

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«САНКТ-ПЕТЕРБУРГСКИЙ 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 139»

**Выполнила:**

Лопатина М. Д., студент группы N34531



(подпись)

**Проверил:**

Попов И. Ю., к.т.н., доцент ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

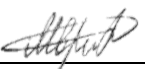
2023 г.

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

Студент	Лопатина Марина Дмитриевна
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34531
Направление (специальность)	11.03.03 Конструирование и технология электронных средств
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 139
Задание	изучить существующие каналы утечки информации, научиться разрабатывать план расположения инженерно-технических средств защиты информации

**Краткие методические указания**

**Рекомендуемая литература**

Руководитель	25.12.2023
	(Подпись, дата)
Студент	 25.12.2023
	(Подпись, дата)

Студент	Лопатина Марина Дмитриевна
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34531
Направление (специальность)	11.03.03 Конструирование и технология электронных средств
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 139

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Создание плана КР	27.11.2023	27.11.2023	
2	Анализ литературы	28.11.2023	30.11.2023	
3	Разработка перечня средств защиты	03.12.2023	10.12.2023	
4	Составление основного текста КР	17.12.2023	23.12.2023	
5	Защита курсовой работы	25.12.2023	25.12.2023	

Руководитель	25.12.2023
	(Подпись, дата)
Студент	25.12.2023
	(Подпись, дата)

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

Студент    Лопатина Марина Дмитриевна

(Фамилия И.О.)

Факультет    Безопасности Информационных Технологий

Группа    N34531

Направление (специальность)    11.03.03 Конструирование и технология электронных средств

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 139

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

**1. Цель и задачи  
работы**

- ☒ Предложены студентом    ☐ Сформулированы при участии студента  
☐ Определены руководителем

Цель данной работы – разработать план размещения комплекса мер инженерно-технической защиты информации для компании ООО «СофтЛайт».

**2. Характер  
работы**

- ☐ Расчет    ☐ Конструирование  
☐ Моделирование    ☒ Другое

**1. Содержание работы**

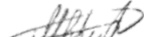
В данной курсовой работе рассмотрены существующие каналы утечки информации, проведен анализ исследуемого предприятия, разработан перечень необходимых средств защиты информации, создан план размещения средств защиты информации.

**2. Выводы**

В результате проведенной работы были проанализированы актуальные каналы утечки информации для организации ООО «СофтЛайт»

Руководитель    25.12.2023

(Подпись, дата)

Студент     25.12.2023

(Подпись, дата)

«\_\_»\_\_\_\_\_20\_\_г.

## СОДЕРЖАНИЕ

ВВЕДЕНИЕ .....	6
1     ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ .....	7
1.1    Описание предприятия.....	7
1.2    Схема организационных структур .....	7
1.3    Схема информационных потоков .....	7
2     ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ .....	9
3     РАССМОТРЕНИЕ ПЛАНА ПОМЕЩЕНИЯ .....	13
3.1    Схема помещения .....	13
3.2    Описание помещения .....	16
3.3    Анализ возможных каналов утечки информации .....	16
3.3.1    Акустические каналы утечки информации .....	17
3.3.2    Электромагнитные каналы утечки информации .....	17
3.3.3    Визуально-оптический канал утечки информации .....	18
3.3.4    Материально-вещественные каналы утечки информации .....	18
4     АНАЛИЗ РЫНКА .....	19
4.1    Защита от утечки информации по акустическим и виброакустическим каналам	19
4.2    Защита от утечки информации по электрическим и электромагнитным каналам	20
4.3    Защита от утечек с использованием побочного электромагнитного излучения и наводок (ПЭМИН) .....	22
4.4    Защита от утечек информации по визуально-оптическим каналам .....	22
5     ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ.....	23
ЗАКЛЮЧЕНИЕ.....	25
СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ .....	26

## **ВВЕДЕНИЕ**

Цель работы – разработать план размещения комплекса мер инженерно-технической защиты информации для компании ООО «СофтЛайт».

Для выполнения поставленной цели необходимо выполнить следующие задачи:

- изучить организационную структуру предприятия;
- составить обоснование защиты информации;
- проанализировать план помещения предприятия;
- проанализировать актуальные каналы утечки информации для предприятия;
- составить перечень средств защиты информации для предприятия;
- составить план размещения средств защиты информации.

# 1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

## 1.1 Описание предприятия

В рамках курсовой работы будет проведено исследование предприятия ООО «СофтЛайт» с целью разработки комплекса инженерно-технических средств защиты информации.

