

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

**Факультет безопасности информационных технологий**

**КУРСОВАЯ РАБОТА**

**По дисциплине:**

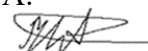
*«Инженерно-технические средства защиты информации»*

**На тему:**

Проектирование системы защиты от утечки информации  
по различным каналам

**Выполнил:**

студент группы N34481  
Гаврилов И.А.



**Проверил:**

к.т.н., доцент ФБИТ  
Попов И.Ю.

**Отметка о выполнении:**

Санкт-Петербург

2023 г.

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

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

<b>Студент</b>	Гаврилов Иван Андреевич (фамилия И.О.)
<b>Факультет</b>	Безопасность Информационных Технологий
<b>Группа</b>	N34481
<b>Направление (специальность)</b>	10.03.01 (Технологии защиты информации 2020)
<b>Руководитель</b>	Попов Илья Юрьевич, к.т.н., доцент ФБИТ (Фамилия И.О., должность, ученое звание, степень)
<b>Дисциплина</b>	Инженерно-технические средства защиты информации
<b>Задание</b>	Разработка комплекса инженерно-технической защиты информации в помещении
<b>Наименование темы</b>	Разработка комплекса инженерно-технической защиты информации в помещении

**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. 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

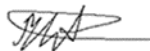
**Рекомендуемая литература**

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

**Руководитель**

(Подпись, дата)

Студент



---

(Подпись, дата)

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

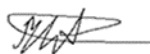
Студент	Гаврилов Иван Андреевич
	(фамилия И.О.)
Факультет	Безопасность Информационных Технологий
Группа	N34481
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении

№ п/п	Наименование этапа	Дата завершения		Оценка и под- пись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	01.10.2023	01.11.2023	
2	Анализ источников	01.11.2023	10.12.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	15.11.2023	15.12.2023	
4	Представление выполненной курсовой работы	05.12.2023	19.12.2023	

Руководитель

(Подпись, дата)

Студент



(Подпись, дата)

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

Студент	Гаврилов Иван Андреевич
	(фамилия И.О.)
Факультет	Безопасность Информационных Технологий
Группа	N34481
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении

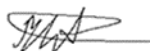
**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РА-  
БОТЫ)**

Цель и задачи работы	Целью работы является повышение защищенности рассматриваемого помещения. Задачами является анализ Защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.
Характер работы	Конструирование
Содержание работы	<ol style="list-style-type: none"><li>1. Введение.</li><li>2. Анализ технических каналов утечки информации.</li><li>3. Руководящие документы</li><li>4. Анализ защищаемых помещений</li><li>5. Анализ рынка технических средств</li><li>6. Описание расстановки технических средств</li><li>7. Заключение</li><li>8. Список литературы</li></ol>
Выводы	В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель

(Подпись, дата)

Студент



(Подпись, дата)

## СОДЕРЖАНИЕ

ВВЕДЕНИЕ .....	8
ОСНОВНАЯ ЧАСТЬ.....	9
1 Анализ защищаемой организации .....	9
1.1 Общее описание.....	9
1.2 Информационные потоки .....	9
1.3 Защищаемое помещение.....	10
1.4. Качественная оценка угроз.....	14
1.4.1. Оптический канал.....	14
1.4.2. Акустический, виброакустический каналы .....	14
1.4.3. Электромагнитный канал.....	14
1.4.4. Закладные устройства .....	14
1.4.5. Материально-вещественный канал.....	14
2. Анализ руководящих документов.....	15
2.1. Перечень руководящих документов .....	15
3. Выбор средств защиты информации .....	16
3.1. Оптический канал.....	16
3.1.1. Шторы.....	16
3.1.2. Доводчики .....	16
3.2. Акустический, виброакустический канал .....	16
3.2.1. Пассивная звукоизоляция .....	16
3.2.2. Излучатели виброакустических помех.....	17
3.3. Электромагнитный канал.....	18
3.3.1. Активная защита от ПЭМИН .....	18
3.3.2. ПЭВМ в защищенном исполнении.....	19
3.4. Защита от закладных устройств.....	21

3.4.1. Обнаружение закладных устройств.....	21
3.4.2. Подавление сигнала закладных устройств.....	23
3.4.2. Подавление микрофонов.....	24
4. Размещение средств защиты .....	26
ЗАКЛЮЧЕНИЕ.....	27
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....	28

## **ВВЕДЕНИЕ**

### **Цель работы**

Повышение защищенности рассматриваемого помещения.

