контролируются e-mail, веб-сервисы, такие сетевые протоколы, как FTP и IM, в том числе тогда, когда компьютер отключен от корпоративной сети. Она также позволяет сканировать внутренние жесткие диски компьютера и находить конфиденциальную информацию.

Компонента сетевого уровня находит места, где конфиденциальная информация выходит за пределы компании, и блокирует ее утечку. Программное обеспечение, которое устанавливается в точках сети, исходящих вблизи периметра. Это дополнительный уровень, позволяющий контролировать смартфоны, гостевые ноутбуки, неподдерживаемые ОС (MAC, Linux) и т.д.

Компонента для баз данных и корпоративных хранилищ обеспечивает защиту и полномасштабный поиск конфиденциальной информации не только на уровне рабочих станций и ноутбуков, но и среди баз данных, веб-серверов, файл-серверов и в других хранилищах.

Типичная схема развертывания DLP-системы на информационную инфраструктуру организации показана на рис. 4.56.

По сетевой архитектуре DLP-системы подразделяются на две большие группы:

– шлюзовые — используется единый сервер, на который направляется весь исходящий сетевой трафик корпоративной информационной системы. Этот шлюз занимается его обработкой в целях выявления возможных утечек конфиденциальных данных (рис. 4.57, 4.58).

– хостовые — основаны на использовании специальных программ — агентов, которые устанавливаются на конечных узлах сети — рабочих станциях, серверах приложений и пр. (рис. 4.59).

У шлюзового решения могут быть два различных режима работы: блокирование и мониторинг трафика.

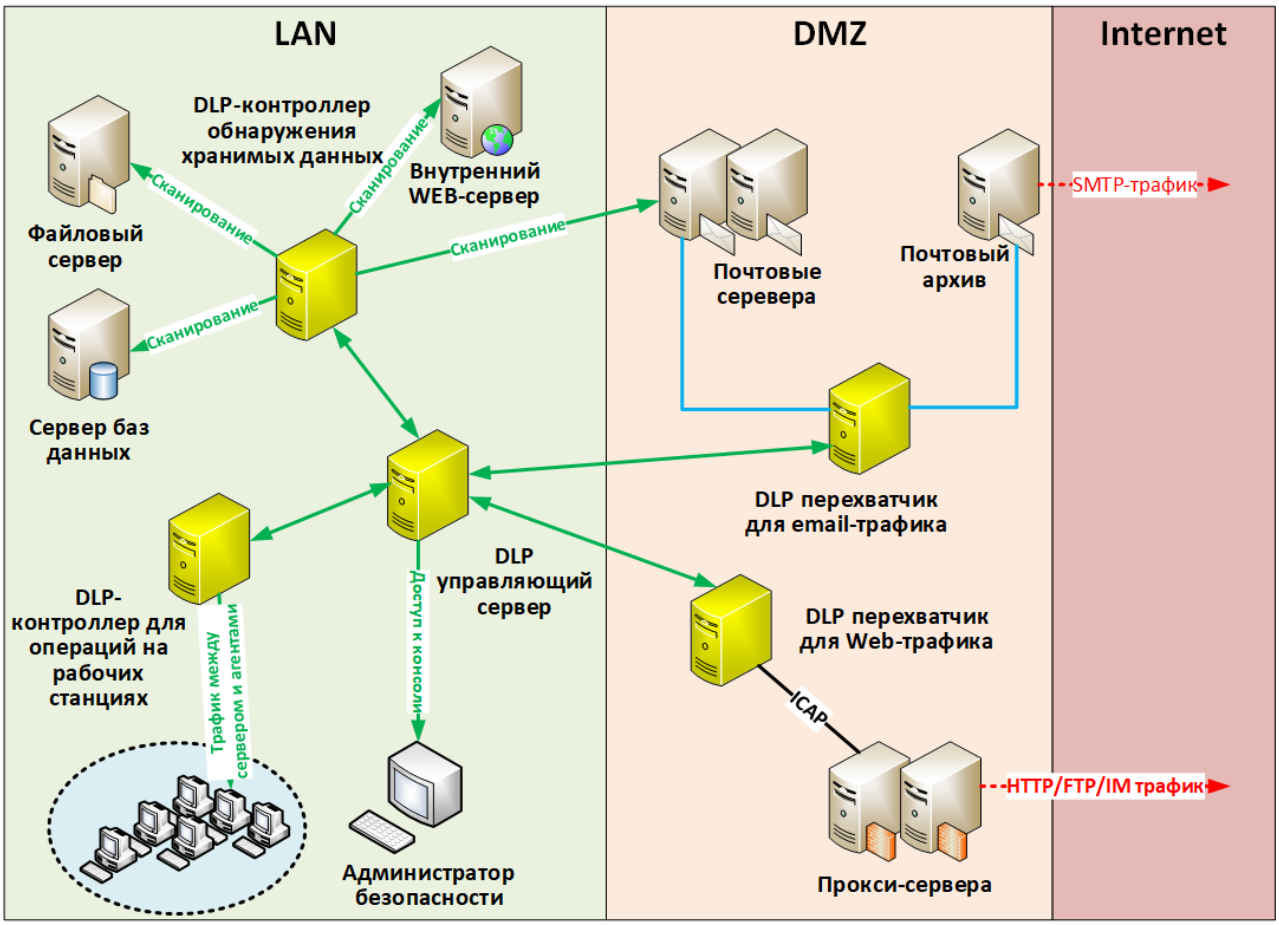


Рис. 4.56. Размещение модулей DLP-системы

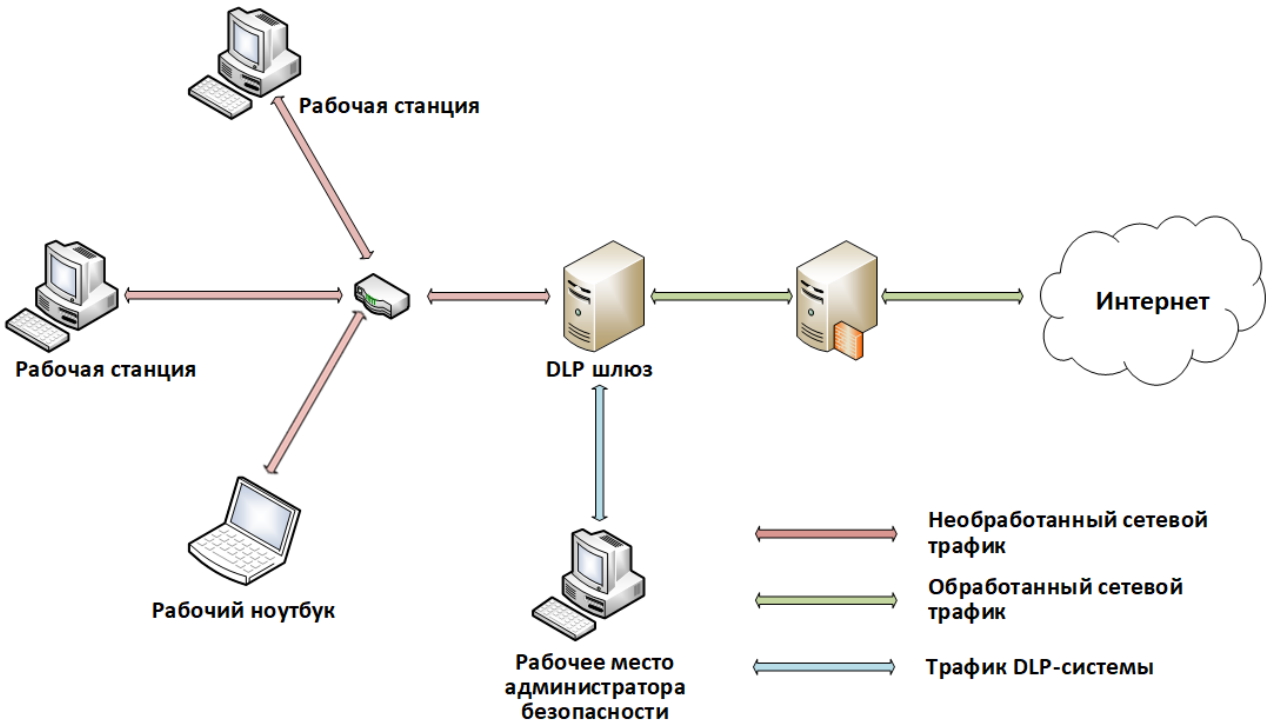


Рис. 4.57. Функциональная схема шлюзового решения, работающего в режиме блокирования

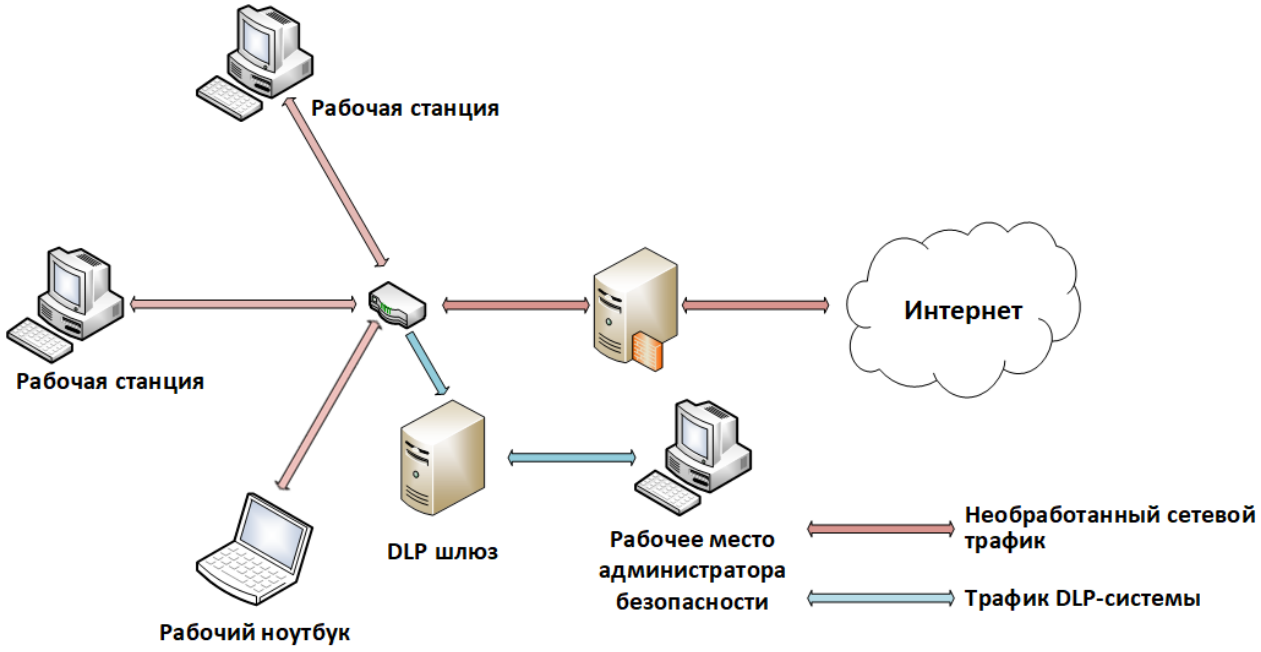


Рис. 4.58. Функциональная схема шлюзового решения,
работающего в режиме мониторинга

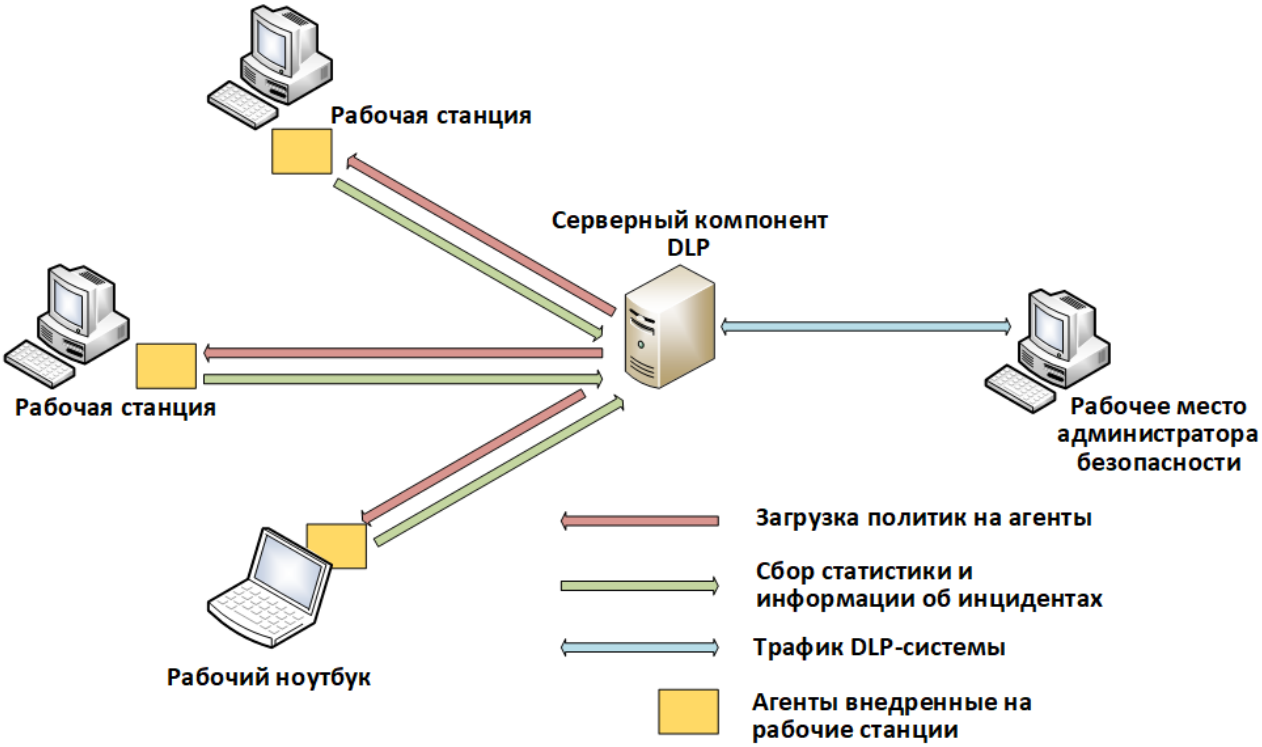


Рис. 4.59. Функциональная схема хостового DLP-решения

DLP-системы могут распознавать критичные документы:

– по формальным признакам — это надежно, но требует предваритель-ной регистрации документов в системе;

– по анализу содержимого — это может давать ложные срабатывания, но позволяет обнаруживать критичную информацию в составе любых документов.

Методы детектирования конфиденциальной информации:

– по описанию контента;

– по индексированию таблиц, баз данных и т.д. (для структурированных данных);

– по индексированию документов (для неструктурированных данных).

Технология детектирования по описанию контента обеспечивает высокий уровень точности и наиболее полезна в тех случаях, когда невозможно или нецелесообразно получить копию информации для индексирования или когда точное содержание неизвестно, но есть его подробное описание. Технология работает как со структурированными, так и неструктурированными данными, используя идентификаторы данных, ключевые слова, словари, сравнение по образцам, сопоставление по типу и размеру файлов, по имени отправителя, получателя и пользователя, по информации о группе пользователей в каталоге AD.

Детектирование по индексированию таблиц, баз данных и т.д. (для структурированных данных) позволяет защитить персональные данные клиентов и сотрудников, а также другие структурированные данные, которые систематизированы в какой-либо базе данных. Например, можно установить политику, в соответствии с которой система будет обнаруживать любые три значения из полей «Имя», «Фамилия», «Номер паспорта», «Номер счета» и «Номер телефона», если эти значения встречаются вместе в письме и соответствуют записи в базе данных.

Технология детектирования по индексированию документов (для неструктурированных данных) обеспечивает точное детектирование неструктурированных данных, сохраненных в виде документов, таких как документы Microsoft Word и PowerPoint, PDF, проектные планы, файлы исходного кода, чертежи CAD/CAM-систем, финансовые отчеты, а также другие виды информации, составляющей государственную, коммерческую и частную тайну. Технология создает сигнатуры для обнаружения выдержек исходного документа, черновиков или различных версий защищаемых документов, а также точных совпадений контента в бинарной форме.

Современная система защиты от утечки информации, как правило, является распределенным программно-аппаратным комплексом, состоящим из большого числа модулей различного назначения. Часть модулей функционирует на выделенных серверах, часть — на рабочих станциях сотрудников компании, часть — на рабочих местах сотрудников службы безопасности. Выделенные сервера могут потребоваться для таких модулей, как база данных, и иногда для модулей анализа информации. Эти модули являются ядром DLP-системы. База данных необходима для хранения информации, начиная от правил контроля и подробной информации об инцидентах и заканчивая всеми документами, попавшими в поле зрения системы за определенный период. В некоторых случаях система даже может хранить копию всего сетевого трафика компании, перехваченного в течение заданного периода времени. Модули анализа информации от-

вечают за анализ текстов, извлеченных другими модулями из различных источников: сетевой трафик, документы на любых устройствах хранения информации в пределах компании. В некоторых системах есть возможность извлечения текста из изображений и распознавание перехваченных голосовых сообщений. Все анализируемые тексты сопоставляются с заранее заданными правилами и отмечаются соответствующим образом при обнаружении совпадения. Для контроля действий сотрудников на их рабочие станции могут быть установлены специальные агенты. Такой агент должен быть защищен от вмешательства пользователя в свою работу (на практике это не всегда так) и может как вести пассивное наблюдение за его действиями, так и активно препятствовать тем из них, которые пользователю запрещены политикой безопасности компании. Перечень контролируемых действий может ограничиваться входом (выходом) пользователя из системы и подключением USB-устройств, а может включать перехват и блокировку сетевых протоколов, теневое копирование документов на любые внешние носители, печать документов на локальные и сетевые принтеры, передачу информации по Wi-Fi и Bluetooth и много другое. Некоторые DLP-системы способны записывать все нажатия на клавиатуре (key-logging) и сохранять копии экрана (screen-shots).

Вопросы для самоконтроля

1. Что значит разграничение и контроль доступа к информации?
2. Аутентификация, авторизация и администрирование действий пользователей.
3. Разновидности методов использования паролей.
4. Перечислите методы идентификации и установления подлинности субъектов и различных объектов.
5. Что такое аппаратные средства аутентификации?
6. Виды аппаратных средств аутентификации и примеры их использования.
7. Что такое биометрическая аутентификация пользователя?
8. Какие разновидности биометрической аутентификации вы знаете?
9. Проблемы обеспечения безопасности ОС.
10. Функции межсетевых экранов.
11. Основные понятия и функции сети VPN.
12. Технологии обнаружения вторжений.
13. Технология анализа защищенности.
14. Дайте определение идентификации и аутентификации пользователя. В чем разница между этими понятиями?
15. Перечислите основные способы аутентификации. Какой, на ваш взгляд, является наиболее эффективным?
16. Приведите классификацию моделей разграничения доступа. Какова их роль в теории информационной безопасности?
17. Каковы основные достоинства и недостатки дискреционных моделей?

18. Приведите примеры использования дискреционных моделей разграничения доступа.

19. В чем суть мандатной политики разграничения доступа?

20. Каковы основные достоинства и недостатки мандатной политики?

5. ПРИНЦИПЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. История криптографии

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. Обобщенная схема представлена на рис. 5.1.

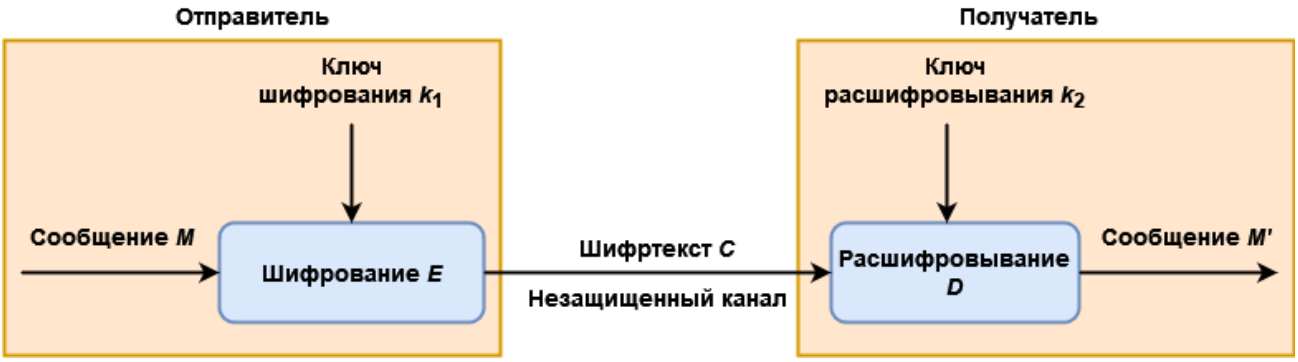


Рис. 5.1. Обобщенная схема криптосистемы шифрования

Зашифровывание информации — процесс преобразования открытой информации (исходный текст) в зашифрованный текст (шифртекст).

Расшифровывание — процесс восстановления исходного текста по криптограмме с использованием ключа шифрования (дешифрование).

Криптографическое преобразование:

$$C = E_{k1}(M),$$

где M — исходный текст передаваемого сообщения (или хранимой информации); E_{k1} — функция криптографического преобразования; k_1 — параметр функции E, называемый ключом шифрования.

Обратное преобразование:

$$M' = D_{k2}(C),$$

где D — является обратной к функции E.

История криптографии насчитывает около 4 тыс. лет. В качестве основного критерия периодизации криптографии возможно использовать технологические характеристики используемых методов шифрования.

Первый период (приблизительно с 3-го тысячелетия до н.э.) характеризуется господством моноалфавитных шифров (основной принцип — замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами).

Второй период (хронологические рамки — с IX в. на Ближнем Востоке (Ал-Кинди) и с XV в. в Европе (Леон Баттиста Альберти) — до начала XX в.) ознаменовался введением в обиход полиалфавитных шифров.

Третий период (с начала и до середины XX в.) характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.

Четвертый период — с середины до 70-х гг. XX в. — период перехода к математической криптографии. В работе Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам — линейному и дифференциальному криптоанализам. Однако до 1975 г. криптография оставалась «классической», или же, более корректно, криптографией с секретным ключом.

Современный период развития криптографии (с конца 1970-х гг. по настоящее время) отличается зарождением и развитием нового направления — криптография с открытым ключом. Ее появление знаменуется новыми техническими возможностями и сравнительно широким распространением криптографии для использования частными лицами. Правовое регулирование использования криптографии частными лицами в разных странах сильно различается — от разрешения до полного запрета.

5.2. Классические шифры

Шифр сдвига — процесс шифрования заключается в замене каждой буквы на другую, отстоянную от исходной на определенное число позиций в алфавите в зависимости от значения ключа. Такой шифр получил название шифра Цезаря (рис. 5.2).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Рис. 5.2. Шифр сдвига

Шифр замены — для того чтобы воспользоваться этим алгоритмом, создается таблица с исходным алфавитом и непосредственно под ним тот же алфавит, но с переставленными буквами (или любой другой набор знаков). Пример на рис. 5.3.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	E	X	G	W	I	Q	V	L	O	U	M	P	J	R	S	T	N	K	H	F	Y	Z	A	D	C

Рис. 5.3. Шифр замены

Один из путей решения указанной проблемы состоит в том, чтобы брать несколько наборов символов вместо стандартного алфавита и шифровать буквы открытого текста, выбирая соответствующие знаки из разных наборов в определенной последовательности. Шифры такого типа носят название полиалфавитных шифров замены. Классическим примером является Шифр Виженера. В шифре Цезаря каждая буква алфавита сдвигается на несколько позиций; например, в шифре Цезаря при сдвиге +3 A стало бы D, B стало бы E и т.д. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться

таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причем каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря (рис. 5.4). На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Рис. 5.4. Квадрат Виженера, или таблица Виженера

Шифры перестановки, или транспозиции, изменяют только порядок следования символов или других элементов исходного текста. Шифры одинарной (простой) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые один раз. Шифры множественной (сложной) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые несколько раз. Пример применения

шифра двойной перестановки представлен ниже на рис. 5.5. Ключ столбцов в шифре 2413, а ключ строк — 4123.

	2	4	1	3
4	Б	А	Й	Т
1	Ы	С	О	Х
2	Р	А	Н	Я
3	Ю	Т	С	Я

	1	2	3	4
4	Й	Б	Т	А
1	О	Ы	Х	С
2	Н	Р	Я	А
3	С	Ю	Я	Т

	1	2	3	4
1	О	Ы	Х	С
2	Н	Р	Я	А
3	С	Ю	Я	Т
4	Й	Б	Т	А

Рис. 5.5. Двойная перестановка

Еще один классический шифр, получивший известность, основан на использовании решетки Кардано. Решетка при наложении на лист бумаги оставляет открытыми лишь некоторые его части. При зашифровке буквы сообщения вписываются в эти отверстия. Пример решетки Кардано показан на рис. 5.6.

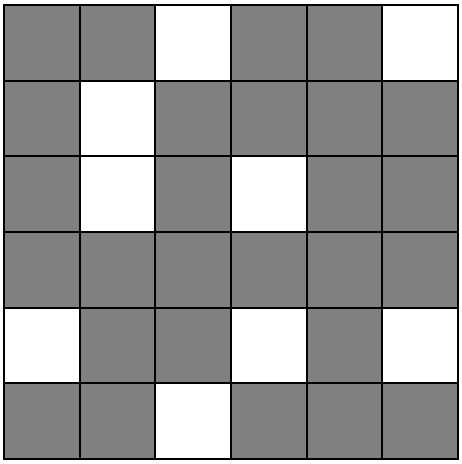


Рис. 5.6. Пример решетки Кардано

Размерность решетки может быть разной и пример ее использования показан на рис. 5.7. Здесь шифруется фраза «от жара и вода кипит».

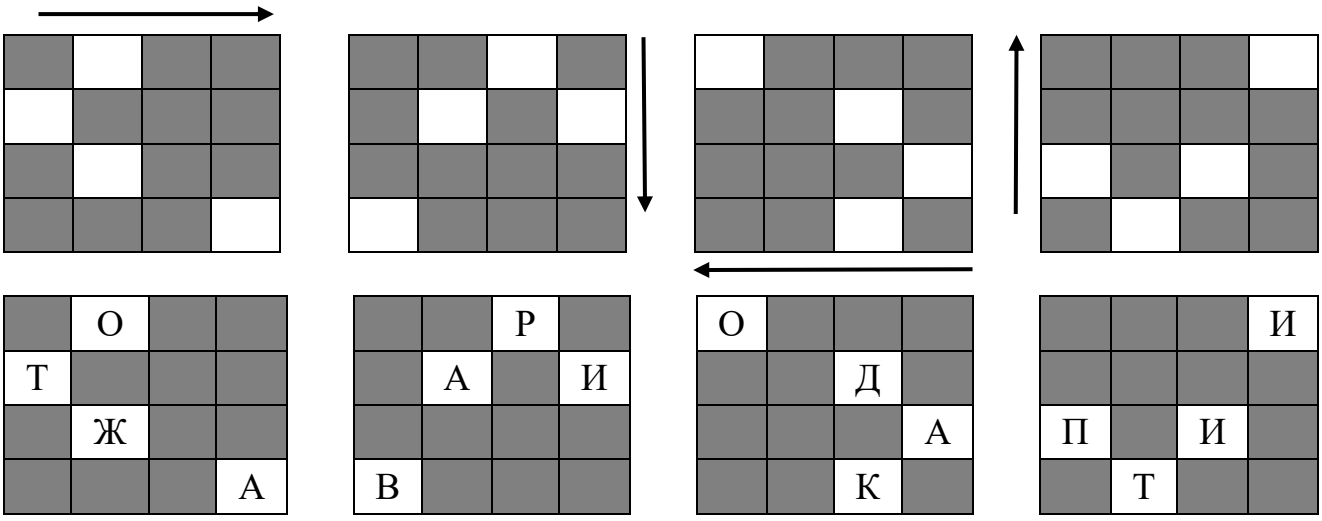


Рис. 5.7. Применение решетки Кардано

5.3. Симметричные криптосистемы

В современной криптографии различают два класса криптосистем: симметричные и асимметричные.

Симметричные криптосистемы (с единым ключом) — используется один и тот же ключ для зашифровывания и расшифровывания информации.

Асимметричные криптосистемы (с двумя ключами) — для шифрования информации и ее последующего расшифровывания используются различные ключи.

Сначала рассмотрим подробнее симметричные криптосистемы, так как они возникли исторически первыми и были единственными до 1975 г. Обобщенная схема такой системы представлена на рис. 5.8.

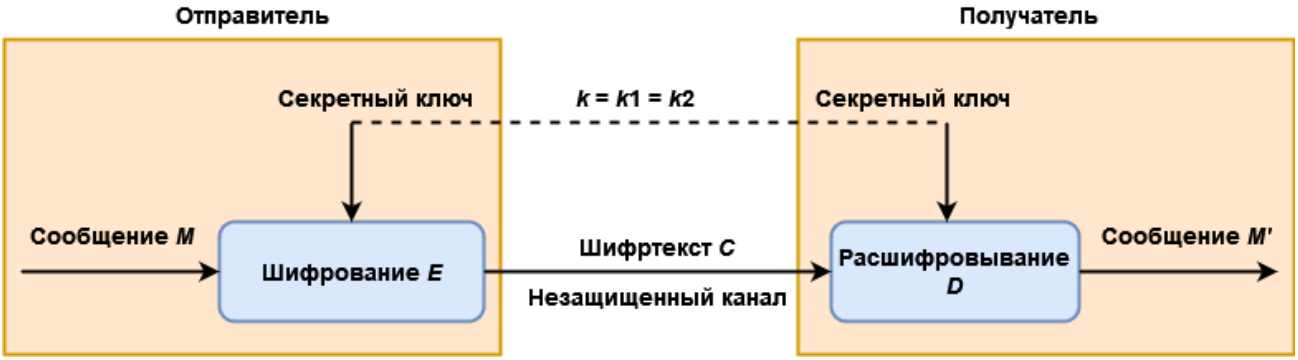


Рис. 5.8. Схема симметричной криптосистемы шифрования

Симметричные криптосистемы характеризуются наиболее высокой скоростью шифрования. Целостность данных обеспечивается присоединением к передаваемым данным специального кода (имитовставки), вырабатываемой по секретному ключу. Идеально подходит для шифрования информации «для себя».

Одной из наиболее известных криптографических систем с закрытым ключом является **DES — Data Encryption Standard**. Эта система первой получила статус государственного стандарта в области шифрования данных. Она разработана специалистами фирмы IBM и вступила в действие в США 1977 г. Эта система уже некоторое время не имеет статуса государственного стандарта, она по-прежнему широко применяется и заслуживает внимания при изучении блочных шифров с закрытым ключом.

DES осуществляет шифрование 64-битовых блоков данных с помощью 56-битового ключа. Расшифрование в DES является операцией обратной шифрованию и выполняется путем повторения операций шифрования в обратной последовательности. При длине ключа 56 бит возможны 2^{56} разных ключей. Если компьютер перебирает за одну секунду 1 000 000 ключей (что примерно равно 2^{20}), то на перебор всех 2^{56} ключей потребуется 2^{36} секунд или чуть более двух тысяч лет, что, конечно, является неприемлемым для злоумышленников.

Если иметь возможность объединить для проведения параллельных вычислений миллион процессоров, то максимальное время подбора ключа сокращается примерно до 18 часов. Процесс шифрования заключается в начальной перестановке битов 64-битового блока, шестнадцати циклах шифрования и, наконец, обратной перестановки битов (рис. 5.9).

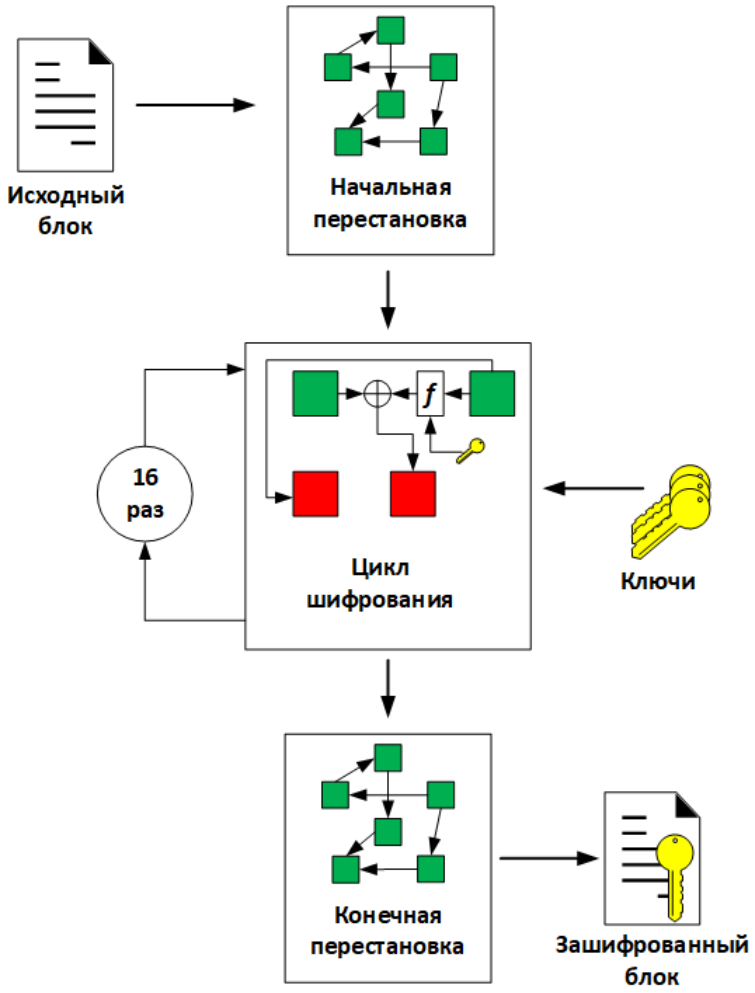


Рис. 5.9. Схема шифрования алгоритма DES

Разберем более детально работу алгоритма DES (рис. 5.10). Пусть из файла считан очередной 8-байтовый блок T, который преобразуется с помощью матрицы начальной перестановки IP, что даст в результате: T(0) = IP(T) (табл. 5.1).

