

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

**Факультет безопасности информационных технологий**

**КУРСОВАЯ РАБОТА**

**По дисциплине:**

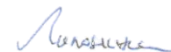
«Инженерно-технические средства защиты информации»

**На тему:**

«Проектирование инженерно-технической системы защиты информации на предприятии.  
Вариант 90»

**Выполнила:**

Липонина Екатерина Алексеевна, студент группы N34501



(подпись)

**Проверил:**

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

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023

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

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

**Студент** Липонина Екатерина Алексеевна

(Фамилия И.О.)

**Факультет** Безопасности информационных технологий

**Группа** N34501

**Направление (специальность)** 10.03.01 Информационная безопасность

**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

**Задание** Спроектировать инженерно-техническую систему защиты информации на выбранном предприятии

**Краткие методические указания**

**Содержание пояснительной записки**

Проводится анализ организационной структуры предприятия, видов обрабатываемой там информации,

составляющей государственную тайну, плана помещения, средств защиты на рынке, а также предлагается план помещения с уже внедрённой активной и пассивной защитой.

Курсовая работа включает разделы:

Введение;

1. Организационная структура предприятия;
2. Обоснование защиты информации;
3. Анализ плана помещения;
4. Анализ рынка;
5. План помещения с активной и пассивной защитой.

Заключение.

**Рекомендуемая литература**

Н.С. Кармановский, О.В. Михайличенко, С.В. Савков «организационно-правовое и методическое обеспечение информационной безопасности»

**Руководитель** Попов Илья Юрьевич

(Подпись, дата)

**Студент** Липонина Екатерина Алексеевна

(Подпись, дата)

19.12.2023

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

**Студент**    Липонина Екатерина Алексеевна

(Фамилия И.О.)

**Факультет**    Безопасности информационных технологий

**Группа**    N34501

**Направление (специальность)**    10.03.01 Информационная безопасность

**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

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Составление плана КР	13.12.2023	13.12.2023	
2	Анализ литературы	14.12.2023	14.12.2023	
3	Составление основного текста КР	15.12.2023	15.12.2023	
4	Представление выполненной КР	20.12.2023	20.12.2023	

**Руководитель**    Попов Илья Юрьевич

(Подпись, дата)

**Студент**    Липонина Екатерина Алексеевна

(Подпись, дата)



19.12.2023

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

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

**Студент**      Липонина Екатерина Алексеевна

(Фамилия И.О.)

**Факультет**      Безопасности информационных технологий

**Группа**      N34501

**Направление (специальность)**      10.03.01 Информационная безопасность

**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

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

**1. Цель и задачи  
работы**

☐ Предложены студентом      ☐ Сформулированы при участии студента

☒ Определены руководителем

Цель данной работы – проектирование инженерно-технической системы защиты информации на  
выбранном предприятии.

**2. Характер  
работы**

☐ Расчет

☐ Конструирование

☐ Моделирование

☒ Другое

Проектирование

### 3. Содержание работы

---

В работе проводится анализ выбранного предприятия и обрабатываемой там информации, выбор подходящих инженерно-технических средств защиты информации и создание плана помещения с уже внедрённой активной и пассивной защитой.

---

### 4. Выводы

В результате выполнения работы был проведён анализ выбранного предприятия и обрабатываемой там информации, рынка инженерно-технических средств защиты информации, а также выполнено проектирование инженерно-технической системы защиты информации.

---

Руководитель    Попов Илья Юрьевич

(Подпись, дата)

Студент    Липонина Екатерина Алексеевна

(Подпись, дата)



19.12.2023

«19» декабрь 2023 г.

## СОДЕРЖАНИЕ

Содержание .....	2
Введение .....	4
1     ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ .....	5
1.1   Область деятельности предприятия .....	5
1.2   Организационная структура предприятия .....	5
1.3   Обрабатываемая информация ограниченного доступа .....	5
1.4   Информационные потоки предприятия .....	6
2     ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ .....	7
2.1   Информация предприятия, составляющая государственную тайну .....	7
2.2   Руководящие документы в области защиты информации, составляющей государственную тайну .....	7
2.3   Требования к степени секретности .....	8
3     АНАЛИЗ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ .....	9
3.1   Описание помещения .....	9
3.2   Каналы утечки информации .....	10
3.2.1   Прямые и косвенные каналы .....	10
3.2.2   Физические каналы .....	10
3.2.3   Технические каналы .....	11
3.3   Методы защиты информации .....	11
3.4   Анализ каналов утечки информации разбираемой организации .....	12
4     АНАЛИЗ РЫНКА .....	13
4.1   Устройства для перекрытия акустического и виброакустического каналов утечки информации .....	13
4.1.1   Пассивная защита .....	13
4.1.2   Активная защита .....	13
4.2   Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации .....	14
4.2.1   Пассивная защита .....	14
4.2.2   Активная защита .....	15
4.3   Устройства для перекрытия утечек с использованием побочного электромагнитного излучения и наводок (ПЭМИН) .....	15
4.4   Устройства для перекрытия оптического канала утечки информации .....	16

