

**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**

на тему:

«Проектирование инженерно-технической системы защиты информации  
на предприятии. Вариант 20»

**Выполнил:**

Ступницкий Иван Витальевич,  
студент группы N34462



(подпись)

**Проверил:**

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



(подпись)

Санкт-Петербург  
2024 г.

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

<b>Студент</b>	Ступницкий Иван Витальевич
	(Фамилия И.О.)
<b>Факультет</b>	Безопасность информационных технологий
<b>Группа</b>	N34462
<b>Направление (специальность)</b>	10.03.01 (Технологии защиты информации)
<b>Руководитель</b>	Попов Илья Юрьевич, к.т.н., доцент ФБИТ университета ИТМО
	(Фамилия И.О., должность, ученое звание, степень)
<b>Дисциплина</b>	Инженерно-технические средства защиты информации
<b>Наименование темы</b>	Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 20
<b>Задание</b>	Разработать системы инженерно-технической защиты информации на предприятии

**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, размещенных на коммуникационной площадке дисциплины.
3. Объект исследований курсовой работы ограничивается заданным помещением.

**Содержание пояснительной записки**

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

**Рекомендуемая литература**

Кармановский Н.С., Михайличенко О.В., Савков С.В.

Организационно-правовое и методическое обеспечение информационной безопасности

Учебное пособие / СПб: НИУ ИТМО, 2013-148с.

**Руководитель**

Попов Илья Юрьевич

(Подпись, дата)

**Студент**

Ступницкий Иван Витальевич



22.02.2024

(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

**Студент**                      Ступницкий Иван Витальевич

(Фамилия И.О.)

**Факультет**                      Безопасность информационных технологий

**Группа**                      N34462

**Направление (специальность)** 10.03.01 (Технологии защиты информации)

**Руководитель**    Попов Илья Юрьевич, к.т.н., доцент ФБИТ университета ИТМО

(Фамилия И.О., должность, ученое звание, степень)

**Дисциплина**                      Инженерно-технические средства защиты информации

**Наименование темы**    Проектирование инженерно-технической системы защиты

информации на предприятии. Вариант 20

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируе мая	Фактическая	
1	Разработка и согласование ТЗ	26.10.2023	26.10.2023	
2	Анализ источников информации	28.10.2023	28.10.2023	
3	Работа над курсовой работой	10.11.2023	10.02.2024	
4	Оформление отчета по курсовой работе	15.11.2023	18.02.2024	
5	Защита курсовой работы	21.12.2023	22.02.2024	

**Руководитель**                      Попов Илья Юрьевич

(Подпись, дата)

**Студент**                      Ступницкий Иван Витальевич



22.02.2024

(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

<b>Студент</b>	Ступницкий Иван Витальевич
	(Фамилия И.О.)
<b>Факультет</b>	Безопасность информационных технологий
<b>Группа</b>	N34462
<b>Направление (специальность)</b>	10.03.01 (Технологии защиты информации)
<b>Руководитель</b>	Попов Илья Юрьевич, к.т.н., доцент ФБИТ университета ИТМО
	(Фамилия И.О., должность, ученое звание, степень)
<b>Дисциплина</b>	Инженерно-технические средства защиты информации
<b>Наименование темы</b>	Проектирование инженерно-технической системы защиты информации на предприятии

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

**1. Цель и задачи работы**

- Предложены студентом
- Сформулированы при участии студента
- Определены руководителем

**Цель:** разработать инженерно-техническую систему защиты информации на предприятии, обеспечивающую надежную защиту данных и минимизацию рисков утечки, повреждения или несанкционированного доступа к информации.

**Задачи:** анализ защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.

**Характер работы**

- Расчет
- Конструирование
- Моделирование
- Другое

## Содержание работы

1. Введение.

2. Организационная структура предприятия.

3. Обоснование защиты информации.

4. Анализ защищаемых помещений.

5. Анализ рынка технических средств.

6. Описание расстановки технических средств.

7. Заключение.

8. Список литературы.

## Выводы

В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель

Попов Илья Юрьевич

(Подпись, дата)

Студент

Ступницкий Иван Витальевич



22.02.2024

(Подпись, дата)

## СОДЕРЖАНИЕ

Введение.....	3
1      Организационная структура предприятия.....	4
1.1   Структура предприятия.....	4
1.2   Структура информационных потоков предприятия .....	5
2      Обоснование защиты информации .....	7
2.1   Руководящие документы.....	7
2.2   Обоснование уровня защищенности.....	9
2.3   Требования к СЗИ.....	9
3      Анализ защищаемого помещения.....	11
3.1   Схема помещения.....	11
3.2   Описание помещения .....	14
3.3   Анализ возможных каналов утечки информации .....	16
4      Анализ рынка технических средств.....	19
4.1   Защита от утечки информации по акустическим и виброакустическим каналам	19
4.2   Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам.....	23
4.3   Защита от утечек посредством ПЭМИН .....	24
4.4   Защита от утечек информации по оптическим каналам .....	27
5      Описание расстановки технических средств.....	28
Заключение.....	32
Список использованных источников .....	33

## ВВЕДЕНИЕ

Средства защиты информации (СЗИ) — это технологические и организационные меры, принимаемые для обеспечения конфиденциальности, целостности и доступности информации. Они направлены на предотвращение несанкционированного доступа (НСД), утечек данных, а также обеспечение надежности информационных систем. СЗИ делятся на организационные, программно-аппаратные, криптографические, а также инженерно-технические, которые служат для защиты каналов связи, по которым передается информация, от утечек, изменения, блокирования, копирования. В современной обстановке повышен риск атак на предприятия с целью получения НСД, поэтому наличие СЗИ как никогда актуально.

В данной работе основной задачей является разработка комплекса инженерно-технической защиты информации, которая обладает статусом государственной тайны с уровнем «секретно». Защищаемый объект состоит из одиннадцати помещений и представляет собой офис предприятия с переговорной, кабинетом директора, двумя санузлами, пятью кабинетами, одним коридором, серверным помещением и кухней. Данная работа состоит из пяти глав:

- в первой главе произведен анализ технических каналов утечки информации;
- во второй приведён перечень управляющих документов;
- в третьей – анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств;
- четвертая глава представляет собой анализ рынка технических средств защиты информации разных категорий;
- пятая глава посвящена разработке схем расстановки выбранных технических средств в защищаемом помещении.



