МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«11» 04 2023 г.

# ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Методические указания по выполнению лабораторных работ для студентов направления подготовки 10.03.01«Информационная безопасность» и специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»

Курск 2023

УДК 004

Составители: Е.А. Кулешова.

Рецензент

Кандидат технических наук, доцент кафедры

вычислительной техники *А.В. Киселев*

**Защита информации от утечки по техническим каналам:** Методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун- т; сост.: Е.А. Кулешова. Курск, 2023. 52 с., Библиогр.: с. 52.

Содержат сведения по вопросам формирования у студентов знаний по основам технической защиты информации, а также развития в процессе обучения системного мышления, необходимого для решения задач технической защиты информации.

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

Предназначены для студентов направления подготовки 10.03.01«Информационная безопасность» и специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Текст печатается в авторской редакции

Подписано в печать. Формат 60х84 1/16.

Усл.печ.л. 3,08 .Уч.-изд.л. 1,97 .Тираж 30 экз. Заказ 246

Юго-Западный государственный университет.

# Оглавление

## Работа №1. Анализ технических средств перехвата информации в оптическом диапазоне

**Цель работы** - ознакомится со способами формирования оптического канала утечки и способами предотвращения утечки информации по оптическим каналам. Провести анализ технических средств перехвата информации в оптическом диапазоне.

В оптическом (видимом) диапазоне волн информация добывается путем визуального, визуально-оптического и телевизионного наблюдения, фото- и киносъемки, а в инфракрасном диапазоне — с использованием приборов ночного видения и тепловизоров.

Наибольшее количество признаков добывается в видимом диапазоне. Но видимый свет как носитель информации имеет малую проникающую способность, дальность его распространения в атмосфере сильно зависит от ее состояния, климатических и погодных условий. Инфракрасные лучи как носители информации обладают большей проникающей способностью и позволяют наблюдать объекты при малой освещенности и даже в темноте. Но при их преобразовании в видимый свет для обеспечения возможности наблюдения объекта человеком происходит значительная потеря информации об объекте.

Так как физическая природа носителя информации в видимом и инфракрасном диапазонах одинакова, то различные средства наблюдения, применяемые для добывания информации в этом диапазоне, имеют достаточно общую структуру. Ее можно представить в виде, приведенном на рис. 1.1.


Рисунок 1.1. - Структурная схема оптического приемника

Большинство средств наблюдения представляют собой оптический приемник, содержащий оптическую систему, светоэлектрический элемент, усилитель и индикатор. В зависимости от вида светочувствительного элемента оптические приборы делятся на **визуально-оптические**, **фотографические** и **оптико-электронные**. В визуально-оптических средствах наблюдения светочувствительным элементом является сетчатка глаза человека, в традиционных фото- и киноаппаратах — фотопленка, а в

оптико-электронных приборах — мишень светоэлектрического преобразователя (СЭП).

Оптическая система или объектив проецирует световой поток от объекта наблюдения на поверхность светочувствительного элемента. Светочувствительный элемент преобразует оптическое изображение в эквивалентное распределение плотности химического вещества или электронное изображение, количество «свободных» электронов каждой точки которого пропорционально яркости соответствующей точки оптического изображения. Способы визуализации изображения для разных типов оптического приемника могут существенно отличаться. Изображение в виде зрительного образа формируется в мозгу человека, на фотопленке — в результате химической обработки светочувствительного слоя, на экране технического средства — путем параллельного или последовательного съема электронов со светоэлектрического элемента, усиления электрических сигналов и формирования под их действием видимого изображения на экране оптического приемника.

Характеристики средств наблюдения определяются, прежде всего, параметрами оптической системы и светоэлектрического элемента, а также зависят от способов обработки электрических сигналов и формирования изображения при индикации. Основными характеристиками являются:

- диапазон длин волн световых лучей, воспринимаемых средством наблюдения;
- чувствительность;
- разрешающая способность;
- поле (угол) зрения и изображения;
- динамический диапазон интенсивности света на входе оптического приемника, не вызывающий искажение изображения на его выходе.

Средства наблюдения в зависимости от назначения создаются для видимого диапазона длин волн или его отдельных участков, а также для различных участков инфракрасного диапазона.

**Чувствительность** средства наблюдения оценивается минимальным уровнем световой энергии, при которой обеспечивается требуемое качество изображения объекта наблюдения. Качество изображения зависит как от яркости и контрастности проецируемого изображения, так и от помех. Помехи создают лучи света, попадающие на вход приемника от других источников света, и тепловые шумы светоэлектрического преобразователя. На экране светочувствительного элемента при посторонней внешней

засветке ухудшается контраст изображения аналогично варианту прямого попадания на экран телевизионного приемника или монитора компьютера яркого солнечного света.

**Разрешающая способность** характеризуется минимальными линейными или угловыми размерами между двумя соседними точками изображения, которые наблюдаются как отдельные. Так как изображение формируется из точек (пикселей), размеры которых определяются разрешающей способностью средства наблюдения, то вероятность обнаружения и распознавания объекта возрастает с повышением разрешающей способности средства наблюдения (увеличением количества пикселей изображения объекта).

Размеры наблюдаемой части пространства характеризуются **полем** и **углом зрения**. Поле зрения — часть пространства, изображение которого проецируется на экран оптического приемника. Угол, под которым средство «видит» предметное пространство, называется **углом поля зрения**. Часть поля зрения, удовлетворяющего требованиям к качеству изображения по резкости, называется **полем** или, соответственно, **углом поля изображения**.

**Динамический диапазон** оптического приемника определяет в дБ интервал силы света на входе оптического приемника, при котором обеспечивается заданное качество изображения на выходе. Чем шире динамический диапазон оптического приемника, тем больше оперативные возможности его применения. Несоответствие динамического диапазона приемника диапазону силы света от объектов наблюдения приводит не только к искажению добываемой информации, но и может вызвать нарушение в работе приемника вплоть до разрушения светочувствительного элемента. Например, если человек посмотрит открытыми глазами на солнце, то он в течение некоторого времени «слепнет».

Наиболее совершенным средством наблюдения в видимом диапазоне является зрительная система человека, включающая глаза и области мозга, осуществляющие обработку сигналов, поступающих с сетчатки глаз.

Уникальные возможности зрительной системы человека обеспечиваются, прежде всего, оптической системой глаза, выполняющего функции объектива. Ее возможности и достигаются в результате того, что его кривизна с помощью специальных глазных мышц изменяется таким образом, чтобы обеспечить на сетчатке глаза максимально четкое изображение объектов, расположенных на различных расстояниях от наблюдателя. Хотя ведутся исследования по созданию подобных

искусственных объективов, но приблизиться к возможностям глаза пока не удается.

**Существует несколько стандартных схем формирования канала**:

1. Объект наблюдения — документ, экран монитора, полезная модель, находящиеся в помещении. Среда передачи оптического сигнала — воздух или воздух в сочетании с оконным стеклом. Устройство или инструмент наблюдения — человеческий глаз, бинокль, фотоаппарат, видеокамера.

2. Объект — оборудование, полезные модели, иные объекты, находящиеся на открытом воздухе, во дворе предприятия, на железнодорожной платформе, в кузове грузовика. Среда передачи сигнала — воздух или безвоздушное пространство космоса при съемках со спутника. Инструменты наблюдения — фотоаппараты, инфракрасные устройства, телевизионные камеры.

3. Объект наблюдения — человек, находящийся в помещении или на открытом пространстве. Среда распространения сигнала — воздух или воздух в сочетании со стеклом, если наблюдатель находится за окном помещения. Устройство снятия информации — глаз, бинокль, фото или видеоаппаратура, иногда аналог инфракрасного прицела стрелкового оружия.

Оптические каналы утечки информации не ограничиваются человеческим зрением, его возможности расширяются при помощи технических средств. Снимаются помехи, вызываемые удаленностью объекта, недостаточной освещенностью помещения, невысоким угловым разрешением. Среди традиционных способов использования оптического канала:

- ✓ просмотр документов и экрана монитора из окна соседнего здания с использованием мощного бинокля;
- ✓ фотографирование документов и монитора камерой мобильного телефона.

Но не менее часто применяются методы снятия оптических излучений, модулированных информацией, при помощи оптических датчиков, работающих в обычном или инфракрасном диапазоне. Документирование полученных данных раньше производилось на фотопленку, сейчас используются электронные носители информации.

Показатели, характеризующие оптический прибор:

- угловое разрешение;
- необходимая для работы степень освещенности;
- частота смены изображения.

Устройства съема данных.

Микрофотокамеры известны многим по детективным книгам и фильмам. Обычно они применяются для фиксации результатов наблюдения

вместе с видеокамерами. Видеокамеры бывают проводными, установленными в помещении, запитываемыми от сети и автономными, носимыми на теле, получающими энергию от аккумуляторных батарей. В большинстве случаев записываемую информацию они передают по радиоканалу на установленный вне пределов охраняемого периметра приемник, сигнал часто шифруется или модулируется.

Особенности современной аппаратуры таковы, что наблюдение ведется при ночном освещении, при удаленности объекта на несколько километров, в инфракрасном диапазоне, который позволяет увидеть исправления, измененные части документа, подделки, прочесть текст на пепле от сожженного письма.

В условиях недостаточной освещенности для снятия информации с оптических каналов утечки применяются приборы ночного видения и тепловизоры. Принципом их работы становится преобразование светового поля слабой интенсивности в поле электронов, с дальнейшим усилением получаемого изображения при помощи макроканального усилителя. Усиленное изображение становится видимым на люминесцентном экране, для большинства приборов оно отображается в зеленой области спектра. Появившееся на экране изображение изучается при помощи регистрирующего прибора, при его отсутствии поможет обычная лупа.

Наблюдение ведется на границе ближнего инфракрасного диапазона (740—1400 нм), дополнительно применяется лазерная инфракрасная подсветка. По этому принципу сконструированы комплекты для ночного дистанционного наблюдения с использованием инфракрасного лазерного фонаря. Такие устройства выполняются в виде визиров, биноклей, устройств прицела для стрелкового оружия.

Тепловизоры предназначены для наблюдения за участками спектра с длинными волнами (8—13 мкм), здесь концентрируется наибольшее тепловое излучение от предметов. Они позволяют проводить наблюдения в условиях обильных осадков. Приборы для документирования изображения — отдельная категория устройств для снятия информации с оптических каналов утечки.

**Предотвращение утечки информации по оптическим каналам.**

Основным способом борьбы с утечкой информации по оптическим каналам связи остается затруднение доступа злоумышленника к объектам, содержащим секретные данные. Вторая задача — выявление закладных устройств. Принципы выявления стандартны:

- фиксация радиосигнала;
- фиксация повышенного электромагнитного излучения;

– просвечивание рентгеновскими лучами с целью выявления проводников;

– поиск проводов, ведущих неизвестно куда.

Поиск побочных электромагнитных излучений, или метод нелинейной локации, применяется наиболее часто. Каждая используемая в закладном устройстве микросхема имеет собственный спектр побочного излучения. Зная применяемые спектры, можно идентифицировать радиоустройство. Электронные схемы управления матрицами камер также излучают характерный спектр, облегчающий поиск. Помешать работе может присущее современному миру большое количество побочных электромагнитных излучений, идущих от оборудования, компьютеров, мобильных телефонов, линий связи.

