

**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**

Вариант №91

Выполнил:

студент группы N34501
Митрохович Г.А.



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	Митрохович Герман Андреевич
	(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 рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

Рекомендуемая литература

Руководитель		(Подпись, дата)
Студент		20.12.2023
		(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Митрохович Герман Андреевич

(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	20.12.2023	20.12.2023	
2	Анализ теоретической составляющей	20.12.2023	20.12.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	20.12.2023	20.12.2023	
4	Представление выполненной курсовой работы	26.12.2023	26.12.2023	

Руководитель

(Подпись, дата)

Студент

26.12.2023

(Подпись, дата)

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

Студент	Митрохович Герман Андреевич
	(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 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		20.12.2023 (Подпись, дата)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	6
1. ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ.....	7
1.1 Информационные потоки	7
1.2 Структура информационных потоков	7
2. РУКОВОДЯЩИЕ ДОКУМЕНТЫ	9
3 ОПИСАНИЕ И АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	10
3.1 Схема помещения	10
3.2 Описание помещений	13
3.3 Каналы утечки информации	15
4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ.....	17
4.1 Выбор средств защиты	17
4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам	17
4.3 Защита от утечки информации по (вибро-) акустическим каналам	19
4.4 Защита от побочных электромагнитных излучений и наводок	21
4.5 Защита от утечек информации по оптическим каналам	23
5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ	24
ЗАКЛЮЧЕНИЕ.....	29
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	30

ВВЕДЕНИЕ

Средства защиты информации (СЗИ) обеспечивают безопасность информационных систем, объединяющих данные в базах, и технологии их обработки. Они предотвращают несанкционированный доступ злоумышленников к ресурсам и информации предприятия, минимизируя риски утечки, потери, искажения, уничтожения, копирования или блокирования данных. Это позволяет предприятию избежать экономических, репутационных и других видов ущерба. Разработка эффективных мер по обеспечению безопасности информации является ключевой задачей в настоящее время. Технические средства защиты информации являются важной частью комплекса мер для поддержания конфиденциальности на предприятии.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации. Защищаемое предприятие состоит из десяти помещений, включая коридоры и представляют собой офис предприятия, для штатных работников, переговорной, кабинетом директора, серверной, санузлом, кухней, главным холлом, бухгалтерией, кабинетом секретаря и коридором.

1. ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

1.1 Информационные потоки

Информационный поток представляет собой обмен сообщениями в рамках логистической системы между ней и внешней средой, необходимый для управления, анализа и контроля логистических операций. Он играет ключевую роль в функционировании предприятия, поэтому корректное управление и защита этого потока являются критически важными для обеспечения конфиденциальности, целостности и доступности информации. Информационные потоки могут существовать в виде бумажных или электронных документов, звука, символов и сигналов.

Информационные потоки подразделяются по разным критериям. Для целей данной работы они классифицируются на две основные категории: открытые и закрытые.

Открытые информационные потоки представляют собой данные, доступные сотрудникам и другим заинтересованным лицам в пределах предприятия без специальных ограничений. Эти потоки включают информацию, не содержащую чувствительных данных и не требующую дополнительных уровней доступа. Примеры открытых информационных потоков включают в себя общие отчеты, обновления проектов и компании. Они способствуют эффективному внутреннему обмену информацией и содействуют открытости и прозрачности внутри организации.

Закрытые информационные потоки содержат конфиденциальную, чувствительную информацию, требующую высокого уровня защиты. Эти потоки включают в себя финансовые данные, персональные записи, интеллектуальную собственность и другие данные, которые, если попадут в неправильные руки, могут причинить ущерб предприятию. Защита закрытых информационных потоков включает в себя строгие политики доступа, шифрование данных, мониторинг активности и другие меры безопасности.

1.2 Структура информационных потоков

На рисунке 1 зеленым цветом обозначены открытые потоки, а красным цветом - закрытые потоки.

К информации, передающейся по открытым потокам, относятся бухгалтерская и финансовая отчетность, налоговые сведения, а также обратная связь от клиентов, обратившихся в службу техподдержки.

К защищаемой информации, передающейся по закрытым потокам, относятся персональные данные клиентов и сотрудников, служебная тайна, коммерческая тайна и сведения о разрабатываемом программном продукте (программный код, назначение и т. д.).