### **Задачи**

- Анализ Защищаемого помещения
- Оценка каналов утечки информации
- Выбор мер пассивной и активной защиты информации



## **ОСНОВНАЯ ЧАСТЬ**

### **1 Анализ защищаемой организации**

#### **1.1 Общее описание**

Наименование организации: ООО “Е-Corp”

Область деятельности: разработки в области ИТ.

Организация работает в режиме B2B — выполняет заказы других организаций на разработку программного обеспечения. За счет объединения людей с творческим подходом в одном рабочем пространстве организация получает преимущество в разработке новых решений.

Руководством организации было принято решение расширить бизнес в сторону B2G разработок. В частности, связанных со сведениями, составляющими государственную тайну уровня “секретно”. Как следствие, необходимо оборудовать арендованное офисное помещение техническими средствами защиты информации.

#### **1.2 Информационные потоки**

Разработка разбита на небольшие группы, каждая из которых работает над отдельным проектом. Заказчик и проектная группа общаются через посредников из отдела продаж - специалистов по связям. Таким образом уменьшается распространенность сведений конфиденциального характера и улучшается взаимопонимание.

Кроме непосредственно разработки имеются: отдел информационной безопасности, инфраструктурный отдел, отдел HR, финансовый отдел.

Большая часть отделов не имеет доступа к государственной тайне - с ней работают отдел продаж, группы разработки и отдел информационной безопасности.

Кроме заказчиков, организация взаимодействует с банком, налоговой, пенсионным фондом, военкоматом и прочими организациями.

Организационная структура предприятия представлена на рисунке 1. Схема информационных потоков представлена на рисунке 2. Красным выделены потоки, по которым передаются сведения, составляющие государственную тайну.

