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

Кафедра защиты информации

**Л. М. Лыньков, Т. В. Борботько**

# *ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ*

Учебно-методическое пособие
для студентов специальностей
«Многоканальные системы телекоммуникаций»,
«Сети телекоммуникаций»
заочной формы обучения



Минск 2007

УДК 681.326.7 (075.8)
ББК 32.973 я 73
О-75

Рецензент

зав. кафедрой интеллектуальных систем БНТУ,
д-р техн. наук В. М. Колешко



**Основы** защиты информации: учеб.-метод. пособие для студ. спец. О-75 «Многоканальные системы телекоммуникаций», «Сети телекоммуникаций» заоч. формы обуч. / Л. М. Лыньков, Т. В. Борботько. – Минск : БГУИР, 2007. – 32 с.: ил.

ISBN 978-985-488-229-1

Учебно-методическое пособие содержит краткий теоретический материал по методологии информационной безопасности, техническим каналам утечки информации и защите объектов от несанкционированного доступа.

Предназначено для студентов высших учебных заведений заочной формы обучения, обучающихся по специальностям «Многоканальные системы телекоммуникаций», «Сети телекоммуникаций».

**УДК 681.326.7 (075.8)**
**ББК 32.973 я 73**

**ISBN 978-985-488-229-1**

**СОДЕРЖАНИЕ**

1. СИСТЕМНАЯ МЕТОДОЛОГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ..... 4
1.1. Основные понятия и терминология ..... 4
1.2. Классификация угроз ..... 5
1.3. Охраняемые сведения и демаскирующие признаки ..... 6

2. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ..... 8
2.1. Классификация технических каналов утечки информации ..... 8
2.2. Нежелательные излучения технических средств обработки информации .. 12
2.3. Утечка информации в волоконно-оптических линиях связи ..... 14

3. ЗАЩИТА ОБЪЕКТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ..... 17
3.1. Интегральные системы безопасности ..... 17
3.2. Противодействие техническим средствам разведки ..... 24
3.3. Методы разграничения доступа и способы их реализации ..... 26

ЛИТЕРАТУРА ..... 31

# 1. СИСТЕМНАЯ МЕТОДОЛОГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 1.1. Основные понятия и терминология

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 защиты (правовых, организационных, физических, технических, программных) информационного объекта.

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 будут рассмотрены 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;
- терминал администратора системы;
- удаленные терминалы,

или нештатными каналами доступа:

- побочным электромагнитным излучением информации с аппаратуры системы;
- побочными наводками информации на цепи электропитания и заземления;
- побочными наводками информации на вспомогательных коммуникациях;
- подключением к внешним каналам связи.

### 1.3. Охраняемые сведения и демаскирующие признаки

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

В соответствии с законом Республики Беларусь «О государственных секретах» к охраняемым сведениям могут быть отнесены сведения, несанкционированное распространение которых создает или может создать угрозу национальной безопасности Республики Беларусь, а также конституционным правам и свободам граждан.

Источниками информации об охраняемых сведениях могут быть различные характеристики объектов защиты, их элементов и создаваемых ими

физических полей. С учетом доступности этих характеристик вводят понятие демаскирующих признаков.

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

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

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

Вторичные ДП – это признаки, которые могут быть получены путем накопления и обработки первичных ДП. Примерами могут служить различного рода образцы (изображения сооружений и военной техники, диаграммы первичного и вторичного излучения объекта, амплитудно-частотные спектры излучений, химический состав вещества и т.д.), процессы (радиосигнал, акустический сигнал, зависимость какого-либо первичного ДП от времени и т.д.) и ситуации, т.е. сочетания различных образцов и процессов, связанные с охраняемыми сведениями об объекте разведки.

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

## 2. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

### 2.1. Классификация технических каналов утечки информации

Техническим каналом утечки информации называется совокупность источника конфиденциальной информации, среды распространения и средства технической разведки.


Рис. 1. Технический канал утечки информации

Каналы утечки информации можно классифицировать по физическим принципам на следующие группы (рис. 2):

- акустические;
- материально-вещественные;
- визуально-оптические;
- электромагнитные.


Рис. 2. Каналы утечки информации

В случае, когда источником информации является голосовой аппарат человека, информация называется речевой. Речевой сигнал – сложный акустический сигнал, основная энергия которого сосредоточена в диапазоне частот от 300 до 4000 Гц.

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

Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, возникают вибрационные колебания. Таким образом, в своем первоначальном состоянии речевой сигнал в помещении присутствует в виде акустических и вибрационных колебаний.

В акустических каналах утечки информации средой распространения речевых сигналов является воздух, и для их перехвата используются высокочувствительные микрофоны и специальные направленные микрофоны, которые соединяются с портативными звукозаписывающими устройствами или со специальными миниатюрными передатчиками.

Автономные устройства, конструктивно объединяющие микрофоны и передатчики, называют закладными устройствами (ЗУ) перехвата речевой информации.

Перехваченная ЗУ речевая информация может передаваться по радиоканалу, сети электропитания, оптическому каналу, соединительным линиям, посторонним проводникам, инженерным коммуникациям в ультразвуковом диапазоне частот.

В виброакустических каналах утечки информации средой распространения речевых сигналов являются ограждающие строительные конструкции помещений (стены, потолки, полы) и инженерные коммуникации (трубы водоснабжения, отопления, вентиляции и т.п.). Для перехвата речевых сигналов в этом случае используются вибродатчики (акселерометры).

