

**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.**

Вариант 41»

Выполнил:

студент группы N34481

Азатжонов Акбаржон Азизжон угли



Проверил преподаватель:

Попов Илья Юрьевич

Отметка о выполнении:

Санкт-Петербург
2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Азатжонов Акбаржон Азизжон угли
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34481
Направление (специальность)	10.03.01. - Технологии защиты информации
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии.
Задание	Проектирование инженерно-технической системы защиты информации на предприятии.

Краткие методические указания

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

Содержание пояснительной записки

Пояснительная записка включает следующие разделы - введение, анализ технических каналов утечки информации, руководящие документы, анализ защищаемых помещений, анализ рынка технических средств, описание расстановки технических средств, заключение, список литературы.

Рекомендуемая литература

1. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.

Руководитель	Попов Илья Юрьевич
	(Подпись, дата)
Студент	Азатжонов Акбаржон Азизжон угли
	(Подпись, дата)



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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Азатжонов Акбаржон Азизжон угли
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34481

Направление (специальность) 10.03.01. - Технологии защиты информации


Руководитель Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО
(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
		Планируемая	Фактическая	
1	Создание плана КР	24.10.2023	24.10.2023	
2	Анализ теоретической составляющей	28.10.2023	28.10.2023	
3	Составление текста КР	02.11.2023	03.11.2023	
4	Представление выполненной КР	26.12.2023	26.12.2023	

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Азатжонов Акбаржон Азизжон угли
(Подпись, дата) 

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент Азатжонов Акбаржон Азизжон угли
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34481

Направление (специальность) 10.03.01. - Технологии защиты информации

Руководитель Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО
(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 предприятия. Задачами является анализ защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.

2. Характер работы

☐ Расчет ☒ Конструирование
☐ Моделирование ☐ Другое

3. Содержание работы

1. Введение. 2. Анализ технических каналов утечки информации. 3. Руководящие документы. 4. Анализ защищаемых помещений. 5. Анализ рынка технических средств. 6. Описание расстановки технических средств. 7. Заключение. 8. Список литературы

4. Выводы

В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Азатжонов Акбаржон Азизжон угли
(Подпись, дата) 

«__» _____ 20__ г.

Оглавление

ВВЕДЕНИЕ.....	6
1. АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ.....	7
2. РУКОВОДЯЩИЕ ДОКУМЕНТЫ	9
3. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ.....	11
4. АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ	15
5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ	20
ВЫВОДЫ.....	23
СПИСОК ЛИТЕРАТУРЫ.....	24

ВВЕДЕНИЕ

Функционирование любого объекта (предприятие) зависит от множества факторов, и один из самых важных – это информация и уровень защиты этой информации от утечек, кражи и потерь. Таким образом, обеспечение безопасности информации становится одной из первостепенных задач, когда речь идет о сохранении работоспособности объекта.

Данная работа базируется на знании физической природы возникновения технических каналов утечки информации и методов ведения технической разведки. Правильное определение потенциальных угроз на предпроектном этапе построения системы противодействия промышленному шпионажу позволит в дальнейшем выбирать оптимальные меры и средства защиты.

При выявлении технических каналов утечки информации необходимо рассматривать всю совокупность элементов защиты, включающую основное оборудование технических средств обработки информации, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы вентиляции и т. п.

В данном курсовом проекте рассмотрен процесс разработки комплекса инженерно-технической защиты информации составляющей государственную тайну с уровнем «секретно» на объекте информатизации. Защищаемый объект состоит из семи помещений: зона приема товара, склад, офисная зона, туалет, кабинет директора, переговорная, зона упаковки.

1. АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечка информации — неправомерная передача конфиденциальных сведений (материалов, важных для различных компаний или государства, персональных данных граждан), которая может быть умышленной или случайной.

Каналы утечки информации — методы и пути утечки информации из информационной системы; паразитная (нежелательная) цепочка носителей информации, один или несколько из которых являются (могут быть) правонарушителем или его специальной аппаратурой.

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

В качестве источника сигнала могут быть:

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

Среда распространения сигнала - физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Она характеризуется набором физических параметров, определяющих условия перемещения сигнала. Основными параметрами, которые надо учитывать при описании среды распространения, являются:

- физические препятствия для субъектов и материальных тел;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;
- вид и мощность помех для сигнала.

