

**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»

Выполнил:

Шапошников Арсений Константинович, студент группы N34491


(подпись)

Проверил:

Попов Илья Юрьевич, доцент ФБИТ, к.т.н.

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

Студент	Шапошников Арсений Константинович (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34491
Направление (специальность)	10.03.01 (Технологии защиты информации)
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	19.12.2023 (Подпись, дата)

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

Студент Шапошников Арсений Константинович
(Фамилия И.О)

Факультет Безопасность информационных технологий

Группа N34491

Направление (специальность) 10.03.01 (Технологии защиты информации)

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	28.10.2023	28.10.2023	
2.	Анализ теоретической составляющей	10.11.2022	10.11.2023	
3.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	15.11.2022	15.11.2023	
4.	Представление выполненной курсовой работы	19.12.2023	19.12.2023	

Руководитель _____
(Подпись, дата)

Студент  19.12.2023
(Подпись, дата)

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

Студент	Шапошников Арсений Константинович (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34491
Направление (специальность)	10.03.01 (Технологии защиты информации)
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 Исследовательская работа
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	19.12.2023 (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)	18
<u>1.6</u>	Описание расстановки технических средств	19

ВВЕДЕНИЕ

Средства обеспечения безопасности информации играют ключевую роль в современном мире, где обеспечение конфиденциальности и целостности данных становится все более критическим для успешного ведения бизнеса. В данной исследовательской работе основное внимание уделяется созданию комплекса инженерно-технической защиты информации, имеющего статус государственной тайны с уровнем «секретно» на объекте информатизации.

Анализ технических каналов утечки информации, представление перечня управляющих документов и детальный обзор защищаемых помещений позволяют выявить потенциальные угрозы и установить требования к техническим средствам обеспечения безопасности. Проведение анализа рынка технических средств защиты информации различных категорий и разработка схем размещения этих средств в защищаемых помещениях являются ключевыми этапами процесса формирования надежной системы защиты.

Принятые меры направлены не только на предотвращение несанкционированного доступа, но также на минимизацию рисков утечек, утраты и искажения важной информации. Кроме того, данное исследование охватывает не только технические аспекты защиты, но также включает в себя анализ управляющих процессов и документации, подчеркивая тем самым 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 является неконтролируемым процессом, при котором конфиденциальные данные покидают организацию или лицо, которым они были доверены. Этот процесс может использовать разнообразные каналы, нарушая безопасность системы. В данном контексте фокус сосредоточен исключительно на технических каналах утечки информации.

Три формы утечки информации включают в себя:

1. **Разглашение информации:** раскрытие конфиденциальных данных без соответствующего разрешения.
2. **Несанкционированный доступ к информации:** нелегальное получение доступа к защищенным данным.
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 данных (рисунок 1).



Рисунок 1 – Структура технического канала утечки информации.

Источниками информационного сигнала могут выступать разнообразные объекты и устройства, использующие различные физические принципы передачи данных. Ниже 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. Этот метод передачи данных, характеризующийся использованием световых волн, предоставляет возможность извлечения информации через визуальное наблюдение. Например, потенциальная угроза утечки данных может возникнуть в результате скрытого наблюдения через окно или частично открытую дверь, где непосредственный визуальный доступ к оптическому каналу может быть осуществлен без использования специализированных средств.

Альтернативным методом может быть использование скрытых устройств, оснащенных функцией фото- или видеозаписи. Такие устройства могут эффективно перехватывать оптически передаваемую информацию, создавая потенциальный риск конфиденциальности данных. Таким образом, в обеспечении безопасности оптического канала важным является не только техническая защита, но и осведомленность относительно возможных угроз, связанных с визуальным доступом и использованием скрытых устройств.

С целью предотвращения подобных утечек рекомендуется устанавливать жалюзи или применять непрозрачные покрытия на видимых поверхностях, таких как окна и стеклянные двери. Также можно использовать доводчики для дверей с целью уменьшения вероятности незаметного наблюдения извне. Эти меры направлены на предотвращение утечек информации через оптический канал и обеспечение дополнительного уровня конфиденциальности.