По виброакустическому каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал, поэтому такие устройства часто называют радиостетоскопами. Возможно использование закладных устройств с передачей информации по оптическому каналу в ближнем инфракрасном диапазоне длин волн, а также по ультразвуковому каналу (инженерные коммуникации).

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

Некоторые элементы вспомогательных технических средств и систем (ВТСС), в том числе трансформаторы, катушки индуктивности, электромагниты вторичных электрочасов, звонков телефонных аппаратов и т.п.,

обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником речевого сигнала. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы (ЭДС), либо к модуляции токов, протекающих по этим элементам в соответствии с изменениями воздействующего акустического поля.

Акустооптический канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих под действием акустического речевого сигнала отражающих поверхностей помещений (оконных стекол, зеркал и т.д.). Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация.

Для организации такого канала предпочтительным является использование зеркального отражения лазерного луча. Однако при небольших расстояниях до отражающих поверхностей (порядка нескольких десятков метров) может быть использовано диффузное отражение лазерного излучения.

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

В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов технических средств передачи информации (ТСПИ) и ВТСС. При этом изменяется взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом. Поэтому этот канал утечки информации называется параметрическим.

Параметрический канал утечки информации может быть реализован и путем «высокочастотного облучения» помещения, где установлены закладные устройства, имеющие элементы, параметры которых (например добротность и резонансная частота объемного резонатора) изменяются под действием акустического (речевого) сигнала.

При облучении помещения мощным высокочастотным сигналом в таком закладном устройстве при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например четвертьволновым

вибратором) происходит образование вторичных радиоволн, т.е. переизлучение электромагнитного поля.

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

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

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

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

Электрический канал утечки информации возникает за счет наводок электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны.

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

Случайной антенной является цепь ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения.

В индукционном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками.

Индукционные датчики применяются в основном для съема информации с симметричных высокочастотных кабелей.

Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные высокочувствительные низкочастотные усилители, снабженные магнитными антеннами.

Параметрический электромагнитный канал может возникать в процессе облучения ТСПИ побочными электромагнитными излучениями ВТСС, вследствие чего может возникнуть переизлучение электромагнитного излучения, которое будет содержать информацию, обрабатываемую в ТСПИ.

## 2.2. Нежелательные излучения технических средств обработки информации

Технические средства, не являющиеся радиопередающими устройствами, являются источниками нежелательных электромагнитных излучений. Такие излучения называются побочными электромагнитными излучениями. Существуют различные причины их возникновения. В цепях различных устройств протекают переменные электрические токи, порождающие электромагнитные поля, излучаемые в окружающее пространство. Структура и параметры электромагнитных полей, создаваемых токоведущими элементами, определяются конструктивными особенностями систем и средств информатизации и связи, а также условиями их размещения и эксплуатации. Такие электромагнитные излучения являются потенциальными носителями опасного сигнала.

Технические средства различного назначения могут иметь в своем составе устройства, которые для выполнения своих основных функций генерируют электромагнитные колебания (эталонные и измерительные генераторы, генераторы тактовых частот, генераторы развертки электронно-лучевых трубок, гетеродины радиоприемных устройств и т.д.).

В отдельных технических средствах, например, в усилительных каскадах, могут возникать паразитные излучения, обусловленные их самовозбуждением за счет паразитных положительных обратных связей. Причины возникновения нежелательных обратных связей в усилителях могут быть различными.

Параметры элементов радиоэлектронной аппаратуры – конденсаторов, резисторов, катушек индуктивности, отрезков соединительных линий – вне полосы рабочих частот существенно отличаются от соответствующих параметров на рабочих частотах. Наличие конечной индуктивности выводов элементов, различных паразитных емкостей, проявление свойств цепей с распределенными параметрами, различные межэлементные соединения образуют большое количество паразитных колебательных систем и обратных связей, свойства которых невозможно предусмотреть и учесть заранее.

Причины возникновения нежелательных обратных связей в усилителях можно разделить на две группы. Первая группа причин связана с наличием внутренних обратных связей через усилительный прибор. Ко второй группе относят внешние обратные связи через паразитные индуктивности, емкости, цепи питания, регулировок и т.д.

К таким каналам можно отнести все виды обратной связи между входной и выходной цепями, в пределах каждого отдельного каскада, в пределах двух, трех и более каскадов. Практически напряжение с выхода усилителя на его вход может передаваться в результате действия следующих основных видов внешних обратных связей:

через емкость между выходной и входной цепями усилителя. Этот вид связи имеет место в тех случаях, когда провода входной цепи проходят рядом с проводами выходной цепи (емкость $C_1$, рис. 3), когда отсутствуют экраны между каскадами или когда они недостаточно экранированы (см. емкость $C_2$, рис. 3), когда среди монтажных проводов имеются провода, не имеющие отношения к высокоточным цепям, но связанные с ними емкостями (см. емкости $C_3$ и $C_4$, рис. 3);

- через взаимоиндуктивности между выходным и входным контурами избирательного усилителя;

- через провода питания активных элементов усилителя;

- через провода регулировок, подключенные к различным точкам усилительных каскадов;

- через шасси и корпус усилителя, являющиеся общим проводом, соединяющим ряд его точек.

В определенных условиях нежелательная обратная связь может оказаться положительной, а условия самовозбуждения – выполненными. Это приводит к возникновению паразитной генерации устройства на этой частоте, предсказать которую заранее практически невозможно.

