Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

Е.В. Каменева

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе высшего образования по направлению подготовки 10.03.01 Информационная безопасность

Оренбург
2019

УДК 004.056(076.5)
ББК 32.971.3я7
К18

Рецензент – доцент, кандидат технически наук Р.Р. Галимов.

К18 **Каменева Е.В.**
Техническая защита информации: методические указания / Е.В.Каменева; Оренбург. гос. ун-т. - Оренбург: ОГУ, 2019.

Методические указания содержат методику работы по выявлению технических каналов утечки информации и изучению средств добывания информации в различных диапазонах волн.

Методические указания предназначены для выполнения лабораторных работ студентами, изучающими дисциплину «Техническая защита информации» обучающихся по направлению подготовки 10.03.01 Информационная безопасность

УДК 004.056(076.5)
ББК 32.971.3я7

Содержание

Введение

Методические указания предназначены для выполнения лабораторных работ студентами, изучающими дисциплину «Техническая защита информации» обучающихся по направлению подготовки 10.03.01 Информационная безопасность. Каждая работа включает и содержат теоретический материал и задания, при выполнении которых обучающиеся приобретают компетенции, необходимые им для формирования уровня знаний, умений и навыков в соответствии с требованиями стандарта высшего образования по направлениям подготовки 10.03.01 Информационная безопасность.

Лабораторный курс содержит семь работ, при выполнении которых студенты получать навыки работы с основными методами и средствами перехвата информации при ее утечке по техническим каналам.

К выполнению лабораторной работы следует приступать после ознакомления с теоретической частью соответствующего раздела и рекомендациями, приведенными в конкретной работе. По результатам каждой лабораторной работы необходимо оформить отчет.

Практикум рекомендован преподавателям как вспомогательный материал в организации и проведении занятий, а также студентам - для аудиторного и самостоятельного освоения лабораторной части дисциплины «Техническая защита информации».

1 Лабораторная работа № 1. Средства перехвата информации в оптическом диапазоне волн

1.1 Цель работы

Ознакомление со средствами добывания информации в оптическом диапазоне волн.

1.2 Теоретическая часть

В общем случае источником оптического сигнала является объект наблюдения, который излучает сигнал или переотражает свет другого, внешнего источника. Отражательная способность объектов наблюдения зависит от длины волны падающего света и спектральных характеристик поверхности объекта наблюдения. Отражательная способность ряда природных фонов (травы, листы и др.) и биологических объектов возрастает в несколько раз при смещении длины волны падающего света в область более длинных волн, а для неживых объектов она меняется мало в широком диапазоне длин волн. Структура оптического (визуального) канала утечки представлена на рисунке 1.1.

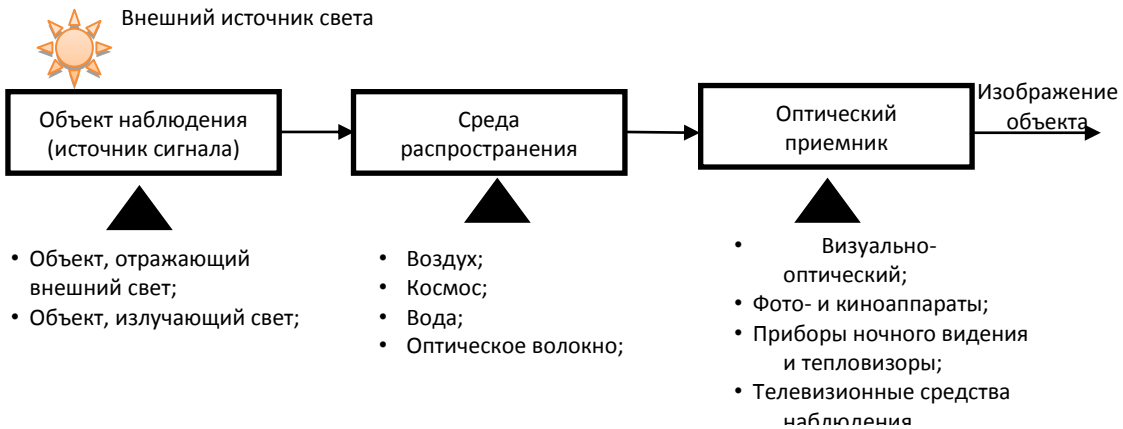

Рисунок 1.1 – Структура оптического (визуального) канала утечки информации

В зависимости от характера информации можно выделить следующие способы ее получения:

- наблюдение за объектами;
- съемка объектов;
- съемка (снятие копий) документов.

В зависимости от условий наблюдения и освещения для наблюдения за объектами могут использоваться различные технические средства. Для наблюдения днем - оптические приборы (монокуляры, подзорные трубы, бинокли, телескопы и т.д.), телевизионные камеры, для наблюдения ночью - приборы ночного видения, телевизионные камеры, тепловизоры.

Для наблюдения с большого расстояния используются средства с длиннофокусными оптическими системами, а при наблюдении с близкого расстояния - камуфлированные скрытно установленные телевизионные камеры. При этом изображение с телевизионных камер может передаваться на мониторы как по кабелю, так и по радиоканалу.

Съемка объектов проводится для документирования результатов наблюдения и более подробного изучения объектов. Для съемки объектов используются телевизионные и фотографические средства.

При съемке объектов, также, как и при наблюдении за ними, использование тех или иных технических средств обусловлено условиями съемки и временем суток. Для съемки объектов днем с большого расстояния используются фотоаппараты и телевизионные камеры с длиннофокусными объективами или совмещенные с телескопами.

Для съемки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи или передачи изображений по радиоканалу.

Съемка объектов ночью проводится, как правило, с близкого расстояния. Для этих целей используются портативные фотоаппараты и телевизионные камеры, совмещенные с приборами ночного видения, или тепловизоры, а также портативные закамуфлированные телевизионные камеры высокой чувствительности, совмещенные с устройствами передачи информации по радиоканалу.

Съемка документов осуществляется, как правило, с использованием портативных фотоаппаратов.

Оптический канал утечки информации, среда распространения которого содержит участки безвоздушного пространства, возникает при наблюдении за наземными объектами с космических аппаратов.

Сложный состав атмосферы вызывает неравномерность (изрезанность) ее амплитудно-частотной характеристики как среды распространения. Участки в ней с малым затуханием называются окнами прозрачности.

В общем случае прозрачность атмосферы зависит от соотношения длины проходящего сквозь нее света и размеров взвешенных в атмосфере частиц. Если размеры частиц соизмеримы с длиной волны света (больше половины длины волны) или больше, то пропускание значительно ухудшается. Поэтому уровень пропускания меняется в зависимости от длины световой волны.

Прозрачность атмосферы среды распространения света оценивается метеорологической дальностью видимости. Метеорологическая видимость даже в окнах прозрачности зависит от наличия в атмосфере взвешенных частиц пыли и влаги, образующих мглу и туман, капелек и кристаллов воды в виде дождя и снега, а также аэрозолей и дымов, содержащих твердые частицы. Все это вызывает замутнение атмосферы и ухудшает видимость.

1.3 Порядок выполнения работы

1. Войдите в среду Internet.

2. В адресной строке наберите http://bnti.ru/ (Техника для спецслужб. Бюро научно-технической информации.)

3. В каталоге технических средств войдите:

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

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

3) в раздел «Оборудование для оперативно-розыскной деятельности» /

«Системы перехвата каналов связи» / «Системы контроля оптических линий связи»

4) в раздел «Тепловизионные и оптические системы»

4. Изучите представленные средства

5. Изученные средства (6-8 шт.) внесите в таблицу 1.1 и проанализируйте ее. Опишите преимущества одних средств перехвата информации в оптическом диапазоне волн перед другими.

Таблица 1.1 – Анализ технических средств перехвата информации в оптическом диапазоне волн

Наименование ТС	Изображение	Технические характеристики

1.4 Контрольные вопросы

1 Структура оптического канала утечки информации.

2 Факторы, влияющие на достоверность добываемой в оптическом диапазоне волн информации.

3 Характеристики среды распространения оптических лучей в атмосфере.

4 Способы и средства наблюдения в оптическом диапазоне.

5 Визуально-оптические приборы.

6 Фото- и кино-аппараты.

7 Средства телевизионного наблюдения.