Приемник выполняет функцию, обратную функции передатчика. Он производит:

- выбор носителя с нужной получателю информацией;
- усиление принятого сигнала до значений, обеспечивающих съём информации;
- съём информации с носителя;
- преобразование информации в форму сигнала, доступную получателю

(человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

Таким образом, описание ТКУИ должно включать в себя:

- источник угрозы (приемник информативного сигнала)
- среда передачи информационного сигнала
- источник (носитель) информации

Основным признаком для классификации технических каналов утечки информации является физическая природа носителя. По этому признаку ТКУИ делятся на:

- оптические;
- радиоэлектронные;
- акустические;
- материально-вещественные.

Носителем информации в оптическом канале является электромагнитное поле (фотоны). Оптический диапазон подразделяется на:

- дальний инфракрасный поддиапазон 100–10 мкм (3–300 ТГц);
- средний и ближний инфракрасный поддиапазон 10–0,76 мкм (30–400 ТГц);
- видимый диапазон (сине-зелёно-красный) 0,76–0,4 мкм (400–750 ТГц).

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон частот радиоэлектронного канала занимает полосу частот от десятков ГГц до звукового.

2. РУКОВОДЯЩИЕ ДОКУМЕНТЫ

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 ТАЙНЫ РЕШЕНИЕ No 199 от 21.01.2011г. "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

На рисунке представлен план защищаемого помещения.