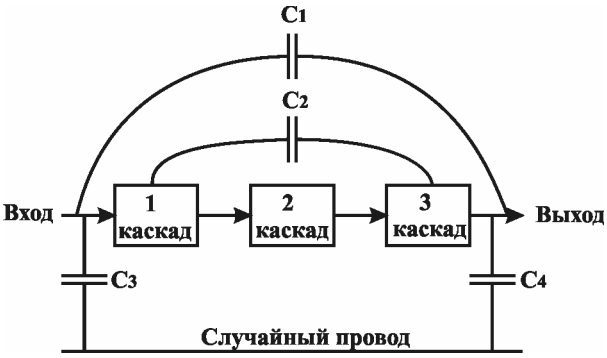



Рис. 3. Образование паразитной емкостной обратной связи в многокаскадном усилителе

Побочные излучения технических средств обработки информации могут иметь место в различных участках частотного диапазона. Низкочастотными излучателями электромагнитных колебаний являются, например, усилительные устройства различного функционального назначения и конструктивного исполнения. На более высоких частотах наблюдаются излучения гетеродинов радиоприемных устройств, измерительных генераторов, генераторов тактовых частот электронно-вычислительной техники и т.д.

Нежелательные излучения различных устройств могут содержать опасные сигналы. В процессе функционирования технических средств обработки информации элементы генераторов, усилителей и других излучающих электромагнитные поля устройств могут оказаться в зоне действия электромагнитных полей опасных сигналов. Воздействие электромагнитного поля опасного сигнала на рассматриваемые устройства может привести к изменению параметров отдельных элементов генератора или усилителя. Результатом такого изменения является паразитная модуляция опасным сигналом нежелательных излучений технических средств. Следствием этого является появление в окружающем пространстве нежелательных излучений, модулированных опасными сигналами, т.е. создаются предпосылки для утечки информации, обрабатываемой техническими средствами.

## 2.3. Утечка информации в волоконно-оптических линиях связи

Основные причины утечки информации в волоконно-оптических линиях связаны с излучением световой энергии в окружающее пространство. Причины этого излучения обусловлены процессами, происходящими при вводе (выводе) излучения в оптический волновод и распространении волн в диэлектрическом волноводе. Кроме того, утечка информации за счет оптического излучения

может иметь место из-за наличия постоянных и разъемных соединений оптических волокон, а также изгибов и повреждений этих волокон.

Рассеяние излучения при вводе оптического сигнала в интегрально-оптический волновод связано с тем, что пучок излучения используемых источников имеет заметно большую ширину, чем толщина световодного слоя волновода. Эффективность ввода излучения источника в световод зависит от степени согласования следующих характеристик: сечения и расходимости светового пучка с геометрическими размерами сердцевины и апертурного угла световода, количества волноводных мод и т.д. Увеличение эффективности ввода излучения в световод достигается применением оптического клея, микролинз и других средств фокусировки излучения. Наибольшее влияние на эффективность ввода излучения источника в световод оказывает поперечное рассогласование, меньшее – продольное и угловое.

В диэлектрическом волноводе толщиной порядка длины распространяющейся в нем волны (l–10 мкм) в зависимости от соотношения показателей преломления волноводного слоя (сердцевины), оболочки и покровного слоя, а также от угла падения световой волны на границе раздела волна может либо канализироваться в волноводном слое (распространяться вдоль волокна путем многократных отражений от границы сердцевина–оболочка (луч 1, рис. 4), либо проникать в оболочку, распространяться вдоль нее и далее выходить в окружающую среду (см. лучи 2, 3, рис. 4).

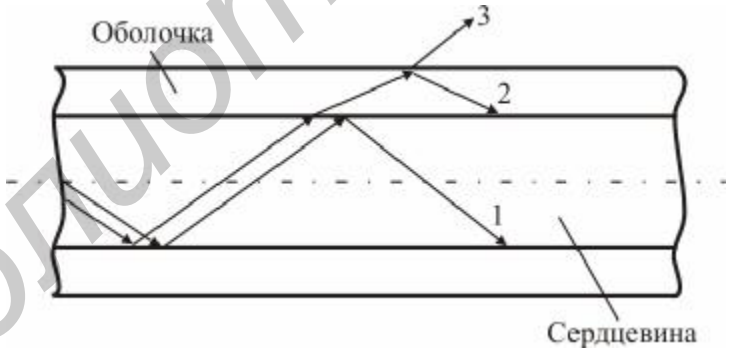


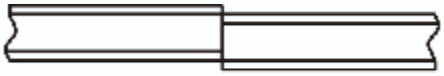

Рис. 4. Распространение оптической волны в диэлектрическом волноводе

В прямолинейных световодах излучение в окружающую среду незначительно. Однако в местах изгибов волноводов интенсивность излучения в оболочку или воздух увеличивается и тем больше, чем сильнее эти изгибы. Интенсивность излучения в окружающее пространство увеличивается и при повреждении оболочки световода.

