

**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»

**Выполнил:**

Нгуен Тхань Чунг, студент группы N34461



(подпись)

**Проверил:**

Н.с., доцент фБИТ

Попов Илья Юрьевич

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

Студент	Нгуен Тхань Чунг
	(Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34461
Направление (специальность)	10.03.01 Технологии защиты информации (2020)
Руководитель	Попов Илья Юрьевич, н.с, доцент факультета безопасности информационных технологий
	(Фамилия И.О, должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии
Задание	Проектирование инженерно-технической системы 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, размещённых на коммуникационной площадке дисциплины;
3. Объект исследований курсовой работы ограничивается заданным помещением.

**Содержание пояснительной записки**

Пояснительная записка включает разделы:

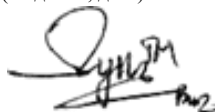
1. Введение;
2. Анализ технических каналов утечки информации;
3. Руководящие документы;
4. Анализ защищаемых помещений;
5. Анализ рынка технических средств;
6. Описание расстановки технических средств;
7. Заключение;
8. Список литературы.

**Рекомендуемая литература**

Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.

**Руководитель**

(Подпись, дата)



**Студент**

(Подпись, дата)

19.12.2023

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

**Студент** Нгуен Тхань Чунг  
(Фамилия И.О.)

**Факультет** Безопасность информационных технологий

**Группа** N34461

**Направление (специальность)** 10.03.01 Технологии защиты информации (2020)

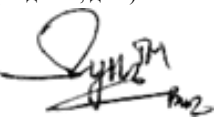
**Руководитель** Попов Илья Юрьевич, н.с, доцент факультета безопасности информационных технологий  
(Фамилия И.О., должность, ученое звание, степень)

**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.	Заполнение задания на курсовую работу	17.11.2023	17.11.2023	
2.	Анализ информации	19.11.2023	20.11.2023	
3.	Написание курсовой работы	14.12.2023	15.12.2023	
4.	Защита курсовой работы	19.12.2023	19.12.2023	

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




**Студент** \_\_\_\_\_ 19.12.2023  
(Подпись, дата)

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

<b>Студент</b>	Нгуен Тхань Чунг		
	(Фамилия И.О)		
<b>Факультет</b>	Безопасность информационных технологий		
<b>Группа</b>	N34461		
<b>Направление (специальность)</b>	10.03.01 Технологии защиты информации (2020)		
<b>Руководитель</b>	Попов Илья Юрьевич, н.с, доцент факультета безопасности информационных технологий		
	(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)**

<b>1. Цель и задачи работы</b>	<input type="checkbox"/> Предложены студентом <input type="checkbox"/> Сформулированы при участии студент <input checked="" type="checkbox"/> Определены руководителем Целью работы является повышение защищенности рассматриваемого помещения. Задачами является анализ Защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.		
<b>2. Характер работы</b>	<input type="checkbox"/> Расчёт <input checked="" type="checkbox"/> Конструирование <input type="checkbox"/> Моделирование <input type="checkbox"/> Другое		
<b>3. Содержание работы</b>	Пояснительная записка включает разделы: введение; анализ технических каналов утечки информации; руководящие документы; анализ защищаемых помещений; анализ рынка технических средств; описание расстановки технических средств; заключение; список литературы.		
<b>4. Выводы</b>	В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.		

<b>Руководитель</b>		
	(Подпись, дата)	
		
<b>Студент</b>		19.12.2023
	(Подпись, дата)	

## СОДЕРЖАНИЕ

Содержание .....	5
Введение .....	6
1     АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ.....	7
2     РУКОВОДЯЩИЕ ДОКУМЕНТЫ .....	10
2.1     Законы Российской Федерации.....	10
2.2     Указы Президента Российской Федерации.....	10
2.3     Постановления Правительства Российской Федерации .....	10
2.4     ФСТЭК России.....	11
3     АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ .....	12
3.1     Обоснование секретности.....	12
3.2     Описание помещения .....	13
3.3     Анализ технических каналов утечки .....	14
3.4     Выбор средств защиты информации .....	14
4     АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ .....	16
4.1     Требования к защите помещений .....	16
4.2     Анализ средств активной инженерно-технической защиты информации.....	17
5     ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ.....	22
Заключение.....	24
Список использованных источников.....	25

## **ВВЕДЕНИЕ**

В контексте прогресса информационных технологий и компьютеризации экономики, одним из важных аспектов в деятельности организации становится обеспечение безопасности информации.