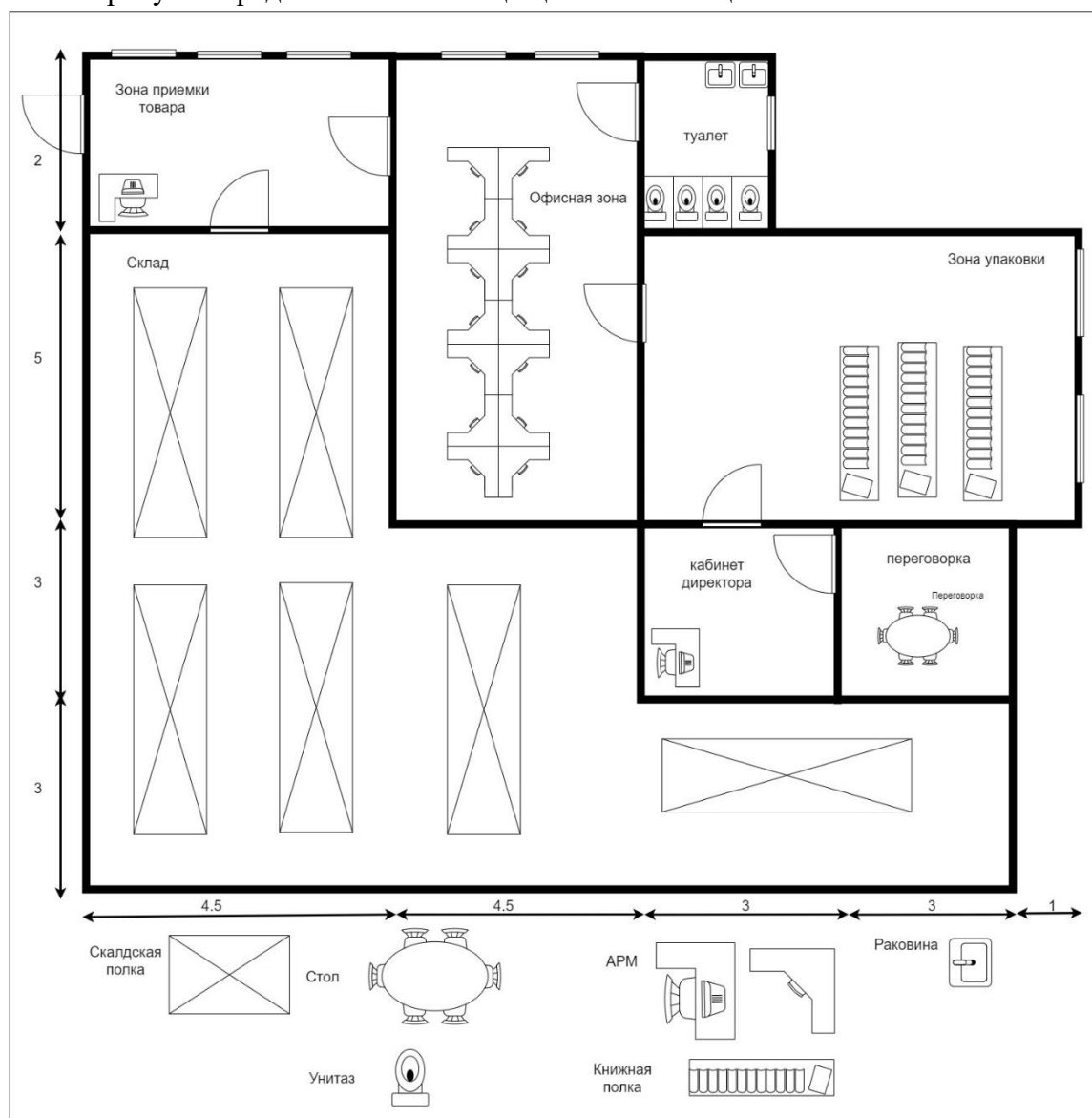


Рисунок 1 – План защищаемого помещения

На рисунке 2 представлена схема информационных потоков.

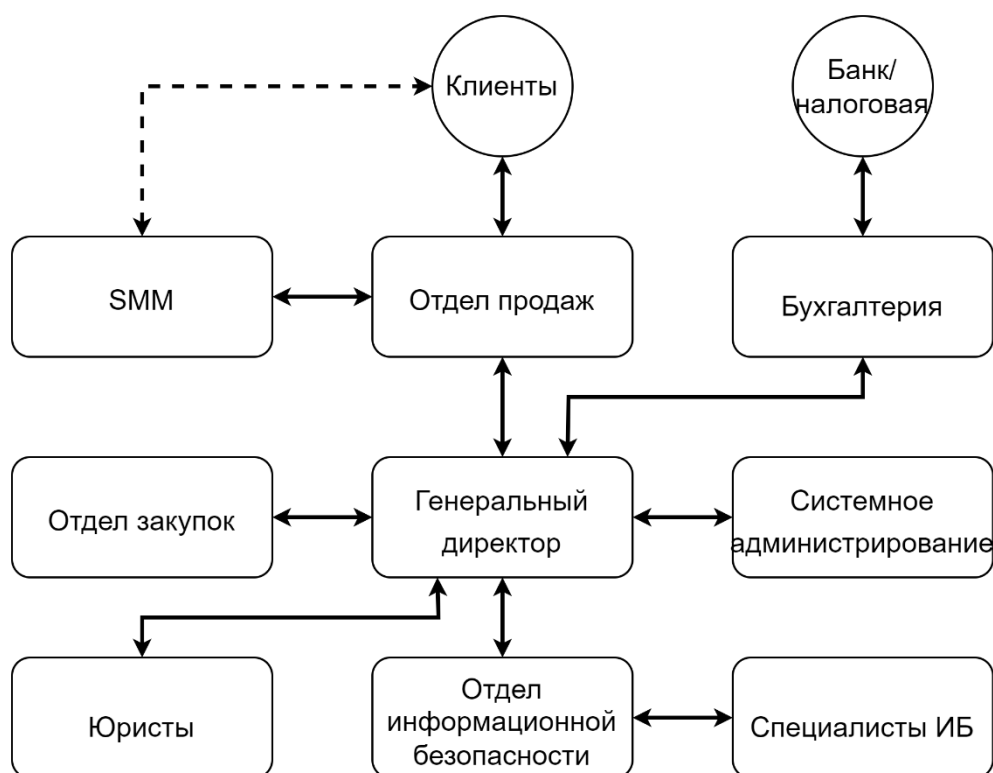


Рисунок 2 – Информационные потоки

Описание информационных потоков:

Открытые потоки:

SMM – клиенты (вопросы, связанные с рекламой)

Закрытые потоки:

Отдел продаж – SMM (вопросы, связанные с привлечением клиентов)

Отдел продаж – клиенты (информация о сделках и предоставленных услугах)

Генеральный директор – юристы (юридические вопросы)

Генеральный директор – отдел закупок (информация о закупаемых товарах)

Генеральный директор – отдел закупок (информация о продаваемых товарах)

Генеральный директор – отдел информационной безопасности (вопросы, связанные с ИБ)

Генеральный директор – системное администрирование (вопросы, связанные с функционированием технического оснащения, ПО, сайта и пр.)

