

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

Факультет безопасности информационных технологий

По дисциплине:

«Инженерно-технические средства защиты информации»

ОТЧЁТ ПО КУРСОВОЙ РАБОТЕ

На тему:

«Проектирование инженерно-технической системы защиты информации на предприятии»

Выполнил:

Севастьянов Никита Владиславович, студент группы N34491



Проверил преподаватель:

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

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Севастьянов Никита Владиславович
	(Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34491
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич, доцент (квалификационная категория "ординарный доцент"), к.т.н.
	(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 защиты курсовой работы представлен в методических указаниях, размещённых на коммуникационной площадке дисциплины.
3. Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

Пояснительная записка включает разделы: введение, анализ технических каналов утечки информации, перечень руководящих документов, анализ защищаемых помещений, анализ рынка технических средств, расстановка технических средств, заключение, список использованных источников.

Рекомендуемая литература

1. Организационно-правовое и методическое обеспечение информационной безопасности / Н.С. Кармановский, О.В. Михайличенко, С.В. Савков./ Учебное пособие. – СПб: НИУ ИТМО, 2013. – 148 с.
2. 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	Севастьянов Н. В.	 (Подпись, дата)

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

(Фамилия И.О.)

Группа N34491

(Фамилия И.О., должность, ученое звание,
степень)

Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии
--------------------------	---

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	17.11.2023	17.11.2023	
2	Анализ теоретической составляющей	15.12.2023	15.12.2023	
3	Разработка комплекса инженернотехнической защиты информации в заданном помещении	17.12.2023	17.12.2023	
4	Представление выполненной курсовой работы	21.12.2023	21.12.2023	

(Подпись, дата)

(Подпись, дата)

Студент	Севастьянов Никита Владиславович
	(Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34491
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич, доцент (квалификационная категория " ординарный доцент "), к.т.н.
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии

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 отчётная

Анализ технических каналов утечки информации; определение основных угроз и уязвимостей; анализ защищаемых помещений; анализ технических средства защиты информации;

описание расстановки технических средств.

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

Студент Севастьянов Н. В.

(Подпись, дата)

(Подпись, дата)

«21» декабря 2023 г.

СОДЕРЖАНИЕ

Введение	6
1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ	7
1.1 Визуально-оптические каналы утечки информации	8
1.2 Акустические каналы утечки информации	9
1.3 Электромагнитные каналы утечки информации	10
1.4 Материально-вещественные каналы утечки информации	11
2 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ	11
3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ.....	13
3.1 Общая информация о предприятии и информационный поток	13
3.2 Описание защищаемых помещений.....	14
3.3 Анализ возможных утечек информации.....	16
3.4 Выбор средств защиты информации.....	17
4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ	18
4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации	19
4.2 Устройства для перекрытия электрического, электромагнитного каналов утечки информации	22
4.3 Устройства для защиты от визуально-оптического канала	24
5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ	25
Заключение	28
Список использованных источников	29

ВВЕДЕНИЕ

Современные компании сталкиваются с растущей угрозой технических каналов утечки информации, способных серьезно подорвать их безопасность и конкурентоспособность. Среди таких каналов выделяются сетевые утечки, утечки через периферийные устройства, акустические и оптические методы проникновения, что делает задачу защиты конфиденциальной информации более сложной и актуальной, чем когда-либо прежде.

В данном контексте проведение анализа проблемы защиты от технических каналов утечки информации представляется критически важным. Целью данного исследования является изучение современных методов обнаружения и предотвращения утечек информации, требующих комплексного подхода, объединяющего технические, организационные и правовые меры.

Средства защиты информации (СЗИ):

Средства защиты информации (СЗИ) играют ключевую роль в обеспечении безопасности информационных систем компаний. Они предоставляют средства предотвращения несанкционированного доступа, снижая риск утечек, искажения, уничтожения, копирования и блокирования информации. Таким образом, они способствуют предотвращению экономического, репутационного и других видов ущерба предприятию.

