

**Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

Факультет безопасности информационных технологий

Дисциплина:

«Инженерно-технические средства защиты информации»

КУРСОВАЯ РАБОТА

«Проектирование инженерно-технической защиты информации на предприятии»

Вариант 24

Выполнил:

Герцен И.А., студент группы N34471

(подпись)

Проверил:

Попов И.Ю., доцент ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Герцен Илья Андреевич
	(Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34471
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

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 рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

Рекомендуемая литература

Руководитель		(Подпись, дата)
Студент		22.12.2023
		(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Герцен Илья Андреевич

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34471

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	24.10.2023	24.10.2023	
2	Анализ теоретической составляющей	28.11.2023	28.11.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	01.12.2023	01.12.2023	
4	Представление выполненной курсовой работы	19.12.2023	22.12.2023	

Руководитель

(Подпись, дата)

Студент

22.12.2023

(Подпись, дата)

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

Студент Герцен Илья Андреевич

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34471

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

Цель данного исследования заключается в усилении общей безопасности рассматриваемого помещения. В процессе работы стоит задача не только провести детальный анализ уровня безопасности и выявить потенциальные угрозы информационной безопасности, но и разработать комплекс мер для усиления как пассивных, так и активных методов защиты данных. Этот подход не просто направлен на повышение степени защищенности помещения, но и на формирование гибких и адаптивных решений, способных эффективно противостоять современным вызовам в области безопасности.

**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 исследования были выявлены общие стратегии по предотвращению утечки важной передовые информации через технические каналы на предприятии. Освещение вопросов кибер- и физической безопасности подчеркнуло, что стратегии защиты должны постоянно эволюционировать и интегрировать

методы предотвращения. Важным выводом стало понимание необходимости не только использования современных технологических решений, но и активного формирования внутренней культуры безопасности в организации. В этом контексте систематическое обучение сотрудников и их активное участие в процессах обеспечения безопасности становятся ключевыми элементами успешной стратегии защиты в современном информационном обществе. Этот комплексный и адаптивный подход является неотъемлемой частью эффективного обеспечения безопасности, особенно в условиях постоянных перемен и неопределенности.

Руководитель _____

Студент _____



(Подпись, дата)

22.12.2023

(Подпись, дата)

«__» _____ 20__ г

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	7
1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ.....	8
1.1 Анализ технических каналов утечки информации.....	8
1.2 Структура информационных потоков на предприятии	9
2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ.....	11
3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ.....	12
3.1 Схема помещения	12
3.2 Описание помещений	13
3.3 Анализ возможных каналов утечки информации.....	15
4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ.....	16
4.1 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам	16
4.2 Защита от утечки информации по акустическим каналам	17
4.3 Защита от ПЭМИН	19
4.4 Защита от утечек информации по оптическим каналам	21
5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ	22
ЗАКЛЮЧЕНИЕ.....	26
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	27

ВВЕДЕНИЕ

В современном мире обеспечение информационной безопасности представляет собой важную задачу для организаций. С увеличением объема цифровых данных и постоянным развитием информационных технологий возрастает угроза утечки конфиденциальной информации. Разглашение этой информации может нанести серьезный ущерб как одному человеку, так и всему государству.

Средства защиты информации обеспечивают защиту информации в информационных системах, по сути, представляющих собой совокупность хранимой в базах данных информации, информационных технологий, обеспечивающих ее обработку, и технических средств. Они позволяют предотвратить несанкционированный доступ злоумышленника к ресурсам и данным предприятия, тем самым снизив риск несанкционированных утечки, утраты, искажения, уничтожения, копирования и блокирования информации и, как следствие, нанесения экономического, репутационного или других видов ущерба предприятию. Технические средства защиты информации являются важной частью комплекса мер по обеспечению режима конфиденциальности на предприятии.

Целью данной работы является разработка комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно» на объекте информатизации. Защищаемый объект состоит из десяти помещений: переговорная, кабинет директора, серверная, два санузла, 4 кабинетами и кухней.

Для достижения поставленной цели необходимо сделать следующие задачи:

- провести анализ технических каналов утечек информации;
- провести анализ защищаемого помещения;
- провести анализ рынка и выбрать инженерно-технические средства защиты информации.