Таблица 5.1

Матрица начальной перестановки IP

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15

Полученная последовательность битов T(0) разделяется на две последовательности по 32 бита каждая: L(0) — левые или старшие биты, R(0) — правые или младшие биты.

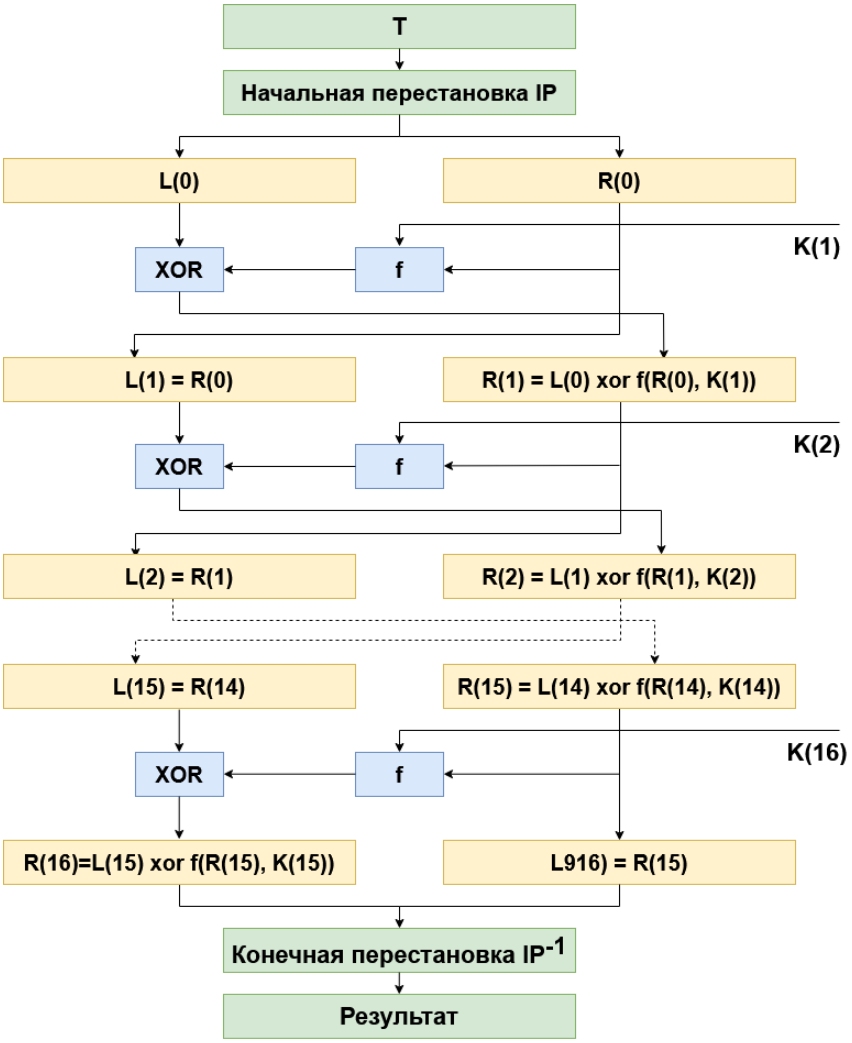


Рис. 5.10. Алгоритм работы DES

Затем выполняется шифрование, состоящее из 16 итераций. Результат *i*-й итерации описывается следующими формулами:

$$L(i) = R(i–1),$$

$$R(i) = L(i–1)\ XOR\ f(R(i–1), K(i)),$$

где *XOR* — операция «исключающее или».

Функция *f* называется функцией шифрования или функцией Фейстеля. Ее аргументы — это 32-битовая последовательность *R*(*i*-1), полученная на (*i*–1)-й итерации, и 48-битовый ключ *K*(*i*), который является результатом преобразования 56-битового ключа *K*. На 16-й итерации получают последовательности *R*(16) и *L*(16) (без перестановки), которые конкатенируют в 64-битовую последовательность *R*(16)*L*(16). Затем позиции битов этой последовательности переставляют в соответствии с матрицей IP^{-1} (табл. 5.2).

Таблица 5.2

Матрица обратной перестановки IP^{-1}

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57

Функция шифрования *f* является сложной функцией и для вычисления ее значения используются следующие функции-матрицы (рис. 5.11):

- *E* — расширение 32-битовой последовательности до 48-битовой;
- сложение по модулю 2 с ключом *K*(*i*);
- *S*1, *S*2, ..., *S*8 — преобразование 6-битового блока в 4-битовый;
- *P* — перестановка бит в 32-битовой последовательности.

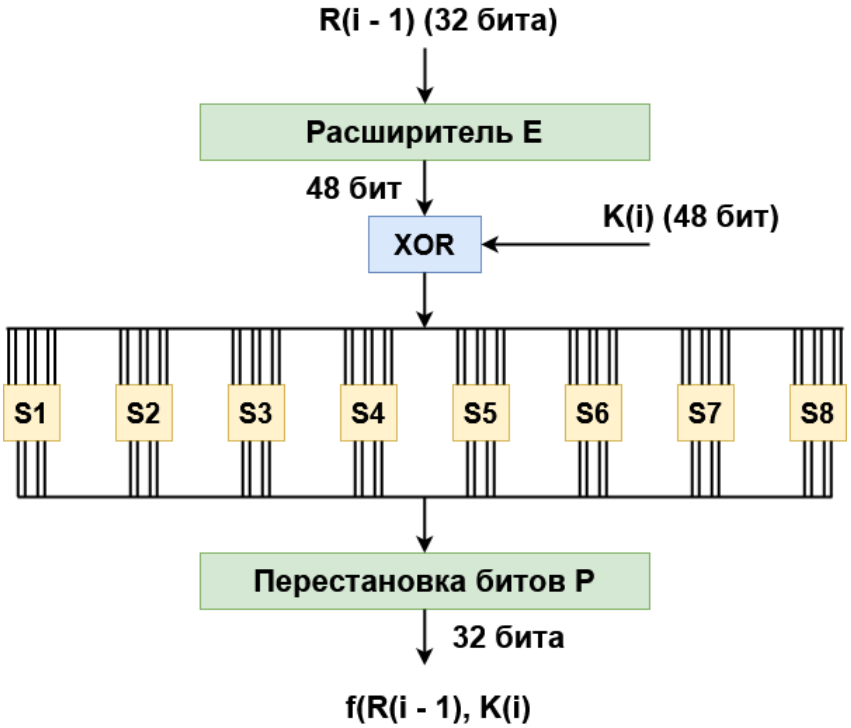


Рис. 5.11. Функция шифрования

Функция расширения *E* в стандарте описывается матрицей, представленной в табл. 5.3.

Таблица 5.3

Функция расширения E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Результатами выполнения функций преобразования *S*1, *S*2, ..., *S*8 будет трансформация 6-битовых блоков 48-битовой последовательности в 4-битовые.

Первый и последний разряды 6-битового блока являются двоичной записью числа *a*, 0<=*a*<=3, средние 4 разряда представляют число *b*, 0<=*b*<=15. Строки таблиц *S*1 – *S*8 нумеруются от 0 до 3, столбцы таблицы нумеруются от 0 до 15. Пара чисел (*a*, *b*) определяет число, находящееся в пересечении строки *a* и столбца *b* (табл. 5.4). Двоичное представление этого числа дает 4-битовый блок.

Таблица 5.4

Преобразования *S*1, *S*2, ..., *S*8

		Номер столбца																
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	
Номер строки	**0**	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	***S*1**
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	***S*2**
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	***S*3**
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	***S*4**
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	***S*5**
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	***S*6**
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	***S*7**
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	***S*8**
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Окончательное значение функции f (32 бит) получается перестановкой P, применяемой к 32-битовому блоку. Перестановка P задана табл. 5.5.

Таблица 5.5

Функция перестановки P

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9

Первый раз алгоритм DES удалось «взломать» за 39 дней с помощью огромной сети, состоящей из десятков тысяч компьютеров. Общественная организация «EFF», занимающаяся проблемами информационной безопасности и личной тайны в сети Internet, инициировала исследование «DES Challenge II» с целью выявления проблем DES. В рамках исследования сотрудники фирмы «RSA Laboratory» построили суперкомпьютер стоимостью 250 тыс. долл. В 1998 г. суперкомпьютер выполнил расшифровку данных, закодированных методом DES с использованием 56-битного ключа, менее чем за три дня.

В СССР работы по созданию алгоритма (или группы алгоритмов) по защите информации криптографическими методами в ЭВМ начались в 1976 г. Изначально работы имели гриф «Совершенно секретно». Затем были понижены до грифа «Секретно». В 1983 г. гриф алгоритма был понижен до пометки «Для служебного пользования». Именно с последней пометкой алгоритм был подготовлен для публикации в 1989 г. ГОСТ 28147-89 утвержден постановлением Госстандарта СССР № 1409 от 2 июня 1989 г., введен в действие с 1 июля 1990 г.

Алгоритм, определяемый ГОСТ 28147-89, схожий с алгоритмом DES, однако оказался более стойким. Имеет длину ключа шифрования 256 бит. Он шифрует информацию блоками по 64 бит, которые затем разбиваются на два субблока по 32 бит ($N1$ и $N2$). Субблок $N1$ обрабатывается определенным образом, после чего его значение складывается со значением субблока $N2$ (сложение выполняется по модулю 2, т.е. применяется логическая операция XOR — «исключающее или»), а затем субблоки меняются местами. Данное преобразование выполняется определенное число раз («раундов»): 16 или 32 в зависимости от режима работы алгоритма. Схема работы алгоритма представлена на рис. 5.12.

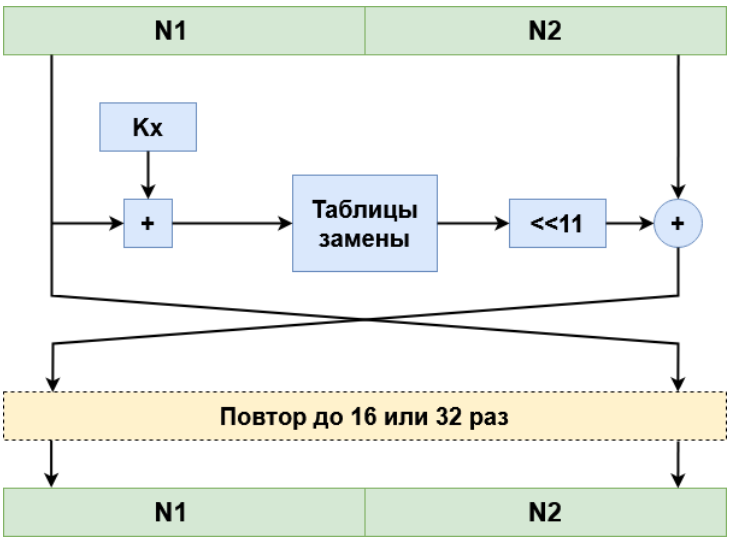


Рис. 5.12. Схема алгоритма ГОСТ 28147-89

В каждом раунде выполняются две операции:

1. Наложение ключа. Содержимое субблока *N*1 складывается по модулю 2 с 32-бит частью ключа *Kx*. Полный ключ шифрования представляется в виде конкатенации 32-бит подключей: *K*0, *K*1, *K*2, *K*3, *K*4, *K*5, *K*6, *K*7. В процессе шифрования используется один из этих подключей — в зависимости от номера раунда и режима работы алгоритма.

2. Табличная замена. После наложения ключа субблок *N*1 разбивается на 8 частей по 4 бит, значение каждой из которых заменяется в соответствии с таблицей замены для данной части субблока. Затем выполняется побитовый циклический сдвиг субблока влево на 11 бит.

В отличие от алгоритма ГОСТ 28147-89, который долгое время оставался секретным, американский стандарт шифрования **AES (Advanced Encryption Standard)**, призванный заменить DES, выбирался на открытом конкурсе, где все заинтересованные организации и частные лица могли изучать и комментировать алгоритмы-претенденты. В отличие от отечественного стандарта шифрования, алгоритм AES представляет блок данных в виде двухмерного байтового массива размером 4×4, 4×6 или 4×8 (допускается использование нескольких фиксированных размеров шифруемого блока информации). Все операции выполняются с отдельными байтами массива, а также с независимыми столбцами и строками (размер блока 128 бит, ключ 128/192/256 бит).

Алгоритм выполняет четыре преобразования:

1. BS (ByteSub) — табличная замена каждого байта массива (рис. 5.13).

Рис. 5.13. Операция BS (табличная замена)

2. SR (ShiftRow) — сдвиг строк массива (рис. 5.14). При этой операции первая строка остается без изменений, а остальные циклически побайтно сдвигаются влево на фиксированное число байт, зависящее от размера массива. Например, для массива размером 4×4 строки 2, 3 и 4 сдвигаются соответственно на 1, 2 и 3 байта.

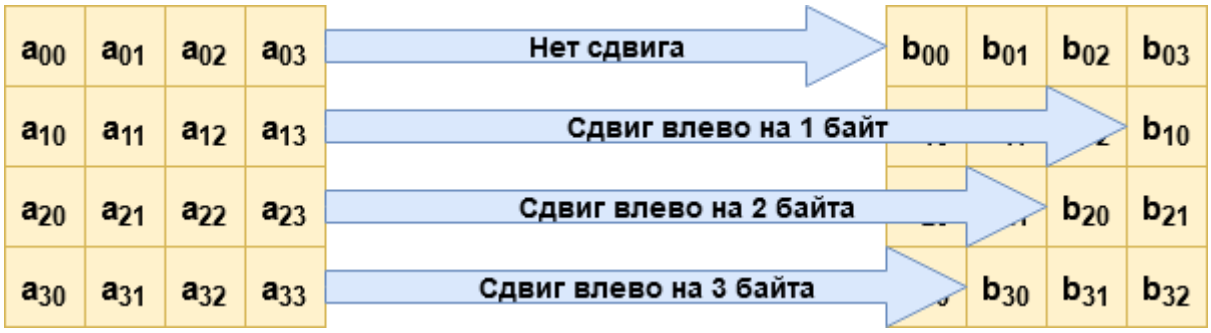


Рис. 5.14. Операция SR (сдвиг строк массива)

3. MC (MixColumn) — операция над независимыми столбцами массива, когда каждый столбец по определенному правилу умножается на фиксированную матрицу c(x) (рис. 5.15).

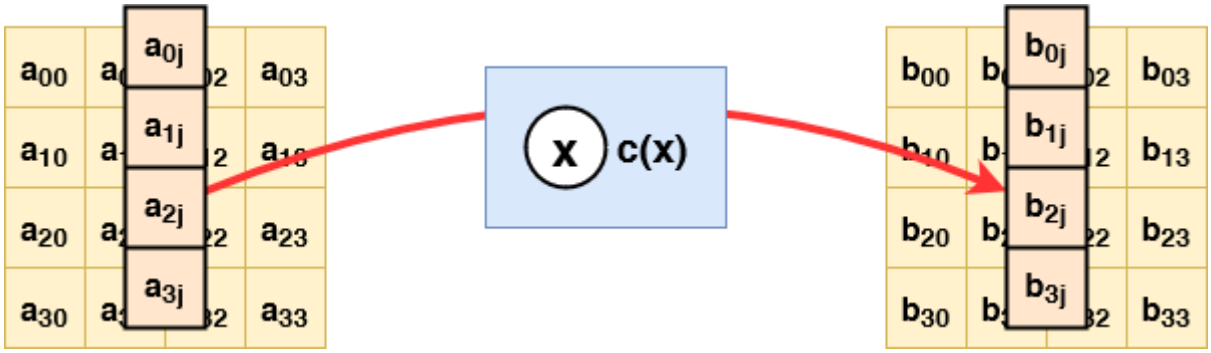


Рис. 5.15. Операция MC (операция над столбцами массива)

4. AK (AddRoundKey) — добавление ключа (рис. 5.16). Каждый бит массива складывается по модулю 2 с соответствующим битом ключа раунда, который, в свою очередь, определенным образом вычисляется из ключа шифрования.

Рис. 5.16. Операция AK (добавление ключа)

Использование симметричных криптосистем в компьютерных сетях порождает проблему распределения ключей шифрования между пользователями. На N пользователей необходимо распределить $N{\cdot}(N-1)/2$ секретных ключей, т.е. число распределяемых секретных ключей растет по квадратичному закону с увеличением числа абонентов сети.

5.4. Асимметричные криптосистемы шифрования

Открытый ключ K используется для шифрования информации, вычисляется из секретного ключа k. Секретный ключ k используется для расшифровывания информации, зашифрованной с помощью парного ему открытого ключа K. С помощью вычислений нельзя вывести секретный ключ k из открытого ключа K.

Принцип действия асимметричного шифрования можно описать следующим образом (рис. 5.17). Абонент B генерирует пару ключей: секретный ключ k_B и открытый ключ K_B. Открытый ключ K_B посылается абоненту A и остальным абонентам (или делается доступным, например на разделяемом ресурсе). Абонент A зашифровывает сообщение с помощью открытого ключа K_B абонента B и отправляет шифртекст абоненту B. Абонент B расшифровывает сообщение с помощью своего секретного ключа k_B. Никто другой (в том числе абонент A) не может расшифровать данное сообщение, так как не имеет секретного ключа абонента B.

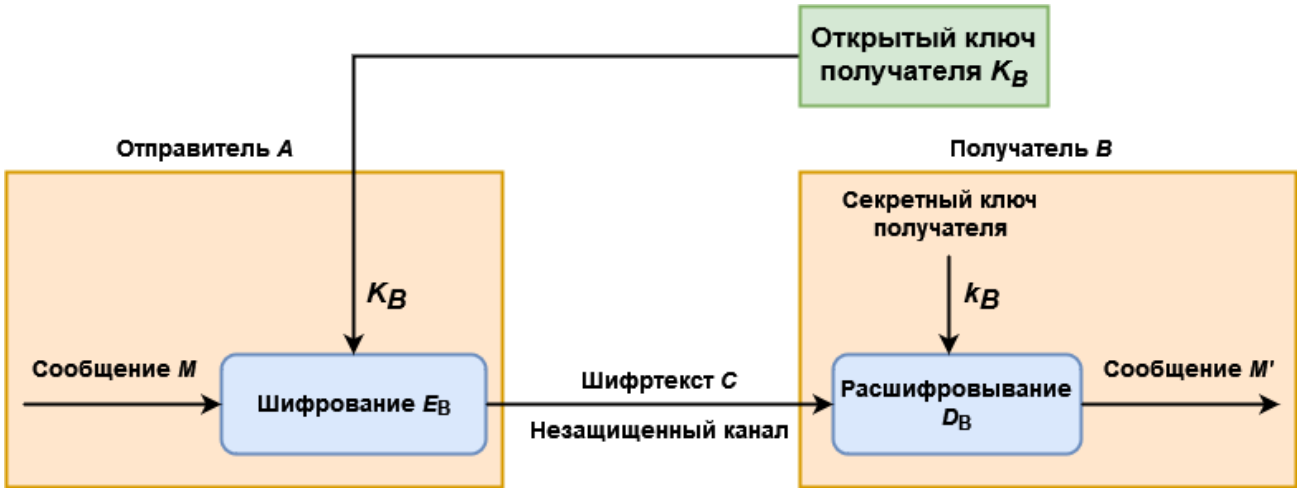


Рис. 5.17. Схема асимметричной криптосистемы шифрования

Характерные особенности асимметричных криптосистем:

– защита информации в асимметричной криптосистеме основана на секретности ключа k_B получателя сообщения;

– открытый ключ K_B и криптограмма C могут быть отправлены по незащищенным каналам, т.е. всем известны K_B и C;

– алгоритмы шифрования и расшифровывания являются открытыми;

– вычисление пары ключей (K_B, k_B) получателем B должно быть простым;

– отправитель A, зная открытый ключ K_B и сообщение M, может легко вычислить криптограмму;

– получатель B, используя секретный ключ k_B и криптограмму C, может легко восстановить исходное сообщение;

– злоумышленник, зная открытый ключ K_B, при попытке вычислить секретный ключ k_B наталкивается на непреодолимую вычислительную проблему.

Концепция асимметричных криптографических систем с открытым ключом основана на применении однонаправленных функций. Однонаправленной функцией называется функция $F(X)$, обладающая двумя свойствами:

– существует алгоритм вычисления значений функции;

– не существует эффективного алгоритма обращения (инвертирования) функции F (т.е. не существует решения уравнения относительно X).

Пример однонаправленной функции — целочисленное умножение. Прямая задача — вычисление произведения двух очень больших целых чисел P и Q, т.е. нахождение значения $P \cdot Q = N$, — относительно несложная задача для компьютера. Обратная задача — факторизация, или разложение на множители большого целого числа, т.е. нахождение делителей P и Q большого целого числа $N = P \cdot Q$, является практически неразрешимой при достаточно больших значениях N.

Преимущества асимметричных криптографических систем перед симметричными криптосистемами:

– в асимметричных криптосистемах решена сложная проблема распределения ключей между пользователями, так как каждый пользователь может сгенерировать свою пару ключей сам, а открытые ключи пользователей могут свободно публиковаться и распространяться по сетевым коммуникациям;

– исчезает квадратичная зависимость числа ключей от числа пользователей; в асимметричной криптосистеме число используемых ключей связано с числом абонентов линейной зависимостью (в системе из N пользователей используются $2N$ ключей), а не квадратичной, как в симметричных системах;

– асимметричные криптосистемы позволяют реализовать протоколы взаимодействия сторон, которые не доверяют друг другу, поскольку при использовании асимметричных криптосистем закрытый ключ должен быть известен только его владельцу.

Недостатки асимметричных криптосистем:

– на настоящий момент нет математического доказательства необратимости используемых в асимметричных алгоритмах функций;

– асимметричное шифрование существенно медленнее симметричного, поскольку при шифровании и расшифровке используются весьма ресурсоемкие операции. По этой же причине реализовать аппаратный шифратор с асимметричным алгоритмом существенно сложнее, чем реализовать аппаратно симметричный алгоритм;

– необходимость защиты открытых ключей от подмены.

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений.

Порядок шифрования по алгоритму RSA следующий:

– выберем два очень больших простых числа p и q;

– определим $\boldsymbol{n}$ как результат умножения p на q ($n = p \times q$);

– выберем большое случайное число, которое назовем $\boldsymbol{d}$ (оно должно быть взаимно простым с m результатом умножения $(p - 1) \times (q - 1)$);

– определим такое число $\boldsymbol{e}$, для которого является истинным следующее соотношение: $(e \times d) \bmod m = 1$ или $e = (1 \bmod m)/d$;

– открытым ключом будут числа $\boldsymbol{e}$ и $\boldsymbol{n}$, а секретным ключом — числа $\boldsymbol{d}$ и $\boldsymbol{n}$;

– разбить шифруемый текст на блоки, каждый из которых может быть представлен в виде числа $\mathbf{M}(i) = 0, 1, ..., n - 1$;

– зашифровать текст, рассматриваемый как последовательность чисел $\mathbf{M}$(i) по формуле $\mathbf{C}(i) = (\mathbf{M}(i)^e) \bmod n$.

Расшифровывание производится с использованием секретного ключа $\{d, n\}$, и необходимо выполнить следующие вычисления: $\mathbf{M}(i) = (\mathbf{C}(i)^d) \bmod n$.

Рассмотрим пример применения метода RSA. Генерируем ключевую пару:

– выберем $p = 3$ и $q = 11$;

– определим $n = 3 \times 11 = 33$;

– найдем $(p - 1) \times (q - 1) = 20$;

– в качестве d выберем любое число, которое является взаимно простым с 20, например $d = 3$.

– выберем число e. В качестве такого числа может быть взято любое число, для которого удовлетворяется соотношение $(e \times 3) \bmod 20 = 1$, например 7.

Зашифруем сообщение «4 1 9», используя ключ {7, 33}:

$$\mathbf{C1} = (4^7) \bmod 33 = 16384 \bmod 33 = 16,$$

$$\mathbf{C2} = (1^7) \bmod 33 = 1 \bmod 33 = 1,$$

$$\mathbf{C3} = (9^7) \bmod 33 = 4782969 \bmod 33 = 15.$$

Шифртекст: «16 1 15»

Расшифруем сообщение {16, 1, 15}, полученное в результате зашифрования по известному ключу, на основе секретного ключа {3, 33}:

$$\mathbf{M1} = (16^3) \bmod 33 = 4096 \bmod 33 = 4,$$

$$\mathbf{M2} = (1^3) \bmod 33 = 1 \bmod 33 = 1,$$

$$\mathbf{M3} = (15^3) \bmod 33 = 3375 \bmod 33 = 9.$$

Вторым алгоритмом асимметричного шифрования, нашедшим широкое практическое применение, является **криптосистема Эль-Гамаля**. Сначала сгенерируется ключевая пара:

– генерируется случайное простое число p;

– выбирается целое число g — первообразный корень p;

– выбирается случайное целое число x такое, что $1 < x < p$;

– вычисляется $y = g\hat{}x \bmod p$;

– открытым ключом является тройка (p, g, y), закрытым ключом — число x.

Примеры наименьших первообразных корней по модулю m представлены в табл. 5.6.

Таблица 5.6

Наименьшие первообразные корни

Модуль m	2	3	4	5	6	7	8	9	10	11	12	13	14
Первообразный корень	1	2	3	2	5	3	–	2	3	2	–	2	3

Далее рассмотрим принцип его действия на примере. Допустим, что нужно зашифровать сообщение **M** = 5. Производим генерацию ключей:

– пусть $p = 11$, $g = 2$;

– выберем $x = 8$ — случайное целое число x такое, что $1 < x < p$;

– вычислим $y = g^x \bmod p = 2^8 \bmod 11 = 3$;

– открытым ключом является тройка (p, g, y) = (11, 2, 3), а закрытым ключом — число $x = 8$.

Производим шифрование, для этого выбираем случайное целое число k, такое, что $1 < k < (p - 1)$. Пусть $k = 9$. Вычисляем число $a = g^k \bmod \text{p} = 2^9 \bmod 11 = 512 \bmod 11 = 6$. Вычисляем число $b = y^k M \bmod p = 3^9\ 5 \bmod 11 = 19683 \cdot 5 \bmod 11 = 9$. Полученная пара ($a$, b) = (6, 9) является шифротекстом.

При расшифровании необходимо получить сообщение **M** = 5 по известному шифротексту (a, b) = (6, 9) и закрытому ключу $x = 8$. Вычисляем **M** по формуле: $\mathbf{M} = b\ (a^x)^{-1} \bmod p = 9\ (6^8)^{-1} \bmod 11 = 5$. Получили исходное сообщение **M** = 5. Более наглядно принцип действия алгоритма показан на рис. 5.18.

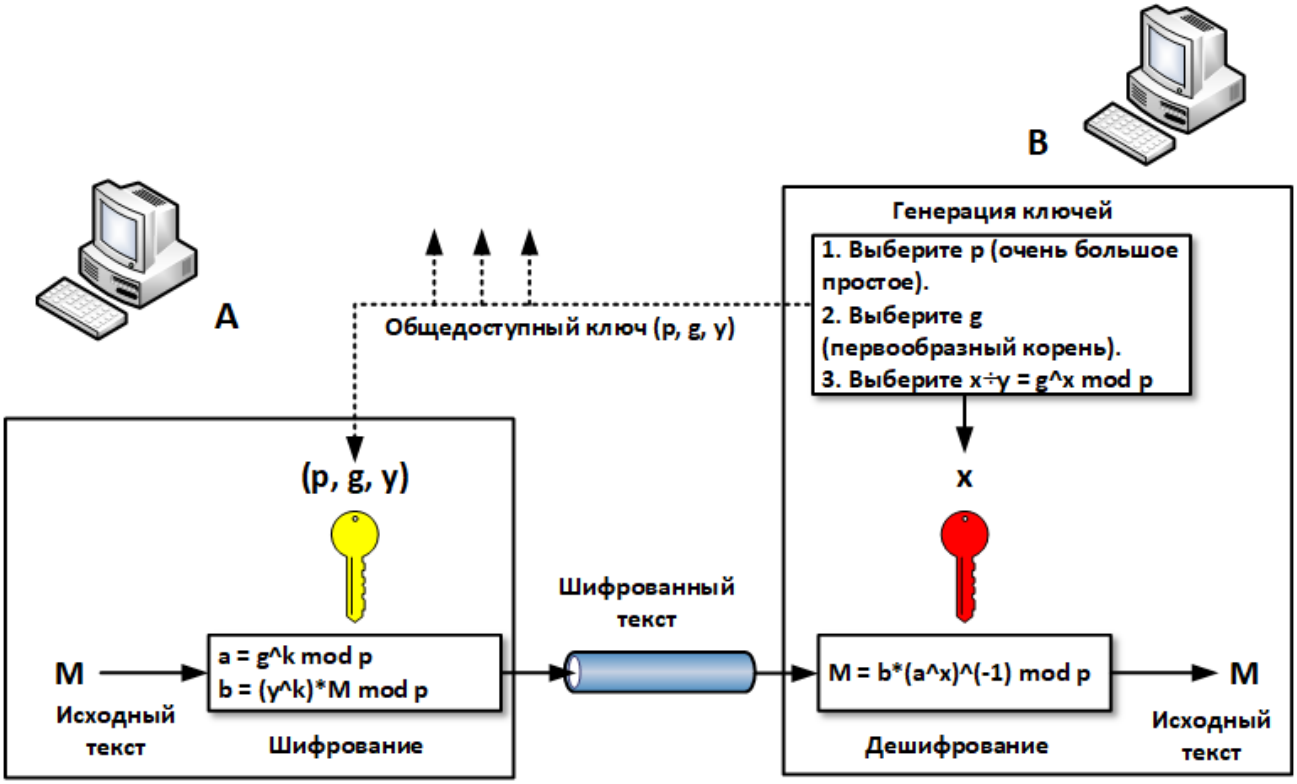


Рис. 5.18. Схема шифрования Эль-Гамаля

Электронная подпись — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию [36]. Информация в электронной форме, подписанная электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

Электронная подпись (ЭП) представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом. Формирование электронной подписи проиллюстрировано на рис. 5.19.

Рис. 5.19. Схема формирования электронной подписи

Процедура формирования цифровой подписи будет следующей. Абонент А — отправитель сообщения — генерирует пару ключей: секретный ключ k_A и открытый ключ K_A. Открытый ключ K_A вычисляется из парного ему секретного ключа k_A. Открытый ключ K_A рассылается остальным абонентам сети (или делается доступным, например, на разделяемом ресурсе) для использования при проверке подписи. Для формирования цифровой подписи отправитель А прежде всего вычисляет значение хеш-функции $h(M)$ подписываемого текста M (дайджест). Далее отправитель А шифрует дайджест m своим секретным ключом k_A. Получаемая при этом пара чисел представляет собой цифровую подпись для данного текста M. Сообщение M вместе с цифровой подписью отправляется в адрес получателя. Дайджест m — относительно короткое число, состоящее из фиксированного небольшого числа битов и характеризующее весь текст M в целом. Хеш-функция — это труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хеш-функции.

Абоненты сети могут проверить электронную подпись полученного сообщения M с помощью открытого ключа K_A отправителя этого сообщения. При проверке ЭП абонент В — получатель сообщения M — расшифровывает принятый дайджест m открытым ключом K_A отправителя А. Кроме того, получатель сам вычисляет с помощью хеш-функции $h(M)$ дайджест m' принятого сообщения M и сравнивает его с расшифрованным. Если m и m' совпадают, то электронная подпись является подлинной (рис. 5.20).

Рис. 5.20. Схема проверки электронной подписи

Функция хеширования (хеш-функция) представляет собой преобразование, на вход которого подается сообщение переменной длины M, а выходом является строка фиксированной длины $h(M)$. Иначе говоря, хеш-функция $h(M)$ принимает в качестве аргумента сообщение (документ) M произвольной длины и возвращает хеш-значение (хеш) $H = h(M)$ фиксированной длины.

Требования к хеш-функции:

– хеш-функция может быть применена к аргументу любого размера;
– выходное значение хеш-функции имеет фиксированный размер;
– хеш-функцию $h(x)$ достаточно просто вычислить для любого x;

– скорость вычисления хеш-функции должна быть такой, чтобы скорость выработки и проверки ЭЦП при использовании хеш-функции была значительно больше, чем при использовании самого сообщения;

– хеш-функция должна быть однонаправленной, т.е. обладать свойством необратимости, иными словами, задача подбора документа M', который обладал бы требуемым значением хеш-функции, должна быть вычислительно неразрешима;

– вероятность того, что значения хеш-функций двух различных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала; т.е. для любого фиксированного x с вычислительной точки зрения невозможно найти $x' \neq x$, такое, что $h(x') = h(x)$.

Формирование электронной подписи с помощью алгоритма асимметричного шифрования Эль-Гамаля показано на рис. 5.21.

