

**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:

студент группы N34461

Полянский Максим Николаевич



(подпись)

Проверил:

доцент ФБИТ, к.т.н.

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	Полянский М.Н.
	(Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34461
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 систему инженерно-технической защиты информации на предприятии


Краткие методические указания

- Курсовая работа выполняется в рамках изучения дисциплины «Инженерно-технические средства защиты информации».
- Порядок выполнения и защиты курсовой работы представлен в методических указаниях, размещенных на коммуникационной площадке дисциплины.
- Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

- Введение.
- Организационная структура предприятия.
- Обоснование защиты информации.
- Анализ защищаемых помещений.
- Анализ рынка технических средств.
- Описание расстановки технических средств.
- Заключение.
- Список литературы.

Рекомендуемая литература

Руководитель		(Подпись, дата)
Студент		19.12.2023
		(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Полянский М.Н.

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34461

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	13.11.2023	13.11.2023	
2	Анализ теоретической составляющей	25.11.2023	25.11.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	03.12.2023	03.12.2023	
4	Представление выполненной 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**

Студент Полянский М.Н.

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34461

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

**2. Характер
работы**

- ☐ Расчет ☐ Конструирование
☐ Моделирование ☒ Другое Проектирование

Содержание работы

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
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

19.12.2023

(Подпись, дата)

«__» _____ 20__ г

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	6
1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ	7
1.1 Общие сведения о защищаемой организации	7
1.2 Структура информационных потоков на предприятии	7
2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ	9
3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	12
3.1 Схема помещения	12
3.2 Анализ возможных каналов утечки информации	13
4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ	15
4.1 Выбор средств защиты	15
4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам	15
4.3 Защита от утечки информации по (вибро-) акустическим каналам	17
4.4 Защита от ПЭМИН	19
4.5 Защита от утечек информации по оптическим каналам	21
5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ	22
ЗАКЛЮЧЕНИЕ	26
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	27

ВВЕДЕНИЕ

В настоящее время информационные технологии играют важнейшую роль в современном обществе и бизнесе, что подчеркивает значимость обеспечения информационной безопасности как одной из основных задач. Средства защиты информации представляют собой комплекс мероприятий и технических решений, направленных на предотвращение несанкционированного доступа, обеспечение 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. Их важность заключается в значительном вкладе в обеспечение конфиденциальности данных на предприятии, а они сами становятся неотъемлемой частью общего комплекса мер по защите информации.

В данной работе рассматривается процесс создания комплекса инженерно-технической защиты информации, для защиты информации, составляющей государственную тайну составляющей государственную тайну с уровнем «совершенно секретно» на объекте информатизации.

1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

1.1 Общие сведения о защищаемой организации

Общее наименование организации: ИнфоТехника

Область деятельности: разработка программного обеспечения.

Защищаемая информация:

1. коммерческая тайна - сведения о заключенных договорах и контрактах, данные о партнерах и клиентах компании, информация о ценовой политике и финансовых операциях;
2. техническая информация конфиденциального характера - состав и структура баз данных, содержащих информацию клиентов, конфигурации используемого серверного и сетевого оборудования, сведения об архитектуре и настройках корпоративных информационных систем;
3. государственная тайна - проекты для государственных учреждений или оборонных организаций, информация о разработке систем защиты от киберугроз, криптографии или технологий, обеспечивающих конфиденциальность данных.

1.2 Структура информационных потоков на предприятии

Организация занимается разработкой программного обеспечения. Организация предлагает услуги как обычным пользователям, так и государственным органам, таким как ФСБ. Следовательно, на предприятии циркулирует гос. тайна.

Структура Организации представлена на рисунке 1.