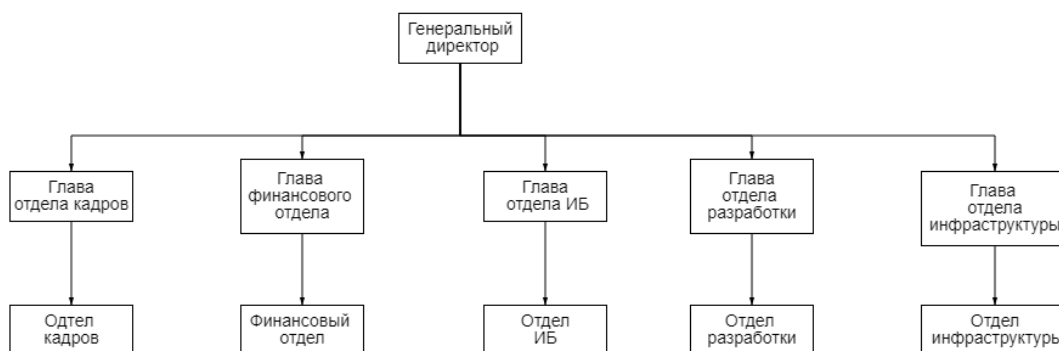


Рисунок 1 – Организационная структура предприятия

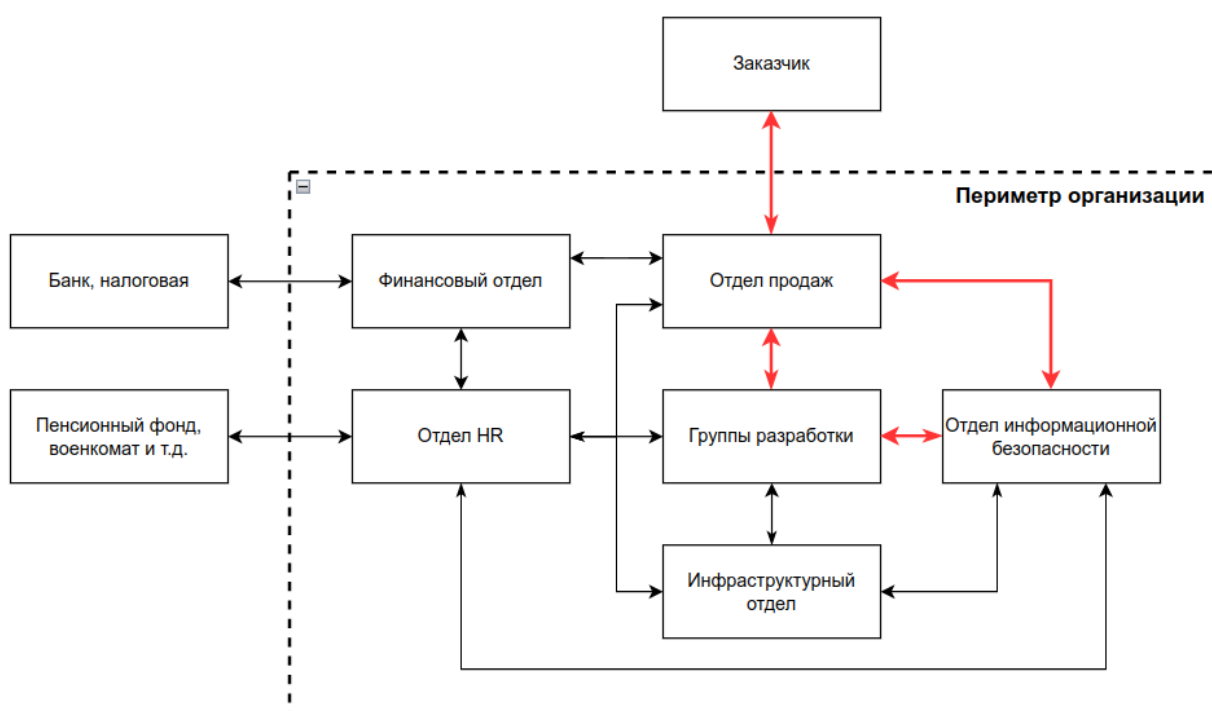


Рисунок 2 - Схема информационных потоков в организации

### 1.3 Защищаемое помещение

Офис организации, в котором планируется вести работу с государственной тайной, расположен на третьем этаже 7-этажного офисного здания. На северной стене расположены окна, выходящие на улицу. Напротив расположены другие офисные здания. На западной и восточной стене расположены окна, выходящие на далеко стоящие здания (20 метров). На южной стене расположены окна, выходящие на офисные здания. Над и под защищаемым помещением также расположены арендуемые офисы. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

Доступы 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.

Арендуемое помещение состоит из:

- Внутреннего коридора;
- Склада;
- Туалетов;
- Комнаты системных администраторов;
- Серверной;
- Переговорной;
- Open-space зоны;
- Зала для презентаций.

Основная работа со сведениями, составляющими государственную тайну будет осуществляться в комнате для ведения закрытых разработок. Также время от времени в переговорной будут проводиться совещания, связанные с данными разработками.

На рисунке 3 представлен план защищаемого помещения. На рисунке 4 приведено описание элементов, изображенных на плане. Список комнат и их площадь приведены в таблице 1.



Рисунок 3 - План помещения



Рисунок 4 - Описание элементов, изображенных на плане

Таблица 1 - Комнаты на плане

Номер	Название	Площадь, м <sup>2</sup>
1	Внутренний коридор	43
2	Лестница	10
3	Туалеты	8x2
4	HR-отдел	9
5	Финансовый отдел	14
6	Комната секретной разработки	15
7	Переговорная	15
8	Зал для презентаций	35
9	Оpen-spase	38
10	Серверная	10
11	Лифты	15

Внутренний коридор не содержит какой-либо мебели. Имеется только два выхода вентиляции.

В каждом туалете имеется унитаз, раковина и мусорное ведро.

В серверной находятся две серверных стойки, две розетки, выход вентиляции. Серверная отделена от зоны open-spase стеной и дверью.

Переговорная содержит четыре розетки, маркерную доску, кресла, выход вентиляции, проектор.

Зона open-spase содержит шесть розеток, восемь рабочих мест, шесть шкафов для оборудования и документов, диван, растение в горшке, три окна с батареями отопления, два выхода вентиляции.

В комнате для ведения закрытых разработок расположены четыре розетки, два шкафа для оборудования и документов, четыре рабочих мест, окно с батареей отопления, выход вентиляции. В ней же сидит директор.

HR-отдел содержит одно рабочее место, сейф, два шкафа, розетка, выход вентиляции.

Финансовый отдел содержит три рабочих места, три розетки, сейф, выход вентиляции.

## **1.4. Качественная оценка угроз**

### **1.4.1. Оптический канал**

Возможен частичный просмотр помещения со стороны улицы. Возможен просмотр помещения из соседних зданий с использованием оптических приборов.

### **1.4.2. Акустический, виброакустический каналы**

Помещение расположено на третьем этаже напротив высотного здания. Окна выходят на улицу. Возможно прослушивание со стороны улицы или соседнего дома с использованием направленных микрофонов. Возможен съем речевой информации с оконных стекол с помощью лазера.

Во всех комнатах, где идёт работа с секретными сведениями, имеется вентиляция. Возможно прослушивание через вентиляцию с использованием стетоскопов, спускаемых микрофонов.

В комнате, где ведутся закрытые разработки, имеются батареи отопления. Возможно прослушивание через систему отопления с использованием стетоскопов.

