

**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
Щукин А.И.

_____ 

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

Студент	Щукин Александр Иванович (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
Задание	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 Щукин Александр Иванович

(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 подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	01.10.2023		
2	Анализ источников	01.11.2023		
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	15.11.2023		
4	Представление выполненной курсовой работы	01.12.2023		

Руководитель

(Подпись, дата)

Студент




(Подпись, дата)

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

Студент	Щукин Александр Иванович (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
(РАБОТЫ)**

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	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
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.....	6
ОСНОВНАЯ ЧАСТЬ.....	7
1 Анализ защищаемой организации.....	7
1.1 Общее описание.....	7
1.2 Информационные потоки.....	7
1.3 Защищаемое помещение.....	8
1.4. Качественная оценка угроз.....	13
1.4.1. Оптический канал.....	13
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.....	14
2.1. Перечень руководящих документов.....	14
2.2. Требования к составу мер защиты.....	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. Пассивная защита от ПЭМИН.....	18
3.3.2. Активная защита от ПЭМИН.....	18
3.3.3. ПЭВМ в защищенном исполнении.....	19
3.4. Защита от закладных устройств.....	20
3.4.1. Обнаружение закладных устройств.....	20
3.4.2. Подавление сигнала закладных устройств.....	21
3.4.2. Подавление микрофонов.....	21
4. Размещение средств защиты.....	22
ЗАКЛЮЧЕНИЕ.....	24
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	25

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 “АрхФеникс”.

Область деятельности: экспериментальные 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.

