

**Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

Факультет безопасности информационных технологий

Дисциплина:

«Инженерно-технические средства защиты информации»

КУРСОВОЙ ПРОЕКТ

«Проектирование системы защиты от утечки информации по различным каналам»

Выполнили:

Провоторов Роман Анатольевич, студент группы N34491



(подпись)

Проверил:

Попов Илья Юрьевич, доцент ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

Студент	<u>Провоторов Роман Анатольевич</u> (Фамилия И.О)
Факультет	<u>Безопасность информационных технологий</u>
Группа	<u>N34491</u>
Направление (специальность)	<u>10.03.01 (Технологии защиты информации 2019)</u>
Руководитель	<u>Попов Илья Юрьевич</u> (Фамилия И.О)
Должность, ученое звание, степень	<u>к.т.н., доцент ФБИТ</u>
Дисциплина	<u>Инженерно-технические средства защиты информации</u>
Наименование темы	<u>Проектирование системы защиты от утечки информации по различным каналам</u>
Задание	<u>Проектирование системы защиты от утечки информации по различным каналам</u>


Краткие методические указания

1. Курсовая работа выполняется в рамках изучения дисциплины «Инженерно-технические средства защиты информации»
2. Порядок выполнения и защиты курсовой работы представлен в методических указаниях, размещённых на коммуникационной площадке дисциплины.
3. Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

1. Введение.
2. Анализ технических каналов утечки информации.
3. Руководящие документы
4. Анализ защищаемых помещений
5. Анализ рынка технических средств
6. Описание расстановки технических средств
7. Заключение
8. Список литературы

Рекомендуемая литература

Руководитель	<u>(Подпись, дата)</u>
Студент	<u> Провоторов Р. А. 15.12.2023</u> (Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

Студент Провоторов Роман Анатольевич
(Фамилия И.О)

Факультет Безопасность информационных технологий

Группа N34491

Направление (специальность) 10.03.01 (Технологии защиты информации 2019)

Руководитель Попов Илья Юрьевич
(Фамилия И.О)


Должность, ученое звание, степень к. т. н., доцент ФБИТ

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование системы защиты от утечки информации по различным каналам

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1.	Разработка и утверждение задания и календарного плана на курсовую работу	18.10.2022	18.10.2022	
2.	Анализ теоретической составляющей	14.11.2022	14.11.2022	
3.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	15.12.2022	15.12.2022	
4.	Представление выполненной курсовой работы	19.12.2022	19.12.2022	

Руководитель _____
(Подпись, дата)


Студент  Провоторов Р. А. 15.12.2023
(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

Студент	<u>Провоторов Роман Анатольевич</u> (Фамилия И.О)
Факультет	<u>Безопасность информационных технологий</u>
Группа	<u>N34491</u>
Направление (специальность)	<u>10.03.01 (Технологии защиты информации 2019)</u>
Руководитель	<u>Попов Илья Юрьевич</u> (Фамилия И.О)
Должность, ученое звание, степень	<u>к. т. н., доцент ФБИТ</u>
Дисциплина	<u>Инженерно-технические средства защиты информации</u>
Наименование темы	<u>Проектирование системы защиты от утечки информации по различным каналам</u>

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы	<u>Целью работы является повышение защищенности рассматриваемого помещения. Задачами является анализ защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.</u>
2. Характер работы	<u>Конструирование</u>
3. Содержание работы	
1) Введение.	
2) Анализ технических каналов утечки информации	
3) Руководящие документы	
4) Анализ защищаемых помещений	
5) Анализ рынка технических средств	
6) Описание расстановки технических средств	
7) Заключение	
8) Список литературы	
4. Выводы	<u>В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.</u>

Руководитель	<u>(Подпись, дата)</u>
Студент	<u> Провоторов Р. А. 15.12.2023</u> (Подпись, дата)