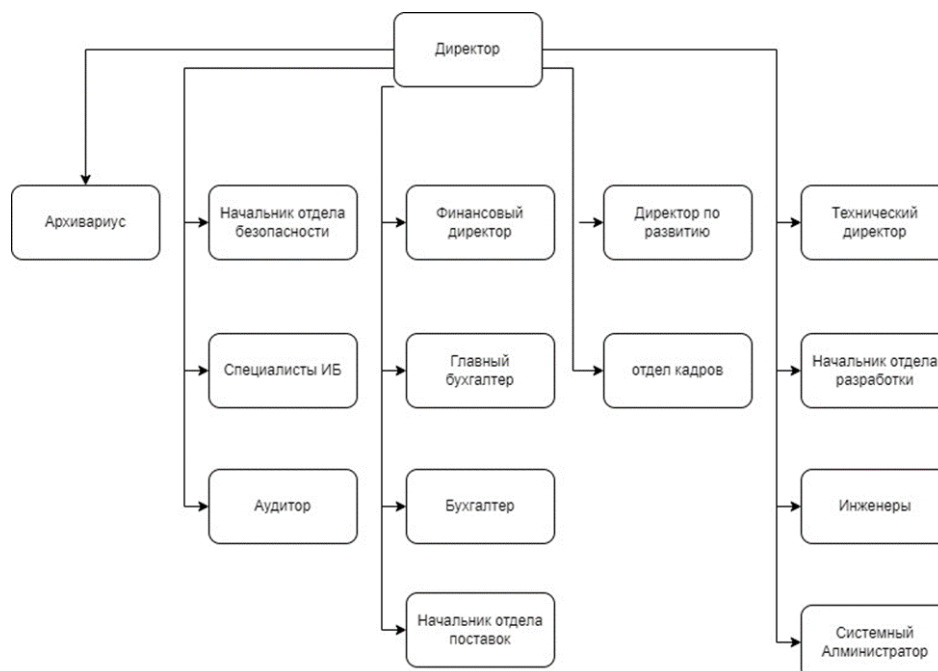


Рисунок 1 – Структура организации

Схема информационных потоков представлена на рисунке 2.

2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Организация сотрудничает с ФСБ, поэтому она в том числе работает с государственной тайной уровня «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:

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.

Основными документами в области защиты информации являются:

-Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

-Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».

-Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины

информационной безопасности Российской Федерации».

-Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».

-Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне».

-Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации».

-Федеральный закон от 27 июля 2006 г. No 152-ФЗ «О персональных данных».

-Постановление Правительства РФ от 1 ноября 2012 г. No 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

-Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1.

-Межведомственная комиссия по защите государственной тайне решение No 199 от 21.01.2011 г.

-"О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".

Также на сайте ФСТЭК существует отдельный раздел, содержащий специальные нормативно-технические документы ФСТЭК России – нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации:

-СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам.

-СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации.

-Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров.

-Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации.

-Временный порядок аттестации объектов информатизации по требованиям безопасности информации.

-Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения.

-Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

-Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

-Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.

-Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.

-Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования.

-Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

-Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Схема помещения

Прежде чем устанавливать технические средства защиты, проведем анализ защищаемого помещения.