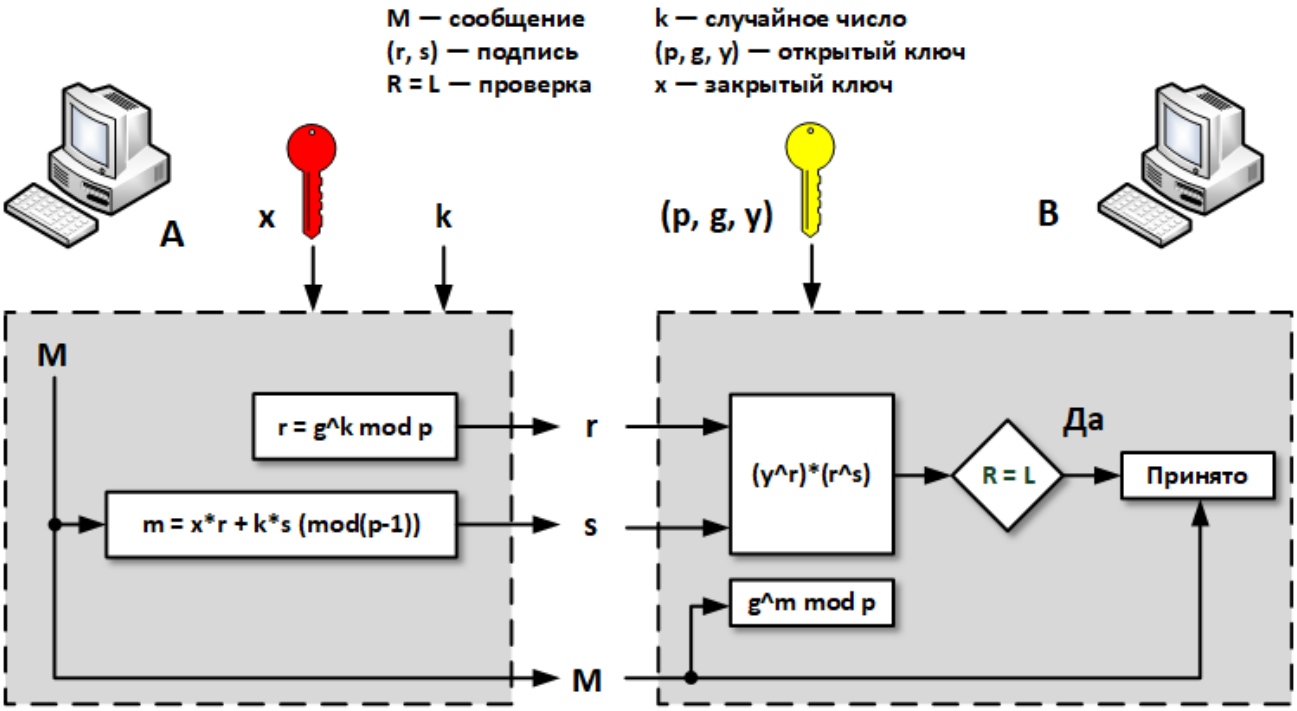


Рис. 5.21. Работа схемы Эль-Гамаля в режиме подписи

В настоящее время действуют следующие отечественные стандарты по криптографической защите:

1. ГОСТ Р 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.
2. ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры.
3. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования.
4. ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

5. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

5.5. Квантовая криптография

В основе квантовой криптографии лежит принцип неопределенности Гейзенберга, согласно которому попытка произвести измерения в квантовой системе вносит в нее нарушения. Свойства квантовых систем:

– невозможно произвести измерение квантовой системы, не нарушив ее;

– невозможно одновременно измерить поляризацию фотона в разных базисах (вертикально-горизонтальном и диагональном);

– невозможно дублировать неизмеренное квантовое состояние.

Квантовая криптография позволяет передавать секретную информацию по открытому (незащищенному) каналу и при этом можно быть полностью уверенным в том, что ее никто не перехватит. Решается задача безопасной пересылки криптографических ключей — квантовое распределение ключей (КРК). Правильно измерить поляризацию фотона (0, 45, 90, 135°) можно только зная базис поляризации («+» или «×»). Если используемый базис при измерении отличается от базиса поляризации, то на выходе получается случайный результат (0 или 1). Если отправитель и получатель не договорились между собой, какой вид поляризации брать за основу, получатель может разрушить посланный отправителем сигнал, не получив никакой полезной информации. Первый протокол квантовой криптографии (BB84) был предложен и опубликован в 1984 г. В протоколе BB84 используются четыре квантовых состояния фотонов, а именно: направления вектора поляризации, одно из которых отправитель выбирает в зависимости от передаваемого бита: 90 или 135° для «1», 45 или 0° для «0».

Алгоритм работы системы, основанной на протоколе BB84 следующий. отправитель посылает получателю последовательность фотонов A_i, поляризация которых выбрана случайным образом и может составлять 0, 45, 90, 135°. Получатель располагает двумя анализаторами: один распознает вертикально-горизонтальную поляризацию, другой — диагональную. Для каждого фотона получатель случайно выбирает один из анализаторов и записывает тип анализатора и результат измерений. Полученный, «сырой», ключ $B_i = A_i$ с вероятностью P = 75 %. То есть он содержит ~ 25 % ошибок. По общедоступному каналу связи получатель сообщает отправителю, какие анализаторы использовались, но не сообщает, какие результаты были получены. Отправитель по общедоступному каналу связи сообщает получателю, какие анализаторы он выбрал правильно. Те фотоны, для которых получатель неверно выбрал анализатор, отбрасываются. Для обнаружения перехвата отправитель и получатель выбирают случайный участок ключа и сравнивают его по общедоступному каналу связи. Если процент ошибок велик, то он может быть отнесен на счет перехвата, и процедура повторяется сначала.

Рассмотрим пример шифрования по протоколу BB84. В табл. 5.7 приводятся обозначения поляризации фотонов.

Таблица 5.7

Поляризация фотонов и кодируемый бит

Обозначение	Поляризация фотонов	Кодируемый бит
|	Вертикальная	0
—	Горизонтальная	1
/	Под углом 45	0
\	Под углом 135	1

В табл. 5.8 приведены обозначения детектирующего фильтра (анализатора).

Таблица 5.8

Обозначение анализатора

Обозначение анализатора	Поляризация фотонов
+	Прямоугольный
×	Диагональный

Отправитель формирует последовательность фотонов применяя разную поляризацию. Получатель случайным образом выбирает анализаторы и проводит измерение. Где анализатор был выбран верно получены истинные значения битов (рис. 5.22).

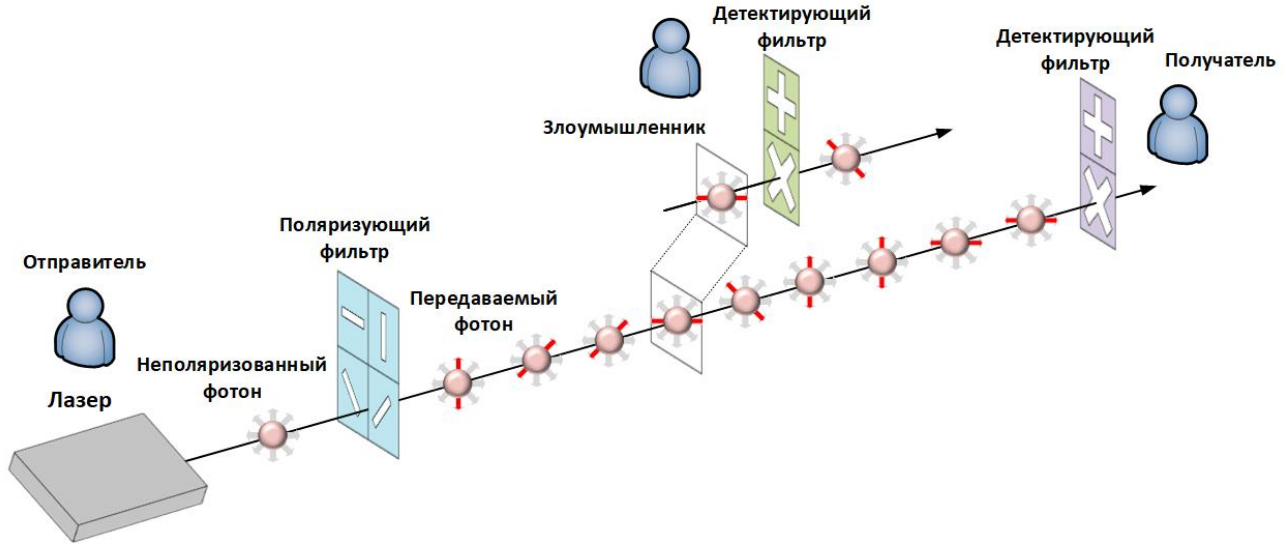


Рис. 5.22. Схема формирования ключа

Получив все фотоны, получатель по открытому каналу сообщает отправителю последовательность фильтров, которые он использовал для поступающих фотонов. О считанных значениях битов он ничего не сообщает. Отправитель говорит получателю, какие фильтры он выбрал правильно. Измеренные с их помощью биты будут использоваться при формировании ключа для шифрования сообщения (табл. 5.9).

Таблица 5.9

Определение ключа по протоколу BB84

Последовательность фотонов отправителя	|	/	/	—	\	|	|	—	—
Последовательность анализаторов получателя	+	×	+	+	×	×	×	+	×
Результаты измерений получателя	0	0	1	1	1	0	1	1	0
Анализаторы выбраны верно	да	да	нет	да	да	нет	нет	да	нет
Ключ	0	0		1	1			1	

На данном этапе квантовая криптография только приближается к практическому уровню использования. Диапазон разработчиков новых технологий квантовой криптографии — от крупнейших мировых институтов до маленьких компаний, только начинающих свою деятельность. Рынок находится на начальной стадии формирования.

Однако можно назвать и ряд практических реализаций системы.

В 1989 г. в Исследовательском центре IBM построили первую работающую квантово-криптографическую систему. Она состояла из квантового канала, содержащего передатчик на одном конце и приемник на другом, размещенные на оптической скамье длиной около метра в светонепроницаемом полутораметровом кожухе размером 0,5 × 0,5 м. Собственно квантовый канал представлял собой свободный воздушный канал длиной около 32 см.

В наше время исследованиями в области квантовой криптографии занимается американская компания Magiq Technologies из Нью-Йорка, выпустившая прототип коммерческой квантовой криптотехнологии собственной разработки. Основной продукт — средство для распределения ключей (quantum key distribution, QKD) Navajo (Навахо). Navajo способен в реальном времени генерировать и распространять ключи средствами квантовых технологий и предназначен для обеспечения защиты от внутренних и внешних злоумышленников.

В октябре 2007 г. на выборах в Швейцарии были повсеместно использованы квантовые сети, начиная с избирательных участков и заканчивая дата-центром ЦИК. Была использована техника, которую еще в середине 90-х разработали в Университете Женевы.

В 2011 г. в Токио прошла демонстрация проекта «Tokyo QKD Network», в ходе которого разрабатывается квантовое шифрование телекоммуникационных сетей. Была проведена пробная телеконференция на расстоянии в 45 км. Связь в системе идет по обычным оптоволоконным линиям. В будущем предполагается применение для мобильной связи.

5.6. Прикладные решения криптографии

Шифрованная файловая система (Encrypting File System — EFS) — средство Windows, позволяющее сохранять сведения на жестком диске в шифрованном формате. Данная функция шифрования присутствует в операционных системах Windows только в выпусках: профессиональная — Professional, кор-

поративная — Enterprise, максимальная — Ultimate. Шифрование обеспечивается при помощи шифрующей файловой системы, которая фактически представляет собой надстройку файловой системы NTFS. Вследствие этого шифрование данного вида недоступно на разделах файловой системы FAT32. Все этапы шифрования производятся при сохранении и открытии файла и проходят практически незаметно. EFS работает, шифруя каждый файл с помощью алгоритма симметричного шифрования, зависящего от версии операционной системы и настроек. При этом используется случайно сгенерированный ключ для каждого файла, называемый File Encryption Key (FEK), выбор симметричного шифрования на данном этапе объясняется его скоростью по отношению к асимметричному шифрованию. FEK (случайный для каждого файла ключ симметричного шифрования) защищается путем асимметричного шифрования, использующего открытый ключ пользователя (сертификат пользователя), шифрующего файл, и алгоритм RSA (рис. 5.23). Схема расшифровывания представлена на рис. 5.24.

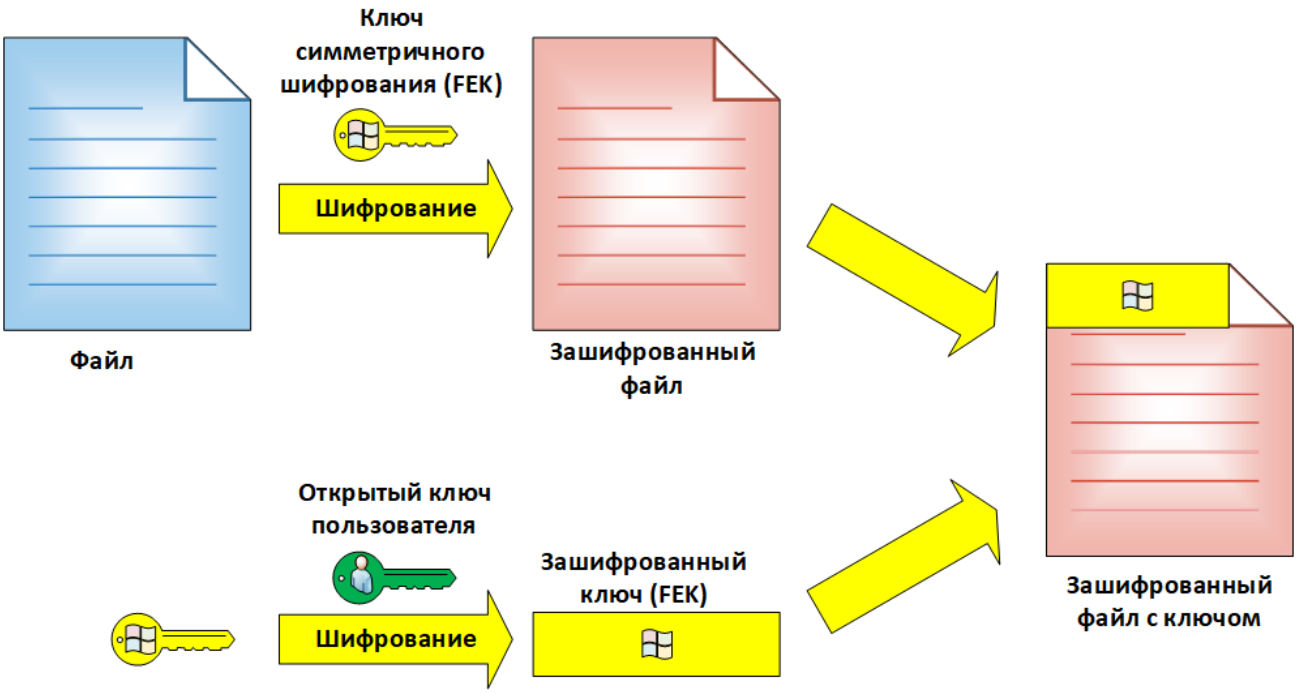


Рис. 5.23. Схема шифрования файла

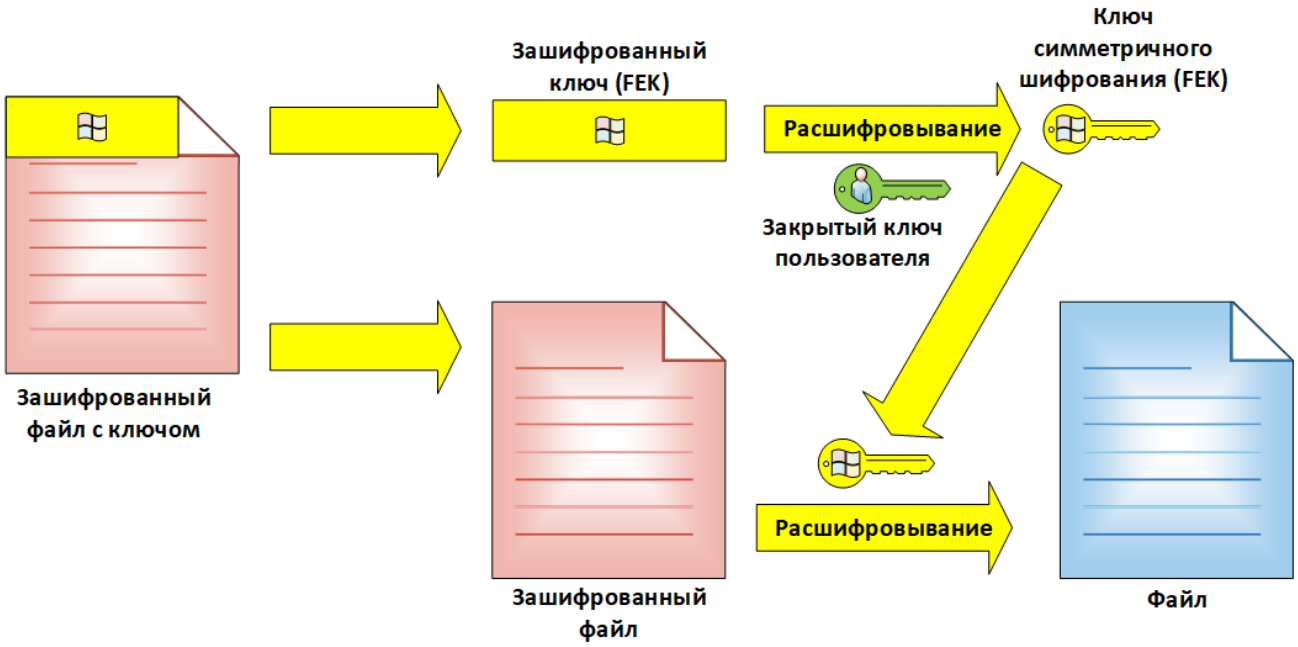


Рис. 5.24. Схема расшифрования файла

Войдя в систему под своей учетной записью, пользователь может открывать и редактировать зашифрованные ранее файлы. При добавлении нового файла в зашифрованный каталог он также будет зашифрован. Перемещение или копирование файла из зашифрованного каталога не приводит к автоматическому расшифрованию при условии, что файл перемещается в раздел NTFS. Остальные пользователи не смогут получить доступ к содержимому файла. Но если они имеют соответствующие разрешения на уровне NTFS, они могут беспрепятственно переименовать или удалить файл. Рекомендуется шифровать не отдельные файлы, а каталоги — это приведет к шифрованию всех файлов, сохраненных в данной папке.

В операционных системах Windows, начиная с версии Windows Vista (только в выпусках: корпоративная — Enterprise, максимальная — Ultimate), присутствует инструмент «**Шифрование диска BitLocker**», который используется для защиты всех файлов, хранящихся на диске с операционной системой. Также с помощью функции «Шифрование BitLocker To Go» можно защитить все файлы, хранящиеся на несъемных дисках (например, внутренних жестких дисках) или на съемных дисках (например, внешних жестких дисках или USB-устройствах флеш-памяти). В отличие от шифрованной файловой системы (Encrypting File System), позволяющей зашифровывать отдельные файлы, BitLocker шифрует диск целиком. Пользователь может входить в систему и работать с файлами как обычно, а BitLocker будет мешать злоумышленникам, пытающимся получить доступ к системным файлам для поиска паролей, а также к диску путем извлечения его из данного компьютера и установки в другой. BitLocker автоматически шифрует все файлы, добавляемые на зашифрованный диск. Файлы будут зашифрованы только при хранении на зашифрованном диске. При их копировании на другой диск или компьютер они будут расшифро-

ваны. При предоставлении общего доступа к файлам по сети они будут зашифрованы на зашифрованном диске, но авторизованные пользователи смогут получать к ним доступ обычным образом. BitLocker всегда можно отключить либо временно (приостановив его), либо на постоянной основе (расшифровав диск). Технология BitLocker дает возможность применять алгоритм шифрования к дискам с данными, на которых используются файловые системы exFAT, FAT16, FAT32 или NTFS. Если же шифрование применяется к диску с операционной системой, то для использования технологии BitLocker данные на этом диске должны быть записаны в формате NTFS. Метод шифрования, который использует технология BitLocker, основан на алгоритме AES с 128-битным ключом. Зашифрованные диски (несъемные или съемные) можно разблокировать с помощью пароля, или смарт-карты, или настроить автоматическую разблокировку дисков при входе в систему.

Прикладная криптосистема PGP (Pretty Good Privacy — «довольно хорошая секретность») была разработана и опубликована в Интернете в 1991 г. программистом и математиком Филиппом Циммерманом, по сути, оказалась первым продуктом подобного уровня, представленным для свободного доступа всему миру. PGP — это система, сочетающая преимущества симметричных и асимметричных криптосистем. Программа использует взаимосвязанные пары ключей: закрытый, хранящийся только у владельца для цели расшифрования данных и их цифрового подписания, и открытый, который не нуждается в защите, может быть широко распространен и используется для шифрования и проверки цифровых подписей (все эти уникальные возможности достигаются за счет особого математического аппарата).

Шифрование PGP осуществляется последовательно хешированием, сжатием данных, шифрованием с симметричным ключом и, наконец, шифрованием с открытым ключом, причем каждый этап может осуществляться одним из нескольких поддерживаемых алгоритмов. Симметричное шифрование производится с использованием одного из семи симметричных алгоритмов (AES, CAST5, 3DES, IDEA, Twofish, Blowfish, Camellia) на сеансовом ключе. Сеансовый ключ генерируется с использованием криптографически стойкого генератора псевдослучайных чисел. Сеансовый ключ зашифровывается открытым ключом получателя с использованием алгоритмов RSA или Elgamal (в зависимости от типа ключа получателя). Каждый открытый ключ соответствует имени пользователя или адресу электронной почты. Первая версия системы называлась «Сеть доверия» и противопоставлялась системе X.509, использовавшей иерархический подход, основанный на удостоверяющих центрах, добавленный в PGP позже. Современные версии PGP включают оба способа.

Криптопровайдер (CSP — Cryptographic Service Provider) — это независимый модуль, позволяющий осуществлять криптографические операции в операционных системах Microsoft, управление которым происходит с помощью функций интерфейса Microsoft CryptoAPI. В ОС Microsoft Windows существуют встроенные криптопровайдеры, однако они не поддерживают российских стандартов шифрования, хеширования и подписи. Сертифицированными ФСБ России криптопровайдерами являются КриптоПро CSP и Сигнал-КОМ CSP, под-

держивающие ГОСТ 28147-89, ГОСТ 34.11-94 и ГОСТ 34.10-2001 для шифрования, хеширования и цифровой подписи соответственно.

КриптоПро — разработанная одноименной компанией линейка криптографических утилит (вспомогательных программ) — так называемых криптопровайдеров. Они используются во многих программах российских разработчиков для генерации электронной подписи (ЭП), работы с сертификатами, организации структуры PKI (Public Key Infrastructure — Инфраструктура открытых ключей) и т.д. СКЗИ «КриптоПро CSP» является системой с открытым распределением ключей. Открытые ключи подписи и шифрования представляются в виде сертификатов открытых ключей, формат которых описан в рекомендация X.509 и RFC 2459. В «КриптоПро CSP» закрытый ключ подписи может быть использован только для формирования ЭЦП. Закрытый ключ шифрования может быть использован как для формирования ключа связи с другим пользователем, так и для формирования ЭЦП. При работе с СКЗИ каждый пользователь, обладающий правом подписи или шифрования, вырабатывает сам на рабочем месте или получает от администратора безопасности (в зависимости от политики безопасности) личные закрытые и открытый ключи. На основе каждого открытого ключа третьей стороной (центром сертификации) формируются сертификат открытого ключа. Для оперирования с секретными ключами в СКЗИ «КриптоПро CSP» для каждого пользователя (приложения) создается ключевой носитель (ключевой контейнер).

Модуль сетевой аутентификации «КриптоПро TLS» предназначен для обеспечения аутентификации клиентских и серверных компонент распределенных приложений и обеспечения конфиденциальности передаваемых данных при взаимодействии по протоколу HTTP(S). Данный программный продукт представляет собой реализацию транспортного протокола TLS 1.0 (RFC 2246) с использованием криптографических функций СКЗИ КриптоПро CSP.

Криптопровайдер Signal-COM CSP поддерживает российские криптографические алгоритмы и обеспечивает к ним доступ из пользовательских приложений через стандартный криптографический интерфейс компании Microsoft — CryptoAPI 2.0. Signal-COM CSP выполнен в соответствии с технологией Cryptographic Service Provider (CSP), благодаря чему российские алгоритмы шифрования и ЭП могут использоваться во многих популярных и широко распространенных приложениях. Алгоритмы шифрования и ЭП могут использоваться в следующих приложениях:

– удостоверяющий центр Microsoft Certification Authority приложения Microsoft Office (MS Outlook, MS Word, MS Excel, MS Power Point, MS Info Path);

– почтовый клиент Microsoft Outlook Express;

– приложение контроля целостности программного обеспечения Microsoft Authenticode;

– почтовый клиент The Bat.

Система **Secret Disk** предназначена для защиты конфиденциальной информации на рабочих станциях и персональных компьютерах под управлением операционных систем семейства Windows. Secret Disk создает зашифрованные

диски, предназначенные для безопасного хранения конфиденциальной информации. Шифрование данных проводится в «прозрачном» режиме — при записи информация автоматически зашифровывается, при чтении — расшифровывается. Доступ к защищенной информации может получить только ее владелец, имеющий USB-ключ или смарт-карту eToken и знающий его PIN-код. Для остальных защищенный диск выглядит как неразмеченная область жесткого диска или файл, содержащий «мусор». Secret Disk позволяет шифровать логические разделы жесткого диска, а также установить защиту системного раздела и ограничить возможность загрузки ОС. Для доступа к защищенному системному разделу необходимо пройти двухфакторную аутентификацию до загрузки ОС. Также Secret Disk позволяет шифровать съемные носители и создавать зашифрованные файлы-контейнеры (так называемые виртуальные диски) (рис. 5.25).

Secret Disk позволяет организовать работу нескольких пользователей на одном компьютере в разных вариантах (у каждого пользователя свой зашифрованный диск, несколько пользователей могут работать с одним зашифрованным диском и т.д.). В Secret Disk реализованы механизмы усиленной защиты и защиты данных от искажения в случае различных программных и аппаратных сбоев, включая перебои электропитания. Secret Disk включает в себя два основных компонента: это программный модуль и электронный ключ eToken.

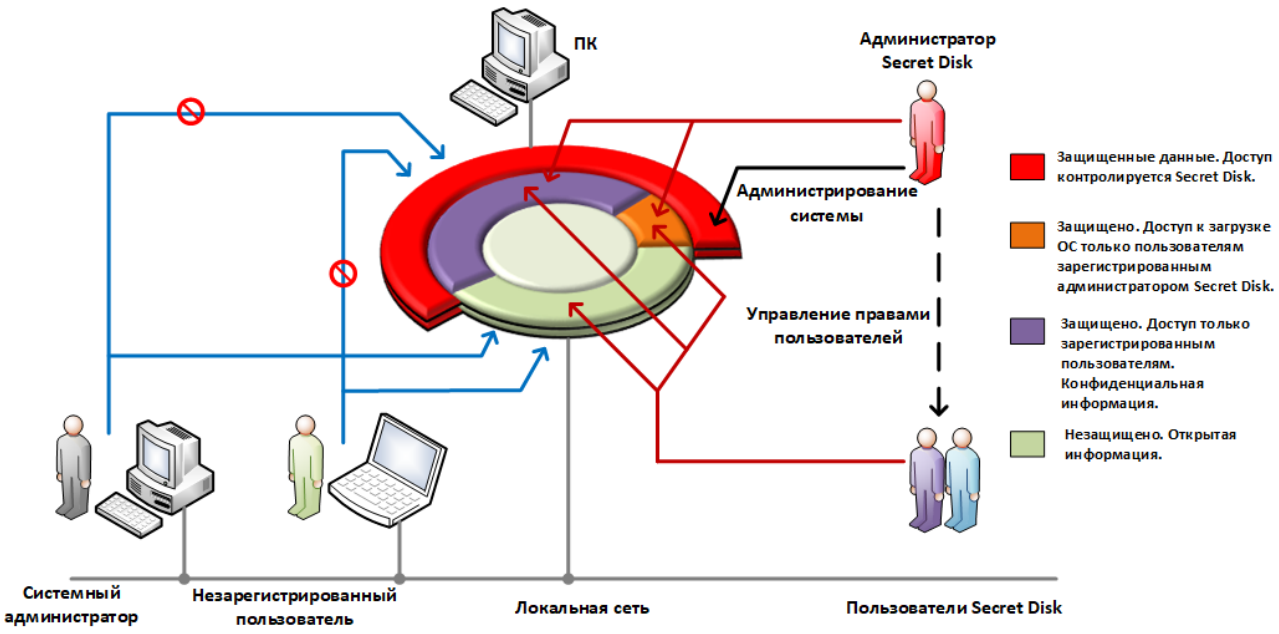


Рис. 5.25. Secret Disk

5.7. Стеганография

Стеганография — это метод организации связи (передачи сообщений), при котором скрывается само наличие связи. В отличие от криптографии, где противник точно может определить, является ли передаваемое сообщение за-

шифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в открытые послания таким образом, чтобы было невозможным заподозрить существование самого встроенного послания. Цель криптографии состоит в блокировании несанкционированного доступа к информации путем шифрования содержания секретных сообщений. Цель стеганографии — в скрытии самого факта существования секретного сообщения.

Компьютерная стеганогорафия основана на двух принципах. Первый принцип заключается в том, что файлы, содержащие оцифрованную информацию (например, изображение или звук), могут быть до некоторой степени видоизменены без потери их функциональности в отличие от других типов данных, требующих абсолютной точности. Второй принцип заключается в неспособности органов чувств человека различать незначительные изменения в цвете изображения или качестве звука, а также видеть служебную информацию, внедренную в файл. Этот принцип особенно легко применять к файлам, несущим избыточную информацию.

Стеганографическая система, или стегосистема, — это совокупность средств и методов, которые используются для формирования скрытого канала передачи информации. Требования к стегосистеме:

– методы скрытия должны обеспечивать аутентичность и целостность информации, в которой скрывается сообщение;

– противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, неизвестной потенциальному противнику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержания скрытого сообщения;

– если противник каким-то образом узнает о факте существования скрытого сообщения, то это не должно позволить ему извлечь скрытую информацию из других данных до тех пор, пока ключ хранится в тайне;

– потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания скрытых сообщений.

Структурная схема стегосистемы представлена на рис. 5.26.

Рис. 5.26. Структурная схема стегосистемы

Сообщение — это любая информация, подлежащая скрытой передаче. В качестве сообщения может использоваться любой вид информации: текст, изображение, аудиосигнал. Встроенное (скрытое) сообщение — это сообщение, встроенное в контейнер. Контейнер — это любая информация, предназначенная для скрытия сообщения. По размеру (протяженности) контейнеры бывают двух типов: непрерывные (потоковые) и ограниченной (фиксированной) длины.

Возможны следующие варианты контейнеров. Контейнер генерируется самой стегосистемой. Такой подход называется конструирующей стеганографией. Контейнер выбирается из некоторого множества генерируемых стегосистемой контейнеров. Такой подход называется селектирующей стеганографией. Контейнер поступает извне стегосистемы. Такой подход называется безальтернативной стеганографией.

В зависимости от вида информации, используемой для встраивания сообщений, контейнеры могут быть визуальные, звуковые, текстовые и др. Визуальный контейнер представляет собой картинку или фотографию, в которой для встраивания сообщений используются небольшие изменения яркости заранее определенных точек растра изображения. Звуковой контейнер представляет собой речевой или музыкальный сигнал, в котором для встраивания сообщений используются младшие биты аудиосигнала, что практически не отражается на качестве звука. Текстовый контейнер представляет собой текстовый файл, подготовленный к печати на принтере, в котором для встраивания сообщений используются небольшие изменения стандартов печати (расстояния между буквами, словами и строками, размеры букв, строк и др.). При выборе контейнера необходимо иметь в виду, что при увеличении объема встраиваемого сообщения снижается надежность стегосистемы (при неизменном размере контейнера). Таким образом, используемый в стегосистеме контейнер накладывает ограничения на размер встраиваемого сообщения.

По аналогии с криптографией по типу стегоключа стегосистемы подразделяются на два вида: с секретным ключом и с открытым ключом. В стегосистеме с секретным ключом используется один ключ, который должен быть определен либо до начала обмена секретными сообщениями, либо передан по защищенному каналу. В стегосистеме с открытым ключом для встраивания и извлечения сообщения используются разные ключи, различие которых состоит в том, что с помощью вычислений невозможно определить один ключ из другого. Поэтому один ключ (открытый) может передаваться свободно по незащищенному каналу связи.

Любая стегосистема должна отвечать следующим требованиям:

– свойства контейнера должны быть модифицированы таким образом, чтобы изменение невозможно было выявить;

– стегосообщение должно быть устойчиво к искажениям, которые могут иметь место при его передаче, включая и различные трансформации (уменьшение, увеличение, преобразование в другой формат, сжатие без потери информации, сжатие с потерей информации и т.д.);

– для сохранения целостности встраиваемого сообщения необходимо использовать коды с исправлением ошибок;

– для повышения надежности встраиваемое сообщение может быть продублировано

Методы компьютерной стеганографии можно разделить в целом на два вида:

– методы, основанные на избыточности визуальной и аудиоинформации;

– методы, основанные на использовании специальных свойств компьютерных форматов.

Методы, основанные на избыточности визуальной и аудиоинформации, для скрытия информации используют младшие разряды цифровых отсчетов цифрового изображения и звука, которые содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия, что и дает возможность скрытия конфиденциальной информации (рис. 5.27).

Рис. 5.27. Метод наименее значащих битов

Младшие биты дают незначительный вклад в изображение по сравнению со старшими. Замена одного или двух младших бит для человеческого глаза будет почти незаметна. Преимуществом этих методов является возможность скрытой передачи большого объема информации и возможность защиты авторского права путем создания скрытого изображения товарной марки, регистрационного номера и т.п. Недостаток метода состоит в том, что за счет введения дополнительной информации искажаются статистические характеристики цифровых потоков. Для снижения компрометирующих признаков требуется коррекция статистических характеристик. Методы, основанные на использовании специальных свойств компьютерных форматов, делятся на:

– методы использования зарезервированных для расширения полей компьютерных форматов данных;

– методы специального форматирования текстовых файлов;

– методы скрытия в неиспользуемых местах компакт-дисков;

– методы использования имитирующих функций;

– методы удаления идентифицирующего файл заголовка.

Методы использования зарезервированных для расширения полей компьютерных форматов данных основаны на том, что многие мультимедийные форматы имеют поля расширения, которые заполняются нулевой информацией и не учитываются программой. В эти поля и записывается скрываемая информация. Методы специального форматирования текстовых файлов в свою очередь делятся на:

– методы использования известного смещения строк, слов, предложений, абзацев;

– методы выбора определенных позиций букв;

– методы использования специальных свойств, не отображаемых на экране полей форматов.