# 1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

## 1.1 Структура предприятия

В данном разделе курсовой работы будет представлена организационная структура предприятия, в котором обрабатывается государственная тайна третьего уровня. На рисунке 1 представлена иерархия персонала организации, который состоит из 24 человек и включает в себя:

- СТО;
- СЕО;
- отдел исследований – 4 человека;
- отдел разработки – 3 человека;
- отдел испытаний – 2 человека;
- отдел инфраструктуры – 2 человека;
- отдел ИБ – 3 человека;
- отдел по работе с клиентами – 3 человека;
- финансовый отдел – 2 человека;
- юридический отдел – 3 человека.

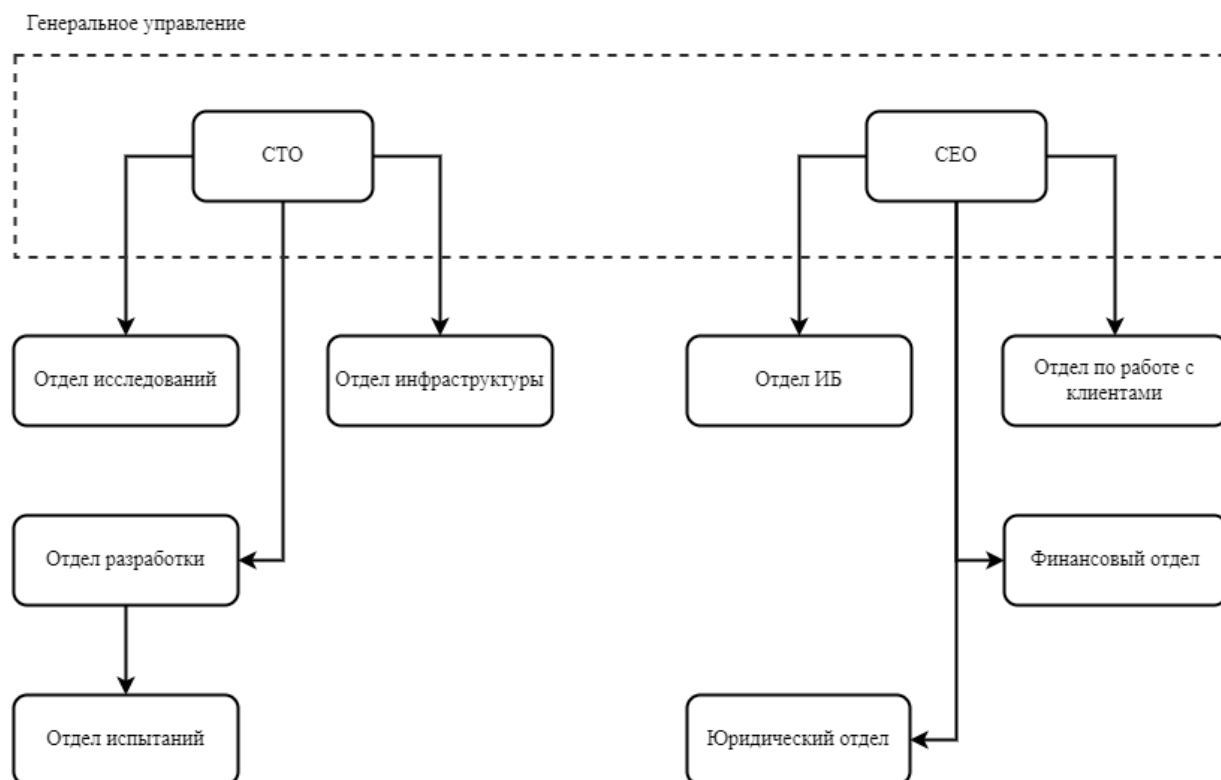


Рисунок 1 – Организационная структура предприятия

Главное руководство состоит из СЕО и СТО, они занимаются принятием ключевых решений и образуют совет генерального управления.

## **1.2 Структура информационных потоков предприятия**

Информационный поток – это совокупность циркулирующих в логистической системе, между логистической системой и внешней средой сообщений, необходимых для управления и контроля логистических операций. Информационный поток может существовать в виде бумажных, электронных носителей, звука, сигналов.

Информационные потоки могут быть классифицированы по-разному, в рамках данной курсовой работы выделены следующие типы информационных потоков: внешние и внутренние (открытые и закрытые).

Внешние потоки представляют из себя информацию, которая передается между компанией и внешними актёрами, например клиентами, а также банками и государственными органами. К открытым потокам относится отчетная информация о налоговых выплатах и финансовых операциях – не требуют специального уровня доступа. К закрытым потокам относятся персональные данные, коммерческая тайна, передача которых должна осуществляться в защищенной среде.

Внутренние потоки представляют из себя информацию, которая не должна быть доступна лицам, не являющимися сотрудниками компании. Данная информация необходима для успешного протекания рабочих процессов. Любая внутренняя информация должна быть защищена от любого внешнего воздействия. К открытым данным относится информация, которая не требует специальных разрешений и доступна всем сотрудникам, например, результаты проведения исследований и разработок, которые не принимали участия в проектах, данные которых составляют гостайну. К закрытой информации относятся финансовые данные, персональные записи, интеллектуальная собственность, а также данные, составляющие гостайну.

На рисунке 2 представлена схема потоков внутри защищаемой организации, на таблице 1 представлены обозначения типов связей информационных потоков. Так, например, данные о разрабатываемом ПО доступны только персоналу отдела испытаний, так как именно он будет проводить тестирование разработанного ПО.