Для выявления закладных устройств, модулирующих работу светодиодной лампы и преобразующих свет в информационный сигнал, необходимо выполнить следующий комплекс действий:

– использование чувствительных фотосенсоров для измерения изменений уровня светимости светодиода. Основу для измерений составит коэффициент пульсаций светодиодов, его значение не должно превышать 4 %;

– визуальная проверка всех ламп в помещении на наличие высокочастотного преобразователя-усилителя цепи;

– анализ структуры помещения, выявление всех отверстий, щелей, прозрачных объектов — окон, части дверей в помещении, перегородок в переговорной на поиск каналов распространения света и изучение пространства вокруг них с целью обнаружения приемных устройств.

Строя систему защиты оптических каналов, необходимо предусмотреть реализацию следующих мероприятий:

1. Построить схему расположения объектов защиты таким образом, чтобы исключить отражение видимого света в сторону гипотетического местоположения злоумышленника.

2. Изменить отражающие свойства объекта защиты. Чехол из оптических метаматериалов способен сделать предметы невидимыми.

3. Снизить уровень освещенности текста или предмета, поставив энергетические ограничения на снятие информации.

4. Применять средства ослабления отраженного света — шторы, жалюзи, темные или матовые стекла, иные ограждения, затрудняющие распространение сигнала.

5. Использовать различные методы маскировки, имитации скрываемых предметов под другие объекты, чтобы ввести злоумышленника в заблуждение.

6. Использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражательного или излученного света и других излучений.

7. Маскировать объекты защиты при помощи варьирования отражательных характеристик и контрастов между цветом и освещенностью фона и объекта.

Понимая финансовый и технический потенциал вероятных противников — конкурентов, технических разведок, можно составить план обеспечения информационной безопасности, основой которого станут затруднения доступа к объектам изучения. Так, при риске съема данных со спутника скрываемое новейшее оборудование необходимо защитить прочной упаковкой, мониторы ставить так, чтобы их не было видно из окон, документы оставлять на столе чистой стороной вверх. Регламентация простых действий снизит уровень рисков использования злоумышленником оптических каналов утечки информации.

**Задание.** Провести анализ технических средств перехвата информации в оптическом диапазоне волн, используя каталог технических средств защиты информации, представленный на сайте **http://bnti.ru/** (Техника для спецслужб. Бюро научно-технической информации.).

Для выполнения данной работы необходимо использовать следующие каталоги:

1) «Оборудование для оперативно-розыскной деятельности» / «Средства скрытого видеонаблюдения»

2) «Оборудование для оперативно-розыскной деятельности» / «Средства скрытого фотографирования»

3) «Оборудование для оперативно-розыскной деятельности» / «Системы перехвата каналов связи» / «Системы контроля оптических линий связи»

4) «Тепловизионные и оптические системы».

Проведите подробный анализ 8-10 средств технической защиты из перечисленных выше каталогов и занесите данные в таблицу.

Пример.

| | Наименование | Изображение | Технические характеристики |
|---|---|---|---|
| 1 | Очки-телекамера |  | ПЗС матрица 1/3 Sony<br>Разрешение 400 твл<br>Минимальная освещённость 0,05Лк<br>Угол обзора 88 ° С<br>Потребляемый ток менее 20мА<br>Рабочие температуры - 10 ° С - + 50 ° С<br>….. и т.д. |
| … | … | … | … |
| 10 | Малогабаритный фотоаппарат "Зенит-МФ-1" |  | Размер кадра на фотопленке, мм 18х24<br>Выдержки, с1/10, 1/30, 1/100<br>Фокусное расстояние объектива, мм28<br>Наибольшее относительное отверстие, мм 1:2,8<br>Емкость кассеты, кадр 14<br>Привод пружинный<br>Габаритные размеры, мм 77,2х40,5х55<br>….. и т.д. |

**Контрольные вопросы:**

1) Перечислите характеристики технического канала утечки информации.

2) Перечислите показатели, характеризующие оптический прибор перехвата.

3) Перечислите принципы выявления закладных устройств оптического перехвата.

4) Каковы основные способом борьбы с утечкой информации по оптическим каналам?

5) Какие мероприятия должны быть предусмотрены при построении системы защиты оптических каналов?

6) Перечислите характеристики средств наблюдения.

## Работа №2. Анализ технических средств перехвата информации в радиоэлектронном и электромагнитном диапазонах

**Цель работы** - ознакомится со способами формирования канала утечки и способами предотвращения утечки информации по техническим каналам. Провести анализ технических средств перехвата информации в радиоэлектронном и электромагнитном диапазонах.

Задачу перехвата электрических, магнитных и электромагнитных волн, а также связанных с ними сигналов выполняют органы радиотехнической разведки. При этом выполняются следующие мероприятия:

- Поиск сигналов с нужной информацией в пространстве, с помощью анализирования частот
- Обнаружение интересующих сигналов и их выделение
- Усиление и последующий съём сигналов
- Определение источников сигналов
- Анализ технических характеристик сигналов
- Целостная обработка полученных данных, производимая с целью определения первичных признаков источника сигнала или текста перехваченного сообщения.

Любой комплекс аппаратуры, используемый для перехвата, можно представить в виде типовой схемы (рис.1).

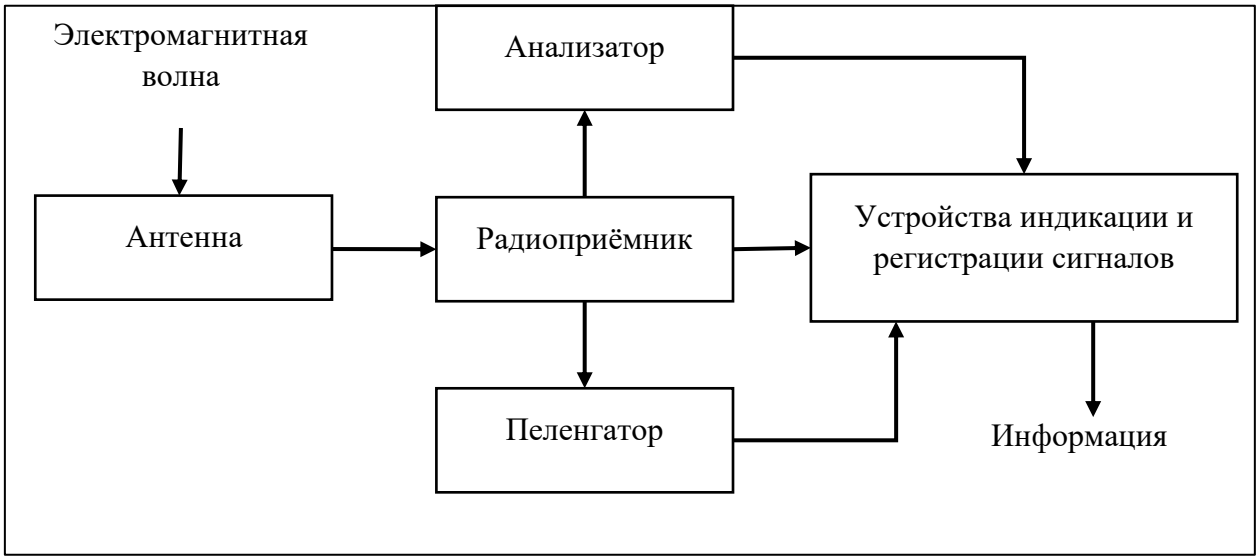



Рисунок 1 – Комплекс средств перехвата радиосигналов

**Антенна** предназначена для пространственной селекции и преобразования электромагнитной волны в совпадающие по амплитуде, фазе и частоте электрические сигналы.

В **радиоприемнике** производится поиск и селекция радиосигналов по частоте, усиление и детектирование выделенных сигналов, усиление и обработка первичных сигналов: речевых, цифровых данных, видеосигналов и т. д.

Для анализа радиосигналов после частотной селекции и усиления они подаются на входы измерительной аппаратуры **анализатора**, определяющей параметры сигналов: частотные, временные, энергетические, виды модуляции, структуру кодов и др.

**Радиопеленгатор** предназначен для определения направления на источник излучения или его координат.

**Регистрирующее устройство** обеспечивает запись сигналов для документирования и последующей обработки.

Антенны представляют собой электромеханические конструкции из токопроводящих элементов, размеры и конфигурация которых определяют эффективность преобразования электрических сигналов в радиосигналы (для передающих антенн) и радиосигналов в электрические сигналы (для приемных антенн).

Классификация антенн:

- По назначению
  - Передающие
  - Приёмные
  - Приёмо-передающие
- По диапазону частот
  - Длинноволновые
  - Средневолновые
  - Коротковолновые
  - Для УКВ
- По типу излучателя
  - Линейные
  - Апертурные
  - Для поверхностных волн
- По месту установки
  - Наземные
  - Автомобильные
  - Самолётные

- На космических аппаратах

**Радиоприемник** – основное техническое средство перехвата, осуществляющее поиск, селекцию, прием и обработку радиосигналов. В состав его входят устройства, выполняющие:

- Перестройку частоты настройки приемника и селекцию нужного радиосигнала;
- Усиление выделенного сигнала;
- Съем информации;
- Усиление низкочастотного первичного сигнала.

Основными техническими характеристиками радиоприемника являются:

- Диапазон принимаемых частот;
- Чувствительность;
- Избирательность;
- Динамический диапазон;
- Качество воспроизведения принимаемого сигнала (уровни нелинейных и фазовых искажений);
- Эксплуатационные параметры.

Различают два вида радиоприемников: прямого усиления и супергетеродинные. Появившиеся первыми приемники прямого усиления уступили супергетеродинным почти во всех радиодиапазонах, за исключением сверхвысоких частот. Такая тенденция объясняется более высокой селективностью и чувствительностью супергетеродинного радиоприемника по сравнению с приемником прямого усиления.

**Задание.** Провести анализ технических средств перехвата информации радиоэлектронном и электромагнитном диапазонах, используя каталог технических средств защиты информации, представленный на сайте **http://bnti.ru/** (Техника для спецслужб. Бюро научно-технической информации.).

Для выполнения данной работы необходимо использовать следующие каталоги:

1) «Оборудование для оперативно-розыскной деятельности» / «Системы перехвата каналов связи» / «Системы перехвата сотовой связи»

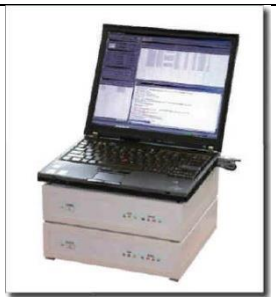
2) «Оборудование для оперативно-розыскной деятельности» / «Системы перехвата каналов связи» / «Системы перехвата спутниковой связи»

3) «Оборудование для оперативно-розыскной деятельности» / «Системы перехвата каналов связи» / «Системы перехвата пейджинговой связи»

4) «Оборудование для оперативно-розыскной деятельности» / «Системы перехвата каналов связи» / «Системы перехвата факсов»

Проведите подробный анализ 8-10 средств технической защиты из перечисленных выше каталогов и занесите данные в таблицу.