1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

1.1 Анализ технических каналов утечки информации

Утечка конфиденциальной информации — это бесконтрольный выход конфиденциальной информации за пределы организации или предприятия, которым она была доверена по службе или стала известна в процессе работы.

Эта утечка может быть следствием:

- разглашения конфиденциальной информации;
- ухода информации по различным, главным образом техническим, каналам;
- несанкционированного доступа к конфиденциальной информации различными способами.

Согласно теме курсовой работы, рассматриваться будет только утечка информации по техническим каналам.

Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка (информации) по техническому каналу – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

ТКУИ подразделяют на: акустические, оптические, радиоэлектронные и материально-вещественные.

Оптический канал утечки представляет собой снятие информации возможно с помощью наблюдения, например, с помощью окон или открытых дверей, также возможно использования фото и видеозаписывающего устройства. Перехват визуальной информации может привести к утечке конфиденциальных данных, в том числе государственной тайны.

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по металлическим проводам.

Электромагнитный канал утечки связан с перехватом электромагнитных излучений, Угроза безопасности представляет собой перехват электромагнитных излучений с помощью специальных устройств, а также считывание информации через систему электропитания.

Акустический и виброакустический канал утечки представляют собой возможность записи и анализа звуковых данных с помощью подслушивающих устройств. В перехватываемых данных может храниться конфиденциальная информация, например

обсуждение проектов. Подслушивание может быть реализована через общую систему отопления или вентиляции, а также из-за наличия окон с выходом на другие здания, появляется возможность съём информации через оконные стекла.

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных носителей с защищаемой информацией. В качестве вещественных носителей чаще всего выступают черновики документов и использованная копировальная бумага, портативные носители информации. С кражей или копированием информации, зафиксированной на материальных носителях, борются в первую очередь организационными мерами, вводя строгий порядок учета и работы с данными видами носителей.

1.2 Структура информационных потоков на предприятии

Информационный поток представляет собой совокупность передаваемых сообщений в логистической системе, служащих для эффективного управления, анализа и контроля логистических операций на предприятии. Корректное управление и обеспечение безопасности информационных потоков играют важную роль в обеспечении конфиденциальности, целостности и доступности данных. Эти потоки могут представляться разнообразными формами, включая бумажные и электронные документы, аудиозаписи, символы и сигналы.

На рисунке 1 представлена схема структуры предприятия и информационных потоков. Красным цветом обозначены открытые потоки, которые включают в себя информацию, не содержащую чувствительных данных и не требующую дополнительных уровней доступа. Черным цветом выделены закрытые потоки, которые содержат важную защищаемую информацию, такую как персональные данные, служебную и коммерческую тайны, информацию об интеллектуальной собственности.