Генеральный директор – бухгалтерия (вопросы, связанные с финансированием, зарплатными выплатами, налогами)

Отдел информационной безопасности – специалисты ИБ (вопросы, связанные с ИБ)

Бухгалтерия – банк/налоговая (вопросы, связанные с движением денежных средств)

Информация ограниченного доступа:

1. Персональные данные сотрудников.
2. Персональные данные клиентов.
3. Техническая информация (логины, пароли и т. д.).
4. Коммерческая тайна (данные о заказах и продажах).
5. Государственная тайна (секретно) – заказы, связанные с государственными заказами.

3.1 Описание помещений

Защите подлежат следующие помещения:

1. Зона приема товара (9 м²)
2. Офисная зона (31,5 м²)
3. Туалет (4 м²)
4. Зона упаковки (35 м²)
5. Кабинет директора (9 м²)
6. Переговорка (9 м²)
7. Склад (94,5 м²)

В зоне приема товара находится стол, стул, компьютер и три окна с батареями под ними.

В складском помещении находится 6 складских полок.

В офисной зоне находится 14 столов, стульев и компьютеров, 2 окна с батареями под ними.

В туалете находится 4 кабинки, две раковины и окно с батареей под ним.

В зоне упаковки находится 3 полки и 2 окна с батареями под ними.

В кабинете директора находится стол, стул, компьютер.

В переговорке находится 6 стульев и стол.

3.2 Анализ возможных утечек информации

Просмотр помещений с улицы ввиду того, что офис находится на 2 этаже, невозможен. Но с северной и восточной сторон находятся здания, допускающие просмотр через окна.

Так как возможно прослушивание помещения из соседних домов через открытые окна и форточки с помощью направленных микрофонов, существует потенциальный канал утечки акустической информации.

Так как возможен съем информации о ведущихся в помещении разговорах с оконных стекол, за счет их вибрации, при использовании лазерного микрофона, при расположении поста перехвата в жилом доме, существует еще один потенциальный канал утечки акустической информации.

В каждом помещении есть розетки, следовательно существует угроза утечки информации по электрическому и электромагнитному каналам.

Материально-вещественный канал утечки информации регулируется политикой безопасности компании, поэтому в рамках курсовой работы не рассматривается.

3.3 Выбор средств защиты информации

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещение средствам защиты, приведенными в таблице 1.

Таблица 1 – Активная и пассивная защита

Каналы	Источники	Пассивная защита	Активная защита
акустический акустоэлектрический	окна, двери, электрические сети, проводка	звукоизоляция переговорной, фильтры для сетей электропитания, обязательное закрытие окон во время важных совещаний	устройства акустического зашумления, генератор белого шума
вибрационный виброакустический	все твердые поверхности помещения, батареи	дополнительное помещение перед переговорной, изолирующие звук и вибрацию обшивки стен	устройства вибрационного зашумления
оптический	окна, двери	жалюзи на окнах, тонируемые или рифленые стекла, доводчики на дверях	бликующие устройства
электромагнитный электрический	розетки, АРМы + бытовая техника	розетки, АРМы + бытовая техника	устройства электромагнитного зашумления

При оценке вероятности использования технической разведкой потенциальных каналов утечки информации следует принимать во внимание окружающую обстановку, с точки зрения возможности по организации и ведению технической разведки, а именно:

1. скрытное размещение поста перехвата (для прослушивания и просмотра помещения, установки лазерного микрофона) в жилом здании, если, например, арендовать квартиру с окнами, расположенными напротив окон защищаемого помещения, вполне реализуемо.

Необходимо, если имеется такая возможность, проверить планы расположения квартир в домах, окна которых выходят на предприятие и изучить потенциально опасные квартиры пригодные для организации поста перехвата, а также получить информацию о том сдаются ли квартиры, проживают ли в квартирах потенциальные конкуренты, имеются ли лица бывшие в конфликте с законом и т.п. Возможности организации постов перехвата на технических этажах и т.п.

4. АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В соответствии с заданием курсовой работы, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «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.

4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита представляет собой:

- усиленные двери;
- дополнительная отделка переговорной звукоизолирующими

материалами.