### **1.4.3. Электромагнитный канал**

В каждой комнате имеются розетки. Возможен съем информации через систему электропитания.

Из проводных каналов связи за пределы помещения выходит только ethernet-кабель общего шлюза. Возможны съем и навязывание информации на этом канале связи.

Работа с секретными сведениями ведется с использованием компьютеров. Возможно прослушивание паразитных электромагнитных полей с последующим восстановлением из них информации.

### **1.4.4. Закладные устройства**

В помещении имеется множество мест, где можно спрятать закладное устройство: цветочные горшки, шкафы и полки с оборудованием, мусорные корзины.

Возможно размещение закладных устройств в стенах, либо их маскировка под розетки, светильники, выключатели.

### **1.4.5. Материально-вещественный канал**

Материально-вещественный канал утечки информации может присутствовать. В рамках курсовой работы данный канал не рассматривается.

## **2. Анализ руководящих документов**

### **2.1. Перечень руководящих документов**

При разработке комплекса защиты информации будем руководствоваться следующими документами:

- Закон “О государственной тайне”;
- Федеральный Закон №149 - “Об информации, информационных технологиях и защите информации”;
- Указ Президента РФ от 30.11.1995 №1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне";
- Постановление Правительства РФ от 15 апреля 1995 г. №333 “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 06.02.2010 N 63 (ред. от 29.10.2022) "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне";
- Постановление Правительства РФ от 26 июня 1995 г, №608 “О сертификации средств защиты информации”;
- 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 27033-2011 “Безопасность сетей”.

### **2.2. Требования к составу мер защиты**

Для получения лицензии на работу с государственной тайной степени “секретно” необходимо выполнить следующие требования:

- 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;
- Все режимные помещения оборудуются аварийным освещением;
- Вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.

### 3. Выбор средств защиты информации

#### 3.1. Оптический канал

##### 3.1.1. Шторы

В качестве средства защиты информации от утечек по оптическому каналу через окна достаточно использовать любые доступные на рынке плотные офисные шторы. В таблице 2 представлен расчет стоимости решения.

Таблица 2 - Расчет стоимости установки штор

Наименование товара / работы / услуги	Количество, шт.	Цена, руб.	Сумма, руб.
Рулонные жалюзи блэкаут для офиса	10	1999	19990
Установка	1	3 000	3 000
ИТОГО			22 990

##### 3.1.2. Доводчики

Для защиты от утечек по оптическому каналу через двери используются доводчики. В таблице 3 представлен расчет стоимости.

Таблица 3 - Расчет стоимости установки доводчиков

Наименование товара / работы / услуги	Количество, шт.	Цена, руб.	Сумма, руб.
Доводчик дверной ISP 430	13	1 651	21 463
Установка	1	3 000	3 000
ИТОГО			24 463

#### 3.2. Акустический, виброакустический канал

##### 3.2.1. Пассивная звукоизоляция

Многие компании предлагают услугу отделки помещения пассивной звукоизоляцией. Цена зависит от площади комнат и высоты потолков. Пассивная звукоизоляция необходима в двух помещениях - комнате для ведения закрытых разработок и переговорной. Расчет стоимости представлен в таблице 4.



Таблица 4 - Расчет стоимости пассивной звукоизоляции

Наименование	Площадь, м <sup>2</sup>	Цена, руб./м <sup>2</sup>	Сумма, руб.
Система звукоизоляции пола (плавающая стяжка) «Стандарт 1»	30	1 140	34 200
Каркасная система звуко-изоляции потолка «Базовая»	30	4 780	143 400
Каркасная система звуко-изоляции стен «Базовая»	83	4 245	352 335
Наименование	Количество, шт.	Цена, руб.	Сумма, руб.
Дверь звукоизоляционная Rw 42dB Prima M900	2	34 050	68 100
ИТОГО			598 035

### 3.2.2. Излучатели виброакустических помех

В таблице 5 приведено сравнение вариантов излучателей виброакустических помех. Стоимость указана с учетом комплектации, необходимой для защиты двух помещений.

