

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

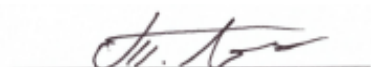
***«Инженерно-технические средства защиты
информации»***

На тему:

**Проектирование инженерно-технической защиты
информации на предприятии**

Выполнил:

Трубников А.С., студент
группы N34501



Проверил преподаватель:

Попов И.Ю., к.т.н.

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Трубников Андрей Сергеевич
	(Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34501
Направление (специальность)	Информационная безопасность
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии
Задание	Разработать системы инженерно-технической 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, размещенных на коммуникационной площадке дисциплины.
3. Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ технических средств защиты информации.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

Рекомендуемая литература

Руководитель		(Подпись, дата)
Студент		28.11.2023
		(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Трубников Андрей Сергеевич

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34501

Направление (специальность) Информационная безопасность

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

(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
		Планируема я	Фактически я	
1	Разработка и утверждение задания и календарного плана на курсовую работу	01.11.2023	01.11.2023	
2	Анализ теоретической составляющей	15.11.2023	15.11.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	28.11.2023	28.11.2023	
4	Представление выполненной курсовой работы	18.12.2023	19.12.2023	

Руководитель _____

(Подпись, дата)

Студент _____

28.11.2023

(Подпись, дата)

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

Студент Трубников Андрей Сергеевич
(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34501

Направление (специальность) Информационная безопасность

Руководитель Попов Илья Юрьевич, к.т.н., доцент ФБИТ
(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

- 1. Цель и задачи работы**
- ☐ Предложены студентом ☐ Сформулированы при участии студента
☒ Определены руководителем

Целью работы является повышение защищенности рассматриваемого помещения. Задачами является анализ защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.

- 2. Характер работы**
- ☐ Расчет ☐ Конструирование
☒ Моделирование Другое _____

Содержание работы

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ технических средств защиты информации
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

3. 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  28.11.2023
(Подпись, дата)

«__» _____ 20__ г

СОДЕРЖАНИЕ

Введение	6
1 Организационная структура предприятия	7
1.1 Общее описание.....	7
1.2 Информационные потоки	7
1.3 Описание защищаемого помещения.....	9
2 Анализ Технических каналов утечки информации	14
2.1 Технические каналы утечки информации.....	14
2.2 Анализ возможных технических каналов утечки информации.....	15
2.2.1 Акустический канал.....	15
2.2.2 Виброакустический канал.....	15
2.2.3 Оптический канал	15
2.2.4 Электромагнитный канал.....	15
2.2.5 Закладные устройства	15
3 Обоснование защиты информации	16
4 Анализ технических средств защиты информации.....	17
4.1 Акустический и виброакустический каналы	17
4.2 Электромагнитный канал.....	18
4.3 Оптический канал.....	19
4.4 Защита от закладных устройств	20
5 Размещение средств защиты.....	22
Заключение.....	25
Список использованных источников.....	26

ВВЕДЕНИЕ

Сегодня информационные технологии играют ключевую роль в современном обществе и бизнесе, поэтому обеспечение информационной безопасности становится одной из главных проблем. Средства защиты информации представляют собой комплекс мероприятий и технических средств, направленных на предотвращение несанкционированного доступа, сохранение целостности данных и защиту от угроз информационной безопасности.

Инженерно-технические средства защиты информации представляют собой специализированные системы и устройства, созданные для обеспечения безопасности в информационной среде. Инженерно-технические средства защиты информации играют значительную роль в обеспечении конфиденциальности данных на предприятии, являясь неотъемлемой частью общего комплекса мер по защите информации.

В рамках данной курсовой работы будет приведен процесс проектирования инженерно-технической системы защиты информации на предприятии. Рассматриваться будут основные этапы проектирования, ключевые компоненты системы, а также факторы, влияющие на эффективность ее функционирования.

1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

1.1 Общие описание

Наименование организации: ООО “АсетоДевелопмент”

Область деятельности: организация, специализирующаяся в области создания программного обеспечения для бизнес-компаний и государственных компаний. Организация занимается разработкой интеллектуальных решений, направленных на оптимизацию и автоматизацию бизнес-процессов различных предприятий.

1.2 Информационные потоки

В основе процесса управления материальными потоками лежит обработка информации, циркулирующей в информационных системах компании. В связи с этим одним из ключевых понятий логистики компании является понятие информационного потока.