Активная защита представляет собой систему виброакустического зашумления. Для защиты помещения для работы с государственной тайной уровня «секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 3Б в соответствии с РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации". Ниже в таблице 4.1 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому каналу.

Таблица 4.1 – Сравнительный анализ средств активной защиты

Устройство	Характеристики	Предназначение	Цена, руб.
Генератор шума АКИП-3501/1	Диапазон частот: 15 МГц – 415 МГц	Генератор шума для акустического зашумления помещения и его защиты от утечки информации по виброканалам	98 400
Генератор шума ГНОМ-3М	Диапазон частот: 0,15 МГц – 1800 МГц	Защита информации, которая обрабатывается на персональных компьютерах и в локальных сетях предприятия, от утечки по каналам ПЭМИН. Данный прибор нивелирует возможность похищения конфиденциальных данных по каналам побочных электромагнитных излучений. Шумогенератор создает помехи, максимально приближенные к белому шуму, благодаря чему никакие жучки и дешифраторы не смогут уловить и расшифровать защищённую в полосе помех информацию.	57 200
Соната «АВ» модель 4Б	175–11200 Гц	Блок электропитания и управления, генератор-акустоизлучатель, генератор-	26400 руб.

		вибровозбудитель, размыкатель телефонной линии, размыкатель слаботочной линии, размыкатель линии Ethernet, пульт управления, блок сопряжения с внешними устройствами, техническое средство защиты речевой информации от утечки по оптико- электронному (лазерному) каналу, генераторный блок "АВ-4Л", вибровозбудитель "СП-4Л".	
--	--	---	--

В результате проведенного анализа средств защиты в качестве системы виброакустической защиты была выбрана «Соната АВ» модель 4В, так как при более низкой стоимости, она не уступает по показателям другим системам.

“Соната-АВ” модель 4Б является комплексом защиты от утечки информации по различным каналам. Производство изделия Соната-АВ” модель 4Б сертифицировано. Сертификат ФСТЭК.

“Соната-АВ” модель 4Б построена по принципу "единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)"

Благодаря этому построению проявляется высокая стойкость защиты информации.

4.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации

Пассивная защита основывается на установке фильтров для сетей электропитания во всех помещениях.

Активная защита основывается на создании в сети белого шума, который скрывает колебания, порождаемые воздействием звуковой волны или работающей электрической техникой.

Для перекрытия **акустоэлектрического** канала были предложены варианты: Размыкатели слаботочных линий “Соната-ВК4.1” предназначены для защиты информации от утечки за счет акустоэлектрических преобразований и ВЧ-навязывания по телефонным линиям, “Соната-ВК4.2” по соединительным линиям систем оповещения и сигнализации, а “Соната-ВК4.3” по линиям компьютерных сетей.

Был выбран “Соната-ВК4.1” из-за распространенности ВЧ-навязывания.

Устройство	Предназначение	Цена, руб.
СПО «Навигатор»	<p>Специальное программного обеспечения «Навигатор» состоит из поисковой и измерительной программы «Навигатор» и программы расчета требуемых показателей защищенности «Навигатор-С». Поисковая и измерительная задача (далее по тексту "измерительная программа") осуществляет поиск и измерение пиковой амплитуды сигналов ПЭМИН и уровня шума, а расчетная задача производит расчет требуемых показателей защищенности. Обе задачи (обе программы) могут использоваться как самостоятельно (обмениваясь данными через файл), так и совместно (расчетная задача вызывается из измерительной, с передачей ей данных измерений). Библиотека расчета требуемых показателей защищенности файл «NCLC7.dll» сертифицирован ФСТЭК России как программное средство контроля защищенности информации от утечки за счет ПЭМИН.</p>	Под заказ
Шатер	<p>Обеспечивает: экранирование радиоэлектронной аппаратуры (РЭА) при проведении экспресс исследований РЭА на наличие побочных электромагнитных излучений и</p>	Под заказ

	наводок (ПЭМИН) по сети электропитания, проведении работ по выявлению специальных электронных устройств перехвата информации.	
Покров 1	Генератор шума (ГШ ПОКРОВ) 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.	32800 руб.

Выбран **“СПО Навигатор”** из-за определенного ценника и большого обхвата применений.

