

**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:**

Туголуков Иван Сергеевич, студент группы N34481

  
(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	Туголуков Иван Сергеевич (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34481
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
Задание	Проектирование системы защиты от утечки информации по различным каналам

**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 \_\_\_\_\_  
(Подпись, дата)

Студент \_\_\_\_\_  
(Подпись, дата)

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

**Студент** Туголуков Иван Сергеевич  
(Фамилия И.О.)

**Факультет** Безопасность информационных технологий

**Группа** N34481

**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	13.11.2022	13.11.2022	
2.	Анализ теоретической составляющей	14.11.2022	14.11.2022	
3.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	20.11.2022	20.11.2022	
4.	Представление выполненной курсовой работы	20.12.2022	20.12.2022	

**Руководитель** \_\_\_\_\_  
(Подпись, дата)

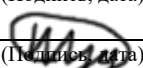
**Студент** \_\_\_\_\_  
(Подпись, дата)

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

Студент	Туголуков Иван Сергеевич (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34481
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

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

1. Цель и задачи работы	Целью работы является повышение защищенности рассматриваемого помещения. Задачами является анализ защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.
2. Характер работы	Конструирование
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	В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель	 (Подпись, дата)
Студент	 (Подпись, дата)

## СОДЕРЖАНИЕ

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 .....	13
1.4.2	Описание помещений .....	14
1.4.3	Анализ способов утечки информации .....	14
1.4.4	Выбор необходимых средств защиты информации .....	15
1.5	Анализ рынка технических средств .....	16
1.5.1	Акустический и виброакустический каналы.....	16
1.5.2	Оптический канал .....	17
1.5.3	Электрический, электромагнитный и акустоэлектрический каналы. Побочное электромагнитное излучение и наводки (ПЭМИН) .....	17
1.1	Описание расстановки технических средств .....	19
1.1.1	Размещение устройств.....	<b>Ошибка! Закладка не определена.</b>

## **ВВЕДЕНИЕ**

Средства обеспечения безопасности информации играют критическую роль в современном мире, где сохранение конфиденциальности и целостности данных становится все более важным аспектом ведения бизнеса. В данной работе фокус устремлен на разработку комплекса инженерно-технической защиты информации, которая обладает статусом государственной тайны с уровнем «секретно» на объекте информатизации.

Анализ технических каналов утечки информации, представление перечня управляющих документов и детальный обзор защищаемых помещений позволят определить потенциальные угрозы и требования к техническим средствам обеспечения безопасности. Осуществление анализа рынка технических средств защиты информации различных категорий и разработка схем размещения этих средств в защищаемых помещениях станут ключевыми этапами процесса создания надежной системы защиты.

Такие меры направлены не только на предотвращение несанкционированного доступа, но и на минимизацию рисков утечек, утраты и искажения важной информации. Кроме того, данная работа охватывает не только технические аспекты защиты, но и анализ управляющих процессов и документации, что подчеркивает комплексный характер предпринятых мер по обеспечению информационной безопасности.

# 1 ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО РАЗЛИЧНЫМ КАНАЛАМ

## 1.1 Анализ технических каналов утечки информации

Утечка информации представляет собой неконтролируемый процесс выхода конфиденциальных данных за пределы организации или лиц, которым эта информация была поручена. Этот процесс может использовать разнообразные каналы, нарушающие безопасность системы. В данном контексте рассматривается утечка информации исключительно по техническим каналам.

Три формы утечки информации включают в себя:

1. Разглашение информации.
2. Несанкционированный доступ к информации.
3. Утечку информации по техническим каналам.

Технический канал утечки информации (ТКУИ) определяется как совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, используемых для добывания защищаемой информации. Утечка по техническому каналу представляет собой неконтролируемое распространение конфиденциальной информации от носителя до технического средства, осуществляющего перехват данных. Этот процесс подразумевает неконтролируемое распространение информации через физическую среду до средства, используемого для перехвата информации (рисунок 1).



Рисунок 1 – Структура технического канала утечки информации.