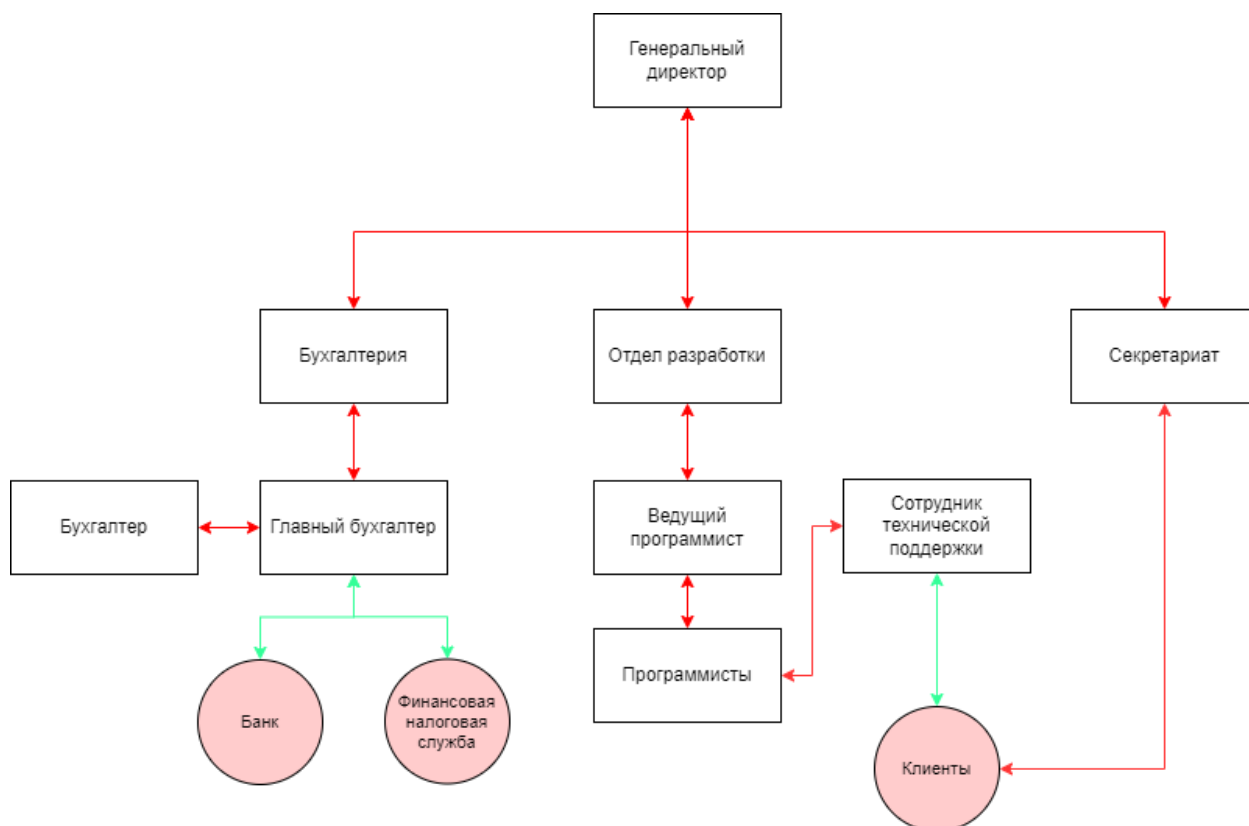


Рисунок 1 – Схема информационных потоков на предприятии

2. РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Для формирования требований по защите информации в организации использовались следующие документы:

1. ГОСТ Р ИСО/МЭК 27001-2006 "Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования";
2. ГОСТ Р 51583-2014 "Порядок создания автоматизированных систем в защищенном исполнении";
3. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "О информации, информационных технологиях и о защите информации";
4. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне";
5. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";
6. Федеральный закон от 21.12.1994 N 69-ФЗ "О пожарной безопасности";
7. Часть 4 статьи 74 Федерального закона от 22 июля 2008 года N 123-ФЗ "Технический регламент о требованиях пожарной безопасности";
8. Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи";
9. Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации".

3 ОПИСАНИЕ И АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Схема помещения

Необходимо провести анализ защищаемого помещения, чтобы разместить технические средства защиты на объекте. План помещения предприятия офисного типа представлен на рисунке 2. В таблице 1 представлены описание обозначений, изображенных на плане.