Активная защита от **утечек по электрическим каналам** связи:

Т. к. у нас уже имеются элементы комплекса сонаты, то добавление еще одного модуля будет удобным и практичным, ведь по остальным характеристикам он не сильно отличается от аналогов, значит **Соната-РС2** подходит нам лучше всего.

4.3 Защита от ПЭМИН

Для реализации активной защиты от ПЭМИН было выбрано устройство НПО «Анна» Соната-РЗ. Данный выбор обоснован тем, что управление его работой и контроль режима работы (исправности) может осуществляться от пульта управления "Соната-ДУ4.1" в комплексе с блоком питания "Соната-ИП4.х", т. е. устройство может быть встроено в систему Соната АВ-4б, выбранную как реализация активной защиты по виброакустическому каналу.

4.4 Защита от утечек по оптическому каналу

Для обеспечения защиты помещения от визуального наблюдения, необходимо установить на окно жалюзи или шторы. С точки зрения удобства содержания были выбраны жалюзи.

5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

Согласно информации, приведённой в 4 главе, выбранные средства защиты информации включают в себя:

- Соната «АВ» модель 4Б со встроенной НПО «Анна»;
- “Соната-ВК4.1” (входит в Соната «АВ» модель 4Б);
- “СПО Навигатор” (устанавливается на АРМ);
- Жалюзи;
- Усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей прокладкой на металлическом каркасе.

Перейдём к оценке количества компонентов и расстановке выбранных технических средств. «Соната АВ» модель 4Б содержит генераторы-акустоизлучатели «СА-4Б1» и генераторы-вибровозбудители «СВ-4Б1».

Согласно официальному сайту НПО «Анна», необходимое количество генераторов-вибровозбудителей «СВ-4Б1» можно предварительно оценить из следующих норм:

- 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;
- один на окно (при установке на оконный переплет);
- один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо-, тепло- и газоснабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Необходимое количество генераторов-акустоизлучателей «СВ-4Б1» можно предварительно оценить из следующих норм:

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

Устройство для защиты линий электропитания, заземления от утечки информации “Соната-РС2” может использоваться в выделенных помещениях до 1 категории включительно, в том числе оборудованных системами звукоусиления речи, без применения дополнительных мер защиты информации. Изделия рассчитаны на подключение к 3-проводной сети энергоснабжения («Фаза», «Ноль» и «Защитное заземление») и обеспечивают формирование несинфазных токов и синфазных и паразитных составляющих шумового напряжения во всех проводниках. При нарушении схемы подключения наличие всех составляющих, а также значение интегрального уровня шума может не обеспечиваться.

По результатам выбора средств защиты информации от утечки построим схему расстановки устройств (Рисунок 3)