Информационный поток — это совокупность циркулирующих в логистической системе между логистической системой и внешней средой сообщений, необходимых для управления и контроля операций. Информационный поток соответствует материальному и может существовать в виде бумажных и электронных документов. Информационный поток может опережать материальный, следовать одновременно с ним или после него.

Информационные потоки можно разделить на два вида: закрытые и открытые. Открытые потоки составляет информация, на распространение которой ограничений не установлено. Закрытые потоки образуют сведения конфиденциального характера, на распространение которых в определенном законом порядке установлены ограничения. Для государственных учреждений, предприятий, организаций, это может быть служебная информация, а также информация, составляющая государственную или военную тайну. Для общественных и частных организаций такого рода потоки образует, прежде всего, информация, составляющая коммерческую тайну, а также профессиональную тайну. Для закрытых потоков, как правило, создается отдельная система регистрации, ознакомления и работы с информацией (прежде всего, ее хранения и использования).

Схема организации представлена на рисунке 1.



Рисунок 1 – Схема организационной структуры предприятия

Информационные потоки в организации двух типов: открытые и закрытые, схема информационных потоков приведена на рисунке 2. В таблице 1 представлены обозначение на схеме.

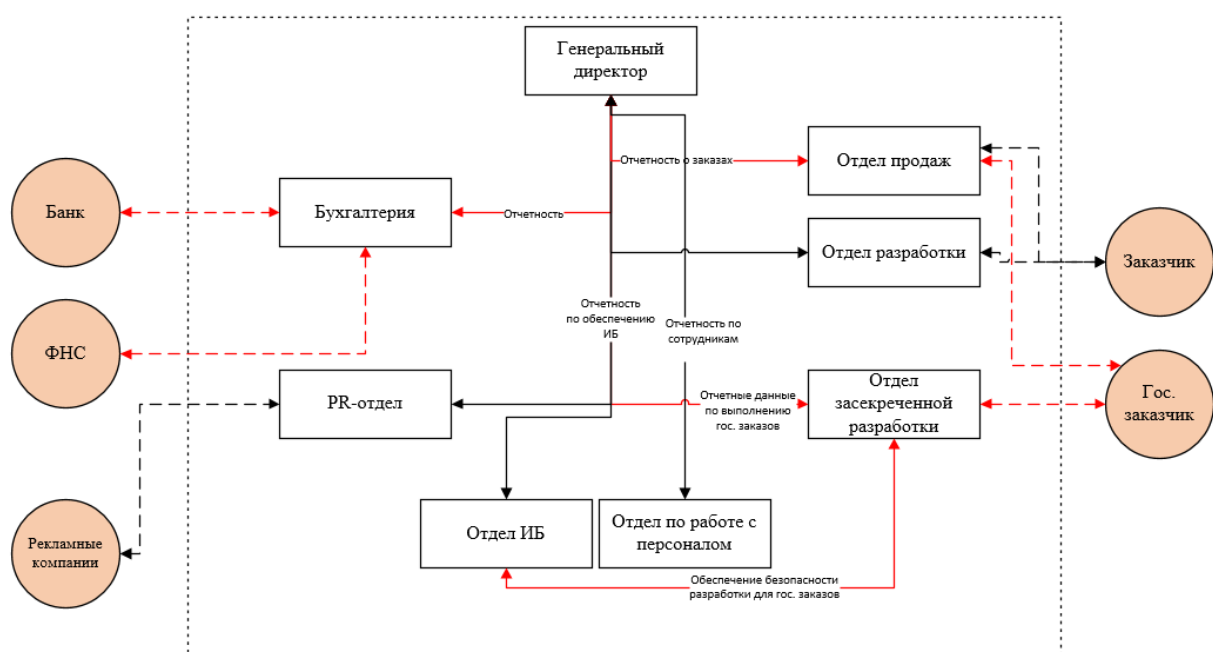


Рисунок 2 – Информационные потоки в организации

Таблица 1 – Обозначение на схеме информационных потоках

Обозначение	Описание
← - - - - - →	Потоки закрытых внешних данных
← - - - - - →	Потоки закрытых внутренних данных
← - - - - - →	Потоки открытых внешних данных
← - - - - - →	Потоки открытых внутренних данных

1.3 Описание защищаемого помещения

Офис организации, в котором планируется вести работу с государственной тайной находится на 4 этаже 5-этажного офисного здания. Здание имеет один вход расположен в восточной части здания и введет в коридор, в котором расположен главный коридор этажа, на котором расположен еще один офис и технические помещения. Окна находятся во всех кабинетах. Окна северной части выходят на проезжую часть и на жилой дом. Окна южной части выходят на коммерческое здание, в котором находятся другие офисы. Окна западной части выходят на задний двор, а также на жилые дома. Над арендуемым помещением находятся другое офисное помещение.

