МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет» (ЮЗГУ)

Кафедра «Информационная безопасность»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_6_» _____ 2017 г.

Комплексное обеспечение информационной безопасности инфокоммуникационных систем

Методические указания к практическим занятиям для студентов укрупненной группы специальностей 10.00.00.

Курск 2017

УДК 004
Составители: М.О. Таныгин, И.В. Калуцкий, А.А. Чеснокова

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности *А.Г. Спеваков*

Комплексное обеспечение информационной безопасности инфокоммуникационных систем: методические указания к практическим занятиям для студентов укрупненной группы специальностей 10.00.00/ Юго-Зап. гос. ун-т; сост.:, М.О. Таныгин И.В. Калуцкий, А.А. Чеснокова, Курск, 2017. 48 с.: ил. 1, табл. 17. Библиогр.: с. 48.

Содержат сведения по вопросам комплексной защиты информации.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Комплексная защита объектов информатизации», «Информационная безопасность», «Информационная безопасность автоматизированных систем», «Информационная безопасность телекоммуникационных систем».

Предназначены для укрупненной группы специальностей 10.00.00

Текст печатается в авторской редакции

Подписано в печать 6.12.17 . Формат 60x84 1/16.
Усл. печ. л. 2,79 . Уч. –изд. л. 2,53 . Тираж 50 экз. Заказ 2384
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Оглавление

ВВЕДЕНИЕ

Одним из основных направлений обеспечения информационной безопасности является комплексная защита информации, которая объективно приобретает все больший вес.

Такая тенденция обусловлена развитием методов и средств добывания информации, позволяющих несанкционированно получать большой объём информации на безопасном расстоянии от источников, огромными достижениями микроэлектроники по выпуску доступных средств нелегального добывания информации, а также достаточно высокими темпами информатизации предприятий и в целом всего общества.

Очевидно, что эффективная защита информации с учетом этих тенденций возможна при более широком использовании технических средств защиты, что предполагает наличие профессиональных знаний и специальных навыков работы с контрольно-измерительной аппаратурой.

1. Теоретический материал. Классификация и краткая характеристика технических каналов утечки информации

Информация может быть представлена в различной форме и на различных физических носителях. Основными формами информации, представляющими интерес с точки зрения защиты, являются:

- документальная;
- акустическая (речевая);
- телекоммуникационная и т.п.

Документальная информация содержится в графическом или буквенно-цифровом виде на бумаге, а также в электронном виде на магнитных и других носителях. Особенность документальной информации в том, что она в сжатом виде содержит сведения, подлежащие защите.

Речевая информация возникает в ходе ведения в помещениях разговоров, а также при работе систем звукоусиления и звуковоспроизведения.

Носителем речевой информации являются акустические колебания (механические колебания частиц упругой среды, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины).

Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 200...300 Гц до 4...6 КГц.

Телекоммуникационная информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче. Носителем информации при ее обработке техническими средствами и передаче по проводным каналам связи является электрический ток, а при передаче по радио и оптическому каналам – электромагнитные волны.

Основными объектами защиты информации являются:

- информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение),

автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звукосопровождение, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), их информативные физические поля. То есть системы и средства, непосредственно обрабатывающие информацию, отнесенную к государственной тайне, а также конфиденциальную информацию. Эти средства и системы часто называют техническими средствами приема, обработки, хранения и передачи информации (ТСПИ);

- технические средства и системы, не относящиеся к средствам и системам информатизации (ТСПИ), но размещенные в помещениях, в которых обрабатывается секретная и конфиденциальная информация. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся : технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, радиотрансляции, часофикации, электробытовые приборы и т.д., а также сами помещения, предназначенные для обработки информации ограниченного распространения.

При организации защиты информации ТСПИ необходимо рассматривать как систему, включающую основное (стационарное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ТСПИ и их элементами), распределительные и коммутационные устройства, системы электропитания, системы заземления.

Отдельные технические средства или группа технических средств, предназначенных для обработки конфиденциальной информации, вместе с помещениями, в которых они размещаются, составляют **объект ТСПИ.** Под объектами ТСПИ понимают также выделенные помещения, предназначенные для проведения закрытых мероприятий.

В качестве элементов каналов утечки информации наибольший интерес представляют ТСПИ и ВТСС, имеющие выход за пределы **контролируемой зоны** (КЗ), т.е. зоны, в которой

исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков.

Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются **посторонними проводниками.**

Зона, в которой возможны перехват (с помощью разведывательного приемника) побочных электромагнитных излучений и последующая расшифровка содержащейся в них информации (т.е. зона, в пределах которой отношение "информационный сигнал/помеха" превышает допустимое нормированное значение), называется (опасной) **зоной 2**.

Пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, называется опасной **зоной 1**.

Случайной антенной является цепь ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения. Случайные антенны могут быть сосредоточенными и распределенными.

Сосредоточенная случайная антенна представляет собой компактное техническое средство, например, телефонный аппарат, громкоговоритель радиотрансляционной сети и т.д. К **распределенным случайным антеннам** относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

Перехват информации, обрабатываемой на объектах ТСПИ, осуществляется по техническим каналам.

Под **техническим каналом утечки информации (ТКУИ)** понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути, под ТКУИ понимают **способ получения с помощью ТСР разведывательной информации** об объекте. Причем под **разведывательной информацией** обычно

понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления.

Сигналы являются материальными носителями информации. По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими и т.д. То есть сигналами, как правило, являются электромагнитные, механические и другие виды колебаний (волн), причем информация содержится в их изменяющихся параметрах.

В зависимости от природы сигналы распространяются в определенных физических средах. В общем случае средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды. Например, воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт (земля) и т.п.

Для приема и измерения параметров сигналов служат технические средства разведки (ТСР).

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата ТСР технические каналы утечки можно разделить на:

электромагнитные, электрические и параметрические - для телекоммуникационной информации;

воздушные (прямые акустические), вибрационные (виброакустические), электроакустические, оптико-электронный и параметрические – для речевой информации.

К электромагнитным каналам утечки информации относятся:

- перехват побочных электромагнитных излучений (ПЭМИ) элементов ТСПИ;
- перехват ПЭМИ на частотах работы высокочастотных (ВЧ) генераторов в ТСПИ и ВТСС;
- перехват ПЭМИ на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио- и радиотехнической разведки, размещенными вне контролируемой зоны.

Электрические каналы утечки информации включают:

- съем наводок ПЭМИ ТСПИ с соединительных линий ВТСС и посторонних проводников;

- съем информационных сигналов с линий электропитания ТСПИ;
- съем информационных сигналов с цепей заземления ТСПИ и ВТСС;
- съем информации путем установки в ТСПИ электронных устройств перехвата информации.

Перехват информационных сигналов по электрическим каналам утечки возможен путем непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам, проходящим через помещения, где установлены ТСПИ, а также к системам электропитания и заземления ТСПИ. Для этих целей используются специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура.

Электронные устройства перехвата информации, устанавливаемые в ТСПИ, часто называют **аппаратными закладками.** Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Наиболее часто закладки устанавливаются в ТСПИ иностранного производства, однако возможна их установка и в отечественных средствах.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а уже затем по команде передается на запросивший ее объект.

Параметрический канал утечки информации образуется путем "высокочастотного облучения" ТСПИ.

Для перехвата информации по данному каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности, и специальные радиоприемные устройства.

В воздушных (прямых акустических) технических каналах утечки информации средой распространения акустических сигналов является воздух. Для перехвата акустических сигналов в качестве датчиков средств разведки используются микрофоны. Сигналы, поступающие с микрофонов, или непосредственно записываются на специальные портативные устройства звукозаписи, или передаются с использованием специальных передатчиков в пункт приема, где осуществляется их запись.

Для перехвата акустической (речевой) информации используются:

- портативные диктофоны и проводные микрофонные системы скрытой звукозаписи;
- направленные микрофоны;
- акустические радио закладки (передача информации по радиоканалу);
- акустические сетевые закладки (передача информации по сети электропитания 220 В);
- акустические ИК-закладки (передача информации по оптическому каналу в ИК- диапазоне длин волн);
- акустические телефонные закладки (передача информации по телефонной линии на высокой частоте);
- акустические телефонные закладки типа "телефонное ухо" (передача информации по телефонной линии "телефону-наблюдателю" на низкой частоте).