Постоянные соединения отрезков оптических волокон между собой осуществляют свариванием, сплавлением или склеиванием в юстировочном

устройстве. Оптические разъемы (соединители) должны допускать многократные соединения-разъединения оптических волокон. Рассогласование волокон возникает из-за имеющихся различий в числовой апертуре, профиле показателя преломления, диаметре сердцевины или из-за погрешностей во взаимной ориентации волокон при их соединении. Основными причинами излучения световой энергии в окружающее пространство в местах соединения оптических волокон являются:

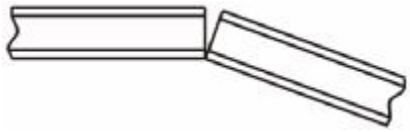
- смещение (осевое несовмещение) стыкуемых волокон (рис. 5, а);
- наличие зазора между торцами стыкуемых волокон (рис. 5, б);
- непараллельность торцевых поверхностей стыкуемых волокон (рис. 5, в);
- угловое рассогласование осей стыкуемых волокон (рис. 5, г);
- различие в диаметрах стыкуемых волокон (рис. 5, д).



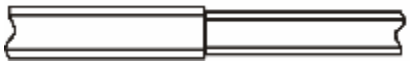
а) смещение стыкуемых волокон

б) наличие зазора между торцами стыкуемых волокон

в) непараллельность торцевых поверхностей стыкуемых волокон



г) угловое рассогласование осей стыкуемых волокон



д) различие в диаметрах стыкуемых волокон

Рис. 5. Внешний вид соединений оптических волокон, вызывающих излучение световой энергии в окружающее пространство

Наиболее интенсивное излучение в окружающее пространство наблюдается при наличии сдвига соединяемых волокон относительно друг друга.

# 3. ЗАЩИТА ОБЪЕКТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

## 3.1. Интегральные системы безопасности

Под интегральной безопасностью понимается такое состояние условий функционирования человека, объектов и технических средств, при котором они надежно защищены от всех возможных видов угроз в ходе непрерывного процесса подготовки, хранения, передачи и обработки информации.

Интегральная безопасность информационных систем включает в себя следующие составляющие:

- физическая безопасность (защита зданий, помещений, подвижных средств, людей, а также аппаратных средств – компьютеров, носителей информации, сетевого оборудования, кабельного хозяйства, поддерживающей инфраструктуры);
- безопасность связи (защита каналов связи от внешних воздействий любого рода);
- безопасность программного обеспечения (защита от вирусов, логических бомб, несанкционированного изменения конфигурации);
- безопасность данных (обеспечение конфиденциальности, целостности и доступности данных).

Интегральный подход основан на объединении различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами
данных.

Понятие интегральной безопасности предполагает обязательную непрерывность процесса обеспечения безопасности как во времени, так и в пространстве (по всему технологическому циклу деятельности) с обязательным учетом всех возможных видов угроз (несанкционированный доступ, съем информации, терроризм, пожар, стихийные бедствия и т.п.).

Современный комплекс защиты территории охраняемых объектов должен включать в себя следующие основные компоненты:

- механическая система защиты;
- система оповещения о попытках вторжения;
- оптическая (обычно телевизионную) система опознавания нарушителей;
- оборонительная система (звуковую и световую сигнализацию, применение в случае необходимости оружия);

- связная инфраструктура;

- центральный пост охраны, осуществляющий сбор, анализ, регистрацию и отображение поступающих данных, а также управление периферийными устройствами;

- персонал охраны (патрули, дежурные на центральном посту).

**Механические системы защиты**

Основой любой механической системы зашиты являются механические или строительные элементы, создающие для лица, пытающегося проникнуть на охраняемую территорию, реальное физическое препятствие. Важнейшей характеристикой механической системы защиты является время сопротивления, то есть время, которое требуется злоумышленнику для ее преодоления. Исходя из требуемой величины названной характеристики должен производиться и выбор типа механической системы защиты.

Как правило, механическими или строительными элементами служат стены и ограды. Если позволяют условия, могут применяться рвы и ограждения из колючей проволоки.

При использовании многорядных механических систем защиты датчики оповещения о попытке вторжения целесообразно располагать между внутренним и внешним ограждением. При этом внутреннее ограждение должно обладать повышенным временем сопротивления.

**Системы оповещения**

В современных системах оповещения (системах тревожной сигнализации) о попытках вторжения на охраняемую территорию находят применение датчики нескольких типов.

В системах защиты периметра территории без ограды используются микроволновые, инфракрасные, емкостные, электрические и магнитные датчики.

С помощью датчиков первых двух типов формируется протяженная контрольная зона барьерного типа. Действие систем с микроволновыми датчиками основывается на контроле интенсивности высокочастотного направленного излучения передатчика, которое воспринимается приемником. Срабатывание сигнализации происходит при прерывании этого направленного излучения. Ложные срабатывания могут быть обусловлены перемещением в контролируемой зоне животных, воздействием растительности, атмосферных

осадков, передвижением транспортных средств, а также воздействием посторонних передатчиков.

При использовании инфракрасных систем оповещения между передатчиком и приемником появляется монохроматическое световое излучение в невидимой области спектра. Срабатывание сигнализации происходит при прерывании одного или нескольких световых лучей. Ложные срабатывания могут быть обусловлены перемещением в контролируемой зоне животных, сильным туманом или снегопадом.

Принцип действия емкостной системы оповещения основывается на формировании электростатического поля между параллельно расположенными так называемыми передающими и воспринимающими проволочными элементами специального ограждения. Срабатывание сигнализации происходит при регистрации определенного изменения электростатического поля, имеющего место при приближении человека к элементам ограждения. Ложные срабатывания могут быть обусловлены перемещением животных, воздействием растительности, обледенением элементов ограждения, атмосферными воздействиями или загрязнением изоляторов.

