Министерство образования Республики Беларусь

Учреждение образования
"Белорусский государственный университет информатики
и радиоэлектроники"

Кафедра сетей и устройств телекоммуникаций

ПРАВОВЫЕ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие по курсам
"Телекоммуникационные системы в банковских технологиях",
"Основы защиты информации",
"Защита объектов связи от несанкционированного доступа"
для студентов специальности
"Телекоммуникационные системы"
дневной формы обучения

Минск 2004

УДК 621.398.25 (075.8)
ББК 32.811 я 73
П 68

Рецензент:
доцент Высшего государственного колледжа связи, канд. техн. наук В.В. Соловьев

Авторы:
В.Ф. Голиков, Л.М. Лыньков, А.М. Прудник, Т.В. Борботько

Правовые и организационно-технические методы защиты информации: Учеб. пособие по курсам "Телекоммуникационные системы в банковских технологиях", "Основы защиты информации", "Защита объектов связи от несанкционированного доступа" для студ. спец. "Телекоммуникационные системы" дневной формы обучения / В.Ф. Голиков, Л.М. Лыньков, А.М. Прудник, Т.В. Борботько. — Мн.: БГУИР, 2004. — 81 с.: ил.

ISBN 985-444-621-2

В учебном пособии рассмотрены основные правовые и нормативные документы и разъяснены основные организационные методы защиты информации. Приводится описание технических каналов утечки информации и организационно-технического комплекса мер по предотвращению утечки информации посредством данных каналов.

Данное учебное пособие предназначено для студентов высших учебных заведений, обучающихся по специальности "Телекоммуникационные системы".

УДК 621.398.25 (075.8)
ББК 32.811 я 73

ISBN 985-444-621-2

СОДЕРЖАНИЕ

1. ОСНОВНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

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 технологическим признакам. 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 изменили облик материального производства, позволили экономить материальные ресурсы, создали новые приборы и системы, в буквальном смысле изменили 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.

1.1. Основные понятия и терминология

Рассмотрим основные понятия и термины науки о защите информации.

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

Информация может существовать в виде бумажного документа, физических полей и сигналов (электромагнитных, акустических, тепловых и т.д.), биологических полей (память человека). В дальнейшем будем рассматривать информацию в документированной (на бумаге, дискете и т. д.) форме и в форме физических полей (радиосигналы, акустические сигналы). Среду, в которой информация создается, передается, обрабатывается или хранится, будем называть **информационным объектом**.

Под **безопасностью информационного объекта** понимается его защищенность от случайного или преднамеренного вмешательства в нормальный процесс его функционирования.

Природа воздействия на информационный объект может быть двух видов:

— непреднамеренной (стихийные бедствия, отказы оборудования, ошибки персонала и т.д.);

— преднамеренной (действия злоумышленников).

Все воздействия могут привести к последствиям (ущербу) трех видов: нарушению конфиденциальности, целостности, доступности.

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

Нарушение целостности — несанкционированное изменение, искажение, уничтожение информации.

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

В отличие от разрешенного (санкционированного) доступа к информации в результате преднамеренных действий злоумышленник получает несанкционированный доступ. Суть несанкционированного доступа состоит в получении нарушителем доступа к объекту в нарушение 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 информационного объекта является противодействие угрозам безопасности.

Защищенный информационный объект — это объект со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Комплексная защита информационного объекта (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.

1.2. Классификация угроз

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

К настоящему времени известно большое количество угроз. Приведем их классификацию:

По виду:

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

— конфиденциальности (несанкционированное получение);

— доступности (работоспособности);

— права 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, ошибками персонала. Методы оценки воздействия этих угроз рассматриваются в других дисциплинах (теории надежности, программировании, инженерной психологии и т. д.).

Преднамеренные угрозы связаны с действиями людей (работники спецслужб, самого объекта, хакеры). Огромное количество разнообразных информационных объектов 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,

или нештатными каналами доступа:

— 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 выполнение законов, и собственниками информации. К таким мерам относятся издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и 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 необходимы 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.

Принципиальным вопросом при определении уровня защищенности объекта является выбор критериев. Рассмотрим один из них - широко известный критерий "эффективность - стоимость".

Пусть имеется информационный объект, который при нормальном (идеальном) функционировании создает положительный эффект (экономический, политический, технический и т.д.). Этот эффект обозначим через E_0. Несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования (нарушается нормальная работа, наносится ущерб из-за утечки информации и т.д.) на величину ΔE. Тогда эффективность функционирования объекта с учетом воздействия несанкционированного доступа

$$E = E_0 - \Delta E. \qquad (1)$$

Относительная эффективность

$$\delta = \frac{E}{E_0} = \frac{E_0 - \Delta E}{E_0} = 1 - \frac{\Delta E}{E_0}. \qquad (2)$$

Уменьшение эффективности функционирования объекта приводит к материальному ущербу для владельца объекта. В общем случае материальный ущерб есть некоторая неубывающая функция от ΔE:

$$U = f(\Delta E). \qquad (3)$$

Будем считать, что установка на объект средств защиты информации уменьшает негативное действие несанкционированного доступа на эффективность функционирования объекта. Обозначим снижение эффективности функционирования объекта при наличии средств защиты через ΔE_3, а коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объект - через К, тогда

$$\Delta E_3 = \frac{\Delta E}{K}, \qquad (4)$$

где $K \geq 1$.

А выражения (1) – (2) примут вид

$$E_З = E_0 - \Delta E_З = E_0 - \frac{\Delta E}{K}, \tag{5}$$

$$\delta_З = \frac{E_З}{E_0} = \frac{E_0 - \Delta E_З}{E_0} = 1 - \frac{\Delta E_З}{E_0} = 1 - \frac{\Delta E}{K E_0}. \tag{6}$$

Стоимость средств защиты зависит от их эффективности, и в общем случае К — есть возрастающая функция от стоимости средств защиты:

$$K = f(C). \tag{7}$$

Поскольку затраты на установку средств защиты можно рассматривать как ущерб владельцу объекта от возможности осуществления несанкционированного доступа, то суммарный ущерб объекту:

$$U_\Sigma = \frac{U}{K} + C = \frac{U}{f(C)} + C. \tag{8}$$

Если эффективность функционирования объекта имеет стоимостное выражение (доход, прибыль и т.д.), то U_Σ непосредственно изменяет эффективность:

$$E_З = E_0 - \frac{\Delta E}{K - C} \tag{9}$$

Таким образом, классическая постановка задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа имеет вид

$$\begin{array}{l} U_\Sigma \to \min \\ C = C_{опт} \end{array}, \tag{10}$$

или

$$\begin{array}{ll} E_З \to \max, & \delta_З \to \max, \\ C = C_{опт} & C = C_{опт}. \end{array} \tag{11}$$

Несмотря на кажущуюся простоту классической постановки задачи, на практике воспользоваться приведенными результатами удается редко. Это объясняется отсутствием зависимостей K = f(C) и особенно ущерба от несанкционированного доступа. И если зависимость коэффициента защищенности от стоимости средств защиты можно получить, имея технические и стоимостные характеристики доступных средств защиты, то оценить реальный ущерб от несанкционированного доступа чрезвычайно трудно, так как этот ущерб зависит от множества трудно прогнозируемых факторов: наличия физических каналов несанкционированного доступа, квалификации злоумышленников, их интереса к объекту, последствий несанкционированного доступа и т.д.

Вместе с тем для объектов, на которые возлагаются ответственные задачи и для которых несанкционированный доступ влечет катастрофические потери эффективности их функционирования, влиянием стоимости средств защиты на эффективность можно пренебречь, т.е. если

$$C << U, \tag{12}$$

то

$$U_{\Sigma} = \frac{U}{f(C)}. \tag{13}$$

В этом случае (11) и (12) принимают вид:

$$\begin{gathered} U_{\Sigma} \to \min, \\ C \le C_{\text{доп}} \end{gathered} \tag{14}$$

или

$$\begin{gathered} E_{\text{з}} \to \max, \qquad \delta_{\text{з}} \to \max, \\ C \le C_{\text{доп}}, \qquad C \le C_{\text{доп}}, \end{gathered} \tag{15}$$

где $C_{\text{доп}}$ — допустимые расходы на защиту.

2. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Основные нормативные документы

Программно-технические методы защиты информации, какими бы совершенными они ни были, в полном объеме не решают задач комплексной защиты объектов информационной безопасности. Используемые при этом физические, аппаратные, программные, криптографические и иные логические и технические средства и методы защиты выполняются без участия человека по заранее предусмотренной процедуре. Для обеспечения комплексного подхода к обеспечению защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение.

Основные правовые акты, регламентирующие защиту информации в Республике Беларусь:

Закон РБ от 6 сентября 1995 г. № 3850-XII "*Об информатизации*",

Закон РБ от 29 ноября 1994 г. № 3411-XII "*О государственных секретах*",

Закон РБ от 3 декабря 1997 г. № 102-З "*Об органах государственной безопасности Республики Беларусь*",

Постановление Совета Министров РБ от 15 февраля 1999 г. № 237 "*О служебной информации ограниченного распространения*",

Постановление Совета Министров РБ от 10 февраля 2000 г. № 186 "*О некоторых мерах по защите информации в Республике Беларусь*".

Закон "Об информатизации"

Закон "Об информатизации" регулирует правоотношения, возникающие в процессе формирования и использования документированной информации информационных ресурсов; создания информационных технологий, автоматизированных или автоматических информационных систем и сетей; определяет порядок защиты информационного ресурса, а также прав и обязанностей субъектов, принимающих участие в процессах информатизации.

Действие настоящего Закона не распространяется на отношения, возникающие при создании и функционировании печати и иных средств массовой информации, и на отношения по обработке недокументированной информации.

Термины, используемые в Законе "Об информатизации", и их определения:

информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах;

документированная информация (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

материальный носитель информации — материал с определенными физическими свойствами, который может быть использован для записи и хранения информации;

информационные процессы — процессы сбора, обработки, накопления, хранения, актуализации и предоставления документированной информации пользователю;

информационный ресурс — организованная совокупность документированной информации, включающая базы данных и знаний, другие массивы информации в информационных системах;

информационная технология — совокупность методов, способов, приемов и средств обработки документированной информации, включая прикладные программные средства, и регламентированного порядка их применения;

автоматизированная или автоматическая информационная система — совокупность информационных ресурсов, информационных технологий и комплекса программно-технических средств, осуществляющих информационные процессы в человеко-машинном или автоматическом режиме;

комплекс программно-технических средств — совокупность общесистемных программных и технических средств, обеспечивающих реализацию информационных процессов;

информационная сеть — комплекс программно-технических средств для передачи и обработки данных по каналам связи;

информационная продукция — материализованный результат информационных процессов, предназначенный для обеспечения информационных потребностей органов государственной власти, юридических и физических лиц;

информационные услуги — информационная деятельность по доведению до пользователя информационной продукции, проводимая в определенной форме;

данные — документированная информация, циркулирующая в процессе ее обработки на электронно-вычислительных машинах;

база данных — совокупность взаимосвязанных данных, организованных по определенным правилам на машинных носителях;

банк данных — организационно-техническая система, включающая одну или несколько баз данных и систему управления ими;

база знаний — совокупность формализованных знаний об определенной предметной области, представленных в виде фактов и правил;

собственник информационных ресурсов, информационных систем, технологий, средств их обеспечения — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;

владелец информационных ресурсов, информационных систем, технологий, средств их обеспечения — субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия, распоряжения в пределах, установленных законом;

пользователь (потребитель) информации — субъект, обращающийся к информационной системе или посреднику за получением необходимой документированной информации.

Ниже приведен ряд наиболее важных глав и статей, которые содержатся в рассматриваемом законе.

Статья 19. Режим доступа к информационным ресурсам

Органы государственной власти, юридические и физические лица имеют равные права на доступ к информационным ресурсам. Исключение составляют случаи, когда запрашиваемые сведения касаются документированной информации ограниченного доступа.

Отнесение информации к документированной информации ограниченного доступа, порядок ее накопления, обработки, охраны и доступа к ней определяются уполномоченными государственными органами при сохранении условий, устанавливаемых законодательством Республики Беларусь.

Защита информационных ресурсов и прав субъектов информатизации

Статья 2. Цели защиты

Целями защиты являются:

предотвращение утечки, хищения, утраты, искажения, подделки, несанкционированных действий по уничтожению, модификации, копированию, бло-

кированию документированной информации и иных форм незаконного вмешательства в информационные системы;

сохранение полноты, точности, целостности документированной информации, возможности управления процессом обработки и пользования в соответствии с условиями, установленными собственником этой информации или уполномоченным им лицом;

обеспечение прав физических и юридических лиц на сохранение конфиденциальности документированной информации о них, накапливаемой в информационных системах;

защита прав субъектов в сфере информатизации;

сохранение секретности, конфиденциальности документированной информации в соответствии с правилами, определенными настоящим Законом и иными законодательными актами.

Статья 23. Права и обязанности субъектов по защите информационных ресурсов

Собственник информационной системы или уполномоченные им лица обязаны обеспечить уровень защиты документированной информации в соответствии с требованиями настоящего Закона и иных актов законодательства.

Информационные ресурсы, имеющие государственное значение, должны обрабатываться только в системах, обеспеченных защитой, необходимый уровень которой подтвержден сертификатом соответствия.

Защита другой документированной информации устанавливается в порядке, предусмотренном ее собственником или собственником информационной системы.

Собственник или владелец информационной системы обязан сообщать собственнику информационных ресурсов обо всех фактах нарушения защиты информации.

Статья 24. Сертификация технических и программных средств по защите информационных ресурсов

Технические и программные средства по защите информационных ресурсов подлежат обязательной сертификации в национальной системе сертификации Республики Беларусь органом сертификации.

Юридические лица, занимающиеся созданием средств по защите информационных ресурсов, осуществляют свою деятельность в этой сфере на основании разрешения органа, уполномоченного Президентом Республики Беларусь.

Статья 25. Предупреждение правонарушений в сфере информатизации

Предупреждение действий, влекущих за собой нарушение прав и интересов субъектов правоотношений в сфере информатизации, установленных настоящим Законом и иным законодательством Республики Беларусь, осуществляется органами государственной власти и управления, юридическими и физическими лицами, принимающими участие в информационном процессе.

Владельцы информационных ресурсов и систем, создатели средств программно-технической и криптографической защиты документированной информации при решении вопросов защиты руководствуются настоящим Законом и нормативными актами специально уполномоченного государственного органа по защите информации.

Закон "О государственных секретах"

Гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации по всем вопросам жизнедеятельности государства и общества. Наряду с этим требуется ограничение распространения определенных сведений, относящихся к обеспечению национальных интересов государства и общества, их безопасности и обороноспособности, преждевременное предание гласности которых может нанести ущерб Республике Беларусь.

Конституционное право граждан на получение, хранение и распространение информации может быть ограничено только законом.

Настоящий Закон определяет правовые основы отнесения сведений к государственным секретам и устанавливает единую систему защиты государственных секретов во всех видах деятельности органов законодательной, исполнительной и судебной власти, органов местного управления и самоуправления, органов государственного контроля и надзора, юридических лиц независимо от форм собственности, а также физических лиц на всей территории Республики Беларусь и в ее учреждениях за рубежом.

Основные понятия, применяемые в законе:

Государственные секреты — защищаемые государством сведения, распространение которых может нанести ущерб национальной безопасности, обороноспособности и жизненно важным интересам Республики Беларусь. Государственные секреты являются собственностью Республики Беларусь.