Информация представляет собой один из ключевых и ценных ресурсов предприятия, который требует должной защиты. Понятие информационной безопасности включает в себя сохранение и защиту информации, включая системы и оборудование, предназначенные для использования, хранения и передачи данных. Другими словами, это комплекс технологий, стандартов и методов управления, необходимых для обеспечения защиты информации.

Главная цель обеспечения информационной безопасности заключается в защите информационных данных и инфраструктуры от случайных или умышленных вмешательств, которые могут привести к потере данных или их несанкционированным изменениям. Обеспечение информационной безопасности способствует непрерывности бизнес-процессов.

В рамках обеспечения защиты информации в информационных системах используются средства защиты, включая технические компоненты, играющие важную роль в системе обеспечения информационной безопасности. В данной работе было проведено проектирование системы инженерно-технической защиты информации с уровнем секретности "совершенно секретно" на объекте информатизации.

## **1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ**

Анализ технических маршрутов утечки информации направлен на выявление и блокировку их использования. В наше время большая часть конфиденциальных данных становится доступной для злоумышленников в результате кибератак, но технические каналы сохраняют свою актуальность. Поэтому по сей день проводится процедура аттестации помещений и оборудования с целью выявления и снижения уровня рисков. Утечка информации наиболее часто происходит через четыре основных вида технических каналов:

- по линиям побочных электромагнитных излучений и наводок (ПЭМИН);
- по линиям телефонной связи;
- через акустические и акустовибрационные каналы;
- по видовым (оптическим) каналам.

Информация передается полем или веществом. Это может быть либо акустическая волна, либо электромагнитное излучение, либо лист бумаги с текстом и т.п. Другими словами, используя те или иные физические поля, человек создает систему передачи информации или систему связи. Система связи в общем случае состоит из передатчика, канала передачи информации, приемника и получателя информации. Легитимная система связи создается и эксплуатируется для правомерного обмена информацией. Однако ввиду физической природы передачи информации при выполнении определенных условий возможно возникновение системы связи, которая передает информацию вне зависимости от желания отправителя или получателя информации – технический канал утечки информации.

Утечка - бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Утечка (информации) по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. Технический канал утечки информации (ТКУИ), так же как и канал передачи информации, состоит из источника сигнала, физической среды его распространения и приемной аппаратуры злоумышленника. На рисунке 1 приведена структура технического канала утечки информации.



Рисунок 1 – Структура технического канала утечки информации

На вход канала поступает информация в виде первичного сигнала. Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода предыдущего канала. В качестве источника сигнала могут быть:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;
- источник опасного сигнала;
- источник акустических волн, модулированных информацией.

Так как информация от источника поступает на вход канала на языке источника (в виде буквенно-цифрового текста, символов, знаков, звуков, сигналов и т. д.), то передатчик производит преобразование этой формы представления информации в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. В общем случае он выполняет следующие функции:

- создает поля или электрический ток, которые переносят информацию;
- производит запись информации на носитель;
- усиливает мощность сигнала (носителя с информацией);
- обеспечивает передачу сигнала в среду распространения в заданном секторе пространства.

Среда распространения носителя - часть пространства, в которой перемещается носитель. Она характеризуется набором физических параметров, определяющих условия перемещения носителя с информацией. Основными параметрами, которые надо учитывать при описании среды распространения, являются:

- физические препятствия для субъектов и материальных тел;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;



- вид и мощность помех для сигнала.

Приемник выполняет функции, обратные функциям передатчика. Он производит:

- выбор носителя с нужной получателю информацией;
- усиление принятого сигнала до значений, обеспечивающих съем информации;
- съем информации с носителя;
- преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

Классификация технических каналов утечки информации приведена на рисунке 2.



Рисунок 2 – Классификация технических каналов утечки информации

## **2 РУКОВОДЯЩИЕ ДОКУМЕНТЫ**

Нормативные документы по противодействию технической разведке:

### **2.1 Законы Российской Федерации**

1. «О безопасности» от 5 марта 1992 г. №2446–1;
2. «О государственной тайне» от 21 июля 1993 г. №5151–1;
3. «О связи» от 16 февраля 1995 г. №15-ФЗ;
4. «Об участии в международном информационном обмене» от 4 июля 1996 г. №85-ФЗ.