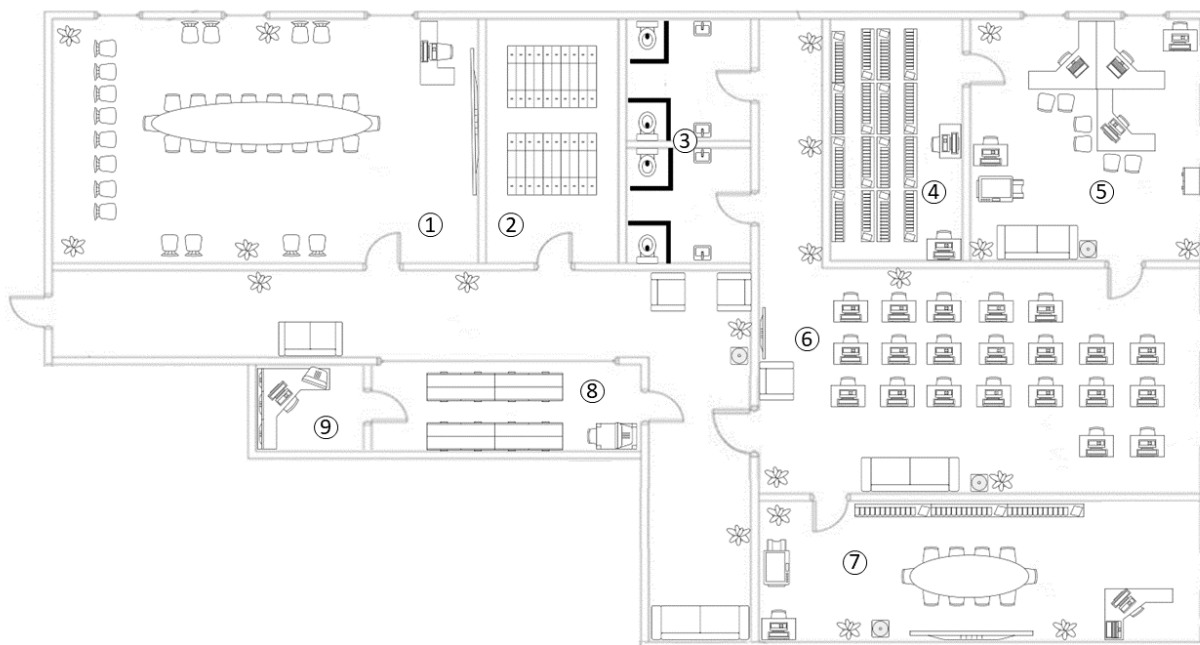


Рисунок 3 – План защищаемого помещения

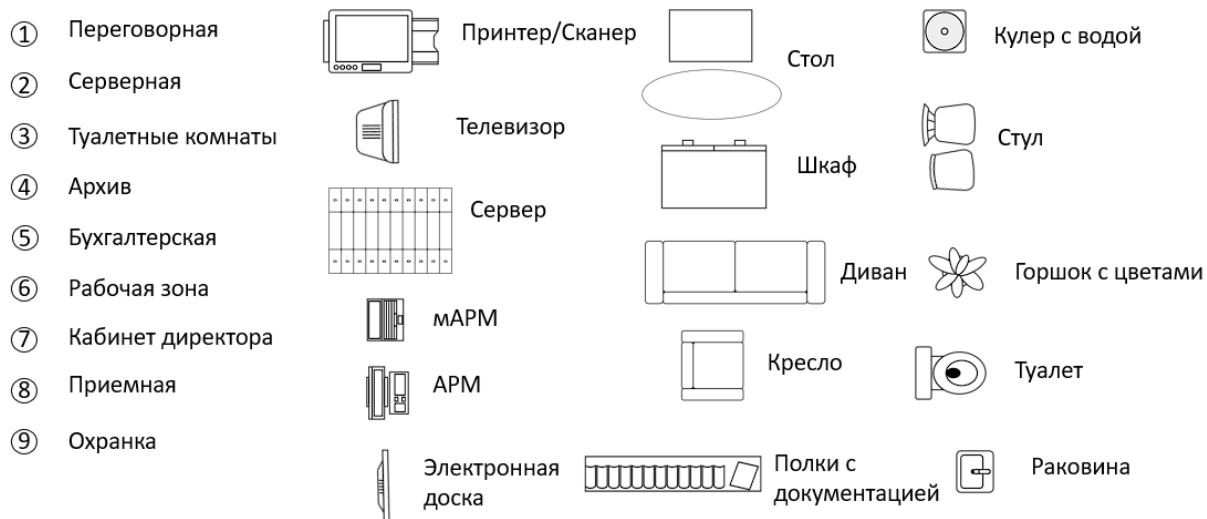


Рисунок 4– Описание обозначений

На рассматриваемом предприятии в рамках курсовой работы имеются следующие помещения, подлежащие инженерно-технической защите:

- 1) Переговорная (60 м²);
- 2) Серверная (25 м²);
- 3) Архив (30 м²);
- 4) Бухгалтерская (35 м²);

- 5) Рабочая зона (75 м²);
- 6) Кабинет директора (50 м²);
- 7) Приемная (20 м²);
- 8) Охранка (10 м²);

В переговорной находятся: большой стол, стулья, электронная доска, АРМ, 4 горшка с цветами. В помещении 3 окна.