Методы использования известного смещения строк, слов, предложений, абзацев основаны на изменении положения строк и расстановки слов в предложении, что обеспечивается вставкой дополнительных пробелов между словами. Методы выбора определенных позиций букв используют принцип нулевого шифра. Акростих является частным случаем этого метода, когда, например, начальные буквы каждой строки образуют сообщение. Методы использования специальных свойств, не отображаемых на экране полей форматов, основаны на использовании специальных скрытых полей для организации сносок и ссылок, например использование черного шрифта на черном фоне.

Методы скрытия в неиспользуемых местах компакт дисков основаны на том, что скрываемая информация записывается в обычно неиспользуемых местах дисков (например, в нулевой дорожке).

Методы использования имитирующих функций основаны на генерации осмысленного текста, скрывающего информацию.

Методы удаления идентифицирующего файл заголовка основаны на том, что скрываемая информация шифруется и в нем удаляется идентифицирующий заголовок, который заранее известен пользователю.

Преимуществом этих методов является простота их реализации, а недостатком — низкая степень скрытности и передача небольших объемов информации.

Вопросы для самоконтроля

1. Классификация методов криптографического закрытия информации.
2. Дайте определение шифра и сформулируйте основные требования к нему.
3. Поясните, что понимается под совершенным шифром.
4. Как организован обмен документами, заверенными цифровой подписью?
5. Что такое средства стеганографической защиты информации?
6. Что такое криптография?
7. Какие используются симметричные алгоритмы шифрования?

8. Какие используются асимметричные алгоритмы шифрования?

9. Что такое криптографическая хеш-функция?

10. Какие используются криптографические хеш-функции?

11. Что такое цифровая подпись?

12. Что такое инфраструктура открытых ключей?

13. Стандарт шифрования данных (DES — Data Encryption Standard).

13. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard).

14. Асимметрично-ключевая криптографическая система: RSA (Riverst — Shamir — Adleman).

15. Асимметрично-ключевые криптографические системы: Эль-Гамаля (ElGamal).

6. ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ

6.1. Вредоносное программное обеспечение

Вредоносная программа (Malware, malicious software — злонамеренное программное обеспечение, программа с потенциально опасными последствиями) — это любое программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы в обход существующих правил разграничения доступа.

Программно-математическое воздействие — это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество несанкционированных функций. Программа с потенциально опасными последствиями способна выполнять любые следующие функции:

– скрывать признаки своего присутствия в программной среде компьютера;

– обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

– разрушать (искажать произвольным образом) код программ в оперативной памяти;

– выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирование, уничтожение, блокирование и т.п.);

– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Наличие в ИС вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных, каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную и криптографическую защиту. «Вредность» или «полезность» программного обеспечения определяется самим пользователем или способом его применения. Общепризнанной классификации вредоносного ПО не существует. Основными видами вредоносных программ являются [37]:

– программные закладки;

– классические программные (компьютерные) вирусы;

– вредоносные программы, распространяющиеся по сети (сетевые черви);

– другие вредоносные программы, предназначенные для осуществления НСД.

К программным закладкам относятся программы, фрагменты кода, инструкции, формирующие недекларированные возможности программного обеспечения. Вредоносные программы могут переходить из одного вида в другой, например, программная закладка может сгенерировать программный вирус, который, в свою очередь, попав в условия сети, может сформировать сетевого червя или другую вредоносную программу, предназначенную для осуществления НСД.

6.2. Компьютерные вирусы

Компьютерный вирус — это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и (или) файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению. Это условие не является достаточным, т.е. окончательным. Жизненный цикл любого компьютерного вируса можно разделить на пять стадий:

- проникновение на чужой компьютер;
- активация;
- поиск объектов для заражения;
- подготовка копий;
- внедрение копий.

При подготовке своих вирусных копий для маскировки от антивирусов могут применять такие технологии, как:

1. Шифрование — в этом случае вирус состоит из двух частей: сам вирус и шифратор.

2. Метаморфизм — при применении этого метода вирусные копии создаются путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, обычно ничего не делающих команд.

Основные цели любого компьютерного вируса — это распространение на другие ресурсы компьютера и выполнение специальных действий при определенных событиях или действиях пользователя (например, 26 числа каждого четного месяца или при перезагрузке компьютера). Специальные действия нередко оказываются вредоносными.

Классификация программных вирусов и сетевых червей по видению ФСТЭК представлена на рис. 6.1. Источником является «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [37].

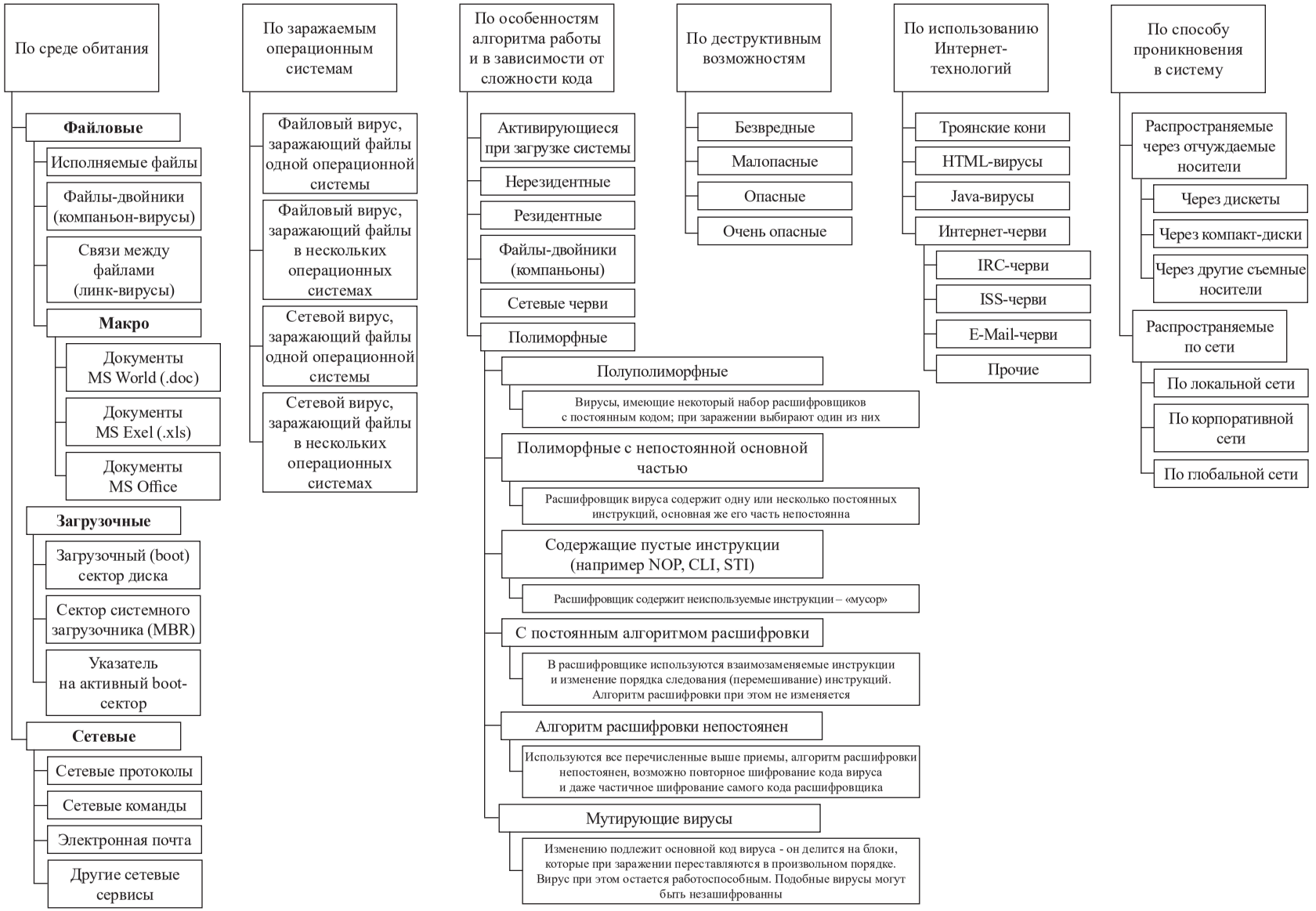


Рис. 6.1. Классификация программных вирусов и сетевых червей

Большое количество всех классов вирусов рассматривать не имеет смысла, можно обратиться к первоисточнику. Поэтому приведем классы, которые наиболее часто фигурируют в литературе по информационной безопасности. Основным параметром классификации является среда обитания вируса. Это могут быть файловые или загрузочные вирусы.

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор. Они внедряются в память компьютера при загрузке с инфицированного диска. При этом системный загрузчик считывает содержимое первого сектора диска, с которого производится загрузка, помещает считанную информацию в память и передает на нее (т.е. на вирус) управление. После этого начинают выполняться инструкции вируса, который, как правило, уменьшает объем свободной памяти, копирует в освободившееся место свой код и считывает с диска свое продолжение (если оно есть), перехватывает необходимые вектора прерываний, считывает в память оригинальный boot-сектор и передает на него управление.

В дальнейшем загрузочный вирус ведет себя так же, как файловый: перехватывает обращения операционной системы к дискам и инфицирует их, в зависимости от некоторых условий совершает деструктивные действия, вызывает звуковые эффекты или видеоэффекты.

Файловые вирусы при своем размножении тем или иным способом используют файловую систему какой-либо операционной системы. По способу заражения файлов вирусы делятся на замещающие («overwriting»), паразитические («parasitic»), компаньон-вирусы («companion»), вирусы-черви, «link»-вирусы и вирусы, заражающие объектные модули (OBJ), библиотеки компиляторов (LIB) и исходные тексты программ.

Метод заражения «overwriting» является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.

К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными. Основными типами таких вирусов являются вирусы, записывающиеся в начало, середину или конец файлов. Незначительная группа паразитических вирусов, не имеющих «точки входа» (EPO-вирусы — Entry Point Obscuring viruses). EPO-вирусы, не записывают команду передачи управления в заголовок файлов и не изменяют адрес точки старта в заголовке EXE-файлов. Они записывают команду перехода на свой код в какое-либо место в середину файла и получают управление не непосредственно при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса. Выполняться эта процедура может крайне редко (например, при выводе сообщения о какой-либо специфической ошибке). В результате вирус может долгие годы «спать» внутри файла и проявить себя только при некоторых ограниченных условиях.

К категории «компаньон» относятся вирусы, не изменяющие заражаемые файлы. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус. Наиболее распространены компаньон-вирусы, использующие особенность ОС первым выполнять файлы с расширением .COM, если в одном каталоге присутствуют два файла с одним и тем же именем, но различными расширениями имени — .COM и .EXE. Такие вирусы создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением .COM, например для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM-файл и никак не изменяет EXE-файл. При запуске такого файла ОС первым обнаружит и выполнит COM-файл, т.е. вирус, который затем запустит и EXE-файл. Вторую группу составляют вирусы, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла. Например, файл XCOPY.EXE переименовывается в XCOPY.EXD, а вирус записывается под именем XCOPY.EXE. При запуске управление получает код вируса, который затем запускает оригинальный XCOPY, хранящийся под именем XCOPY.EXD. В третью группу входят «Path-companion» вирусы. Они либо записывают свой код под именем заражаемого файла, но «выше» на один уровень в прописываемых путях (ОС, таким образом, первым обнаружит и запустит файл-вирус), либо переносят файл-жертву на один подкаталог ниже и т.д.

Возможно существование и других типов компаньон-вирусов, использующих иные оригинальные идеи или особенности других операционных систем.

Файловые черви являются в некотором смысле разновидностью компаньон-вирусов, но при этом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на запуск своей копии, например INSTALL.EXE или WINSTART.BAT. Существуют вирусы-черви, использующие довольно необычные приемы, например записывающие свои копии в архивы (ARJ, ZIP и пр.). Некоторые вирусы записывают команду запуска зараженного файла в BAT-файлы.

Link-вирусы, как и компаньон-вирусы, не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

Вирусы, заражающие библиотеки компиляторов, объектные модули и исходные тексты программ, достаточно экзотичны и практически не распространены. Вирусы, заражающие OBJ- и LIB-файлы, записывают в них свой код в формате объектного модуля или библиотеки. Зараженный файл, таким образом, не является выполняемым и не способен на дальнейшее распространение вируса в своем текущем состоянии. Носителем же «живого» вируса становится COM- или EXE-файл.

Макровирусы (macro viruses) являются программами на языках (макроязыках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. Наибольшее распространение получили макровирусы для пакета прикладных программ Microsoft Office. Для существования вирусов в конкретной системе (редакторе) необходимо наличие встроенного в систему макроязыка с возможностями:

– привязки программы на макроязыке к конкретному файлу;

– копирования макропрограмм из одного файла в другой;

– получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы).

Данным условиям удовлетворяют прикладные программы Microsoft Word, Excel и Microsoft Access. Они содержат в себе макроязыки: Word Basic, Visual Basic for Applications. При этом:

– макропрограммы привязаны к конкретному файлу или находятся внутри файла;

– макроязык позволяет копировать файлы или перемещать макропрограммы в служебные файлы системы и редактируемые файлы;

– при работе с файлом при определенных условиях (открытие, закрытие и т.д.) вызываются макропрограммы (если таковые есть), которые определены специальным образом или имеют стандартные имена.

Приведем другие виды классификации вирусов.

По режиму функционирования:

– резидентные вирусы — вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

– транзитные (нерезидентные) вирусы — вирусы, которые выполняются только в момент запуска зараженной программы.

По деструктивным возможностям вирусы подразделяются на:

– безвредные вирусы — это вирусы, никак не влияющие на работу компьютера за исключение, быть может, уменьшения свободного места на диске и объема оперативной памяти;

– неопасные вирусы — вирусы, которые проявляют себя в выводе различных графических, звуковых эффектов и прочих безвредных действий;

– опасные вирусы — это вирусы, которые могут привести к различным сбоям в работе компьютеров, а также их систем и сетей;

– очень опасные вирусы — это вирусы, приводящие к потере, уничтожению информации, потере работоспособности программ и системы в целом.

6.3. Сетевые черви

К сетевым относятся черви, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основ-

ным принципом работы сетевого червя является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые черви при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или по крайней мере подтолкнуть пользователя к запуску зараженного файла.

Червь (сетевой червь) — это вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом. Жизненный цикл червей состоит из таких стадий:

- проникновение в систему;
- активация;
- поиск объектов для заражения;
- подготовка копий;
- распространение копий.

В зависимости от способа проникновения в систему черви делятся на типы:

- классические сетевые черви — используют для распространения локальные сети и Интернет;
- почтовые черви — распространяются с помощью почтовых программ;
- IM-черви — используют системы мгновенного обмена сообщениями;
- IRC-черви — распространяются по каналам IRC;
- P2P-черви — при помощи пиринговых файлообменных сетей.

После проникновения на компьютер червь должен активироваться. По методу активации все черви можно разделить на две большие группы:

- требуют активного участия пользователя;
- не требуют активного участия пользователя.

Отличительная особенность червей из первой группы — это использование обманных методов. Например, когда получатель инфицированного файла вводится в заблуждение текстом письма и добровольно открывает вложение с почтовым червем, тем самым его активируя. В последнее время наметилась тенденция к совмещению этих двух технологий — такие черви наиболее опасны и часто вызывают глобальные эпидемии. Сетевые черви могут кооперироваться с вирусами — такая пара способна самостоятельно распространяться по сети (благодаря червю) и в то же время заражать ресурсы компьютера (функции вируса).

6.4. Вредоносные программы для осуществления НСД

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;

– программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИС;

– программы-генераторы компьютерных вирусов;

– программы, демонстрирующие уязвимости средств защиты информации и др.

Чаще всего такие программы называются трояны или программы класса троянский конь. В отличие от вирусов и червей они не обязаны уметь размножаться. Это программы, написанные только с одной целью — нанести ущерб целевому компьютеру путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях. **Троян (троянский конь)** — программа, основной целью которой является вредоносное воздействие по отношению к компьютерной системе.

Некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы с целью проникновения в нее. Однако в большинстве случаев они проникают на компьютеры вместе с вирусом либо червем, т.е. такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу. Нередко пользователи сами загружают троянские программы из Интернета. Жизненный цикл троянов состоит всего из трех стадий:

– проникновение в систему;

– активация;

– выполнение вредоносных действий.

Главная цель написания троянов — это производство несанкционированных действий, они классифицируются по типу вредоносной нагрузки.

Клавиатурные шпионы (Trojan-SPY), постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры с целью последующей их передачи своему автору.

Похитители паролей (Trojan-PSW) предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат.

Утилиты скрытого удаленного управления (Backdoor) — это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером.

Анонимные SMTP-сервера и прокси-сервера (Trojan-Proxy) — такие трояны на зараженном компьютере организовывают несанкционированную отправку электронной почты, что часто используется для рассылки спама.

Модификаторы настроек браузера (Trojan-Cliker) — трояны, которые меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки для организации несанкционированных обращений к Интернет-ресурсам.

Инсталляторы прочих вредоносных программ (Trojan-Dropper) — трояны, представляющие возможность злоумышленнику производить скрытую установку других программ.

Загрузчики вредоносных программ (Trojan Downloader) — трояны, предназначенные для загрузки на компьютер-жертву новых версий вредоносных программ или рекламных систем.

Уведомители об успешной атаке (Trojan-Notifier) — трояны данного типа предназначены для сообщения своему хозяину о зараженном компьютере.

«Бомбы» в архивах (ARCBomb) — трояны, представляющие собой архивы, специально оформленные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные — зависание или существенное замедление работы компьютера, заполнение диска большим количеством пустых данных.

Логические бомбы — чаще не столько трояны, сколько троянские составляющие червей и вирусов, суть работы которых состоит в том, чтобы при определенных условиях (дата, время суток, действия пользователя, команда извне) произвести определенное действие, например уничтожение данных.

Утилиты дозвона — это тип троянов, представляющий собой утилиты доступа в Интернет через платные службы. Такие трояны прописываются в системе как утилиты дозвона по умолчанию и влекут за собой крупные счета за пользование Интернетом.

Кроме троянов к вредоносным программам, способствующим получению несанкционированного доступа, можно отнести условно опасные программы, т.е. такие, о которых нельзя однозначно сказать, что они вредоносны. Такие программы обычно становятся опасными только при определенных условиях или действиях пользователя. К ним относятся:

1. Riskware — вполне легальные программы, которые сами по себе не опасны, но обладают функционалом, позволяющим злоумышленнику использовать их с вредоносными целями. К riskware относятся обычные утилиты удаленного управления, которыми часто пользуются администраторы больших сетей, клиенты IRC, программы для загрузки файлов из Интернета, утилиты восстановления забытых паролей и др.

2. Рекламные утилиты (adware) — условно-бесплатные программы, которые в качестве платы за свое использование демонстрируют пользователю рекламу, чаще всего в виде графических баннеров. После официальной оплаты и регистрации обычно показ рекламы заканчивается и программы начинают работать в обычном режиме. Проблема adware кроется в механизмах, которые используются для загрузки рекламы на компьютер. Кроме того, что для этих целей часто используются программы сторонних и не всегда проверенных производителей, даже после регистрации такие модули могут автоматически не удаляться и продолжать свою работу в скрытом режиме.

3. Хакерские утилиты — к этому виду программ относятся программы скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), автоматизации создания сетевых червей, компьютерных вирусов и троянских программ (конструкторы вирусов), наборы программ, которые используют хакеры для скрытного взятия под контроль взломанной системы (RootKit) и другие подобные утилиты. То есть такие специфические программы, которые обычно используют только хакеры.

4. Злые шутки — программы, которые намеренно вводят пользователя в заблуждение путем показа уведомлений, например, о форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит. Текст таких сообщений целиком и полностью отражает фантазию автора.

В связи с усложнением и возрастанием разнообразия программного обеспечения число вредоносных программ быстро возрастает. Сегодня известно более 120 тыс. сигнатур компьютерных вирусов. Вместе с тем далеко не все из них представляют реальную угрозу. Во многих случаях устранение уязвимостей в системном или прикладном программном обеспечении привело к тому, что ряд вредоносных программ уже не способен внедриться в них. Часто основную опасность представляют новые вредоносные программы.

6.5. Признаки заражения компьютера и его защита

С компьютером происходят «странные» вещи, а именно:

– на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы;

– неожиданно открывается и закрывается лоток CD-ROM-устройства;

– произвольно, без участия пользователя, на компьютере запускаются какие-либо программы;

– на экран выводятся предупреждения о попытке какой-либо из программ выйти в Интернет, хотя пользователь никак не инициировал такое ее поведение.

Характерные признаки поражения вирусом через почту:

– знакомые говорят вам о сообщениях от вас, которые вы не отправляли;

– в почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Косвенные признаки заражения компьютера:

– частые зависания и сбои в работе компьютера;

– медленная работа компьютера при запуске программ;

– невозможность загрузки операционной системы;

– исчезновение файлов и каталогов или искажение их содержимого;

– частое обращение к жесткому диску (часто мигает лампочка на системном блоке);

– браузер «зависает» или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

Защита от вредоносных программ осуществляется посредством антивирусного программного обеспечения. На сегодняшний день известны два алгоритма обнаружения вредоносных программ — это сигнатурный анализ и эвристический анализ.

Сигнатурный анализ. Самый простой метод обнаружения заключается в том, что для поиска известных вирусов используются так называемые маски. Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса.

Эвристический анализ. Для того чтобы размножаться, компьютерный вирус должен совершать какие-то конкретные действия: копирование в память, запись в секторы и т.д. Эвристический анализатор (который является частью антивирусного ядра) содержит список таких действий и проверяет программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов.

6.6. Эволюция компьютерных вирусов

Идея создания неких механизмов, способных (по аналогии с биологическим миром) «размножаться», были сформулированы Джоном фон Нейманом (конец 40-х — начало 50-х гг. XX в.) в серии своих лекций. В 1966 г. вышла его монография «Теория самовоспроизводящихся автоматов», по сути, это мысленный эксперимент, рассматривающий возможность существования «механического» организма (например, компьютерного кода), который бы повреждал машины, создавал собственные копии и заражал новые машины аналогично тому, как это делает биологический вирус.

В 1961 г. ряд специалистов Bell Telephone Laboratories (США) (в том числе и Роберт Моррис — старший) изобрели игру «Дарвин». Ее сюжет и смысл были просты: игрок руководил «расой», которая должна была уничтожить своих конкурентов. Выигрывал тот, кто захватит всю отданную под игровой процесс оперативную память. Особых действий в игре не требовалось: необходимо было лишь размножить принадлежащих к своей расе на свободные ячейки ОЗУ или же захватить ячейки противника. Подобный алгоритм очень похож на логику работы деструктивных программ.

Программа Creeper, о которой часто говорят как о первом вирусе, была создана в 1971 г. сотрудником компании BBN. Creeper был создан как тестовая программа, чтобы проверить, возможна ли в принципе самовоспроизводящаяся программа. Заразив новый жесткий диск, Creeper пытался удалить себя с предыдущего компьютера. Creeper не совершал никаких вредоносных действий. На зараженных системах вирус обнаруживал себя сообщением: «I'M THE CREEPER… CATCH ME IF YOU CAN» («я Крипер… поймай меня, если сможешь»). Для удаления этого вируса была создана программа Reaper.

Вирус Rabbit (также известный как Wabbit) был создан в 1974 г. с вредоносной целью и мог самовоспроизводиться. Попав на компьютер, он делал большое количество копий себя, значительно ухудшал работоспособность системы и в итоге приводил к отказу компьютера. Имя («Кролик») было дано вирусу из-за того, что он очень быстро самовоспроизводился.

Логическая игра Pervading Animal была разработана в 1975 г. для операционной системы Exec 8. Смысл ее заключался в том, что пользователь загадывал какое-нибудь животное, а программа должна была его угадать за 20 вопросов. Если это не удавалось, игра предлагала модернизировать ее, после чего появлялась возможность задавать дополнительные наводящие вопросы. Игра пользовалась популярностью, и, чтобы упростить процедуру распространения копий, автор создал программу PERVADE, которая устанавливалась на компь-

ютер вместе с игрой ANIMAL. Пока пользователь играл в игру, PREVADE проверял все доступные пользователю директории на компьютере, а затем копировал ANIMAL во все директории, где этой программы не было. Вредоносной цели здесь не было, но ANIMAL и PREVADE подпадают под определение троянца: по сути, внутри программы ANIMAL была запрятана другая программа, которая выполняла действия без согласия пользователя.

Elk Cloner (1981 г., был написан 15-летним школьником Ричардом Скрента для компьютеров Apple II). Он записывал свое тело в загрузочные сектора дискет и после каждой 50-й загрузки вирус выводил на экран текст:

«Elk Cloner: программа с индивидуальностью
Она проникнет во все ваши диски
Она внедрится в ваши чипы
Да, это — Cloner!
Она прилипнет к вам как клей
Она даже изменит оперативную память
Cloner выходит на охоту!»

В 1983 г. американский ученый Фред Коэн (Fred Cohen) в своей диссертационной работе, посвященной исследованию самовоспроизводящихся компьютерных программ, впервые ввел термин «компьютерный вирус». 10 ноября 1983 г. состоялась первая демонстрация самовоспроизводящейся программы, после чего была опубликована фундаментальная работа «Computer Viruses: theory and experiments» с подробным описанием проблемы (1984 г.). Компьютерный вирус (историческое) — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ.

В 1984 г. вышли в свет первые антивирусные программы — CHK4BOMB и BOMBSQAD. Их автором был Энди Хопкинс (Andy Hopkins). Программы анализировали загрузочные модули и позволяли перехватывать запись и форматирование, выполняемые через BIOS. На то время они были очень эффективны и быстро завоевали популярность.

Brain (1986 г.) — первый вирус для IBM-совместимых компьютеров. Был написан двумя братьями-программистами из Пакистана в целях отслеживания пиратских копий их медицинского программного обеспечения и не был нацелен на причинение вреда. Вирус инфицировал загрузочные сектора дискет (5,25”, 360 кБ), постепенно и незаметно заполнял все содержимое дискеты. Отличительной чертой его была впервые использованная стелс-функция (он «прятался» в загрузочном секторе, который не проверялся существующими антивирусами), что делало невозможным его обнаружение. Пиратская программа отжирала оперативку, замедляла работу диска и иногда мешала сохранить данные. Она не уничтожала данные и содержала следующее сообщение: «Добро пожаловать в подземелье… Берегитесь этого вируса… Свяжитесь с нами для лечения…». В заголовке были указаны реальные контакты. В течение нескольких месяцев программа вышла за пределы Пакистана, и к лету 1987 г. эпидемия достигла глобальных масштабов (тысячи компьютеров по всему ми-

ру). Проблема оказалась в том, что Brain распространялся и по другим дискетам, а не только по копиям их программы.

В 1986 г. Немецкий программист Ральф Бюргер (Ralf Burger) открыл возможность создания программой своих копий путем добавления своего кода к исполняемым DOS-файлам формата *.com. Опытный образец программы — Virdem был продемонстрирован в декабре 1986 г. По результатам исследований Бюргер выпустил книгу «Computer Viruses. A high-tech disease», послужившую толчком к написанию тысяч компьютерных вирусов, частично или полностью использовавших описанные автором идеи. В этой книге ко всему прочему была изложена концепция резидентных вирусов. Огромное количество компьютерных вирусов были направлены на интерпретатор команд MS-DOS — command.com.

Lehigh (1987 г.) — первый вредоносный вирус, вызвавший локальную эпидемию в Лехайском университете (США). Заражению подвергался интерпретатор command.com. После четырех перезагрузок вирус обнулял первые 32 сектора диска, на котором он находился. Был обнаружен студенческими консультантами Вычислительного центра Лехайского университета. Они обратили внимание, что начиная с 18 октября 1987 г. пользователи начали в массовом порядке возвращать выданные им дискеты, заявляя, что они дефектны. В течение нескольких дней было уничтожено содержимое сотен дискет из библиотеки университета и личных дискет студентов. Всего за время эпидемии было заражено около 4 тыс. компьютеров.

Suriv (иерусалимская группа) (1987 г., Израиль), семейство резидентных файловых вирусов, ориентированных на MS-DOS. Самая известная модификация Jerusalem (Black Friday, BlackBox) способна заражать *.exe файлы достаточно универсальным способом. При запуске зараженной программы вирус проверял наличие своей копии в памяти компьютера. В случае своего отсутствия в памяти его действия сводились к загрузке вредоносного кода в память, последующему перехвату файловых операций и заражению запускаемых пользователем *.com и *.exe файлов. Фаза проявления Suriv наступала через некоторое время после того, как вирус становился резидентным (в зависимости от даты и дня недели). В «обычный» день (не пятницу, 13-го) проявление данного вируса состояло в замедлении работы компьютера. Например, команда DIR приводила к медленному «выползанию» строк на экран. В силу перехвата вирусом прерывания от таймера (8h) при каждом прерывании вирус выполнял нескольких тысяч команд. Вторым визуальным эффектом было «вырывание» кусков изображения с появлением на экране черного окна в левом нижнем углу экрана (скроллинг части экрана). Если текущий день недели — пятница, 13-е, то в такой день вирус не заражал, а просто удалял файлы с диска.

Mike RoChenle — псевдоним автора первой известной вирусной мистификации. В октябре 1988 г. он разослал на станции BBS (bulletin board system — электронная доска объявлений) большое количество сообщений о вирусе, который передается от модема к модему со скоростью 2 400 бит/с. В качестве панацеи предлагалось перейти на использование модемов со скоростью

1 200 бит/с. Как это ни смешно, многие пользователи действительно последовали этому совету.

Червь Морриса (конец 1988 г.) — первый вредоносный сетевой червь. Написан 23-летним аспирантом Корнельского университета (США) Робертом Моррисом — младшим. Вирус не предполагал вредоносной функции, а целью его написания было исследование распространения программ в сети. Вирус Морриса был запущен в Arpanet и был нацелен только на ПЭВМ типа Sun 3 и VAX, которые использовали варианты ОС Unix версии 4 BSD. Для проникновения на компьютер использовался подбор паролей (в том числе и по словарю 400 ключевых слов) и последующая «маскировка» под легального пользователя системы. Из-за ошибок в разработке, вызвавших превышение скорости размножения и распространения, программа забирала «под себя» большую часть (или все) вычислительные и сетевые ресурсы. Червь Морриса заразил, по разным оценкам, от 6 000 до 9 000 компьютеров в США (включая центр NASA) и парализовал их работу на срок до пяти суток. Общая стоимость прямых и косвенных потерь оценивается в 96 млн долл.

Aids Information Diskette (декабрь 1989 г.) — первая эпидемия троянской программы-вымогателя. Ее автор разослал около 20 тыс. дискет с вирусом по адресам в Европе, Африке и Австралии, похищенным из баз данных Организации всемирного здравоохранения и журнала PC Business World. После запуска вредоносная программа инфицировала систему, постепенно повреждая файлы компьютера, через 90 загрузок ОС все файлы на диске становились недоступными, кроме одного — с сообщением, предлагавшим прислать 189 долл. на указанный адрес. Автор первого трояна (признанный позднее невменяемым), был задержан в момент обналичивания чека и осужден за вымогательство.

Cascade (1988–1991 гг.) — семейство резидентных зашифрованных вирусов (первый вирус с шифрованием своего тела), вызывающее характерный видеоэффект — осыпание букв на экране (с блокированием ввода). Это первый резидентный вирус, зафиксированный в СССР.

Начало 90-х гг. XX в. окончательно сместило цели написания вредоносного ПО в область личных корыстных (реже идейных) целей.

Chameleon (начало 1990 г.) — первый полиморфный вирус. Его автор Марк Уошбурн за основу для написания программы взял сведения о вирусе Vienna (из книги Бюргера) и добавил к ним усовершенствованные принципы самошифрации вируса Cascade — свойство изменять внешний вид (метаморфизм) как тела вируса, так и самого расшифровщика.

DiskKiller (1990 г.) — этим вирусом была заражена дискета бесплатного приложения к журналу PC Today. В июле 1990 г. подписчикам разошлось около 50 тыс. экземпляров. Действие DiskKiller сводилось к уничтожению всей информации на жестком диске. Первая в истории компрометация крупной компании с помощью вредоносного ПО.

В начале 1990 г. впервые были обнаружены и первые российские вирусы — Peterburg (Пакость-1 и Пакость-2), Voronezh (Пакость-3).

Win.Vir (конец 1992 г.) — первый вирус, поражающий исполняемые файлы Microsoft Windows 3.1. Эпидемии не вызвал и его появление осталось

практически незаметным. Однако он положил начало эпохи вирусов для Windows.

OneHalf (Slovak Bomber, Explosion-II, Freelove) (лето 1994 г.) — сложный резидентный файлово-загрузочный полиморфный вирус. Первый шифратор, вызвавший глобальную эпидемию во всем мире, в том числе в России. Заражал MBR и boot-сектора дискет, а также *.com и *.exe файлы. На зараженном компьютере вирус постепенно шифровал данные пользователя, при этом пользователь ничего не замечал, поскольку OneHalf перехватывал обращения к уже зашифрованным дорожкам и моментально расшифровывал их на лету. Затем OneHalf анализировал три параметра: зашифрованость половины диска, кратность системной даты четырем, четность счетчика заражений (содержался в теле самого вируса). При положительной проверке на дисплей выводилось сообщение: «Dis is one half. Press any key to continue…».

С 1994 г. рост вредоносного ПО начинается в геометрической прогрессии. При этом интенсивно появляются и технологические идеи для создания вредоносного ПО.

Shifter (январь 1994 г.) — первый вирус, заражающий объектные модули (OBJ-файлы).

SrcVir (апрель 1994 г.) — семейство вирусов, заражающих исходные тексты программ (C и Pascal).

Concept (август 1995 г.) — первый макровирус, поражавший документы Microsoft Word.

Linux.Bliss (февраль 1997 г.) — первый вирус для ОС Linux.

Наиболее разрушительные вирусы были созданы в конце 90-х, предпосылками к этому послужило развитие Интернета.