ООО «СофтЛайт» – IT компания, специализирующаяся на разработке программного обеспечения на заказ. Деятельность компании нацелена на выполнение B2B-решений, помимо этого компания разрабатывает ПО для государственных органов и работает со сведениями составляющими государственную тайну уровня «секретно».

## 1.2 Схема организационных структур

На рисунке 1 представлена схема структуры исследуемого предприятия.

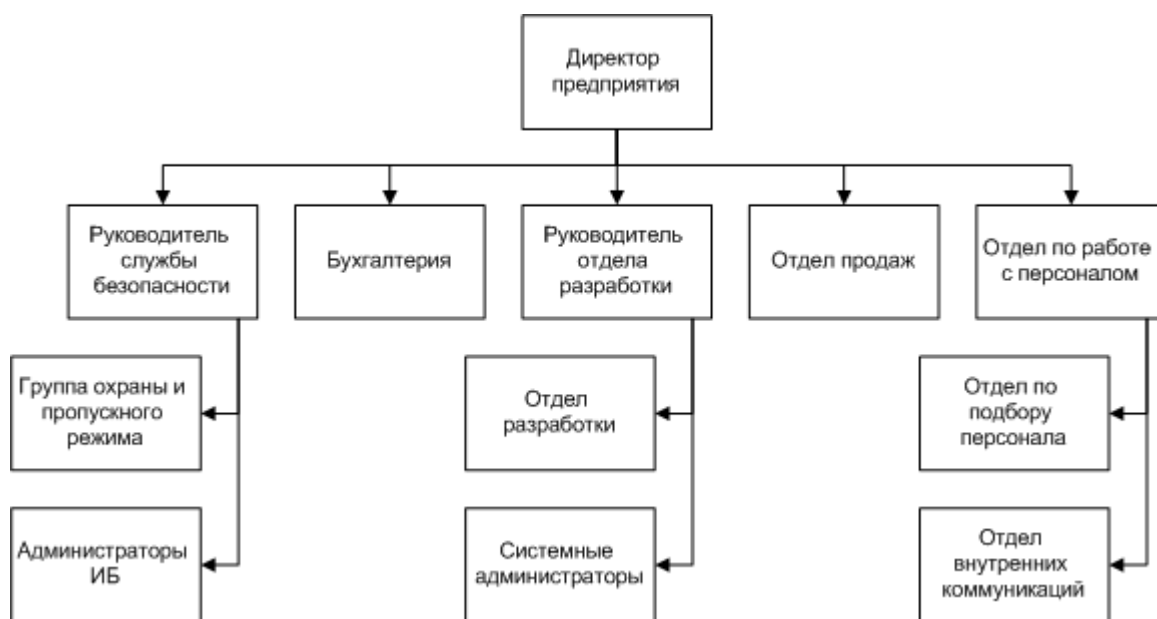


Рисунок 1 – Структура предприятия

## 1.3 Схема информационных потоков

На рисунке 2 представлена схема основных информационных потоков предприятия.