В серверной расположены 2 сервера. В помещении нет окон.

В архиве расположены полки с документацией, 2 АРМа. В помещении нет окон.

В бухгалтерской расположены 3 АРМа, 2 мАРМа, шкаф, принтер, кулер, диван, 3 горшка с цветами, стулья. В помещении 5 окон.

В рабочей зоне расположены 19 АРМов, 6 горшков с цветами, электронный экран, кулер, диван, кресло. В помещении 2 окна.

В кабинете директора расположены полки с документацией, большой стол, стулья, 2 АРМа, мАРМ, кулер, 3 горшка с цветами, принтер, электронный экран.

Офис расположен на третьем этаже трёхэтажного здания, окна выходят в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

3.2 Анализ возможных каналов утечки информации

В каждом помещении существуют потенциальные пути для нежелательной утечки информации, связанные с электромагнитными и электрическими утечками информации, то есть с использованием компьютеров и розеток. Декоративные элементы, такие как комнатные растения, могут использоваться для установки закладных устройств, которые могут использоваться для передачи информации через акустический канал.

Существуют также риски утечки информации через оптические каналы, например, из-за незакрытых окон и незащищенных дверей. Важно учитывать также виброакустический канал, который может быть использован для передачи информации из-за наличия твердых поверхностей, таких как стены или батареи отопления.

Вещественно-материальный канал утечки информации возможен ввиду наличия вещественных носителей информации, однако он не перекрывается техническими средствами защиты.

Акустический, вибро-акустический и электроакустический. Акустический канал утечки информации формируется из трех элементов:

- источника — голоса при разговоре в помещении с коллегами или по

телефону;

- среды распространения — воздуха для акустического сигнала, металлических конструкций и стекол для виброакустического;

- приемника — электронного закладного устройства, совмещающего функции снятия информации и передачи ее по радиосигналу.

Электрический (электромагнитный) - Он разделяет способы перехвата данных на:

- перехват побочных электромагнитных излучений;
- перехват побочных электромагнитных излучений на частотах работы высокочастотных генераторов;

- перехват побочных электромагнитных излучений на частотах самовозбуждения усилителей низкой частоты.

4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

4.1 Выбор средств защиты

Для обеспечения высокого уровня комплексной безопасности информации, которая отнесена к категории «совершенно секретно» в зависимости от её типа, требуется оснащение помещения специальными средствами и устройствами, перечисленными в таблице 1. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки такой конфиденциальной информации.

Таблица 1 – Активная и пассивная защита информации

Каналы	Источники	Активная защита	Пассивная защита
Акустический Электроакустический	Стены, двери, окна, электрические сигналы	Устройства акустического зашумления	Защитные экраны и фильтры для сетей электропитания, изоляция особо важных помещений
Виброакустический	Стекла, стены и иные твердые поверхности	Устройства вибрационного зашумления	Изоляция переговорной, использование антивибрационных материалов и звукозащитных экранов
Визуально- оптический	Окна и стеклянные поверхности, двери	Жалюзи, бликующие устройства	Защитные экраны и фильтры для сетей электропитания
Электрический Электромагнитный	Компьютеры, сервера, бытовая техника, розетки	Устройства электромагнитного зашумления	Защитные экраны и фильтры для сетей электропитания

4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам

Пассивная защита в данном контексте включает в себя установку фильтров в электропитании всех помещений, направленных на минимизацию возможных электромагнитных и электрических утечек информации.

Система активной защиты основана на использовании белого шума в сети. Эта система генерирует постоянный фоновый шум, который маскирует колебания, возникающие от звуковых волн или работы электронных устройств. Для более детального

анализа представлены модели устройств и их характеристики в таблице 2. Эти меры активной защиты направлены на обеспечение дополнительного уровня безопасности и предотвращение возможных технических каналов утечки информации в защищаемых помещениях.