Защита государственных секретов — принятие предусмотренных настоящим Законом и подзаконными актами правовых, организационных, инже-

нерно-технических и иных мер по ограничению распространения сведений, отнесенных в установленном порядке к государственным секретам. Защита государственных секретов - обязанность всех органов законодательной, исполнительной и судебной власти, органов местного управления и самоуправления, органов государственного контроля и надзора, юридических лиц независимо от форм собственности, а также физических лиц, имеющих их.

Разглашение государственных секретов — передача, предоставление, пересылка, утрата носителей секретной информации, а также сообщение, публикация и доведение государственных секретов любыми другими способами до юридических и физических лиц, которым не предоставлено **право ознакомления с ними**.

Утрата государственных секретов — выход сведений, составляющих государственные секреты, из законного владения или пользования в результате утери либо хищения.

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.

Категории государственных секретов

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 либо 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.

Тяжесть последствий и размеры ущерба определяются в порядке, установленном настоящим Законом.

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".

Присвоение указанным носителям государственных секретов других ограничительных грифов, не предусмотренных настоящей статьей, запрещается.

Закон "Об органах государственной безопасности Республики Беларусь"

Настоящий Закон определяет правовые основы, принципы, основные задачи и направления деятельности органов государственной безопасности Республики Беларусь:

Организация и обеспечение криптографической и инженерно-технической безопасности шифрованной, засекреченной и кодированной связи в Республике Беларусь и ее учреждениях за рубежом, осуществление государственного контроля за этой деятельностью;

Обеспечение государственных органов, предприятий, учреждений и организаций правительственной и оперативной связью, а также организация и обеспечение криптографической и инженерно-технической безопасности шифрованной, засекреченной и кодированной связи в Республике Беларусь и ее учреждениях за рубежом, осуществление государственного контроля за этой деятельностью.

Правительственная и оперативная связь

Правительственная (телефонная и документальная) и оперативная (телефонная) связь являются специальными системами электрической связи, обеспечивающими секретность передаваемой по ним информации.

Правительственная связь организуется в интересах государственных органов.

Оперативная связь организуется в интересах правоохранительных органов.

Подразделения правительственной связи органов государственной безопасности обеспечивают государственные органы, предприятия, учреждения и организации правительственной и оперативной связью, а также организуют деятельность республиканских органов государственного управления, предприятий, учреждений и организаций по обеспечению криптографической и инженерно-технической безопасности шифрованной, засекреченной и кодированной связи в Республике Беларусь и ее учреждениях за рубежом, осуществляют государственный контроль за этой деятельностью. Они должны:

Осуществлять контроль в пределах своей компетенции за использованием на территории Республики Беларусь излучающих радиоэлектронных средств любого назначения и запрещать использование этих средств, работающих с нарушением установленных правил обращения с информацией, составляющей государственную тайну, либо создающих радиопомехи функционированию средств правительственной и оперативной радиосвязи;

Осуществлять государственный контроль за состоянием криптографической и инженерно-технической безопасности шифрованной, засекреченной и кодированной связи в государственных органах, на предприятиях, в учреждениях и организациях независимо от их ведомственной принадлежности, а также секретно-шифровальной работы в учреждениях Республики Беларусь, находящихся за рубежом.

Постановление Совета Министров "О служебной информации ограниченного распространения"

Служебная информация ограниченного распространения - сведения, распространение которых в соответствии с действующим законодательством РБ организации считают нежелательными в интересах своей деятельности.

На документах, содержащих такую информацию, проставляется гриф "Для служебного пользования".

В постановлении приводится перечень сведений ограниченного распространения:

— мобилизационные вопросы;

— наука и техника;

— оборона и государственная безопасность;

— правоохранительная деятельность.

Постановление Совета Министров
"О некоторых мерах по защите информации в Республике Беларусь"

Установить, что при обработке информации, отнесенной к госсекретам и служебной информации ограниченного распространения с использованием средств электронно-вычислительной техники, должны применяться защищенные по требованиям безопасности информации компьютерные системы, изготавливаемые, как правило, на предприятиях РБ. В обоснованных случаях могут применяться компьютерные системы импортного производства, прошедшие специальные исследования и обеспеченные защитой, необходимый уровень которой подтвержден сертификатом соответствия.

2.2. Правовая защита от компьютерных преступлений

В 1983 г. Международная организация экономического сотрудничества и развития определила под термином *"компьютерная преступность"* (или "связанная с компьютерами преступность") любые незаконные, неэтичные или неправомерные действия, связанные с автоматической обработкой данных и/или их передачей.

Данный термин, возникший первоначально как средство для обозначения появившихся новых способов совершения преступлений, по своему содержанию давно уже перерос в криминологическое понятие, обозначающее самостоятельный вид преступности. В настоящее время этот вид преступности включает в себя в зависимости от уголовно-правового регулирования в тех или иных странах уже целый перечень такого рода деяний и способов их совершения.

С целью унификации национальных законодательств в 1989 г. Комитетом министров Европейского Совета был согласован и утвержден Список правонарушений, рекомендованный странам - участницам ЕС для разработки единой уголовной стратегии по разработке законодательства, связанного с компьютерными преступлениями. Рекомендованный Европейским Советом Список компьютерных преступлений включает в себя так называемые “Минимальный” и “Необязательный списки нарушений”.

"Минимальный список нарушений" содержит следующие восемь видов компьютерных преступлений:

1. Компьютерное мошенничество.

Ввод, изменение, стирание или повреждение данных ЭВМ или программ ЭВМ, или же другое вмешательство в ход обработки данных, которое влияет на результат обработки данных таким образом, что служит причиной экономических потерь или вызывает состояние потери имущества другого человека с намерением незаконного улучшения экономического положения для себя или другого человека (или как альтернатива с намерением к незаконному лишению этого человека его имущества).

2. Подделка компьютерной информации.

Несанкционированное стирание, повреждение, ухудшение или подавление данных ЭВМ или программ ЭВМ, или другое вмешательство в ход обработки данных различными способами, или создание таких условий, которые будут, согласно национальному законодательству, составлять такое правонарушение, как подделка в традиционном смысле такого нарушения.

3. Повреждение данных ЭВМ или программ ЭВМ.

Несанкционированное стирание, повреждение, ухудшение или подавление данных ЭВМ или программ ЭВМ.

4. Компьютерный саботаж.

Ввод, изменение, стирание, повреждение данных ЭВМ или программ ЭВМ, или вмешательство в системы ЭВМ с намерением препятствовать функционированию компьютера или системы передачи данных.

5. Несанкционированный доступ.

Несанкционированный доступ к системе ЭВМ через сеть с нарушением средств защиты.

6. Несанкционированный перехват данных.

Несанкционированный перехват данных с помощью технических средств связи как в пределах компьютера, системы или сети, так и извне.

7. Несанкционированное использование защищенных компьютерных программ.

Незаконное воспроизведение, распространение программ или связь с программой ЭВМ, которая защищена в соответствии с законом.

8. Несанкционированное воспроизведение схем.

Несанкционированное воспроизведение схемных решений, защищенных в соответствии с законом о полупроводниковых изделиях (программах), или коммерческая эксплуатация или незаконное импортирование для той же цели схемы или полупроводникового изделия как продукта, произведенного с использованием данных схем.

"Необязательный список нарушений" включает в себя следующие четыре вида компьютерных преступлений:

Незаконное изменение данных ЭВМ или программ ЭВМ;

Компьютерный шпионаж;

Приобретение с использованием незаконных средств или путем несанкционированного раскрытия, пересылка или использование торговых или коммерческих секретов при помощи подобных методов или других незаконных средств с тем или иным намерением, наносящим экономический ущерб человеку путем доступа к его секретам или позволяющим получить незаконное экономическое преимущество для себя или другого человека;

Неразрешенное использование ЭВМ.

Использование системы ЭВМ или компьютерной сети без соответствующего разрешения является преступным, когда оно:

инкриминируется в условиях большого риска потерь, вызванных неизвестным лицом, использующим систему или наносящим вред системе или ее функционированию;

инкриминируется неизвестному лицу, имеющему намерение нанести ущерб и использующему для этого систему или наносящему вред системе или ее функционированию;

применяется в случае, когда теряется информация с помощью неизвестного автора, который использовал данную систему или нанес вред системе или ее функционированию.

Использование без разрешения защищенной программы ЭВМ или ее незаконное воспроизводство с намерением исправить программу таким образом, чтобы вызвать незаконную экономическую выгоду для себя или другого человека, или причинить вред законному владельцу данной программы, также является преступлением.

В 1995 г. рабочей группой Программного комитета СНГ был подготовлен модельный Уголовный кодекс для государств - участников СНГ, содержащий специальную главу "Преступления против информационной безопасности"", в которую были включены следующие составы компьютерных преступлений.

Статья 286. Несанкционированный доступ к компьютерной информации

1. Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся "нару-

шением системы защиты и повлекший по неосторожности изменение, уничтожение либо блокирование информации, а равно вывод из строя компьютерного оборудования либо иной значительный ущерб — преступление средней тяжести.

2. Действия, предусмотренные частью первой статьи, повлекшие по неосторожности тяжкие последствия, — преступление средней тяжести.

Статья 287. Модификация компьютерной информации

1. Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, а равно внесение в них заведомо ложной информации при отсутствии признаков хищения чужого имущества или причинения имущественного ущерба путем обмана или злоупотребления доверием, причинившее значительный ущерб или создавшее угрозу его причинения, — преступление небольшой тяжести.

2. То же действие:

а) сопряженное с несанкционированным доступом к компьютерной системе или сети — преступление средней тяжести;

б) повлекшее по неосторожности тяжкие последствия — преступление средней тяжести.

Статья 288. Компьютерный саботаж

1. Уничтожение, блокирование или приведение в непригодное состояние компьютерной информации или программы, вывод из строя компьютерного оборудования, а равно разрушение компьютерной системы, сети или машинного носителя - преступление средней тяжести.

2. То же действие:

а) сопряженное с несанкционированным доступом к компьютерной системе или сети - тяжкое преступление;

б) повлекшее умышленно или по неосторожности тяжкие последствия — тяжкое преступление.

Статья 289. Неправомерное завладение компьютерной информацией

Несанкционированное копирование или иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, а равно перехват информации, передаваемой с использованием средств компьютерной связи, — преступление небольшой тяжести.

Принуждение к передаче информации, хранящейся в компьютерной системе, сети или на машинных носителях, под угрозой оглашения позорящих све-

дений о лице или его близких, предания гласности сведений о таких обстоятельствах, которые потерпевший желает сохранить в тайне, а равно под угрозой применения насилия над лицом или его близкими либо под угрозой уничтожения либо повреждения имущества лица, его близких и других лиц, в ведении или под охраной которых находится эта информация, — преступление средней тяжести.

Действия, классифицируемые как тяжкое преступление, предусмотренные частями первой и второй настоящей статьи:

а) сопряженные с применением насилия над лицом или его близкими;

б) совершенные по предварительному сговору группой лиц;

в) причинившие значительный ущерб потерпевшему;

г) совершенные с целью получения особо ценной информации.

Действия, предусмотренные частями первой, второй или третьей настоящей статьи, классифицируемые как особо тяжкие преступления:

а) совершенные организованной группой;

б) совершенные с причинением тяжкого вреда здоровью или смерти либо иных тяжких последствий.

Статья 290. Изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Изготовление с целью сбыта, а равно сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети, — преступление небольшой тяжести.

Статья 291. Разработка, использование и распространение вредоносных программ

Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на иных носителях, а также разработка специальных вирусных программ, заведомое их использование или распространение носителей с такими программами — преступление средней тяжести.

То же деяние, повлекшее по неосторожности тяжкие последствия, — преступление средней тяжести.

Статья 292. Нарушение правил эксплуатации компьютерной системы или сети

Нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, если это повлекло по неосторожно-

сти уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования или причинение иного значительного ущерба — преступление небольшой тяжести.

То же деяние, совершенное при эксплуатации компьютерной системы или сети, содержащей информацию особой ценности, — преступление средней тяжести.

Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности тяжкие последствия, — преступление средней тяжести.

Некоторые из сформулированных в модельном Уголовном кодексе составов компьютерных преступлений нашли свое отражение в проектах Уголовных кодексов государств - участников СНГ. Так, в проект Уголовного кодекса Российской Федерации включена глава "Преступления против информационной безопасности", содержащая следующие составы преступлений.

Статья 62. Неправомерный доступ к компьютерной информации

Неправомерный доступ к информации в компьютерной системе или сети, а равно введение в компьютерную систему или сеть заведомо ложной информации - преступление небольшой тяжести.

Те же деяния, классифицируемые как преступление небольшой тяжести:

а) повлекшие модификацию, уничтожение, блокирование или копирование информации либо вывод из строя компьютерного оборудования;

б) совершенные группой лиц по предварительному сговору или организованной группой;

в) совершенные лицом, имеющим допуск к компьютерной системе или сети.

Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные в отношении информации ограниченного доступа, находящейся на машинном носителе, в компьютере, компьютерной системе или сети, а равно повлекшие тяжкие последствия, — преступления средней тяжести.

Статья 63. Создание, использование и распространение вирусных программ

Создание компьютерных программ или внесение изменений в существующие компьютерные программы, приводящих к несанкционированному уничтожению, блокированию, модификации, копированию информации или нарушению работы компьютерного оборудования, а равно использование либо распространение носителей с такими программами — преступление небольшой тяжести.

Те же деяния, повлекшие тяжкие последствия, — преступления средней тяжести.

Статья 64. Нарушение правил эксплуатации компьютерной системы или сети

Нарушение правил эксплуатации компьютерной системы или сети лицами, имеющими доступ к этой системе или сети, если это повлекло уничтожение, блокирование, модификацию компьютерной информации или нарушение работы компьютерного оборудования, — преступление небольшой тяжести.

То же деяние, классифицируемое как преступление средней тяжести:

а) повлекшее тяжкие последствия;

б) совершенное группой лиц по предварительному сговору или организованной группой;

в) совершенное в отношении компьютерной системы или сети, содержащей информацию ограниченного доступа.

Наличие в законодательстве специальных норм, сформулированных законодателем как формальные составы преступлений, позволяет применять уголовную ответственность вне зависимости от того, какую цель преследовал преступник и наступили ли определенные общественно опасные последствия. При этом правоохранительные органы освобождаются от обязанности доказывать корыстную цель или намерение причинить ущерб, так как часто будучи "схваченным за руку", нарушитель ссылается, как правило, на то, что осуществил несанкционированный доступ не с целью совершить кражу или нанести материальный ущерб, а просто для того, чтобы попробовать свои силы.

В новом Уголовном кодексе Республики Беларусь, принятом в 1999 году, в раздел XII "Преступления против информационной безопасности" включена глава 31 "Преступления против информационной безопасности", которая содержит следующие составы компьютерных преступлений.

Статья 349. Несанкционированный доступ к компьютерной информации

Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты и повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, — наказывается штрафом или арестом на срок до шести месяцев.

То же действие, совершенное из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети, — наказывается штрафом или

лишением права занимать определенные должности, или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

Несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи, компьютеризованной системы, компьютерной сети, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, — наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

Статья 350. Модификации компьютерной информации

Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации) — наказываются штрафом или лишением права занимать определенные должности, или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

Модификация компьютерной информации, сопряженная с несанкционированным доступом к компьютерной системе или сети либо повлекшая по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса, — наказывается ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 351. Компьютерный саботаж

Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж) — наказываются штрафом или лишением права занимать определенные должности, или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет.

Компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия, наказывается лишением свободы на срок от трех до десяти лет.

Статья 352. Неправомерное завладение компьютерной информацией

Несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда, наказываются общественными работами или штрафом, или арестом на срок до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети — наказываются штрафом или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет.

Статья 354. Разработка, использование либо распространение вредоносных программ

Разработка компьютерных программ или внесение изменения в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами — наказываются штрафом или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

Те же действия, повлекшие тяжкие последствия, — наказываются лишением свободы на срок от трех до десяти лет.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда, — наказывается штрафом или лишением права зани-

мать определенные должности, или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.

То же деяние, совершенное при эксплуатации компьютерной системы или сети, содержащей информацию особой ценности, — наказывается лишением права занимать определенные должности или заниматься определенной деятельностью, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

Деяния, предусмотренные частями первой или второй настоящей статьи и повлекшие по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса, — наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности, или заниматься определенной деятельностью или без лишения.

В раздел VIII нового Уголовного кодекса Республики Беларусь включена глава 24 "Преступления против собственности", которая содержит следующие составы компьютерных преступлений.

Статья 212. Хищение путем использования компьютерной техники

Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации наказывается штрафом или лишением права занимать определенные должности, или заниматься определенной деятельностью, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

То же деяние, совершенное повторно, либо группой лиц по предварительному сговору, либо сопряженное с несанкционированным доступом к компьютерной информации, — наказывается ограничением свободы на срок от двух до пяти лет или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью, или без лишения.

Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные в крупном размере, наказываются лишением свободы на срок от пяти до десяти лет с конфискацией имущества или без конфискации и с лишением права нанимать определенные должности или заниматься определенной деятельностью, или без лишения

Деяния, предусмотренные частями первой, второй и третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, — наказываются лишением свободы на срок от шести до пятнадцати лет с конфискацией имущества, с лишением прав занимать определенные должности или заниматься определенной деятельностью, или без лишения.

Статья 216. Причинение имущественного ущерба без признаков хищения

Причинение ущерба в значительном размере посредством извлечения имущественных выгод в результате обмана, злоупотребления доверием или путем модификации компьютерной информации при отсутствии признаков хищения наказывается штрафом или исправительными работами на срок до двух лет или арестом на срок до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью, или без лишения.

3. ГОСУДАРСТВЕННОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Государственное регулирование в области защиты информации

Государство занимает важное место в системе защиты информации в любой стране, в том числе и в Беларуси. Государственная политика обеспечения информационной безопасности исходит из следующих положений:

ограничение доступа к информации есть исключение из общего принципа открытости информации и осуществляется только на основе законодательства;

доступ к какой-либо информации, а также вводимые ограничения доступа осуществляются с учетом определяемых законом прав собственности на эту информацию;

юридические и физические лица, собирающие, накапливающие и обрабатывающие персональные данные и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;

государство формирует национальную программу информационной безопасности и объединяет усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности страны;

государство формирует нормативно-правовую базу, регламентирующую права, обязанности и ответственность всех субъектов, действующих в информационной сфере;

государство осуществляет контроль за созданием и использованием средств защиты информации посредством их обязательной сертификации и лицензирования деятельности в области защиты информации;

государство прилагает усилия для противодействия информационной экспансии США и других развитых стран, поддерживает интернационализацию глобальных информационных сетей и систем;

государство проводит протекционистскую политику, поддерживающую деятельность отечественных производителей средств информатизации и защиты информации, и осуществляет меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов.

Система информационной безопасности является составной частью общей системы национальной безопасности страны и представляет собой совокупность органов государственной власти и управления и предприятий, согла-

сованно осуществляющих деятельность по обеспечению информационной безопасности. 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:

Государственный центр безопасности информации (ГЦБИ);

структурные подразделения по защите информации органов государственного управления, предприятий, организация 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 последовательности 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.

Мероприятия по защите информации осуществляются как за счет бюджетных ассигнований, выделяемых целевым назначением, так и за счет средств предприятий, учреждений и организаций независимо от форм собственности. Финансирование НИОКР в области защиты информации, производства средств защиты информации и контроля эффективности защиты осуществляется за счет госбюджетных ассигнований, выделяемых целевым назначением гензаказчику, а также средств предприятий, учреждений и организаций различных форм собственности и частных лиц. Генеральным заказчиком технических, программных, программно-аппаратных и криптографических средств защиты информации, аппаратуры контроля эффективности защиты информации общего применения и научно-технической продукции по общесистемным исследованиям проблем защиты информации является ГЦБИ.

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 части 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.

3.2. Лицензирование деятельности юридических и физических лиц по защите информации

Деятельность юридических и физических лиц по защите информации лицензируется.

Положение о лицензировании в области защиты информации разработано Государственным центром безопасности информации при Совете Безопасности РБ. Эта же организация и выдает лицензии.

3.2.1. Основные виды лицензируемой деятельности, состав, содержание работ и применяемые термины

1. Под "техническими средствами защиты и контроля защищенности информации" понимаются:

защищенные от модификации, разрушения и утечки информации средства вычислительной техники, связи, хранения, отображения и размножения информации, подлежащей защите;

технические средства защиты информации общепромышленного исполнения и специального назначения;

инструментальные средства контроля защищенности информации.

2. К терминам "разработка, производство технических средств" относится цикл от исследований, согласно техническому заданию, до сдачи заказчику технического средства, изготовленного по конструкторской документации.

3. Термины "монтаж, наладка технических средств" включают установку, соединение (сборку) и приведение в рабочее состояние технических средств, устранение неисправностей в них.

4. К "специальным исследованиям технических средств" относится комплекс мероприятий по качественному и количественному исследованию воз-

можностей утечки информации по техническим каналам и выработке рекомендаций по ее защите.

5. Под "проведением работ по контролю защищенности информации" понимается: постоянное или периодическое проведение комплекса работ, обеспечивающих проверку выполнения организационных и технических мероприятий по защите информации, исключающих ее разрушение, искажение или утечку по техническим каналам.

6. К терминам "разработка, производство программных средств защиты информации" относятся: разработка и производство специальных программ, с помощью которых осуществляются разграничение доступа к информации и предупреждение от несанкционированного ее использования.

7. К терминам "разработка, производство программно-аппаратных средств защиты информации" относятся: разработка и производство средств, содержащих в своем составе элементы, реализующие функции защиты информации, в которых программные (микропрограммные) и аппаратные части полностью взаимозависимы и неразделимы.

8. Термины "монтаж, наладка программных средств защиты информации" включают в себя:

установку, приведение в рабочее состояние и сопровождение на объектах заказчика программных средств защиты информации;

внедрение программных средств контроля эффективности мер по защите информации;

установку антивирусных программ.

9. Под термином "средства криптографии, реализованные в программных и программно-аппаратных комплексах защиты информации" подразумеваются средства:

обеспечения подлинности данных (электронная цифровая подпись);

обеспечения целостности данных (код аутентификации сообщения, имитовставка, хеш-функция);

обеспечения конфиденциальности данных (шифрование);

управления ключевой системой (выполнение задач генерации, распределения, использования, хранения, уничтожения и восстановления ключей).

3.2.2. Основные требования к организациям, претендующим на получение лицензий на работы в области защиты информации

К организациям, претендующим на право получения лицензии на работы по защите информации, предъявляются требования по:

— уровню квалификации специалистов;

— наличию и качеству измерительной базы;

— наличию и качеству производственных помещений;

— наличию режимного органа и обеспечению охраны материальных ценностей и секретов заказчика (при необходимости);

— наличию нормативно-технической и методической документации в лицензируемой области деятельности.

Требования к помещениям, предназначенным для проведения измерений при специсследованиях, их техническая и технологическая оснащенность рассматриваются как совокупность требований к разработанной технологии проведения измерений, измерительной аппаратуре, стендам и т.п., а также к организации их содержания, обслуживания и поверки, выполнение которых позволяет организации, претендующей на проведение указанных в заявке работ, получить лицензию на право их проведения.

3.3. Сертификация и аттестация средств защиты объектов информации

В соответствии со статьей 24 Закона Республики Беларусь "Об информатизации" технические и программные средства защиты информационных ресурсов подлежат обязательной сертификации в национальной системе сертификации Республики Беларусь соответствующим органом по сертификации. Документами, регламентирующими вопросы сертификации в РБ, являются:

ГОСТ РБ "Национальная система сертификации Республики Беларусь";

СТБ 5.1.01-96 "Основные положения";

СТБ 5.1.02-96 "Общие требования и порядок аккредитации";

СТБ 5.1.03-96 "Органы по сертификации систем качества. Общие требования и порядок аккредитации";

СТБ 5.1.04-96 "Порядок проведения сертификации продукции. Общие требования";

СТБ 5.1.05-96 "Сертификация систем качества. Порядок проведения";

СТБ 5.1.06-96 "Положение об экспертах-аудиторах по качеству";

СТБ 5.1.07-96 "Реестр. Общие требования и порядок ведения".

Органом по сертификации средств защиты информации в республике является ГЦБИ.

К числу основных задач органа по сертификации средств защиты информации могут быть отнесены:

разработка нормативных документов на средства защиты и классификация их по функциональным свойствам;

разработка нормативных документов на методы испытаний средств защиты и их гармонизация с аналогичными документами зарубежных фирм и организаций;

выбор способов подтверждения соответствия средств защиты информации требованиям нормативных документов;

сертификация средств защиты информации и выдача сертификатов на их применение;

ведение реестра сертифицированных средств защиты информации;

инспекционный контроль за качеством продукции, которой присвоен тот или иной класс (уровень) защитных свойств;

приостановка или отмена действия выданных сертификатов.

Для интеграции систем защиты информации и удешевления их стоимости проектные решения по системам защиты информации должны быть стандартизированы в рамках международных организаций, отдельных государств, областей деятельности, конкретных организаций и фирм. Для решения этой задачи осуществляется гармонизация международных, национальных, отраслевых и фирменных нормативных документов по защите информации. Международной организацией по стандартизации - ИСО/МЭК разработаны стандарты, связанные с защитой информации. Основным нормативным документом-стандартом, определяющим структуру и функции систем защиты информации, является стандарт 180 7498-2 1989 "*Системы обработки информации. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты*". В этом документе рассмотрены вопросы терминологии по защите информации, приводится общее описание служб и механизмов защиты, уделено внимание проблемам взаимодействия служб, механизмов и уровней защиты, рассмотрены вопросы управления защитой при взаимодействии систем.

4. ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Организационно-административные методы защиты информации

Они регламентируют процессы создания и эксплуатации информационных объектов, а также взаимодействие пользователей и систем таким образом, чтобы несанкционированный доступ к информации становился либо невозможным, либо существенно затруднялся.

Организационно-административные методы защиты информации охватывают все компоненты автоматизированных информационных систем на всех этапах их жизненного цикла: проектирования систем, строительства зданий, помещений и сооружений, монтажа и наладки оборудования, эксплуатации и модернизации систем. К организационно-административным мероприятиям защиты информации относятся:

выделение специальных защищенных помещений для размещения ЭВМ и средств связи и хранения носителей информации;

выделение специальных ЭВМ для обработки конфиденциальной информации;

организация хранения конфиденциальной информации на специальных промаркированных магнитных носителях;

использование в работе с конфиденциальной информацией технических и программных средств, имеющих сертификат защищенности и установленных в аттестованных помещениях;

организация специального делопроизводства для конфиденциальной информации, устанавливающего порядок подготовки, использования, хранения, уничтожения и учета документированной информации;

организация регламентированного доступа пользователей к работе на ЭВМ, средствам связи и к хранилищам носителей конфиденциальной информации;

установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;

разработка и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфиденциальной информации, которые регламентируют деятельность всех звеньев объекта защиты в процессе обработки, хранения, передачи и использования информации;

постоянный контроль за соблюдением установленных требований по защите информации.

4.2. Организационно-технические методы защиты информации

Они охватывают все структурные элементы автоматизированных информационных систем на всех этапах их жизненного цикла. Организационно-техническая защита информации обеспечивается осуществлением следующих мероприятий:

ограничение доступа посторонних лиц внутрь корпуса оборудования за счет установки механических запорных устройств или замков;

отключение ЭВМ от локальной вычислительной сети или сети удаленного доступа (региональные и глобальные вычислительные сети) при обработке на ней конфиденциальной информации, кроме случаев передачи этой информации по каналам связи;

использование для отображения конфиденциальной информации жидкокристаллических, а для печати — струйных принтеров или термопечати с целью снижения утечки информации по электромагнитному каналу. При использовании обычных дисплеев и принтеров с этой же целью рекомендуется включать устройства, создающие дополнительный шумовой эффект (фон), — генераторы шума, кондиционер, вентилятор, или обрабатывать другую информацию на рядом стоящей ЭВМ;

установка клавиатуры и печатающих устройств на мягкие прокладки с целью снижения утечки информации по акустическому каналу;

размещение оборудования для обработки конфиденциальной информации на расстоянии не менее 2,5 м от устройств освещения, кондиционирования, связи, металлических труб, теле- и радиоаппаратуры;

организация электропитания ЭВМ от отдельного блока питания (с защитой от побочных электромагнитных излучений или от общей электросети через фильтр напряжения);

использование бесперебойных источников питания (БИП) персональных компьютеров для силовых электрических сетей с неустойчивым напряжением и плавающей частотой. Основное назначение бесперебойных источников питания — поддержание работы компьютера после исчезновения напряжения в электрической сети. Это обеспечивается за счет встроенных аккумуляторов, которые подзаряжаются во время нормальной работы. БИП мгновенно предупредит своего владельца об аварии электропитания и позволит ему в течение некоторо-

го времени (от нескольких минут до нескольких часов) аккуратно закрыть файлы и закончить работу. Кроме обычных для БИП функций они могут выполнять функцию высококлассного стабилизатора напряжения и электрического фильтра. Важной особенностью устройства является возможность непосредственной связи между ним и сетевой операционной системой.

4.3. Физические средства защиты информации

Физические средства защиты информации предназначены для внешней охраны территории объектов, защиты ЭВМ, систем и объектов на базе вычислительной техники. В настоящее время используются преимущественно чисто механические средства физической защиты при доминирующем участии человека. Однако достижения микроэлектроники и появление микропроцессоров создали объективную базу для разработки и внедрения наряду с традиционными механическими системами универсальных автоматизированных электронных систем физической защиты, предназначенных для охраны территории и помещений, организации пропускного режима и наблюдения, систем пожарной сигнализации, систем предотвращения хищения носителей. Элементную базу таких систем составляют различные датчики, сигналы которых обрабатываются микропроцессорами, электронные интеллектуальные ключи и замки на микропроцессорах, устройства определения биометрических характеристик человека и т.д. Современные физические средства защиты предоставляют широкие возможности для решения многих задач обеспечения информационной безопасности. Так, для организации охраны оборудования (узлов и блоков компьютеров, средств передачи данных) и перемещаемых носителей информации (дискеты, магнитные ленты, распечатки) можно использовать:

различные замки (механические, с кодовым набором, с управлением от микропроцессора, радиоуправляемые), которые устанавливают на входные двери, ставни, сейфы, шкафы, устройства и блоки системы;

микровыключатели, фиксирующие открывание или закрывание дверей и окон;

инерционные датчики, для подключения которых можно использовать осветительную сеть, телефонные провода и проводку ТВ-антенн;

специальные наклейки из фольги или другого магнитопроводного материала, которые наклеиваются на все документы, приборы, узлы и блоки системы для предотвращения их выноса из помещения. При этом около выхода из охраняемого помещения размещается специальная установка, принцип дейст-

вия которой аналогичен действию детектора металлических объектов. Эта установка подает сигнал тревоги при любой попытке вынести за пределы помещения предмет с наклейкой;

специальные сейфы и металлические шкафы для установки в них отдельных узлов и блоков компьютера для вычислительной системы (принтер, файл-сервер и т.п.) и перемещаемых носителей информации (магнитные ленты, диски, распечатки). Для нейтрализации утечки информации по электромагнитным каналам используют экранирующие и поглощающие материалы и изделия.