Цель работы:

Целью данной работы является повышение защищенности рассматриваемого помещения. Для достижения этой цели предполагается решение следующих задач:

1. **Анализ технических каналов утечки информации:** Исследование различных путей, по которым может происходить утечка информации, включая сетевые, периферийные, акустические и оптические каналы.
2. **Определение основных угроз и уязвимостей:** Идентификация потенциальных опасностей и слабых мест, которые могут быть использованы злоумышленниками.
3. **Анализ защищаемого помещения:** Изучение особенностей помещения, включая физическую структуру, доступ и контроль.
4. **Анализ технических средств защиты информации:** Рассмотрение эффективности существующих технических средств и их соответствия поставленным задачам.
5. **Описание расстановок технических средств:** Разработка оптимальных конфигураций установки средств защиты, учитывая особенности помещения и выявленные угрозы.

Данное исследование имеет практическую значимость для разработки комплекса мер по обеспечению надежной защиты от технических каналов утечки информации, предостерегая компанию от возможных угроз и минимизируя риски нежелательных последствий.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечка информации — это неконтролируемое распространение информации за пределы организации, помещения, здания, какой-либо территории, а также определенного круга лиц, которые имеют доступ к этой информации. В случае обнаружения утечки важно своевременно ее ликвидировать, но лучше всего заранее принять превентивные меры по защите информации с ограниченным доступом.

Технический канал утечки информации (ТКУИ) – это путь информации, который она может пройти от источника информации до приемника/получателя в процессе случайной утечки или целенаправленного несанкционированного получения закрытой информации. Если меры по защите информации не были приняты заранее, то могут быть задействованы любые каналы утечки. Если же защита информации предусмотрена – то будет задействован наиболее слабозащищенный канал.

В природе существуют только 4 средства переноса информации – это световые лучи, звуковые волны, электромагнитные волны, а также материальные носители (бумага, фото, магнитные носители и т. д.). Эти средства являются составляющими любой системы связи, в которой помимо них обязательно присутствуют:

- Источник информации.
- Передатчик.
- Канал передачи информации.
- Приемник.
- Получатель сведений.

Утечка (информации) по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. Технический канал утечки информации (ТКУИ), так же как и канал передачи информации, состоит из источника сигнала, физической среды его распространения и приемной аппаратуры злоумышленника. На рисунке 1 приведена структура технического канала утечки информации.



Рисунок 1 – Структура технического канала утечки информации

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

- Визуально-оптические каналы утечки информации.
- Акустические каналы утечки информации.
- Электромагнитные каналы утечки информации.
- Материально-вещественные каналы утечки информации.

Каждому виду каналов утечки информации свойственны свои специфические особенности.

1.1 Визуально-оптические каналы утечки информации

В последнее время стало уделяться большое внимание утечке визуальной информации, получаемой в виде изображений объектов или копий документов путем наблюдения за объектом, съемки объекта и съемки (копирования) документов. В зависимости от условий наблюдения обычно используются соответствующие технические средства, в том числе: оптика (бинокли, подзорные трубы, телескопы, монокуляры), телекамеры, приборы ночного видения, тепловизоры и т. п.

Для документирования результатов наблюдения проводится съемка объектов с помощью фотографических и телевизионных средств, соответствующих условиям съемки. Для снятия копий документов используются электронные и специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют видеозакладки.

Основным способом борьбы с утечкой информации по оптическим каналам связи остается затруднение доступа злоумышленника к объектам, содержащим секретные данные. Вторая задача — выявление закладных устройств.

1.2 Акустические каналы утечки информации

Акустическая информация — информация, носителем которой является акустический сигнал.

Акустический сигнал — возмущение упругой среды, проявляющееся в возникновении акустических колебаний различной формы и длительности.

Различают первичные и вторичные акустические сигналы. К первичным относятся: сигналы, создаваемые музыкальными инструментами, пением, речью; шумовые сигналы, создаваемые для сопровождения различных музыкальных и речевых художественных передач (шум поезда, треск кузнечика и т. п.). Ко вторичным акустическим сигналам относятся сигналы, воспроизводимые электроакустическими устройствами, то есть первичные сигналы, прошедшие по электроакустическим трактам связи и вещания и соответственно видоизменённые по своим параметрам.

В зависимости от формы акустических колебаний различают простые (тональные) и сложные сигналы. Тональный — это сигнал, вызываемый колебанием, совершающимся по синусоидальному закону. Сложный сигнал включает целый спектр гармонических составляющих.