На рассматриваемом предприятии имеются следующие помещения:

- Коридор – 30м² (на плане под номером 1);
- Кабинет директора – 18,5 м² (на плане под номером 5);
- Приемная – 21,3 м² (на плане под номером 4);
- Open-space офис 49,3 м² (на плане под номером 3);
- Туалеты 13 м² (на плане под номером 2);
- Комната администраторов 18 м² (на плане под номером 7);
- Комната разработчиков 21 м² (на плане под номером 6);
- Бухгалтерия 18 м² (на плане под номером 8);
- Комната для отдыха 25 м² (на плане под номером 9);
- Переговорная 20 м² (на плане под номером 10);

На рисунке 3 представлен план помещения рассматриваемой организации. В таблице 2 приведено описание обозначений, используемых на плане.

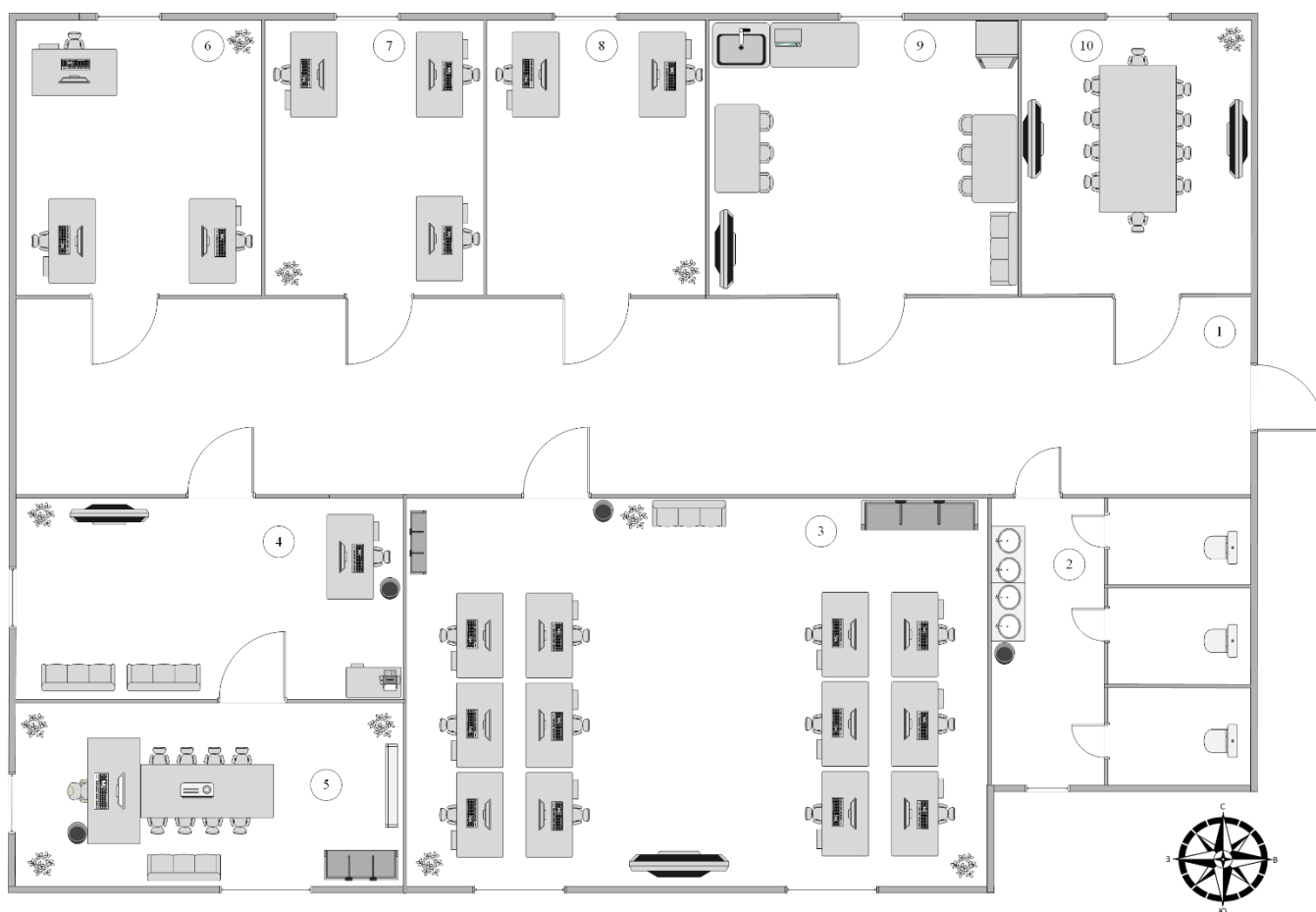



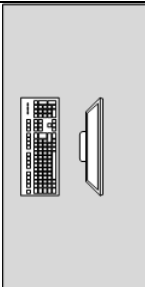
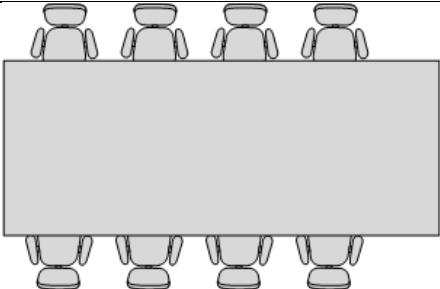






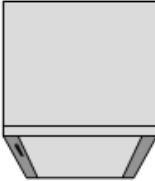

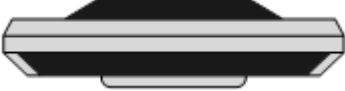

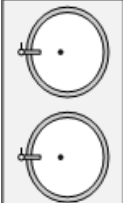
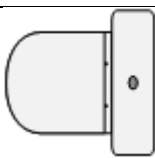



Рисунок 3 – План защищаемого помещения

Таблица 2 – Обозначения на плане

Обозначение	Описание
	Окно
	Дверь
	Персональное рабочее место с ПК.

	Стол, предназначенный для приема пищи
	Офисный стул
	Кресло руководителя
	Стол руководителя, оборудованный персональным компьютером
	Стол для переговоров на 8 человек
	проектор
	Интерактивная доска для проектора
	Шкаф
	Кресло
	урна