4.5	Расстановка инженерно-технических средств защиты информации .....	16
5	ПЛАН ПОМЕЩЕНИЯ С АКТИВНОЙ И ПАССИВНОЙ ЗАЩИТОЙ .....	17
	Заключение.....	19
	Список использованных источников.....	20

## **ВВЕДЕНИЕ**

Цель работы – разработка комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно».

Для достижения поставленной цели необходимо решить следующие задачи:

- провести анализ организационной структуры выбранного предприятия;
- обосновать необходимость в защите информации;
- провести анализ плана помещения выбранного предприятия;
- провести анализ рынка инженерно-технических средств защиты информации;
- создать план помещения с активной и пассивной защитой.



# 1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

## 1.1 Область деятельности предприятия

Предприятие АО «Алмазы Архангельска» занимается добычей алмазов, в том числе разведкой месторождений, добычей, обработкой и продажей алмазного сырья.

## 1.2 Организационная структура предприятия

На рисунке 1.1 представлена организационная структура предприятия.



Рисунок 1.1 – Организационная структура предприятия

## 1.3 Обработка информации ограниченного доступа

В предприятии обрабатываются следующие виды информации:

- коммерческая тайна;
- персональные данные;
- служебная информация;
- государственная тайна.

## 1.4 Информационные потоки предприятия

На рисунке 1.2 представлены информационные потоки предприятия

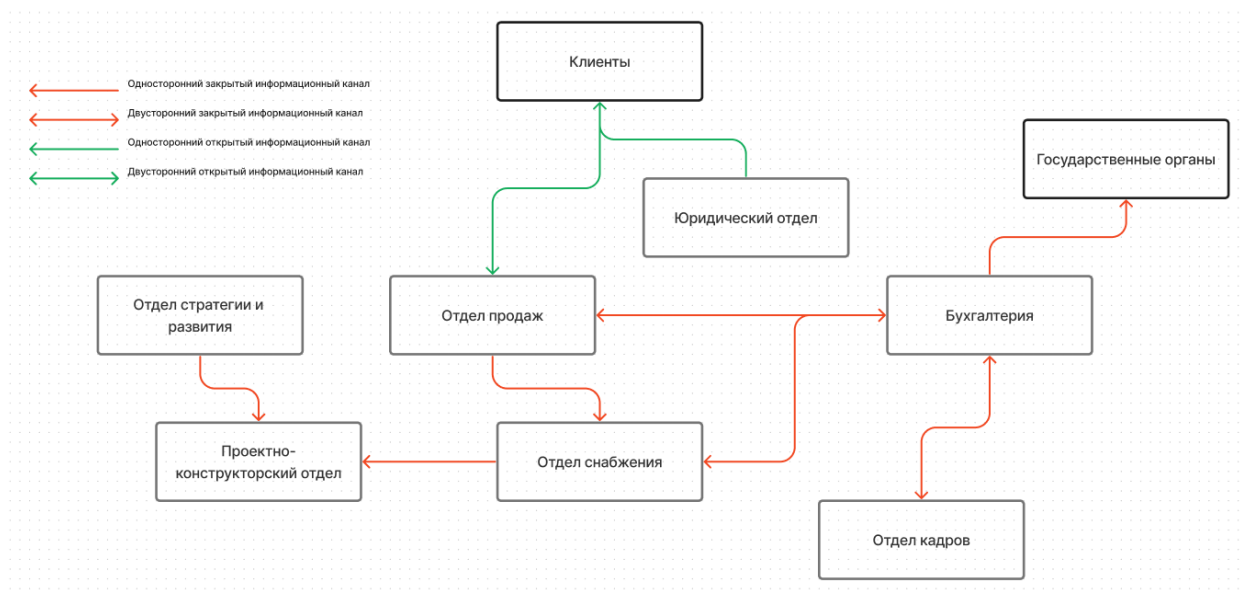


Рисунок 1.2 – Информационные потоки предприятия

## **2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ**

### **2.1 Информация предприятия, составляющая государственную тайну**

Необходимость в использовании инженерно-технических средств защиты информации напрямую зависит от обрабатываемой в предприятии информации. Как уже было описано в пункте 1.3, в предприятии обрабатывается информация, относящаяся к государственной тайне.