### **2.2 Указы Президента Российской Федерации**

1. «Вопросы защиты государственной тайны» от 30.03.1994 г. №614;
2. Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203;
3. «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;
4. «Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. №212.

### **2.3 Постановления Правительства Российской Федерации**

1. «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870;
2. «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. №1233;
3. «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. №973;
4. «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» от 15 апреля 1995 г. №333.

## **2.4 ФСТЭК России**

1. Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам;
2. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации;
3. Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей;
4. Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации.

### 3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

#### 3.1 Обоснование секретности

Предприятие «Рино Танк» работает в военной сфере, исследуя и производя танки и радиолокационные средства обнаружения.

Область деятельности: исследование и производство танков.

Государственной тайной является информация, охраняемая государством в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной деятельности, распространение которой может причинить ущерб государству.

В соответствии с версией курсовой работы уровень секретности информации ограниченного доступа, относящейся к государственной тайне, – «совершенно секретно». К совершенно секретной информации должны относиться сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести вред интересам министерства.

Поскольку предприятие занимается производством танков, информация, обрабатываемая в охраняемом помещении, которым является офис предприятия, относится к категории совершенно секретной информации.

В состав офиса входят отделы кадров, бухгалтерии и информационных технологий. Поток информации, предусмотренный должностными обязанностями и организационными документами, представлен на схеме потоков данных (рис. 3). Государственная информация передается по открытым каналам, а конфиденциальная информация (персональные данные, коммерческая тайна, профессиональная тайна, судебная тайна) и государственная тайна передается по закрытым потокам.

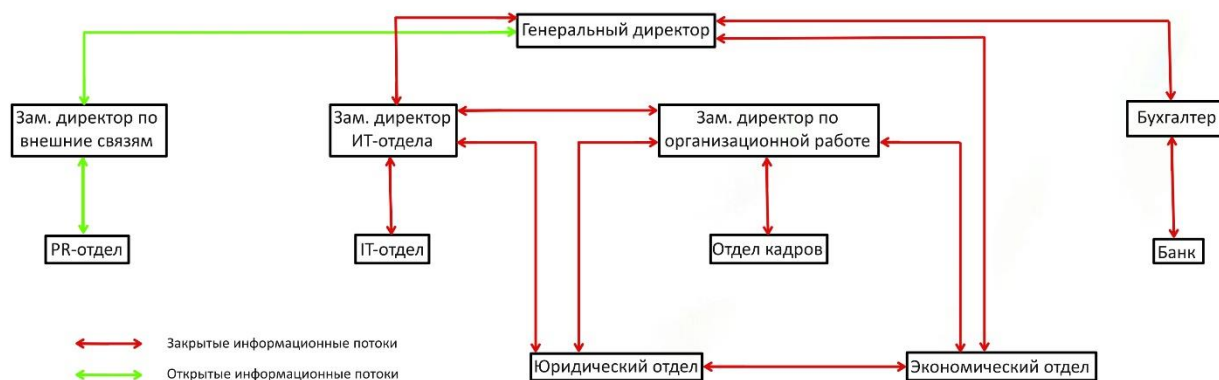


Рисунок 3 – Открытые и закрытые информационные потоки предприятия

### 3.2 Описание помещения

Имеется только один вход и выход. Для всех окон используются решетки с внешней стороны, а с внутренней - жалюзи, плотно закрывающие видимость снаружи. На рисунке 4 представлен план защищаемого помещения. В таблице 1 представлена легенда плана защищаемого помещения.