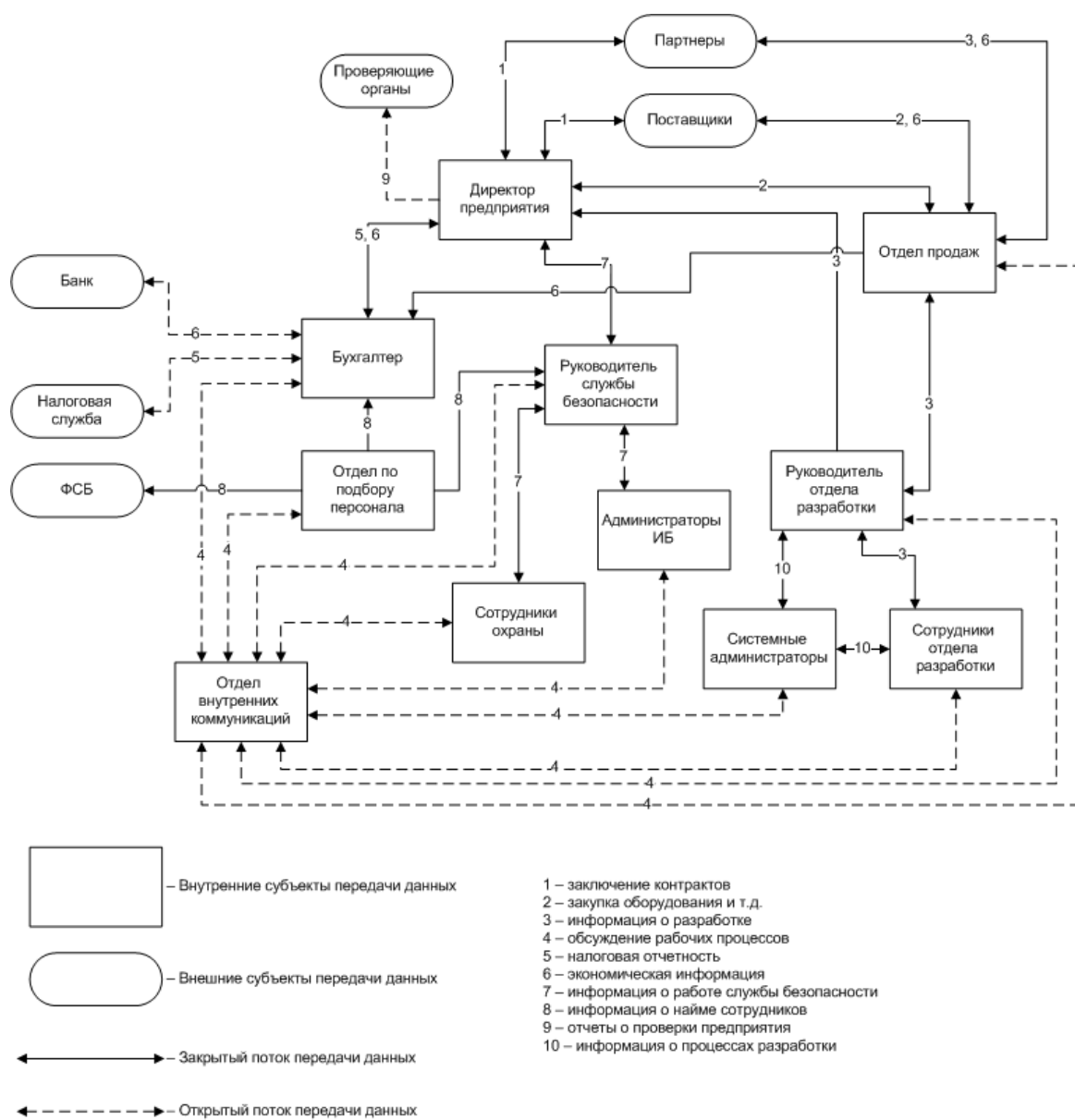


Рисунок 2 – Схема информационных потоков



## **2       ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ**

Так как компания работает с государственной тайной, необходимо провести анализ нормативной базы для обоснования защиты информации:

- Закон РФ от 21 июля 1993 г. N 5485-I «О государственной тайне»;
- Постановление Правительства РФ от 22 ноября 2012 г. № 1205 «Об утверждении правил организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны»;
- Постановление Правительства РФ от 04.09.1995 N 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»;
- Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.;
- «Типовые нормы и правила 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.

Согласно Закону РФ от 21 июля 1993 г. N 5485-I «О государственной тайне»:

«Допуск предприятий, учреждений и организаций к 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, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию».

Согласно Постановлению Правительства РФ от 04.09.1995 N 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»:

«3. Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на сведения особой важности, совершенно секретные и секретные.

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».

Согласно Руководящему документу Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.:

«2.18. При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В»

В таблице 1 представлена классификация классов защищенности.

Таблица 1 – Классификация классов защищенности

Первая группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится	1А	В случае обработки секретной информации с грифом «особая важность»
	1Б	В случае обработки секретной информации с грифом не выше «совершенно секретно»

информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)	1В	В случае обработки секретной информации с грифом не выше «секретно»
	1Г	АС, в которых циркулирует служебная информация
	1Д	АС, в которых циркулируют персональные данные
Вторая группа (АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности)	2А	Информация, составляющая гостайну
	2Б	Служебная тайна или персональные данные
Третья группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)	3А	Информация, составляющая гостайну
	3Б	Служебная тайна или персональные данные

В соответствии с этой классификацией можно сказать, что, рассматривая организация имеет класс защищенности 1В.

Согласно «Типовым нормам и правилам 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:

- стены или перегородки между обычными и защищенными помещениями должны быть бетонными, железобетонными или металлическими с толщиной стен — от 10 см, или кирпичными с толщиной стен от 12 см;

- в помещениях для работы с гостайной 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;

- обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании;

- вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений;

- перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации.

### 3 РАССМОТРЕНИЕ ПЛАНА ПОМЕЩЕНИЯ

#### 3.1 Схема помещения

На рисунке 3 представлена схема защищаемого помещения.

