Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Л. М. Лыньков, В. Ф. Голиков, Т. В. Борботько

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ И УПРАВЛЕНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТЬЮ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для студентов учреждений, обеспечивающих получение высшего образования по специальностям, закрепленным за УМО

Минск БГУИР 2013

УДК 004.056(076)
ББК 32.973.26-018.2я73
Л88

Р е ц е н з е н т ы :
кафедра автоматизированных систем управления войсками учреждения образования «Военная академия Республики Беларусь», (протокол №9 от 25.05.2011);

заведующий кафедрой интеллектуальных систем Белорусского национального технического университета, доктор технических наук, профессор В. М. Колешко;

доцент кафедры проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент В. М. Алефиренко

Лыньков, Л. М.

Л88 Основы защиты информации и управления интеллектуальной собственностью : учеб.-метод. пособие / Л. М. Лыньков, В. Ф. Голиков, Т. В. Борботько. – Минск : БГУИР, 2013. – 243 с. : ил.

ISBN 978-985-488-811-8.

В пособии рассмотрены правовые, организационные и технические методы защиты информации. Приводится описание технических каналов утечки информации и организационно-технического комплекса мер по предотвращению утечки информации посредством данных каналов. Рассмотрены инженерно-технические методы защиты объектов от несанкционированного доступа, криптографической защиты информации и особенности защиты информации в автоматизированных системах.

УДК 004.056(076)
ББК 32.973.26-018.2я73

ISBN 978-985-488-811-8

СОДЕРЖАНИЕ

1. МЕТОДОЛОГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 6

1.1. Введение в защиту информации 6

1.2. Классификация угроз информационной безопасности 8

1.3. Классификация методов защиты информации 10

1.4. Охраняемые сведения 11

1.5. Демаскирующие признаки 13

1.6. Контрольные вопросы 16

2. ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ 17

2.1. Правовое обеспечение защиты информации 17

2.2. Государственное регулирование в сфере защиты информации 20

2.3. Контрольные вопросы 23

3. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ 24

3.1. Классификация 24

3.2. Акустические каналы утечки информации 25

3.3. Материально-вещественный и визуально-оптический каналы утечки информации 33

3.4. Электромагнитные каналы утечки информации 34

3.5. Утечка информации по цепям заземления 36

3.6. Утечка информации по цепям электропитания 37

3.7. Перехват информации в телефонных каналах связи 40

3.8. Высокочастотное навязывание 45

3.9. Контрольные вопросы 47

4. ПАССИВНЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ 48

4.1. Экранирование электромагнитных полей 48

4.2. Конструкции экранов электромагнитного излучения 51

4.3. Фильтрация 59

4.4. Заземление технических средств 63

4.5. Звукоизоляция помещений 66
4.6. Контрольные вопросы 71
5. АКТИВНЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ 73
5.1. Акустическая маскировка 73
5.2. Электромагнитная маскировка 78
5.3. Обнаружение закладных устройств 80
5.4. Технические средства обнаружения закладных устройств 84
5.5. Контрольные вопросы 90
6. ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА 91
6.1. Категорирование объектов 91
6.2. Классификация помещений и территории объекта 93
6.3. Инженерные заграждения 96
6.4. Технические средства охраны периметра объекта 101
6.5. Охранное телевидение 112
6.6. Системы контроля и управления доступом 121
6.7. Управляемые преграждающие устройства 125
6.8. Контрольные вопросы 130
7. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ 131
7.1. Основы построения криптосистем 131
7.2. Симметричные криптосистемы 140
7.3. Стандарт шифрования данных ГОСТ 28147–89 147
7.4. Асимметричные криптосистемы 163
7.5. Электронная цифровая подпись 165
7.6. Аутентификация пользователей в телекоммуникационных системах 175
7.7. Контрольные вопросы 183
8. ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ 184
8.1. Политика безопасности 184
8.2. Механизмы защиты 190

8.3. Принципы реализации политики безопасности 199
8.4. Защита транзакций в Интернет 204
8.5. Атаки в компьютерных сетях 217
8.6. Межсетевые экраны 225
8.7. Контрольные вопросы 241
ЛИТЕРАТУРА 242

1. МЕТОДОЛОГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ученые, анализируя тот или иной отрезок истории развития человеческого общества, присваивают ему краткое наименование, в основе которого лежит наиболее характерное свойство, присущее именно данному отрезку истории. Известны различные классификации, например по классовым признакам, по технологическим и т. д. Если следовать технологической классификации, то сегодня человечество переходит от индустриального общества к информационному. Информация из абстрактного «знания» превращается в материальную силу. Информационные технологии коренным образом меняют облик материального производства, позволяют экономить материальные ресурсы, создавать новые приборы и системы, в общем, в буквальном смысле изменяют наши представления о времени и пространстве.

Однако широкое внедрение в жизнь информационных технологий, управляющих жизненно важными процессами, к сожалению, сделало их достаточно уязвимыми со стороны естественных воздействий среды и искусственных воздействий со стороны человека. Возникла проблема обеспечения безопасности информационных систем в широком смысле слова или защиты информации в более узкой постановке.

1.1. Введение в защиту информации

Целями защиты являются: предотвращение утечки, хищения, утраты, искажения, подделки, несанкционированных действий по уничтожению, модификации, копированию, блокированию документированной информации и иных форм незаконного вмешательства в информационные системы.

Под **информацией** будем понимать сведения о лицах, предметах, фактах, событиях, явлениях и процессах.

Информация может существовать в виде документа (бумажного), в виде физических полей и сигналов (электромагнитных, акустических, тепловых и т. д.), в виде биологических полей (память человека).

В дальнейшем будем рассматривать информацию в документированной (на бумаге, дискете и т.д.) форме, в форме физических полей (радиосигналы, акустические сигналы). Среду, в которой информация либо создается, либо передается, обрабатывается, хранится, будем называть **информационным объектом.**

Под **безопасностью информационного объекта** (ИО) будем понимать его защищенность от случайного или преднамеренного вмешательства в нормальный процесс его функционирования.

Природа воздействия на ИО может быть двух видов: непреднамеренной (стихийные бедствия, отказы, ошибки персонала и т. д.); преднамеренной (действия злоумышленников). Все воздействия могут привести к последствиям (ущербу) трех видов: нарушению конфиденциальности; нарушению целостности; нарушению доступности.

Нарушение конфиденциальности – нарушение свойства информации быть известной только определенным субъектам.

Нарушение целостности – несанкционированное изменение, искажение, уничтожение информации.

Нарушение доступности (отказ в обслуживании) – нарушается доступ к информации, нарушается работоспособность объекта, доступ в который получил злоумышленник.

В отличие от разрешенного (санкционированного) доступа к информации в результате преднамеренных действий злоумышленник получает несанкционированный доступ (НСД). Суть НСД состоит в получении нарушителем доступа к объекту в нарушении установленных правил.

Под **угрозой информационной безопасности** объекта будем понимать возможные воздействия на него, приводящие к ущербу.

Некоторое свойство объекта, делающее возможным возникновение и реализацию угрозы, будем называть **уязвимостью.**

Действие злоумышленника, заключающееся в поиске и использовании той или иной уязвимости, будем называть **атакой.**

Целью защиты ИО является противодействие угрозам безопасности.

Защищенный ИО – объект со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Комплексная защита ИО – совокупность методов и средств (правовых, организационных, физических, технических, программных).

Политика безопасности – совокупность норм, правил, рекомендаций, регламентирующих работу средств защиты ИО от заданного множества угроз безопасности.

Схематично основное содержание предмета защиты информации представлено на рис. 1.1.

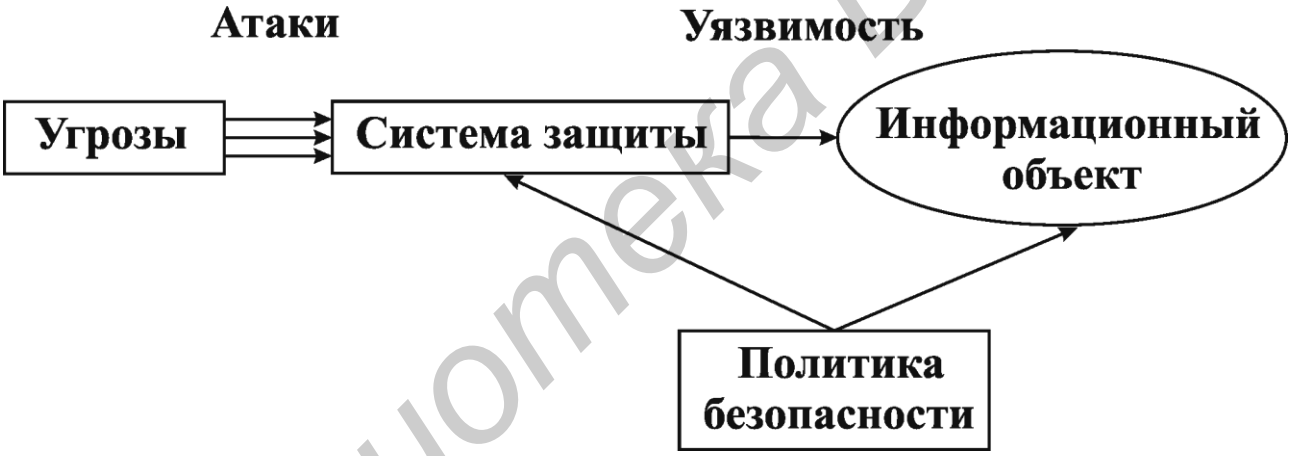


Рис. 1.1. Содержание предмета защиты информации

1.2. Классификация угроз информационной безопасности

Под **угрозой информационной безопасности объекта** будем понимать возможные воздействия на него, приводящие к ущербу. К настоящему времени известно большое количество угроз. Приведем упрощенную их классификацию. Угрозы делятся по свойству информации, против которого они направлены:

– физической и логической целостности (уничтожение или искажение информации);

– конфиденциальности информации;

– доступности (работоспособности);

– праву собственности.

По происхождению:

– случайные (отказы, сбои, ошибки, стихийные явления);

– преднамеренные (злоумышленные действия людей).

По источникам:

– люди (персонал, посторонние);

– технические устройства;

– модели, алгоритмы, программы;

– внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).

Рассмотрим более подробно перечисленные угрозы.

Случайные угрозы обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибок персонала. Методы оценки воздействия этих угроз рассматриваются в других дисциплинах (теории надежности, программировании, инженерной психологии и т. д.).

Преднамеренные угрозы связаны с действиями людей. Это и работники спецслужб, хакеры, работники самого объекта. Огромное количество разнообразных ИО делает бессмысленным перечисление всех возможных угроз для информационной безопасности, поэтому в дальнейшем при изучении того или иного раздела мы будем рассматривать основные угрозы для конкретных объектов.

Например, для несанкционированного доступа к информации вычислительной системы злоумышленник может воспользоваться штатными каналами доступа, если нет никаких мер защиты:

– через терминалы пользователей;

– через терминал администратора системы;

– через удаленные терминалы.

И через нештатные каналы:

– побочное электромагнитное излучение информации с аппаратуры системы;

– побочные наводки информации по сети электропитания и заземления;

– побочные наводки информации на вспомогательных коммуникациях;

– подключение к внешним каналам связи.

1.3. Классификация методов защиты информации

Все методы защиты информации по характеру проводимых действий можно разделить на законодательные (правовые); организационные; технические; комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие **правовые акты**, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс **организационных мер**, проводимых прежде всего государством, ответственным за выполнением законов, и собственниками информации. К таким мерам относятся и издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходи-

мы **технические устройства**. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты.

Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т. е. **комплексно.**

1.4. Охраняемые сведения

Технические средства, системы и другие объекты защиты обладают определенными характерными для них свойствами, а их функционирование сопровождается различными процессами. Выявление и анализ таких свойств и процессов позволяет получить представление о самом объекте защиты и об информации, циркулирующей в его элементах. Среди сведений, получаемых об объекте защиты при ведении разведки, могут быть так называемые **охраняемые сведения**, т. е. сведения, содержащие государственную тайну или отнесенные к другой категории конфиденциальной информации.

В соответствии с Законом «О государственных секретах» к охраняемым сведениям могут быть отнесены сведения, несанкционированное распространение которых создает или может нанести ущерб национальной безопасности, обороноспособности и жизненно важным интересам Республики Беларусь. Государственные секреты являются собственностью Республики Беларусь. Установление и снятие ограничений на распространение сведений, составляющих государственные секреты, производится в определенном настоящим законом порядке.

Носители сведений, составляющих государственные секреты – имеющие их физические лица, а также материальные объекты (документы, изделия и т. п.), в том числе физические поля, в которых сведения, составляющие государственные секреты, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Государственные секреты Республики Беларусь подразделяются на две категории: государственная тайна и служебная тайна.

Государственная тайна – государственные секреты, разглашение или утрата которых может повлечь тяжкие последствия для национальной безопасности, обороноспособности, экономических и политических интересов Республики Беларусь, а также создать реальную угрозу безопасности правам и свободам граждан.

Служебная тайна – государственные секреты, разглашение или утрата которых может нанести ущерб национальной безопасности, обороноспособности, политическим и экономическим интересам Республики Беларусь, а также правам и свободам граждан. Сведения, составляющие служебную тайну, как правило, имеют характер отдельных данных, входящих в состав сведений, являющихся государственной тайной, и не раскрывают ее в целом.

В зависимости от важности сведений, составляющих государственные секреты, характера и объема мер, необходимых для их защиты, устанавливаются три степени секретности для носителей (в виде материальных объектов) таких сведений: особой важности, совершенно секретно, секретно.

В соответствии со степенью секретности носителям сведений, составляющих государственную тайну, присваиваются ограничительные грифы: «Особой важности» и «Совершенно секретно», а носителям сведений, составляющих служебную тайну, – «Секретно».

В зависимости от степени секретности сведений, составляющих государственные секреты, устанавливаются три формы допуска к государственным секретам, соответствующие степени секретности этих сведений:

– форма №1 – допуск к сведениям особой важности и их носителям;

– форма №2 – допуск к совершенно секретным сведениям и их носителям;

– форма №3 – допуск к секретным сведениям и их носителям.

Наличие допуска формы №1 является основанием для доступа к сведениям допуска формы №2 и допуска формы №3, а наличие допуска формы №2 является основанием для доступа к сведениям допуска формы №3.

1.5. Демаскирующие признаки

Источниками информации об охраняемых сведениях могут быть различные характеристики объектов защиты, их элементов и создаваемых ими физических полей. С учетом доступности этих характеристик вводят понятие **демаскирующих признаков**.

Демаскирующие признаки (ДП) – это характеристики любого рода, поддающиеся обнаружению и анализу с помощью разведывательной аппаратуры и являющиеся источниками информации об охраняемых сведениях. Демаскирующие признаки делятся на первичные и вторичные.

Первичные ДП представляют собой физические характеристики объектов и среды, непосредственно регистрируемые специальной аппаратурой и содержащие информацию об охраняемых сведениях. Примером первичных ДП могут служить напряженность и поляризация электромагнитного поля, амплитуда, частота и фаза переменного электрического тока, уровень радиационного излучения, процентное содержание химического вещества в среде, сила и частота звуковых колебаний, яркость и длина волны светового излучения объекта и т. п.

Очевидно, что именно первичные ДП являются источниками информации, получаемой с помощью технических средств разведки (ТСР). Общее количество информации об объекте, получаемой с помощью ТСР, принципиально не может превышать количества информации, содержащейся во всех первичных ДП, характерных для этого объекта. Вместе с тем в ряде случаев именно первичные ДП содержат всю информацию об охраняемых сведениях. Поэтому их знание имеет первостепенное самостоятельное значение для противодействия ТСР.

Вторичные ДП – признаки, которые могут быть получены путем накопления и обработки первичных ДП. Примерами могут служить различного рода образцы (изображения сооружений и военной техники, диаграммы первичного и вторичного излучения объекта, амплитудно-частотные спектры излучений,

химический состав вещества и т. д.), процессы (радиосигнал, акустический сигнал, зависимость какого-либо первичного ДП от времени и т. д.) и ситуации, т. е. сочетания различных образцов и процессов, связанные с охраняемыми сведениями об объекте разведки.

Для разработки и реализации эффективных мероприятий по защите информации необходим учет всех без исключения возможностей ТСР, а это предполагает наличие максимально достоверных перечней охраняемых сведений и их демаскирующих признаков (рис. 1.2).

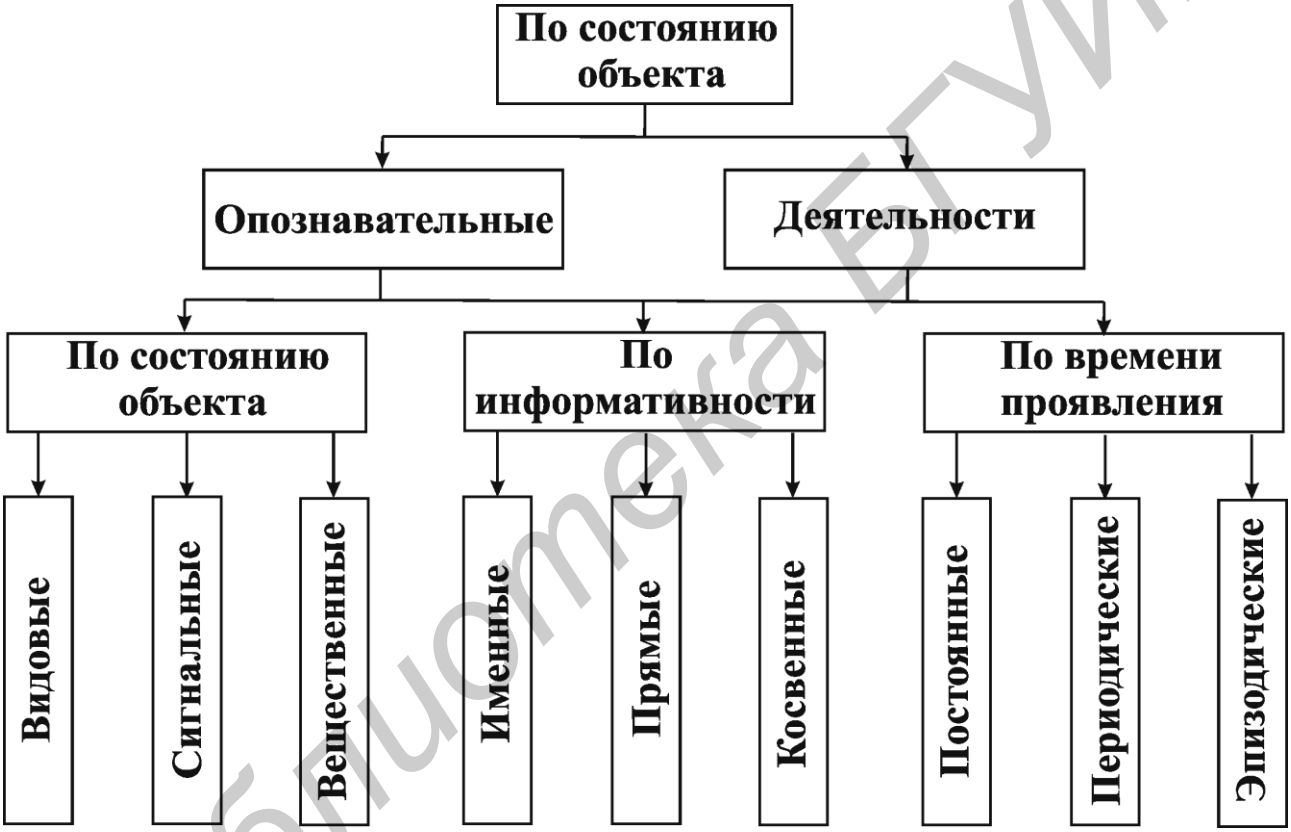


Рис. 1.2. Классификация демаскирующих признаков

По состоянию объектов демаскирующие признаки разделяются на опознавательные признаки и признаки деятельности. **Опознавательные ДП** описывают объекты в статическом состоянии: их назначение, принадлежность, параметры. **Признаки деятельности** объектов характеризуют этапы и режимы функционирования объектов, например этап создания новой продукции: научные исследования, подготовка к производству, изготовление новой продукции,

ее испытания и т. д. Все признаки объекта по характеру проявления можно разделить на 3 группы:

1) внешнего вида – видовые демаскирующие признаки;

2) признаки излучений – сигнальные демаскирующие признаки;

3) материально-вещественные признаки.

К **видовым признакам** относятся форма объекта, его размеры, детали объекта, тон, цвет и структура его поверхности и др.

Любое материальное тело с температурой выше абсолютного нуля (–273 °С) излучает электромагнитные (тепловые) поля, обусловленные тепловым движением электронов атомов вещества. Радиоэлектронные средства излучают функциональные и побочные электромагнитные поля, механические движения частей приборов и машин создают акустические поля.

Признаки излучений описывают параметры полей и электрических сигналов, генерируемых объектом: их мощность, частоту, вид (аналоговый, импульсный), ширину спектра и т. д.

Вещественные признаки определяют физический и химический состав, структуру и свойства веществ материального объекта. Таким образом, совокупность демаскирующих признаков рассмотренных трех групп представляет модель объекта, описывающую его внешний вид, излучаемые им поля, внутреннюю структуру и химический состав содержащихся в нем веществ.

Важнейшим показателем признака является его **информативность**. Информативность можно оценивать мерой в интервале [0–1], соответствующей значению вероятности обнаружения объекта по некоторому признаку. Чем признак более индивидуален, т. е. принадлежит меньшему числу объектов, тем он более информативен. Наиболее информативен **именной** признак, присущий только одному конкретному объекту. Такими признаками являются, например, фамилия, имя, отчество человека.

Информативность остальных демаскирующих признаков, принадлежащих рассматриваемому объекту и называемых **прямыми**, колеблется в преде-

лах [0–1]. Признаки, непосредственно не принадлежащие объекту, но отражающие свойства и состояние объекта, называются **косвенными**. Эти признаки являются, как правило, результатом взаимодействия рассматриваемого объекта с окружающей средой. К ним относятся, например, следы ног или рук человека, автомобиля и других движущихся объектов. Информативность косвенных признаков в общем случае ниже информативности прямых. Однако есть исключения, например, информативность четких отпечатков пальцев соответствует информативности именных признаков.

По времени проявления признаки могут быть:

– **постоянными**, не изменяющимися в течение жизненного цикла объекта;

– **периодическими**, например следы на снегу;

– **эпизодическими**, проявляющимися при определенных условиях, например случайно появившееся на поверхности объекта пятно краски.

1.6. Контрольные вопросы

1. Что называется информацией?
2. Что называется угрозой информационной безопасности? Приведите примеры.
3. Какая информация относится к охраняемым сведениям?
4. Перечислите носители охраняемых сведений.
5. Какие категории демаскирующих признаков вы знаете?

2. ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Правовое обеспечение защиты информации

Правовое обеспечение включает в себя:

1) нормотворческую деятельность по созданию законодательства, регулирующего общественные отношения в области защиты информации;

2) исполнительную и правоприменительную деятельность по исполнению законодательства в области информации, информатизации, защиты информации органами государственной власти и управления организациями (юридическими лицами), гражданами.

Нормотворческая деятельность:

– оценка состояния действующего законодательства и разработка программы его совершенствования;

– создание организационно-правовых механизмов обеспечения защиты информации;

– формирование правового статуса всех субъектов в системе защиты информации и определение их ответственности за обеспечение информационной безопасности;

– разработка организационно-правового механизма сбора и анализа статистических данных о воздействии угроз информационной безопасности и их последствиях с учетом всех категорий информации;

– разработка законодательных и других нормативных актов, регулирующих порядок ликвидации последствий воздействий угроз, восстановление права и ресурсов, реализации компенсационных мер.

Исполнительная и правоприменительная деятельность:

– разработка процедур применения законодательства и нормативных актов к субъектам, совершившим преступления и проступки при работе с закрытой информацией;

– разработка составов правонарушений с учетом специфики уголовной, гражданской, административной и дисциплинарной ответственности.

Деятельность по правовому обеспечению информационной безопасности строится на трех фундаментальных положениях:

1) *соблюдение законности* (предполагает наличие законов и иных нормативных документов, их применение и исполнение субъектами права в области информационной безопасности);

2) *обеспечение баланса интересов отдельных субъектов и государства* (предусматривает приоритет государственных интересов как общих интересов всех субъектов). Ориентация на свободы, права и интересы граждан не принижает роль государства в обеспечении национальной безопасности в целом и в области информационной безопасности в частности);

3) *неотвратимость наказания* (выполняет роль важнейшего профилактического инструмента в решении вопросов правового обеспечения).

Нормативно-правовая база в области защиты информации основывается на общегосударственных документах и ведомственных документах.

Общегосударственные документы:

1) законы, кодексы;

2) Указы Президента Республики Беларусь;

3) постановления Совета Министров.

Ведомственные документы:

1) межведомственные;

2) внутриведомственные.

Основные правовые акты, регламентирующие защиту информации в Республике Беларусь:

1. Указ Президента Республики Беларусь от 9 ноября 2010 г. №575 «Об утверждении Концепции национальной безопасности Республики Беларусь». Представляет собой совокупность официальных взглядов на сущность и содержание деятельности Республики Беларусь по обеспечению баланса интересов личности, общества, государства и их защите от внутренних и внешних угроз и обеспе-

чивает единство подходов к формированию и реализации государственной политики обеспечения национальной безопасности, а также методологическую основу совершенствования актов законодательства в различных сферах национальной безопасности, разработки документов стратегического планирования.

2. Закон Республики Беларусь «Об информации, информатизации и защите информации» от 19 октября 2008 года является основой для регулирования общественных отношений, возникающих при:

– поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также пользовании информацией;

– создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов;

– организации и обеспечении защиты информации.

3. Постановление Совета Министров Республики Беларусь от 26 мая 2009 г. №673 «О некоторых мерах по реализации Закона Республики Беларусь «Об информации, информатизации и защите информации» и о признании утратившими силу некоторых постановлений Совета Министров Республики Беларусь». Регламентирует порядок:

– защиты информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено;

– аттестации систем защиты информации;

– проведения государственной экспертизы средств защиты информации.

4. Постановление Совета Министров Республики Беларусь от 20 октября 2003 г. №1389 «О внесении изменений и дополнений в некоторые постановления Правительства Республики Беларусь и признании утратившими силу некоторых решений Правительства Республики Беларусь по вопросам лицензирования» . Устанавливает порядок выдачи специальных разрешений (лицензий) на осуществление деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи.

Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи» от 28 декабря 2009 года определяет правовые основы применения электронных документов, определяет основные требования, предъявляемые к электронным документам, а также правовые условия использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе.

2.2. Государственное регулирование в сфере защиты информации

Государство занимает важное место в системе защиты информации в любой стране, в том числе и в Республике Беларусь. Государственная политика обеспечения информационной безопасности исходит из положений Концепции национальной безопасности Республики Беларусь.

Система информационной безопасности является составной частью общей системы национальной безопасности страны и представляет собой совокупность взаимодействующих субъектов обеспечения национальной безопасности и средств, используемых ими для осуществления деятельности по защите и реализации национальных интересов Республики Беларусь и обеспечению безопасности личности, общества и государства.

В систему входят:

– органы государственной власти и управления, решающие задачи обеспечения информационной безопасности в пределах своей компетенции;

– государственные и межведомственные комиссии и советы, специализирующиеся на проблемах информационной безопасности;

– структурные и межотраслевые подразделения по защите информации органов государственной власти и управления, а также структурные подразделения предприятий, проводящие работы с использованием сведений, отнесенных к государственной тайне, или специализирующиеся на проведении работ в области защиты информации;

– научно-исследовательские, проектные и конструкторские организации, выполняющие работы по обеспечению информационной безопасности;

– учебные заведения, осуществляющие подготовку и переподготовку кадров для работы в системе обеспечения информационной безопасности.

Государственную систему защиты информации Республики Беларусь составляют:

– Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ);

– структурные подразделения по защите информации органов государственного управления, предприятий, организаций и учреждений;

– головные предприятия (организации, учреждения) по направлениям защиты информации;

– сертификационные и испытательные центры (лаборатории), предприятия, учреждения и организации различных форм собственности по оказанию услуг в области защиты информации.

Основными функциями системы информационной безопасности страны являются:

– разработка и реализация стратегии обеспечения информационной безопасности;

– оценка состояния информационной безопасности в стране, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения и нейтрализации этих угроз;

– координация и контроль деятельности субъектов системы информационной безопасности.

Первоочередные мероприятия по реализации государственной политики информационной безопасности должны включать:

– создание нормативно-правовой базы реализации государственной политики в области информационной безопасности, в том числе определение после-

довательности и порядка разработки законодательных и нормативно-правовых актов, а также механизмов практической реализации принятого законодательства;

– анализ технико-экономических параметров отечественных и зарубежных программно-технических средств обеспечения информационной безопасности и выбор перспективных направлений развития отечественной техники;

– формирование государственной научно-технической программы совершенствования и развития методов и средств обеспечения информационной безопасности, предусматривающей их использование в национальных информационных и телекоммуникационных сетях и системах с учетом перспективы вхождения страны в глобальные информационные сети и системы;

– создание системы сертификации на соответствие требованиям информационной безопасности отечественных и закупаемых импортных средств информатизации, используемых в государственных органах власти и управления.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных компьютерных системах и сетях являются:

– лицензирование деятельности предприятий в области защиты информации;

– аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;

– сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в отношении защищенности информации от утечки по техническим каналам;

– введение территориальных, частотных, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

– создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

2.3. Контрольные вопросы

1. Какие направления включает в себя правовое обеспечение защиты информации?

2. Дайте краткую характеристику нормотворческой деятельности в сфере защиты информации.

3. Каким образом реализуются исполнительная и правоприменительная деятельности?

4. На каких документах основывается нормативно-правовая база в сфере защиты информации?

5. Охарактеризуйте кратко структуру системы информационной безопасности в Республике Беларусь.

3. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

3.1. Классификация

Технический канал утечки информации – совокупность источника конфиденциальной информации, среды распространения и средства технической разведки для перехвата информации (рис. 3.1).

Рис. 3.1. Технический канал утечки информации

Источники конфиденциальной информации:

– человек;

– электронная аппаратура;

– документы (содержание);

– здания и сооружения (внешний вид).

Среда распространения конфиденциальной информации:

– воздушная;

– твердые вещества (строительные конструкции);

– электрические цепи.

Средства технической разведки:

– визуально-оптические (оптические увеличительные приборы);

– оптоэлектронные (телевизионные, приборы ночного видения, тепловизоры и т. д.);

– акустические (закладные устройства, направленные микрофоны, электронные стетоскопы и т. д.);

– радиоперехвата (перехвата сообщений радио-, сотовой связи и т. д.);

– фотографические;

– электронные (для перехвата сигналов в проводных коммуникациях).

По физическим принципам возникновения каналы утечки информации можно разделить на следующие группы (рис. 3.2):

– акустический;

– материально-вещественный;

– визуально-оптический;

– электромагнитный.

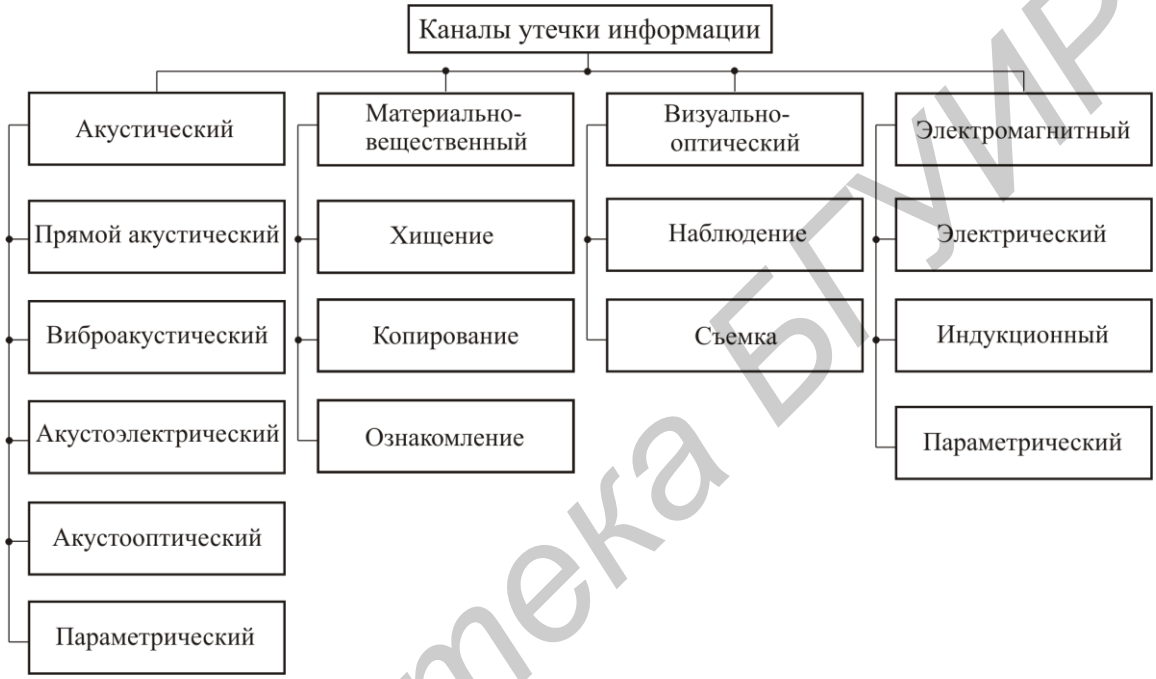


Рис. 3.2. Классификация каналов утечки информации

3.2. Акустические каналы утечки информации

В случае когда источником информации является голосовой аппарат человека, информация называется **речевой.**

Области спектра звука, в которых сосредоточивается основная мощность акустического сигнала, называются **формантами**. Большинство звуков речи имеют одну или две форманты. Форманты звуков речи расположены в области частот от 150…200 до 8600 Гц. Основная энергия подавляющей части формант сосредоточена в диапазоне частот 300…3400 Гц, что позволило ограничить спектр речевого сигнала, передаваемого по стандартному телефонному каналу, этой полосой.

Психологическая (с учетом чувствительности уха на разных частотах) интенсивность акустических сигналов изменяется в широких пределах (0…130 дБ). Для человека как основного источника соотношение между уровнем громкости и его качественной оценкой характеризуется следующими данными: очень тихая речь (шепот) – 5…10 дБ, тихая речь – 30…40 дБ, речь умеренной громкости 50…60 дБ, громкая речь – 60…70 дБ, крик – 70…80 дБ и более. Для сравнения: звук сирены «скорой помощи» – 100 дБ, а шум реактивного двигателя на расстоянии 5 м – 120 дБ.

Голосовой аппарат человека является первичным источником акустических колебаний, которые представляют собой возмущения воздушной среды в виде волн сжатия и растяжения (рис. 3.3).

Рис. 3.3. Структурная схема прямого акустического канала утечки информации

Перехват информации средствами технической разведки в данном случае может реализовываться за счет применения закладных устройств, устанавливаемых внутри помещения или при помощи направленных микрофонов, путем перехвата акустических сигналов через открытые окна, двери. В данном случае акустическая волна без существенного ослабления попадает в средство технической разведки. Таким образом, образуется **прямой** акустический канал утечки информации.

Закладное устройство (ЗУ) – автономное устройство для перехвата речевой информации, конструктивно объединяющее микрофон и передатчик (рис. 3.4).

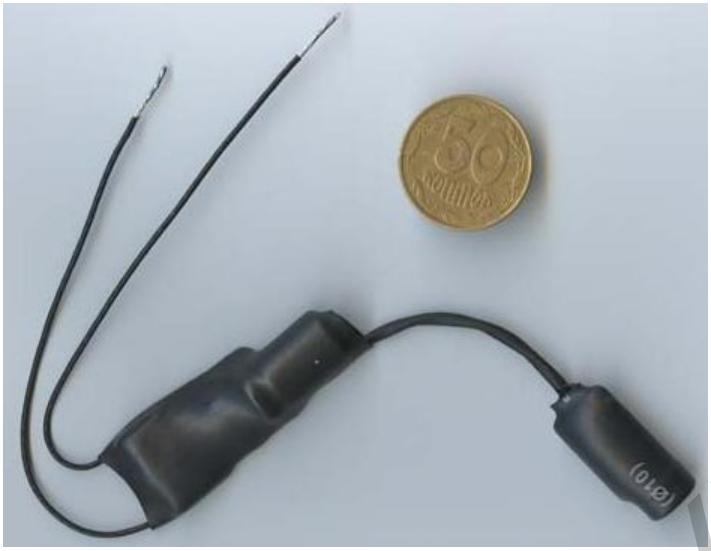


Рис. 3.4. Внешний вид закладного устройства типа «электронные уши»

Перехваченная ЗУ речевая информация может передаваться по радиоканалу, сети электропитания, оптическому каналу, телефонной линии, посторонним проводникам, инженерным коммуникациям в ультразвуковом диапазоне частот. Прием информации, передаваемой закладными устройствами, осуществляется, как правило, на специальные приемные устройства, работающие в соответствующем диапазоне длин волн.

Направленный микрофон – электронное устройство, обладающее высокими чувствительностью и помехоустойчивостью за счет его узкой диаграммы направленности (рис. 3.5).

Рис. 3.5. Внешний вид направленного микрофона ТМ-341

Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится

речевой источник, возникают вибрационные колебания. Таким образом, в своем первоначальном состоянии речевой сигнал в помещении присутствует в виде акустических и вибрационных колебаний. В данном случае строительные конструкции выполняют преобразование акустических колебаний в вибрационные и возникает виброакустический (вибрационный) канал утечки информации (рис. 3.6).

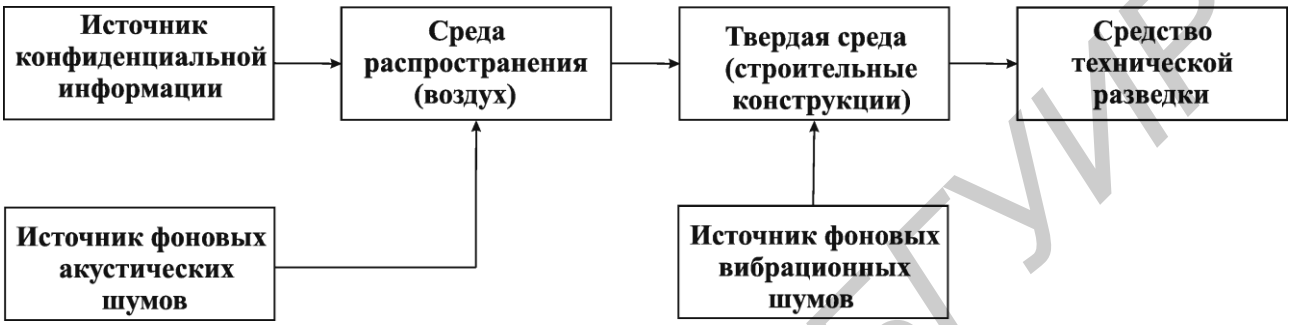


Рис. 3.6. Структурная схема виброакустического канала утечки информации

Перехват информации в виброакустических каналах обеспечивается электронными стетоскопами (рис. 3.7), выполняющими преобразование механических колебаний строительных конструкций (пол, потолок, стены) в электрические. В качестве преобразователей, подключаемых к электронному стетоскопу, используются акселерометры.

а б

Рис. 3.7. Внешний вид электронного стетоскопа (а) и подключаемых к нему преобразователей (б)

По виброакустическому каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал, поэтому такие устройства часто называют радиосте-

тоскопами. Возможно использование закладных устройств с передачей информации по инженерным коммуникациям (ультразвуковые колебания).

Акустоэлектрические каналы утечки информации возникают за счет преобразований акустических сигналов в электрические.

Некоторые элементы вспомогательных технических средств и систем, в том числе трансформаторы, катушки индуктивности, электромагниты звонков телефонных аппаратов и т. п. обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником речевого сигнала. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы, либо к модуляции токов, протекающих по этим элементам в соответствии с изменениями воздействующего акустического поля.

Вспомогательные технические средства и системы (ВТСС), кроме указанных элементов, могут содержать непосредственно акустоэлектрические преобразователи. К таким ВТСС относятся некоторые типы датчиков охранной и пожарной сигнализации, громкоговорители ретрансляционной сети и т. д. Эффект акустоэлектрического преобразования в специальной литературе называют «микрофонным эффектом».

Электромеханический вызывной звонок телефонного аппарата – типичный представитель индуктивного акустоэлектрического преобразователя, микрофонный эффект которого проявляется при положенной микротелефонной трубке (рис. 3.8).

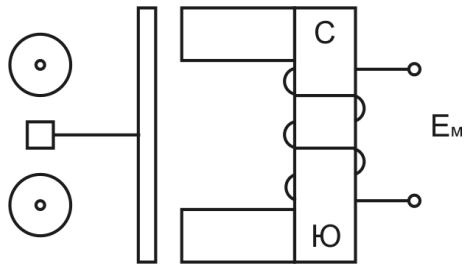


Рис. 3.8. Схема электромеханического звонка

Электродвижущая сила микрофонного эффекта звонка может быть определена по формуле

$$E_M = \eta p, \tag{3.1}$$

где p – акустическое давление;

η – акустическая чувствительность звонка.

Акустическая чувствительность звонка вычисляется по формуле

$$\eta = \frac{FS\mu_0\omega S_M}{d^2 Z_M}, \tag{3.2}$$

где F – магнитодвижущая сила постоянного магнита;

S – площадь якоря (пластины);

μ_0 – магнитная проницаемость сердечника;

ω – число витков катушки;

S_M – площадь плоского наконечника;

d – размер зазора;

Z_M – механическое сопротивление.

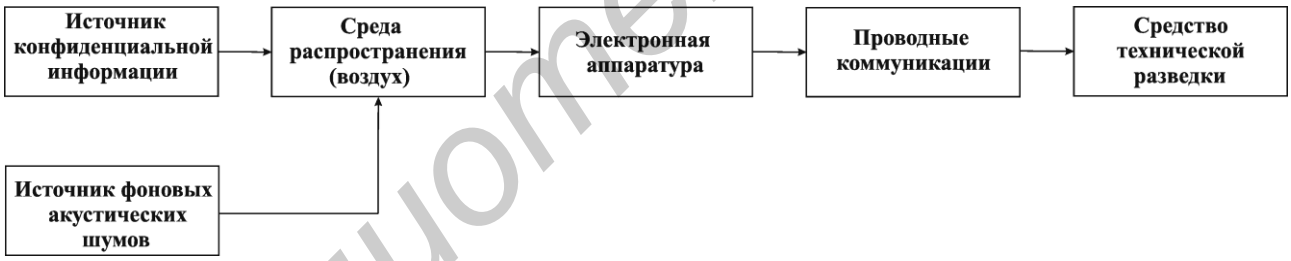


Рис. 3.9. Структурная схема акустоэлектрического канала утечки информации

Таким образом, речь воздействия на элементы электронной аппаратуры, содержащей в себе элементы, обладающие микрофонным эффектом, преобразуется ими в электрический сигнал. Если электронная аппаратура подключена к проводным коммуникациям, например к линии связи, то данный сигнал может быть перехвачен при подключении к такой линии, что обуславливает возникновение акустоэлектрического канала утечки информации (рис. 3.9).

Акустооптический канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих под действием речевого сигнала

отражающих поверхностей (отражатель-модулятор) помещений (оконных стекол, зеркал и т. д.). Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация (рис. 3.10).

Рис. 3.10. Структурная схема акустооптического канала утечки информации

Для перехвата речевой информации по данному каналу используются сложные лазерные системы, которые часто называют «лазерными микрофонами». Работают они, как правило, в ближнем инфракрасном диапазоне длин волн.

На рис. 3.11 приведен простейший вариант подобной системы: луч лазера падает на стекло окна под некоторым углом (например 45 градусов). На границе стекло–воздух происходит модуляция луча речевыми колебаниями. Отражённый луч принимается фотодетектором, расположенным с другой стороны окна под углом, равным углу падения луча лазера. Такая система требует тщательной юстировки.

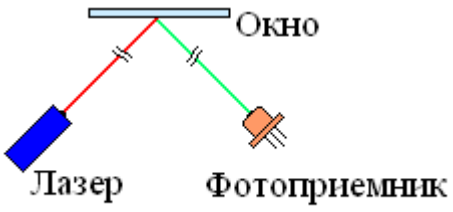


Рис. 3.11. Схема реализации лазерного микрофона

Второй способ, использующий сплиттер (делитель пучка) и приведенный на рис. 3.12, несколько сложнее, но он позволяет совместить лазер и детектор.

Отпадает необходимость в тщательной юстировке системы. Применение сплиттера позволяет свести падающий и отражённый луч в одну точку.

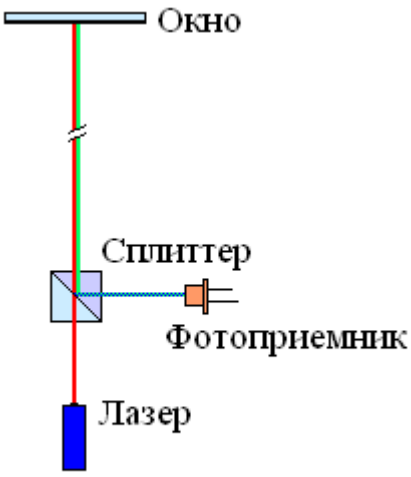


Рис. 3.12. Схема реализации лазерного микрофона с использованием сплиттера

Лазерные акустические системы дистанционного зондирования имеют дальность действия при приеме диффузноотраженного излучения до 100 м, при нанесении на стекла специального покрытия – более 300 м, а при установке на оконных стеклах триппель-призм – более 500 м.

Современная электронная техника (технические средства обработки информации) в своем составе содержит один или несколько генераторов для выработки стабильных опорных частот и т. д. В результате воздействия акустического поля на электронную аппаратуру меняется давление на все элементы высокочастотных генераторов технических средств передачи информации и ВТСС. При этом изменяется взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т. п., что может привести к изменениям параметров высокочастотного сигнала, например к модуляции его информационным сигналом. Поэтому этот канал утечки информации называется параметрическим (рис. 3.13).

Параметрический канал утечки информации может быть реализован и путем «высокочастотного облучения» помещения, где установлены закладные устройства, имеющие элементы, параметры которых (например добротность и

резонансная частота объемного резонатора) изменяются под действием акустического (речевого) сигнала.

Рис. 3.13. Структурная схема параметрического канала утечки информации

При облучении помещения мощным высокочастотным сигналом в таком закладном устройстве при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например четвертьволновым вибратором) происходит образование вторичных радиоволн, т. е. переизлучение электромагнитного поля (рис. 3.14).

Рис. 3.14. Структурная схема параметрического канала утечки информации

3.3. Материально-вещественный и визуально-оптический каналы утечки информации

Утечка информации по материально-вещественному каналу обусловлена хищением, копированием и ознакомлением с информацией, представленной на бумажном, электронном или каком-либо другом носителе.

Отраженный от объекта свет содержит информацию о внешнем виде (видовых признаках) объекта, а излучаемый объектом свет – о параметрах излучений (признаках сигналов). Запись информации производится в момент отражения падающего света путем изменения его яркости и спектрального состава.

Излучаемый свет содержит информацию об уровне и спектральном составе источников видимого света, а в инфракрасном диапазоне по характеристикам излучений можно также судить о температуре элементов излучения.

Визуально-оптический канал образуется вследствие получения информации путем применения различных оптических приборов, позволяющих уменьшить величину порогового контраста и увеличить контраст объекта на окружающем фоне.

3.4. Электромагнитные каналы утечки информации

Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве побочные электромагнитные излучения (ПЭМИ), которые в той или иной степени связаны с обрабатываемой информацией (электромагнитный канал).

Физические явления, лежащие в основе появления этих излучений, имеют различный характер, но тем не менее они могут рассматриваться как непреднамеренная передача конфиденциальной информации по некоторой «побочной системе связи», образованной источником излучения, средой и средством перехвата информации.

Регистрация средством технической разведки ПЭМИ источника информации (персональный компьютер и др.) распространяющихся через воздушную среду обусловливает возникновение индукционного канала утечки информации (рис. 3.15).

Кроме того, в индукционном канале используется эффект возникновения вокруг кабеля связи ПЭМИ при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками. Индукционные датчики применяются в основном для перехвата информации с симметричных высокочастотных кабелей.

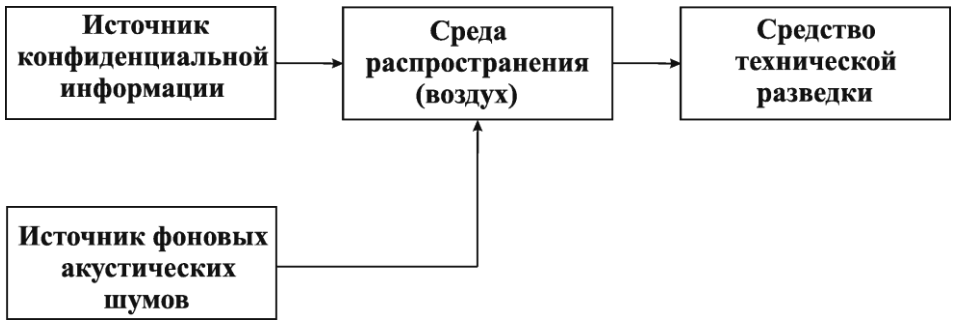


Рис. 3.15. Структурная схема индукционного канала утечки информации

Электрический канал утечки информации (рис. 3.16) возникает за счет наводок ПЭМИ технических средств обработки информации (ТСОИ) на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны (сеть электропитания, цепи охранной и пожарной сигнализации и т. д.). В этом случае наводка обусловлена тем, что данные проводники выступают в качестве случайных антенн (цепь ВТСС или посторонние проводники, способные принимать ПЭМИ).

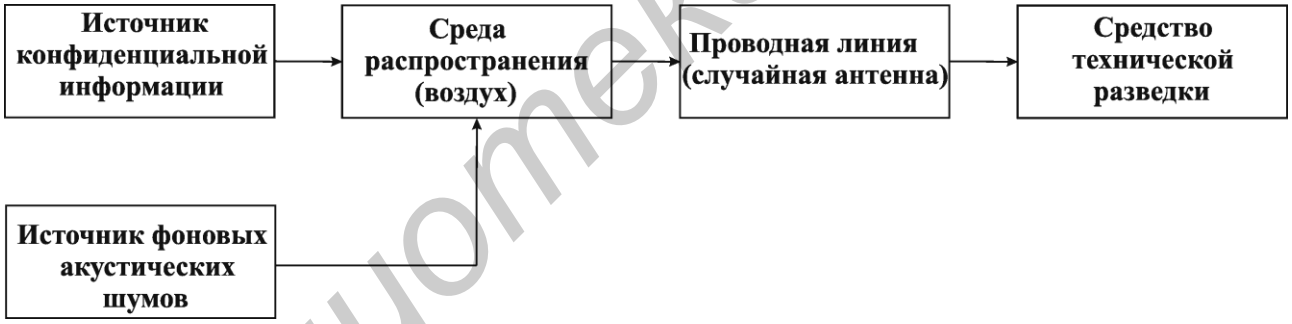


Рис. 3.16. Структурная схема электрического канала утечки информации

Наводки электромагнитных излучений ТСОИ возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСОИ и посторонних проводников или линий ВТСС. Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий ТСОИ и посторонних проводников.

Параметрический электромагнитный канал может возникать в процессе облучения ТСОИ побочными электромагнитными излучениями ВТСС, вследствие чего может произойти переизлучение электромагнитной волны, которое будет содержать информацию, обрабатываемую в ТСОИ.

3.5. Утечка информации по цепям заземления

Заземлением называется преднамеренное соединение объекта с заземляющим устройством, осуществляемое путем создания системы проводящих поверхностей и электрических соединений, предназначенных для выполнения различных функций.

Одной из причин попадания опасного (информационного) сигнала в систему заземления является наличие ПЭМИ – носителя информационного сигнала в местах расположения элементов системы. Это ПЭМИ будет наводить в расположенной поблизости системе заземления ток опасного сигнала.

Проникновение опасного сигнала в цепи заземления может быть связано с образованием так называемых контуров заземления. Рассмотрим два устройства, соединенные парой проводников, один из которых является сигнальным, а другой служит для протекания обратных токов (рис. 3.17).

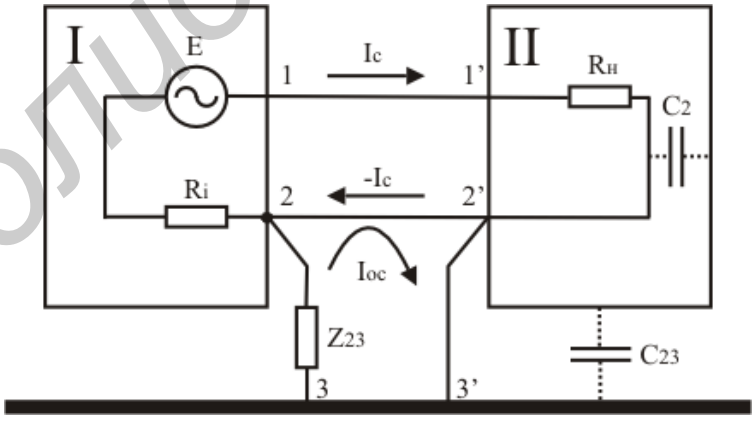


Рис. 3.17. Образование контуров заземления между двумя устройствами

Пусть возвратный проводник соединен с корпусом первого I устройства, а корпус – с землей. Если этот проводник соединен с корпусом второго II устройства, также имеющего электрический контакт с землей (соединение

2'–3'), то образуется замкнутый проводящий контур 2–2'–3'–3–2. Внешнее электромагнитное поле источника опасного сигнала наводит в этом контуре ЭДС, вызывая протекание тока $I_{\text{о.с}}$, который, в свою очередь, создает на участке 2–3 падение напряжения $U_{\text{о.с}}$ (опасного сигнала), равное

$$U_{\text{о.с}} = I_{\text{о.с}} \cdot Z_{2-3}, \qquad (3.3)$$

где $Z_{2–3}$ – сопротивление участка цепи 2–3.