Источниками информационного сигнала могут быть разнообразные объекты и устройства, использующие различные физические принципы передачи данных. В данном контексте рассматриваются следующие источники сигнала:

- Объект наблюдения, отражающий электромагнитные и акустические волны: этот источник, включает объекты, которые отражают волны, что может быть использовано для получения информации.
- Объект наблюдения, излучающий собственные (тепловые) электромагнитные волны: это включает объекты, излучающие тепловые волны в оптическом и радиодиапазонах.
- Передатчик функционального канала связи: Он представляет собой устройство, выполняющее передачу информации по функциональному каналу связи.
- Закладное устройство: этот источник включает в себя устройства, которые незаметно внедряются для наблюдения или сбора данных.
- Источник опасного сигнала, источник акустических волн, модулированных информацией: это включает устройства, которые могут создавать опасные сигналы или модулировать акустические волны для передачи информации.

После получения сигнала информация преобразуется в форму, подходящую для записи на носитель данных с характеристиками, соответствующими среде передачи. Среда передачи сигнала описывается физическими параметрами, определяющими условия передачи сигнала.

Технические средства коммуникации и информации делятся на различные категории в зависимости от физических свойств носителя и характера канала связи. Например, оптические, радиоэлектронные, электрические, электромагнитные, индукционные, акустические, акустоэлектрические, вибро-акустические, материально-вещественные среды могут быть использованы для передачи информации. Для каждой из них требуются соответствующие методы и средства защиты, учитывающие их физические особенности и потенциальные угрозы утечки информации.

В оптическом канале передачи данных электромагнитное поле, представленное фотонами, служит носителем информации. Возможность извлечения данных существует через визуальное наблюдение, например, путем скрытого наблюдения через окно или частично открытую дверь. Альтернативой может быть использование скрытых устройств с функцией фото- или видеозаписи, что особенно актуально для утечки графически представленных данных.



В целях защиты от подобных утечек рекомендуется устанавливать жалюзи или применять непрозрачные покрытия на видимых поверхностях, таких как окна и стеклянные двери. Также можно использовать доводчики для дверей, чтобы уменьшить возможность незаметного наблюдения извне. Эти меры направлены на предотвращение утечек информации через оптический канал и обеспечение дополнительного уровня конфиденциальности.

Носителем информации в радиоэлектронном канале являются радиоволны, передающие данные через электромагнитное поле. Извлечение информации может осуществляться через перехват радиосигналов, например, при помощи радиоприемника или другого устройства для приема радиоволн. Альтернативой может быть использование специализированных устройств для взлома беспроводных связей или атак на беспроводные сети. Этот метод утечки информации особенно актуален для сетей Wi-Fi, Bluetooth и других беспроводных коммуникаций.

Носителем информации в электрическом канале являются электрические сигналы, передаваемые через провода и цепи. Извлечение информации может осуществляться путем перехвата электрических сигналов, например, при помощи устройств для считывания данных с электрических линий или проводов. Альтернативой может быть использование методов, таких как проводные атаки, при которых злоумышленники физически подключаются к электрическим линиям для сбора информации. Этот метод утечки информации часто применяется в контексте сетевых соединений и передачи данных через проводные каналы.

Носителем информации в электромагнитном канале являются электромагнитные волны, такие как радиоволны и микроволны, передающие данные через пространство. Извлечение информации возможно через перехват электромагнитных волн, например, с использованием антенн и радиоприемных устройств. Альтернативой может быть применение технологий подслушивания или перехвата беспроводных коммуникаций. Этот метод утечки информации актуален в контексте беспроводных сетей, сотовой связи, радиосвязи и других форм беспроводной передачи данных.

Носителем информации в индукционном канале являются изменения магнитного поля, приводящие к индукции электрических сигналов в проводящих средах. Извлечение информации возможно через перехват индукционных сигналов, например, с использованием специализированных индукционных петель или антенн. Альтернативой может быть использование технологий подслушивания, способных регистрировать индуцированные электрические сигналы. Этот метод утечки информации актуален в

контексте аудиосистем, слушательных устройств и прочих приложений, где звуковая информация преобразуется в электрические сигналы.