Согласно Закону РФ "О государственной тайне" статье 5 «Перечень сведений, составляющих государственную тайну» пункту 2 «сведения в области экономики, науки и техники» государственную тайну составляют в том числе сведения:

- «о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации)»;

Так как предприятие АО «Алмазы Архангельска» занимается добычей алмазов, сведения об объемах запасов в недрах, добычи, производства и потребления алмазов являются необходимыми для работы предприятия, а также составляют государственную тайну.

- «о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства»

Так как добыча и обработка алмазов требует развития науки и техники, имеющих экономическое значение, эта информация также может быть отнесена к категории государственной тайны.

### **2.2 Руководящие документы в области защиты информации, составляющей государственную тайну**

Основными документами в области защиты информации, составляющей государственную тайну, являются

- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;

- Закон РФ «О государственной тайне» от 21.07.1993 N 5485–1;
- МЕЖВЕДОМСТВЕННАЯ КОМИССИЯ ПО ЗАЩИТЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ РЕШЕНИЕ № 199 от 21.01.2011г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".

А также нормативно-технические документы ФСТЭК России:

- Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам.

### 2.3 Требования к степени секретности

К сведениям **особой важности** следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

К **совершенно секретным** сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

К **секретным** сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

Таким образом, сведения, обрабатываемые на предприятии, можно отнести к *секретным* сведениям.

### 3 АНАЛИЗ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

#### 3.1 Описание помещения

На рисунке 3.1 представлен план помещения офиса предприятия.

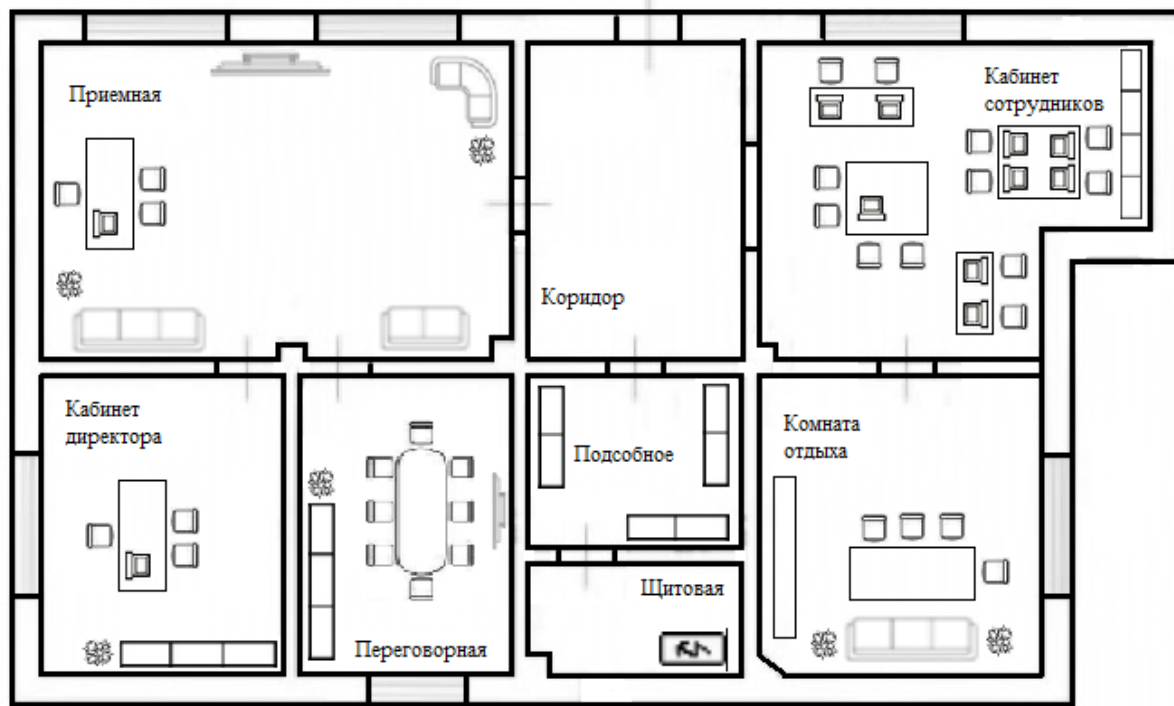


Рисунок 3.1 – План помещения

Помещение включает в себя:

Таблица 3.1 – Предназначение и наполнение комнат

Помещение	Предназначение	Объекты
Кабинет директора	Место работы директора	АРМ, мебель
Приемная	Место ожидания приема у директора или переговоров	Мебель, экран
Переговорная	Место проведения переговоров	Мебель, экран
Коридор	Переход в другие помещения	
Подсобное	Хранение	Шкаф (3 штуки)
Щитовая	Электроснабжение	Электрощиток
Кабинет сотрудников	Место работы сотрудников	Мебель, АРМ (9 штук)
Комната отдыха	Место отдыха сотрудников	Кофемашина, мебель

Особое внимание следует уделить следующим помещениям:

- Кабинет директора: директор работает с информацией, составляющей государственную или коммерческую тайну;
- Переговорная: в помещении могут вестись обсуждения информации, содержащей государственную или коммерческую тайну;
- Щитовая: место, содержащее доступ к электрической сети помещения;
- Кабинет сотрудников: сотрудники могут работать с информацией, составляющей государственную или коммерческую тайну.

### **3.2 Каналы утечки информации**

Ниже будут разобраны существующие каналы утечки информации по различным классификациям, а также их применимость для разбираемой организации.

#### **3.2.1 Прямые и косвенные каналы**

Косвенные каналы не требуют непосредственного доступа к техническим средствам информационной системы. Прямые соответственно требуют доступа к аппаратному обеспечению и данным информационной системы.

Таким образом, косвенные каналы включают, но не ограничиваются следующими сценариями:

- Утечка через внешний носитель информации;
- Утечка через неутраченные документы и иной мусор;
- Считывание электромагнитных и иных излучений.

Прямые каналы включают, но не ограничиваются следующими сценариями:

- Прямое копирование через АРМ организации;
- Утечка в неформальной атмосфере;
- Копирование с внешних носителей информации.

#### **3.2.2 Физические каналы**

Физическими называют каналы утечки информации, возникающие из-за слабой организации физической защиты данных от несанкционированного изучения и копирования, а также от похищения.

Физические каналы утечки включают, но не ограничиваются следующими сценариями:

- Перевозка документов без должной охраны;
- Подслушивание разговоров между сотрудниками;
- Хранение документации без сейфов.

### **3.2.3 Технические каналы**

Технические каналы в свою очередь подразделяются на естественные и искусственные.

Естественный технический канал утечки информации появляется в результате способности физических объектов излучать тепло и свет, производить шумы, испускать радиоактивные лучи. Информация об интересующем объекте может быть получена путем косвенного изучения его физических характеристик и состава.

Искусственный канал утечки создается путем внедрения в линии связи закладных устройств, установки в рабочих помещениях малогабаритных приборов перехвата.

Вне зависимости от происхождения канала утечки используется также разделение, описанное в пунктах ниже.

- Акустический – извлечение информации из звука, исходящего с объекта информационной деятельности, например, прослушка;
- Виброакустический – извлечение информации из вибраций, порождаемых акустикой при влиянии на физические объекты, например, стены;
- Оптический – извлечение визуальной информации, например при фотографировании или ином визуальном наблюдении;
- Электромагнитный – снятие индуктивных наводок с полей информационной системы;
- Электрический – извлечение передаваемой по кабельным линиям связи;
- Материально-вещественные – извлечение информации через физические объекты, вроде флеш-накопителей или документов.

### **3.3 Методы защиты информации**

Методы защиты информации подразделяются на активные и пассивные. *Пассивные* методы снижают сигнал (электромагнитный, или иной), скрывают видимость или иначе ограничивают распространение информации, тогда как *активные* создают маскировочные сигналы, для сокрытия естественных сигналов.

### 3.4 Анализ каналов утечки информации разбираемой организации

Согласно нормативным документам для государственной тайны типа «секретно» требуется оснастить помещение средствами защиты, представленными в таблице 3.2.