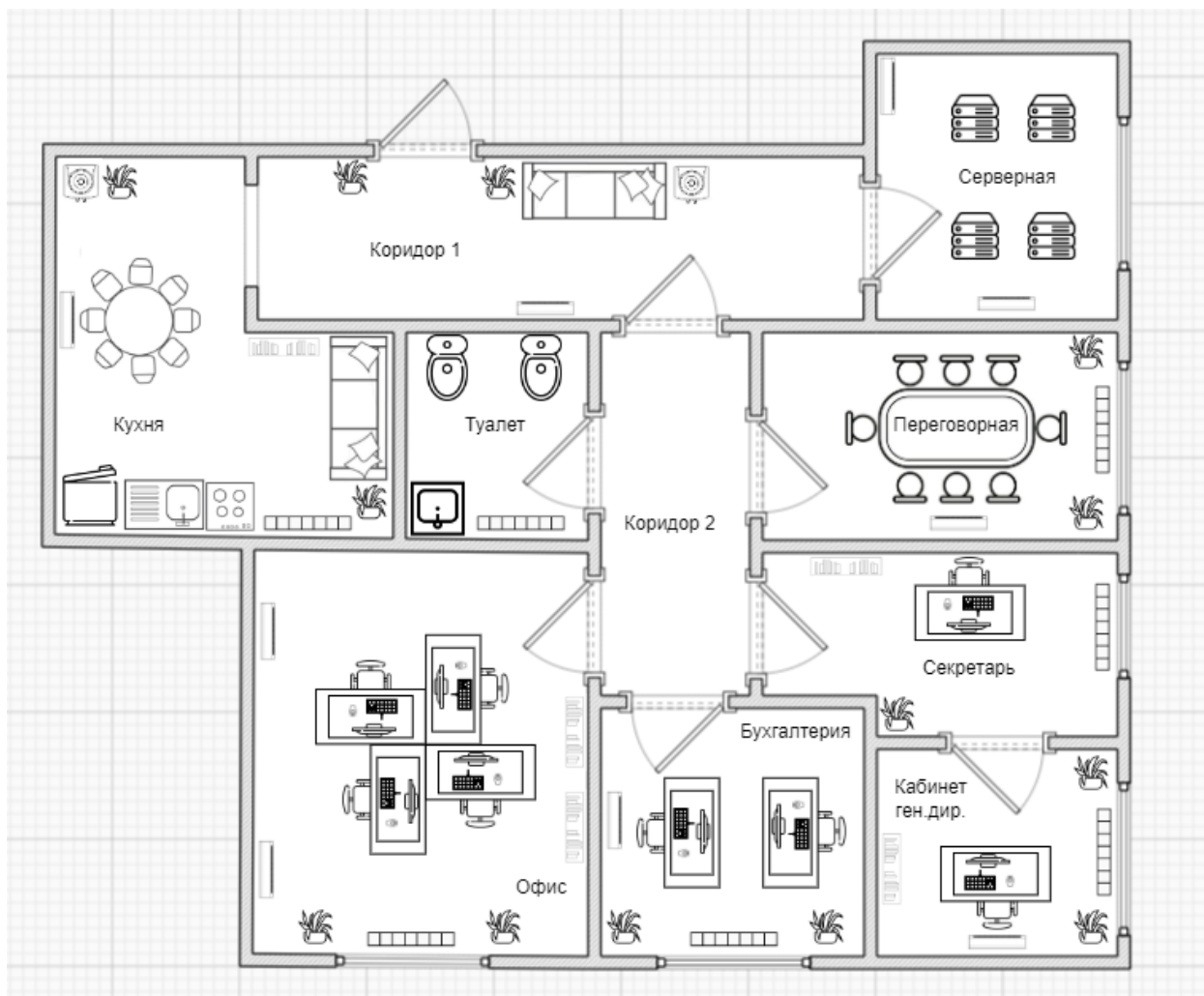



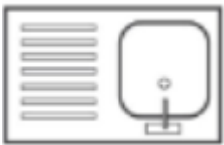

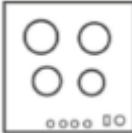




Рисунок 2 – План защищаемого помещения

Таблица 1 – Описание обозначений

Обозначение	Описание
	Офисный стул
	Компьютерный стол
	Стол переговоров
	Кухонный стол
	Компьютер
	Полка
	Радиатор отопления
	Кулер для воды
	Туалет

Продолжение таблицы 1

Обозначение	Описание
	Раковина
	Комнатное растение
	Кондиционер
	Раковина на кухне
	Диван
	Печь
	Холодильник
	Сервер

3.2 Описание помещений

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

- кабинет директора (2,93 м²);
- переговорная комната (4,56 м²);
- офис разработки (8,36 м²);
- офис бухгалтерии (4,04 м²);
- серверная комната (3,97 м²);
- кухня (6,33 м²);
- кабинет секретаря (3,89 м²);
- коридор 1 (6,10м²).