Помещение состоит из 10 комнат. Номера на плане здания соответствуют следующим помещениям:

1. Холл
2. Переговорная №1
3. Компьютерный зал №1
4. Компьютерный зал №2
5. Серверная
6. Столовая
7. Кабинет директора
8. Переговорная №2
9. Туалет
10. Зал ожидания

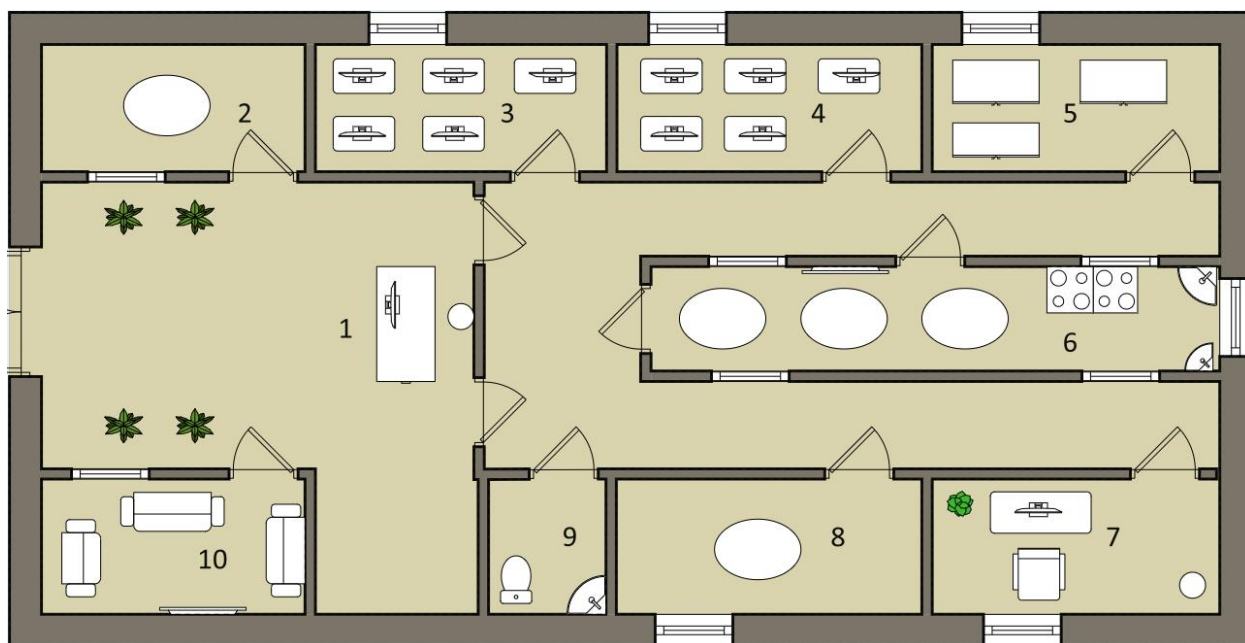



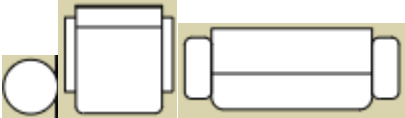
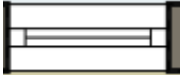



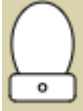



Рисунок 4 – План помещения предприятия

Таблица 1 – Условные обозначения

№	Условное обозначение	Описание объекта
1		Стандартное АРМ

2		Северная
3		Стол
4		Стул
5		Окно
6		Растения
7		Плита
8		Раковина
9		Унитаз
10		ЖК-телевизор

### 3.3 Анализ технических каналов утечки

В комнате возможно размещение закладных устройств. Практически в каждой комнате есть розетки и электроприборы, поэтому можно получить информацию по электрическим и электромагнитным каналам. Кроме того, актуальны лазерные, акустические и виброакустические каналы утечки информации. Также актуальны технические каналы утечки специфической информации, такие как съемка объектов, съемка документов и наблюдение за объектом.

### 3.4 Выбор средств защиты информации

Для обеспечения инженерно-технической защиты сверхсекретной информации от утечки по техническим каналам необходимо оборудовать защищаемые помещения средствами информационной безопасности. Выбранные средства активной и пассивной защиты представлены в таблице 2.