Носителем информации в акустическом канале являются звуковые волны, передающие звуковую информацию через воздух или другие среды. Извлечение информации возможно через подслушивание звуковых сигналов, например, с использованием микрофонов или акустических датчиков. Альтернативой может быть использование технологий для анализа звукового спектра и преобразования звука в понятные данные. Этот метод утечки информации применим, например, в случае разговоров, аудиоконференций или других акустических событий.

Носителем информации в акустоэлектрическом канале являются ультразвуковые волны в твердых средах, способные создавать электрические сигналы при их воздействии на материалы. Извлечение информации возможно через регистрацию электрических сигналов, индуцированных ультразвуковыми волнами. Альтернативой может быть использование специальных устройств, способных преобразовывать акустическую энергию в электрические сигналы. Этот метод утечки информации может быть актуален, например, в системах медицинского оборудования, где ультразвук применяется для визуализации внутренних структур.

Носителем информации в вибро-акустическом канале являются вибрационные волны, которые передаются через твердые объекты и структуры. Извлечение информации возможно через регистрацию вибраций и их преобразование в звуковые или электрические сигналы. Альтернативой может быть использование специализированных устройств, способных регистрировать вибрационные колебания и интерпретировать их как информацию. Этот метод утечки информации может быть актуален, например, в сфере безопасности, когда злоумышленники пытаются получить конфиденциальные данные через вибрации, передаваемые по поверхности объекта.

Носителем информации в материально-вещественном канале являются физические объекты или материалы, содержащие конфиденциальную информацию. Извлечение информации возможно через физический доступ к данным объектам, например, путем копирования бумажных документов или съема изображений. Альтернативой может быть использование технологий сканирования, фотографирования или других методов, чтобы создать копию важных материалов. Этот метод утечки информации может быть актуален для бумажных документов, физических носителей, таких как USB-флеш-накопители, или других материальных объектов, хранящих конфиденциальные данные.

## 1.2 Общие сведения об организации на территории помещения

Организация специализируется на логистике военного снаряжения, включая броне-комплекты, что делает предоставляемые ею "сведения, раскрывающие объемы поставок" классифицированными как государственная тайна в соответствии с "Перечнем сведений, отнесенных к государственной тайне". Уровень секретности данных сведений определен как "секретно".