Если отсутствует проводник 2'–3' или соединение проводника 2–2' с корпусом второго устройства, то возможность образования контура заземления полностью не исключается. В этих случаях контур может состоять из проводников 2–2', 3–3', земляной шины и паразитных емкостей между сигнальной цепью и корпусом второго устройства C_2, а также между корпусом второго устройства и землей $C_{2–3}$.

3.6. Утечка информации по цепям электропитания

Как правило, провода общей сети питания распределяются по различным помещениям, где расположены технические системы, и соединены с различными устройствами. Вследствие этого образуется нежелательная связь между отдельными техническими средствами. Кроме того, провода сети питания являются линейными антеннами, способными излучать или воспринимать электромагнитные поля. На практике значительная часть нежелательных наводок между удаленными друг от друга устройствами происходит с участием сети питания. При этом возможны различные ситуации. В случае асимметричной наводки, когда провода сети питания прокладываются вместе и имеют одинаковые емкости относительно источников и приемников наводки, в них наводятся напряжения, одинаковые по величине и по фазе относительно земли и корпуса приборов. На рис. 3.18 представлены действительная и эквивалентная схемы нежелательной асимметричной связи двух устройств, питающихся от общей сети.

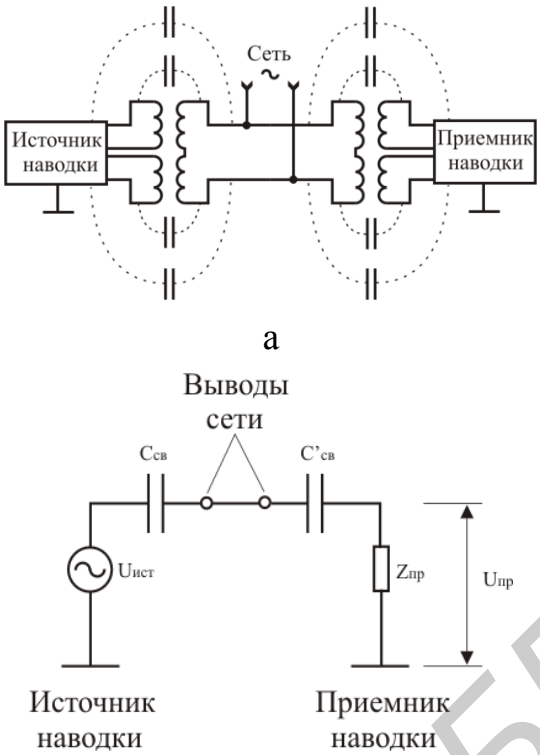


Рис. 3.18. Действительная (а) и эквивалентная (б) схемы нежелательной асимметричной связи двух устройств

На рис. 3.19 показан прием опасного сигнала через сеть питания, в которой наводятся напряжения за счет электромагнитного поля, излучаемого техническими средствами, а на рис. 3.20 показано излучение опасного сигнала через цепи питания источника наводки.

Все рассмотренные виды распространения наводок по сети питания являются асимметричными или однопроводными, поскольку оба провода сети питания передают сигнал наводки в одном направлении.

Симметричное распространение наводки имеет место в тех случаях, когда на проводах сети индуцируются различные напряжения относительно земли. Тогда между проводами образуется разность потенциалов, и по проводам сети проходят токи наводки в разных направлениях (рис. 3.21).

Вследствие этого в приемнике наводки индуцируются равные по величине и обратные по знаку напряжения. Поэтому симметрично распространяющаяся наводка не может проникнуть в высокочастотную часть приемника наводки. Проникновение симметричной наводки через силовой трансформатор

путем передачи напряжения, наведенного в первичной обмотке, во вторичную маловероятно вследствие существенных отличий частот сети питания и сигнала наводки.

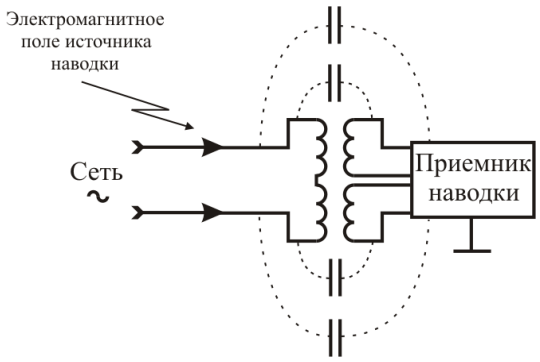


Рис. 3.19. Утечка информации по цепям электропитания за счет побочных электромагнитных наводок

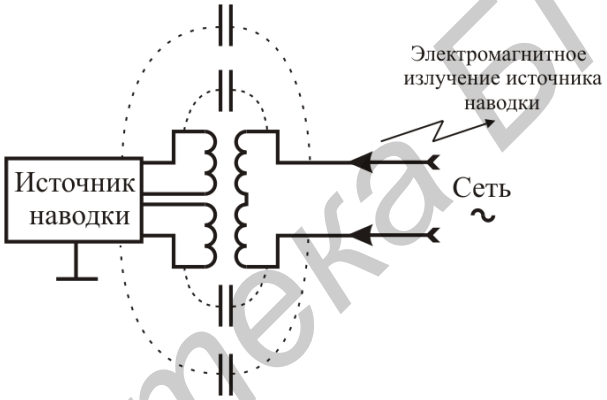


Рис. 3.20. Утечка информации по цепям электропитания за счет побочного электромагнитного излучения

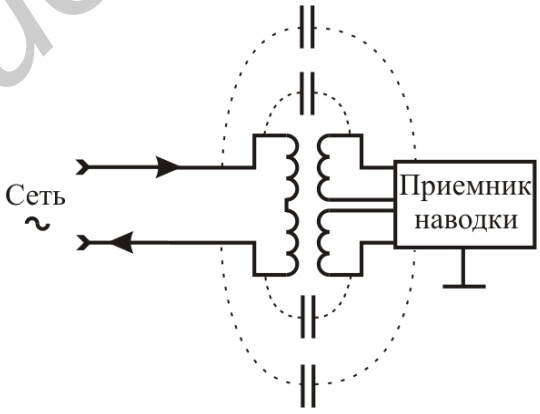


Рис. 3.21. Симметричное распространение наводки по цепям электропитания

Симметричное распространение наводки опасно только при асимметрии приемника наводки относительно проводов сети питания. Например, если в один из проводов сети питания ввести предохранитель, то провода сети будут

иметь разные емкости относительно приемника наводки. Через них будут передаваться напряжения, разность которых приведет к наводке в приемнике.

Одними из основных устройств, без которых невозможна работа любого технического средства, являются вторичные источники питания, предназначенные для преобразования энергии сети переменного тока или постоянного тока в энергию постоянного или переменного тока с напряжением, необходимым для питания аппаратуры технических средств.

При определенных условиях вторичные источники питания совместно с подводящими питающими линиями могут создавать условия для утечки информации, циркулирующей в техническом средстве. Несмотря на большое разнообразие конкретных технических решений схем построения таких источников питания, все они содержат в своем составе трансформаторы, выпрямители, сглаживающие фильтры, стабилизаторы и обладают конечным внутренним сопротивлением. При наличии в составе технических средств усилительных каскадов токи усиливаемых в них сигналов замыкаются через вторичный источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, изменяющееся в соответствии с законом изменения усиливаемого (опасного) сигнала.

При недостаточном затухании в фильтре источника питания это напряжение может быть обнаружено в питающей сети.

3.7. Перехват информации в телефонных каналах связи

Рассмотрим потенциальные возможности перехвата речевой информации, передаваемой по телефонным линиям. Телефонную систему связи можно представить в виде нескольких условных зон (рис. 3.22). К зоне «А» относится телефонный аппарат (ТА) абонента. Сигнал с аппарата по телефонному проводу попадает в распределительную коробку (РК) (зона «Б») и оттуда в магистральный кабель (зона «В»). После коммутации на автоматической телефонной станции (АТС) (зона «Г») сигнал распространяется по многоканальным кабелям

(зона «Д») до следующей автоматической телефонной станции (АТС). В каждой зоне имеются свои особенности по перехвату информации, но принципы, на которых построена техника несанкционированного подключения, практически не отличается (рис. 3.22).

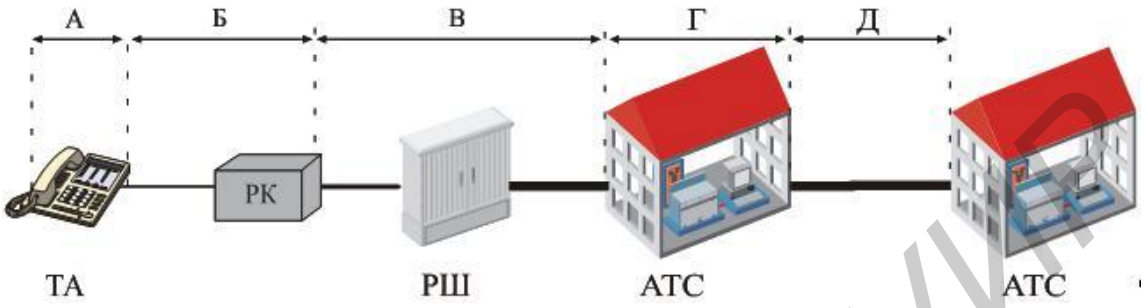


Рис. 3.22. Основные зоны перехвата информации в каналах телефонной связи

Наиболее опасными зонами, с точки зрения вероятности применения подслушивающих устройств, считаются зоны «А», «Б» и «В» (рис. 3.23).

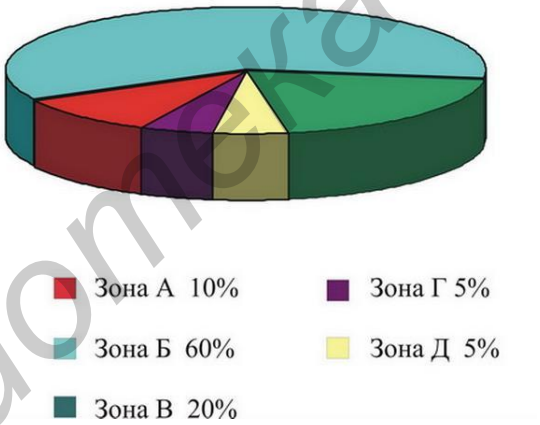


Рис. 3.23. Вероятность подключения к телефонному каналу связи в соответствующих зонах

Непосредственное подключение к линии – это самый простой и распространенный способ подслушивания телефонных разговоров. Для негосударственных организаций, занимающихся промышленным шпионажем, реально доступным местом подключения для перехвата информации являются зоны «А», «Б», «В». Подключение может быть:

– контактным;

– бесконтактным.

Шунт подслушивающего устройства в зонах «А» и «Б» может быть установлен в любом месте, где есть доступ к телефонным проводам или телефонному аппарату: в телефонной розетке или любом другом месте телефонной линии на всем ее протяжении вплоть до распределительной коробки.

В зоне «В» при использовании магистрального кабеля подключение подслушивающего устройства маловероятно. Это связано с тем, что для этого необходимо проникнуть в систему телефонной канализации, т. е. в систему подземных сооружений, состоящую из одной или нескольких объединенных в блоки труб и смотровых устройств (колодцев), предназначенную для прокладки кабеля, его монтажа и осмотра. Таким образом, необходимо не только разобраться в подземных коммуникациях, но и определить в многожильном кабеле нужную пару среди сотен и сотен ей подобных.

Способы и устройства для перехвата информации в зоне «А»:

– внедрение в телефонный аппарат передающих устройств, использующих для передачи голоса радиоканал или проводные линии. Такие устройства могут передавать как телефонные разговоры, так и речь в помещении и иметь как автономное питание, так и использовать напряжение телефонной линии;

– прослушивание акустических сигналов в помещении при помощи высокочувствительных приборов за счет паразитных акустоэлектрических преобразований в телефонном аппарате;

– прослушивание помещения при помощи «высокочастотного навязывания» телефонного аппарата, когда он сам становится модулятором навязываемого сигнала.

В техническом плане самым простым способом незаконного подключения в зоне «Б» и «В» является контактное параллельное подключение устройства перехвата.

Такой тип подключения имеет существенный недостаток для злоумышленника: его довольно легко можно обнаружить из-за сильного падения напряжения, приводящего к заметному ухудшению слышимости в основном теле-

фонном аппарате, что является следствием присоединения дополнительной нагрузки. В связи с этим более эффективным является подключение с помощью согласующего устройства (рис. 3.24). Такой способ не так сильно снижает напряжение в телефонной линии, что значительно затрудняет обнаружение факта подключения к линии как самим абонентом, так и с помощью аппаратуры контроля.

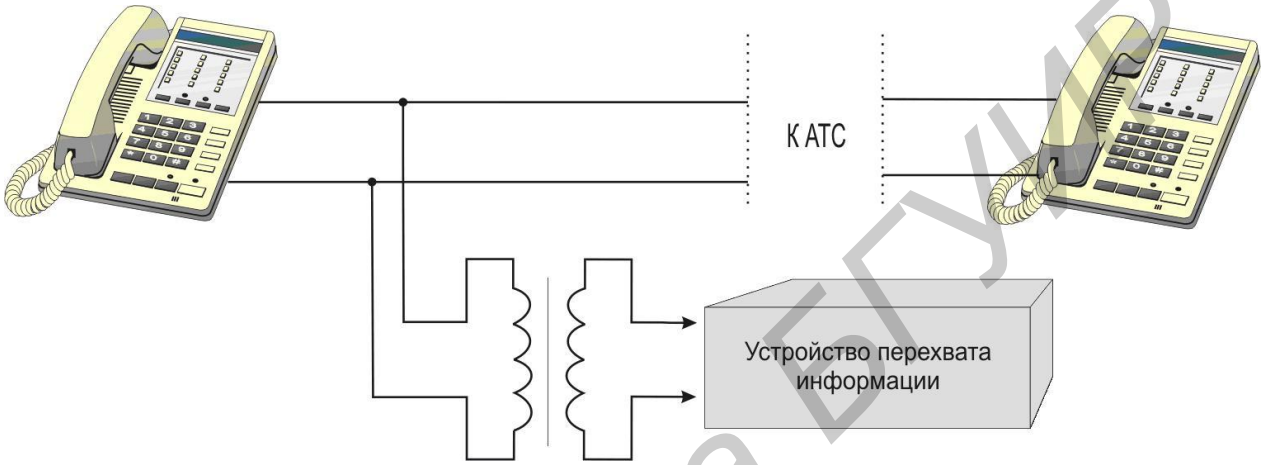


Рис. 3.24. Подключение к телефонной линии через согласующее устройство

Известен и способ контактного подключения к линиям связи с компенсацией падения напряжения. Устройство перехвата и компенсирующий источник напряжения при этом способе должны подключаться к линии последовательно (рис. 3.25). Общим недостатком всех видов контактного подключения для злоумышленника является необходимость нарушения целостности провода и влияние подключенного устройства на характеристики линии связи.

Наиболее скрытным является бесконтактный метод подключения, при этом для перехвата информации обычно применяется индуктивный датчик, выполненный в виде трансформатора (рис. 3.26). При этом два провода телефонного кабеля отделяются друг от друга и на одном из них закрепляется замкнутый магнитопровод датчика. Обычно для удобства установки магнитопровод делается из двух разделяющихся частей, которые соединяются при установке. Во время разговора по телефонной линии протекает электрический ток, пропорциональный звуковому давлению, которое создают своими голосовыми аппаратами абоненты. Этот ток одинаков для каждого телефонного провода, но

направлен в противоположные стороны. Вокруг каждого из проводов телефонной линии возникает переменное магнитное поле, пропорциональное переменному току. Магнитное поле от провода, охваченного магнитопроводом, создает в нем переменный магнитный поток, который наводит ЭДС в катушке, намотанной на одну из частей магнитопровода.

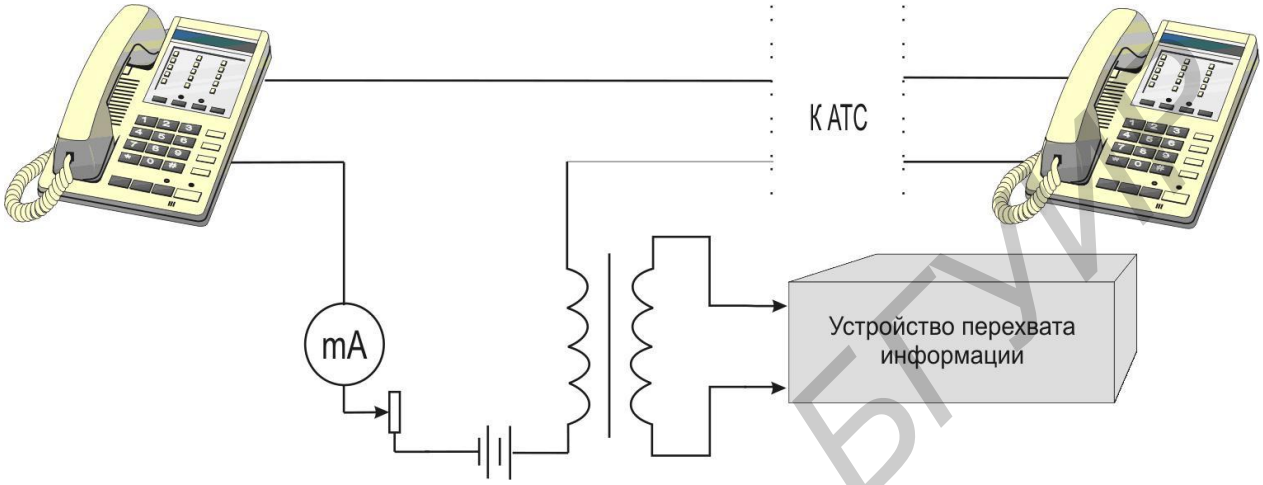


Рис. 3.25. Подключение к телефонной линии
с компенсацией падения напряжения

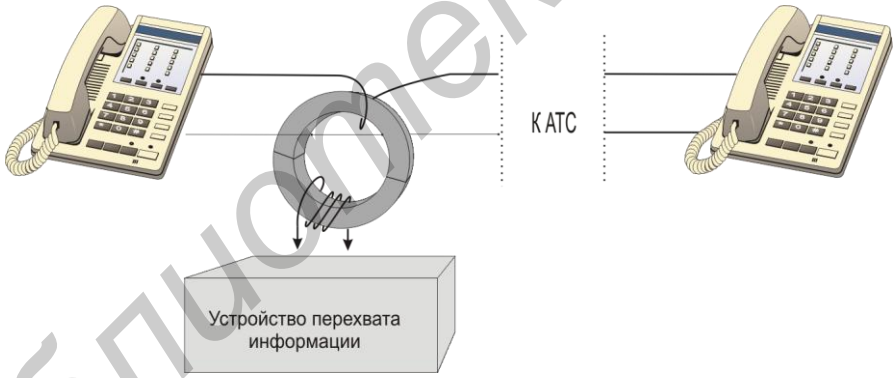


Рис. 3.26. Способ подключения к телефонной линии
с помощью индуктивного датчика

Принимаемый с этой катушки сигнал подается на вход усилителя, диктофона, радиозакладки или других типов подслушивающих устройств. Однако в этом случае для нормальной работы устройства необходим усилитель низкой частоты.

Противодействие устройствам перехвата информации подключаемых через индуктивный датчик, обеспечивается методом «выжигания». Он реализует-

ся путем подачи в телефонную линию высоковольтных (напряжение более 1500 В) импульсов, приводящих к электрическому тепловому пробою полупроводниковых приборов во входных каскадах электронных устройств перехвата информации и блоков их питания, гальванически подключенных к телефонной линии. Подача высоковольтных импульсов осуществляется при отключении телефонного аппарата от линии. При этом для уничтожения параллельно подключенных устройств подача высоковольтных импульсов осуществляется при разомкнутой, а последовательно подключенных устройств – при короткозамкнутой (как правило, в телефонной коробке или щите) телефонной линии.

3.8. Высокочастотное навязывание

Перехват обрабатываемой техническими средствами информации может осуществляться путем специальных воздействий на элементы технических средств. Одним из методов такого воздействия является высокочастотное навязывание, т. е. воздействие на технические средства высокочастотных сигналов. В настоящее время используются два способа высокочастотного навязывания:

1) посредством контактного введения высокочастотного сигнала в электрические цепи, имеющие функциональные или паразитные связи с техническим средством;

2) путем излучения высокочастотного электромагнитного поля. Возможность утечки информации при использовании высокочастотного навязывания связана с наличием в цепях технических средств нелинейных или параметрических элементов. Навязываемые высокочастотные колебания воздействуют на эти элементы одновременно с низкочастотными сигналами, возникающими при работе этих средств и содержащими конфиденциальные сведения. В результате взаимодействия на таких элементах высокочастотные навязываемые колебания оказываются промодулированными низкочастотными опасными сигналами. Распространение высокочастотных колебаний, модулированных опасными сиг-

налами, по токоведущим цепям или излучение их в свободное пространство создают возможность утечки речевой информации.

На рис. 3.27 представлена схема, иллюстрирующая принцип реализации высокочастотного навязывания в телефонном аппарате при положенной микротелефонной трубке (т. е. в ситуации, когда телефонный разговор не ведется и цепь питания микрофона разомкнута).

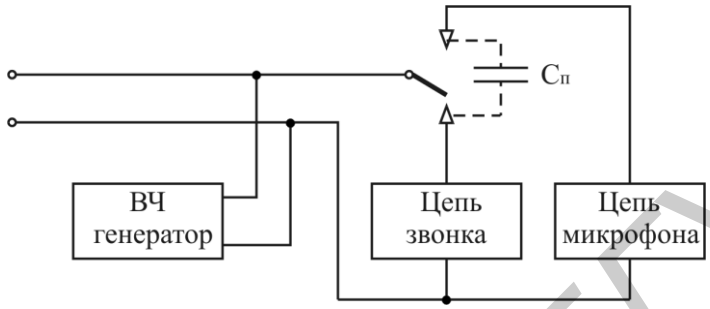


Рис. 3.27. Принцип реализации высокочастотного навязывания в телефонном аппарате

В рассматриваемом случае в телефонную линию подаются от специального высокочастотного генератора высокочастотные колебания с частотой более 100 кГц. Низкочастотные (опасные) сигналы формируются в ТСОИ на элементах, обладающих свойствами электроакустических преобразователей (звонок, микрофон и т. д.), которые преобразуют акустические сигналы (разговорную речь в помещении, где расположен телефонный аппарат) в электрические.

Несмотря на то что цепь микрофона телефонного аппарата разомкнута рычажным переключателем, между цепью микрофона и выходом линии существует паразитная емкость C_n порядка 5…15 пФ. На достаточно высоких частотах емкостное сопротивление этого переключателя будет относительно невысоким, поэтому навязываемые высокочастотные колебания через емкость C_n будут приложены к микрофону. Если в это время на микрофон действует достаточное звуковое давление опасного сигнала, обусловленное ведением разговоров в помещении, где расположен телефонный аппарат, то на выходе микрофона появится напряжение опасного сигнала. Происходит модуляция высоко-

частотных колебаний опасным речевым сигналом. Аналогичные явления наблюдаются и в звонковой цепи телефонного аппарата.

Излучение высокочастотных колебаний, промодулированных опасным сигналом, в свободное пространство осуществляется с помощью случайной антенны – телефонного провода. Промодулированный высокочастотный сигнал распространяется также в телефонной абонентской линии за пределы контролируемой территории. Следовательно, прием высокочастотных колебаний можно осуществлять либо путем подключения приемного устройства к телефонной линии, либо по полю.

3.9. Контрольные вопросы

1. Что называется техническим каналом утечки информации?
2. Какова особенность утечки речевой информации по акустическим каналам?
3. Чем обусловлена утечка информации в электромагнитных каналах?
4. Какие причины утечки информации по цепям заземления?
5. Что называется случайной антенной?
6. Чем обусловлены наводки в сети электропитания?
7. Какие выделяю зоны в телефонном канале связи с точки зрения подключения к нему для перехвата информации?
8. Охарактеризуйте типы подключений к линиям телефонной связи.
9. Какова цель высокочастотного навязывания?

4. ПАССИВНЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Пассивные методы защиты информации – предназначены для предотвращения или существенного затруднения перехвата информации по техническим каналам за счет снижения соотношения сигнал/шум на входе средства технической разведки путем уменьшения уровня сигнала.

4.1. Экранирование электромагнитных полей

Рассмотрим процесс экранирования электромагнитного поля при падении плоской волны на бесконечно протяженную металлическую пластину толщиной d, находящуюся в воздухе (рис. 4.1).

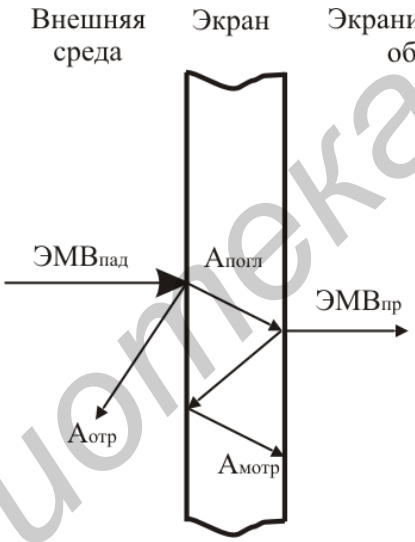


Рис. 4.1. Экранирование электромагнитного поля металлическим экраном

В этом случае на границе раздела двух сред с различными электрофизическими характеристиками (воздух–металл и металл–воздух) волна претерпевает отражение и преломление, а в толще экрана ввиду его проводящих свойств происходит частичное поглощение энергии электромагнитного поля. Таким образом, электромагнитная волна при взаимодействии с экраном отражается от его поверхности, частично проникает в стенку экрана, претерпевает поглощение в материале экрана, многократно отражается от стенок экрана и, в конечном счете, частично проникает в экранируемую область.

В результате общая эффективность экранирования (величина потерь энергии электромагнитной волны) металлической пластиной определяется суммой потерь за счет поглощения (затухания) энергии в толще материала $A_{погл}$, отражения энергии от границ раздела внешняя среда–металл и металл–экранируемая область $A_{отр}$ и многократных внутренних отражений в стенках экрана $A_{мотр}$:

$$A_{дБ} = A_{погл} + A_{отр} + A_{мотр}. \quad (4.1)$$

Потери на поглощение связаны с поверхностным эффектом в проводниках, приводящим к экспоненциальному уменьшению амплитуды проникающих в металлический экран электрических и магнитных полей.

Это обусловлено тем, что токи, индуцируемые в металле, вызывают омические потери и, следовательно, нагрев экрана.

Глубина проникновения δ определяется как величина, обратная коэффициенту затухания, и зависит от частоты: чем больше частота, тем меньше глубина проникновения. В СВЧ-диапазоне глубина проникновения δ в металлах имеет малую величину и тем меньше, чем больше проводимость металла и его магнитная проницаемость.

$$\delta = \frac{1}{\sqrt{\pi \mu f \sigma}}, \quad (4.2)$$

где μ – абсолютная магнитная проницаемость материала экрана;

f – частота электромагнитного поля;

σ – удельная проводимость материала экрана.

Выражение для определения потерь на поглощение экраном толщиной d может быть представлено в следующем виде:

$$A_{погл} = 8,68 d \sqrt{\frac{\omega \mu \sigma}{2}} = 8,68 \frac{d}{\delta}. \quad (4.3)$$

Таким образом, потери на поглощение растут пропорционально толщине экрана, магнитной проницаемости и удельной проводимости его материала, а также частоте электромагнитного поля.

Потери на отражение на границе раздела двух сред связаны с различными значениями полных характеристических сопротивлений этих сред. При прохождении волны через экран она встречает на своем пути две границы раздела: воздух–металл и металл–воздух.

Хотя электрическое и магнитное поля отражаются от каждой границы поразному, суммарный эффект после прохождения обеих границ одинаков для обеих составляющих поля. При этом наибольшее отражение при входе волны в экран (на первой границе раздела) испытывает электрическая составляющая поля, а при выходе из экрана (на второй границе раздела) наибольшее отражение испытывает магнитная составляющая поля. Для металлических экранов потери на отражение определяются выражением

$$A_{отр} = 20\lg\left(94{,}25\sqrt{\frac{\sigma}{\omega\mu}}\right). \qquad (4.4)$$

Откуда следует, что потери на отражение велики у экрана, изготовленного из материала с высокой проводимостью и малой магнитной проницаемостью.

Потери на многократные отражения в стенках экрана связаны с волновыми процессами в толще экрана и в основном определяются отражением от его границ. Для электрических полей почти вся энергия падающей волны отражается от первой границы (воздух–металл) и только небольшая ее часть проникает в экран. Поэтому многократными отражениями внутри экрана для электрических полей можно пренебречь.

Для магнитных полей большая часть падающей волны проходит в экран, в основном отражаясь только на второй границе (металл–воздух), тем самым создавая предпосылки к многократным отражениям между стенками экрана.

Корректирующий коэффициент $A_{мотр}$ многократного отражения для магнитных полей в экране с толщиной стенки d при глубине проникновения δ равен

$$A_{мотр} = 20\lg\left(1 - \exp\left(-\frac{2d}{y}\right)\right). \quad (4.5)$$

Величина $A_{мотр}$ имеет отрицательное значение, т. е. многократные отражения в толще экрана ухудшают эффективность экранирования. С уменьшением эффективности можно не считаться в случаях, когда на данной частоте выполняется условие $d > \delta$, но им нельзя пренебрегать при применении тонких экранов, когда толщина экрана меньше глубины проникновения.

4.2. Конструкции экранов электромагнитного излучения

Защита информации от утечки по электромагнитному каналу может быть обеспечена за счет снижения уровней ПЭМИ средств обработки информации при размещении их в экранированных помещениях, а также экранировании непосредственно таких средств.

Для изготовления экранов ЭМИ применяются различные материалы, объединяемые в единую конструкцию (рис. 4.2).

Выбор материала экрана проводится исходя из обеспечения требуемой эффективности экранирования в заданном диапазоне частот при определенных ограничениях. Эти ограничения связаны с массогабаритными характерными экрана, его влиянием на экранируемый объект, с механической прочностью и устойчивостью экрана против коррозии, с технологичностью его конструкции и т. д.

Под эффективностью экранирования будем понимать отношение действующих значений напряженности электрического поля E_1 (магнитного поля H_1) в данной точке при отсутствии экрана к напряженности электрического поля E_2 (магнитного поля H_2) в той же точке при наличии экрана:

$$Э_{0E} = \frac{E_1}{E_2}, \quad Э_{0H} = \frac{H_1}{H_2}. \tag{4.6}$$

Рис. 4.2. Классификация конструкций экранов электромагнитного излучения

Здесь эффективность выражается в относительных единицах (разах). На практике обычно данную величину представляют в логарифмических единицах – децибелах (дБ):

$$Э_{0E} = 20\lg\frac{E_1}{E_2}, \quad Э_{0H} = 20\lg\frac{H_1}{H_2}. \tag{4.7}$$

Однослойные конструкции экранов ЭМИ листовой формы и в виде сеток выполняются из разнообразных материалов (сталь, медь, алюминий, цинк, латунь), в том числе металлических. Металлические материалы удовлетворяют требованию устойчивости против коррозии при использовании соответствующих защитных покрытий.

Наиболее технологичными являются конструкции экранов из стали, так как при их изготовлении и монтаже можно широко использовать сварку. Толщина стали выбирается исходя из назначения конструкции экрана и условий

его сборки, а также из возможности обеспечения сплошных сварных швов при изготовлении.

Использование сетчатых экранов ЭМИ обеспечивает снижение их материалоемкости. В случае когда расстояние между микропроводом сетчатого экрана соответствует λ/2, он по своим экранирующим свойствам эквивалентен сплошному металлическому листу.

Сетчатые экраны ЭМИ могут изготавливаться путем машинной вязки полотна, в процессе которой совместно с ассистирующей нитью (рис. 4.3) в вязальное оборудование поступает микропровод, диаметр (рис. 4.4) и материал (рис. 4.5) которого влияет на экранирующие свойства формируемой таким образом конструкции. Эффективность экранирования данных материалов уменьшается с ростом частоты. Подобные конструкции характеризуются высоким коэффициентом отражения и обладают значительной стоимостью, вследствие использования металлов и их сплавов, что в значительной степени ограничивает их практическое использование.

Рис. 4.3. Схема расположения ассистирующей нити и микропровода (а) и внешний вид сетчатого экрана ЭМИ (б)

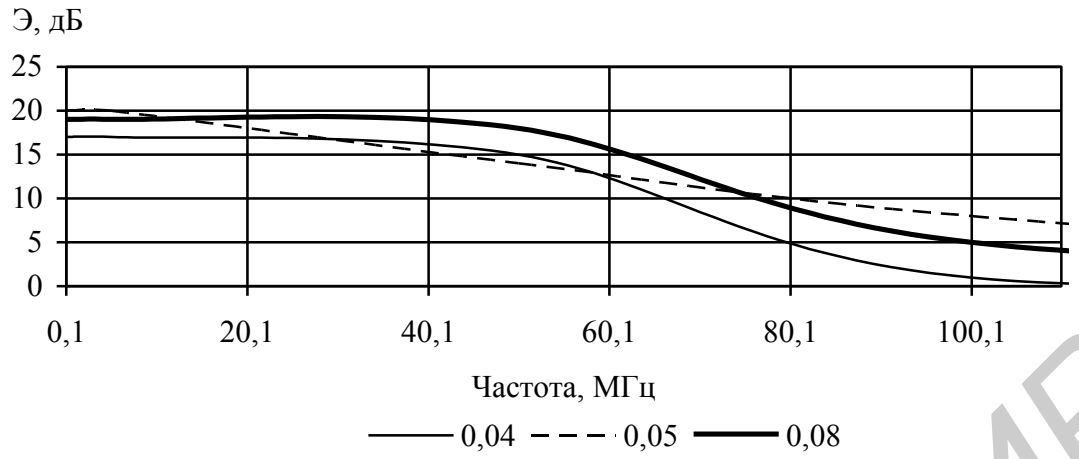


Рис. 4.4. Частотная зависимость эффективности экранирования для сетчатых экранов ЭМИ с различным диаметром микропровода

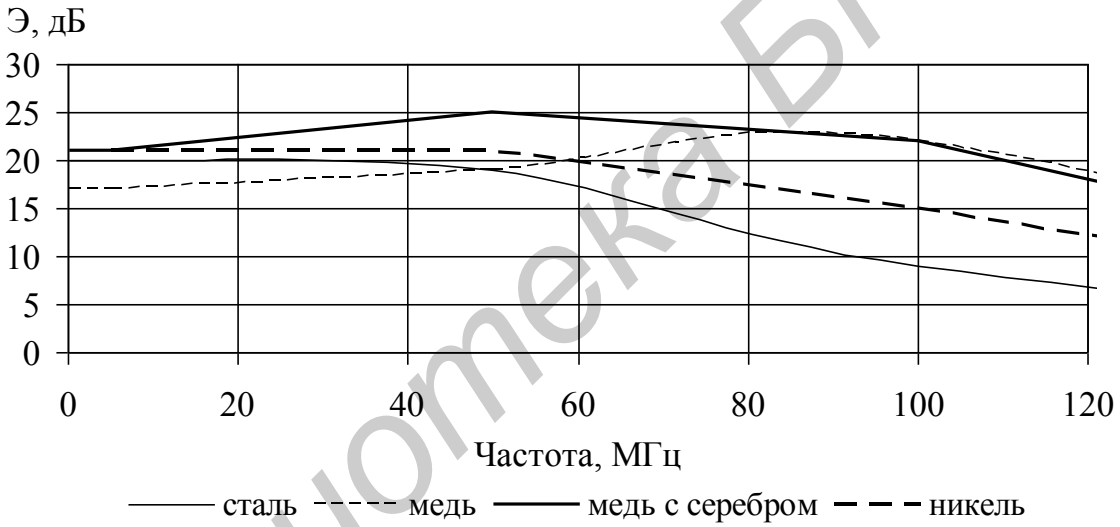


Рис. 4.5. Частотная зависимость эффективности экранирования для сетчатых экранов ЭМИ с микропроводом из различных материалов

Пониженным значением коэффициента отражения обладают экраны ЭМИ, конструктивно выполненные в виде четвертьволнового поглотителя, в котором радиопоглощающий материал (РПМ) находится на некотором расстоянии от отражающей ЭМВ поверхности. Поглощение достигает максимального значения на частоте, соответствующей длине волны, четверть которой равна расстоянию между верхней поверхностью поглощающего материала и отража-

ющей поверхностью, а также на всех ее высших нечетных гармониках (рис. 4.6).

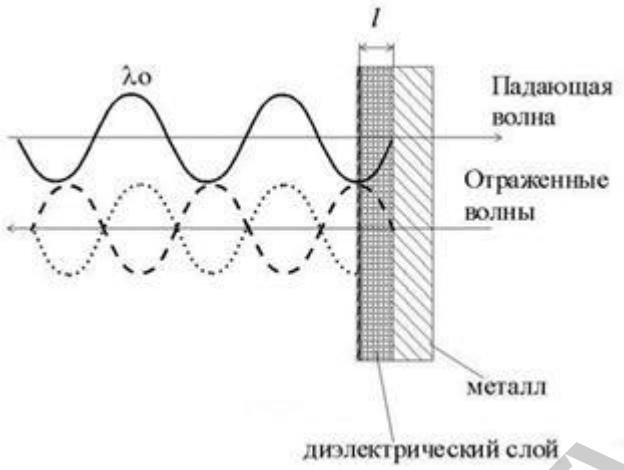


Рис. 4.6. Схема взаимодействия с ЭМИ четвертьволнового экрана

В настоящее время находят широкое применение четвертьволновые РПМ различного типа: резонансные, содержащие дипольные решетки, РПМ с плавно-неоднородным изменением параметров с толщиной покрытия, например диэлектрической проницаемости (рис. 4.7).

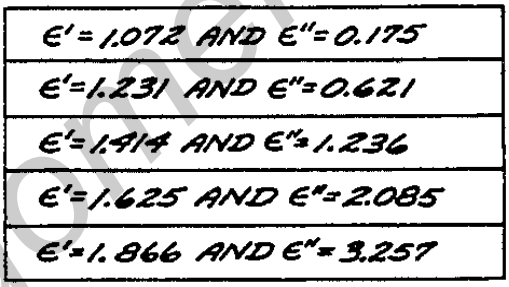


Рис. 4.7. Схематичное изображение градиентного экрана ЭМИ

Конструкции четвертьволновых экранов ЭМИ широко используются в технике. Они являются высокоэффективными с точки зрения подавления ЭМВ, но в узкой полосе частот, что обусловлено конструктивными их особенностями и представляется главным их недостатком.

Одной из важнейших задач, решаемых при создании РПМ, является уменьшение массы конструкции, что достигается путем использования порошкообразных материалов, в том числе магнитных.

Размер частиц и магнитная проницаемость порошкообразных материалов применяемых в конструкциях экранов ЭМИ, определяют их рабочий диапазон частот. Недостатком таких материалов, как и четвертьволновых РПМ, является их узкодиапазонность, а при использовании магнитных порошкообразных материалов – высокая стоимость.

Использование магнитных материалов в виде порошков, в том числе специальной формы, позволяет создавать эффективные экраны ЭМИ с граничной частотой до 10 ГГц, однако массовое практическое использование сдерживается их высокой стоимостью, обусловленной сложным технологическим процессом изготовления и дорогостоящим сырьем. Такие материалы, как правило, имеют значительную толщину, что является их недостатком.

Снижение толщины рабочего слоя РПМ достигается при совместном использовании проводящих и диэлектрических материалов, что приводит, как правило, к уменьшению механической прочности таких конструкций экранов ЭМИ. Устранение данного недостатка выполняется за счет применения композиционных материалов, получаемых путем закрепления вышеуказанных компонент А в связующем веществе В (рис. 4.8). Однако данные материалы, как правило, узкополосные и обладают значительной стоимостью.

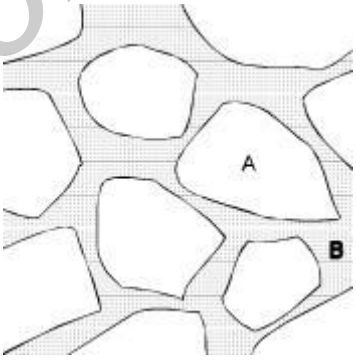


Рис. 4.8 – Схематичное изображение экрана ЭМИ, выполненного на основе композиционного материала

Для создания оптически прозрачных конструкций экранов ЭМИ используются стекла с токопроводящим покрытием. Такие экраны должны обеспечивать требуемую эффективность экранирования при ухудшении их оптических

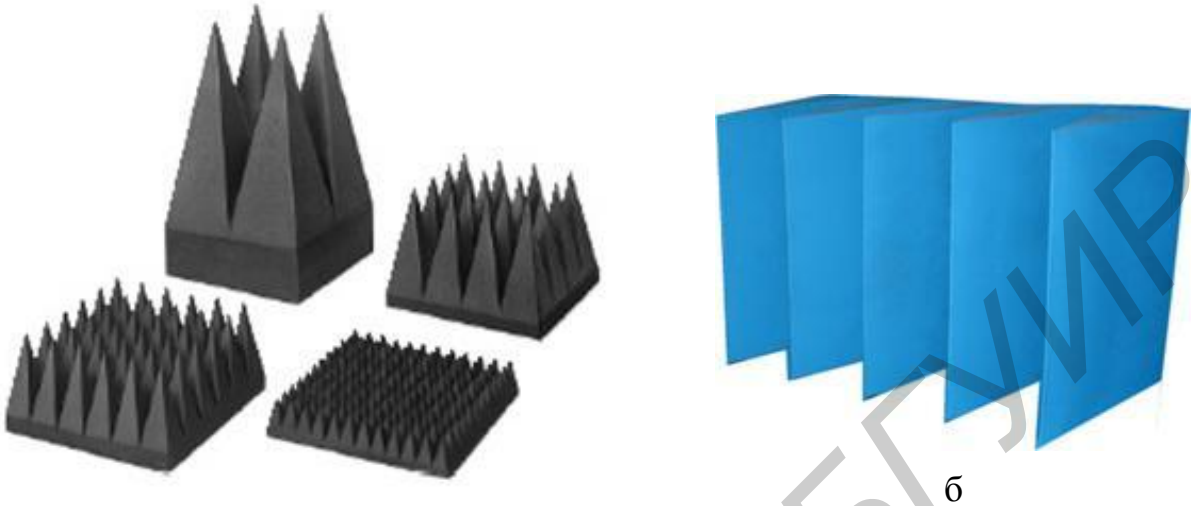
характеристик не ниже заданных граничных значений. Электрические и оптические свойства стекол с токопроводящим покрытием зависят от природы окислов, составляющих пленку, условий и методов ее нанесения и свойств самого стекла. Наибольшее распространение получили пленки на основе оксида олова, оксида индия – олова и золота, так как они обеспечивают наибольшую механическую прочность, химически устойчивы и плотно соединяются со стеклянной подложкой. Такие конструкции экранов используются для уменьшения уровня ЭМИ видеодисплейных терминалов (мониторов) (рис. 4.9), которое распространяется в сторону пользователя. Такие материалы могут использоваться для экранирования оконных проемов защищаемых помещений.

Рис. 4.9. Внешний вид экрана ЭМИ «Русский щит»
для видеодисплейного терминала

Создание широкодиапазонных экранов ЭМИ может быть также реализовано за счет выполнения их в виде многослойной конструкции, где каждый из слоев обладает определенным, отличным друг от друга комплексом свойств. Создание таких экранов ЭМИ в первую очередь приводит к увеличению толщины и веса конструкции, что не всегда оправдывается их эффективностью.

Формирование геометрических неоднородностей на поверхности экрана ЭМИ (пирамидальной, клиновидной формы) (рис. 4.10) позволяет обеспечить широкодиапазонность характеристик отражения. Взаимодействие с ЭМВ в подобных конструкциях обусловлено не только параметрами материала, из которого она изготовлена, но и сложной формой волноведущей поверхно-

сти (рис. 4.11). В таких конструкциях падающая ЭМВ преобразуется в поверхностную волну и по мере ее переотражения от неоднородностей поверхности ее энергия уменьшается.



а б

Рис. 4.10. Внешний вид фрагментов конструкций экранов ЭМИ с геометрическими неоднородностями поверхности пирамидальной (а) и клиновидной (б) формы

Рис. 4.11. Внешний вид фрагментов конструкций экранов ЭМИ со сложной формой волноведущей поверхности

Комбинированные конструкции экранов ЭМИ имеют, как правило, многослойную структуру, выполняемую с учетом принципов построения выше рассмотренных конструкций.

4.3. Фильтрация

Одним из методов локализации опасных сигналов, циркулирующих в технических средствах и системах обработки информации, является фильтрация. В источниках электромагнитных полей и наводок фильтрация осуществляется с целью предотвращения распространения нежелательных электромагнитных колебаний за пределы устройства – источника опасного сигнала. Фильтрация в устройствах – рецепторах электромагнитных полей и наводок – должна исключить их воздействие на рецептор.

В системах и средствах информатизации и связи фильтрация может осуществляться:

– в высокочастотных трактах передающих и приемных устройств для подавления нежелательных излучений – носителей опасных сигналов – и исключения возможности их нежелательного приема;

– различных сигнальных цепях технических средств для устранения нежелательных связей между устройствами и исключения прохождения сигналов, отличающихся по спектральному составу от полезных сигналов;

– цепях электропитания, управления, контроля, коммутации технических средств для исключения прохождения опасных сигналов по этим цепям;

– проводных и кабельных соединительных линиях для защиты от наводок;

– цепях пожарной и охранной сигнализации для исключения прохождения опасных сигналов и воздействия навязываемых высокочастотных колебаний.

Одна из возможных схем фильтрации опасных сигналов, создаваемых или воспринимаемых техническим средством по различным цепям, представлена на рис. 4.12.

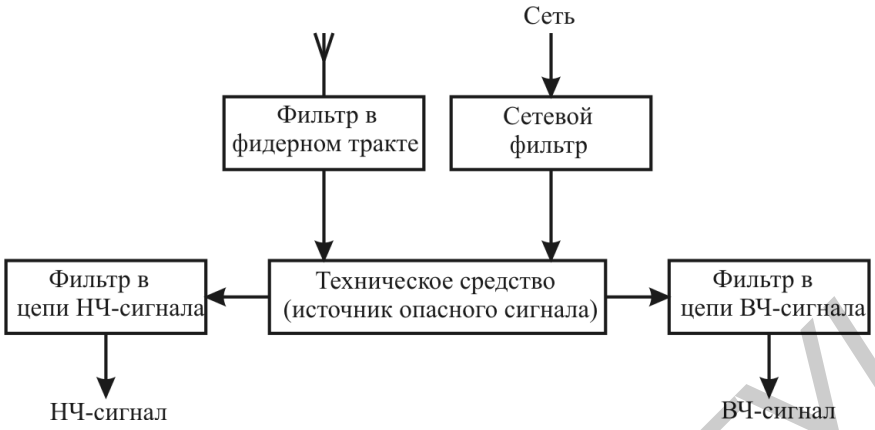


Рис. 4.12. Обобщенная схема фильтрации

Фильтрация в различных цепях осуществляется с помощью фильтров, дросселей и трансформаторов.

В целях фильтрации в технических средствах систем информатизации и связи широко используют различные фильтры (нижних и верхних частот, полосовые, заграждающие и т. д.). Основное назначение фильтра – пропускать без значительного ослабления сигналы с частотами, лежащими в рабочей полосе, и подавлять сигналы с частотами, лежащими за пределами этой полосы.

Количественно эффективность ослабления (фильтрации) нежелательных (в том числе и опасных) сигналов защитным фильтром оценивается в соответствии с выражением

$$\mathrm{A} = 20\lg\left(\frac{U_1}{U_2}\right) = 10\lg\left(\frac{P_1}{P_2}\right), \qquad (4.8)$$

где $U_1(P_2)$ – напряжение (мощность) опасного сигнала на входе фильтра;

$U_2(P_2)$ – напряжение (мощность) опасного сигнала на выходе фильтра при включенной нагрузке.

Основные требования, предъявляемые к защитным фильтрам, заключаются в следующем:

– величины рабочих напряжения и тока фильтра должны соответствовать величинам напряжения и тока цепи, в которой фильтр установлен;

– эффективность ослабления нежелательных сигналов должна быть не меньше заданной в защищаемом диапазоне частот;

– ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным, не влияющим на качество функционирования системы;

– габариты и масса фильтров должны быть, по возможности, минимальными;

– фильтры должны обеспечивать функционирование при определенных условиях эксплуатации (температура, влажность, давление, удары, вибрация и т. д.);

– конструкции фильтров должны соответствовать требованиям техники безопасности.

К фильтрам цепей питания наряду с общими предъявляются следующие дополнительные требования:

– затухание, вносимое такими фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть незначительным (например 0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая в зависимости от конкретных условий может быть достаточно широкой (до 10^{10} Гц);

– сетевые фильтры должны эффективно работать при больших проходящих токах, высоких напряжениях и высоких уровнях мощности рабочих и подавляемых электромагнитных колебаний;

– ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими (например уровни гармонических составляющих напряжения питания с частотами выше 10 кГц должны быть на 80 дБ ниже уровня основной гармоники).

Фильтры нижних частот. Фильтр, у которого полоса прозрачности находится в пределах от ω = 0 (постоянный ток) до некоторой граничной частоты ω_n, называется фильтром нижних частот (ФНЧ) (рис. 4.13, а).

Полоса прозрачности (пропускания) фильтра – полоса частот, в которой ослабление сигнала фильтром составляет не более 3 дБ.

Фильтры верхних частот. Фильтр, у которого полоса прозрачности занимает все частоты выше некоторой определенной граничной частоты ω_n, называется фильтром верхних частот (ФВЧ). В таком фильтре постоянный ток и все колебания с частотами ниже определенной граничной частоты должны задерживаться, а колебания частот $\omega > \omega_n$ – пропускаться (рис. 4.13, б).

Полосовые фильтры. Полосовые фильтры (ПФ) характеризуются тем, что обе частоты ω_{n1}, и ω_{n2} ограничивающие полосу прозрачности, конечны и ни одна из них не равна нулю (рис. 4.13, в).

В ряде случаев ставится задача задержания определенной полосы частот и в то же время пропускания всех остальных частот. Такая задача решается **заграждающим фильтром (ЗФ)** (рис. 4.13, г).

С точки зрения конструктивного исполнения фильтры могут быть выполнены на элементах с сосредоточенными параметрами (фильтры, предназначенные для работы на частотах до 300 МГц) и на элементах с распределенными параметрами (коаксиальные, волноводные, полосковые, применяемые на частотах выше 1 ГГц). В диапазоне частот 300 МГц…1 ГГц могут использоваться фильтры, включающие элементы как с сосредоточенными, так и с распределенными параметрами.

Разделительные трансформаторы. Должны обеспечивать развязку первичной и вторичной цепей по сигналам наводки. Это означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки. Проникновение наводок во вторичную обмотку объясняется наличием нежелательных резистивных и емкостных цепей связи между обмотками.

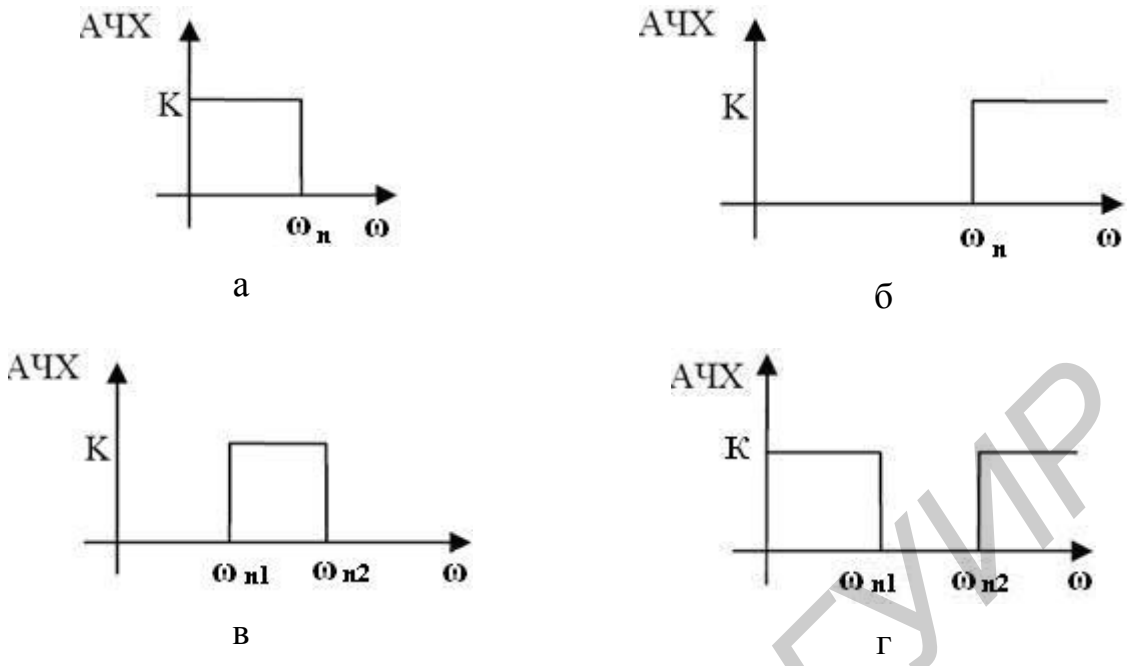


Рис. 4.13. Амплитудно-частотные характеристики ФНЧ (а), ФВЧ (б), ПФ (в), ЗФ (г)

Для уменьшения связи обмоток по сигналам наводок часто применяется внутренний экран, выполняемый в виде заземленной фольги, укладываемой между первичной и вторичной обмотками. С помощью этого экрана наводка, действующая в первичной обмотке, замыкается на землю.