Таблица 2 – Средства инженерно-технической защиты информации

№	Каналы	Источники	Пассивная защита	Активная защита
1	Акустический Акустоэлектрический	Двери, окна, проводка	Сетевые фильтры, звукоизоляция кабинета директора и переговорных	Устройства акустического зашумления
2	Электромагнитный Электрический	Бытовые приборы, телевизоры, розетки, АРМ, ноутбуки	Сетевые фильтры	Устройства электромагнитного зашумления
3	Виброакустический	Пол, окна, двери, стены, столы	Изолирующие звук и вибрацию материалы стен	Устройства виброакустического зашумления и защиты
4	Съемка объектов, съемка документов, наблюдение за объектом	Двери, окна	Доводчики на двери, жалюзи на окнах	Устройства, блокирующие обзор
5	Лазерный			

## **4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

### **4.1 Требования к защите помещений**

В соответствии с заданием курсовой работы предприятие работает с информацией 2 степени секретности или с информацией, представляющей государственную тайну с грифом «совершенно 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:

Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения, проверить на предмет наличия закладных устройств и иных средств несанкционированного получения информации

Все режимные помещения оборудуются аварийным освещением.

- 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;

- 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;

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

- помещения, где хранятся секретные документы и носители государственной тайны, оборудуются охранной и аварийной сигнализацией;

- 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.



## 4.2 Анализ средств активной инженерно-технической защиты информации

Рассмотрим устройства предотвращения протечек по техническим каналам, актуальным для рассматриваемого помещения.

Для защиты от протечек необходимо предусмотреть акустико-шумовые устройства (табл. 3).

Таблица 3 – Средства активной защиты от утечки по акустическому, виброакустическому и акустоэлектрическому каналам

№	Устройство	Характеристики	Цена, руб	Описание
1	ГЕНЕРАТОР ШУМА ЛГШ-303	Диапазон частот акустической помехи: 180 ... 11 300 Гц Время автономной работы: до 5 часов Непрерывной работы от одного комплекта батарей Средняя наработка на отказ: не менее 5000 ч	15 600	Генератор шума ЛГШ-303 – акустический подавитель диктофонов и микрофонов, предназначенный для обеспечения конфиденциальности переговоров в помещении либо в салоне автомобиля. Эта мобильная глушилка прослушки, несмотря на компактные размеры, обеспечивает надежное подавление любых микрофонов в радиусе до 2-3 метров. Шумовая помеха, которую создает и транслирует подавитель, блокирует как кинематические и цифровые, так и лазерные микрофоны.
2	ГЕНЕРАТОР ШУМА ЛГШ-304	Диапазон частот акустической помехи: 175- 11200 Гц	25 200	Генератор ЛГШ-304 предназначен для защиты акустической речевой информации, содержащей сведения, составляющие

		<p>Время автономной работы: не менее 8 часов</p> <p>не более 10 ВА</p> <p>от 1 до 40 °С</p> <p>630–800 мм рт.ст.</p> <p>Средняя наработка на отказ: не менее 6 000 ч</p>		<p>государственную тайну, и иной информации с ограниченным доступом, циркулирующей (обрабатываемой) в помещениях, путем формирования акустических маскирующих шумовых помех.</p> <p>Изделие акустической защиты информации ЛГШ-304 соответствует типу «Б» средства акустической защиты информации с активным (содержащим в своей конструкции индивидуальный задающий источник шума) преобразователем, питаемым по линии вторичного электропитания от центрального блока питания.</p>
3	Система акустических и виброакустических помех Буран	<p>Частота, Гц: 100 – 11 200 Гц</p> <p>Электропитание: 220 В ± 10 %, 50-60 Гц</p> <p>Максимальное число акустических излучателей, подключаемых к каналу 3 параллельно: при максимальном уровне сигнала (0 дБ); 3 (нагрузка –</p>	67 500	<p>Система акустических и виброакустических помех «Буран» является средством активной акустической и вибрационной защиты акустической речевой информации типа А, соответствует требованиям ФСТЭК России к средствам защиты акустической речевой информации по 2 классу защиты и может устанавливаться в выделенных помещениях.</p>

		95 %) / при среднем уровне сигнала (-20 дБ) 10 (нагрузка – 95 %)		
--	--	--	--	--

Из рассматриваемых средств безопасности было решено выбрать «Система акустических и виброакустических помех Буран», поскольку с его помощью можно защитить информацию одновременно по акустическому, акустоэлектрическому и виброакустическому каналам. Пассивная защита от утечек по акустическим, виброакустическим и акустоэлектрическим каналам содержит следующие компоненты:

- сетевые фильтры;
- усиленные двери;
- звуко-виброизоляционные стеновые материалы.