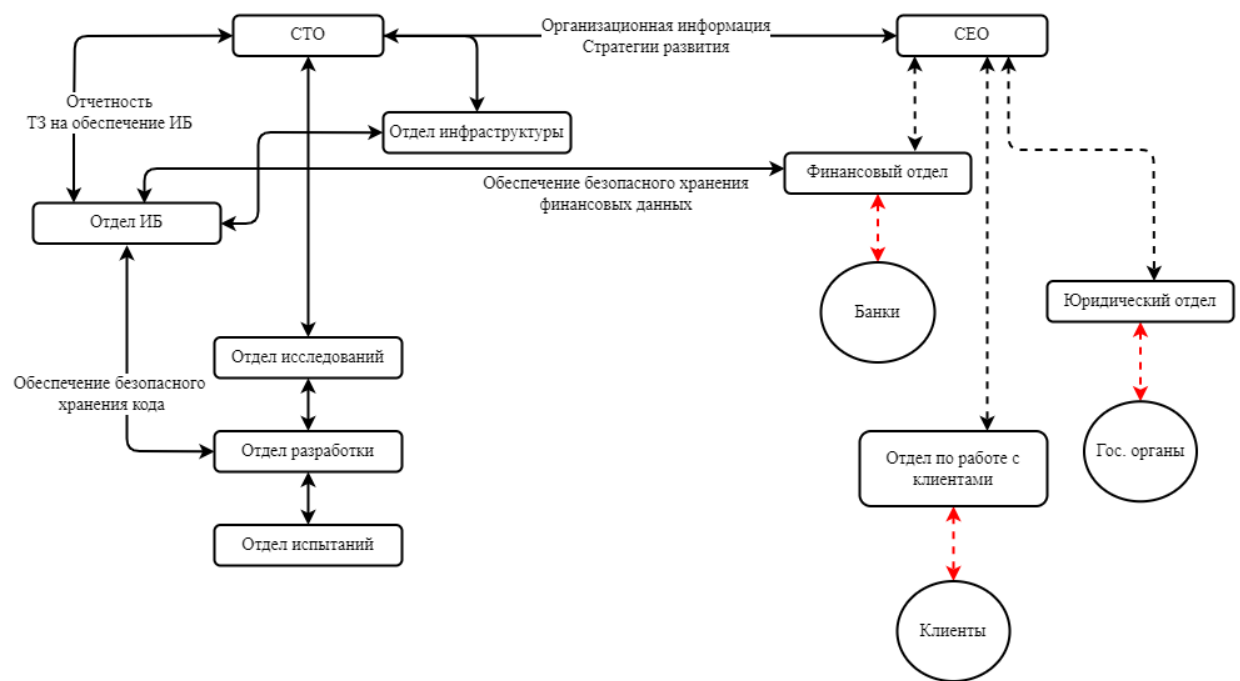


Рисунок 2 – Информационные потоки в предприятии

Таблица 1 – Обозначения типов связей на рисунке 2

	Информационные потоки закрытых внутренних данных
	Информационные потоки открытых внутренних данных
	Информационные потоки внешних данных

## **2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ**

### **2.1 Руководящие документы**

При разработке комплекса защиты информации необходимо руководствоваться следующими нормативными актами, регламентами и руководящими документами:

#### **1. Указы Президента РФ:**

- «Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. №212;
- «Вопросы защиты государственной тайны» от 30.03.1994 г. №614;
- «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203;
- «О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. №1108;
- «Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. №71 с изменениями, внесенными Указами Президента Российской Федерации от 21 апреля 1996 г. №573, от 14 июня 1997 г. №594;
- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644;
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188;
- Указ Президента РФ от 06.10.2004 N 1286 (ред. от 02.04.2012) "Вопросы Межведомственной комиссии по защите государственной тайны".

#### **2. Постановления Правительства Российской Федерации:**

- Постановление Правительства РФ от 15.04.1995 N 333 (ред. от 05.05.2012) "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны";
- Постановление Правительства РФ от 26 июня 1995 г, №608 «О сертификации средств защиты информации»;

- Постановление Правительства РФ от 04.09.1995 N 870 (ред. от 22.05.2008) "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности";
- Постановление Правительства РФ от 06.02.2010 N 63 (ред. от 01.11.2012) "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне";
- Постановление Правительства РФ от 22.11.2012 N 1205 "Об утверждении Правил организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны".

### 3. Федеральные законы:

- «О государственной тайне» от 21.07.1993 №5151–1;
- "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г. N 149-ФЗ;
- «О безопасности» от 5 марта 1992 г. №2446–1.

### 4. Документы ФСТЭК:

- СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам;
- СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации;
- Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров;
- 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.

### 5. Государственные стандарты:

- ГОСТ Р ИСО/МЭК 27001-2021 «Системы менеджмента информационной безопасности. Требования»;
- ГОСТ Р ИСО/МЭК 27002-2021 «Свод норм и правил менеджмента информационной безопасности»;

- ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Методы менеджмента безопасности информационных технологий».

## **2.2 Обоснование уровня защищенности**

**Наименование организации:** «Взор»

**Область деятельности:** разработка ПО и настройка оптических систем.

Организация специализируется на разработке ПО и программных модулей, позволяющих повысить эффективность оптических систем, используемых на летательных аппаратах, в том числе состоящих на вооружении войск Российской Федерации. В числе обрабатываемых данных присутствуют сведения относящиеся к сведениям в военной области, «о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники». Уровень секретности данных сведений определен как «секретно».

## **2.3 Требования к СЗИ**

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «секретно». Согласно требованиям «Типовых норм и правил проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденных Решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199, защита рассматриваемых помещений должна удовлетворять следующим критериям:

1. В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри — звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 см. Дверь устанавливается на металлический каркас;
2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании;

3. По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене;
4. Все режимные помещения оборудуются аварийным освещением;
5. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений;
6. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

### 3 АНАЛИЗ ЗАЩИЩАЕМОГО ПОМЕЩЕНИЯ

#### 3.1 Схема помещения

Для корректного размещения технических средств защиты информации на объекте необходимо провести анализ защищаемого помещения. На рисунке 3 представлен план помещения офисного типа. В таблице 2 представлено описание используемых обозначений.