Разделительные трансформаторы используются с целью решения ряда задач, в том числе для:

– разделения по цепям питания источников и рецепторов наводки, если они подключаются к одним и тем же шинам переменного тока;

– устранения асимметричных наводок;

– ослабления симметричных наводок в цепи вторичной обмотки, обусловленных наличием асимметричных наводок в цепи первичной обмотки.

4.4. Заземление технических средств

Основные требования, предъявляемые к системе заземления, заключаются в следующем:

– система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с объектом;

– сопротивления заземляющих проводников, а также земляных шин должны быть незначительными;

– каждый заземляемый элемент должен быть присоединен к заземлителю или к заземляющей магистрали при помощи отдельного ответвления. Последовательное включение в заземляющий проводник нескольких заземляемых элементов запрещается;

– в системе заземления должны, по возможности, отсутствовать замкнутые контуры, образованные соединениями или нежелательными связями между сигнальными цепями и корпусами устройств, между корпусами устройств и землей;

– следует избегать использования общих проводников в системах экранирующих заземлений, защитных заземлений и сигнальных цепей;

– качество электрических соединений в системе заземления должно обеспечивать минимальное сопротивление контакта, надежность и механическую прочность контакта в условиях климатических воздействий и механических нагрузок;

– контактные соединения должны исключать возможность образования оксидных пленок на контактирующих поверхностях и связанных с этими пленками нелинейных явлений;

– контактные соединения должны исключать возможность образования гальванических пар для предотвращения коррозии в цепях заземления;

– запрещается использовать в качестве заземляющего устройства нулевые фазы электросетей, металлоконструкции зданий, трубы систем отопления, водоснабжения, канализации и т. д.

Комплексные сопротивления заземляющих проводников должны обладать минимальными активным сопротивлением и собственной индуктивностью. Поэтому заземляющие проводники должны иметь минимально возможную длину $l_з$, которая значительно меньше длины волны электромагнитного поля

λ – источника наводки. На практике должно выполняться условие $l_з < 0{,}02\lambda$. Для уменьшения сопротивления форма и размеры поперечного сечения заземляющих проводников должны выбираться таким образом, чтобы на частоте наводки обеспечивались малые активное и реактивное сопротивления. Сопротивление заземления этих средств не должно превышать 4 Ом.

Для устранения замкнутых контуров в системе заземления используют различные методы. На рис. 4.14 представлены три способа разрыва нежелательных контуров в цепях заземления: а) – с помощью разделительных трансформаторов; б) – с помощью дросселей, работающих в синфазном режиме, в) – с помощью оптронов.

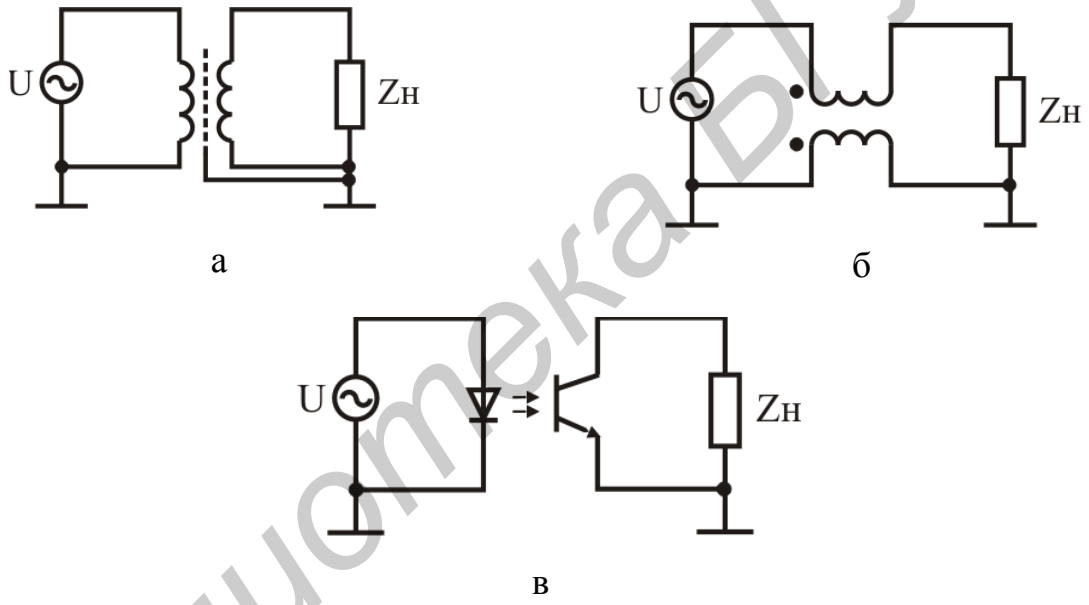


Рис. 4.14. Способы разрыва нежелательных контуров в цепях заземления

В целях исключения использования общих проводников в системах различных заземлений можно изолировать друг от друга цепи возврата сигнальных токов, цепи возврата постоянных токов питания и цепи возврата переменных токов питания. В этом случае необходимо построить систему заземления, состоящую из трех независимых контуров, сходящихся в одной точке. Такой подход позволяет оптимизировать каждую заземляющую цепь в отдельности. Например, цепи заземления схем распространения сигналов в диапазоне частот до нескольких мегагерц должны иметь низкое сопротивление и по ним должен

течь маленький ток. Заземляющая цепь источников питания постоянного тока должна быть рассчитана на низкое сопротивление, но на значительно больший ток, а заземления источников питания по сети переменного тока должны иметь низкое сопротивление и выдерживать токи в сотни ампер.

4.5. Звукоизоляция помещений

Защита речевой информации от утечки по акустическим каналам может быть реализована за счет создания защищенных методом звукоизоляции помещений.

Выделение акустического сигнала на фоне естественных шумов происходит при определенных соотношениях сигнал/шум. Производя звукоизоляцию, добиваются его снижения до предела, затрудняющего (исключающего) возможность выделения речевых сигналов, проникающих за пределы контролируемой зоны по акустическому или виброакустическому (ограждающие конструкции, трубопроводы) каналам.

Для сплошных, однородных, строительных конструкций ослабление акустического сигнала, характеризующее качество звукоизоляции на средних частотах, рассчитывается по формуле

$$K = 20\lg\ q_{\text{ог}} f\ \ - 45,7, \qquad (4.9)$$

где $q_{\text{ог}}$ – масса 1 м^2 ограждения, кг;

f – частота звука, Гц.

При выборе ограждающих конструкций выделенных помещений в процессе проектирования необходимо руководствоваться следующими правилами:

– в качестве перекрытий рекомендуется использовать акустически неоднородные конструкции;

– в качестве полов целесообразно использовать конструкции на упругом основании или конструкции, установленные на виброизоляторы;

– потолки целесообразно выполнять подвесными, звукопоглощающими со звукоизолирующим слоем;

– в качестве стен и перегородок предпочтительно использование многослойных акустически неоднородных конструкций с упругими прокладками (резина, пробка, ДВП, МВП и т. п.).

Прохождение волн через препятствия осуществляется различными путями:

– через поры, окна, щели, двери и т. д. (путем воздушного переноса);

– через материал стен, по трубам тепло-, водо- и газоснабжения и т. д. за счет их продольных колебаний (путем материального переноса);

– через материал стен и перегородок помещения за счет их поперечных колебаний (путем мембранного переноса).

Звукоизоляция помещений обеспечивается за счет использования звукопоглощающих материалов – имеющих сквозную пористость и относительно высокий коэффициент звукопоглощения (более 0,2) и обладающих динамическим модулем упругости не более 150 кгс/см^2.

По форме звукопоглощающие материалы разделяют на штучные (блоки, плиты), рулонные (маты, полосовые прокладки, холсты), рыхлые и сыпучие (вата минеральная, стеклянная, керамзит, шлак).

По величине относительного сжатия (жесткости) звукопоглощающие и звукоизоляционные строительные материалы подразделяются на мягкие, полужесткие и твердые.

Мягкие звукопоглощающие материалы изготавливают на основе минеральной ваты или стекловолокна с минимальным объемом (до 3 % по массе) связующего или без него. К ним относятся маты или рулонные полотна с объёмной массой до 70 кг/м^3, которые обычно применяются в сочетании с защитными перфорированными листовыми экранами (алюминий, гипсокартон, жесткий ПВХ) или с покрытием пористой плёнкой. Коэффициент звукопоглощения этих материалов на средних частотах (250…1000 Гц) достигает значений 0,7…0,95.

Рис. 4.15. Внешний вид минераловатного мата М1-100

Полужесткие материалы включают в себя минераловатные или стекловолокнистые плиты с объёмной массой 80…130 кг/м^3 при содержании синтетического связующего 10…15 % по массе (рис. 4.16), а также древесно-волокнистые плиты с объёмной массой 180…300 кг/м^3. Поверхность плит покрывается пористой краской или плёнкой. Коэффициент звукопоглощения полужёстких материалов на средних частотах составляет 0,5…0,75. Сюда входят звукопоглощающие материалы с ячеистым строением – пенополиуретан, полистирол, а также базальтовые звукопоглощающие маты, получаемые из очень тонкого базальтового волокна с покрытием из стеклоткани.

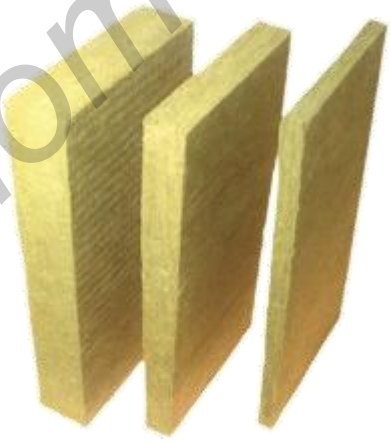


Рис. 4.16. Внешний вид минераловатных плит П-75

У **твердых материалов** объемная масса составляет 300…400 кг/м^3 и коэффициент звукопоглощения порядка 0,5. Их производят на основе гранулированной или суспензированной минеральной ваты и коллоидного связующего.

К ним относятся материалы, в состав которых входят пористые заполнители (вспученный перлит, вермикулит, пемза).

Звукопоглощающая способность материалов обусловлена их пористой структурой и наличием большого числа открытых сообщающихся между собой пор, максимальный диаметр которых обычно не превышает 2 мм (общая пористость должна составлять не менее 75 % по объёму). Большая удельная поверхность материалов, создаваемая стенками открытых пор, способствует активному преобразованию энергии звуковых колебаний в тепловую энергию вследствие потерь на трение.

Обычно пористые материалы используют в сочетании со сплошными. Один из распространенных видов пористых материалов – облицовочные звукопоглощающие материалы. Их изготавливают в виде плоских плит или рельефных конструкций (пирамид, клиньев и т. д.), располагаемых или вплотную или на небольшом расстоянии от сплошной строительной конструкции (стены, перегородки, ограждения и т. п.).

Отдельную группу звукопоглощающих материалов составляют резонансные поглотители. Они подразделяются на мембранные и резонаторные. **Мембранные поглотители** представляют собой натянутый холст (ткань), тонкий фанерный (картонный) лист, под которым располагают хорошо демпфирующий материал (материал с большой вязкостью — например поролон, губчатую резину, строительный войлок и т. д.). В такого рода поглотителях максимум поглощения достигается на резонансных частотах.

Перфорированные **резонаторные поглотители** представляют собой систему воздушных резонаторов, в устье которых расположен демпфирующий материал. Наиболее распространенными являются перфорированные плиты (рис. 4.17), которые монтируются на некотором расстоянии от твердой стены.

Рис. 4.17. Внешний вид фрагмента перфорированной плиты СМЛ-ППГЗ

Повышение звукоизоляции стен и перегородок помещений достигается применением слоистых или раздельных их конструкций. В многослойных перегородках и стенах целесообразно подбирать материалы слоев с резко отличающимися акустическими сопротивлениями (например бетон–поролон).

Основными конструктивными параметрами, определяющими звукоизолирующую способность многослойных конструкций, являются материал и толщина обшивок, вид каркаса и способ крепления к нему обшивок, толщина промежутка между слоями, вид звукопоглощающего материала и степень заполнения им промежутка.

Звукоизолирующая способность сложных стен, имеющих дверные и оконные проемы, зависит от звукоизоляции дверей и окон. Увеличение звукоизолирующей способности дверей достигается плотной пригонкой полотна дверей к коробке, устранением щелей между дверью и полом, применением уплотняющих прокладок, обивкой или облицовкой полотен дверей специальными материалами и т. д. При недостаточной звукоизоляции однослойных дверей используются двойные двери с тамбуром, облицованные звукопоглощающим материалом.

Звукопоглощающая способность окон, так же как и дверей, зависит главным образом от поверхностной плотности стекла и прижатия притворов. Обычные окна с двойными переплетами обладают более высокой (на 4…5 дБ) звукоизолирующей способностью по сравнению с окнами со спаренными переплетами. Применение упругих прокладок значительно улучшает звукоизоляционные качества окон. В случаях когда необходимо обеспечить повышенную

звукоизоляцию, применяют окна специальной конструкции (например, двойное окно с заполнением оконного проема органическим стеклом толщиной 20…40 мм и с воздушным зазором между стеклами не менее 100 мм). Повышенное звукопоглощение обеспечивается применением конструкции окон на основе стеклопакетов с герметизацией и заполнением зазора между стеклами различными газовыми смесями.

Между помещениями зданий и сооружений проходит много технологических коммуникаций (трубы тепло-, газо-, водоснабжения и канализации, кабельная сеть энергоснабжения, вентиляционные короба и т. д.). Для них в стенах и перекрытиях сооружений делают соответствующие отверстия и проемы. Их надежная звукоизоляция обеспечивается применением специальных гильз, прокладок, глушителей, вязкоупругих заполнителей и т. д. Обеспечение требуемой звукоизоляции в вентиляционных каналах достигается использованием акустических фильтров и глушителей.

Во временно используемых помещениях используют складные экраны. Применение звукопоглощающих материалов, преобразующих кинетическую энергию звуковой волны в тепловую, имеет некоторые особенности, связанные с необходимостью создания оптимального соотношения прямого и отраженного от преграды акустических сигналов. Чрезмерное звукопоглощение снижает уровень сигнала, большое время реверберации приводит к ухудшению разборчивости речи.

4.6. Контрольные вопросы

1. Какие эффекты наблюдаются при взаимодействии электромагнитной волны с металлическими экранами электромагнитного излучения?

2. Как влияет соотношение толщины и глубины проникновения электромагнитной волны в металлический экран электромагнитного излучения на его эффективность экранирования?

3. Какие технические характеристики материалов обуславливают их выбор для использования в конструкциях электромагнитных экранах?

4. Какими преимуществами обладают сетчатые металлические экраны электромагнитного излучения над сплошными?

5. Какие конструкции электромагнитных экранов обладают наименьшим коэффициентом отражения?

6. Какие материалы используются при создании однослойных экранов и каково их влияние на их экранирующие свойства?

7. Какие конструкции электромагнитных экранов имеют широкий рабочий диапазон частот?

8. Каким образом обеспечивается локализация наводок в проводных линиях?

9. Охарактеризуйте способы устранения замкнутых контуров в системах заземления.

10. Какие способы распространения акустических волн через твердые среды Вы знаете?

11. Какие материалы относят к мягким, полужестким и твердым звукоизоляционным?

12. Какими конструктивными параметрами определяется звукоизолирующая способность многослойных конструкций звукоизолирующих материалов?

13. Чем определяется звукоизоляция сложных стен?

14. Каким образом обеспечивается звукоизоляция технологических коммуникаций?

5. АКТИВНЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Активные методы защиты информации – предназначены для предотвращения или существенного затруднения перехвата информации по техническим каналам за счет снижения соотношения сигнал/шум на входе средства технической разведки путем уменьшения уровня шума.

5.1. Акустическая маскировка

Мероприятия акустической маскировки позволяют обеспечить:

– неузнаваемость голоса диктора;

– существенное снижение неразборчивости речи диктора;

– скрыть факт передачи речевой информации.

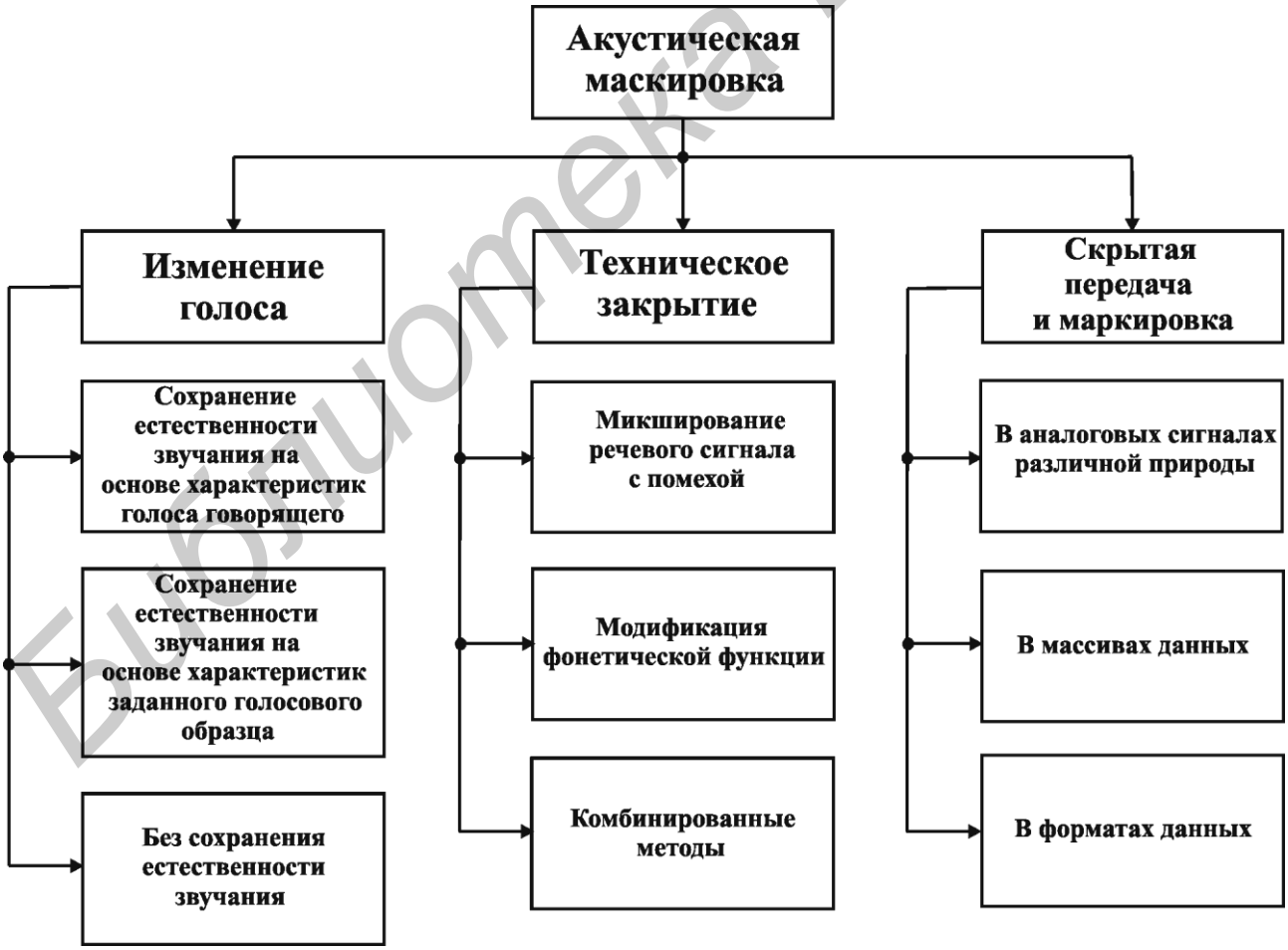


Рис. 5.1. Классификация методов акустической маскировки

Реализация первого направления позволяет обеспечить неузнаваемость голоса диктора, что затрудняет его идентификацию. Это достигается путем изменения или генерации тех или иных параметров речевого сигнала (характеристики четырех формантных областей (средняя частота, частотный диапазон, энергия), огибающая спектра и т. д.). Изменение голоса диктора в данном случае может обеспечиваться при сохранении естественности ее звучания за счет использования некоторых характеристик голоса диктора или заданного голосового образца. При отсутствии естественности звучания голос имеет механический оттенок.

Под техническим закрытием речи будем понимать технологии маскирования речи, относящиеся к методам и средствам смысловой защиты речевой информации и имеющие цель обеспечения неразборчивости защищаемого речевого сообщения. Их реализация на практике может быть выражена в микшировании речи шумами и помехами и/или в модификации речевого сигнала по вычисляемым из его описаний параметрам по заранее известному закону преобразования (закрытия–восстановления). При микшировании речевого сигнала с помехой необходимо обеспечить превышение ее уровнем уровня речи.

Под модификацией речи будем понимать такое преобразование исходного речевого сигнала, прежде всего его фонетической функции, с целью достижения его неразборчивости и/или неузнаваемости по известному заданному закону, когда параметры этого преобразования на передающем конце канала связи либо известны заранее, либо выделяются из самого исходного сигнала и не изменяются в процессе всего сеанса связи. На приемном конце эти параметры преобразования либо также известны заранее, либо выделяются из принятого модифицированного сигнала с целью восстановления неразборчивого речевого сигнала по тому же заранее известному закону. Данный метод реализуется за счет использования маскираторов речи.

Особую популярность в последнее время получила стеганография, используемая в области сокрытия конфиденциальной информации в графических

изображениях, передаваемых по телекоммуникационным сетям. В тоже время прогресс, достигнутый в области разработки устройств передачи речевых сообщений, а также в средствах вычислительной техники, открывает новые возможности как для скрытой передачи конфиденциальной информации в аналоговых и цифровых аудио сигналах и речи, так и для скрытой передачи в информационных контейнерах различного рода на основе использования динамично развивающихся технологий мультимедиа, компьютерной и сотовой телефонии.

В настоящее время широко применяются методы компьютерной стеганографии, основанные на использовании естественных шумов, которые содержат цифровые массивы, полученные стандартными способами преобразования из аналоговых акустических и видеосигналов. Эти шумы являются ошибками квантования и не могут быть полностью устранены. Использование шумовых бит для передачи дополнительной конфиденциальной информации позволяет создавать скрытый канал передачи данных. В качестве шумовых бит обычно рассматриваются младшие разряды значений отсчетов, которые являются шумом с точки зрения точности измерений и несут наименьшее количество информации, содержащейся в отсчете.

Для защиты информации от утечки по виброакустическому, акустооптическому каналам используют метод микширования речевого сигнала распространяющегося в виде механических колебаний в ограждающих конструкциях с различными шумовыми сигналами. Технически это реализуется за счет использования автоматических генераторов шума. Именно поэтому акустическую маскировку часто называют **акустическим зашумлением.**

Большую группу генераторов шума составляют устройства, принцип действия которых основан на усилении колебаний первичных источников шумов. В качестве источников шумовых колебаний используются полупроводниковые и другие электронные приборы и элементы. Роль оконечных электроакустических преобразователей, осуществляющих преобразование электрических коле-

баний в акустические колебания речевого диапазона длин волн, обычно выполняют электромеханические, пьезоэлектрические преобразователи и малогабаритные широкополосные громкоговорители (рис. 5.2).

Рис. 5.2. Внешний вид устройства защиты речевой информации «Прибой-Р»

При закреплении электромеханических, пьезоэлектрических преобразователей, например на оконном стекле защищаемого помещения, виброколебания, создаваемые средством маскировки, вызывают интенсивные колебания стекла с амплитудой, существенно превышающей амплитуду его колебаний, вызванных речевым сигналом. Вследствие этого при лазерно-локационном зондировании оконного стекла отраженный от него акустический сигнал оказывается промодулированным не только речевым информационным сигналом, но и в значительной степени помеховым. Это приводит к существенному ухудшению условий приема и восстановления перехваченных речевых сообщений.

Аналогичное ухудшение условий перехвата будет иметь место и при наличии виброакустического канала утечки информации, например при перехвате речевого сигнала скрытно размещенным на оконном стекле или на стене защищаемого помещения электронным стетоскопом. Уровень маскирующего вибрационного шума должен превосходить уровень информационного сигнала на определенную нормами виброакустической защиты величину.

Временной случайный процесс, близкий по своим свойствам к шумовым колебаниям, может быть получен с помощью цифровых генераторов шума, формирующих последовательности двоичных символов, называемых псевдослучайными.

Наряду с шумовыми помехами в целях активной акустической маскировки используют и другие помехи.

Виды акустических помех, создаваемых средствами защиты:

– «белый» шум – имеет равномерный спектр в полосе частот речевого сигнала;

– «окрашенный» шум – формируется из «белого» в соответствии с огибающей амплитудного спектра скрываемого речевого сигнала;

– «речеподобные» помехи – формируются путем микширования в различных сочетаниях отрезков речевых сигналов, музыкальных фрагментов и шумовых помех или формируется из фрагментов скрываемого речевого сигнала при многократном наложении с различными уровнями.

«Речеподобные» помехи:

– «речеподобная» помеха-1 – формируется из фрагментов речи трех дикторов радиовещательных станций при примерно равных уровнях смешиваемых сигналов;

– «речеподобная» помеха-2 – формируется из одного доминирующего речевого сигнала или музыкального фрагмента и смеси фрагментов радиопередач с шумом;

– «речеподобная» помеха-3 – формируется из фрагментов скрываемого речевого сигнала при многократном их наложении с различными уровнями.

Акустические колебания, создаваемые средствами активной акустической маскировки, могут отрицательно воздействовать на людей, находящихся в зашумленном помещении, и приводить к их быстрой и повышенной утомляемости.

Основные требования, которым должны удовлетворять современные средства акустического зашумления:

– временные, спектральные и корреляционные характеристики помех должны быть близки соответствующим характеристикам полезного сигнала;

– средства создания помех должны обеспечивать требуемое превышение помехи над полезным сигналом в каждой выделенной полосе частот, исключающее возможность выделения сигнала на фоне помехи;

– элементы крепления электромеханических преобразователей не должны существенно искажать помеховый сигнал;

– следует учитывать, что создаваемые средствами маскировки виброколебания могут раздражающе воздействовать на нервную систему человека, вызывая различные функциональные отклонения.

5.2. Электромагнитная маскировка

Этот метод основан на создании активных маскирующих помех (как правило, шумовых) в заданном диапазоне частот и реализуется с помощью систем активной защиты. Такие системы подразделяются на системы линейного и пространственного зашумления.

Системы линейного зашумления применяются для маскировки опасных сигналов в проводах, кабелях, различных токоведущих линиях и конструкциях, выходящих за пределы контролируемой территории. Объектами линейного зашумления являются, например, провода, цепи и устройства технических средств, подверженные воздействию низкочастотных электромагнитных полей, возникающих при работе ТСОИ, а также элементы и устройства, обладающие свойствами электроакустических преобразователей.

В простейшем случае система линейного зашумления представляет собой генератор шумового сигнала, формирующий шумовое маскирующее напряжение с заданными спектральными, временными и энергетическими характери-

стиками, который подключается в зашумляемую токоведущую линию (рис. 5.3).

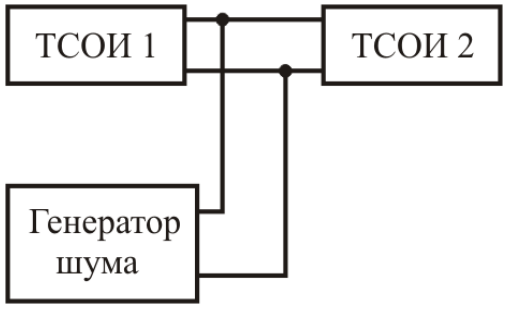


Рис. 5.3. Схема включения системы генератора шумового сигнала

Рис. 5.4. Внешний вид устройства линейного зашумления «SEL SP-44»

Системы пространственного зашумления применяют для создания маскирующих помех в окружающем пространстве (рис. 5.5). В состав системы входят:

– генераторы шумового сигнала;

– усилители, обеспечивающие необходимую мощность шумового сигнала в заданном диапазоне частот;

– антенны;

– устройства коммутации и контроля.

Цель зашумления считается достигнутой в том случае, когда отношение опасный сигнал/шум на границе контролируемой территории в окружающем пространстве или в токоведущей линии уменьшается до требуемого уровня, не позволяющего средствам перехвата качественно решать задачи обнаружения и анализа опасного сигнала. Способы размещения и подключения систем линейного и пространственного зашумления определяются особенностями схемного

решения, расположения и монтажа защищаемых объектов и средств зашумления.

Рис. 5.5. Внешний вид устройства пространственного зашумления «ПАЗК-01»

При применении систем активной зашиты необходимо учитывать их возможное влияние на качество работы защищаемых и других технических средств, расположенных в зоне действия электромагнитных полей, создаваемых ими.

5.3. Обнаружение закладных устройств

Речевая информация, циркулирующая в помещении, может негласно транслироваться за его пределы при помощи ЗУ.

Закладные устройства занимают ведущее место среди средств технического шпионажа. Для повышения скрытности работы мощность передатчика ЗУ делается небольшой, но достаточной для перехвата высокочувствительным приемником с небольшого расстояния (20…400 м). Рабочую частоту для повышения скрытности нередко выбирают вблизи несущей частоты мощной радиостанции. Микрофоны делают как встроенными, так и выносными. Они бывают двух типов: акустическими (чувствительнымик голосам людей) или вибрационными (преобразующими в электрические сигналы колебания, возникающие от человеческой речи в разнообразных жестких конструкциях). Для повышения скрытности они камуфлируются специальным образом и имеют дистанционное включение или выключение, например, по голосу человека (VOX-закладки).

В качестве канала связи они обычно используют сеть электропитания, телефонные линии или радиоканал (рис. 5.6).

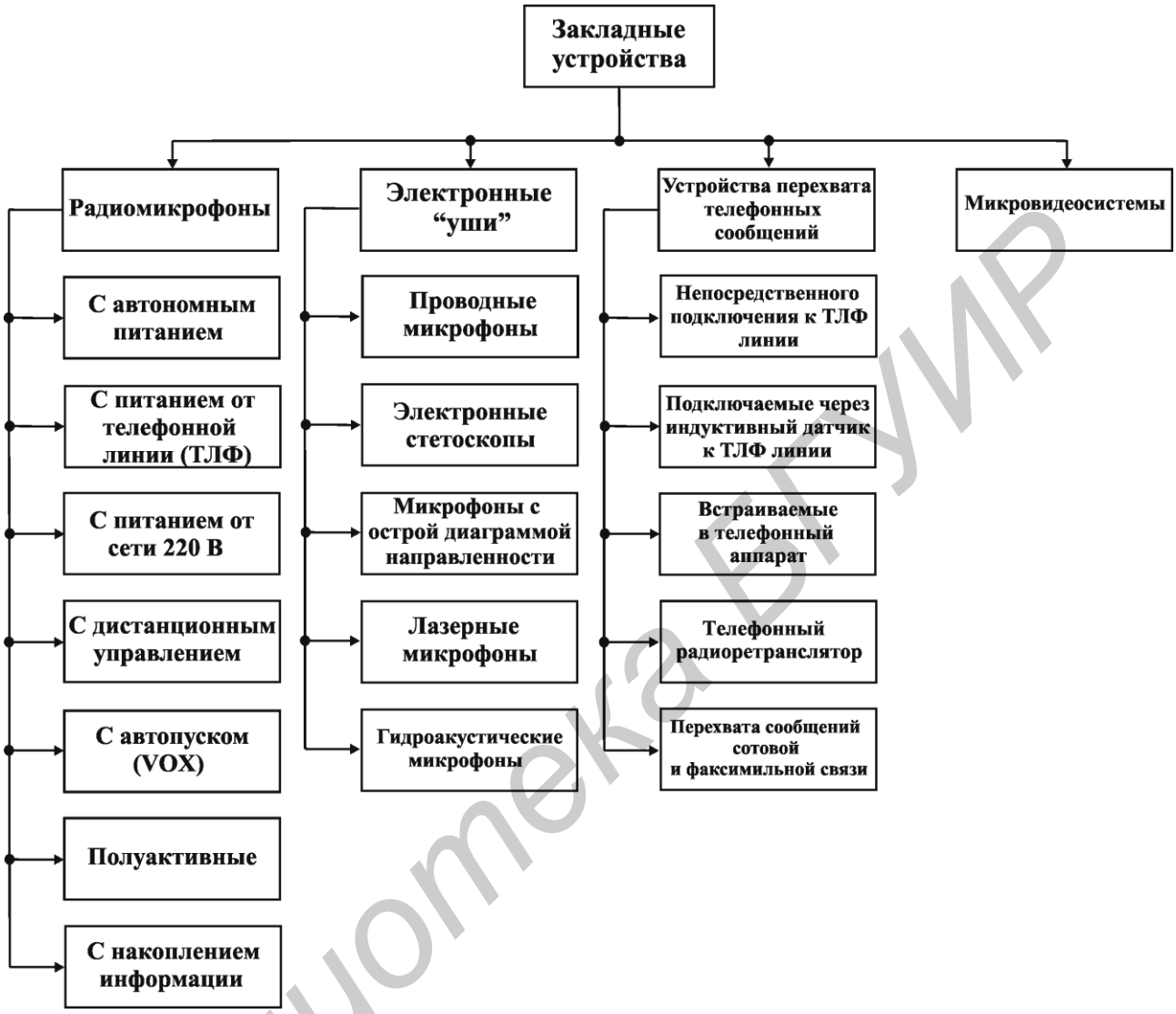


Рис. 5.6. Классификация закладных устройств

Поиск и обнаружение закладных устройств может осуществляться визуально, а также с использованием специальной аппаратуры.

Обнаружение закладных устройств, так же как и любых других объектов, производится по их демаскирующим признакам. Каждый вид электронных устройств перехвата информации имеет свои демаскирующие признаки, позволяющие обнаружить закладку.

Наиболее информативными признаками проводной микрофонной системы являются:

– тонкий провод неизвестного назначения, подключенный к малогабаритному микрофону (часто закамуфлированному и скрытно установленному) и выходящий в другое помещение;

– наличие в линии (проводе) неизвестного назначения постоянного (в несколько вольт) напряжения и низкочастотного информационного сигнала.

Демаскирующие признаки автономных некамуфлированных акустических закладок включают:

– признаки внешнего вида – малогабаритный предмет неизвестного назначения;

– одно или несколько отверстий малого диаметра в корпусе;

– наличие автономных источников питания (например аккумуляторных батарей);

– наличие полупроводниковых элементов, выявляемых при облучении обследуемого устройства нелинейным радиолокатором;

– наличие в устройстве проводников или других деталей, определяемых при просвечивании его рентгеновскими лучами.

Камуфлированные акустические закладки по внешнему виду на первый взгляд не отличаются от объекта имитации, особенно если закладка устанавливается в корпус бытового предмета без изменения его внешнего вида. Такие закладки можно выявить путем разборки предмета.

Закладки, устанавливаемые в малогабаритные предметы, ограничивают возможности последних. Эти ограничения могут служить косвенными признаками ЗУ. Чтобы исключить возможность выявления закладки путем ее разборки, места соединения разбираемых частей склеивают.

Некоторые камуфлированные ЗУ не отличаются от оригиналов даже при тщательном внешнем осмотре. Их можно обнаружить только при просвечивании предметов рентгеновскими лучами.

К основным методам поиска закладных устройств можно отнести:

– специальное обследование выделенных помещений;

– поиск ЗУ с использованием технических средств;

– измерение параметров линий электропитания, телефонных линий связи и т. д.;

– проведение тестового «прозвона» всех телефонных аппаратов, установленных в проверяемом помещении, с контролем (на слух) прохождения всех вызывных сигналов автоматических телефонных станций.

Поисковые работы ЗУ классифицируются в соответствии со следующими критериями.

1. По характеру выполняемых работ:

а) ***разовая проверка.*** Разовые работы, которые обычно производятся перед проведением важных переговоров или после посещения защищаемого помещения определенными личностями;

б) ***профилактическая проверка.*** Периодически проводимый комплекс мероприятий, направленных на поддержание на должном уровне информационной безопасности объекта. Обычно производится в совокупности с другими организационно-техническими видами информационного обеспечения;

в) ***конспиративная проверка.*** Этот вид работ производится в случаях очевидной утечки информации, и является наиболее трудоемким видом проверок, требующим большой подготовительной работы как со стороны поисковиков, так и со стороны руководства предприятия заказчика. Основной задачей в данном виде работ является не только обнаружение канала утечки информации или средства перехвата, но и сохранение производимых мер в тайне;

г) ***послепроверочная консультация.*** По результатам проведенного обследования объекта даются рекомендации по выбору и установке средств защиты информации, а также по реализации необходимых мер для устранения или предотвращения каналов утечки.

2. По глубине проводимых проверок:

а) ***первый уровень.*** В результате проверки могут быть обнаружены радиоизлучающие изделия, установленные непосредственно в проверяемом или

смежных с ним помещениях. При этом если устройства в момент проверки находятся в пассивном состоянии, то они могут быть не выявлены;

б) ***второй уровень.*** Могут быть обнаружены все устройства первого уровня плюс сетевые передатчики, использующие в качестве канала передачи сеть питания 220 В 50 Гц;

в) ***третий уровень.*** Могут быть выявлены все изделия второго уровня плюс все типы кабельных микрофонных систем, а также оргтехника, работающая в режиме передачи за границы зоны охраны сигнала, содержащего полезную информацию.

г) ***четвертый уровень.*** Могут быть выявлены все типы заносных и закладных электронных устройств перехвата информации и естественные каналы утечки информации.

5.4. Технические средства обнаружения закладных устройств

Индикаторы электромагнитных излучений. Простейший индикатор электромагнитного поля состоит из антенны, широкополосного усилителя, амплитудного детектора и порогового устройства, которое срабатывает, если сигнал на выходе детектора превысит регулируемый пороговый уровень. Порог устанавливается так, чтобы индикатор не реагировал на внешние излучения (фон). В результате подслушивающее устройство обнаруживается только в тех точках помещения, где уровень его поля превосходит фоновый на 15…20 дБ (рис. 5.7).

Для повышения чувствительности используются режекторные фильтры, настроенные на частоты мощных внешних источников данного региона (телевизионные и радиовещательные станции), или пространственная компенсация внешних электромагнитных полей.

Некоторые устройства оснащаются простейшими средствами идентификации: звуковой выход позволяет прослушивать демодулированный сигнал и

выявлять радиомикрофоны методом так называемой «акустической обратной связи», вызывающей самовозбуждение в тракте радиомикрофон – индикатор.

Рис. 5.7. Внешний вид широкополосного индикатора «Редут»

Индикаторы поля отличаются небольшими размерами и массой, простотой, быстродействием и низкой стоимостью. Однако из-за недостаточной чувствительности и избирательности они не обеспечивают требуемой достоверности обнаружения. Поэтому эти устройства рекомендуются лишь для предварительного обследования помещения или ручной локализации радиомикрофонов, обнаруженных более совершенными системами.

Индикаторы-частотомеры. Отличаются от индикаторов электромагнитных излучений встроенным счетчиком – частотомером, который измеряет частоту радиосигнала, превысившего установленный порог, и помогает оператору идентифицировать сигнал подслушивающего устройства (рис. 5.8).

Кроме того, некоторые индикаторы можно подключать к компьютеру и сканирующему радиоприемнику. В этой конфигурации индикатору поручается предварительный анализ электромагнитной обстановки с последующей проверкой результатов сканером. Индикаторы-частотомеры сохраняют основной недостаток индикаторов поля: достоверно обнаружить источник излучения они могут только в непосредственной близости от него.

Нелинейные локаторы. Используются для физического обнаружения и определения местоположения скрытно размещенных электронных устройств, которые могут находиться в выключенном состоянии (рис. 5.9). Нелинейный локатор излучает СВЧ-сигнал и принимает его вторую гармонику, которая об-

разуется из-за нелинейных эффектов в полупроводниковых приборах. Чтобы исключить ложное срабатывание локатора, создаваемое контактами металл-окисел в строительных конструкциях, более совершенные изделия принимают и анализируют уровни не только второй, но и третьей гармоники.

Рис. 5.8. Внешний вид индикатора-частотомера «Raksa-120»

Рис. 5.9. Внешний вид нелинейного локатора SEL SP-61/M «Катран»

Анализаторы спектра. Измерительные приборы, которые широко используются для обнаружения и идентификации сигналов оператором по форме их спектров. Обладая высокой чувствительностью, они могут подключаться к антенне или кабельным линиям и воспроизводить на экране спектральные панорамы или спектры отдельных радиосигналов. Главное преимущество анализаторов спектра высокая скорость сканирования и наглядное отображение результатов. Однако они, как правило, не располагают средствами автоматизации операций обнаружения и довольно дороги.

Рис. 5.10. Внешний вид анализатора спектра Agilent Technologies N1996A

Сканирующие радиоприемники. Современные сканеры могут автоматически перестраиваться в диапазоне до нескольких ГГц и обнаруживать сигналы с различными видами модуляции (рис. 5.11). Эти изделия можно разделить на две группы. Первые обладают уникальными параметрами, однако их размеры, масса и, главное, стоимость весьма высоки.

Изделия второй группы появились в результате эволюции связных, в основном коротковолновых радиоприемников. Сканеры, обладающие высокой чувствительностью, частотной избирательностью и широким диапазоном анализа, обнаруживают сигналы радиомикрофонов с большой достоверностью. Однако эксплуатация их в качестве автономных устройств из-за ограниченных возможностей по вводу, хранению и отображению данных требует весьма высокой квалификации оператора.

Компьютерные программы управления сканерами. Большинство современных сканеров можно подключить к компьютеру, который значительно расширяет возможности управления, отображения и хранения информации об исследуемых сигналах. Наряду с функциями управления, а также накопления и обработки данных о радиоспектрах специализированное программное обеспечение способно решать отдельные задачи идентификации сигналов подслушивающих устройств.

Рис. 5.11. Внешний вид сканирующего приемника «Скорпион-XL»

Микрокомпьютерные комплексы обнаружения радиомикрофонов. В этих изделиях объединяется аппаратура поиска сигналов: антенны, адаптеры для подключения к кабельным линиям, специализированные сканирующие радиоприемники, а также устройства индикации и регистрации данных. Функции управления и отображения поручаются микрокомпьютеру, который организует также отдельные автоматические процедуры обнаружения и идентификации сигналов.

Компьютерные комплексы контроля помещений и зданий (радиомониторинга). Представляют собой аппаратно-программные системы на базе стандартных узлов компьютера и недорогого сканера, которые оснащаются дополнительной аппаратурой и программами (рис. 5.11). Располагают возможностями для реализации «интеллектуальных» процедур обнаружения любой сложности.

Тепловизоры. Техническое средство, обеспечивающее преобразование электромагнитного излучения (теплового), излучаемого различными объектами в видимое изображение (рис. 5.12). Поиск ЗУ на основе метода теплового неразрушающего контроля базируется на том, что закамуфлированное закладное устройство, сложно обнаруживаемое в видимом диапазоне длин волн, имеет

демаскирующие признаки в коротковолновой (3…5 мкм) и длинноволновой (8…14 мкм) областях инфракрасного (ИК) спектра. Работа ЗУ сопровождается поглощением и выделением тепла, изменяя внутреннюю его энергию, которая в состоянии термодинамического равновесия пропорциональна температуре вещества. В результате этого поверхности физических тел (объекта контроля и ЗУ) приобретают специфическое температурное распределение и таким образом могут быть четко разграничены.

Рис. 5.12. Внешний вид автоматизированного комплекса радиомониторинга «Крона НМ»

В случае установки ЗУ в электронную аппаратуру их обнаружение ведется путем поиска, места контакта электронных компонентов (точечный источник ИК излучения) и модулей, имеющих температуру, в месте контакта значительно превышающую температуру окружающей среды.

Рис. 5.13. Внешний вид тепловизора «FLIR b50»

5.5. Контрольные вопросы

1. Какая цель изменения голоса диктора?

2. Какими методами обеспечивается неразборчивость речи диктора?

3. Что такое стеганография и в чем ее сущность?

4. Какие шумовые сигналы создаются техническими средствами защиты?

5. Какое влияние оказывают шумовые сигналы средств технической защиты на человека?

6. Какое назначение систем линейного зашумления?

7. Для каких целей используются системы пространственного зашумления?

8. На какие группы делятся закладные устройства?

9. Какие каналы передачи информации используют закладные устройства?

10. На какие категории классифицируются работы по поиску закладных устройств?

11. Дайте краткую характеристику техническим средствам обнаружения закладных устройств.

6. ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

6.1. Категорирование объектов

Категория охраняемого объекта – комплексная оценка состояния объекта, учитывающая его экономическую или иную, например культурную, значимость в зависимости от концентрации сосредоточенных ценностей, последствий от возможных преступных посягательств на них, сложности обеспечения требуемой надежности охраны. Результат оценки может быть выражен качественно или количественно. Примером качественных оценок служат так называемые перечневые классификаторы (список категорий объектов с краткими пояснениями). Приведем классификацию, основанную на оценке ущерба от реализации угроз (табл. 6.1).

К **категории А** следует отнести особо важные объекты, на которых возможный ущерб в случае реализации основных угроз безопасности максимален по характеру и по масштабам. Его последствия выходят за пределы территории объектов и не могут быть локализованы в пространстве и во времени за счет принятия немедленных ликвидационных мер. Характер ущерба заключается в создании угрозы для жизни и здоровья персонала и населения, а также в негативном воздействии на природную среду.

К **категории Б** предлагается отнести важные объекты, на которых характер возможного ущерба заключается в угрозе для жизни и здоровья персонала объекта, а его последствия не выходят за пределы территории объекта и могут быть локализованы путем принятия ликвидационных мер. К этой же категории предлагается отнести объекты, возможный ущерб которых носит материальный характер, но его масштабы имеют региональное значение.

Прочие объекты (**категория В**) характеризуются тем, что возможный ущерб носит локальный и в основном материальный характер и по масштабу может иметь как региональное, так и международное значение.

Таблица 6.1

Классификация объектов

Категория	Наименование категории	Ущерб или последствия от осуществления угроз	Назначение или принадлежность объектов
А	Особо важные	Особо крупный или невосполнимый материальный ущерб, экологическая катастрофа на объекте или в регионе, гибель большого числа людей на объекте или в регионе, политические последствия, утечка государственных секретов, другие особо тяжкие последствия	Хранилища и депозитарии банков, предприятия по производству или хранилища химически опасных, наркотических и взрывчатых веществ, боеприпасов, ядерных материалов; предприятия оборонного профиля; правительственные учреждения; энергетические комплексы
Б	Важные	Значительный материальный или финансовый ущерб, угроза здоровью или жизни людей, утечка государственных или коммерческих секретов	Кассовые залы банков, подъезды инкассаторских машин; помещения для хранения и работы с конфиденциальной информацией; крупные торговые центры; производственные помещения
В	Прочие	Материальный или финансовый ущерб; информационный ущерб; нарушение комфортности личной жизни или служебной деятельности	Магазины, служебные помещения, офисы, производственные помещения, жилые помещения

В свою очередь, каждую категорию объектов можно классифицировать по масштабу или размеру нанесенного ущерба в результате несанкционированного доступа (НСД) нарушителей.

Например, особо важные объекты предлагается дополнительно разделить на три группы безопасности (№1, 2, 3). Номер группы определяет масштаб воз-

можного ущерба, который может иметь последствия, соответственно, трансграничного, государственного, регионального значений.

Для других категорий объектов можно использовать предложенную в табл. 6.2 классификацию по группам значимости и уровням защищенности. При этом следует заметить, что при установлении уровня защищенности необходимо дополнительно учитывать возможные угрозы безопасности для конкретного объекта, которые определяются в основном сложившейся криминогенной обстановкой в данном регионе.

Принадлежность объекта к соответствующей категории и группе необходимо определять на начальной стадии проектирования системы информационной безопасности (СИБ), т. к. от этого зависит не только уровень его защищенности, но и планируемая тактика действий сил охраны. От этой тактики зависят общие затраты на создание СИБ.

Разница в тактике действий сил охраны должна учитываться в процессе создания СИБ: при определении структуры, количественного состава и оснащенности сил охраны, а также при выборе типов и взаимного расположения инженерных средств задержки нарушителя. Оптимизация структуры СИБ по критерию «эффективность–стоимость» позволяет обеспечить достаточно эффективную защиту объекта от НСД нарушителей при минимальных затратах ресурсов.

6.2. Классификация помещений и территории объекта

К вопросу классификации служебных помещений с точки зрения их безопасности существует несколько подходов. Учитывая, что степень безопасности от перечисленных выше угроз тесно связана прежде всего с режимом пребывания в помещениях сотрудников и посетителей, целесообразно проводить классификацию по степени режимных ограничений и возможности доступа в них. Предлагается все помещения и территорию разбить на шесть категорий или зон, представленных в табл. 6.2.

Таблица 6.2

Классификация территории и помещений объекта связи

Категория зоны	**I**	**II**	**III**	**IV**	**V**	**VI**
Наименование зоны	Свободная зона	Наблюдаемая зона	Регистрационная зона	Режимная зона	Зона усиленной защиты	Зона высшей защиты
Пример функционального назначения	Места свободного посещения	Комнаты приема посетителей	Кабинеты сотрудников	Секретариат, подразделения множительной оргтехники, компьютерные залы, архивы	Материальные склады	Кабинеты высших руководителей, комнаты для ведения конфиденциальных переговоров, специальные хранилища
Условия доступа сотрудников	Свободный	Свободный	Свободный	По служебным удостоверениям или идентификационным картам	По спецдокументам	По спецдокументам
Условия доступа посетителей	Свободный	Свободный	Свободный с регистрацией по удостоверениям личности	По разовым пропускам	По спецпропускам	По спецпропускам
Наличие охраны	Есть	Есть	Есть	Усиленная охрана	Усиленная охрана	Усиленная охрана
Наличие технических средств охраны	Нет	Средства наблюдения	Охранная сигнализация	Охранная сигнализация, система контроля доступа	Охранная сигнализация (два рубежа), система контроля доступа, механическое усиление	Охранная сигнализация (два рубежа), система контроля доступа, защита утечки информации, механическое усиление

I. Свободная зона – помещения и прилегающая территория, доступ в которые свободен для любой категории лиц. За этими территориями

не ведется наблюдения и там не размещено никаких технических средств охраны и безопасности. Примером такой зоны может быть бюро пропусков, справочное бюро и др.

II. Наблюдаемая зона – помещения и территория, доступ в которые также не ограничен, но за ними ведется систематическое наблюдение силами службы безопасности или охраны. Наблюдение может вести лицо, находящееся в данном помещении или в других помещениях, с помощью оптических или телевизионных приборов. Типичным примером может служить вестибюль объекта, территория служебной автостоянки и др.

III. Регистрационная зона – зона, вход в которую свободен для любого желающего при условии, что он предъявит для регистрации документ, удостоверяющий его личность. Такая система часто используется в учреждениях, работающих с большим числом клиентов.

IV. Режимная зона – зона, на входе в которую находится пост охраны. Проход допускается либо по пропускам установленной формы, либо по именным заявкам лиц, имеющих соответствующее право.

V. Зона усиленной защиты – это, как правило, помещения, куда допускаются только сотрудники предприятия, а для посторонних лиц доступ туда возможен только по специальным пропускам или в сопровождении уполномоченных лиц. Такого рода помещения, как правило, оборудуются средствами контроля доступа и охранной сигнализацией. Вход в эту зону может также контролироваться постом охраны.

VI. Зона высшей защиты – зона, вход в которую ограничен не только для клиентов и посетителей, но и для собственных сотрудников, не имеющих прямого отношения к данным помещениям. Хорошим примером могут служить помещения высшего руководства или помещения, связанные с хранением и обработкой особо ценной и конфиденциальной информации. Зона высшей защиты оборудуется инженерно-техническими средствами, приборами контроля и наблюдения и дополнительными постами охраны.

Представленные шесть категорий режимности помещений практически способны охватить все варианты функционального назначения служебных помещений. Отметим факторы, регламентирующие помещение по одной из вышеуказанных категорий:

– условия доступа сотрудников предприятия;

– условия доступа клиентов и посторонних лиц;

– наличие и вид физической охраны;

– виды использования технических средств наблюдения и охраны.