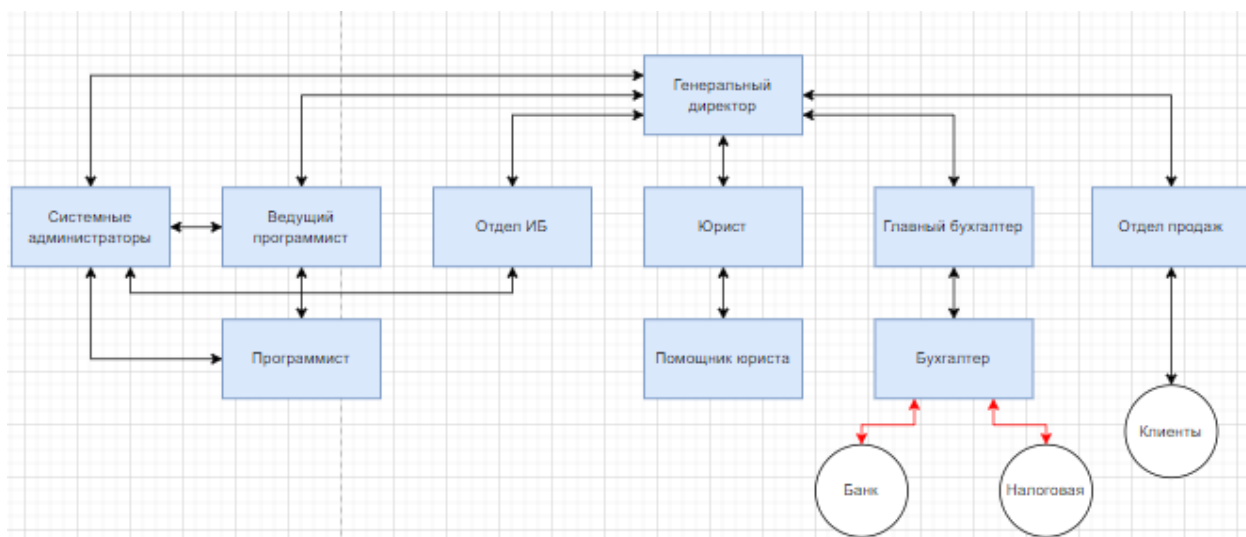


Рисунок 1 – Схема информационных потоков на предприятии

2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Защищаемое предприятие содержит защищаемую информацию, такую как персональные данные, коммерческую тайну и государственную тайну.

В связи с этим составлен список руководящих документов, в которых содержатся требования к защите информации:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».
3. Закон РФ «О государственной тайне» от 21.07.1993 N 5485–1.
4. Федеральный закон от 27 июля 2006 г. No 152-ФЗ «О персональных данных».
5. 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».
6. Приказ ФТЭК России от 11.02.2013 N 17 «Об утверждении требований к защите информации, не составляющей государственную тайну».
7. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
8. Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне».
9. Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации».
10. Межведомственная комиссия по защите государственной тайны 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».
11. СТР. Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам.
12. СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации.

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Схема помещения

Для размещения технических средств защиты на объекте необходимо провести анализ защищаемого помещения, представленного на плане офисного типа предприятия (рисунок 2).

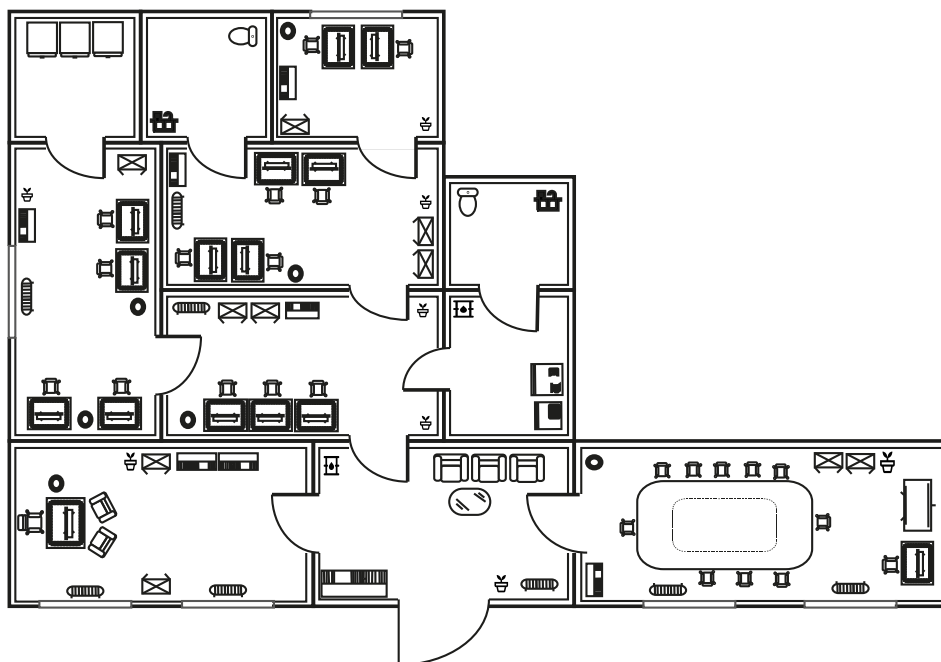
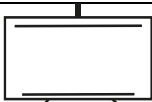
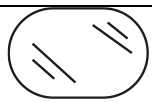


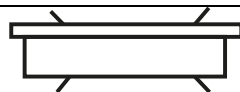


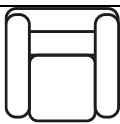



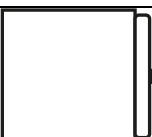
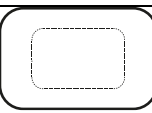
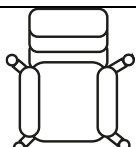



Рисунок 2 – План защищаемого помещения

В таблице 1 представлено описание обозначений, использованных на плане.