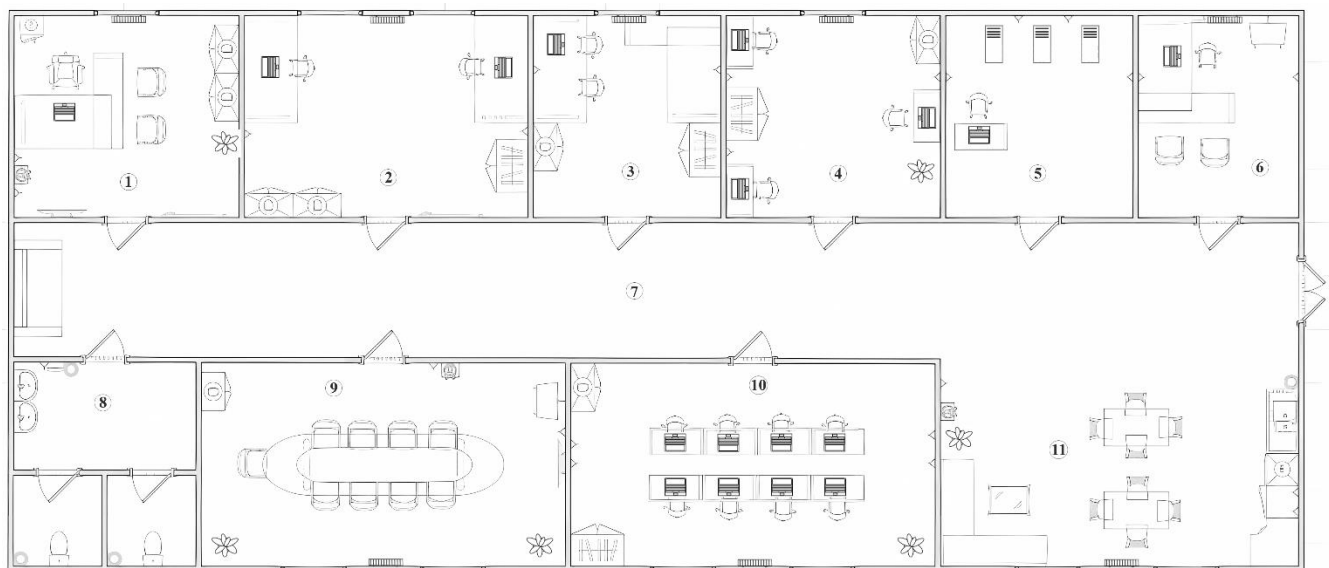




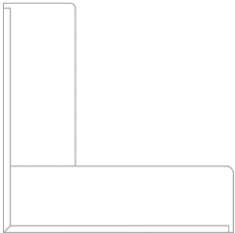

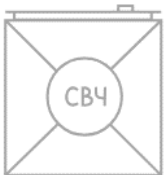

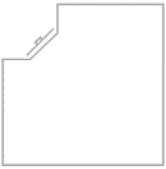











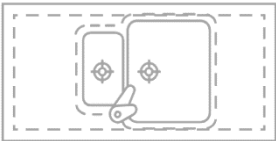
Рисунок 3 – План защищаемого помещения

Таблица 2 – Расшифровка обозначений

Обозначение	Описание
	АРМ
	Батарея отопления
	Диван
	Диспенсер полотенце



Обозначение	Описание
	Журнальный стол
	Кресло офисное
	Кресло руководителя
	Кулер
	Кухонный диван
	Магнитно-маркерная доска
	Микроволновая печь
	Напольный шкаф с дверцей
	Напольный шкаф угловой
	Рабочий стол

Обозначение	Описание
	Раковина-тюльпан
	Розетка
	Сейф
	Серверная стойка
	Стол для переговоров
	Стол кухонный
	Стол (большой)
	Стол угловой
	Столешница с двойной мойкой

Обозначение	Описание
	Стул кухонный
	Стул для переговорной
	ТВ панель
	Унитаз напольный
	Урна для мусора
	Флипчарт
	Цветок напольный
	Шкаф гардеробный
	Шкаф офисный

### 3.2 Описание помещения

На рассматриваемом предприятии в рамках курсовой работы имеются следующие помещения, подлежащие инженерно-технической защите:

- кабинет директора (15,87 м<sup>2</sup>);
- кабинет отдела исследований (20 м<sup>2</sup>);
- кабинет отдела испытаний (13,23 м<sup>2</sup>);
- кабинет отдела разработки (15,11 м<sup>2</sup>);
- серверное помещение (13,21 м<sup>2</sup>);
- кабинет для работы с клиентами (11,32 м<sup>2</sup>);
- коридор (60,51 м<sup>2</sup>);
- туалетная комната (12,45 м<sup>2</sup>);
- переговорная комната (25,87 м<sup>2</sup>);
- офис (25,79 м<sup>2</sup>);
- кухня (25,33 м<sup>2</sup>).

Кабинет директора включает в себя: один сейф, одно кресло руководителя, два стула для переговорной, один стол угловой, один АРМ, один кулер, одну батарею отопления, один цветок напольный, два офисных шкафа, одну ТВ панель, две розетки, одну магнитно-маркерную доску, одну дверь и одно окно.

Кабинет отдела исследований включает в себя: два стола (больших), два АРМ, два офисных кресла, одну батарею отопления, одну магнитно-маркерную доску, два офисных шкафа, один шкаф гардеробный, две розетки, одну дверь и два окна.

Кабинет отдела испытаний включает в себя: две розетки, два АРМ, два кресла офисных, один стол (большой), один стол угловой, один офисный шкаф, один шкаф гардеробный, одну батарею, одну дверь и одно окно.

Кабинет отдела разработки включает в себя: три рабочих стола, три АРМ, три кресла офисных, один шкаф офисный, один шкаф гардеробный, один цветок напольный, три розетки, одну батарею отопления, одну дверь и одно окно.

Серверное помещение включает в себя: три серверные стойки, один рабочий стол, одно АРМ, одно кресло офисное, четыре розетки и одну дверь.

Кабинет для работы с клиентами включает в себя: один стол угловой, одно АРМ, одно кресло офисное, один флипчарт, два стула для переговорной, две розетки, одну батарею отопления и одну дверь.

Коридор соединяет все кабинеты между собой и включает в себя один диван.

Туалетная состоит из двух кабинок с унитазами и урнами для мусора. Перед кабинками расположено место с двумя раковинами, одной розеткой, одной урной для мусора и одним диспенсером полотенец.

Переговорная комната включает в себя: один стол для переговоров, девять стульев для переговорной, один шкаф офисный, два напольных цветка, один кулер, один флипчарт, одну ТВ-панель, две розетки, одну батарею отопления, одну дверь и два окна.

Офис включает в себя: один шкаф офисный, один шкаф гардеробный, один цветок напольный, четыре розетки, восемь рабочих столов, восемь офисных кресел, восемь АРМ, одну батарею отопления, одну дверь и два окна.