	СВЧ-печь
	Холодильник
	Раковина для кухни
	Телевизор
	принтер
	Сдвоенная раковина
	Туалет
	Комнатное растение

Кабинет директора включает в себя: один стул руководителя, стол с персональным компьютером, проектор, урну, 8 офисных стульев, диван, шкаф, интерактивную доску для проектора, 3 комнатных растения. Данное помещение имеет 8 розеток.

Приемочная включает в себя: персональный стол с компьютером, урну, два дивана, телевизор, комнатное растение, стол, принтер, офисное кресло. Данное помещение имеет 6 розеток.

Комната разработчиков включает в себя: 3 персональных стола с компьютером, комнатное растение. Данное помещение имеет 9 розеток.

Комната администраторов включает в себя: 3 персональных стола с компьютером, комнатное растение. Данное помещение имеет 12 розеток.

Кабинет бухгалтеров включает в себя: 2 персональных стола с компьютером, комнатное растение. Данное помещение имеет 6 розеток.

Комната отдыха включает в себя: 3 стола, 6 стульев, 1 телевизор, 1 диван, свч-печь, раковину, холодильник. Данное помещение имеет 8 розеток.

Переговорная включает в себя: 1 стол, 10 офисных кресел, 2 телевизора, комнатное растение. Данное помещение имеет 12 розеток

Орен-спасе офис включает в себя: 12 столов с персональным компьютером, 1 диван, урну, 3 комнатных растений, 12 офисных кресел, 2 шкафа, телевизор. Данное помещение имеет 30 розеток

Коридор не имеет мебели.