Пример.

| | Наименование | Изображение | Технические характеристики |
|---|---|---|---|
| 1 | Система перехвата мобильной спутниковой связи Thuraya "IB0501" |  | Передача голоса на стационарный или портативный терминалы: Thuraya SO-2510, SG-2520, Hughes 7100/7101 (сняты с производства), Ascom 21 (снят с производства). SMS.<br>Передача данных и факсов на скорости 9,6 kbit/s.<br>Мобильный сервис передачи данных GMPRS на терминалах SO и SG — 60 кбит/с к терминалу и 15 кбит/с в канале.<br>….. и т.д. |
| … | … | … | … |
| 10 | Система мониторинга GSM-сетей с алгоритмом шифрования A5/1 "SIM - Phoenix" |  | рабочий диапазон 900 MHz/ 1800MHz GSM<br>алгоритм A5/1 и A5/2<br>полная система мониторинга с BTS<br>функция реального времени отслеживание до 7 соединений одновременно<br>….. и т.д. |

**Контрольные вопросы:**

1. Какие задачи выполняют органы радиотехнической разведки?
2. Из чего состоит типовой комплекс перехвата радиосигналов?
3. Что такое антенна?
4. Что такое радиоприёмник?
5. Функции радиоприёмника
6. Виды радиоприёмников

## Работа №3. Анализ технических средств перехвата информации в акустическом диапазоне

**Цель работы** - ознакомится со способами формирования канала утечки и способами предотвращения утечки информации по акустическим каналам. Провести анализ технических средств перехвата информации в акустическом диапазоне.

Под акустической информацией обычно понимается информация, носителями которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическая информация называется речевой.

Первичными источниками акустических сигналов являются механические колебательные системы, например, органы речи человека, а вторичными - преобразователи различного типа, например, громкоговорители.

В соответствии с, под утечкой информации по техническому каналу понимается неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

В зависимости от физической природы возникновения информационных сигналов, среды их распространения технические каналы утечки акустической (речевой) информации можно разделить на прямые акустические (воздушные), акустовибрационные (вибрационные), акустооптические (лазерные), акустоэлектрические и акустоэлектромагнитные (параметрические).

### Средства перехвата акустической информации

В прямых акустических (воздушных) технических каналах утечки информации (рисунок 1) средой распространения акустических сигналов является воздух. В качестве датчиков средств разведки используются высокочувствительные микрофоны, преобразующие акустический сигнал в электрический.

В аппаратуре акустической разведки используются микрофоны различных типов с чувствительностью 30 - 60 мВ/Па, обеспечивающие регистрацию речи средней громкости на удалении до 7 - 10 м от её источника. При этом частотный диапазон составляет в основном от 50-100 Гц до 5 - 20 кГц.

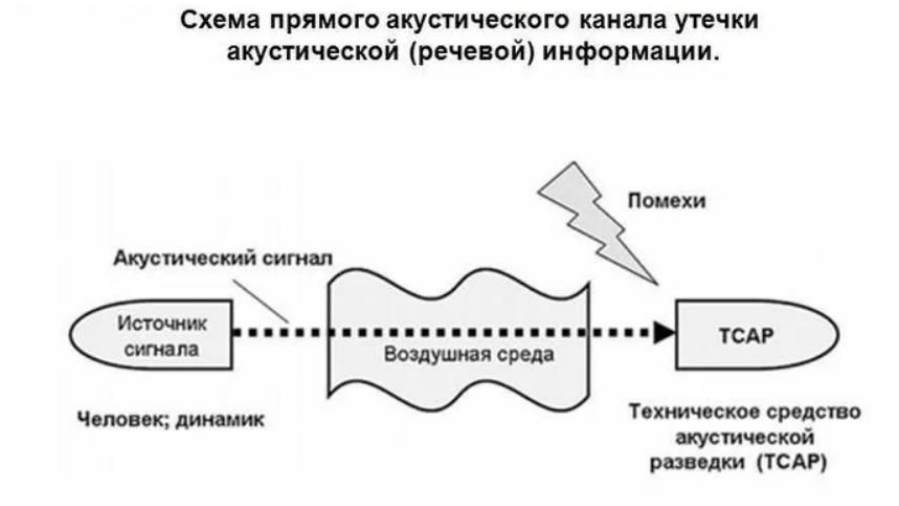



Рисунок 1 - Распространения акустических сигналов

Перехват акустической (речевой) информации из выделенных помещений по данному каналу может осуществляться:

1. С использованием портативных устройств звукозаписи (диктофонов), скрытно установленных в выделенном помещении;
2. С использованием электронных устройств перехвата информации (закладных устройств) с датчиками микрофонного типа (преобразователями акустических сигналов, распространяющихся в воздушной среде), скрытно установленных в выделенном помещении, с передачей информации по радиоканалу, оптическому каналу, электросети 220 В, телефонной линии, соединительным линиям ВТСС и специально проложенным кабелям;
3. С использованием направленных микрофонов, размещённых в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны;
4. Без применения технических средств (из-за недостаточной звукоизоляции ограждающих конструкций выделенных помещений и их инженерно-технических систем) посторонними лицами (посетителями, техническим персоналом) при их нахождении в коридорах и смежных помещениях (непреднамеренное прослушивание).

Использование тех или иных средств акустической разведки определяется возможностью доступа в контролируемое помещение посторонних лиц. Если посторонние лица не имеют постоянного доступа в выделенное помещение, но имеется возможность его регулярного кратковременного посещения под различными предлогами (например, для проверки системы освещения, кондиционирования или уборки помещения), то для перехвата речевой информации могут использоваться портативные устройства звукозаписи (в основном цифровые диктофоны), которые скрытно

устанавливаются в интерьерах помещений, как правило, непосредственно перед проведением закрытого мероприятия (рисунок 2). После окончания мероприятия диктофон из помещения изымается. Такие устройства также могут камуфлироваться под предметы повседневного обихода, например, книги, письменные приборы, пачки сигарет и т.д.

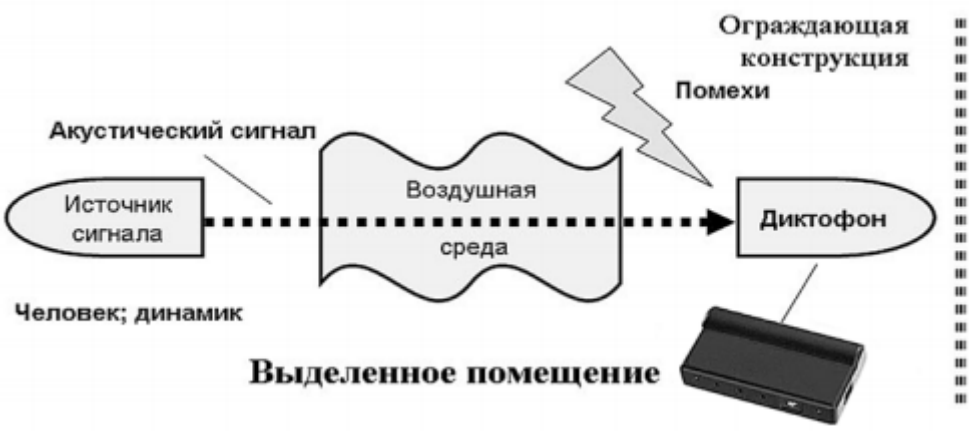



Рисунок 2 - Перехват речевой информации с помощью диктофона

В настоящее время зарубежными и отечественными фирмами выпускается огромное количество портативных цифровых диктофонов, которые очень легко спрятать практически в любом помещении. Цифровые диктофоны могут быть встроены в авторучку, наручные часы и т.п.

Недостатком способа перехвата речевой информации с использованием портативных диктофонов является необходимость повторного проникновения в выделенное помещение с целью изъятия диктофона для прослушивания записанных разговоров. Такого недостатка лишены электронные устройства перехвата информации (закладные устройства).

Под закладными устройствами обычно понимают портативные устройства съёма информации, скрытно внедряемые (закладываемые) в выделенные помещения, в том числе в ограждающие конструкции, оборудование, предметы интерьера, а также в технические средства и системы обработки информации, вспомогательные технические средства и системы.

Перехватываемая акустическими закладками информация может передаваться на приёмные пункты по радио- и оптическому каналам, специально проложенным линиям, электросети переменного тока, телефонным линиям и т.д.

В том случае, если имеется постоянный неконтролируемый доступ в выделенное помещение, в нём заранее могут быть установлены миниатюрные микрофоны, соединительные линии которых выводятся в специальные

помещения, где устанавливается регистрирующая или передающая аппаратура. Причём длина соединительного кабеля может достигать 10 км. Такие системы перехвата акустической информации часто называют проводными микрофонными системами (рисунок 12).

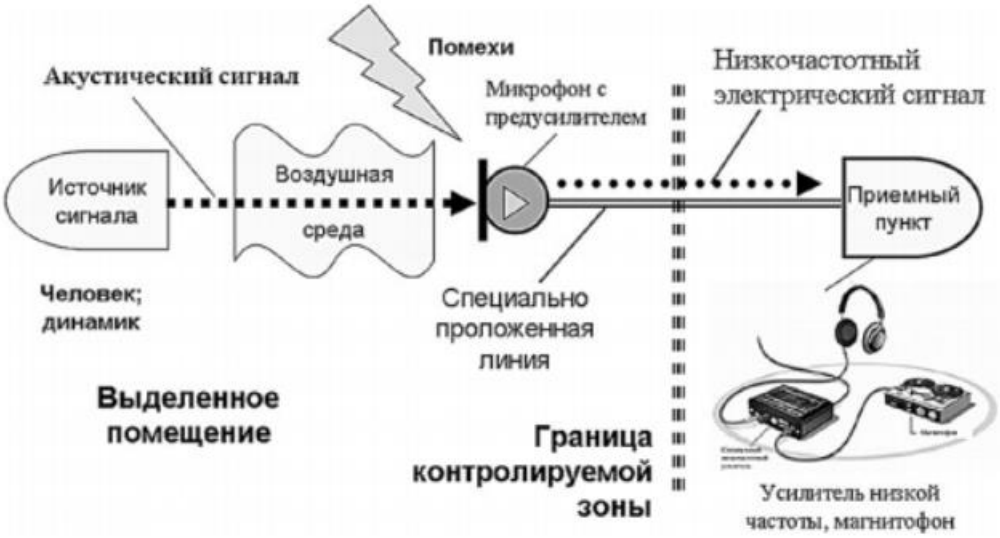



Рисунок 3 - Перехват речевой информации с помощью диктофона

**Задание.** Провести анализ технических средств перехвата информации в акустическом диапазоне волн, используя каталог технических средств защиты информации, представленный на сайте **http://bnti.ru/** (Техника для спецслужб. Бюро научно-технической информации.).

Для выполнения данной работы необходимо использовать следующие каталоги:

1) «Средства многоканальной видео-, аудиозаписи и оповещения» / «Средства многоканальной записи телефонных переговоров»

2) «Средства многоканальной видео-, аудиозаписи и оповещения» / «Средства многоканальной записи переговоров»

3) «Оборудование для оперативно-розыскной деятельности» / «Средства акустического контроля»

4) «Оборудование для оперативно-розыскной деятельности» / «Средства контроля телефонных переговоров»

Проведите подробный анализ 8-10 средств технической защиты из перечисленных выше каталогов и занесите данные в таблицу.