Электрические системы оповещения базируются на использовании специального ограждения с токопроводящими проволочными элементами. Критерием срабатывания сигнализации является регистрация изменений электрического сопротивления токопроводящих элементов при прикосновении к ним. Ложные срабатывания могут быть вызваны животными, растительностью или загрязнением изоляторов.

Принцип действия систем с магнитными датчиками предполагает контроль параметров магнитного поля. Срабатывание сигнализации происходит при регистрации искажений, которые обусловлены появлением в зоне действия датчиков предметов из ферромагнитного материала. Ложное срабатывание может иметь место из-за изменений характеристик почвы, обусловленных, например, продолжительным дождем.

При наличии механической системы защиты территории (например ограды, расположенной по периметру) находят применение системы оповещения с вибрационными датчиками, датчиками звука, распространяющегося по твердым телам, акустическими датчиками, электрическими переключателями, а также системы с электрическими проволочными петлями.

Вибрационные датчики закрепляются непосредственно на элементах ограды. Срабатывание сигнализации происходит при появлении на выходе датчиков сигналов, которые обусловлены вибрациями элементов ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем или градом.

Датчики звука также устанавливаются непосредственно на элементы ограды и контролируют распространение по ним звуковых колебаний. Срабатывание сигнализации происходит при регистрации так называемых шумов прикосновения к элементам ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем, градом или срывающимися с элементов ограды сосульками.

Действие систем с электрическими переключателями основано на регистрации изменения состояния переключателей, вмонтированных в ограду, которое происходит при соответствующем изменении натяжения проволочных элементов или нагрузки на направляющие трубки ограды. Ложные срабатывания сигнализации могут быть вызваны очень сильным ветром при недостаточном натяжении элементов ограды.

Для контроля участков почвы по периметру охраняемой территории находят применение системы оповещения с датчиками звука, распространяющегося по твердым телам, а также с датчиками давления.

В системах первого типа регистрируются звуковые, сейсмические колебания. Срабатывание сигнализации происходит при регистрации сотрясений почвы, например, ударного шума. Ложные срабатывания могут быть обусловлены перемещением достаточно крупных животных, движением транспорта вблизи охраняемой территории.

В системах второго типа используются пневматические или емкостные датчики давления, позволяющие регистрировать изменения нагрузки на почву. Срабатывание сигнализации происходит при регистрации соответствующего роста давления, например, ударного. Ложные срабатывания возможны из-за перемещений достаточно крупных животных, разгерметизации пневматических датчиков или коррозии.

### Системы опознавания

Обязательным условием надежного функционирования всего комплекса защиты охраняемой территории является последующий анализ поступающих сообщений о проникновении для точного определения их вида и причин

появления. Названное условие может быть выполнено посредством использования систем опознавания.

Наиболее широкое распространение в подобных системах получили телевизионные установки дистанционного наблюдения. Несомненно, что объект со стационарными постами охраны обладает более высокой защищенностью, однако при этом значительно возрастают затраты на его охрану. Так, при необходимости круглосуточного наблюдения требуется трехсменная работа персонала охраны. В этих условиях телевизионная техника становится средством повышения эффективности работы персонала охраны, прежде всего при организации наблюдения в удаленных, опасных или труднодоступных зонах.

Вся контролируемая системой оповещения зона разграничивается на отдельные участки протяженностью не более 100 м, на которых устанавливается по крайней мере одна передающая телекамера. При срабатывании датчиков системы оповещения, установленных на определенном участке контролируемой зоны, изображение, передаваемое соответствующей телекамерой, автоматически выводится на экран монитора на центральном посту охраны. Кроме того, при необходимости должно быть обеспечено дополнительное освещение данного участка. Немаловажно, чтобы внимание дежурного охранника было быстрее привлечено к выведенному на экран монитора изображению.

Фактические причины срабатывания сигнализации во многих случаях могут быть идентифицированы только при условии достаточно высокой оперативности дежурного охранника. Важно, что данное положение прежде всего имеет место при действительных попытках вторжения на охраняемую территорию и при преднамеренных обманных действиях злоумышленников. Одним из перспективных путей выполнения выше сформулированного условия является применение устройства видеопамяти, которое обеспечивает автоматическую запись изображения сразу же после срабатывания сигнализации. При этом дежурному охраннику предоставляется возможность вывести из устройства памяти на экран монитора первые кадры изображения и идентифицировать причину срабатывания датчиков системы оповещения.

Отличительной особенностью некоторых объектов является их большая протяженность. Большое количество площадок таких объектов может быть расположено на значительном удалении друг от друга, что серьезно удорожает монтаж и эксплуатацию оборудования. В этих случаях можно применить

систему малокадрового телевидения типа Slowscan. Она функционирует на больших дальностях, имеет невысокую стоимость и совместима с любой существующей замкнутой телевизионной системой, которая уже установлена на объекте. Для передачи видеокадров и команд в этой системе используется телефонная сеть общего пользования.