В радиоэлектронном канале носителем информации являются радиоволны, передающие данные через электромагнитное поле. Извлечение информации возможно путем перехвата радиосигналов, например, с использованием радиоприемника или другого устройства для приема радиоволн. Альтернативой может быть применение специализированных устройств для взлома беспроводных связей или атак на беспроводные сети. Этот метод утечки информации особенно актуален в случае сетей Wi-Fi, Bluetooth и других беспроводных коммуникаций.

В электрическом канале носителем информации служат электрические сигналы, передаваемые по проводам и цепям. 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 используется в контексте сетевых соединений и передачи данных по проводным каналам.

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

В индукционном канале носителем информации служат изменения магнитного поля, которые приводят к индукции электрических сигналов в проводящих средах. Извлечение информации возможно путем перехвата 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 других приложений, где звуковая информация преобразуется в электрические сигналы.

В акустическом канале носителем информации являются звуковые волны, передающие звуковую информацию через воздух или другие среды. Извлечение информации возможно путем подслушивания 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.

В акустоэлектрическом канале носителем информации 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.

В вибро-акустическом канале носителем информации являются вибрационные волны, передающиеся 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.

В материально-вещественном канале носителем информации 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

Название организации: «Быстро и в точку»

Организация специализируется на логистике военного оборудования, включая головные обтекатели для баллистических ракет, 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".