Кухня включает в себя: три розетки, один напольный цветок, один кухонный диван, один кулер, один журнальный стол, два кухонных стола, восемь кухонных стульев, одну урну для мусора, одну столешницу с двойной мойкой, один напольный шкаф угловой, один напольный шкаф с дверцей, одну микроволновую печь, одну батарею отопления и два окна.

Офисы отделов компании расположены внутри одного бизнес-центра. Здание бизнес-центра располагается на охраняемой территории отдельно от остальных. Окна не имеют рядом с собой пристроек, выступов, балконов и других элементов, при помощи которых посторонние лица могли бы проникнуть в помещение. Над и под защищаемым помещением расположены арендуемые офисы. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

Доступ к помещениям здания ограничен системой контроля и управления доступом. Допуск в общие помещения имеют все арендаторы и обслуживающий персонал, доступ к офису имеют только сотрудники организации-арендатора.

### **3.3 Анализ возможных каналов утечки информации**

Для определения состава средств защиты информации, которые необходимо установить, сначала следует выделить возможные каналы утечки информации, которые делятся на следующие типы:

- акустические (акустоэлектрические) – утечка по такому каналу возможна, например, из-за закладных устройств, которые могут быть спрятаны в системах хранения, цветах или вентиляционных шахтах;
- вибрационные (виброакустические) – утечка через стекла, тонкие стены, батареи, любой твердый предмет, совершающий вибрации;
- электромагнитные (электрические) – утечки, связанные с электронными устройствами: АРМ, бытовая техника, розетки и проводка;
- визуально-оптические – утечка через открытые окна, прозрачные перегородки и незакрытые двери;

- материально-вещественные – хищение имущества, в рамках данной курсовой работы не рассматривается. Считается, что контроль взаимодействия с физическими носителями информации строго регулируется политикой компании.

В таблице 3 представлены возможные каналы утечки информации для данного помещения, вероятные источники данных утечек, а также необходимые СЗИ, в соответствии с типом конфиденциальной информации – государственная тайна типа «секретно».

Таблица 3 – Каналы утечки и соответствующие СЗИ

Канал утечки	Источники	Пассивная защита	Активная защита
Акустический (акустоэлектрический)	Окна, двери, электрические сети, проводка, вентиляция	Звукоизоляция помещений, акустические экраны, фильтры для цепей электропитания	Акустические извещатели
Вибрационный (виброакустический)	Радиаторы отопления, любые твердые поверхности в помещениях	Изоляция поверхностей за счет дополнительной обшивки, наличие тамбурного помещения	Вибрационные извещатели
Электромагнитный (электрический)	Розетки, бытовая техника, офисная техника	Фильтры для сетей электропитания, защитные экраны	Устройства электромагнитного зашумления
Визуально- оптический	Окна, двери	Средства преграждения отраженного света, доводчики на дверях	Маскирующие средства сокрытия объектов

Средства защиты информации подразделяются на две категории: активные и пассивные. К числу пассивных средств технической защиты относятся разнообразные экранирующие устройства, маски различного предназначения, разделительные устройства в электроснабжающих сетях, защитные фильтры и прочие средства. Основное назначение пассивного подхода заключается в минимизации уровня сигнала, исходящего от источника информации. Применение материалов, поглощающих звук, при отделке стен или экранирование технических устройств, способствует достижению данной цели.

В отличие от пассивных средств, активные технические средства защиты предоставляют устройства, способные генерировать активные помехи (или их имитации) для противодействия техническому шпионажу. В результате такие устройства могут нарушать нормальное функционирование систем скрытного сбора информации. Активные методы предотвращения утечки информации включают в себя обнаружение и нейтрализацию данных устройств.

## 4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

### 4.1 Защита от утечки информации по акустическим и виброакустическим каналам

Принцип функционирования канала основан на способности звуковой волны индуцировать механические колебания в преградах, включая атмосферный воздух, через которые она проходит во время распространения. Эти колебания затем преобразуются в связанный текст с использованием соответствующего оборудования. Для уменьшения вероятности утечки информации по такому каналу необходимо минимизировать акустический сигнал от источника звука, подаваемого на коммуникационные сети, которые служат средой его передачи и могут быть подвержены перехвату. Пассивная защита акустического и виброакустического каналов утечки информации включает в себя:

- усиленные двери;
- тамбурное помещение перед переговорной;
- дополнительную отделку переговорной звукоизолирующими материалами.

Система активной защиты включает в себя методы виброакустического подавления, которые создают в среде распространения сильный помеховый сигнал, не поддающегося фильтрации злоумышленником с использованием имеющегося технического оборудования. Для обеспечения безопасности помещений, где проводится работа со сведениями государственной важности уровня «секретно», рассматривается применение технических средств активной защиты информации для объектов информатизации категории не ниже 1В. В таблице 4 приведен сравнительный анализ подходящих средств активной защиты помещений по виброакустическому каналу.

Таблица 4 – Перечень возможных средств виброакустической защиты

Модель	Цена, руб	Характеристики	Состав
ЛГШ-404	35 100	Диапазон воспроизводимого шумового сигнала: 175–11200 Гц. До 20 излучателей на канал Сертифицирован ФСТЭК России по 2 классу защиты Органы регулировки выходного шумового сигнала защищены от	Вибровозбудитель - «ЛВП10» Акустический излучатель - «ЛВП-2а» Виброэкран - «ЛИСТ-1»



Модель	Цена, руб	Характеристики	Состав
		<p>несанкционированного изменения и обнаружение</p> <p>несанкционированного доступа к ним</p> <p>Возможность регулировки уровня шумового сигнала и частотной коррекции сигнала для каждого выхода в отдельности, а также возможность дистанционного включения и выключения при помощи проводного пульта ДУ</p>	
Соната АВ-4Б	44 200	<p>Диапазон воспроизводимого шумового сигнала: 175–11200 Гц.</p> <p>Максимальное количество излучателей: 239 шт.</p> <p>Мониторинг с помощью СПО «Инспектор»</p> <p>Сертификат ФСТЭК</p> <p>8 шагов регулировки уровней шума в каждой октавной полосе</p> <p>10 шагов регулировки интегральных уровней шума</p>	<p>БПУ - «Соната-ИП4.3»</p> <p>Генераторы</p> <p>акустоизлучатели - «СА-4Б», «СА-4Б1» Генератор вибровозбудитель - «СВ-4Б»</p> <p>Размыкатель телефонной линии - «Соната-ВК4.1»</p> <p>Размыкатель слаботочной линии - «Соната-ВК4.2»</p> <p>Размыкатель линии Ethernet - «Соната-ВК4.3»</p> <p>Пульт управления - «Соната-ДУ4.3»</p> <p>Блоки сопряжения с внешними устройствами - «Соната-СК4.1», «Соната-СК4.2»</p>