Виды технических каналов утечки акустической информации: Воздушные, электроакустические, вибрационные, параметрические, оптико-электронные (лазерный).

Акустический канал утечки информации реализуется в следующем:

- Подслушивание разговоров на открытой местности и в помещениях, находясь рядом или используя направленные микрофоны (бывают параболические, трубчатые или плоские). Направленность 2-5 градусов, средняя дальность действия наиболее распространённых — трубчатых составляет около 100 метров. При хороших климатических условиях на открытой местности параболический направленный микрофон может работать на расстояние до 1 км;
- Негласная запись разговоров на диктофон или магнитофон (в том числе цифровые диктофоны, активизирующиеся голосом);
- Подслушивание разговоров с использованием выносных микрофонов (дальность действия радиомикрофонов 50–200 метров без ретрансляторов).

Чтобы предотвратить утечку информации по акустическому каналу, необходимо снизить или исключить возможность выхода информации за счет контроля акустических полей. В этом случае профессионалы проводят сразу комплекс мероприятий — архитектурную перепланировку пространства, повышение звукоизоляции,

звукопоглощения, звукоподавления, а также проводят режимные меры по строгому контролю пребывания людей в отслеживаемой зоне.

1.3 Электромагнитные каналы утечки информации

Электромагнитный канал перехвата информации. Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки. Данный канал наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Телефонный канал утечки информации для подслушивания телефонных переговоров (в рамках промышленного шпионажа) возможен:

- Гальванический съём телефонных переговоров (путём контактного подключения подслушивающих устройств в любом месте абонентской телефонной сети). Определяется путём ухудшения слышимости и появления помех, а также с помощью специальной аппаратуры;
- Телефонно-локационный способ (путём высокочастотного навязывания). По телефонной линии подаётся высокочастотный тональный сигнал, который воздействует на нелинейные элементы телефонного аппарата (диоды, транзисторы, микросхемы) на которые также воздействует акустический сигнал. В результате в телефонной линии формируется высокочастотный модулированный сигнал. Обнаружить подслушивание возможно по наличию высокочастотного сигнала в телефонной линии. Однако дальность действия такой системы из-за затухания ВЧ сигнала в двухпроводной линии не превышает ста метров. Возможное противодействие: подавление в телефонной линии высокочастотного сигнала;
- Индуктивный и ёмкостной способ негласного съёма телефонных переговоров (бесконтактное подключение).

В качестве защиты от утечки информации по визуально-оптическому каналу следует снизить освещенность защищаемого объекта и его отражательные свойства, использовать различные пространственные ограждения (ширмы, экраны, шторы, ставни, темные стекла), применять специальную маскировку и средства сокрытия защищаемых объектов (аэрозольные завесы, сетки, краски, укрытия).

1.4 Материально-вещественные каналы утечки информации

Материальные — информация на бумаге или других физических носителях информации.

Материально-вещественный канал утечки информации — позволяют получать информацию путём хищения или нелегального доступа к носителям информации: флеш-картам, дискам, бумажным документам и т.д. Получение информации может произойти, например, при краже документов или внешних дисков, а также посредством копирования, фотографирования или скачивания данных с носителя информации.

Материально-вещественные каналы также нуждаются в защите, так как различные материальные носители могут содержать в себе важнейшую секретную информацию. К примеру, любое производственное предприятие имеет отходы, в которых могут содержаться различные испорченные документы, бракованные детали, жидкости или газообразные вещества, и часто они бесконтрольно отправляются за пределы контролируемой зоны. Для защиты материально-вещественных каналов от утечки информации разрабатывается целый комплекс организационных мер.

2 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ

Основными документами в области защиты информации являются:

- 1 Федеральный закон РФ от 09.02.2009 N 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;
- 2 Федеральный закон РФ от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- 3 Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 4 Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- 5 Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
- 6 Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»;
- 7 Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;

8 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:

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

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

3 Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров;

4 Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации;

5 Временный порядок аттестации объектов информатизации по требованиям безопасности информации;

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

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

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

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

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

11 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.

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Общая информация о предприятии и информационный поток

Объектом исследования и защиты является компания: ООО «SEVA». Информационный поток представляет собой упорядоченное движение информации в письменной, устной и электронной формах внутри организации и между ней и внешней средой.