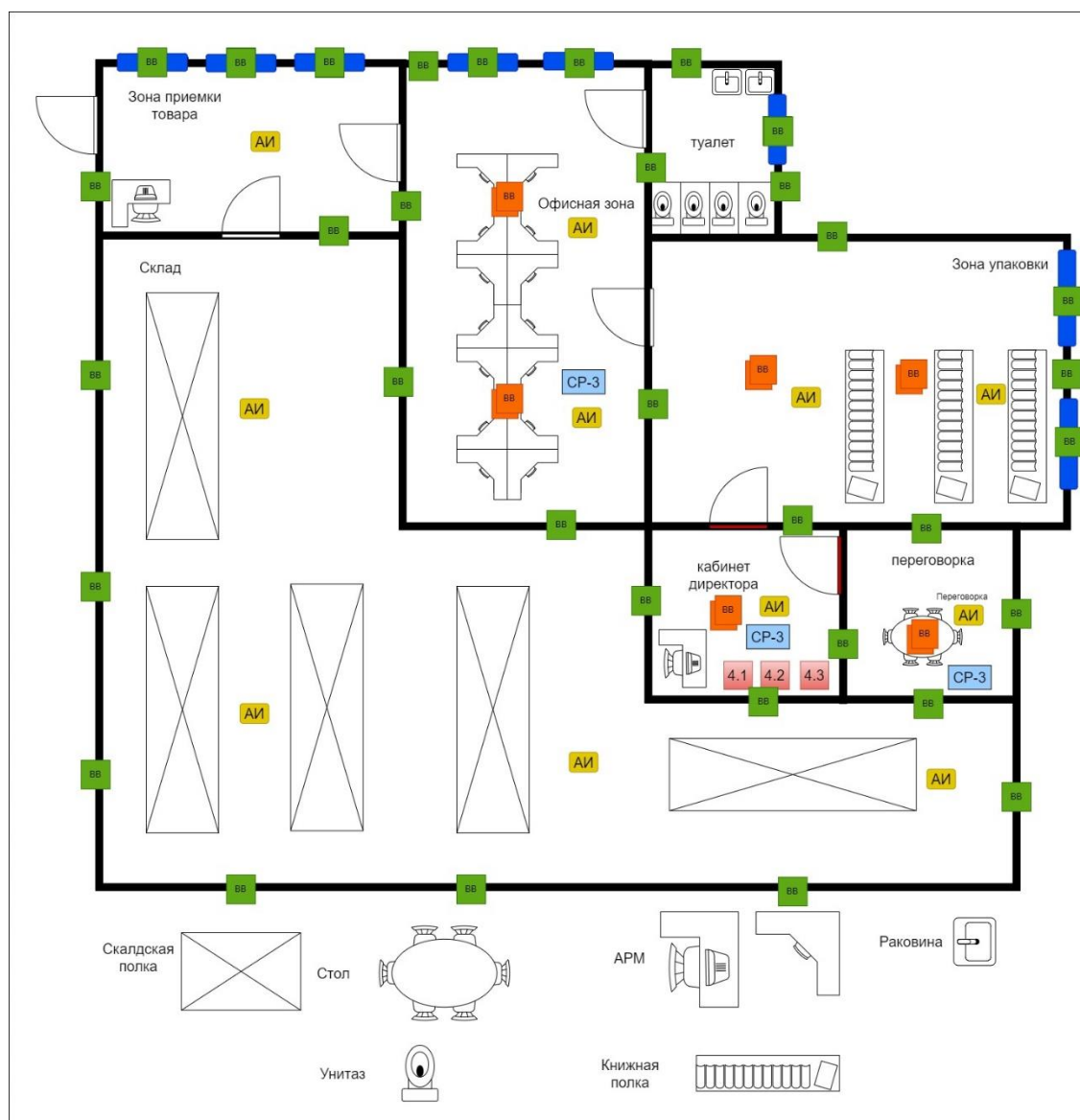


Рисунок 3 – Схема расстановки устройств

Таблица 4 – Технические средства

Название	Условное обозначение
Блок электропитания и управления «Соната-ИП4.3»	БП
«Соната-СА-4Б1» Генератор акустоизлучатель	АИ
«Соната-СВ-4Б» генератор вибровозбудитель (стены и батареи)	ВВ





«Соната-СВ-4Б» генератор вибровозбудитель (потолок и пол)	
Размыкатели «Соната-ВК4.1» «Соната-ВК4.2» «Соната-ВК4.3»	
Жалюзи	
Укрепленная дверь	

Таблица 5 – Технические средства

Название	Цена, руб.	Количество, шт.	Сумма, руб.
Блок электропитания и управления «Соната-ИП4.3»	25 600	1	25 600
«Соната-СА-4Б1» Генератор акустоизлучатель	3 540	11	38 940
«Соната-СВ-4Б» генератор вибровозбудитель	3 540	46	162 840
Генератор шума для электросети СонатаРС2	23 600	1	23 600
Усиленная дверь RW 47	80 125	1	80 125
Пульт управления «Соната-ДУ4.3»	5 760	1	5 760
Генераторный блок «Соната-АВ-4Л»	7 680	1	7 680
Размыкатели «Соната-ВК4.1» «Соната-ВК4.2» «Соната-ВК4.3»	6 000	3	18 000
«Соната-РС2»	23 600	1	23 600
Жалюзи	1 200	3	3 600
Итого:			389 745

ВЫВОДЫ

В ходе данной работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении и описаны необходимые меры их защиты. Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для нашего объекта. Был разработан план установки и произведен расчет сметы затрат. В результате была предложена защита от утечек информации по акустическому, виброакустическому, оптическому, акустоэлектрическому, электрическому, электромагнитному, оптико-электронному техническим каналам защиты информации, обеспечена защита от ПЭМИН.

СПИСОК ЛИТЕРАТУРЫ

1. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.;
2. "Руководящий документ "Защита от несанкционированного доступа к информации. Термины и определения";
3. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.