При этом:

экранирование рабочих помещений, где установлены системы электронной обработки и передачи данных, осуществляется путем покрытия стен, пола и потолка металлизированными обоями, токопроводящей эмалью и штукатуркой, проволочными сетками или фольгой, установки загородок из токопроводящего кирпича, многослойных стальных, алюминиевых или из специальной пластмассы листов;

для защиты окон применяют металлизированные шторы и стекла с токопроводящим слоем;

все отверстия закрывают металлической сеткой, соединяемой с шиной заземления или настенной экранировкой;

на вентиляционных каналах монтируют так называемые предельные магнитные ловушки, препятствующие распространению радиоволн. Для защиты от наводок на электрические цепи узлов и блоков автоматизированных систем обработки информации, а также на коммуникационные электрические цепи широко используют экранированный кабель для внутристоечного, внутриблочного, межблочного и наружного монтажа;

экранируют эластичные соединители (разъемы), всевозможные сетевые фильтры подавления электромагнитных излучений, провода, наконечники, дроссели, конденсаторы и другие помехоподавляющие радио- и электроизделия;

на водопроводных, отопительных, газовых и других металлических трубах помещают разделительные диэлектрические вставки, которые осуществляют разрыв электромагнитной цепи. Для контроля электропитания могут использоваться электронные отслеживающие устройства, которые устанавливаются в местах ввода сети переменного напряжения.

4.4. Страхование как метод защиты информации

Определение защитных свойств технических средств осуществляется путем непосредственных испытаний. Заключение (сертификат) банковского сертификационного центра должно явиться основой для системы страховых гарантий. Для предотвращения банковских информационных рисков необходимо страхование:

электронного документооборота при заключении и исполнении договоров с участием банков, при оформлении первичных платежных документов с применением цифровой (электронной) подписи;

от несанкционированного доступа в информационную сеть;

от разрушения или потери информации в результате программных или аппаратных сбоев;

от прямых убытков, связанных с незаконным использованием программных и аппаратных средств информационной системы;

от потерь рабочего времени и ухудшения качества обслуживания клиентов, вызванных поломками или некорректным функционированием аппаратных средств.

5. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

5.1. Источники образования технических каналов утечки информации

Физические преобразователи аудиоинформации — передатчики каналов утечки информации.

При разговоре, в беседе, на совещании каналами утечки информации могут быть акустический, виброакустический, гидроакустический и акустоэлектрический сигналы; при телефонном разговоре, дополнительно к предыдущему, — электросигнал в линии и различные наводки и влияния [1]; при радиотелефонном разговоре, дополнительно к предыдущему, - электромагнитный сигнал; в случае речевой почты добавляется акустический шум принтера (пишущей машинки).

Акустическая энергия, возникающая при разговоре, может вызвать акустические (т. е. механические) колебания элементов электронной аппаратуры, что в свою очередь приводит к появлению электромагнитного излучения или к его изменению при определенных обстоятельствах. Наиболее чувствительными элементами радиоэлектронной аппаратуры к акустическим воздействиям являются катушки индуктивности и конденсаторы переменной емкости.

Индуктивные и емкостные акустоэлектрические преобразователи

Если в поле постоянного магнита поместить катушку индуктивности (рамку) и вращать ее хотя бы под воздействием воздушного потока, то на ее выходе появится ЭДС индукции.

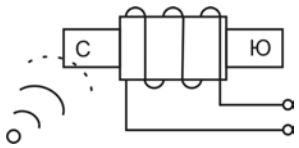

Рис. 1. Устройство электродинамического преобразователя

Воздушный поток переменной плотности возникает и при разговоре человека. Поэтому в соответствии с разговором (под воздействием его воздушного потока) будет вращаться катушка (рамка), что вызовет пропорционально изменяющуюся ЭДС индукции на ее концах. Таким образом можно связать акустическое воздействие на провод в магнитном поле с возникающей ЭДС индукции на его концах - это типичный пример из группы индукционных акусти-

ческих преобразователей. Представителем этой группы является, например, электродинамический преобразователь (рис. 1).

Рассмотрим акустическое воздействие на катушку индуктивности с сердечником. Механизм и условия возникновения ЭДС индукции в такой катушке сводятся к следующему. Под воздействием акустического давления появляется вибрация корпуса и обмотки катушки. Вибрация вызывает колебания проводов обмотки в магнитном поле, что и приводит к появлению ЭДС индукции на концах катушки:

$$E = -\frac{d}{dt}(\Phi_c + \Phi_в), \qquad (16)$$

где Φ_c — магнитный поток, замыкающийся через сердечник; $\Phi_в$ — магнитный поток, замыкающийся через обмотки по воздуху.

ЭДС зависит от вектора магнитной индукции, магнитной проницаемости сердечника, угла между вектором и осью катушки, угла между вектором и осью сердечника и площадей поперечных сечений сердечника и катушки. Индуктивные преобразователи подразделяются на электромагнитные, электродинамические и магнитострикционные. К электромагнитным преобразователям относятся такие устройства, как громкоговорители, электрические звонки (в том числе и вызывные звонки телефонных аппаратов), электрорадиоизмерительные приборы. Примером непосредственного использования этого эффекта для целей акустического преобразования является электродинамический микрофон (рис. 2).

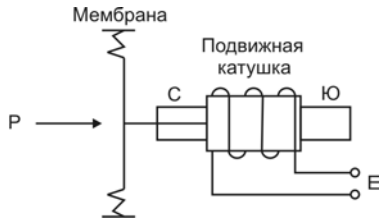

Рис. 2. Электродинамический микрофон

ЭДС на выходе катушки определяется по формуле

$$E = -L\frac{di}{dt}, \qquad (17)$$

где $L = 4k\pi\mu_0\omega^2 S/l$ — индуктивность; здесь k — коэффициент, зависящий от соотношения параметров; l — длина намотки катушки; μ_0 — магнитная прони-

цаемость; S — площадь поперечного сечения катушки; ω — число витков катушки.

Возникновение ЭДС на выходе такого преобразователя принято называть микрофонным эффектом. Можно утверждать, что микрофонный эффект может проявляться как в электродинамической, так и в электромагнитной, конденсаторной и других конструкциях, широко используемых в акустоэлектрических преобразователях самого различного назначения и исполнения.

Емкостные преобразователи

Емкостные преобразовывающие элементы превращают изменение емкости в изменение электрического потенциала, тока, напряжения.

Для простейшего конденсатора, состоящего из двух пластин, разделенных слоем диэлектрика (воздух, парафин и др.), емкость определяется по формуле

$$C = \varepsilon S / d, \qquad (18)$$

где ε — диэлектрическая проницаемость диэлектрика; S — площадь поверхности каждой пластины; d — расстояние между пластинами.

Из этого соотношения следует, что емкость конденсатора зависит от расстояния между пластинами. При наличии в цепи емкости постоянного источника тока и нагрузки воздействующее на пластины акустическое давление, изменяя расстояние между пластинами, приводит к изменению емкости. Изменение емкости приводит к изменению сопротивления цепи и соответственно, к падению напряжения на сопротивлении нагрузки пропорционально акустическому давлению. Эти зависимости используются в конструкции конденсаторных микрофонов. Принципиальная схема конденсаторного микрофона приведена на рис. 3.

Когда на микрофон действует волна звукового давления Р, диафрагма Д движется относительно неподвижного электрода — жесткой пластины П. Это движение вызывает переменное изменение электрической емкости между диафрагмой и задней пластиной, а следовательно, производит соответствующий электрический сигнал на выходе.

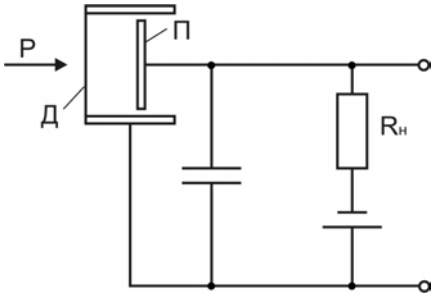

Рис. 3. Устройство конденсаторного микрофона

Конденсаторы переменной емкости с воздушным диэлектриком являются одним из основных элементов перестраиваемых колебательных контуров генераторных систем. Они устроены так, что одна система пластин вдвигается в другую систему пластин, образующих конденсатор переменной емкости. На такой конденсатор акустическое давление оказывается довольно просто, изменяя его емкость, а следовательно, и характеристики устройства, в котором он установлен, приводя к появлению неконтролируемого канала утечки информации.

Микрофонный эффект

Электромеханический вызывной звонок телефонного аппарата — типичный представитель индуктивного акустоэлектрического преобразователя, микрофонный эффект которого проявляется при положенной микротелефонной трубке. На рис. 4 приведена схема телефонного аппарата, а на рис. 5 — схема вызывного звонка.

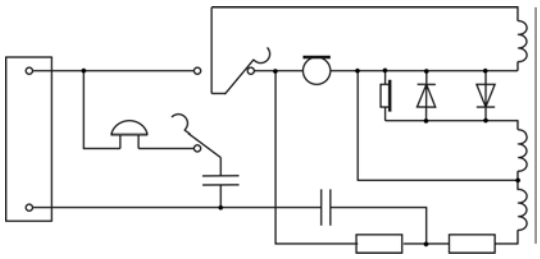

Рис. 4. Схема телефонного аппарата

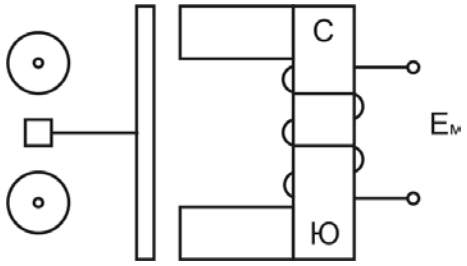

Рис. 5. Схема вызывного звонка

ЭДС микрофонного эффекта звонка может быть определена по формуле

$$E_{М.Э} = \eta p, \qquad (19)$$

где p — акустическое давление; $\eta = FS\mu_0\omega S_М / d^2 z_М$ — акустическая чувствительность звонка; здесь F — магнитодвижущая сила постоянного магнита; S — площадь якоря (пластины); μ_0 — магнитная проницаемость сердечника; ω — число витков катушки; $S_М$ — площадь плоского наконечника; d — значение зазора; $z_М$ — механическое сопротивление.

На таком же принципе (электромеханического вызывного звонка) образуется микрофонный эффект и в отдельных типах электромеханических реле различного назначения (рис. 6). Акустические колебания воздействуют на якорь реле. Колебания якоря изменяют магнитный поток реле, замыкающийся по воздуху, что приводит к появлению на выходе катушки реле ЭДС микрофонного эффекта.

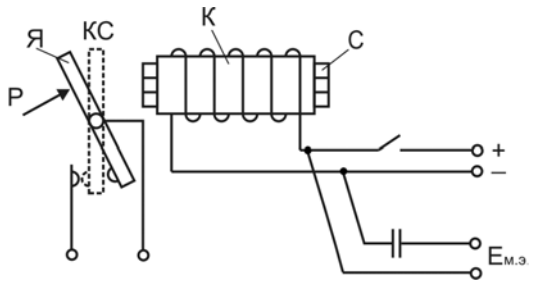

Рис. 6. Схема работы реле: КС — контактная система; К — катушка; С - сердечник

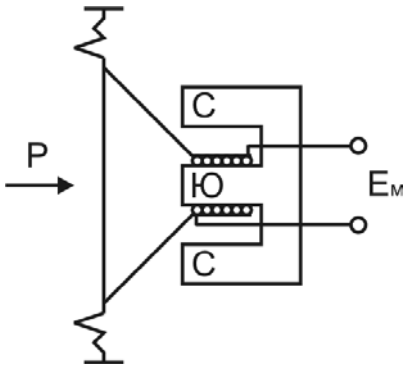

Рис. 7. Схема громкоговорителя

Динамические головки прямого излучения, устанавливаемые в абонентских громкоговорителях, имеют достаточно высокую чувствительность к акустическому воздействию (2–3 мВ/Па) и довольно равномерную в речевом диапазоне частот амплитудно-частотную характеристику, что обеспечивает высокую разборчивость речевых сигналов. Схема динамической головки представлена на рис. 7. ЭДС микрофонного эффекта динамической головки

$$E_м = \eta p, \qquad (20)$$

где $\eta = BlS/z_м$ — акустическая чувствительность; здесь l — длина проводника, движущегося в магнитном поле с индукцией B; S — площадь поверхности, подверженной влиянию давления акустического поля; $z_м$ — механическое сопротивление.

Известно, что абонентские громкоговорители бывают однопрограммные и многопрограммные. В частности, у нас в стране находят достаточно широкое распространение трехпрограммные абонентские громкоговорители.

Трехпрограммные абонентские громкоговорители в соответствии с ГОСТ 18.286-88 (приемники трехпрограммные проводного вещания) имеют основной канал (НЧ) и каналы радиочастоты (ВЧ), включенные через усилитель-преобразователь. Усилитель-преобразователь обеспечивает преобразование ВЧ сигнала в НЧ сигнал с полосой 100–6400 Гц за счет использования встроенных гетеродинов. Так, например, в трехпрограммном громкоговорителе "Маяк-202" используются два гетеродина для второй и третьей программ ВЧ: один вырабатывает частоту 78 кГц, другой - 120 кГц.

Наличие сложной электронной схемы построения трехпрограммных громкоговорителей (обратные связи, взаимные переходы, гетеродины) способствует прямому проникновению сигнала, наведенного динамической головкой,

на выход устройства (в линию). Не исключается и излучение наведенного сигнала на частотах гетеродинов (78 и 120 кГц).

Исполнительное устройство вторичных электрочасов представляет собой шаговый электродвигатель, управляемый трехсекундными разнополярными импульсами напряжением ±24 В, поступающими с интервалом 57 с от первичных электрочасов.

Микрофонный эффект вторичных часов, обусловленный акустическим эффектом шагового электродвигателя, проявляется в основном в интервалах ожидания импульсов управления. Схематически устройство шагового двигателя представлено на рис. 8.

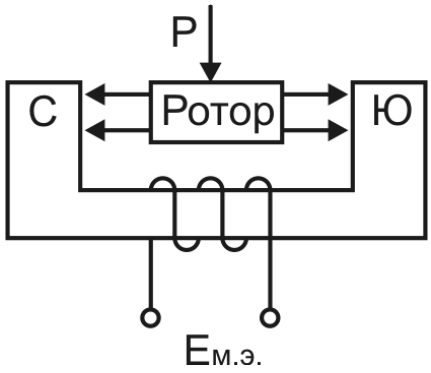

Рис. 8. Устройство шагового двигателя

Степень проявления микрофонного эффекта вторичных электрочасов существенно зависит от их конструкции: в пластмассовом, деревянном или металлическом корпусе; с открытым или закрытым механизмом; с жестким или "мягким" креплением.