По степени открытости и уровню значимости информационные потоки делятся на открытые и закрытые. Организация ООО «SEVA» имеет вторую степень секретности информации ("совершенно секретно"). В соответствии с классификацией "совершенно секретно" к сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации.

Перечень защищаемых информационных активов:

- Персональные данные сотрудников.
- Персональные данные клиентов.
- Государственная тайна.
- Конфиденциальная информация, содержащая коммерческую тайну.
- Техническая конфигурация программного обеспечения.

Закрытые информационные потоки:

- Информация между директорами компании.
- IT-отдел.
- Юридические консультации компании.

Открытые информационные потоки:

- Информация о взаимодействии между клиентами и компанией.
- Информация о некоторых продуктах, разрешенная к публикации, от отдела разработки.
- Информация о взаимодействии со сторонними предприятиями (банками).

На рисунке 2 представлены информационные и организационные потоки предприятия

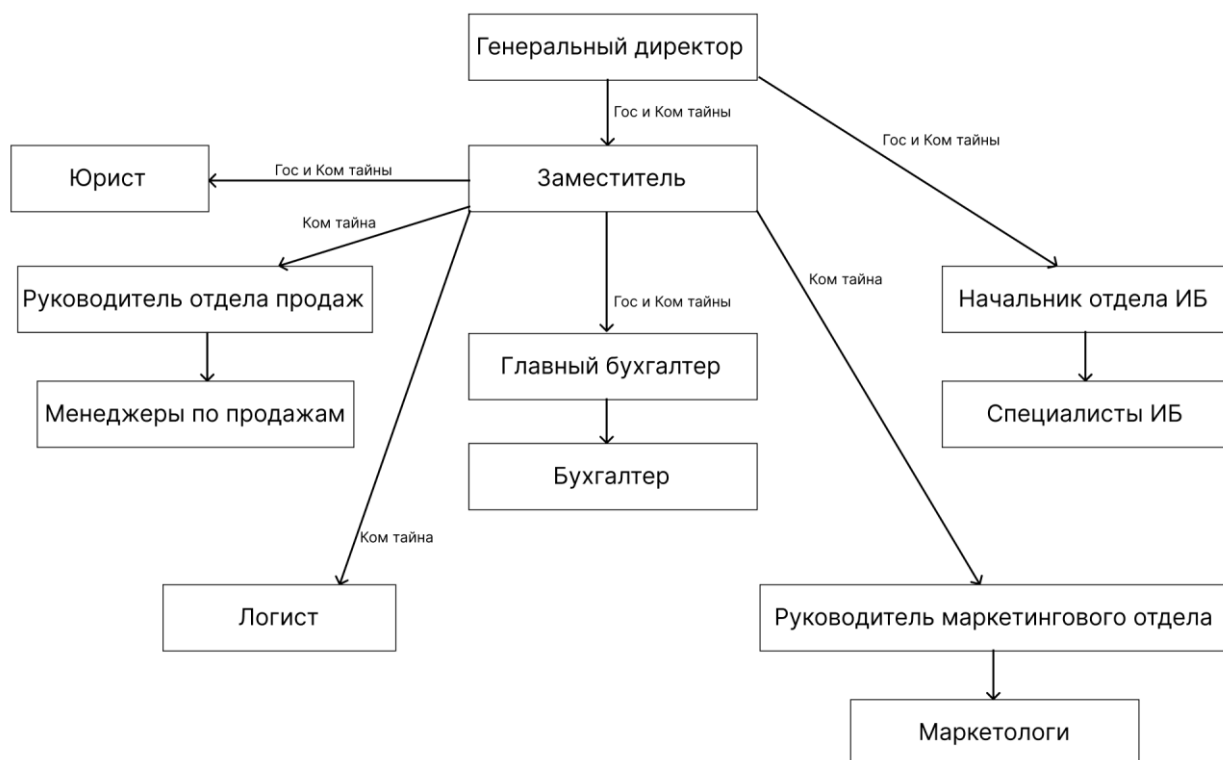


Рисунок 2 – Информационные и организационные потоки предприятия

3.2 Описание защищаемых помещений

На рисунке 3 представлен план помещения:

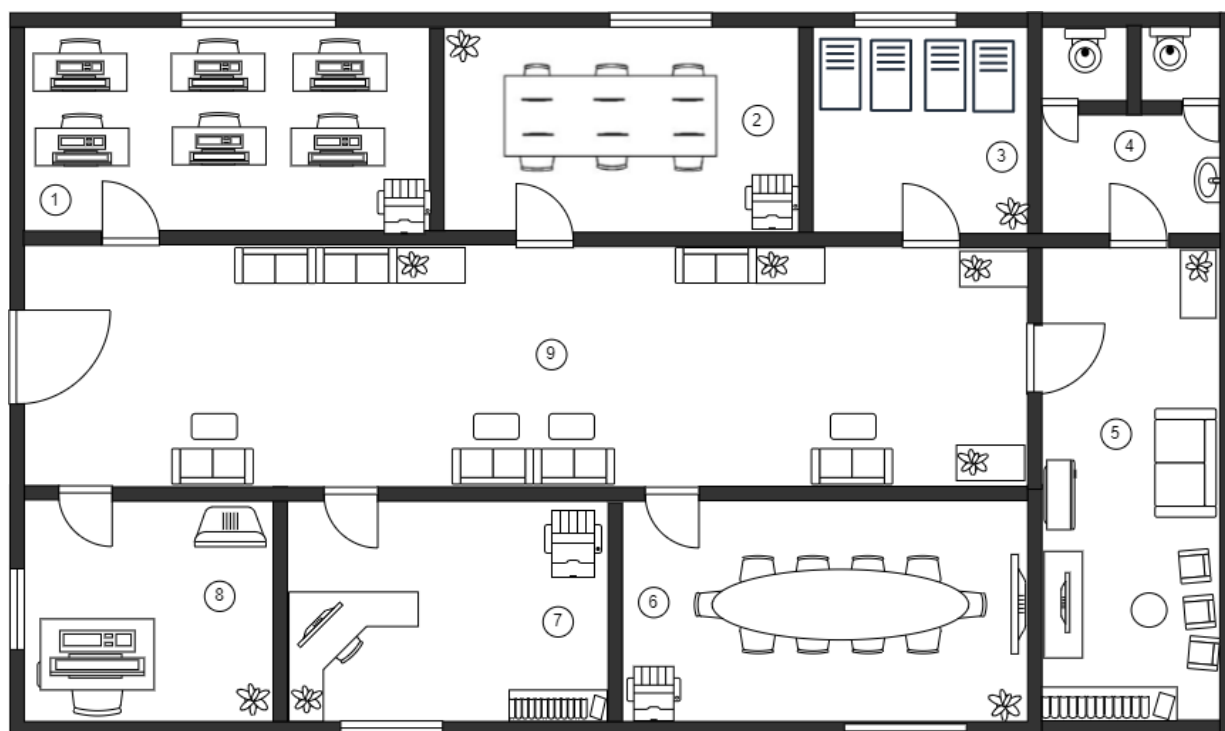


Рисунок 3 – План помещения


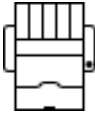


В таблице 1 представлены номера помещений на плане, их назначение.



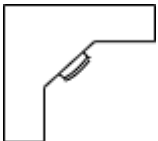


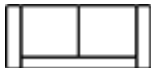
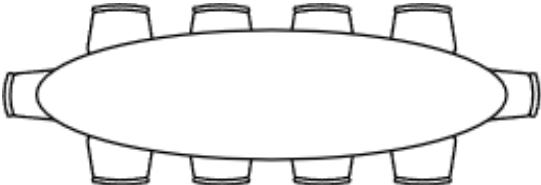




Таблица 1 – Условные обозначения

№	Назначение	Площадь (m^2)	Оснащение помещения
1	Офис 1	24	8 рабочих мест, 1 притер, 1 окно, стол, стул
2	Офис 2	21	6 ПК, 1 принтер, 1 окно, стол, стул
3	Серверное помещение	12	4 сервера, 1 окно
4	Туалет	8	1 раковина, 2 кабинки
5	Зона отдыха	30	1 микроволновая печь, 1 книжный шкаф, кресло, 1 диван, 1 стол, 1 телевизор
6	Переговорная	26	Стол для переговоров, 10 стульев, ТВ для презентаций, 1 окно, 1 притер
7	Кабинет директора	18	1 книжный шкаф, 1 притер, 1 ПК, стол, стул
8	Охрана	13	2 ПК
9	Коридор	60	Диван, стол