Таблица 5 - Сравнение излучателей виброакустических помех

Наименование	Возможности	Стоимость, руб.
ЛГШ-404	<ul style="list-style-type: none"> <li>Учет времени работы</li> <li>Контроль и защита органов регулировки уровня выходного шумового сигнала</li> <li>Проводное дистанционное управление и контроль</li> <li>Диапазон частот: 175 - 11 200 Гц</li> <li>Круглосуточная непрерывная работа</li> <li>Средний срок службы: 7 лет</li> </ul>	136 000
БАРОН	<ul style="list-style-type: none"> <li>4 канала формирования помех</li> <li>Возможность беспроводного дистанционного включения комплекса</li> <li>Полностью цифровое управление</li> <li>Интеллектуальный интерфейс</li> <li>Возможность подключения к каждому выходному каналу различных типов вибро- и акустических излучателей и их комбинаций за счет наличия низкоомного и высокоомного выходов.</li> </ul>	62 500
SI-3002	<ul style="list-style-type: none"> <li>Автоматическое программирование</li> </ul>	29 000

	<p>уровня шума анализатором SI-4000</p> <ul style="list-style-type: none"> <li>• Возможность подключения акустических, электромагнитных, керамических излучателей</li> <li>• Сохранение запрограммированного уровня шума в энергонезависимой памяти прибора</li> </ul>	
--	--	--

Был сделан выбор в пользу “ЛГШ-404”. У него имеется возможность гибкой настройки силы помех, что может быть критичным при использовании системы вблизи помещений, контролируемых другими организациями. Также присутствие встроенного анализатора акустической обстановки будет очень полезным при настройке оборудования.

### 3.3. Электромагнитный канал

#### 3.3.1. Активная защита от ПЭМИН

В таблице 6 приведено сравнение средств активной защиты от ПЭМИН. Стоимость указана с учетом комплектации, необходимой для защиты двух помещений.

Таблица 6 - Сравнение средств активной защиты от ПЭМИН

Наименование	Возможности	Стоимость, руб.
ГЕНЕРАТОР ШУМА ЛГШ-501	<ul style="list-style-type: none"> <li>• Оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима</li> <li>• Оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех</li> <li>• Обеспечивает защиту органов регулирования уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним</li> <li>• Имеет возможность подключения проводного пульта дистанционного управления</li> </ul>	2 * 33 000
БАЗОВЫЙ ГЕНЕРАТОР МАСКИРУЮЩИХ РАДИОПОМЕХ ГШ-111Б	<ul style="list-style-type: none"> <li>• Интерфейс для управления и контроля ГШ по сети Ethernet 10/100 Мбит/с</li> <li>• Систему управления и индикации (плечная клавиатура, ЖКИ-индикатор и светодиоды)</li> <li>• Модуль питания генератора + 12В / 1,5 А с устройством наведения сигнала на цепи электропитания и заземления НС-111</li> </ul>	2 * 33 000

	<ul style="list-style-type: none"> <li>● На задней панели генератора расположены отдельные выходы для подключения магнитной и радиочастотных антенн, а также выход на внешнее устройство наведения шумового сигнала на провода</li> </ul>	
Гамма-ГШ18	<ul style="list-style-type: none"> <li>● Учет времени работы</li> <li>● Защита от несанкционированного изменения настроек</li> <li>● Время непрерывной работы: не ограничено</li> <li>● Срок службы: от 10 лет</li> <li>● Гарантия: 3 года</li> </ul>	2 * 29 400

По результатам сравнения был выбран “ЛГШ-501” по причине больших возможностей по настройке, эффективности и защиты от несанкционированного изменения настроек.

### **3.3.2. ПЭВМ в защищенном исполнении**

В таблице 7 приведено сравнение комплексов ПЭВМ. Стоимость указана с расчетом на 5 рабочих мест, которые необходимо обеспечить для ведения закрытых разработок.

Таблица 7 - Сравнение комплексов ПЭВМ

Наименование	Возможности	Стоимость, руб.
ПЕРСОНАЛЬ- НЫЙ КОМПЬ- ЮТЕР НА CORE-I3	<ul style="list-style-type: none"> <li>● Процессор: intel i3 от 3.3 ГГц</li> <li>● Память: 8 GB</li> <li>● Жесткий диск: 256 Gb</li> <li>● Операционная система: Windows 10 / Astra Linux SE</li> <li>● МДЗ: ПАК «Соболь 4» / Dallas Lock</li> <li>● СЗИ от НСД: Secret net Studio 8 / Dallas Lock</li> <li>● Антивирус (ФСТЭК): Dr.web</li> <li>● Идентификатор: iButton/JaCarta/Guardant</li> <li>● Монитор: 23.8"</li> <li>● Клавиатура: Проводная</li> <li>● Мышь: Проводная</li> </ul>	4 * 229 000
ПЕРСОНАЛЬ- НЫЙ КОМПЬ- ЮТЕР НА CORE-I5	<ul style="list-style-type: none"> <li>● Процессор: intel i5 2.90ГГц</li> <li>● Память: 16 GB</li> <li>● Жесткий диск: SSD 480 Gb</li> <li>● Операционная система: Windows 10 / Astrs Linux SE</li> <li>● МДЗ: ПАК «Соболь 4» / Dallas Lock</li> <li>● СЗИ от НСД: Secret net Studio 8 / Dallas Lock</li> <li>● Антивирус (ФСТЭК): Dr.web</li> <li>● Идентификатор: iButton/JaCarta/Guardant</li> <li>● Монитор: Dell 23.8"</li> <li>● Клавиатура: Проводная</li> <li>● Мышь: Проводная</li> </ul>	4 * 239 000
ПЕРСОНАЛЬ- НЫЙ КОМПЬ- ЮТЕР НА CORE-I7	<ul style="list-style-type: none"> <li>● Процессор: intel i7 2.90ГГц</li> <li>● Память: 32 GB</li> <li>● Жесткий диск: SSD 960 Gb</li> <li>● Операционная система: Windows 10 / Astrs Linux SE</li> <li>● МДЗ: ПАК «Соболь 4» / Dallas Lock</li> <li>● СЗИ от НСД: Secret net Studio 8 / Dallas Lock</li> <li>● Антивирус (ФСТЭК): Dr.web</li> <li>● Идентификатор: iButton/JaCarta/Guardant</li> <li>● Монитор: Dell 23.8"</li> <li>● Клавиатура: Проводная</li> <li>● Мышь: Проводная</li> </ul>	4* 254 000