СОДЕРЖАНИЕ

Введение	6
1 Проектирование системы защиты от утечки информации по различным каналам	7
1.1 Анализ технических каналов утечки информации	7
1.2 Общие сведения об организации на территории помещения	11
1.3 Руководящие документы	12
1.4 Анализ защищаемых помещений	13
1.4.1 План помещения и описание присутствующей мебели	13
1.4.2 Описание помещений	15
1.4.3 Анализ способов утечки информации	16
1.4.4 Выбор необходимых средств защиты информации	17
1.5 Анализ рынка технических средств	17
1.5.1 Акустический и виброакустический каналы	17
1.5.2 Оптический канал	19
1.5.3 Электрический, электромагнитный и акустоэлектрический каналы	19
1.5.1 Побочное электромагнитное излучение и наводки (ПЭМИН)	20
1.6 Описание расстановки технических средств	20
1.6.1 Размещение устройств	20
Заключение	22
Список использованных источников	23

ВВЕДЕНИЕ

Средства обеспечения безопасности информации предназначены для защиты данных в информационных системах. Эти системы включают в себя хранилища данных, информационные технологии для их обработки и соответствующее техническое оборудование. Их целью является предотвращение несанкционированного доступа злоумышленников к ресурсам и данным предприятия, что снижает риск утечек, утраты, искажения, уничтожения, копирования и блокирования информации. Это, в свою очередь, помогает избежать экономических, репутационных и других видов ущерба для предприятия. Разработка эффективного комплекса мер для достижения этой цели является одной из наиболее актуальных задач современности.

В данной работе рассматривается процесс создания комплекса инженерно-технической защиты информации, которая является государственной тайной с уровнем «секретно» на объекте информатизации. Объект защиты включает в себя шесть помещений: кабинет директора, переговорную, офис для сотрудников, кухню/зону отдыха, коридор и архив.

В процессе работы будет проведен анализ технических каналов утечки информации, представлен перечень управляющих документов, проанализированы защищаемые помещения с точки зрения возможных утечек информации и определены требуемые технические средства для обеспечения защиты. Также будет проведен анализ рынка технических средств защиты информации различных категорий, а разработаны схемы размещения выбранных технических средств в защищаемых помещениях.

1 ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО РАЗЛИЧНЫМ КАНАЛАМ

1.1 Анализ технических каналов утечки информации

Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена. Утечка информации может осуществляться по различным каналам. Каналом утечки информации называют канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.

Существует три формы утечки информации:

- разглашение информации;
- несанкционированный доступ к информации;
- утечка информации по техническим каналам.

Согласно теме данной работы, рассматриваться будет только утечка информации по техническим каналам.

Технический канал утечки информации (ТКУИ) - совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка - бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Утечка (информации) по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.



Рисунок 1 – Структура технического канала утечки информации.

На рисунке 1 представлена схема структуры технического канала утечки информации. На вход ТКУИ поступает информация в виде первичного сигнала, представляющего собой носитель с информацией от её источника.

Источниками сигнала могут быть:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;
- источник опасного сигнала;

источник акустических волн, модулированных информацией.

Затем полученная информация преобразуется в форму, предназначенную для записи на носитель данных, соответствующий характеристикам среды передачи. Среда передачи сигнала - это физическая среда, через которую информационный сигнал может распространяться и быть зарегистрированным приемником. Она описывается набором физических параметров, которые определяют условия передвижения сигнала. После этого приемник извлекает информацию с носителя, обрабатывает полученный сигнал (путем усиления) и преобразует информацию в форму сигнала, доступную для восприятия получателю (человеку или техническому устройству).

Согласно физическим свойствам носителя и характеру канала связи технические средства коммуникации и информации делятся на следующие категории:

- Оптические;
- Радиоэлектронные;
- Электрические;
- Электромагнитные;
- Индукционные;
- Акустические;
- Акустоэлектрические;

- Вибро-акустические;
- Материально-вещественные.

Носителем информации в оптическом канале является электромагнитное поле, представленное фотонами. Извлечение информации возможно через наблюдение, например, путем подглядывания через окно или приоткрытую дверь. Альтернативой является применение скрытого устройства с функцией фото- или видеозаписи. Этот метод утечки информации актуален для графического представления данных. Защита осуществляется установкой жалюзи или применением непрозрачных покрытий на всех внешне видимых поверхностях (окна, стеклянные двери и т. д.), а также с использованием доводчиков для дверей.