CIH (1998 г.) — ущерб, нанесенный вирусом, составил порядка 80 млн долл. Вирус был написан программистом из Тайваня и стал одним из самых разрушительных в истории. «Чих» заражал исполняемые файлы и активировался каждый год 26 апреля — в день годовщины аварии на Чернобыльской АЭС. CIH перезаписывал FlashBIOS, после чего материнские платы становились непригодными к использованию. Первый и последний вирус, который наносил вред аппаратной части ПК.

Melissa (1999 г.) — 26 марта 1999 г. этот макровирус, распространявшийся по электронной почте, заразил около 20 % офисных компьютеров по всему миру. Крупнейшие корпорации, такие как Intel, были вынуждены прекратить работу внутри своих локальных сетей. Ущерб — от 300 до 500 млн долл.

ILOVEYOU (2000 г.) — скрипт, написанный на макроязыке Visual Basic. Так же, как и Melissa, распространялся по электронной почте с темой письма «I love you». Вирус рассылал свои копии по всем данным адресной книги почтового клиента. Все логины и пароли, найденные червем на компьютере, отсылались автору программы. Последний, кстати, и не пытался скрываться: он является жителем Филиппин, где наказаний за компьютерные преступления не предусмотрено.

Code Red (2001 г.) — сетевой червь, использующий ошибку в сетевом сервисе Microsoft IIS. В заданный день зараженные компьютеры должны были

начать DDOS-атаку по списку различных серверов, среди которых были системы правительства США. Огромные масштабы эпидемии и как итог — убытки в 2,5 млрд (!) долл.

Blaster (2003 г.) — сетевой червь, выводивший на зараженных компьютерах сообщение о необходимости перезагрузки. Через пару дней после его выпуска в Интернет (11 августа) были заражены миллионы компьютеров по всему миру.

Sobig.F (2003 г.) — сетевой червь, распространявшийся по электронной почте. Размножавшийся с огромной скоростью вирус скачивал на зараженный компьютер дополнительные файлы, «сжигая» трафик и ресурсы системы. Интересная особенность — 10 сентября вирус прекращал свою деятельность, больше не представляя угрозы для пользователя. Автор Sobig.F, за информацию о котором Microsoft предлагала 250 тыс. долл., не найден до сих пор.

Bagle (2004 г.) — сетевой червь, распространявшийся по классическому способу, используя файловые вложения в электронных письмах. На зараженном компьютере устанавливалась специальная «лазейка», через которую злоумышленник получал полный доступ к системе. Вирус имеет более ста модификаций.

MyDoom — в январе 2004 г. этот вирус быстро распространился по всему Интернету, в результате чего средняя скорость загрузки сайтов в глобальной сети уменьшилась на 50 %. Червю принадлежит рекорд по скорости распространения: менее чем за сутки было заражено около 2 млн компьютеров. Точную цифру из-за масштабов эпидемии привести невозможно. Вирус был создан неизвестным программистом в качестве эксперимента и самостоятельно прекратил свою деятельность 12 февраля того же года.

Sasser (2004 г.) — вирус вызвал «перерыв» в работе французских спутниковых каналов передачи данных, отменил рейсы некоторых авиакомпаний, не говоря уже об обычных компьютерах, чья работа была полностью приостановлена. Распространялся Sasser благодаря ошибке в системе безопасности Windows 2000 и XP, запуская на зараженном компьютере сканер портов. Вирус был написан 17-летним немецким школьником. Интересен тот факт, что парень запустил вирус в сеть в День своего совершеннолетия.

WannaCry (в переводе означает «хочется плакать») — вредоносная программа, сетевой червь и программа-вымогатель денежных средств, поражающая компьютеры под управлением операционной системы Microsoft Windows. После заражения компьютера программный код червя шифрует почти все хранящиеся на компьютере файлы и предлагает заплатить денежный выкуп в криптовалюте за их расшифровку. В случае неуплаты выкупа в течение 7 дней с момента заражения возможность расшифровки файлов теряется навсегда. Массовое распространение WannaCry началось 12 мая 2017 г., одними из первых были атакованы компьютеры в Испании, а затем и в других странах. Среди них по количеству заражений лидируют Россия, Украина и Индия. В общей сложности за короткое время от червя пострадало 500 тыс. компьютеров, принадлежащих частным лицам, коммерческим организациям и правительственным учреждениям, в более чем 200 странах мира. Распространение червя блокиро-

вало работу множества организаций по всему миру: больниц, аэропортов, банков, заводов и др. В частности, в ряде британских госпиталей было отложено выполнение назначенных медицинских процедур, обследований и срочных операций.

Вопросы для самоконтроля

1. Компьютерные вирусы и проблемы антивирусной защиты.
2. Условия существования вредоносных программ.
3. Жизненный цикл вирусов.
4. Основные каналы распространения вирусов и других вредоносных программ.
5. Признаки заражения компьютера.
6. Построение системы антивирусной защиты корпоративной сети.
7. Профилактика заражения вирусами компьютерных систем.
8. Что такое эвристический алгоритм поиска вирусов.
9. Что такое сигнатурный поиск вирусов.
10. Дайте краткую характеристику угрозы безопасности, обозначаемую термином «вирус».
11. Дайте краткую характеристику угрозы безопасности, обозначаемую термином «сетевой червь».
12. Дайте краткую характеристику угрозы безопасности, обозначаемую термином «троянский конь».
13. Укажите существенные отличия компьютерных вирусов от сетевых червей.

7. ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

7.1. Концепция инженерно-технической защиты информации

Инженерно-техническая защита информации включает комплекс организационных и технических мер по обеспечению информационной безопасности техническими средствами и решает следующие задачи:

– предотвращение проникновения злоумышленника к источникам информации с целью ее уничтожения, хищения или изменения;

– защита носителей информации от уничтожения в результате воздействия стихийных сил;

– предотвращение утечки информации по различным техническим каналам.

Для обеспечения эффективности ИТЗИ необходимо определить:

– перечень объектов, защищаемых техническими средствами в данной организации, здании, помещении;

– виды информационных угроз, которым подвергаются защищаемые информационные ресурсы со стороны злоумышленников;

– различные способы и средства, применяемые в ИБ, учитывающие как методы реализации угроз, так и затраты на их предотвращение;

– структуру организации ТЗ на некоторых объектах.

По содержанию любая информация может быть отнесена к семантической (в переводе с латинского — содержащей смысл) или к информации о признаках материального объекта — признаковой (рис. 7.1).

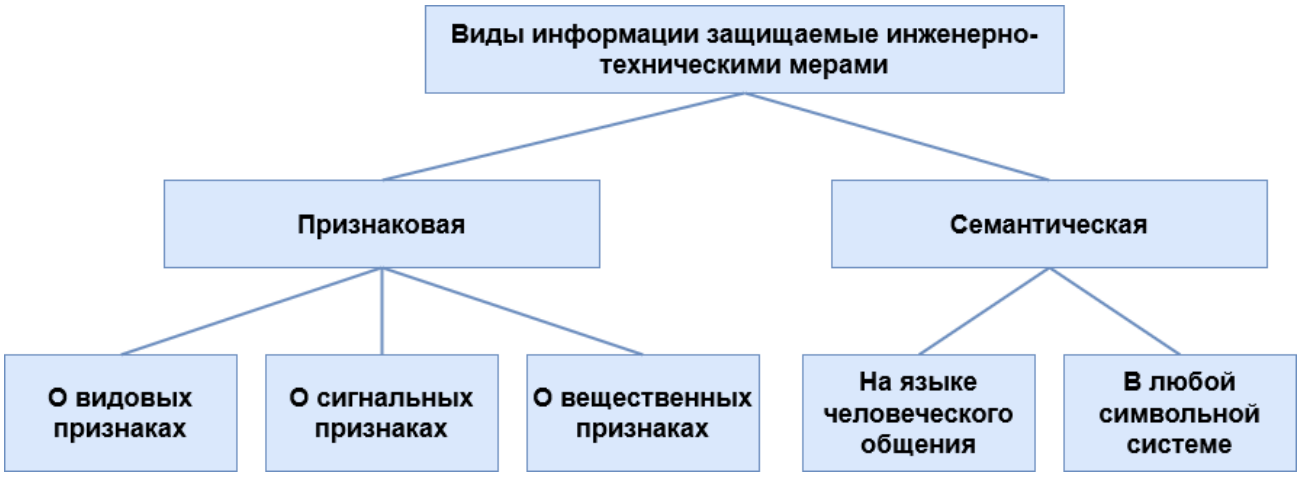


Рис. 7.1. Виды информации защищаемой техническими средствами

Признаковая информация — любая информация содержится на материальных носителях в виде значений их признаков, т.е. она отображается на носителях информации на языке признаков. Язык признаков является универсальным языком представления информации в материальном мире. Признаковая информация является первичной и описывает конкретный материальный объект на языке его признаков.

Семантическая информация — продукт абстрактного мышления человека и отображает объекты, явления как материального мира, так и создаваемые им образы и модели с помощью символов на языках общения людей. Семантическая информация по отношению к признаковой является вторичной. Если признак привязан к конкретному объекту, то символьная (семантическая) информация абстрактна. Сущность семантической информации не зависит от характеристик носителя. Содержание текста, например, не зависит от качества бумаги, на которой он написан, или физических параметров другого носителя.

Меры инженерно-технической защиты информации могут классифицироваться по различным параметрам (рис. 7.2).

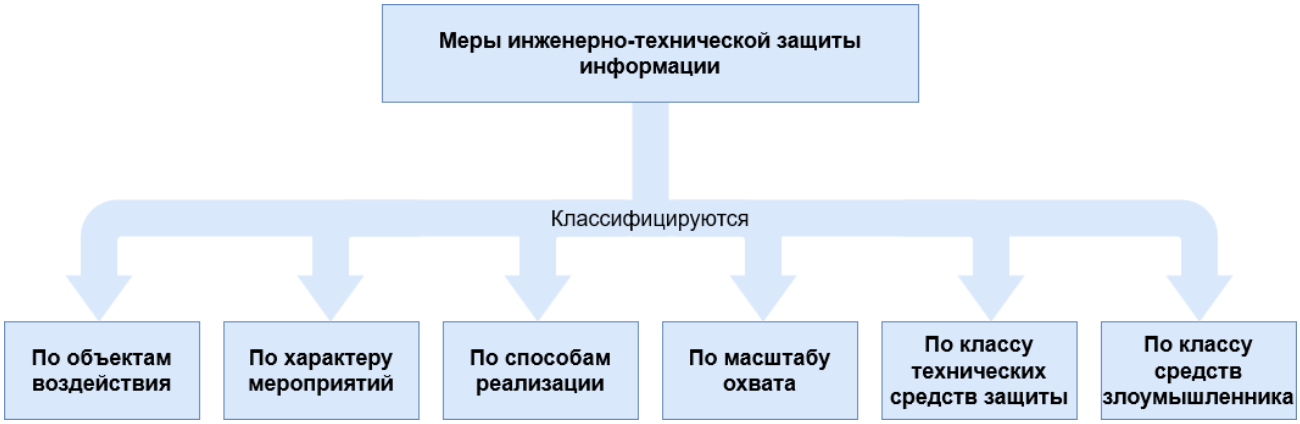


Рис. 7.2. Классификация инженерно-технических мер защиты информации

Концепция инженерно-технической защиты информации состоит в следующем: объектами защиты являются материальные носители информации. Методы защиты предполагают использование материальных средств. По виду реализации угрозы делятся на две группы:

– физическое воздействие внешних сил на источники информации, в результате которого возможны ее изменение, уничтожение, хищение и блокирование (угрозы воздействия на источник информации);

– несанкционированное распространение носителя с защищаемой информацией от ее источника до злоумышленника, которое приводит к хищению информации (угрозы утечки информации).

7.2. Угрозы, нейтрализуемые инженерно-техническими методами

Угрозы воздействия на информацию представляют собой силы различной физической природы (механической, электрической, электромагнитной, тепловой и др.), система защиты должна создавать вокруг носителей информации с локальными размерами преграды — рубежи защиты от этих сил. Задача решается подсистемой физической защиты источников информации.

Несанкционированное распространение носителя с информацией от ее источника к злоумышленнику называется утечкой информации. Она может возникнуть в результате:

– утери источника информации (документа, продукции и др.);
– разглашения сведений;
– подслушивания;
– наблюдения;
– перехвата электромагнитных полей и электрических сигналов, содержащих защищаемую информацию;
– сбора отходов дело- и промышленного производства.

В основе утечки лежит неконтролируемый перенос конфиденциальной информации посредством акустических, световых, электромагнитных, радиационных и других полей и материальных объектов. По физической природе возможны следующие средства переноса информации:

– световые лучи;
– звуковые волны;
– электромагнитные волны;
– материалы и вещества.

Физический путь несанкционированного распространения носителя с защищаемой информацией от ее источника к злоумышленнику образует канал утечки информации. Классификация технических каналов утечки информации представлена на рис. 7.3.

Рис. 7.3. Классификация технических каналов утечки информации

С учетом физической природы образования каналы утечки информации можно разделить на следующие группы:

– визуально-оптические;

– акустические (включая и акустико-преобразовательные);
– электромагнитные (включая магнитные и электрические);
– материально-вещественные.

Визуально-оптические каналы — это, как правило, непосредственное или удаленное (в том числе и телевизионное) наблюдение. Переносчиком информации выступает свет, испускаемый источником конфиденциальной информации или отраженный от него в видимом, инфракрасном и ультрафиолетовом диапазонах (рис. 7.4).

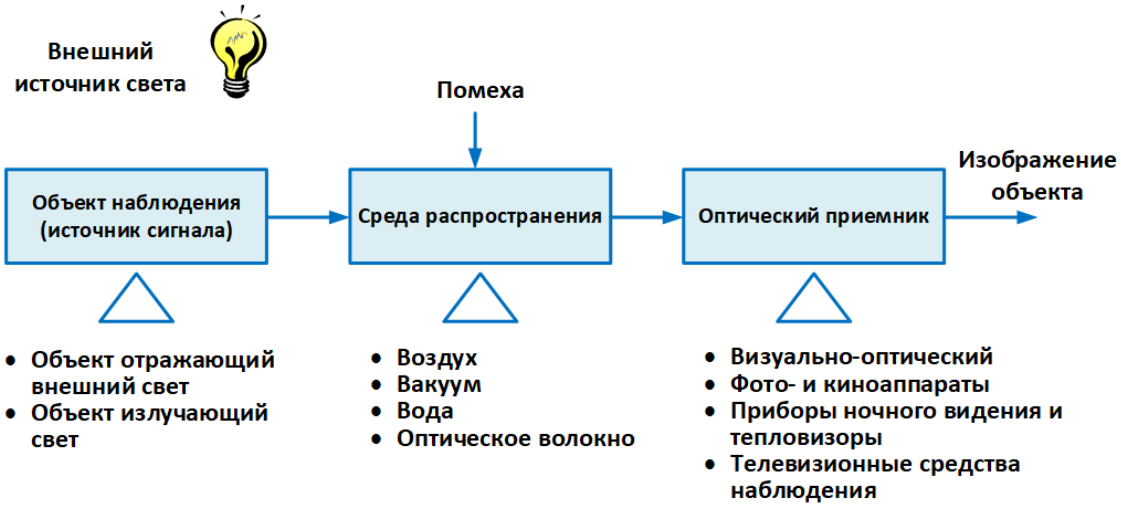


Рис. 7.4. Визуально-оптический канал утечки информации

Акустические каналы. Для человека слух является вторым по информативности после зрения. Поэтому одним из довольно распространенных каналов утечки информации является акустический канал. В акустическом канале переносчиком информации выступает звук (рис. 7.5).

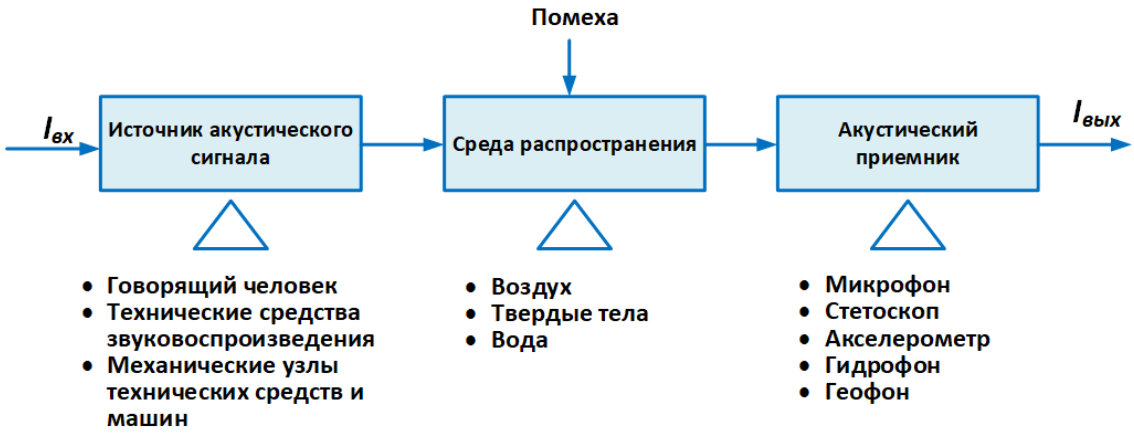


Рис. 7.5. Акустический канал утечки информации

Примеры реализации визуально-оптического и акустического каналов утечки информации представлены на рис. 7.6–7.8.

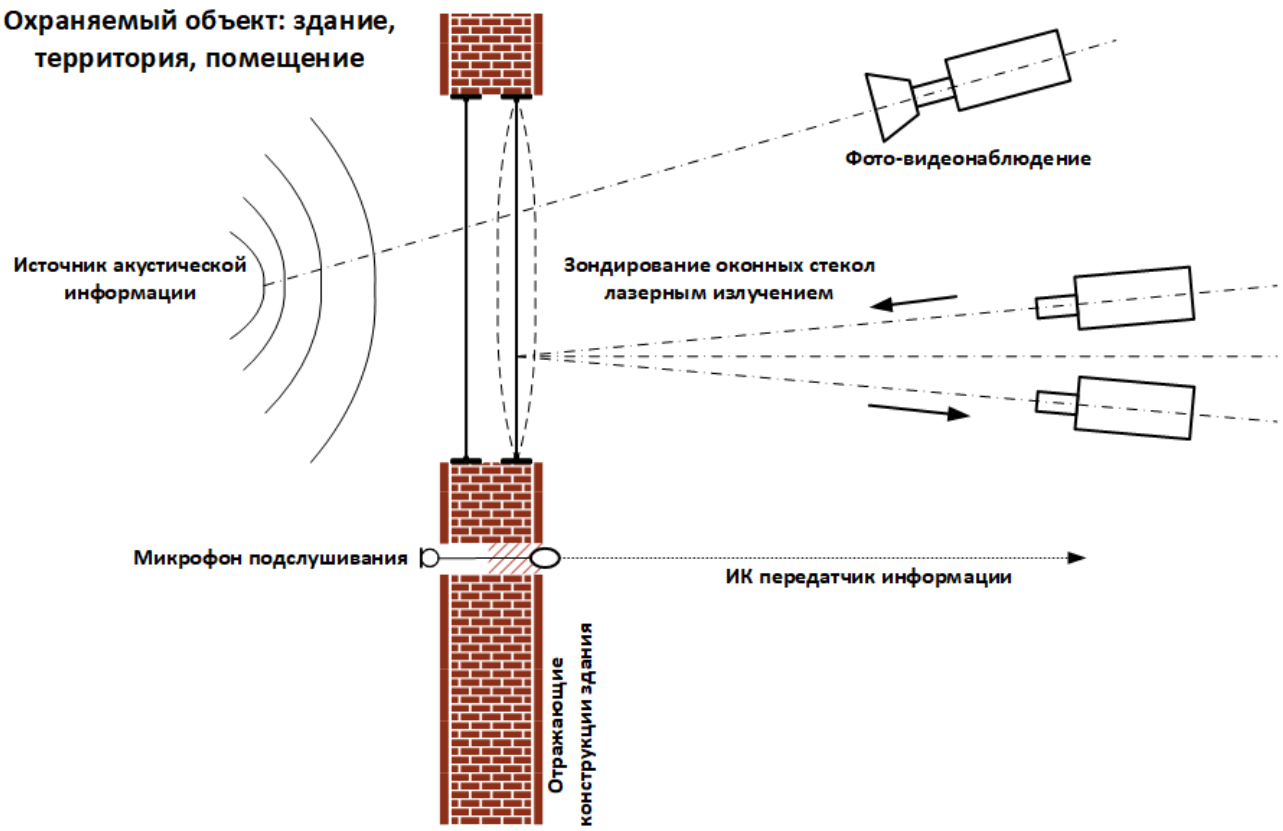


Рис. 7.6. Визуально-оптический и акустический канал утечки информации

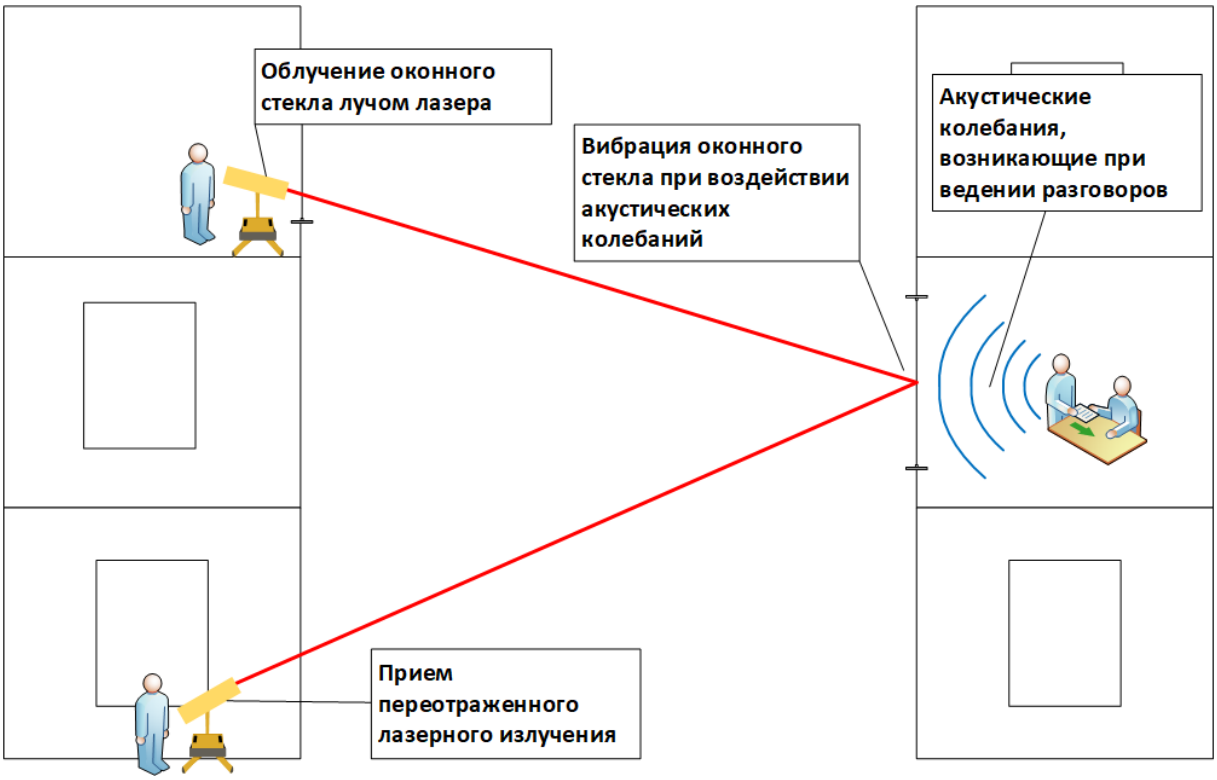


Рис. 7.7. Акустический канал утечки информации

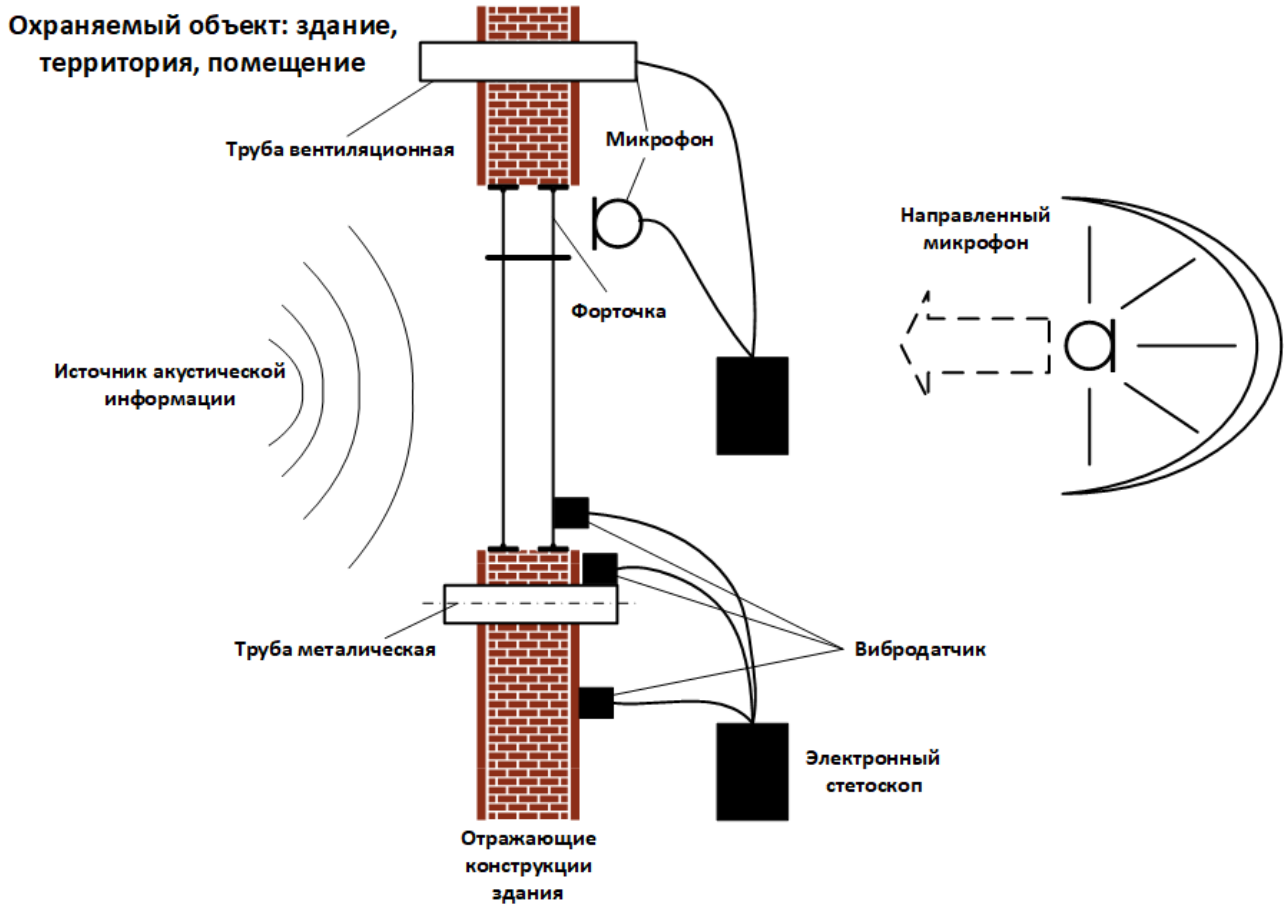


Рис. 7.8. Акустические каналы утечки информации

Электромагнитные каналы. Переносчиком информации являются электромагнитные волны в диапазоне от сверхдлинных с длиной волны 10 000 м (частоты менее 30 Гц) до субмиллиметровых с длинной волны 1–0,1 мм (частоты от 300 до 3 000 ГГц) (рис. 7.9).

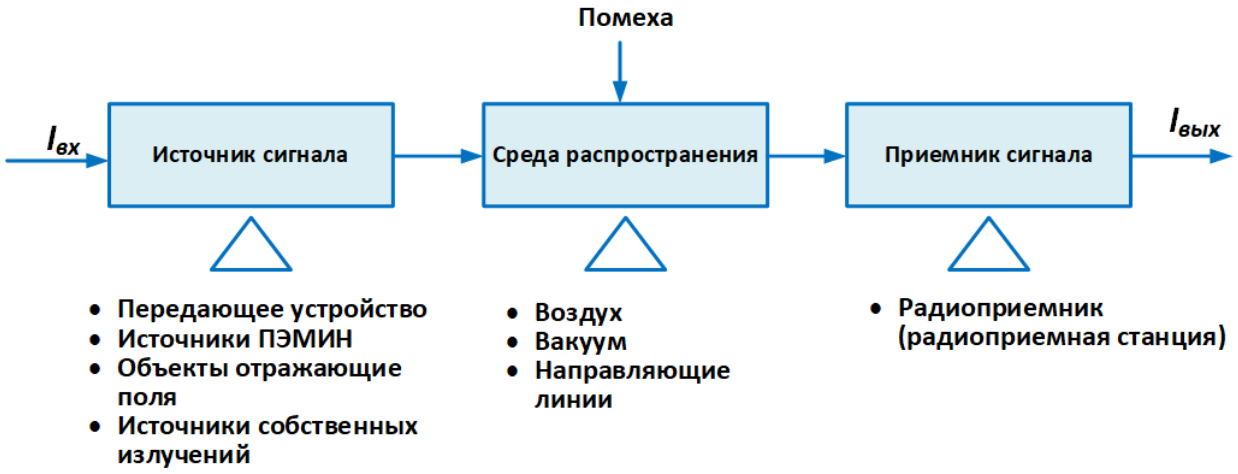


Рис. 7.9. Электромагнитный канал утечки информации

Примеры реализации электромагнитных каналов утечки информации представлены на рис. 7.10–7.14.