В вибрационных (виброакустических) технических каналах утечки информации средой распространения акустических сигналов являются ограждения конструкций зданий, сооружений (стены, потолки, полы), трубы водоснабжения, канализации и другие твердью тела.

Для перехвата акустических колебаний в этом случае используются средства разведки с контактными микрофонами:

- электронные стетоскопы;
- радио стетоскопы (передача информации по радиоканалу).

Электроакустические технические каналы утечки информации возникают за счет преобразований акустических сигналов в электрические (электроакустических преобразований) и включают перехват акустических колебаний через ВТСС, обладающие "микрофонным эффектом", а также путем **"высокочастотного навязывания".**

Перехват акустических колебаний в данном канале утечки информации осуществляется путем **непосредственного подключения** к соединительным линиям ВТСС, обладающих "микрофонным эффектом", специальных высокочувствительных **низкочастотных усилителей.** Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать

разговоры, ведущиеся в помещениях, где установлены эти аппараты.

Технический канал утечки информации путем **"высокочастотного навязывания"** может быть осуществлен путем несанкционированного контактного введения токов высокой частоты от **генератора,** подключенного в линию (цепь), имеющую функциональную связь с нелинейными или параметрическими элементами ВТСС, на которых происходит модуляция высокочастотного сигнала информационным. Информационный сигнал в данных элементах ВТСС появляется вследствие электроакустического преобразования акустических сигналов в электрические. В силу того, что нелинейные или параметрические элементы ВТСС для высокочастотного сигнала, как правило, представляют собой несогласованную нагрузку, промодулированный высокочастотный сигнал будет отражаться от нее и распространяться в обратном направлении по линии или излучаться. Для приема излученных или отраженных высокочастотных сигналов используется **специальные приемники** с достаточно высокой чувствительностью.

Оптико-электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол окон, картин, зеркал и т.д.). Для перехвата речевой информации по данному каналу используются сложные лазерные акустические локационные системы (ЛАЛС), иногда называемые **"лазерными микрофонами".**

Параметрические технические каналы утечки информации могут быть реализованы путем **"высокочастотного облучения"** помещения, где установлены полуактивные закладные устройства или технические средства, имеющие элементы, некоторые параметры которых изменяются по закону изменения акустического (речевого) сигнала. Для перехвата информации по данному каналу необходимы специальный передатчик с направленным излучением и приемник.

2. Задание на практические занятия

Защищаемым объектом является здание общей площадью не менее 300 кв.м. Объект должен иметь не менее 20 помещений, из которых не менее 17 защищаемые. Здание может быть, как одноэтажным, так и многоэтажным. Количество этажей выбирается самостоятельно. В одном из помещений рассматриваемого здания «организовать» защищенное помещение одного из трех типов: «комната переговоров», «конференц-зал», «зал презентаций», - с указанием реальных средств и мер защиты, а также расчетом необходимых затрат. Должна быть предусмотрена максимальная защита выделенного помещения.

При выполнении цикла практических работ по выбранному объекту должен быть проведён ряд мероприятий, указанный в практических работах. Для обеспечения защищенности объекта разрешено использовать только средства инженерно-технической защиты информации.

Средства и материалы для обеспечения ИТЗИ объекта выбираются с помощью сравнительного анализа средств защиты как минимум 3-х производителей.

Таблица 1. Варианты заданий

№ варианта п/п	Канал утечки	Количество помещений	Выделенное помещение
1	Электро-магнитный + материально-вещественный	23, 18 защищаемых	Конференц-зал
2	Вибро-акустический + материально-вещественный	22, 17 защищаемых	Комната переговоров
3	Оптический + материально-вещественный	24, 20 защищаемых	Зал презентаций
4	Вибро-акустический + материально-вещественный	23, 20 защищаемых	Зал презентаций
5	Оптический + материально-вещественный	22, 18 защищаемых	Конференц-зал
6	Электро-магнитный + материально-вещественный	21, 18 защищаемых	Комната переговоров
7	Электро-магнитный + материально-вещественный	23, 19 защищаемых	Конференц-зал
8	Оптический + материально-вещественный	25, 21 защищаемых	Зал презентаций
9	Электро-магнитный + материально-вещественный	23, 20 защищаемых	Комната переговоров
10	Вибро-акустический + материально-вещественный	22, 19 защищаемых	Зал презентаций

Продолжение таблицы 1. Варианты заданий

11	Оптический + материально-вещественный	24, 21 защищаемых	Конференц-зал
12	Вибро-акустический + материально-вещественный	25, 21 защищаемых	Комната переговоров
13	Электро-магнитный + материально-вещественный	24, 22 защищаемых	Зал презентаций
14	Оптический + материально-вещественный	25, 22 защищаемых	Конференц-зал
15	Электро-магнитный + материально-вещественный	24, 21 защищаемых	Комната переговоров
16	Вибро-акустический + материально-вещественный	25, 23 защищаемых	Комната переговоров
17	Вибро-акустический + материально-вещественный	25, 21 защищаемых	Зал презентаций
18	Электро-магнитный + материально-вещественный	24, 22 защищаемых	Конференц-зал
19	Оптический + материально-вещественный	25, 22 защищаемых	Комната переговоров
20	Вибро-акустический + материально-вещественный	23, 20 защищаемых	Зал презентаций
21	Оптический + материально-вещественный	22, 18 защищаемых	Конференц-зал
22	Электро-магнитный + материально-	21, 18 защищаемых	Комната переговоров

	вещественный		
23	Оптический + материально-вещественный	24, 21 защищаемых	Зал презентаций
24	Вибро-акустический + материально-вещественный	25, 21 защищаемых	Конференц-зал
25	Электро-магнитный + материально-вещественный	24, 22 защищаемых	Комната переговоров

Обратите внимание, что зал презентаций – это помещение со стеклянной стеной или стенами. Комната переговоров – изолированное помещение без окон. Конференц-зал – помещение со средствами аудио- и видеосвязи.

3. Методические указания по выполнению практических работ

3.1. Работа 1 Моделирование объектов защиты

Моделирование объектов защиты включает:

– структурирование защищаемой информации;

– разработку моделей объектов защиты.

Для структурирования информации в качестве исходных данных используются:

– перечень сведений, составляющих государственную, ведомственную или коммерческую тайну;

– перечень источников информации в организации.

Структурирование информации проводится путем классификации информации в соответствии со структурой, функциями и задачами организации с привязкой элементов информации к ее источникам. Детализацию информации целесообразно проводить до уровня, на котором элементу информации соответствует один источник.

Схема классификации разрабатывается в виде графа-структуры, нулевой (верхний) уровень иерархии которой соответствует понятию “конфиденциальная информация”, а *n*-ый (нижний) – элементам информации одного источника из перечня источников организации. Основное требование к схеме классификации – общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня, т. е. одна и та же информация не должна указываться в разных элементах классификации.

Результаты структурирования оформляются в виде:

– схемы классификации информации, пример которой приведен на рисунке 1;

– таблицы, вариант формы которой приведен в таблице 2.