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон частот радиоэлектронного канала охватывает полосу частот от десятков ГГц до звукового.

Электромагнитный ТКУИ связан с перехватом электромагнитных излучений на частотах работы передатчиков систем и средств связи. Этот метод используется для перехвата информации, передаваемой по каналам радио-, радиорелейной, спутниковой связи. Напряженность электрического поля в точке приема (перехвата) пропорциональна мощности передатчика, высоте антенн, и обратно пропорциональна расстоянию. Этот канал утечки актуален в наличии электронной вычислительной техники, компьютеров или других средств обработки информации в помещении. Электромагнитное излучение, создаваемое при работе технических устройств, известно как побочное электромагнитное излучение и наводки (ПЭМИН); защита осуществляется с использованием специальных технических устройств, создающих электромагнитный шум, чтобы скрыть это излучение.

Электрический ТКУИ связан с возможностью съема информации через контактное подключение аппаратуры злоумышленника к кабельным линиям связи. Электрические колебания, генерируемые в процессе работы электрических устройств, содержат данные о подключенных устройствах. Защита осуществляется с использованием специальных фильтров для электросетей, которые маскируют электрические колебания, порождаемые вычислительной техникой.

Индукционный ТКУИ связан с бесконтактным съемом информации с кабельных линий связи. Эта возможность основана на эффекте образования вокруг кабеля электромагнитного поля, модулированного информационным сигналом. Данное поле перехватывается специальным индукционным датчиком, затем усиливается и демодулируется на аппаратуре злоумышленника. Следует отметить, что обнаружение бесконтактных закладных устройств представляет трудность, поскольку они не изменяют характеристики канала связи. Защита осуществляется с применением специальных программных и аппаратных средств, способных выявлять подобные закладки.

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Съём информации возможен как через подслушивание извне помещения (в случае отсутствия звукоизоляции), так и с использованием закладных устройств с функцией аудиозаписи. Этот метод утечки актуален при передаче информации в звуковой форме (диалоги, совещания и др.). Защита осуществляется с использованием звукоизолирующих материалов, предотвращающих распространение звука за пределы помещения, а также с использованием специальных программных и аппаратных средств, способных выявлять подобные закладные устройства.

В акустоэлектрическом канале информация представлена в форме акустических колебаний, которые воздействуют на электрические сети, вызывая электрические колебания. Сняв эти колебания, можно восстановить исходный акустический сигнал. Этот метод утечки информации актуален в случае наличия электрических сетей, связанных с внешней территорией в контролируемом помещении. Например, в телефонной сети, подав небольшое напряжение на входящую телефонную линию и сняв его на входе, можно получить распространяющуюся в помещение звуковую информацию. Защита осуществляется с использованием специальных фильтров для сетей электропитания, которые скрывают колебания, вызванные воздействием на электрические сети.

В виброакустическом канале информация изначально представлена акустическими колебаниями, которые воздействуют на твердую поверхность, преобразуясь в вибрационные колебания. Этот метод утечки информации актуален практически всегда, так как связан с наличием твердых поверхностей в контролируемом помещении, включая

стены, потолок, пол и другие поверхности. Защита осуществляется с использованием специальных технических устройств, передающих на защищаемую твердую поверхность белый шум, который скрывает вибрационные колебания, вызванные акустическими волнами.

В материально-вещественном канале утечка информации происходит путем несанкционированного распространения вещественных носителей с защищаемой информацией за пределы контролируемой зоны. В качестве таких носителей чаще всего выступают черновики документов и использованная копировальная бумага, а также портативные устройства хранения информации (HHD, SSD, карты памяти и прочее). Против кражи или копирования информации, зафиксированной на материальных носителях, предпринимаются организационные меры, включая введение строгого контроля и учета этих видов носителей данных.

В дополнение к вышеупомянутому, стоит выделить оптико-электронные ТКУИ, связанные с перехватом акустических сигналов при помощи лазерного зондирования оконных стекол. Отдельной угрозой также является возможность проникновения злоумышленника на охраняемую территорию, что делает не менее актуальным вопрос обеспечения контроля доступа к этой территории.