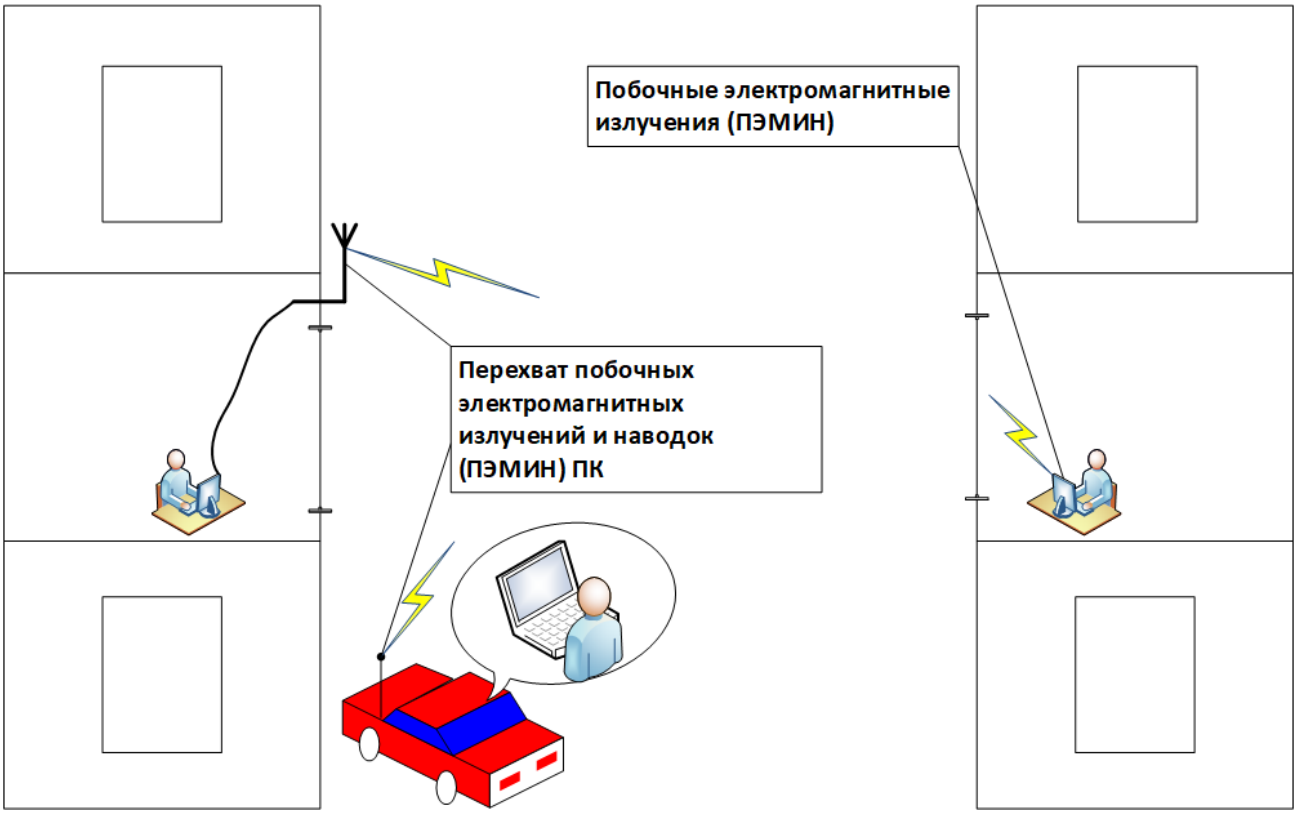


Рис. 7.10. Канал, образованный за счет перехвата побочных электромагнитных излучений и наводок

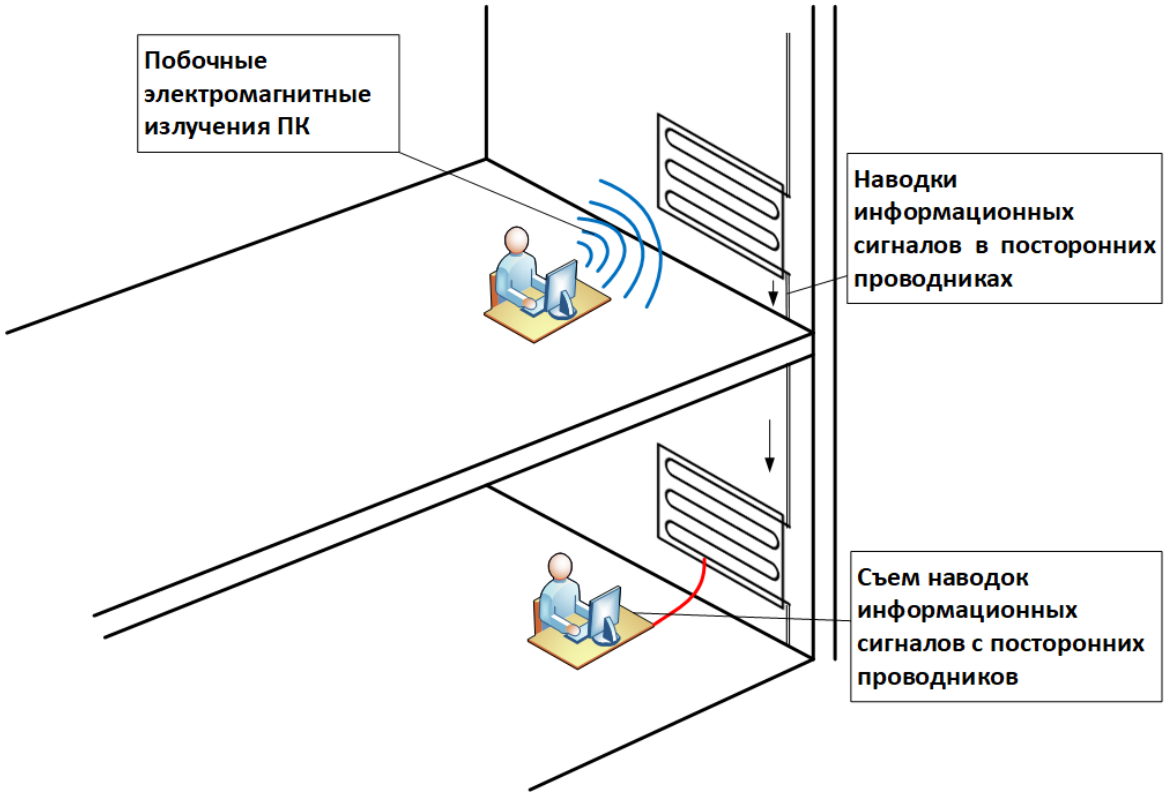


Рис. 7.11. Канал, образованный за счет наводок информационных сигналов в посторонних проводниках

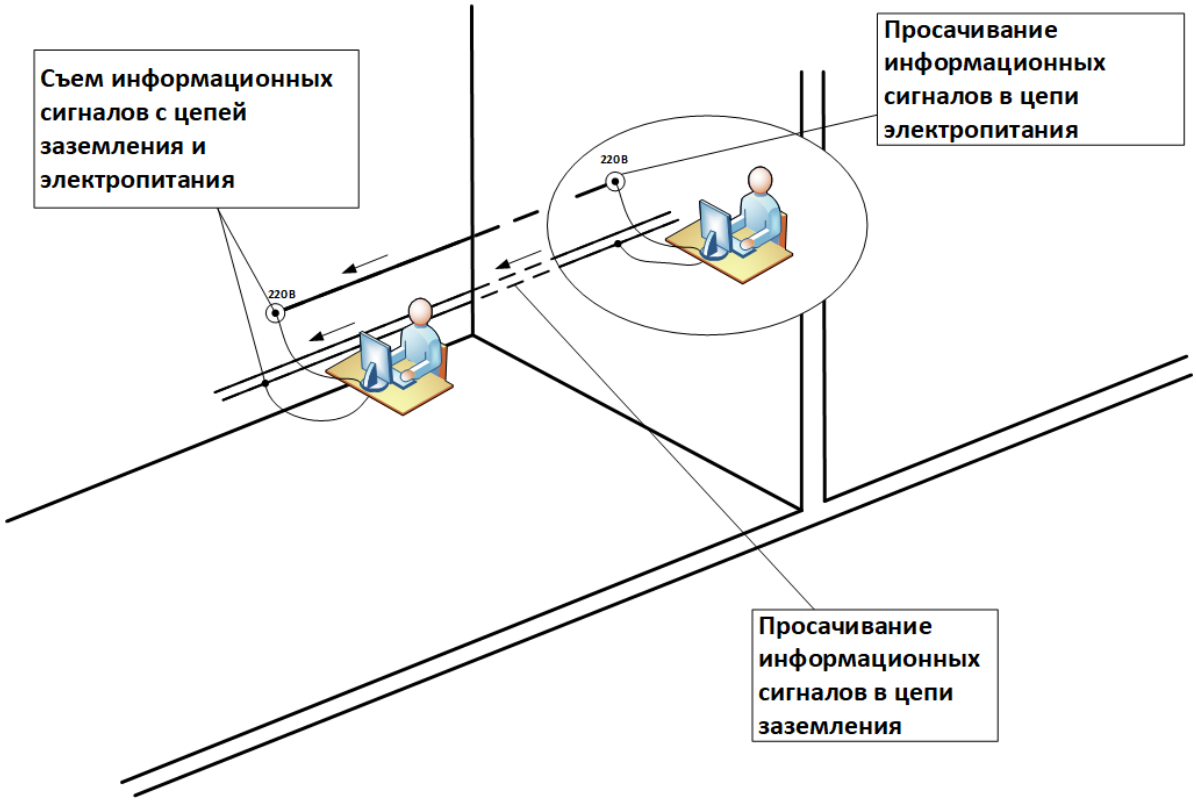


Рис. 7.12. Канал, образованный за счет просачивания информационных сигналов в цепи заземления и электропитания

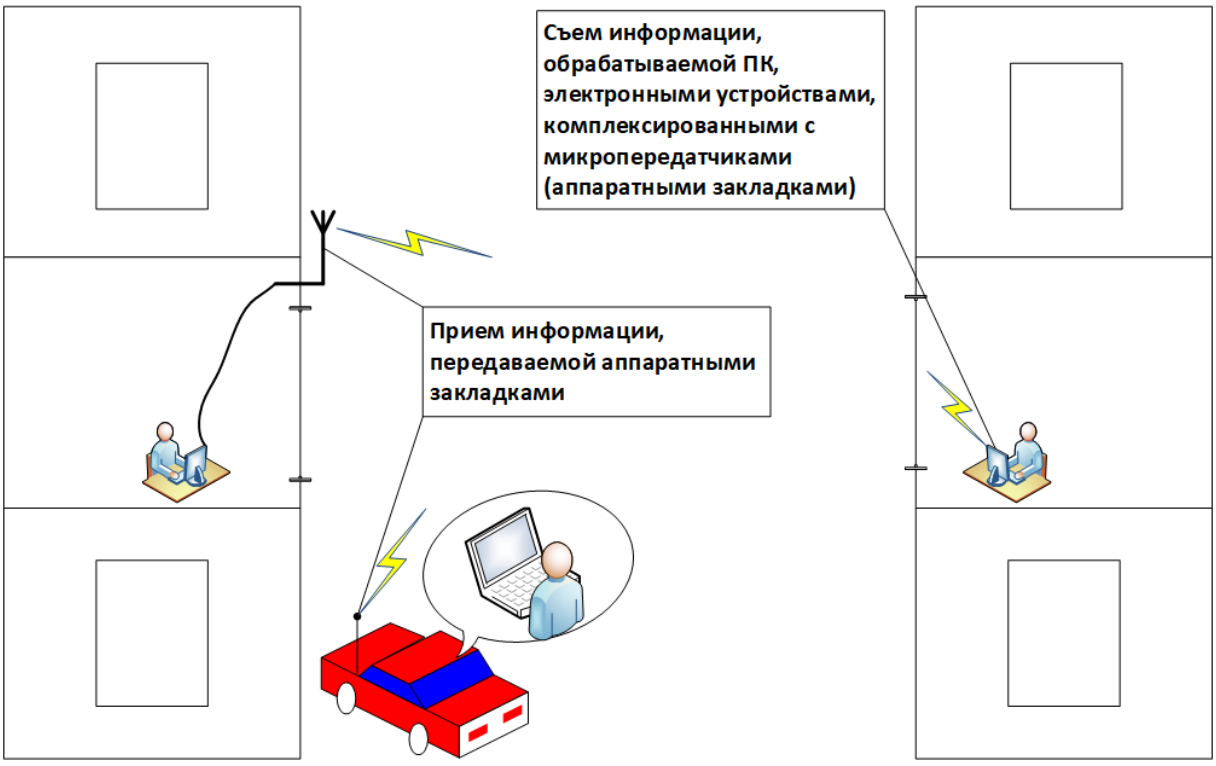


Рис. 7.13. Канал, образованный за внедрения радиозакладок

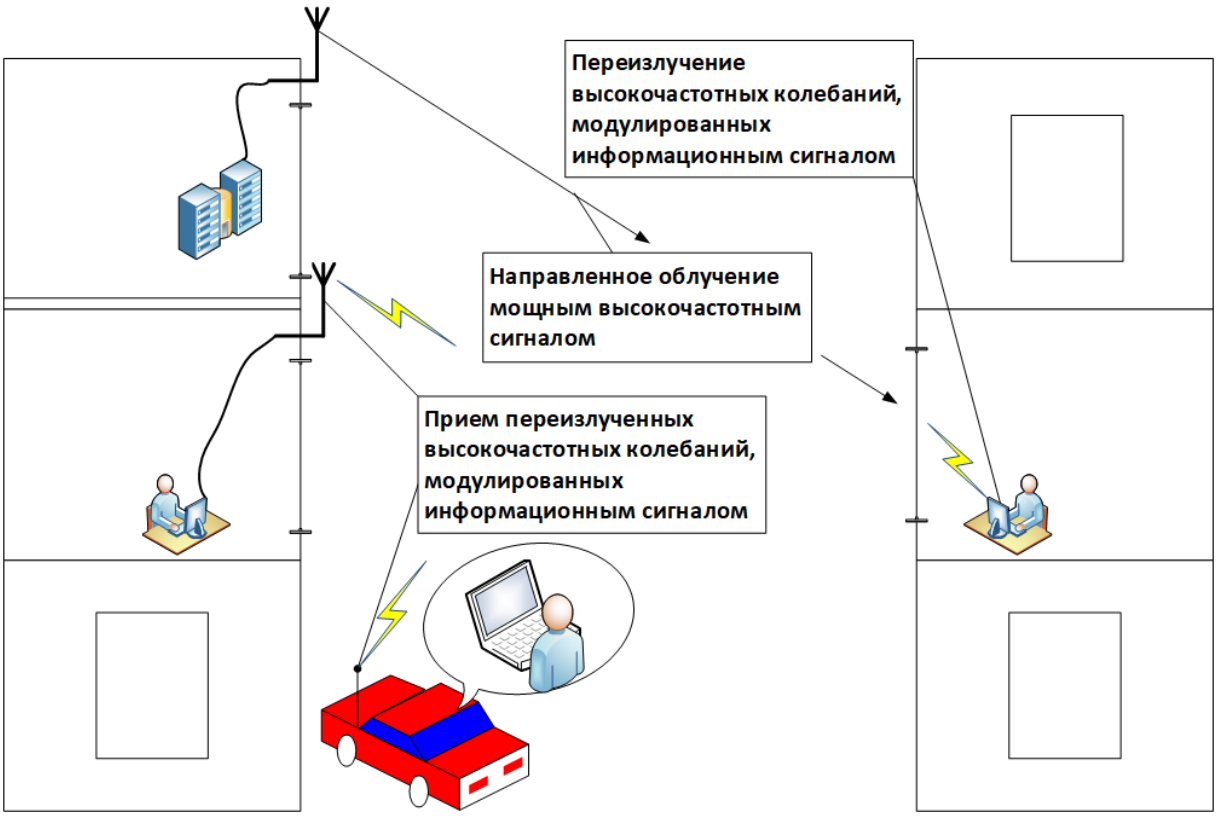


Рис. 7.14. Канал, образованный за счет высокочастотного навязывания

Материально-вещественными каналами утечки информации выступают самые различные материалы в твердом, жидком и газообразном или корпускулярном (радиоактивные элементы) виде. Очень часто это различные отходы производства, бракованные изделия, черновые материалы и др. (рис. 7.15).

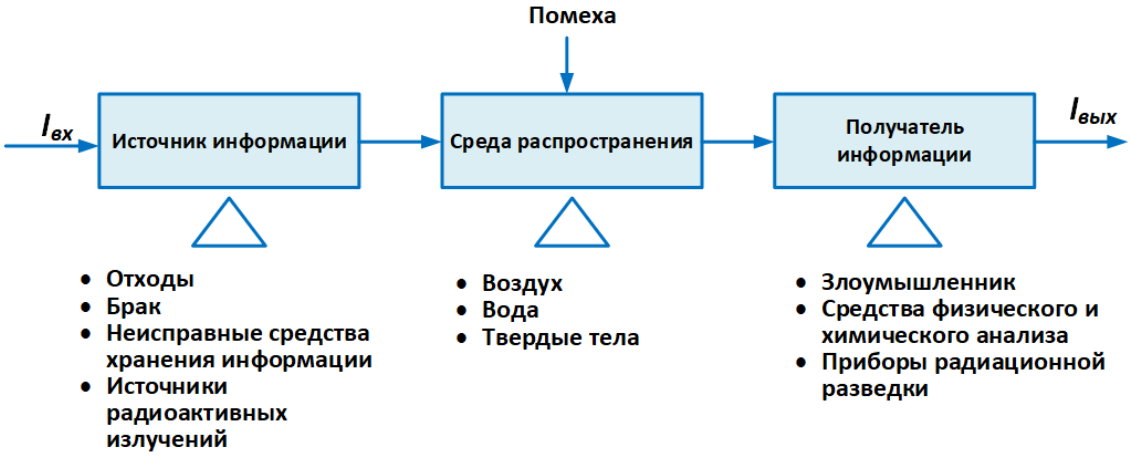


Рис. 7.15. Материально-вещественный канал утечки информации

На рис. 7.16 и 7.17 показаны различные сценарии образования технических каналов утечки информации.

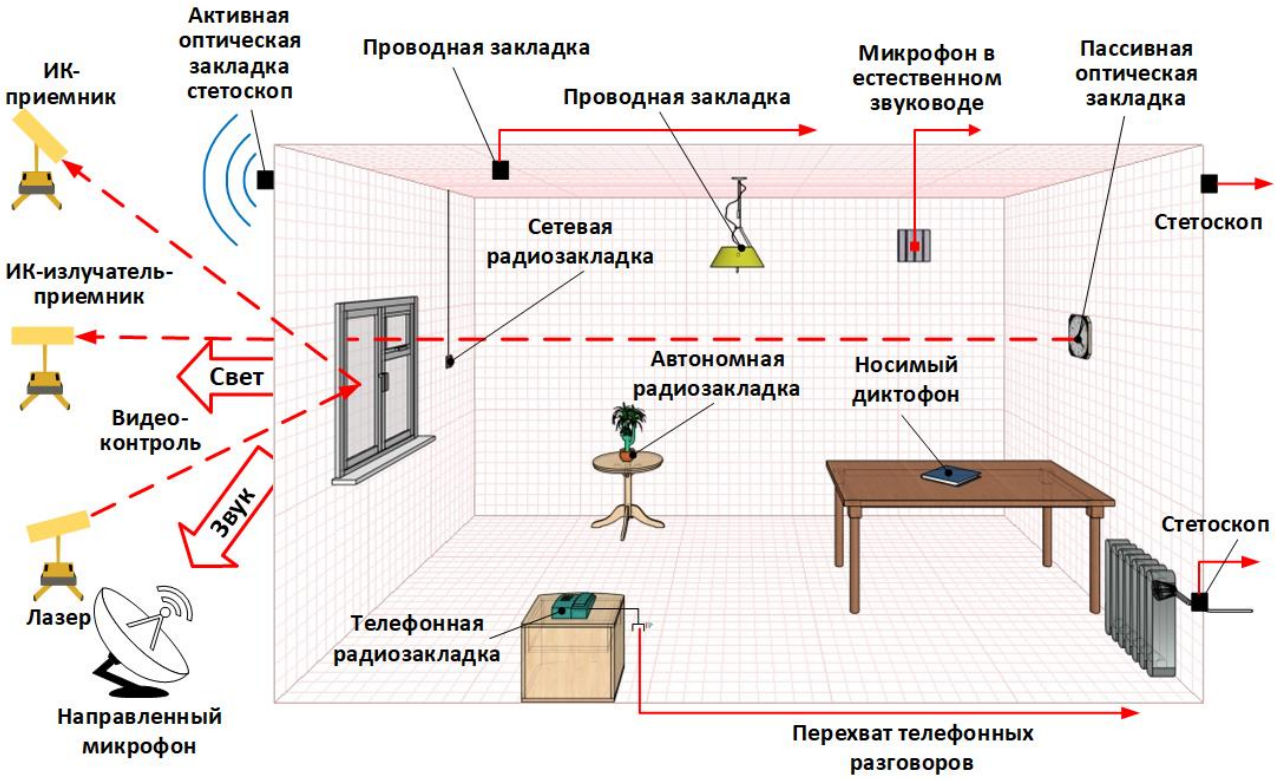


Рис. 7.16. Сценарии утечки речевой информации

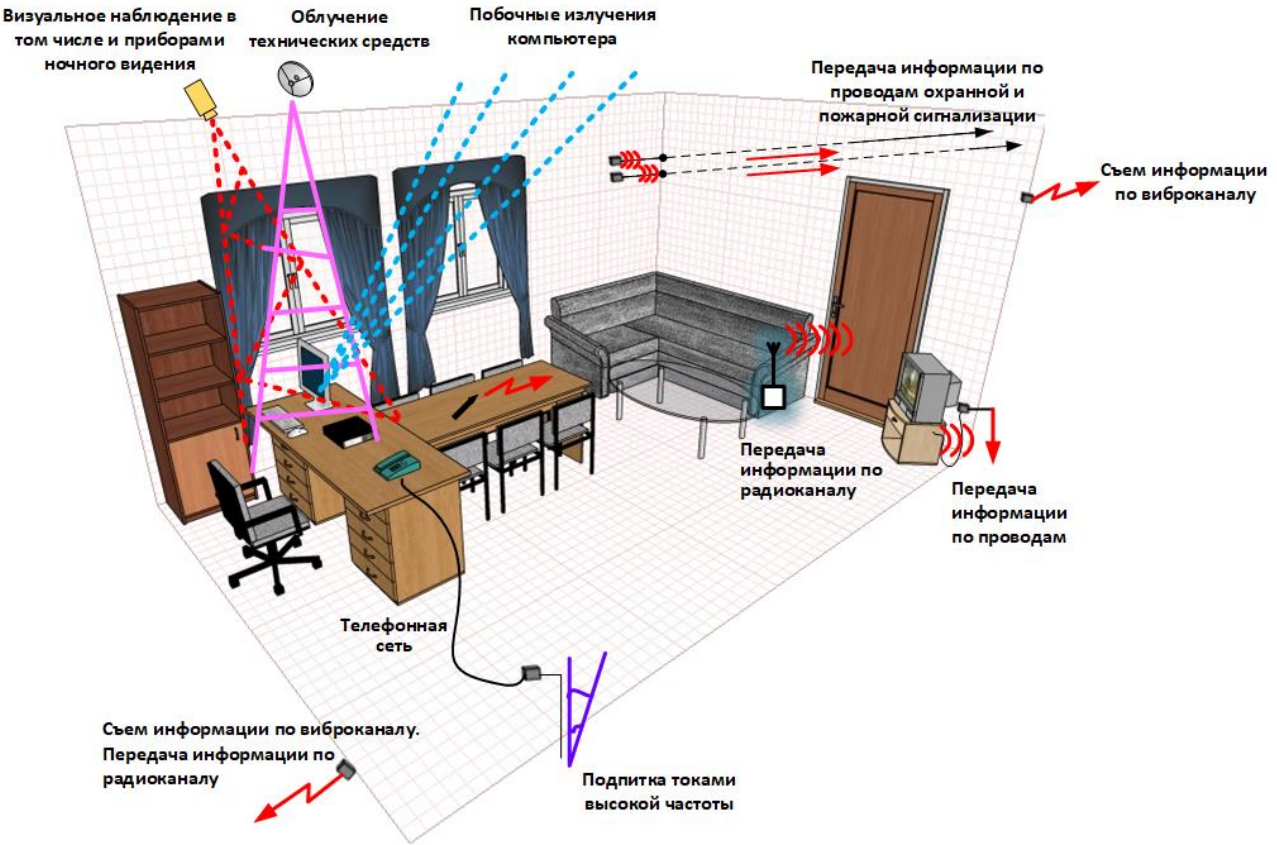


Рис. 7.17. Технические каналы утечки информации

7.3. Система инженерно-технической защиты информации

В состав системы инженерно-технической защиты информации входят подсистема физической защиты и подсистема защиты информации от утечки.

Подсистема физической защиты создается для противодействия преднамеренным угрозам воздействия на источники информации злоумышленника и стихийных сил. Средства этой подсистемы реализуют методы физической защиты с помощью инженерных конструкций и технических средств охраны.

Физические средства защиты информации — это разнообразные устройства, приспособления, конструкции, предназначенные для создания препятствий на пути движения злоумышленников. К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов, других возможных видов преступных действий. Методы физической защиты источников информации должны обеспечивать:

– задержку злоумышленника или иного источника угрозы на время, большее времени нейтрализации угрозы;

– обнаружение злоумышленника или источника иной угрозы;

– нейтрализацию угроз воздействия на источник информации.

Все физические средства защиты объектов можно разделить на три категории:

– средства обнаружения — охранная сигнализация и охранное телевидение т.д.;

– средства предупреждения — заборы вокруг объектов, усиленные двери, стены, потолки, решетки на окнах и другие меры;

– системы ликвидации угроз — средства пожаротушения и т.д.

Структура подсистемы физической защиты представлена на рис. 7.18.

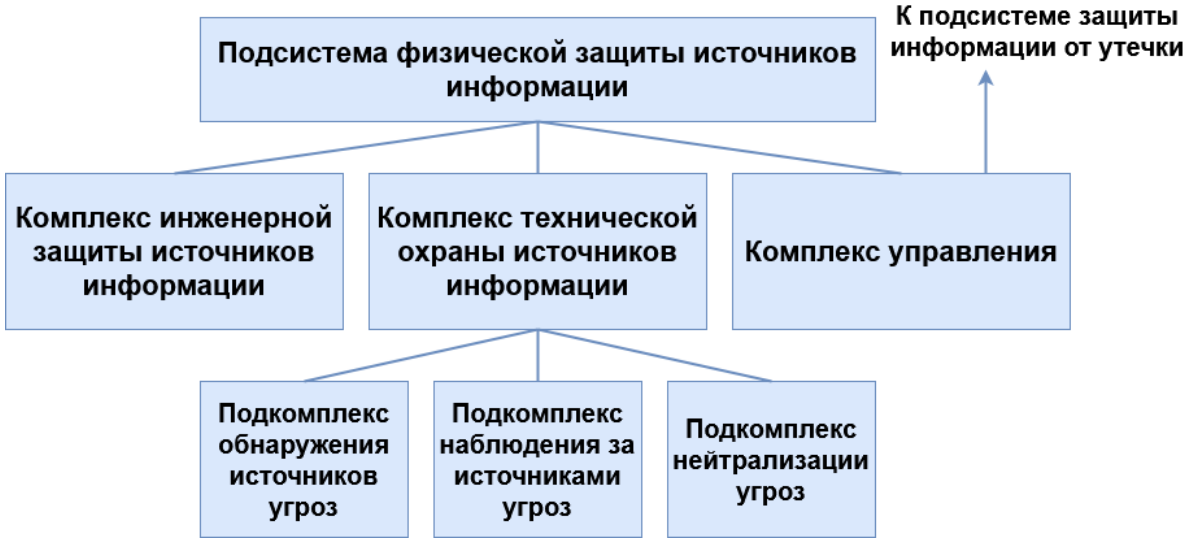


Рис. 7.18. Структура подсистемы физической защиты

Комплекс инженерной защиты предназначен для механического воспрепятствования проникновению злоумышленника к объектам защиты. Он включает инженерные конструкции, создающие механические преграды на пути злоумышленника, и комплексы управления доступом людей и автотранспорта на охраняемую территорию. Комплекс технической охраны имеет в своем составе:

– подкомплекс обнаружения источников угроз:
- извещатели;
- шлейфы;
- контрольно-приемные приборы;
- средства передачи извещения на пост охраны;

– подкомплекс наблюдения за источниками угроз:
- камеры видеонаблюдения;
- мониторы;
- средства преобразования видеосигнала;
- видеорегистраторы;
- дежурное освещение;

– подкомплекс нейтрализации угроз:
- охрана;
- тревожная сигнализация;
- средства пожаротушения.

Подсистема инженерно-технической защиты информации от утечки предназначена для снижения до допустимых значений величины риска (вероятности) несанкционированного распространения информации от ее источника, расположенного внутри контролируемой зоны, к злоумышленнику. Для достижения этой цели система должна иметь механизмы (силы и средства) обнаружения и нейтрализации угроз подслушивания, наблюдения, перехвата и утечки информации по вещественному каналу. Структура подсистемы инженерно-технической защиты информации от утечки представлена на рис. 7.19.

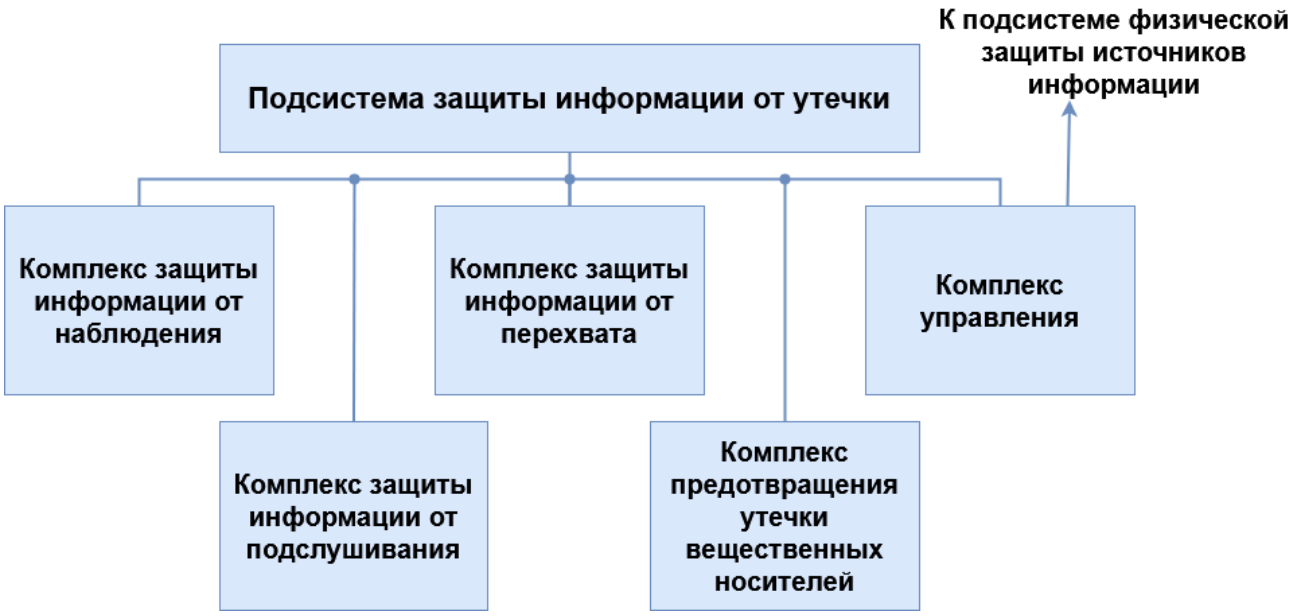


Рис. 7.19. Структура подсистемы защиты информации от утечки

Комплекс защиты информации от утечки по визуально-оптическим каналам предполагает реализацию следующих мероприятий:

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

– уменьшить отражательные свойства объекта защиты;

– уменьшить освещенность объекта защиты (энергетические ограничения);

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

– применять средства маскирования, имитации и другие с целью защиты и введения в заблуждение злоумышленника;

– использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражательного или излученного света и других излучений;

– осуществлять маскировку объектов защиты, варьируя отражательными свойствами и контрастом фона.

Защита информации от утечки по акустическим каналам включает реализацию следующих мер:

– использование специальных вставок и прокладок для вибрационной развязки;

– применение специальных фильтров низкой частоты и ограничителей в соединительных линиях;

– применение специальных фильтров низкой частоты в линиях электропитания;

– создание вибрационных помех.

Структура применяемых мер представлена на рис. 7.20.

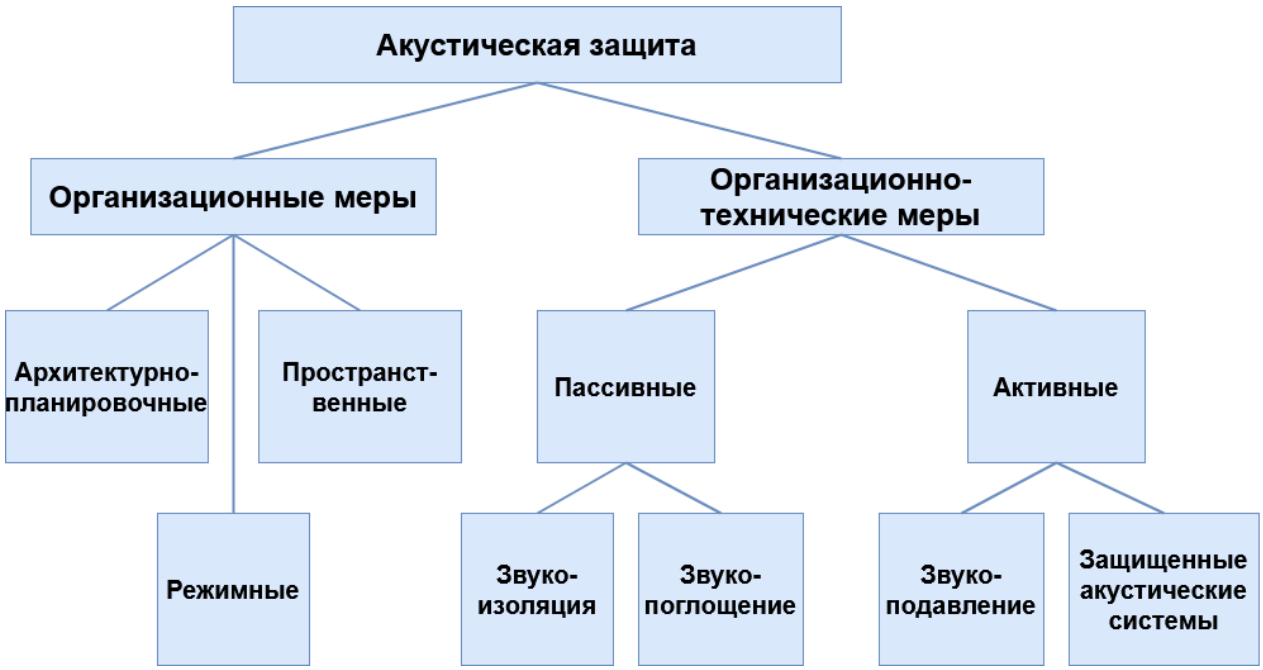


Рис. 7.20. Защита информации от утечки по акустическим каналам

Применение данных мер проиллюстрировано на рис. 7.21–7.25.