Пример.

| | Наименование | Изображение | Технические характеристики |
|---|---|---|---|
| 1 | Акустический усилитель - насадка с коррекцией АЧХ "Гнездо-03" |  | Акустическое усиление речевого сигнала - +6дБ. Подавление внеполосных помех – не менее 6дБ. Конструктивные размеры – L=40мм., Dвн=8мм., Dвнутр=6мм. ….. и т.д. |
| … | … | … | … |
| 10 | Система слежения за подвижными объектами "Курс" |  | Максимальное количество отсчётов, хранимое в энергонезависимой памяти 4096<br>Источник питания:<br>- встроенная LiPol аккумуляторная батарея 3,6 В, 3300 мА/ч<br>- внешний источник 12 В, 1,5 А<br>….<br>и т.д. |

**Контрольные вопросы**

1 Область применения параболического микрофона?

2 Перечислите акустические закладные устройства.

3 Перечислите акустические закладки использующие телефонные линии.

4 Перечислите методы обработки речевых сигналов.

5 Назовите основные характеристики направленных микрофонов.

## Работа №4. Анализ технических средств перехвата информации в каналах, образованных средствами вычислительной техники

**Цель работы** - ознакомится со способами формирования канала утечки и способами предотвращения утечки информации. Провести анализ технических средств перехвата информации в каналах, образованных средствами вычислительной техники.

Вычислительная техника относится к техническим средствам приема, обработки, хранения и передачи информации.

Под техническими средствами приема, обработки, хранения и передачи информации (ТСПИ) понимают технические средства, непосредственно обрабатывающие конфиденциальную информацию. Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации.

Под техническим каналом утечки информации (ТКУИ) понимают совокупность источника информации (передатчика), линии связи (физической среды – канал с шумами), по которой распространяется информационный сигнал, и технических средств перехвата информации (приемника).

При выявлении ТКУИ ТСПИ необходимо рассматривать как систему, включающую основное оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ТСПИ и их элементами), распределительные и коммутационные устройства, системы электропитания, системы заземления. Такие технические средства называют также *основными техническими средствами.*

Наряду с ТСПИ в помещениях устанавливаются технические средства и системы, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся совместно с ТСПИ и которые могут находиться в зоне электромагнитного поля, создаваемого ТСПИ. 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, средства и системы кондиционирования, электрофикации, радиофикации, часофикации, электробытовые приборы и т.д.

В качестве ТКУИ наибольший интерес представляют ВТСС, имеющие выход за пределы контролируемой зоны (КЗ). Контролируемая зона - территория (либо здание, группа помещений, помещение), на которой исключено неконтролируемое пребывание лиц и транспортных средств, не имеющих постоянного или разового допуска. В КЗ, посредством проведения технических и режимных мероприятий, должны быть созданы условия, предотвращающие возможность утечки из нее конфиденциальной информации. КЗ определяется руководством организации, исходя из конкретной обстановки в месте расположения объекта и возможностей использования технических средств перехвата.

Кроме соединительных линий ТСПИ и ВТСС за пределы КЗ 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.

Случайной антенной является цепь ВТСС или посторонние проводники, способные принимать ПЭМИН. Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенная случайная антенна представляет собой компактное техническое средство (например, телефонный аппарат). К распределенным случайным антеннам относятся кабели, провода, металлические трубы и другие токопроводящие коммуникации.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, ТКУИ можно разделить на *электромагнитные, электрические, параметрические и вибрационные.*

К электромагнитным относятся ТКУИ, возникающие за счет различного вида побочных электромагнитных излучений и наводок (ПЭМИН) ТСПИ:

- электромагнитные излучения элементов ТСПИ;

- излучений на частотах работы высокочастотных (ВЧ) генераторов ТСПИ и ВТСС;

- излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Отметим что, ПЭМИН — это нежелательное информационное электромагнитное излучение, возникающее в результате нелинейных процессов в электрических цепях при обработке информации техническими средствами и приводящее к утечке информации.

*Электромагнитные излучения элементов ТСПИ.* В ТСПИ носителем информации является электрический ток, параметры которого (амплитуда,

частота, либо фаза) изменяются по закону изменения информационного сигнала. При прохождении электрического тока по токоведущим элементам ТСПИ вокруг них возникает электрическое и магнитное поля. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, несущего информацию.

*Электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ и ВТСС.* В состав ТСПИ и ВТСС могут входить различного рода высокочастотные генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных и телевизионных устройств и т.д. В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах ВЧ-генераторов наводятся электрические сигналы, которые могут вызвать паразитную модуляцию собственных ВЧ-колебаний генераторов. Эти модулированные ВЧ-колебания излучаются в окружающее пространство.

*Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ.* Самовозбуждение УНЧ ТСПИ (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т.п.) возможно за счет образования случайных паразитных обратных связей, что приводит к переводу усилителя в режим автогенерации сигналов. Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе УНЧ в нелинейный режим работы, т.е. в режим перегрузки.

Перехват ПЭМИН ТСПИ и ВТСС осуществляется средствами радиотехнической разведки, размещенными вне КЗ.

Электрические каналы ТКУИ возникают за счет:

- наводок электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы КЗ;

- просачивания информационных сигналов в линии электропитания;
- просачивания информационных сигналов в цепи заземления ТСПИ;
- использования закладных устройств (ЗУ).

*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.

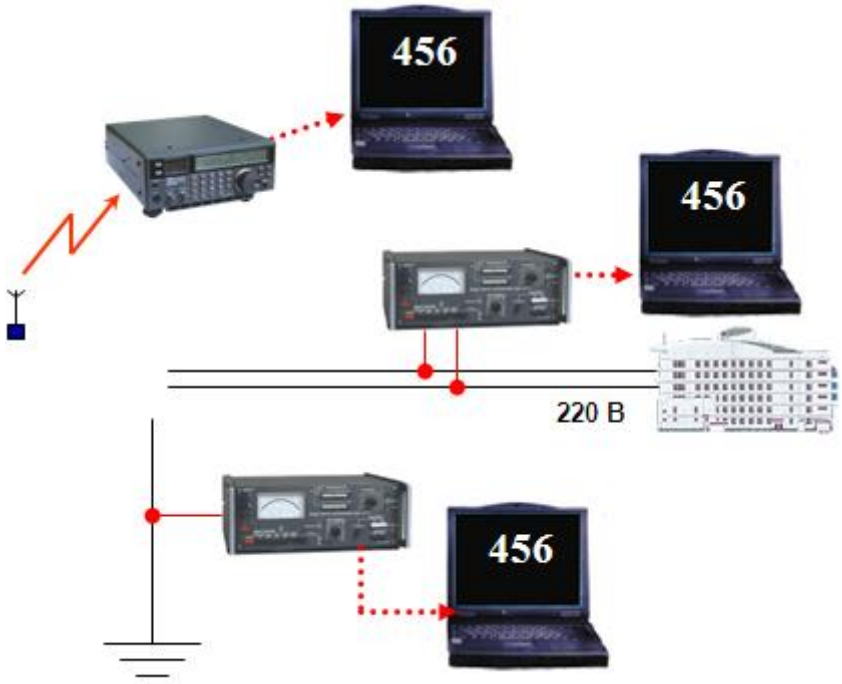
*Просачивание информационных сигналов в линии электропитания* возможно при наличии магнитных связей между выходным трансформатором усилителя (например, УНЧ) и трансформатором блока питания. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении дополнительное напряжение, которое может быть обнаружено в линии электропитания. Информационный сигнал может проникнуть в линию электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

*Просачивание информационных сигналов в цепи заземления.* Кроме заземляющих проводников, служащих для непосредственного соединения ТСПИ с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы КЗ. К ним относятся нулевой провод сети электропитания, экраны соединительных кабелей, металлические трубы систем отопления и водоснабжения, металлическая арматура железобетонных конструкций и т.д. Все эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, в которую могут просачиваться информационные сигналы.

Перехват информационных сигналов возможен путем непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам, проходящим через помещения, где установлены ТСПИ, а также к их системам электропитания и заземления.

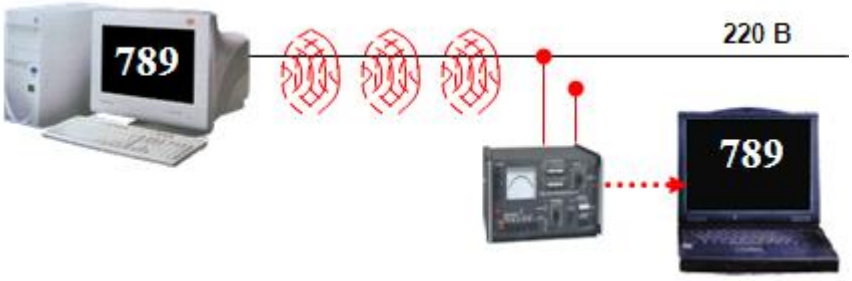
В частном случае, съем информации, обрабатываемой в ТСПИ, возможен также путем установки в них электронных устройств перехвата - *закладных устройств (ЗУ).* Эти устройства представляют собой мини-передатчики, излучение которых модулируется информационным сигналом.

Электронные устройства перехвата информации, устанавливаемые в ТСПИ, иногда называют аппаратными закладками. При этом, перехваченная с помощью ЗУ информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а затем по команде передается на контрольный пункт перехвата.

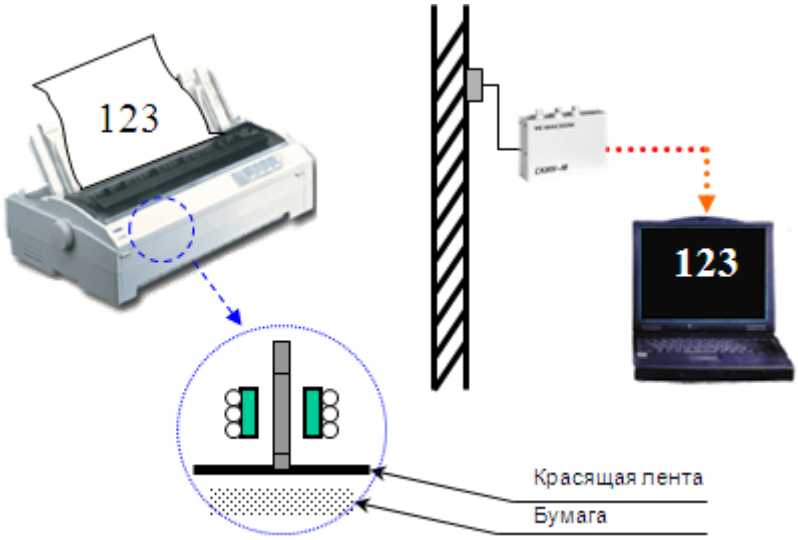



**Параметрический канал**. В этом случае перехват информации возможен путем «высокочастотного облучения» ТСПИ. При взаимодействии облучающего электромагнитного поля с элементами ТСПИ происходит переизлучение электромагнитного поля. В ряде случаев это вторичное излучение имеет модуляцию, обусловленную воздействием информационного сигнала. Поскольку переизлученное электромагнитное поле имеет параметры, отличные от облучающего поля, данный канал утечки информации часто называют *параметрическим.*

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



**Вибрационный канал**. Некоторые ТСПИ имеют в своем составе печатающие устройства, для которых можно найти соответствие между распечатываемым символом и его акустическим образом. Данный принцип лежит в основе канала утечки информации по вибрационному каналу.