1.2 Общие сведения об организации на территории помещения

Организация производит логистику различных стратегически важных микросхем для военно-промышленного комплекса, а следовательно, имеет «сведения, раскрывающие объемы поставок», которые относятся к государственной тайне в соответствии с «Перечень сведений, отнесенных к государственной тайне». Степень секретности данных сведений – «секретно». Все работы, проводимые в сфере информационной безопасности проводятся отдельной компанией.

Рассмотрим структурную схему организации (рисунок 2) и информационные потоки организации (рисунок 3).

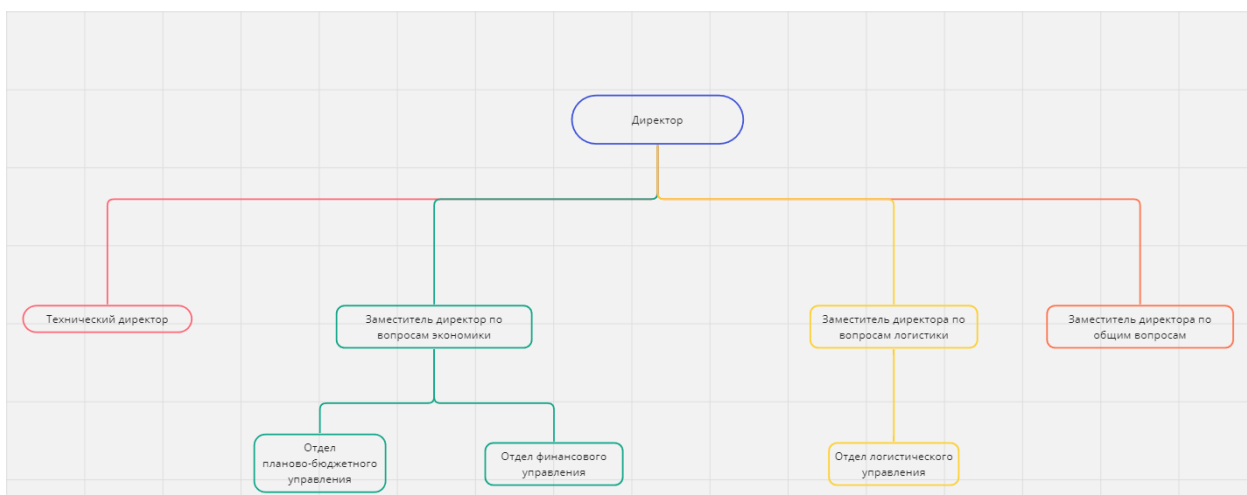


Рисунок 2 – Структурная схема организации

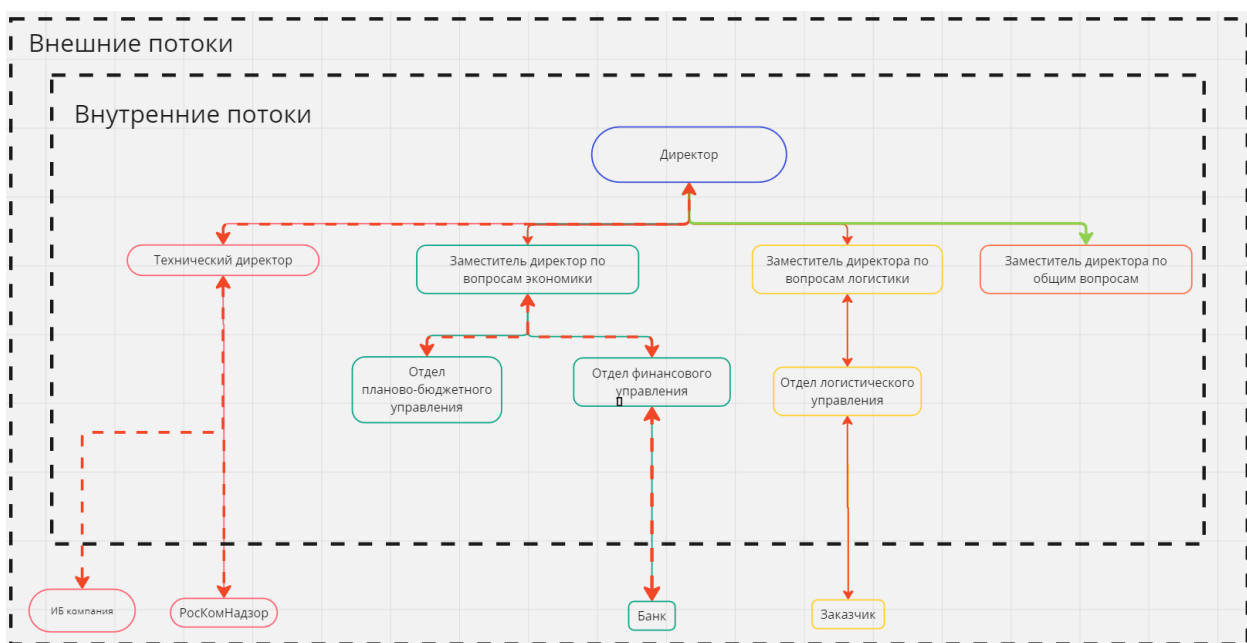


Рисунок 3 – Информационные потоки

На рисунке 2 представлены информационные потоки организации, красными стрелками обозначены закрытые потоки, в которых может передаваться информация ограниченного доступа, а зелеными – открытые. Закрытые потоки в схеме разделены на информацию конфиденциального характера – красная пунктирная линия, и информацию с грифом «секретно» - красная сплошная линия.

1.3 Руководящие документы

- Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров;

- Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации;
- Временный порядок аттестации объектов информатизации по требованиям безопасности информации;
- Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения;
- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;
- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации;
- Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации;
- Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования;
- Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей;

- Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам;

1.4 Анализ защищаемых помещений

1.4.1 План помещения и описание присутствующей мебели

Теперь перейдем к анализу помещений, для которых требуется защита от утечек (рисунок 4).