В магнитоэлектрическом измерительном приборе имеются неподвижный постоянный магнит и подвижная рамка, которая поворачивается вокруг своей оси под воздействием собственного магнитного поля, создаваемого измеряемым напряжением, и магнитного поля постоянного магнита. Рамка соединена со стрелкой, конец которой перемещается по шкале измерения (рис. 9).

Если акустические колебания воздействуют на рамку, она вращается под их давлением и на ее концах возникает ЭДС индукции.

Практически аналогичная ситуация будет при воздействии акустических колебаний на электромагнитный измерительный прибор. Различие между магнитоэлектрическим и электромагнитным приборами сводится к тому, что в электромагнитном приборе вместо постоянного магнита используется электромагнит.

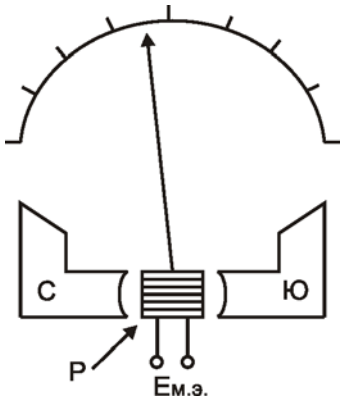

Рис. 9. Устройство магнитоэлектрического измерительного прибора

Следует отметить, что ЭДС микрофонного эффекта возникает и может использоваться в состоянии покоя прибора, когда он не используется для конкретных измерений.

Представителем индукционных акустоэлектрических преобразователей являются различные трансформаторы (повышающие, понижающие, входные, выходные, питания и др.).

Трансформатор состоит из замкнутого сердечника из мягкой стали или феррита, на котором имеются как минимум две изолированные друг от друга катушки (обмотки) с разными числами витков.

Акустическое влияние на сердечник и обмотку трансформатора (например, на входной трансформатор усилителя звуковых частот) приведет к появлению микрофонного эффекта. Если ЭДС индукции появляется в первичной обмотке, то во вторичной обмотке она увеличивается на значение коэффициента трансформации.

Магнитострикция — изменение размеров и формы кристаллического тела при намагничивании — вызывается изменением энергетического состояния кристаллической решетки в магнитном поле и, как следствие, расстояний между узлами решетки. Наибольших значений магнитострикция достигает в ферро- и ферритомагнетиках, в которых магнитное взаимодействие частиц особенно велико.

Обратное по отношению к магнитострикции явление — Виллари-эффект (изменение намагничиваемости тела при его деформации). Виллари-эффект обусловлен изменением под действием механических напряжений доменной структуры ферромагнетика, определяющей его намагниченность. В усилителях

с очень большим коэффициентом усиления входной трансформатор на ферритах при определенных условиях вследствие магнитострикционного эффекта способен преобразовывать механические колебания в электрические.

Пьезоэлектрический эффект

Изучение свойств твердых диэлектриков показало, что некоторые из них поляризуются не только с помощью электрического поля, но и в процессе деформации при механических воздействиях на них. Поляризация диэлектрика при механическом воздействии на него называется прямым **пьезоэлектрическим эффектом**. Этот эффект имеется у кристаллов кварца и у всех сегнетоэлектриков. Чтобы его наблюдать, из кристалла вырезают прямоугольный параллелепипед, грани которого должны быть ориентированы строго определенным образом относительно кристалла. При сдавливании параллелепипеда одна его грань заряжается положительно, а другая — отрицательно. Оказывается, что в этом случае плотность поляризованного заряда грани прямо пропорциональна давлению и не зависит от размеров параллелепипеда. Если сжатие заменить растяжением параллелепипеда, то заряды на его гранях изменяют знаки на обратные.

У пьезокристаллов наблюдается и обратное явление. Если пластину, вырезанную из пьезокристалла, поместить в электрическое поле, зарядив металлические обкладки, то она поляризуется и деформируется, например сжимается. При перемене направления внешнего электрического поля сжатие пластинки сменяется ее растяжением (расширением). Такое явление называется обратным пьезоэлектрическим эффектом.

Чтобы воспринять изменение заряда или напряжения, к пьезоэлектрическому материалу подсоединяют две металлические пластины, которые фактически образуют пластины конденсатора, емкость которого определяется соотношением:

$$C = Q/U, \qquad (21)$$

где Q — заряд; U— напряжение.

На практике в качестве пьезоэлектрического материала применяются кристаллы кварца, рочелиевая соль, синтетические кристаллы (сульфат лития) и поляризованная керамика (титанат бария).

Кварцевые пластины широко используются в пьезоэлектрических микрофонах, охранных датчиках, стабилизаторах генераторов незатухающих колеба-

ний. На рис. 10 показано устройство пьезоэлектрического микрофона. Когда звуковое давление P отклоняет диафрагму 1, ее движение вызывает деформацию пьезоэлектрической пластины 2, которая, в свою очередь, вырабатывает электрический сигнал на выходных контактах.

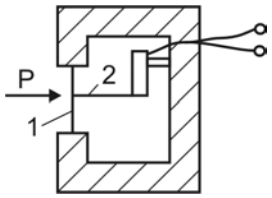

Рис. 10. Устройство пьезоэлектрического микрофона

Излучатели электромагнитных колебаний

Каждое электрическое (электронное) устройство является источником магнитных и электромагнитных полей широкого частотного спектра, характер которых определяется назначением и схемными решениями, мощностью устройства, материалами, из которых оно изготовлено, и его конструкцией.

Известно, что характер поля изменяется в зависимости от расстояния до передающего устройства. Оно делится на две зоны: ближнюю и дальнюю. Для ближней зоны расстояние r значительно меньше длины волны электромагнитного сигнала ($r<<\lambda$), и поле имеет ярко выраженный магнитный (или электрический) характер, а в дальней зоне ($r>>\lambda$) поле носит явный электромагнитный характер и распространяется в виде плоской волны, энергия которой делится поровну между электрической и магнитной компонентами.

Так как длина волны определяет расстояние и тем более назначение устройства, принцип работы и другие характеристики, то правомерно классифицировать излучатели электромагнитных сигналов на низкочастотные, высокочастотные и оптические.

Низкочастотными излучателями электромагнитных колебаний в основном являются звукоусилительные устройства различного функционального назначения и конструктивного исполнения. В ближней зоне таких устройств наиболее мощным выступает магнитное поле опасного сигнала. Такое поле усилительных систем достаточно просто обнаруживается и принимается посредством магнитной антенны и селективного усилителя звуковых частот.

К группе высокочастотных излучателей относятся ВЧ автогенераторы, модуляторы ВЧ колебаний и устройства, генерирующие паразитные ВЧ колебания по различным причинам и условиям.

Источниками опасного сигнала выступают ВЧ генераторы радиоприемников, телевизоров, измерительных генераторов, мониторы ЭВМ.

Модуляторы ВЧ колебаний, как и элементы, обладающие нелинейными характеристиками (диоды, транзисторы, микросхемы), порождают нежелательные составляющие высокочастотного характера. Довольно опасным источником высокочастотных колебаний могут быть усилители и другие активные элементы технических средств в режиме паразитной генерации из-за нежелательной положительной обратной связи.

Источниками излучения высокочастотных колебаний в различной радиотехнической аппаратуре являются встроенные в них генераторы, частота которых по тем или иным причинам может быть промодулирована речевым сигналом. Встроенные генераторы (гетеродины) обязательно имеются в радиоприемниках, телевизорах, магнитофонах, трехпрограммных громкоговорителях и ряде электроизмерительных приборов. К ним примыкают различные усилительные системы — усилители низкой частоты, системы звукоусиления, способные по тем или иным причинам войти в режим самовозбуждения, т.е. по существу стать неконтролируемым гетеродином.

В качестве примера модуляции речью частоты автогенераторов можно рассмотреть микрофонный эффект гетеродинов радиоприемников бытового назначения. Основным элементом гетеродина радиоприемника является колебательный контур с конденсатором переменной емкости. Период собственных колебаний гетеродина определяется условием равенства реактивных сопротивлений катушки индуктивности и конденсатора $x_L=x_C$. Частоту w_0, при которой выполняется это равенство, называют собственной частотой колебательного контура. Ее значение определяется из выражения $\mathrm{w}_0 = 1/\sqrt{\mathrm{LC}}$. Под воздействием акустического давления будет меняться расстояние между пластинами переменного воздушного конденсатора гетеродина. Изменение расстояния приведет к изменению емкости, последнее — к изменению частоты гетеродина по закону акустического давления (произойдет частотная модуляция частоты гетеродина акустическим сигналом).

Кроме конденсаторов акустическому воздействию подвержены катушки индуктивности с поперечными сердечниками, монтажные провода значительной длины, в результате чего они также создают микрофонный эффект.

Практика показала, что акустическая реакция гетеродина возможна на расстоянии до нескольких метров, особенно в помещениях с хорошей акусти-

кой. В зависимости от типа приемника прием такого сигнала возможен на значительном расстоянии, иногда достигающем 1, 2 км.

Источником излучения высокочастотных колебаний в аппаратуре звукозаписи является генератор стирания-подмагничивания (ГСП), частота которого *F* может быть промодулирована речевым сигналом за счет нелинейных элементов в усилителе записи, а также из-за наличия общих цепей электропитания.

В цепях технических средств, находящихся в зоне воздействия мощных высокочастотных излучений $F_{пер}$, наводятся сигналы напряжения до единиц и даже десятков вольт. Если в указанных цепях имеются нелинейные элементы (НЭ), параметры которых (индуктивность, емкость или сопротивление) изменяются под действием низкочастотных сигналов $F_{зв}$, то в окружающем пространстве будет создаваться вторичное поле высокочастотного излучения F_c, модулированное низкочастотным сигналом.

В качестве НЭ могут выступать телефон, различные датчики (ВЧ навязывание по проводам), приемники, магнитофоны (ВЧ навязывание по эфиру) (рис. 11).

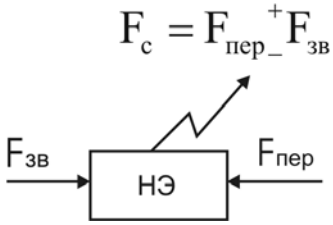

Рис. 11. Схема образования высокочастотного излучения нелинейным элементом

Оптические излучатели

К оптическим преобразователям относятся приборы, преобразующие световую энергию в электрическую и обратно. Простейшим прибором этого типа является *светодиод* — прибор, излучающий свет при пропускании через *p-n*-переход тока в прямом направлении. Обратный светодиоду прибор именуется фотодиодом. *Фотодиод* — это приемник оптического излучения, преобразующий его в электрические сигналы. Кроме того, фотодиод, преобразующий свет в электрическую энергию, выступает и как источник электрической энергии — *солнечный элемент*.

Более сложными оптическими преобразователями являются электронно-оптические преобразователи (ЭОП) и передающие телевизионные трубки различного исполнения (приборы с зарядовой связью, видиконы и пр.).

В технических каналах утечки информации в оптических системах опасным является акустооптический эффект. *Акустооптический эффект* — это явление преломления, отражения или рассеяния света, вызванное упругими деформациями стеклянных отражающих поверхностей или волоконно-оптических кабелей под воздействием звуковых колебаний.

Основным элементом оптического кабеля волоконно-оптических систем является волоконный световод в виде тонкого стеклянного волокна цилиндрической формы. Волоконный световод имеет двухслойную конструкцию и состоит из сердцевины и оболочки с различными оптическими характеристиками (показателями преломления η_1 и η_2). Сердцевина служит для передачи электромагнитной энергии. Назначение оболочки — создание лучших условий отражения на границе сердцевина-оболочка и защита от излучения в окружающее пространство.

Передача волны по световоду осуществляется за счет отражений ее от границы сердечника и оболочки, имеющих разные показатели преломлении (η_1 и η_2). В отличие от обычных электрических проводов, в световодах нет двух проводников и передача происходит волноводным методом в одном волноводе за счет многократного отражения волны от границы раздела сред. Наибольшее распространение получили волоконные световоды двух типов: ступенчатые и градиентные.

В современных волоконно-оптических системах в процессе передачи информации используется модуляция источника света по амплитуде, интенсивности и поляризации.

Внешнее акустическое воздействие на волоконно-оптический кабель приводит к изменению его геометрических размеров (толщины), что вызывает изменение пути движения света, т.е. изменение интенсивности, причем пропорционально значению этого воздействия.

Волоконные световоды как преобразователи механического давления в изменение интенсивности света являются источником утечки акустической информации за счет акустооптического (или акустоэлектрического) преобразования — микрофонного эффекта в волоконно-оптических системах передачи информации (используется также в охранных системах).

При слабом закреплении волокон в разъемном соединителе световодов проявляется акустический эффект модуляции света акустическими полями. Акустические волны вызывают смещение соединяемых концов световода относительно друг друга. Таким образом, осуществляется амплитудная модуляция

излучения, проходящего по волокну. Это свойство находит практическое применение в гидрофонах с колеблющимися волоконными световодами.

Глубина модуляции зависит от двух параметров, один из которых определяется конструкцией и свойствами волокна, а другой зависит от давления.

Чувствительность световода к давлению определяется значением соотношения

$$Ч = \Delta\varphi \Big/ \varphi \cdot \Delta\rho, \qquad (22)$$

где $\Delta\varphi$ — сдвиг фазы, вызываемый изменением давления $\Delta\rho$.

5.2. Классификация технических каналов утечки информации

Каналы утечки информации можно классифицировать по физическим принципам на следующие группы:

— акустические (включая и акустопреобразовательные);

— визуально-оптические (наблюдение, фотографирование);

— электромагнитные (в том числе магнитные и электрические);

— материально-вещественные (бумага, фото, магнитные носители, отходы и т.п.).

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

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 опасного излучения, средой и, возможно, приемной стороной (злоумышленником). При этом в отличие от традиционных систем связи, в которых передающая и приемная стороны преследуют одну цель — передать и принять информацию с наибольшей достоверностью, в случае побочной системы связи "передающая сторона" заинтересована в максимально возможном ухудшении (ослаблении, ликвидации) передачи информации. Побочную систему связи принято называть *техническим каналом утечки информации*.

Правомерно предполагать, что образованию каналов утечки информации способствуют определенные обстоятельства и причины технического характера. К последним можно отнести несовершенство схемных решений (конструк-

тивных и технологических), принятых для данной категории технических средств, и эксплуатационный износ элементов изделия (изменение параметров элементов, аварийный выход/вывод из строя).

В любых технических средствах существуют те или иные физические преобразователи, выполняющие соответствующие им функции, основанные на определенном физическом принципе действия. Знание всех типов физических преобразователей позволяет решать задачу определения возможных неконтролируемых проявлений физических полей, образующих каналы утечки информации.

Преобразователем является прибор, который преобразует изменение одной физической величины в изменение другой. Преобразователь обычно преобразует неэлектрическую величину в электрический сигнал и наоборот.

Примером конкретной реализации преобразователей является звукоусилительная система, в которой микрофон (входной преобразователь) превращает звук (воздействующую физическую величину) в электрический сигнал. Последний передается и усиливается усилителем низкой (звуковой) частоты (преобразователь по мощности), а затем поступает на громкоговоритель (выходной преобразователь), воспроизводящий звук, существенно более громкий, нежели тот, который воспринимается микрофоном.

Каждый преобразователь действует на определенных физических принципах и образует присущий этим принципам побочный канал передачи информации – канал утечки.

Функции приборов и устройств электросвязи можно разделить на два основных вида: обработку электрических сигналов и преобразование какого-либо внешнего физического воздействия в электрические сигналы. Во втором случае основную роль выполняют датчики и преобразователи.