8 Средства наблюдения в инфракрасном диапазоне.

9 Тепловизоры.

10 Особенности добывания информации с ВОЛС.

2 Лабораторная работа № 2. Средства перехвата информации в радиоэлектронном и электромагнитном диапазонах волн

2.1 Цель работы

Ознакомление со средствами добывания информации в радиоэлектронном и электромагнитном диапазонах волн.

2.2 Теоретическая часть

В радиоэлектронном канале передачи носителем информации является электрический ток и электромагнитное поле с частотами колебаний от звукового диапазона до десятков ГГц.

Радиоэлектронный канал относится к наиболее информативным каналам утечки в силу следующих его особенностей:

− независимости функционирования канала от времени суток и года, существенно меньшая зависимость его параметров по сравнению с другими каналами от метеоусловий;

− высокой достоверности добываемой информации, особенно при перехвате ее в функциональных каналах связи (за исключением случаев дезинформации);

− большого объема добываемой информации;

− оперативности получения информации вплоть до реального масштаба времени;

− скрытности перехвата сигналов и радиотеплового наблюдения.

Структура радиоэлектронного канала утечки информации в общем случае включает источник сигнала или передатчик, среду распространения электрического тока или электромагнитной волны и приемник сигнала.

Радиоэлектронные каналы в зависимости от вида источников сигналов можно разделить на каналы 1 и 2-го вида.

В каналах утечки **1-го вида,** представленном на рисунке 2.1, производится перехват информации, передаваемой по функциональному каналу связи.

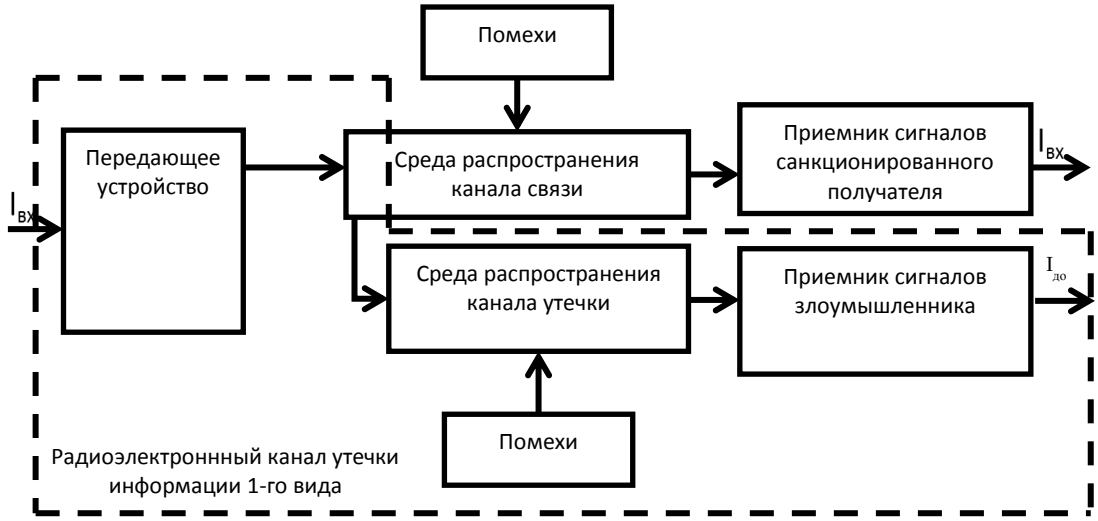

Рисунок 2.1 – Структура радиоэлектронного канала 1-го вида

С этой целью приемник сигнала канала утечки информации настраивается на параметры сигнала или подключается (контактно или дистанционно) к проводам соответствующего канала связи. Такой канал Утечки имеет общий с функциональным каналом связи источник сигналов — передатчик и часть среды радиоканала или проводного функционального канала до точки подключения средства съема.

Перехватываемые сигналы передающих устройств функциональных каналов связи имеют мощность от долей Вт до миллиона Вт (МВт). Но так как места расположения приемников функционального канала и канала утечки информации в общем случае не совпадают, то перехватываемый сигнал имеет меньшую мощность, чем сигнал на входе приемника функционального канала связи.

Радиоэлектронный канал утечки **2-го вида**, представленный на рисунке 2.2, имеет собственный набор элементов: передатчик сигналов, среду распространения и приемник сигналов.

Передатчик сигналов этого канала утечки информации образуется случайно (без участия источника или получателя информации) или специально устанавливается в помещении злоумышленником. Такими передатчиками могут быть случайные источники опасных сигналов и закладные устройства. Опасные сигналы, как отмечалось ранее, возникают в результате акустоэлектрических преобразований, побочных низкочастотных и высокочастотных полей, паразитных

связей и наводок в проводах и элементах радиосредств. Предпосылки для них создаются в результате конструктивных недоработок при разработке радиоэлектронного средства, объективных физических процессов в их элементах, изменениях параметров в них из-за старения или нарушений правил эксплуатации, неучете полей вокруг средств или токонесущих проводов при их прокладке в здании и т. д.

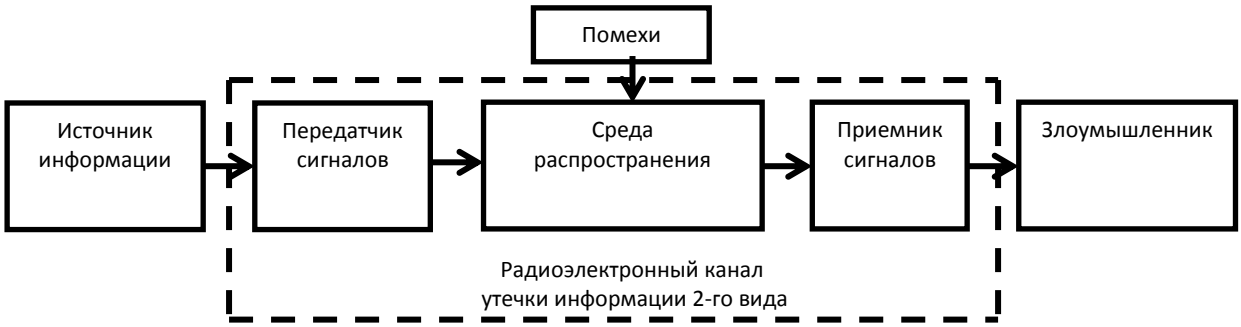

Рисунок 2.2 – Структура радиоэлектронного канала 2- вида

Особенностями передатчиков канала **2-го вида** являются малые уровни электрических сигналов — единицы и доли мВ и мощность радиосигналов, не превышающая десятки мВт (для радиозакладок). В результате этого протяженность таких каналов невелика и составляет десятки и сотни метров. Поэтому для добывания информации с использованием такого канала утечки приемник необходимо приблизить к источнику на величину длины канала утечки или установить ретранслятор.

Средой распространения сигналов радиоэлектронного канала утечки информации являются атмосфера, безвоздушное пространство (для канала 1-го вида) и направляющие — электрические провода различных типов и волноводы. Носитель в виде электрического тока распространяется по проводам, а электромагнитное поле — в атмосфере, в безвоздушном пространстве или по направляющим — волноводам. В приемнике производится выделение (селекция) носителя с интересующей получателя информацией по частоте, усиление выделенного слабого сигнала и съем с него информации — демодуляция.

Среда распространения радиоэлектронных каналов утечки существенно различается для электрических и радиосигналов. Электрические сигналы как носители информации могут быть аналоговыми или дискретными, их спектр может содержать частоты от десятков Гц до десятков ГГц. Электрические сигналы распространяются по направляющим линиям связи, связывающим источники и приемники сигналов как внутри организации, так внутри населенного пункта, города, страны, земного шара в целом. Способы и средства передачи электрических сигналов по проводам рассматриваются теорией и техникой проводной связи.

2.3 Порядок выполнения работы

1. Войдите в среду Internet.

2. В адресной строке наберите http://bnti.ru/ (Техника для спецслужб. Бюро научно-технической информации.)

3. В каталоге технических средств войдите:

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

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

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

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

4. Изучите представленные средства

5. Изученные средства (6-8 шт.) внесите в таблицу 2.1 и проанализируйте ее. Опишите преимущества одних средств перехвата информации перед другими.