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

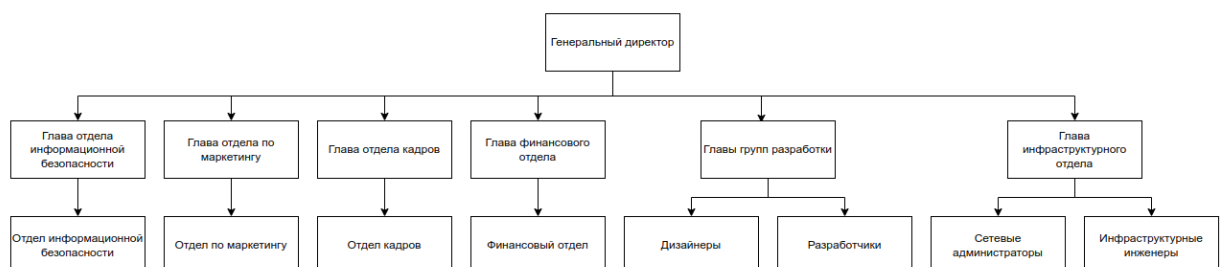


Рисунок 1 - Иерархическая структура организации

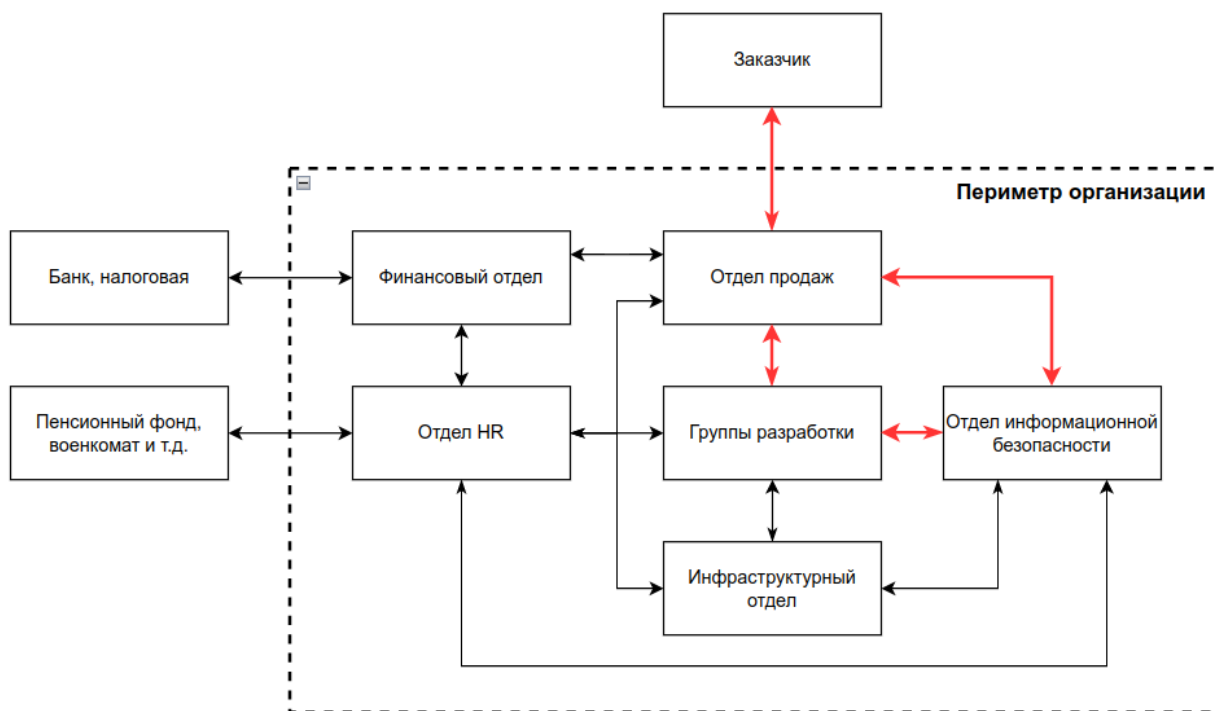


Рисунок 2 - Схема информационных потоков в организации

1.3 Защищаемое помещение

Офис организации, в котором планируется вести работу с государственной тайной, расположен на третьем этаже 21-этажного офисного здания. На северной стене расположены окна, выходящие на улицу. Напротив расположены другие офисные здания. Западная и восточная стены граничат с другими арендуемыми офисами. Южная стена связывает офис с техническими помещениями. Над и под защищаемым помещением также расположены арендуемые офисы. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

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

Арендуемое помещение состоит из:

- Внутреннего коридора,
- Склада,
- Туалетов,
- Комнаты системных администраторов,
- Серверной,
- Переговорной,

- Open-space зоны,
- Комнаты для ведения закрытых разработок.

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.

Наглядная модель помещения представлена на рисунках 3-7.