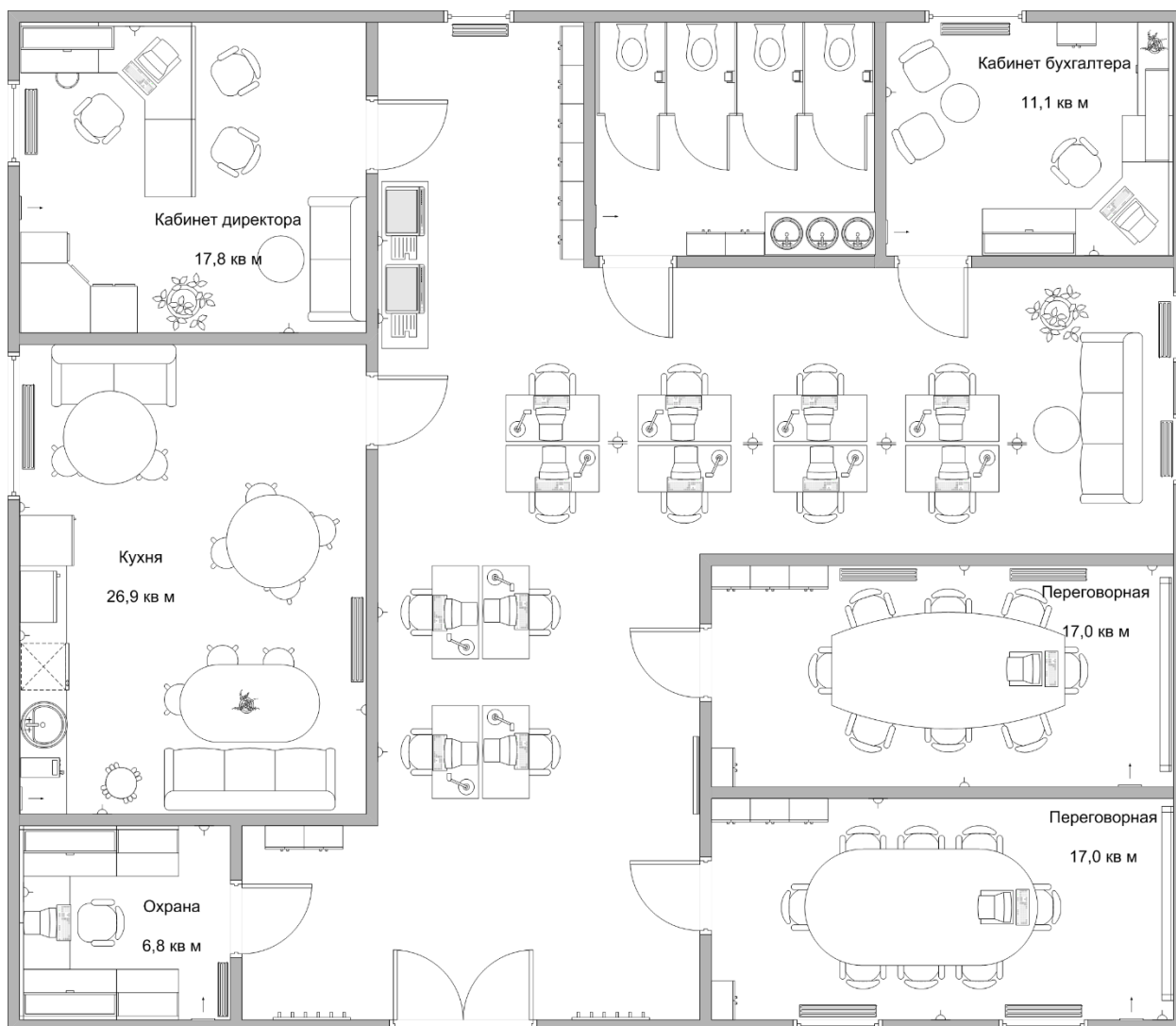


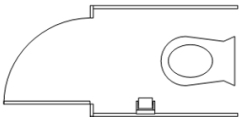


















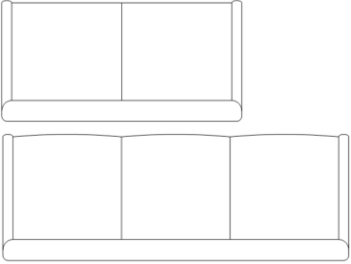
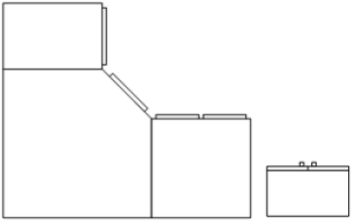
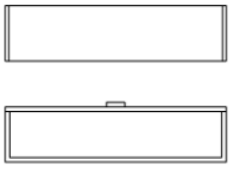
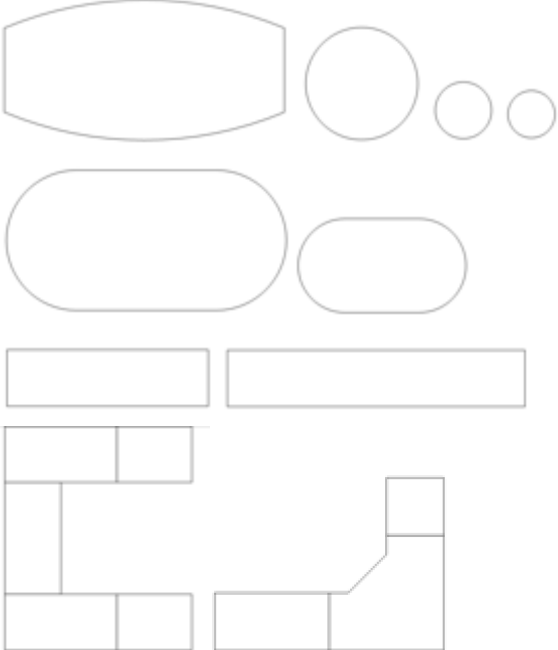
Рисунок 3 – План помещения

В таблице 2 представлены условные обозначения плана.

Таблица 2 – Условные обозначения

	Двери
	Стена
	Окно

	Стул
	Цветы в горшках
	Туалетная кабинка
	Корзина для мусора
	Раковина
	Батарея
	Розетка
	Вентиляция
	Настольная лампа
	Вешалка
	Доска для объявлений
	Экран для проектора
	Компьютер
	МФУ
	Тумбочка
	Посудомоечная машина
	Микроволновая печь

	Холодильник
	Кофемашина
	Диван
	Шкаф
	Подвесная полка
	Стол

### **3.2 Описание помещения**

На предприятии имеются следующие комнаты, подлежащие инженерно-технической защите:

1. Кабинет директора – 17,8 кв м
2. Кухня – 26,9 кв м
3. Кабинет охраны – 6,8 кв м
4. Главный холл – 78,3 кв м
5. Туалетные комнаты – 10,8 кв м
6. Кабинет бухгалтера – 11,1 кв м
7. Переговорная комната – 17 кв м
8. Переговорная комната – 17 кв м

В кабинете директора есть рабочее место (рабочий стол, кресло, компьютер), 2 кресла для приёма посетителей, диван и журнальный столик, шкаф, цветок в горшке, батарею, 2 розетки, окно и дверь.

Кухня содержит: 3 обеденных стола, 2 дивана, 12 стульев, кухонную поверхность, кофемашину, микроволновую печь, холодильник, посудомоечную машину, раковину, цветок в горшке, 2 батареи, 4 розетки, окно и дверь.

В кабинете охраны есть рабочее место, батарея, 2 розетки, дверь.