**Задание.**

1) Изучить технические средства перехвата информации в каналах, образованных средствами вычислительной техники, используя каталог технических средств защиты информации, представленный на сайте **http://bnti.ru/** (Техника для спецслужб. Бюро научно-технической информации.). Для выполнения данной работы необходимо использовать следующие каталоги: «Оборудование для оперативно-розыскной деятельности / Системы контроля электронной информации / Системы контроля электронной информации в компьютерных сетях»

2) Изучить состав «кейлоггеров», представленных на сайте **https://www.keyloggers.com/ru/**

3) Провести подробный анализ 8-10 средств технической защиты из перечисленных выше каталогов и занести данные в таблицу.

Пример.

| | Наименование | Изображение | Технические характеристики |
|---|---|---|---|
| 1 | Комплекс сбора и анализа Wi-Fi трафика "Виток-WiFi" |  | Число поддерживаемых адаптеров Wi-Fi: 1..16; Поддерживаемые стандарты передачи данных: IEEE 802.11 ….. и т.д. |

| | | | |
|---|---|---|---|
| … | … | … | … |
| 10 | Spyrix Personal Monitor PRO |  | Доступен на 9 языках, дружественный и понятный интерфейс. В отличие от других рассмотренных кейлоггеров можно использовать для мониторинга вашего компьютера с мобильного телефона с помощью ….. и т.д. |

**Контрольные вопросы**

1) Что такое технические средства приема, обработки, хранения и передачи информации (ТСПИ)?

2) Перечислите технические каналы утечки информации, как они классифицируются в зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата?

3) Что такое ВТСС?

4) Что такое случайная антенна?

5) Что такое электромагнитные каналы утечки информации?

6) Что такое параметрические каналы утечки информации?

## Работа №5. Анализ технических средств перехвата информации в материально-вещественном канале утечки

**Цель работы** - ознакомится со способами формирования канала утечки и способами предотвращения утечки информации. Провести анализ технических средств перехвата информации в материально-вещественном канале утечки.

Деятельность предприятий, имеющих дело с ценной коммерческой информацией, во многом зависит от надежности ее защиты. Для получения сведений о секретных технологиях и экспериментальных разработках злоумышленники пользуются различными материально-вещественными каналами утечки данных. Информация, проходящая по таким каналам, добывается путем исследования веществ или материальных объектов, случайно оказавшихся за пределами рабочей зоны. В этом случае утечка информации происходит по техническим причинам или по недосмотру персонала.

**Структура вещественных каналов**

Особенность материально-вещественного канала утечки информации состоит в том, что его наличие позволяет получать секретные сведения, находясь за пределами предприятия. Для получения информации изучаются внешние признаки объектов, физические и химические свойства твердых, газообразных и жидких веществ, случайно попадающих в окружающую среду с территории производства.

**В структуру канала, по которому происходит утечка информации, входят:**

– Источники данных;

– Линии физического перемещения носителей информации по каналу (людей или вещественных объектов);

– Технические средства перехвата информационных сигналов.

– О деятельности предприятия судят по так называемым «демаскирующим признакам», которые обнаруживаются с помощью специальных средств и приборов.

– Демаскирующие признаки подразделяют на следующие группы:

– Видовые (цвет, структура поверхности, форма предметов);

– Сигнальные (параметры излучений: мощность, амплитуда, диапазон);

– Вещественные (ими являются физические и химические характеристики объектов).

Для получения конфиденциальных данных по таким каналам утечки информации злоумышленники используют прямые и косвенные демаскирующие признаки объектов.

**Источниками информации в данном случае служат:**

– Элементы бракованной продукции, не отправленные на утилизацию;

– Макеты оборудования, черновики записей, сделанных при проведении опытов, разработке планов и проектов. Не уничтоженные вовремя объекты с важной информацией могут попадать в мусорные контейнеры, вывозимые за территорию предприятия;

– Забракованные копии рабочих документов, копировальная бумага и другие отходы делопроизводства, оказавшиеся в корзине для мусора;

– Испорченные электронные носители информации, дефектные жесткие диски компьютеров, вывозимые на мусорные свалки, расположенные за территорией предприятия;

– Твердые, жидкие и газообразные отходы производства, утилизированные не по правилам;

– Радиоактивные отходы.

Нередко подобные объекты важной информации попадают за пределы предприятия по вине сотрудников и посетителей, не знакомых с правилами конфиденциальности.

Утечка данных происходит также, если частицы используемых веществ вывозятся за территорию завода при транспортировке грузов и людей.

Промышленные отходы, пригодные для получения важной информации, могут выноситься с территории предприятия потоками атмосферного воздуха. Нередко они обнаруживаются в каналах со сточными водами. Природу радиоактивных материалов, применяемых в производстве, можно установить, улавливая излучение.

Лицами, заинтересованными в получении данных с использованием вещественного канала утечки информации, являются владельцы конкурентных фирм, шантажисты, сотрудники зарубежной разведки. Для улавливания излучений и проведения анализов используются различные аппараты и приборы. Оценка информации, поступающей из таких каналов, производится с помощью вычислительной техники.

**Методы получения информации с использованием вещественных каналов**

К основным аналитическим методам, используемым для изучения материальных источников, полученных по вещественным каналам утечки информации, относятся: химический, биологический, физический и физико-химический анализ.

**Химический анализ**

Информация о химическом составе материалов и процентном соотношении отдельных компонентов получается с помощью методов аналитической химии.

При осуществлении качественного анализа получают информацию о чувствительности веществ к определенным химическим реактивам, их способности вступать в специфичные реакции с кислотами, щелочами, окислителями и другими компонентами.

В количественном анализе информацию получают, используя такие методы, как гравиметрия (измерение массы веществ), титрование (определение количества нейтрализующего реагента), фотохимия (исследование воздействия света на анализируемые вещества).

**Биологический анализ**

В качестве источников важной коммерческой информации используются твердые, жидкие и газообразные отходы производства. При осуществлении качественного и количественного анализов применяются биологические индикаторы – живые микроорганизмы (бактерии, дрожжевые и плесневые грибки), способные обитать в средах определенного состава.

**Физические и физико-химические методы**

Исследование вещественных объектов, получаемых по каналам утечки информации, производится с помощью методов термодинамики, спектрометрии, хроматографии, радиоактивного анализа.

Утечка данных по каналу распространения вещественных объектов информации нередко становится причиной ее перехвата злоумышленниками. Основными источниками похищаемой информации при этом являются черновые наброски рабочих документов, случайно сохраненные образцы бракованной продукции, а также отходы, являющиеся источниками радиоактивного излучения.

Утечке ценных сведений по каналам подобного типа способствует небрежное отношение людей к уничтожению ненужных рабочих материалов, неправильная утилизация отработанных веществ, несоблюдение требований к защите информации.

**Задание.** Провести анализ технических средств перехвата информации в материально-вещественном канале утечки, используя каталог технических средств защиты информации, представленный на сайте **http://bnti.ru/** (Техника для спецслужб. Бюро научно-технической информации.).

Для выполнения данной работы необходимо использовать следующие каталоги:

1) «Антитеррористическое оборудование» / «Средства обнаружения и идентификации веществ»
2) «Досмотровое оборудование» / «Средства обнаружения радиации»

Проведите подробный анализ 8-10 средств технической защиты из перечисленных выше каталогов и занесите данные в таблицу.

Пример.

| | Наименование | Изображение | Технические характеристики |
|---|---|---|---|
| 1 | Дозиметр гамма-излучения и потока бета-частиц "Дефендер" |   | Технические характеристики<br>– Диапазон показаний уровня радиоактивного фона. мкЗв/ч: до 1000<br>– Регистрируемая энергия гамма-излучения. МэВ: от 0.1<br>– Диапазон измерения накопленной дозы, Зв: до 1000<br>– Пороги предупреждения, мкЗв/ч: от 0,3 до 100<br>– ……<br>и т.д. |
| … | … | … | … |

| | | | |
|---|---|---|---|
| 10 | Прибор поисковый нейтронного излучения "НСД - А03" |  | Используется для: поиска источников нейтронного излучения; поиск аплутониевых загрязнений; инспектирования ядерных отходов; мониторинга полей нейтронного излучения.<br>– Абсолютная эффективность детектора по нейтронному излучению (для спектра деления), $с^{-1}см^{-2}$не менее 20<br>– Число ложных срабатываний, за 10 мин, не более 1<br>– ……<br>и т.д. |

**Контрольные вопросы**

1) Особенность материально-вещественного канала утечки информации.
2) Основные источники информации в материально-вещественном канале.
3) Утечка какого вида информации возможна в материально-вещественном канале?
4) Приемники информации в материально-вещественном канале утечки информации
5) Средства обнаружения утечки информации о радиоактивных веществах.

## Работа №6. Моделирование объекта защиты

**Цель работы** - изучить информацию по проектированию модели защиты объекта. Научиться разрабатывать проект защиты какого-либо смоделированного объекта на примере простых помещений.

Моделирование является основным методом анализа объекта защиты, выявления возможных угроз и построения соответствующей системы защиты. Моделирование предусматривает создание модели и ее исследование. Модель объекта защиты представляет собой описание объекта с учетом всех элементов информации, их источников и их месторасположений. В модели учитываются существенные для решаемой задачи элементы, связи и свойства изучаемого объекта.

Для создания полной модели объекта защиты необходимо для начала определить ту информацию, которую необходимо защищать, поэтому необходимо провести её структурирование. Структурирование информации представляет собой многоуровневый процесс детализации и конкретизации тематических вопросов перечней сведений. Оно проводится путем классификации информации в соответствии со структурой, функциями и задачами организации с привязкой элементов информации к ее источникам

Структурирование производится путем классификации защищаемой информации в соответствии с функциями, задачами и дальнейшей привязкой элементов информации к их носителям. Детализацию информации целесообразно проводить до уровня, на котором элементу информации соответствует один источник.

Моделирование состоит в анализе на основе пространственных моделей возможных путей распространения информации за пределы контролируемой зоны.

Ценность информации, а значит, и размер ущерба от реализации угрозы в отношении источника определяет уровень конфиденциальности информации. Ценность каждого уровня конфиденциальности - это доля от ценности всех элементов информации. Соответствие уровней конфиденциальности информации её ценности схематично показано на схеме:

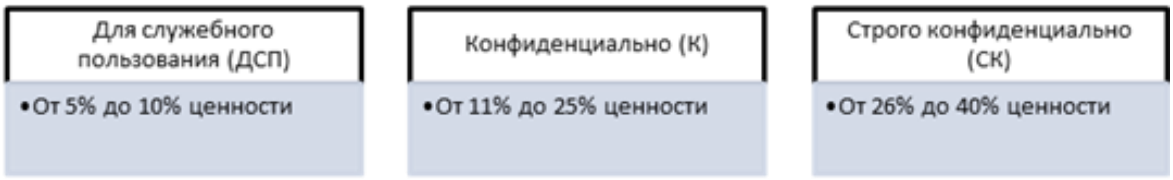



Рисунок 1 - Уровни конфиденциальности информации

На основе этой схемы разрабатывается таблица структурной модели защиты. (см табл. 1). В первом столбце которой указывается номер элемента информации в схеме классификации. Во 2-м, 3-м и 4-м столбцах таблицы указываются наименование элемента информации, предполагаемая для него ценность информации и в соответствии с этим уровень конфиденциальности. В столбце 5 указывается носитель информации, а в 6 —места размещения носителя или место его хранения (возможные рабочие места людей-источников информации, места расположения, размещения или хранения других носителей).