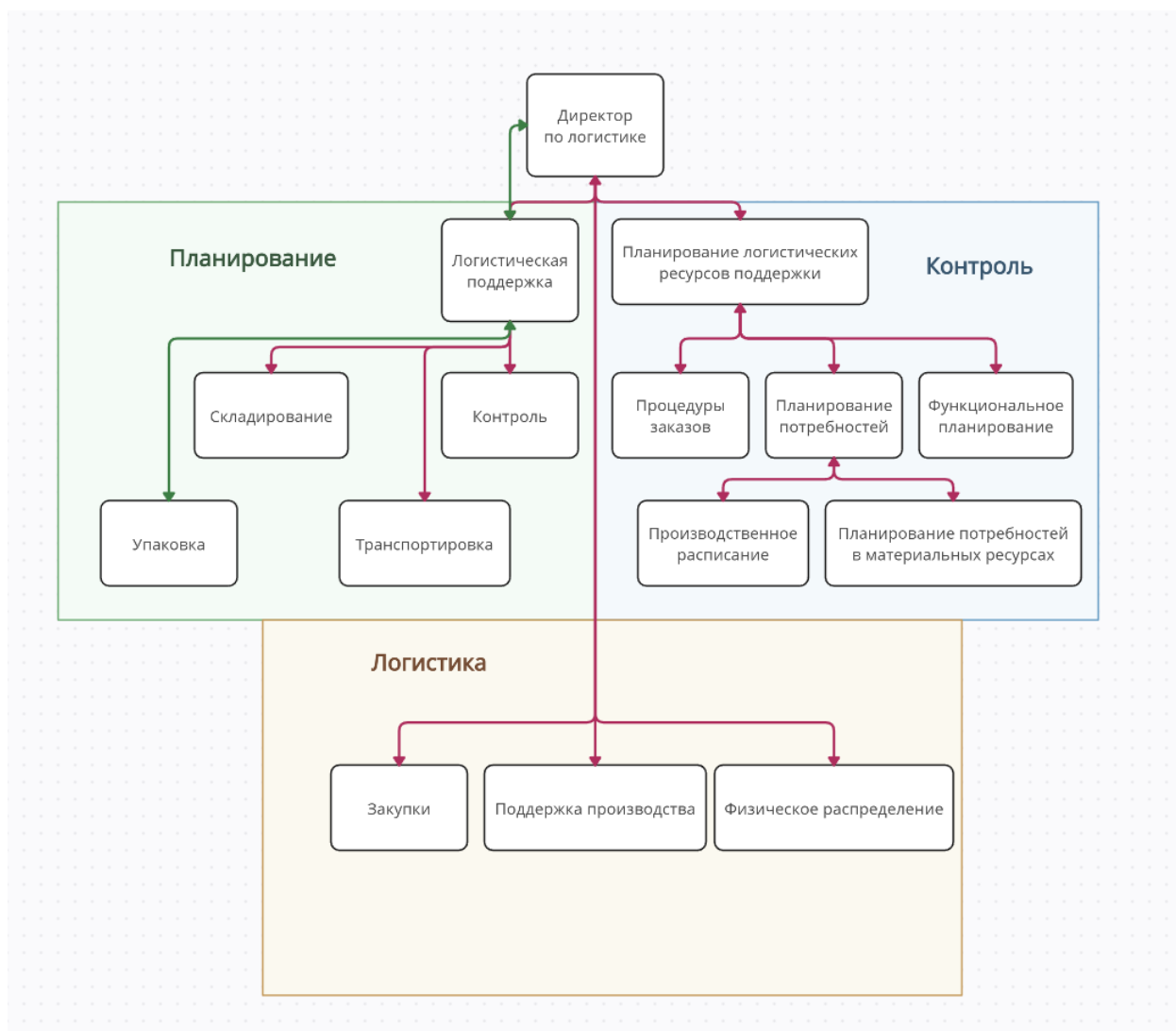


Рисунок 2 – Организационно-функциональная структура организации

На рисунке 2 представлены информационные потоки организации. Красные стрелки обозначают закрытые потоки, где передача информации ограничена по доступу, в то время как зеленые стрелки представляют открытые потоки.

### 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

План помещений представлен на рисунках 3-4.