Таблица 2.1 – Анализ технических средств перехвата информации в радиоэлектронном и электромагнитном диапазонах волн

Наименование ТС	Изображение	Технические характеристики

2.4 Контрольные вопросы

1 Задачи и характеристики радиоэлектронной разведки и ее особенности.

2 Назначение и функции антенн.

3 Назначение и функции радиоприемников.

4 Назначение и функции анализаторов.

5 Назначение и функции пеленгаторов.

6 Назначение и функции устройств индикации и регистрации.

7 Средства воздушной разведки, размещаемые на самолетах.

8 Средства космической разведки, размещаемые на космических аппаратах.

9 Средства наземной разведки, размещаемые на поверхности Земли.

10 Технические средства радиотепловой разведки.

3 Лабораторная работа № 3. Средства перехвата информации в акустическом диапазоне волн

3.1 Цель работы

Ознакомление со средствами добывания информации в акустическом диапазоне волн.

3.2 Теоретическая часть

Источником образования акустического канала утечки информации являются вибрирующие, колеблющиеся тела и механизмы, такие как голосовые связки человека, движущиеся элементы машин, телефонные аппараты, звукоусилительные системы и т.д.

Распространение звука в пространстве осуществляется звуковыми волнами. Упругими, или механическими, волнами называются механические возмущения (деформации), распространяющиеся в упругой среде. Тела, которые, воздействуя на среду, вызывают эти возмущения, называются источниками волн. Распространение упругих волн в среде не связано с переносом вещества. В неограниченной среде оно состоит в вовлечении в вынужденные колебания все более и более удаленных от источника волн частей среды.

Упругая волна является продольной и связана с объемной деформацией упругой среды, вследствие чего может распространяться в любой среде — твердой, жидкой и газообразной.

Когда в воздухе распространяется акустическая волна, его частицы образуют упругую волну и приобретают колебательное движение, распространяясь во все стороны, если на их пути нет препятствий. В условиях помещений или иных ограниченных пространств на пути звуковых волн возникает множество препятствий, на которые волны оказывают переменное давление (двери, окна, стены, потолки, полы и т.п.), приводя их в колебательный режим. Это воздействие звуковых волн и является причиной образования акустического канала утечки информации.

Акустические каналы утечки информации образуются за счет:

− распространение акустических колебаний в свободном воздушном пространстве;

− воздействия звуковых колебаний на элементы и конструкции зданий;

− воздействия звуковых колебаний на технические средства обработки информации.

Механические колебания стен, перекрытий, трубопроводов, возникающие в одном месте от воздействия на них источников звука, передаются по строительным конструкциям на значительные расстояния, почти не затухая, не ослабляясь, и излучаются в воздух как слышимый звук. Опасность такого акустического канала утечки информации по элементам здания состоит в большой и неконтролируемой дальности распространения звуковых волн, преобразованных в упругие продольные волны в стенах и перекрытиях, что позволяет прослушивать разговоры на значительных расстояниях.

Еще один канал утечки акустической информации образуют системы воздушной вентиляции помещений, различные вытяжные системы и системы подачи чистого воздуха. Возможности образования таких каналов определяются конструктивными особенностями воздуховодов и акустическими характеристиками их элементов: задвижек, переходов, распределителей и др. Структура акустического канала утечки информации в общем виде представлена на рисунке 3.1.

Рисунок 3.1 - Структура акустического канала утечки информации в общем виде

В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата, акустические каналы утечки информации также можно разделить на:

- воздушные;
- вибрационные;
- электроакустические;
- оптико-электронные;
- параметрические.

3.3 Порядок выполнения работы

1. Войдите в среду Internet.

2. В адресной строке наберите http://bnti.ru/ (Техника для спецслужб. Бюро научно-технической информации.)

3. В каталоге технических средств войдите:

1) в раздел «Оборудование для оперативно-розыскной деятельности» / «Средства акустического контроля»

2) в раздел «Оборудование для оперативно-розыскной деятельности» / «Средства контроля телефонных переговоров»

3) в раздел «Средства многоканальной видео-, аудиозаписи и оповещения» / «Средства многоканальной записи телефонных переговоров»

4) в раздел «Средства многоканальной видео-, аудиозаписи и оповещения» / «Средства многоканальной записи переговоров»

4. Изучите представленные средства

5. Изученные средства (6-8 шт.) внесите в таблицу 3.1 и проанализируйте ее. Опишите преимущества одних средств перехвата информации перед другими.

Таблица 3.1 – Анализ технических средств перехвата информации в акустическом диапазоне волн

Наименование ТС	Изображение	Технические характеристики

3.4 Контрольные вопросы

1 Технические средства перехвата информации в акустическом канале утечки информации

2 Технические средства перехвата информации в виброакустическом канале утечки информации

3 Технические средства перехвата информации в электроакустическом канале утечки информации

4 Технические средства перехвата информации в акустооптическом канале утечки информации

5 Технические средства перехвата информации в акустоэлектро-магнитном канале утечки информации

4 Лабораторная работа № 4. Средства перехвата информации в каналах, образованных средствами вычислительной техники

4.1 Цель работы

Ознакомление со средствами добывания информации в радиоэлектронном и электромагнитном диапазонах волн.

4.2 Теоретическая часть

Для обработки информации ограниченного доступа широко используются различные информационные системы, основу ко-торых составляют средства вычислительной техники (СВТ). Поэтому объекты информатизации, на которых обработка информации осуществляется с использованием СВТ, часто называются «объектами СВТ».

При рассмотрении объекта СВТ, как объекта защиты от утечки информации по техническим каналам, его необходимо рассматривать как объект, включающий:

− технические средства и системы, непосредственно обрабатывающие информацию ограниченного доступа, вместе с их соединительными линиями (под соединительными линиями понимают совокупность проводов и кабелей, прокладываемых между отдельными ТСОИ и их элементами);

− вспомогательные технические средства и системы вместе с их соединительными линиями;

− посторонние проводники;

− систему электропитания;

− систему заземления.

К техническим средствам обработки информации ограниченного доступа (ТСОИ) относятся:

− технические средства автоматизированных систем управления, электронно-вычислительные машины и их отдельные элементы, в дальнейшем именуемые средствами вычислительной техники (СВТ);

− средства изготовления и размножения документов;

− аппаратура звукоусиления, звукозаписи, звуковоспроизведения и синхронного перевода;

− системы внутреннего телевидения;

− системы видеозаписи и видео-воспроизведения;

− системы оперативно-командной связи;

− системы внутренней автоматической телефонной связи, включая и соединительные линии перечисленного выше оборудования и т.д.

Данные технические средства и системы в ряде случаев именуются ***основными техническими средствами и системами (ОТСС).***

Наряду с техническими средствами и системами, обрабатывающими информацию ограниченного доступа, в помещениях, где они установлены, как правило, находятся и другие технические средства и системы, которые в обработке информации ограниченного доступа непосредственно не участвуют. К ним относятся:

− системы и средства городской автоматической телефонной связи;

− системы и средства передачи данных в системе радиосвязи;

− системы и средства охранной и пожарной сигнализации;

− системы и средства оповещения и сигнализации;

− контрольно-измерительная аппаратура;

− системы и средства кондиционирования;

− системы и средства проводной радиотрансляционной сети и приёма программ радиовещания и телевидения (абонентские громкоговорители, средства радиовещания;

− телевизоры и радиоприёмники и т.д.);

− средства электронной оргтехники;

− системы и средства электрочасофикации и иные технические средства и системы.

Такие технические средства и системы называются ***вспомогательными техническими средствами и системами (ВТСС).***

Через помещения, в которых установлены технические средства обработки информации ограниченного доступа, могут проходить провода и кабели, не относящиеся к ТСОИ и ВТСС, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции, которые называются ***посторонними проводниками (ПП).***

Электропитание ТСОИ и ВТСС осуществляется от распределительных устройств и силовых щитов, которые специальными кабелями соединяются с трансформаторной подстанцией городской электросети.

Все технические средства и системы, питающиеся от электросети, должны быть заземлены. Типовая система заземления включает общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с техническими средствами.