Кабинет директора:

- компьютерный стол,
- компьютер,
- 2 комнатных растения,
- книжная полка,
- кондиционер,
- офисный стул.

Переговорная комната:

- стол для переговоров,
- 8 стульев,
- кондиционер,
- 2 комнатных растения,
- радиатор отопления.

Офис разработки:

- 4 компьютерных стола,
- 4 офисных стула,
- 4 компьютера,
- 2 кондиционера,
- 2 комнатных растения,
- радиатор отопления,
- 2 книжные полки.

Офис бухгалтерии:

- 2 компьютерных стола,
- 2 офисных стула,
- 2 компьютера,
- 2 комнатных растения,
- радиатор отопления,
- кондиционер.

Серверная комната:

- 4 сервера,
- 2 кондиционера.

Кухня:

- 8 стульев,
- кухонный стол,
- диван,
- 2 комнатных растения,
- кондиционер,
- кулер для воды,
- холодильник,
- раковина,
- печь,
- радиатор отопления,
- книжная полка.

Коридор 1:

- диван,
- 2 комнатных растений,
- кулер для воды,
- кондиционер.

Кабинет секретаря:

- комнатное растение,
- компьютерный стол,

- офисный стул,
- компьютер,
- радиатор отопления,
- книжная полка.

3.3 Каналы утечки информации

Проведем анализ возможных каналов утечки информации в предложенной организации с учетом специфики помещений и используемого оборудования.

1. Электромагнитные и электрические каналы:

- Компьютеры: источник электрических сигналов и электромагнитных полей, которые могут быть подвержены перехвату и анализу.
- Серверная комната: сервера могут испускать электромагнитные излучения при работе, которые могут быть использованы для перехвата информации.

2. Акустический канал:

- Комнатные растения: могут использоваться для скрытой установки устройств для аудиозаписи и передачи информации через звуковые волны.
- Переговорная комната: Место, где могут быть проведены незаконные аудиозаписи переговоров.

3. Оптические каналы:

- Окна и двери: Незакрытые окна и небезопасные двери могут привести к визуальной утечке информации.

4. Виброакустический канал:

- Твердые поверхности (стены, батареи отопления): могут передавать вибрации, которые могут быть использованы для перехвата звука из помещения.

5. Вещественно-материальный канал:

- Носители информации: Книжные полки, компьютеры, документы и другие предметы могут использоваться для несанкционированного доступа к информации.

Учитывая вышеупомянутые каналы утечки информации, следует принять соответствующие меры по обеспечению безопасности:

- Установка устройств для защиты от электромагнитных и электрических утечек;
- Установка устройств для защиты от виброакустических и акустических каналов утечки;
- Проведение регулярной проверки помещений на наличие скрытых устройств слежения и установка устройств защиты для обеспечения защиты от вещественно-материальных утечек;
- Обеспечение физической безопасности и защиты от визуального восприятия конфиденциальной информации, закрывая окна и двери при работе с конфиденциальной информацией.

4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

4.1 Выбор средств защиты

Для обеспечения необходимого уровня комплексной безопасности информации, требуется оснастить помещения специальными средствами и устройствами, перечисленными в таблице 2. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки конфиденциальной информации.

Таблица 2 – Активная и пассивная защита информации

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

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

Пассивная защита включает себя размещение фильтров в электропитании всех помещений.

Активная защита заключается в использовании системы белого шума в сети, которая создает фоновый шум, маскирующий колебания, вызванные звуковыми волнами или работой электронных устройств. Модели устройств, относительно которых будет идти дальнейший анализ, и их характеристики представлены в таблице 3.