Модель	Цена, руб	Характеристики	Состав
			Техническое средство защиты речевой информации от утечки по оптико-электронному (лазерному) каналу - «Соната-АВ4Л»: Генераторный блок АВ4Л» + вибровозбудитель «СП-4Л»
Камертон-5	46 000	Диапазон воспроизводимого шумового сигнала: 90–11200 Гц. 1 класс защиты Сертификация ФСТЭК Максимальное количество подключаемых модулей: ВД-80/ВД-120 = 4шт.; АС-Ш/АСП = 4шт. Интерфейс управления: пленочная клавиатура + ЖК экран	Виброизлучатель (ВД-80 и ВД-120): 2 шт. Акустоизлучатель (АС-Ш и АСП): 2 шт. Размыкатель локальной сети Р-8И: 2 шт. Распределительная коробка РК-1: 1 шт. Остальные компоненты докупаются отдельно
«ШОРОХ 5Л»	21 500	Диапазон рабочих частот: 20–20000 Гц Количество подключаемых излучателей на канал до 35 шт. Интерфейс управления: RS-485; настройка излучателей в интерфейсе ПО; пульт ДУ. Сертификация ФСТЭК	Блок питания и управления «БПУ-1» Вибровозбудитель «ПЭД-8А» Акустические излучатели «АИ-8А», «АИ-8А/Мини», «АИ-8А/П», «АИ-8А/У» Пульт ДУ Управляемый размыкатель линии

Модель	Цена, руб	Характеристики	Состав
SEL SP-157 ШАГРЕНЬ	47 400	<p>Диапазон воспроизводимого шумового сигнала: 90–11200 Гц</p> <p>Максимальное количество излучателей: 64 шт.</p> <p>Индикация: диодная + звуковая + ЖК дисплей</p> <p>Сертификат ФСТЭК</p> <p>2 конструктивно-независимых выхода, по 4 канала на каждом</p> <p>Средство виброакустической защиты 1 класса</p> <p>комбинированного типа</p> <p>ЖК двухстрочный экран</p> <p>Непрерывный контроль состояния системы и каждого отдельного излучателя</p> <p>Возможность регулировки уровня шума каждого излучателя.</p> <p>Возможность дистанционного управления (проводного и по ИК-каналу)</p>	<p>Вибропреобразователь SEL SP-157VP</p> <p>Вибропреобразователь SEL SP-157VPS</p> <p>Акустоизлучатель SEL SP-157AS</p> <p>Регулятор выносной SEL SP-157P</p> <p>Все устройства от 1 шт. – дополнительные устройства приобретаются отдельно</p>

В результате сравнения, для обеспечения защиты от виброакустической разведки была выбрана система «Соната АВ-4Б». Этот выбор обосновывается оптимальным сочетанием цены и характеристик, предоставляемых системой. Она обеспечивает возможность построения автоматической контрольной системы всех компонентов с минимальными затратами на оборудование и монтаж, а также позволяет изменять настройки генераторов-излучателей без простоя, что приводит к созданию адаптивной системы виброакустической защиты. Эта система способна обеспечить соответствие требованиям по безопасности при различных сценариях использования помещения.

#### 4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам

Для обеспечения пассивной защиты сети 220 В применяются сетевые помехоподавляющие фильтры. Такие фильтры блокируют информативные сигналы, возникающие при работе устройств. Необходимо учесть, что для эффективной работы помехоподавляющих фильтров необходимо качественное заземление.

Для обеспечения активной защиты сети 220 В применяются методы, формирующие шумовой сигнал посредством использования специальных генераторов, который превосходит по уровню сигналы устройств съёма информации или информативные сигналы. В таблице 5 представлены средства активной защиты от утечек по электрическому сигналу.

Таблица 5 – Средства защиты информации от утечек по электрическому каналу

Модель	Цена, руб	Особенности
Сетевой генератор шума «ЛГШ-221»	36 400	Сертификат ФСТЭК 2 класса защиты Визуальная система индикации режимов Конструкция обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружения Спектральная плотность напряжения шумового сигнала в диапазоне частот 10–500 кГц: от 10 до 50 дБ Спектральная плотность напряжения шумового сигнала в диапазоне частот 0,5–30 МГц: от 10 до 58 дБ Спектральная плотность напряжения шумового сигнала в диапазоне частот 30–400 МГц: от 10 до 47 дБ Диапазон регулировки уровня выходного шумового сигнала: от 20 дБ Рабочий диапазон частот: от 0,01 до 400 МГц Время непрерывной работы составляет ~ 12 часов Количество фаз: 1 Напряжение: 187–242 В Потребляемая мощность: ~ 36 Вт

Модель	Цена, руб	Особенности
Генератор шума «Соната-РС3»	32 400	Сертификат ФСТЭК Рабочий диапазон частот: до 2 ГГц, регулировка уровня шума в 3 частотных полосах Количество фаз: 1 Ток нагрузки: сеть ~220 В +10%/-15%, 50 Гц Виды индикации: световая, звуковая (исправность / отказ) Потребляемая мощность: не более 10 Вт Продолжительность непрерывной работы: не менее 8 часов
Генератор шума «SEL SP-44»	26 000	Сертификат ФСТЭК Управление: ручное, ДУ, RS-485 Уровень шума / затухания: 12–90 дБ Напряжение: 220 В ± 10%, 50 Гц Рабочий диапазон частот: от 0,01 до 400 МГц Количество фаз: 1 Диапазон регулировки уровня шума в каждом поддиапазоне: от 20 дБ

В результате анализа, из представленных вариантов был выбран генератор шума «Соната-РС3». Отличительными особенностями являются упрощенная интеграция с элементами компании «Соната», которые были выбраны ранее; малая потребляемая мощность и больший диапазон охватываемых частот по сравнению с конкурентами.