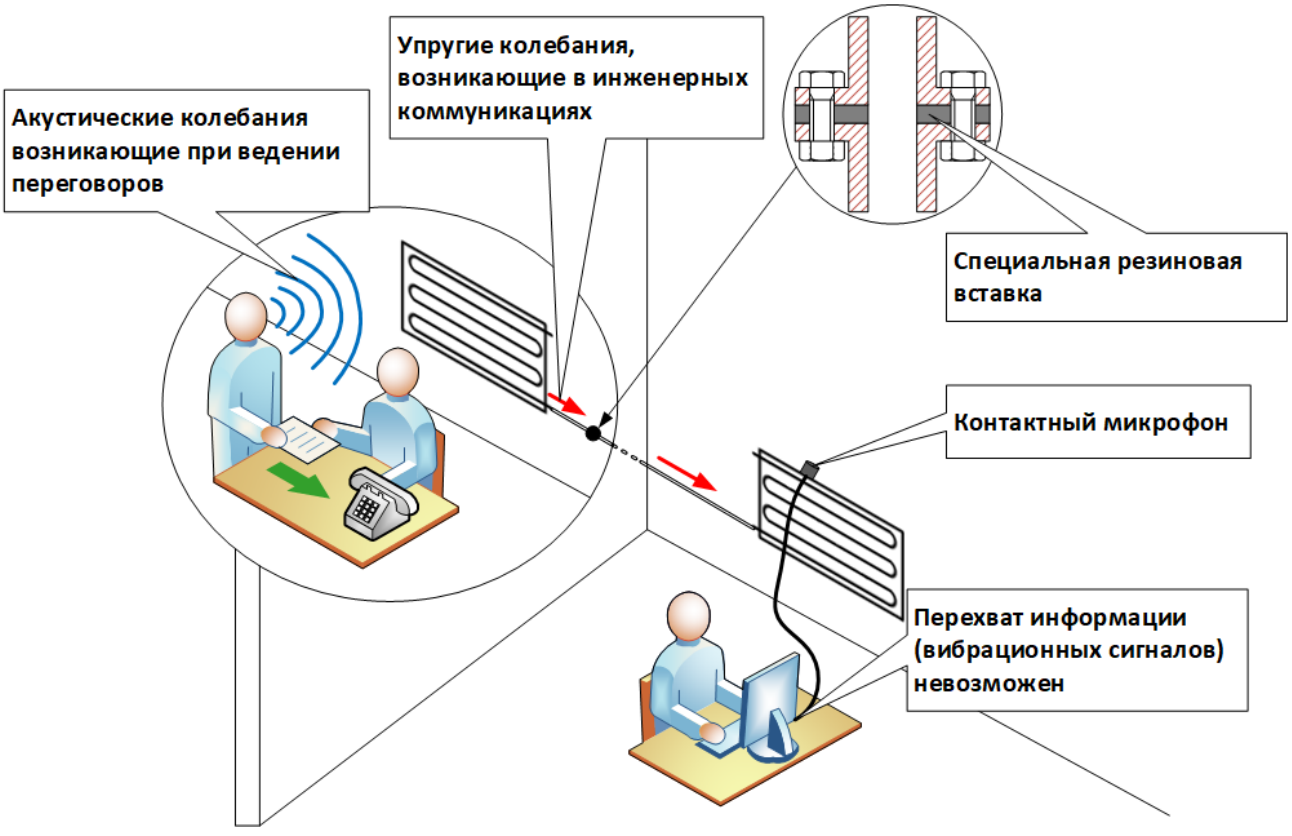


Рис. 7.21. Специальные вставки и прокладки для вибрационной развязки

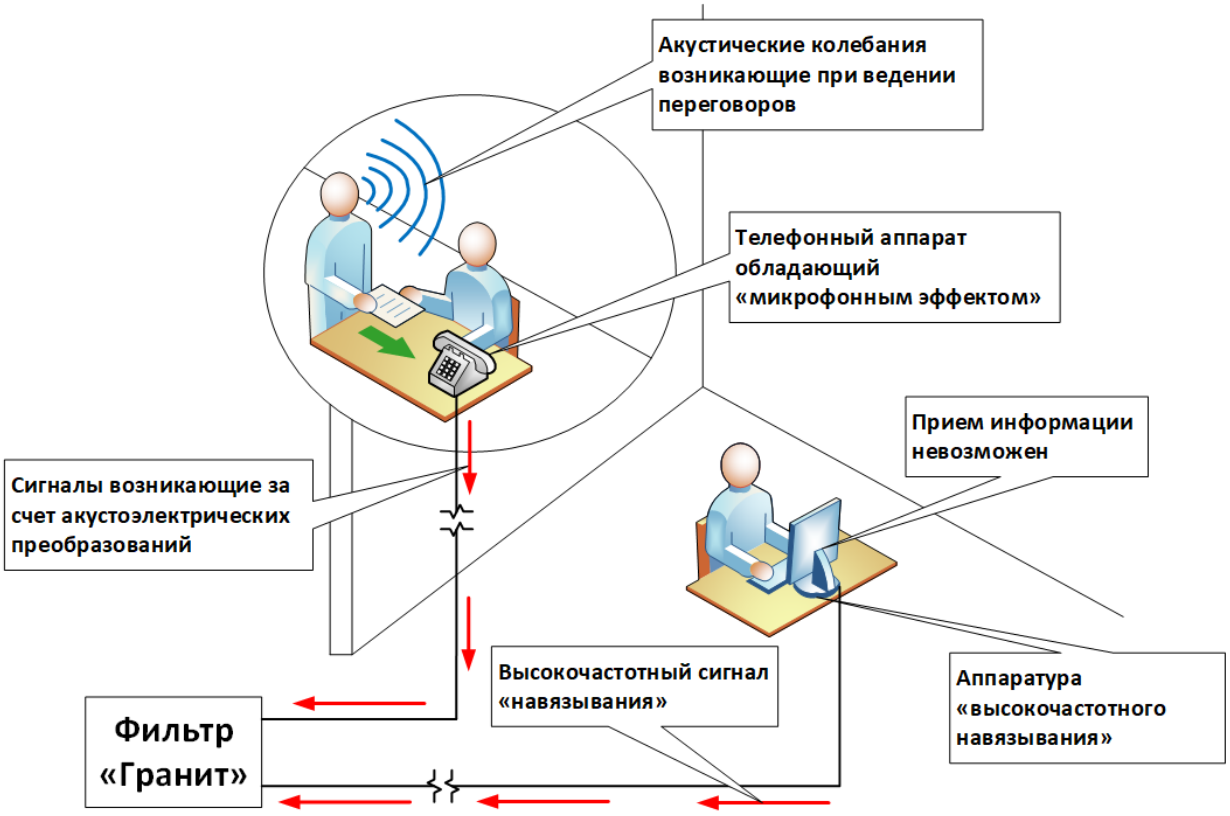


Рис. 7.22. Специальные фильтры низкой частоты и ограничители в соединительных линиях

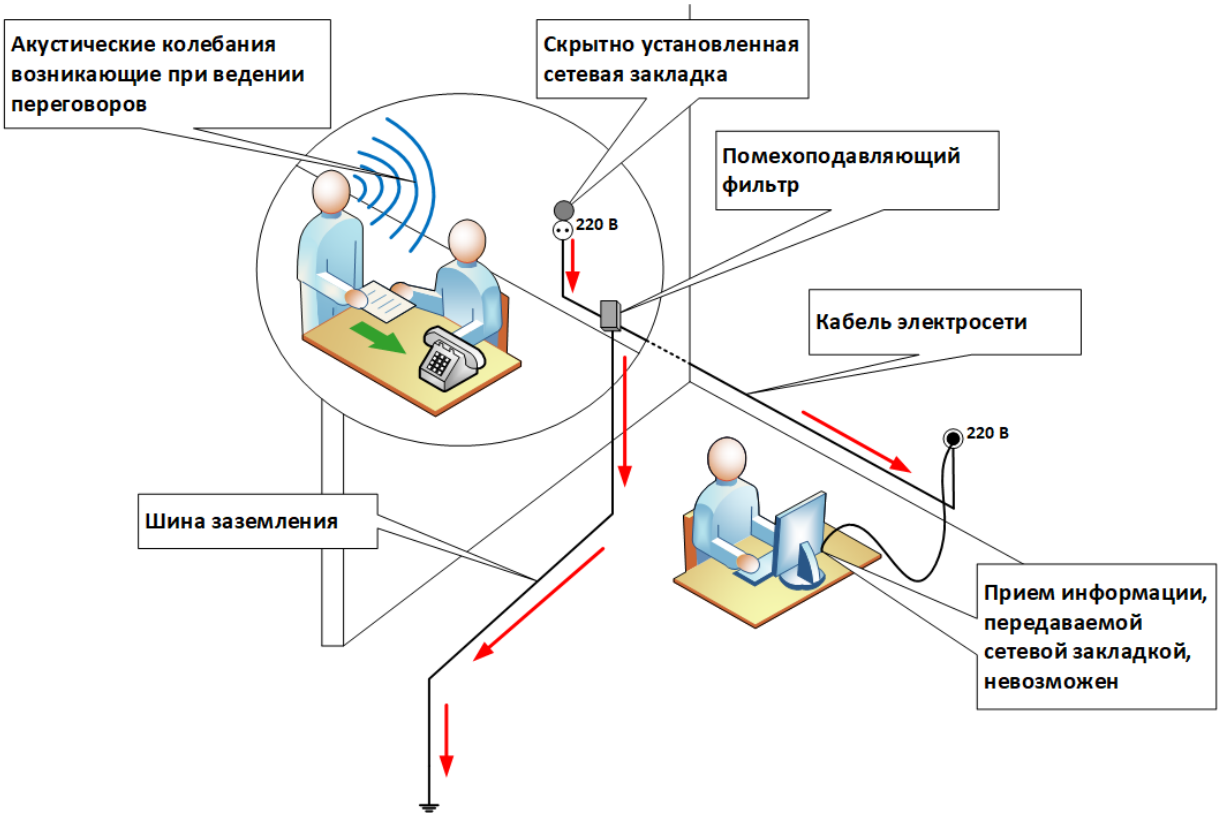


Рис. 7.23. Специальные фильтры низкой частоты в линиях электропитания

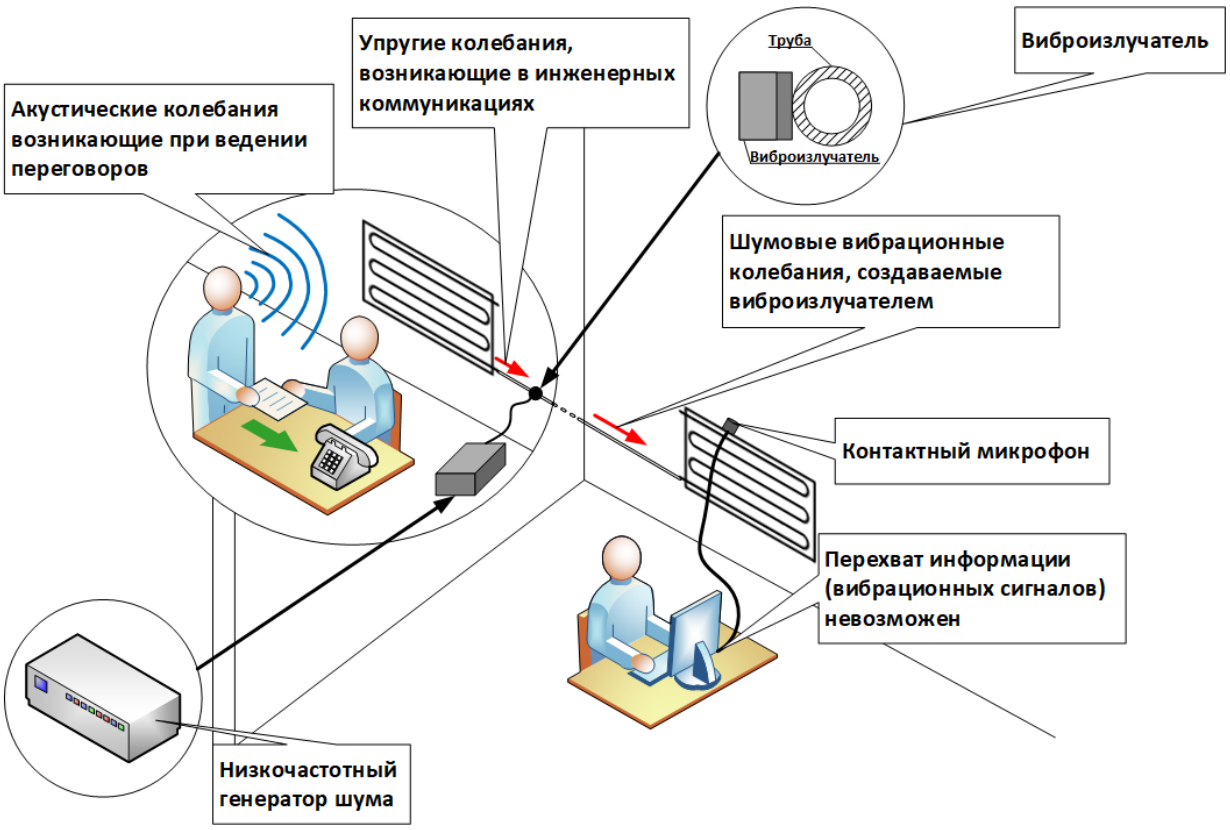


Рис. 7.24. Создание вибрационных помех в инженерных коммуникациях

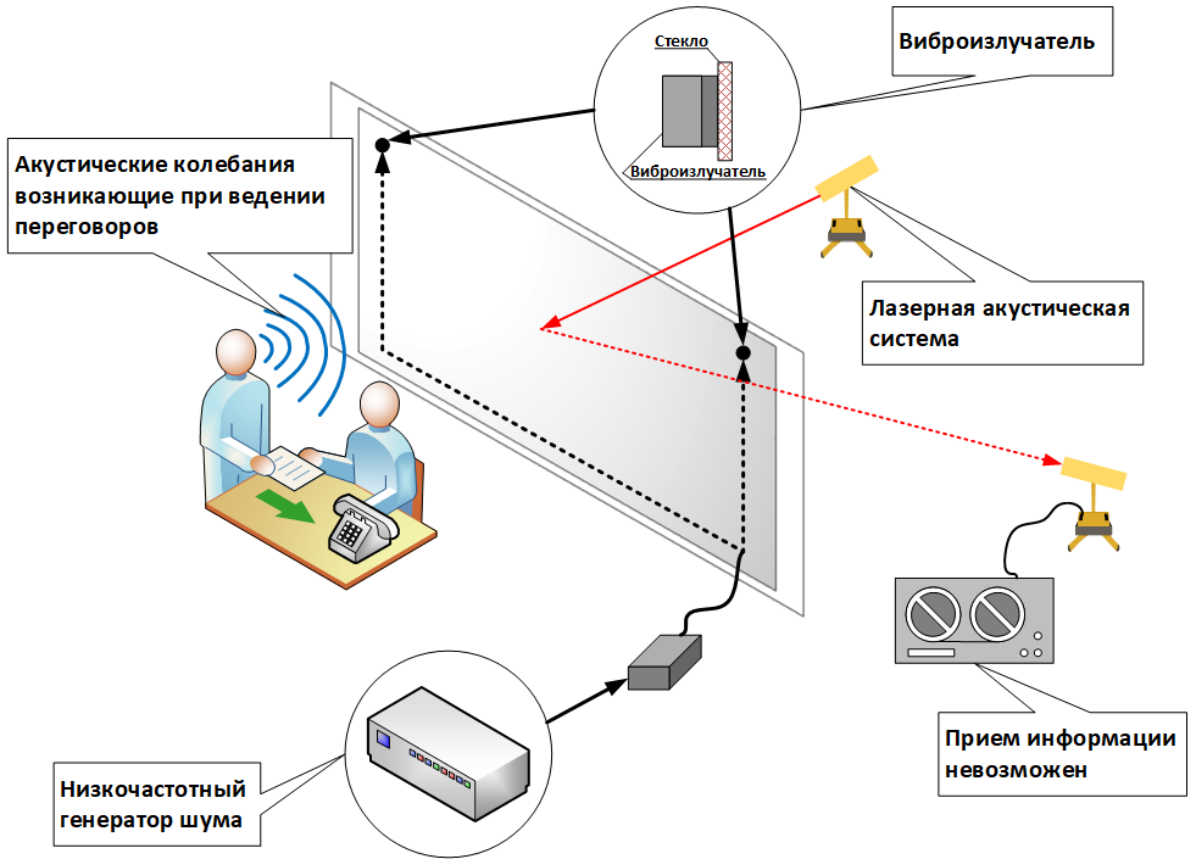


Рис. 7.25. Создание вибрационных помех в оконных стеклах

Защита информации от утечки по электромагнитным каналам предполагает реализацию мер, обеспечивающих:

– защиту от утечки за счет микрофонного эффекта;
– защиту от утечки за счет электромагнитного излучения;
– защиту от утечки за счет паразитной генерации;
– защиту от утечки по цепям питания;
– защиту от утечки по цепям заземления;
– защиту от утечки за счет взаимного влияния проводов и линий связи;
– защиту от утечки за счет высокочастотного навязывания.

Конкретные защитные действия от утечки по электромагнитному каналу включают применение пассивных мер, таких как экранирование и фильтрация, а также активных, таких как постановка маскирующих помех (рис. 7.26–7.28).

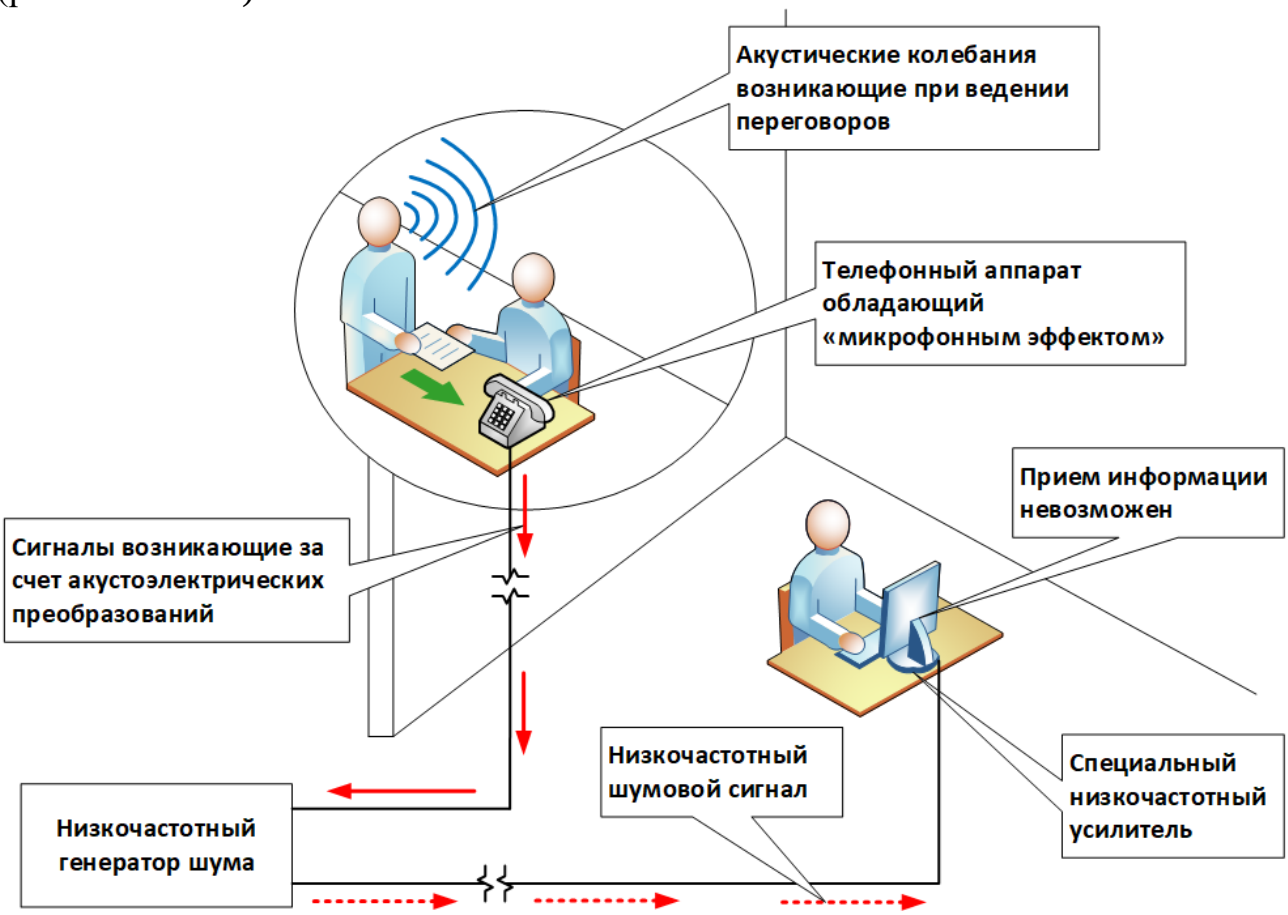


Рис. 7.26. Создание маскирующих помех в линиях связи

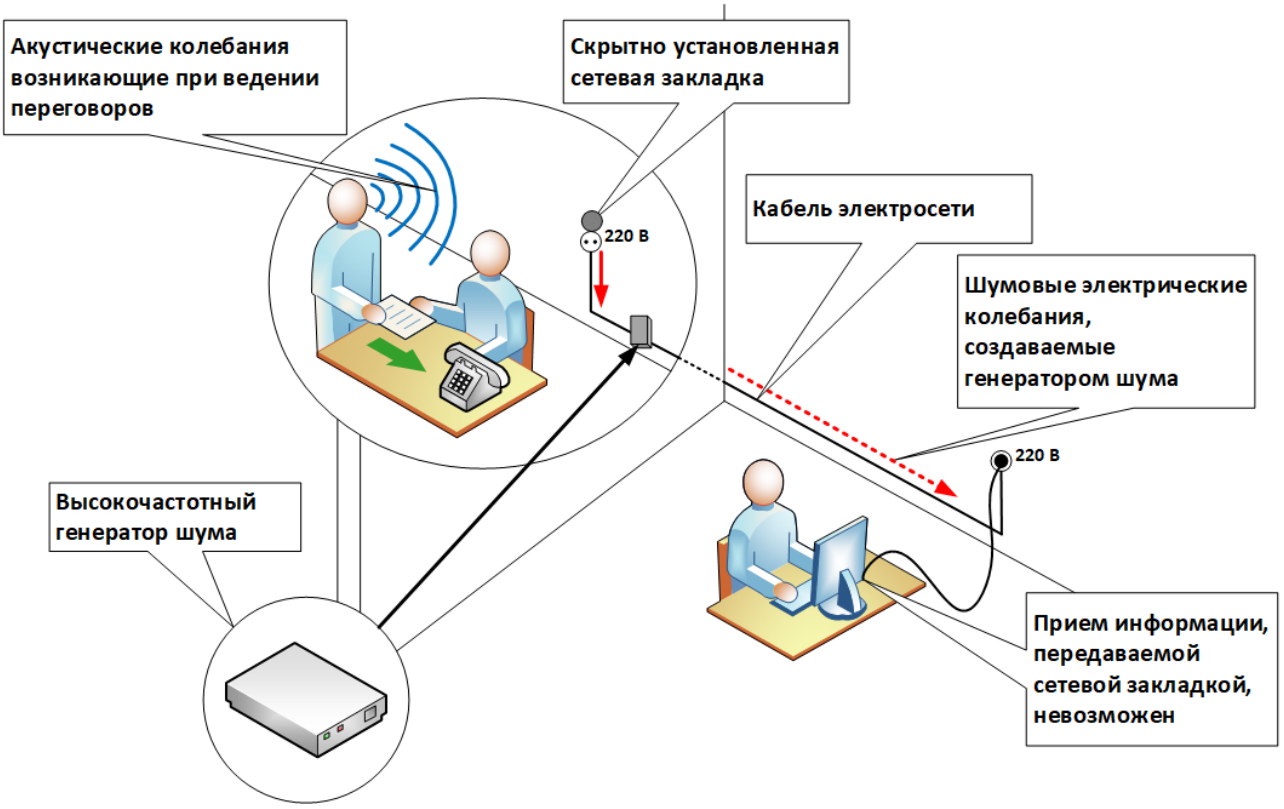


Рис. 7.27. Создание маскирующих помех в линиях электропитания

Рис. 7.28. Создание высокочастотных электромагнитных помех

Не малую роль для нейтрализации электромагнитных каналов утечки информации играют аппаратные средства защиты информации. Наличие электромагнитного канала утечки информации не может быть обнаружено органами чувств человека и здесь обязательно требуется помощь технических средств.

Аппаратные средства защиты информации — это самые различные по принципу действия, устройству и возможностям технические устройства, обеспечивающие защиту от утечки, пресечение разглашения и противодействие несанкционированному доступу к источникам конфиденциальной информации. Аппаратные средства защиты информации применяются для решения следующих задач:

– проведение специальных исследований технических средств обеспечения производственной деятельности на наличие возможных каналов утечки информации;

– выявление каналов утечки информации на различных объектах и в помещениях;

– локализация каналов утечки информации;

– поиск и обнаружение средств несанкционированного съема информации;

– противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям.

Защита информации от утечки по материально-вещественным каналам включает:

– учет отдельных листов с записями, использованной копировальной бумаги, макетов, бракованных узлов и деталей;

– сбор черновиков документов и различных записей на отдельных неучтенных листках в специальные опечатанные ящики;

– уничтожение бумажных и стирание (уничтожение) машинных носителей;

– разборка макетов и блоков, разрушение механических деталей.

Структура системы инженерно-технической защиты информации представлена на рис. 7.29.

Рис. 7.29. Структура системы инженерно-технической защиты информации

Вопросы для самоконтроля

1. Приведите определение закладочного устройства.
2. Перечислите демаскирующие признаки автономных некамуфлированных акустических закладок.
3. Перечислите демаскирующие признаки полуактивных акустических радиозакладок.
4. Какие технические средства применяют для выявления радиозакладочных устройств?
5. Чем принципиально различаются методы пассивной и активной защиты речевой информации?
6. Что называют звуковой маскировкой?
7. Какими особенностями характеризуются распространение звуковых колебаний в инженерных конструкциях?
8. Каким образом осуществляется съем речевой информации по виброакустическому каналу?
9. В чем заключается эффект акустоэлектрических преобразований?
10. Какие устройства с акустоэлектрическим эффектом могут входить в состав некоторых технических средств?

11. В чем заключается эффект модуляционного акустоэлектрического преобразования?

12. Причины и последствия модуляции информационным речевым сигналом высокочастотных колебаний у генераторов технических средств.

13. Каким образом осуществляется перехват речевого сигнала в акустоэлектрическом канале?

14. Что понимается под утечкой информации?

15. Каким образом классифицируются каналы утечки информации?

16. Инженерная защита объектов информатизации.

17. Техническая охрана объектов информатизации.

18 Каковы принципиальные отличия инженерно-технической защиты информации от прочих методов обеспечения информационной безопасности?

19. Каковы цели и задачи инженерно-технической защиты информации?

20. Что такое «опасные сигналы»?

21. Какие типы технических каналов утечки (оптические, акустические, электромагнитные, материально-вещественные и т.д.) представляют наибольшую угрозу информационной безопасности?

8. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

8.1. Стандарты информационной безопасности

Проблемой информационной компьютерной безопасности начали заниматься с того момента, когда компьютер стал обрабатывать данные. С развитием компьютерных сетей и ростом спроса на электронные услуги стал особенно актуальным вопрос стандартизации подходов к ее решению. Главная задача стандартов информационной безопасности — создать основу для взаимодействия между производителями, потребителями и экспертами продуктов ИТ.

Исторически первым стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Оранжевая книга). «Оранжевая книга» была впервые опубликована в августе 1983 г. В ней были заложены основные понятия, такие как безопасная система, доверенная система [38].

Безопасная система — это система, которая обеспечивает управление доступом к информации таким образом, что только авторизованные лица или процессы, действующие от их имени, получают право работы с информацией.

Доверенная система — система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа.

В рассматриваемых «Критериях…» и безопасность, и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности (статической). Вопросы доступности «Оранжевая книга» не затрагивает. Степень доверия оценивается по двум основным критериям: политика безопасности и уровень гарантированности.

Политика безопасности — набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию.

Уровень гарантированности — мера доверия, которая может быть оказана архитектуре и реализации ИС. В частности, политика безопасности определяет, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности — это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия. Уровень гарантированности — мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.

Доверенная вычислительная база — это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор. Границу доверенной вычислительной базы называют периметром безопасности.

Согласно «Оранжевой книге», политика безопасности должна обязательно включать в себя следующие элементы:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом.

Произвольное управление доступом (дискреционное) — это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

Безопасность повторного использования объектов — важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из «мусора». Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и внешних носителей в целом. Информация о субъектах также представляет собой объект, важно исключить «повторное использование субъектов». Когда пользователь покидает организацию, следует не только лишить его возможности входа в систему, но и запретить доступ ко всем объектам. В противном случае новый сотрудник может получить ранее использовавшийся идентификатор, а с ним и все права своего предшественника. Современные интеллектуальные периферийные устройства усложняют обеспечение безопасности повторного использования объектов. Принтер может буферизовать несколько страниц документа, которые останутся в памяти даже после окончания печати. Необходимо предпринять специальные меры, чтобы «выгрузить» их оттуда.

Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, метка объекта — степень конфиденциальности содержащейся в нем информации. Согласно «Оранжевой книге», метки безопасности состоят из двух частей — уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, категории — неупорядоченное. Назначение последних — описать предметную область, к которой относятся данные. Механизм категорий позволяет разделить информацию по отсекам, что способствует лучшей защищенности.

Принудительное (или мандатное) управление доступом основано на сопоставлении меток безопасности субъекта и объекта. Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у

объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен — читать можно только то, что положено. Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, «конфиденциальный» субъект может записывать данные в секретные файлы, но не может — в несекретные (разумеется, должны также выполняться ограничения на набор категорий).

«Оранжевая книга» определила ранжирование информационных систем по степени доверия безопасности. Определяется четыре уровня доверия — D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием степени доверия.

Аналогом «Оранжевой книги» является международный стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» (издан 1 декабря 1999 г.) [39]. По историческим причинам данный стандарт часто называют «Общими критериями» («Common Criteria»). «Общие критерии» (ОК) обобщили содержание и опыт использования «Оранжевой книги», развили европейские и канадские критерии и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США. В отличие от «Оранжевой книги», ОК не содержат предопределенных «классов безопасности». Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и (или) конкретной информационной системы. ОК содержат два основных вида требований безопасности:

– функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;

– требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в «Общих критериях» представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это значительно больше, чем число аналогичных сущностей в «Оранжевой книге». Функциональные требования:

– идентификация и аутентификация;

– защита данных пользователя;

– защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);

– управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);

– аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);

– доступ к объекту оценки;

– приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);

– использование ресурсов (требования к доступности информации);

– криптографическая поддержка (управление ключами);

– связь (аутентификация сторон, участвующих в обмене данными);

– доверенный маршрут/канал (для связи с сервисами безопасности).

Форма представления требований доверия, в принципе, та же, что и для функциональных требований. Специфика состоит в том, что каждый элемент требований доверия принадлежит одному из трех типов:

– действия разработчиков;

– представление и содержание свидетельств;

– действия оценщиков.

Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Классы:

– разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);

– поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);

– тестирование;

– оценка уязвимостей (включая оценку стойкости функций безопасности);

– поставка и эксплуатация;

– управление конфигурацией;

– руководства (требования к эксплуатационной документации);

– поддержка доверия (для поддержки этапов жизненного цикла после сертификации);

– оценка профиля защиты;

– оценка задания по безопасности.

Общие критерии были приняты в качестве национального стандарта и в Российской Федерации в 2002 г. Это три части:

ГОСТ Р ИСО/МЭК 15408-1-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

ГОСТ Р ИСО/МЭК 15408-2-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

ГОСТ Р ИСО/МЭК 15408-3-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

Стандарт подвергался изменениям и дополнениям и в настоящее время действующие версии:

ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

На основе этого стандарта принят Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Части 1–3», утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 19 июня 2002 г. № 187 [30]. Руководящий документ направлен на обеспечение практического использования ГОСТ Р ИСО/МЭК 15408-2002 в деятельности заказчиков, разработчиков и пользователей продуктов и систем ИТ при формировании ими требований, разработке, приобретении и применении продуктов и систем информационных технологий, предназначенных для обработки, хранения или передачи информации, подлежащей защите в соответствии с требованиями нормативных правовых документов или требованиями, устанавливаемыми собственником информации. Руководящий документ предназначен также для органов сертификации и испытательных лабораторий, аккредитованных в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 (Гостехкомиссии России), для использования при проведении оценки и сертификации безопасности ИТ.

С точки зрения международных стандартов информационная безопасность — это управляемое состояние. Международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «Управление информационной безопасностью — Информационные технологии» («Information technology — Information security management») является одним из наиболее известных стандартов в области защиты информации. Данный стандарт был разработан на основе первой части Британского стандарта BS 7799-1:1995 «Практические рекомендации по управлению информационной безопасностью» («Information security management — Part 1: Code of practice for information security management»). У нас в Российской Федерации действовал ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью». Затем международная организация по стандартизации ИСО приняла решение управление информационной безопасностью регламентировать отдельной серией стандартов и были разработаны:

ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».

ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

ГОСТ Р ИСО/МЭК 27003-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности».

ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

ГОСТ Р ИСО/МЭК 27031-2012 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».

Имеется и ряд сопутствующих стандартов, не входящих в серию 27000:

ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ГОСТ Р ИСО/МЭК 29100-2013 «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности».

ГОСТ Р 53647.6-2012 «Менеджмент непрерывности бизнеса. Требования к системе менеджмента персональной информации для обеспечения защиты данных».

Техническая спецификация X.800 появилась немногим позднее «Оранжевой книги», но весьма полно и глубоко трактует вопросы информационной безопасности распределенных систем. Документ разработан Международным союзом электросвязи (МСЭ, International Telecommunication Union, ITU). Это — международная организация, определяющая рекомендации в области телекоммуникаций и радио, а также регулирующая вопросы международного использования радиочастот (распределение радиочастот по назначениям и по странам). Основан как Международный телеграфный союз в 1865 г., с 1947 г. является специализированным учреждением ООН.

Рекомендации X.800 (X.800: Security architecture for Open Systems Interconnection for CCITT applications) являются основополагающим документом в области защиты распределенных систем. В нем выделяют следующие сервисы безопасности и исполняемые ими роли:

1. Аутентификация. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

2. Управление доступом. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

3. Конфиденциальность данных. Обеспечивает защиту от несанкционированного получения информации. Отдельно стоит упомянуть конфиденциальность трафика (это защита информации, которую можно получить, анализируя сетевые потоки данных).

4. Целостность данных подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры — с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

5. Неотказуемость (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является аутентификация источника данных.

Практически все механизмы сетевой безопасности могут быть реализованы на третьем уровне эталонной модели OSI. Средства безопасности для IP описываются семейством спецификаций IPsec, разработанных рабочей группой IP Security Инженерного совета Интернета (Internet Engineering Task Force, IETF). IETF — открытое международное сообщество проектировщиков, ученых, сетевых операторов и провайдеров, созданное в 1986 г. и занимающееся развитием протоколов и архитектуры Интернета.

Основные составляющие архитектуры средств безопасности для IP-уровня — это прежде всего протоколы обеспечения аутентичности (протокол аутентифицирующего заголовка — Authentication Header, AH) и конфиденциальности (протокол инкапсулирующей защиты содержимого — Encapsulating Security payload, ESp), а также механизмы управления криптографическими ключами. На более низком архитектурном уровне располагаются конкретные алгоритмы шифрования, контроля целостности и аутентичности. Наконец, роль фундамента выполняет так называемый домен интерпретации (Domain of Interpretation, DOI), являющийся, по сути, базой данных, хранящей сведения об алгоритмах, их параметрах, протокольных идентификаторах и т.п. (рис. 8.1).