Кроме этого, нанесение на план здания защищаемого объекта, например, категорий режимности всех помещений, позволит наглядно увидеть все недостатки в распределении помещений по функциональному назначению. Наиболее оптимальным способом распределения помещений является компактное размещение в одном месте помещений одной и той же категории. При этом желательно, чтобы между собой соседствовали зоны одинаковых или не слишком различающихся категорий. Например попасть в помещение IV зоны можно только из помещения III или V зоны. Это позволит наиболее экономным способом разместить средства инженерного усиления строительных конструкций и технические средства безопасности.

6.3. Инженерные заграждения

Заграждение в составе системы охраны периметра объекта выполняет роль преграды, изменяющей условия передвижения нарушителя по направлению к охраняемому объекту.

Характеризуется **временем сопротивления** – время, необходимое на преодоление данного заграждения.

По назначению ограждения делятся на следующие виды:

– основные – препятствуют свободному входу нарушителя на территорию объекта;

– дополнительные – предназначены для повышения укрепленности основных ограждений;

– предупредительные – устанавливаются с внутренней или внешней стороны основного ограждения с вывешиванием на них запрещающих надписей («Стой», «Запретная зона», «Не подходить» и т.д.) и предназначены для ограничения доступа к нему людей.

Для защиты верхней части капитальных заборов применяется также армированная колючая лента (АКЛ «Егоза»), изготавливаемая путем армирования колючей ленты стальной оцинкованной проволокой диаметром 2,5 мм. Колючая лента заградительная представляет собой оцинкованную ленту толщиной 0,5 мм, имеющую обоюдоострые, симметрично расположенные шипы (рис. 6.1).

Рис. 6.1. Внешний вид АКЛ «Егоза»

Все заграждения в зависимости от назначения можно разделить на четыре типа: сигнализационные, сигнализационно-электризуемые (электрошоковые), строительные (технические) и строительно-сигнализационные.

Сигнализационные ограждения образовывают проводящие металлические конструкции, являющиеся чувствительным элементом периметрового средства обнаружения, которое называется заградительным (перемежающиеся линии колючей проволоки, закрепленные на деревянных или бетонных столбах

и включенные в два активных шлейфа, чувствительных к обрыву и короткому замыканию смежных линий).

Сигнализационно-электризуемые заграждения представляют собой систему токонесущих проводов (изолированных от опор), по которой распространяются импульсы высокого напряжения (3…10 кВ), вызывающие болевой шок у нарушителя при касании.

Строительные заграждения весьма разнообразны, их классификация дана на рис. 6.2.

Рис. 6.2. Строительные заграждения

Видимость сквозь заграждение определяется конструкцией, выбираемой в соответствии с пониманием безопасности и эстетики.

Высота заграждения является параметром, который определяет его проходимость, время преодоления, опасность падения, которой подвергает себя нарушитель наверху. В целом высота заграждения должна определяться разумным компромиссом между охранной функцией и эстетикой. Стоимость заграждения (материалы, работа) приблизительно пропорциональна его высоте, в то

время как стоимость сигнализационного блокирования рубежа от его высоты (в рассматриваемых пределах) зависит в слабой степени.

Фундамент (прежде всего ленточный, по всему периметру) является практически обязательной частью заграждения, поскольку:

– обеспечивает меньшую подвижность заграждения при действии сильного ветра, который является существенным помеховым фактором для всех периметровых систем охраны, установленных на или вблизи заграждения;

– при глубине свыше 50…80 см он обеспечивает достаточно надежную защиту от подкопа;

– способствует большей долговечности всего заграждения.

Выбор полотна и опор заграждения, как правило, определяется с учетом стоимости, строительной нагрузки и конструкции, а также, в большей степени, выполняемой охранной функции (рис. 6.3).

а б

Рис. 6.3. Внешний вид фрагментов: монолитного (а) и сетчатого (б) заграждений

Важным звеном в системе охраны периметра объекта является полоса грунта шириной до 3 м, примыкающая к заграждению с внутренней стороны периметра объекта (**зона отчуждения**). Она предназначена для размещения периметровых систем охраны (в том числе и в грунте) и формирования зоны обнаружения, что накладывает ограничения на посадку деревьев, кустов, а также на перемещение людей в этой зоне.

Для обнаружения прохода нарушителя через зону отчуждения она может оборудоваться **контрольно-следовой полосой** из взрыхленного грунта шириной не менее 1,5 м (рис. 6.4).

Рис. 6.4. Внешний вид контрольно-следовой полосы

Примером комплексного использования инженерных решений укрепления периметра защищаемого объекта может служить Берлинская стена – инженерно-технически укрепленная государственная граница Германской Демократической Республики (1961–1989 гг.) с Западным Берлином (рис. 6.5).

Время возведения 1961–1975 гг. Общая протяженность – 155 км, в том числе по территории Берлина – 43,1 км. Средняя высота – 3,6 м.

Состав:

– железобетонное монолитное ограждение;

– ограждение из металлической сетки;

– сигнальное ограждение под электрическим напряжением;

– земляные рвы;

– противотанковые укрепления;

– контрольно-следовая полоса;

– сторожевые вышки и др.

Рис. 6.5. Внешний вид некоторых участков «Берлинской стены»

6.4. Технические средства охраны периметра объекта

Техническое средство охраны – вид техники, предназначенный для использования силами охраны с целью повышения эффективности обнаружения нарушителя и обеспечения контроля доступа на объект охраны.

Любая периметральная система охраны должна отвечать определенному набору критериев, некоторые из которых перечислены ниже:

– возможность раннего обнаружения нарушителя – еще до его проникновения на объект;

– точное следование контурам периметра, отсутствие «мертвых» зон;

– скрытая установка датчиков системы;

– независимость параметров системы от сезона (зима, лето) и погодных условий (дождь, ветер, град и т. д.);

– невосприимчивость к внешним факторам «нетревожного» характера – индустриальные помехи, шум проходящего рядом транспорта, мелкие животные и птицы;

– устойчивость к электромагнитным помехам – грозовые разряды, источники мощных электромагнитных излучений и т. п.

Каждое средство обнаружения строится на определенном физическом принципе, на основе которого действует его чувствительный элемент.

Чувствительный элемент – первичный преобразователь, реагирующий на воздействие на него (прямое или косвенное) объекта обнаружения и воспринимающий изменение состояния окружающей среды.

Средство обнаружения (СО) – устройство, предназначенное для автоматического формирования сигнала с заданными параметрами (сигнала тревоги) вследствие вторжения или преодоления объектом обнаружения чувствительной зоны (зоны обнаружения) данного устройства

Чувствительная зона СО (зона чувствительности) – участок, появление в котором объекта обнаружения вызывает возникновение полезного сигнала с уровнем, превышающим уровень шума или помехи.

Внутри зоны чувствительности располагается **зона обнаружения СО** – зона, где СО обеспечивает заданную вероятность обнаружения (рис. 6.6).

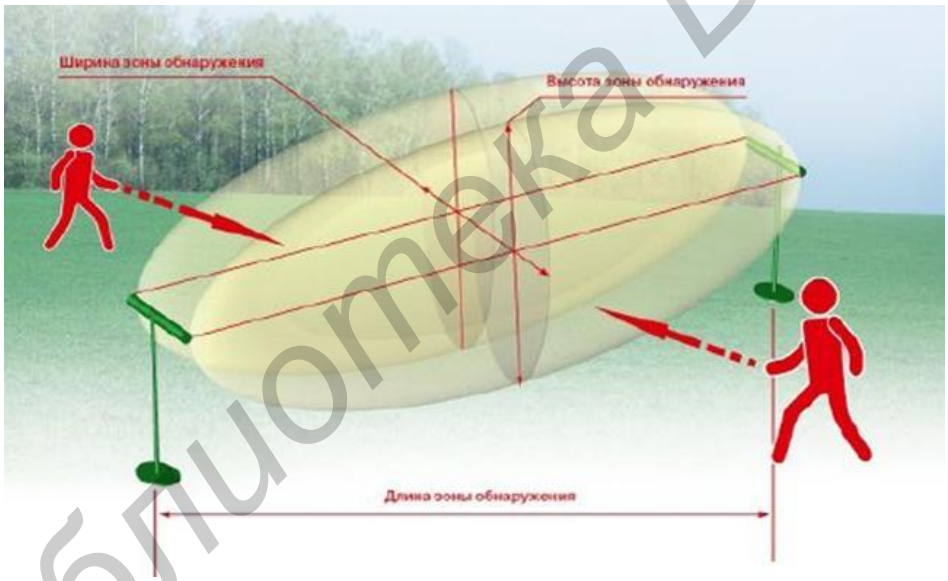


Рис. 6.6. Внешний вид контрольно-следовой полосы

6.4.1. Радиоволновые и радиолучевые средства обнаружения

Позволяют оборудовать скрытые или маскируемые рубежи охраны периметра.

Различие между радиоволновыми средствами обнаружения (РВСО) и радиолучевыми (РЛСО) состоит в способе формирования чувствительной зоны:

РВСО использует ближнюю зону распространения радиоволн (менее 10 длин волн), а РЛСО – дальнюю зону (более 100 длин волн) (рис. 6.7).

а

б

Рис. 6.7. Внешний вид РВСО (а) и РЛСО (б)

В зависимости от принципа действия различают:

– **пассивные РВСО и РЛСО** используют собственное излучение объекта обнаружения или вызываемое им изменение электромагнитных полей (ЭМП) внешних источников (как правило, вещательных теле- и радиостанций).

– **активные РВСО и РЛСО** используют собственный источник ЭМП для формирования чувствительной зоны.

По конструкционному исполнению:

– **однопозиционные** имеют общий блок приемопередатчика (пассивные РВСО и РЛСО всегда являются однопозиционными);

– **двухпозиционные** имеют разнесенные блоки передатчика и приемника.

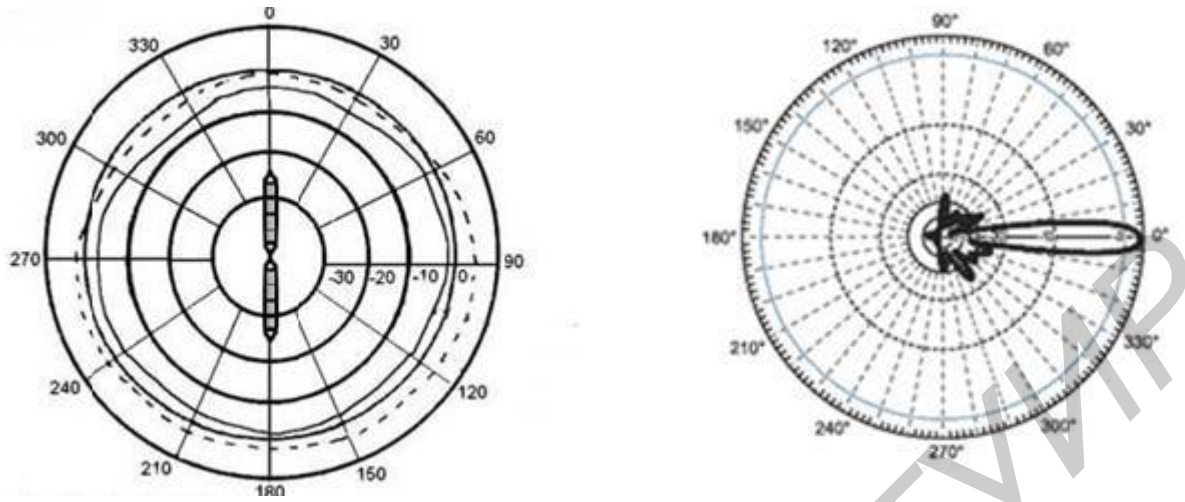
Форма чувствительной зоны для пассивных РВСО определяется формой диаграммы направленности антенны (рис. 6.8).

В первом случае она, как правило, круговая, а используемый диапазон 10 Гц…10 ГГц.

Во втором случае, как правило, чувствительная зона имеет лучевую форму и используются метровый и дециметровый диапазоны.

В РВСО в качестве чувствительных элементов используются кабели. На некотором расстоянии параллельно друг другу прокладываются два кабеля (две антенны) специальной конструкции (рис. 6.9). Зазоры между разреженными

проводами «экрана» своеобразного коаксиального кабеля образуют щелевую антенну.



а б

Рис. 6.8. Схематичное изображение круговой (а) и лучевой (б) диаграмм направленности

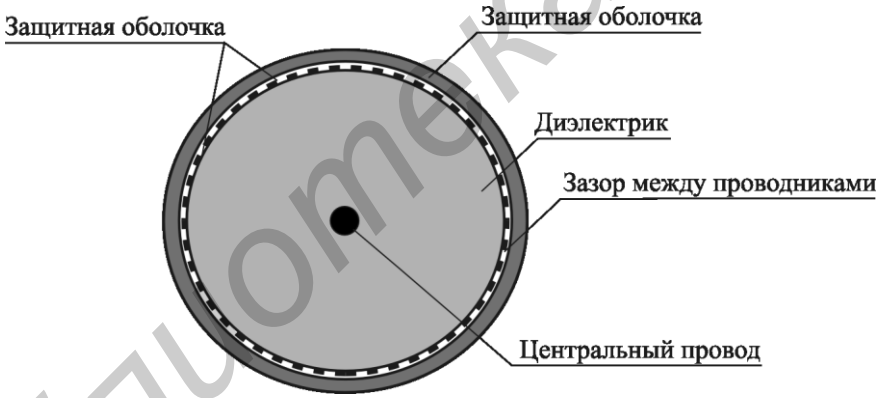


Рис. 6.9. Конструкция кабеля радиоволновой системы

Один из кабелей служит передающей антенной, другой – приемной антенной. При возбуждении первой антенны высокочастотными колебаниями она начинает излучать электромагнитное поле, воспринимаемое второй антенной. При этом приемник, подключенный к приемной антенне, принимает сигнал. Если в окрестности двух антенн появляется тело определенного объема с диэлектрической и/или магнитной проницаемостью, отличной от проницаемости свободного пространства, электромагнитное поле, воспринимаемое приемной антенной, искажается (изменяются его амплитуда и фаза). Это изменение де-

тектируется и анализируется приемником-анализатором. Если анализируемый сигнал превышает пороговое значение, формируется сигнал тревоги.

Во избежание образования мертвых зон кабели смежных зон охраны размещают с некоторым перекрытием (2…5 м) в продольном направлении.

РЛСО содержат передатчики и приемники с узконаправленными антеннами. Используемый диапазон частот обычно лежит в пределах 10…40 ГГц. Сечение радиолуча в горизонтальной (а) и вертикальной (б) плоскостях показано на рис. 6.10. Рабочей зоной радиолучевых систем считают зону на участке BC. На участке AB луч слишком узкий, и его можно обойти. На участке CD площадь поперечного сечения луча слишком велика по сравнению с площадью потенциального нарушителя, и обнаруживающая способность системы оказывается пониженной. В то же время наличие луча на достаточно протяженном участке CD за пределами рабочей зоны накладывает серьезные ограничения на минимальные размеры зоны отчуждения. При использовании одиночных совмещенных приемопередатчиков типа радиолокаторов зона отчуждения должна превышать размеры участка CD.

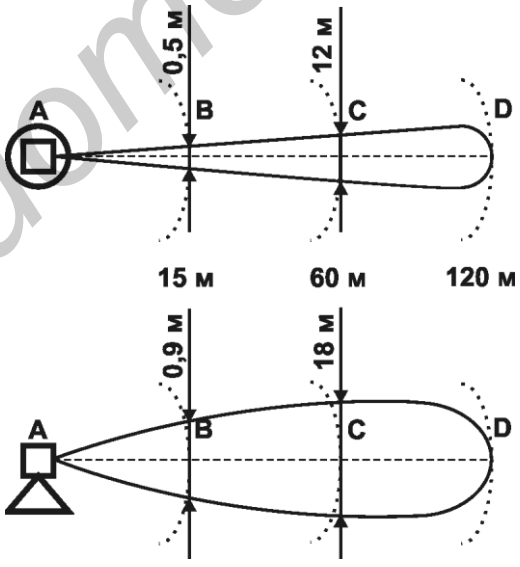


Рис. 6.10. Схематичное изображение зоны обнаружения радиолучевой системы

РЛСО чаще всего используют для контроля протяженных прямолинейных участков, когда имеется достаточно свободного пространства для вынесения приемников и передатчиков за пределы охраняемых зон. РЛСО, как прави-

ло, применяются одновременно с другими средствами, которые позволяют закрыть присущие РЛСО мертвые зоны.

6.4.2. Оптические средства обнаружения

Используются для блокирования объемов помещений, проходов, коридоров, периметров.

Пассивные инфракрасные средства обнаружения (ИКСО):

– обладают высокими показателями обнаружения и помехоустойчивости;

– обладают широким разнообразием конфигураций зон обнаружения;

– удобны в эксплуатации;

– экономичны;

– экологически безопасны и не создают помех другим средствам электронной техники;

– дешевле других средств, предназначенных для блокирования помещений.

Принцип действия ИКСО основан на регистрации теплового излучения нарушителя (пассивные ИКСО) или изменения ИК-излучения при взаимодействии его с нарушителем (активные ИКСО).

Функционально ИКСО предназначены:

– для охраны протяженных рубежей и периметров;

– для охраны помещений и отдельных предметов.

Активные ИКСО применяются для охраны протяженных рубежей и периметров. Для охраны помещений и отдельных предметов предпочтение отдается **пассивным ИКСО** (рис. 6.11).

Зона обнаружения ИКСО представляет собой набор лучей различной конфигурации, расходящихся от СО по радиальным направлениям в одной или нескольких плоскостях. В связи с тем что в ИКСО используются сдвоенные пироприемники, каждый луч в горизонтальной плоскости расщепляется на два (рис. 6.12).

а б

Рис. 6.11. Внешний вид пассивного ИКСО (а) и активного ИКСО (б)

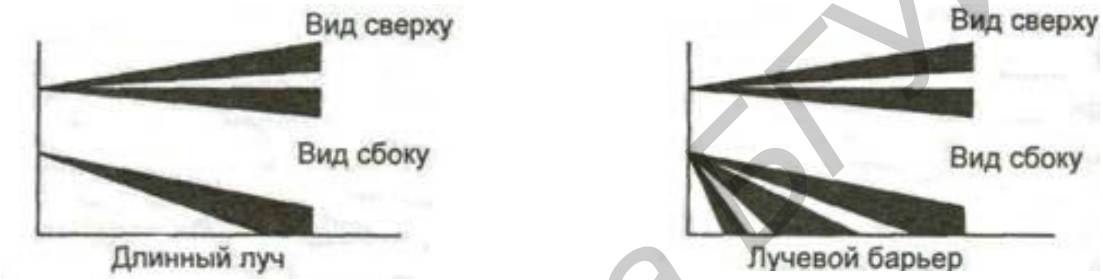


Рис. 6.12. Внешний вид зон обнаружения ИКСО

Для обнаружения нарушителя на расстоянии 10…20 м желательно, чтобы в вертикальной плоскости ширина луча не превышала 5…10°(человек практически полностью перекрывает луч). На меньших расстояниях чувствительность детектора в этом луче существенно возрастает, что может привести к ложным срабатываниям, например от мелких животных.

Факторы, ограничивающие возможность применения ИКСО:

– туман с метеорологической дальностью видимости менее 200…250 м;

– необходимость обогрева оптических систем активных ИКСО в весенне-осенний и зимний периоды года.

6.4.3. Сейсмические средства обнаружения

Сейсмические средства обнаружения (ССО) регистрируют и обрабатывают сигналы, возникающие в результате колебаний подстилающей поверхности

(грунт) при пересечении человеком охраняемой зоны. Предназначены для блокирования участков протяженных рубежей периметров объектов.

Рис. 6.13. Внешний вид ССО

Чувствительный элемент сейсмического средства обнаружения (ССО) может быть точечный (сейсмоприемники) или протяженный (трибокабели, эластичные трубы с жидкостью с датчиками давления, волоконно-оптические преобразователи) (рис. 6.14).

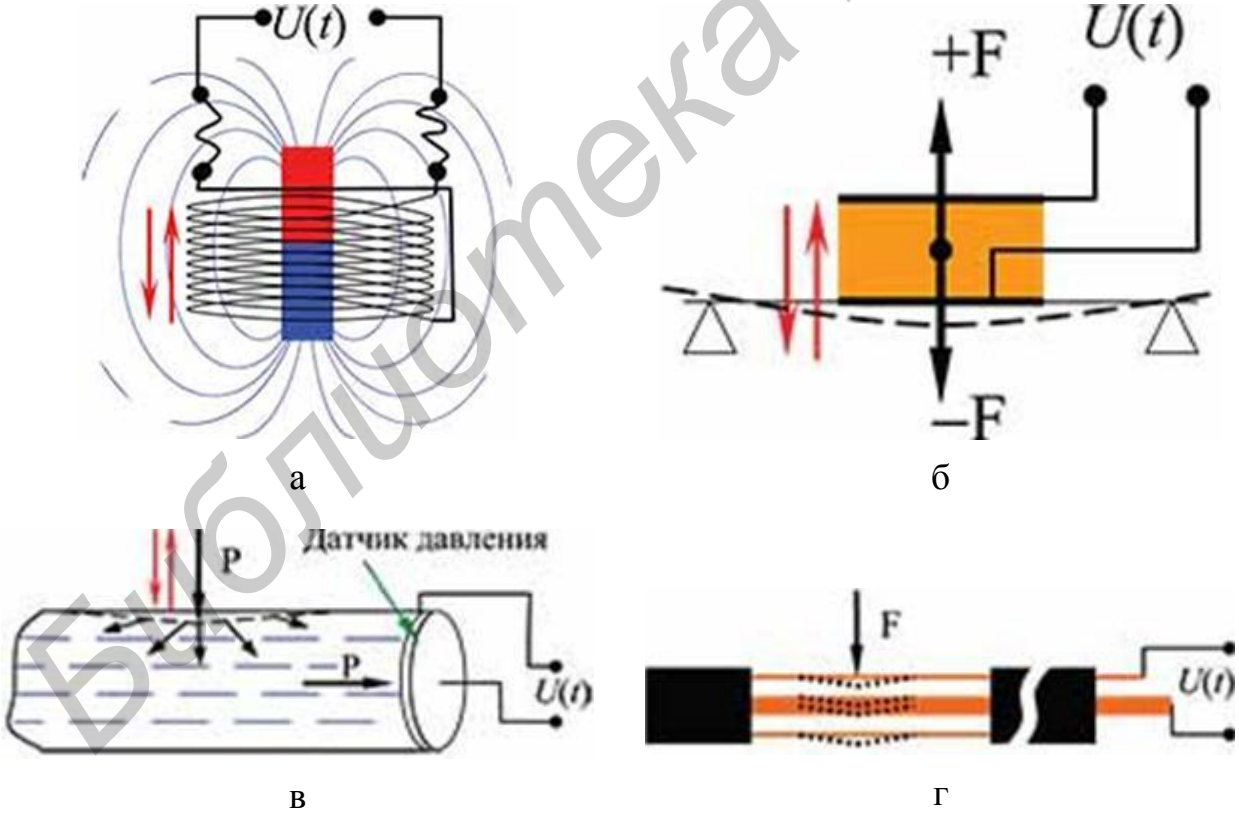


Рис. 6.14. Схематичное изображение чувствительного элемента ССО точечного типа (электродинамического (а), пьезоэлектрического (б)) и протяженного типа (гидродинамического (в), трибоэлектрического(г))

Классы ССО:

– первый – зона обнаружения близкая по форме к кругу, радиус которого не превышает 3…5 м;

– второй – протяженность зоны обнаружения 10…100 м, ширина 5…20 м.

ССО предназначены для обнаружения человека, перемещающегося со скоростью 0,5...6 м/с.

Факторами, влияющими на характеристики динамических волн в физических средах, являются:

– условия возбуждения колебаний;

– фильтрующие свойства физических сред, обусловленные их характеристиками (упругостью, поглощением), наличием неоднородностей;

– фильтрующие свойства приемной аппаратуры, включая и свойства колебательной системы «приемник–почва».

6.4.4. Магнитометрические средства обнаружения

Магнитометрические средства обнаружения (МСО) предназначены для регистрации факта проноса в их чувствительной зоне предметов, выполненных из металлов или их сплавов (рис. 6.15).

Рис. 6.15. Внешний вид некоторых МСО

По физическим принципам действия существуют следующие магнитометрические средства обнаружения (МСО):

С использованием эффекта переизлучения сигнала (СОП). На передатчик МСО подается опорный сигнал с постоянной частотой и амплитудой, которой он излучается в окружающую среду. За счет явления самоиндукции во встреченном на пути сигнала проводящем предмете наводится ЭДС, которая в свою очередь, вызывает излучение этим предметом «вторичного» поля, т. е. имеет место переизлучение сигнала. Переизлученный сигнал принимается приемником.

Достоинства:

– селективность по объектам из различных металлов и их сплавов;

– направленность системы.

С использованием эффекта переизлучения сигнала с одной катушкой индуктивности для передачи и приема сигналов (СОИН). Катушка индуктивности возбуждается переменным током. При приближении катушки к металлическому предмету сигнал переизлучается, что наводит в ней дополнительную ЭДС.

Достоинства:

– селективность по объектам из различных металлов и их сплавов;

– простота конструкции.

Недостаток – необходимость компенсации параметров катушки от температуры.

С использованием эффекта биения частоты (СОБ). Содержит два генератора МСО-1 и МСО-2 (рис. 6.16). Частота первого стабильна и не зависит от внешних дестабилизирующих факторов, а частота второго может изменяться. Частоты генераторов поступают на устройство сравнения, выделяющее разностную частоту. Сигнал на выходе устройства появляется в случае неравенства частот. Изменение частоты второго генератора происходит за счет измене-

ния параметров колебательного контура, определяющего частоту настройки генератора.

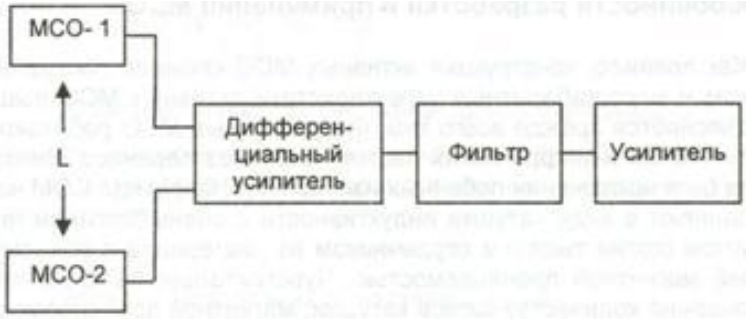


Рис. 6.16. Функциональная схема МСО с использованием эффекта биения частоты

С использованием эффекта самоиндукции (СОИМ). Его принцип действия похож на МСО с использованием эффекта переизлучения сигнала. Отличие заключается в том, что в МСО с использованием эффекта самоиндукции сигнал излучается и принимается в виде одиночных импульсов.

С использованием эффекта локального искажения магнитного поля Земли (магнитометр) (СОМ). Принцип действия этого вида МСО основан на явлении локального искажения магнитного поля Земли ферромагнитными материалами. Он обладает максимальной дальностью обнаружения.

Сравнительная характеристика рассмотренных МСО приведена в табл. 6.3.

Таблица 6.3

Сравнительная характеристика МСО

Тип МСО	Дальность обнаружения пистолета Макарова, м	Возможность селекции цветных металлов	Сравнительная помехоустойчивость
1	2	3	4
СОП	0,5	Имеется возможность определения вида металла	Высокая. Имеется возможность отстройки от внешних дестабилизирующих факторов

Окончание табл. 6.3

1	2	3	4
СОБ	0,1	Отсутствует	Слабая. Имеется возможность паразитной синхронизации
СОИН	0,4	Аналогично СОП	Слабая. Зависит от колебаний температуры
СОИМ	0,5	Отсутствует	Высокая. Имеется возможность отстройки от внешних дестабилизирующих факторов. Является источником помех импульсного характера
СОМ	1	Отсутствует	Слабая. Чувствителен к внешним магнитным полям

6.5. Охранное телевидение

Упрощенно функции охранного телевидения можно свести к двум основным:

– обнаружение;

– идентификация.

Обнаружение на охраняемой территории объектов сводится к предоставлению оператору визуальной информации либо выработке автоматическим устройством сигнала тревоги при обработке соответствующих видеосигналов. Это позволяет с определенной достоверностью вырабатывать суждение о наличии в данный момент тревожной ситуации (а в случае анализа видеозаписей – о том, что тревожная ситуация имела место).

Второй задачей является идентификация объектов (людей, автомобилей и т. д.). Идентификация наиболее важна при анализе видеозаписей, т. е. при расследовании происшествий. Для выполнения идентификации требуется значительно больший по сравнению с обнаружением объем визуальной информации, и здесь на первое место выходит достоверность, а скорость реакции охраны уходит на второй план.

В общем виде систему охранного телевидения можно рассматривать как замкнутую систему управления (рис. 6.17).

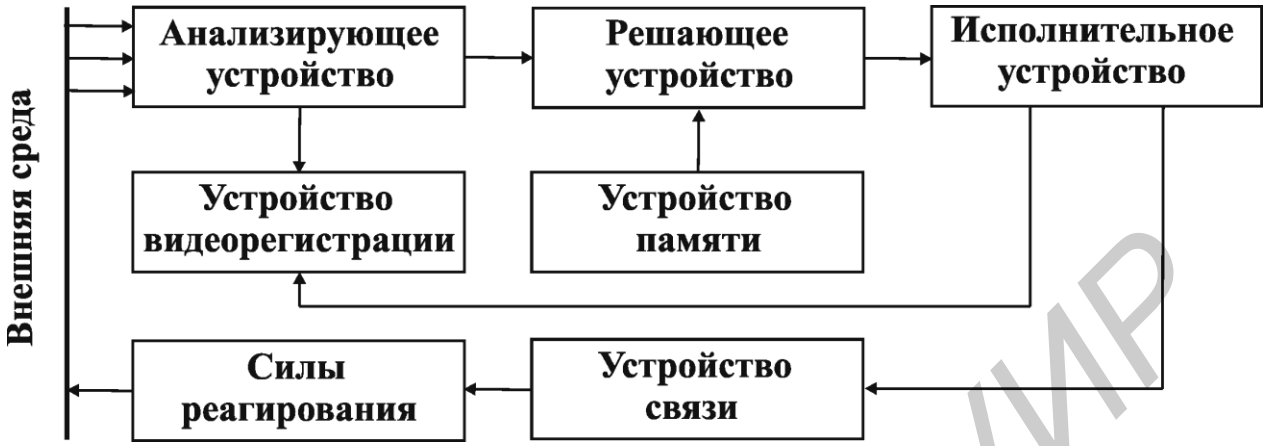


Рис. 6.17. Структурная схема системы охранного телевидения

Анализирующее устройство (видеокамера) (рис. 6.18) воспринимает воздействие из внешней среды и преобразует его к виду, приемлемому для принятия решения.

а б

Рис. 6.18. Внешний вид видеокамеры SANYO VCC-6585P (а) и купольной видеокамеры AXIS 216FD-V (б)

Если в качестве **решающего устройства** выступает человек, то на выходе анализирующего устройства должно присутствовать изображение контролируемой зоны (отображается на мониторе) – реализуется функция **видеонаблюдения.** Если решающим устройством является электронное устройство, то на выходе анализирующего устройства должен быть видеосигнал.

Устройство памяти хранит априорную информацию о возможной опасности (пороговые значения напряжения или кода, соответствующие тревожной ситуации, информация о разрешенных временных «окнах» и т. д.).

Решающее устройство вырабатывает сигнал для исполнительного устройства, с целью получения большей информации оно может автоматически изменять режим работы анализирующего устройства на заранее установленный.

Устройство связи служит для передачи тревожной информации силам реагирования.

Устройство видеорегистрации (цифровой видеорегистратор) служит для организации протокола событий, что позволяет проводить расследование произошедших событий (рис. 6.19). Кроме того, видеозапись позволяет уменьшить и влияние «человеческого фактора» охраны.

Рис. 6.19. Внешний вид цифрового видеорегистратора, встроенного в монитор Pinetron PDR-SC2004

Рассмотрим способы представления визуальной информации оператору.

Параллельный способ. Используется несколько видеомониторов, ко входу каждого из которых подключена видеокамера – при этом образуются независимые параллельные каналы.

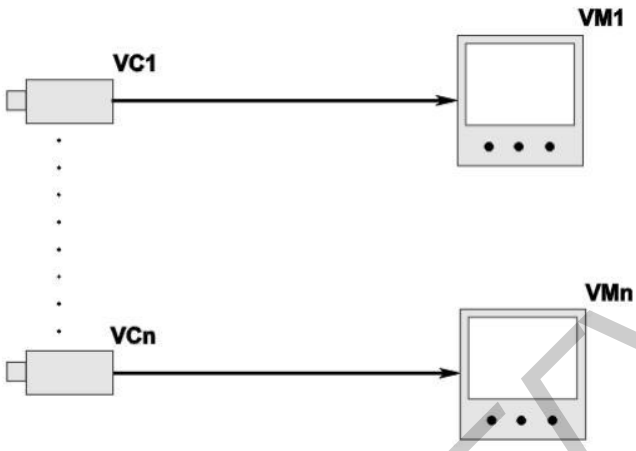


Рис. 6.20. Схематичное изображение параллельного способа передачи визуальной информации

Достоинства:

– простота;

– стоимость ниже, чем с использованием разделителя экрана или видеомультиплексора;

– нет потери информации от оцифровки видеосигналов и переключения видеокамер;

– высокая живучесть системы (замена оборудования из одного канала на оборудование из другого канала).

Недостатки:

– из требований эргономики следует, что количество видеомониторов (каналов) в расчете на одного оператора не должно превышать 6…8;

– при наличии одного устройства видеорегистрации невозможно осуществлять видеозапись по всем каналам одновременно;

– при увеличении числа каналов возрастает занимаемая видеомониторами площадь.

Последовательный способ. Реализуется за счет использования видеокоммутаторов, которые осуществляют коммутацию видеокамер с низкой частотой (секунды или десятки секунд на канал) (рис. 6.21). Видеокоммутаторы являются простейшими и самыми экономичными устройствами обработки видеосигналов (рис. 6.22).

Рис. 6.21. Внешний вид видеокоммутатора

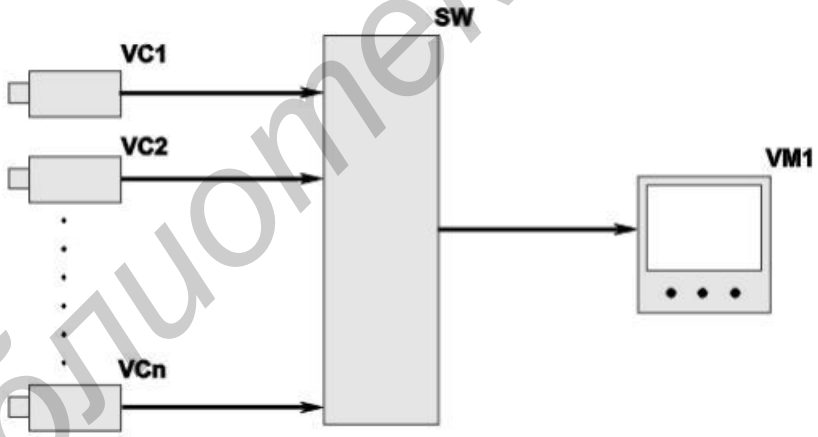


Рис. 6.22. Схематичное изображение способа передачи визуальной информации с использованием видеокоммутатора

Такой способ передачи визуальной информации характеризуется неконтролируемым временем. **Неконтролируемое время** – промежуток времени, в течение которого сигнал с данной видеокамеры на экран видеомонитора и устройство видеозаписи не поступает (рис. 6.23).

Для облегчения работы оператора некоторые видеокоммутаторы содержат **входы тревоги.** При срабатывании датчика системы обнаружения на видеомониторе появляется изображение тревожной зоны, включается акустическая и оптическая сигнализация. При одновременном срабатывании нескольких датчиков тревожные зоны отображаются поочередно в соответствии с выбранным временем наблюдения.

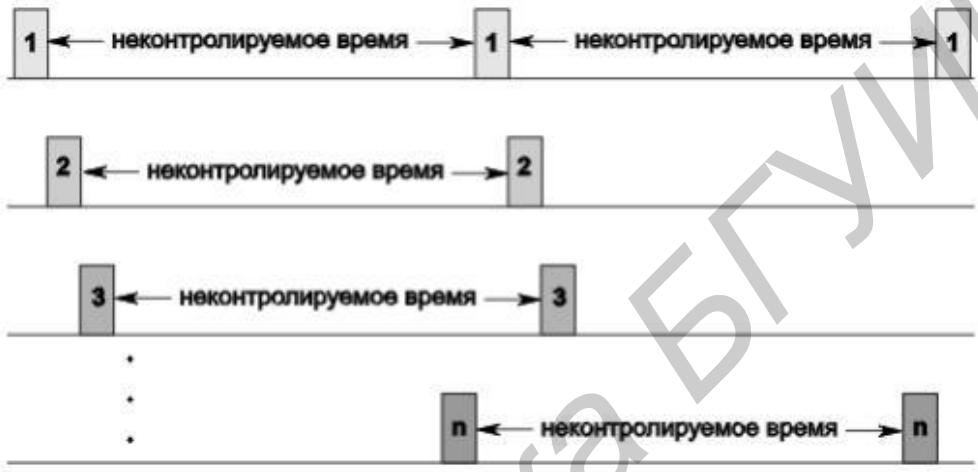


Рис. 6.23. Схематичное изображение передачи сигналов видеокамер на вход монитора с использованием видеокоммутатора

Достоинства:

– простота обслуживания;

– отсутствие потери качества изображения, вызванного оцифровкой;

– возможность использования видеомониторов небольшого размера.

Недостатки:

– наличие неконтролируемого времени;

– быстрое утомление оператора при непрерывном переключении каналов;

– невозможность осуществления видеозаписи по всем каналам одновременно с помощью одного видеомагнитофона.

Разделители экрана (квадраторы) (рис. 6.24) позволяют одновременного отображать на экране видеомонитора изображения от четырех видеокамер (рис. 6.25).

Рис. 6.24. Внешний вид квадратора Polyvision PVQ-602

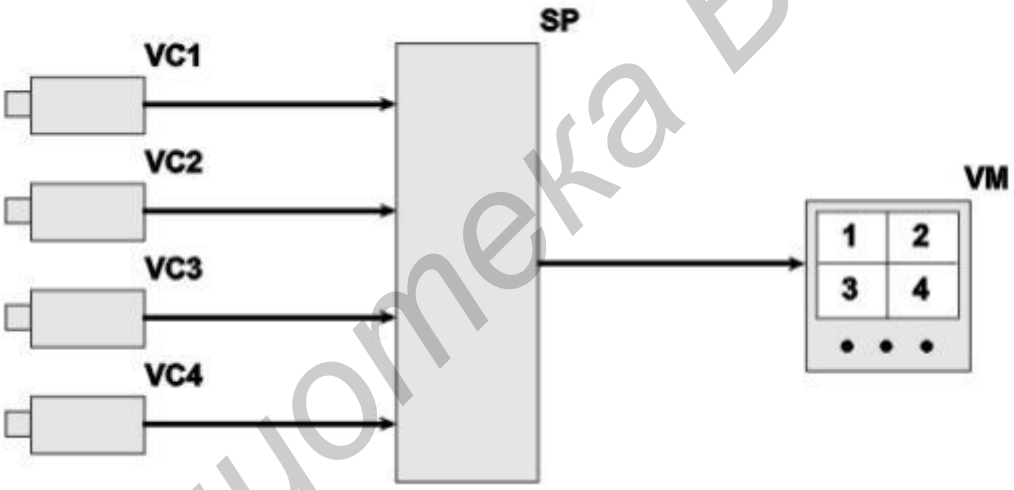


Рис. 6.25. Схематичное изображение способа передачи визуальной информации с использованием квадратора

Достоинства:

– практически отсутствует потеря информации на время переключения видеокамер;

– последовательное отображение на видеомониторе полноэкранных изображений (в ручном или автоматическом режимах).

Четырем сегментам на экране видеомонитора соответствует четыре области памяти разделителя экрана, обновление которых может осуществляться либо последовательно, либо параллельно.

При необходимости получения изображений с помощью одного разделителя экрана более чем от 4 видеокамер может использоваться **двухстраничный разделитель экрана** (8 видеовходов, коммутируемых группами по 4) (рис. 6.26).

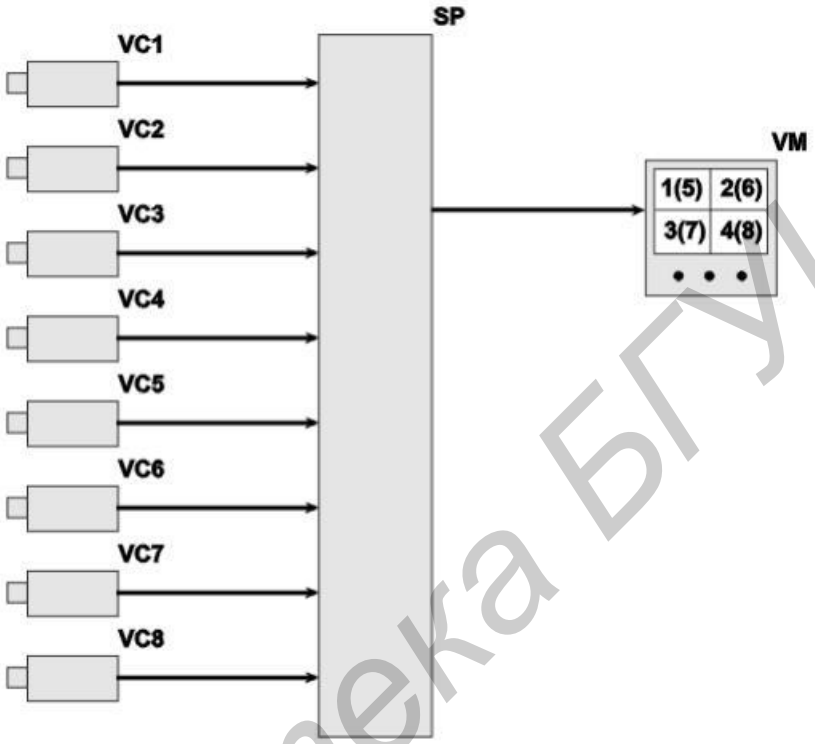


Рис. 6.26. Схематичное изображение способа передачи визуальной информации с использованием двухстраничного квадратора

Недостатки:

– наличие неконтролируемого время для видеокамер;

– не позволяют получить видеозапись приемлемого качества (выходной сигнал подвергается цифровой обработке, что снижает разрешающую способность).

Видеомультиплексор (рис. 6.27) – устройство для организация видеозаписи с минимальными потерями сигналов от нескольких видеокамер на один охранный видеомагнитофон (рис. 6.28).

Видеомультиплексор формирует на своем выходе мультиплексированный видеосигнал, получаемый переключением видеокамер с частотой полей.

Достоинство – на видеомагнитофон поступают с частотой полей видеосигналы, соответствующие полноэкранному отображению.

Рис. 6.27. Внешний вид видеомультиплексора Samsung SDM-160MP

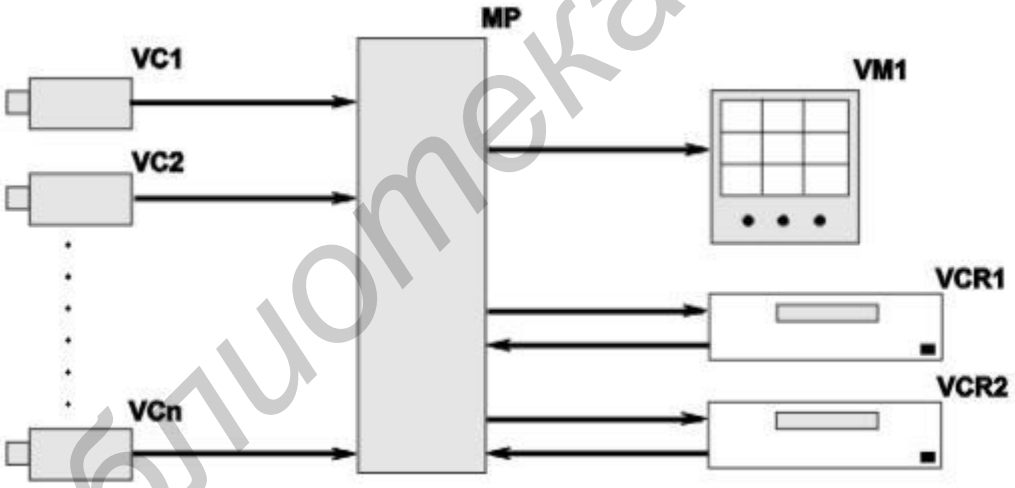


Рис. 6.28. Схематичное изображение способа передачи визуальной информации с использованием видеомультиплексора

Повышение информативности отдельных каналов может достигаться за счет уменьшения информативности оставшихся каналов (перераспределение потоков видеоинформации). Для ускорения обновления информации порядок коммутации каналов может изменяться. В этом случае возможны следующие режимы:

– приоритетный (переключение каналов происходит не по порядку: к каналу с тревогой обращение идет чаще, каждый раз после обращения к очередному каналу);

– эксклюзивный (отображаются только каналы с тревогой).

По функциональным возможностям видеомультиплексоры делятся на следующие виды:

– симплексные – отображают мультисценовое изображение в данный момент только в одном режиме (например, без записи);

– дуплексные – обеспечивают видеозапись на одном видеорегистраторе с одновременным видеонаблюдением в мультисценовом режиме или просмотром записанного с другого видеорегистратора на дополнительном видеомониторе;

– триплексные – на экране видеомонитора одновременно могут отображаться мультисценовые изображения, наблюдаемые и воспроизводимые с видеорегистратора.

6.6. Системы контроля и управления доступом

Под системой контроля и управления доступом (СКУД) (рис. 6.29) понимают объединенные в комплексы технические средства, обеспечивающие возможность доступа определенных лиц в определенные зоны (территория, здание, помещение) или к определенной аппаратуре, техническим средствам и предметам (ПЭВМ, автомобиль, сейф и т. д.) и ограничивающие доступ лиц, не имеющих такого права.

Рис. 6.29. Структурная схема СКУД

Состав СКУД:

– устройства ввода идентификационных признаков;

– устройства управления;

– исполнительные устройства (управляемые преграждающие устройства).

Идентификация – процедура распознавания субъекта по его идентификатору.

Идентификатор – уникальный признак субъекта доступа.

В процессе идентификации субъект предъявляет системе свой идентификатор и она проверяет его наличие в своей базе данных. Субъекты с известными системе идентификаторами считаются легальными (законными), остальные субъекты относятся к нелегальным.

Способы ввода идентификатора:

– ручной, осуществляемый путем нажатия клавиш, поворота переключателей и т. д.;

– контактный в результате непосредственного контакта между считывателем и идентификатором;

– дистанционный (бесконтактный) при поднесении идентификатора к считывателю на определенное расстояние.

Аутентификация – процедура проверки подлинности субъекта, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует.

Авторизация – процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации.

По способу управления преграждающими устройствами СКУД можно классифицировать:

– автономные (локальные) – для управления одним или несколькими преграждающими устройствами без передачи информации на центральный пульт и без контроля со стороны оператора;

– централизованные (сетевые) – для управления преграждающими устройствами с обменом информацией с центральным пультом, контролем и управлением системой со стороны оператора;

– универсальные (включающие функции автономных и сетевых систем) – работают в сетевом режиме под руководством центрального устройства управления и переходят в автономный режим при возникновении отказов в сетевом оборудовании или центральном устройстве.

По количеству точек доступа и пользователей СКУД можно разделить:

– малые – единицы точек доступа (офисы);

– средние – десятки точек доступа и тысячи пользователей (банки, предприятия, учреждения, гостиницы);

– большие – сотни точек доступа и десятки тысяч пользователей (крупные промышленные предприятия, аэропорты).

6.6.1. Автономные СКУД

Автономные системы – предназначены для обеспечения контроля и управления доступом в отдельное помещение.

Состав автономных СКУД:

– автономный контроллер – хранит базу данных идентификаторов и управляет работой остальных элементов системы;

– электромагнитный замок – используется в качестве исполнительного устройства;

– датчик положения двери – обеспечивает правильность работы всей системы;

– считыватель для устройств идентификации;

– кнопка открывания двери изнутри.

Для идентификации пользователя используются различные типы карт с соответствующими считывателями (магнитные, Proximity, Touch Memory и т. д.).

Автономные системы с накоплением информации – отличием является возможность системы накапливать информацию о всех фактах входа–выхода через точку прохода (в формате: время, дата, идентификационный номер).

Рис. 6.30. Структурная схема автономной СКУД

Рис. 6.31. Структурная схема автономной СКУД с накоплением информации

Данная информация хранится в памяти контролера и может быть по необходимости востребована. Для получения информации и представления её в

наглядном виде используется специальное программное обеспечение. Программное обеспечение позволяет оператору системы решать задачи: отслеживания перемещения сотрудников по территории, учета рабочего времени сотрудников, визуально контролировать личность владельца устройства идентификации.

6.6.2. Сетевые СКУД

Сетевые системы предназначены для обеспечения контроля и управления доступом на крупных объектах (банки, учреждения, предприятия и т. п.) (рис. 6.32, 6.33).

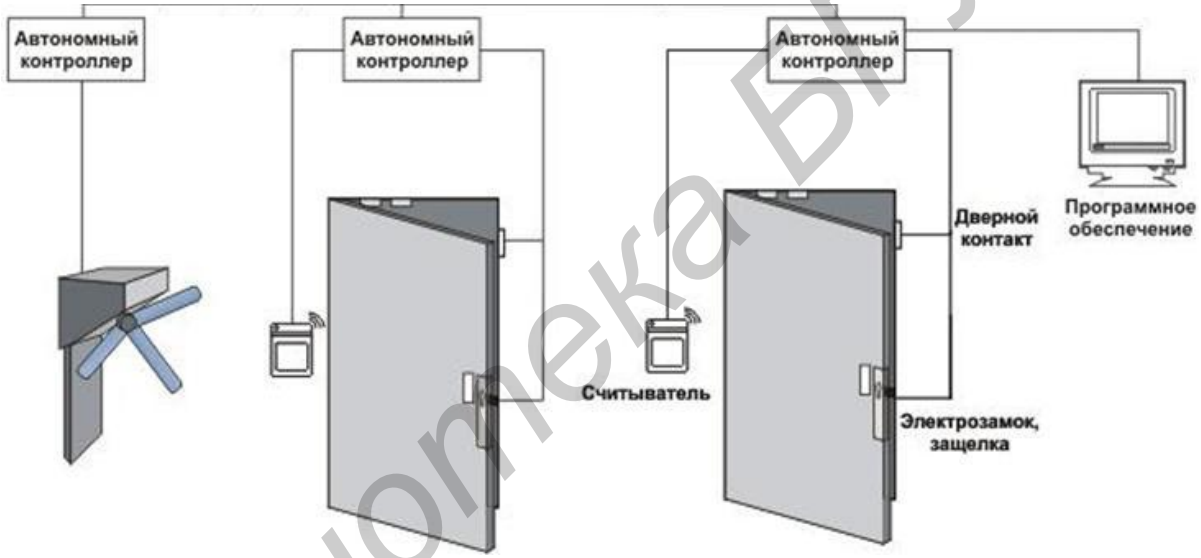


Рис. 6.32. Структурная схема сетевой СКУД

6.7. Управляемые преграждающие устройства

Для управления доступом на объект применяют турникеты и шлюзовые кабины (шлюзы), в помещение – двери с электромагнитными и электромеханическими замками, открываемыми вручную или автоматически.

Турникеты делятся по виду перекрытия прохода на следующие виды (рис. 6.34):

– с частичным перекрытием;

– полным перекрытием.

Турникеты делятся по способу управления на следующие виды:

– ручное (ножное);

– полуавтоматическое;

– автоматическое.