Особые преимущества в системах охраны имеют камеры на приборах с зарядовой связью (ПЗС). По сравнению с обычными трубочными камерами они обладают меньшими габаритами, более высокой надежностью, практически не нуждаются в техническом обслуживании, отлично работают в условиях низкой освещенности, обладают чувствительностью в инфракрасной области спектра. Однако наиболее важным является то, что видеоинформация на чувствительном элементе указанной камеры сразу представлена в цифровой форме и без дополнительных преобразований пригодна для дальнейшей обработки. Это дает возможность легко идентифицировать различия или изменения элементов изображения, реализовать в камере встроенный датчик перемещений. Подобная камера со встроенным детектором и маломощным ИК-осветителем может вести наблюдение охраняемой территории и при появлении нарушителя в поле зрения распознавать изменения элементов изображения и подавать сигнал тревоги.

### Оборонительные системы

Для предотвращения развития вторжения на охраняемую территорию используется оборонительная система, в которой находят применение осветительные или звуковые установки. В обоих случаях субъект, пытающийся проникнуть на охраняемую территорию, информируется о том, что он обнаружен охраной. Таким образом, на него оказывается целенаправленное психологическое воздействие. Кроме того, использование осветительных установок обеспечивает благоприятные условия для действий охраны.

Для задержания преступника охрана предпринимает соответствующие оперативные меры или вызывает милицию (полицию). Если злоумышленнику удалось скрыться, то для успеха последующего расследования важное значение приобретает информация, которая может быть получена с помощью рассмотренной выше системы опознавания.

### Связная инфраструктура

Современный рынок технических средств предоставляет разработчикам широкие возможности выбора аппаратуры и каналов связи. Однако с учетом

интегрального подхода в качестве связной инфраструктуры целесообразно использовать структурированные кабельные системы.

**Центральный пост и персонал охраны**

Сложные комплексы защиты охраняемых территорий, состоящие, как правило, из нескольких систем, могут эффективно функционировать только при условии, что работа всех технических установок постоянно контролируется и управляется с центрального поста охраны. Учитывая повышенную психологическую нагрузку на дежурных охранников центрального поста, необходимость оперативной выработки и реализации оптимальных решений в случае тревоги, к центральным устройствам комплексов защиты предъявляются особые требования. Так, они должны обеспечивать автоматическую регистрацию и отображение всех поступающих в центральный пост сообщений и сигналов тревоги, выполнение всех необходимых процедур. Важную роль играет и уровень эргономики аппаратуры, которой оснащаются рабочие места дежурных охранников.


Рис. 6. Структурная схема интегральной системы безопасности объекта

### Интегральный комплекс физической защиты

На рис. 6 представлена блок-схема интегрального комплекса физической защиты объекта, обеспечивающего функционирование всех рассмотренных выше систем. Отличительной особенностью подобных комплексов является интеграция различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных.

Необходимо отметить, что в рассматриваемой блок-схеме технические средства скомпонованы по системам достаточно условно для того, чтобы схема приобрела более логичную форму и была бы более понятна. На самом деле одни и те же средства выполняют различные функции для разных систем обеспечения безопасности.

## 3.2. Противодействие техническим средствам разведки

Противодействие техническим средствам разведки (ТСР) представляет собой совокупность согласованных мероприятий, предназначенных для исключения или существенного затруднения добывания охраняемых сведений с помощью технических средств.

Добывание информации предполагает наличие информационных потоков от физических носителей охраняемых сведений к системе управления. При использовании ТСР такие информационные потоки образуются за счет перехвата и анализа сигналов и полей различной физической природы. Источниками информации для технической разведки являются содержащие охраняемые сведения объекты. Это позволяет непосредственно влиять на качество добываемой злоумышленником информации и в целом на эффективность его деятельности путем скрытия истинного положения и навязывания ложного представления об охраняемых сведениях.

Искажение или снижение качества получаемой информации непосредственно влияет на принимаемые злоумышленником решения и через его систему управления – на способы и приемы исполнения решения. Непосредственный контакт принципиально необходим на этапах добывания информации и исполнения решения, причем добывание информации должно предшествовать принятию решения и его исполнению злоумышленником. Поэтому противодействие ТСР должно носить упреждающий характер и реализовываться заблаговременно.

Любая система технической разведки (рис. 7) содержит следующие основные элементы:

- технические средства разведки (ТСР);
- каналы передачи информации (КПИ);
- центры сбора и обработки информации (ЦСОИ).

Технические средства разведки представляют собой совокупность разведывательной аппаратуры, предназначенной для обнаружения демаскирующих признаков, предварительной обработки, регистрации перехваченной информации и ее передачи через КПИ в ЦСОИ. В ЦСОИ информация от различных ТСР накапливается, классифицируется, анализируется и предоставляется потребителям (автоматизированным системам управления или лицам, принимающим решения. Таким образом, в системе технической разведки реализуется обнаружение и анализ демаскирующих признаков (ДП).

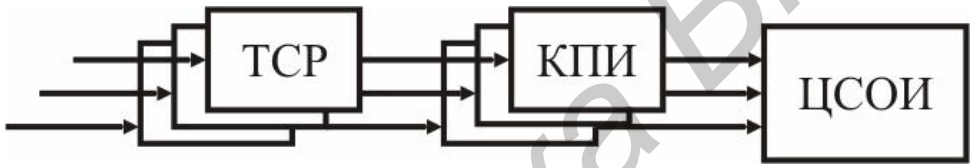



Рис. 7. Упрощенная структурная схема системы технической разведки

Обнаружение ДП по физической сути заключается в выполнении следующих операций:

- поиск и обнаружение энергии ДП в пространстве, во времени, по спектру и т.д.;
- выделение ДП из искусственных и естественных помех.