Главный холл является открытым пространством с рабочими местами для большинства сотрудников, то есть 12 рабочих мест, диван и журнальный столик, рабочий стол, 2 принтера, 8 шкафов, 2 вешалки для одежды, доска для объявлений, цветок в горшке, 3 батареи, 12 розеток, 3 окна, 8 дверей.

Туалетная комната состоит из 4 кабинок, 3 раковин, 2 шкафов и двери.

В кабинете бухгалтера есть рабочее место, 2 кресла для посетителей и журнальный столик, шкаф, цветок в горшке, цветок в горшке, батарея, 2 розетки, окно и дверь.

В первой переговорной комнате: большой стол, 8 кресел, компьютер, 4 шкафа, экран для проектора, 2 батареи, 3 розетки, дверь.

Во второй переговорной комнате, по сравнению с первой ещё есть 2 окна.

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

Выделяют следующие виды технических каналов утечки информации:

- акустические каналы утечки информации;
- электромагнитные каналы утечки информации;
- визуально-оптические каналы утечки информации;



- материально-вещественные каналы утечки информации.

Далее будут более подробно рассмотрен каждый канал утечки информации.

### **3.3.1 Акустические каналы утечки информации**

В **акустических каналах** утечки информации средой распространения речевых сигналов является воздух, и для их перехвата используются высокочувствительные микрофоны и специальные направленные микрофоны. Микрофоны соединяются с портативными звукозаписывающими устройствами или миниатюрными передатчиками.

Автономные устройства, конструктивно объединяющие микрофоны и передатчики, называют закладными устройствами (ЗУ) перехвата речевой информации.

Источниками утечки информации по акустическому каналу на рассматриваемом предприятии могут быть: открытые двери или окна, плохая звукоизоляция, вентиляционные шахты, проводка, ЗУ в цветочных горшках или других местах.