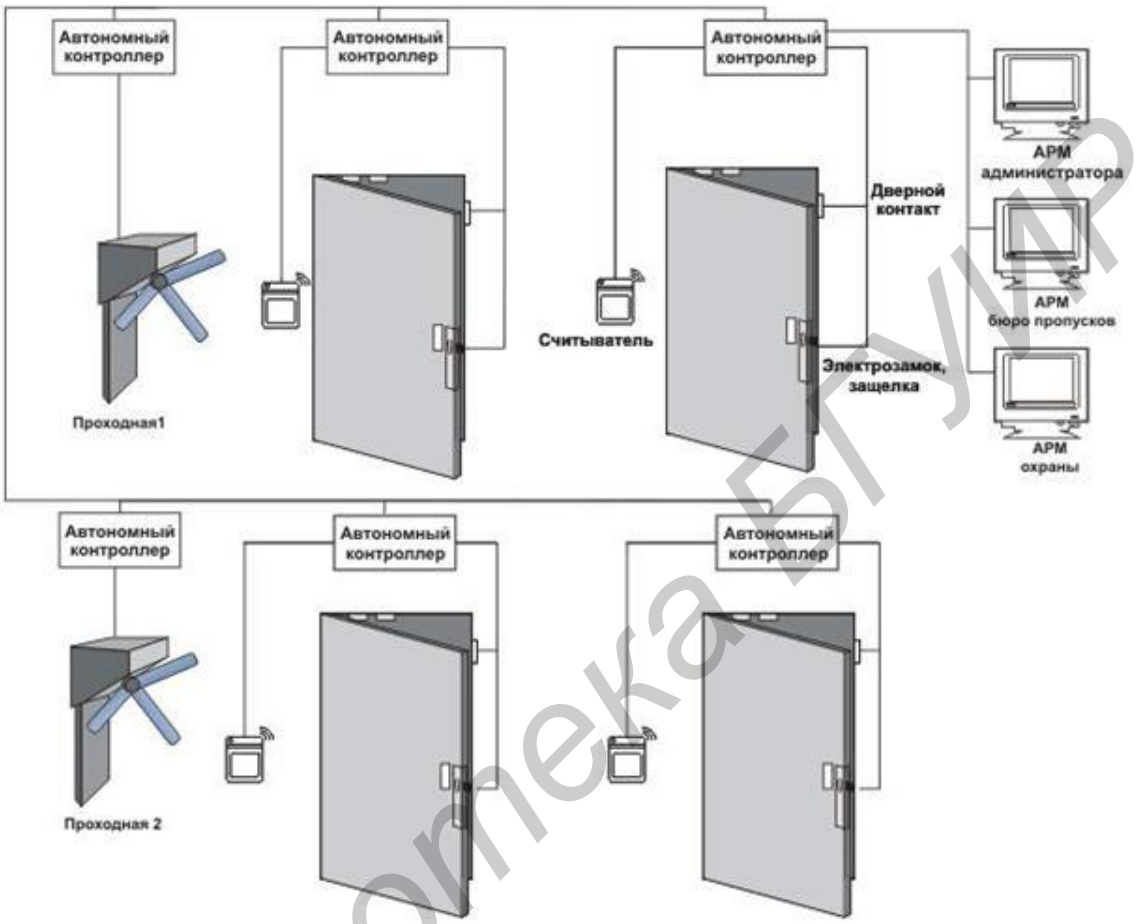


Рис. 6.33. Структурная схема сетевой СКУД крупного объекта

а

б

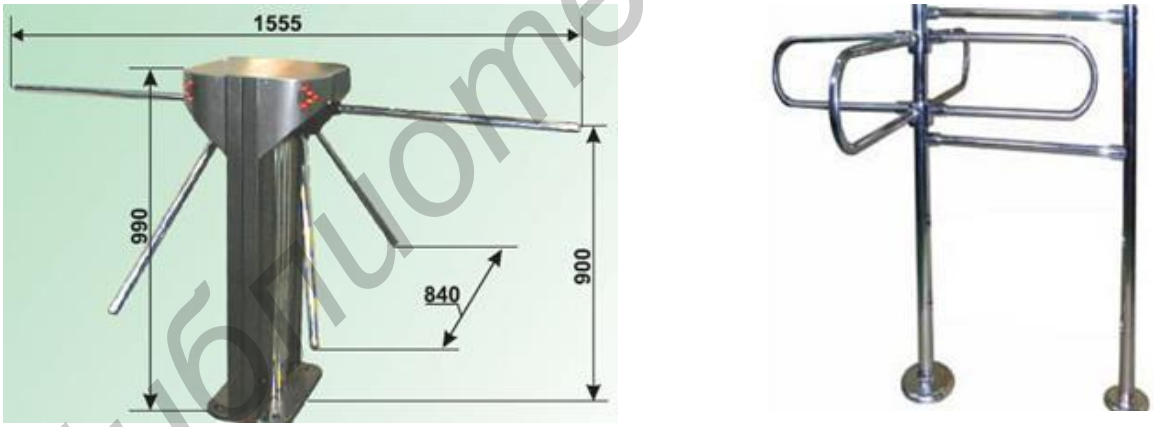
Рис. 6.34. Внешний вид турникетов с частичным перекрытием (а) и полным перекрытием (б) прохода

Турникеты бывают «нормально открытые» и «нормально закрытые» (рис. 6.35), а также поясные и в полный рост.

а б

Рис. 6.35. Внешний вид «нормально открытых» (а) и «нормально закрытых» (б) турникетов

Наиболее распространены трехлопастные турникеты с вращающимся в одном направлении преграждающимся устройством – **триподы** и **роторные** (рис. 6.36). Они обеспечивают гарантированный единовременный проход одного человека.



а б

Рис. 6.36. Внешний вид трипода (а) и роторного (б) турникетов

Достоинства:

– высокая пропускная способность;

– дешевле шлюзовых кабин.

Недостаток – конструкция триподов и роторных турникетов не мешает задерживаемому применить против сотрудников охраны оружие.

Для систем управления доступом с высоким уровнем защиты применяют управляемые преграждающие устройства закрытого типа – шлюзовые кабины (рис. 6.37).

Рис. 6.37. Внешний вид шлюзовой кабины

Шлюзовая кабина тамбурного типа представляет собой закрытую конструкцию с двумя дверями, которые одновременно не открываются. После прохода человека в шлюз входная дверь закрывается, проводится его аутентификация и по разрешающей команде контролера СКУД открывается выходная дверь, расположенная уже на территории организации. В случае отказа на допуск обе двери блокируются для выяснения службой безопасности личности находящегося в шлюзе человека.

Шлюзовые кабины делятся на следующие виды:

– полуавтоматические;

– автоматические.

В полуавтоматических шлюзовых кабинах применяются распашные двери, которые открываются вручную и закрываются доводчиком (рис. 6.38), но блокируются с помощью электромагнитных или электромеханических замков, управляемых контроллером.

В автоматических шлюзовых кабинах двери открываются и закрываются с помощью электромеханических приводов, управляемых контроллером СКУД.

Рис. 6.38. Внешний вид доводчика, установленного на дверном полотне

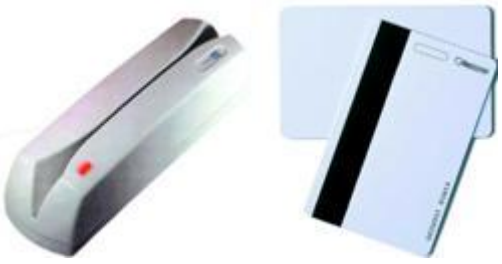
В шлюзовые кабины могут устанавливаться:

– считыватели (рис. 6.39);

– датчики вносимых или выносимых предметов (оружия, взрывчатых, радиоактивных веществ).

а

б



в

Рис. 6.39. Внешний вид считывателя и устройств Touch Memory (а), Proximity (б), магнитных карт (в)

Закрытая конструкция шлюза оказывает психологическое давление на человека, стремящегося проникнуть на территорию организации без надежных документов.

Двери и стены шлюзов выполняются из ударопрочного стекла или пластика.

Турникеты и шлюзовые кабины имеют механическую устойчивость:

– нормальную;

– повышенную (взлом посредством нанесения ударов и применения различных инструментов);

– высокую устойчивость (пуле- и взрывоустойчивость сплошного перекрытия проходного проема).

6.8. Контрольные вопросы

1. В соответствие с какими критериями объекту присваивают ту или иную категорию?

2. С какой целью классифицируют помещения и территории объекта?

3. Каким техническим параметром характеризуются инженерные заграждения?

4. По каким критериям классифицируются заграждения?

5. Какие критерии предъявляются к техническим средствам охраны периметра объекта?

6. Дайте краткую характеристику техническим средствам охраны периметра.

7. Какие функции выполняет охранное телевидение?

8. Какие устройства входят в состав системы охранного телевидения?

9. Дайте краткую характеристику способам представления визуальной информации оператору.

10. Какие устройства входят в систему контроля и управления доступом?

11. В чем различие между автономными и сетевыми системами контроля и управления доступом?

12. Дайте краткую классификацию управляемым преграждающим устройствам.

7. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

7.1. Основы построения криптосистем

Криптография – наука о методах, алгоритмах, программных и аппаратных средствах преобразования информации в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования.

Исторически сложилось так, что криптография длительное время использовалась исключительно как средство обеспечения конфиденциальности сообщений. Областью применения криптографии была область защиты государственной тайны: в военной, дипломатической и разведывательной сферах. Поэтому естественно, что криптография находилась в руках спецслужб. Всякие упоминания об этой науке в открытой печати были запрещены, хотя работы велись полным ходом, огромное число специалистов трудилось в этой области: математики, инженеры, разведчики. Криптографическая империя СССР противостояла аналогичной империи США. Часть специалистов трудилась над созданием стойких криптоалгоритмов, другая часть – над раскрытием чужих криптосистем.

В конце XX века обстановка в сфере использования криптографии коренным образом меняется. Здесь несколько причин. Главная – бурное развитие вычислительной техники, появление на этой базе информационных технологий. Доступность информационных технологий широкому кругу коммерческих компаний и частным лицам породила потребность, во-первых, обеспечивать конфиденциальность той информации, которая циркулирует в телекоммуникационных системах (ТКС), во-вторых, обеспечивать ряд функций, таких, как аутентификация субъектов системы, целостность сообщений, истинность документов и т. д. Оказалось, что все это можно обеспечить, используя принципы криптографии.

Криптография, обслуживающая задачи управления, бизнеса, телекоммуникаций, получила название открытой. Открытые криптотехнологии (ЭЦП,

идентификация и аутентификация, защита от несанкционированного доступа (НСД)) становятся коммерческими продуктами и распространяются без особых ограничений. Платежные системы: банковские, индивидуальные на основе пластиковых карт, локальные и корпоративные компьютерные сети – вот далеко не полный перечень применения криптографических технологий.

Наряду с решением задач обеспечения конфиденциальности, целостности и доступности информации существует задача анализа стойкости используемых криптопреобразований. Эта задача решается наукой, называемой криптоанализ. Криптография и криптоанализ составляют науку **криптологию**.

7.1.1. Общие принципы криптографической защиты информации

Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, имеет вид, представленный на рис. 7.1.

Отправитель генерирует открытый текст исходного сообщения *M*, которое должно передаваться по открытому каналу. Отправитель шифрует текст с помощью обратимого преобразования E и ключа К: $E_к$ и получает шифротекст $C = E_к(M)$, который отправляет получателю. Получатель, приняв шифротекст C, расшифровывает его с помощью обратного преобразования $D = E_К^{-1}$ и получает исходное сообщение в виде открытого текста $M : M = D(C) = E_К^{-1}(E_К(M))$.

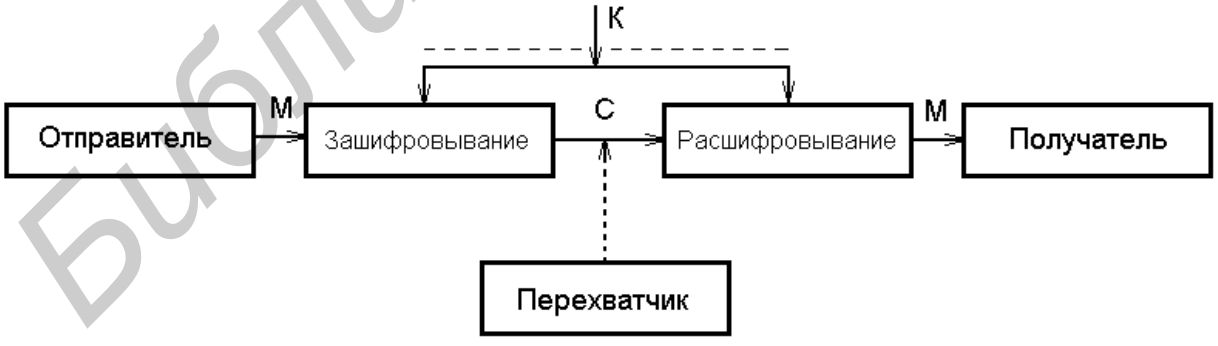


Рис. 7.1. Обобщенная схема симметричной криптографической системы

Преобразование $E_к$ выбирается из семейства криптографических преобразований, называемых **криптоалгоритмами**. Параметр, с помощью которого выбирается конкретное преобразование, называется **криптографическим**

ключом К. Система, в которой осуществляется зашифровывание и расшифровывание сообщений, называется **криптосистемой**.

Формально криптосистема – это однопараметрическое семейство $E_{\mathrm{K}\ \mathrm{K}\in\overline{\mathrm{K}}}$ обратимых преобразований $E_{\mathrm{K}}:\overline{M}\to\overline{C}$ из пространства $\overline{M}$ сообщений открытого текста в пространство $\overline{C}$ шифрованных текстов. Параметр К (ключ) выбирается из конечного множества $\overline{\mathrm{K}}$, называемого пространством ключей. Криптосистема может иметь разные варианты реализации: набор инструкций, аппаратные или программные средства, аппаратно-программные средства.

Вообще говоря, преобразование зашифровывания может быть симметричным или асимметричным относительно преобразования расшифровывания. Поэтому различают два класса криптосистем: симметричные криптосистемы и асимметричные криптосистемы. Иногда их называют: одноключевые (с секретным ключом) и двухключевые (с открытым ключом). Схема симметричной криптосистемы с одним секретным ключом К была показана на рис. 7.1. Обобщенная схема асимметричной криптосистемы с двумя разными ключами K_1 и K_2 показана на рис. 7.2.

В этой криптосистеме один из ключей является открытым K_1, а другой K_2 – секретным. Для этой криптосистемы $C=E_{\mathrm{K}_1}\ M$, а $M=D_{\mathrm{K}_2}\ C\ =E_{\mathrm{K}_2}^{-1}\ E_{\mathrm{K}_1}\ M$.

В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей, например спецсвязью. В асимметричной криптосистеме передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют в месте его генерации.

Злоумышленник при атаке на криптосистему может не только считывать шифротексты, передаваемые по каналу связи, но и пытаться их изменить по своему усмотрению.

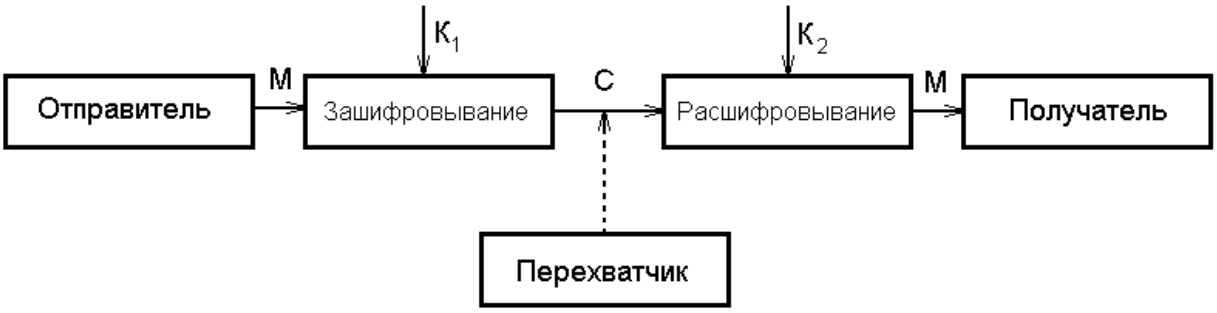


Рис. 7.2. Обобщенная схема асимметричной криптографической системы

Любая попытка со стороны злоумышленника расшифровать шифротекст C для получения открытого текста M или зашифровать свой собственный текст M^1 для получения правдоподобного шифротекста C^1, не имея подлинного ключа, называется криптоатакой.

Свойство криптосистемы противостоять криптоатаке называется криптостойкостью. Оно измеряется в затратах злоумышленника, которые он несет, вскрывая криптосистему. Например, криптостойкость может выражаться в количестве машинного времени, затраченного на вскрытие криптосистемы.

Фундаментальное правило криптоанализа, впервые сформулированное голландцем А. Керкхоффом еще в XIX веке заключается в том, что стойкость шифра (криптосистемы) должна определяться только секретностью ключа. Иными словами, правило Керкхоффа состоит в том, что весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитику противника. Это обусловлено тем, что криптосистема, реализующая семейство криптографических преобразований, обычно рассматривается как открытая система. Такой подход отражает очень важный принцип технологии защиты информации: защищенность системы не должна зависеть от секретности чего-либо такого, что невозможно быстро изменить в случае утечки секретной информации. Обычно криптосистема представляет собой совокупность аппаратных и программных средств, которую можно изменить только при значительных затратах времени и средств, тогда как ключ является легко изменяемым объектом.

Именно поэтому стойкость криптосистемы определяется только секретностью ключа.

Другое, почти общепринятое допущение в криптоанализе состоит в том, что криптоаналитик имеет в своем распоряжении шифротексты сообщений.

Существует четыре основных типа криптоаналитических атак. Конечно, все они формулируются в предположении, что криптоаналитику известны применяемый алгоритм шифрования и шифротексты сообщений. Перечислим эти криптоаналитические атаки.

1. Криптоаналитическая атака при наличии только известного шифротекста. Криптоаналитик имеет только шифротексты $C_1, C_2, ..., C_i$ нескольких сообщений, причем все они зашифрованы с использованием одного и того же алгоритма шифрования $E_{\text{К}}$. Работа криптоаналитика заключается в том, чтобы раскрыть исходные тексты $M_1, M_2, ..., M_i$ по возможности большинства сообщений или, еще лучше, вычислить ключ К, использованный для зашифровывания этих сообщений, с тем, чтобы расшифровать и другие сообщения, зашифрованные этим ключом.

2. Криптоаналитическая атака при наличии известного открытого текста. Криптоаналитик имеет доступ не только к шифротекстам $C_1, C_2, ..., C_i$ нескольких сообщений, но также к открытым текстам $M_1, M_2, ..., M_i$ этих сообщений. Его работа заключается в нахождении ключа К, используемого при шифровании этих сообщений, или алгоритма расшифровывания $D_{\text{К}}$ любых новых сообщении, зашифрованных тем же самым ключом.

3. Криптоаналитическая атака при возможности выбора открытого текста. Криптоаналитик не только имеет доступ к шифротекстам $C_1, C_2, ..., C_i$ и связанным с ними открытым текстам $M_1, M_2, ..., M_i$ нескольких сообщений, но и может по желанию выбирать открытые тексты, которые затем получает в зашифрованном виде. Такой криптоанализ получается более мощным по сравнению с криптоанализом с известным открытым текстом, потому что криптоана-

литик может выбрать для шифрования такие блоки открытого текста, которые дадут больше информации о ключе. Работа криптоаналитика состоит в поиске ключа К, использованного для шифрования сообщений, или алгоритма расшифровывания D_K новых сообщений, зашифрованных тем же ключом.

4. Криптоаналитическая атака с адаптивным выбором открытого текста. Это особый вариант атаки с выбором открытого текста. Криптоаналитик может не только выбирать открытый текст, который затем шифруется, но и изменять свой выбор в зависимости от результатов предыдущего шифрования. При криптоанализе с простым выбором открытого текста криптоаналитик обычно может выбирать несколько крупных блоков открытого текста для их шифрования, при криптоанализе с адаптивным выбором открытого текста он имеет возможность выбрать сначала более мелкий пробный блок открытого текста, затем выбрать следующий блок в зависимости от результатов первого выбора и т. д. Эта атака предоставляет криптоаналитику еще больше возможностей, чем предыдущие типы атак.

Кроме перечисленных криптоаналитических атак существует силовая атака (перебор всех возможных значений ключа). С появлением мощных компьютеров и сетей этот вид атаки становится очень актуальным. Он может сочетаться с перечисленными ранее аналитическими атаками. В связи с этим ключ криптосистемы должен обладать определенными свойствами: если рассматривать его совокупность двоичных знаков, то это должна быть случайная равномерно распределенная последовательность длины, которая делала бы перебор всех возможных значений ключа практически невозможным.

7.1.2. Блочные и поточные шифры

Применение функции шифрования ко всему сообщению в целом реализуется очень редко. Практически все применяемые криптографические методы связаны с разбиением сообщения на большое число фрагментов (или знаков) фиксированного размера, каждый из которых шифруется отдельно. Такой под-

ход существенно упрощает задачу шифрования, так как сообщения обычно имеют различную длину.

Можно выделить следующие характерные признаки методов шифрования данных:

– выполнение операций с отдельными битами или блоками;

– зависимость или независимость функции шифрования от результатов шифрования предыдущих частей сообщения;

– зависимость или независимость шифрования отдельных знаков от их положения в тексте.

В соответствии с этим различают три основных способа шифрования:

– поточные шифры;

– блочные шифры;

– блочные шифры с обратной связью.

1. Поточное шифрование. Состоит в том, что каждый бит открытого текста и соответствующий бит ключа преобразовываются по определенному алгоритму (например складываются по модулю 2). К достоинствам поточных шифров относятся высокая скорость шифрования, относительная простота реализации и отсутствие размножения ошибок. Недостатком является необходимость использовать для каждого сообщения другой ключ. Это обусловлено тем, что если два различных сообщения шифруются на одном и том же ключе, то эти сообщения легко могут быть расшифрованы ($C_1 = M_1 + \mathrm{K}, C_2 = M_2 + \mathrm{K}, C_1 + C_2 = M_1 + M_2$, считая M_2 ключом, можно вычислить M_1, т. к. M_2 не обладает свойствами ключа). Поэтому часто используют дополнительный, случайно выбираемый ключ сообщения, который передается в начале сообщения и применяется для модификации ключа шифрования. В результате разные сообщения будут шифроваться с помощью различных последовательностей. Это требует передачи информации синхронизации перед заго-

ловком сообщения, которая должна быть принята до расшифровывания любого сообщения.

Поточные шифры широко применяются для шифрования преобразованных в цифровую форму речевых сигналов и цифровых данных, требующих оперативной доставки потребителю информации.

2. Блочное шифрование. При блочном шифровании открытый текст сначала разбивается на равные по длине блоки, затем применяется зависящая от ключа функция шифрования для преобразования блока открытого текста длиной m бит в блок шифротекста такой же длины. При блочном шифровании каждый бит блока шифротекста зависит от значений всех бит соответствующего блока открытого текста и никакие два блока открытого текста не могут быть представлены одним и тем же блоком шифротекста. При этом небольшие изменения в шифротексте вызывают большие и непредсказуемые изменения в соответствующем открытом тексте и наоборот. Вместе с тем применение блочного шифра имеет серьезные недостатки. Первый из них заключается в том, что вследствие детерминированного характера шифрования при фиксированной длине блока 64 бита можно осуществить криптоанализ шифротекста «со словарем» в ограниченной форме. Это обусловлено тем, что идентичные блоки открытого текста длиной 64 бита в исходном сообщении представляются идентичными блоками шифротекста, что позволяет криптоаналитику сделать определенные выводы о содержании сообщения. Другой потенциальный недостаток этого шифра связан с размножением ошибок. Результатом изменения только одного бита в принятом блоке шифротекста будет неправильное расшифровывание всего блока. Это, в свою очередь, приведет к появлению искаженных бит (от 1 до 64) в восстановленном блоке исходного текста.

Из-за отмеченных недостатков блочные шифры редко применяются в указанном режиме для шифрования длинных сообщений. Однако в финансовых

учреждениях, где сообщения часто состоят из одного или двух блоков, блочные шифры широко используют в режиме прямого шифрования. Такое применение обычно связано с возможностью частой смены ключа шифрования, поэтому вероятность шифрования двух идентичных блоков открытого текста на одном и том же ключе очень мала.

Криптосистема с открытым ключом также является системой блочного шифрования и должна оперировать блоками довольно большой длины. Это обусловлено тем, что криптоаналитик знает открытый ключ шифрования и мог бы заранее вычислить и составить таблицу соответствия блоков открытого текста и шифротекста. Если длина блоков мала, например 30 бит, то число возможных блоков не слишком большое (при длине 30 бит это $2^{30} \approx 10^9$), и может быть составлена полная таблица, позволяющая моментально расшифровать любое сообщение с использованием известного открытого ключа.

3. Блочное шифрование с обратной связью. Как и при блочном шифровании, сообщения разбивают на ряд блоков, состоящих из m бит. Для преобразования этих блоков в блоки шифротекста, которые также состоят из m бит, используются специальные функции шифрования. Однако если в блочном шифре такая функция зависит только от ключа, то в блочных шифрах с обратной связью она зависит как от ключа, так и от одного или более предшествующих блоков шифротекста.

Практически важным шифром с обратной связью является шифр со сцеплением блоков шифротекста. В этом случае m бит предыдущего шифротекста суммируются по модулю 2 со следующими m битами открытого текста, а затем применяется алгоритм блочного шифрования под управлением ключа для получения следующего блока шифротекста. Достоинством криптосистем блочного шифрования с обратной связью является возможность применения их для обнаружения манипуляций сообщениями, производимых активными перехватчиками. При этом используется факт размножения ошибок в таких шиф-

рах, а также способность этих систем легко генерировать код аутентификации сообщений. Поэтому системы шифрования с обратной связью используют не только для шифрования сообщений, но и для их аутентификации. Криптосистемам блочного шифрования с обратной связью свойственны некоторые недостатки. Основным из них является размножение ошибок, так как один ошибочный бит при передаче может вызвать ряд ошибок в расшифрованном тексте. Другой недостаток связан с тем, что разработка и реализация систем шифрования с обратной связью часто оказываются более трудными, чем систем поточного шифрования.

На практике для шифрования длинных сообщений применяют поточные шифры или шифры с обратной связью. Выбор конкретного типа шифра зависит от назначения системы и предъявляемых к ней требований.

7.2. Симметричные криптосистемы

7.2.1. Основные понятия и определения

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур зашифровывания–расшифровывания. В соответствии со стандартом ГОСТ 28147–89 под шифром понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования.

Ключ – это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма. Основной характеристикой шифра является криптостойкость, которая определяет его стойкость к раскрытию методами криптоанализа. Обычно эта характеристика определяется интервалом времени, необходимым для раскрытия шифра.

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований:

– достаточная криптостойкость (надежность закрытия данных);

– простота процедур шифрования и расшифровывания;

– незначительная избыточность информации за счет шифрования;

– нечувствительность к небольшим ошибкам шифрования и др.

В той или иной мере этим требованиям отвечают:

– шифры перестановок;

– шифры замены;

– шифры гаммирования;

– шифры, основанные на аналитических преобразованиях шифруемых данных.

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста. При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены.

Шифрование гаммированием заключается в том, что символы шифруемого текста складываются с символами некоторой случайной последовательности, именуемой гаммой шифра. Стойкость шифрования определяется в основном длиной (периодом) неповторяющейся части гаммы шифра. Поскольку с помощью ЭВМ можно генерировать практически бесконечную гамму шифра, то данный способ является одним из основных для шифрования информации в автоматизированных системах.

Шифрование аналитическим преобразованием заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле). Например, можно использовать правило умножения вектора на матрицу, причем умножаемая матрица является ключом шифрования (поэтому ее размер и содержание должны храниться в секрете), а символами умножаемого вектора последовательно служат символы шифруемого текста.

Процессы зашифровывания и расшифровывания осуществляются в рамках некоторой криптосистемы. Характерной особенностью симметричной криптосистемы является применение одного секретного ключа как при зашифровывании, так и при расшифровывании сообщений.

Как открытый текст, так и шифротекст образуются из букв, входящих в конечное множество символов, называемое алфавитом. Примерами алфавитов являются конечное множество всех заглавных букв, конечное множество всех заглавных и строчных букв и цифр и т. п. В общем случае некоторый алфавит можно представить как $\sum = a_0, a_1, \ldots, a_{m-1}$.

Объединяя по определенному правилу буквы из алфавита Σ, можно создать новые алфавиты:

– алфавит $\sum^2$ содержит m^2 биграмм $a_0a_0, a_0a_1, \ldots, a_{m-1}a_{m-1}$;

– алфавит $\sum^3$ содержит m^3 триграмм $a_0a_0a_0, a_0a_0a_1, \ldots, a_{m-1}a_{m-1}a_{m-1}$.

В общем случае, объединяя по n букв, получаем алфавит $\sum^n$, содержащий m^n – n-грамм. Например, английский алфавит $ABCD...XYZ$ объемом $m = 26$ букв позволяет сгенерировать $26^2 = 676$ биграмм $AA, AB, ..., ZZ$, $26^3 = 17576$ триграмм $AAA, AAB, ...ZZY, ZZZ$.

При выполнении криптографических преобразований полезно заменить буквы алфавита целыми числами $0, 1, 2, ...$ Это позволяет упростить выполнение необходимых алгебраических манипуляций. Например, можно установить взаимно-однозначное соответствие между русским алфавитом {АБВГ…ЮЯ} и

множеством целых чисел $\sum_{32} = 0,1,2,...,31$, между английским алфавитом {ABCD…YZ} и множеством целых чисел $\sum_{32} = 0,1,2,...,26$.

В дальнейшем будет обычно использоваться алфавит $\bar{\sum}_m = 0,1,2,...,m-1$, содержащий m «букв» в виде чисел. Замена букв традиционного алфавита числами позволит более четко сформулировать основные концепции и приемы криптопреобразований. В то же время в большинстве иллюстраций будет использоваться алфавит естественного языка.

Текст с n буквами из алфавита $\bar{\sum}_m$ можно рассматривать как n-грамму $\bar{X} = x_0, x_1, ..., x_{n-1}$, где $x \in \bar{Z}_m$ для некоторого целого $n = 1,2,3,...$. Через $\bar{Z}_{m,n}$ будем обозначать множество n-грамм, образованных из букв множества $\bar{Z}_m$.

Криптографическое преобразование E представляет собой совокупность преобразований $E = E^n : 1 \le n < \infty$, $E^n : \bar{Z}_{m,n} \to \bar{Z}_{m,n}$. Преобразование E^n определяет, как каждая n-грамма открытого текста $\bar{x} \in \bar{Z}_{m,n}$ заменяется n-граммой шифротекста $\bar{y}$, т. е. $\bar{y} = E^n \bar{x}$, причем $\bar{x}$, $\bar{y} \in \bar{Z}_{m,n}$, при этом обязательным является требование взаимной однозначности преобразования E n на множестве $\bar{Z}_{m,n}$.

Криптографическая система может трактоваться как семейство криптографических преобразований $E = E_K : K \in \bar{k}$, помеченных параметром K называется ключом. Множество значений ключа образуют ключевое пространство $\bar{k}$.

7.2.2. Традиционные симметричные криптосистемы

Традиционные (классические) методы шифрования отличаются симметричной функцией шифрования. К ним относятся шифры перестановки, шифры простой и сложной замены, а также некоторые их модификации и комбинации.

Следует отметить, что комбинации шифров перестановок и шифров замены образуют все многообразие применяемых на практике симметричных шифров.

1. Шифры перестановок.

Правило перестановок символов – является ключом и задается различными предметами: цилиндром (скитала, древние греки), размером таблицы, условным словом или фразой (шифрующие таблицы в эпоху Возрождения), магическим квадратом в Средние века.

2. Шифры простой замены.

В шифрах простой замены каждый символ открытого текста заменяется символом того же или другого алфавита по определенному правилу. Широко известны и исследованы шифры Цезаря. Такие шифры имеют слабость по отношению к атакам на основе подсчета частот появления букв в шифротексте. Более устойчивыми являются биграммные шифры (замена двух букв) и *n*-граммные шифры, позволяющие маскировать частоту появления букв.

3. Шифры сложной замены.

Шифры сложной замены называют многоалфавитными, т. к. для шифрования каждого символа исходного сообщения применяют свой шифр простой замены. Многоалфавитная подстановка последовательно и циклически меняет используемые алфавиты. Например, в r-алфавитной подстановке символ x_0 исходного текста заменяется символом y_0 из алфавита B_0, x_1 на y_1 из B_1, x_{r-1} на y_{r-1} из B_{r-1}, x_r на y_r из B_r. Многоалфавитная подстановка маскирует естественную статистику исходного языка, т. к. конкретный символ из алфавита A может быть преобразован в несколько символов шифровальных алфавитов B. К шифрам сложной замены относят шифры Гронсфельда, Вижинера, Вернама. В 20-х годах были созданы первые шифровальные машины (электромеханиче-

ские), реализующие шифры сложной замены. Эти машины использовались до 60-х годов.

4. Шифрование методом гаммирования.

Под гаммированием понимают процесс наложения по определенному закону гаммы шифра на открытые данные. **Гамма шифра** – это псевдослучайная последовательность, выработанная по заданному алгоритму для зашифровывания открытых данных и расшифровывания зашифрованных данных. Процесс зашифровывания заключается в генерации гаммы шифра и наложении полученной гаммы на исходный открытый текст обратимым образом, например с использованием операции сложения по модулю 2.

Следует отметить, что перед зашифровыванием открытые данные разбивают на блоки T_0 одинаковой длины, обычно по 64 бита. Гамма шифра вырабатывается в виде последовательности блоков $Г_ш$ аналогичной длины.

Уравнение зашифровывания можно записать в виде $T_ш^i = Г_ш^i \oplus T_0^i$, $i = 1,2,...,M$, где $T_ш^i$ – i-й блок шифротекста, $Г_ш^i$ – i-й блок гаммы шифра, T_0^i – i-й блок открытого текста, M – количество блоков открытого текста.

Процесс расшифровывания сводится к повторной генерации гаммы шифра и наложению этой гаммы на зашифрованные данные. Уравнение расшифровывания имеет вид $T_0^i = Г_ш^i \oplus T_ш^i$. Получаемый этим методом шифротекст достаточно труден для раскрытия, поскольку теперь ключ является переменным. По сути дела, гамма шифра должна изменяться случайным образом для каждого шифруемого блока. Если период гаммы превышает длину всего шифруемого текста и злоумышленнику не известна ни какая часть исходного текста, то такой шифр можно раскрыть только прямым перебором всех вариантов ключа. В этом случае криптостойкость шифра определяется длиной ключа.

7.2.3. Современные симметричные криптосистемы

По мнению К. Шеннона, в практических шифрах необходимо использовать два общих принципа: рассеивание и перемешивание.

Рассеивание представляет собой распространение влияния одного знака открытого текста на много знаков шифротекста, что позволяет скрыть статистические свойства открытого текста.

Перемешивание предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текстов. Однако шифр должен не только затруднять раскрытие, но обеспечивать легкость зашифровывания и расшифровывания при известном пользователю секретном ключе.

Распространенным способом достижения эффектов рассеивания и перемешивания является использование составного шифра, т. е. такого шифра, который может быть реализован в виде некоторой последовательности простых шифров, каждый из которых вносит свой вклад в значительное суммарное рассеивание и перемешивание.

В составных шифрах в качестве простых шифров чаще всего используются простые перестановки и подстановки. При перестановке просто перемешивают символы открытого текста, причем конкретный вид перемешивания определяется секретным ключом. При подстановке каждый символ открытого текста заменяют другим символом из того же алфавита, а конкретный вид подстановки также определяется секретным ключом. Следует заметить, что в современном блочном шифре блоки открытого текста и шифротекста представляют собой двоичные последовательности обычно длиной 64 бита. В принципе, каждый блок может принимать 2^{64} значений. Поэтому подстановки выполняются в очень большом алфавите, содержащем до $2^{54} \approx 10^{19}$ символов.

При многократном чередовании простых перестановок и подстановок, управляемых достаточно длинным секретным ключом, можно получить очень стойкий шифр с хорошим рассеиванием и перемешиванием.

7.3. Стандарт шифрования данных ГОСТ 28147–89

ГОСТ 28147–89 представляет собой 64-битовый блочный алгоритм с 256-битовым ключом. Он предназначен для аппаратной и программной реализации, удовлетворяет криптографическим требованиям и не накладывает ограничений на степень секретности защищаемой информации.

Алгоритм предусматривает четыре режима работы:

1) шифрование данных в режиме простой замены;

2) шифрование данных в режиме гаммирования;

3) шифрование данных в режиме гаммирования с обратной связью;

4) выработка имитовставки.

Основными режимами шифрования являются режимы с использованием гаммирования, однако они базируются на использовании шифрования данных в режиме простой замены.

7.3.1. Режим простой замены

1. Шифрование открытых данных в режиме простой замены. Открытые данные, подлежащие шифрованию, разбивают на 64-разрядные блоки T_0. Процедура шифрования 64-разрядного блока T_0 в режиме простой замены включает 32 цикла $j = 1, 2, \ldots, 32$. В ключевое запоминающее устройство вводят 256 бит ключа K в виде восьми 32-разрядных подключей (чисел) K_i:

$$K = K_7 K_6 K_5 K_4 K_3 K_2 K_1 K_0 .$$

Последовательность бит блока

$$T_0 = a_1\ 0\ , a_2\ 0\ , \ldots, a_{31}\ 0\ , a_{32}\ 0\ , b_1\ 0\ , b_2\ 0\ , \ldots, b_{31}\ 0\ , b_{32}\ 0$$

разбивают на две последовательности по 32 бита: $b\ 0$ и $a\ 0$, где $b\ 0$ – левые или старшие биты, $a\ 0$ – правые или младшие биты.

Работа алгоритма в режиме простой замены изображена на рис. 7.3.

Обозначения на схеме:

N_1, N_2 – 32-разрядные накопители;

СМ_1 – 32-разрядный сумматор по модулю 2^{32} $+$;

СМ_2 – 32-разрядный сумматор по модулю 2 $\oplus$;

R – 32-разрядный регистр циклического сдвига;

КЗУ – ключевое запоминающее устройство на 256 бит, состоящее из восьми 32-разрядных накопителей $X_0, X_1, X_2, \ldots, X_7$;

S – блок подстановки, состоящий из восьми узлов замены (S-блоков замены) $S_1, S_2, S_3, \ldots, S_8$.

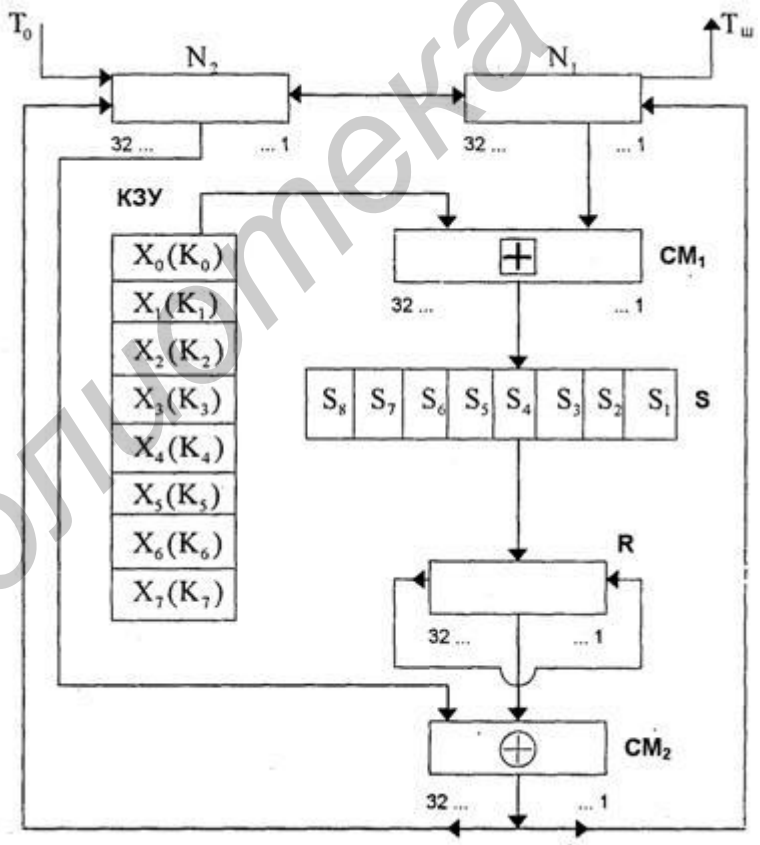


Рис. 7.3. Схема реализации режима простой замены

Эти последовательности вводят в накопители N_1 и N_2 перед началом первого цикла шифрования. В результате начальное заполнение накопителя N_1

$$a\ 0 \quad = \quad a_{32}\ 0\ ,\ \ a_{31}\ 0\ ,\ \ \ldots,\ \ a_{2}\ 0\ ,\ \ a_{1}\ 0$$
$$32, \qquad 31, \qquad \ldots, \quad 2, \qquad 1 \qquad \leftarrow \textit{номер разряда } N_1,$$

начальное заполнение накопителя N_2

$$b\ 0 \quad = \quad b_{32}\ 0\ ,\ \ b_{31}\ 0\ ,\ \ \ldots,\ \ b_{2}\ 0\ ,\ \ b_{1}\ 0$$
$$32, \qquad 31, \qquad \ldots, \quad 2, \qquad 1 \qquad \leftarrow \textit{номер разряда } N_2.$$

Первый цикл $j=1$ процедуры шифрования 64-разрядного блока открытых данных можно описать уравнениями

$$\begin{cases} a\ 1 = f\ \ a\ 0 + \mathrm{K}_0\ \ \oplus b\ 0\ , \\ b\ 1 = a\ 0\ . \end{cases}$$

Здесь $a\ 1$ – заполнение N_1 после 1-го цикла шифрования;

$b\ 1$ – заполнение N_2 после 1-го цикла шифрования;

f – функция шифрования.

Аргументом функции f является сумма по модулю 2^{32} числа $a\ 0$ (начального заполнения накопителя N_1) и числа K_0 подключа, считываемого из накопителя X_0 КЗУ. Каждое из этих чисел равно 32 битам.

Функция f включает две операции над полученной 32-разрядной суммой ($a\ 0 + \mathrm{K}_0$).

Первая операция называется подстановкой (заменой) и выполняется блоком подстановки S. Блок подстановки S состоит из восьми узлов замены (S блоков замены) S_1, S_2, S_3,…, S_8 с памятью 64 бит каждый. Поступающий из CM_1 на блок подстановки S 32-разрядный вектор разбивают на восемь последовательно идущих 4-разрядных векторов, каждый из которых преобразуется в четырехразрядный вектор соответствующим узлом замены. Каждый узел замены можно представить в виде таблицы-перестановки шестнадцати четырехразрядных двоичных чисел в диапазоне 0000…1111. Входной вектор указывает адрес строки в таблице, а число в этой строке является выходным вектором. Затем четырехразрядные выходные векторы последовательно объединяют в

32-разрядный вектор. Узлы замены (таблицы-перестановки) представляют собой ключевые элементы, которые являются общими для сетей ТКС и редко изменяются. Эти узлы замены должны сохраняться в секрете.

Вторая операция – циклический сдвиг влево (на 11 разрядов) 32-разрядного вектора, полученного с выхода блока подстановки *S*. Циклический сдвиг выполняется регистром сдвига *R*. Затем результат работы функции шифрования f суммируют поразрядно по модулю 2 в сумматоре $\mathrm{СМ}_2$ с 32-разрядным начальным заполнением $b\ 0$ накопителя N_2. Затем полученный на выходе $\mathrm{СМ}_2$ результат (значение $a\ 1$) записывают в накопитель N_1, а старое значение N_1 (значение $a\ 0$) переписывают в накопитель N_2 (значение $b\ 1 = a\ 0$). Первый цикл завершен. Последующие циклы осуществляются аналогично, при этом во втором цикле из КЗУ считывают заполнение X_0 – подключ K_1, в третьем цикле – подключ K_2 и т. д., в восьмом цикле – подключ K_7. В циклах с 9-го по 16-й, а также в циклах с 17-го по 24-й подключи из КЗУ считываются в том же порядке: $\mathrm{K}_0, \mathrm{K}_1, \mathrm{K}_2, \ldots, \mathrm{K}_6, \mathrm{K}_7$. В последних восьми циклах с 25-го по 32-й порядок считывания подключей из КЗУ обратный: $\mathrm{K}_7, \mathrm{K}_6, \ldots, \mathrm{K}_2, \mathrm{K}_1, \mathrm{K}_0$. Таким образом, при шифровании в 32 циклах осуществляется следующий порядок выборки из КЗУ подключей:

$$\mathrm{K}_0, \mathrm{K}_1, \mathrm{K}_2, \mathrm{K}_3, \mathrm{K}_4, \mathrm{K}_5, \mathrm{K}_6, \mathrm{K}_7, \mathrm{K}_0, \mathrm{K}_1, \mathrm{K}_2, \mathrm{K}_3, \mathrm{K}_4, \mathrm{K}_5, \mathrm{K}_6, \mathrm{K}_7,$$
$$\mathrm{K}_0, \mathrm{K}_1, \mathrm{K}_2, \mathrm{K}_3, \mathrm{K}_4, \mathrm{K}_5, \mathrm{K}_6, \mathrm{K}_7, \mathrm{K}_7, \mathrm{K}_6, \mathrm{K}_5, \mathrm{K}_4, \mathrm{K}_3, \mathrm{K}_2, \mathrm{K}_1, \mathrm{K}_0.$$

В 32-м цикле результат из сумматора $\mathrm{СМ}_2$ вводится в накопитель N_2, а в накопителе N_1 сохраняется прежнее заполнение. Полученные после 32-го цикла шифрования заполнения накопителей N_1 и N_2 являются блоком шифрованных данных $\mathrm{T}_{\mathrm{Ш}}$, соответствующим блоку открытых данных T_0.

Уравнения шифрования в режиме простой замены имеют вид

$$\begin{cases} a\ j\ = f\ \ a\ \ j-1\ + \mathrm{K}_{\,j-1\ \mathrm{mod}8}\ \oplus b\ \ j-1 \\ b\ \ j\ = a\ \ j-1 \end{cases} \quad при\ j = 1\ldots 24,$$

$$\begin{cases} a\ \ j\ = f\ \ a\ \ j-1\ + \mathrm{K}_{\,32-j\ \mathrm{mod}8}\ \oplus b\ \ j-1 \\ b\ \ j\ = a\ \ j-1 \end{cases} \quad при\ j = 25\ldots 31,$$

$$\begin{cases} a\ \ 32\ = a\ \ 31 \\ b\ \ 32\ = f\ \ a\ \ 31\ + \mathrm{K}_0\ \oplus b\ \ 31 \end{cases} \quad при\ j = 32.$$

где $a\ \ j\ = a_{32}\ \ j\ , a_{31}\ \ j\ , \ldots, a_1\ \ j$ – заполнение N_1 после j-го цикла шифрования;

$b\ \ j\ = b_{32}\ \ j\ , b_{31}\ \ j\ , \ldots, b_1\ \ j$ – заполнение N_2 после j-го цикла шифрования, $j = 1\ldots 32$.

Блок зашифрованных данных $\mathrm{T_Ш}$ (64 разряда) выводится из накопителей N_1, N_2 в следующем порядке: из разрядов 1…32 накопителя N_1, затем из разрядов 1…32 накопителя N_2, т. е. начиная с младших разрядов:

$$\mathrm{T_Ш} = a_1\ \ 32\ , a_2\ \ 32\ , \ldots, a_{31}\ \ 32\ , a_{32}\ \ 32\ , b_1\ \ 32\ , b_2\ \ 32\ , \ldots, b_{31}\ \ 32\ , b_{32}\ \ 32\ .$$

Остальные блоки открытых данных зашифровываются в режиме простой замены аналогично.

2. Расшифровывание в режиме простой замены. Криптосхема, реализующая алгоритм расшифровывания в режиме простой замены, имеет тот же вид, что и при шифровании (см. рис. 7.3).

В КЗУ вводят 256 бит ключа, на котором осуществлялось шифрование. Зашифрованные данные, подлежащие расшифровыванию, разбиты на блоки $\mathrm{T_Ш}$ по 64 бита в каждом. Ввод любого блока

$$\mathrm{T_Ш} = a_1\ \ 32\ , a_2\ \ 32\ , \ldots, a_{31}\ \ 32\ , a_{32}\ \ 32\ , b_1\ \ 32\ , b_2\ \ 32\ , \ldots, b_{31}\ \ 32\ , b_{32}\ \ 32$$

в накопители N_1 и N_2 производят так, чтобы начальное значение накопителя N_1 имело вид

$$a_{32}\ 32\ ,\quad a_{31}\ 32\ ,\quad \ldots,\quad a_2\ 32\ ,\quad a_1\ 32$$
$$32,\qquad 31,\qquad \ldots,\quad 2,\qquad 1 \qquad \leftarrow \textit{номер разряда}\ \mathrm{N}_1,$$

а начальное заполнение накопителя N_2:

$$b_{32}\ 32\ ,\quad b_{31}\ 32\ ,\quad \ldots,\quad b_2\ 32\ ,\quad b_1\ 32$$
$$32,\qquad 31,\qquad \ldots,\quad 2,\qquad 1 \qquad \leftarrow \textit{номер разряда}\ \mathrm{N}_2.$$

Расшифровывание осуществляется по тому же алгоритму, что и шифрование, с тем изменением, что заполнения накопителей $X_0, X_1, X_2, \ldots, X_7$ считываются из КЗУ в циклах расшифровывания в следующем порядке:

$$\mathrm{K}_0,\mathrm{K}_1,\mathrm{K}_2,\mathrm{K}_3,\mathrm{K}_4,\mathrm{K}_5,\mathrm{K}_6,\mathrm{K}_7,\mathrm{K}_7,\mathrm{K}_6,\mathrm{K}_5,\mathrm{K}_4,\mathrm{K}_3,\mathrm{K}_2,\mathrm{K}_1,\mathrm{K}_0,$$
$$\mathrm{K}_7,\mathrm{K}_6,\mathrm{K}_5,\mathrm{K}_4,\mathrm{K}_3,\mathrm{K}_2,\mathrm{K}_1,\mathrm{K}_0,\mathrm{K}_7,\mathrm{K}_6,\mathrm{K}_5,\mathrm{K}_4,\mathrm{K}_3,\mathrm{K}_2,\mathrm{K}_1,\mathrm{K}_0.$$

Уравнения расшифровывания имеют вид

$$\begin{cases} a\ 32-j\ = f\ \ a\ 32-j+1\ + \mathrm{K}_{j-1}\ \oplus b\ 32-j+1 \\ b\ 32-j\ = a\ 32-j+1 \end{cases} \qquad \textit{при } j = 1\ldots 8,$$

$$\begin{cases} a\ 32-j\ = f\ \ a\ 32-j+1\ + \mathrm{K}_{32-j\ \mathrm{mod}8}\ \oplus b\ 32-j+1 \\ b\ 32-j\ = a\ 32-j+1 \end{cases} \qquad \textit{при } j = 9\ldots 31,$$

$$\begin{cases} a\ 0\ = a\ 1 \\ b\ 0\ = f\ \ a\ 1\ + \mathrm{K}_0\ \oplus b\ 1 \end{cases} \qquad \textit{при } j = 32.$$

Полученные после 32-х циклов работы заполнения накопителей N_1 и N_2 образуют блок открытых данных:

$$\mathrm{T}_0 = a_1\ 0\ , a_2\ 0\ , \ldots, a_{31}\ 0\ , a_{32}\ 0\ , b_1\ 0\ , b_2\ 0\ , \ldots, b_{31}\ 0\ , b_{32}\ 0\ ,$$

соответствующий блоку зашифрованных данных $\mathrm{T}_{\text{Ш}}$. При этом состояние накопителя N_1:

$$a_{32}\ 0\ ,\quad a_{31}\ 0\ ,\quad \ldots,\quad a_2\ 0\ ,\quad a_1\ 0$$
$$32,\qquad 31,\qquad \ldots,\quad 2,\qquad 1 \qquad \leftarrow \textit{номер разряда}\ N_1,$$

состояние накопителя N_2:

$$b_{32}\ 0\ ,\quad b_{31}\ 0\ ,\quad \ldots,\quad b_2\ 0\ ,\quad b_1\ 0$$
$$32,\qquad 31,\qquad \ldots,\quad 2,\qquad 1 \qquad \leftarrow \textit{номер разряда}\ N_2.$$

Аналогично расшифровываются остальные блоки зашифрованных данных.

Если алгоритм зашифровывания в режиме простой замены 64-битного блока T_0 обозначить через A, то

$$A\ T_0 = A\ a\ 0\ ,b\ 0\ = a\ 32\ ,b\ 32\ = T_Ш.$$

Следует иметь в виду, что режим простой замены допустимо использовать для шифрования данных только в ограниченных случаях при выработке ключа и шифровании его с обеспечением имитозащиты для передачи по каналам связи или для хранения в памяти ЭВМ.

7.3.2. Режим гаммирования

1. Зашифровывание открытых данных в режиме гаммирования. Криптосхема, реализующая алгоритм шифрования в режиме гаммирования, показана на рис. 7.4. Открытые данные разбивают на 64-разрядные блоки

$$T_0^1, T_0^2, \ldots, T_0^i, \ldots, T_0^m,$$

где T_0^i – i-й 64-разрядный блок открытых данных, $i = 1 \ldots m$, m определяется объемом шифруемых данных.

Эти блоки поочередно зашифровываются в режиме гаммирования путем поразрядного сложения по модулю 2 в сумматоре $СМ_5$ с гаммой шифра $Г_Ш$, которая вырабатывается блоками по 64 бита, т. е.

$$Г_Ш = Г_Ш^1, Г_Ш^2, \ldots, Г_Ш^i, \ldots, Г_Ш^m,$$

где $Г_Ш^i$ – i-й 64-разрядный блок, $i = 1 \ldots m$.

Число двоичных разрядов в блоке T_0^m может быть меньше 64, при этом не использованная для зашифровывания часть гаммы шифра из блока $Г_Ш^m$ отбрасывается.

Уравнение шифрования данных в режиме гаммирования имеет вид

$$\mathrm{T}_{\mathrm{Ш}}^{\,i} = \mathrm{T}_0^{\,i} \oplus \Gamma_{\mathrm{Ш}}^{\,i},$$

где $\Gamma_{\mathrm{Ш}}^{\,i} = \mathrm{A}\ Y_{i-1} + C_2, Z_{i-1} + C_1\ ,\ i = 1\ldots m;\ \mathrm{T}_{\mathrm{Ш}}^{\,i}$ – i-й блок 64-разрядного блока зашифрованного текста; $\mathrm{A}\ *$ – функция шифрования в режиме простой замены; C_1, C_2 – 32-разрядные двоичные константы; Y_i, Z_i – 32-разрядные двоичные последовательности.