В таблице 2 представлены описание мебели в помещении

Таблица 2 – Условные обозначения

Обозначение	Описание
	Рабочий стол с АРМ
	Принтер
	Сервер
	ПК для видеонаблюдения

	Телевизор, компьютер
	Микроволновая печь
	Стол директора и стул
	Книжный шкаф
	Стол
	Диван
	Стол для переговоров и стулья
	Цветок
	Кресло
	Туалет
	Раковина

Рассматриваемое помещение расположено на втором этаже многоэтажного офисного здания с окнами, выходящими на оживленные улицы. Окна не соприкасаются с пожарными и эвакуационными лестницами, крышами зданий, выступами на стенах, балконами и другими элементами, которые могут служить возможным маршрутом для посторонних лиц. Помещения сгруппированы в угловой части офисного здания.

Стены здания и внутренние перегородки выполнены из железобетона толщиной не менее 10 см, обеспечивая надежную физическую защиту. Такая конструкция способствует снижению риска вторжения или несанкционированного доступа.

Дополнительно отмечается отсутствие элементов, таких как балконы, выступы на стенах и другие возможные точки входа, что дополнительно укрепляет безопасность помещения.

Расположение окон в стороне от потенциальных опасностей, таких как пожарные лестницы, также способствует укреплению общей защиты. Такие меры призваны

минимизировать возможные риски и обеспечить надежное функционирование помещения.

3.3 Анализ возможных утечек информации

В помещениях присутствуют декоративные элементы, где можно спрятать закладное устройство. В каждом помещении имеются розетки, а значит, актуальны электрический и электромагнитный каналы утечки информации. Также есть угроза снятия информации по вибрационному и оптическому каналам, а также акустическому, виброакустическому, акустоэлектрическому.

Материально-вещественный канал утечки информации регулируется строгой политикой компании в отношении физических носителей информации, и в рамках курсовой работы не рассматривается.

3.4 Выбор средств защиты информации

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «совершенно секретно» требуется оснастить помещение средствам защиты, приведенными в таблице 3.

Таблица 3 – Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
Акустический, акустоэлектрический	окна, двери, электрические сети, проводка и розетки	Звукоизоляция, фильтры для акустического канала	Устройства акустического зашумления
Вибрационный, виброакустический	Батареи и все твердые поверхности помещений (стены, пол, окна, двери)	Изолирующие звук и вибрацию материалы стен	Устройства вибрационного зашумления
Оптический	Окна, двери	Жалюзи на окнах, доводчики на двери, уменьшить попадание света на защищаемый объект	Применять специальную маскировку и средства сокрытия защищаемых объектов

Электромагнитный, электрический	АРМ, ПК, ноутбуки, Телевизор, проектор, телефон, принтер, серверы	Фильтры для сетей питания, экранирующие материалы, помехоподавляющие фильтры	Устройства электромагнитного зашумления
------------------------------------	---	---	---

4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В соответствии с заданием курсовой работы предприятие работает с информацией 2 степени секретности или с информацией, представляющей государственную тайну с грифом «совершенно секретно».

Согласно требованиям «Типовых норм и правил проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденных Решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199, защита рассматриваемых помещений должна удовлетворять следующим критериям:

1 В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри – звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 см. Дверь устанавливается на металлический каркас;

2 Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании;

3 По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями 20 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;

7 Помещения, где хранятся секретные документы и носители государственной тайны, оборудуются охранной и аварийной сигнализацией.

4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Защита информации от утечки по акустическому каналу – комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей.

Основными мероприятиями в этом виде защиты выступают организационные и организационно-технические меры. Из организационных мер – проведение архитектурно-планировочных, пространственных и режимных мероприятий, а организационно-технические — пассивные (звукоизоляция, звукопоглощение) и активные (звукоподавление) мероприятия. Возможно проведение и технических мероприятий с помощью применения специальных защищенных средств ведения конфиденциальных переговоров.