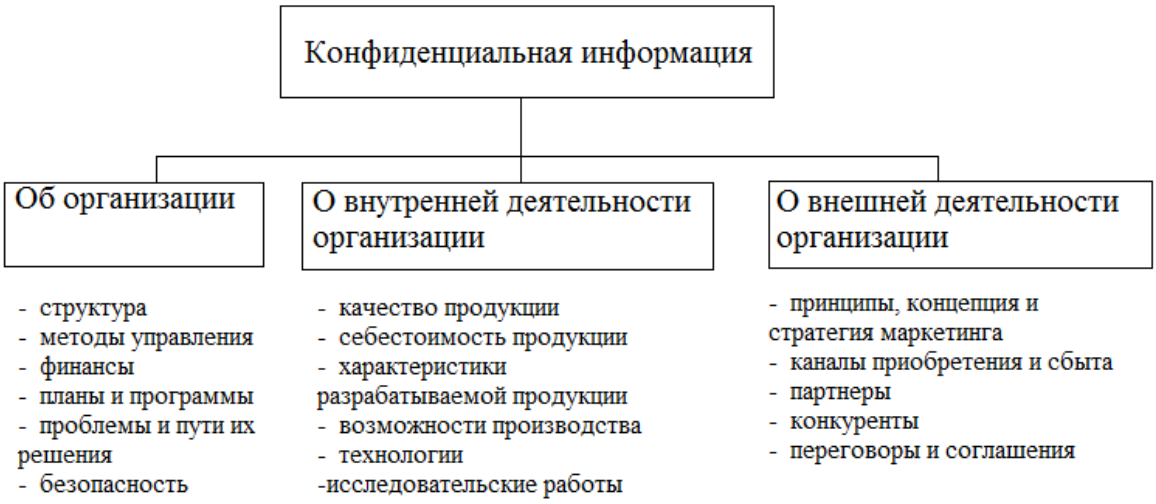

Рисунок 1 - Вариант структуры конфиденциальной информации

Таблица 2. Оформление результатов структурирования

№ элемента информации	**Наименование элемента информации**	**Гриф конфиденциальности информации**	**Цена информации**	**Наименование источника информации**	**Местонахождение источника информации**
1	2	3	4	5	6

Таблица разрабатывается на основе схемы классификации информации. В первом столбце указывается номер элемента информации в схеме классификации.

Порядковый номер элемента информации соответствует номеру тематического вопроса в структуре информации. Значность номера равна количеству уровней структуры, а каждая цифра – порядковому номеру тематического вопроса на рассматриваемом уровне среди вопросов, относящихся к одному тематическому вопросу на предыдущем уровне. Например, номер 2635 соответствует информации 5-го тематического вопроса на 4-м уровне, входящего в 3-й укрупненный вопрос 3-го уровня, который, в свою очередь, является частью 6-го тематического вопроса 2-го уровня, представляющего собой вопрос 2-й темы 1-го уровня.

В столбце “наименование элемента информации” указывается тематический вопрос, соответствующий порядковому номеру этого элемента.

Гриф и цена элемента могут быть назначены исходя из принятой шкалы классификации конфиденциальной информации, отраженной в табл.3. Здесь цена информации $\bar{Z}$ выражается в условной стоимости единицы информации.

В столбце 5 (табл.2) указывается наименование источника (фамилия человека, название документа или его номер по книге учета, наименование и номер изделия и т.д.), а в графе 6 – места размещения или хранения (возможные рабочие места людей-источников информации, места расположения, размещения или хранения других носителей).

Эти места в общем случае представляют собой:

– помещения (служебные, лаборатории, офисы, цеха, склады, квартиры и др.);

– письменные столы рабочих мест сотрудников, хранилища и сейфы, шкафы деревянные и металлические в помещениях.

В помещениях размещается большинство источников информации: люди, документы, разрабатываемая продукция и ее элементы, средства обработки и хранения информации и др., а также источники функциональных и опасных сигналов.

Таблица 3. Классификация конфиденциальной информации

Категория (гриф) важности	**Относительная стоимость бита информации, $\bar{Z}_k$**	**Требуемая надежность защиты Q (%)**	**Категория защиты**
ОВ	10^4	99,99	Предельно высокий уровень
СС	10^3	99,9	Высокий уровень
С	10^2	99,0	Достаточный уровень
ДСП	10	90,0	Допустимый уровень
О	1	37,0	Низкий уровень

Задача моделирования объектов защиты состоит в объективном описании и анализе источников конфиденциальной информации и существующей системы ее защиты.

Моделирование объектов защиты включает:

– определение источников защищаемой информации;

– описание пространственного расположения основных мест размещения источников защищаемой информации;

– выявление путей распространения носителей с защищаемой информации за пределы контролируемых зон (помещений, зданий, территории организации);

– описание с указанием характеристик существующих преград на путях распространения носителей с информацией за пределы контролируемых зон.

Моделирование проводится на основе пространственных моделей контролируемых зон с указанием мест расположения источников защищаемой информации – планов помещений, этажей зданий, территории в целом. На планах помещений указываются в масштабе места размещения ограждений, экранов, воздухопроводов, батарей и труб отопления, элементов интерьера и других конструктивных элементов, способствующих или затрудняющих распространение сигналов с защищаемой информацией, а также места размещения и зоны действия технических средств охраны и телевизионного наблюдения. Их параметры целесообразно объединить в таблице, вариант которой приведен в виде табл.3.

Таблица 4. Параметры объектов защиты

1	Название помещения			
2	Этаж		Площадь, $м^2$	
3	Количество окон, тип сигнализации, наличие штор на окнах		Куда выходят окна	
4	Двери, кол-во, одинарные, двойные		Куда выходят двери	
5	Соседние помещения, название, толщина стен			
6	Помещение над потолком, название, толщина перекрытий			
7	Помещение под полом, название, толщина перекрытий			
8	Вентиляционные отверстия, места			

	размещения, размеры отверстий		
9	Батареи отопления, типы, куда выходят трубы		
10	Цепи электропитания	Напряжение, (В), количество розеток электропитания, входящих и выходящих кабелей	
11	Телефон	Типы, места установки телефонных аппаратов, тип кабеля	
12	Радиотрансляция	Типы громкоговорителей места установки	
13	Электрические часы	Тип, куда выходит кабель электрических часов	
14	Бытовые радиосредства	Радиоприемники, телевизоры, аудио и видеомагнитофоны, их кол-во и типы	
15	Бытовые электроприборы	Вентиляторы и др., места их размещения	
16	ПЭВМ	Кол-во, типы. состав, места размещения	
17	Технические средства охраны	Типы и места установки извещателей, зоны действий излучений	
18	Телевизионные средства наблюдения	Места установки, типы и зоны наблюдения телевизионных трубок	
19	Пожарная сигнализация	Типы извещателей, схемы соединения и вывода шлейфа	
20	Другие средства		

Контрольные вопросы к практической работе 1

1. Для чего производится структурирование информации?
2. Как определяется цена информации?
3. Зачем необходимо указывать места размещения информации?
4. Влияет ли наличие каналов распространения информации на модель объекта защиты и почему?
5. Могут ли быть бытовые приборы источником угроз для информации?

3.2. Работа 2 Моделирование угроз безопасности информации

Моделирование угроз безопасности информации предусматривает анализ способов ее хищения, изменения и уничтожения с целью оценки наносимого этими способами ущерба.

Моделирование угроз включает:

– моделирование способов физического проникновения злоумышленника к источникам информации;

– моделирование технических каналов утечки информации.

Для создания **модели угрозы физического проникновения**, достаточно близкой к реальной, необходимо “перевоплотиться” в злоумышленника, т. е. попытаться мысленно проиграть с позиции злоумышленника варианты проникновения к источнику информации. Чем больше при этом будет учтено факторов, влияющих на эффективность проникновения, тем выше адекватность модели. В условиях отсутствия информации о злоумышленнике, его квалификации, технической оснащенности во избежание грубых ошибок лучше переоценить угрозу, чем ее недооценить, хотя такой подход и может привести к увеличению затрат на защиту.

На основе такого подхода модель злоумышленника выглядит следующим образом:

– злоумышленник представляет серьезного противника, тщательно готовящего операцию проникновения, изучает: обстановку вокруг территории организации, наблюдаемые механические преграды, средства охраны, телевизионного наблюдения и дежурного (ночного) освещения, а также сотрудников с целью добывания от них информации о способах и средствах защиты;

– имеет в распоряжении современные технические средства проникновения и преодоления механических преград;

– всеми доступными способами добывает и анализирует информацию о расположении зданий и помещений организации, о рубежах охраны, о местах хранения источников информации, видах и типах средств охраны, телевизионного наблюдения, освещения и местах их установки;

– проводит анализ возможных путей проникновения к источникам информации и ухода после выполнения задачи.