Таблица 3 – Активная защита от утечек информации по электрическим каналам

Модель	Цена, руб.	Характеристики	Особенности
Соната-РС3	32 400	Работа от сети ~220 В +10%/-15%, 50 Гц. Потребляемая мощность – 10Вт. Продолжительность работы не менее 8 часов.	Звуковая и световая индикация работы. Возможно дистанционное управление посредством проводного пульта.
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.
Соната- РС1	16 520	Диапазон частот до 1 ГГц, регулировка уровня шума в 1 частотной полосе. Напряжение 220 В.	Возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus)
Генератор шума Покров	32 800	Диапазон частот 10 кГц – 6000 МГц. Мощность 15 Вт.	Централизованное управление и контроль по Ethernet (для исполнения 2), для применения в системах пространственного

		Наработка на отказ 5000 часов.	зашумления. Независимая регулировка уровней электромагнитного поля шумового сигнала и шумового сигнала в линии электропитания и заземления.
--	--	-----------------------------------	--

На основании анализа, проведенного в таблице 2, был выбран генератор шума «Покров». Оптимальный вариант по соотношению цена и качество позволяют установить достаточное количество подобных устройств в помещениях. Кроме того, этот выбор был обоснован самым широким диапазоном частот.

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

Пассивные меры безопасности включают в себя создание тамбурной зоны перед переговорной комнатой и установку усиленных дверей. Для обеспечения звукоизоляции переговорной комнаты и кабинета генерального директора используются специальные материалы для звукоизоляции стен.

Таблица 4 – Активная защита от утечек информации по (вибро-)акустическим каналам

Модель	Цена, руб.	Характеристики	Особенности
ЛГШ-404	35 100	Электропитание 220 В/50 Гц. Максимальное количество излучателей – 40. Диапазон воспроизводимого шумового сигнала 175–11200 Гц.	Вариативность количества подключаемых к генераторному блоку преобразователей. К двухканальному виброакустическому генератору шума ЛГШ-404 можно одновременно подключить до 20 ЛВП-10 и до 20 ЛВП-2А. Счетчик времени наработки и световая индикация режима работы. Проводной пульт

			дистанционного управления в комплекте
Шорох 5Л	21 500	<p>Максимальное количество излучателей – 40.</p> <p>Электропитание 220 (+10% - 15%) В (есть возможность работы системы от источника питания 12В).</p> <p>Количество октавных полос для регулировки уровня мощности шума – 7.</p>	<p>Сетевой генератор шума.</p> <p>Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.</p>

Продолжение таблицы 4

Модель	Цена, руб.	Характеристики	Особенности
Соната АВ-4Б	44 200	<p>Диапазон воспроизводимого шумового сигнала 175–11200 Гц.</p> <p>Выходное напряжение В 12,5 ± 0,5.</p> <p>Электропитание сеть ~220 В/50 Гц.</p>	<p>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.</p>

SEL SP-157 Шагрень	47 400	Диапазон воспроизводимого шумового сигнала 90–11200 Гц. Максимальное количество излучателей – 64. Электропитание 220В/50Гц.	Защита паролем настроек системы. Отсчёт времени наработки генерации шума по каждому каналу с выводом на экран. Непрерывный контроль состояния системы и каждого отдельного излучателя.
-----------------------	--------	---	--

На основе анализа, представленного в таблице 4, было принято решение в пользу системы «СОНАТА АВ-4Б» в качестве оптимального выбора. В сравнении с альтернативными системами, предназначенными для предотвращения утечек информации через акустические и вибрационные каналы, данная система получила признание как наиболее востребованная и имеет множество положительных отзывов. Одной из особенностей «Соната АВ-4Б» является применение принципа «единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)», что гарантирует высокую надежность в защите информации.

4.4 Защита от побочных электромагнитных излучений и наводок

Таблица 5 – Активная защита от побочных электромагнитных излучений и наводок

Модель	Цена, руб.	Характеристики	Особенности
ЛГШ 503	44 200	Диапазон частот 10 кГц - 1800 МГц Уровень шума от -26 дБ (мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц). ц. Мощность – 45 Вт.	Оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Оснащен счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы в режиме формирования маскирующих помех. Прибор имеет возможность подключения проводного дистанционного

			управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».
--	--	--	---

Продолжение таблицы 5

Модель	Цена, руб.	Характеристики	Особенности
Соната-РЗ.1	39 000	Электропитание – 220 В +10%/-15%, 50 Гц. Мощность – 10 Вт. Продолжительность непрерывной работы не менее 8 ч	Обеспечивает защиту информации от утечки за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума, а также наводок на линии сети электропитания и заземления путем индуцирования в них маскирующих шумовых напряжений.
ЛГШ-513	33 120	Диапазон частот 10 кГц - 1800 МГц. Уровень шума от -18 дБ(мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц). Мощность – не более 45 ВА. Режим работы – круглосуточно.	Изделие «ЛГШ-513» оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Изделие «ЛГШ-513» оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех.