На данный момент единственным подходящим для ведения современной разработки ПЭВМ является “ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР НА CORE-I7”. Будем использовать его.

### 3.4. Защита от закладных устройств

#### 3.4.1. Обнаружение закладных устройств

В таблице 8 приведено сравнение комплексов для обнаружения закладных устройств. Стоимость указана с учетом полной необходимой комплектации.

Таблица 8 - Сравнение комплексов для обнаружения закладных устройств

Наименование	Возможности	Стоимость, руб.
Крона-M12	<ul style="list-style-type: none"><li>● Сверхвысокая скорость сканирования – до 25 ГГц/сек</li><li>● Малые габариты и вес – выполнено в едином компактном экранированном корпусе</li><li>● Встроенные аккумуляторы обеспечивают автономную работу до 4 часов</li><li>● Режим «Водопад» позволяет оценить изменения с течением времени и обнаружить даже замаскированные сигналы</li><li>● Оснащается комплектом для обследования проводных линий и ИК диапазона</li><li>● Мультисенсорный дисплей позволяет управлять комплексом без дополнительных устройств ввода</li><li>● Возможно подключение клавиатуры и мыши для стационарной работы</li></ul>	1 980 000
СПЕКТР-ЭКС-ПРЕСС	<ul style="list-style-type: none"><li>● Комплекс использует до четырех пространственно разнесенных антенн для поиска, оценки параметров, идентификации и локализации источников радиоизлучений в частотном диапазоне 10-6000 МГц.</li><li>● Автоматический конвертор проводных линий комплекса «Спектр-Экспресс» обеспечивает обнаружение сигналов от «сетевых» микрофонов в различных проводных линиях, а подключение ИК-датчика позволяет выявлять устройства негласного съема информации, работающие в инфракрасном диапазоне.</li><li>● Скорость панорамного обзора в одноканальной конфигурации составляет до 1150 МГц/с при разрешении по частоте 2 кГц.</li><li>● Высокая производительность дает возможность комплексу обнаруживать сигналы от радиомикрофонов, работающих в режиме накопления информации и кратковременной передачи её в эфир.</li><li>● Обнаружение и различение сигналов выполняется цифровым параллельным анализатором спектра с разрешением 2 кГц.</li></ul>	1 350 000

	<p>Высокое разрешение цифрового анализатора спектра позволяет различать и обнаруживать узкополосные сигналы от радиомикрофонов, работающих рядом с легальными радиосредствами.</p> <ul style="list-style-type: none"> <li>● Специализированное программное обеспечение комплекса позволяет обнаруживать и идентифицировать сигналы от различных типов устройств негласного съема информации, в том числе использующих цифровые виды модуляции, шумоподобную структуру, режим псевдослучайной или программной перестройки рабочей частоты, сверхкоротких посылок (СКП) и т.д.</li> <li>● С помощью встроенной системы видеозахвата комплекс «Спектр-Экспресс» выводит на сенсорный дисплей протектированное изображение от скрытых беспроводных видеокамер.</li> </ul>	
Крона-М6	<ul style="list-style-type: none"> <li>● Исследование электромагнитной обстановки.</li> <li>● Радиомониторинг и поиск несанкционированных источников излучения и скрытых устройств.</li> <li>● Измерение уровней базовых станций и точек доступа.</li> <li>● Контроль работы аппаратуры подавления сотовой связи и беспроводного доступа внутри заданной зоны.</li> <li>● Обнаружение сверхкратковременных радиосигналов и сигналов с псевдослучайной перестройкой рабочей частоты (ППРЧ).</li> <li>● Непрерывное накопление спектра сигнала, что позволяет быстро обнаруживать широкополосные шумоподобные сигналы (ШПС).</li> <li>● Накопление фоновой панорамы.</li> <li>● Радиомониторинг на фоне заранее заготовленной эталонной панорамы.</li> <li>● Составление списков обнаруженных сигналов.</li> <li>● Работа в автономном режиме с выполнением установленных заданий.</li> </ul>	1 360 000