При моделировании действий квалифицированного злоумышленника необходимо также исходить из предположения, что он хорошо представляет современное состояние технических средств защиты информации, типовые варианты их применения, слабые места и “мертвые” зоны диаграмм направленности активных средств охраны.

Возможные пути проникновения злоумышленников отмечаются линиями на планах (схемах) территории, этажей и помещений зданий, а результаты анализа пути заносятся в табл. 5.

Таблица 5. Результаты анализа пути проникновения злоумышленников

№ элемента информации	Цена информации	Путь проникновения злоумышленника	Оценки реальности канала	Величина угрозы	Ранг угрозы
1	2	3	4	5	6

Моделирование технических каналов утечки информации по существу является единственным методом достаточно полного исследования их возможностей с целью последующей разработки способов и средств защиты информации. В основном применяются вербальные и математические модели.

Обнаружение и распознавание каналов утечки информации, так же как любых объектов, производится по их демаскирующим признакам. В качестве достаточно общих признаков или индикаторов каналов утечки информации могут служить признаки, указанные в табл. 6. Приведенные индикаторы являются лишь ориентирами при поиске потенциальных каналов утечки. В конкретных условиях их состав существенно больший.

Потенциальные каналы утечки определяются для каждого источника информации, причем их количество может не ограничиваться одним или двумя. Например, от источника информации – руководителя фирмы утечка информации возможна по следующим каналам:

– через дверь в приемную или коридор;
– через окно на улицу или во двор;
– через вентиляционное отверстие в соседние помещения;
– с опасными сигналами по радиоканалу;

– с опасными сигналами по кабелям, выходящим из помещения;
– по трубам отопления в другие помещения здания;
– через стены, потолок и пол в соседние помещения;
– с помощью закладных устройств за территорию фирмы.

Таблица 6. Признаки каналов утечки информации

Вид канала	**Индикаторы**
Оптический	Окна, выходящие на улицу, близость к ним противоположных домов и деревьев. Отсутствие на окнах занавесок, штор, жалюзей. Просматриваем ость содержания документов на столах со стороны окон, дверей, шкафов в помещении. Просматриваемость содержания плакатов на стенах помещения для совещания из окон и дверей. Малое расстояние между столами сотрудников в помещении. Просматриваемость экранов мониторов ПЭВМ на столах сотрудников со стороны окон, дверей или других сотрудников. Складирование продукции во дворе без навесов. Малая высота забора и дырки в нем. Переноска и перевозка образцов продукции в открытом виде. Появление возле территории организации (предприятия) посторонних людей (в том числе в автомобилях) с биноклями, фотоаппаратами, кино и видеокамерами.
Радиоэлектронный	Наличие в помещении радиоэлектронных средств, ПЭВМ, ТА городской и внутренней АТС, громкоговорителей трансляционной сети и других предметов. Выход окон помещения на улицу, близость к ним улицы и противоположных домов Применение средств радиосвязи. Параллельное размещение кабелей в одном жгуте при разводке их внутри здания и на территории организации. Отсутствие заземления радио и электрических приборов. Длительная и частая парковка возле организации чужих автомобилей, в особенности с сидящими в машине людьми
Акустический	Малая толщина дверей и стен помещения Наличие в помещении открытых вентиляционный отверстий Отсутствие экранов на отопительных батареях Близость окон к улице и ее домам. Появление возле организации людей с достаточно большими сумками, длинными и толстыми зонтами. Частая и продолжительная парковка возле организации чужих автомобилей.
Материально-вещественный	Отсутствие закрытых и опечатанных ящиков для бумаги и твердых отходов с демаскирующими веществами. Применение радиоактивных веществ. Неконтролируемый выброс газов с демаскирующими веществами, слив в водоемы и вывоз на свалку твердых отходов. Запись сотрудниками конфиденциальной информации на неучтенных листах бумаги.

Применительно к моделям каналов утечки информации целесообразно иметь модели, описывающие каналы в статике и динамике.

Статическое состояние канала характеризуют структурная и пространственная модели. Структурная модель описывает структуру (состав и связи элементов) канала утечки. Пространственная модель содержит описание положения канала утечки в пространстве: места расположения источника и приемника сигналов, удаленность их от границ территории организации, ориентация вектора распространения носителя информации в канале утечки информации и его протяженность. Структурную модель канала целесообразно представлять в табличной форме, пространственную – в виде графа на плане помещения, здания, территории организации, прилегающих внешних участков среды. Структурная и пространственная модели не являются автономными, а взаимно дополняют друг друга.

Динамику канала утечки информации описывают функциональная и информационная модели. Функциональная модель характеризует режимы функционирования канала, интервалы времени, в течение которых возможна утечка информации, а информационная содержат характеристики информации, утечка которой возможна по рассматриваемому каналу: количество и ценность информации, пропускная способность канала, прогнозируемое качество принимаемой злоумышленником информации.

Указанные модели объединяются и увязываются между собой в рамках комплексной модели канала утечки. В ней указываются интегральные параметры канала утечки информации: источник информации и ее вид, источник сигнала, среда распространения и ее протяженность, место размещения приемника сигнала, информативность канала и величина угрозы безопасности информации.

Каждый вид канала содержит свой набор показателей источника и приемника сигналов в канале, позволяющих оценить максимальную дальность канала и показатели возможностей органов государственной и коммерческой разведки.

Так как приемник сигнала является принадлежностью злоумышленника и точное место его размещения и характеристики не известны, то моделирование канала проводится применительно к

гипотетическому приемнику. В качестве приемника целесообразно рассматривать приемник, параметры которого соответствуют современному уровню, а место размещения выбрано рационально. Уважительное отношение к интеллекту и техническим возможностям противника гарантирует от крупных ошибок в значительно большей степени, чем пренебрежительное.

Если возможное место размещения приемника сигналов выбрано, то в ходе моделирования канала рассчитывается энергетика носителя на входе приемника с учетом мощности носителя на выходе источника, затухания его в среде распространения, уровня помех, характеристик сигнала и его приемника.

Например, разрешение при фотографировании людей и предметов, находящихся в служебном помещении, с расстояния L легко оценить по известной формуле: $H = hL/f$, где h – разрешение в долях мм системы “объектив-фотопленка”, f – фокусное расстояние телеобъектива фотоаппарата, L – расстояние от объекта наблюдения до фотоаппарата. Если фотографирование производится фотоаппаратом “Фотоснайпер ФС-122” с f = 300 мм и h = 0.03 мм (разрешение 33 лин/мм), то для L = 50 м H равно 5 мм. Учитывая, что для обнаружения и распознавания объекта его изображение должно состоять не менее чем из 9 точек, то минимальные размеры объекта составляют 15х15 мм. Очевидно, что на фотографии можно будет рассмотреть человека, продукцию, но нельзя прочитать машинописный текст на бумаге или экране монитора.

Затухание акустической волны на границе контролируемой зоны зависит от множества факторов, таких как конструкция помещения, материал стен, тип и количество дверей и окон, наличие звукопоглощающих элементов и т.п. Для ориентировочной оценки можно использовать данные, приведенные в нижеследующих таблицах.

Значения ослабления звука ограждениями, выполненными из некоторых часто применяемых строительных материалов, указаны в табл.7.

Таблица 7. Звукопоглощающие свойства некоторых строительных конструкций

Материал	Толщина	Звукоизоляция на частотах (Гц), дБ					
		125	250	500	1000	2000	4000
Кирпичная стена	0,5 кирпича	39	40	42	48	54	60
Отштукатуренная с двух сторон стена	1 кирпич	36	41	44	51	58	64
	1,5 кирпича	41	44	48	55	61	65
	2 кирпича	45	45	52	59	65	70
	2,5 кирпича	47	55	60	67	70	70
Стена из железобетонных блоков	40 мм	32	36	35	38	47	53
	100мм	40	40	44	50	55	60
	200мм	42	44	51	59	65	65
	300мм	45	50	58	65	69	69
	400мм	48	55	61	68	70	70
	800мм	55	61	68	70	70	70
Стена из шлакоблоков	220мм	42	42	48	54	60	63
Перегородка из древесно-стружечной плиты	20см	23	26	26	26	26	26

Уровень акустического сигнала за ограждением можно приближенно оценить по формуле (1):

$$R_{ог} \approx R_{рс} + 6 + 10lg\, S_{ог} - K_{ог}\ дБ, \quad (1)$$

где $R_{рс}$ – уровень речевого сигнала в помещении (перед ограждением), дБ;

$S_{ог}$ – площадь ограждения, м^2;

$K_{ог}$ – звукоизолирующая способность ограждения, дБ.