Ряд соединительных линий ВТСС, посторонних проводников, а также линии электропитания и заземления могут выходить за пределы ***контролируемой зоны объекта (КЗ),*** под которой понимается пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц (посетителей, работников различных технических служб, не являющихся сотрудниками организации), а также транспортных средств. Границей контролируемой зоны могут являться периметр охраняемой территории организации, а также ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

Для перехвата информации, обрабатываемой СВТ, используются ***технические средства разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН).***

В зависимости от природы образования информативного сигнала технические каналы утечки информации можно разделить на естественные и специально создаваемые.

Естественные каналы утечки информации образуются за счёт побочных электромагнитных излучений, возникающих при обработке информации СВТ (электромагнитные каналы утечки информации), а также вследствие наводок информативных сигналов в линиях электропитания СВТ, соединительных линиях ВТСС и посторонних проводниках (электрические каналы утечки информации).

К **специально создаваемым каналам утечки информации** относятся каналы, создаваемые путём внедрения в СВТ электронных устройств перехвата информации (закладных устройств) и путём «высокочастотного облучения» СВТ.

4.3 Порядок выполнения работы

1. Войдите в среду Internet.

2. В адресной строке наберите http://bnti.ru/ (Техника для спецслужб. Бюро научно-технической информации.)

3. В каталоге технических средств войдите в раздел «Оборудование для оперативно-розыскной деятельности / Системы контроля электронной информации / Системы контроля электронной информации в компьютерных сетях»

4. В адресной строке наберите https://www.keyloggers.com/ru/

На главной странице изучите состав представленных «кейлоггеров».

5. Изученные средства (6-8 шт.) внесите в таблицу 4.1 и проанализируйте ее. Опишите преимущества одних средств перехвата информации перед другими.

Таблица 4.1 – Анализ технических средств перехвата информации в каналах, образованных средствами вычислительной техники.

Наименование ТС	Изображение	Технические характеристики

4.4 Контрольные вопросы

1 Основные технические средства и системы (определение, состав).

2 Вспомогательные технические средства и системы (определение, состав).

3 Схема технического канала утечки информации, обрабатываемого средствами вычислительной техники.

4 Классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники.

5 Электромагнитные каналы утечки информации, обрабатываемой средствами вычислительной техники.

6 Электрические каналы утечки информации, обрабатываемой средствами вычислительной техники.

5 Лабораторная работа № 5. Средства добывания информации в материально-вещественном канале утечки

5.1 Цель работы

Ознакомление со средствами добывания информации в материально-вещественном канале утечки.

5.2 Теоретическая часть

Особенность материально-технического канала утечки вызвана спецификой источников и носителей информации по сравнению с другими каналами. Источниками и носителями информации в нем являются субъекты (люди) и материальные объекты (макротела и микрочастицы). Утечка информации в этих каналах сопровождается физическим перемещением людей и материальных тел с информацией за пределами контролируемой зоны. Структура материально-вещественного канала утечки информации представлена на рисунке 5.1.

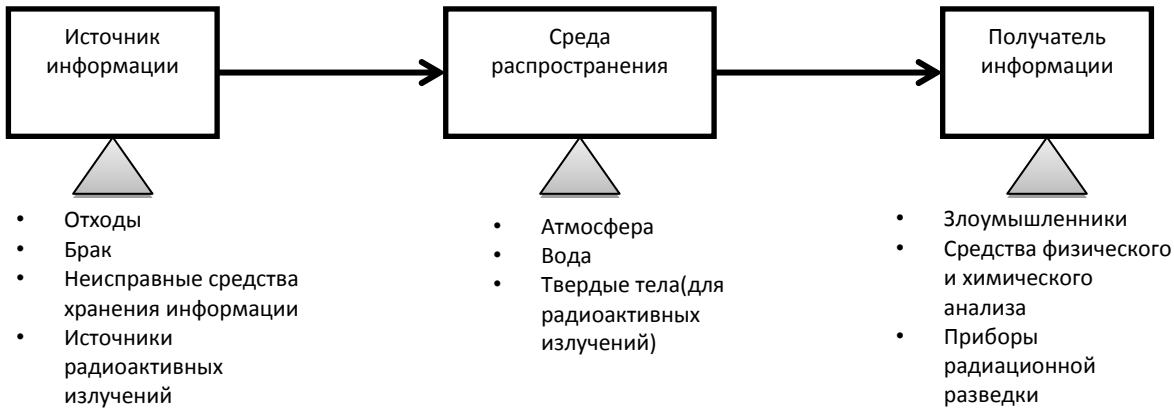

Рисунок 5.1 – Структура материально-вещественного канала утечки информации

Основными источниками информации вещественного канала утечки информации являются следующие:

− черновики различных документов и макеты материалов, узлов, блоков, устройств, разрабатываемых в ходе научно-исследовательских и опытно-конструкторских работ, ведущихся в организации;

− отходы делопроизводства и издательской деятельности в организации, в том числе использованная копировальная бумага, забракованные листы при оформлении документов и их размножении;

− отходы промышленного производства опытного и серийного выпуска продукции, содержащей защищаемую информацию в газообразном, жидком и твердом виде;

− содержащие защищаемую информацию электронные носители, нечитаемые из-за их физических дефектов и искажений загрузочных или других секторов;

− бракованная продукция и ее элементы;

− радиоактивные материалы.

Перенос информации в этом канале за пределы контролируемой зоны возможен следующими субъектами и объектами:

− людьми (сотрудниками организации, посетителями, представителями вторсырья и др.) и управляемыми ими техническими средствами;

− воздушными массами атмосферы;

− жидкой средой;

− излучениями радиоактивных веществ.

Эти носители могут переносить все виды информации: семантическую и признаковую, а также демаскирующие вещества.

Семантическая информация содержится в черновиках документов, схем, чертежей; информация *о видовых и сигнальных демаскирующих признаках* — в бракованных узлах и деталях, в характеристиках радиоактивных излучений и т.д.; *демаскирующие вещества* — в газообразных, жидких и твердых отходах производства.

Приемники информации этого канала достаточно разнообразны. Это эксперты зарубежной разведки или конкурента, приборы для физического и химического

анализа, средства вычислительной техники, приемники радиоактивных излучений и др.

В рамках вещественного канала ведется химическая и радиационная разведка. Демаскирующие вещества добываются в основном путем взятия проб веществ в твердой, жидкой и воздушной средах. Развиваются активные и пассивные методы и средства анализа веществ, в основном в воздушных средах. В активных методах предусматривается посылка лазерного луча к исследуемой воздушной смеси и анализ излучений результатов взаимодействия. В пассивных методах производится анализ спектра собственных излучений веществ.

Потери носителей с ценной информацией возможны при отсутствии в организации четкой системы учета ее носителей. Например, испорченный машинисткой лист отчета может быть выброшен ею в корзину для бумаги, из которой он будет уборщицей перенесен в бак для мусора на территории организации, а далее при перегрузке бака или транспортировке мусора на свалку лист может быть унесен ветром и поднят прохожим. Конечно, вероятность обеспечения случайного контакта с этим листом злоумышленника невелика, но если последний активно занимается добыванием информации, то область пространства, в котором возможен контакт, значительно сужается и вероятность утечки повышается.

Для предприятий химической, парфюмерной, фармацевтической и других сфер разработки и производства продукции, технологические процессы которых сопровождаются использованием или получением различных газообразных или жидких веществ, возможно образование каналов утечки информации через выбросы в атмосферу газообразных или слив в водоемы жидких демаскирующих веществ.

Подобные каналы образуются при появлении возможности добывания демаскирующих веществ в результате взятия злоумышленниками проб воздуха, воды, земли, снега, пыли на листьях кустарников и деревьев, на траве и цветах в окрестностях организации.

В зависимости от розы (направлений) и скорости ветра демаскирующие вещества в газообразном виде или в виде взвешенных твердых частиц могут

распространяться на расстояние в единицы и десятки км, достаточное для безопасного взятия проб злоумышленниками. Аналогичное положение наблюдается и для жидких отходов.

Конечно, концентрация демаскирующих веществ при удалении от источника убывает, но при утечке их в течение некоторого времени концентрация может превышать допустимые значения за счет накопления демаскирующих веществ в земле, растительности, подводной флоре и фауне.

Отходы могут продаваться другим предприятиям для использования в производстве иной продукции, очищаться перед сливом в водоемы, уничтожаться или подвергаться захоронению на время саморазрушения или распада. Последние операции выполняются для высокотоксичных веществ, утилизация которых другими способами экономически нецелесообразна, и для радиоактивных отходов, которые нельзя нейтрализовать физическими или химическими способами.