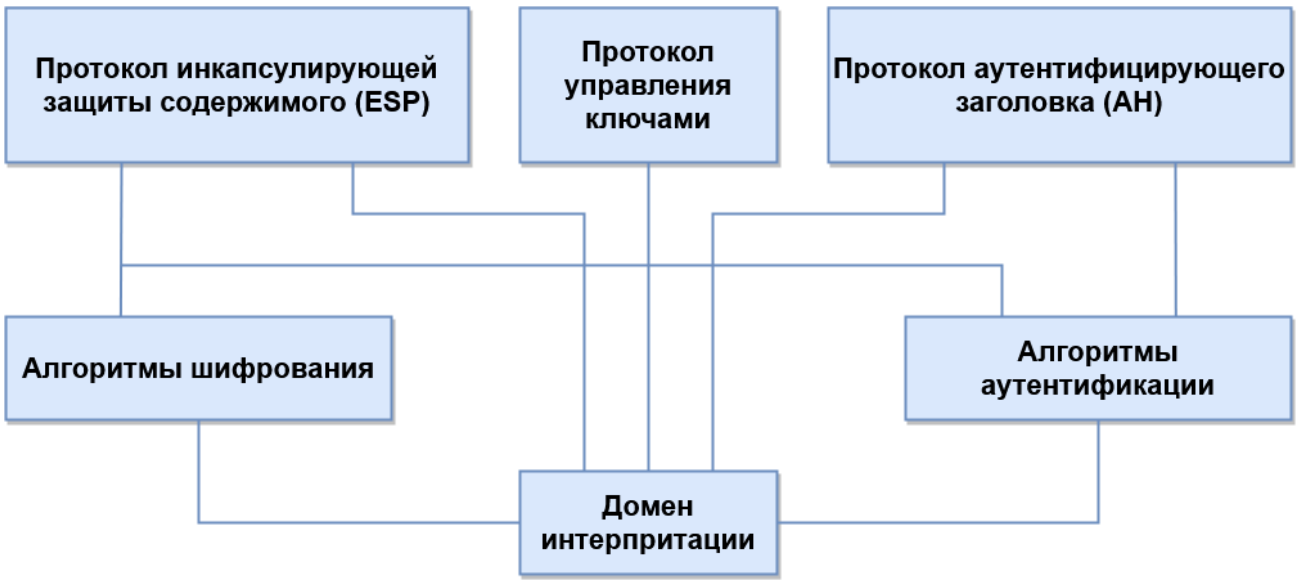


Рис. 8.1. Основные элементы архитектуры средств безопасности IP-уровня

Имеется ряд стандартов для беспроводных сетей. Протокол безопасности WEP (Wired Equivalent Privacy — эквивалент проводной безопасности) — первая технология защиты беспроводных сетей, изначально заложенная в спецификациях стандарта 802.11. Технология позволяла шифровать поток передаваемых данных между точкой доступа и персональным компьютером в рамках локальной сети. Шифрование данных осуществлялось с использованием алгоритма RC4 на ключе со статической составляющей от 40 до 104 бит и с дополнительной случайной динамической составляющей (вектором инициализации) размером 24 бит; в результате шифрование данных производилось на ключе размером от 64 до 128 бит. В 2001 г. были найдены способы, позволяющие путем анализа данных, передаваемых по сети, определить ключ. Перехватывая и анализируя сетевой трафик активно работающей сети, можно вскрывать 40-битный ключ в течение часа, а 128-битный ключ — примерно за четыре часа. Полученный ключ позволял нарушителю входить в сеть под видом легального пользователя. Технология WEP не обеспечивает надлежащего уровня безопасности корпоративной сети предприятия, но ее вполне достаточно для домашней беспроводной сети, когда объем перехваченного сетевого трафика слишком мал для анализа и вскрытия ключа.

Стандарт IEEE 802.11X — использует протокол расширенной аутентификации Extensible Authentication Protocol (EAP), протокол защиты транспортного уровня Transport Layer Security (TLS) и сервер доступа RADIUS (Remote Access Dial-in User Server). В отличие от протокола WEP, стандарт IEEE 802.11X использует динамические 128-битные ключи, периодически меняющиеся во времени. Секретный ключ пересылается пользователю в зашифрованном виде после прохождения этапа аутентификации. Время действия ключа ограничено временем действующего на данный момент сеанса. После окончания текущего сеанса создается новый секретный ключ и снова высылается пользователю. Для шифрования данных, как и в протоколе WEP, используется алгоритм RC4 с некоторыми изменениями.

Стандарт безопасности WPA (Wi-Fi Protected Access) — главной особенностью является динамическая генерация ключей шифрования данных, построенная на базе протокола TKIP (Temporal Key Integrity Protocol) и позволяющая обеспечить конфиденциальность и целостность передаваемых данных. По протоколу TKIP сетевые устройства работают с 48-битовым вектором инициализации (в отличие от 24-битового вектора WEP) и реализуют правила изменения последовательности его битов, что исключает повторное использование ключей. WPA изначально разрабатывался как временный стандарт, но получил широкое распространение.

Стандарт IEEE 802.11i (WPA2) — в основе лежит концепция надежно защищенной сети — Robust Security Network (RSN), в соответствии с которой точки доступа и сетевые устройства должны обладать отличными техническими характеристиками, высокой производительностью и поддержкой сложных алгоритмов шифрования данных. Технология IEEE 802.11i является дальнейшим развитием стандарта WPA, поэтому в этих стандартах реализовано много

аналогичных решений, например архитектура системы безопасности по аутентификации и обновлению ключевой информации сети.

Следует отметить и наличие международных стандартов безопасности облачных вычислений:

ISO/IEC TS 27017: 2015 «Информационные технологии — Руководство по мерам информационной безопасности для использования сервисами облачных вычислений, основанное на стандарте ISO/IEC 27002».

ISO/IEC 27040: 2015 «Информационные технологии — Безопасность хранения данных» (Information technology — Security techniques — Storage security).

ISO/IEC 27018: 2014 «Свод практик по мерам защиты персональных данных при оказании публичных облачных услуг» (Code of practice for data protection controls for public cloud computing services).

Стандарты и руководства США по облачным вычислениям:

NIST SP 800–144 «Руководство по обеспечению безопасности и защиты персональных данных при использовании публичных облачных вычислений» (Guidelines on Security and Privacy in Public Cloud Computing).

NIST SP 500–299 «Базовая архитектура обеспечения безопасности облачных вычислений» (Cloud Computing Security Reference Architecture).

В области криптографической защиты информации у нас действуют национальные стандарты:

ГОСТ Р 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.

ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования.

ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры.

ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

Криптография традиционно не охвачена международной стандартизацией, поэтому в США действуют свои федеральные стандарты:

FIPS 140-2 (Security Requirem ents for Cryptographic Modules) «Требования безопасности для криптографических модулей».

FIPS PUB 113 (Computer Data Authentication) «Проверка Подлинности Данных».

FIPS PUB 186-2 (Digital Signature Standard (DSS)) «Стандарт цифровой подписи (DSS)».

FIPS PUB 180-2 (Secure Hash Standard) «Стандарт безопасной хеш-функции».

FIPS PUB 198a (The Keyed-Hash Message Authentication Code (HMAC)) «Ключ-хеш проверки подлинности сообщения».

8.2. Лицензирование в области защиты информации

Лицензирование — деятельность лицензирующих органов по предоставлению, переоформлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, осуществлению лицензионного контроля, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования [40].

Лицензия — специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим органом на бумажном носителе или в форме электронного документа, подписанного электронной подписью, в случае, если в заявлении о предоставлении лицензии указывалось на необходимость выдачи такого документа в форме электронного документа [40].

В соответствии с федеральным законом «О лицензировании отдельных видов деятельности» лицензированию подлежат следующие виды деятельности в области защиты информации:

– 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);

– разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;

– деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

– разработка и производство средств защиты конфиденциальной информации;

– деятельность по технической защите конфиденциальной информации.

Лицензирование осуществляется органами исполнительной власти, являющимися регуляторами в области защиты информации. В зависимости от конкретных видов деятельности лицензирующими органами являются ФСБ и ФСТЭК [41].

В компетенции ФСБ России входит:

1. 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).

2. Разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации.

3. Деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

ФСБ России и ФСТЭК России лицензируют разработку и производство средств защиты конфиденциальной информации.

В компетенции ФСТЭК России входит деятельность по технической защите конфиденциальной информации.

Лицензирование этих видов деятельности регулируется рядом постановлений правительства:

– постановление Правительства РФ «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию 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)» от 16 апреля 2012 г. № 313;

– постановление Правительства РФ «Об утверждении Положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации» от 12 апреля 2012 г. № 287;

– постановление Правительства РФ «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» от 16 апреля 2012 г. № 314;

– постановление Правительства РФ «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» от 3 марта 2012 г. № 171;

– постановление Правительства РФ «О лицензировании деятельности по технической защите конфиденциальной информации» от 3 февраля 2012 г. № 79;

– постановление Правительства РФ «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. № 333.

Лицензирование деятельности по разработке и производству средств защиты конфиденциальной информации осуществляет Федеральная служба по техническому и экспортному контролю, а в части разработки и производства средств защиты конфиденциальной информации, устанавливаемых на объектах Администрации Президента Российской Федерации, Совета Безопасности Российской Федерации, Федерального Собрания Российской Федерации, Правительства Российской Федерации, Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации и Высшего Арбитражного Суда Российской Федерации, — Федеральная служба безопасности Российской Федерации [42].

8.3. Сертификация в области защиты информации

Сертификация — форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, документам по стандартизации или условиям договоров [43].

Сертификат соответствия — документ, удостоверяющий соответствие объекта требованиям технических регламентов, документам по стандартизации или условиям договоров [43].

Система сертификации — совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом [43].

Согласно ст. 5 ФЗ № 184, сертификация проводится «в отношении… продукции (работ, услуг), используемой в целях защиты сведений, составляю-

щих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа; продукции (работ, услуг), сведения о которой составляют государственную тайну; соответственно указанной продукции обязательными требованиями наряду с требованиями технических регламентов являются требования, установленные государственными заказчиками, федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности, обороны, внешней разведки, противодействия техническим разведкам и технической защиты информации, и (или) государственными контрактами (договорами)».

Статья 28 закона РФ «О государственной тайне» от 21 июля 1993 г. № 5485-I устанавливает обязательную сертификацию в отношении средств защиты информации: «Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности. Организация сертификации средств защиты информации возлагается на федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области обороны, в соответствии с функциями, возложенными на них законодательством Российской Федерации. Сертификация осуществляется в соответствии с настоящим Законом в порядке, установленном Правительством Российской Федерации. Координация работ по организации сертификации средств защиты информации возлагается на межведомственную комиссию по защите государственной тайны» [18].

Постановлением Правительства РФ «О сертификации средств защиты информации» от 26 июня 1995 г. № 608 утверждено Положение, согласно которому технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации [44]. Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных Федеральной службой безопасности Российской Федерации [44].

Система сертификации средств защиты информации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам. Системы сертификации создаются Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации, Министерством обороны Российской Федерации, уполномоченными проводить работы по сертификации средств защиты информации в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации.

Указом Президента РФ от 16 августа 2004 г. № 1085 ФСТЭК России установлены полномочия организовывать 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 [9].

Согласно Положению о системе сертификации средств защиты информации ФСТЭК России сертификация средств защиты информации осуществляется на соответствие требованиям по безопасности информации, установленным нормативными правовыми актами ФСТЭК России, а также техническими условиями, техническим заданием, заданием по безопасности, согласованными заявителями на сертификацию с ФСТЭК России [45].

Сертификации в системе сертификации ФСТЭК России подлежат:

– средства противодействия иностранным техническим разведкам, а также средства контроля эффективности противодействия иностранным техническим разведкам;

– средства технической защиты информации, включая средства, в которых они реализованы, а также средства контроля эффективности технической защиты информации;

– средства обеспечения безопасности информационных технологий, включая защищенные средства обработки информации.

Организационная структура системы сертификации ФСТЭК следующая:

– федеральный орган по сертификации (ФСТЭК РФ);

– организации, аккредитованные ФСТЭК России в качестве органа по сертификации;

– организации, аккредитованные ФСТЭК России в качестве испытательной лаборатории;

– изготовители средств защиты информации.

Указом Президента РФ от 11 августа 2003 г. № 960 для решения основных задач ФСБ России предусмотрены функции осуществлять и организовывать в соответствии с федеральным законодательством сертификацию средств защиты информации, систем и комплексов телекоммуникаций, технических средств, используемых для выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах, специальных технических средств, предназначенных для негласного получения информации, технических средств обеспечения безопасности и (или) защиты информации; определяет основные направления деятельности органов безопасности в этих областях [10].

Приказом ФСБ РФ от 13 ноября 1999 г. № 564 утверждено Положение о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (СЗИ-ГТ), и о ее знаках соответствия [46]. Органы по сертификации системы сертификации СЗИ-ГТ проводят обязательную сертификацию средств защиты информации, используемых при работе со сведениями, составляющими государственную

тайну, в том числе иностранного производства. Номенклатура СЗИ-ГТ разрабатывается ФСБ России на основании видов средств защиты информации, подлежащих сертификации в системе сертификации СЗИ-ГТ и утверждается по согласованию с Межведомственной комиссией по защите государственной тайны [46]. По правилам системы сертификации СЗИ-ГТ по инициативе разработчика, изготовителя или потребителя может также проводиться добровольная сертификация средств защиты информации, не предназначенных для работы со сведениями, составляющими государственную тайну [46].

Организационная структура системы сертификации СЗИ-ГТ:

– ФСБ России (федеральный орган исполнительной власти, уполномоченный проводить работу по обязательной сертификации средств защиты информации);

– центральный орган системы сертификации (создается при необходимости);

– органы по сертификации СЗИ-ГТ;

– испытательные центры (лаборатории);

– учебно-методический центр;

– заявители (разработчики, изготовители, продавцы, потребители СЗИ-ГТ).

Согласно Положению о сертификации средств защиты информации по требованиям безопасности информации система сертификации средств защиты информации по требованиям безопасности информации включает в себя аттестацию объектов информатизации по требованиям безопасности информации [47]. Данный вид деятельности регламентируется Положением по аттестации объектов информатизации по требованиям безопасности информации [48]. Система аттестации объектов информатизации по требованиям безопасности информации является составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в установленном Госстандартом России порядке. Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации, которым является Гостехкомиссия России [48]. Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России. Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленными в «Аттестате соответствия». Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров. В остальных случаях аттестация носит добро-

вольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации. Аттестация проводится органом по аттестации в установленном Положением порядке в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из следующего основного перечня работ:

– анализ исходных данных по аттестуемому объекту информатизации;

– предварительное ознакомление с аттестуемым объектом информатизации;

– проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;

– проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;

– проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;

– проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

– анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

В соответствии с Приказом ФСТЭК от 11 февраля 2013 г. № 17 для обеспечения защиты информации, содержащейся в государственной информационной системе, проводятся ее обязательная аттестация по требованиям защиты информации перед вводом ее в действие.

8.4. Управление информационной безопасностью

Обеспечение информационной безопасности нуждается в комплексном подходе к разработке средств защиты как на техническом, так и на организационном уровне. ИБ не может быть обеспечена разовым мероприятием, например покупкой конкретного набора средств защиты. Средства защиты нуждаются в постоянном обновлении, поскольку новые угрозы и новые уязвимости все время появляются в процессе жизненного цикла ИС. Обеспечение ИБ — это постоянный процесс, который называется процессом управления информационной безопасностью.

Управление информационной безопасностью (Security information management, SIM) — это циклический процесс, включающий:

– осознание степени необходимости защиты информации и постановку задач;

– сбор и анализ данных о состоянии информационной безопасности в организации;

– оценку информационных рисков;

– планирование мер по обработке рисков;

– реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий;

– мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия.

Проблема управления информационной безопасностью встала еще во времена появления персональных компьютеров и Интернета как массовых продуктов. Получившие доступ к новым технологиям хакеры начали активно их использовать для воровства данных кредитных карт и других видов мошенничества. Британский институт стандартов (BSI) при участии коммерческих организаций начал разработку стандарта управления информационной безопасностью. Результатом работы BSI в 1995 г. стало принятие национального британского стандарта BS 7799 управления информационной безопасностью организации. Стандарт состоял из двух частей: первая часть стандарта (BS 7799:1) носила рекомендательный характер, а вторая (BS 7799:2) предназначалась для сертификации и содержала ряд обязательных требований, не входивших в первую часть. При разработке стандарта ставилась задача обеспечения государственных и коммерческих организаций инструментом для создания эффективных систем информационной безопасности на основе современных методов управления.

В 1999 г. в международной организации по стандартизации ИСО было принято решение взять за основу стандарта в области информационной безопасности BS 7799:1. В результате вышел в свет международный стандарт ISO 17799, который базировался на стандарте BS 7799:1. Изначально была предусмотрена только сертификация по стандарту BS 7799:2. Процедура сертификации по стандарту ISO появилась после выхода в 2005 г. стандарта ISO 27001:2005 [50].

В настоящее время система менеджмента информационной безопасности (далее — СМИБ) представлена целой серией международных стандартов, значительное количество которых принято в Российской Федерации в качестве национальных. Далее представляем не исчерпывающий перечень, а только наиболее значимые:

ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary (Информационная технология. Методы обеспечения безопасности. Система менеджмента информационной безопасности. Общий обзор и терминология).

ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements (Информационная технология. Методы обеспечения безопасности. Система менеджмента информационной безопасности. Требования).

ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security management (Информационная технология.

Методы обеспечения безопасности. Свод правил по управлению защитой информации).

ISO/IEC 27003:2017, Information technology — Security techniques — Information security management system — Guidance (Информационная технология. Методы обеспечения безопасности. Система менеджмента информационной безопасности. Руководство).

ISO/IEC 27004:2016, Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation (Информационная технология. Методы обеспечения безопасности. Система менеджмента информационной безопасности. Мониторинг, измерение, анализ и оценка).

ISO/IEC 27005:2018, Information technology — Security techniques — Information security risk management (Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности).

ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems (Требования для органов, обеспечивающих аудит и сертификацию систем менеджмента информационной безопасности).

ISO/IEC 27007:2020, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing (Информационная безопасность, кибербезопасность и защита конфиденциальности. Рекомендации по аудиту систем менеджмента информационной безопасности).

ISO/IEC 27011:2016, Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations (Информационная технология. Методы обеспечения безопасности. Руководящие указания по управлению защитой информации организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002).

Согласно ГОСТ Р ИСО/МЭК 27001-2021, система менеджмента информационной безопасности (СМИБ) (information security management system; ISMS) — часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности [51].

Область применения ГОСТ Р ИСО/МЭК 27001-2021 такова, что он предназначен для применения организациями любой формы собственности (например, коммерческими, государственными и некоммерческими). Стандарт предполагает использовать процессный подход для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ организации. В стандарте представлена модель PDCA: «планирование (Plan) — осуществление (Do) — проверка (Check) — действие (Act)», которая может быть применена при структурировании всех процессов СМИБ (рис. 8.2).

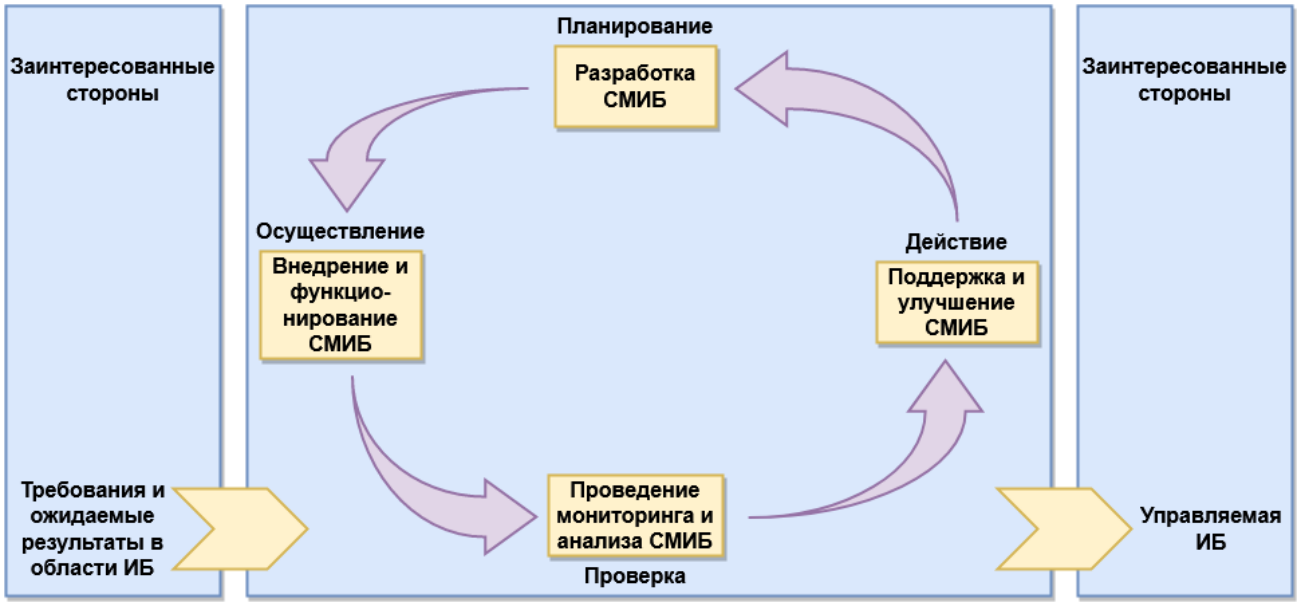


Рис. 8.2. Процессный подход в СМИБ

В соответствии с процессной моделью стандарт определяет четыре этапа создания СУИБ (табл. 8.1):

– разработка системы менеджмента информационной безопасности;

– внедрение и функционирование системы менеджмента информационной безопасности;

– проведение мониторинга и анализа системы менеджмента информационной безопасности;

– поддержка и улучшение системы менеджмента информационной безопасности.

Таблица 8.1

Модель PDCA

Планирование (разработка СМИБ)	Разработка политики, установление целей, процессов и процедур СМИБ, относящихся к менеджменту риска и улучшению информационной безопасности, для достижения результатов, соответствующих общей политике и целям организации
Осуществление (внедрение и обеспечение функционирования СМИБ)	Внедрение и применение политики информационной безопасности, мер управления, процессов и процедур СМИБ
Проверка (проведение мониторинга и анализа СМИБ)	Оценка, в том числе по возможности количественная, результативности процессов относительно требований политики, целей безопасности и практического опыта функционирования СМИБ и информирование высшего руководства о результатах для последующего анализа
Действие (поддержка и улучшение СМИБ)	Проведение корректирующих и превентивных действий, основанных на результатах внутреннего аудита или другой соответствующей информации, и анализа со стороны руководства в целях достижения непрерывного улучшения СМИБ

Основа стандарта ГОСТ Р ИСО/МЭК 27001-2021 — система управления рисками, связанными с информацией. Система управления рисками позволяет получать ответы на следующие вопросы: на каком направлении информационной безопасности требуется сосредоточить внимание? сколько времени и средств можно потратить на данное техническое решение для защиты информации?

Менеджмент рисков происходит по классической схеме: поиск, классификация, ранжирование, оценка, план по снижению рисков, принятие остаточных рисков и регулярный пересмотр рисков.

Следующий стандарт из серии, являющийся национальным, ГОСТ Р ИСО/МЭК 27002-2021, предлагает рекомендации и основные принципы введения, реализации, поддержки и улучшения менеджмента информационной безопасности в организации. Стандарт может служить практическим руководством по разработке стандартов безопасности организации для эффективной практики менеджмента безопасности организаций и способствует укреплению доверия в отношениях между организациями.

Меры и средства контроля и управления безопасностью, предлагаемые стандартом, включают:

- политику безопасности;
- организационные аспекты информационной безопасности;
- менеджмент активов;
- безопасность, связанная с персоналом;
- физическую защиту и защиту от воздействия окружающей среды;
- менеджмент коммуникаций и работ;
- управление доступом;
- приобретение, разработку и эксплуатацию информационных систем;
- менеджмент инцидентов информационной безопасности;
- менеджмент непрерывности бизнеса;
- соответствие.

Заслуживает рассмотрения ГОСТ Р ИСО/МЭК 27004-2021, который содержит рекомендации по разработке и использованию измерений и мер измерения для проведения оценки эффективности реализованной системы менеджмента информационной безопасности. Процесс измерений затрагивает политику, менеджмент риска информационной безопасности, меры и средства контроля и управления и цели их применения, процессы и процедуры, а также поддерживает процесс проверки СМИБ, помогая определить, требуется ли изменять или совершенствовать какие-либо из процессов или мер и средств контроля и управления СМИБ. Процесс измерений реализуется в виде программы измерений, связанных с информационной безопасностью.

ГОСТ Р ИСО/МЭК 27005-2010 рассматривает вопросы менеджмента риска информационной безопасности [54]. Риск информационной безопасности (information security risk) — возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации. Он измеряется исходя из комбинации вероятности события

и его последствия. Стандарт поддерживает общие концепции, определенные в ИСО/МЭК 27001, и предназначен для содействия адекватному обеспечению информационной безопасности на основе подхода, связанного с менеджментом риска. Стандарт применим для организаций всех типов (например, коммерческих предприятий, государственных учреждений, некоммерческих организаций), планирующих осуществлять менеджмент рисков, которые могут скомпрометировать информационную безопасность организации. Процесс менеджмента риска информационной безопасности представлен на рис. 8.3.

Рис. 8.3. Процесс менеджмента риска информационной безопасности

Вопросы для самоконтроля

1. Цели применения стандартов информационной безопасности.
2. Охарактеризуйте основные положения «Оранжевой книги».
3. Почему в современных стандартах отказываются от единых шкал, характеризующих уровень безопасности?
4. Каковы основные положения Европейских критериев безопасности информационных технологий?
5. Чем различаются «информационная система» и «продукт информационных технологий»?
6. Для чего вводятся критерии адекватности?

7. Что такое профиль защиты?

8. Опишите структуру «Общих критериев безопасности информационных технологий».

9. Опишите технологию применения «Общих критериев безопасности информационных технологий».

10. Каковы тенденции развития международной нормативной базы в области информационной безопасности?

11. Система сертификации РФ в области защиты информации.

12. Основные правила и документы системы сертификации РФ в области защиты информации.

13. Понятие «риска информационной безопасности».

14. Система сертификации РФ в области защиты информации.

15. Основные правила системы сертификации РФ в области защиты информации.

16. Основные документы системы сертификации РФ в области защиты информации.

ПРИМЕЧАНИЯ

1. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 5 дек. 2016 г. № 646 // Официальный интернет-портал правовой информации. 6 декабря 2016 г. URL: http://www.pravo.gov.ru ; То же // Собрание законодательства РФ. 2016. Ст. 7074, № 50.

2. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) : утв. приказом Гостехкомиссии России от 30 авг. 2002 г. № 282.

3. Об информации, информационных технологиях и о защите информации (с изменениями и дополнениями) : федер. закон от 27 июля 2006 г. № 149-ФЗ.

4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. — Москва : Стандартинформ, 2006.

5. О Концепции сотрудничества государств — участников Содружества Независимых Государств в сфере обеспечения информационной безопасности и о Комплексном плане мероприятий по реализации Концепции сотрудничества государств — участников Содружества Независимых Государств в сфере обеспечения информационной безопасности на период с 2008 по 2010 год : решение Совета глав государств СНГ (принято в г. Бишкеке 10 окт. 2008 г.).

6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : (выписка) (утв. ФСТЭК РФ 15 февр. 2008 г.).

7. Цифровая экономика Российской Федерации : нац. прогр. : принята в соответствии с указом Президента России «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» от 7 мая 2018 г. № 204 и утв. 24 дек. 2018 г. на заседании президиума Совета при Президенте России по стратегическому развитию и национальным проектам.

8. Вопросы Межведомственной комиссии по защите государственной тайны» (с изм. и доп.) : указ Президента РФ от 6 окт. 2004 г. № 1286.

9. Вопросы Федеральной службы по техническому и экспортному контролю» (с изм. и доп.) : указ Президента РФ от 16 авг. 2004 г. № 1085.

10. Вопросы Федеральной службы безопасности Российской Федерации (с изм. и доп.) : указ Президента РФ от 11 авг. 2003 г. № 960.

11. Вопросы Федеральной службы охраны Российской Федерации» (с изм. и доп.) : указ Президента РФ от 7 авг. 2004 г. № 1013.

12. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. — Москва : Стандартинформ, 2006.

13. Методика оценки угроз безопасности информации : (утв. ФСТЭК РФ 5 февр. 2021 г.). / ФСТЭК России. — URL: https://fstec.ru/component/attachments/download/2919 (дата обращения 20.12.2021).

14. Конвенция об обеспечении международной информационной безопасности (концепция), 2011 год.

15. Конвенция о защите персональных данных физических лиц при их автоматизированной обработке, 1981 год.

16. Конституция Российской Федерации : (принята всенар. голосованием 12 дек. 1993 г. с изм., одобр. в ходе общерос. голосования 1 июля 2020 г.).

17. О стандартизации в Российской Федерации : федер. закон : от 29 июня 2015 г. № 162-ФЗ (с изм. и доп.).

18. О государственной тайне : закон РФ от 21 июля 1993 г. № 5485-1 (с изм. и доп.).

19. Об утверждении Перечня сведений конфиденциального характера : Указ Президента РФ от 6 марта 1997 г. № 188 (с изм. и доп.).

20. О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ (с изм. и доп.).

21. О коммерческой тайне : федер. закон от 29 июля 2004 г. № 98-ФЗ (с изм. и доп.).

22. Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности : постановление Правительства РФ от 3 нояб. 1994 г. № 1233 (с изм. и доп.).

23. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. — Москва : ИПК «Издательство стандартов», 2011.

24. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. — Москва : Стандартинформ, 2009.

25. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. — Москва : Стандартинформ, 2014.

26. ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения. — Москва : Стандартинформ, 2019.

27. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации : руководящий док. Гостехкомиссии России (от 30 марта 1992 г.).

28. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации : руководящий док. Гостехкомиссии (от 30 марта 1992 г.)

29. Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей : руководящий док. Гостехкомиссии (от 30 марта 1992 г.)

30. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий : руководящий док. Гостехкомиссии (от 19 июня 2002 г.)

31. ГОСТ Р 58883-2020. Защита информации. Идентификация и аутентификация. Общие положения. — Москва : Стандартинформ, 2020.

32. ГОСТ Р 59453.1-2021. Защита информации. Формальная модель управления доступом. Ч. 1. Общие положения. — Москва : Стандартинформ, 2021.

33. Требования безопасности информации к операционным системам : метод. док. (утв. ФСТЭК 1 июня 2017 г.).

34. Выписка из перечня средств защиты информации, сертифицированных ФСБ России / ФСБ России. — URL: http://clsz.fsb.ru/files/download/svedeniya_po_
sertifikatam_08.21.doc (дата обращения 20.12.2021).

35. Государственный реестр сертифицированных средств защиты информации ФСТЭК России / ФСТЭК России. — URL: https://fstec.ru/component/attach
ments/download/489 (дата обращения 20.12.2021).

36. Об электронной подписи : федер. закон от 6 апр. 2011 г. № 63-ФЗ (с изм. и доп.).

37. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : (выписка) : (утв. ФСТЭК 15 февр. 2008 г.).

37. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : (выписка) : (утв. ФСТЭК 15 февр. 2008 г.).

38. Department of Defense Trusted Computer System Evaluation Criteria, TCSEC, DoD 5200.28-STD, Dec. 26, 1985.

39. ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation, Common Criteria.

40. О лицензировании отдельных видов деятельности : федер. закон от 4 мая 2011 г. № 99-ФЗ (ред. от 30 дек. 2015 г.).

41. Об организации лицензирования отдельных видов деятельности : постановление Правительства РФ от 21 нояб. 2011 г. № 957.

42. О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации : постановление Правительства РФ от 3 марта 2012 г. № 171.

43. О техническом регулировании : федер. закон от 27 дек. 2002 г. № 184-ФЗ.

44. О сертификации средств защиты информации : постановление Правительства РФ от 26 июня 1995 г. № 608.

45. Положение о системе сертификации средств защиты информации : (утв. приказом ФСТЭК России от 3 апр. 2018 г. № 55).

46. Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих госу-

дарственную тайну, и о ее знаках соответствия : приказ ФСБ РФ от 13 нояб. 1999 г. № 564.

47. Положение о сертификации средств защиты информации по требованиям безопасности информации : (утв. приказом Гостехкомиссии РФ от 27 окт. 1995 г. № 199).

48. Положение по аттестации объектов информатизации по требованиям безопасности информации : (утв. Гостехкомиссией РФ 25 нояб. 1994 г.).

49. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ Федер. службы по техн. и экспорт. контролю от 11 февр. 2013 г. № 17.

50. ISO/IEC 27001:2005, Information security management systems — Requirements (Система менеджмента информационной безопасности. Требования).

51. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

52. ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности.

53. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание.

54. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87995.html (дата обращения: 27.05.2022). — Режим доступа: для авторизир. пользователей.

2. Технологии защиты информации в компьютерных сетях : учеб. пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — Саратов : Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102207.html (дата обращения: 27.05.2022). — Режим доступа: для авторизир. пользователей.

3. Фомин, Д. В. Информационная безопасность : учебник / Д. В. Фомин. — DOI: https://doi.org/10.23682/118876. — Москва : Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/118876.html (дата обращения: 27.05.2022). — Режим доступа: для авторизир. пользователей.

4. Информационная безопасность. Практические аспекты : учебник для вузов / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург : Интермедия, 2021. — 240 с. — ISBN 978-5-4383-0205-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/103997.html (дата обращения: 27.05.2022). — Режим доступа: для авторизир. пользователей.

5. Голиков, А. М. Защита информации в цифровых системах связи : учебник / А. М. Голиков. — DOI: https://doi.org/10.23682/122465. — Москва : Ай Пи Ар Медиа, 2022. — 284 с. — ISBN 978-5-4497-1742-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/122465.html (дата обращения: 26.07.2022). — Режим доступа: для авторизир. пользователей.

6. Костромитин, К. И. Инженерно-техническая защита информации и технические средства охраны на критически важных объектах : учеб. пособие / К. И. Костромитин. — Москва : Ай Пи Ар Медиа, 2022. — 137 с. — ISBN 978-5-4497-1765-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/122647.html (дата обращения: 29.08.2022). — Режим доступа: для авторизир. пользователей.

Учебное издание

Бусько Михаил Михайлович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие

Издается в авторской редакции

Дизайн обложки
А. А. Мартыновой

ИД № 06318 от 26.11.01.
Подписано в печать 05.09.2022. Формат 60×90 1/16. Бумага офсетная. Печать цифровая. Усл. печ. л. 14,0. Тираж 300 экз. (1-й з-д 1–30). Заказ .

Издательский дом Байкальского государственного университета.
664003, г. Иркутск, ул. Ленина, 11.

Отпечатано в ИПО БГУ.