В качестве средства обеспечения пассивной защиты информации был выбран сетевой фильтр «Соната-ФС 10.1», который имеет сертификат ФСТЭК и может применяться в сетях до 10 А. Его стоимость составляет 50 400 руб.

#### **4.3 Защита от утечек посредством ПЭМИН**

ПЭМИН (побочные электромагнитные излучения и наводки) – канал утечки информации через излучение элементов компьютера. Злоумышленник может перехватить и декодировать эти излучения для получения сведений обо всей информации, обрабатываемой в компьютере. Приемные электронные устройства устанавливаются в

компьютер, параллельно подсоединяются к сетям электропитания или заземления, просто размещаются недалеко от работающего оборудования или перехватывают данные при помощи антенны. Чаще всего перехватываются и дешифровываются излучения, вырабатываемые:

- при выводе данных на монитор;
- при вводе информации с клавиатуры;
- при записи данных на жесткий диск или их копировании со съемных носителей.

Для обеспечения активной защиты используются генераторы радиопомех, которые перекрывают шумом побочные излучения защищаемого объекта путем формирования на границе контролируемой зоны широкополосной шумовой электромагнитной помехи. В таблице 6 представлен перечень подобных СЗИ.

Таблица 6 – Средства активной защиты от ПЭМИН

Модель	Цена	Особенности
«ЛГШ-501»	29 900	<p>Соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок»</p> <p>Сертификат ФСТЭК (2 класс защиты)</p> <p>Оснащено визуальной системой индикации режимов работы</p> <p>Конструкция обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружения несанкционированного доступа к ним</p> <p>Спектральная плотность напряжения шумового сигнала в диапазоне частот (мкВ/<math>\sqrt{\text{кГц}}</math>):</p> <ul style="list-style-type: none"> <li>– От 0,01 до 30 МГц: от 10 до 58 дБ</li> <li>– От 30 до 400 МГц: от 10 до 47 дБ</li> </ul> <p>Спектральная плотность напряженности магнитного поля шума в диапазоне частот от 0,01 до 30 МГц: от 20 до 65 дБ</p> <p>Диапазон регулировки уровня: ~ 20 дБ</p> <p>Показатель электромагнитной совместимости: ~ 70 м</p> <p>Наработка до отказа: ~ 12 000 ч</p> <p>Срок службы: ~ 7 лет</p> <p>Ресурс: ~ 27 000 ч</p>

Модель	Цена	Особенности
Генератор шума ПУЛЬСАР	24 525	<p>Энтропийный коэффициент качества шума на выходе генератора не менее 0,97</p> <p>Рабочий диапазон частот до 6 ГГц</p> <p>Конструкция обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружения несанкционированного доступа к ним</p> <p>Сертификат ФСТЭК (2 класс защиты)</p> <p>Диапазон регулировки уровня: ~ 20 дБ</p>
Генератор шума «Покров»	32 800	<p>Сертификат ФСТЭК (2 класс защиты)</p> <p>Вид индикации: светодиоды</p> <p>Управление: Ethernet</p> <p>Диапазон частот: 0,01–6000 МГц</p> <p>Электропитание выполнено в виде сетевого удлинителя с 5 розетками типа F</p> <p>Мощность: 15 Вт</p> <p>Наработка на отказ: 50000 ч</p> <p>Диапазон шумового сигнала:</p> <ul style="list-style-type: none"> <li>– для электрической составляющей: 0,01–3000 МГц</li> <li>– для магнитной составляющей: 0,01–30 МГц</li> <li>– для электрических сигналов, наведённых на цепи электропитания: 0,01–400 МГц</li> </ul>
«Соната-Р3.1»	33 120	<p>Продолжительность непрерывной работы: не менее 8 ч</p> <p>Возможность повышения уровня излучаемого электромагнитного поля шума в диапазоне частот 0,01...200 МГц за счет применения дополнительной антенны ВЕЕР</p> <p>Мощность: 10 Вт</p> <p>Диапазон частот: соответствует требованиям документа "Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок"</p> <p>Сертификат ФСТЭК (2 класс защиты)</p>

В результате анализа к использованию был выбран генератор «ЛГШ-501», который в сравнении с вышеперечисленными приборами имеет сравнимые характеристики и меньшую стоимость.

#### **4.4 Защита от утечек информации по оптическим каналам**

Для предотвращения утечек информации по визуально-оптическому каналу были выбраны следующие решения:

- установка на окна жалюзи, штор или тонирующую пленку;
- установка доводчиков на двери, для предотвращения наблюдения через приоткрытую дверь.



## 5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В предыдущей главе были выбраны следующие средства защиты, которые планируются к установке в защищаемом помещении:

- виброакустическая защита «Соната АВ-4Б»;
- усиленные двери со звукоизолирующей прокладкой на металлическом каркасе:  $R_w$  31dB Prima GL900;
- генератор шума «Соната-РСЗ»;
- сетевой фильтр «Соната-ФС 10.1»;
- активная защита от ПЭМИН «ЛГШ-501»;
- защитные жалюзи;
- дверные доводчики.

Для определение необходимого количества каждого из средств защиты информации будет использована информация с официального веб-сайта производителя НПО «АННА» для предварительной оценки количества вибровозбудителей «Соната СВ-4Б»:

- стены – один на каждые 3–5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- потолок, пол – один на каждые 15–25 м<sup>2</sup> перекрытия;
- окна – один на окно (при установке на оконный переплет);
- двери – один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Необходимое количество генераторов-акустоизлучателей «Соната СА-4Б» можно предварительно оценить из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8–12 м<sup>3</sup> надпотолочного пространства или др. пустот.

Усиленные двери будут установлены на помещения, в которых будет происходить обсуждение конфиденциальной информации. Дверные доводчики будут установлены на всех дверях. На всех окнах будут установлены жалюзи.

Итоговое количество требуемых технических средств для рассматриваемого объекта защиты и их расчетная стоимость представлены в таблице 7.