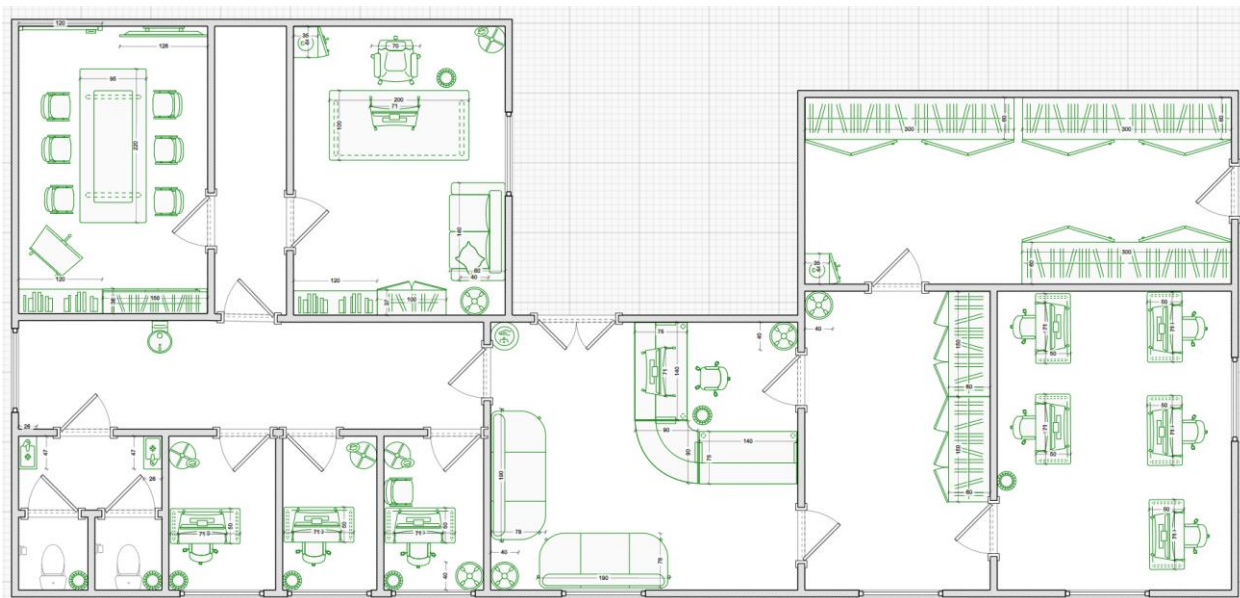


Рисунок 3 – План помещения с мебелью

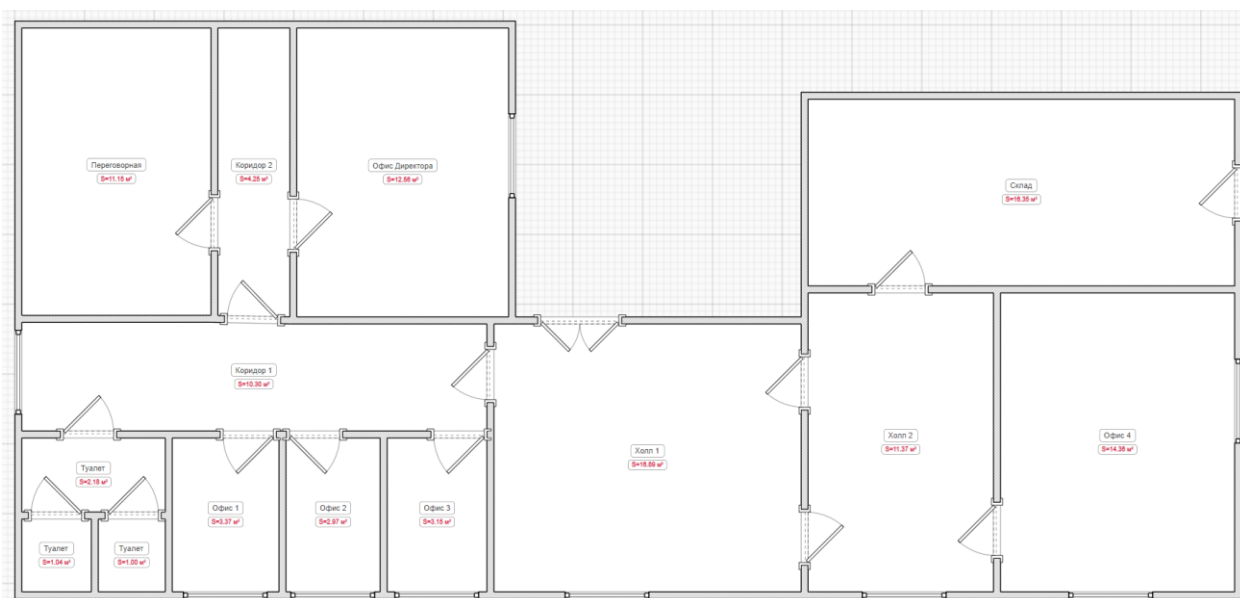


Рисунок 4 – План помещения с размерами

### **1.4.2 Описание помещений**

Переговорная: магнитно-маркерная доска, телевизор, стул (6 шт.), флипчарт, стол, шкаф (2 шт.).

Офис Директора: сейф, стол, кресло, компьютер, диван, шкаф (2 шт.), вешалка, корзина.

Офис 1-2: стол, кресло, компьютер, шкаф (2 шт.), вешалка, корзина.

Офис 3: стол, кресло (2 шт.), компьютер, шкаф (2 шт.), вешалка, корзина.

Офис 4: стол (5 шт.), кресло (5 шт.), компьютер (5 шт.), корзина.

Холл 1: ресепшн-стойка, кресло, компьютер, диван (2 шт.), санитайзер на стойке.

Холл 2: шкаф (2 шт.).

Склад: сейф, шкаф (3 шт.).