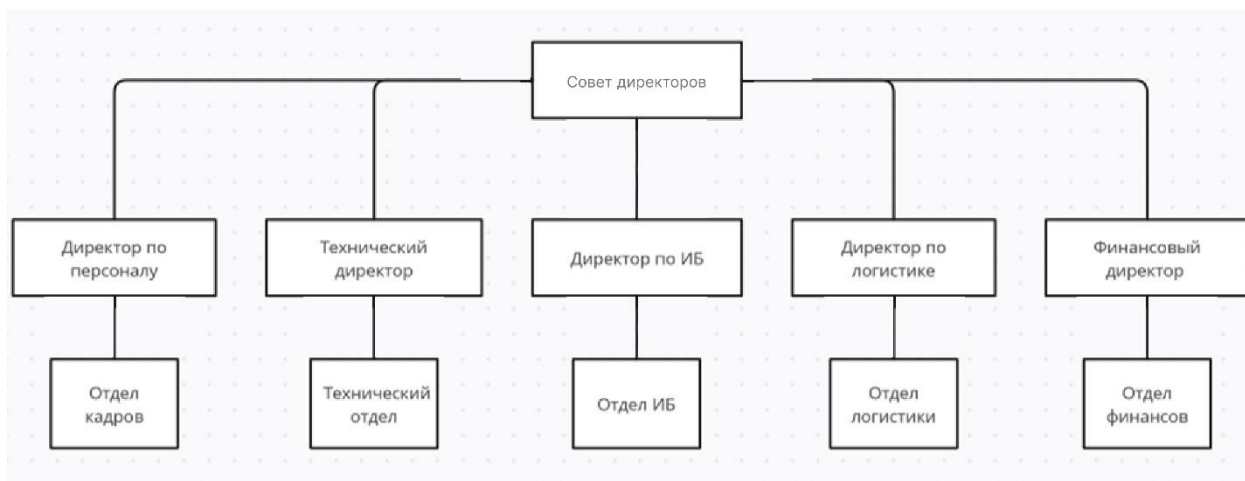


Рисунок 2 – Структурная схема организации

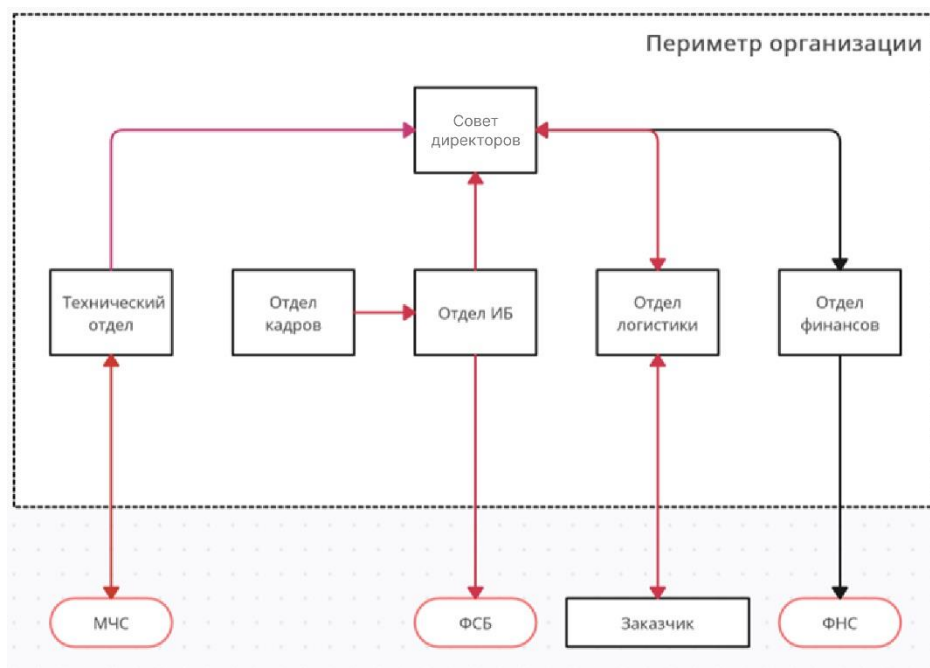


Рисунок 3 – Информационные потоки организации

На рисунке 3 представлены информационные потоки организации. Красные стрелки обозначают закрытые потоки, где передача информации ограничена по доступу, в то время как черные 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

Проведем анализ помещения организации.

1.4.1 План помещения

План помещений представлен на рисунке 4.