Окна помещений не имеют смежности с пожарными и эвакуационными лестницами, балконами и другими частями здания, которые могут быть использованы посторонними лицами для доступа в рассматриваемое помещение. Стены и внутренние перегородки здания выполнены из железобетона и имеют толщину не менее 15 см.

К защите от возможных потенциальных утечек информации по техническим каналам подлежат следующие помещения: кабинет директора, комнату для переговоров, комнату разработчиков.

2 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

2.1 Технические каналы утечки информации

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация. Среда распространения бывает однородной, например, только воздух при распространении электромагнитного излучения, или неоднородной, когда сигнал переходит из одной среды в другую. Носителями ПД могут быть люди, работающие с ИСПДн, технические средства, вспомогательные средства и т.д. Главное, что информация при этом отображается в виде полей, сигналов, образов, количественных характеристиках физических величин.

Источниками сигнала могут быть:

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

Каналы утечки информации можно разделить по физическим свойствам и принципам функционирования:

- акустические — запись звука, подслушивание и прослушивание;
- акустоэлектрические — получение информации через звуковые волны с дальнейшей передачей её через сети электропитания;
- виброакустические — сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;
- оптические — визуальные методы, фотографирование, видеосъемка, наблюдение;
- электромагнитные — копирование полей путём снятия индуктивных наводок;
- радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съёма речевой информации «закладных устройств», модулированные информативным сигналом;

– материальные — информация на бумаге или других физических носителях информации

2.2 Анализ возможных технических каналов утечки информации

2.2.1 Акустический канал

Возможна утечка информации по акустическому каналу. Рассматриваемое помещение находится между домами, поэтому можно прослушивать здание со стороны улицы или домов с помощью специальных приборов, например, с помощью направленного микрофона, также возможно прослушивать через спускаемые микрофоны, которые можно спустить с крыши.

2.2.2 Виброакустический канал

Возможна утечка через специальные приборы. С помощью лазера можно снимать колебания на окнах, также с помощью стетоскопов можно снимать информацию через поверхности, которые отражают звуковые колебания, например, вентиляция, трубы, батареи.

2.2.3 Оптический канал

Здание рассматриваемого помещения расположено на оживленной улице и граничит с дорогой, коммерческим зданием и жилыми домами, поэтому возможен просмотр помещения через окна из соседних зданий с использованием различных оптических приборов, таких как бинокль, телескоп, фотоаппарат с хорошим объективом и другие.

2.2.4 Электромагнитный канал

В рассматриваемом помещении есть устройства, которые во время работы генерируют побочные электромагнитные излучения, такие излучения могут перехватываться портативными средствами радиоразведки.

2.2.5 Закладные устройства

В рассматриваемом помещении есть множество мест, где можно спрятать закладное устройство: цветочные горшки, шкафы и полки с оборудованием, мусорные корзины. Также возможно маскировка закладных устройств под розетки, выключатели или размещение таких устройств в стенах, в вентиляциях.

3 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Согласно выданному заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «секретно». В руководящем документе «Типовые нормы и правила проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденный решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199, для защиты помещений для хранения информации составляющих государственную тайну перечислены следующие критерии:

1. В помещениях для работы с государственной тайной 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.
2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.
3. 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.
4. Все режимные помещения оборудуются аварийным освещением.
5. 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.
6. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Инженерно-технические средства защиты информации можно разделить на два вида: пассивные и активные. К пассивным техническим средствам защиты относятся экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры и т. д. Цель пассивного способа – максимально ослабить сигнал от источника информативного сигнала, например, за счет отделки стен звукопоглощающими материалами или экранирования технических средств. Активное техническое средство защиты – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации.

В данной работе будем использовать активные и пассивные технические средства защиты информации.

4.1 Акустический и виброакустический каналы

Рассмотрим два типа защиты – пассивный и активный.

В качестве пассивной защиты будем использовать звукоизолирующие материалы. Стоимость такой защиты будет зависеть от площади помещения. Общая площадь кабинета директора, переговорной и комнаты разработчиков составляет 59 м². Стоимость пассивных элементов средств технической защиты информации представлены в таблице 3.