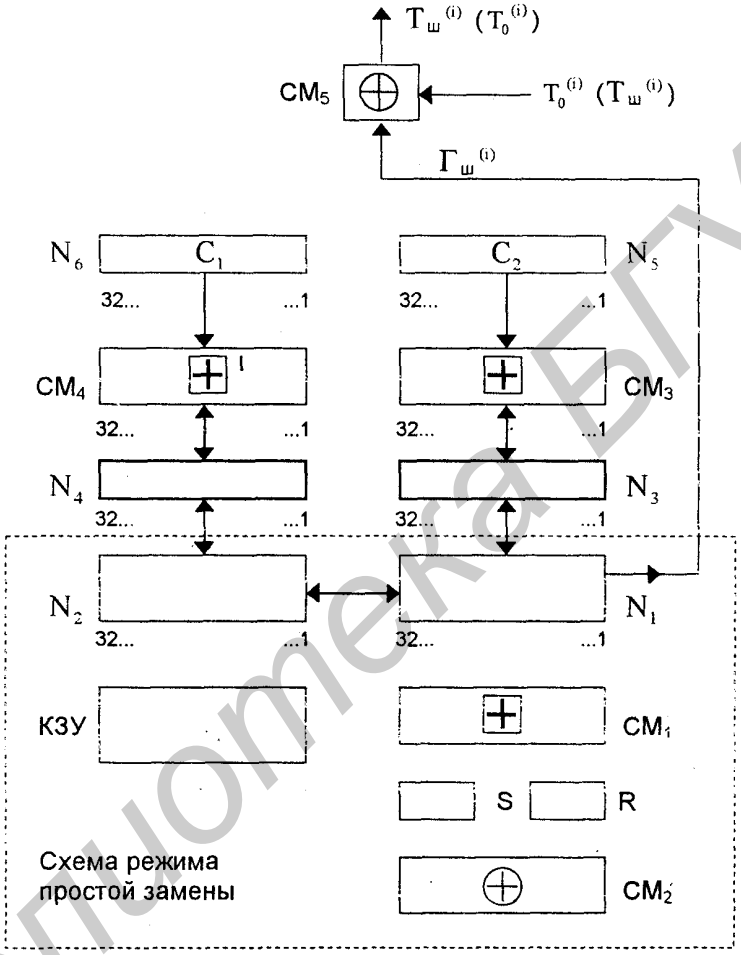


Рис. 7.4. Схема реализации режима гаммирования

Величины Y_i, Z_i определяются итерационно по мере формирования гаммы $\Gamma_{\mathrm{Ш}}$ следующим образом:

$$Y_0, Z_0\ = \mathrm{A}\ \tilde{S}\ ,$$

где $\tilde{S}$ – синхропосылка (64-разрядная двоичная последовательность),

$$Y_i, Z_i\ =\ Y_{i-1} + C_2, Z_{i-1} + C_1\ , i = 1\ldots m.$$

Рассмотрим реализацию процедуры шифрования в режиме гаммирования. В накопители N_6 и N_5 заранее записаны 32-разрядные двоичные константы C_1 и C_2, имеющие следующие значения (в шестнадцатеричной форме):

$$C_1 = 01010104_{16}, C_2 = 01010101_{16}.$$

В КЗУ вводится 256 бит ключа; в накопители N_1 и N_2 – 64-разрядная двоичная последовательность (синхропосылка)

$$\tilde{S} = S_1, S_2, \ldots, S_{64} .$$

Синхропосылка $\tilde{S}$ является исходным заполнением накопителей N_1 и N_2 для последовательной выработки m блоков гаммы шифра.

Исходное заполнение накопителя N_1:

$$\begin{array}{cccccc} S_{32}, & S_{31}, & \ldots, & S_2, & S_1 & \\ 32, & 31, & \ldots, & 2, & 1 & \leftarrow \textit{номер разряда } N_1, \end{array}$$

состояние накопителя N_2:

$$\begin{array}{cccccc} S_{64}, & S_{63}, & \ldots, & S_{34}, & S_{33} & \\ 64, & 63, & \ldots, & 34, & 33 & \leftarrow \textit{номер разряда } N_2. \end{array}$$

Исходное заполнение N_1 и N_2 (синхропосылка $\tilde{S}$ шифруется в режиме простой замены. Результат шифрования

$$\mathrm{A}\ \tilde{S} = Y_0, Z_0$$

переписывается в 32-разрядные накопители N_3 и N_4 так, что заполнение N_1 переписывается в N_3, а заполнение N_2 – в N_4.

Заполнение накопителя N_4 суммируют по модулю $2^{32}-1$ в сумматоре CM_4 с 32-разрядной константой C_1 из накопителя N_6. Результат записывается в N_4. Заполнение накопителя N_3 суммируется по модулю 2^{32} в сумматоре CM_3 с 32-разрядной константой C_3 из накопителя N_5. Результат записывается в N_3. Заполнение N_3 переписывают в N_1, а заполнение N_4 – в N_2, при этом заполнения N_3, N_4 сохраняются. Заполнение накопителей шифруется в режиме простой замены.

Полученное в результате шифрования заполнение накопителей N_1 и N_2 образует первый 64-разрядный блок гаммы шифра:

$$\Gamma_{\text{Ш}}^{1} = \gamma_1^{(1)}, \gamma_2^{(1)}, \ldots, \gamma_{63}^{(1)}, \gamma_{64}^{(1)} ,$$

который суммируют поразрядно по модулю 2 в сумматоре СМ_5 с первым 64-разрядным блоком открытых данных:

$$\text{T}_0^{1} = t_1^{1}, t_2^{1}, \ldots, t_{63}^{1}, t_{64}^{1} .$$

В результате суммирования по модулю 2 значений $\Gamma_{\text{Ш}}^{1}$ и T_0^{1} получают первый 64-разрядный блок зашифрованных данных:

$$\text{T}_{\text{Ш}}^{1} = \Gamma_{\text{Ш}}^{1} \oplus \text{T}_0^{1} = \tau_1^{1}, \tau_2^{1}, \ldots, \tau_{63}^{1}, \tau_{64}^{1} ,$$

где $\tau_i^{1} = t_i^{1} \oplus \gamma_i^{1}$, $i = 1 \ldots 64$.

Для получения следующего 64-разрядного блока гаммы шифра $\Gamma_{\text{Ш}}^{2}$ заполнение N_4 суммируется по модулю $2^{32} - 1$ в сумматоре СМ_4 с константой C_1 из N_6. Результат записывается в N_4. Заполнение N_3 суммируется по модулю 2^{32} в сумматоре СМ_3 с константой C_2 из N_5. Результат записывается в N_3. Новое заполнение N_3 переписывают в N_1, а новое заполнение N_4 – в N_2, при этом заполнения N_3 и N_2 сохраняют. Заполнения N_1, N_2 шифруют в режиме простой замены.

Полученное в результате шифрования заполнение накопителей N_1 и N_2 образует второй 64-разрядный блок гаммы шифра $\Gamma_{\text{Ш}}^{2}$, который суммируется поразрядно по модулю 2 в сумматоре СМ_5 со вторым блоком открытых данных T_0^{2}:

$$\text{T}_{\text{Ш}}^{2} = \Gamma_{\text{Ш}}^{2} \oplus \text{T}_0^{2} .$$

Аналогично вырабатываются блоки гаммы шифра $\Gamma_{\text{Ш}}^{3}, \Gamma_{\text{Ш}}^{4}, \ldots, \Gamma_{\text{Ш}}^{m}$ и шифруются блоки открытых данных $\text{T}_0^{3}, \text{T}_0^{3}, \ldots, \text{T}_0^{m}$.

В канал связи или память ЭВМ передаются синхропосылка $\tilde{S}$ и блоки зашифрованных данных:

$$\mathrm{Т}_{\mathrm{Ш}}^{1}, \mathrm{Т}_{\mathrm{Ш}}^{2}, \ldots, \mathrm{Т}_{\mathrm{Ш}}^{m} .$$

2. Расшифровывание в режиме гаммирования. При расшифровывании криптосхема имеет тот же вид, что и при шифровании.

Уравнение расшифровывания

$$\mathrm{Т}_{0}^{i} = \mathrm{Т}_{\mathrm{Ш}}^{i} \oplus \Gamma_{\mathrm{Ш}}^{i} = \mathrm{Т}_{\mathrm{Ш}}^{i} \oplus \mathrm{A}\ Y_{i-1} + \mathrm{C}_2, Z_{i-1} + \mathrm{C}_1\ , \ i = 1 \ldots m.$$

Следует отметить, что расшифровывание данных возможно только при наличии синхропосылки, которая не является секретным элементом шифра и может храниться в памяти ЭВМ или передаваться по каналам связи вместе с зашифрованными данными.

Рассмотрим реализацию процедуры расшифровывания. В КЗУ вводят 256 бит ключа, с помощью которого осуществляется шифрование данных $\mathrm{Т}_{0}^{1}, \mathrm{Т}_{0}^{2}, \ldots, \mathrm{Т}_{0}^{m}$. В накопители N_1 и N_2 вводится синхропосылка и осуществляется процесс выработки m блоков гаммы шифра $\Gamma_{\mathrm{Ш}}^{1}, \Gamma_{\mathrm{Ш}}^{2}, \ldots, \Gamma_{\mathrm{Ш}}^{m}$. Блоки зашифрованных данных $\mathrm{Т}_{\mathrm{Ш}}^{1}, \mathrm{Т}_{\mathrm{Ш}}^{2}, \ldots, \mathrm{Т}_{\mathrm{Ш}}^{m}$ суммируются поразрядно по модулю 2 в сумматоре $\mathrm{СМ}_5$ с блоками гаммы шифра $\Gamma_{\mathrm{Ш}}^{1}, \Gamma_{\mathrm{Ш}}^{2}, \ldots, \Gamma_{\mathrm{Ш}}^{m}$. В результате получаются блоки открытых данных $\mathrm{Т}_{0}^{1}, \mathrm{Т}_{0}^{2}, \ldots, \mathrm{Т}_{0}^{m}$, при этом $\mathrm{Т}_{0}^{m}$ может содержать меньше 64 разрядов.

7.3.3. Режим гаммирования с обратной связью

Криптосхема, реализующая алгоритм шифрования в режиме гаммирования с обратной связью, имеет вид, показанный на рис. 7.5.

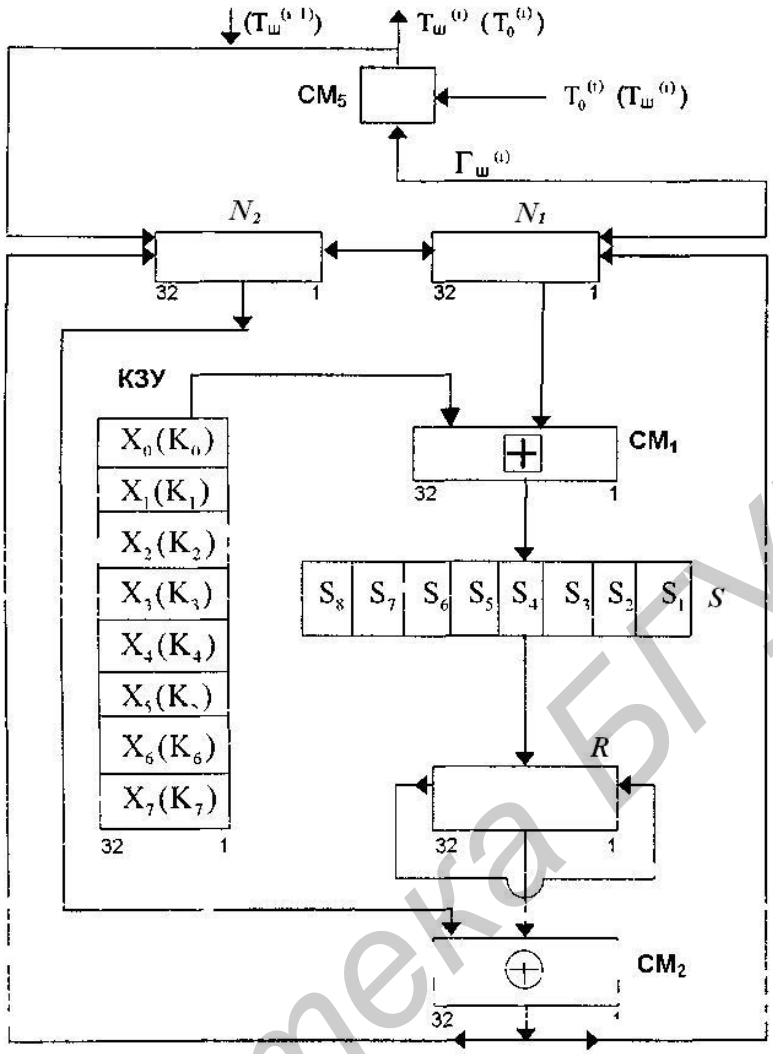


Рис. 7.5. Схема реализации режима гаммирования с обратной связью

1. Шифрование открытых данных в режиме гаммирования с обратной связью. Открытые данные, разбитые на 64-разрядные блоки $T_0^1, T_0^2, \ldots, T_0^m$, шифруются в режиме гаммирования с обратной связью путем поразрядного сложения по модулю 2 с гаммой шифра $\Gamma_{Ш}$, которая вырабатывается блоками по 64 бита: $\Gamma_{Ш}^1, \Gamma_{Ш}^2, \ldots, \Gamma_{Ш}^m$.

Число двоичных разрядов в блоке T_0^m может быть меньше 64, при этом не использованная для шифрования часть гаммы шифра из блока $\Gamma_{Ш}^m$ отбрасывается.

Уравнения шифрования в режиме гаммирования с обратной связью имеют вид:

$$\mathrm{T}_{\mathrm{Ш}}^{1} = \mathrm{A}\ \tilde{\mathrm{S}}\ \oplus \mathrm{T}_{0}^{\ 1} = \Gamma_{\mathrm{Ш}}^{1} \oplus \mathrm{T}_{0}^{\ 1},$$

$$\mathrm{T}_{\mathrm{Ш}}^{i} = \mathrm{A}\ \mathrm{T}_{\mathrm{Ш}}^{i-1}\ \oplus \mathrm{T}_{0}^{\ i} = \Gamma_{\mathrm{Ш}}^{i} \oplus \mathrm{T}_{0}^{\ i},\ i = 2 \ldots m.$$

Здесь $\mathrm{T}_{\mathrm{Ш}}^{i}$ – i-й 64-разрядный блок шифрованного текста; $\mathrm{A}\ *$ – функция шифрования в режиме простой замены; m определяется объемом открытых данных.

Аргументом функции $\mathrm{A}\ *$ на первом шаге итеративного алгоритма является 64-разрядная синхропосылка S, а на всех последующих шагах – предыдущий блок зашифрованных данных $\mathrm{T}_{\mathrm{Ш}}^{i-1}$.

Процедура шифрования данных в режиме гаммирования с обратной связью реализуется следующим образом. В КЗУ вводятся 256 бит ключа, в накопители N_1 и N_2 вводится синхропосылка $\tilde{S} = S_1, S_2, \ldots, S_{64}$ из 64 бит. Исходное заполнение накопителей N_1 и N_2 шифруется в режиме простой замены. Полученное в результате шифрования заполнение накопителей N_1 и N_2 образует первый 64-разрядный блок гаммы шифра $\Gamma_{\mathrm{Ш}}^{1} = \mathrm{A}\ \tilde{S}$, который суммируется поразрядно по модулю 2 в сумматоре $\mathrm{СМ}_5$ с первым 64-разрядным блоком открытых данных:

$$\mathrm{T}_{0}^{\ 1} = t_1^{\ 1}, t_2^{\ 1}, \ldots, t_{63}^{1}, t_{64}^{1}.$$

В результате получают первый 64-разрядный блок шифрованных данных

$$\mathrm{T}_{\mathrm{Ш}}^{1} = \Gamma_{\mathrm{Ш}}^{1} \oplus \mathrm{T}_{0}^{\ 1},$$

где $\mathrm{T}_{\mathrm{Ш}}^{1} = \tau_1^{\ 1}, \tau_2^{\ 1}, \ldots, \tau_{63}^{1}, \tau_{64}^{1}$.

Блок шифрованных данных $\mathrm{T}_{\mathrm{Ш}}^{i}$ одновременно является также исходным состоянием накопителей N_1 и N_2 для выработки второго блока гаммы

шифра $\Gamma_{Ш}^{2}$, и поэтому по обратной связи $\mathrm{T}_{Ш}^{1}$ записывается в указанные накопители N_1 и N_2.

Заполнение накопителя N_1:

$$\begin{array}{llllll} \tau_{32}^{1}, & \tau_{31}^{1}, & \ldots, & \tau_{2}^{1}, & \tau_{1}^{1} & \\ 32, & 31, & \ldots, & 2, & 1 & \leftarrow \textit{номер разряда } N_1. \end{array}$$

Заполнение накопителя N_2:

$$\begin{array}{llllll} \tau_{64}^{1}, & \tau_{63}^{1}, & \ldots, & \tau_{34}^{1}, & \tau_{33}^{1} & \\ 32, & 31, & \ldots, & 2, & 1 & \leftarrow \textit{номер разряда } N_1. \end{array}$$

Заполнение накопителей N_1 и N_2 шифруется в режиме простой замены. Полученное в результате шифрования заполнение накопителей N_1 и N_2 образует второй 64-разрядный блок гаммы шифра $\Gamma_{Ш}^{2}$, который суммируется поразрядно по модулю 2 в сумматоре СМ со вторым блоком открытых данных T_{0}^{2}:

$$\mathrm{T}_{Ш}^{2} = \Gamma_{Ш}^{2} \oplus \mathrm{T}_{0}^{2}.$$

Выработка последующих блоков гаммы шифра $\Gamma_{Ш}$ и шифрование соответствующих блоков открытых данных T_{0}^{i} $i = 3 \ldots m$ производятся аналогично. Если длина последнего m-го блока открытых данных T_{0}^{m} меньше 64 разрядов, то из $\Gamma_{Ш}^{m}$ используется только соответствующее число разрядов гаммы шифра, остальные разряды отбрасываются.

В канал связи или память ЭВМ передаются синхропосылка $\tilde{S}$ и блоки зашифрованных данных $\mathrm{T}_{Ш}^{1}, \mathrm{T}_{Ш}^{2}, \ldots, \mathrm{T}_{Ш}^{m}$.

2. Расшифровывание в режиме гаммирования с обратной связью. При расшифровывании криптосхема имеет тот же вид, что и при шифровании.

Уравнения расшифровывания:

$$\mathrm{T}_{0}^{1} = \mathrm{A}\ \tilde{S} \oplus \mathrm{T}_{Ш}^{1} = \Gamma_{Ш}^{1} \oplus \mathrm{T}_{Ш}^{1},$$

$$\mathrm{T}_0^{\,i} = \Gamma_{\mathrm{Ш}}^{\,i} \oplus \mathrm{T}_{\mathrm{Ш}}^{\,i} = \mathrm{A}\ \mathrm{T}_{\mathrm{Ш}}^{\,i-1} \oplus \mathrm{T}_{\mathrm{Ш}}^{\,i},\ i = 2 \ldots m.$$

Реализация процедуры расшифровывания шифрованных данных в режиме гаммирования с обратной связью происходит следующим образом. В КЗУ вводят 256 бит того же ключа, на котором осуществлялось шифрование открытых блоков $\mathrm{T}_0^{\,1}, \mathrm{T}_0^{\,2}, \ldots, \mathrm{T}_0^{\,m}$. В накопители N_1 и N_2 вводится синхропосылка $\tilde{S}$. Исходное заполнение накопителей N_1 и N_2 (синхропосылка $\tilde{S}$) шифруется в режиме простой замены. Полученное в результате шифрования заполнение N_1 и N_2 образует первый блок гаммы шифра

$$\Gamma_{\mathrm{Ш}}^{\,1} = \mathrm{A}\ \tilde{S}\ ,$$

который суммируется поразрядно по модулю 2 в сумматоре $\mathrm{СМ}_5$ с блоком шифрованных данных $\mathrm{T}_{\mathrm{Ш}}^{\,1}$. В результате получается первый блок открытых данных

$$\mathrm{T}_0^{\,2} = \Gamma_{\mathrm{Ш}}^{\,2} \oplus \mathrm{T}_{\mathrm{Ш}}^{\,2}.$$

Блок шифрованных данных $\mathrm{T}_{\mathrm{Ш}}^{\,1}$ является исходным заполнением накопителей N_1 и N_2 для выработки второго блока гаммы шифра $\Gamma_{\mathrm{Ш}}^{\,2}$: $\Gamma_{\mathrm{Ш}}^{\,2} = \mathrm{A}\ \mathrm{T}_{\mathrm{Ш}}^{\,1}$. Полученное заполнение накопителей N_1 и N_2 шифруется в режиме простой замены. Образованный в результате шифрования блок $\Gamma_{\mathrm{Ш}}^{\,2}$ суммируется поразрядно по модулю 2 в сумматоре $\mathrm{СМ}_5$ со вторым блоком шифрованных данных $\mathrm{T}_{\mathrm{Ш}}^{\,2}$. В результате получают второй блок открытых данных. Аналогично в N_1 и N_2 последовательно записывают блоки шифрованных данных $\mathrm{T}_{\mathrm{Ш}}^{\,2}, \mathrm{T}_{\mathrm{Ш}}^{\,3}, \ldots, \mathrm{T}_{\mathrm{Ш}}^{\,m}$, из которых в режиме простой замены вырабатываются блоки гаммы шифра $\Gamma_{\mathrm{Ш}}^{\,3}, \Gamma_{\mathrm{Ш}}^{\,4}, \ldots, \Gamma_{\mathrm{Ш}}^{\,m}$. Блоки гаммы шифра суммируются поразрядно по модулю 2 в сумматоре $\mathrm{СМ}_5$ с блоками шифрованных данных $\mathrm{T}_{\mathrm{Ш}}^{\,3}, \mathrm{T}_{\mathrm{Ш}}^{\,4}, \ldots, \mathrm{T}_{\mathrm{Ш}}^{\,m}$.

В результате получают блоки открытых данных $\mathrm{T}_0^{\,3}, \mathrm{T}_0^{\,4}, \ldots, \mathrm{T}_0^{\,m}$, при этом последний блок открытых данных $\mathrm{T}_0^{\,m}$ может содержать меньше 64 разрядов.

7.3.4. Режим выработки имитовставки

Имитовставка – это блок из P бит, который вырабатывают по определенному правилу из открытых данных с использованием ключа и затем добавляют к зашифрованным данным для обеспечения их имитозащиты.

Имитозащита – это защита системы шифрованной связи от навязывания ложных данных.

В стандарте ГОСТ 28147–89 определяется процесс выработки имитовставки, который единообразен для любого из режимов шифрования данных. Имитовставка $И_p$ вырабатывается из блоков открытых данных либо перед шифрованием всего сообщения, либо параллельно с шифрованием по блокам. Первые блоки открытых данных, которые участвуют в выработке имитовставки, могут содержать служебную информацию (например адресную часть, время, синхропосылку) и не шифруются.

Значение параметра P (число двоичных разрядов в имитовставке) определяется криптографическими требованиями с учетом того, что вероятность навязывания ложных помех равна $1/2^P$.

Для выработки имитовставки открытые данные представляют в виде последовательности 64-разрядных блоков $\mathrm{T}_0^{\,i}$, $i = 1 \ldots m$. Первый блок открытых данных $\mathrm{T}_0^{\,1}$ подвергают преобразованию $\tilde{\mathrm{A}} *$, соответствующему первым 16 циклам алгоритма шифрования в режиме простой замены. В качестве ключа для выработки имитовставки используют ключ длиной 256 бит, по которому шифруют данные.

Полученное после 16 циклов 64-разрядное число $\tilde{\mathrm{A}}\ \mathrm{T}_0^{\,1}$ суммируют по модулю 2 со вторым блоком открытых данных $\mathrm{T}_0^{\,2}$. Результат суммирования $\tilde{\mathrm{A}}\ \mathrm{T}_0^{\,1} \oplus \mathrm{T}_0^{\,2}$ снова подвергают преобразованию $\tilde{\mathrm{A}} *$.

Полученное 64-разрядное число $\tilde{A}\ \tilde{A}\ T_0^1 \oplus T_0^2$ суммируют по модулю 2 с третьим блоком T_0^3 и снова подвергают преобразованию $\tilde{A} *$, получая 64-разрядное число $\tilde{A}\ \tilde{A}\ \tilde{A}\ T_0^1 \oplus T_0^2 \oplus T_0^3$, и т. д.

Последний блок T_0^m (при необходимости дополненный нулями до полного 64-разрядного блока) суммируют по модулю 2 с результатом вычислений на шаге $m-1$, после чего шифруют в режиме простой замены, используя преобразование $\tilde{A} *$.

Из полученного 64-разрядного числа выбирают отрезок $И_P$ (имитовставку) длиной P бит:

$$И_P = \left[a^m_{32-P+1}\ 16\ , a^m_{32-P+2}\ 16\ , \ldots, a^m_{32}\ 16\ \right],$$

где $a_i^{\ m} - i$ бит 64-разрядного числа, полученного после 16-го цикла последнего преобразования $\tilde{A} *$, $32 - P + 1 \le i \le 31$.

Имитовставка $И_P$ передается по каналу связи в конце шифрованных данных, т. е.

$$T^1_Ш, T^2_Ш, \ldots, T^m_Ш, И_P.$$

Поступившие к получателю шифрованные данные $T^1_Ш, T^2_Ш, \ldots, T^m_Ш$ расшифровываются, и из полученных блоков открытых данных $T_0^1, T_0^2, \ldots, T_0^m$ аналогичным образом вырабатывается имитовставка $И'_P$, которая сравнивается с $И_p$. В случае несовпадения блок открытых данных считается ложным.

7.4. Асимметричные криптосистемы

Концепция криптосистемы с открытым ключом.

Эффективными системами криптографической защиты данных являются асимметричные криптосистемы, называемые также криптосистемами с откры-

тым ключом. В таких системах для шифрования данных используется один ключ, а для расшифрования другой (отсюда и название – асимметричные). Первый ключ является открытым и может быть опубликован для использования всеми пользователями системы, которые шифруют данные. Расшифрование данных с помощью открытого ключа невозможно. Для расшифрования данных получатель зашифрованной информации использует второй ключ, который является секретным. Разумеется, ключ расшифрования не может быть определен из ключа шифрования.

Обобщенная схема асимметричной криптосистемы с открытым ключом показана на рис. 7.6.

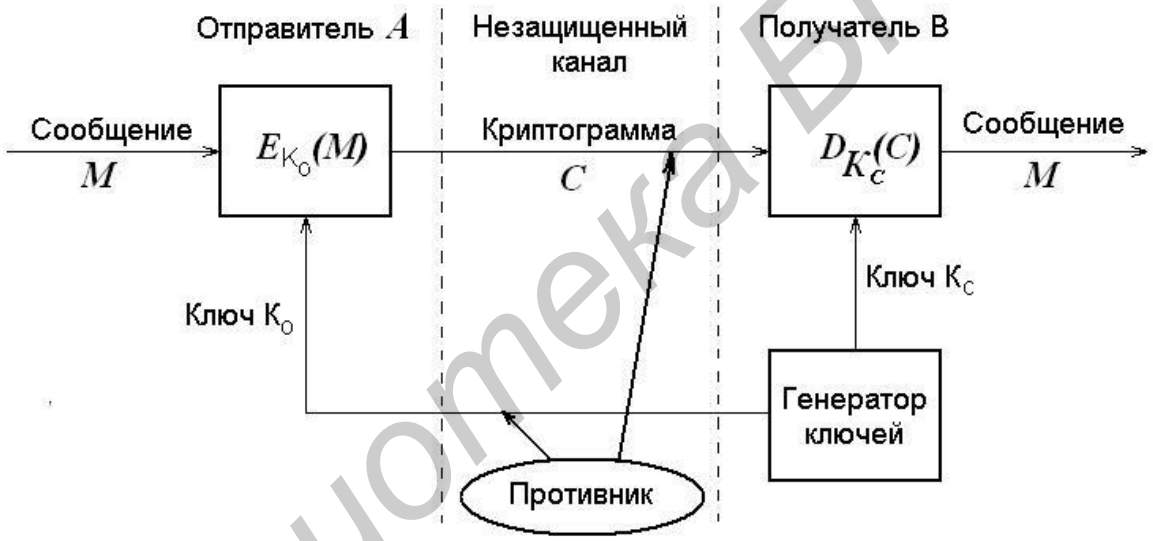


Рис. 7.6. Обобщенная схема асимметричной криптосистемы с открытым ключом

В этой криптосистеме применяют два различных ключа: K_0 – открытый ключ отправителя *A*; K_c – секретный ключ получателя *B*. Генератор ключа целесообразно располагать на стороне получателя *B* (чтобы не пересылать секретный ключ K_c по незащищенному каналу). Значения ключей K_0, K_c – зависят от начального состояния генератора ключей.

Раскрытие секретного ключа K_c по известному ключу K_0 должно быть вычислительно неразрешимой задачей.

Характерные особенности асимметричных криптосистем:

– открытый ключ $К_0$ и криптограмма C могут быть отправлены по незащищенному каналу, т. е. могут быть известны противнику;

– алгоритмы шифрования $E_{К_0}(M) \to C$ и расшифрования $D_{К_С}(C) \to M$ являются открытыми;

– защита информации в асимметричной криптосистеме основана на секретности ключа $К_с$.

У. Диффи и М. Хелман сформулировали требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы:

– вычисление пары ключей ($К_0$, $К_с$) получателем B на основе начального условия должно быть простым;

– отправитель A, зная открытый ключ $К_0$ и сообщение M, может легко вычислить криптограмму $C = E_{К_0} \ M \ ;$

– получатель B, используя секретный ключ $К_с$ и криптограмму C, может легко восстановить исходное сообщение $M = D_{К_С} \ C \ = D_{К_С} \ E_{К_0} \ M \ ;$

– противник, зная открытый ключ $К_с$, при попытке вычислить секретный ключ $К_с$ наталкивается на непреодолимую вычислительную проблему;

– противник, зная пару ($К_0$, С), при попытке вычислить исходное сообщение M, наталкивается на непреодолимую вычислительную проблему.

7.5. Электронная цифровая подпись

7.5.1. Общие сведения

При обмене сообщениями через ТКС возникает задача подтверждения их подлинности (подтверждения авторства и целостности). Такая же проблема существует и при переходе от юридически значимых бумажных документов к электронным. Сообщения, для которых эта проблема актуальна, будем в дальнейшем называть электронными документами.

Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий, к которым относятся:

– активный перехват – нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их;

– маскарад – абонент *C* посылает документ абоненту *B* от имени абонента *A*;

– ренегатство – абонент *A* заявляет, что не посылал сообщения абоненту *B*, хотя на самом деле послал;

– подмена – абонент *B* изменяет или формирует новый документ и заявляет, что получил его от абонента *A*;

– повтор – абонент *C* повторяет ранее переданный документ, который абонент *A* посылал абоненту *B*.

В обычной (бумажной) информатике эти проблемы решаются за счет того, что информация в документе и рукописная подпись автора жестко связаны с физическим носителем (бумагой). В электронных документах на машинных носителях такой связи нет.

Естественно, что для электронных документов традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе совершенно непригодны, поэтому для подтверждения подлинности документа используется специфическая криптографическая процедура, называемая электронной цифровой подписью (ЭЦП).

ЭЦП функционально аналогична обычной рукописной подписи и обладает ее основными достоинствами:

– удостоверяет, что подписанный текст исходит от лица, поставившего подпись;

– не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;

– гарантирует целостность подписанного текста.

ЭЦП представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом.

Технология ЭЦП включает две процедуры: 1) процедуру постановки подписи; 2) процедуру проверки подписи. В процедуре постановки подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи – открытый ключ отправителя.

При формировании ЭЦП отправитель прежде всего вычисляет хэш-функцию $h\ M$ подписываемого документа *M*. Вычисленное значение хэш-функции $h\ M$ представляет собой один короткий блок информации m, характеризующий весь документ M в целом. Затем число m «шифруется» секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЭЦП для данного документа *M*. В принципе можно обойтись без предварительного хэширования документа, а «шифровать» весь документ, однако в этом случае придется иметь дело с гораздо большим по размерам файлом. Употребление слова «шифровать» здесь весьма условное и справедливо при использовании алгоритма RSA, для других алгоритмов точнее говорить «преобразовывать».

При проверке ЭЦП получатель сообщения снова вычисляет хэш-функцию $m = h\ M$ принятого по каналу документа M, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению m хэш-функции.

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания.

В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более электронных подписей. Каждая подпись содержит следующую информацию:

– дату подписи;

– срок окончания действия ключа данной подписи;

– информацию о лице, подписавшем файл (ФИО, должность, краткое наименование фирмы);

– идентификатор подписавшего (имя открытого ключа);

– собственно цифровую подпись.

7.5.2. Однонаправленные хэш-функции

Хэш-функция предназначена для сжатия подписываемого документа M до нескольких десятков или сотен бит. Хэш-функция h принимает в качестве аргумента сообщение (документ) M произвольной длины и возвращает хэш-значение $h(M) = H$ фиксированной длины. Обычно хэшированная информация является сжатым двоичным представлением основного сообщения произвольной длины. Следует отметить, что значение хэш-функции $h(M)$ сложным образом зависит от документа M и не позволяет восстановить сам документ *M*.

Хэш-функция должна удовлетворять целому ряду условий:

– хэш-функция должна быть чувствительна к всевозможным изменениям в тексте *M*, таким, как вставки, выбросы, перестановки и т. п.;

– хэш-функция должна обладать свойством необратимости, т. е. задача подбора документа M', который обладал бы требуемым значением хэш-функции, должна быть вычислительно неразрешима;

– вероятность того, что значения хэш-функции двух различных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала.

Большинство хэш-функций строится на основе однонаправленной функции f, аргументами которой являются две величины: блок исходного документа M_i и хэш-значение H_{i-1} предыдущего блока документа (рис. 7.7): $H_i = f(M_i, H_{i-1})$.

Хэш-значение, вычисляемое при вводе последнего блока текста, становится хэш-значением всего сообщения *M*. В результате однонаправленная хэш-функция всегда формирует выход фиксированной длины n (независимо от длины входного текста).

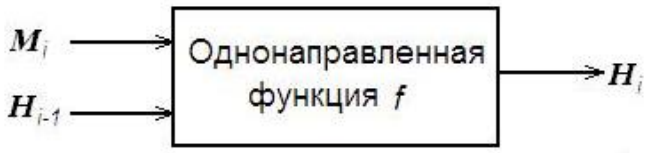


Рис. 7.7. Общая схема вычисления однонаправленной хэш-функции

Часто функции хэширования строят, используя в качестве однонаправленной функции симметричный блочный алгоритм шифрования (DES, ГОСТ 28147–89) в режиме с обратной связью, принимая последний блок шифротекста за хэш-значение всего документа. Так как длина блока в указанных алгоритмах невелика (64 бита), то часто в качестве хэш-значения используют два блока шифротекста. Одна из возможных схем хэширования на основе блочного алгоритма шифрования изображена на рис. 7.8.

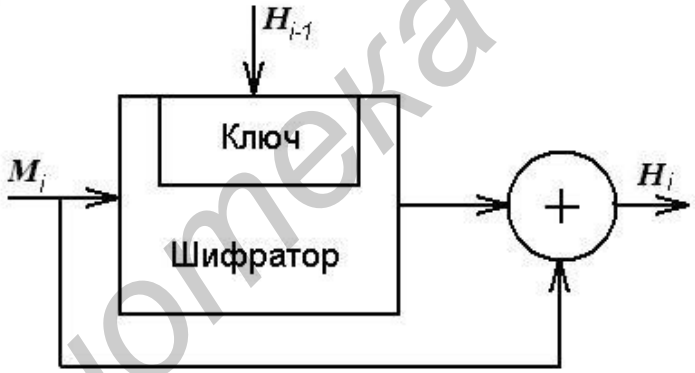


Рис. 7.8. Схема вычисления однонаправленной функции хэширования на базе блочного алгоритма шифрования

7.5.3. Алгоритм электронной цифровой подписи RSA

Первой и наиболее известной во всем мире конкретной системой ЭЦП стала система RSA, математическая схема которой была разработана в 1977 г. в Массачуссетском технологическом институте США.

Сначала необходимо вычислить пару ключей (секретный ключ и открытый ключ). Для этого отправитель (автор) электронных документов вычисляет два больших простых числа P и Q, затем находит их произведение $n = P \cdot Q$ и

значение функции Эйлера $\varphi\ n\ =\ P-1\ \cdot\ Q-1$. Далее отправитель вычисляет число K_0 из условий: $K_0 \le \varphi\ n$, НОД $K_0, \varphi\ n\ =1$ и число K_c из условий: $K_c < n$, $K_0 \cdot K_C \equiv 1 \mathrm{mod}\ \varphi\ n$.

Пара чисел (K_0, n) является открытым ключом. Эту пару чисел автор передает партнерам по переписке для проверки его цифровых подписей. Число K_c сохраняется автором как секретный ключ для подписывания. Обобщенная схема формирования и проверки цифровой подписи RSA показана на рис. 7.9.

Допустим, что отправитель хочет подписать сообщение M перед его отправкой. Сначала сообщение M (блок информации, файл, таблица) сжимают с помощью хэш-функции h в целое число $m = h\ M$. Затем вычисляют цифровую подпись S под электронным документом M, используя хэш-значение m и секретный ключ K_c: $S = m^{K_C} \bmod n$.

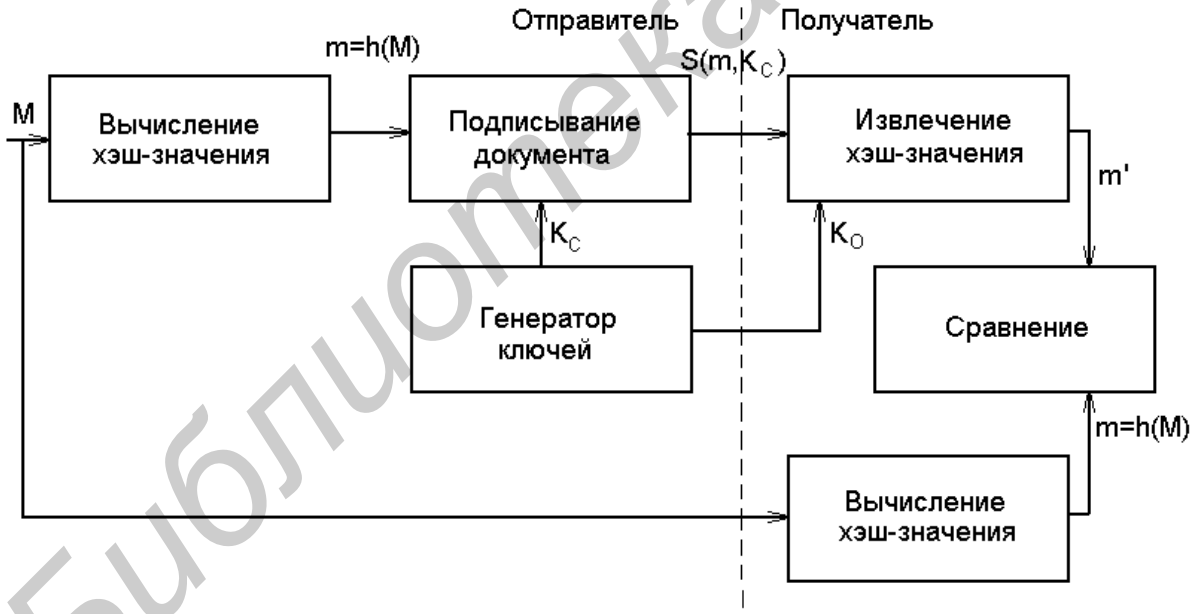


Рис. 7.9. Обобщенная схема алгоритма ЭЦП RSA

Пара M, S передается партнеру-получателю как электронный документ M, подписанный цифровой подписью S, причем подпись S сформирована обладателем секретного ключа K_c. После приема пары M, S получатель вычисляет хэш-значение сообщения M двумя разными способами. Прежде всего он

восстанавливает хэш-значение m', применяя криптографическое преобразование подписи S с использованием открытого ключа $К_0$: $m' = S^{K_O} \bmod n$. Кроме того, он находит результат хэширования принятого сообщения M с помощью такой же хэш-функции h: $m = h\ M$. Если соблюдается равенство вычисленных значений, т. е. $S^{K_O} \bmod n = h\ M$, то получатель признает пару M, S подлинной. Доказано, что только обладатель секретного ключа $К_с$ может сформировать цифровую подпись S по документу *M*, а определить секретное число $К_с$ по открытому числу $К_0$ не легче, чем разложить модуль N на множители. Кроме того, можно строго математически доказать, что результат проверки цифровой подписи S будет положительным только в том случае, если при вычислении S был использован секретный ключ $К_с$, соответствующий открытому ключу $К_0$. Поэтому открытый ключ $К_0$ иногда называют «идентификатором» подписавшего.

Недостатками алгоритма цифровой подписи RSA являются:

1. При вычислении модуля n ключей $К_с$ и $К_0$ для системы цифровой подписи RSA необходимо проверять большое количество дополнительных условий, что выполнить практически трудно. Невыполнение любого из этих условий делает возможным фальсификацию цифровой подписи со стороны того, кто обнаружит такое невыполнение при подписании важных документов, а такую возможность нельзя допускать даже теоретически.

2. Для обеспечения криптостойкости цифровой подписи RSA по отношению к попыткам фальсификации на уровне, например, национального стандарта США на шифрование информации (алгоритм DES), т. е. 10^{18}, необходимо использовать при вычислениях n, $К_с$ и $К_0$ целые числа не менее 2^{512} (или около 10^{154}) каждое, что требует больших вычислительных затрат, превышающих на 20…30 % вычислительные затраты других алгоритмов цифровой подписи при сохранении того же уровня криптостойкости.

3. Цифровая подпись RSA уязвима к так называемой мультипликативной атаке. Иначе говоря, алгоритм цифровой подписи RSA позволяет злоумышленнику без знания секретного ключа K_c сформировать подписи под теми документами, у которых результат хэширования можно вычислить как произведение результатов хэширования уже подписанных документов.

7.5.4. Белорусские стандарты ЭЦП и функции хэширования

Белорусские стандарты, регламентирующие использование электронной цифровой подписи, официальное название которых «Процедура выработки и проверки ЭЦП» и «Функция хэширования», были разработаны группой белорусских специалистов в 1999 г. и официально приняты в 2000 г.

В этих стандартах наряду с элементами классических процедур ЭЦП используются современные идеи, позволяющие увеличить криптостойкость и быстродействие. Так, открытый ключ и секретный ключ связаны известным соотношением

$$K_0 = a^{K_C} \bmod P,$$

которое позволяет легко вычислить K_0 по K_c, но очень сложно решение обратной задачи – вычисления K_C по K_0. К подписываемому сообщению добавляется случайная компонента t, что усложняет возможный подбор хэш-значения злоумышленником по известному тексту сообщения.

Обозначения, принятые в стандарте СТБ-1176.02–99:

– B_p – множество, состоящее из чисел $1, 2, \ldots, p-1$;

– $c := d$ – присвоение параметру c значения d;

– $c \bmod d$ – остаток от деления c на d, где c – натуральное число или ноль, d – натуральное число;

– $c^{-1} \bmod d$ – натуральное число b, такое, что $b < d$ и $(cb) \bmod d = 1$, где c и d – взаимно простые числа;

– $\lceil c \rceil$ – наименьшее целое число, не меньше чем c;

– $\lfloor c \rfloor$ – наибольшее целое число, не большее чем c;

– $c = \sum_{i=0}^{k-1} c_i (2^b)^i$ – разложение неотрицательного целого числа c по основанию 2^b, где k и b – натуральные числа,

– c_i – целое число, $0 \le c_i < 2^b$;

– $\oplus$ – бинарная операция, определенная на множестве неотрицательных целых чисел по формуле $d \oplus b = \sum_{i=0}^{k-1} d_i + b_i \bmod 2 \ 2^i$, где $d = \sum_{i=0}^{k-1} d_i 2^i$, $b = \sum_{i=0}^{k-1} b_i 2^i$, $d_0, \ldots, d_{k-1}, b_0, \ldots, b_{k-1} \in \{0,1\}$;

– $\circ$ – операция $\circ : B_p \times B_p \to B_p$ определяется для любых $c \in B_p$ и $d \in B_p$ по формуле $c \circ d = (cd(2^{l+2})^{-1}) \bmod p$;

– $c^{(k)}$ – степень числа на основе операции $\circ$, определяется индуктивно по формуле $c^{(k)} = \begin{cases} c, & k = 1, \\ c^{(k-1)} \circ c, & k > 1. \end{cases}$, где k – натуральное число;

– h – функция хэширования, процедура вычисления значений которой соответствует СТБ.

Процедура выработки ЭЦП.

1. Выбираются параметры l и r, которые определяют уровень криптографической стойкости ЭЦП. Число l является длиной записи числа p в системе счисления по основанию 2, r является длиной записи числа q в системе счисления по основанию 2.

2. В соответствии с выбранными l и r генерируются простые числа p и q, такие, что q делит $p-1$ нацело.

3. Генерируется случайное число d, $0 < d < p$.

4. Вычисляется $a = d^{\left(\frac{p-1}{q}\right)}$. Если $a \equiv 2^{l+2} \bmod p$, то перейти к п. 3.

5. Генерируется случайное число x, $0 < x < q$, которое является секретным ключом.

6. Вычисляется число $y = a^{x}$, которое является открытым ключом.

7. Генерируется случайное число k, $0 < k < q$.

8. Вычисляется $t = a^{k}$. Далее число t разлагается по основанию 2^8, т. е. $t = \sum_{i=0}^{n-1} t_i (2^8)^i$. Таким образом получаются коэффициенты $t_0, t_1, \ldots, t_{n-1}$.

9. Формируется последовательность $M_t = t_0, t_1, \ldots, t_{n-1}, m_1, m_2, \ldots, m_z$, состоящая из коэффициентов $t_0, t_1, \ldots, t_{n-1}$ и блоков открытого текста $m_1, m_2, \ldots, m_z$.

10. Вычисляется значение хэш-функции $U = h(M_t)$. Если $U = 0$, то перейти к п. 6.

11. Вычисляется $V = (k - xU) \bmod q$. Если $V = 0$, то перейти к п. 6.

12. Вычисляется $S = U \cdot 2^r + V$. ЭЦП последовательности M_t есть число S.

13. Отправляется M_t, S.

Процедура проверки ЭЦП.

1. Вычисляется $V = S \bmod 2^r$.

2. Вычисляется $U = (S - V)/2^r$.

3. Если хотя бы одно из условий $0 < U < 2^r$ и $0 < V < q$ не выполнено, то ЭЦП считается недействительной и работа алгоритма завершается.

4. Вычисляется $t' = a^{V} \circ y^{U}$.

5. Число t' разлагается по основанию 2^8, т. е. $t' = \sum_{i=0}^{n-1} t'_i (2^8)^i$. Таким образом, получаются коэффициенты $t'_0, t'_1, \ldots, t'_{n-1}$.

6. Формируется последовательность $M'_t = t'_0, t'_1, \ldots, t'_{n-1}, m_1, m_2, \ldots, m_z$, состоящая из коэффициентов $t'_0, t'_1, \ldots, t'_{n-1}$ и блоков открытого текста $m_1, m_2, \ldots, m_z$.

7. Вычисляется хэш-функция $W = h\ M'_t$.

8. Проверяется условие $W = U$. При совпадении W и U принимается решение о том, что ЭЦП была создана при помощи личного ключа подписи x, связанного с открытым ключом проверки подписи y, а также ЭЦП и последовательность M_t не были изменены с момента их создания. В противном случае подпись считается недействительной.

Стандарт «Процедура выработки и проверки ЭЦП» содержит алгоритмы и процедуры выработки и проверки электронной цифровой подписи, а также подробные инструкции:

– по выбору величин r и l (размер p и q);

– генерации p и q;

– генерации a.

7.6. Аутентификация пользователей в телекоммуникационных системах

7.6.1. Общие сведения

Аутентификация пользователей обеспечивает работу в сети только санкционированных пользователей. Чаще всего аутентификация проводится при входе в сеть, но может проводиться и во время работы. Обычно проводится после процесса идентификации, во время которого пользователь сообщает свой идентификатор (называет себя). В процедуре аутентификации участвуют две стороны: пользователь доказывает свою подлинность, а сеть проверяет это доказательство и принимает решение. В качестве доказательства используют:

– знание секрета (пароля);

– владения уникальным предметом (физическим ключом);

– предъявления биометрической характеристики (отпечатка пальца, рисунка радужной оболочки глаза, голоса).

Наиболее распространенное средство аутентификации – пароль. Используется как при входе в систему, так и в процессе работы. Пароль может вводиться с клавиатуры, с различных носителей цифровой информации или комбинировано. При использовании паролей необходимо соблюдать необходимые требования: по правилам генерации (длина, случайность символов), хранения (хранить в защищенном месте), использования (в зашифрованном виде), отзыва.

В качестве субъектов аутентификации могут выступать не только пользователи, но и различные устройства или процессы. Причем процесс аутентификации может носить обоюдный характер. Обе стороны должны доказать свою подлинность. Например, пользователь, обращающийся к корпоративному серверу, должен убедится, что имеет дело с сервером своего предприятия. В этом случае процедура называется «взаимная аутентификация».

7.6.2. Удаленная аутентификация пользователей с использованием пароля

Процесс удаленной аутентификации обычно выполняют в начале сеанса связи. Рассмотрим аутентификацию с использованием пароля.

Пусть стороны *A* и *B* знают друг друга и имеют одинаковый секретный ключ $К_{AB}$. Пользователь *A* вводит свой персональный идентификатор (PIN). Его программа, используя ключ и PIN, вырабатывает пароль *P*, который вместе с PIN передается по сети к пользователю *B*. Пользователь *B* по PIN находит в своей базе ключ $К_{AB}$, с помощью которого вырабатывает *P*. После чего сравнивает значение полученного пароля и выработанного. Схема описанной аутентификации приведена на рис. 7.10.

Рассмотренная схема имеет существенный недостаток: злоумышленник может перехватить пароль *P* и PIN и позднее использовать их для своей аутентификации. Для устранения этого недостатка используют механизм отметки времени («временной штемпель»). Суть этого механизма заключается в том, что при выработке пароля наряду с ключом используется текущее время в виде некоторого интервала, в пределах которого пароль действителен; аналогично

вырабатывается пароль на стороне *B*, и в этом случае устаревшим паролем нельзя воспользоваться.

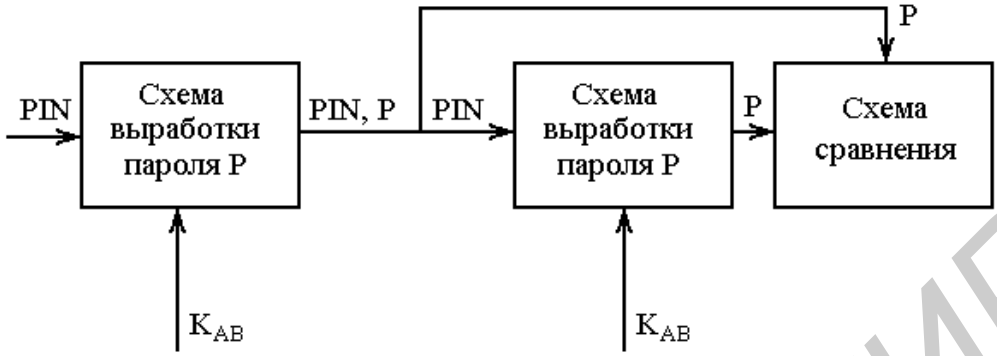


Рис. 7.10. Схема аутентификации с использованием пароля

7.6.3. Удаленная аутентификация пользователей с использованием механизма запроса-ответа

Процедура состоит в следующем. Если пользователь *A* хочет быть уверенным, что сообщения, получаемые им от пользователя *B*, не являются ложными, он включает в посылаемое для *B* сообщение непредсказуемый элемент - запрос *X* (например некоторое случайное число). При ответе пользователь *B* должен выполнить над этим элементом некоторую операцию (например вычислить некоторую функцию $f(X)$). Это невозможно осуществить заранее, так как пользователю *B* не известно, какое случайное число *X* придет в запросе. Получив ответ с результатом действий *B*, пользователь *A* может быть уверен, что *B* – подлинный. Недостаток этого метода – возможность установления закономерности между запросом и ответом.

Механизм запрос–ответ используется в более сложной процедуре аутентификации – **«рукопожатии».**

Процедура **«рукопожатия»** базируется на указанном выше механизме и заключается во взаимной проверке ключей, используемых сторонами. Иначе говоря, стороны признают друг друга законными партнерами, если докажут друг другу, что обладают правильными ключами. Процедуру рукопожатия

обычно применяют в компьютерных сетях при организации сеанса связи между пользователями, пользователем и хост-компьютером, между хост-компьютерами и т. д.

Рассмотрим в качестве примера процедуру рукопожатия для двух пользователей *A* и *B*. (Это допущение не влияет на общность рассмотрения. Такая же процедура используется, когда вступающие в связь стороны не являются пользователями). Пусть применяется симметричная криптосистема. Пользователи *A* и *B* разделяют один и тот же секретный ключ $К_{AB}$. Вся процедура показана на рис. 7.11.