Таблица 8. Звукоизоляция окон

Схема остекления	Звукоизоляция (дБ) на частотах, Гц					
	125	250	500	1000	2000	4000
Одинарное остекление:						
толщина 3 мм	17	17	22	28	31	32
толщина 4 мм	18	23	26	31	32	32
толщина 6 мм	22	22	26	30.	27	25
Двойное остекление с воздушным промежутком:						
57 мм (толщина 3 мм)	15	20	32	41	49	46
90 мм (толщина 3 мм)	21	29	38	44	50	48
57 мм (толщина 4 мм)	21	31	38	46	49	35
90 мм (толщина 4 мм)	25	33	41	47	48	36

Таблица 9. Звукоизоляция обычных дверей

Конструкция двери	Условия применения	Звукоизоляция (дБ) на частотах, Гц					
		125	250	500	1000	2000	4000
Дверь щитовая, облицованная фанерой с двух сторон	без прокладки	21	23	24	24	24	23
	с прокладкой из пористой резины	27	27	32	35	34	35
Типовая дверь ГТ-327	без прокладки	13	23	31	33	34	36
	с прокладкой из пористой резины	29	30	31	33	34	41

Таблица 10. Звукоизоляция специальных дверей

Конструкция двери	Звукоизоляция (дБ) на частотах, Гц					
	125	250	500	1000	2000	4000
Дверь звукоизолирующая облегченная	18	30	39	42	45	43
Дверь звукоизолирующая облегченная, двойная с зазором более 200 мм	25	42	55	58	60	60
Дверь звукоизолирующая тяжелая	24	36	45	51	50	49
Дверь звукоизолирующая тяжелая, двойная с зазором более 300 мм	34	46	60	60	65	65
Дверь звукоизолирующая тяжелая, двойная с облицовкой тамбура	45	58	65	70	70	70

При расчетах следует иметь в виду, что уровень звука при умеренной речи составляет 50…60 дБ, а громкая речь соответствует 70…80 дБ.

Степень ослабления электромагнитного излучения зависит от размеров контролируемой зоны и от наличия преград на пути распространения электромагнитной волны. Экранирующие свойства некоторых элементов здания приведены в табл.11.

Таблица 11. Экранирующие свойства элементов знания

Тип здания	Ослабление, дБ на частоте		
	100 МГц	500 МГц	1 ГГц
Деревянное здание с толщиной стен 20 см	5-7	7-9	9-11
Кирпичное здание с толщиной стен 1.5 кирпича	13-15	5-17	16-19
Железобетонное здание с ячейкой арматуры 15х15 см н толщиной 160 мм	20-25	18-19	15-17

Примечание: указанные в таблице данные получены для стен, 30% площади которых занимают оконные проемы с обычным стеклом. Если оконные проемы закрыты металлической решеткой с ячейкой 5 см, то экранирование увеличивается на 30-40 %. Экранирующие свойства кирпичных и железобетонных стен зданий в 2-3 раза выше, чем деревянных.

Все выявленные потенциальные каналы утечки информации и их характеристики записываются в таблицу (например, такой формы, как табл.12).

Наименование источника информации заимствуются из табл. 2. В графе 4 указываются основные элементы среды распространения и возможные места размещения приемника сигналов. По физической природе носителя определяется вид канала утечки информации.

Таблица 12. Потенциальные каналы утечки информации

№ элемента информации	Цена информации	Источник сигнала	Путь утечки информации	Вид канала	Оценки реальности канала	Величина угрозы	Ранг угрозы
1	2	3	4	5	6	7	8

Оценка показателей угроз безопасности (графы 6-8) представляет достаточно сложную задачу в силу следующих обстоятельств:

– добывание информации нелегальными путями не афишируется и фактически отсутствуют или очень скудно

представлены в литературе реальные статистические данные по видам угроз безопасности информации. Кроме того, следует иметь, что характер и частость реализации угроз зависят от криминогенной обстановки в районе нахождения организации и данные об угрозах, например, в странах с развитой рыночной экономикой, не могут быть однозначно использованы для российских условий;

– многообразие способов, вариантов и условий доступа к защищаемой информации существенно затрудняют возможность выявления и оценки угроз безопасности информации. Каналы утечки информации могут распространяться на достаточно большие расстояния и включать в качестве элементов среды распространения труднодоступные места;

– априори не известен состав, места размещения и характеристики технических средств добывания информации злоумышленника.

Оценки угроз информации в результате проникновения злоумышленника к источнику или ее утечки по техническому каналу проводятся с учетом вероятности реализуемости рассматриваемого пути или канала, а также цены соответствующего элемента информации. Поэтому могут быть созданы два типа моделей угроз информации: **статистическая и экономическая**.

Для понимания статистической модели информационных угроз рассмотрим некоторую условную зону информационной защиты. Допустим, что речь идет о защите конфиденциальных разговоров в некотором служебном помещении. Для конкретного помещения всегда можно составить достаточно полный перечень угроз и их сценариев. Все угрозы будут пронумерованы и будут иметь описательную часть. Наиболее полной статистической характеристикой каждой из угроз является вероятность P(T) ее реализации за некоторое заданное время T или связанная с ней величина p плотности вероятности угрозы в единицу времени* . Статистическая модель предполагает составление таблиц, где для каждой из угроз вместе с описательной ее частью указывается ее вероятность (графа 6 табл. 12).

Приведем пример.

Качественное описание: угроза Sp – виброакустический контроль помещения со стороны соседних помещений (применение стетоскопов).

Статистическое описание: вероятность угрозы $P(T)$ = 0,1% за время T = 5 лет или плотность вероятности $p = P(T)/T$ = 0,02% в год.

К сожалению, практически этот путь нереален. Дело в том, что величины $P_к$ как правило, не известны даже для классов предприятий, не говоря уже о конкретном коммерческом учреждение. Эти величины зависят от региона, криминогенности обстановки, вида бизнеса и многих других причин.

Отсутствие точных величин вероятностей $P_к$ информационных угроз принципиально ограничивает возможность использования методов статистических решений, теория которых хорошо развита для различных прикладных задач.

Однако рекомендуемые теорией правила выбора средств и методов информационной защиты не всегда требуют знаний абсолютных величин $\{P\}$. Эти правила предусматривают сравнение между собой так называемых ранговых коэффициентов, пропорциональных вероятностям $P_к$. Формально это означает, что вместо величин $P_к$ можно использовать любые другие характеристики, пропорциональные $P_к$.

Конструктивной в этом отношении является экономическая модель информационных угроз. В основу модели заложена идея о том, что все угрозы должны быть в конечном итоге экономически оправданы. Действительно, реализация любой информационной угрозы сопряжена с определенными затратами: тратятся средства на изучение обстановки, разработку плана и технологии угрозы, приобретение оборудования и необходимых специальных технических средств, имеются расходы и на этапе реализации угрозы. Источник угрозы надеется на то, что все эти затраты окупятся теми конфиденциальными сведениями, которые он получит. Мерой такого сопоставления является величина отношения Z/b, где Z – эквивалентная стоимость полученных сведений, а b – совокупные затраты по организации канала утечки информации.

Чем больше величина Z/b, тем больше вероятность угрозы. В первом приближении плотность вероятности угрозы

пропорциональна величине $\alpha = Z/b$, называемой в дальнейшем **коэффициентом опасности угрозы.**

Используя экономическую модель угроз, можно сделать следующие общие выводы:

– чем больше информационная значимость зоны *Z*, тем больше вероятность угрозы при прочих равных условиях;

– чем меньше затраты на реализацию угрозы (малозатратные угрозы), тем больше вероятность угрозы;

– высокопрофессиональные (затратные) угрозы реальны (вероятны) только для зон защиты с большой значимостью.