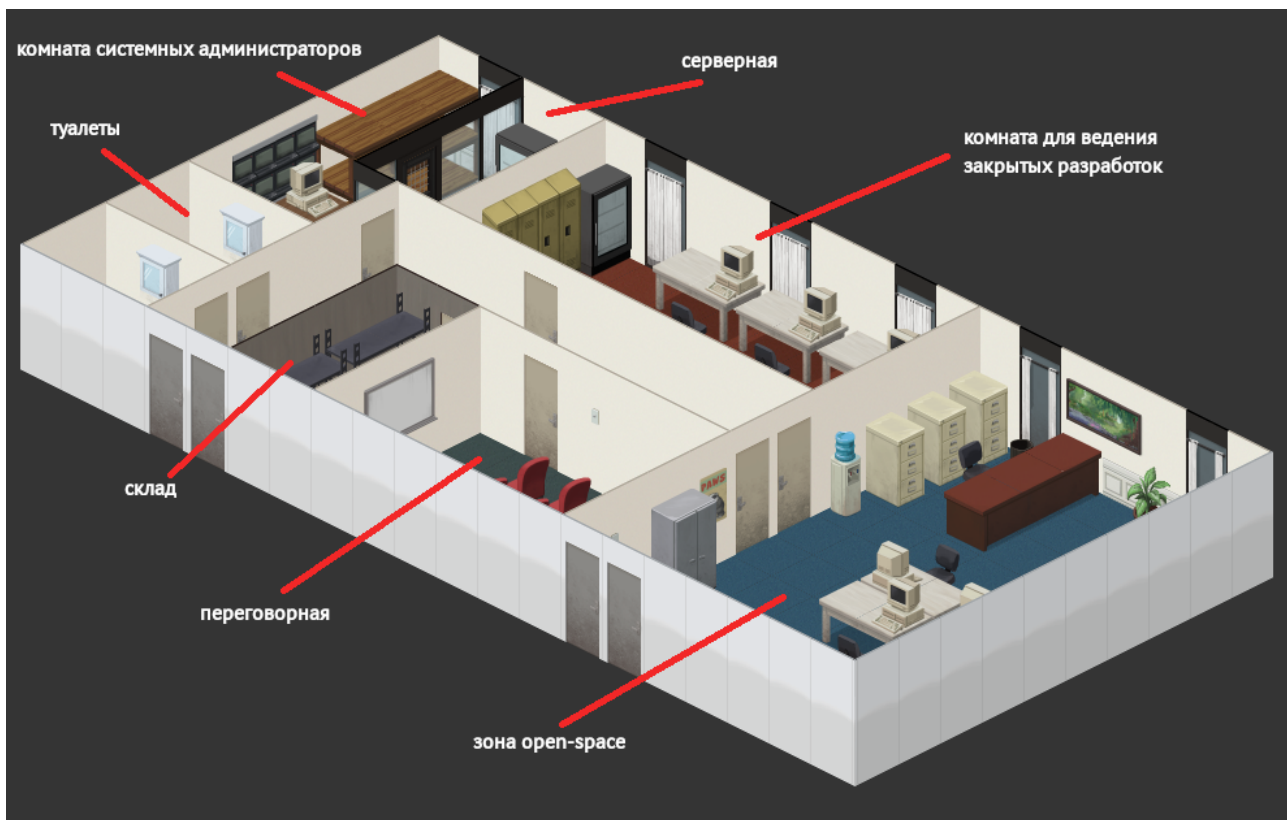


Рисунок 3 - Модель защищаемого помещения



Рисунок 4 - Модель зоны open-space

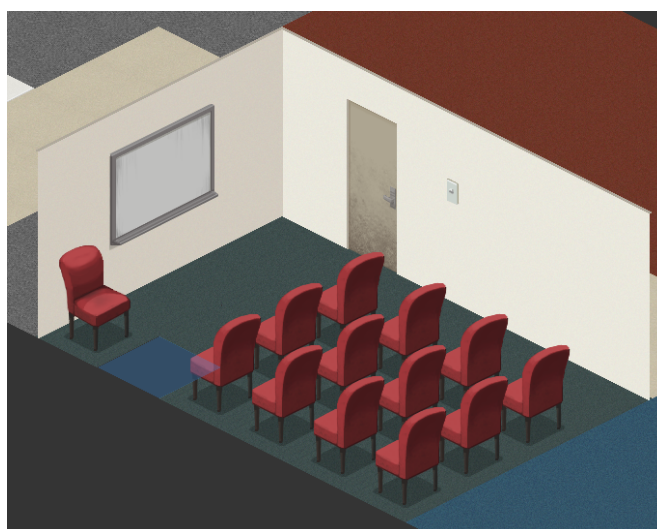


Рисунок 5 - Модель переговорной



Рисунок 6 - Модель комнаты системных администраторов



Рисунок 7 - Модель комнаты для ведения закрытых разработок

На рисунке 8 представлен план защищаемого помещения. На рисунке 9 приведено описание элементов, изображенных на плане. Список комнат и их площадь приведены в таблице 1.