Генератор шума Пульсар	24 525	Диапазон частот 10 кГц - 6 ГГц. Электропитание – однофазная сеть переменного тока 187–242 В. Мощность – 50 ВА.	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).
------------------------------	--------	--	---

Был выбран генератор шума «ЛГШ-503» в качестве активного средства защиты от ПЭМИН. Этот выбор обоснован широким диапазоном частот (от 10 кГц до 1800 МГц) и возможностью круглосуточной работы. Также устройство поддерживает использование проводного дистанционного управления и контроля, что обеспечивается программно-аппаратным комплексом «Паутина».

4.5 Защита от утечек информации по оптическим каналам

Для обеспечения защиты помещения от возможной фото-видеосъемки или визуального наблюдения следует установить жалюзи на окна и также воспользоваться доводчиками для дверей.

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 «Покров»;
- система виброакустической защиты «Соната АВ-4Б»;
- генератор шума «ЛГШ-503» от ПЭМИН
- жалюзи на шесть окон;
- четыре усиленных 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);
- 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


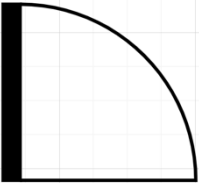

Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Сетевой генератор шума «Покров»	32 800	1	32 800
Генератор шума «ЛГШ-503»	44 200	4	176 800
Блок электропитания и управления «Соната-ИП4.3»	21 600	1	21 600
Генератор-акустоизлучатель «Соната СА-4Б1»	3 540	10	35 400
Генератор-вибровозбудитель «Соната СА-4Б»	7 440	63	468 720
Рызмыкатель телефонной линии «Соната ВК4.1»	6 000	3	18 000
Рызмыкатель слаботочной линии «Соната ВК4.2»	6 000	1	6 000
Рызмыкатель 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	4	334 476
Итого			1 136 876

В четырех помещениях установлены усиленные звукоизолирующие двери, как изображено на схеме 3. На каждом из окон установлены шторы в количестве 6 штук. Системы «Соната СА-4Б1» и «Соната СВ-4Б» размещены согласно рекомендациям производителя. «ЛГШ-221» и «ЛГШ-503» расположены рядом с устройством «Соната-ИП4.3» и подключены к нему. Все выключатели установлены согласно предписаниям производителя. В таблице 7 приведены обозначения устройств с их описанием.

Таблица 7 – Описание обозначений устройств

Обозначение	Устройство	Количество, шт.
БПУ	Блок электропитания и управления «Соната-ИП4.3»	1
АИ	Генератор-акустоизлучатель «Соната СА-4Б1»	10
ВВ	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)	16
ВВ	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)	25
ВВ	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)	20
ВВ	Генератор-вибровозбудитель «Соната СВ-4Б» (трубопровод)	2
РЛЕ	Размыкатель линии «Ethernet» «Соната-ВК4.3»	1
РСЛ	Размыкатель слаботочной линии «Соната-ВК4.2»	1
РТЛ	Размыкатель телефонной линии «Соната-ВК4.1»	3
СГШ	Сетевой генератор шума «Покров»	1

Продолжение таблицы 7

Обозначение	Устройство	Количество, шт.
	Генератор шума «ЛГШ-503»	4
	Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	4
	Шторы-плиссе BlackOut	6

ЗАКЛЮЧЕНИЕ

В ходе разработки текущей курсовой работы был осуществлен анализ как открытых, так и закрытых информационных потоков в организации. Также был составлен перечень руководящих документов, необходимых для эффективного функционирования предприятия. Далее был проведен детальный анализ уровня безопасности помещений, в результате которого были выявлены потенциальные каналы утечки информации.

На основе анализа были выбраны соответствующие средства защиты информации, опираясь на актуальные рыночные данные. Затем был разработан план размещения технических средств защиты информации, и были произведены расчеты стоимости его внедрения.

В результате выполненной работы был создан план по обеспечению защиты помещений от потенциальных каналов утечки информации, включая ПЭМИН, а также электрические, акустоэлектрические, электромагнитные, акустические, виброакустические и оптические пути передачи информации.

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. Detector Systems: Системы комплексной безопасности [Электронный ресурс]. – Режим доступа: <https://detsys.ru/> (дата обращения: 01.11.2023).