Таблица 1 – Описание обозначений

Обозначение	Описание
	Интерактивная доска с проектором
	Журнальный стол
	Книжная полка
	Комнатное растение
	Компьютер

	Компьютерный стол
	Кофе машина
	Кресло
	Кулер для воды
	Кухонный стол
	СВЧ-печь
	Сервер
	Стол переговоров
	Стул руководителя
	Унитаз

3.2 Описание помещений

На рассматриваемом предприятии имеются следующие помещения:

- кабинет директора (20,2 м²);
- переговорная комната (24,1 м²);
- офис 1 (19,4 м²);
- офис 2 (19,1 м²);
- офис 3 (19,5 м²);
- офис 4 (12,1 м²);

- серверная комната (8,7 м²);
- кухня (9,6 м²);
- главный холл (14,1 м²).

Кабинет директора включает в себя: один стул руководителя, два стула, один компьютерный стол, два книжных шкафа, два шкафа для документов, одно мусорное ведро для бумаги, два радиатора отопления, два окна и одно комнатное растение. Данное помещение оснащено шестью розетками.

В переговорной комнате находятся одиннадцать стульев, один стол для переговоров, один компьютерный стол, один компьютер, один книжный шкаф, два шкафа для документов, одна интерактивная доска с проектором, один кулер для воды, два радиатора отопления, два окна и одно комнатных растения. Переговорная комната оснащена восьмью розетками.

В офисе 1 стоят три стула, три компьютерных стола, три компьютера, один книжный шкаф, два шкафа для документов, мусорное ведро и два комнатных растения. В данном помещении находятся шесть розеток.

В офисе 2 есть четыре стула, четыре компьютерных стола, четыре компьютера, один книжный шкаф, два шкафа для документов, одно мусорное ведро для бумаги и одно комнатное растение. Данное помещение оснащено восьмью розетками.

В офисе 3 находятся четыре стула, четыре компьютерных стола, четыре компьютера, один книжный шкаф, один шкаф для документов, два мусорных ведра для бумаги, один радиатор отопления, одно окно и одно комнатное растение. Офис 3 оснащен восьмью розетками.

В офисе 4 находятся два стула, два компьютерных стола, два компьютера, один книжный шкаф, один шкаф для документов, одно мусорное ведро для бумаги, одно окно и одно комнатное растение. В данном помещении 4 розетки.

В серверной комнате расположены три сервера. В данном помещении есть девять розеток.

В кухне есть кулер для воды и кухонный стол, на котором находятся одна кофемашина, одна микроволновая печь и один чайник. Данное помещение включает в себя пять розеток.

Главный холл предназначен для сотрудников предприятия и посетителей. В нем находятся три кресла, один журнальный стол, один книжный шкаф, один кулер для воды, один радиатор отопления, одно комнатное растения и одно окно.

3.3 Анализ возможных каналов утечки информации

В каждом помещении существуют потенциальные маршруты для нежелательной утечки информации, связанные с электромагнитными и электрическими протечками, такими как использование компьютеров и розеток. Декоративные элементы, вроде комнатных растений, могут служить средствами для установки подслушивающих устройств, которые способны передавать информацию через акустический канал.

Существует также риск утечки информации через оптические каналы, например, из-за незакрытых окон или незащищенных дверей. Необходимо также учитывать виброакустический канал, который может использоваться для передачи информации через твердые поверхности, такие как стены или батареи отопления.

Существует возможность вещественно-материального канала утечки информации из-за наличия материальных носителей данных, однако этот канал не может быть полностью заблокирован с использованием технических средств защиты.

В таблице 2 представлены возможные средства пассивной и активной защиты.