Таблица 3.2 – Требования к защите информации

Каналы утечки	Источник	Пассивная защита	Активная защита
Акустический	Окна, двери, электрические сети, любые объекты с плохой звукоизоляцией	Звукоизоляция	Устройства акустического зашумления
Виброакустический	Твердые физические объекты	Рифленая поверхность	Устройства вибрационного зашумления
Оптический	Окна, двери	Шторы, жалюзи, доводчики на дверях	Устройства оптического зашумления
Электромагнитный, электрический	Розетки, электрические сети, АРМ	Фильтры для электросетей	Устройства электромагнитного зашумления

Каналы утечки информации для разбираемой организации представлены в таблице 3.3.

Таблица 3.3 – Каналы утечки для организации

Канал утечки	Реализация внутри организации
Акустический	Кабинеты содержат окна, двери, есть возможность подслушивания.
Виброакустический	Кабинет директора, переговорная и кабинет сотрудников содержат стены, которые можно просмотреть снаружи помещения.
Оптический	Кабинет директора, переговорная и кабинет сотрудников содержат окна, двери кабинета директора и переговорной выходят в приемную, в которую есть доступ посторонним.
Электромагнитный, электрический	В помещения проведено электричество, есть розетки для подключения АРМ.



## 4 АНАЛИЗ РЫНКА

### 4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации

#### 4.1.1 Пассивная защита

Пассивная защита предполагает установку усиленных дверей, а также отделку звукоизолирующими материалами. Сравнение некоторых материалов представлено в таблице 4.1.1.

Минеральные мембраны	Гасит звуковые колебания за счет разницы в плотности, массе и толщине компонентов.
Панели с песком	Хорошо защищают от воздушного шума, но не спасают от механического
Вспененный каучук	Похож на минеральные мембраны, но дороже в цене и сложнее в монтаже
Рубероид	Низко эффективен

Было решено использовать панели с песком, как самое экономически выгодное, но подходящее решение.

#### 4.1.2 Активная защита

Активная защита представляет собой виброакустическое зашумление, достижимое при помощи приборов, представленных в таблице 4.1.2.

	<b>СОНАТА АВ модель 4Б</b>	<b>SI-3030</b>	<b>ШТОРМ-10</b>	<b>Барон-S1</b>
Диапазон частот	90–11200 Гц	175 Гц - 5,6 кГц	90 – 11300 Гц	60–16000 Гц
Количество каналов	3	3	4	2
Количество подключаемых излучателей	5 аудио + 30 вибро	3	Конфигурируется	2
Сертификат	ФСТЭК	ФСТЭК	ФСТЭК	ФСТЭК

Примечания	Индивидуальная регулировка интегрального уровня	Прибор имеет высокий КПД, обладает большой выходной мощностью, благодаря новым техническим решениям	Наличие подсистемы формирования шумового сигнала для защиты акустической речевой информации от утечки за счет акустоэлектрических преобразований в слаботочных линиях связи, включая ЛВС, телефонные линии различных стандартов, слаботочные двухпроводные симметричные линии охранно- пожарных сигнализаций, систем управления доступом, систем оповещения и т.п.	Речеподобные помехи, наличие клонеров для записи и последующей имитации.
------------	--	--	--	--

По соотношению характеристик, была выбрана модель ШТОРМ-10.

## 4.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации

### 4.2.1 Пассивная защита

Пассивная защита реализуется за счет фильтров для сетей электропитания или экранирующих прокладок. Последние разобраны в таблице 4.2.1.

Таблица 4.2.1 – Экранирующие прокладки

	Aaronia X-Dream	"ТЕКО ТЭМП-МП-80"	"ТЕКО ТЭМП-СН"
Диапазон частот	100 МГц – 18 ГГц	100 МГц – 10 ГГц	100 МГц – 10 ГГц

Эффективность экранирования, дБ	До 120	До 70	До 65
Плотность, г/кв. м	130	80	100
Материал	Полиэстер/медь	Полиэстер/медь/никель	Нейлон/серебро
Толщина, мм	0,5	0,08	0,28

Был выбран Aaronia X-Dream за счет превалирующих характеристик.

#### 4.2.2 Активная защита

Активная защита реализуется при помощи применения генераторов белого шума, то есть широкополосного шумового сигнала с уровнем, существенно превышающим прочие полезные сигналы. В таблице 4.2.2 приведено сравнение для генераторов.