Таблица 2 – Активная защита от утечек информации по электрическим каналам

Модель	Цена, руб.	Характеристики	Особенности
ФП-6	50 556	Ток нагрузки – 20 А. Уровень шума/затухания – 60 дБ. Напряжение – при постоянном токе - 500 В / при переменном токе с частотой 50 Гц - 220 В / при переменном токе с частотой 400 Гц - 115 В. Частотный диапазон – 0,01 - 1800 МГц. Количество фаз – 1. Тип соединения – экранированный кабель (2 шт) в комплекте.	Фильтр ФП-6 предотвращает утечки информации по цепям электропитания, а также защищает средства оргтехники от внешних помех. ФП-6 ослабляет любые сигналы в диапазоне 0,01–1800 МГц с эффективностью 60 дБ и, соответственно, не пропускают информативные сигналы, возникающие при работе средств оргтехники. Сертификат ФСТЭК.
Генератор шума СОНАТА-РС3	32 400	Ток нагрузки – сеть ~220 В +10%/-15%, 50 Гц. Напряжение – 220 В. Количество фаз – 1. Потребляемая мощность 10 Вт.	Устройство для активной защиты информации от утечки по сети электропитания. Предназначено для подключения к 3-проводной сети. Звуковая и световая индикация работы. Сертифицировано ФСТЭК.
ФСПК-40	59 800	Ток нагрузки – 40 А. Уровень шума/затухания – защита информации	Устройство защиты речевой информации от утечки по электросети. Два фильтруемых провода (ноль, фаза). Подавление

		от утечки за счет побочных электромагнитных наводок на линии электропитания по 2 классу защиты. Напряжение 220/380 В. Частотный диапазон – 0,15–1000 МГц. Количество фаз – 1. Тип соединения – подключение к цепям электропитания с 2 проводами (ноль и фаза, без заземления).	помех, побочных излучений, наводок в диапазоне 0,15–1000 МГц. Напряжение питающей сети 220/380 В, частота – 50Гц. Класс электробезопасности – I (ГОСТ Р 12.1.019–2009 ССБТ). Сертифицировано ФСТЭК.
ЛГШ-221	36 400	Диапазон частот 10 кГц – 400 МГц. Диапазон регулировки уровня выходного шумового сигнала не менее 20 дБ. Мощность, потребляемая от сети не более 45 ВА.	Сетевой генератор шума. Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.

На основании анализа, проведенного в таблице 2, был выбран генератор шума Соната РС3. Оптимальный вариант, так как устройством возможно управлять дистанционно посредством проводного пульта, а также у устройство есть сертификат от ФСТЭК.

4.3 Защита от утечки информации по (вибро-) акустическим каналам

Пассивные меры безопасности охватывают установку тамбурной зоны перед переговорной комнатой и усиление дверей для дополнительной защиты. Для обеспечения звукоизоляции переговорной комнаты и кабинета директора применяются специализированные материалы, способствующие снижению звуковой проницаемости стен и, таким образом, повышению конфиденциальности обсуждаемой информации.

Активные меры безопасности включают в себя систему виброакустической

маскировки. Для обеспечения безопасности помещения, где обрабатывается информация с уровнем секретности "совершенно секретно", рассматриваются технические средства активной защиты информации, соответствующие категории не ниже 1Б (таблица 3). Эти меры направлены на предотвращение возможных технических каналов утечки информации, обеспечивая дополнительный уровень безопасности в защищаемых помещениях.