Проиллюстрируем предлагаемую методику количественного оценивания информационных угроз на конкретном примере. Рассмотрим акустические угрозы в отношении некоторого условного помещения.

Составим полный перечень возможных каналов утечки речевой информации (характеристики канала связи не учитываем). Допустим, что перечень включает в себя 15 видов информационных угроз, сведенных в табл.13.

Для каждой из угроз экспертно определяем основные характеристики канала утечки информации, в том числе: длительность *T* работы (за год); среднюю величину q (дБ) динамического диапазона; полосу частот ΔF; затраты в *b(s)* на реализацию угрозы (учтем для простоты только стоимость специальных технических средств). Эти данные представлены в табл.13.

Таблица 13. Основные характеристики канала утечки информации

Код угрозы	Вид угрозы	Δ F (кГц)	T (час)	q (дБ)	I (Мб)	b (дол.)	α Мб / дол.
1	2	3	4	5	6	7	8
Sp1	Вносимая или заранее установленная автономная радиозакладка, в том числе с дистанционным управлением ДУ	3,5	200	40	$4{,}35 \times 10^3$	1000	4,35

Код угрозы	Вид угрозы	Δ F (кГц)	T (час)	q (дБ)	I (Мб)	b (дол.)	α Мб дол.
1	2	3	4	5	6	7	8
Sp2	Долговременная радиозакладка с сетевым питанием, в том числе с ДУ	3,5	3000	40	$6,3x10^4$	500	126
Sp3	Использование естественных звуководов	3,5	3000	30	$4,7x10^4$	300	157
Sp4	Контроль стен (стетоскопы)	3,5	3000	10	$1,57x10^4$	1000	15,7
Sp5	Контроль труб (стетоскопы)	2,0	1500	10	$4,5x10^3$	1000	4,5
Sp6	Использование вносимых диктофонов	3,5	50	40	$1,05x10^3$	1500	0,7
Sp7	Направленные микрофоны	2,0	200	10	$6x10^2$	2000	0,3
Sp8	Мимический канал	3.5	1500	30	$2,36x10^4$	6000	3,94
Sp9	Лазерный контроль оконных стекол	2,5	1500	20	$1,1x10^4$	100 000	0,11
Sp10	Пассивные оптические закладки-отражатели	3,5	1500	30	$2,35x10^4$	50 000	0,47
Sp11	Проводные (телефонные) закладки	3.5	3000	20	$3,14x10^4$	200	157
Sp12	Проводные (пассивные) закладные устройства сложных модификаций	3,5	2000	20	$2,1x10^4$	400	52,3
Sp13	Сетевые проводные закладки	3,5	3000	40	$6,3x10^4$	400	157
Sp14	Специальные проводные системы	3,5	3000	40	$6,3x10^4$	5000	12,6
Sp15	Активные системы повышенной энергетической скрытности	3,5	3000	40	$6,3x10^4$	30 000	2,1

Для каждой из угроз рассчитываем коэффициент опасности угроз α (2):

$$\alpha = \frac{\overline{Z}I}{b} = \overline{Z}\frac{\Delta F T \log_2(1+q)}{b} \quad (2)$$

где $\bar{Z}$ – стоимость бита информации (принимается равной 1, поскольку все угрозы сравниваются между собой);

I – объем “похищенной” информации (при реализации угрозы);

ΔF – полоса пропускания канала;

q – среднеспектральное отношение мощности сигнала к мощности помехи.

Результаты расчетов отображаются в той же таблице.

Аналогичным образом формируется (для данного помещения) спектр сигнальных угроз. Исходные данные для него отражены в таблице 14.

Таблица 14. Данные для спектра сигнальных угроз

Код угроз	Наименование угрозы	T(час)	m (шт)	I_1 (Мб)	l x m	F_k (Гц)	q (дБ)	I (Мб)	b (дол.)	α Мб / дол.
S1	Перехват побочных излучений от ЭВМ	3000						10^3	40000	0,02
S2	Применение закладных устройств в ЭВМ	3000						10^3	20000	0,05
S3	Программные хищения из банка данных ЭВМ	3000						10^3	10000	0,10
S4	Копирование информации с магнитных носителей	3000	50	1,44				72	1000	0.07
S5	Внешний (через окна) видеоконтроль с документированием	200			250x250	25	10	$4,7x10^5$	10000	47
S6	Специальный видеоконтроль через малые отверстия в ограждающих конструкциях	1000			250x250	25	40	$7,0x10^5$	40000	175

S7	Использование вносимых, кратковременного действия видеоконтрольных устройств или микрофотокамер	100			250x250	25	40	$2,6x10^2$	1000	0,26

Коэффициенты α опасности угроз сигнальной информации оценивались по формуле:

$\alpha = \bar{Z}\, I/b,$

где I – общий объем информации по каналу ее утечки за время анализа T (принято, что $T = 1$ год);

b – стоимость реализации угрозы;

$\bar{Z}$ – средняя стоимость информации (принята при расчетах равной 1).

Входящая в формулу величина I объема информации принималась равной:

$I = 10^3$ Мб – для вариантов хищения информации с жесткого диска ЭВМ;

$I = mI_1$, – для вариантов копирования дискет (документов), где m – число дискет, а $I_1 = 1,44$ Мб – емкость дискеты;

$I = (l \times m)F_k \log_2(1 + q)\, T$ – для вариантов видеоконтроля,

где $l \times m$ – число элементов (число pixel) разрешения в поле изображения; F_k – частота кадров; q – отношение сигнал/помеха; T – время штатной работы (хорошая видимость и др.).

Следует подчеркнуть, что все исходные данные были условными, хотя и отражали в первом приближении реальные возможности угроз и их экономическую основу. Основная цель примеров – проиллюстрировать методику формирования спектров угроз.

На основании полученных данных можно заполнить графы 7 и 8 табл.12.

Контрольные вопросы к практической работе 2

1. Классификация каналов утечек информации

2. Какие характеристику могут быть у канала утечки информации?

3. Что собой представляет статистическая модель угроз?

4. Как оцениваются показатели угроз безопасности?

5. Какой постулат закладывается в основу формирования модели угроз?

3.3. Работа 3. Разработка организационных и технических мер по инженерно-технической защите информации.

Меры по защите информации целесообразно разделить на 2 группы: организационные и технические. При такой классификации к техническим относятся меры, реализуемые путем установки новых или модернизации используемых инженерных и технических средств защиты информации. Основу организационных мер инженерно-технической защиты информации составляют меры, определяющие порядок использования этих средств.

Организационные меры инженерно-технической зашиты информации включают, прежде всего, мероприятия по эффективному использованию технических средств регламентации и управления доступом к защищаемой информации, а также по порядку и режимам работы технических средств защиты информации. Организационные меры инженерно-технической защиты информации являются частью ее организационной защиты, основу которой составляют регламентация и управление доступом.

Регламентация – это установление временных, территориальных и режимных ограничений в деятельности сотрудников организации и работе технических средств, направленные на обеспечение безопасности информации.

Регламентация предусматривает:

– установление границ контролируемых и охраняемых зон;

– определение уровней защиты информации в зонах;

– регламентация деятельности сотрудников и посетителей (разработка распорядка дня, правил поведения сотрудников в организации и вне ее и т. д.);

– определение режимов работы технических средств, в том числе сбора, обработки и хранения защищаемой информации на ПЭВМ, передачи документов, порядка складирования продукции и т. д.

Управление доступом к информации включает следующие мероприятия:

– идентификацию лиц и обращений;
– проверку полномочий лиц и обращений;
– регистрацию обращений к защищаемой информации;
– реагирование на обращения к информации.

Идентификация пользователей, сотрудников, посетителей, обращений по каналам телекоммуникаций проводится с целью их надежного опознавания.

Проверка полномочий заключается в определении прав лиц и обращений по каналам связи на доступ к защищаемой информации. Для доступа к информации уровень полномочий обращения не может быть ниже разрешенного. С целью обеспечения контроля над прохождением носителей с закрытой информацией производится регистрация (протоколирование) обращений к ним путем записи в карточках, журналах, на магнитных носителях.