Таблица 3 – Стоимость звукоизоляции для помещений

Вид звукоизоляции	Цена, руб/м ² с установкой	Единиц товара, шт	Конечная стоимость, руб
Звукоизоляция стен	4400	59	259 600
Звукоизоляция пола	2635	47	123 845
Звукоизоляция потолка	3800	59	224 200
Звукоизолирующая дверь	60000	3	180 000

Стоимость одной двери составляет 60 000 рублей, три двери обойдутся в 180 000 рублей. Итоговая стоимость пассивной защиты составляет 787 045 рублей.

В таблице 4 приведен сравнительный анализ активной защиты от утечек информации по акустическим каналам

Таблица 4 – СЗИ от утечек информации по виброакустическому каналу

Наименование	Характеристики	Стоимость, руб
ЛГШ-404	Учет времени работы; Контроль и защита органов регулировки уровня выходного шумового сигнала; Диапазон частот: 175 - 11 200 Гц; Круглосуточная непрерывная работа; Средний срок службы: 7 лет.	34 100
Шорох 5Л	Количество октавных полос для регулировки уровня мощности шума – 7. Диапазон частот 125 Гц – 8 кГц Расширенная диагностика работы каждого излучателя и параметров соединительной линии Диапазон регулировки уровня шумового сигнала в полосе октавных фильтров, не менее 18 дБ Диапазон регулировки общего уровня шумового сигнала, не менее 30 дБ	21 500
ANG-2200	Диапазон частот 125 Гц – 4 кГц Диапазон регулировки выходного уровня 20 дБ	14 500
SI-3030	Количество независимых каналов 3 Спектр шумовой помехи 175 Гц - 5,6 кГц Дискретность спектра шумовой помехи 0,005Гц Диапазон регулировки выходного уровня 40 дБ Диапазон регулировки АЧХ 20 дБ	30 000

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. Также обладает высокой мощностью выходного шума и широким диапазоном выходного сигнала.

4.2 Электромагнитный канал

В таблице 5 приведено сравнение средств активной защиты от ПЭМИН.

Таблица 5 – СЗИ от утечек информации по электромагнитному каналу

Наименование	Характеристики	Стоимость, руб
Пульсар	Защита от несанкционированного изменения настроек Учет времени работы Диапазон рабочих частот от 10 кГц до 6 ГГц; Мощность 50 Вт	24 525
Соната-РК1	Диапазон частот 0,01 - 1000 МГц Максимальная спектральная плотность мощности до 60 дБ	18 800
ЛГШ 503	Диапазон частот 10 кГц – 1800 МГц. Уровень шума до 50 дБ	44 200

Был сделан выбор в пользу Пульсар. У него имеется широкий диапазон частот от 10 кГц-6 ГГц, а также неплохая мощность и невысокая цена.

4.3 Оптический канал

В таблице 6 приведен список средств защиты от утечек информации по оптическому каналу.

Таблица 6 – СЗИ для оптического канала

Наименование	Описание	Стоимость, руб
Blackout рулонные шторы	Рулонные шторы, которые не пропускают свет.	2800
Дверные доводчики APECS Vanger DC-120-SL 26414	Доводчики позволяют закрывать двери в автоматическом режиме.	1400

В качестве пассивных средств защиты информации от утечек по оптическому каналу были выбраны шторы и дверные доводчики.

4.4 Защита от закладных устройств

В качестве защиты от закладных устройств будет использоваться специальные комплексы для обнаружения закладных устройств. В таблице 7 приведен анализ таких комплексов.

Таблица 7 – Анализ комплексов для обнаружения закладных устройств

Наименование	Характеристики	Стоимость, руб
ST131.S "ПИРАНЬЯ II"	Сканирование радиозфира, проводных коммуникаций и инфракрасного диапазона Контроль работы систем защиты виброакустического подавления Частотный диапазон до 6ГГц	550 000
Комплекс СИГНАЛ-PM	Частотный диапазон от 1 МГц до 7.25 ГГц Отображает панораму радиозфира в графическом представлении.	900 000
ANDRE ADVANCED	радиочастотный спектр в диапазоне от 10 кГц до 6 ГГц	300 000

Был сделан выбор в пользу ST131.S "ПИРАНЬЯ II". У него имеется широкий диапазон частот до 6 ГГц, а также неплохая мощность и имеет несколько быстроменяющихся антенн.