Таблица 3 – Активная защита от утечек информации по (вибро-)акустическим каналам

Модель	Цена, руб.	Характеристики	Особенности
Генератор шума ЛГШ-303	15 600	Диапазон частот акустической помехи – 180–11300 Гц. Средняя наработка на отказ – не менее 5000 ч. Средний срок службы – 5 лет. Время автономной работы – до 5 часов.	Мобильно и предназначено для работы в помещениях, (автомобилях) и других местах не требующих стационарных средств защиты информации по прямому акустическому каналу. В непрерывном режиме изделие работает до пяти часов при температуре окружающей среды от плюс 1 до плюс 40 °С, относительная влажность не более 80 % (при температуре + 25 °С).
Шорох 5Л	21 500	Диапазон регулировки уровня шумового сигнала в полосе октавных фильтров, не менее 18 дБ. Диапазон регулировки общего уровня шумового сигнала, не менее 30 дБ. Частота переменного напряжения электропитания 50±2 Гц. Потребляемая мощность при полной нагрузке, не более 130 ВА.	Система «Шорох-5Л» относится к средствам активной акустической и вибрационной защиты информации 1-го класса тип «Б». Система представляет собой комплекс устройств, состоящий из блока питания и управления «БПУ-1» с активными вибровозбудителями «ПЭД-8А» и активными акустическими излучателями «АИ-8А/Н» и «АИ-8А/Мини».

Соната АВ-4Б	44 200	Диапазон воспроизводимого шумового сигнала 175–11200 Гц. Выходное напряжение В $12,5 \pm 0,5$. Электропитание сеть ~220 В/50 Гц.	Комплект состоит из блоков электропитания и управления, генераторов-акустоизлучателей, генераторов-вибровозбудителей, размыкателя телефонной линии, размыкателя слаботочной линии, размыкателя линии Ethernet, пульта управления, блоков сопряжения из внешних устройств. Технического средства защиты речевой информации от утечки по оптико-электронному (лазерному) каналу и прочих аксессуаров.
--------------	--------	---	---

Исходя из анализа, представленного в таблице 3, было принято решение о выборе системы Соната АВ-4Б. По сравнению с альтернативными системами, предназначенными для защиты от утечек информации через акустические и вибрационные каналы, данная система считается наиболее востребованной и получила множество положительных отзывов.

4.4 Защита от ПЭМИН

ПЭМИН – побочные электромагнитные излучения и наводки. Вариант защиты компьютерной информации методом зашумления (радиомаскировки) предполагает использование генераторов шума в помещении, где установлены средства обработки конфиденциальной информации. Зашумление обеспечивается типами генераторов, представленными в таблице 4.

Таблица 4 – Активная защита от ПЭМИН

Модель	Цена, руб.	Характеристики	Особенности
СОНАТА-РЗ.1	33 120	Наличие регулировки уровня шума. Диапазон частот – соответствует требованиям документа "Требования к средствам активной защиты"	Техническое средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок типа (класса) АБ(2). Соответствует

		<p>информации от утечки за счет побочных электромагнитных излучений и наводок" (ФСТЭК России, 2014) - по 2 классу защиты.</p> <p>Электропитание – сеть 220 В +10%/-15%, 50 Гц.</p> <p>Мощность – 10 Вт. Режим работы – продолжительность непрерывной работы не менее 8 ч.</p>	<p>современным требованиям.</p> <p>Может устанавливаться в выделенных помещениях до 1-й категории включительно, в том числе оборудованных системами звукоусиления речи, без применения дополнительных мер защиты информации. Сертификат ФСТЭК 3539.</p>
Генератор шума ГНОМ-3М	57 200	<p>Диапазон частот 10 кГц - 1800 МГц. Уровень шума от -26 дБ (мкА/м*$\sqrt{\text{кГц}}$) до 50 дБ(мкВ/м*$\sqrt{\text{кГц}}$).</p> <p>Мощность – 45 Вт.</p>	<p>Предназначен для активной защиты информации, обрабатываемой на электронно-вычислительной технике.</p> <p>Имеет 4 выхода для подключения к цепям электропитания и к антенным контурам. Прост в эксплуатации и не требует дополнительных настроек. Имеет сертификат ФСТЭК.</p>
Генератор шума Пульсар	24 525	<p>Диапазон частот 10 кГц - 6 ГГц.</p> <p>Электропитание – однофазная сеть переменного тока 187–242 В.</p> <p>Мощность – 50 ВА.</p>	<p>Имеет защиту регулятора уровня выходного шумового сигнала от нелегального доступа (и сигнализирует об этом). Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук).</p>
Генератор шума ЛГШ-501	29 900	Присутствует регулировка уровня шума, диапазон	Оснащено визуальной системой индикации