Реагирование на любое обращение к информации заключается либо в разрешении доступа к информации, либо в отказе. Отказ может сопровождаться включением сигнализации, оповещением службы безопасности или правоохранительных органов, задержанием злоумышленника при его попытке несанкционированного доступа к защищаемой информации.

Технические меры предусматривают применение способов и средств, препятствующих утечке информации за пределы контролируемой зоны. Очевидно, что выбор инженерно-технических средств защиты представляет непростую задачу, так как от него зависит, с одной стороны, надежность защиты, а с другой – цена, которую необходимо заплатить, чтобы эту защиту обеспечить.

Таким образом, выбор инженерно-технических средств локальной защиты информации всегда представляет собой процесс сопоставления требований и возможностей.

Возможности инженерно-технических средств защиты информации определяются их тактико-техническими характеристиками (уровнями ослабления сигналов, уровнями создаваемых помех, уровнями экранировки и т. п.). Требования должны учитывать специфику зон защиты, степень важности информации, допустимый риск (допустимые потери) и др.

Ниже излагается одна из моделей общего методического подхода к проблеме.

Применяя средства активной или пассивной защиты, мы тем или иным способом уменьшаем пропускную способность каналов утечки информации. Происходит обесценивание информации, то есть в конечном итоге снижение стоимости ущерба* . Активные средства обеспечивают это путем создания помех, а средства пассивной защиты – путем ослабления уровня информационного сигнала.

Пусть $C_0 = \Delta F \log_2(1+q_0)$ – пропускная способность канала утечки информации без применения средств защиты, а $C_1 = \Delta F \log_2(1+q_1)$ – пропускная способность канала утечки информации после применения соответствующего средства защиты, которое обеспечивает зашумление или экранировку канала на величину $\Delta B = 10\lg(q_0/q_1)$. Тогда относительное уменьшение пропускной способности канала можно записать как (3):

$$\frac{C_0 - C_1}{C_0} = 1 - \frac{C_1}{C_0} = 1 - \frac{\lg(1+q_1)}{\lg(1+q_0)} \qquad (3)$$

Предположим, что в результате примененного средства защиты канал утечки информации полностью потерял свою пропускную способность, т.е. $C_1 = 0$. В этом случае эффективность защиты будет 100%. Однако это будет лишь в случае, когда $P_{\text{сигн}} = 0$ (что лишено практического смысла) или $P_{\text{шума}} = \infty$, (что невозможно). Поэтому имеет смысл определить, какой уровень зашумления или экранировки необходим для обеспечения заданного уровня эффективности защиты, воспользовавшись соотношениями (4):

$$Q = 1 - \frac{\lg(1+q_1)}{\lg(1+q_0)} \text{ и } \Delta B = 10\lg(q_0/q_1) \quad (4).$$

Рассмотрим в качестве примера случай защиты информации с грифом “секретно” (уровень 3). Из табл.3 находим, что нужна защита с эффективностью не менее 99%. Канал утечки информации предполагался качественным с динамическим диапазоном $q_0 = 40$ дБ ($P_с/P_ш = 10000$), то есть уровень пороговой его чувствительности, например по акустике, соответствовал тихой, шепотной речи. Решая систему уравнений, найдем, что требуемый при этом уровень зашумления (экранировки) $\Delta B = 50$ дБ.

Имея требования по эффективности защиты и используя рассмотренные зависимости, можно оценить величину ΔB (дБ) необходимого зашумления или экранировки канала утечки информации для каждой категории важности. Получим таблицу 15, отображающую требования к защите от утечки информации по высококачественному (q_0 = 40 дБ) каналу.

Для понимания методики выбора инженерно-технических средств защиты рассмотрим сначала случай одной зоны защиты (одной физической формы проявления информации) и статистической модели угроз.

Таблица 15. Требования к защите от утечки информации

Категория секретности	Q	Δ В, дБ
ОВ	0,9999	70
СС	0,999	60
С	0,99	50
ДСП	0,9	38

Общие экономические потери П будут слагаться из потерь от реализации угроз $\sum_{k=1}^{N} P_k Z_k (1-\Psi_k)$ и потерь, связанных с расходами на безопасность:

$$\Pi = \sum_{k=1}^{N} [[P_k Z_k (1-\Psi_k) + B_k \Psi], \quad (5)$$

где k – номер информационной угрозы (k = 1,2...N);

N – общее число угроз рассматриваемого физического вида;

B_k, – стоимость инженерно-технического средства защиты;

P_k, – вероятность угрозы с номером k;

Z_k, – эквивалентная стоимость информации, теряемой при реализации угрозы с номером k;

Ψ_k – целочисленная функция принимающая значение Ψ_k =1, если противодействие угрозе k предусматривается системой защиты, и Ψ_k = 0, если противодействие отсутствует. Эту функцию назовем функцией выбора или решений.

Как уже отмечалось, стратегия информационной защиты должна состоять в выборе таких противодействий, с такой их стоимостью и качествами, чтобы обеспечивался минимум общих потерь $П$ при условии ограниченности общих средств на защиту, то есть

$$\sum_{k=1}^{N} B_k \Psi_k \leq B_0 \quad (6)$$

Получили известную вариационную задачу линейного программирования. Ее решение хорошо известно специалистам. Оно принимается по величине ранговых коэффициентов η_k:

$$\eta_k = P_k Z_k / B_k. \quad (7)$$

Чем больше величина η_k,. тем больше оснований применить данное средство для защиты от угрозы с номером k.

Выбор решений осуществляется таким образом путем сопоставления рангов между собой и отбора тех из них, которые имеют наибольшую величину, а сумма соответствующих им затрат не превышает общих средств на защиту.

При такой сравнительной метрологии нет необходимости знать абсолютные величины вероятностей P_i, и абсолютные значения стоимости Z_i, информации. Достаточно использовать любые другие величины, им пропорциональные. Можно, в частности, отказаться от статистической модели угроз и использовать экономическую модель. В этом случае в качестве рангового коэффициента предлагается использовать величины

$$\eta_i = \alpha_i I_i Z_i / B_i \quad (8)$$

где I_i – объем информации в i-ом канале ее утечки.

Отбирая максимальные ранги, осуществим выбор инженерно-технических средств защиты.

Следующим шагом является расчет получающейся при этом эффективности Q защиты информации. Для статистической модели имеем:

$$Q = \frac{\sum_{i=1}^{N} P_i Z_i \Psi_i}{\sum_{i=1}^{N} P_i Z_i}, \quad (9)$$

где числитель характеризует величину ущерба, который предотвращен применением технических средств защиты, а знаменатель – общую величину среднего ущерба при реализации рассматриваемых угроз.

В случае использования экономической модели угроз и соответствующих ей рангов имеем:

$$Q = \frac{\sum_{i=1}^{N} \eta_i B_i \Psi_i}{\sum_{i=1}^{N} \eta_i B_i} \qquad (10)$$

Частная (для данной зоны) рентабельность защиты ρ составит при этом величину:

$$\rho = \frac{\sum_{i=1}^{N} \eta_i B_i \Psi_i - B_0}{\sum_{i=1}^{N} \eta_i B_i} = Q - \frac{B_0}{\sum_{i=1}^{N} \eta_i B_i} \qquad (11)$$

Сформулируем последовательность операций в рекомендуемой теорией технологии выбора инженерно-технических средств защиты:

– составляется перечень угроз и на основе экономической модели определяется их спектр;

– для каждой из угроз определяются средства защиты, обеспечивающие требуемый для этой зоны уровень защиты;

– определяется стоимость этих средств;

– для каждой из угроз оцениваются ранги;

– выбираются средства (решения) с максимальными рангами при условии, что суммарная стоимость не превысит выделенных ассигнований;

– производится расчет эффективности защиты как функции ассигнований.