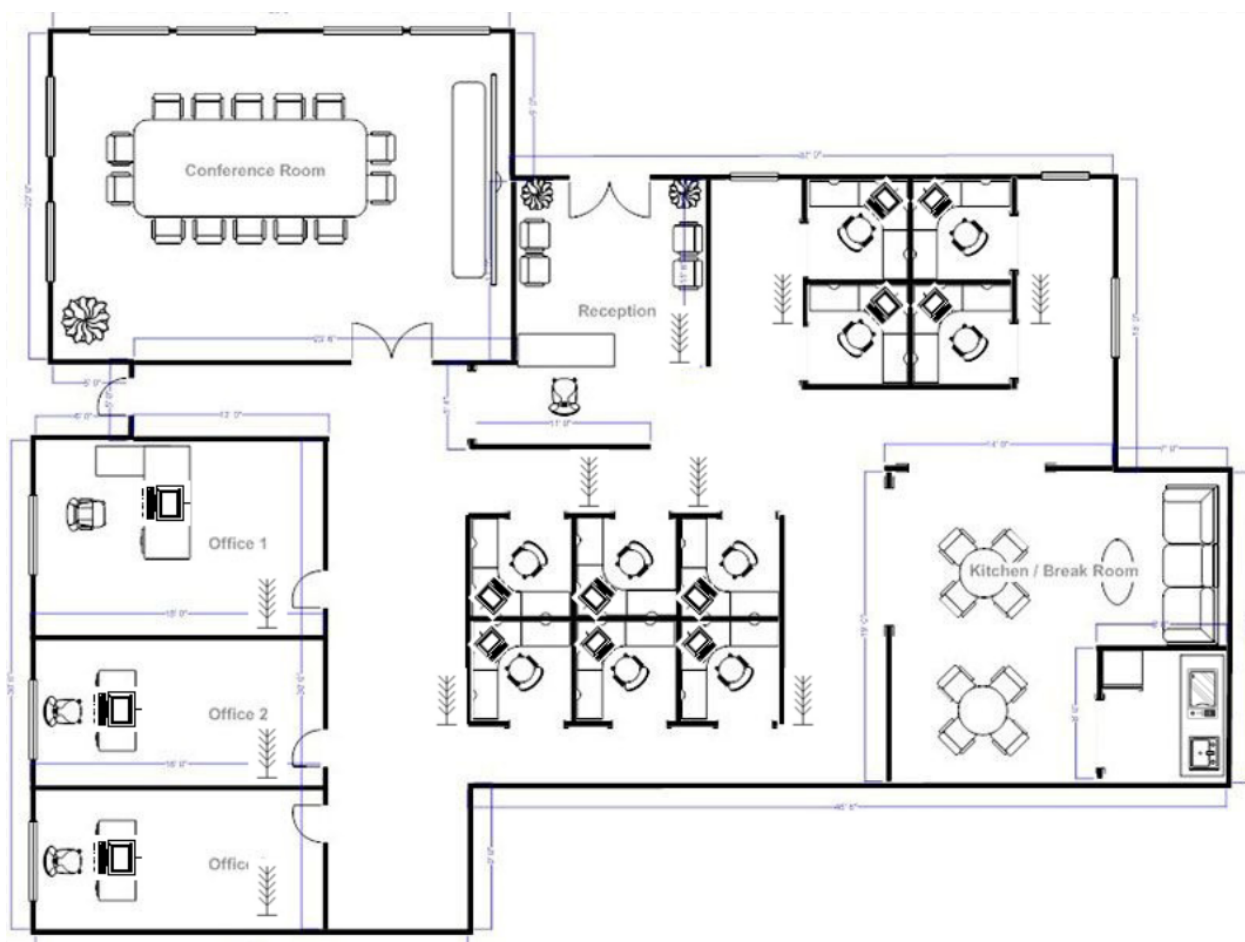


Рисунок 4 – План помещения с мебелью

Описание мебели представлено на рисунке 5.



- Проектор



- Холодильник



- Стул



- Горшок с цветами



- Стол



- Диван



- Раковина



- Кресло



- Вешалки



- Компьютер



- Микроволновая печь

Рисунок 5 - описание мебели

1.4.2 Описание помещений

Теперь определим защищаемые помещения.

В нашем случае это будут:

- Кабинет директора (Office 1) (4,8м на 3,6 м, $S = 17,3 \text{ м}^2$);
- Кабинет заместителя директора по вопросам экономики (Office 2) (4.8м на 2,7 м $S = 13 \text{ м}^2$)
- Кабинет технического директора (Office 3) (4.8м на 2,7 м $S = 13 \text{ м}^2$)
- Переговорная (Conference room) (6,5 м на 3,5 м $S = 22,75 \text{ м}^2$);
- Приемная (Reception) (3м на 3м, $S = 9 \text{ м}^2$);
- Кухня/зал (Kitchen/Break room) (4 м на 3.5 м, $S = 14 \text{ м}^2$).

Теперь опишем данные помещения:

Для ведения переговоров выделено обособленное помещение, в котором помимо стола и стульев имеется проектор. В помещении есть 6 окон, 1 горшок с цветами и 4 розетки.

Для работы директора организации также выделено помещение, в нем присутствует 1 окно, 1 рабочее место с персональным компьютером (стол, кресло и компьютер), 3 розетки и вешалка.

Для работы директора заместителя директора по вопросам экономики выделено помещение, в нем присутствует 1 окно, 1 рабочее место с персональным компьютером (стол, кресло и компьютер), 2 розетки и вешалка.

Для работы технического директора выделено помещение, в нем присутствует 1 окно, 1 рабочее место с персональным компьютером (стол, кресло и компьютер), 2 розетки и вешалка.

Для организации досуга работников имеется комната с залом и кухней. В ней есть 5 розеток, холодильник, а также декоративные элементы в виде дивана, книжного столика, два стола для приема пищи (4 стула на каждом) и микроволновая печь

Также, присутствует приёмная, которая включает в себя 2 горшка с цветами, вешалку, 4 стула для гостей и рабочее место (стол и кресло).

Для работы обычных сотрудников выделены рабочие места в центре офиса (в целом - 10 штук). Каждое рабочее место представляет из себя стол, компьютер и кресло и вешалка (одна на два рабочих)

Помещение в целом расположено на первом этаже офисного здания, окна выходят в закрытый контролируемый двор. Имеется только один вход (северные двери) и выход в территорию для курения (западные двери). Все окна имеют с внешней стороны решетки, а с внутренней используются шторы, плотно закрывающие видимость снаружи.