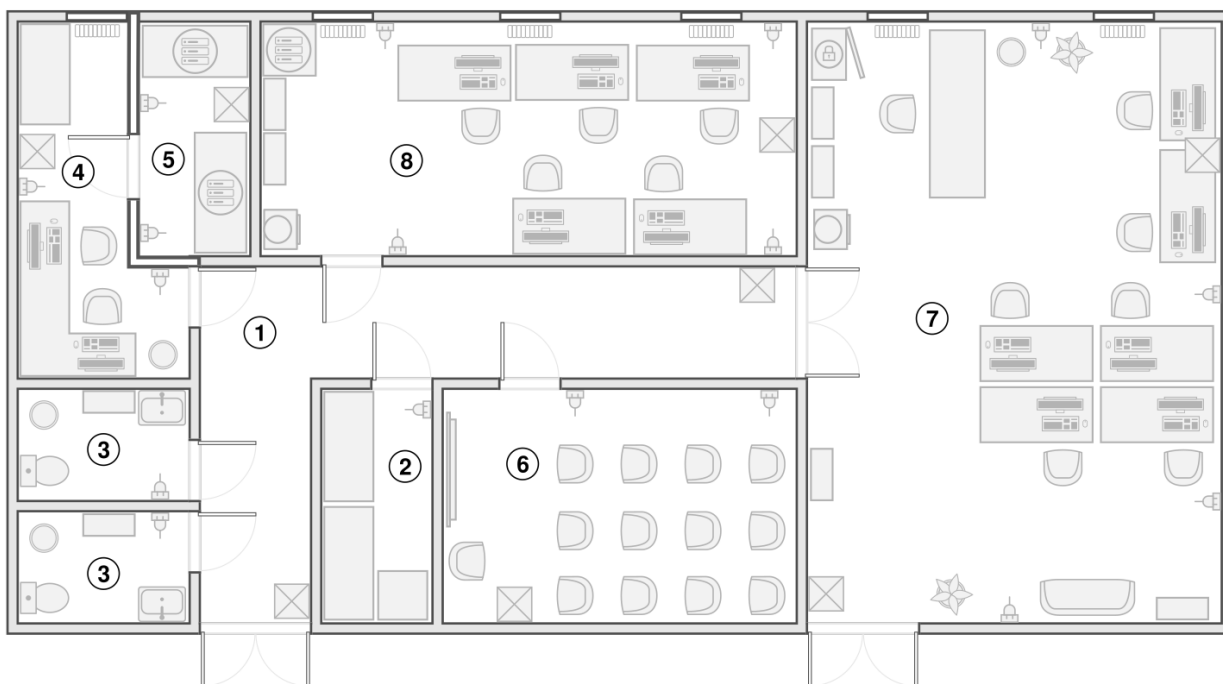


Рисунок 8 - План помещения



Рисунок 9 - Описание элементов, изображенных на плане

Таблица 1 - Комнаты на плане

Номер	Название	Площадь, м ²
1	Внутренний коридор	18
2	Склад	5
3	Туалеты	8
4	Комната администраторов	4
5	Серверная	5
6	Переговорная	9
7	Зона open-space	45
8	Комната для ведения закрытых разработок	23

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

На складе расположено несколько полок и коробки с различным оборудованием и материалами.

В каждом туалете имеется унитаз, раковина, мусорное ведро, шкаф и розетка.

В комнате администраторов находятся два рабочих места, столы и полки для хранения оборудования, мусорное ведро и две розетки, окно с батареей отопления, выход вентиляции.

В серверной находятся две серверных стойки, две розетки, выход вентиляции. Серверная отделена от комнаты администраторов стеклянной стеной и дверью.

Переговорная содержит две розетки, маркерную доску, кресла, выход вентиляции.

Зона open-space содержит четыре розетки, семь рабочих мест, сейф для документов, три шкафа для оборудования и документов, кулер, холодильник, диван, мусорное ведро, два растения в горшках, два окна с батареями отопления, два выхода вентиляции.