Также рассмотрим устройства для подавления сигналов закладных устройств (таблица 8)

Таблица 8 – Сравнение средств для подавления сигналов закладных устройств

Наименование	Характеристики	Стоимость, руб
МОЗАИКА-НВ	Диапазон излучаемых частот: 880-925, 925-960, 1710-1805, 1805-1880, 1900-1980, 2010-2025, 2110-2175	185 000
Завеса-12СТН	Блокируемые стандарты сотовой связи: GSM 900 / 1800; E-GSM; 3G; 3G+; 4G+; 4G-LTE; 4G-LTE 800; DECT; UMTS; WCDMA; Блокируемые стандарты спутниковой связи: GPS (NavStar)L1 Глонасс L1 Galileo E1	112 000
ЛГШ-716	Блокировка сотовой связи, Bluetooth, WiFi 2.4 ГГц	90 000

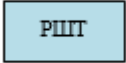
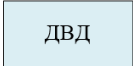


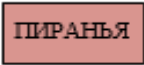
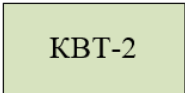
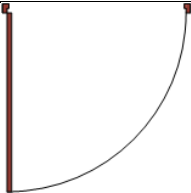

Квартет-2	Блокирует стандарты DECT, 4G, GSM, NMT-450i, CDMA, 3G, Wi-Fi, Bluetooth. Возможность выборочного блокирования отдельных стандартов	142 000
-----------	--	---------

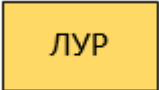
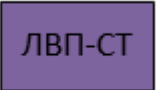
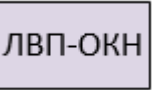
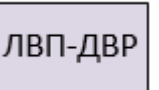
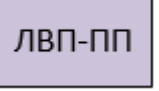
В качестве подавителя сигналов закладных устройств был выбран Квартет-2, так у него широкий выбор стандартов и можно настроить радиус действия и диапазон частот.

5 РАЗМЕЩЕНИЕ СРЕДСТВ ЗАЩИТЫ

В таблице 9 представлены обозначение средств защиты информации на плане, а также их конечная стоимость

Таблица 9 – Выбранные средства защиты информации

Устройство	Обозначение	Стоимость, руб	Количество, шт	Итоговая стоимость, руб
Рулонная штора Blackout		2800	11	30 800
Дверные доводчики		1400	10	14000
Блок питания и управления ЛГШ (входит в комплект)		0	1	0
Генератор электромагнитного шума Пульсар		24 525	3	73 575
Многофункциональное поисковое устройство ST131.S "ПИРАНЬЯ II"		550 000	1	550 000
Устройство блокирования работы систем цифровой связи и передачи данных Квартет-2		142 000	3	426 000
Шумоизолирующие двери		60 000	3	180 000
Виброакустический шумогенератор ЛГШ- 404		35 100	3	105 300

Размыкатель слаботочных линий, телефона и Ethernet "ЛУР"		5 590	3	16 770
электромагнитный вибропреобразователь «ЛВП-10» (стены)		5200	15	78 000
электромагнитный вибропреобразователь «ЛВП-10» (окна)		5200	4	20 800
электромагнитный вибропреобразователь «ЛВП-10» (двери)		5200	3	15600
электромагнитный вибропреобразователь «ЛВП-10» (пол, потолок)		5200	6	31200

На рисунке 3 представлен план с размещенными средствами защиты информации.

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной работы был проведен анализ существующих технических каналов утечки информации. Был проведен анализ потенциальных каналов утечки информации в выбранном защищаемом помещении и были описаны и приведены необходимые меры защиты рассматриваемого помещения.

Был проведен анализ рынка существующих технических средств защиты информации для противодействия рассматриваемым каналам утечки информации. Был произведен план установки инженерно-технических средств защиты информации. Также был произведен расчет итоговой стоимости средств защиты информации для рассматриваемого помещения, где обрабатывается и хранится информация с грифом «государственная тайна».

Итоговое значение суммы затрат составило 1 542 045 рублей.

Цель курсовой работы была достигнута, все поставленные задачи выполнены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Маркарян Юрий Каренович Исследование информационных потоков в логистической системе // Символ науки. 2016. №12-1.
2. Оборудование для защиты информации // INFOSECUR URL: <https://infosecur.ru/product/oborudovanie-dlya-zashchity-informatsii/> (дата обращения: 08.12.2023).
3. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012 (дата обращения: 05.12.2023).
4. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.