Утечка информации о радиоактивных веществах возможна в результате выноса радиоактивных веществ сотрудниками организации или регистрации злоумышленником их излучений с помощью соответствующих приборов.

Утечка информации о радиоактивных веществах возможна по двум каналам: оптическому, носителями информации в котором являются электромагнитные поля в виде у-излучений, и вещественному, носителями информации в котором являются элементарные α - и β -частицы.

Дальность канала утечки информации о радиоактивных веществах через их излучения невелика: для α-излучений она составляет в воздухе единицы мм, β-излучений — см, только γ-излучения можно регистрировать на удалении в сотни и более метров от источника излучения.

Вещественные признаки продукции, содержащие защищаемую информацию, определяются в результате химического, физико-химического и физического анализа. Основу химического анализа составляют химические реакции изучаемого вещества в растворе. Физико-химический анализ предусматривает измерение физических величин, изменение которых обусловлено химическими реакциями.

Физический анализ учитывает изменение физических характеристик добытой пробы, вызванных исследуемым веществом.

Принципы и методы определения химического состава вещества рассматривает аналитическая химия, которая включает качественные и количественные методы анализа. Для аналитической химии характерно применение не только традиционных химических методов, но и физико-химических и физических методов, а также биологических методов.

5.3 Порядок выполнения работы

1. Войдите в среду Internet.

2. В адресной строке наберите http://bnti.ru/ (Техника для спецслужб. Бюро научно-технической информации.)

3. В каталоге технических средств войдите:

1) в раздел «Антитеррористическое оборудование» / «Средства обнаружения и идентификации веществ»

2) в раздел «Досмотровое оборудование» / «Средства обнаружения радиации»

4. Изучите представленные средства

5. Изученные средства (6-8 шт.) внесите в таблицу и проанализируйте ее. Опишите преимущества одних средств перехвата информации перед другими.

Таблица 5.1 – Анализ технических средств перехвата информации в каналах, образованных средствами вычислительной техники.

Наименование ТС	Изображение	Технические характеристики

5.4 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.

6 Лабораторная работа № 6. Моделирование объекта защиты

6.1 Цель работы

Получить навыки моделирования объекта защиты

6.2 Теоретическая часть

Моделирование объектов защиты является одним из главных этапов разработки технической системы защиты информации.

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 информации разрабатывается в виде графа-структуры, представленной на рисунке 6.1, нулевой (верхний) уровень иерархии который соответствует понятию «защищаемая 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 (И) не должна указываться в разных элементах (Э) классификации.

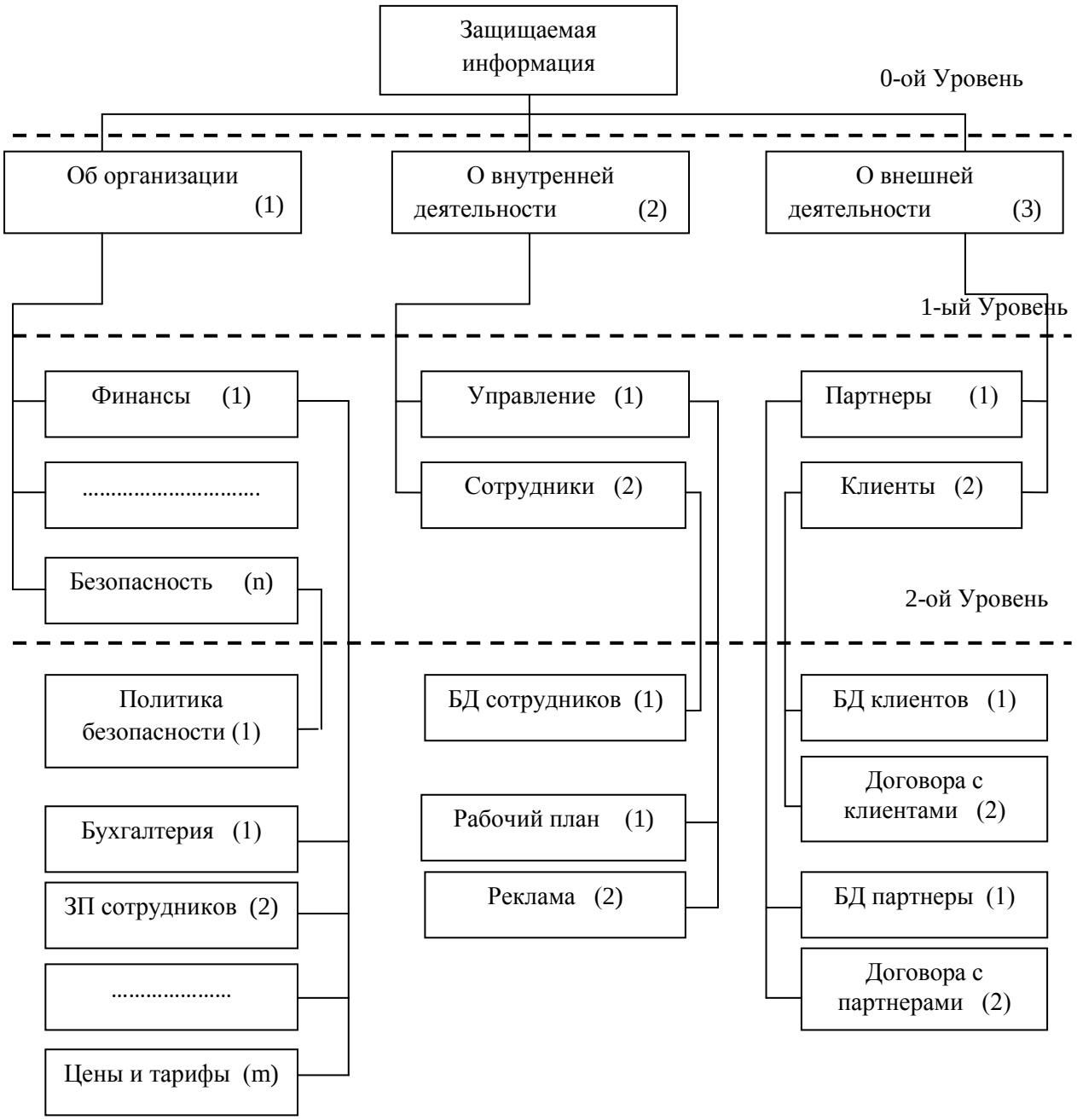

Рисунок 6.1 – Граф-структура защищаемой информации

На основе схемы классификации информации разрабатывается таблица 6.1, 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 (тематического вопроса) и его характеристики: гриф и цена. В столбце 5 указывается носитель информации (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).

Таблица 6.1 – Элементы информации, подлежащие защите

№ элемента информации	Элемент информации	Гриф конфиденциальности элемента информации	Цена	Носитель информации	Местонахождение источника информации
0111	Бухгалтерия	КТ	500000	HDD ПК, договоры, отчеты	Бухгалтерия /Серверная
0112	ЗП сотрудников	КТ	200000	HDD ПК, договоры, отчеты	Бухгалтерия /Серверная
…….	……	……	…..	…….	……
01n1	Политика безопасности	КИ	100000	Документы службы безопасности	Служба безопасности

Задача моделирования объектов защиты состоит в объективном описании и анализе источников конфиденциальной информации и существующей системы ее защиты. Для построения точной модели объекта защиты необходимо:

– 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 таблицу, вариант которой приведен в таблице 6.2.