		<p>регулировки уровня выходного шумового сигнала не менее 20 дБ. Диапазон частот – 0,01–1800 МГц. Уровень шума – от -28 дБ(мкА/м*$\sqrt{\text{кГц}}$) до 57 дБ(мкВ/м*$\sqrt{\text{кГц}}$). Электропитание – однофазная сеть переменного тока 187 В-242 В. Мощность – не более 45 ВА. Режим работы – круглосуточно.</p>	<p>нормального режима работы и визуально-звуковой системой индикации аварийного режима. Оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех. Обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.</p>
--	--	--	--

В качестве средства активной защиты от ПЭМИН был выбран генератор шума Соната-РЗ.1. Этот выбор обоснован соответствию требованиям к документам ФСТЭК, а также наличие возможности, в случае необходимости, дополнительного повышения уровня излучаемого электромагнитного поля шума в диапазоне частот 0,01...200 МГц за счет применения опционально поставляемой дополнительной антенны ВЕЕР.

4.5 Защита от утечек информации по оптическим каналам

Для предотвращения возможности использования оптического канала для утечки информации можно воспользоваться следующими средствами:

- шторы;
- жалюзи;
- тонированные пленки на стеклах.

Среди предложенных вариантов защиты от оптического канала утечки информации использование жалюзи выделяется как наиболее эффективное решение. Жалюзи не только препятствуют визуальному наблюдению, но также успешно защищают от солнечных лучей. При выборе таких средств важно учитывать их адаптивность к конкретным потребностям и особенностям окружающей среды, чтобы обеспечить максимальный уровень безопасности.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В предыдущей главе был проанализирован рынок инженерно-технических средств и были выбраны лучшие средства защиты информации из них, которые включает в себя:

- сетевой генератор шума «Соната-РС3»;
- система виброакустической защиты «Соната АВ-4Б»;
- генератор шума «Соната-РЗ.1» от ПЭМИН
- жалюзи на окна;
- три усиленные двери с толщиной 4 мм, обшитые металлическим листом не менее 2 мм, внутри – звукоизоляционный материал.

Для каждого помещения оптимальное количество акустоизлучателей и вибровозбудителей зависит от различных факторов, таких как звукоизоляция, форма, материалы стен, местоположение, уровень фонового шума и другие подобные аспекты.

Согласно информации на официальном веб-сайте производителя НПО «АННА» для выбранной системы виброакустической защиты, предварительную оценку необходимого количества вибровозбудителей «Соната СВ-4Б» можно провести, руководствуясь следующими стандартами:

- стены – один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- потолок, пол – один на каждые 15...25 м² перекрытия;
- окна – один на окно (при установке на оконный переплет);
- двери – один на дверь (при установке на верхнюю перекладину дверной коробки);

Предварительная оценка необходимого количества акустоизлучателей «Соната СВ-4Б» может быть выполнена из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8...12 м³ надпотолочного пространства или других пустот.

В таблице 5 содержится список мер защиты, предназначенных для применения во всех помещениях, а также конечная стоимость.