Туалет: раковина (2 шт.), унитаз (2 шт.).

Коридор: питьевой фонтанчик.

Помещения расположены на первом этаже здания, где территория ограничена забором. Имеется 1 вход и 1 выход на дворовую территорию. На внешней стороне окон стоят металлические решетки, а на внешней шторы и жалюзи. Стены состоят из железобетона, где минимальная толщина 15 см.

### **1.4.3 Анализ способов утечки информации**

В каждом помещении используются декоративные элементы, которые могут потенциально скрывать закладные устройства. Кроме того, каждое помещение, требующее защиты, оборудовано розетками. В результате возникают следующие актуальные угрозы:

- Закладное устройство: возможность скрытой установки устройств, которые могут использоваться для незаконного сбора информации.
- Электрические и электромагнитные каналы утечки: потенциальные пути для несанкционированной передачи информации через электрические системы и электромагнитные волны.
- Вибрационные и оптические каналы утечки: угроза, связанная с возможностью передачи информации через вибрации или оптические средства.
- Акустические, виброакустические, акустоэлектрические каналы утечки: риски, связанные с возможностью использования звуковых, виброакустических и акустоэлектрических средств для утечки конфиденциальной информации.

Такие угрозы требуют внимательного внедрения мер безопасности для защиты помещений от потенциальных утечек информации.

#### 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, мебель, техническое оборудование	Использование вибропоглощающих материалов, установка дополнительного помещения с виброзащитой	Использование вибрационных детекторов, систем анализа виброакустических сигналов, вибрационное зашумление
Оптический	Окна, двери, оптические устройства	Применение штор и жалюзи, установка доводчиков для дверей.	Использование инфракрасных детекторов, систем блокировки оптических каналов, бликующие устройства
Электромагнитный и электрический	ПК, розетки, техника	Установка фильтров для сетей, экранирование электромагнитных волн, защита от электрических полей	Использование детекторов электромагнитных излучений, систем шифрования данных, электромагнитное зашумление
Акустический и акустоэлектрический	Окна, двери, аудиоустройств а	Применение звукоизоляции, установка фильтров для электросетей, использование акустических экранов	Использование акустических детекторов, систем антивирусной акустики, акустическое зашумление

## 1.5 Анализ рынка технических средств

### 1.5.1 Акустический и виброакустический каналы

Введение пассивных мер безопасности включает в себя установку усиленных дверей в кабинете директора и переговорной, а также дополнительное помещение (коридор 2). Эти меры направлены на укрепление физических барьеров и предотвращение несанкционированного доступа.

Для средств виброакустического зашумления будет проведено сравнение компонентов с целью выбора наиболее эффективных в данном контексте (таблица 2).

Таблица 2 – Виброакустические средства защиты

Средство защиты	Шорох-5Л	ЛГШ-403	ЛГШ-402	СОНАТА АВ-4Б
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	Соответствует требованиям по 1-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	Габаритные размеры не более 35 x 30 мм	Габаритные размеры не более 40 x 25 мм	Габаритные размеры не более 40 x 25 мм	Габаритные размеры не более 19 x 47 мм
Акустические излучатели	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	Габаритные размеры не более 53 x 38 мм
Напряжение питания	220 В +-15%	176 / 230 В	187 / 242 В	220 В
Диапазон рабочих частот	190 / 11 700 Гц	170 / 12 900 Гц	175 / 11 200 Гц	175 / 11200 Гц
Потребляемая мощность	Не более 130 ВА	Не более 2,5 В	Не более 20 ВА	Не более 10 В
Интервал уровня регулировки звукового давления	Не менее 30 дБ	не менее 40 дБ	Не менее 35 дБ	Не менее 35 дБ

Учитывая потенциальные угрозы, такие как закладные устройства, электромагнитные каналы утечки и другие, предусмотрены меры пассивной защиты, такие как усиленные двери в кабинетах, а также активные меры, включая систему виброакустических помех ЛГШ-403. Эта система выбрана в результате тщательного



анализа, учитывающего требования к грифу секретности и оптимальные технические характеристики.