Таблица 4.2.2 – Генераторы шума

	ГНОМ-3М	Соната-РС2	ЛГШ-513
Диапазон частот	150кГц...1800мГц	0.01–2000 МГц	0.009–1800 МГц
Диапазон регулировки уровня шума	25 - 75 дБ	Не менее 35 дБ	Не менее 20 дБ
Потребляемая мощность	40ВА	Не более 10 Вт	Не более 45 ВА
Сертификат	ФСТЭК	ФСТЭК по 1 классу защиты	ФСТЭК по 2 классу защиты
Примечания	Генерирует шум с коэффициентом качества не менее 0.8	По цепям электропитания, заземления и ПЭМИН	По цепям электропитания, заземления и ПЭМИН

В качестве генератора шума был выбран Соната-РС2.

#### 4.3 Устройства для перекрытия утечек с использованием побочного электромагнитного излучения и наводок (ПЭМИН)

Так как и ШТОРМ-10, и Соната-РС2, выбранные в предыдущем пункте, работают также с ПЭМИН, то отдельное устройство отбирать не планируется.

#### **4.4   Устройства   для   перекрытия   оптического   канала   утечки информации**

Для перекрытия оптического канала утечки будем использовать жалюзи на окнах и доводчики на дверях.

#### **4.5   Расстановка инженерно-технических средств защиты информации**

Согласно информации, содержащейся в предыдущих пунктах, было решено установить в помещении следующие средства защиты в количестве и качестве, указанных в таблице 4.5.

Таблица 4.5 – Расстановка СЗИ

Средство защиты	Канал утечки	Количество и место
ШТОРМ-10	Акустический, ПЭМИН	Один на помещение, устанавливается согласно требованиям по эксплуатации.
Соната-РС2	Электрический и электромагнитный, ПЭМИН	Один на помещение, устанавливается согласно требованиям по эксплуатации.
Жалюзи	Оптический	На каждое окно (6 штук).
Доводчики двери	Акустический, оптический	На каждую дверь (7 штук).
Панели с песком	Акустический	В кабинете директора и переговорной.
Aaronia X-Dream	Электрический	Для кабинета сотрудников.
Размыкатели слаботоковых линий SI-5020	ПЭМИН	В составе ШТОРМ-10.
Размыкатели линий электропитания	ПЭМИН	В составе ШТОРМ-10.
Размыкатели линий Ethernet	ПЭМИН	В составе Соната
Виброизлучатель ВИ-3М	Виброакустический	Для стен, полов, потолков и на двери.









## 5 ПЛАН ПОМЕЩЕНИЯ С АКТИВНОЙ И ПАССИВНОЙ ЗАЩИТОЙ







На рисунке 5 приведен план помещения с активной и пассивной защитой, в таблице 5 приведены условные обозначения для плана.



Рисунок 5 – План помещения с активной и пассивной защитой

Таблица 5 – Условные обозначения

	Блок энергопотребления и управления ШТОРМ-10
	Блок энергопотребления и управления Соната
	Жалюзи
	Доводчики дверей
	Панели с песком (звукоизоляция)
	Aaronia X-Dream
	Размыкатели слаботочных линий
	Размыкатели линий электропитания

	Размыкатели линий Ethernet
	Виброизлучатель ВИ-3М (стена)
	Виброизлучатель ВИ-3М (окно)
	Виброизлучатель ВИ-3М (потолок)
	Виброизлучатель ВИ-3М (пол)
	Виброизлучатель ВИ-3М (дверь)

## **ЗАКЛЮЧЕНИЕ**

В результате выполнения работы был проведён анализ выбранного предприятия и обрабатываемой там информации, рынка инженерно-технических средств защиты информации, а также выполнено проектирование инженерно-технической системы защиты информации.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

6. Н.С. Кармановский, О.В. Михайличенко, С.В. Савков. ОРГАНИЗАЦИОННО-ПРАВОВОЕ И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: студенческое пособие. – Текст: электронный. – 2013. – URL: <https://books.ifmo.ru/file/pdf/1093.pdf> (дата обращения: 15.12.2023).
7. О государственной тайне: Закон РФ от 21.07.1993 N 5485-1 (ред. от 04.08.2023) // Собрание Законодательства Российской Федерации.
8. Способы и средства защиты информации от утечки по техническим каналам: сайт. Текст: электронный. – 2016. – URL: <https://cyberleninka.ru/article/n/sposoby-i-sredstva-zaschity-informatsii-ot-utechki-po-tehnicheskim-kanalam> (дата обращения: 15.12.2023) – Загл. с экрана.