Чтобы обеспечить защиту помещения от наблюдения, киносъемки и утечки по лазерному каналу, на окнах необходимо установить жалюзи или шторы. С точки зрения удобства ухода были выбраны жалюзи. Также необходимо учитывать электромагнитный шум, чтобы противодействовать электромагнитным и электрическим утечкам (табл. 4).

Таблица 4 – Средства активной защиты от утечки по электрическому и электромагнитному каналам

№	Устройство	Характеристики	Цена, руб	Описание
1	Соната-РСЗ	Световая, звуковая (исправность / отказ) Длительность – не менее 7 лет Сеть ~220 В +10%/- 15%, 50 Гц Продолжительность непрерывной работы, часов, не менее 8	32 400	Устройство для защиты линий электропитания, заземления от утечки информации предназначено для защиты объектов вычислительной техники от утечки информации за счет наводок на линии электропитания и заземления. Может использоваться в выделенных помещениях до 1 категории включительно.

2	ГЕНЕРАТОР ШУМА ЛГШ-501	<p>Рабочий диапазон частот, МГц: 0.01 ÷ 1800</p> <p>Диапазон регулировки уровня выходного шумового сигнала, не менее, 20 дБ</p> <p>Показатель электромагнитной совместимости, Рэмс, не менее, 70 м</p> <p>Режим работы: непрерывный, круглосуточный</p> <p>Средняя наработка на отказ, не менее, 1200 часов</p>	29 900	Изделие предназначено для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.
3	ГЕНЕРАТОР ШУМА ЛГШ-513	<p>Рабочий диапазон частот, МГц: 0.01 ÷ 1800</p> <p>Диапазон регулировки уровня выходного шумового сигнала, не менее, 20 дБ</p> <p>Показатель электромагнитной совместимости, Рэмс, не менее, 70 м</p> <p>Режим работы: непрерывный, круглосуточный</p>	39 900	Изделие предназначено для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.

		Средняя наработка на отказ, не менее, 1200 часов Напряжение питания (однофазная сеть переменного тока), 187 ÷ 242 В		
--	--	--	--	--

Из списка рассмотренных предлагается выбрать «ГЕНЕРАТОР ШУМА ЛГШ-501» для предотвращения утечек по электромагнитным и электрическим каналам. Выбор оправдан невысокой ценой и широким спектром решаемых задач.

Пассивная защита от утечек по электрическим и электроакустическим каналам предполагает использование сетевых фильтров. Учитывая популярность среди покупателей, был выбран фильтр ФСП-1Ф-7А (Фильтр сетевой помехоподавляющий).

## 5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

Выбранные средства защиты информации включают в себя (табл. 5):

- система акустических и виброакустических помех Буран;
- генератор шума «ЛГШ-501»;
- ФСП-1Ф-7А;
- усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей прокладкой на металлическом каркасе;
- блэкаут-жалюзи.

Таблица 5 – Перечень компонентов инженерно-технической защиты

№	Устройство	Условное обозначение	Цена, руб	Количество	Общая стоимость
1	Модуль дистанционного управления по проводному каналу «Буран-ДУ»		5 000	2	10 000
2	Виброакустический генератор «Буран»		35 000	2	70 000
3	Размыкатель аналоговых телефонных линий "Буран-К1"		3 500	1	3 500
4	Размыкатель линий оповещения и сигнализации "Буран-К2"		3 500	2	7 000
5	Размыкатель компьютерных сетей "Буран-К3"		3 500	2	7 000
6	Генератор шума «ЛГШ-501»		30 000	1	30 000
7	ФСП-1Ф-7А		15 000	4	60 000

8	Усиленные звукоизоляционные двери Phoenix		90 000	6	540 000
9	Вибропреобразователь для стен «Молот» с креплением	МОЛОТ	4 300	6	25 800
10	Преобразователь акустический "Рупор"	РУПОР	2 000	5	10 000
11	Вибропреобразователь для коммуникаций «Серп-Т» с креплением	СЕРП-Т	3 000	5	15 000
12	Блэкаут-жалюзи		1 500	6	7 500
Итого					785 800