Таким образом, введение системы виброакустических помех ЛГШ-403 представляет собой комплексную меру, обеспечивающую безопасность информации и подчеркивая важность принятых мер по защите конфиденциальных данных. В ее состав входят:

- генератор шума ЛГШ-403 (6 000 руб.)
- вибропреобразователь для стен, полов, потолков ЛВП-2с (3 640 руб.)
- вибропреобразователь для окон ЛВП-2о (3 640 руб.)
- акустический излучатель ЛВП-2а (3 640 руб.)
- вибропреобразователь для трубопроводов ЛВП-2т (3 640 руб.)
- размыкатели ЛУР (5 590 руб.)

### **1.5.2 Оптический канал**

В рамках обеспечения защиты помещения от потенциальных угроз по оптическим каналам приняты следующие меры. В помещении установлены шторы и жалюзи, предназначенные для блокировки визуального доступа и предотвращения возможных попыток наблюдения извне. Эти шторы и жалюзи, как элемент пассивной защиты, играют важную роль в создании барьера для оптических методов утечки информации.

Дополнительно к этим мерам, применяются доводчики для дверей с целью обеспечения плотного и надежного закрытия. Эти доводчики вносят элемент активной защиты, предотвращая возможные проникновения через двери и поддерживая высокий стандарт безопасности помещения.

Такие шаги по обеспечению физической защиты через шторы и доводчики демонстрируют системный и комплексный подход к обеспечению безопасности в рамках принятых стандартов и требований по защите информации.

### **1.5.3 Электрический, электромагнитный и акустоэлектрический каналы. Побочное электромагнитное излучение и наводки (ПЭМИН)**

В целях обеспечения пассивной защиты было принято решение об установке фильтров для сетей электропитания во всех помещениях. Эти фильтры представляют собой эффективные средства контроля и фильтрации электромагнитных помех, направленных на сеть электропитания.

Установка таких фильтров способствует снижению уровня электромагнитных шумов и помех, что в свою очередь способствует повышению общей электромагнитной совместимости и надежности сетей электропитания. Это имеет важное значение для поддержания стабильности работы оборудования и предотвращения возможных негативных воздействий на электронные системы.

Для средств активных средств будет проведено сравнение компонентов с целью выбора наиболее эффективных в данном контексте (таблица 3).

Таблица 3 – Электрические и электромагнитные каналы утечки

<b>Изделие</b>	<b>Соната-РС2</b>	<b>ЛГШ - 503</b>	<b>ЛГШ-513</b>
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.

После проведенного анализа было принято решение в пользу выбора средства защиты ЛГШ-513. Это решение обусловлено множеством преимуществ, которые предоставляет данное средство. ЛГШ-513 охватывает широкий спектр защиты, включая электрические, электромагнитные каналы, а также предоставляет защиту от воздействия ПЭМИН (переносимых электромагнитных излучений наведенного характера).

Кроме того, у ЛГШ-513 есть привлекательные аспекты, такие как приемлемая цена, что делает его более доступным средством защиты. Важно отметить, что при закрытии нескольких каналов утечки данный продукт продемонстрировал свою эффективность.

Таким образом, выбор ЛГШ-513 обоснован как оптимальное решение, сочетающее в себе эффективность, широкий охват защиты и разумную цену.

## 1. Описание расстановки технических средств

Выбранные нами средства защиты:

- система постановки виброакустических и акустических помех ЛГШ-403;
- генератор шума ЛГШ-513;
- жалюзи;
- штора;
- усиленные двери.

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;
- стены: один вибропреобразователь ЛВП-2с на каждые 6 м<sup>2</sup>;
- полы и потолки: один вибропреобразователь ЛВП-2с на каждые 6 м<sup>2</sup>;
- окна: 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);
- трубопровод: один вибропреобразователь ЛВП-2т на каждый независимый участок инженерно-технических коммуникаций (например, водопровод и т.д.);
- для воздуховодов, вентиляции, двойных дверных коробок и прочих замкнутых объемов: по одному акустическому излучателю ЛВП-2а на каждые 40 м<sup>3</sup> каждого замкнутого объема.

Итоговые затраты представлены в таблице 4.