Был выбран комплекс “СПЕКТР-ЭКСПРЕСС” как наиболее multifunctional-ный.

### 3.4.2. Подавление сигнала закладных устройств

В таблице 9 представлено сравнение средств подавления сигналов закладных устройств.

Таблица 9 - Сравнение средств подавления сигналов закладных устройств

Наименование	Возможности	Стоимость, руб.
Подавитель "UltraSonic-ШАЙБА-50-GSM"	<ul style="list-style-type: none"><li>● Круговое распространение ультразвуковых помех на 360 градусов. Благодаря распространению ультразвукового излучения во все стороны достигается максимальный эффект защиты от аудиозаписи.</li><li>● Ультразвуковая помеха. Подавитель оснащен 48 ультразвуковыми излучателями, которые напрямую воздействуют на мембрану микрофона записывающего устройства, что не позволяет произвести запись разговора.</li><li>● Блокировка 10-ти частот беспроводной связи. Встроенный радиочастотный подавитель блокирует любую передачу данных через сотовую связь и мобильный интернет в радиусе до 15 метров.</li></ul>	52 000
ЛГШ-725	<ul style="list-style-type: none"><li>● Блокировка сотовой связи, Bluetooth, WiFi 2.4 и 5 ГГц</li><li>● Независимая регулировка мощности по каждому диапазону</li><li>● Дистанционное управление</li><li>● Время постоянной работы: не ограничено</li><li>● Срок службы: 10 лет</li></ul>	142 025
Блокиратор "Завеса-12СТН"	<p>Блокируемые стандарты сотовой связи:</p> <ul style="list-style-type: none"><li>● GSM 900 / 1800; E-GSM;</li><li>● 3G; 3G+;</li><li>● 4G+; 4G-LTE; 4G-LTE 800;</li><li>● DECT;</li><li>● UMTS;</li><li>● WCDMA.</li></ul> <p>Особенности:</p> <ul style="list-style-type: none"><li>● Блокиратор подавляет 14 стандартов связи, которые используются с целью организации каналов утечки информации, спутниковым слежением за автомобилями и грузами, имеет высокую выходную мощность и рассчитан на круглосуточную эксплуатацию.</li><li>● Блокиратор оснащен защищенными от</li></ul>	111 409

	<p>внешних воздействий, встроенными в корпус высокоэффективными малогабаритными антеннами.</p> <ul style="list-style-type: none"> <li>• Блокиратор рассчитан на работу от бортовой сети автомобиля (12 Вольт) или на работу от сети 220 Вольт.</li> <li>• Завеса12 СТН имеет профессиональную надежность и рассчитана на непрерывную длительную работу. Допускается круглосуточная эксплуатация блокиратора при соблюдении мер температурного режима и вентиляции. Гарантийный срок эксплуатации 1 год.</li> </ul>	
--	--	--

Было выбрано средство подавления сигналов “ЛГШ-725” - независимая настройка мощности по каждому диапазону важна при использовании системы вблизи помещений, контролируемых другими организациями.

### **3.4.2. Подавление микрофонов**

В таблице 10 представлено сравнение средств подавления микрофонов.