Пассивная защита представляет собой:

- усиленные двери;
- установка фильтров для сетей электропитания;
- установка жалюзи на окна;
- применением звукопоглощающих облицовок, специальных дополнительных тамбуров дверных проемов, двойных оконных переплетов.

Активная защита представляет собой систему виброакустического зашумления. Для защиты помещения для работы с государственной тайной уровня «совершенно секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1Б.

Ниже в таблице 4 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому и акустическому каналу.

Таблица 4 – Сравнительный анализ средств активной защиты от утечки информации по виброакустическому и акустическому каналу

Средство защиты	Характеристики	Назначение	Цена (руб)
Система активной акустической и вибрационной защиты акустической речевой	Диапазон воспроизводимого шумового сигнала: 175–11200 Гц.	Сертифицировано ФСТЭК. Система защиты речевой информации от утечки по техническим каналам "Соната-АВ" модель 4Б, предназначена	44200

информации "Соната-АВ" модель 4Б	Максимальная продолжительность непрерывной работы: 8ч.	для защиты речевой информации в выделенных помещениях, от утечки по акустическим, виброакустическим, акустоэлектрическим и оптико- электронным (лазерным) каналам.	
Система акустических и виброакустических помех Буран	Диапазон рабочих частот: 100–11 200 Гц. Максимальное число пьезоэлектрических виброизлучателей, подключенных к каналам параллельно: 8 и 10 соответственно. Продолжительность непрерывной работы: 24 часа.	Система акустических и виброакустических помех «Буран» является средством активной акустической и вибрационной защиты акустической речевой информации типа А, соответствует требованиям ФСТЭК России к средствам защиты акустической речевой информации по 2 классу защиты и может устанавливаться в выделенных помещениях.	67500
Система виброакустической защиты Камертон-5	Диапазон рабочих частот от 90–11200 Гц.	Сертифицировано ФСТЭК. Комплекс технических средств для защиты речевой информации от несанкционированного съема через виброакустические каналы. Гарантирует невозможность прослушки разговоров посредством лазерных и направленных микрофонов через окна, инженерные коммуникации,	46000

		вентиляцию, межкомнатные перегородки, пр.	
Система постановки виброакустических и акустических помех ЛГШ-404	Диапазон рабочих частот: 175–11200Гц. Количество подключаемых излучателей на каналдо 20 шт.	Сертифицировано ФСТЭК. Система постановки виброакустических и акустических помех предназначена для противодействия специальным средствам несанкционированного съема информации, использующим в качестве канала утечки ограждающие конструкции помещения.	35100
Система защиты по виброакустическому и акустоэлектрическому каналам SEL-155 «Сонет»	Диапазон воспроизводимого шумового сигнала: от 0,01 до 1800 МГц.	Сертифицировано ФСТЭК. Система SEL-155 «Сонет» предназначена для защиты речевой информации, циркулирующей в выделенных помещениях, от её утечки путём создания маскирующих акустических помех в смежных воздушных пространствах и маскирующих вибрационных помех в ограждающих конструкциях и инженерно-технических коммуникациях	22000

По результатам анализа была выбрана система НПО Соната «АВ» модель АВ-4Б.

Данная система имеет сертификат ФСТЭК, достаточную комплектацию и приемлемую стоимость. Улучшенная аппаратная настройка элементов модели «Соната АВ- 4Б» позволяет изменить настройки генераторов и построить гибкую систему виброакустической.

4.2 Устройства для перекрытия электрического, электромагнитного каналов утечки информации

В качестве методов защиты и ослабления электромагнитных полей используется установка электрических фильтров, применяются пассивные и активные экранирующие устройства и специальное размещение аппаратуры и оборудования.

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.

Устройства активной защиты помещений по электрическому и электромагнитному каналу представлены в Таблице 5.