К пассивной защите можно отнести средства звукоизоляции, а к активной устройства акустического зашумления.

В **виброакустических каналах** утечки информации средой распространения речевых сигналов являются ограждающие строительные конструкции помещений (стены, потолки, полы) и инженерные коммуникации (трубы водоснабжения, отопления, вентиляции и т. п.). Для перехвата речевых сигналов в этом случае используются вибродатчики.

Вибродатчик, соединенный с электронным усилителем называют электронным стетоскопом. Электронный стетоскоп позволяет осуществлять прослушивание речи с помощью головных телефонов и ее запись на диктофон.

Источниками утечки могут быть: твердые поверхности (стены, потолки, полы), батареи, вентиляционные трубы.

Пассивные методы защиты: звукоизоляция с использованием antivибрационных материалов, а активные: устройства вибрационного зашумления.

### **3.3.2 Электромагнитные каналы утечки информации**

**Электрический канал** перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры перехвата к кабельным линиям связи. Самый простой способ — это непосредственное параллельное подключение к линии связи.

**Электромагнитный канал** перехвата информации. Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки.

**ПЭМИН** (Побочные Электромагнитные Излучения и Наводки). Одним из возможных каналов утечки информации является излучение элементов компьютера. Принимая и декодируя эти излучения, можно получить сведения обо всей информации, обрабатываемой в компьютере.

Основными источниками получения информации по этим каналам утечки являются: розетки, бытовая техника, компьютеры, кабели.

Из методов пассивной защиты можно использовать фильтры для сетей электропитания, а из активных устройства электромагнитного зашумления.

### **3.3.3 Визуально-оптический канал утечки информации**

Основные способы утечки информации с помощью визуальных методов, фотографирования, видеосъёмки, наблюдения.

В рассматриваемом предприятии утечка информации возможна через окна или открытые двери.

В качестве пассивной защиты можно использовать жалюзи, шторы, зеркальные пленки для защиты окон и использование доводчиков для дверей.

### **3.3.4 Материально-вещественные каналы утечки информации**

Материально-вещественный канал – позволяют получать информацию путём хищения или нелегального доступа к носителям информации.

Защититься от утечек по материально-физическим каналам помогут организационные и технические меры. Первые предполагают внедрение системы учета физических носителей и документов, а также допусков к ним, принтерам, копировальной и другой технике с обязательным документированием. А вторые подразумевают использование СКУД.

## 4 АНАЛИЗ РЫНКА

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

Из средств пассивной защиты буду использовать дополнительную отделку кабинета директора и переговорных комнат звукоизолирующими материалами, а также усиленные двери.

Из активных средств защиты будут использоваться систему виброакустического зашумления. В таблице 3 представлены сравнительные характеристики систем.

Таблица 3 – Сравнение систем виброакустической защиты

Модель	Характеристика	Особенности	Стоимость
ЛГШ-404, генератор шума	Диапазон частот: 90...11200 Гц Электропитание: 220 В, 50 Гц Количество подключаемых излучателей: до 64	соответствует типу «А» - средства акустической и вибрационной защиты информации с центральным генераторным блоком и подключаемыми к нему по линиям связи пассивными преобразователями; соответствует требованиям «Требования к средствам активной акустической и вибрационной защиты акустической речевой информации» (ФСТЭК России, 2015) – по 1 классу защиты; оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима.	35 100 руб.
Генератор виброакустического шума SEL SP-157G	Диапазон частот: 90–11.2 кГц Электропитание: 220 В, 50 Гц Количество излучателей на 1 канале: до 32	Принцип действия основан на формировании широкополосных акустических и виброакустических маскирующих шумовых помех (аналоговый белый шум или смешанный с цифровой речеподобной помехой). Система состоит из центрального генераторного блока и подключаемых к нему по проводам пассивных электромагнитных (вибрационных) или	29 900 руб.

		электродинамических (акустических) преобразователей (излучателей).	
Виброакустическая защита Соната АВ-4Б	Диапазон частот: 175–11200 Гц Электропитание: 220 В, 50 Гц Количество излучателей на 1 канале: 239 шт	производство изделия Соната-АВ” модель 4Б сертифицировано. Сертификат ФСТЭК; построена по принципу "единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)"	44 200 руб.

По результатам сравнительного анализа была выбрана «Соната АВ-4Б» так как есть возможность подключения к одному питающему шлейфу, система имеет максимальное количество подключаемых устройств. Помимо этого, система считается одной из самых востребованных на рынке.

#### **4.2 Защита от утечки информации по электрическим и электромагнитным каналам**

Пассивная защита заключается в установке сетевых фильтров.