Таблица 6.2 – Технический паспорт объекта

Название помещения	ООО «Банк»			
Этаж	1	Площадь, м2	333,5	
Количество окон, тип сигнализации. Наличие штор на окнах	36	Двойной стеклопакет, 18 окон выходит на проезжую часть, остальные 18 во внутренний двор, вертикальные жалюзи		
Двери, количество, одинарные , двойные	47	Одинарные,36 выходят в коридор,5 в тамбур, 4 в смежные помещения; двойные, 2 выходят на улицу		
Соседние помещения, название. Толщина стен	нет			
Помещение над потолком, название. Толщина перекрытий	Кровля. Толщина перекрытия – 220мм			
Помещение под полом, название. Толщина перекрытий.	Подвал. Толщина перекрытия – 220мм			
Наличие комнат с неконтролируемым доступом	нет			
Наличие хранилищ бумажных документов	13	Архив на 2-ом этаже, сейфы		
Вентиляционные отверстия, места размещения, размеры отверстий	В сантехузлах – принудительно обязательное 0,3м			
Батареи отопления, типы. Куда выходят трубы	Чугунные радиаторы. Выход - подвал			
Цепи электропитания, количество розеток	220 В, один входящий (исходящий) кабель в каждой кабинет. Источники бесперебойного питания в каждом кабинете			56
Телефон, количество	Стационарный. Места установки – стол. Тип кабеля – ТРП (2-х жильный)			33
Радиотрансляция	нет			
Бытовые электроприборы, количество	Электрочайник			17

Продолжение таблицы 6.2

АРМ, расположение, количество	Монитор и системный блок. Расположение – стол	37
Технические характеристики АРМ	Процессор AMD :Тип процессора - A9-9425, Количество ядер – 2, Частота процессора - 3.1 ГГц, Кэш-память - 1 МБ, Сокет - BGA (FT4), ОЗУ 8 Гб, объём жесткого диска 1 Тб, монитор Samsung SynsMaster 173s, ОС Windows 10	
Количество и тех. характеристики серверов	HPE ProLiant MicroServer Gen10	3
Количество коммутаторов ЛВС	Производитель D-Link, Промышленный управляемый коммутатор 2 уровня с 10 портами 10/100/1000Base-T и 2 портами 1000Base-X SFP (8 портов с поддержкой PoE 802.3af/802.3at (30 Вт), PoE□бюджет до 240 Вт)	4
Выход в Internet, тип подключения	через proxy-сервер	
Характеристика ПО	Информационное ПО: сетевое, СУБД Microsoft SQL Server 2013, 3 БД, объем БД 300 ГБ. Дополнительное ПО: Microsoft Office 2003, антивирусный пакет Kaspersky Internet Security	
Порядок доступа в помещения	Доступ в помещения в течение рабочего дня осуществляется с помощью контроллера доступа и(или) ключа, помещения закрываются на ключ в конце рабочего дня. Ключ и идентификатор доступа сдаются под роспись на КПП.	
Технические средства охраны, количество извещателей	Система охранной сигнализации реализована на базе интегрированной системы. Магнитоконтакные извещатели (двери, окна); извещатель охранный объемный оптико- электронный; извещатель охранный поверхностный звуковой; извещатель охранный поверхностный емкостной.	 47 36 28 13
Телевизионные средства наблюдения	Телекамеры стационарные внутренние; телекамеры уличные;	20 9
Пожарная сигнализация	Пожарный извещатель дымовой. В каждом кабинете 2шт. Пожарный извещатель тепловой	 55 10
Другие средства	Контроллер системы доступа Оконные решетки (диаметр прутьев – 7мм., расстояние между прутьями -100 мм., глубина заделки – 100мм.). Расположены на всех окнах здания.	

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 6.2, 6.3, 6.4 и 6.5 представлены внутренний план помещения, схема освещения и отопления помещения, схема пожарной сигнализации помещения и схема расположения ТСПИ и телефонной линии в помещении соответственно. (Необходимо указать схемы всех этажей в отдельности).

На плане территории организации отмечаются места размещения здания (зданий), забора, контрольно-пропускного пункта, граничащие с территорией улицы и здания, места размещения и зоны действия технических средств охраны, телевизионной системы наблюдения и наружного освещения, места вывода из организации кабелей, по которым могут передаваться сигналы с информацией.

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.