В комнате для ведения закрытых разработок расположены четыре розетки, серверная стойка, два шкафа для оборудования и документов, кулер, пять рабочих мест, три окна с батареями отопления, 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, восстановление 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.
Рулонная штора “Blackout”	6	900	5 400
Установка	1	2 000	2 000
ИТОГО			7 400

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 “БУЛАТ ULTIMATE”	13	1 300	16 900
Установка	1	3 000	3 000
ИТОГО			19 900

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 ²	Цена, руб./м ²	Сумма, руб.
Звукоизоляция пола с установкой	32	4 500	144 000
Звукоизоляция потолка с отделкой	32	3 700	118 400
Звукоизоляция стен с отделкой	116	4 100	475 600
Наименование	Количество, шт.	Цена, руб.	Сумма, руб.
Звукоизолирующие двери с установкой	2	60 000	120 000
ИТОГО			858 000

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"> – учет времени работы; – контроль и защита органов регулировки уровня выходного шумового сигнала; – проводное дистанционное управление и контроль; – диапазон частот: 175 - 11 200 Гц; – круглосуточная непрерывная работа; – средний срок службы: 7 лет. 	136 000
КАМЕРТОН-5	<ul style="list-style-type: none"> – диапазон частот: 90 - 11 200 Гц; – круглосуточная непрерывная работа. 	92 000
Буран	<ul style="list-style-type: none"> – частотная коррекция спектра помехового сигнала; – мониторинг уровня нагрузки каналов; – учет времени работы; – защита от несанкционированного изменения настроек; – диапазон частот: 100 - 11 200 Гц; – непрерывная работа до 24 часов. 	89 800

Был сделан выбор в пользу ЛГШ-404. У него имеется возможность регулировки уровня шумового сигнала, что может быть критичным при использовании системы вблизи помещений, контролируемых другими организациями.

3.3. Электромагнитный канал

3.3.1. Пассивная защита от ПЭМИН

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

Наименование	Возможности	Стоимость, руб.
ЛФС-10-1Ф	<ul style="list-style-type: none"> – До 10 А тока – Срок службы: 7 лет 	6 * 47 100
ФП-6	<ul style="list-style-type: none"> – До 20 А тока – Срок службы: 5 лет – Гарантия: 1 год 	6 * 55 556
СОНАТА-ФС 10.1	<ul style="list-style-type: none"> – До 10 А тока – Гарантия: 2 года 	6 * 50 400

Был выбран ЛФС-10-1Ф как наиболее надежный и дешевый.

3.3.2. Активная защита от ПЭМИН

В таблице 7 приведено сравнение средств активной защиты от ПЭМИН. Стоимость указана с учетом комплектации, необходимой для защиты двух помещений. Таблица 7 - Сравнение средств активной защиты от ПЭМИН

Наименование	Возможности	Стоимость, руб.
Соната-РЗ.1	<ul style="list-style-type: none"> – регулировка мощности; – удаленное управление; – время непрерывной работы: 8 часов; – гарантия: 2 года. 	2 * 33 000
Пульсар	<ul style="list-style-type: none"> – защита от несанкционированного изменения настроек; – учет времени работы. 	2 * 19 000
Гамма-ГШ18	<ul style="list-style-type: none"> – учет времени работы; – защита от несанкционированного изменения настроек; – время непрерывной работы: не ограничено; – срок службы: от 10 лет; 	2 * 29 400

	– гарантия: 3 года.	
--	---------------------	--

По результатам сравнения был выбран “Тамма-ГШ18” как наиболее надёжный.

3.3.3. ПЭВМ в защищенном исполнении

В таблице 8 приведено сравнение комплексов ПЭВМ. Стоимость указана с расчетом на 5 рабочих мест, которые необходимо обеспечить для ведения закрытых разработок.

Таблица 8 - Сравнение комплексов ПЭВМ

Наименование	Возможности	Стоимость, руб.
ЛИС-40НС	<ul style="list-style-type: none"> – процессор: Intel Core i5 / i7; – оперативная память: DDR4 от 8 ГБ; – постоянная память: SSD от 256 ГБ, HDD от 500 ГБ; – операционная система: по выбору. 	5 * 188 500
ЛИС-40.1	<ul style="list-style-type: none"> – процессор: Intel Core i3-10110U; – оперативная память: DDR4 8 ГБ; – постоянная память: HDD 1 ТБ. 	5 * 230 000
Гамма МБ-16-01	<ul style="list-style-type: none"> – процессор: Intel Bay Trail J1900; – оперативная память: DDR3 4 ГБ; – постоянная память: HDD 320 ГБ; – операционная система: Free DOS. 	5 * 280 000

На данный момент единственным подходящим для ведения современной разработки ПЭВМ является “ЛИС-40НС”. Будем использовать его.