Стены здания железобетонные, толщиной не менее 10 см.

1.4.3 Анализ способов утечки информации

Во всех помещениях используются декоративные элементы, в которые потенциально могут быть заложены закладные устройства.

Каждое помещение, требующее защиты, оснащено розетками

Таким образом, актуальны следующие угрозы:

- Закладное устройство;
- Электрические и электромагнитные каналы утечки;
- Вибрационные и оптические каналы утечки;
- Акустические, виброакустические, акустоэлектрические каналы утечки.

1.4.4 Выбор необходимых средств защиты информации

Таблица 1 – Средства защиты информации

Каналы утечки	Источники утечки	Пассивная защита	Устройства активной защиты
Вибрационный и виброакустический	Твердые поверхности	Добавление дополнительного помещения перед переговорной	Вибрационное шумление
Оптический	Окна, двери	Шторы, доводчики для плотного закрывания дверей	Бликующие устройства
Электромагнитный и электрический	ПК, розетки, техника	Фильтры для сетей	Электромагнитное шумление
Акустический и акустоэлектрический	Окна, двери	Звукоизоляция, фильтры для сетей электропитания	Акустическое шумление

1.5 Анализ рынка технических средств

Теперь проведем сравнение средств

1.5.1 Акустический и виброакустический каналы

Пассивной защитой будет выступать усиленные двери в кабинет директора и переговорную, дополнительное помещение перед переговорной.

Средствами виброакустического зашумления будет выбрано на основании сравнении компонентов таблицы 2.

Таблица 2 – Виброакустические средства защиты

Средство защиты	Шорох-5Л	ЛГШ-403	ЛГШ-402
Сертификация и соответствие требованиям	Соответствует требованиям по 1-му классу защиты	Соответствует требованиям по 3-му классу защиты	Соответствует требованиям по 4-му классу защиты
Генератор шума	-	Габаритные размеры – не более 82 x 67 x 22 мм.	Габаритные размеры – не более 145 x 100 x 50 мм.
Вибропреобразователи	«ПЭД-8А» Габаритные размеры не более 35 x 30 мм	Габаритные размеры не более 40 x 25 мм	Габаритные размеры не более 40 x 25 мм
Акустические излучатели	«АИ-8А/Н» и «АИ-8А/Мини» Габаритные размеры не более 170 x 71 мм	Габаритные размеры не более 66 x 66 x 25 мм	Габаритные размеры не более 66 x 66 x 25 мм
Напряжение питания	220 В +/-15%	176 / 230 В	187 / 242 В
Диапазон рабочих частот	190 / 11 700 Гц	170 / 12 900 Гц	175 / 11 200 Гц
Потребляемая мощность	Не более 130 ВА	Не более 2,5 В	Не более 20 ВА
Интервал уровня регулировки звукового давления	Не менее 30 дБ	не менее 40 дБ	Не менее 35 дБ

Таким образом, по результатам анализа выбрана система постановки виброакустических помех ЛГШ-403. Выбрано именно эта система, так как она соответствует требованиям к грифу “Секретно” и обладает наилучшими характеристиками по диапазону рабочих частот, интервалу уровня регулировки звукового давления, а также меньшими габаритными размерами, что будет удобнее при установке системы.

В ее состав входят:

- Генератор шума ЛГШ-403
- Вибропреобразователь для стен, полов, потолков ЛВП-2с
- Вибропреобразователь для окон ЛВП-2о
- Акустический излучатель ЛВП-2а
- Вибропреобразователь для трубопроводов ЛВП-2т
- Размыкатели ЛУР

Стоимость самого генератора шума (средняя цена по рынку) – 6000 рублей/шт., а каждой комплектующей - 3640 рублей/шт, размыкатели - 5 590 рублей/шт.

1.5.2 Оптический канал

Обеспечение защиты помещения по оптическим каналам будет осуществлено с помощью штор, которые уже были установлены в помещении. Также используются доводчики для плотного закрывания дверей.

1.5.3 Электрический, электромагнитный и акустоэлектрический каналы

Пассивная защита основывается на установке фильтров для сетей электропитания во всех помещениях.