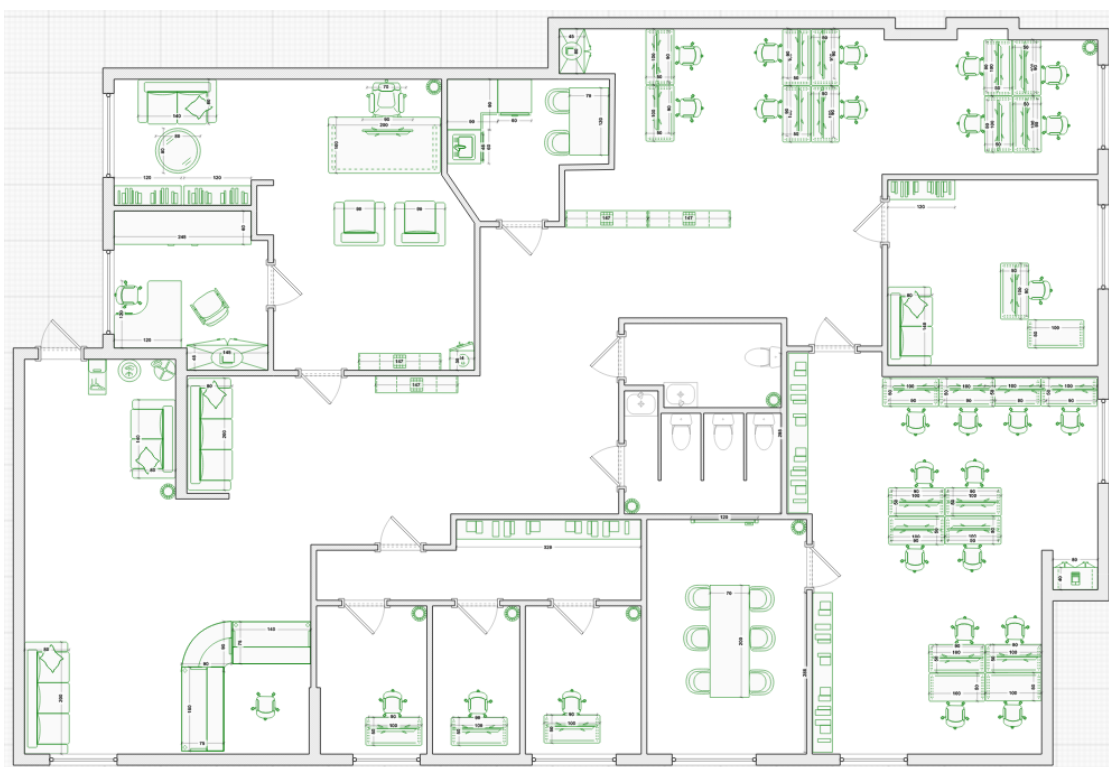


Рисунок 4 – План помещения с размерами

1.4.2 Описание помещений

Офис директора: сейф, стол (2 шт.), кресло (3 шт.), компьютер, диван, шкаф (2 шт.), стеллаж, корзина.

Кабинет секретаря: стол, кресло (2 шт.), шкаф (2 шт.).

Кухня: стол, стул (2 шт.), шкаф (3 шт.), раковина.

Офис 1: стол (10 шт.), кресло (10 шт.), компьютер (10 шт.), корзина, шкаф, стеллаж (2 шт.).

Кабинет заместителя директора: стол (2 шт.), кресло, компьютер, диван, шкаф.

Офис 2: стол (12 шт.), кресло (12 шт.), компьютер (12 шт.), шкаф (3 шт.).

Переговорная: стул (6 шт.), маркерная доска, стол, корзина.

Коридор 1: шкаф.

Офис 3: стол, стул, компьютер, корзина.

Офис 4: стол, стул, компьютер, корзина.

Офис 5: стол, стул, компьютер, корзина.

Туалет: раковина (2 шт.), унитаз (4 шт.), корзина (2 шт.).

Коридор 2: диван, стеллаж.

Стойка регистрации: ресепшн-стойка (3 шт.), стул, диван (2 шт.), бахиломат, санитайзер на стойке, вешалка, корзина.

Помещения расположены на первом этаже здания, где территория ограничена забором. Имеется 1 вход. На внешней стороне окон стоят металлические решетки, а на внутренней – жалюзи. Стены состоят из железобетона, где минимальная толщина 10 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

Оптимальные средства защиты выбраны с учетом угроз, особенностей помещения и стандартов безопасности.

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	Вибрационное зашумление
Оптический	Окна, двери	Применение штор и жалюзи, установка доводчиков для дверей.	Использование инфракрасных детекторов, систем блокировки оптических каналов
Электромагнитный и электрический	ПК, розетки, техника	Установка фильтров для сетей, экранирование электромагнитных волн, защита от электрических полей	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

Проанализируем рынок технических средств.

1.5.1 Акустический и виброакустический каналы

Введение пассивных мер безопасности включает в себя установку усиленных дверей в кабинете директора, переговорной и кабинете заместителя директора. 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	СОНАТА АВ-4Б	ЛГШ-402
Сертификация и соответствие требованиям	Соответствует требованиям по 1-му классу защиты	Соответствует требованиям по 3-му классу защиты	Соответствует требованиям по 1-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	Габаритные размеры не более 35 x 30 мм	Габаритные размеры не более 40 x 25 мм	Габаритные размеры не более 19 x 47 мм	Габаритные размеры не более 40 x 25 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 53 x 38 мм	Габаритные размеры не более 66 x 66 x 25 мм
Напряжение питания	220 В +-15%	176 / 230 В	220 В	187 / 242 В
Диапазон рабочих частот	190 / 11 700 Гц	170 / 12 900 Гц	175 / 11200 Гц	175 / 11 200 Гц