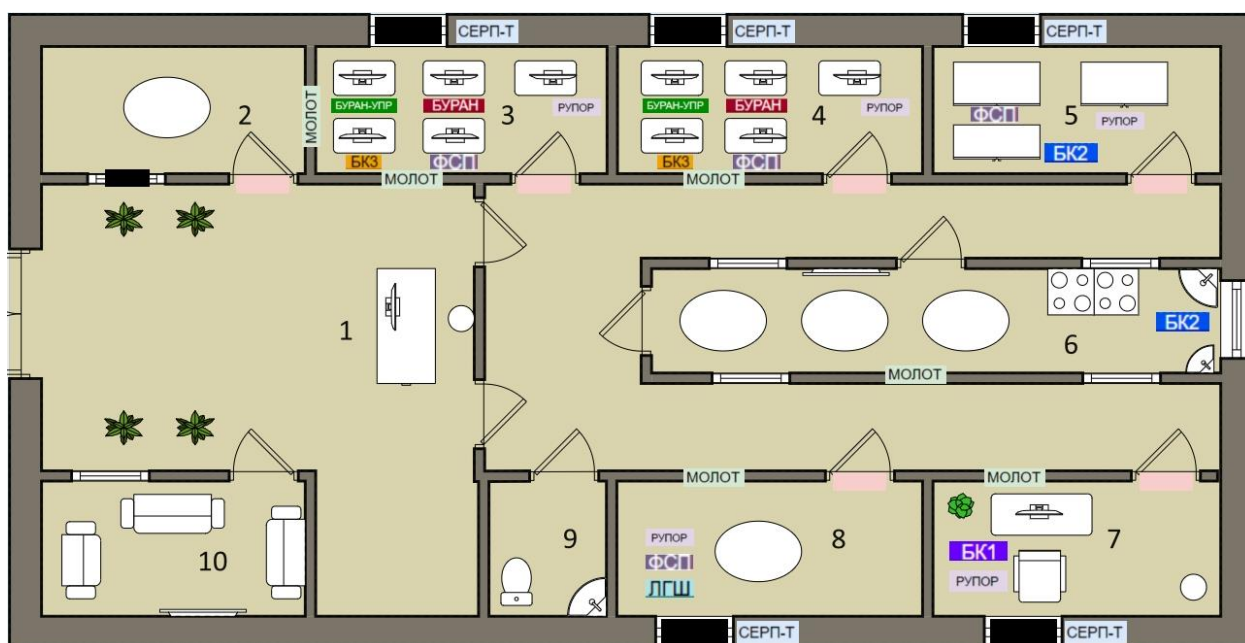


Рисунок 5 – План расстановки СЗИ

## **ЗАКЛЮЧЕНИЕ**

После завершения расследования был проведен анализ технических путей, способствующих утечке информации. В отношении объекта, находящегося под защитой, были тщательно изучены различные технические каналы утечки информации и определены соответствующие превентивные меры. На рынке была проведена оценка действующих механизмов защиты инженерно-технологических данных, результатом которой стал выбор мер защиты, адаптированных к конкретному охраняемому объекту. В последующем было дано разграничение размещения выбранных средств защиты на охраняемом объекте с комплексным расчетом общих затрат на инженерно-техническую защиту информации.

Конечный результат этих усилий материализовался в виде тщательно разработанной системы, направленной на защиту охраняемой информации от несанкционированного распространения по техническим каналам.



## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010. - 436 с.
2. ГЕНЕРАТОР ШУМА ЛГШ-513 – URL: [Генератор шума ЛГШ-513 | Купить \(labpps.ru\)](#)
3. ГЕНЕРАТОР ШУМА ЛГШ-501 – URL: [Генератор шума ЛГШ-501 | Купить \(labpps.ru\)](#)
4. Соната-РС3 Средство активной защиты информации от утечки по сети электропитания и линиям заземления (1 класс) - URL: [Соната-РС3 Средство активной защиты информации от утечки по сети электропитания и линиям заземления \(1 класс\) \(irsural.ru\)](#)
5. Система акустических и виброакустических помех Буран – URL: [Система Буран - система акустических и виброакустических помех \(infosecur.ru\)](#)
6. Генератор акустического шума – URL: [ЛГШ-304, Генератор акустического шума \(kogr.org\)](#)
7. ГЕНЕРАТОР ШУМА ЛГШ-303 – URL: [Генератор шума ЛГШ-303 купить, быстрая доставка, цена - Detector Systems \(detsys.ru\)](#)