Таблица 1 - Структурная модель объекта защиты

| № присвоенный элементу | Наименование элемента информации | Уровень конфиденциальности информации | Ценность информации, % | Наименование источника информации | Местонахождение источника информации |
|---|---|---|---|---|---|
| 1 | Данные о сделках юр. лиц | К | 20 | Электронная и бумажная документация, специалисты | Кабинет 1 |
| 2 | Данные о патентах и авторских правах | К | 15 | Электронная и бумажная документация, специалисты отдела, БД на электронных носителях | Кабинет 1 |
| 3 | Данные о сделках физических лиц | К | 15 | Электронная и бумажная документация, специалисты отдела | Кабинет 2 |
| 4 | Данные о сотрудниках отдела | ДСП | 10 | БД на электронных носителях | Кабинет 3 |

| | | | | | |
|---|---|---|---|---|---|
| 5 | Информация о подготавливаемых проектах | ДСП | 10 | Электронная документация, специалисты отдела | Кабинет 4 |
| … | … | … | … | … | … |
| n | Данные о спорных делах | СК | 30 | Бумажная документация | Кабинет 4 |

Моделирование объекта защиты включает в себя также описание пространственного расположения основных мест размещения источников информации, выявления путей распространения носителей защищаемой информации за пределы контролируемых зон, описание с указанием характеристик существующих преград на путях распространения носителей с информацией за пределы контролируемых зон.

Моделирование проводится на основе пространственной модели (табл. 2) контролируемых зон с указанием расположения источников информации и состоит в анализе на основе рассмотренных пространственных моделей, какие могут быть пути распространения информации за пределы контролируемой зоны.

Таблица 2 - Пространственная модель объекта защиты

| | | |
|---|---|---|
| 1 | Наименование организации | «…» |
| 2 | Помещения | «Кабинет 1» - бухгалтерия<br>«Кабинет 2» - серверная<br>и т.д |
| 3 | Этаж | Пятый этаж пятиэтажного здания |
| 4 | Окна | В Кабинете 1 и Кабинете 2 есть по одному окну, выходящие на автостоянку, жалюзи на окнах отсутствуют. |
| 5 | Двери | Из Кабинета 1 и Кабинета 2 в общий коридор ведут одинарные деревянные двери с толщиной 30мм. |
| 6 | Соседние помещения | Отдел кадров, общий коридор, перегородка - кирпичная кладка толщиной 200 мм, толщина наружной стены 500 мм, стены монолитные. |
| 7 | Помещение над потолком | Чердак, плиты 250 мм, утеплитель 50 мм |
| 8 | Помещение под полом | Офис другой фирмы |
| 9 | Вентиляция | Отсутствует |
| 10 | Батареи отопления | Батареи отопления есть в каждой комнате |
| 11 | Цепи электропитания | Цепь электропитания организации подключена |

| | | |
|---|---|---|
| | | к городской сети через трансформаторный блок. Напряжение в цепи 220 В. Распределительный щит в подвале здания. Всего в помещении 8 розеток. |
| 12 | Телефон | В помещениях отсутствуют тел. аппараты |
| 13 | Радиотрансляция | Отсутствует |
| 14 | Бытовые радиосредства | Отсутствует |
| 15 | Бытовые электроприборы | К Кабинете 1 и Кабинете 2 по одному принтеру Samsung ML-1640 Series |
| 16 | ПК | В Кабинете 1 находятся 3 ПК с ОС Windows 7 Professional, в Кабинете 2 находятся 4 ПК с ОС Windows 7 Professional |
| 17 | Сеть | Имеется маршрутизатор, подключенный к сети интернет. К нему напрямую подключены все компьютеры локальной сети. |
| 18 | Технические средства охраны | Магнитоконтактные датчики системы охраны Smartec ST-DM122, проводные, установлены на дверях Кабинета 1 и Кабинета 2. |
| 19 | Телевизионные средства наблюдения | Отсутствуют |
| 20 | Пожарная сигнализация | Пожарный извещатель дымовой. В каждом кабинете. |
| 21 | Внутренняя АТС | Отсутствует |

На планах этажей здания указываются выделенные (с защищаемой информацией) и соседние помещения, схемы трубопроводов водяного отопления, воздухопроводов вентиляции, кабелей электропроводки, телефонной и вычислительной сетей, радиотрансляции, заземления, зоны освещенности дежурного освещения, места размещения и зоны наблюдения телевизионных камер и т. д. На рисунках 2, 3, 4 и 5 представлены внутренний план помещения, схема освещения и отопления помещения, схема пожарной сигнализации помещения и схема расположения технических средств, непосредственно обрабатывающие конфиденциальную информацию и телефонной линии в помещении соответственно. (Необходимо указать схемы всех этажей в отдельности).