Контрольные вопросы к практической работе 3

1. Как происходит расчёт эффективности защиты информации?
2. Как происходит выбор средств защиты объектов?
3. Какие могут предъявляться требования к эффективности средств защиты?
4. Что такое организационные методы защиты и что они в себя включают?
5. Опишите модель оценки эффективности средств защиты

3.4. Работа 4 Выбор средств защиты информации

Применим теорию к задаче выбора средств защиты речевой информации для некоторого условного помещения. Примем для определенности, что производственная площадь составляет 30 м^2, высота потолка 3 м, имеются два окна, выходящие на улицу, этажность невысокая, что позволяет реализовываться угрозам, связанным с дистанционным контролем. Начальным этапом технологии выбора средств является составление полного перечня информационных угроз с определением их спектра. Будем считать эту задачу решенной. Воспользуемся данными таблицы 13. На втором этапе производится оценка рангов средств защиты. В качестве промежуточного шага рассчитываются их приоритеты.

Понятие приоритетов средств защиты следует из формулы для ранговых коэффициентов. Чисто формально эту формулу можно записать так:

$$\eta_i = \alpha_i \times \beta_i \quad (12)$$

где α_i, – коэффициент опасности угрозы, а β_i,- некоторый коэффициент, зависящий только от средства защиты и важности защищаемой информации:

$$\beta_i = I_i Z_i / B_i. \quad (13)$$

Этот коэффициент можно рассматривать как меру приоритетности средства защиты. Чем больше величина β_i,тем больше оснований для применения средства защиты либо по причине его низкой стоимости, либо потому, что оно защищает от утечки большого объема информации.

В табл. 16 представлены промежуточные числа α и β и конечный (ранг η) результат расчетов для экспертно выбранных 14 видов защиты речевой информации.

В табл.17 представлены ранжированные (в порядке уменьшения рангов) противодействия акустическим угрозам. Там же указан рост затрат на защиту и соответствующий этим затратам рост эффективности *Q* защиты.

Таблица 16. Результаты расчетов

Код средства защиты	Вид противодействия	Виды угроз	B (дол.)	α Мб дол.	β Мб дол.	η	Общий ранг (η_0)
1	2	3	4	5	6	7	8
П1	Применение электромагнитной экранировки помещения (S=120м^2)	Spl Sp2	8000	4,35 126	0,54 7.87	2,34 991,6	994
П2	Радиомониторинг с использованием сканеров	Sp1 Sp2	4500	4,35 126	0,96 14,0	4,17 1764	1768
П3	Зашумление естественных звуководов	Sp3	600	157	78,3	1,23x10^4	1,23x10^4
П4	Зашумление стен	Sp4	3000	15,7	5,23	82,1	82,1
П5	Зашумление труб системы отопления	Sp5	600	4,5	7,5	33,7	33,7
Пб	Использование рентгенепросмотровых устройств (контроль вещей)	Sp6	8000	0,7	0,13	0,10	0,10
П7	Применение магнитомеров (обнаружение диктофонов)	Sp6	1500	0,7	0,7	0,49	0,49
П8	Повышение звукоизоляции окон и дверей	Sp7	1000	0,3	0,6	0,18	0,18
П9	Использование специальных жалюзей и штор	Sp8 Sp9 Sp10	500	3,94 0,11 0,47	47,2 22,0 47,0	186 2,42 22,1	210,5
П10	Специальный осмотр телефонных аппаратов	Sp11	200	157	157	2,46x10^4	2,46x10^4
П11	Применение фильтра в телефонной сети	Spl2	50	52,3	420	2,2x10^4	2,2x10^4
П12	Применение специальных переговорных устройств	Sp14	1000	12,6	63.0	793	793
П13	Применение фильтра в электросети	Sp13	300	157	210	3,3x10'	3,3x10^4
П14	Контроль извне, поиск КП и др.	Sp14	10 000	2,1	6,3	13,2	13,2

Примечание. Расчет проводился для Z =1.

Из таблицы видно, что для защиты речевой информации с достаточным уровнем ($Q > 99$ %) необходимо не менее 15 тыс. дол. на помещение площадью 30 м^2. При высоком уровне защиты ($Q >$ 99,9 %) эта цифра увеличивается до 28 тыс. дол.

Ниже приводится перечень инженерно-технических средств, обеспечивающих достаточный уровень защиты речевой информации ($Q \geq 99$ %):

– применение фильтров в электросети;

– осмотр телефонных аппаратов, поиск закладных устройств;

– применение специального фильтра в телефонной сети;

– зашумление естественных звуководов;

– осуществление радиомониторинга с использованием сканеров;

– применение электромагнитной экранировки помещений;

– применение (при необходимости) специальных переговорных устройств;

– использование специальных жалюзи и штор.

Для нахождения наилучшего набора средств защиты (по критерию стоимость/эффективность) рекомендуется повторить расчет для других устройств защиты, обладающих необходимыми характеристиками. Сравнивая полученные варианты, выбираем тот, который при обеспечении заданной эффективности требует меньше затрат, или при выделенных ресурсах позволяет повысить эффективность защиты и повысить ее рентабельность.

Таблица 17. Противодействия акустическим угрозам

NN	Код защиты	Код угроз	Ранг (η_0)	Стоимость противодействия, (дол.)	Нарастание затрат (дол.)	Рост эффективности Q(%)
1	2	3	4	5	6	7
1	П13	Sp13	$3{,}3 \times 10^4$	300	300	24,4
2	П10	Spl1	$2{,}46 \times 10^4$	200	500	36.6
3	П11	Sp12	$2{,}2 \times 10^4$	50	550	39,3
4	П3	Sp3	$1{,}23 \times 10^4$	600	1150	57,5
5	П2	Spl, Sp2	1768	4500	5650	77,1

NN	Код защиты	Код угроз	Ранг (η_0)	Стоимость противодействия, (дол.)	Нарастание затрат (дол.)	Рост эффективности Q(%)
1	2	3	4	5	6	7
6	П1	Spl, Sp2	994	8000	13 650	96.8
7	П12	Sp14	793	1000	14650	98,7
8	П9	Sp8, Sp9 Sp10	210	500	15 150	99.0
9	П4	Sp4	82	3000	18 150	99,6
10	П5	Sp5	34	600	18750	99,7
11	П14	Sp15	13	10000	28750	99,9
12	П7	Sp6	0.5	1500	30250	99,99
13	П8	Sp7	0,2	1000	31 250	99,99
14	П6	Sp6	0.1	8000	39250	100

Контрольные вопросы к практической работе 4

1. Перечислите средства обеспечения безопасности передачи речевой информации.

2. Что такое приоритет средства защиты?

3. Каким критерием следует руководствоваться при выборе средств защиты?

4. Какие существуют средства противодействия акустическим угрозам?

5. Как применение электромагнитной экранировки помещений повышает защищённость информации от утечек по акустическому каналу?

Список сокращений

ТСПИ – технические средства приема, обработки, хранения и передачи информации

ВТСС – вспомогательные технические средства и системы

КПП – контрольно-пропускной пункт

ПЭВМ – персональная электронно-вычислительная машина

ТА – телефонный аппарат

АТС – автоматическая телефонная станция

КЗ – контролируемая зона

ТКУИ – технический канал утечки информации

ТСР – технические средства разведки

ПЭМИ – побочные электромагнитные излучения

ВЧ – высокочастотный

УНЧ – усилители низкой частоты

ИК – диаазон – инфракрасный диапазон

ЛАЛС – лазерные акустические локационные системы

Библиографический список

1. Торокин А.А. Основы инженерно-технической защиты информации. – М.: Изд-во “Ось-89”, 1998 г. – 336 с.

2. Хорев А.А Способы и средства защиты информации. М.: МО РФ, 2000 г. – 316 с.

3. Энциклопедия промышленного шпионажа/ Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко / под общ. Ред. Е.В Куренкова. – С. Петербург: ООО “Изд-во Полигон”, 1999. – 512 с.

4. Корнеев И.К, Степанов Е.А. Информационная безопасность и защита информации: Учебное пособие. –М.: ИНФРА – М, 2001. – 304с. – (Серия высшее образование).

5. Хорев А. А. Технические каналы утечки акустической (речевой) информации. – «Специальная Техника» № 1, 1998.

6. Железняк В.К., Макаров Ю.К., Хорев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации. – «Специальная техника» №4, 2000.

7. Хорев А.А., Методы и средства защиты телефонных линий.