3.4. Защита от закладных устройств

3.4.1. Обнаружение закладных устройств

В таблице 9 приведено сравнение комплексов для обнаружения закладных устройств. Стоимость указана с учетом полной необходимой комплектации.

Таблица 9 - Сравнение комплексов для обнаружения закладных устройств

Наименование	Возможности	Стоимость, руб.
Крона-М6	<ul style="list-style-type: none"> – сканирование радиоэфира, проводных коммуникаций и инфракрасного диапазона; – обнаружение кратковременных сигналов, шумоподобных сигналов; – контроль работы аппаратуры подавления; – автономная работа: до 4 часов. 	1 360 000
ST131.S "ПИРАНЬЯ II"	<ul style="list-style-type: none"> – сканирование радиоэфира, проводных коммуникаций и инфракрасного диапазона; – контроль работы систем защиты виброакустического подавления. 	543 600
ST-167 "Бетта"	<ul style="list-style-type: none"> – простейший поиск источников радиосигнала; – избирательный прием сигнала; – постоянный мониторинг с созданием базы 	96 000

	<p>данных событий;</p> <ul style="list-style-type: none"> – работа по расписанию. 	
--	--	--

Был выбран комплекс ST131.S "ПИРАНЬЯ II" как наиболее многофункциональный.

3.4.2. Подавление сигнала закладных устройств

В таблице 10 представлено сравнение средств подавления сигналов закладных устройств.

Таблица 10 - Сравнение средств подавления сигналов закладных устройств

Наименование	Возможности	Стоимость, руб.
Блокиратор сотовой связи ЛГШ-716	<ul style="list-style-type: none"> – блокировка сотовой связи, Bluetooth, WiFi 2.4 ГГц; – время постоянной работы: не ограничено; – срок службы: 10 лет. 	89 700
Блокиратор стандартов Wi-Fi, Bluetooth ЛГШ-702	<ul style="list-style-type: none"> – блокировка Bluetooth, WiFi 2.4 ГГц; – время постоянной работы: не ограничено; – срок службы: 10 лет. 	61 100
ЛГШ-725	<ul style="list-style-type: none"> – блокировка сотовой связи, Bluetooth, WiFi 2.4 и 5 ГГц; – независимая регулировка мощности по каждому диапазону; – дистанционное управление; – время постоянной работы: не ограничено; – срок службы: 10 лет. 	247 000

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 11 представлено сравнение средств подавления микрофонов.

Таблица 11 - Сравнение средств подавления микрофонов

Наименование	Возможности	Стоимость, руб.
Бубен-Ультра	<ul style="list-style-type: none"> – три типа помех: ультразвуковой диапазон, сложная звуковая помеха, речеподобная помеха; – возможность автономной работы: до 6 часов; – радиус подавления: до 5 м; – различные варианты маскировки. 	2*48 000
BugHunter DAudio bda-5	<ul style="list-style-type: none"> – три типа помех: два вида ультразвука, акустическая помеха; – радиус подавления: до 10 м; – дистанционное управление. 	1*145 600
BugHunter DAudio bda-3 Voices	<ul style="list-style-type: none"> – ультразвуковой диапазон; – автономная работа; – радиус подавления: до 3 м; – дистанционное управление. 	2*68 900

Был сделан выбор в пользу средства “Бубен-Ультра” и его маскированного исполнения под систему оповещения.

4. Размещение средств защиты

На рисунке 10 изображены условные обозначения устанавливаемого оборудования. На рисунке 11 приведен план размещения оборудования.