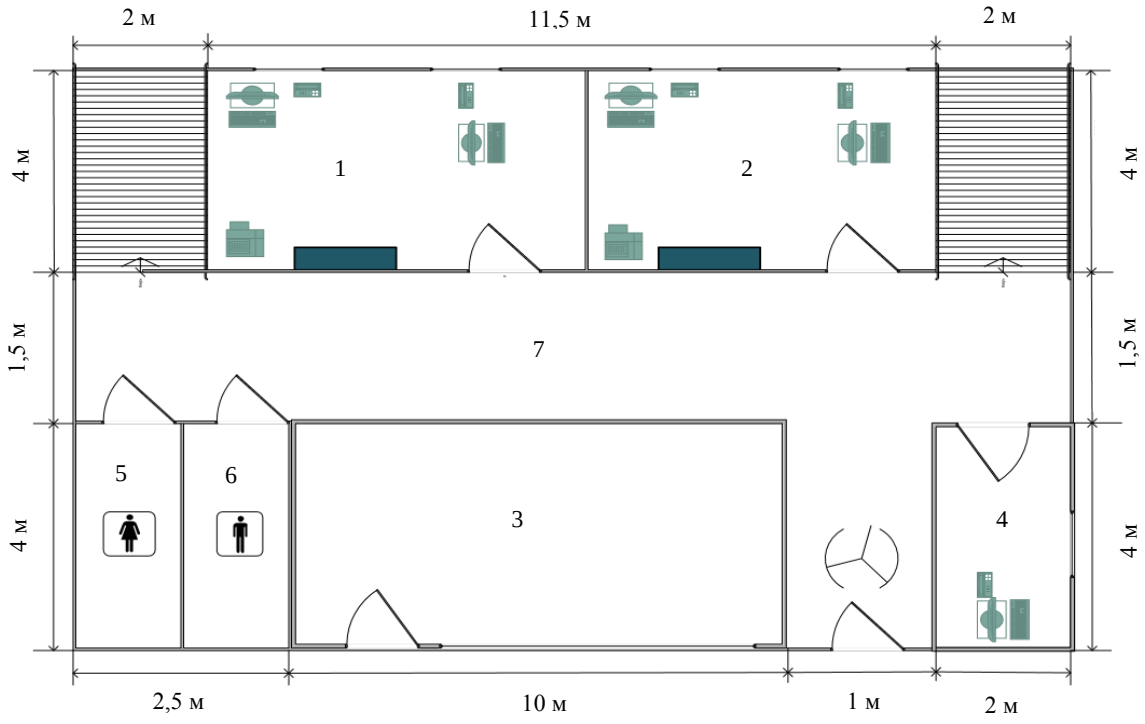

Рисунок 6.2 – Внутренний план помещения

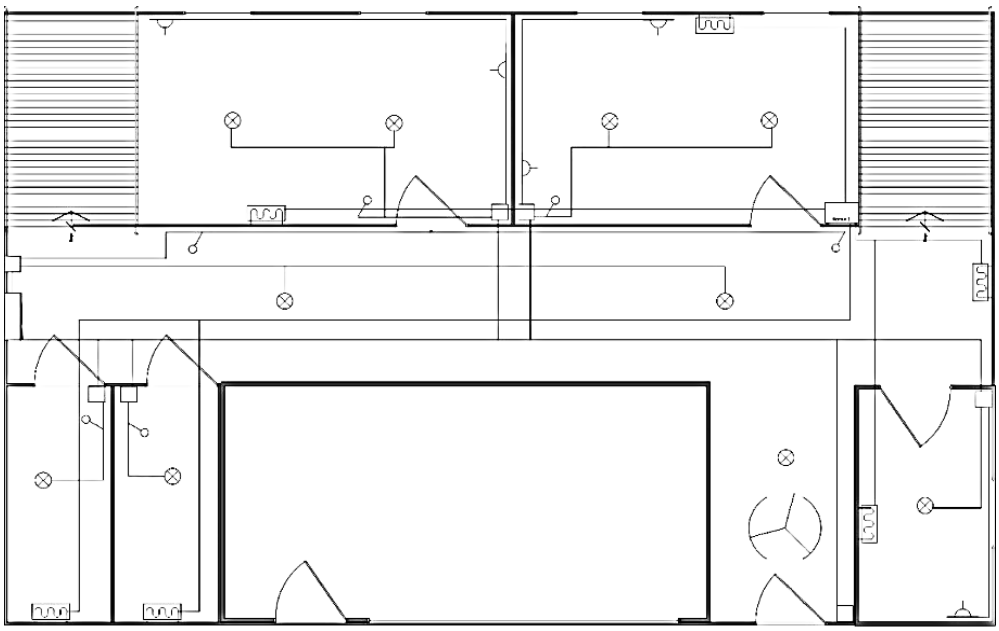

Рисунок 6.3 – Схема освещения и отопления помещения

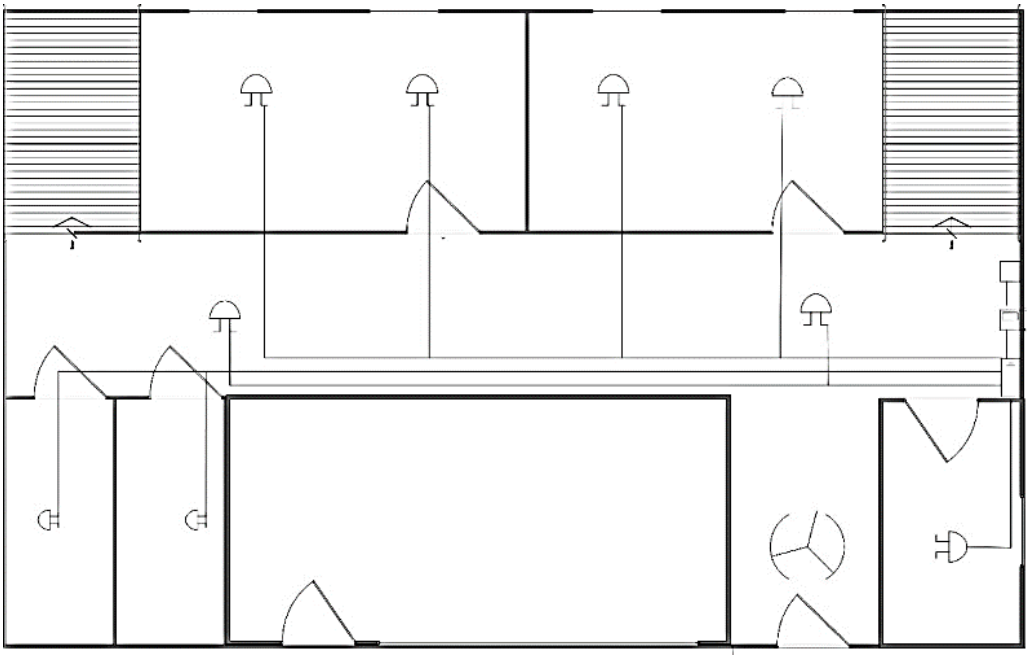

Рисунок 6.4 – Схема пожарной сигнализации помещения

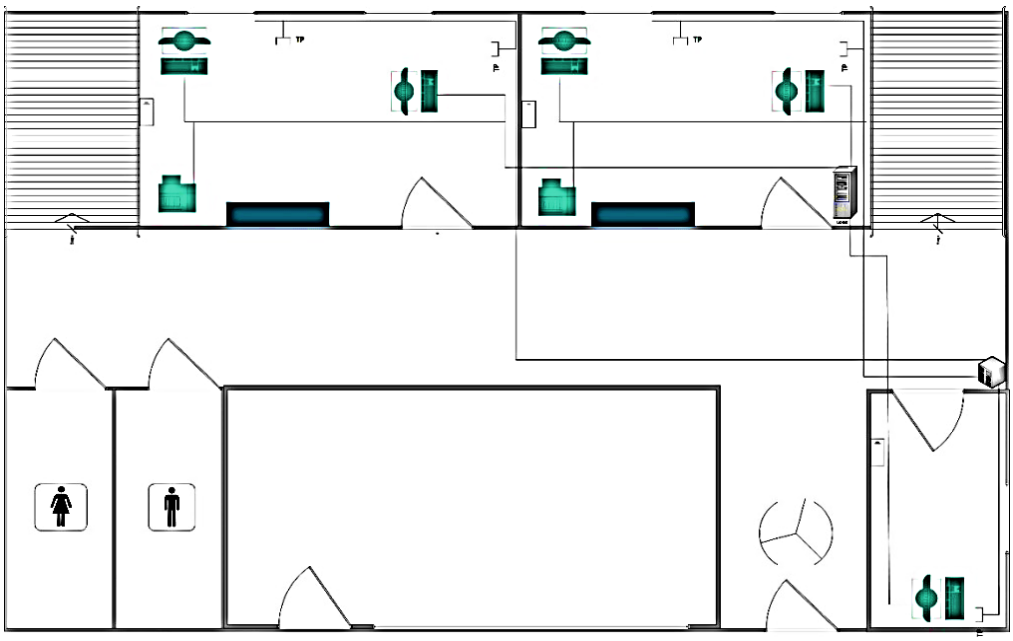

Рисунок 6.5 – Схема расположения ТСПИ и телефонной линии в помещении

6.3 Порядок выполнения работы

1. Определить название организации в соответствии с вариантом, указанным в таблице 6.3.

Таблица 6.3 – Варианты заданий для выполнения лабораторной работы

Вариант	Наименование ОИ	Вариант	Наименование ОИ
1	Отделение ПАО Сбербанка России	11	ГБУЗ «МИАЦ»
2	Страховая компания «Согаз»	12	Газпромэнерго
3	Научно-исследовательский институт «Волга-Урал НИПИГаз»	13	Оренбургский центр занятости населения
4	МФЦ г. Оренбург	14	ОГУ
5	Департамент информационных технологий Оренбургской области	15	Пенсионный фонд Росси по г. Оренбургу
6	МУ МВД «Оренбургское»	16	Оренбургский областной Военный комиссариат
7	Оренбургский областной арбитражный суд	17	Казначейство РФ по Оренбургской области
8	Следственный комитет РФ по Оренбургской области	18	Орский завод холодильного оборудования
9	ФНС РФ г. Оренбурга Дзержинского района	19	Медногорский медно-серный комбинат
10	ПАО «Стрела»	20	ОАО РОСТЕЛЕКОМ г.Оренбург

2. Разработать классификацию информации, подлежащей защите в виде графа-структуры.

3. На основе граф-структуры составить таблицу элементов информации.

4. Разработать технический паспорт объекта защиты в виде таблицы.

5. Разработать планы помещений и схемы размещения в них ОТСС и ВТСС.

6.4 Контрольные вопросы

1 Что включает моделирование объекта защиты?

2 Что из себя представляет схема классификации защищаемой информации?

3 Назовите основные характеристики элементов информации.

4 Обоснуйте необходимость заполнения технического паспорта объекта.

5 Обоснуйте необходимость разработки плана помещения и схем размещения ОТСС и ВТСС.

7 Лабораторная работа № 7. Моделирование технических каналов утечки информации (2ч.)

7.1 Цель работы

Получить навыки моделирования угроз и каналов утечки информации.

7.2 Теоретическая часть

Моделирование угроз и каналов утечки 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.

Действия злоумышленника по добыванию информации, как и других материальных ценностей, определяются поставленными целями и задачами, его мотивами, квалификацией и технической оснащенностью.

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 собой серьезного противника, тщательно готовящего операцию проникновения, изучающего 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.

В зависимости от квалификации, способов подготовки и физического проникновения в организацию злоумышленников разделяют на следующие типы:

– ***неподготовленный,*** который ограничивается внешним осмотром объекта. проникает в организацию через двери и окна, при срабатывании тревожной сигнализации убегает;

– ***подготовленный,*** изучающий систему охраны объекта и готовящий несколько вариантов проникновения в организацию, в основном, путем взлома инженерных конструкций;

– ***квалифицированный,*** который тщательно готовится к проникновению, выводит из строя технические средства охраны, применяет наиболее эффективные способы проникновения.

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 таблицу.