Потребляемая мощность	Не более 130 ВА	Не более 2,5 В	Не более 10 В	Не более 20 ВА
Интервал уровня регулировки звукового давления	Не менее 30 дБ	не менее 40 дБ	Не менее 35 дБ	Не менее 35 дБ

В свете потенциальных угроз, таких как использование закладных устройств и электромагнитных каналов для утечки информации, приняты комплексные меры по обеспечению безопасности. К ним относятся не только пассивные защитные меры, такие как усиленные двери в кабинетах, но и активные меры, включая внедрение системы виброакустических помех ЛГШ-403. Выбор этой системы произведен после тщательного анализа, учитывающего требования по грифу секретности и оптимальные технические характеристики.

Система виброакустических помех ЛГШ-403 представляет собой комплексное решение, направленное на обеспечение безопасности информации и являющееся важной составляющей общей стратегии по защите конфиденциальных данных. Она включает в себя следующие компоненты:

- 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 целях обеспечения защиты помещения от возможных угроз через оптические каналы были приняты следующие меры безопасности. Внутри помещения установлены специальные шторы и жалюзи, предназначенные для блокировки визуального доступа и предотвращения попыток наблюдения извне. Эти элементы, выступающие в качестве пассивных средств защиты, играют ключевую роль в формировании барьера для предотвращения оптических методов утечки информации.

Дополнительно к этим мерам вводятся доводчики для дверей с целью обеспечения тщательного и надежного закрытия. Эти доводчики, действуя как активные средства защиты, предотвращают возможные попытки проникновения через двери, поддерживая высокий уровень безопасности помещения.

Эти шаги, направленные на физическую защиту через использование штор и доводчиков, подчеркивают системный и комплексный подход к обеспечению безопасности в соответствии с установленными стандартами и требованиями по защите информации.

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

С целью обеспечения пассивной защиты было принято решение установить фильтры для сетей электропитания во всех помещениях. Эти фильтры представляют собой эффективные средства контроля и фильтрации электромагнитных помех, направленных на сеть электропитания.

Эксплуатация 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

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.

После проведенного анализа было принято решение в пользу выбора средства защиты ЛГШ-513. Это решение обусловлено рядом преимуществ, которые предоставляет

данное средство. ЛГШ-513 охватывает широкий спектр защиты, включая электрические и электромагнитные каналы, а также обеспечивает защиту от воздействия ПЭМИН.

Кроме того, ЛГШ-513 выделяется привлекательными аспектами, такими как приемлемая цена, что делает его более доступным средством защиты.

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

1.6 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 м²;
- полы и потолки: один вибропреобразователь ЛВП-2с на каждые 6 м²;
- окна: один вибропреобразователь ЛВП-2о на каждое стекло.

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	8	312 000
Усиленная дверь Lars Grau	46 940	3	140 820
Размыкатели ЛУР	5 590	9	50 310
Blackout-жалюзи 2х3м	5 280	10	52 800
ЛВП-2с	3 640	37	134 680
ЛВП-2о	3 640	10	36 400
Итого			843 410