Таблица 2 – Активная и пассивная защита информации

Каналы	Источники	Активная защита	Пассивная защита
Акустический	Стены, двери, окна, электрические сигналы	Устройства акустического зашумления	Звукоизоляция переговорной, фильтры для сетей электропитания
Виброакустический	Стекла, стены и иные твердые поверхности	Устройства вибрационного зашумления	Изолирующие звук и вибрацию обшивки стен, дополнительное помещение перед переговорной,
Визуально-оптический	Окна и стеклянные поверхности, двери	Жалюзи, бликующие устройства	Фильтры для сетей электропитания
Электрический Электромагнитный	Компьютеры, сервера, бытовая техника, розетки	Устройства электромагнитного зашумления	Фильтры для сетей электропитания

4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

4.1 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 3. Эти меры активной защиты направлены на обеспечение дополнительного уровня безопасности и предотвращение возможных технических каналов утечки информации в защищаемых помещениях.

Таблица 3 – Активная защита от утечек информации по электрическим каналам

Модель	Цена, руб.	Характеристики	Особенности
Генератор шума SEL SP-44	26 000	Уровень шума затухания 12–90 дБ. Напряжение 220 В \pm 10% 50 Гц. Диапазон частот 10 кГц – 400 МГц. Количество фаз – 1 с заземлением.	Наличие сертификата ФСТЭК, разрешающего использование устройства в выделенных помещениях 3–1 категорий. Функция самодиагностики для оперативного выявления неисправностей и сбоев в работе
Генератор шума ЛГШ-221	36 400	Ток нагрузки – сеть \sim 220 В +10%/-15%, 50 Гц. Напряжение – 220 В. Количество фаз – 1. Потребляемая мощность 10 Вт.	Звуковая и световая индикация работы. Возможно дистанционное управление посредством проводного пульта. Сертифицировано ФСТЭК.
ЛФС-10-1Ф	47 060	Ток нагрузки – 10 А. Напряжение – 220 В с частотой 50 Гц. Уровень шума затухания – не менее	Есть действующие сертификаты ФСТЭК и ГОСТ Р. Прибор для пассивной защиты данных от утечки по кабелям электропроводки. Сглаживает

		60 дБ. Количество фаз – 1. Тип соединения – двухштырьковый разъём / 2 pin.	скачки напряжения, подавляет высокочастотные помехи в сети. Разрешен к применению в целях защиты государственной тайны
--	--	--	--

На основании анализа, проведенного в таблице 2, был выбран генератор шума ЛГШ-221. Оптимальное соотношение цены и качества делает возможным установку достаточного числа подобных устройств в помещениях. Этот выбор дополнительно обоснован наличием сертификата от ФСТЭК и высоким ресурсом работы генератора, который составляет 27 000 часов.

4.2 Защита от утечки информации по акустическим каналам

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

Активные меры безопасности включают в себя систему виброакустической маскировки (таблица 4). Эти меры направлены на предотвращение возможных технических каналов утечки информации, обеспечивая дополнительный уровень безопасности в защищаемых помещениях.

Таблица 4 – 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)
Соната АВ-4Б	44 200	Диапазон воспроизводимого шумового сигнала 175–11200 Гц. Выходное напряжение В 12,5 ± 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.
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)

Исходя из анализа, представленного в таблице 5, было принято решение о выборе системы Соната АВ-4Б. По сравнению с альтернативными системами, предназначенными для предотвращения утечек информации через акустические и вибрационные каналы, данное устройство выделяется как наиболее востребованное, получившее положительные отзывы, и обладающее оптимальным соотношением цена-качество.

4.3 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. В таблице 5 представлены средства активной защиты от ПЭМИН.

Таблица 5 – Активная защита от ПЭМИН

Модель	Цена, руб.	Характеристики	Особенности
Генератор шума ПОКРОВ	32 800	Наличие регулировки уровня шума. Диапазон частот – 0,01–6000 МГц (для изделия, выпускаемого по ВСЦТ.464214.003 ТУ). Электропитание – выполнен в виде сетевого удлинителя с 5 розетками типа F. Мощность – 15 Вт. Режим работы – круглосуточно.	Предназначен для защиты информации от утечки по техническим каналам за счет ПЭМИН путем излучения в окружающее пространство электромагнитного поля шумового сигнала и наводок на линии электропитания и заземления. Является средством активной защиты информации от утечки за счет ПЭМИН типов "А" и "Б", соответствует требованиям ФСТЭК России по 2 классу (сертификат №3757 от 09.06.2017). Сертификат ФСТЭК, СП