Физический смысл анализа ДП раскрывают следующие операции:

- разделение ДП различных объектов;
- оценка параметров ДП (определение их объективных характеристик);
- сокращение избыточности информации;
- регистрация, накопление и классификация ДП;
- нахождение местоположения источника ДП;
- распознавание смыслового содержания ДП;
- выявление охраняемых сведений.

В соответствии с приведенной классификацией главными направлениями снижения эффективности ТСР являются противодействие обнаружению ДП и противодействие их анализу.

При противодействии обнаружению ДП преследуется цель скрытия от ТСР демаскирующих признаков. Соответственно все организационные и технические способы, предназначенные для исключения или существенного затруднения обнаружения ДП, составляют одно из главных направлений противодействия ТСР – скрытие.

Другим основным направлением является техническая дезинформация, которая объединяет все организационно-технические меры противодействия, направленные на затруднение анализа ДП и навязывание противнику ложной информации.

Скрытие, обеспечивая противодействие обнаружению, всегда затрудняет или исключает возможность проведения анализа демаскирующего признака. Техническая дезинформация, наоборот, затрудняя анализ, как правило, не влияет на возможность обнаружения объекта разведки.

Некоторые ТСР предназначены для обеспечения активного воздействия на любые объекты, чьи сигналы оказываются в заданных диапазонах поиска и обнаружения. Техническая дезинформация в такой ситуации может оказаться неэффективной. Поэтому реализация стратегии скрытия объекта является более радикальным направлением противодействия ТСР, чем техническая дезинформация.

Однако на практике часто встречаются ситуации, когда невозможно обеспечить при ограниченных ресурсах надежное скрытие объекта (например крупного здания или сооружения) или отдельных демаскирующих признаков (таких, как мощные непрерывные электромагнитные излучения радиоэлектронных и оптических систем на открытой местности). В подобных ситуациях цели противодействия техническим средствам разведки могут достигаться только применением методов и средств технической дезинформации.

Кроме рассмотренных мер ПД ТСР, предполагающих нормальное функционирование всех составных частей системы разведки, возможно проведение активных действий по выявлению и выведению из строя элементов системы разведки.

### 3.3. Методы разграничения доступа и способы их реализации

Основными функциями системы разграничения доступа (СРД) являются:

- реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;

- реализация ПРД субъектов и их процессов к устройствам создания твердых копий;

- изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;

- управление потоками данных в целях предотвращения записи данных на носители несоответствующего грифа;

- реализация правил обмена данными между субъектами для автоматизированных систем (АС) и средств вычислительной техники, построенных по сетевым принципам.

Функционирование СРД опирается на выбранный способ разграничения доступа. Наиболее прямой способ гарантировать защиту данных – это предоставить каждому пользователю вычислительную систему как его собственную. В многопользовательской системе похожих результатов можно добиться использованием модели виртуальной ЭВМ.

При этом каждый пользователь имеет собственную копию операционной системы. Монитор виртуального персонального компьютера для каждой копии операционной системы будет создавать иллюзию, что никаких других копий нет и что объекты, к которым пользователь имеет доступ, являются только его объектами. Однако при разделении пользователей неэффективно используются ресурсы АС.

В АС, допускающих совместное использование объектов доступа, существует проблема распределения полномочий субъектов по отношению к объектам. Наиболее полной моделью распределения полномочий является матрица доступа. Матрица доступа является абстрактной моделью для описания системы предоставления полномочий.

Строки матрицы соответствуют субъектам, а столбцы – объектам; элементы матрицы характеризуют право доступа (читать, добавлять информацию, изменять информацию, выполнять программу и т.д.). Чтобы изменять права доступа, модель может, например, содержать специальные права владения и управления. Если субъект владеет объектом, он имеет право изменять права доступа других субъектов к этому объекту. Если некоторый субъект управляет другим субъектом, он может удалить права доступа этого субъекта или передать свои права доступа этому субъекту. Для того чтобы реализовать функцию управления, субъекты в матрице доступа должны быть также определены в качестве объектов.

Элементы матрицы установления полномочий (матрицы доступа) могут содержать указатели на специальные процедуры, которые должны выполняться при каждой попытке доступа данного субъекта к объекту, и принимать решение о возможности доступа. Основами таких процедур могут служить следующие правила:

- решение о доступе основывается на истории доступов других объектов;
- решение о доступе основывается на динамике состояния системы (права доступа субъекта зависят от текущих прав других субъектов);
- решение о доступе основывается на значении определенных внутрисистемных переменных, например значений времени и т.п.

В наиболее важных АС целесообразно использование процедур, в которых решение принимается на основе значений внутрисистемных переменных (время доступа, номера терминалов и т.д.), так как эти процедуры сужают права доступа.

Матрицы доступа реализуются обычно двумя основными методами – либо в виде списков доступа, либо мандатных списков. Список доступа приписывается каждому объекту, и он идентичен столбцу матрицы доступа, соответствующей этому объекту. Списки доступа часто размещаются в словарях файлов. Мандатный список приписывается каждому субъекту, и он равносилен строке матрицы доступа, соответствующей этому субъекту. Когда субъект имеет права доступа по отношению к объекту, то пара (объект – права доступа) называется мандатом объекта.