Многообразные эффекты внешнего мира не ограничиваются в своих проявлениях лишь электрическими сигналами. Многочисленны различные физические явления (например звук, свет, давление и т. д.), их можно насчитать десятки. Для преобразования информации о физических явлениях в форму электрического сигнала в электронных системах используются чувствительные устройства — датчики. Они являются началом любой электронной системы. Датчики — это источники электрического сигнала.

Существуют два вида датчиков:

— специально разработанные для создания необходимого электрического сигнала;

— случайные, являющиеся результатом несовершенства схемы или устройства.

По форме преобразования датчики могут быть разделены на преобразователи сигнала и преобразователи энергии. Например, если рассматриваются фотодатчики, то фотодиод преобразует энергию света в электрический сигнал, тогда как солнечный элемент преобразует энергию света в электроэнергию.

На преобразователь воздействуют определенные силы, в ответ на которые порождается определенная реакция (рис. 12).

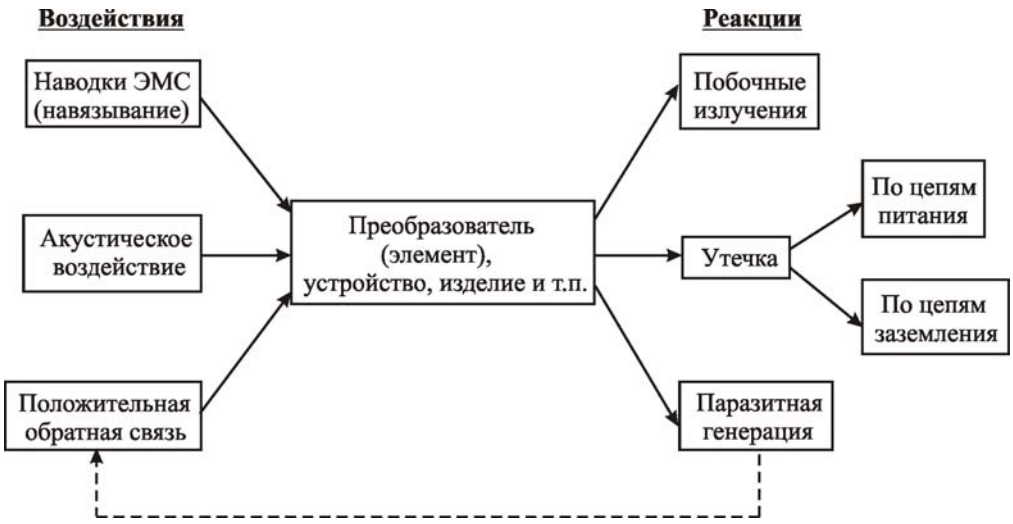

Рис. 12. Варианты образования опасных сигналов

Любой преобразователь характеризуется определенными параметрами. Наиболее важными из них являются:

чувствительность — отношение изменения выходного сигнала к изменению сигнала на его входе;

разрешающая способность — характеризует наибольшую точность, с которой осуществляется преобразование;

линейность — характеризует равномерность изменения выходного сигнала в зависимости от входного;

инертность или время отклика — равны времени установления выходного сигнала в ответ на изменение входного сигнала;

полоса частот — эта характеристика показывает, на каких частотах воздействия на входе еще воспринимаются преобразователем, создавая на выходе допустимый уровень сигнала.

По физической природе имеется значительное количество различных первичных преобразователей, среди которых выделяются такие группы преоб-

разователей, как фотоэлектрические, термоэлектрические, пьезоэлектрические, электромагнитные и акустоэлектрические, широко использующиеся в современных системах связи, управления и обработки информации.

Помимо преобразователей источниками каналов утечки информации могут быть различного рода излучатели электромагнитных колебаний, а также паразитные связи и наводки по электрическим и электромагнитным полям.

Таким образом, основными источниками образования технических каналов утечки любой, в том числе конфиденциальной, информации являются:

преобразователи физических величин;

излучатели электромагнитных колебаний;

паразитные связи и наводки на провода и элементы электронных устройств.

Каждую из этих групп в свою очередь можно декомпозировать по принципам преобразования или иным параметрам. Так, преобразователи могут быть классифицированы по принципам на индуктивные, емкостные, пьезоэлектрические и оптические. При этом по виду преобразования они могут быть и акустическими и электромагнитными. Излучатели электромагнитных колебаний декомпозируются по диапазону частот на низкочастотные, высокочастотные и оптические.

Паразитные связи и наводки проявляются в виде обратной связи (наиболее характерна положительная обратная связь), утечки по цепям питания и заземления.

5.3. Паразитные связи и наводки

Элементы, цепи, тракты, соединительные провода и линии связи любых электронных систем и схем постоянно находятся под воздействием собственных (внутренних) и сторонних (внешних) электромагнитных полей различного происхождения, индуцирующих или наводящих в них значительные напряжения. Такое воздействие называют электромагнитным влиянием, или просто влиянием на элементы цепи. Так как такое влияние образуется непредусмотренными связями, то говорят о паразитных (вредных) связях и наводках, которые также могут привести к образованию каналов утечки информации.

Основными видами паразитных связей в схемах электромагнитных устройств являются емкостные, индуктивные, электромагнитные, электромеханические и связи через источники питания и заземления радиоэлектронных

средств. Рассмотрим паразитные связи и наводки на примере широко распространенных усилительных схем различного назначения.

Паразитные емкостные связи

Эти связи обусловлены наличием электрической емкости между элементами, деталями и проводниками усилителей, несущих потенциал сигнала. Так как сопротивление емкости, создающей паразитную емкостную связь, падает с ростом частоты $X_c = 1/\omega C$, проходящая через нее энергия с повышением частоты увеличивается. Поэтому паразитная емкостная связь может привести к самовозбуждению на частотах, превышающих высшую рабочую частоту усилителя.

Чем больше усиление сигнала между цепями и каскадами, имеющими емкостную связь, тем меньшей емкости достаточно для его самовозбуждения. При усилении в 10^5 раз (100 дБ) для самовозбуждения усилителя звуковых частот иногда достаточно емкости между входной и выходной цепями $C_{пс} = 0{,}01$ пФ.

Индуктивные связи

Такие связи обусловлены наличием взаимоиндукции между проводниками и деталями усилителя, главным образом, между его трансформаторами. Паразитная индуктивная обратная связь между трансформаторами усилителя, например между входным и выходным трансформаторами, может вызвать самовозбуждение в области рабочих частот и на гармониках.

Для усилителей с малым входным напряжением (микрофонные, магнитофонные и др.) очень опасна индуктивная связь входного трансформатора с источниками переменных магнитных полей (трансформаторами питания). При расположении такого источника в нескольких десятках сантиметров от входного трансформатора наводимая на вторичной обмотке трансформатора средних размеров ЭДС может достигнуть нескольких милливольт, что в сотни раз превосходит допустимое значение. Значительно слабее паразитная индуктивная связь проявляется при тороидальной конструкции входного трансформатора. Паразитная индуктивная связь ослабляется при уменьшении размеров трансформаторов.

Электромагнитные связи

Паразитные электромагнитные связи приводят к самовозбуждению отдельных каскадов звуковых и широкополосных усилителей на частотах порядка десятков и сотен мегагерц. Эти связи обычно возникают между выводными проводниками усилительных элементов, образующими колебательную систему

с распределенными параметрами на резонансной частоте определенного значения.

Электромеханические связи

Паразитные электромеханические связи проявляются в устройствах, корпус которых имеет жесткую механическую связь с включенным на вход усилителя громкоговорителем, в усилителях, расположенных близко от громкоговорителя, а также в усилителях, подвергающихся вибрации (сотрясению). Механические колебания диффузора близкорасположенного громкоговорителя через корпус последнего и шасси усилителя, а также через воздух передаются усилительным элементам. Вследствие микрофонного эффекта эти колебания вызывают в цепях усилителя появление переменной составляющей тока, создающей паразитную обратную связь.

Транзисторы почти не обладают микрофонным эффектом, поэтому паразитная электромеханическая связь проявляется в основном в ламповых усилителях.

Обратная связь в усилителях

Обратная связь представляет собой передачу сигналов из последующих цепей в предыдущие, т.е. в направлении, обратном нормальному, например из выходной цепи усилительного элемента или усилителя в его входную цепь.

В системах с обратной связью, используемых в качестве усилителя, термином устойчивость определяют наличие или отсутствие в системе собственных установившихся колебаний. В то время как система, не имеющая цепей обратной связи, всегда устойчива, введение обратной связи может оказаться причиной возникновения колебаний в системе.

Амплитудные и фазовые характеристики усилителя и цепи обратной связи являются функциями частоты, и по этой причине обратная связь может быть положительной при одних частотах и отрицательной - при других. Следовательно, система, имеющая отрицательную обратную связь в среднечастотном диапазоне, может оказаться системой с положительной обратной связью при частотах, удаленных от этого диапазона, и быть каналом утечки информации.

5.4. Утечка информации по линиям питания

Обратные связи через источники питания в многокаскадном усилителе возникают вследствие того, что источник питания имеет внутреннее сопротивление.

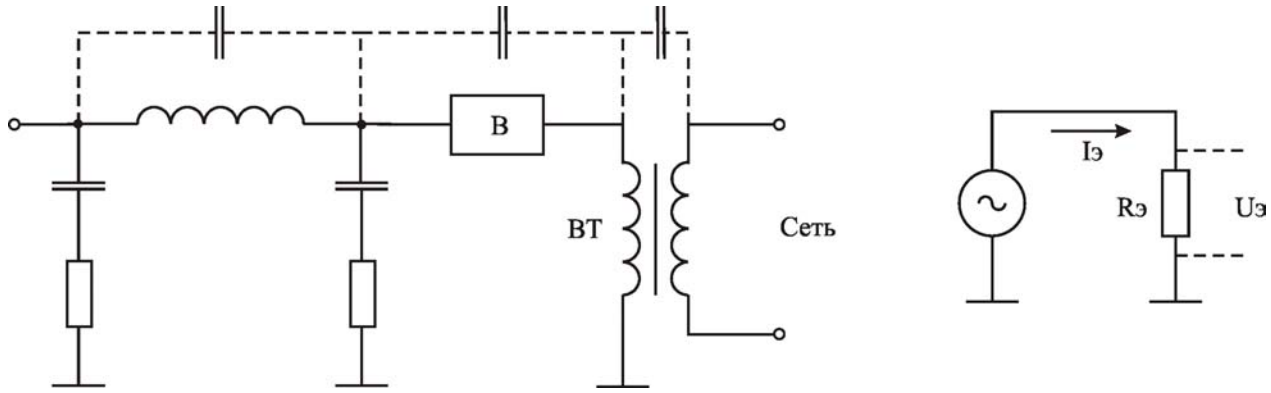

Рис. 13. Схема утечки информации по цепям питания: В — выпрямитель; ВТ - входной трансформатор

Так, выходной ток сигнала $I_{вых}$, проходя через источник питания $E_{пит}$, создает на внутреннем сопротивлении z последнего падение напряжения $U = I_{вых}z$. Это напряжение вместе с постоянной составляющей напряжения источника питания подается на предыдущие каскады, а затем через элементы межкаскадной связи попадает на входы усилительных элементов, создавая в усилителе паразитную обратную связь. В зависимости от фазы по отношению к сигналу это напряжение может увеличивать амплитуду сигнала и привести к самовозбуждению. Опасный сигнал может попасть в цепь электрического питания, создавая канал утечки информации. В линию электропитания высокая частота передается посредством паразитных емкостей трансформаторов блоков питания (рис. 13).

5.5. Утечка информации по цепям заземления

Заземление — это устройство, состоящее из заземлителей и проводников, соединяющих заземлители с электронными и электрическими установками, приборами, машинами. Заземлителем называют проводник или группу проводников, выполненных из проводящего материала и находящихся в непосредственном соприкосновении с грунтом. Заземлители могут быть любой формы — в виде труб, стержня, полосы, листа проволоки и т. п. Заземлители в основном выполняют защитную функцию и предназначаются для соединения с землей приборов защиты.

Отношение потенциала заземлителя $U_з$ к стекающему с него току $I_з$ называется **сопротивлением заземлителя** $R_з$. Значение сопротивления заземлителя зависит от удельного сопротивления грунта и площади соприкосновения заземлителей с землей.

5.6. Взаимные влияния в линиях связи

С целью рассмотрения результатов влияния друг на друга параллельно проложенных линий связи приняты следующие основные определения (рис. 14):

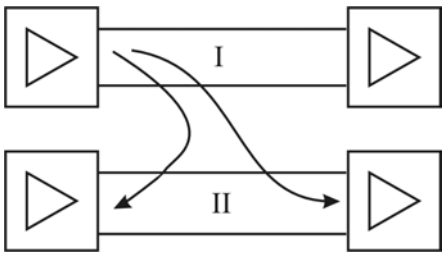

Рис. 14. Сигналы в цепях от взаимных влияний

влияющая цепь — цепь, создающая первичное влияющее электромагнитное поле (цепь I);

цепь, подверженная влиянию, — цепь, на которую воздействует влияющее электромагнитное поле (цепь II*);*

непосредственное влияние — сигналы, индуцированные непосредственно электромагнитным полем влияющей цепи, в цепи, подверженной влиянию.

В зависимости от структуры влияющего электромагнитного поля и конструкции цепи, подверженной влиянию, различают систематические и случайные влияния. К систематическим влияниям относятся взаимные наводки, возникающие по всей длине линии. К случайным относятся влияния, возникающие вследствие ряда случайных причин и не поддающиеся точной оценке. Существуют реальные условия наводок с одного неэкранированного провода на другой, параллельный ему провод той же длины, когда оба они расположены над "землей". В таблице приведены примерные данные взаимного влияния различных типов линий и меры их защиты.

Взаимное влияние различных типов линий и меры их защиты

Тип линии	Преобладающее влияние	Меры защиты
Воздушные линии связи	Систематическое влияние, возрастающее с увеличением частоты сигнала	Скрещивание цепей, оптимальное расположение цепей

Тип линии	Преобладающее влияние	Меры защиты
Коаксиальный кабель	Систематическое влияние через третьи цепи (с повышением частоты влияние убывает вследствие поверхностного эффекта)	Экранирование и ограничение диапазона рабочих частот снизу
Симметричный кабель	Систематическое и случайное влияние, возрастающее с частотой	Оптимизация шагов скрутки и конструкций кабеля, пространственное разделение цепей, экранирование
Оптический кабель	Систематическое и случайное влияние (от частоты сигнала практически не зависит)	Экранирование оптических волокон, пространственное разделение оптических волокон

С определенной степенью обобщения множество каналов утечки информации может быть обусловлено следующими причинами и явлениями:

за счет микрофонного эффекта элементов электронных схем;

за счет магнитного поля электронных схем и устройств различного назначения и использования;

за счет электромагнитного излучения низкой и высокой частот;

за счет возникновения паразитной генерации усилителей различного назначения;

по цепям питания электронных систем;

по цепям заземления электронных систем;

из-за взаимного влияния проводов и линий связи;

за счет высокочастотного навязывания мощных радиоэлектронных средств и систем;

волоконно-оптическими системами связи.

Каждый из этих каналов в зависимости от конкретной реализации элементов, узлов и изделий будет иметь определенное проявление, специфические

характеристики и особенности образования в зависимости от условий расположения и исполнения.