Таблица 5 – Необходимое оборудование

Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Сетевой генератор шума «Соната-РС3»	32 400	1	32 400
Генератор шума «Соната-РЗ.1»	33 120	1	33 120


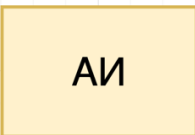
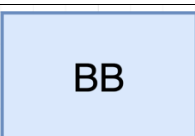
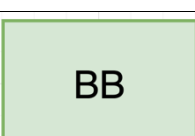
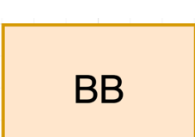
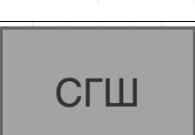
Блок электропитания и управления «Соната-ИП4.3»	21 600	1	21 600
Генератор-акустоизлучатель «Соната СА-4Б1»	3 540	33	116 820
Генератор-вибровозбудитель «Соната СА-4Б»	7 440	80	595 200
Размыкатель телефонной линии «Соната ВК4.1»	6 000	7	42 000
Размыкатель слаботочной линии «Соната ВК4.2»	6 000	1	6 000
Размыкатель линии «Ethernet» «Соната ВК4.1»	6 000	4	24 000
Пульт управления «Соната-ДУ 4.3»	7 680	1	7 680
Шторы-плиссе Blackout	4 900	11	53 900
Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	83 619	3	250 857
Итого			1 183 577

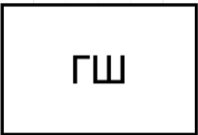

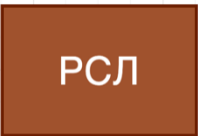

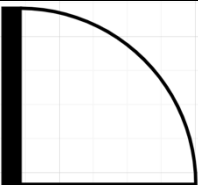

В помещении установлены усиленные звукоизолирующие двери, как показано на рисунке 5. На каждом окне установлены шторы. Системы «Соната СА-4Б1» и «Соната СВ-4Б» размещены в соответствии с указаниями производителя. «Соната-РС3» и «Соната-Р3.1» находятся рядом с «Соната-ИП4.3» и подключены к ней. Все выключатели установлены в соответствии с рекомендациями производителя. В таблице 6 приведены описание обозначений устройств.



Рисунок 5 – Схема расстановки устройств

Таблица 6 – Описание обозначений устройств

Обозначение	Устройство	Количество, шт.
	Блок электропитания и управления «Соната-ИП4.3»	1
	Генератор-акустоизлучатель «Соната СА-4Б1»	33
	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)	38
	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)	17
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери)	19
	Сетевой генератор шума «Соната-РС3»	1

	Генератор шума «Соната-Р3.1»	1
	Размыкатель линии «Ethernet» «Соната-ВК4.3»	7
	Размыкатель слаботочной линии «Соната-ВК4.2»	1
	Размыкатель телефонной линии «Соната-ВК4.1»	4
	Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	3
	Шторы-плиссе BlackOut	11

ЗАКЛЮЧЕНИЕ

В рамках данной курсовой работы была проведена комплексная разработка инженерно-технической системы безопасности на предприятии. Основной акцент был сделан на анализе технических каналов утечки информации, а также разработке и внедрении эффективных средств и устройств для их перекрытия.

В ходе исследования были выделены и проанализированы различные технические каналы, представляющие потенциальные угрозы для безопасности предприятия. На основе полученных данных были разработаны мероприятия по минимизации рисков и предотвращению утечек информации.

Основываясь на полученных результатах, были предложены конкретные рекомендации по установке устройств на плане предприятия, а также проведен расчет стоимости реализации предложенных мероприятий. Это позволяет предприятию не только повысить уровень безопасности, но и рационально распределить бюджет на внедрение системы безопасности.

Инженерно-техническая система безопасности, разработанная в рамках данной работы, представляет собой комплексный и эффективный инструмент для защиты информационных ресурсов предприятия. Проведенные исследования и разработки могут служить основой для дальнейших улучшений и модернизации систем безопасности, а также применяться в других сферах бизнеса с целью обеспечения надежной защиты от угроз информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.
2. Хорев А. А. Техническая защита информации: учебное пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010. — 436 с.
3. Рагозин, Ю. Н. Инженерно-техническая защита информации: учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург: Интермедия, 2018. — 168 с.— ISBN 978-5-4383-0161-5.
4. Кармановский Н. С., Михайличенко О. В., С. В. Савков. Организационно-правовое и методическое обеспечение информационной безопасности //Электрон. дан. — Санкт-Петербург: НИУ ИТМО. – 2013