Генератор шума ЛГШ-501	29 900	Присутствует регулировка уровня шума, диапазон регулировки уровня выходного шумового сигнала не менее 20 дБ. Диапазон частот – 0,01–1800 МГц. Уровень шума – от -28 дБ(мкА/м*√кГц) до 57 дБ(мкВ/м*√кГц). Электропитание – однофазная сеть переменного тока 187 В-242 В. Мощность – не более 45 ВА. Режим работы – круглосуточно.	Оснащено визуальной системой индикации 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.
Базовый генератор маскирующих радиопомех ГШ-111Б	39 000	Наличие регулировки уровня шума. Диапазон частот 10 кГц - 1800 МГц. Уровень шума от 0 до - 30 дБ. Электропитание сетевое 220 В 50 Гц или через внешний адаптер постоянного тока 12 В 2А.	На задней панели генератора расположены отдельные выходы для подключения магнитной и радиочастотных антенн, а также выход на внешнее устройство наведения шумового сигнала на провода. Интерфейс для управления и контроля ГШ по сети Ethernet 10/100 Мбит/с.

В качестве средства активной защиты от ПЭМИН был выбран генератор шума ЛГШ-501. Этот выбор обоснован широким диапазоном частот (от 0,01 до 1800 МГц) и круглосуточным режимом работы.

4.4 Защита от утечек информации по оптическим каналам

Для предотвращения функционирования оптического канала утечки информации можно установить шторы, жалюзи, либо тонирование пленки на стеклах. Были выбраны жалюзи как наиболее приемлемый вариант защиты ввиду своей удобства и экономичности.

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 «ЛГШ-221»;
- система виброакустической защиты «Соната АВ-4Б»;
- генератор шума «ЛГШ-501» от ПЭМИН
- жалюзи на семь окон;
- три усиленные двери с толщиной 4 мм, обшитые металлическим листом не

менее 2 мм, внутри – звукоизоляционный материал.

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);
- трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

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

Таблица 6 – Необходимое оборудование

Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Сетевой генератор шума «ЛГШ-221»	36 400	1	36 400
Генератор шума «ЛГШ-501»	29 900	3	89 700

Блок электропитания и управления «Соната-ИП4.3»	21 600	1	21 600
Генератор-акустоизлучатель «Соната СА-4Б1»	3 540	15	53 100
Генератор-вибровозбудитель «Соната СА-4Б»	7 440	71	528 400
Размыкатель телефонной линии «Соната ВК4.1»	6 000	2	12 000
Размыкатель слаботочной линии «Соната ВК4.2»	6 000	1	6 000
Размыкатель линии «Ethernet» «Соната ВК4.1»	6 000	1	6 000
Пульт управления «Соната-ДУ 4.3»	7 680	1	7 680
Шторы-плиссе Blackout	4 900	6	29 400
Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	83 619	3	250 857
Итого			1 041 137

В трех помещениях установлены усиленные звукоизолирующие двери, как показано на рисунке 3. На каждом окне установлены шторы. Системы «Соната СА-4Б1» и «Соната СВ-4Б» размещены в соответствии с указаниями производителя. «ЛГШ-221» и «ЛГШ-501» находятся рядом с «Соната-ИП4.3» и подключены к ней. Все выключатели установлены в соответствии с рекомендациями производителя. В таблице 7 приведено описание обозначений устройств.