Таблица 10 - Сравнение средств подавления микрофонов

Наименование	Возможности	Стоимость, руб.
Бубен-Ультра	<ul style="list-style-type: none"> <li>• Три типа помех: ультразвуковой диапазон, сложная звуковая помеха, речеподобная помеха</li> <li>• Возможность автономной работы: до 6 часов</li> <li>• Радиус подавления: до 5 м</li> <li>• Различные варианты маскировки</li> </ul>	2*48 000
ULTRASONIC-SPYLINE-24-LIGHT	<ul style="list-style-type: none"> <li>• Бесшумная работа. Блокиратор крепится под столом для переговоров при помощи специально предусмотренного крепления так, что заметить его совершенно невозможно.</li> <li>• Направленная запись. Записывать диалог будет доступно только вам, так как звукозаписывающие датчики направляются в сторону оппонентов.</li> <li>• Блокировка за счет ультразвуковых частот. Гаджет оснащен 22 встроенными ультразвуковыми излучателями, благодаря которым можно заблокировать любую запись на диктофон в радиусе десяти метров.</li> </ul>	2*24 800
КАНОНИР-К7	<ul style="list-style-type: none"> <li>• Использует сразу 2 способа защиты от прослушки, поэтому гарантированно блокирует любые акустические устройства съема информации. Подавление происходит с помощью генерации звуковой речеподобной помехи и ультразвука</li> <li>• Не мешает общению собеседников, так как ультразвук не слышим человеческим ухом, а громкость речеподобной помехи можно настроить</li> <li>• Кроме встроенного динамика имеет выход на колонки, что позволяет защититься даже от лазерных микрофонов</li> <li>• Работает как от электросети, так и от аккумулятора, поэтому подходит не только для стационарного использования в помещениях, где есть доступ к розетке, но и в любом нужном вам месте</li> <li>• Радиус до 4 метров</li> </ul>	3* 37 000

Был сделан выбор в пользу средства “ ULTRASONIC-SPYLINE-24-LIGHT ” по причине его незаметности и радиуса действия.

#### 4. Размещение средств защиты

На рисунке 5 изображены условные обозначения устанавливаемого оборудования.

На рисунке 6 приведен план размещения оборудования.

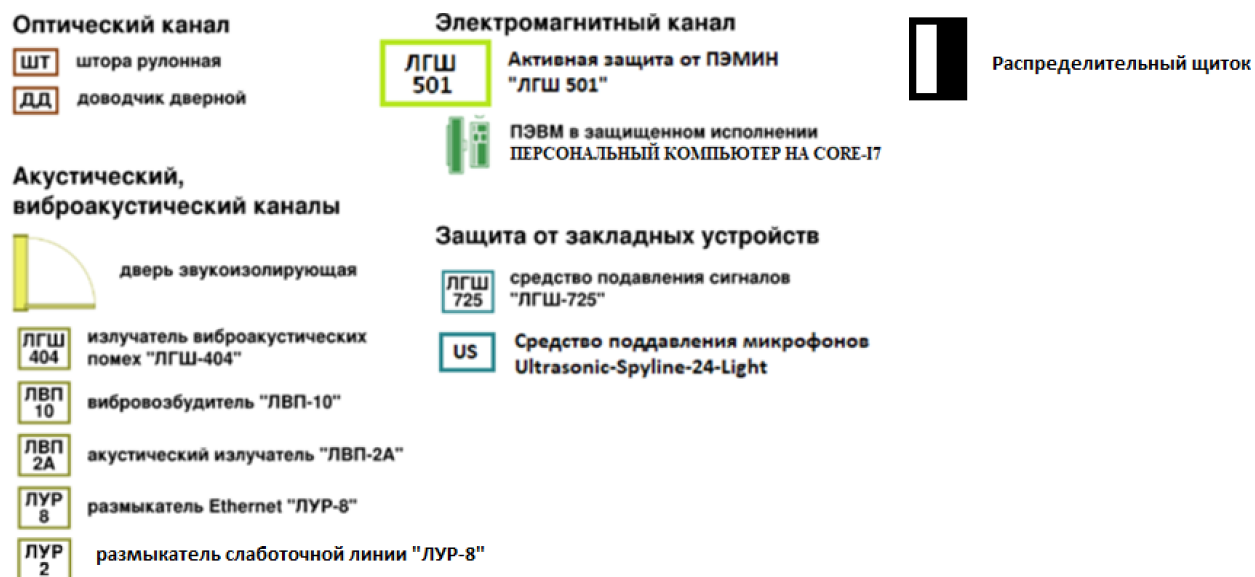


Рисунок 5 - условные обозначения технических средств защиты информации



Рисунок 6 - план размещения технических средств защиты информации

## **ЗАКЛЮЧЕНИЕ**

В ходе данной работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении и описаны необходимые меры их защиты. Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для нашего объекта. Был разработан план установки и произведен расчет стоимости предложенных активных и пассивных средств защиты информации.

В результате была предложена защита от утечек информации по оптическому, акустическому, виброакустическому, электромагнитному каналам, обеспечена защита от ПЭМИН.

Итоговая цена системы защиты информации составляет 3 348 113 рублей.

## **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Кармановский Н.С., Михайличенко О.В., Савков С.В.. Организационно-правовое и методическое обеспечение информационной безопасности. Учебное пособие – Санкт-Петербург: НИУ ИТМО, 2013. - 151 с. – экз.