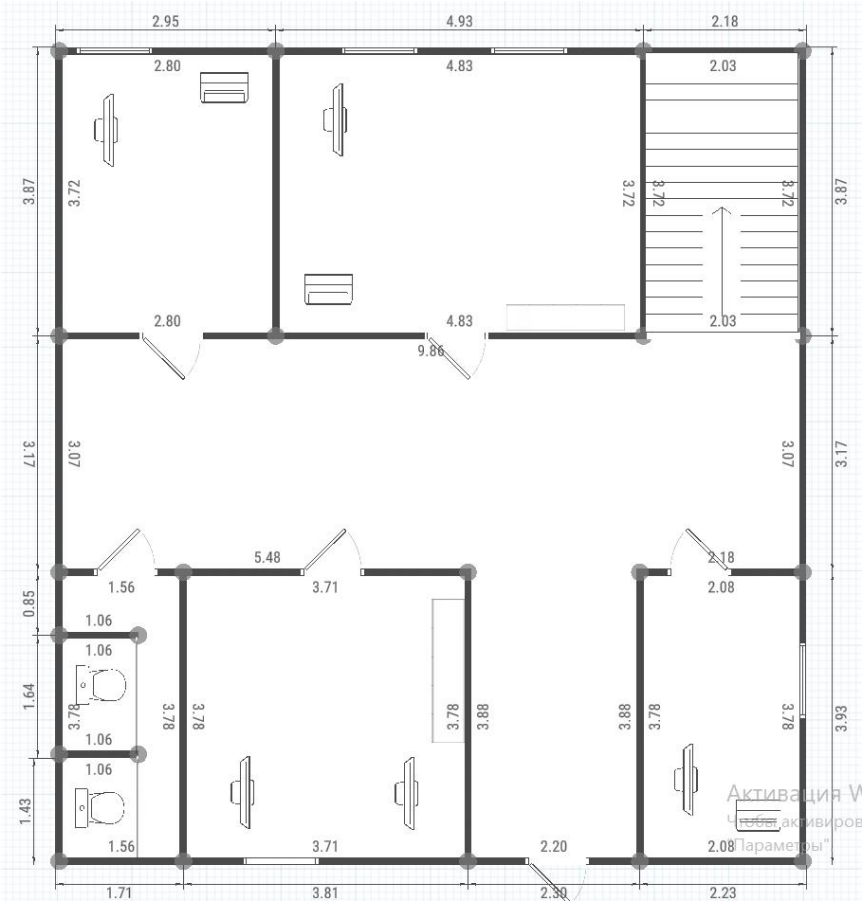



Рисунок 2 - Внутренний план помещения

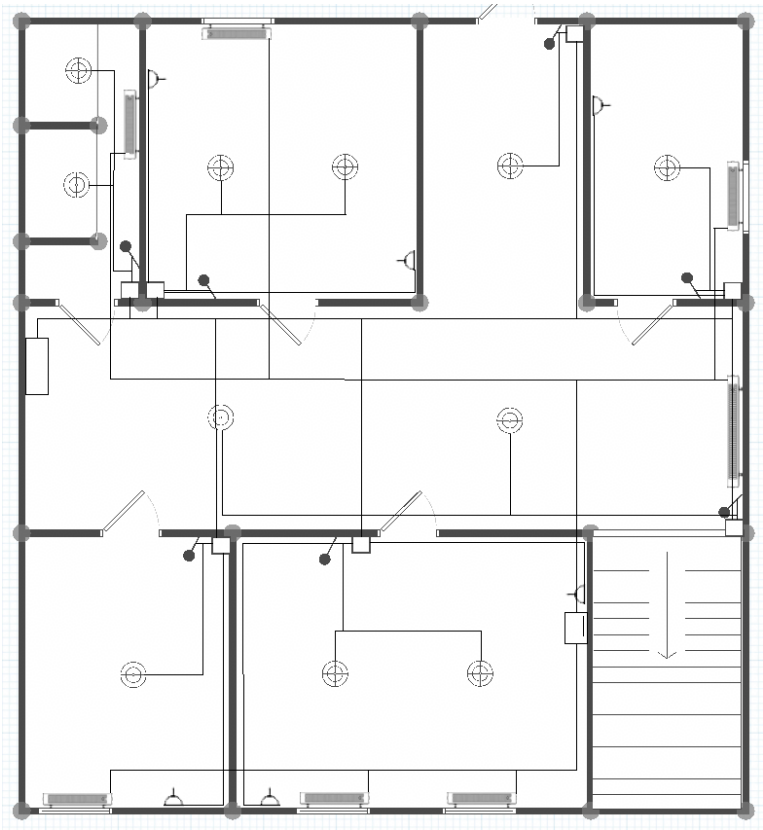


Рисунок 3 - Схема освещения и отопления помещения

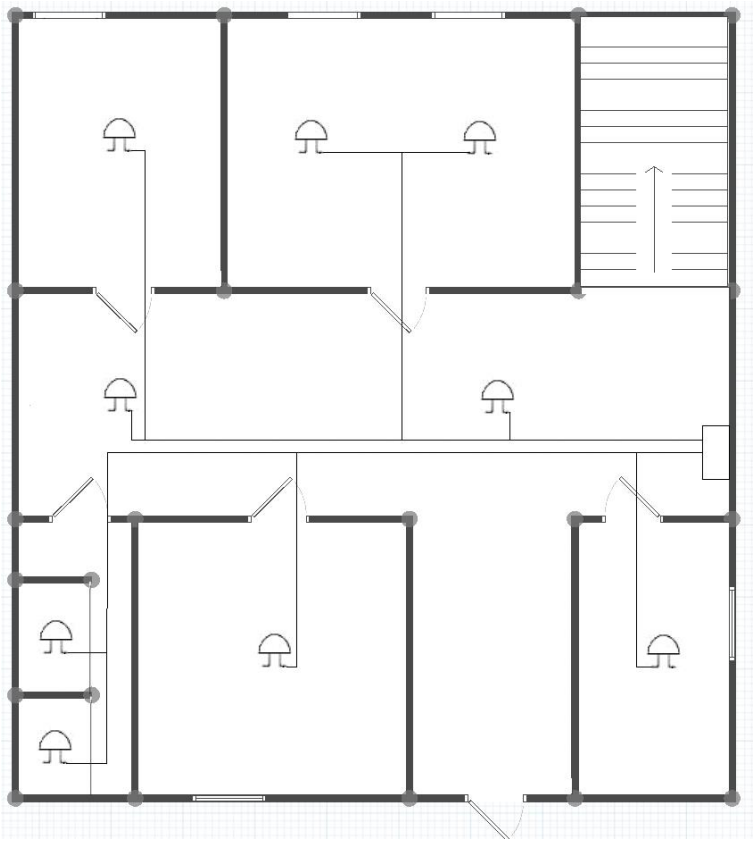


Рисунок 4 - Схема пожарной сигнализации помещения

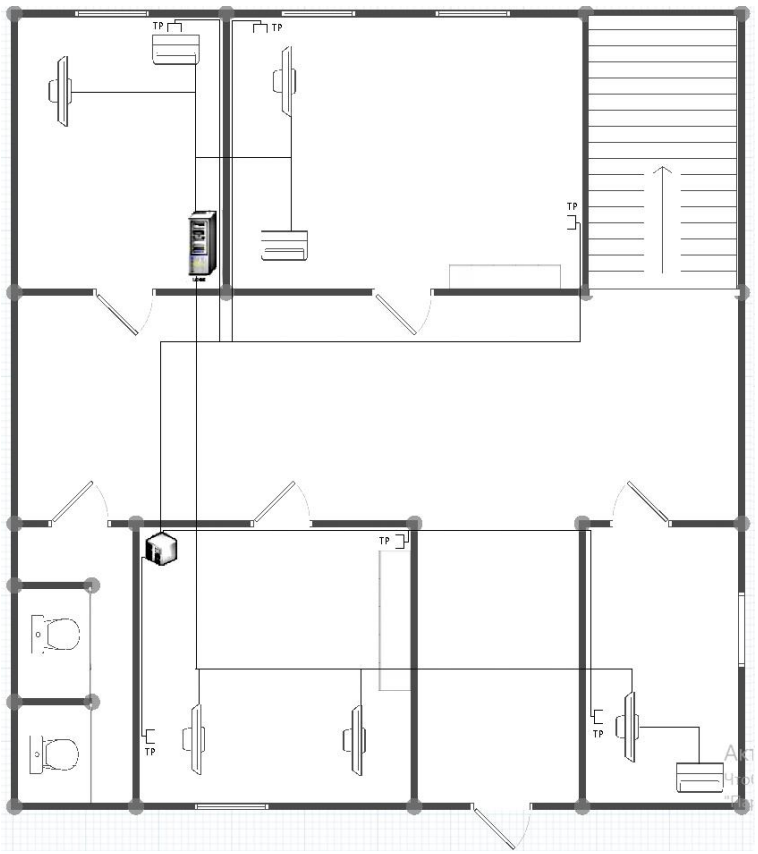


Рисунок 5 - Схема расположения ТСПИ и телефонной линии в помещении

**Задание.**

В процессе моделирования необходимо выполнить анализ возможных путей распространения информации за пределы контролируемой зоны и определить уровни сигналов на их границах на основе рассмотренных пространственных моделей. В результате моделирования определяется состояние безопасности информации и слабые места существующей системы ее защиты.

Результаты моделирования оформляются на планах и в таблицах:

1. Разработать структурную модель объекта защиты по примеру таблицы 1.
2. Разработать пространственную модель объекта защиты по примеру таблицы 2.
3. Разработать планы помещений и схемы размещения в них ОТСС и ВТСС.

**Варианты**

Таблица 3 - Варианты заданий для выполнения работы

| Вариант | Наименование организации | Вариант | Наименование организации |
|---|---|---|---|
| 1 | Отделение ПАО Сбербанка России | 11 | Курский областной арбитражный суд |
| 2 | РПИ «КурскПромРПИ» | 12 | ЮЗГУ(деканат) |
| 3 | РН-Черноземье | 13 | Курский центр занятости населения |
| 4 | Курский завод «Маяк» | 14 | ФНС г.Курска |
| 5 | Управление развития информационных технологий | 15 | Пенсионный фонд России по г. Курску |
| 6 | Отделение ПАО Экспобанка | 16 | Курский Военный комиссариат |
| 7 | ОБУЗ Областной перинатальный центр г. Курск | 17 | Курский аккумуляторный завод |
| 8 | АО «Авиаавтоматика» им. В. В. Тарасова» | 18 | МУ МВД г.Курска |
| 9 | Курский Федеральный аграрный научный центр | 19 | МФЦ г. Курск |
| 10 | Научно-технический комплекс «Техносфера» | 20 | Следственный комитет РФ по Курской области |

**Контрольные вопросы**

1 Какой основной объект анализа объекта защиты?

2 Что необходимо для создания полной модели объекта защиты?

3 Какие бывают уровни конфиденциальности информации?

4 Какие объекты обычно указывают на планах этажей зданий?

5 Что определяет уровень конфиденциальности информации?

## Работа № 7. Моделирование технических каналов утечки информации

**Цель работы -** изучить возможности составления структурной модели каналов утечки информации.

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.

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 ее 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, риск канала и величина потенциального ущерба.

Оценка показателей угроз безопасности 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 частота 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;

- оценка угроз безопасности информации основывается на прогнозе действий органов разведки. Учитывая скрытность подготовки и проведения разведывательной операции, их прогноз приходится проводить в условиях острой информационной недостаточности;

- 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.

Моделирование угроз безопасности информации предусматривает выявление угроз и их анализ с целью оценки возможного ущерба в случае их реализации.

Учитывая существенные различия процессов реализации угроз воздействия и утечки информации, **моделирование угроз целесообразно разделить на**:

– моделирование каналов несанкционированного доступа к защищаемой информации источников преднамеренных и случайных воздействий;

– моделирование технических каналов утечки информации.

**Модель физического проникновения** предполагает выбор конкретного пути преодоления злоумышленником преград для доступа к защищаемым элементам информации.

Действия злоумышленника по добыванию информации определяются поставленными целями и задачами, квалификацией, технической оснащенностью и др.

Прогнозирование источников информации является одним из основных условий ее эффективной защиты. При достаточно высокой точности прогноза создается возможность предотвратить вторжение или создать запас времени для предотвращения угроз не только методами защиты источников информации, но и воздействием на источник угроз.

**Модель нарушителя** – это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, их технических и материальных средствах и т. д.

Правильно разработанная модель нарушителя является гарантией построения адекватной системы обеспечения информационной безопасности. Необходимо представить, что наш нарушитель является довольно серьезной угрозой и имеет:

- представление об объекте, на который собирается совершать атаку;
- собственные каналы связи и доступ к интернету с высокой пропускной способностью;
- большие финансовые возможности;
- высокий уровень знаний в области IT;
- современные методы проникновения в информационные системы и воздействия на потоки данных в ней;
- может предпринимать усилия для получения представления о принципах функционирования системы защиты, внедрять своего представителя в службу безопасности;
- непредсказуемые цели;
- желание идти до победного конца.

В зависимости от квалификации, способов подготовки и физического проникновения в организацию может обладать следующими характеристиками:

- типовые знания о методах построения вычислительных систем, сетевых протоколов, использование стандартного набора программ;
- высокий уровень знаний сетевых технологий, опыт работы со специализированными программными продуктами и утилитами;
- высокие знания в области программирования, системного проектирования и эксплуатации вычислительных систем;
- обладание сведениями о средствах и механизмах защиты атакуемой системы;
- нарушитель являлся разработчиком или принимал участие в реализации системы обеспечения информационной безопасности.

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

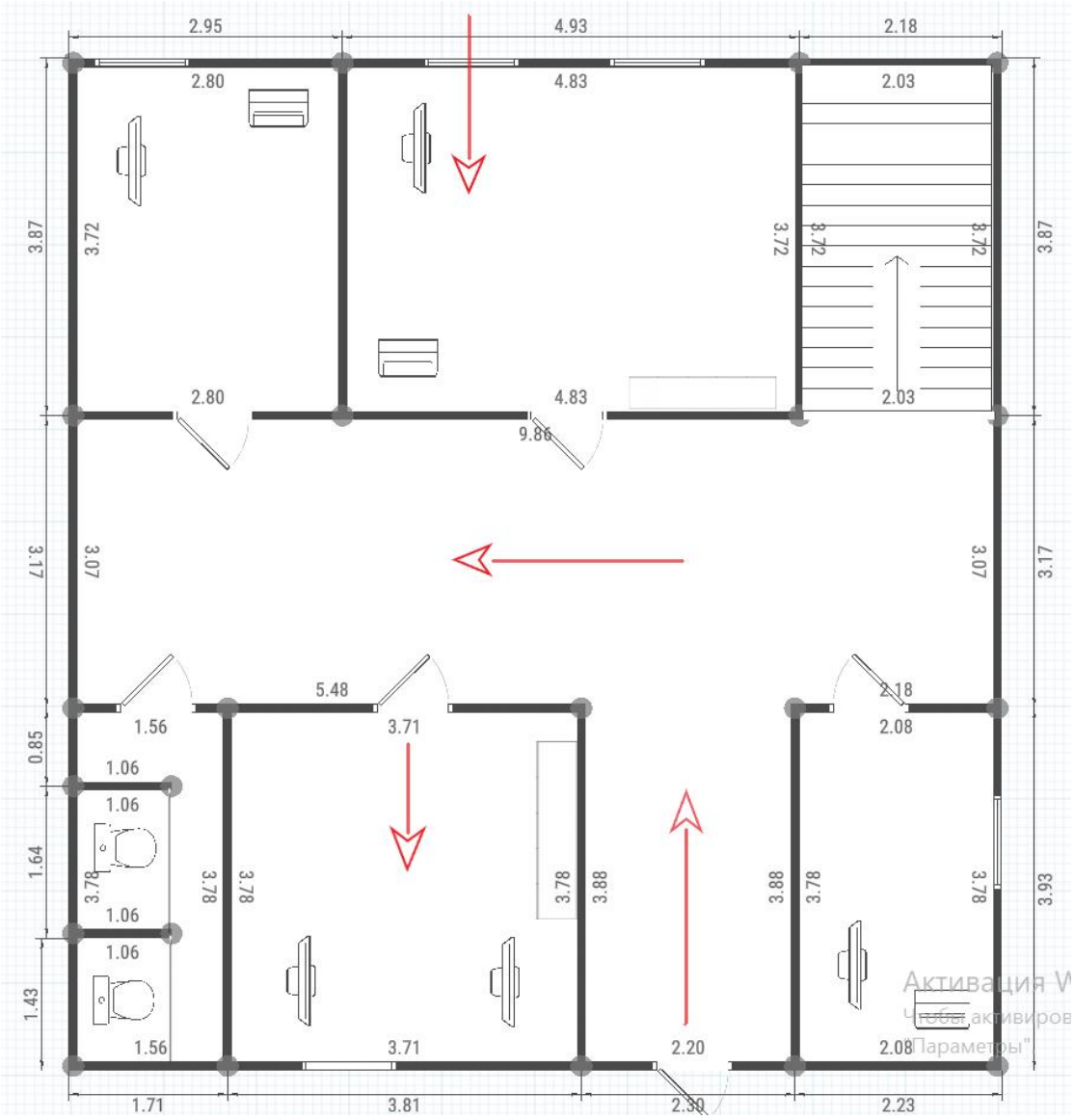



Рисунок 1 - Схема проникновения злоумышленника на объект защиты

Моделирование позволяет выявить сами каналы утечки информации, оценку их реальности, ранг и величину угрозы.