А активная защита основывается на создании в сети белого шума, который скрывает колебания, порождаемые воздействием звуковой волны или работающей электрической техникой. В таблице 4 приведен сравнительный анализ средств активной защиты от утечки информации по электрическим и электромагнитным каналам.

Таблица 4 – Сравнение защиты по электрическим и электромагнитным каналам

Модель	Характеристика	Особенности	Стоимость
Генератор шума ЛГШ-503	широкополосные шумовые помехи в диапазоне частот от 0,01 МГц до 2000 МГц. Электропитание: 220 В, 50 Гц.	предназначен для активной защиты объектов информатизации от утечки по сети электропитания ("фаза", "ноль" и "защитное заземление"), и для противодействия средствам несанкционированного съема информации по каналам ПЭМИ; устройство может эксплуатироваться круглосуточно.	44 200 руб.
Генератор шума Соната-РС3	Диапазон частот: до 2 ГГц; Кол-во фаз: 1;	Средство активной защиты информации от утечки по сети электропитания и линиям заземления;	20 160 руб.

	Электропитание: ~220 В, 50 Гц	Может использоваться в выделенных помещениях до 1 категории включительно.	
Генератор шума SEL SP-44	Диапазон частот: 0,01–300 МГц Количество независимых каналов шумового сигнала: 2	Сертификат ФСТЭК; техническое средство защиты информации, обрабатываемой на объектах вычислительной техники 1, 2 и 3 категории, от утечки за счёт наводок по цепям электропитания и заземления путём постановки маскирующих помех в цепях электропитания и заземления; может устанавливаться в выделенных помещениях до 1 категории включительно; Устройство имеет высший класс устойчивости к импульсным помехам и допускает длительную работу в условиях эквивалентного короткого замыкания. Применение ключевых выходных усилителей существенно повышает экономичность, надежность и стабильность параметров изделия, позволяет эксплуатировать его в более жестких климатических условиях	24 000 руб.

По результатам анализа был выбран ЛГШ-503, так как он имеет самый большой диапазон частот и защищает не только от электрического, электромагнитного каналов, но и от ПЭМИН, благодаря этому стоимость устройства также можно считать достаточно выгодной.

#### **4.3    Защита от утечек с использованием побочного электромагнитного излучения и наводок (ПЭМИН)**

Так как в пункте 4.2 в качестве средства защиты от утечек по электрическим и электромагнитным каналам был выбран генератор шума ЛГШ-503, который также для противодействия средствам несанкционированного съема информации по каналам ПЭМИН, то отдельное устройство выбирать не требуется.

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

Для защиты от утечек по визуально-оптическим каналам будут использоваться доводчики на двери. Также на все окна будут установлены жалюзи, так как этот вариант намного дешевле и проще в установке по сравнению с защитными пленками.

## 5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

Согласно сравнительному анализу, приведенному в 4 разделе, для защиты помещения были выбраны следующие средства защиты информации:

- виброакустическая система защиты «Соната АВ-4Б»;
- усиленные двери в кабинет директора и переговорные комнаты;
- звукоизоляция кабинета директора и переговорных комнат;
- генератор шума ЛГШ-503;
- сетевой фильтр;
- жалюзи на каждое окно;
- доводчики дверные на каждую дверь.

На рисунке 4 представлен план расположения комплекса инженерно-технических средств защиты, а в таблице 5 представлены условные обозначения для этого плана.