Таблица 7 – Оценка стоимости технических средств защиты

Средство защиты	Цена, руб	Количество, шт.	Итоговая стоимость, руб
Генератор акустоизлучатель «Соната-СА-4Б»	7 440	16	119 040
Генератор вибровозбудитель «Соната-СВ-4Б»	7 440	62	461 280
Система «Соната АВ-4Б»	44 200	1	44 200
Сетевой фильтр «Соната-ФС 10.1»	50 400	2	100 800
Генератор шума «ЛГШ-501»	29 900	8	239 200
Сетевой генератор шума «Соната-РС3»	32 400	7	226 800
Размыкатель Ethernet «Соната- ВК4.3»	6 000	1	6 000
Размыкатель слаботочной линии «Соната-ВК 4.2»	6 000	2	12 000
Доводчик дверной «ISP 440»	1 640	9	14 760
Дверь «Rw 31dB Prima GL900»	28 950	8	231 600
Рулонные жалюзи	2 700	9	24 300
<b>Итого</b>			1 479 980

На рисунке 4 представлена схема расположения активных и пассивных СЗИ. На таблице 8 приведена расшифровка условных обозначений схемы.

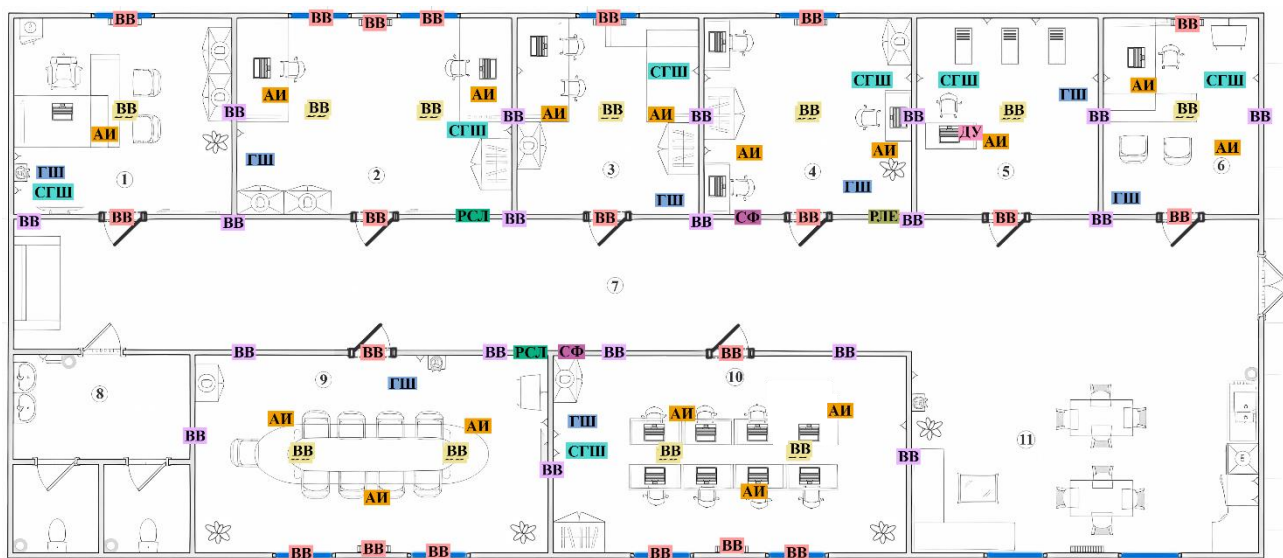




Рисунок 4 – Схема расположения СЗИ

Таблица 8 – Условные обозначения на схеме

Условное обозначение	Средство защиты
<b>АИ</b>	Генератор акустоизлучатель «Соната-СА-4Б»
<b>ВВ</b>	Генератор вибровозбудитель «Соната-СВ-4Б» на окна, двери и радиаторы отопления
<b>ВВ</b>	Генератор вибровозбудитель «Соната-СВ-4Б» на пол и потолок
<b>ВВ</b>	Генератор вибровозбудитель «Соната-СВ-4Б» на стены
<b>ДУ</b>	Пульт управления «СОНАТА-ДУ 4.3»
<b>СФ</b>	Сетевой фильтр «Соната-ФС 10.1»
<b>ГШ</b>	Генератор шума «ЛГШ-501»
<b>СГШ</b>	Сетевой генератор шума «Соната-РС3»
<b>РЛЕ</b>	Размыкатель Ethernet «Соната-БК4.3»
<b>РСЛ</b>	Размыкатель слаботочной линии «Соната-БК 4.2»

	Дверь «Rw 31dB Prima GL900»
	Рулонные жалюзи

## **ЗАКЛЮЧЕНИЕ**

В ходе выполнения курсовой работы был произведен теоретический обзор технических каналов утечки информации, анализ защищаемого предприятия, включая описание структуры предприятия, составление подробного плана помещений, описание информационных каналов.

Для выбора необходимых средств технической защиты информации был проведен анализ рынка существующих решений для противодействия рассматриваемым каналам утечки и выбраны наиболее подходящие для объекта решения. На основе выбранных средств был разработан план установки и произведен расчет финансовых затрат, которые указаны в разделе 5 данной работы.

В результате была предложена защита от утечек информации по акустическому, виброакустическому, оптическому, акустоэлектрическому, электрическому, электромагнитному, оптико-электронному каналам. Затраты на обеспечение защиты составляют

1 479 980 руб., что можно считать достаточно оправданной суммой для объекта, который хранит и обрабатывает информацию, составляющую государственную тайну с грифом уровня «секретно».

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Рагозин, Ю. Н. Инженерно-техническая защита информации: учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург: Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст: электронный // Лань: электроннобиблиотечная система. — URL: <https://e.lanbook.com/book/103203> (дата обращения: 05.12.2023). — Режим доступа: для авториз. Пользователей
2. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Н. С. Кармановский, О. В. Михайличенко, С. В. Савков. — Санкт-Петербург: НИУ ИТМО, 2013. — 148 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/43579> (дата обращения: 20.12.2023). — Режим доступа: для авториз. пользователей.
3. Скрипник, Д. А. Общие вопросы технической защиты информации: учебное пособие / Д. А. Скрипник. — 2-е изд. — Москва: ИНТУИТ, 2016. — 424 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/100275> (дата обращения: 20.12.2023). — Режим доступа: для авториз. пользователей.
4. Каторин, Ю. Ф. Защита информации техническими средствами: учебное пособие / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак. — Санкт-Петербург: НИУ ИТМО, 2012. — 416 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/40850> (дата обращения: 25.12.2023). — Режим доступа: для авториз. пользователей.
5. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам: Учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. — Москва: Горячая линия-Телеком, 2005. — 416 с.