Оптический канал

- ШТ** штора рулонная
- ДД** доводчик дверной

Акустический, виброакустический каналы



дверь звукоизолирующая

- ЛГШ 404** излучатель виброакустических помех "ЛГШ-404"
- ЛВП 10** вибровозбудитель "ЛВП-10"
- ЛВП 2А** акустический излучатель "ЛВП-2А"
- ЛУР 8** размыкатель Ethernet "ЛУР-8"
- ЛУР 2** размыкатель слаботочной линии "ЛУР-2"

Электромагнитный канал

- ЛФС 10** пассивная защита от ПЭМИН "ЛФС-10-1Ф"
- ГГШ 18** активная защита от ПЭМИН "Гамма ГШ-18"
- ПЭВМ в защищенном исполнении "ЛИС-40НС"

Защита от закладных устройств

- ЛГШ 725** средство подавления сигналов "ЛГШ-725"
- БУ** средство подавления микрофонов "Бубен Ультра"

Рисунок 10 - условные обозначения технических средств защиты информации

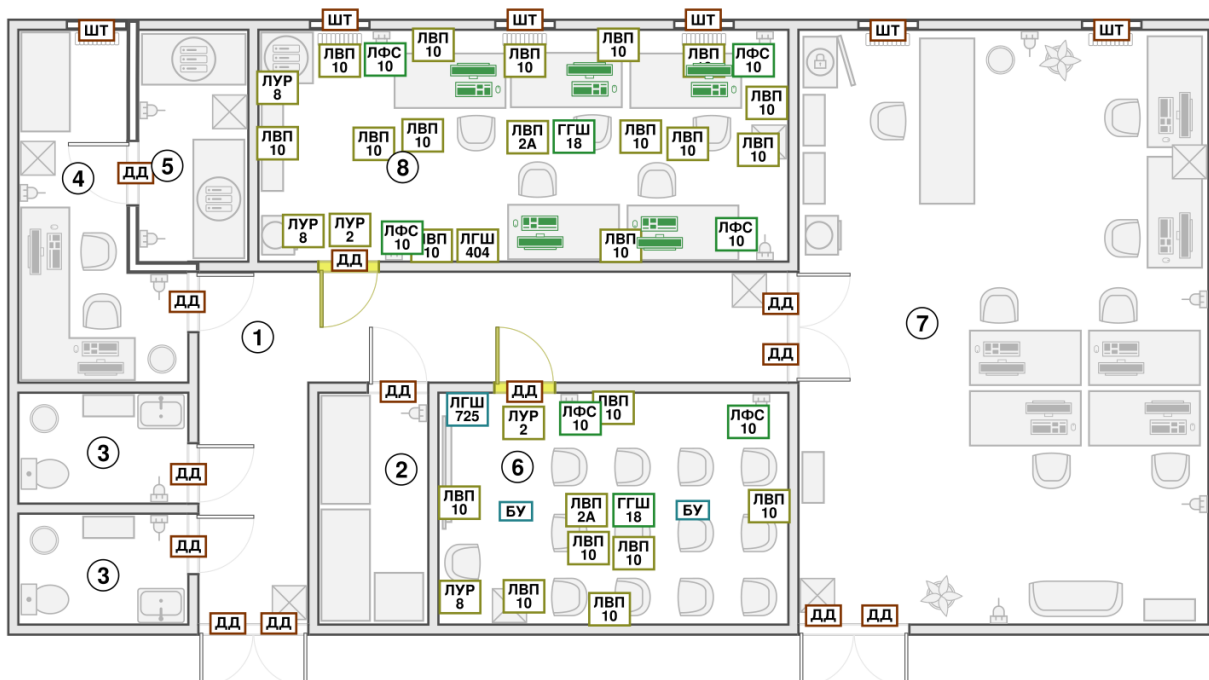


Рисунок 11 - план размещения технических средств защиты информации

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 3 191 800 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.
2. 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
3. Специализированный холдинг. Лаборатория ПППШ. URL: <https://labpps.ru> (дата обращения: 01.11.2023)
4. НЕЛК. Нестандартная электроника. URL: <https://nelk.ru/catalog> (дата обращения: 02.11.2023)