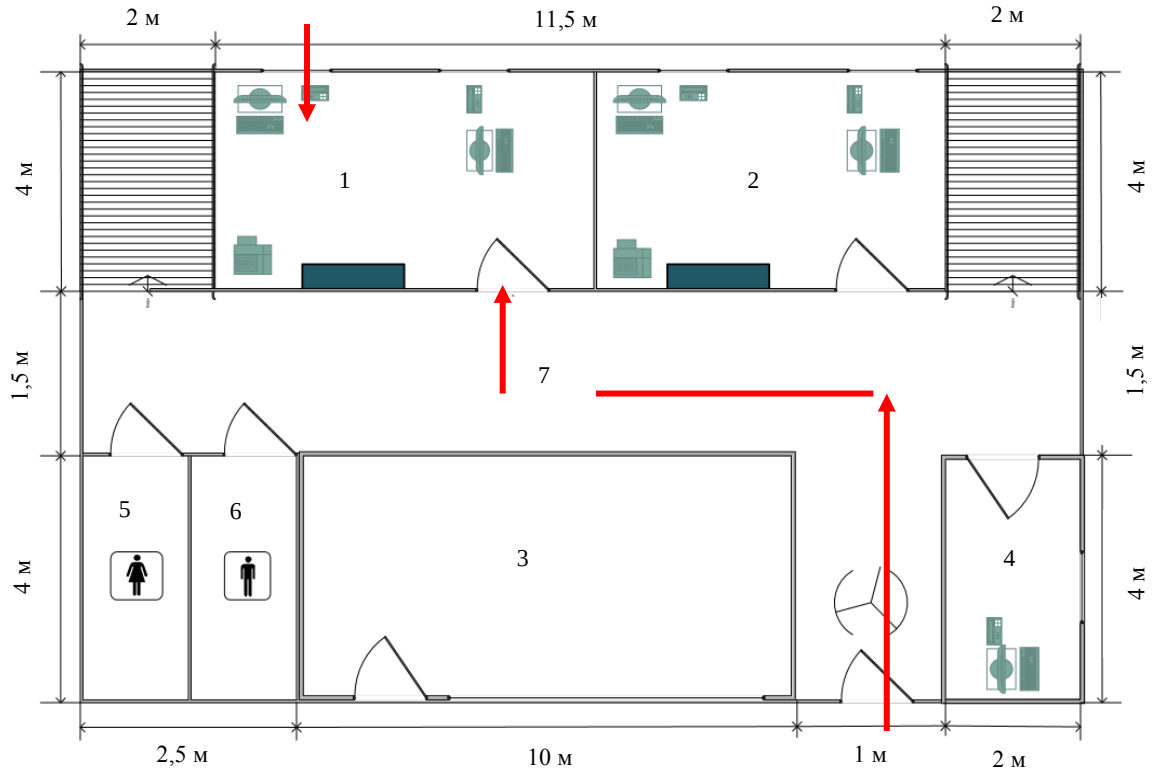

Рисунок 7.1 – Схема проникновения злоумышленника на объект защиты

При моделировании технических каналов утечки, помимо выявления самих каналов, определяется оценка реальности канала, величина и ранг угрозы.

Обнаружение и распознавание каналов утечки информации, как и любых объектов, производится по их демаскирующим признакам. В качестве достаточно общих индикаторов каналов утечки информации могут служить указанные в таблице 7.1 демаскирующие признаки.

Приведенные индикаторы являются лишь ориентирами при поиске потенциальных каналов утечки.

Таблица 7.1– Индикаторы технических каналов утечки информации

Вид канала	**Индикаторы**
Оптический	Окна, выходящие на улицу, близость к ним домов и деревьев. Отсутствие на окнах занавесок, штор, жалюзи. Читаемость содержания документов на столах. Читаемость содержания плакатов на стенах помещения. Малое расстояние между столами сотрудников в помещении. Читаемость экранов мониторов ПЭВМ на столах сотрудников со стороны окон, дверей или других сотрудников. Появление возле территории организации посторонних людей (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. Применение средств радиосвязи. Параллельное размещение кабелей в одном жгуте при разводке их внутри здания и на территории организации. Отсутствие заземления радио и электрических приборов.
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	Наличие 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.

Структурная схема использования технических каналов утечки информации злоумышленником оформляется в таблицу 7.2 модели угроз.

Таблица 7.2 – Модель угроз утечки информации по техническим каналам

№ элемента информации	Цена информации, руб, $С_и$	Источник сигнала, передатчик	Путь утечки	Вид канала	Оценка реальности пути, $Р_р$	Ущерб от реализации угрозы ,руб	Ранг угрозы
1	2	3	4	5	6	7	8
0111	500000	Электромагнитное поле с волнами видимого диапазона	Хищение информации путем видео- или фото-захвата, отображенной на мониторах, бумажных носителях	Оптический	0,2	100000	4
…	….	….	…..	……	……	…..	….
0112	200000	Монитор, системный блок, принтер, кабели, ПЭМИ	С помощью сканирования ПЭМИ широкополосными приемниками можно восстановить информацию,	Электромагнитный	0,5	100000	4

Оценки угроз безопасности информации в результате проникновения злоумышленника к источнику конфиденциальной информации или ее утечки по техническому каналу носят вероятностный характер. При этом рассматривается вероятность $Р_р$ реализуемости рассматриваемого пути или канала, а также цены соответствующего элемента информации $С_и$.

Реальность пути связана с вероятностью выбора злоумышленником пути. Определяется с помощью метода экспертных оценок. Вероятность зависит от простоты реализации именно этого пути проникновения.

Угроза безопасности информации, выраженной в величине ущерба $C_{уи}$ от попадания ее к злоумышленнику, определяется для каждого пути или канала по формуле (1.1):

$$C_{уи} = C_и \times P_р \quad (1.1)$$

Разработка модели угроз безопасности информации заканчивается присваиванием им ранга. Ранг угроз каждая организация устанавливаем самостоятельно.

В данной лабораторной работе ранжирование угроз провести по таблице 7.3.

Таблица 7.3 - Ранжирование угроз информации

Величина угрозы	Ранг угрозы
Более 5×10^5	1
$2\times10^5 \ldots 5\times10^5$	2
$5\times10^4 \ldots 2\times10^5$	3
$2\times10^4 \ldots 5\times10^4$	4
$10^2 \ldots 2\times10^4$	5

На каждый потенциальный способ проникновения злоумышленника к источнику информации и на канал утечки информации целесообразно завести карточку, в которую заносятся в табличной форме характеристики моделей канала.

На этапе разработки способов и средств предотвращения проникновения злоумышленника и утечки информации по рассматриваемому каналу к карточке добавляется приложение с перечнем мер по защите и оценками затрат на нее.

7.3 Порядок выполнения работы

1. На основе моделей объекта, разработанных в лабораторной работе №6, разработайте схемы проникновения злоумышленника на объект защиты.

2. Разработайте Модель угроз утечки информации по техническим каналам для объекта защиты.

7.4 Контрольные вопросы

1 Назовите характеристики каналов утечки информации.

2 Назовите демаскирующие признаки оптического канала утечки информации.

3 Назовите демаскирующие признаки акустического канала утечки информации.

4 Назовите демаскирующие признаки радиоэлектронного канала утечки информации.

5 Назовите демаскирующие признаки материально-вещественного канала утечки информации.

6 Назовите основные виды нарушителей.

Список использованных источников

1. Аверченков, В.И. Разработка системы технической защиты информации : учеб. пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стереотип. – М. : ФЛИНТА, 2011. – 187 с.

2. ГОСТ Р 50922- 2006. Защита информации. Основные термины и определения. - Введ. 2008-02-01. - М.: Стандартинформ, 2007. - 12 с.

3. Каторин, Ю.Ф., Защита информации техническими средствами: учебное пособие / под редакцией Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак. – СПб: НИУ ИТМО, 2012. – 416 с.

4. Креопалов, В.В. Технические средства и методы защиты информации. Учебно-практическое пособие [Электронный ресурс] / В.В. Креопалов - Евразийский открытый институт, 2011. ЭБС УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА. Режим доступа: http://biblioclub.ru/index.php?page=book&id=90753

5. Рембовский, А.М., Выявление технических каналов утечки информации / А.М. Рембовский– М. : Вестник МГТУ, 2003. – 270 с.

6. Титов, А. А. Инженерно-техническая защита информации: учебное пособие [Электронный ресурс] / А. А. Титов. - Томский государственный университет систем управления и радиоэлектроники, 2010. ЭБС УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА. Режим доступа: http://biblioclub.ru/index.php?page=book&id=208567

7. Титов, А.А. Технические средства защиты информации: учебное пособие для студентов специальностей «Организация и технология защиты информации» и «Комплексная защита объектов информатизации». – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2010. – 77 с.

8. Торокин, А. А. Инженерно-техническая защита информации: учеб. пособие для вузов / А. А. Торокин. - М. : Гелиос АРВ, 2005. - 960 с.

9. Хорев, А. А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники / А.А. Хорев // Специальная Техника. – 2010 - № 2. – С. 39-57.