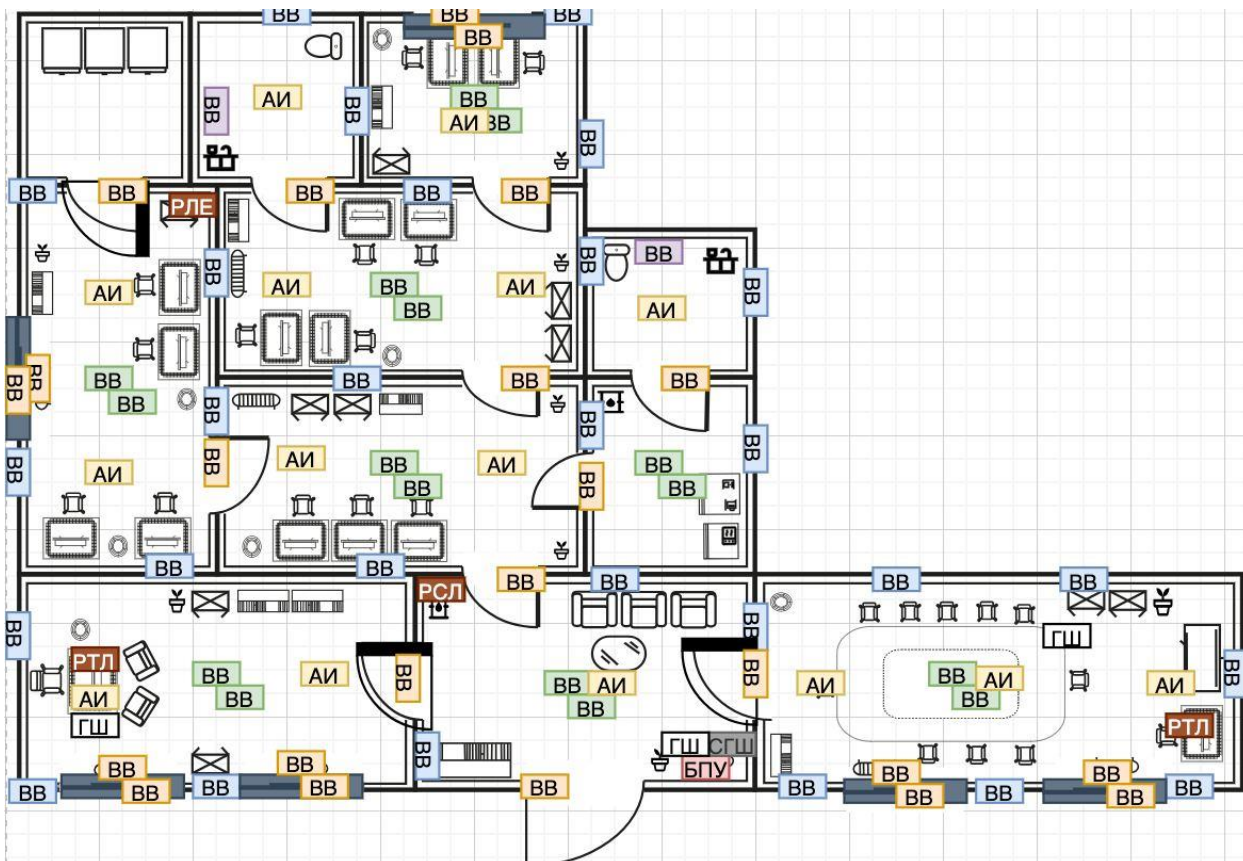










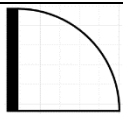



Рисунок 3 – Схема расстановки устройств

Таблица 7 – Описание обозначений устройств

Обозначение	Устройство	Количество, шт.
	Блок электропитания и управления «Соната-ИП4.3»	1
	Генератор-акустоизлучатель «Соната СА-4Б1»	15
	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)	30
	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)	16
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)	23
	Генератор-вибровозбудитель «Соната СВ-4Б» (трубопровод)	2

	Сетевой генератор шума «ЛГШ-221»	1
	Генератор шума «ЛГШ-501»	1
	Размыкатель телефонной линии «Соната ВК4.1»	2
	Размыкатель слаботочной линии «Соната ВК4.2»	1
	Размыкатель линии «Ethernet» «Соната ВК4.1»	1
	Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	3
	Шторы-плиссе BlackOut	6

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной курсовой работы был проведен анализ потенциальных каналов утечки информации. Эти каналы включают акустические, виброакустические, оптические, электрические и электромагнитные технические каналы, а также каналы, связанные с ПЭМИН. Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для нашего объекта, также был разработан план установки выбранных средств защиты. В результате была предложена система защиты от утечек информации через различные технические каналы.

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.
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.