На практике списки доступа используются при создании новых объектов и определении порядка их использования или изменении прав доступа к объектам. С другой стороны, мандатные списки объединяют все права доступа субъекта. Когда, например, выполняется программа, операционная система должна быть способна эффективно выявлять полномочия программы. В этом случае списки возможностей более удобны для реализации механизма предоставления полномочий.

Некоторые операционные системы поддерживают как списки доступа, так и мандатные списки. В начале работы, когда пользователь входит в сеть или начинает выполнение программы, используются только списки доступа. Когда субъект пытается получить доступ к объекту в первый раз, список доступа анализируется и проверяются права субъекта на доступ к объекту. Если права есть, то они приписываются в мандатный список субъекта и права доступа проверяются в дальнейшем проверкой этого списка.

При использовании обоих видов списков список доступа часто размещается в словаре файлов, а мандатный список – в оперативной памяти, когда субъект активен. С целью повышения эффективности в техническом обеспечении может использоваться регистр мандатов.

Третий метод реализации матрицы доступа – так называемый механизм замков и ключей. Каждому субъекту приписывается пара (А, К), где А – определенный тип доступа, а К – достаточно длинная последовательность символов, называемая замком. Каждому субъекту также предписывается последовательность символов, называемая ключом. Если субъект захочет получить доступ типа А к некоторому объекту, то необходимо проверить, что субъект владеет ключом к паре (А, К), приписываемой конкретному объекту.

К недостаткам применения матриц доступа со всеми субъектами и объектами доступа можно отнести большую размерность матриц. Для уменьшения размерности матриц установления полномочий применяют различные методы сжатия:

- установление групп пользователей, каждая из которых представляет собой группу пользователей с идентичными полномочиями;
- распределение терминалов по классам полномочий;
- группировка элементов защищаемых данных в некоторое число категорий с точки зрения безопасности информации (например по уровням конфиденциальности).

По характеру управления доступом системы разграничения разделяют на дискреционные и мандатные.

Дискреционное управление доступом дает возможность контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам и т.п.). Например, владельцам объектов предоставляется право ограничивать доступ к этому объекту других пользователей. При таком управлении доступом для каждой пары (субъект–объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта к данному объекту. Однако имеются и другие задачи управления доступом, которые не могут быть решены только дискреционным управлением. Одна из таких задач – позволить администратору АС контролировать формирование владельцами объектов списков управления доступом.

Мандатное управление доступом позволяет разделить информацию на некоторые классы и управлять потоками информации при пересечениях границ этих классов.

Во многих системах реализуется как мандатное, так и дискреционное управление доступом. При этом дискреционные правила разграничения доступа являются дополнением мандатных. Решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должны контролироваться не только единичный акт доступа, но и потоки информации.

Обеспечивающие средства для системы разграничения доступа выполняют следующие функции:

- идентификация и опознавание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
- регистрация действий субъекта и его процесса;
- предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- реакция на попытки НСД, например, сигнализацию, блокировку, восстановление системы защиты после НСД;
- тестирование всех функций защиты информации специальными программными средствами;
- очистка оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными путем двукратной произвольной записи;
- учет выходных печатных и графических форм и твердых копий в АС;
- контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

Для каждого события должна регистрироваться следующая информация: дата и время; субъект, осуществляющий регистрируемое действие; тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа); успешно ли осуществилось событие (обслужен запрос на доступ или нет).

Выдача печатных документов должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе общего количества листов (страниц). Вместе с выдачей документа может автоматически оформляться учетная карточка документа с указанием даты выдачи документа,

учетных реквизитов документа, краткого содержания (наименования, вида, шифра кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа.

Автоматическому учету подлежат создаваемые защищаемые файлы, каталоги, тома, области оперативной памяти персонального компьютера, выделяемые для обработки защищаемых файлов, внешних устройств и каналов связи.

## ЛИТЕРАТУРА

1. Ярочкин, В. И. Информационная безопасность: учеб. для вузов / В. И. Ярочкин. – изд. 2-е. – Минск : Академический проект, 2005. – 544 с.

2. Бузов, Г. А. Защита от утечки информации по техническим каналам: учеб. пособие для подготовки экспертов системы Гостехкомиссии России / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев – М.: Горячая линия - Телеком, 2005. – 416 с.

3. Конеев, И. Р. Информационная безопасность предприятия / И. Р. Конев. – СПб. : БХВ-Петербург, 2003. – 752 с.

4. Галатенко, В. А. Основы информационной безопасности: курс лекций / В. А. Галатенко. – М.: Интернет-Университет Информационных Технологий, 2003. – 280 с.

Св. план 2007, поз. 108

Учебное издание

**Лыньков** Леонид Михайлович
**Борботько** Тимофей Валентинович

# *ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ*

Учебно-методическое пособие
для студентов специальностей
«Многоканальные системы телекоммуникаций»,
«Сети телекоммуникаций»
заочной формы обучения

Редактор Т. П. Андрейченко
Корректор Е. Н. Батурчик
Компьютерная верстка Е. Г. Реут

---

| | | |
|---|---|---|
| Подписано в печать 19.11.2007. | Формат 60x84 1/16. | Бумага офсетная. |
| Гарнитура «Таймс». | Печать ризографическая. | Усл. печ. л. 1,98. |
| Уч.-изд. л. 1,7. | Тираж 100 экз. | Заказ 385. |

---

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0056964 от 01.04.2004. ЛП №02330/0131666 от 30.04.2004.
220013, Минск, П. Бровки, 6