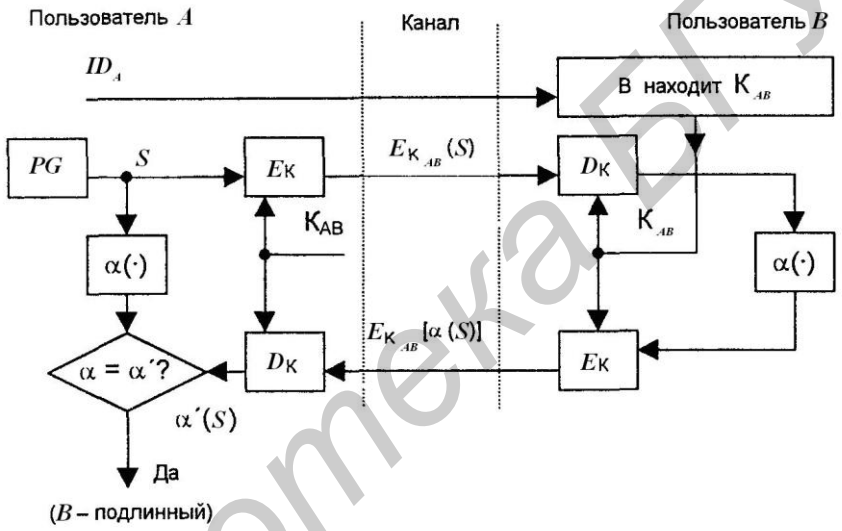


Рис. 7.11. Схема процедуры рукопожатия (пользователь *A* проверяет подлинность пользователя *B*)

Пусть пользователь *A* инициирует процедуру рукопожатия, отправляя пользователю *B* свой идентификатор ID_A в открытой форме. Пользователь *B*, получив идентификатор ID_A, находит в базе данных секретный **ключ** $К_{AB}$ и вводит его в свою криптосистему.

Тем временем **пользователь *A*** генерирует случайную **последовательность *S*** с помощью псевдослучайного генератора PG и отправляет ее **пользователю *B*** в виде криптограммы $E_{К_{AB}}\ S$. Пользователь *B* расшифровывает эту криптограмму и раскрывает исходный вид последовательности *S*. Затем оба

пользователя A и B преобразуют последовательность S, используя открытую одностороннюю функцию a^*.

Пользователь B шифрует сообщение $a\ S$ и отправляет эту криптограмму **пользователю *A***. Наконец, пользователь A расшифровывает эту криптограмму и сравнивает полученное сообщение $a'\ S$ с исходным $a\ S$. Если эти сообщения равны, пользователь A признает подлинность пользователя B.

Очевидно, пользователь B проверяет подлинность пользователя A таким же способом. Обе эти процедуры составляют процедуру рукопожатия, которая обычно выполняется в самом начале любого сеанса связи между любыми двумя сторонами в компьютерных сетях.

Достоинством модели рукопожатия является то, что ни один из участников сеанса связи не получает никакой секретной информации во время процедуры подтверждения подлинности.

Процедура рукопожатия была рассмотрена в предположении, что пользователи A и B доверяют друг другу и имеют общий **секретный сеансовый ключ**. Однако нередки ситуации, когда пользователи должны осуществить взаимную аутентификацию не доверяя друг другу и не обмениваясь никакой конфиденциальной информацией.

7.6.4. Протоколы идентификации с нулевой передачей знаний

Описанная выше ситуация характерна при использовании интеллектуальных карт (смарт-карт) для разнообразных коммерческих, гражданских и военных применений (кредитные карты, карты социального страхования, карты доступа в охраняемое помещение, компьютерные пароли и ключи и т. п.) Во многих приложениях главная проблема заключается в том, чтобы при предъявлении интеллектуальной карты оперативно обнаружить обман и отказать обманщику в допуске, ответе или обслуживании.

Для безопасного использования интеллектуальных карт разработаны протоколы идентификации с нулевой передачей знаний. Секретный ключ владель-

ца карты становится неотъемлемым признаком его личности. Доказательство знания этого секретного ключа с нулевой передачей этого знания служит доказательством подлинности личности владельца карты.

1. Упрощенная схема идентификации с нулевой передачей знаний. Схему идентификации с нулевой передачей знаний предложили в 1986 г. У. Фейге, А. Фиат и А. Шамир. Она является наиболее известным доказательством идентичности с нулевой передачей конфиденциальной информации.

Рассмотрим упрощенный вариант схемы идентификации с нулевой передачей знаний для более четкого выявления ее основной концепции. Прежде всего выбирают случайное значение модуля n, который является произведением двух больших простых чисел. Модуль n должен иметь длину 512…1024 бит. Это значение n может быть представлено группе пользователей, которым придется доказывать свою подлинность. В процессе идентификации участвуют две стороны:

1) сторона *A*, доказывающая свою подлинность,

2) сторона *B*, проверяющая представляемое стороной *A* доказательство.

Для того чтобы сгенерировать открытый и секретный ключи для стороны *A*, доверенный арбитр (Центр) выбирает некоторое число V, которое является квадратичным вычетом по модулю n. Иначе говоря, выбирается такое число V, при котором сравнение $x^2 \equiv V \bmod n$ имеет решение и существует целое число $V^{-1} \bmod n$.

Выбранное значение V является **открытым ключом** для *A*. Затем вычисляют наименьшее значение *S*, для которого $S = sqrt\ V^{-1} \mod n$. Это значение *S* является секретным ключом для *A*.

Теперь можно приступить к выполнению протокола идентификации.

1. Сторона *A* выбирает некоторое случайное число r, где $r < n$. Затем она вычисляет $x = r^2 \bmod n$ и отправляет x стороне *B*.

2. Сторона *B* посылает *A* случайный бит b.

3. Если $b=0$, тогда *A* отправляет r стороне *B*. Если $b=1$, то *A* отправляет стороне *B* $y=r\cdot S \bmod n$.

4. Если $b=0$, то сторона *B* проверяет, что $x=r^2 \bmod n$,чтобы убедиться, что *A* знает $sqrt\ \ x$. Если $b=1$, сторона *B* проверяет, что $x=y^2\cdot V \bmod n$, чтобы быть уверенной, что *A* знает $sqrt\ \ V^{-1}$.

Эти шаги образуют один цикл протокола, называемый аккредитацией. Стороны *A* и *B* повторяют этот цикл t раз при разных случайных значениях r и b до тех пор, пока *B* не убедиться, что *A* знает значение *S*.

Если сторона *A* не знает значения *S*, она может выбрать такое значение r, которое позволит ей обмануть сторону *B*, если *B* отправит ей $b=0$, либо *A* может выбрать такое r, которое позволит обмануть *B*, если *B* отправит ей $b=1$. Но этого невозможно сделать в обоих случаях. Вероятность того, что *A* обманет *B* в одном цикле, составляет $1/2$. Вероятность обмануть *B* t циклах равна $1/2^{\ t}$.

Для того чтобы этот протокол работал, сторона *A* никогда не должна повторно использовать значение r. Если *A* поступила бы таким образом, а сторона *B* отправила бы стороне *A* на шаге 2 другой случайный бит b, то *B* имела бы оба ответа *A*. После этого *B* может вычислить значение *S*, и для *A* все закончено.

2. Параллельная схема идентификации с нулевой передачей знаний. Параллельная схема идентификации позволяет увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.

Как и в предыдущем случае, сначала генерируется число n как произведение двух больших чисел. Для того чтобы сгенерировать открытый и секретный ключи для стороны *A*, сначала выбирают К различных чисел $V_1, V_2, ...V_{\text{К}}$, где каждое V_i является квадратичным вычетом по модулю n. Иначе говоря, значение V_i выбирают таким, что сравнение $x^2 \equiv V_i \bmod n$ имеет решение и существу-

ет $V_i^{-1} \bmod n$. Полученная строка $V_1, V_2, ... V_K$ является открытым ключом. Затем вычисляют такие наименьшие значения S_i, что $S_i = sqrt\ V_i^{-1} \bmod n$. Эта строка $S_1, S_2, ... S_K$ является секретным ключом стороны *A*.

Процесс идентификации имеет следующий вид:

1) сторона *A* выбирает некоторое случайное число r, где $r < n$. Затем она вычисляет $x = r^2 \bmod n$ и посылает x стороне *B*;

2) сторона *B* отправляет стороне *A* некоторую случайную двоичную строку из К бит: $b_1, b_2, ... b_K$;

3) сторона *A* вычисляет $y = r \cdot S^{b_1} \cdot S^{b_2} \cdot ... \cdot S^{b_K} \bmod n$.

Перемножаются только те значения S_i, для которых $b_i = 1$. Например, если $b_i = 1$, то сомножитель S_i входит в произведение, если же $b_i = 0$, то S_i не входит в произведение, и т. д. Вычисленное значение y отправляется стороне *B*;

4) сторона *B* проверяет, что $x = y^2 \cdot V_1^{b_1} \cdot V_2^{b_2} \cdot ... \cdot V_K^{b_K} \bmod n$.

Фактически, сторона *B* перемножает только те значения V_i, для которых $b_i = 1$. Стороны *A* и *B* повторяют этот протокол t раз, пока *B* не убедиться, что *A* знает $S_1, S_2, ... S_K$.

Вероятность того, что *A* может обмануть *B*, равна $1/2^{Kt}$. Рекомендуются в качестве контрольного значения брать вероятность обмана *B* равной $1/2^{20}$ при $K = 5$ и $t = 4$.

Стороны *A* и *B* повторяют этот протокол t раз, каждый раз с разным случайным числом r, пока сторона *B* не будет удовлетворена.

При малых значениях величин, как в данном примере, не достигается настоящей безопасности. Но если n представляет собой число длиной 512 бит и более, сторона *B* не сможет узнать ничего о секретном ключе стороны *A*, кроме того факта, что сторона *A* знает этот ключ.

7.7. Контрольные вопросы

1. Какое название носит параметр, с помощью которого выбирается криптографическое преобразование?

2. Чем определяется криптостойкость криптосистемы?

3. Дайте краткую характеристику криптоаналитическим атакам.

4. Какие требования предъявляются к шифрам криптографической защиты информации?

5. Какие шифры могут использоваться в традиционных симметричных криптосистемах?

6. Дайте краткую характеристику стандарту шифрования данных ГОСТ 28147–89.

7. Какие режимы работы стандарта шифрования данных ГОСТ 28147–89, и в чем их сущность?

8. В чем сущность концепции криптосистем с открытым ключом?

9. Какие виды злоумышленных действий, направленных на электронные документы, вы знаете?

10. Какие процедуры включает в себя технология электронной цифровой подписи?

11. Для чего предназначена хэш-функция, и каким условиям она должна удовлетворять?

12. Дайте краткую характеристику алгоритму электронной цифровой подписи RSA.

13. В чем сущность выработки и проверки электронной цифровой подписи в соответствие с белорусским стандартом?

14. Какие аутентификационные факторы пользователь может предъявить в качестве доказательства своей подлинности?

15. Сравните удаленную аутентификацию пользователя с помощью пароля и механизма запроса–ответа.

16. Какими преимуществами обладают протоколы идентификации с нулевой передачей знаний?

8. ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

8.1. Политика безопасности

Политика безопасности – набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в системе.

Политика безопасности представляет собой некоторый набор требований, прошедших соответствующую проверку, реализуемых при помощи организационных мер и программно-технических средств и определяющих архитектуру системы защиты. Ее реализация для конкретной АСОИ осуществляется при помощи средств управления механизмами защиты.

Для конкретной организации политика безопасности должна быть индивидуальной, зависимой от конкретной технологии обработки информации, используемых программных и технических средств, расположения организации т. д.

Под «системой» мы будем понимать некоторую совокупность субъектов и объектов и их отношений между ними.

Субъект – активный компонент системы, который может явиться причиной потока информации от объекта к объекту или изменения состояния системы.

Объект – пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту подразумевает доступ к содержащейся в нем информации.

Основу политики безопасности составляет способ управления доступом, определяющий порядок доступа субъектов системы к объектам системы. Название этого способа, как правило, определяет название политики безопасности.

Для изучения свойств способа управления доступом создается его формальное описание – математическая модель. При этом модель должна отражать состояния всей системы, ее переходы из одного состояния в другое, а также

учитывать, какие состояния и переходы можно считать безопасными в смысле данного управления.

В настоящее время лучше всего изучены два вида политики безопасности – избирательная и полномочная – основанные, соответственно, на избирательном и полномочном способах управления доступом.

Кроме того, существует набор требований, усиливающий действие этих политик и предназначенный для управления информационными потоками в системе.

Необходимо отметить, что средства защиты, предназначенные для реализации какого-либо из названных выше способов управления доступом, только предоставляют возможности надежного управления доступом или информационными потоками. Определение прав доступа субъектов к объектам и/или информационным потокам (полномочий субъектов и атрибутов объектов, присвоение меток критичности и т. д.) входит в компетенцию администрации системы.

8.1.1. Избирательная политика безопасности

Основой избирательной политики безопасности является избирательное управление доступом, которое подразумевает, что:

– все субъекты и объекты системы должны быть идентифицированы;

– права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа (рис. 8.1). Такая модель получила название матричной.

Матрица доступа представляет собой прямоугольную матрицу, в которой объекту системы ($O_1 \ldots O_n$) соответствует строка, а субъекту ($C_1 \ldots C_n$) – столбец.

На пересечении столбца и строки матрицы указывается тип (типы) разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа

субъекта к объекту, как «доступ на чтение» (Read Only), «доступ на запись» (Write Only), «доступ на чтение-запись» (Read-Write) и др.

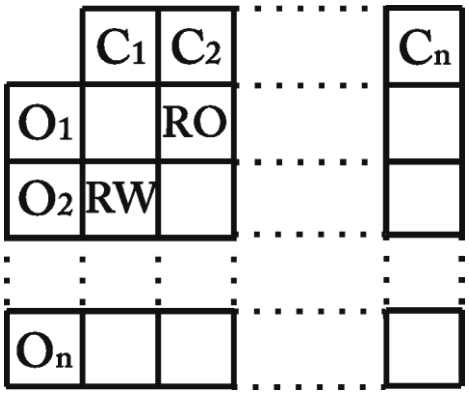


Рис. 8.1. Матрица доступа

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей ИУД. Например, доступ субъекта к конкретному объекту может быть разрешен только в определенные дни (дата-зависимое условие), часы (время-зависимое условие) в зависимости от других характеристик субъекта (контекстно-зависимое условие) или в зависимости от характера предыдущей работы. Такие условия на доступ к объектам обычно используются в системах управления базами данных. Кроме того, субъект с определенными полномочиями может передать их другому субъекту (если это не противоречит правилам политики безопасности).

Решение на доступ субъекта к объекту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно избирательное управление доступом реализует принцип «что не разрешено, то запрещено», предполагающий явное разрешение доступа субъекта к объекту.

Матрица доступа (МД) – наиболее примитивный подход к моделированию систем, который, однако, является основой для более сложных моделей, наиболее полно описывающих различные стороны реальных автоматизированных систем.

Вследствие больших размеров и разреженности МД хранение полной матрицы представляется нецелесообразным, поэтому во многих средствах защиты используют более экономные представления МД.

Каждый из этих способов представления МД имеет свои достоинства и недостатки, обусловливающие область их применения. Поэтому в каждом конкретном случае надо знать, во-первых, какое именно представление использует средство защиты и, во-вторых, какие особенности и свойства имеет это представление.

Избирательная политика безопасности наиболее широко применяется в коммерческом секторе, так как ее реализация на практике отвечает требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость и небольшие накладные расходы.

8.1.2. Полномочная политика безопасности

Основу полномочной политики безопасности составляет полномочное управление доступом (Mandatory Access Control; MAC), которое подразумевает следующее:

– все субъекты и объекты системы должны быть однозначно идентифицированы;

– каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

– каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

В случае, если совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру, и, таким образом, в системе можно реализовать иерархически не исходящий (по ценности) поток информации (например от рядовых исполнителей к руководству). Чем важнее объект или субъект, тем выше

его метка критичности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки критичности.

Каждый субъект кроме уровня прозрачности имеет текущее значение уровня безопасности, которое может изменяться от некоторого минимального значения до значения его уровня прозрачности.

Для моделирования полномочного управления доступом используется модель Белла-Лападулла, включающая в себя понятия безопасного (с точки зрения политики) состояния и перехода. Для принятия решения на разрешение доступа производится сравнение метки критичности объекта с уровнем прозрачности и текущим уровнем безопасности субъекта. Результат сравнения определяется двумя правилами: простым условием защиты и *-свойством. В упрощенном виде они определяют, что информация может передаваться только «наверх», т. е. субъект может читать содержимое объекта, если его текущий уровень безопасности не ниже метки критичности объекта, и записывать в него, если не выше (*-свойство).

Простое условие защиты гласит, что любую операцию над объектом субъект может выполнять только в том случае, если его уровень прозрачности не ниже метки критичности объекта.

Основное назначение полномочной политики безопасности – регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние. При этом она функционирует на фоне избирательной политики, придавая требованиям последней иерархически упорядоченный характер (в соответствии с уровнями безопасности).

Изначально полномочная политика безопасности была разработана в интересах Министерства обороны США для обработки информации с различными грифами секретности. Ее применение в коммерческом секторе сдерживается следующими основными причинами:

– отсутствием в коммерческих организациях четкой классификации хранимой и обрабатываемой информации, аналогичной государственной классификации (грифы секретности сведений);

– высокой стоимостью реализации и большими накладными расходами.

8.1.3. Управление информационными потоками

Помимо управления доступом субъектов к объектам системы проблема защиты информации имеет еще один аспект.

Для того чтобы получить информацию о каком-либо объекте системы, вовсе не обязательно искать пути несанкционированного доступа к нему. Можно получать информацию, наблюдая за работой системы и, в частности, за обработкой требуемого объекта. Иными словами, при помощи каналов утечки информации. По этим каналам можно получать информацию не только о содержимом объекта, но и о его состоянии, атрибутах и так далее в зависимости от особенностей системы и установленной защиты объектов. Эта особенность связана с тем, что при взаимодействии субъекта и объекта возникает некоторый поток информации от субъекта к объекту (информационный поток).

Информационные потоки существуют в системе всегда. Поэтому возникает необходимость определить, какие информационные потоки в системе являются «легальными», т. е. не ведут к утечке информации, а какие – ведут. Таким образом, возникает необходимость разработки правил, регулирующих управление информационными потоками в системе.

Для этого необходимо построить модель системы, которая может описывать такие потоки. Такая модель разработана Гогеном и Мисгаером и называется потоковой. Модель описывает условия и свойства взаимного влияния (интерференции) субъектов, а также количество информации, полученной субъектом в результате интерференции.

Управление информационными потоками в системе не есть самостоятельная политика, так как оно не определяет правил обработки информации.

Управление информационными потоками применяется обычно в рамках избирательной или полномочной политики, дополняя их и повышая надежность системы защиты.

Управление доступом (избирательное или полномочное) сравнительно легко реализуемо (аппаратно или программно), однако оно неадекватно реальным автоматизированным системам из-за существования в них скрытых каналов. Тем не менее управление доступом обеспечивает достаточно надежную защиту в простых системах, не обрабатывающих особо важную информацию. В противном случае средства защиты должны дополнительно реализовывать управление информационными потоками. Организация такого управления в полном объеме достаточно сложна, поэтому его обычно используют для усиления надежности полномочной политики: восходящие (относительно уровней безопасности) информационные потоки считаются разрешенными, все остальные – запрещенными.

Отметим, что кроме способа управления доступом политика безопасности включает еще и другие требования, такие, как подотчетность, гарантии и т. д.

Избирательное и полномочное управление доступом, а также управление информационными потоками – вот на чем строится вся защита.

8.2. Механизмы защиты

Достоверная вычислительная база (ДВБ) – абстрактное понятие, обозначающее полностью защищенный механизм вычислительной системы (включая аппаратные и программные средства), отвечающий за поддержку реализации политики безопасности.

Основой ДВБ является **ядро безопасности** – элементы аппаратного и программного обеспечения, защищенные от модификации и проверенные на корректность, которые разделяют все попытки доступа субъектов к объектам.

Ядро безопасности является реализацией концепции монитора ссылок – абстрактной концепции механизма защиты.

Помимо ядра безопасности ДВБ содержит другие механизмы, отвечающие за жизнедеятельность системы. К ним относятся планировщики процессов, диспетчеры памяти, программы обработки прерываний, примитивы ввода – вывода и другие программно-аппаратные средства, а также системные наборы данных.

Под монитором ссылок понимают концепцию контроля доступа субъектов к объектам в абстрактной машине. Схематически монитор ссылок изображен на рис. 8.2.

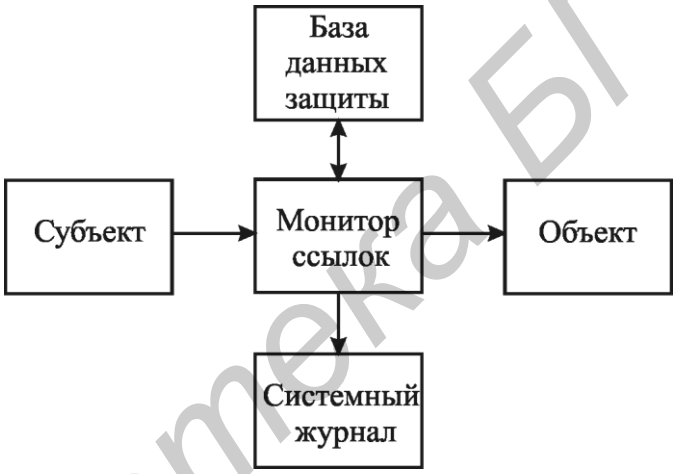


Рис. 8.2. Концепция монитора ссылок

Под базой данных защиты понимают базу данных, хранящую информацию о правах доступа субъектов системы к объектам. Основу базы данных защиты составляет матрица доступа или ее представления, которая служит основой избирательной политики безопасности.

Любая операционная система, поддерживающая ИУД, использует МД и операции над ней, поскольку МД – удобный инструмент контроля использования и передачи привилегий. Однако вследствие больших размеров и разреженности МД хранение полной матрицы представляется нецелесообразным, поэтому во многих системах используют более экономные представления МД: по строкам, по столбцам, поэлементно.

Профиль. Профилем называется список защищаемых объектов системы и прав доступа к ним, ассоциированный с каждым субъектом. При обращении к объекту профиль субъекта проверяется на наличие соответствующих прав доступа. Таким образом, МД представляется своими строками.

В системах с большим количеством объектов профили могут иметь большие размеры и вследствие этого ими трудно управлять; изменение профилей нескольких субъектов может потребовать большого количества операций и привести к трудностям в работе системы. Поэтому профили обычно используются лишь администраторами безопасности для контроля работы субъектов, однако такое их применение весьма ограничено.

Список контроля доступа. Это представление МД по столбцам – каждому объекту соответствует список субъектов вместе с их правами. В современных условиях списки контроля доступа (СКД) – лучшее направление реализации ИУД, поскольку это очень гибкая структура, предоставляющая пользователям много возможностей.

Мандат или билет. Это элемент МД, определяющий тип доступа определенного субъекта к определенному объекту (т. е. субъект имеет «билет» на доступ к объекту). Каждый раз билет выдается субъекту динамически – при запросе доступа – и также динамически билет может быть изъят у субъекта. Поскольку распространение билетов происходит очень динамично и они могут размещаться непосредственно внутри объектов, то контроль за распространением очень затруднен. В чистом виде билетный механизм хранения и передачи привилегий используется редко. Однако реализация других механизмов присвоения привилегий (например с использованием СКД) часто осуществляется с помощью билетов.

При реализации полномочной политики безопасности база данных защиты также содержит метки критичности всех объектов и уровни прозрачности субъектов системы.

Монитор ссылок должен выполнять следующие функции:

1) проверять права доступа каждого субъекта к любому объекту на основании информации, содержащейся в базе данных защиты и положений политики безопасности (избирательной или полномочной);

2) при необходимости регистрировать факт доступа и его параметры в системном журнале.

Реализующее монитор ссылок ядро безопасности должно обладать следующими свойствами:

– контролировать все попытки доступа субъектов к объектам;

– иметь защиту от модификации, подделки, навязывания;

– быть протестировано и верифицировано для получения гарантий надежности;

– иметь небольшой размер и компактную структуру.

В терминах модели Белла-Лападулла (избирательном и полномочном видах политики безопасности) монитор ссылок должен контролировать состояния системы и переходы из одного в другое. Ниже приведены основные функции, которые должно выполнять ядро безопасности совместно с другими службами ОС.

1. Идентификация, аутентификация и авторизация субъектов и объектов системы. Эти функции необходимы для подтверждения подлинности субъекта, законности его прав на данный объект или на определенные действия, а также для обеспечения работы субъекта в системе и поддержания разрешительного порядка доступа к системе и соблюдения политики безопасности: авторизованный (разрешенный) доступ имеет только тот субъект, чей идентификатор удовлетворяет результатам аутентификации. Они выполняются как в процессе работы (при обращении к наборам данных, устройствам, ресурсам), так и при входе в систему.

2. Контроль входа пользователя в систему и управление паролями. Эти функции являются частным случаем перечисленных выше: при входе в систему и вводе имени пользователя осуществляется идентификация, при вводе пароля – аутентификация, и если пользователь с данными именем и паролем

зарегистрирован в системе, ему разрешается доступ к определенным объектам и ресурсам (авторизация). Однако при входе в систему существуют отличия при выполнении этих функций. Они обусловлены тем, что в процессе работы система уже имеет информацию о том, кто работает, какие у него полномочия (на основе информации в базе данных защиты) и так далее, и поэтому может адекватно реагировать на запросы субъекта. При входе в систему это все только предстоит определить. В данном случае возникает необходимость организации «достоверного маршрута» – пути передачи идентифицирующей информации от пользователя к ядру безопасности для подтверждения подлинности. Как показывает практика, вход пользователя в систему – одно из наиболее уязвимых мест защиты; известно множество случаев взлома пароля, входа без пароля, перехвата пароля и т. д. Поэтому при выполнении входа и пользователь, и система должны быть уверены, что они работают непосредственно друг с другом, между ними нет других программ и вводимая информация истинна.

Достоверный маршрут реализуется привилегированными процедурами ядра безопасности, работа которого обеспечивается механизмами ДВБ, а также некоторыми другими механизмами, выполняющими вспомогательные функции. Они проверяют, например, не занят ли, терминал, с которого осуществляется вход в систему, никаким другим пользователем, который имитировал окончание работы.

3. Регистрация и протоколирование. Аудит. Эти функции обеспечивают получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля, а также регистрацию действий, признанных администрацией потенциально опасными для безопасности системы. Такими средствами могут быть различные системные утилиты или прикладные программы, выводящие информацию непосредственно на системную консоль или другое определенное для этой цели устройство, а также системный журнал. Кроме того, почти все эти средства контроля могут не только обнаружить какое-либо событие, но и фиксировать его. Например, большинство систем имеет

средства протоколирования сеансов работы отдельных пользователей (всего сеанса или его отдельных параметров).

Большинство систем защиты имеют в своем распоряжении средства управления системным журналом. Как было показано выше, системный журнал является составной частью монитора ссылок и служит для контроля соблюдения политики безопасности. Он является одним из основных средств контроля, помогающим администратору предотвращать возможные нарушения. Свойства системного журнала:

– способен оперативно фиксировать происходящие в системе события;

– может помочь выявить средства и априорную информацию, использованные злоумышленником для нарушения;

– может помочь определить, как далеко зашло нарушение, подсказать метод его расследования и способы исправления ситуации.

Содержимое системного журнала и других наборов данных, хранящих информацию о результатах контроля, должны подвергаться периодическому просмотру и анализу (аудиту) с целью проверки соблюдения политики безопасности.

4. Противодействие «сборке мусора». После окончания работы программы обрабатываемая информация не всегда полностью удаляется из памяти. Части данных могут оставаться в оперативной памяти, на дисках и лентах, других носителях. Они хранятся на диске до перезаписи или уничтожения. При выполнении этих действий на освободившемся пространстве диска находятся их остатки.

Хотя при искажении заголовка файла эти остатки прочитать трудно, однако с помощью специальных программ и оборудования такая возможность все-таки реализуется. Этот процесс называется «сборкой мусора» (disk scavenging). Он может привести к утечке важной информации.

Для защиты от «сборки мусора» используются специальные средства, которые могут входить в ядро безопасности ОС или устанавливаться дополнительно.

5. Контроль целостности субъектов. Согласно модели Белла-Лападулла, множество субъектов системы есть подмножество множества объектов, т. е. каждый субъект одновременно является объектом. При этом под содержимым субъекта обычно понимают содержимое контекста процесса, куда входит содержимое общих и специальных регистров (контекст процесса постоянно изменяется). Кроме содержимого или значения субъект имеет ряд специфических атрибутов: приоритет, список привилегий, набор идентификаторов и другие характеристики. В этом смысле поддержание целостности субъекта, т. е. предотвращение его несанкционированной модификации, можно рассматривать как частный случай этой задачи для объектов вообще.

В то же время субъект отличается от объекта тем, что является, согласно определению, активным компонентом системы. В связи с этим для защиты целостности субъекта, в качестве представителя которого выступает процесс, вводится такое понятие, как рабочая среда, или область исполнения процесса. Эта область является логически защищенной подсистемой, которой доступны все ресурсы системы, относящиеся к соответствующему процессу. Другими словами, область исполнения процесса является виртуальной машиной. В рамках этой области процесс может выполнять любые санкционированные действия без опасения нарушения целостности. Таким образом, реализуется концепция защищенной области для отдельного процесса.

Контроль целостности обеспечивается процедурами ядра безопасности, контролируемыми механизмами поддержки ДВБ. Основную роль играют такие механизмы, как поддержка виртуальной памяти (для создания области данного процесса) и режим исполнения процесса (определяет его возможности в рамках данной области и вне ее).

Область исполнения процесса может содержать или вкладываться в другие подобласти, которые составляют единую иерархическую структуру системы. Процесс может менять области: это действие называется переключением области процесса. Оно всегда связано с переходом центрального процессора в привилегированный режим работы.

Механизмы поддержки областей исполнения процесса обеспечивают контроль их целостности достаточно надежно. Однако даже разделенные процессы должны иметь возможность обмениваться информацией. Для этого разработаны несколько специальных механизмов, чтобы можно было осуществлять обмен информацией между процессами без ущерба безопасности или целостности каждого из них. К таким механизмам относятся, например, кластеры флагов событий, почтовые ящики и другие системные структуры данных. Следует, однако, учитывать, что с их помощью может осуществляться утечка информации, поэтому если использование таких механизмов разрешено, их обязательно следует контролировать.

6. Контроль доступа. Под контролем доступа будем понимать ограничение возможностей использования ресурсов системы программами, процессами или другими системами (для сети) в соответствии с политикой безопасности. Под доступом понимается выполнение субъектом некоторой операции над объектом из множества разрешенных для данного типа. Примерами таких операций являются чтение, открытие, запись набора данных, обращение к устройству и т. д.

Контроль должен осуществляться при доступе к следующим объектам:

– оперативной памяти;

– разделяемым устройствам прямого доступа и последовательного доступа;

– разделяемым программам и подпрограммам;

– разделяемым наборам данных.

Основным объектом внимания средств контроля доступа являются совместно используемые наборы данных и ресурсы системы. Совместное использование объектов порождает ситуацию «взаимного недоверия», при которой разные пользователи одного объекта не могут до конца доверять друг другу. Тогда, если с этим объектом что-нибудь случиться, все они попадают в круг подозреваемых.

Существует четыре основных способа разделения субъектов по отношению к совместно используемым объектам:

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

– временное – субъекты с различными правами доступа к объекту получают его в различные промежутки времени;

– логическое – субъекты получают доступ к совместно используемому объекту в рамках единой операционной среды, но под контролем средств разграничения доступа, которые моделируют виртуальную операционную среду «один субъект – все объекты»; в этом случае разделение может быть реализовано различными способами: разделение оригинала объекта, разделение с копированием объекта и т. д;

– криптографическое – все объекты хранятся в зашифрованном виде, права доступа определяются наличием ключа для расшифровки объекта.

Существует множество различных вариантов одних и тех же способов разделения субъектов, они могут иметь разную реализацию в различных средствах защиты.

Контроль доступа субъектов системы к объектам (не только к совместно используемым, но и к индивидуальным) реализуется с помощью тех же механизмов, которые реализуют ДВБ, и осуществляется процедурами ядра безопасности.

8.3. Принципы реализации политики безопасности

Как уже отмечалось выше, настройка механизмов защиты – дело сугубо индивидуальное для каждой системы и даже для каждой задачи. Поэтому дать ее подробное описание довольно трудно. Однако существуют общие принципы, которых следует придерживаться, чтобы облегчить себе работу, так как они проверены практикой.

1. Группирование. Это объединение множества субъектов под одним групповым именем; всем субъектам, принадлежащим одной группе, предоставляются равные права (рис. 8.3). Принципы объединения пользователей в группы могут быть самые разные: ссылки на одни и те же объекты, одинаковый характер вычислений, работа над совместным проектом и т. д. При этом один и тот же субъект может входить в несколько различных групп и, соответственно, иметь различные права по отношению к одному и тому же объекту.

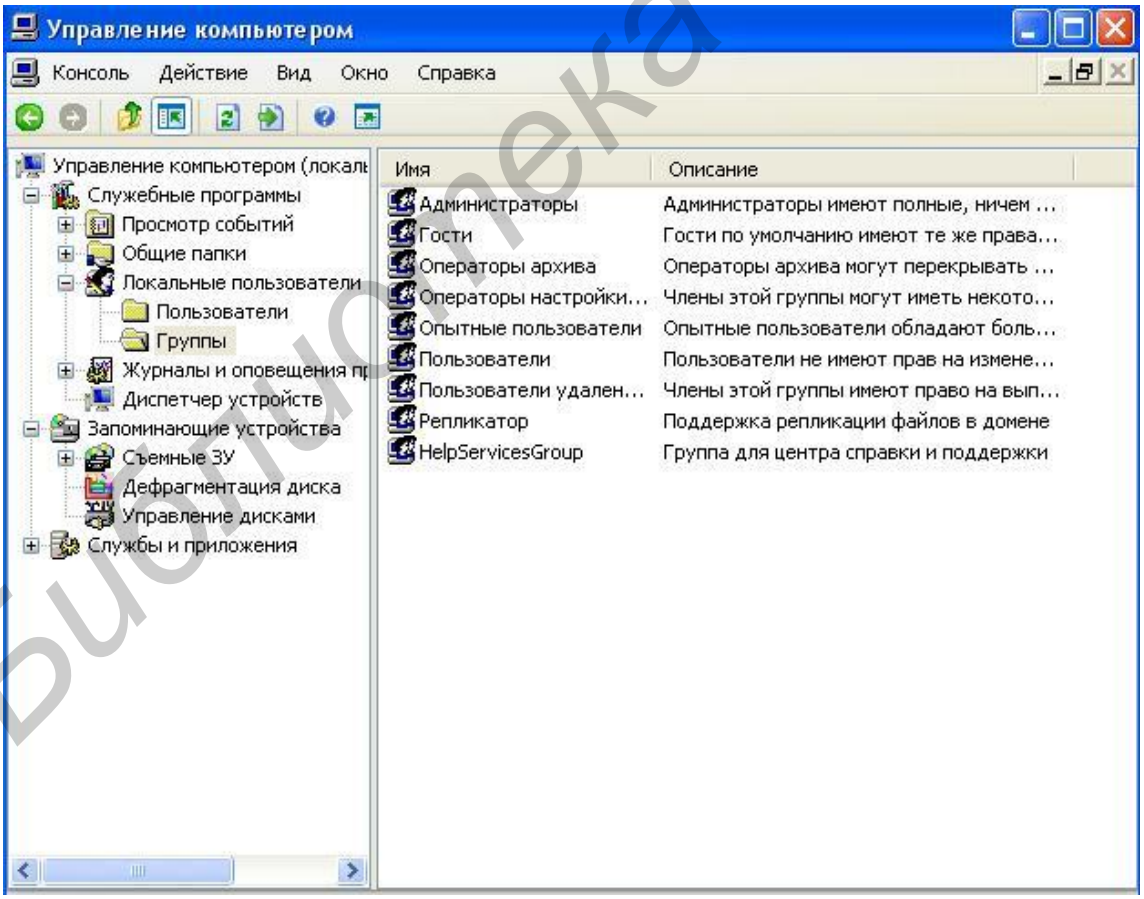


Рис. 8.3. Внешний вид окна «Управление компьютером» в Windows XP, обеспечивающего доступ к группам пользователей

Механизм группирования может быть иерархическим. Это означает, что каждый субъект является членом нескольких групп, упорядоченных по принципу «быть подмножеством». Контроль за состоянием групп очень важен, поскольку члены одной группы имеют доступ к большому числу объектов, что не способствует их безопасности. Создание групп и присвоение групповых привилегий должно производиться администратором безопасности, руководителем группы или каким-либо другим лицом, несущим ответственность за сохранность групповых объектов.

2. Правила умолчания. Большое внимание при назначении привилегий следует уделять правилам умолчания, принятым в данных средствах защиты; это необходимо для соблюдения политики безопасности (рис. 8.4.). Например, во многих системах субъект, создавший объект и являющийся его владельцем, по умолчанию получает все права на него. Кроме того, он может эти права передавать кому-либо.

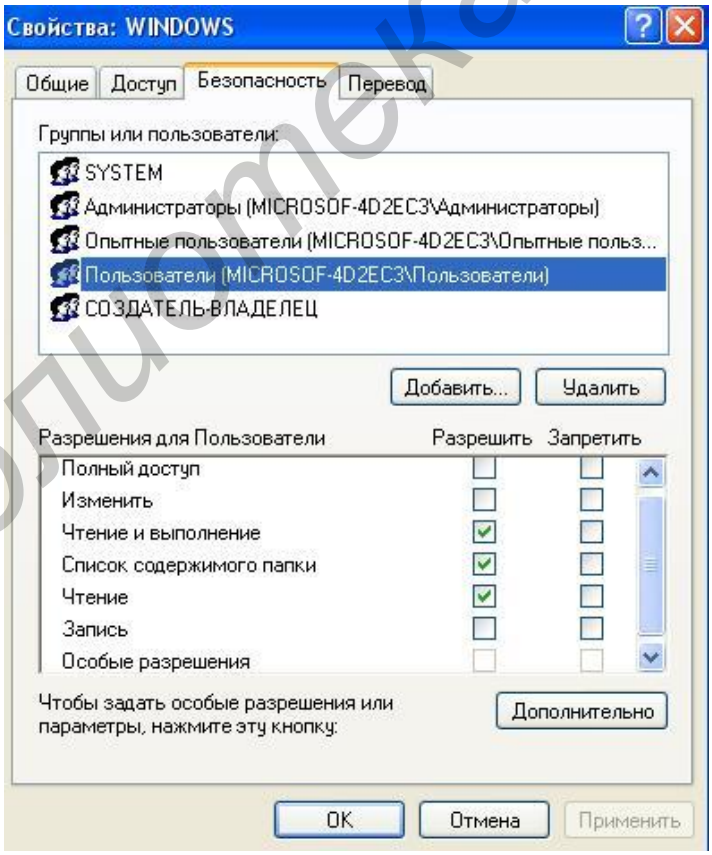


Рис. 8.4. Права доступа (по умолчанию) пользователей группы «Пользователи» к папке Windows

В различных средствах защиты используются свои правила умолчания, однако принципы назначения привилегий по умолчанию в большинстве систем одни и те же. Если в системе используется древовидная файловая структура, то необходимо принимать во внимание правила умолчания для каталогов. Корректное использование правил умолчания способствует поддержанию целостности политики безопасности.

3. Минимум привилегий. Это один из основополагающих принципов реализации любой политики безопасности, используемый повсеместно. Каждый пользователь и процесс должен иметь минимальное число привилегий, необходимых для работы. Определение числа привилегий для всех пользователей, позволяющих, с одной стороны, осуществлять быстрый доступ ко всем необходимым для работы объектам, а с другой, запрещать доступ к чужим объектам – проблема достаточно сложная. От ее решения во многом зависит корректность реализации политики безопасности.

4. «Надо знать». Этот принцип во многом схож с предыдущим. Согласно ему, полномочия пользователей в свою очередь назначаются сообразно их обязанностям. Доступ разрешен только к той информации, которая необходима пользователям для работы.

5. Объединение критичной информации. Во многих системах сбор, хранение и обработка информации одного уровня производится в одном месте (узле сети, устройстве, каталоге). Это связано с тем, что проще защитить одним и тем же способом большой массив информации, чем организовывать индивидуальную защиту для каждого набора.

Для реализации этого принципа могут быть разработаны специальные программы, управляющие обработкой таких наборов данных. Это будет простейший способ построения защищенных областей.

6. Иерархия привилегий. Контроль объектов системы может иметь иерархическую организацию. Такая организация принята в большинстве коммерческих систем.

При этом схема контроля имеет вид дерева, в котором узлы – субъекты системы, ребра – право контроля привилегий согласно иерархии, корень – администратор системы, имеющий право изменять привилегии любого пользователя (рис. 8.5).

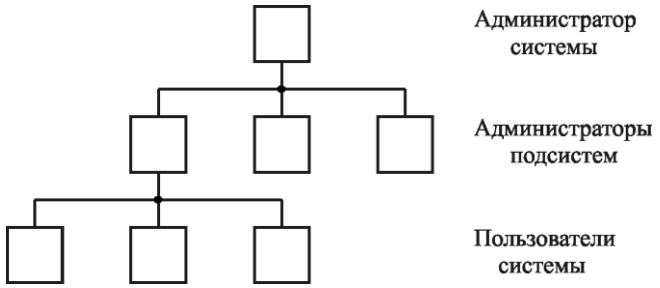


Рис. 8.5. Схематичное изображение иерархической реализации привилегий в автоматизированной системе

Узлами нижележащих уровней являются администраторы подсистем, имеющие права изменять привилегии пользователей этих подсистем (в их роли могут выступать руководители организаций, отделов). Листьями дерева являются все пользователи системы. Вообще говоря, субъект, стоящий в корне любого поддерева, имеет право изменять защиту любого субъекта, принадлежащего этому поддереву.

Достоинство такой структуры – точное копирование схемы организации, которую обслуживает автоматизированная система. Поэтому легко составить множество субъектов, имеющих право контролировать данный объект. Недостаток иерархии привилегий – сложность управления доступом при большом количестве субъектов и объектов, а также возможность получения администратором системы (как высшего по иерархии) доступа к любому набору данных.

7. Привилегии владельца. При таком контроле каждому объекту соответствует единственный субъект с исключительным правом контроля объекта – владелец. Как правило, это его создатель. Владелец обладает всеми разрешенными для этого типа данных правами на объект, может разрешать доступ любому другому субъекту, но не имеет права никому передать привилегию на

корректировку защиты. Однако такое ограничение не касается администраторов системы: они имеют право изменять защиту любых объектов.

Главным недостатком принципа привилегий владельца является то, что при обращении к объекту пользователь должен предварительно получить разрешение у владельца (или администратора). Это может приводить к сложностям в работе (например при отсутствии владельца или просто нежелании его разрешить доступ). Поэтому такой принцип обычно используется при защите личных объектов пользователей.

8. Свободная передача привилегий. При такой схеме субъект, создавший объект, может передать любые права на него любому другому субъекту вместе с правом корректировки СКД этого объекта. Тот, в свою очередь, может передать все эти права другому субъекту.

Естественно, при этом возникают большие трудности в определении круга субъектов, имеющих в данный момент доступ к объекту (права на объект могут распространяться очень быстро и так же быстро исчезать), и поэтому такой объект легко подвергнуть несанкционированной обработке. В силу этих обстоятельств подобная схема применяется достаточно редко – в основном в исследовательских группах, работающих над одним проектом (когда все имеющие доступ к объекту заинтересованы в его содержимом).

В чистом виде рассмотренные принципы реализации политики безопасности применяются редко. Обычно используются их различные комбинации. Ограничение доступа к объектам в ОС включает в себя ограничение доступа к некоторым системным возможностям, например ряду команд, программам и так далее, если при использовании их нарушается политика безопасности. Вообще, набор полномочий каждого пользователя должен быть тщательно продуман, исключены возможные противоречия и дублирования, поскольку большое количество нарушений происходит именно из-за этого. Может произойти утечка информации без нарушения защиты, если плохо была спроектирована или реализована политика безопасности.

Политика безопасности и механизмы поддержки ее реализации образуют единую защищенную среду обработки информации. Эта среда имеет иерархическую структуру, где верхние уровни представлены требованиями политики безопасности, далее следует интерфейс пользователя, затем идут несколько программных уровней защиты (включая уровни ОС), и, наконец, нижний уровень этой структуры представлен аппаратными средствами защиты. На всех уровнях, кроме верхнего, должны реализовываться требования политики безопасности, за что, собственно, и отвечают механизмы защиты.

В различных системах механизмы защиты могут быть реализованы поразному; их конструкция определяется общей концепцией системы. Однако одно требование должно выполняться неукоснительно: эти механизмы должны адекватно реализовывать требования политики безопасности.

8.4. Защита транзакций в Интернет

8.4.1. Классификация типов мошенничества в электронной коммерции

Транзакция – последовательность операций, представляющих собой одну логическую единицу работы с данными.

Высокий уровень мошенничества в Интернете является сдерживающим фактором развития электронной коммерции (ЭК), поскольку покупатели, торговля и банки ограничивают использование этой технологии из-за опасности понести финансовые потери.

Приведем классификацию возможных типов мошенничества в Интернет, приводимую международными платежными системами Visa и MasterCard:

– транзакции, выполненные мошенниками с использованием правильных реквизитов карточки (номер карточки, срок ее действия и т. п.);

– компрометация данных (получение данных о клиенте через взлом базы данных торговых предприятий или путем перехвата сообщений покупателя, со-

держащих его персональные данные) с целью их использования в мошеннических целях;

– создание магазинов, возникающих, как правило, на непродолжительное время, для того чтобы исчезнуть после получения от покупателей средств за несуществующие услуги или товары;

– злоупотребления торговых предприятий, связанные с увеличением стоимости товара по отношению к предлагавшейся покупателю цене или повтором списаний со счета клиента;

– создание магазинов и торговых агентов, чьей целью является сбор информации о реквизитах карт и других персональных данных покупателей.

В соответствии с данными международных платежных систем все конфликты, связанные с ЭК, делятся в основном на три класса:

1) владелец карты утверждает, что никогда не проводил транзакцию через Интернет;

2) владелец карты утверждает, что заказ ЭК не был выполнен;

3) владелец карты оспаривает размер транзакции.

8.4.2. Протокол SSL

Самый известный протокол Интернета – SSL (Secure Socket Layer). Этот протокол был разработан компанией Netscape и является составной частью всех известных Интернет-браузеров и Web-серверов (сегодня используется версия 3.0 протокола SSL). Протокол реализуется между транспортным и сеансовым уровнями эталонной модели взаимодействия открытых систем (OSI). Это, с одной стороны, означает возможность использования протокола для организации защищенной сессии между программами, работающими по различным протоколам прикладного уровня OSI (FTP, SMTP, Telnet, HTTP и т. п.), а с другой – закрытие любых данных, передаваемых в SSL-сессии, что приводит к снижению производительности протокола.

Последняя версия протокола SSL поддерживает три режима аутентификации:

1) взаимную аутентификацию сторон;

2) одностороннюю аутентификацию сервера (без аутентификации клиента);

3) полную анонимность.

Очевидно, что последний вариант представляет собой экзотический случай, так как взаимодействующие стороны оказываются незащищенными от возможных атак, связанных с подменой участников, хотя при этом и обеспечивается защита от несанкционированного доступа самого установленного соединения.

В упрощенном виде процедура установления защищенного режима взаимодействия между клиентом и Web-сервером в соответствии с протоколом SSL выглядит следующим образом (рассмотрим вариант односторонней аутентификации сервера со стороны клиента).

Этап установления SSL-сессии («рукопожатие»).

1. КЛИЕНТ посылает СЕРВЕРУ запрос (Client hello) на установление защищенного соединения, в котором передает некоторые формальные параметры этого соединения:

– текущее время и дату;

– случайную последовательность (RAND_CL) длиной 28 байтов;

– набор поддерживаемых клиентом симметричных криптографических алгоритмов и хэш-алгоритмов, используемых при формировании кода для проверки целостности передаваемого сообщения (MAC – Message Authentication Code);

– набор поддерживаемых алгоритмов сжатия (все реализации протокола SSL должны поддерживать метод Compression Method null).

Следует отметить, что КЛИЕНТ имеет возможность в запросе указать идентификатор SSL-сессии, которая была установлена ранее или поддерживается в настоящий момент времени. В этом случае процедура согласования параметров для устанавливаемой сессии не требуется (используются параметры, согласованные для сессии с указанным в запросе идентификатором SSL-сессии).

Кроме того, инициировать SSL-сессию может и Web-СЕРВЕР. Для этого СЕРВЕР может в любой момент времени направить КЛИЕНТУ сообщение Hello request, которое информирует КЛИЕНТА о том, чтобы он направил СЕРВЕРУ сообщение Client Hello.

2. СЕРВЕР обрабатывает запрос от КЛИЕНТА и в ответном сообщении (Server hello) передает ему следующий согласованный набор параметров:

– идентификатор SSL-сессии;

– конкретные криптографические алгоритмы из числа предложенных клиентом (если по какой-либо причине предложенные алгоритмы или их параметры не удовлетворяют требованиям сервера, сессия закрывается);

– сертификат сервера, заверенный цифровой подписью ЦС (в формате X.509 v.3);

– случайную последовательность (RAND_SERV);

– цифровую подпись для перечисленных выше данных.

3. КЛИЕНТ проверяет полученный сертификат СЕРВЕРА с помощью открытого ключа ЦС, который ему известен; при положительном результате проверки КЛИЕНТ выполняет следующие действия (при отрицательном результате проверки сессия закрывается):

– генерирует случайную 48-байтную последовательность Pre_MasterSecret (часть совместного секрета, известного только СЕРВЕРУ и КЛИЕНТУ); шифрует ее на открытом ключе сервера, полученном в сертификате сервера, и посылает СЕРВЕРУ;

– с помощью согласованных хэш-алгоритмов формирует главный совместный секрет (MasterSecret), используя в качестве параметров часть совместного секрета Pre_MasterSecret, посланную СЕРВЕРУ на предыдущем шаге случайную последовательность RAND_CL и полученную от него случайную последовательность RAND_SERV;

– используя MasterSecret, вычисляет криптографические параметры SSL-сессиии: формирует общие с сервером сеансовые секретные ключи симметричного алгоритма шифрования (для приема и для передачи) и секреты для вычисления MAC;

– переходит в режим защищенного взаимодействия.

4. СЕРВЕР расшифровывает полученный Pre_MasterSecret с помощью своего секретного ключа и выполняет над ним те же операции, что и КЛИЕНТ:

– с помощью согласованных хэш-алгоритмов формирует главный совместный секрет (MasterSecret), используя в качестве параметров Pre_MasterSecret посланную КЛИЕНТУ на предыдущем шаге случайную последовательность RAND_SERV и полученную от него случайную последовательность RAND_CL;

– используя MasterSecret, вычисляет криптографические параметры SSL-сессии: формирует общие с клиентом сеансовые секретные ключи одноключевого алгоритма шифрования и секрет для вычисления MAC;

– переходит в режим защищенного взаимодействия.

Поскольку при формировании параметров SSL-сессии КЛИЕНТ и СЕРВЕР пользовались одними и теми же исходными данными (согласованными алгоритмами, общим секретом Pre_MasterSecret и случайными последовательностями RAND_CL и RAND_SERV), то очевидно, что в результате описанных выше действий они выработали одинаковые сеансовые секретные ключи шифрования и секреты, используемые для защиты целостности передаваемых сообщений.

5. Для проверки идентичности параметров SSL-сессии КЛИЕНТ и СЕРВЕР посылают друг другу тестовые сообщения, содержание которых известно каждой из сторон:

– КЛИЕНТ формирует сообщение из собственных посылок в адрес СЕРВЕРА на этапе 1 и посылок, полученных от СЕРВЕРА на этапе 1, внося элемент случайности в виде последовательности MasterSecret, уникальной для данной сессии; формирует код для проверки целостности сообщения (MAC), шифрует сообщение на общем сеансовом секретном ключе и отправляет СЕРВЕРУ;

– СЕРВЕР, в свою очередь, формирует сообщение из собственных посылок в адрес СЕРВЕРА на этапе 1, посылок, полученных от КЛИЕНТА на этапе 1, и последовательности MasterSecret; формирует код для проверки целостности сообщения (MAC), шифрует сообщение на общем сеансовом секретном ключе и отправляет КЛИЕНТУ;

– в случае успешной расшифровки и проверки целостности каждой из сторон полученных тестовых сообщений SSL-сессия считается установленной и стороны переходят в штатный режим защищенного взаимодействия.

Этап защищенного взаимодействия с установленными криптографическими параметрами SSL-сессии.

1. Каждая сторона при передаче сообщения формирует код для последующей проверки целостности сообщения на приемной стороне (MAC) и шифрует исходное сообщение вместе с кодом на своем секретном сеансовом ключе.

2. Каждая сторона при приеме сообщения расшифровывает его и проверяет на целостность (вычисляется MAC и сверяется с кодом проверки целостности, полученным вместе с сообщением); в случае обнаружения нарушения целостности сообщения SSL-сессия закрывается.