Таблица 4 – Общие затраты

Изделие	Цена, руб. (1 шт.)	Количество, шт.	Цена, руб. (общее)
ЛГШ-403	19 400	6	116 400
ЛГШ-513	39 000	7	273 000
Усиленная дверь Lars Grau	46 940	4	187 760
Размыкатели ЛУР	5 590	7	39 130
Blackout-жалюзи 2х3м	5 280	6	31 680
ЛВП-2с	3 640	35	127 400

Изделие	Цена, руб. (1 шт.)	Количество, шт.	Цена, руб. (общее)
ЛВП-2о	3 640	6	21 840
ЛВП-2т	3 640	6	21 840
ЛВП-2а	5 200	6	21 840
<b>Итого</b>			<b>840 890</b>

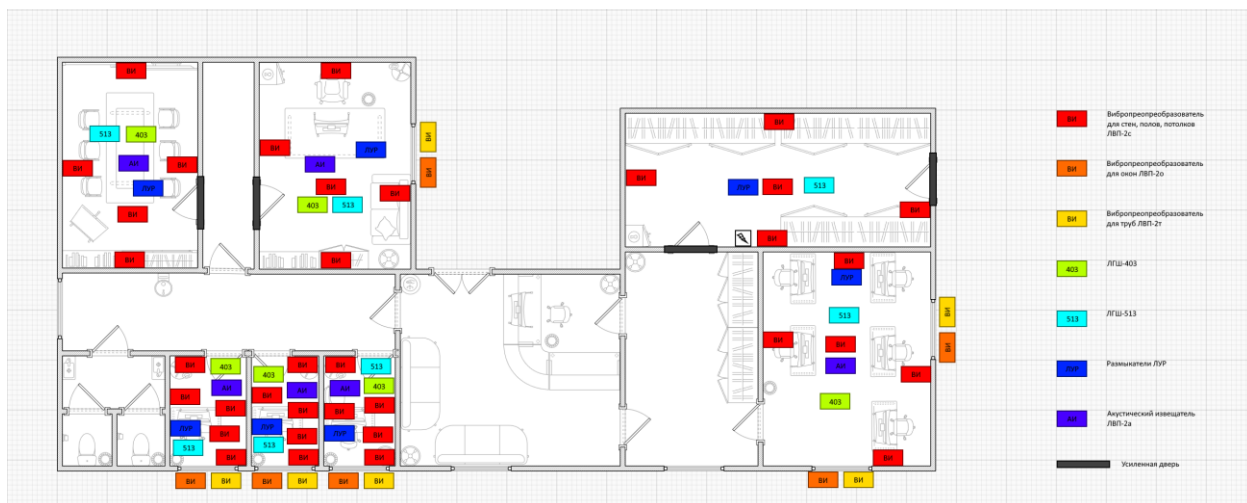


Рисунок 5 – Схема размещения устройств

## **ЗАКЛЮЧЕНИЕ**

В ходе выполнения курсовой работы был осуществлен комплекс деятельности, направленный на обеспечение безопасности помещения. Этот процесс включал в себя несколько важных этапов. В начале работы был разработан план помещения, что предоставило базовый каркас для последующих мероприятий.

После этого был проведен тщательный анализ теоретического материала, связанного с безопасностью информации, и изучены возможные каналы утечки секретной информации. На основе полученных данных были выделены необходимые меры для обеспечения безопасности, как пассивные, так и активные.

Были проанализированы различные средства защиты от утечек, включая как существующие, так и новые технологии. Этот этап позволил выбрать оптимальные средства защиты, а также учесть их совместимость и взаимодействие.

В итоге был разработан подробный план установки выбранных средств, как пассивных, так и активных, с учетом особенностей помещения и требований к безопасности. Это планирование стало ключевым этапом в обеспечении эффективной системы защиты информации в данном помещении.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.
2. Хорев А. А. Техническая защита информации: учебное пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010. — 436 с.
3. Detector Systems: Системы комплексной безопасности [Электронный ресурс]. – Режим доступа: <https://detsys.ru/> (дата обращения: 01.10.2023)
4. 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: 17.10.2023).