Произвести распознавание и обнаружение каналов утечки информации можно по их демаскирующим признакам. В таблице 7.1 в качестве достаточно общих индикаторов каналов утечки информации служат указанные демаскирующие признаки.

Приведенные индикаторы являются лишь ориентирами при поиске потенциальных каналов утечки. В конкретных условиях их состав существенно больший.

Таблица 7.1- Признаки или индикаторы каналов утечки информации

| Вид канала | Индикаторы |
|---|---|
| Оптический | Окна, выходящие на улицу, близость к ним противоположных домов и деревьев. Отсутствие на окнах занавесок, штор, жалюзей. Просматриваемость 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 люден (в том числе в автомобилях) с биноклями фотоаппаратами, кино и видеокамерами. |
| Радио-электронный | 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. 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 ч на территории организации. Отсутствие заземления радио и электрических приборов. Длительная к 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 отводов. Запись сотрудниками конфиденциальной информации на неучтенных листах бумаги. |

Потенциальные каналы утечки определяются для каждого источника информации, причем их количество может не ограничиваться одним или двумя. Примеры возможных каналов:

**Оптические каналы**

• объект наблюдения в кабинете — окно кабинета — окно противоположного дома — оптический прибор злоумышленника;

• объект наблюдения в кабинете — приоткрытая дверь — злоумышленник;

• объект наблюдения в кабинете — телевизионное закладное устройство — проводной или радиоканал — телевизионный приемник злоумышленника.
Риск утечки информации при наблюдении оценивается следующим образом:
• семантической документальной информации, отображаемой на плакатах — очень высокий, остальной документальной информации — очень низкий;
• о видовых признаках людей — средний;
• о видовых признаках продукции — низкий;
• о видовых признаках веществ и материалов — очень низкий.

**Акустические каналы**

• источник речевого сигнала — стена в соседнее помещение — акустический приемник злоумышленника;
• источник речевого сигнала — приоткрытая дверь в приемную — акустический приемник;
• источник акустического сигнала— закладное устройство — радиоканал — радиоприемник злоумышленника;
• источник акустического сигнала— стекло окна— модулированный лазерный луч — фотоприемник лазерной системы подслушивания;
• источник акустического сигнала— воздухопровод— акустический приемник;
• источник акустического сигнала — случайный акустоэлектрический преобразователь в техническом средстве— побочное излучение технического средства — радиоприемник;
• источник акустического сигнала — случайный акустоэлектрический преобразователь в техническом средстве — проводные кабели, выходящие за пределы контролируемой зоны;
• источник акустического сигнала— воздушная среда помещения — диктофон у злоумышленника.
Риск утечки информации при подслушивании оценивается следующим образом:
Для оценки угроз речевой информации необходимо оценить уровень акустического сигнала в возможных местах размещения акустического приемника злоумышленника.
• приемная - высокий;
• коридор - низкий
• смежные с кабинетом помещения - низкий;
• помещения с трубами отопления, проходящими через кабинет - средний;
• помещения, акустически связанные с кабинетом через воздуховоды вентиляции – средний.

**Радиоэлектронные каналы**

• коммутационное оборудование и кабели внутренней АТС
• электрические приборы
• передатчики акустических и телевизионных закладных устройств
• побочные электромагнитными излучениями основных и вспомогательных технических средств и систем

Риск утечки информации по радиоэлектронным каналам оценивается следующим образом:

• перехват радиоизлучений ПЭВМ из кабинета – средний,
• перехват электрических сигналов акустоэлектрических преобразователей — низкий.
• перехват побочных электромагнитных излучений радиоэлектронных средств и электрических приборов, размещенных и работающих в кабинете во время разговора - низкий.
• перехват опасных сигналов, содержащих речевую информацию, распространяющихся по проводам телефонных линий связи, трансляции, часов единого времени, электропитания и заземления - высокий
• подслушивание с помощью акустических закладных устройств, установленных в кабинете- высокий;
• скрытое наблюдение с помощью предварительно установленных телевизионных камер;

**Вещественные каналы**

• скрытное проникновение к источникам информации, хранящихся в ящиках стола, в компьютере, в сейфе-средний;
• запись сотрудниками конфиденциальной информации на неучтенных листах бумаги-средний;
• остальные – низкий

Все выявленные потенциальные каналы утечки информации и их характеристики записываются в таблицу 7.2. Наименование источника информации заимствуются из таблицы 7.1. В графе 4 указываются основные элементы среды распространения и возможные места размещения приемника сигналов. По физической природе носителя определяется вид канала утечки информации.

Таблица 7.2 - Модель потенциальных каналов утечки информации

| № элемента информации | Стоимость элемента информации, руб. ($С_и$) | Источник сигнала, передатчик | Путь утечки | Вид канала | Оценка реальности канала, ($Р_р$) | Ущерб от реализации угрозы ,руб ($С_{уи}$) | Ранг угрозы |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 400000 | Электромагнитное поле с волнами видимого диапазона | Хищение информации путем видео- или фотозахвата, отображенной на мониторах, бумажных носителях | Оптический | 0,2 | 80000 | 3 |
| 2 | 80000 | Материальный носитель, отображающий имеющую значение для дела информацию в форме физического сигнала. | Наличие закрытых и опечатанных ящиков для бумаги и твердых отходов с демаскирующими веществами. Применение радиоактивных веществ. Запись сотрудниками конфиденциальной информации на неучтенных листах бумаги. | Материально-вещественный | 0,2 | 13000 | 5 |
| 3 | 100000 | Утечка из электрических сетей связи; утечки информационных сигналов в цепях электропитания технических средств обработки информации | Наличие в помещении радиоэлектронных средств, ПК. ТА городской и внутренней АТС, громкоговорителей трансляционной сети и других предметов. Применение средств радиосвязи. Отсутствие заземления радио и электрических приборов. | Радио-электронный | 0,3 | 25000 | 4 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | 200000 | Сотрудники предприятия, приборы и средства, воспроизводящие раннее записанные звуки | Перехват речевой информации через стену в соседнее помещение с помощью акустического приемника, диктофона | Акустический | 0,7 | 140000 | 3 |
| .... | ..... | .... | .... | .... | .... | ..... | .... |
| 10 | 500000 | Монитор, системный блок, принтер, кабели, ПЭМИ | С помощью сканирования ПЭМИ широкополосными приемниками можно восстановить информацию | Электромагнитный | 0,25 | 125000 | 3 |

В графе 4 указываются основные элементы канала утечки информации (источника сигналов, среды распространения и возможные места размещения приемника сигналов).

По физической природе носителя определяется вид канала утечки информации, который указывается в столбце 5.

Оценка реальности канала утечки информации по рассматриваемому каналу оценивается близостью параметров канала и сигнала на входе его приемника к нормативным значениям, при которых риск (вероятность) утечки ниже допустимого значения (столбец 6):

$Рр=С_{ку}/С_{и}$

где $С_{ку}$ – стоимость канала утечки информации

$С_{и}$ – стоимость элемента информации

При определении реальности канала следует учитывать степень выполнения временного и энергетического условий разведывательного контакта с источником информации. Для обеспечения временного контакта надо или знать время проявления демаскирующих признаков объекта или наблюдение должно вестись непрерывно в течение, например, рабочего дня. Для выполнения энергетического условия разведывательного контакта необходимо, чтобы длина канала была больше расстояния от источника информации до злоумышленника или его приемника сигнала.

Возможности оценки угрозы безопасности информации в результате проникновения злоумышленника к источнику конфиденциальной

информации или его утечки через технические каналы носят вероятностный характер. Это означает, что рассматривается вероятность $P_p$ реализации рассматриваемого пути или канала и цены на соответствующий элемент информации.

Реальность пути связана с вероятностью выбора злоумышленником пути. Это делается с помощью метода экспертных оценок. В конечном счете вероятность определенного пути проникновения зависит от его простоты реализации.

Угроза безопасности информации, выраженной в величине ущерба $C_{yu}$ от попадания ее к злоумышленнику, рассчитывается для каждого пути или канала по формуле:

$$C_{yu} = C_u \times P_p$$

Моделирование угроз информационной безопасности завершается присвоением им ранга. Для каждой организации ранг устанавливается самостоятельно.

В данной лабораторной работе ранжирование угроз провести по таблице 7.3.

Таблица 7.3 - Ранжирование угроз информации

| Ранг угрозы | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Величина угрозы | Более $5 \times 10^5$ | $2 \times 10^5$ ... ... $5 \times 10^5$ | $5 \times 10^4$ ... ... $2 \times 10^5$ | $2 \times 10^4$ ... ... $5 \times 10^4$ | $10^2$ ... ... $2 \times 10^4$ |

Для каждого потенциального способа проникновения злоумышленника к источникам информации и на каналы утечки информации целесообразно завести карточку, в которую заносятся характеристики моделей канала.

В карточку добавляется приложение с перечнем мер по защите на этапе разработки способов и средств предотвращения проникновения злоумышленника и утечки информации по рассматриваемому каналу.

**Порядок выполнения работы**

1. Определите возможные каналы утечки информации для защищаемого объекта.
2. Графически изобразите на плане предприятия выявленные технические каналы утечки информации (на основе моделей объекта, разработанных в работе №6).

3. Результаты анализа занесите в таблицу 7.2. Указать не менее 10 технических каналов утечки.

**Контрольные вопросы**

1 Назовите элементы, содержащиеся в любой системе технической разведки.

2 Назовите достоинства и недостатки технической разведки.

3 Назовите прямые и побочные каналы утечки информации.

4 Назовите способы достижения противодействия распознаванию типа объекта.

5 Как осуществляется защита от оптической и оптикоэлектронной разведок?

6 Назовите методы борьбы с системами и средствами управления противника.

7 Назовите этапы защиты от внедряемых на объекты разведывательных устройств.

8 Назовите демаскирующие признаки сетевых акустических закладок.

9 Какие существуют пассивные методы акустической защиты?

10 Назовите способ предотвращения несанкционированного использования сотовых телефонов.

## Список литературы


1. Котенко В. В. Теория информации: учебное пособие / В.В. Котенко. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 240 с. // Режим доступа - https://biblioclub.ru/index.php?page=book&id=561095. – Текст: электронный.
2. Горбунов, А. В. Проектирование защищённых оптических телекоммуникационных систем : учебное пособие : [16+] / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёнкин. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 128 с. :– URL: https://biblioclub.ru/index.php?page=book&id=598665 (дата обращения: 20.08.2021). Режим доступа: по подписке. – Текст : электронный.
3. Зайцев А.П. Технические средства и методы защиты информации [Текст]: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.
4. Титов А.А. Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие / А.А. Титов. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. - 195 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=208567
5. Меньшаков Ю.К. Основы защиты от технических разведок[Текст]: учебное пособие / Ю.К. Меньшаков. – М.: Издательство МГТУ им. Н.Э. Баумана, 2011. – 478 с.
6. Меньшаков Ю.К. Виды и средства иностранных технических средств разведок[Текст]: учебное пособие Ю.К. Меньшаков. – М.: Издательство МГТУ им. Н.Э. Баумана, 2009. – 656 с.
7. Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебно-практическое пособие / В.В. Креопалов. - М. : Евразийский открытый институт, 2011. - 278 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=90753
8. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=429070
9. Информационная безопасность и защита информации [Текст]: учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.
10. Грибунин В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.