Описанная процедура установления SSL-сессии, безусловно, не обладает полнотой изложения, однако дает представление о возможностях протокола SSL.

Как следует из описания протокола SSL, асимметричные алгоритмы шифрования используются только на этапе установления защищенной сессии. Для защиты информационного обмена от несанкционированного доступа используются только симметричные алгоритмы. Это делается в первую очередь для того, чтобы повысить производительность протокола SSL.

Для защиты трафика в Интернете помимо протокола SSL используется протокол S-HTTP (Secure HTTP). Этот протокол обеспечивает целостность и защиту документов, передаваемых по протоколу HTTP. В отличие от протокола SSL, расположенного между транспортным уровнем (TCP) и протоколами сеансового уровня, протокол S-HTTP находится на прикладном уровне OSI, что позволяет с его помощью защищать не транспортное соединение, а данные, передаваемые по соединению. Это повышает производительность протокола защиты информации, но ценой ограничения применимости механизма защиты только приложением HTTP.

Достоинства протокола:

1) широкое распространение протокола SSL, которое объясняется в первую очередь тем, что он является составной частью всех известных Интернет-браузеров и Web-серверов. Это означает, что фактически любой владелец карты, пользуясь стандартными средствами доступа к Интернету, получает возможность провести транзакцию с использованием SSL;

2) простота протокола для понимания всех участников ЭК;

3) хорошие операционные показатели (скорость реализации транзакции). Последнее достоинство связано с тем, что протокол в процессе передачи данных использует только симметричные протоколы шифрования.

Недостатками протокола SSL в приложении к ЭК являются:

1) отсутствие аутентификации клиента Интернет-магазином, поскольку сертификаты клиента в протоколе почти не используются. Использование «классических» сертификатов клиентами в схемах SSL является делом практически бесполезным. Такой «классический» сертификат, полученный клиентом в одном из известных центров сертификации, содержит только имя клиента и, что крайне редко, его сетевой адрес;

2) протокол SSL не позволяет аутентифицировать клиента обслуживающим банком;

3) при использовании протокола SSL торговое предприятие (ТП) аутентифицируется только по своему адресу в Интернете (URL). Это значит, что клиент, совершающий транзакцию ЭК, не аутентифицирует ТП в полном смысле. Аутентификация ТП только по URL облегчает мошенническим ТП доступ к различным системам ЭК. В частности, торговые предприятия, занимающиеся сбором информации о картах клиентов, могут получить сертификат в каком-либо известном центре сертификации общего пользования на основании только своих учредительных документов;

4) протокол SSL не поддерживает цифровой подписи, что затрудняет процесс разрешения конфликтных ситуаций, возникающих в работе платежной системы (цифровая подпись используется в начале установления SSL-сессии при аутентификации участников сессии). Для доказательства проведения транзакции требуется либо хранить в электронном виде весь диалог клиента и ТП (включая процесс установления сессии), что дорого с точки зрения затрат ресурсов памяти и на практике не используется, либо хранить бумажные копии, подтверждающие получение клиентом товара;

5) при использовании SSL не обеспечивается конфиденциальность данных о реквизитах карты для ТП.

8.4.3. Протокол SET

Для операций с кредитными карточками используется протокол SET (Secure Electronic Transactions), разработанный совместно компаниями Visa, MasterCard, Netscape и Microsoft.

В отличие от SSL протокол SET узко специализирован. Целью SET является обеспечение необходимого уровня безопасности для платежного механизма, в котором участвует три или более субъектов. При этом предполагается, что транзакция реализуется через Интернет.

На базовом уровне SET осуществляет следующие функции:

Аутентификация. Все участники кредитных операций идентифицируются с помощью электронных подписей. Это касается клиента-покупателя, продавца, банка, выдавшего кредитную карточку, и банка-продавца.

Конфиденциальность. Все операции производятся в зашифрованном виде.

Целостность сообщений. Информация не может быть подвергнута модификации по дороге, в противном случае это будет сразу известно.

Совместимость. Должна быть предусмотрена совместимость с любыми программными продуктами и с любыми сервис-провайдерами.

Независимость от транспортного протокола. Безопасность операций не должна зависеть от уровня безопасности транспортного протокола. Такие гарантии особенно важны, так как протокол SET ориентирован для работы в Интернете.

На более высоком уровне протокол SET поддерживает все возможности, предоставляемые современными кредитными карточками:

– регистрацию держателя карточки;

– регистрацию продавца;

– запрос покупки;

– авторизацию платежа;

– перевод денег;

– кредитные операции;

– возврат денег;

– отмену кредита;

– дебитные операции.

Окончательная версия протокола SET была выпущена в мае 1997 года. Протокол работает с четырьмя субъектами: владельцем кредитной карточки, банком, эту карточку выпустившим (issuer – эмитент), продавцом (merchant) и банком, где помещен счет продавца (acquirer). Помимо этих функциональных субъектов в процессе обычно (опционно) участвуют центры сертификации, в задачу которых входит подтверждение подлинности предъявляемых параметров аутентификации, причем в случае крупных сделок с этими центрами должны взаимодействовать все участники. Основной целью сертификатов является подтверждение того, что присланный общедоступный ключ прибыл от настоящего отправителя.

Схема взаимодействия субъектов при использовании протокола SET показана на рис. 8.6 (взаимодействия с центром сертификации не показаны).

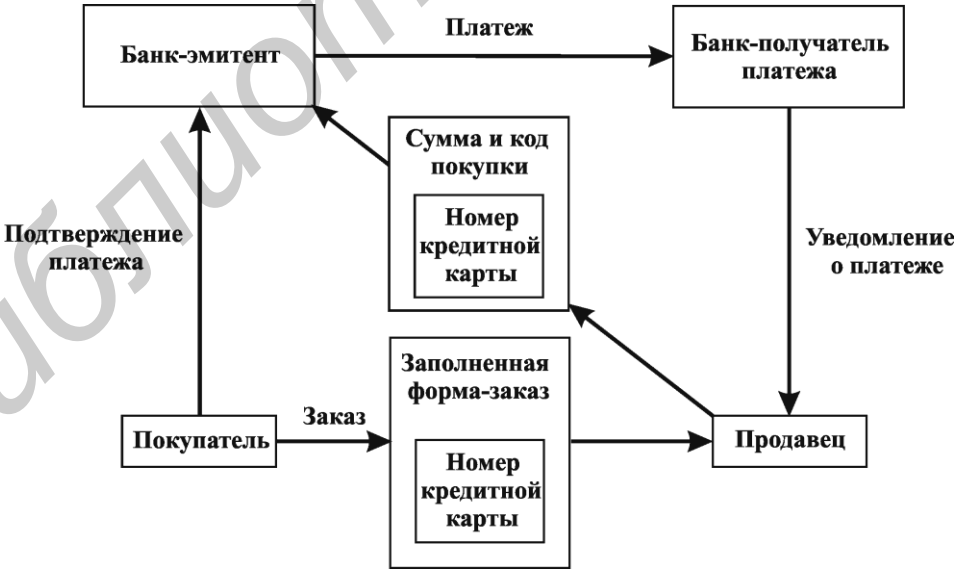


Рис. 8.6. Схема взаимодействия субъектов при использовании протокола SET

Протокол SET помогает реализовать следующие процедуры.

1. Покупатель инициализирует покупку. При этом покупатель выбирает продавца, просматривает его WEB-сайт, принимает решение о покупке, заполняет бланк заказа. Все это делается до вступления в дело протокола SET. Взаимодействие участников сделки регламентируется протоколом IOTP. SET начинает свою работу, когда покупатель нажимает клавишу оплаты. При этом сервер посылает ЭВМ-покупателю сообщение, которое и запускает соответствующую программу. Процедура эта может быть реализована с помощью PHP- или CGI-скрипта или JAVA-аплета.

2. Программа клиента посылает заказ и информацию об оплате. Для этого формируется два сообщения, одно содержит данные о полной стоимости покупки и номере заказа, второе – номер кредитной карточки покупателя и банковскую информацию. Сообщение о заказе шифруется с использованием симметричного метода (например DES) и вкладывается в цифровой конверт, где используется общедоступный ключ продавца. Сообщение об оплате шифруется с привлечением общедоступного ключа банка (эмитента кредитной карты). В результате продавец не получает доступа к номеру кредитной карточки покупателя. Программа генерирует хэш-дайджест (SHA1) обоих сообщений с использованием секретного ключа покупателя. Это позволяет продавцу и банку проконтролировать целостность сообщения, но препятствует прочтению части, ему не предназначенной (например номера кредитной карты продавцом).

3. Продавец выделяет часть, адресованную банку, и направляет ее по месту назначения. Программа SET WEB-сервера продавца генерирует запрос авторизации серверу банка, где находится счет продавца. При формировании запроса авторизации используется электронная подпись продавца, базирующаяся на его секретном ключе, что позволяет однозначно его идентифицировать. Этот запрос шифруется с помощью ключа сессии и вкладывается в цифровой конверт, где используется общедоступный ключ банка.

4. Банк проверяет действительность кредитной карточки, расшифровывает запрос авторизации продавца и идентифицирует продавца. После этого осуществляется проверка авторизации покупателя. При этом посылается запрос авторизации, снабженный электронной подписью, банку, выпустившему кредитную карточку.

5. Банк, выпустивший карточку, выполняет авторизацию и подписывает чек, если кредитная карточка покупателя в порядке. Отклик, снабженный соответствующей подписью, посылается банку продавца.

6. Банк продавца авторизует данную операцию и посылает подтверждение, подписанное электронным образом, WEB-серверу продавца.

7. WEB-сервер продавца завершает операцию, выдавая клиенту подтверждение на экран, и заносит результат операции в соответствующую базу данных.

8. Продавец осуществляет подтверждение выполнения операции своему банку. Деньги покупателя переводятся на счет продавца.

9. Банк, выпустивший карточку, посылает счет покупателю, и SET уведомляет покупателя об изменениях на его счете (раз в месяц).

Итак, каждый шаг реализации протокола SET сопровождается аутентификацией. Это препятствует какому-то внешнему субъекту стать посредником и видоизменять сообщения. Для нормальной работы протокола SET все участники должны зарегистрироваться и снабдить партнеров своим общедоступным ключом.

8.4.4. Сравнительная характеристика протоколов SSL и SET

В табл. 8.1 приведены результаты сравнения протоколов SET и SSL по отношению к наиболее вероятным типам мошенничества в ЭК.

Важным критерием сравнения протоколов является вычислительная мощность (производительность) компьютеров и серверов владельца карты, ТП и шлюза обслуживающего банка (аппаратно-программного комплекса, конвер-

тирующего сообщения ЭК в стандартные сообщения платежной системы), необходимая для реализации того или иного протокола. Проведенные исследования показали, что время, затрачиваемое компьютером покупателя на криптографические операции, при использовании SSL на порядок меньше аналогичной величины при применении протокола SET.

Таблица 8.1

Результаты сравнения протоколов SET и SSL

Тип мошенничества	SET решает проблему?	SSL решает проблему?
Мошеннические транзакции по «правильным» картам	Да	Нет
Злоупотребления магазинов	Да	Нет
Фиктивные магазины	Нет	Нет
Фиктивные банки	Да	Нет
Компрометация данных	Да	Да

Несмотря на убедительные преимущества протокола SET, его внедрение связано с возникновением различного рода проблем. В первые два–три года распространения стандарта по миру главной проблемой являлось отсутствие взаимной совместимости продуктов различных поставщиков программных средств, поддерживающих протокол SET. Проблема успешно была решена (и эффективно решается сегодня для новых разработчиков ПО) усилиями компании SET Co и разработчиков ПО. Сегодня на рынке продается около 50 различных решений ЭК, в основе которых лежит протокол SET, более чем от 20 поставщиков программного обеспечения.

К другой проблеме следует отнести высокую стоимость решений, реализующих протокол SET; принимая во внимание наличие уже развитой базы электронных магазинов, применяющих протокол SSL, а также пока приемлемый для торговли уровень мошенничества, магазины не спешат инвестировать средства в новое решение. Это хорошо видно на примере Дании, являющейся одним из лидеров по внедрению протокола SET, компании которой при заключении договоров на обслуживание предлагают Интернет-магазинам обе техно-

логии – SSL и SET. Количество заключенных договоров на работу по технологии SSL в 10 раз больше, чем по стандарту SET.

Кроме того, отсутствие инфраструктуры Интернет-магазинов, использующих стандарт SET, сдерживает банки-эмитенты от инвестиций в SET.

Таким образом, на сегодняшний день большинство платежных Интернет-систем используют протокол SSL и различного рода технологические решения для уменьшения уровня мошенничества при проведении транзакций.

8.5. Атаки в компьютерных сетях

8.5.1. Общие сведения об атаках

Атакой на компьютерную сеть (КС) называется действие или последовательность действий нарушителя, которые приводят к реализации угроз путем использования уязвимостей этой КС. Уязвимости делят на уязвимости за счет наличия недостатков в аппаратно-программном продукте по вине разработчика; уязвимости, добавленные администратором при настройке КС; уязвимости, внесенные пользователем КС (короткий пароль, игнорирование политики безопасности). Атака состоит из следующих этапов: сбор информации; реализация атаки, завершение атаки.

Сбор информации. Изучение окружения атакуемой системы (определяется провайдер жертвы, адреса доверенных узлов, трафик, режим работы организации, телефонные номера и т. д.); идентификация топологии сети (определяется количество компьютеров, способ их соединения, организация выхода в глобальную сеть); идентификация узлов (проводится разведка IP-адреса узла, его доступности); идентификация сервисов и портов (определяется наличие установленных сервисов типа Telnet, FTP, Web-сервера и наличие доступа к ним, открытость портов); идентификации ОС (определяется тип ОС); определение роли узла (маршрутизатор, межсетевой экран, сервер); определение уязви-

мостей узла (на основе собранной информации определяется наличие уязвимостей).

Реализация атаки. Реализация атаки заключается в проникновении в систему и установления контроля над ней. Контроль может быть непосредственный, например, через Telnet или с помощью установленной программы.

Завершение атаки. На этом этапе злоумышленник убирает следы своей атаки с целью невозможности его идентификации. Для этого используют подмену адреса источника атаки путем создания пакетов с фальшивыми адресами источника; проводят очистку журнала регистрации событий. Либо атаку проводят с уже взломанных промежуточных серверов или proxy-серверов. Маскируют внедренные программы путем присоединения их к стандартным, либо присвоением им названий, похожих на названия стандартных программ. Изменяют контрольные суммы файлов и папок.

Большинство известных атак можно разбить на следующие группы: удаленное проникновение (атака, в результате которой реализуется удаленное управление компьютером через сеть); локальное проникновение (внедряется программа, которая управляет компьютером (Get Admin); удаленный отказ в обслуживании (перегрузка потоком сообщений узла, который не в состоянии их переработать); локальный отказ в обслуживании (узел занят обработкой некоторой задачи и все остальные игнорирует (зацикливание)); сетевое сканирование (сеть подвергается запросам программы, анализирующей топологию, доступные сервисы и уязвимости (nmap, Satan)); взлом паролей (запуск программы, подбирающие пароли пользователей (Crack)); анализ протоколов (с помощью анализатора протоколов просматривается трафик. Извлекаются идентификаторы, пароли).

8.5.2. Технология обнаружения атак

Технология обнаружения атак основывается на признаках, описывающих нарушения политики безопасности (что); источниках информации, в которых

ищутся признаки нарушения политики безопасности (где); методах анализа информации, получаемой из соответствующих источников (как).

Признаками атак являются: повтор определенных событий; неправильные или несоответствующие текущей ситуации команды; признаки работы средств анализа уязвимостей; несоответствующие параметры сетевого трафика; непредвиденные атрибуты; необъяснимые проблемы.

Повтор определенных событий. Злоумышленник, пытаясь осуществить несанкционированное проникновение, вынужден совершать определенные действия несколько раз, т. к. с одного раза он не достигает своей цели. Например, подбор пароля при аутентификации; сканирование портов с целью обнаружения открытых.

Неправильные или несоответствующие текущей ситуации команды. Обнаружение неправильных запросов или ответов, ожидаемых от автоматизированных процессов и программ. Например, в процессе аутентификации почтовых клиентов системы вместо традиционных процедур вдруг обнаружены иные команды – это свидетельствует о попытке злоумышленника получить доступ к файлу паролей почтового шлюза.

Признаки работы средств анализа уязвимостей. Имеется ряд средств автоматизированного анализа уязвимостей сети: nmap,Satan, Internet Scanner, которые в определенном порядке обращаются к различным портам с очень небольшим интервалом времени. Такие обращения являются признаками атак.

Несоответствующие параметры сетевого трафика. Например, некорректные параметры входного и выходного трафика (в КС приходят из внешней сети пакеты, имеющие адреса источника, соответствующие диапазону адресов внутренней сети; из КС выходят пакеты с адресом источника, находящегося во внешней сети; адрес источника запрещен, адрес источника и получателя совпадают); некорректные значения параметров различных полей сетевых пакетов (взаимоисключающие флаги); аномалии сетевого трафика (параметры сетевого трафика отличатся от традиционных: коэффициент загрузки, размер пакета,

среднее число фрагментированных пакетов, использование нетипичного протокола); непредвиденные атрибуты (запросы пользователей, их действия характеризуются неким типовым профилем, отклонения от него – это признак атаки, например работа в нерабочее время в выходные, во время отпуска; нетипичное местоположение пользователя, нетипичные запросы сервисов и услуг).

Необъяснимые проблемы. Проблемы с программным и аппаратным обеспечением, с системными ресурсами, с производительностью.

Источниками информации об атаках являются журналы регистрации событий (ЖРС) или сетевой трафик.

Журналы регистрации событий ведутся рабочими станциями, серверами, межсетевыми экранами (МСЭ), системами обнаружения атак. Типовая запись в таком журнале ведется по указанной в табл. 8.2:

Таблица 8.2

Форма журнала регистрации событий

Дата	Время	Источник (программа, которая регистрирует событие)	Категория (название события: вх., вых., изм. политики доступа к объекту)	Код события	Пользователь (субъект, с которым связано событие: Ad, User, system)	Компьютер (место, на котором произошло событие)

Изучение сетевого трафика позволяет проводить анализ содержания пакетов или последовательностей пакетов.

Примеры обнаружения атак по ЖРС и сетевому трафику.

Обнаружение сканирования портов. Отслеживая записи в ЖРС, замечаем, что идет поток запросов из одного адреса через короткие промежутки времени (5–10 запросов в секунду) к портам, номера которых перебираются последовательно (это признак простейшего сканирования). В более сложном ска-

нировании признаки маскируют: увеличивают временные интервалы между запросами и номера портов изменяют по случайному закону.

Обнаружение подмены адреса источника сообщения. Каждому пакету присваивается уникальный идентификатор, и если пакеты исходят из одного источника, то очередной пакет получает номер на 1 больше. Если приходят пакеты из разных источников, а их идентификаторы последовательно нарастают, то это свидетельствует о фальшивом адресе источника.

Аналогично можно использовать поле времени жизни. Пакеты, отправленные из различных источников, при приеме в узле имеют одинаковые значения (примерно) оставшегося времени жизни, хотя они должно быть разными. Следовательно, они отправлены из одного источника.

Обнаружение идентификации типа ОС. Специальной программой формируются пакеты уровня TCP, в заголовках которых используются комбинации флагов, не соответствующие стандартам. По реакции узла на эти пакеты определяется тип ОС. Данная комбинация флагов и является признаком идентификации типа ОС.

Обнаружение троянских программ. При передаче троянской программы идет обращение к портам с вполне определенными номерами. Поэтому если получены пакеты с этими номерами портов, то это свидетельствует о возможном наличии в передаваемых данных троянской программы. Кроме того, троянские программы могут быть распознаны по наличию ключевых слов в поле данных.

Обнаружение атак «Отказ в обслуживании». Обнаружение производится по превышению числа запросов в единицу времени; по совпадению адресов отправителя и получателя; по номерам портов, указанным в пакетах (пересылка пакета с 19 на 17 или 13 на 37 зацикливает атакуемый компьютер).

Для координации деятельности мирового сообщества по защите в сети Интернет создан Координационный центр CERT/CC. Он собирает всю инфор-

мацию об атаках и дает рекомендации пользователям. Адрес этого центра в Интернете: www.cept.org.

8.5.3. Методы анализа информации при обнаружении атак

Способы обнаружения атак.

Способы обнаружения атак можно разделить на обнаружение признаков аномального поведения защищаемой системы; обнаружение признаков злоумышленных действий субъектов.

Обнаружение признаков аномального поведения защищаемой системы. Составляется совокупность признаков нормального (без вмешательства злоумышленника) поведения системы – эталон признаков нормального поведения. Реальное поведение непрерывно или дискретно сравнивается с эталонным, если они не совпадают, то возможно это следствие злоумышленных действий. Таким образом, отклонение реального поведения от эталонного – признак атаки. Структурная схема системы для обнаружения признаков аномального поведения защищаемой системы изображена на рис. 8.7

Рис. 8.7. Обнаружение признаков аномального поведения защищаемой системы

При данном способе обнаруживаются любые атаки (в том числе и неизвестные), приводящие к отклонению поведения от нормального. При этом необходимо иметь эталон признаков нормального поведения. Это возможно, если процесс функционирования системы является стабильным (каждый день решаются одни и те же задачи, например в супермаркете, банке) и описывается

некой устойчивой совокупностью признаков. Все изменения в поведении таких систем – плановые, прогнозируемые и могут быть учтены путем корректировки эталона (подключение филиала банка). Режим работы систем жестко регламентируем. Для таких систем целесообразно использовать описанный способ. Например, сотрудники организации используют электронную почту только в рабочее время: $t \in$ [9–00, 18–00] – эталон; если $t_{\text{Р}}$ = 23–15, то имеет место отклонение от эталона.

Обнаружение признаков злоумышленных действий субъектов. Создается база шаблонов признаков злоумышленных действий. Реальные действия субъекта сравниваются с шаблонами признаков злоумышленных действий. При обнаружении совпадений делается вывод о наличии атаки. Таким образом, совпадение действия субъекта с одним из шаблонов – признак атаки (рис. 8.8).

Рис. 8.8. Обнаружение признаков злоумышленных действий субъектов

Данный способ должен применяться для систем, решающих разнообразные задачи, взаимодействуя с различными узлами, поведение которых является нестабильным и для которых невозможно составить эталон нормального поведения. Он требует наличия базы шаблонов признаков злоумышленных действий и не пригоден для обнаружения неизвестных атак.

Методы анализа информации.

Составление эталона признаков нормального поведения системы – сложная задача, т. к. в компьютерной системе протекает большое количество про-

цессов, она взаимодействует с различными пользователями, действия которых трудно формализуются. Аналогичные трудности встречаются и при реализации второго способа обнаружения атак.

Принята следующая классификация признаков (параметров): числовые параметры (размер сообщения, длительность временного интервала); категориальные параметры (имя файла, команда, ключевое слово); параметры активности (количество соединений в единицу времени).

Чем больше признаков используется, тем больше шансов обнаружить атаку, но, с другой стороны, анализ слишком большого количества параметров требует больших вычислительных ресурсов, при этом производительность контролируемого узла, объем операционной и дисковой памяти снижается. Большинство числовых параметров поведения системы носит случайный характер и имеют разброс значений от одного наблюдения к другому. Поэтому при составлении эталона необходимо оперировать с вероятностными характеристиками этих случайных величин (МОЖ, дисперсия, квантиль, закон распределения). Следовательно, при таком подходе задача сравнения эталона с реальным поведением может рассматриваться как задача статистической классификации. Например как задача проверки статистической гипотезы или задача распознавания образов.

При использовании аппарата проверки статистической гипотезы выдвигается гипотеза (одномерная), что среднее значение эталонного признака $\overline{X}_{Эj}$, равно среднему значению реального признака $\overline{X}_{Pj}$ т.е. H_0: $\overline{X}_{Эj} = \overline{X}_{Pj}$ при альтернативе H_1: $\overline{X}_{Эj} \neq \overline{X}_{Pj}$. Наблюдая реальные значения X_{PJ} и имея решающее правило, гипотезу можно принимать или отвергать с заданной вероятностью.

Ограничения. Необходимо знать законы распределения величин X_{PJ}, $X_{ЭJ}$. Особенно сложно определить $f(X_{ЭJ}/H_1)$. Для этого необходимо имитировать атаку на систему и определить условную плотность вероятности (т. е. обучить систему обнаружения).

Описанную процедуру следует применять для всех признаков поведения. И если хотя бы по одному из них результат отрицателен, то принимается решение о наличии атаки. При этом существуют ошибки: ложная тревога и пропуск атаки. Вероятность ошибок тем больше, чем реальные вероятностные характеристики признаков отличаются от гипотетических.

Перспективным способом анализа информации при обнаружении атак можно считать теорию нейронных сетей.

К настоящему времени информационное сообщество накопило большое количество информации о злоумышленных действиях. Известно, что негативные действия сопровождаются определенными признаками. Поскольку в сетях все действия осуществляются посредством генерации битовых потоков (сигнатур), то по многим повторяющимся атакам имеется банк сигнатур(строка символов, определенные команды, последовательность команд). В задачах обнаружения признаков злоумышленных действий эти сигнатуры играют роль шаблонов. Сетевой трафик анализируется на наличие в нем сигнатур атак. Эта задача детерминированная. Детектор обнаружения ищет совпадение сигнатур трафика с сигнатурами атак. Например, ищет некорректные значения полей в заголовке пакетов. При этом обеспечивается простота реализации, высокая скорость функционирования, отсутствие ложных тревог, однако невозможно обнаружить неизвестные атаки (шаблоны отсутствуют), небольшая модификация атаки делает ее необнаруживаемой.

8.6. Межсетевые экраны

8.6.1. Общие сведения

При подключении любой закрытой компьютерной сети к открытым сетям, например к сети Интернет, высокую актуальность приобретают угрозы несанкционированного вторжения в закрытую сеть из открытой, а также угрозы несанкционированного доступа из закрытой сети к ресурсам открытой. Подоб-

ный вид угроз характерен также для случая, когда объединяются отдельные сети, ориентированные на обработку конфиденциальной информации совершенно разного уровня секретности. При ограничении доступа этих сетей друг к другу возникают угрозы нарушения установленных ограничений.

Неправомерное вторжение во внутреннюю сеть из внешней может выполняться как с целью несанкционированного использования ресурсов внутренней сети, например хищения информации, так и с целью нарушения ее работоспособности.

Угрозы несанкционированного доступа во внешнюю сеть из внутренней сети актуальны в случае ограничения разрешенного доступа во внешнюю сеть правилами, установленными в организации. Такое ограничение, что особенно характерно для взаимодействия с открытыми сетями, может понадобиться в следующих случаях: для предотвращения утечки конфиденциальных данных; при запрете доступа, например в учебных заведениях; к информации нецензурной и нежелательной направленности; в случае запрета служебного доступа к развлекательным компьютерным ресурсам в рабочее время.

Бороться с рассмотренными угрозами безопасности межсетевого взаимодействия средствами универсальных операционных систем не представляется возможным. Универсальная операционная система – это слишком большой и сложный комплекс программ, который, с одной стороны, может содержать внутренние ошибки и недоработки, а с другой, не всегда обеспечивает защиту от ошибок администраторов и пользователей.

Поэтому проблема защиты от несанкционированных действий при взаимодействии с внешними сетями успешно может быть решена только с помощью специализированных программно-аппаратных комплексов, обеспечивающих целостную защиту компьютерной сети от враждебной внешней среды. Такие комплексы называют межсетевыми экранами, брандмауэрами или системами FireWall. Межсетевой экран устанавливается на стыке между внутренней и

внешней сетями и берет на себя функции противодействия несанкционированному межсетевому доступу.

8.6.2. Функции межсетевого экранирования

Для противодействия несанкционированному межсетевому доступу брандмауэр должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис. 8.9). При этом все взаимодействия между этими сетями должны осуществляться только через межсетевой экран. Организационно экран входит в состав защищаемой сети.

Межсетевой экран должен учитывать протоколы информационного обмена, положенные в основу функционирования внутренней и внешней сетей. Если эти протоколы отличаются, то брандмауэр должен поддерживать многопротокольный режим работы, обеспечивая протокольное преобразование отличающихся по реализации уровней модели OSI для объединяемых сетей. Чаще всего возникает необходимость в совместной поддержке стеков протоколов SPX/IPX и TCP/IP.

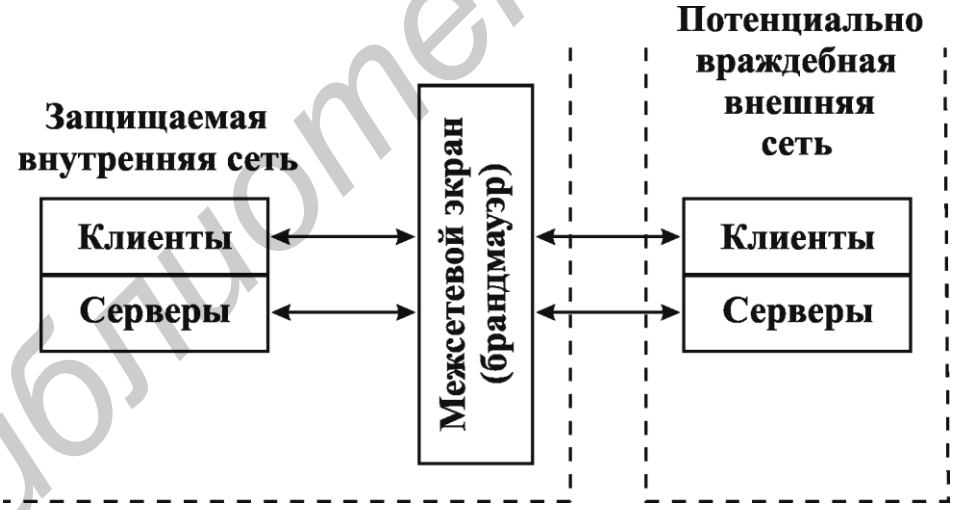


Рис. 8.9. Схема подключения межсетевого экрана

Брандмауэр не является симметричным. Для него отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю сеть и наоборот. В общем случае работа межсетевого экрана основана на динамическом выполнении двух групп функций: фильтрации проходящих через него информационных потоков; посредничества при реализации межсетевых взаимодействий.

В зависимости от типа экрана эти функции могут выполняться с различной полнотой. Простые межсетевые экраны ориентированы на выполнение только одной из данных функций. Комплексные экраны обеспечивают совместное выполнение указанных функций защиты. Собственная защищенность брандмауэра достигается с помощью тех же средств, что и защищенность универсальных систем.

Чтобы эффективно обеспечивать безопасность сети, комплексный брандмауэр обязан управлять всем потоком, проходящим через него, и отслеживать свое состояние. Для принятия управляющих решений по используемым сервисам межсетевой экран должен получать, запоминать, выбирать и обрабатывать информацию, полученную от всех коммуникационных уровней и от других приложений. Недостаточно просто проверять пакеты по отдельности.

Устройство, подобное межсетевому экрану, может использоваться и для защиты отдельного компьютера. В этом случае экран, уже не являющийся межсетевым, устанавливается на защищаемый компьютер. Такой экран, называемый брандмауэром компьютера или системой сетевого экранирования, контролирует весь исходящий и входящий трафик независимо от всех прочих системных защитных средств. При экранировании отдельного компьютера поддерживается доступность сетевых сервисов, но уменьшается или вообще ликвидируется нагрузка, индуцированная внешней активностью. В результате снижается уязвимость внутренних сервисов защищаемого таким образом компьютера, поскольку первоначально сторонний злоумышленник должен преодолеть экран, где защитные средства сконфигурированы особенно тщательно и жестко.

8.6.3. Фильтрация трафика

Фильтрация информационных потоков состоит в их выборочном пропускании через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов принятой политики безопасности. Поэтому межсетевой экран удобно представлять как последовательность фильтров, обрабатывающих ин-

формационный поток. Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем выполнения следующих стадий: 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.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например преобразование данных, регистрация событий и др. Соответственно, правила фильтрации определяют перечень условий, по которым с использованием указанных критериев анализа осуществляется: разрешение или запрещение дальнейшей передачи данных; выполнение дополнительных защитных функций.

В качестве критериев анализа информационного потока могут использоваться следующие параметры: служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные; непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов; внешние характеристики потока информации, например временные, частотные характеристики, объем данных и т. д.

Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация. В общем случае, чем выше уровень модели OSI, на котором брандмауэр фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты.

8.6.4. Выполнение функций посредничества

Функции посредничества межсетевой экран выполняет с помощью специальных программ, называемых экранирующими агентами или просто программами-посредниками. Данные программы являются резидентными и запре-

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

Функции фильтрации межсетевой экран может выполнять без применения программ-посредников, обеспечивая прозрачное взаимодействие между внутренней и внешней сетью. Вместе с тем программные посредники могут и не осуществлять фильтрацию потока сообщений.

В общем случае экранирующие агенты, блокируя прозрачную передачу потока сообщений, могут выполнять следующие функции: идентификацию и аутентификацию пользователей; проверку подлинности передаваемых данных; разграничение доступа к ресурсам внутренней сети; разграничение доступа к ресурсам внешней сети; фильтрацию и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации; трансляцию внутренних сетевых адресов для исходящих пакетов сообщений; регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов; кэширование данных, запрашиваемых из внешней сети.

Идентификация и аутентификация пользователей необходима не только при их доступе из внешней сети во внутреннюю, но и наоборот. Распространенным способом аутентификации является использование одноразовых паролей. Пароль не должен передаваться в открытом виде через общедоступные коммуникации. Это предотвратит получение несанкционированного доступа путем перехвата сетевых пакетов, что возможно, например, в случае стандартных сервисов типа Telnet.

Удобно и надежно также применение цифровых сертификатов, выдаваемых доверительными органами, например центром распределения ключей. Большинство программ-посредников разрабатывается таким образом, чтобы пользователь аутентифицировался только в начале сеанса работы с межсетевым экраном. После этого от него не требуется дополнительная аутентификация в течение времени, определяемого администратором.

Проверка подлинности получаемых и передаваемых данных необходима не только для аутентификации электронных сообщений, но и мигрирующих программ (Java, ActiveX Controls), по отношению к которым может быть выполнен подлог. Проверка подлинности сообщений и программ заключается в контроле их цифровых подписей. Для этого также могут применяться цифровые сертификаты.

Разграничение доступа к ресурсам внутренней или внешней сети. Способы разграничения к ресурсам внутренней сети ничем не отличаются от способов разграничения, поддерживаемых на уровне операционной системы. При разграничении доступа к ресурсам внешней сети чаще всего используется один из следующих подходов:

– разрешение доступа только по заданным адресам во внешней сети;

– фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам;

– накопление и обновление администратором санкционированных информационных ресурсов внешней сети в дисковой памяти брандмауэра и полный запрет доступа во внешнюю сеть.

Фильтрация и преобразование потока сообщений выполняется посредником на основе заданного набора правил. Здесь следует различать два вида программ посредников: экранирующие агенты, ориентированные на анализ потока сообщений для определенных видов сервиса, например FTP, HTTP, Telnet; универсальные экранирующие агенты, обрабатывающие весь поток сообщений,

например агенты, ориентированные на поиск и обезвреживание компьютерных вирусов или прозрачное шифрование данных.

Программный посредник анализирует поступающие к нему пакеты данных, и если какой-либо объект не соответствует заданным критериям, то посредник либо блокирует его дальнейшее продвижение, либо выполняет соответствующие преобразования, например обезвреживание обнаруженных компьютерных вирусов. При анализе содержимого пакетов важно, чтобы экранирующий агент мог автоматически распаковывать проходящие файловые архивы.

Брандмауэры с посредниками позволяют также организовывать защищенные виртуальные сети (Virtual Private Network - VPN), например безопасно объединить несколько локальных сетей, подключенных к Интернету, в одну виртуальную сеть. VPN обеспечивают прозрачное для пользователей соединение локальных сетей, сохраняя секретность и целостность передаваемой информации путем ее динамического шифрования. При передаче по Интернету возможно шифрование не только данных пользователей, но и служебной информации: конечных сетевых адресов, номеров портов и т. д.

Трансляция внутренних сетевых адресов. Данная функция реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов посредник выполняет автоматическое преобразование IP-адресов компьютеров-отправителей в один «надежный» IP-адрес, ассоциируемый с брандмауэром, из которого передаются все исходящие пакеты. В результате все исходящие из внутренней сети пакеты оказываются отправленными межсетевым экраном, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешней сетью. IP-адрес брандмауэра становится единственным активным IP-адресом, который попадает во внешнюю сеть.

При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа. Кроме повышения безопасности трансляция адресов позволяет иметь внутри сети собственную систему адресации, не согласованную с адресацией во внешней сети, например в сети Ин-

тернет. Это эффективно решает проблему расширения адресного пространства внутренней сети и дефицита адресов внешней сети.

Регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и составление отчетов. В качестве обязательной реакции на обнаружение попыток выполнения несанкционированных действий должно быть определено уведомление администратора, т. е. выдача предупредительных сигналов. Многие межсетевые экраны содержат мощную систему регистрации, сбора и анализа статистики. Учет может вестись по адресам клиента и сервера, идентификаторам пользователей, времени сеансов, времени соединений, количеству переданных/принятых данных, действиям администратора и пользователей. Системы учета позволяют произвести анализ статистики и предоставляют администраторам подробные отчеты. За счет использования специальных протоколов посредники могут выполнить удаленное оповещение об определенных событиях в режиме реального времени.

Кэширование данных, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска брандмауэра, называемого в этом случае proxy-сервером. Поэтому если при очередном запросе нужная информация окажется на proxy-сервере, то посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботиться только о периодическом обновлении содержимого proxy-сервера. За счет использования специальных протоколов посредники могут выполнить удаленное оповещение об определенных событиях в режиме реального времени.

Кэширование данных, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска брандмауэра, называемого в этом случае proxy-сервером. Поэтому если при очередном запросе нужная информация окажется на proxy-сервере, то посредник предоставляет ее без об-

ращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботиться только о периодическом обновлении содержимого proxy-сервера. Функция кэширования успешно может использоваться для ограничения доступа к информационным ресурсам внешней сети. В этом случае все санкционированные информационные ресурсы внешней сети накапливаются и обновляются администратором на proxy-сервере. Пользователям внутренней сети разрешается доступ только к информационным ресурсам proxy-сервера, а непосредственный доступ к ресурсам внешней сети запрещается. Экранирующие агенты намного надежнее обычных фильтров и обеспечивают большую степень защиты. Однако они снижают производительность обмена данными между внутренней и внешней сетями и не обладают той степенью прозрачности для приложений и конечных пользователей, которая характерна для простых фильтров.

8.6.5. Особенности межсетевого экранирования на различных уровнях модели OSI

Брандмауэры поддерживают безопасность межсетевого взаимодействия на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Поэтому комплексный межсетевой экран 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. Соответственно различают такие неделимые брандмауэры (рис. 8.10), как экранирующий маршрутизатор, экранирующий транспорт (шлюз сеансового уровня), а также экранирующий шлюз (шлюз прикладного уровня).

Учитывая, что используемые в сетях протоколы (TCP/IP, SPX/IPX) не однозначно соответствуют модели OSI, экраны перечисленных типов при выполнении своих функций могут охватывать и соседние уровни эталонной модели. Например, прикладной экран может осуществлять автоматическое зашифровывание сообщений при их передаче во внешнюю сеть, а также автоматическое расшифро-

вывание криптографически закрытых принимаемых данных. В этом случае такой экран функционирует не только на прикладном уровне модели OSI, но и на уровне представления. Шлюз сеансового уровня при своем функционировании охватывает транспортный и сетевой уровни модели OSI. Экранирующий маршрутизатор при анализе пакетов сообщений проверяет их заголовки не только сетевого, но и транспортного уровня.

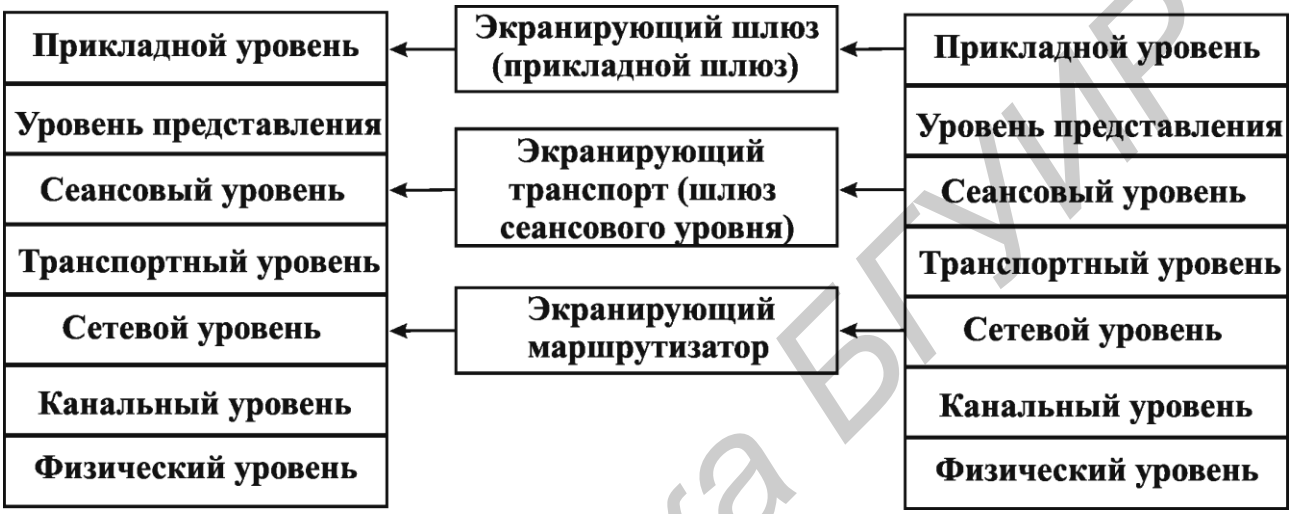


Рис. 8.10. Типы межсетевых экранов, функционирующих на отдельных уровнях модели OSI

Межсетевые экраны каждого из типов имеют свои достоинства и недостатки. Многие из используемых брандмауэров являются либо прикладными шлюзами, либо экранирующими маршрутизаторами, не поддерживая полную безопасность межсетевого взаимодействия. Надежную же защиту обеспечивают только комплексные межсетевые экраны, каждый из которых объединяет экранирующий маршрутизатор, шлюз сеансового уровня, а также прикладной шлюз.

8.6.6. Экранирующий маршрутизатор

Экранирующий маршрутизатор, называемый еще пакетным фильтром, предназначен для фильтрации пакетов сообщений и обеспечивает прозрачное взаимодействие между внутренней и внешней сетями. Он функционирует на сетевом уровне модели OSI, но для выполнения своих отдельных функций может охватывать и транспортный уровень эталонной модели. Решение о том, пропустить или от-

браковать данные, принимается для каждого пакета независимо, на основе заданных правил фильтрации. Для принятия решения анализируются заголовки пакетов сетевого и транспортного уровней. В качестве анализируемых полей IP- и TCP (UTP)-заголовков каждого пакета выступают адрес отправителя; адрес получателя; тип пакета; флаг фрагментации пакета; номер порта источника; номер порта получателя.

Адреса отправителя и получателя являются IP-адресами. Эти адреса заполняются при формировании пакета и остаются неизменными при передаче его по сети.

Поле типа пакета содержит код протокола ICMP, соответствующего сетевому уровню, либо код протокола транспортного уровня (TCP или UDP), к которому относится анализируемый IP-пакет.

Флаг фрагментации пакета определяет наличие или отсутствие фрагментации IP-пакетов. Если флаг фрагментации для анализируемого пакета установлен, то данный пакет является подпакетом фрагментированного IP-пакета.

Номера портов источника и получателя добавляются драйвером TCP или UDP к каждому отправляемому пакету сообщения и однозначно идентифицируют приложение-отправитель, а также приложение, для которого предназначен этот пакет. Например при использовании протокола передачи файлов FTP-реализация данного протокола на сервере по умолчанию получает номер TCP-порта 21. Каждый Telnet-сервер по умолчанию имеет TCP-порт 23. Для возможности фильтрации пакетов по номерам портов необходимо знание принятых в сети соглашений относительно выделения номеров портов протоколам высокого уровня.

При обработке каждого пакета экранирующий маршрутизатор последовательно просматривает заданную таблицу правил, пока не найдет правила, с которым согласуется полная ассоциация пакета. Здесь под ассоциацией понимается совокупность параметров, указанных в заголовках данного пакета. Если экранирующий маршрутизатор получил пакет, не соответствующий ни од-

ному из табличных правил, он применяет правило, заданное по умолчанию. Из соображений безопасности это правило обычно указывает на необходимость отбраковки всех пакетов, не удовлетворяющих ни одному из других правил.

В качестве пакетного фильтра может использоваться как обычный маршрутизатор, так и работающая на сервере программа, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Современные маршрутизаторы, например маршрутизирующие устройства компаний Cisco, позволяют связывать с каждым портом несколько десятков правил и фильтровать пакеты как на входе, так и на выходе.

К достоинствам экранирующих маршрутизаторов относятся: простота самого экрана, а также процедур его конфигурирования и установки; прозрачность для программных приложений и минимальное влияние на производительность сети; низкая стоимость, обусловленная тем, что любой маршрутизатор в той или иной степени представляет возможность фильтрации пакетов.

Однако экранирующие маршрутизаторы не обеспечивают высокой степени безопасности, так как проверяют только заголовки пакетов и не поддерживают многие необходимые функции защиты, например аутентификацию конечных узлов, криптографическое закрытие пакетов сообщений, а также проверку их целостности и подлинности. Экранирующие маршрутизаторы уязвимы для таких распространенных сетевых атак, как подделка исходных адресов и несанкционированное изменение содержимого пакетов сообщений. «Обмануть» межсетевые экраны данного типа не составляет труда: достаточно сформировать заголовки пакетов, которые удовлетворяют разрешающим правилам фильтрации.

8.6.7. Шлюз сеансового уровня

Шлюз сеансового уровня, называемый еще экранирующим транспортом, предназначен для контроля виртуальных соединений и трансляции IP-адресов при взаимодействии с внешней сетью. Он функционирует на сеансовом уровне модели OSI, охватывая в процессе своей работы также транспортный и сетевой уровни

эталонной модели. Защитные функции экранирующего транспорта относятся к функциям посредничества.

Контроль виртуальных соединений заключается в контроле квитирования связи, а также контроле передачи информации по установленным виртуальным каналам.

При контроле квитирования связи шлюз сеансового уровня следит за установлением виртуального соединения между рабочей станцией внутренней сети и компьютером внешней сети, определяя, является ли запрашиваемый сеанс связи допустимым. Такой контроль основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP. Однако если пакетный фильтр при анализе TCP-заголовков проверяет только номера портов источника и получателя, то экранирующий транспорт анализирует другие поля, относящиеся к процессу квитирования связи.

Чтобы определить, является ли запрос на сеанс связи допустимым, шлюз сеансового уровня выполняет следующие действия. Когда рабочая станция (клиент) запрашивает связь с внешней сетью, шлюз принимает этот запрос, проверяя, удовлетворяет ли он базовым критериям фильтрации, например, может ли DNS-сервер определить IP-адрес клиента и ассоциированное с ним имя. Затем, действуя от имени клиента, шлюз устанавливает соединение с компьютером внешней сети и следит за выполнением процедуры квитирования связи по протоколу TCP.

8.6.8. Прикладной шлюз

Прикладной шлюз, называемый также экранирующим шлюзом, функционирует на прикладном уровне модели OSI, охватывая также уровень представления, и обеспечивает наиболее надежную защиту межсетевых взаимодействий. Защитные функции прикладного шлюза, как и экранирующего транспорта, относятся к функциям посредничества. Однако прикладной шлюз, в отличие от шлюза сеансового уровня, может выполнять существенно большее количество

функций защиты, к которым относятся следующие: идентификация и аутентификация пользователей при попытке установления соединений через брандмауэр; проверка подлинности информации, передаваемой через шлюз; разграничение доступа к ресурсам внутренней и внешней сетей; фильтрация и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации; регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов; кэширование данных, запрашиваемых из внешней сети.

Учитывая, что функции прикладного шлюза относятся к функциям посредничества, он представляет собой универсальный компьютер, на котором функционируют программные посредники (экранирующие агенты) – по одному для каждого обслуживаемого прикладного протокола (HTTP, FTP, SMTP, NNTP и др).

Посредник каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе. Так же как и шлюз сеансового уровня, прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию через шлюз и функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетью. Однако посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня. Во-первых, посредники прикладного шлюза связаны с конкретными приложениями (программными серверами), а во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели OSI.

Прикладные шлюзы используют в качестве посредников специально разработанные для этой цели программные серверы конкретных служб TCP/IP – серверы HTTP, FTP, SMTP, NNTP и др. Эти программные серверы функционируют на брандмауэре в резидентном режиме и реализуют функции защиты, относящиеся к соответствующим службам TCP/IP. Трафик UDP обслуживается специальным транслятором содержимого UDP-пакетов.

Как и в случае шлюза сеансового уровня, для связи между рабочей станцией внутренней сети и компьютером внешней сети соответствующий посредник прикладного шлюза образует два соединения: от рабочей станции до брандмауэра и от брандмауэра до места назначения. Но в отличие от канальных посредников, посредники прикладного шлюза пропускают только пакеты, сгенерированные теми приложениями, которые им поручено обслуживать. Например, программа-посредник службы HTTP может обрабатывать лишь трафик, генерируемый этой службой. Если в сети работает прикладной шлюз, то входящие и исходящие пакеты могут передаваться лишь для тех служб, для которых имеются соответствующие посредники. Так, если прикладной шлюз использует только программы-посредники HTTP, FTP и Telnet, то он будет обрабатывать лишь пакеты, относящиеся к этим службам, блокируя при этом пакеты всех остальных служб.

Фильтрация потоков сообщений реализуется прикладными шлюзами на прикладном уровне модели OSI. Соответственно, посредники прикладного шлюза, в отличие от канальных посредников, обеспечивают проверку содержимого обрабатываемых пакетов. Они могут фильтровать отдельные виды команд или информации в сообщениях протоколов прикладного уровня, которые им поручено обслуживать. Например, для службы FTP возможно динамическое обезвреживание компьютерных вирусов в копируемых из внешней сети файлах. Кроме того, посредник данной службы может быть сконфигурирован таким образом, чтобы предотвращать использование клиентами команды PUT, предназначенной для записи файлов на FTP-сервер. Такое ограничение уменьшает риск случайного повреждения хранящейся на FTP-сервере информации и снижает вероятность заполнения его гигабайтами ненужных данных.

При настройке прикладного шлюза и описании правил фильтрации сообщений используются такие параметры, как название сервиса, допустимый временной диапазон его использования, ограничения на содержимое сообщений, свя-

занных с данным сервисом, компьютеры, с которых можно пользоваться сервисом, идентификаторы пользователей, схемы аутентификации и др.

8.7. Контрольные вопросы

1. Какие основные положения избирательного и полномочного управления доступом?

2. В чем заключается сущность управления информационными потоками?

3. Охарактеризуйте функции ядра безопасности.

4. Каким образом реализуется контроль доступа субъектов к совместно используемым объектам?

5. Дайте краткую характеристику формам представления матрицы доступа.

6. Дайте краткую характеристику принципам реализации политики безопасности.

7. Какие существуют типы мошенничества в электронной коммерции?

8. Какие режимы аутентификации поддерживает протокол SSL?

9. Каким образом вырабатываются сеансовые ключи шифрования при использовании протокола SSL?

10. Какие функции выполняет протокол SET на базовом уровне?

11. Сравните достоинства и недостатки протоколов SSL и SET?

12. Дайте краткую характеристику этапам атаки на компьютерную сеть.

13. В чем сущность обнаружения атак?

14. Какие способы обнаружения атак вы знаете и в чем их сущность?

15. Какие функции может выполнять межсетевой экран?

16. Дайте краткую характеристику применению межсетевого экранирования для различных уровней модели OSI.

ЛИТЕРАТУРА

1. Бузов, Г. А. Защита от утечки информации по техническим каналам : учеб. пособие для подготовки экспертов системы Гостехкомиссии России / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия – Телеком, 2005. – 416 с.

2. Торокин, А. А. Инженерно-техническая защита информации / А. А. Торокин. – М. : Гелиос АРВ, 2005. – 960 с.

3. Магауенов, Р. Г. Системы охранной сигнализации: основы теории и принципы построения : учеб. пособие / Р. Г. Магауенов. – М. : Горячая линия – Телеком, 2004. – 367 с.

4. Гедзберг, Ю. Охранное телевидение / Ю. Гедзберг. – М. : Горячая Линия – Телеком, 2006. – 312 с.

5. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. – М. : ДМК, 2000. – 448 с.

6. Голдовский, И. Безопасность платежей в Интернете / И. Голдовский. – СПб. : Питер, 2001. – 240 с.

7. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В. Ф. Шаньгин. – М. : ИД «Форум»: Инфра-М, 2011. – 416 с.

Св. план 2011, поз. 93

Учебное издание

Лыньков Леонид Михайлович
Голиков Владимир Федорович
Борботько Тимофей Валентинович

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ И УПРАВЛЕНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТЬЮ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редакторы *И. П. Острикова*, *Е. С. Чайковская*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *В. М. Задоля*

Подписано в печать 25.03.2013. Формат 60x84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 14,3. Уч.-изд. л. 14,0. Тираж 150 экз. Заказ 365.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6