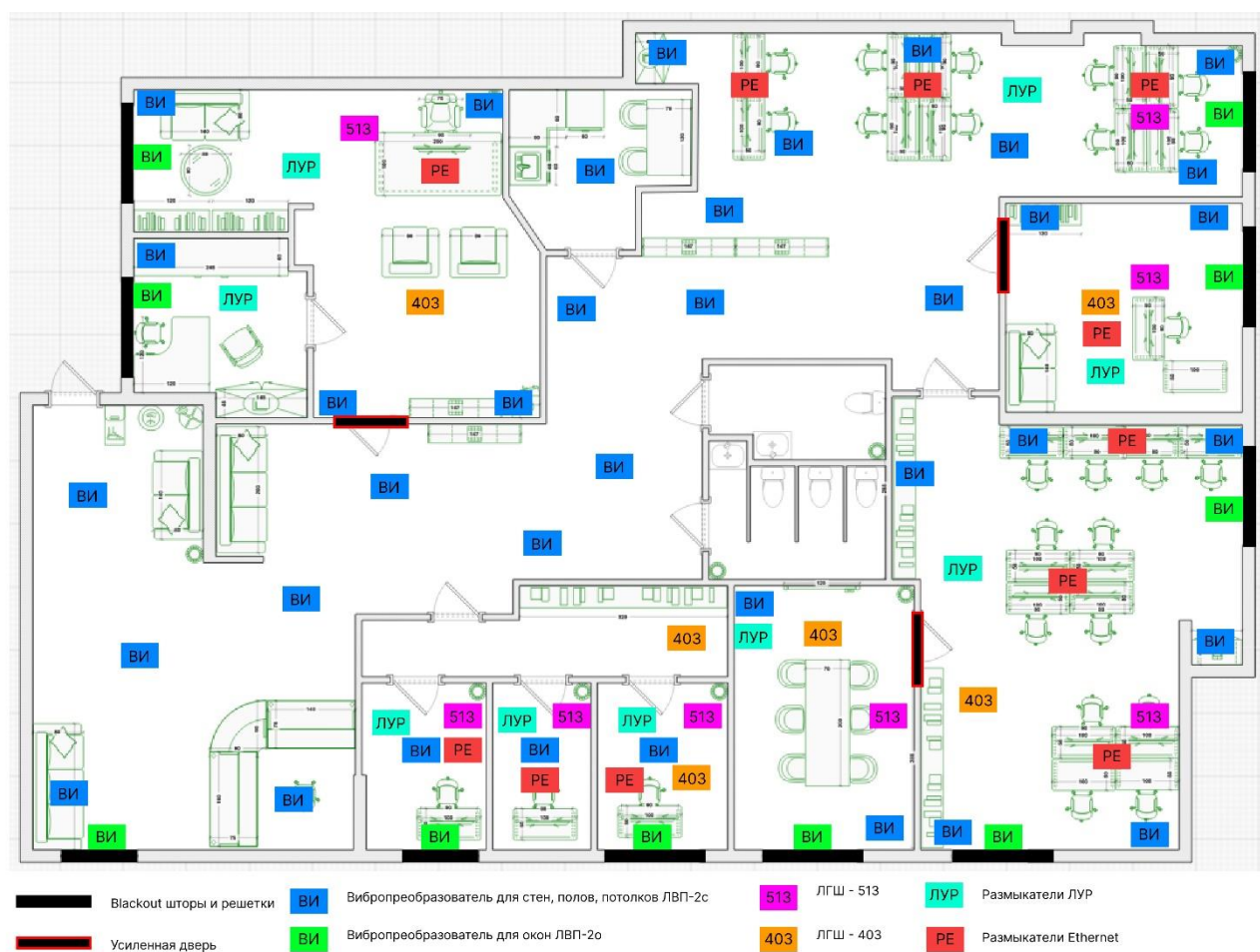


Рисунок 3 – Схема размещения устройств

ЗАКЛЮЧЕНИЕ

В рамках выполнения курсовой работы был проведен комплекс мероприятий для обеспечения безопасности помещения. Начальным этапом стала разработка плана помещения, который послужил основой для последующих шагов. Следующим этапом был анализ теоретического материала по безопасности информации и изучение возможных каналов утечки конфиденциальной информации. На основе полученных данных были определены необходимые меры безопасности, включая пассивные и активные методы. Также были рассмотрены различные средства защиты от утечек. Этот этап позволил выбрать оптимальные средства защиты, учитывая их взаимодействие и совместимость. В результате был разработан детальный план установки выбранных средств, включая пассивные и активные компоненты, с учетом особенностей помещения и требований к безопасности.

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).