Наличие и конкретные характеристики каждого источника образования канала утечки информации изучаются, исследуются и определяются конкретно для каждого образца технических средств на специально оборудованных для этого испытательных стендах и в специальных лабораториях для последующего использования в конкретных условиях.

5.7. Несанкционированный доступ в электромагнитных каналах

5.7.1. Способы незаконного подключения к линиям связи

Незаконное подключение. Самым простым способом незаконного подключения является контактное подключение, например параллельное подключение телефонного аппарата, довольно широко распространенное в жизни и в быту. Но оно легко обнаруживается вследствие существенного падения напряжения, приводящего к ухудшению слышимости в основном телефонном аппарате. В техническом отношении метод контактного подключения заключается в том, что он реализуется непосредственным включением в провода телефонного либо телеграфного аппарата.

Более совершенным является подключение к линиям связи или проводам с помощью согласующего устройства. Известен способ контактного подключения аппаратуры к линиям связи с компенсацией падения напряжения. Подслушивающая аппаратура и компенсирующий источник напряжения при этом способе включаются в линию последовательно.

Используется еще один способ перехвата телеграфных передач при помощи включения в линию низкоомного чувствительного реле (рис. 15). Контакты реле будут замыкать местную цепь телеграфного аппарата в соответствии с током, проходящем по линии. Механическое реле может применяться на низких скоростях телеграфирования, на высоких же скоростях (факс, линии передачи данных) используют электронные реле. При этом для устойчивости работы аппаратуры перехвата не исключается использование усилителей тока.

Бесконтактное подключение к линии связи осуществляется двумя путями:

за счет электромагнитных наводок в рамке, параллельно приложенной к проводам;

с помощью сосредоточенной индуктивности, охватывающей контролируемую линию.

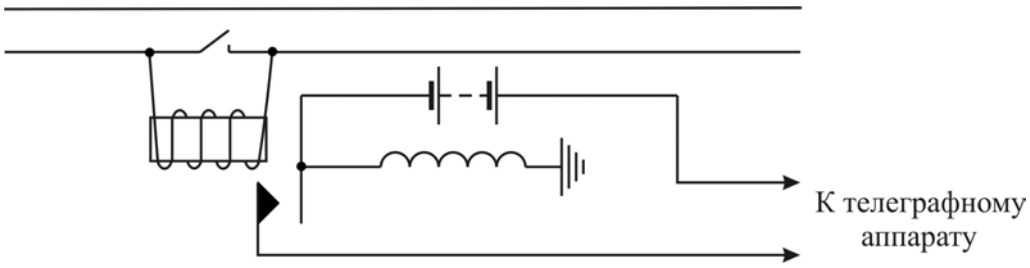

Рис. 15. Перехват телеграфных передач при помощи реле

В обоих случаях подслушивание реализуется за счет электромагнитной индукции. Так, двухпроводная телефонная линия с разнесенными неперевитыми проводами (именуемая часто "лапша") индуктирует в параллельных проводах ЭДС, т. е. готова к подслушиванию.

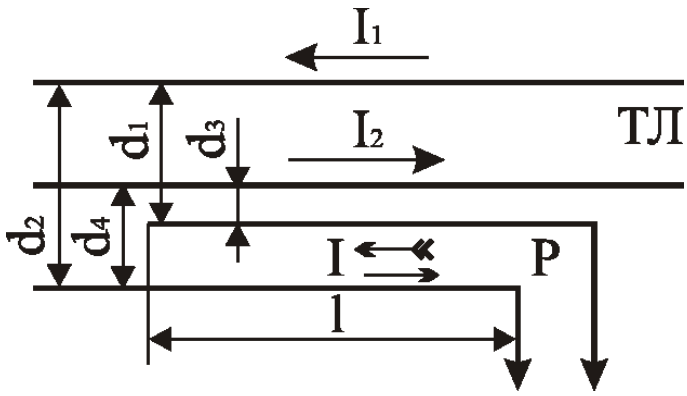

Рис. 16. Подслушивание двухпроводной линии на рамку

На рис. 16 I_1, I_2 — токи в двухпроводной телефонной линии (ТЛ), а d_1, d_2, d_3 и d_4 - расстояния между рамкой и проводами подслушиваемой линии. Ток I_1 индуктирует в рамке Р ток I одного направления (стрелка без оперения), а ток I_2 индуктирует в рамке ток I противоположного направления (стрелка с оперением). В рамке будет циркулировать ток, равный разности индуктированных токов. Этот ток, попадая в усилитель поста подслушивания, усиливается и поступает на головные телефоны и магнитофон. ЭДС, наведенная в рамке, будет тем больше, чем больше активная длина рамки l, больше разнос проводов двухпроводной линии и чем ближе к линии находится рамка.

Индуктивный съем информации с телефонной линии. В связи со слабым влиянием индуктивного датчика на параметры телефонной линии обнару-

жить его техническими средствами практически невозможно. Отсутствие гальванического контакта и надежная изоляция проводящих элементов датчика от телефонной линии в зоне подключения датчика делают невозможным его "выжигание". Встает вопрос о возможности исключить или подавить индуктивный съем информации (без использования скремблера). Остановимся на принципе работы классического индуктивного датчика (рис. 17).

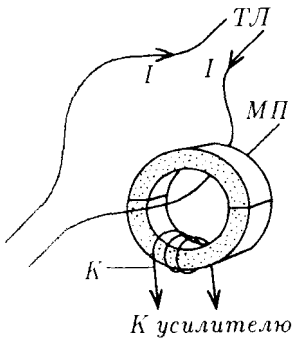

Рис. 17. Принцип работы индуктивного датчика

Два провода телефонного кабеля отделяются один от другого, и на один из них надевается замкнутый магнитопровод датчика. Обычно для удобства установки магнитопровод делается из двух разделяющихся частей, которые соединяются при установке. Во время разговора по телефонным проводам течет переменный электрический ток, пропорциональный звуковому давлению (звуку), которое создают говорящие абоненты. Этот ток одинаков для каждой жилы телефонного провода, но направлен в противоположные стороны. Вокруг каждой из жил ТЛ возникает переменное магнитное ноле, пропорциональное переменному току. Магнитное поле от жилы, охваченной магнитопроводом МП, создает в нем переменный магнитный поток, который наводит ЭДС в катушке К, намотанной на одну из "половинок" магнитопровода. Таким образом, на концах катушки возникает напряжение, изменяющееся вместе со звуковыми колебаниями. Далее оно усиливается и подается на вход радиопередатчика, диктофона или другого устройства.

Существуют различные способы подавления телефонных закладок, которые реализованы в аппаратуре. Самым распространенным из них является подача в телефонную линию сигнала на частотах, не входящих в стандартный телефонный диапазон. Это может быть либо шум, легко принимаемый человеческим ухом и потому затрудняющий прослушивание, либо ультразвуковой тон, "подавляющий" усилитель подслушивающего устройства. Сам телефонный ап-

парат такие помехи практически не пропускает, и говорящие не испытывают значительных неудобств. По той же причине такой способ совершенно не действует на самое доступное подслушивающее устройство — параллельный телефон. Совершенно очевидно, что телефонные закладки, фильтрующие частоты, не входящие в телефонный диапазон, невозможно подавить таким образом. В индуктивных датчиках эта задача решается просто: магнитопровод делается из специального материала, который очень хорошо усиливает магнитное поле на звуковых частотах и очень плохо "работает" в остальном диапазоне.

Другим способом является подача в линию синфазной помехи на частотах телефонного диапазона. Токи от такой помехи движутся по обоим проводам телефонного кабеля в одну и ту же сторону и, дойдя до трансформатора телефонного аппарата, компенсируют друг друга, не вызывая помех в трубке телефона. Индуктивный датчик вместе с полезным сигналом снимает и помеху, в результате подслушивание становится невозможным. Если, конечно, вид помехи выбран правильно (т.е. ее нельзя отделить от полезного сигнала известными методами).

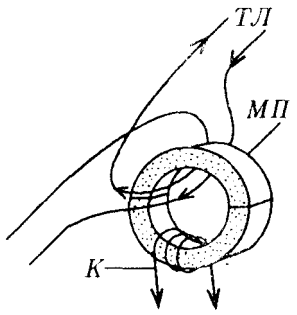

Рис. 18. Способ установки индуктивного датчика, исключающий подавление синфазной помехой

Существует метод подключения индуктивного датчика, при котором описываемый способ подавления не работает. Для этого достаточно через кольцо магнитопровода пропустить второй провод, предварительно свернув ее кольцом (рис. 18). При таком размещении второй жилы направления полезных токов совпадают (стрелками показаны направления полезных токов). Токи от помехи в проводах внутри кольца противоположны по направлению и взаимокомпенсируются, в то время как поток от полезных токов удвоится.

Способом подавления индуктивных датчиков является уменьшение тока в телефонной сети до предела, когда говорящие еще слышат друг друга, но сигнал, снимаемый датчиком, слаб настолько, что становится сравним с уровнем

естественных помех. В простейших подслушивающих системах эффект от предложенного способа может появиться уже из-за того, что не хватает усиления (малая глубина АРУ). При достаточной глубине АРУ проблемой станет отношение сигнал/шум в усиленном сигнале. В настоящее время появились достаточно эффективные датчики (например, "Траверс-04"), имеющие очень низкий уровень собственного шума и высокую чувствительность.

Способом защиты телефонной линии от телефонных закладок является изменение напряжения на линии. Такой способ полезен для борьбы с гальванически подключаемыми закладками, но неэффективен против индуктивного съема информации.

Представляемые на современном рынке односторонние средства подавления используют один из четырех описанных способов либо их комбинацию. Поэтому можно сделать вывод о том, что если индуктивный датчик типа "Траверс-04" правильно установить (см. рис. 18), то он аппаратно не обнаружим и не уничтожим односторонними аппаратами (т.е. не скремблерами).

5.7.2. 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 сигналами, по токоведущим цепям или излучение их в свободное пространство создают реальную возможность утечки закрытой информации.

На рис. 19 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).

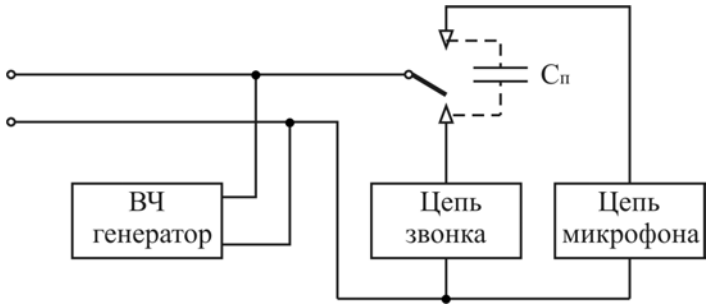

Рис. 19. Принцип реализации высокочастотного навязывания в телефонном аппарате

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 рычажковым переключателем, между цепью микрофона и выходом линии существует паразитная емкость $С_п$ порядка 5-15 пФ. На достаточно высоких частотах емкостное сопротивление этого переключателя будет относительно невысоким, поэтому навязываемые высокочастотные колебания через емкость $С_п$ 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 высокочастотных 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.

5.8. Утечка информации по прямому акустическому каналу

Наиболее простым способом перехвата речевой информации является подслушивание (прямой перехват). Разведываемые акустические сигналы могут непосредственно приниматься ухом человека, реагирующим на изменение звукового давления, возникающего при распространении звуковой волны в окружающем пространстве. Диапазон частот акустических колебаний, слышимых человеком, от 16 - 25 Гц до 18 - 20 кГц в зависимости от индивидуальных особенностей слушателя. Человек воспринимает звук в очень широком диапазоне звуковых давлений, одной из базовых величин этого диапазона является стандартный порог слышимости. Под ним условились понимать эффективное значение звукового давления, создаваемого гармоническим звуковым колебанием частотой F=1000 Гц, едва слышимым человеком со средней чувствительностью слуха. Порогу слышимости соответствует звуковое давление $P=2\cdot10^{-5}$ Па. Верхний предел определяется значением P=20 Па, при котором наступает болевое ощущение (стандартный порог болевого ощущения).

В случаях, когда уровни звукового давления, создаваемого звуковой волной, ниже порога слышимости, когда нет возможности непосредственно прослушивать речевые сообщения или требуется их зафиксировать (записать), используют микрофон.

Микрофон является преобразователем акустических колебаний в электрические сигналы. В зависимости от физического явления, приводящего к такому преобразованию, различают основные типы микрофонов:

— электродинамические;
— электромагнитные;
— электростатические;
— пьезоэлектрические;
— магнитострикционные;
— контактные и т.д.

Действие электродинамического преобразователя основано на использовании явления электромагнитной индукции (рис. 20). В кольцевом зазоре 1 магнитной системы, имеющей постоянный магнит 2, находится подвижная катушка 3, соединенная с диафрагмой 4. При воздействии на диафрагму 4 звукового давления она вместе с подвижной катушкой 3 совершает колебания в маг-

нитном поле, создаваемом магнитной системой 2. В витках катушки 3, пересекающих магнитные силовые линии, возникает напряжение, являющееся выходным сигналом микрофона. Его величина определяется выражением [2]:

$$U = Bl\frac{F}{Z_M}\frac{R_H}{R_i + R_H}, \qquad (23)$$

где B — индукция в зазоре магнитной системы; l — длина проводника обмотки подвижной катушки; F — сила звукового давления, действующая на диафрагму микрофона; Z_M — механическое сопротивление акустомеханической системы микрофона; R_i — внутреннее сопротивление микрофона; R_H — сопротивление нагрузки микрофона.

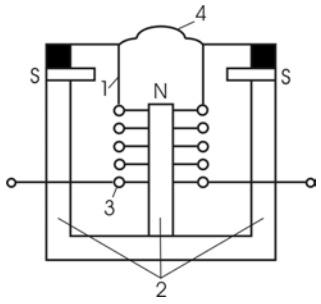

Рис. 20. Действие электродинамического преобразователя

Электромагнитный микрофон работает следующим образом (рис. 21). Перед полюсными наконечниками 2 магнита 3 располагается ферромагнитная диафрагма 1 или скрепленный с нею якорь. При колебаниях диафрагмы под воздействием на нее звукового давления изменяется магнитное сопротивление магнитной системы, а следовательно, и магнитный поток через витки обмотки, намотанной на магнитопровод этой системы. В результате на зажимах этой обмотки возникает переменное напряжение низкой частоты, являющееся выходным сигналом микрофона. Его величина равна [2]:

$$U = \omega\frac{\Phi_0}{d}\frac{F}{Z_M}\frac{R_H}{R_i + R_H}, \qquad (24)$$

где Φ_0 — величина магнитного потока, исходящего из полюса магнитной системы; d — величина зазора между полюсом и якорем (диафрагмой); ω — число витков обмотки.

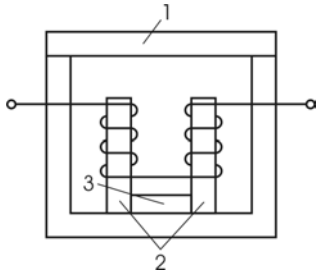

Рис. 21. Принцип работы электромагнитного микрофона

Электростатический (конденсаторный) микрофон представляет собой конденсатор, состоящий из двух пластин, разделенных слоем диэлектрика (рис. 22). Одна из пластин является мембраной 1, которая может колебаться под действием звукового давления относительно второй неподвижной пластины 2. При колебаниях мембраны емкость конденсатора изменяется с частотой воздействующего на мембрану звукового давления. Вследствие этого в электрической цепи появляется переменный ток той же частоты и возникает падение напряжения на нагрузочном сопротивлении, являющееся выходным напряжением микрофона [2]:

$$U = \frac{E}{d}\frac{F}{\omega Z_M}\frac{R_H}{R_i + R_H}, \qquad (25)$$

где d — величина зазора между диафрагмой и неподвижным электродом; Z — внутреннее электрическое (емкостное) сопротивление микрофона.