Выберем средство активной защиты.

Таблица 3 – Электрические и электромагнитные каналы утечки

Изделие	Соната-РС2	ЛГШ - 503	ЛГШ-513
Соответствует требованиям документов	Соответствует требованиям по 1-му классу защиты	Соответствует требованиям по 2-му классу защиты	Соответствует требованиям по 2-му классу защиты
Диапазон частот	0.01–2000 МГц	0,01–1800 МГц	0,009–1800 МГц

Диапазон регулировки уровня шума	Не менее 35 дБ	Не менее 20 дБ	Не более 20 дБ
Потребляемая мощность	Не более 10 Вт	Не более 45 ВА	Не более 45 ВА
Стоимость	24 000 руб.	44 200 руб.	39 000 руб.

По результатам анализа, было выбрано средство защиты ЛГШ-513, так как оно имеет наиболее широкий спектр и защищает от электрического, электромагнитного каналов, а также ПЭМИН. А также имеет приемлемую цену, при условии закрытия нескольких каналов утечки.

1.1.1 Побочное электромагнитное излучение и наводки (ПЭМИН)

Средством ПЭМИН было выбрано входящее в состав ЛГШ-513. Модификация ЛГШ-513Ф соответствует требованиям ФСБ России к средствам активной защиты информации, обрабатываемой техническими средствами от утечки за счет ПЭМИН.

1.2 Описание расстановки технических средств

Выбранные нами средства защиты:

- Система постановки виброакустических и акустических помех ЛГШ-403;
- Генератор шума ЛГШ-513;
- Дверные доводчики – 8 шт.(По одному доводчику на одиночную дверь и по два доводчика на двойные);
- Усиленные двери – 3 шт (В кабинеты директора, заместителя директора по вопросам экономики и переговорную).

Для ЛГШ-403 предусмотрены рекомендуемые правила установки:

- Количество вибропреобразователей и места их размещения определяются индивидуально для каждого конкретного помещения, в зависимости от его

размеров, расположения, конструкции и материалов ограждающих поверхностей.

- Для стен: один вибропреобразователь ЛВП-2с на каждые 6 м².
- Для полов и потолков: один вибропреобразователь ЛВП-2с на каждые 6 м².
- Для окон: один вибропреобразователь ЛВП-2о на каждое стекло или ЛВП-2т на раму каждого оконного проема, или один акустический излучатель ЛВП-2а на межрамное пространство (в случае использования оконных блоков с 2-мя или 3-мя отдельными рамами).
- Для трубопроводов: один вибропреобразователь ЛВП-2т на каждый независимый участок инженерно-технических коммуникаций (например, водопровод и т.д.).
- Для воздухопроводов, вентиляции, двойных дверных коробок и прочих замкнутых объемов: по одному акустическому излучателю ЛВП-2а на каждые 40 м³ каждого замкнутого объема.

1.2.1 Размещение устройств

Каждая дверь оснащена доводчиком для избежания утечек информации по оптическому каналу. Установлены 3 двери в кабинеты директора, заместителя директора по вопросам экономики и переговорную. Каждое окно оснащено шторами с внутренней стороны и решетками с внешней стороны.

На батареи в количестве 9 шт. установлены вибропреобразователи для водопроводов. Также раковина оснащена вибропреобразователем для водопроводов.

В кабинете директора и переговорной установлены размыкатели ЛУР. Сделано это для того, чтобы, в случае совещания или приема у директора, можно было отключить линии питания или ethernet в данном помещении.



Рисунок 6 – Схема размещения устройств

ЗАКЛЮЧЕНИЕ

В ходе данной курсовой работы был составлен план помещения, изучен теоретический материал, проведен анализ возможных каналов утечки секретной информации, описаны необходимые меры. Были выбраны меры защиты информации, проанализированы существующие средства защиты от различных утечек. Также был разработан план установки выбранных пассивных и активных средств защиты.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.
2. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.
3. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст : непосредственный // Молодой ученый. — 2016. — № 3 (107). — С. 69-72. — URL: <https://moluch.ru/archive/107/25842/> (дата обращения: 17.12.2022).