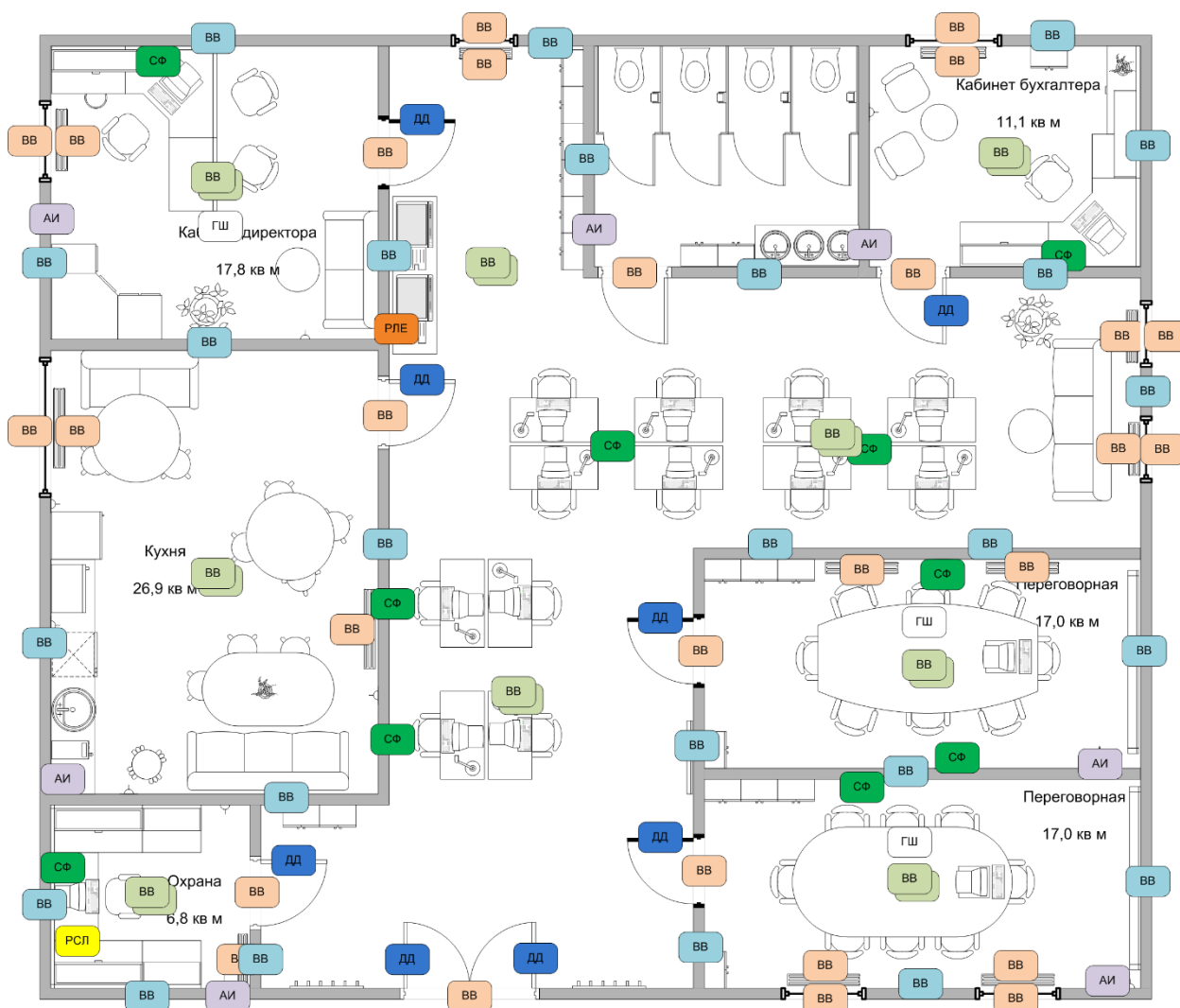
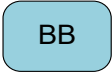
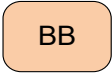
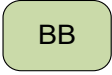




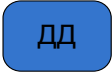

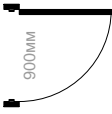



Рисунок 4 – План расположения инженерно-технических средств защиты

Таблица 5 – Условные обозначения

Условное обозначение	Средство защиты
	Генератор-вибровозбудитель «Соната СВ-4Б» (на стены)
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)
	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)
	Генератор-акустоизлучатель «Соната СА-4Б1» (вентиляция)
	Генератор шума «ЛГШ-503»
	Размыкатель линии «Ethernet» «Соната-ВК4.3»
	Размыкатель слаботочной линии «Соната-ВК4.2»
	Дверной доводчик
	Сетевой фильтр
	Усиленная дверь
	Жалюзи



## **ЗАКЛЮЧЕНИЕ**

В ходе выполнения курсовой работы был проведен теоретический анализ существующих каналов утечки информации, анализ потенциальных каналов утечки информации для компании ООО «СофтЛайт». Был проведен анализ рынка современных инженерно-технических средств защиты информации. По результатам анализа был сформирован перечень необходимых мер защиты для противодействия утечки информации. В результате выполнения работы была предложена защита от утечек информации по акустическому, виброакустическому, электромагнитному, визуально-оптическому каналам, а также обеспечена защита от ПЭМИН. И был разработан план размещения инженерно-технических средств защиты.

## СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Кармановский Н.С., Михайличенко О.В., Савков С.В.. Организационноправовое и методическое обеспечение информационной безопасности. Учебное пособие – Санкт-Петербург: НИУ ИТМО, 2013. - 151 с.
2. Требования к режимным помещениям и их оборудованию : сайт. – Текст : электронный. – 2023. – URL : <https://licenziya-fsb.com/trebovaniya-k-rezhimnym-pomeshheniyam> – Загл. с экрана.