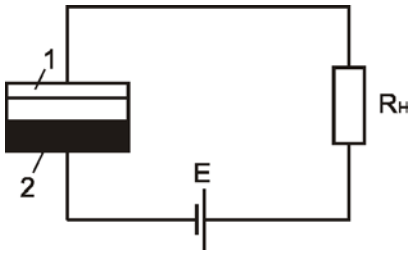

Рис. 22. Устройство электростатического (конденсаторного) микрофона

Действие пьезоэлектрических электроакустических преобразователей основано на проявлении пьезоэлектрического эффекта, т.е. на возникновении поляризации диэлектрика при механическом воздействии на него. Этот эффект наблюдается в кристаллах кварца, сегнетоэлектриках и некоторых других материалах. В пьезоэлектрическом микрофоне (рис. 23) звуковое давление воздей-

ствует непосредственно или через диафрагму 1 и соединенный с ней стержень 2 на пьезоэлектрический элемент (кристалл, пьезокерамику) 3. При деформации

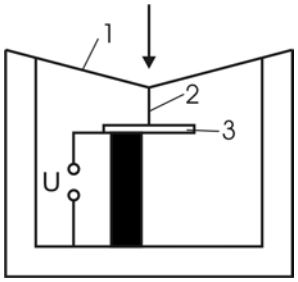

Рис. 23. Устройство пьезоэлектрического микрофона

последнего на его обкладках вследствие пьезоэлектрического эффекта возникает напряжение, являющееся выходным сигналом микрофона [2]:

$$U = k\frac{F}{\omega Z_M}\frac{R_H}{R_i + R_H}, \qquad (26)$$

где k — пьезоэлектрический коэффициент.

В магнитострикционных преобразователях под действием механических напряжений изменяется доменная структура ферромагнетика, определяющая его намагниченность. Вследствие этого при определенных условиях осуществляется преобразование механических колебаний в электрические.

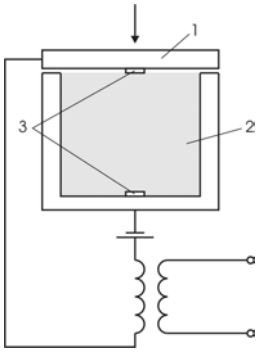

Рис. 24. Принцип действия контактных микрофонов на примере угольного микрофона

Принцип действия контактных микрофонов основан на изменении сопротивления контакта в зависимости от звукового давления. Например, при воздействии звукового давления на диафрагму 7 угольного микрофона (рис. 24) она совершает колебания. В такт с этими колебаниями изменяется сила сжатия зерен угольного порошка (засыпки) 2, вследствие чего изменяется сопротивле-

ние засыпки между электродами 3—3. При постоянном напряжении, приложенном к этим электродам, изменяется и величина тока, протекающего через микрофон. Если включить микрофон в первичную обмотку трансформатора, то на зажимах его вторичной обмотки будет возникать переменное напряжение, соответствующее воздействующему на микрофон акустическому сигналу. Величина выходного напряжения микрофона определяется выражением [3]

$$U = \frac{kF}{\omega Z_M} \frac{U_0 R_H n}{R_i n^2 + R_H}, \qquad (26)$$

где U_0 — величина приложенного к микрофону постоянного напряжения; n — коэффициент трансформации трансформатора; k — отношение коэффициента модуляции к величине смещения диафрагмы микрофона.

К микрофонам, используемым в технике акустической разведки, предъявляют высокие требования. Преобразование звука в электрический сигнал должно осуществляться с высокой информационной точностью, необходимо обеспечить высокую разборчивость и узнаваемость речевого сигнала, избежать появления различных искажений в пределах динамического диапазона в заданной полосе частот. Кроме того, микрофоны должны обладать направленными свойствами, высокой чувствительностью и приемлемыми массогабаритными характеристиками.

При необходимости передать перехваченное речевое сообщение на расстояние используют проводные, радио- и другие каналы, по которым сообщение, преобразованное в электрический, оптический, радио- или другого вида сигнал, передается на пункт прослушивания. В этих случаях используемые устройства называются закладными устройствами для перехвата акустической информации. В состав радиозакладки может быть включено запоминающее устройство, в которое предварительно записывается перехваченная речевая информация. Ее передача в пункт прослушивания в этом случае осуществляется не в реальном масштабе времени, а с определенной временной задержкой, что повышает скрытность радиозакладных устройств.

Структурная схема, иллюстрирующая прямой перехват акустической информации, представлена на рис. 25.

К настоящему времени разработано достаточно большое количество типов направленных микрофонов и закладных подслушивающих устройств.

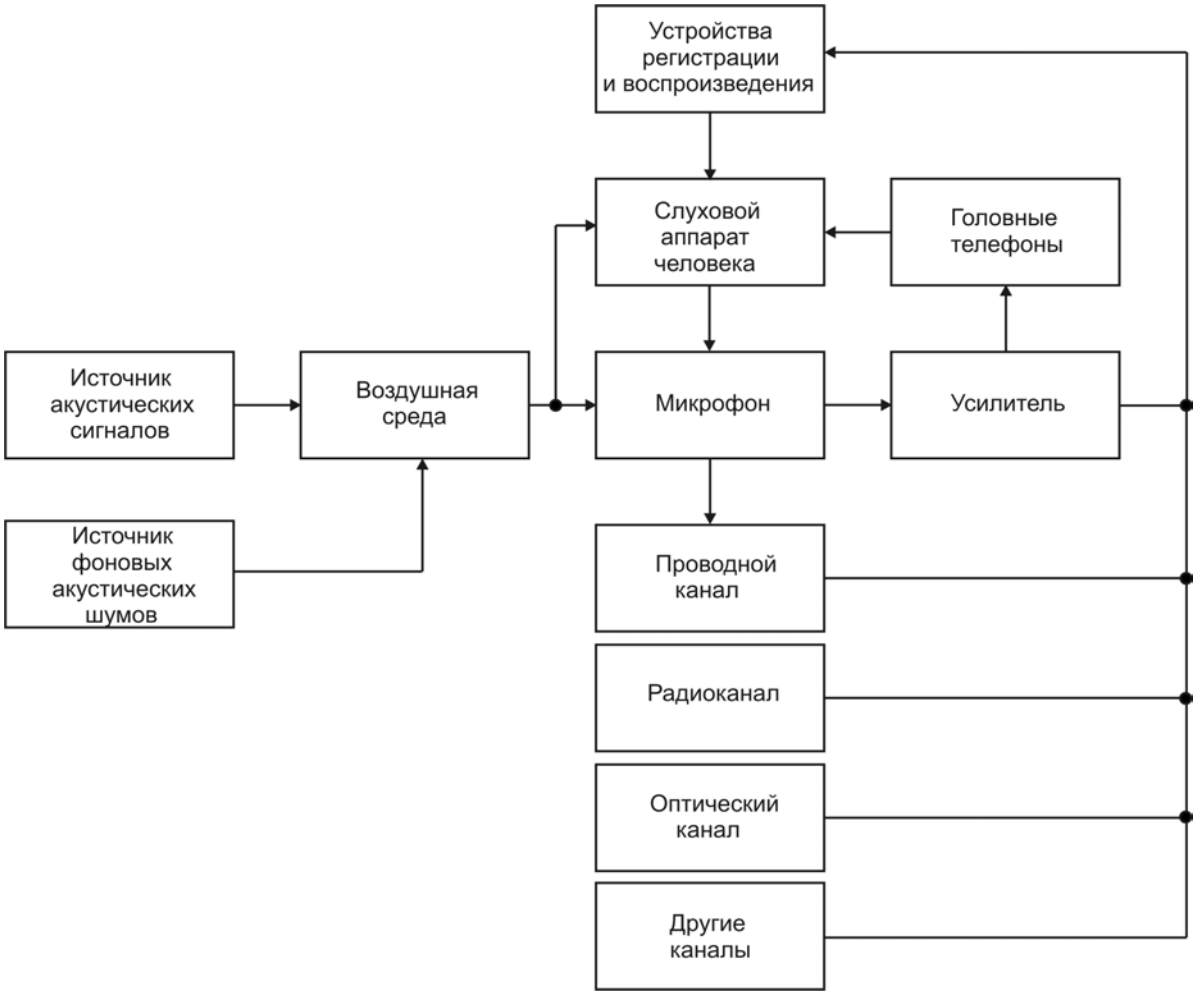

Рис. 25. Структурная схема прямого перехвата акустической информации

5.9. Защита информации от утечки по прямому акустическому каналу

На основании вышеприведенных схем электронных устройств, их описания и анализа можно сделать вполне обоснованный вывод об относительной легкости несанкционированного доступа к конфиденциальной информации или, проще говоря, — шпионажа с применением электронных средств.

Информация может быть не только похищена, но и искажена или даже частично или полностью уничтожена в результате информационной диверсии. При этом информационной агрессии может подвергнуться любой объект формирования, преобразования или хранения данных, канал их передачи, обладатель, хранитель ценной информации.

Очевидно, что информацию необходимо защищать всеми доступными, но не противоречащими закону средствами. Однако следует отметить, что абсолютной защиты, гарантирующей полную неприкосновенность тайн, не сущест-

вует. К сожалению, даже неквалифицированный похититель секретов может нанести обладателю ценной, важной и секретной, но не защищенной информации вполне ощутимый и иногда непоправимый ущерб. При этом он может использовать самые простейшие устройства, собираемые "на коленках" за пару часов из подручных средств, а иногда на подобное конструирование уходит всего несколько минут.

Для несанкционированного доступа могут быть использованы передатчики-закладки, принимающие от встроенных микрофонов сигналы, и преобразующие, передающие их в эфир различные ретрансляторы, например телефонные, преобразующие электрический сигнал от телефонной линии в АМ или ЧМ-радиосигнал, преобразователи, усилители и другие электронные средства, а также достаточно сложные комплексы, состоящие из приемников, передатчиков, различных конвертеров и усилителей. Эти устройства могут использоваться по отдельности или совместно, в комплексе. Такие комплексы принимают радиосигнал, усиливают, преобразуют и передают его иногда на другой радиочастоте.

Часто при конструировании устройств несанкционированного доступа к конфиденциальной информации в качестве основы используются стандартные средства связи, даже без значительных переделок.

Необходимо констатировать, что для целей электронного шпионажа и информационной агрессии применяется широкий спектр электронных средств. При этом могут быть использованы не только чрезвычайно сложные и дорогие аппараты, основанные на достижениях современной науки, но и очень простые, дешевые, иногда достаточно эффективные устройства — особенно в условиях отсутствия защиты конфиденциальной информации.

Вот несколько простейших примеров-опытов, иллюстрирующих возможности по перехвату информации.

Из большого листа плотной бумаги с ворсом под бархат изготавливается труба диаметром 10–15 см и длиной 1,5–2 м. В один конец этой трубы вставляется чувствительный микрофон. Это может быть, например, динамический микрофон типа МД64, МД200 или даже миниатюрный МКЭ-3. Микрофон необходимо подключить с помощью экранированного кабеля к чувствительному усилителю с малым уровнем собственных шумов. Если длина кабеля превышает 0,5 м, то лучше воспользоваться микрофонным усилителем, имеющим дифференциальный вход, например УНЧ на ОУ. Это позволит уменьшить синфазную составляющую помех — различного рода наводки от ближайших электро-

магнитных устройств (фон 50 Гц от сети 220 В) и т.д. Теперь о втором конце данной бумажной трубы: если его направить на источник звука, например на группу разговаривающих людей, то можно услышать речь на расстоянии 100 и более метров. И усилитель, и микрофон, снабженный такой трубой, позволяют достаточно хорошо все слышать на таком значительном удалении. Расстояние может быть даже увеличено при использовании специальных селективных фильтров, позволяющих выделять или подавлять сигнал в узких полосах частот, что дает возможность повысить уровень полезного сигнала в условиях неизбежно существующих помех. В упрощенном варианте вместо спецфильтров можно применить полосовой фильтр в УНЧ или воспользоваться обычным эквалайзером — многополосным регулятором тембра, в крайнем случае традиционным, т.е. обычным двухполосным регулятором тембра НЧ и ВЧ [4].

Конструирование чувствительного и малошумящего УНЧ имеет свои особенности. Наибольшее влияние на качество воспроизведения звуков и разборчивость речи оказывают амплитудно-частотная характеристика (АЧХ) усилителя, уровень его шумов, параметры микрофона (АЧХ, диаграмма направленности, чувствительность и т.д.) или заменяющих его датчиков, а также их взаимная согласованность с усилителем. Усилитель должен иметь достаточное усиление - при использовании микрофона это 60-80 дБ, т.е. в 1000-10 000 раз. Учитывая особенности приема полезного сигнала и его низкую величину в условиях сравнительно значительного уровня помех, которые существуют всегда, целесообразно в конструкции усилителя предусмотреть возможность коррекции АХЧ, т.е. частотной селекции обрабатываемого сигнала. При этом необходимо учитывать, что наиболее информативный участок звукового диапазона сосредоточен в полосе от 300 Гц до 3–3,5 кГц. Правда, иногда с целью уменьшения помех эту полосу сокращают еще больше. Использование полосового фильтра в составе усилителя позволяет значительно увеличить дальность прослушивания (в 2 и более раз). Еще большей дальности можно достичь использованием в составе УНЧ селективных фильтров с высокой добротностью, позволяющих выделять или подавлять сигнал на определенных частотах. Это дает возможность значительно повысить соотношение сигнал/шум.

Однако, несмотря на широкую номенклатуру специализированных микросхем и ОУ и их высокие параметры, УНЧ на транзисторах в настоящее время не потеряли своего значения. Использование современных малошумящих транзисторов, особенно в первом каскаде, позволяет создать оптимальные по параметрам и сложности усилители: малошумящие, компактные, экономичные, рас-

считанные на низковольтное питание. Поэтому транзисторные УНЧ часто оказываются хорошей альтернативой усилителям на интегральных микросхемах.

Для минимизации электрических помех целесообразно для подключения микрофона к УНЧ использовать экранированные провода минимальной длины. Электретный микрофон МЭК-3 рекомендуется монтировать непосредственно на плате первого каскада микрофонного усилителя. При необходимости значительного удаления микрофона от УНЧ следует использовать усилитель с дифференциальным входом, а подключение осуществлять витой парой проводов в экране. Экран подключается к схеме в одной точке общего провода максимально близко к первому ОУ, что обеспечивает минимизацию уровня наведенных в проводах электрических помех.

ЛИТЕРАТУРА

1. Информатика и вычислительная техника: Научно-технический сборник. — М.; 1994, № 2, 3.

2. Акустика: Справочник / А.П. Ефимов, А.В. Никонов, М.А. Сапожков, В.И. Шоров / Под ред. М.А. Сапожникова. Изд. 2-е, перераб. и доп. — М.: Радио и связь, 1989. — 336 с.

3. Сапожков М.А. Электроакустика: Учебник для вузов. — М.: Связь, 1978. — 272 с.

4. Рудометов Е.А., Рудометов В.Е. Электронные устройства двойного применения. — М.: Изд-во АСТ, 2000. — 208 с.