Таблица 5 – Сравнительный анализ средств активной защиты от утечки информации по электрическому и электромагнитному каналу

Средство защиты	Характеристики	Назначение	Цена (руб)
Генератор шума «Соната РС2»	Диапазон частот до 2 ГГц, диапазон регулировки уровня шума не менее 35 дБ. Регулировка уровня шума в 3 частотных полосах. Индикация нормального/аварийного режима работы.	Сертифицировано ФСТЭК. Устройство для защиты линий электропитания, заземления от утечки информации "Соната-РС2" (сертифицировано ФСТЭК) предназначены для защиты объектов вычислительной техники от утечки информации за счет наводок на линии электропитания и заземления и может использоваться в выделенных помещениях до 1 категории включительно.	23600
Сетевой генератор шума ЛГШ-221	Диапазон рабочих температур: от 1 до 40°C Диапазон рабочих частот: 0,01 ÷ 400 МГц	Изделие предназначено для использования в целях защиты информации, содержащей сведения, составляющие	36400

	Режимы работы: круглосуточный	государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет наводок путем формирования маскирующих шумоподобных помех. Изделие является средством активной защиты информации от утечки за счет наводок информативного сигнала на цепи заземления и электропитания, выходящие за пределы контролируемой зоны.	
Сетевой помехоподавляющий фильтр ЛППФ-10- 1Ф	Диапазон рабочих температур: от 1 до 40°C Время непрерывной работы прибора: круглосуточно	Сертифицировано ФСТЭК. Изделие предназначено для установки в выделенном помещении для обеспечения подавления сигналов в фазном и нулевом проводах розеточной сети. Изделие является средством пассивной специальной защиты технических средств от утечки информации за счет наводок, т.е. преобразования излучения технических средств в электрический сигнал в сети электропитания, выходящей за пределы контролируемой зоны.	47100
«Соната-РЗ» средство активной	Световая и звуковая индикация, потребляемая мощность	Сертифицировано ФСТЭК. Средство активной защиты информации "Соната-РЗ.1",	97200

защиты информации от утечки за счет ПЭМИН (Побочное электромагнитное излучение и наводки)	30 Вт, электропитание от сети 220 В Время непрерывной работы 8ч	предназначено для защиты информации от утечки информации за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и токоведущие инженерные коммуникации. ПЭМИН Соната-РЗ.1 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.	
---	--	--	--

В результате анализа был выбран генератор шума «Соната РС2». Данный выбор обоснован особенностями конструкции устройства, которые позволяют получать

эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники.

И был выбран «Соната-РЗ» средство активной защиты информации от утечки за счет ПЭМИН, так как оно обладает лучшими характеристиками по сравнению с другими средствами пассивной защиты от ПЭМИН.

4.3 Устройства для защиты от визуально-оптического канала








С целью защиты информации от утечки по визуально-оптическому каналу рекомендуется:

Средства преграждения или значительного ослабления отраженного света: ширмы, шторы, ставни, темные стекла, преграды;

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В таблице 6 описано, где разместить оборудование, а также количество оборудования и стоимость его оснащения.

Таблица 6 – Описание расстановок технических средств на помещении и расчет стоимости оснащения

Устройства	Место для размещения	Условное обозначение	Цена за штуку (руб)	Количество (штук)	Общая стоимость (руб)
Рулонные шторы Роллайт 2	На каждом окне		1000	6	6000
Усиленные звукоизоляционные двери	Дверь		25500	8	204000
Блок электропитания и управления Соната-ИП 4.3	Стены		21600	1	21600
Размыкатель телефонной линии Соната-ВК 4.1	В каждой комнате есть такое оборудование, как телефоны		6000	3	18000
Размыкатель линии «Ethernet» «Соната-ВК4.3»	По линиям компьютерных сетей		6000	1	6000
Генератор зашумления Соната-РС2	Около проводников, у стен		23600	7	165200
Генератор вибровозбудителей СВ-4Б	стены - на каждые 3-5 метров периметра для капитальной стены при условии		7440	22	163680

	установки излучателей на уровне половины высоты помещения				
	Потолок, пол	СВ	7440	9	66960
	Окна	СВ	7440	6	44640
	Дверь (при установке на верхнюю перекладину дверной коробки)	СВ	7440	8	59520
Генератор акустоизлучателей СА-4Б1	Один на каждый вентиляционный канал или дверной тамбур; Один на каждые 8–12 м ³	СА	3540	12	42480
Соната-РЗ	подключена напрямую к «Соната-ИП4.3»	-	97200	1	97200
ИТОГ					895280

На рисунке 4 прдставлен план помещения после расстановки технических средств

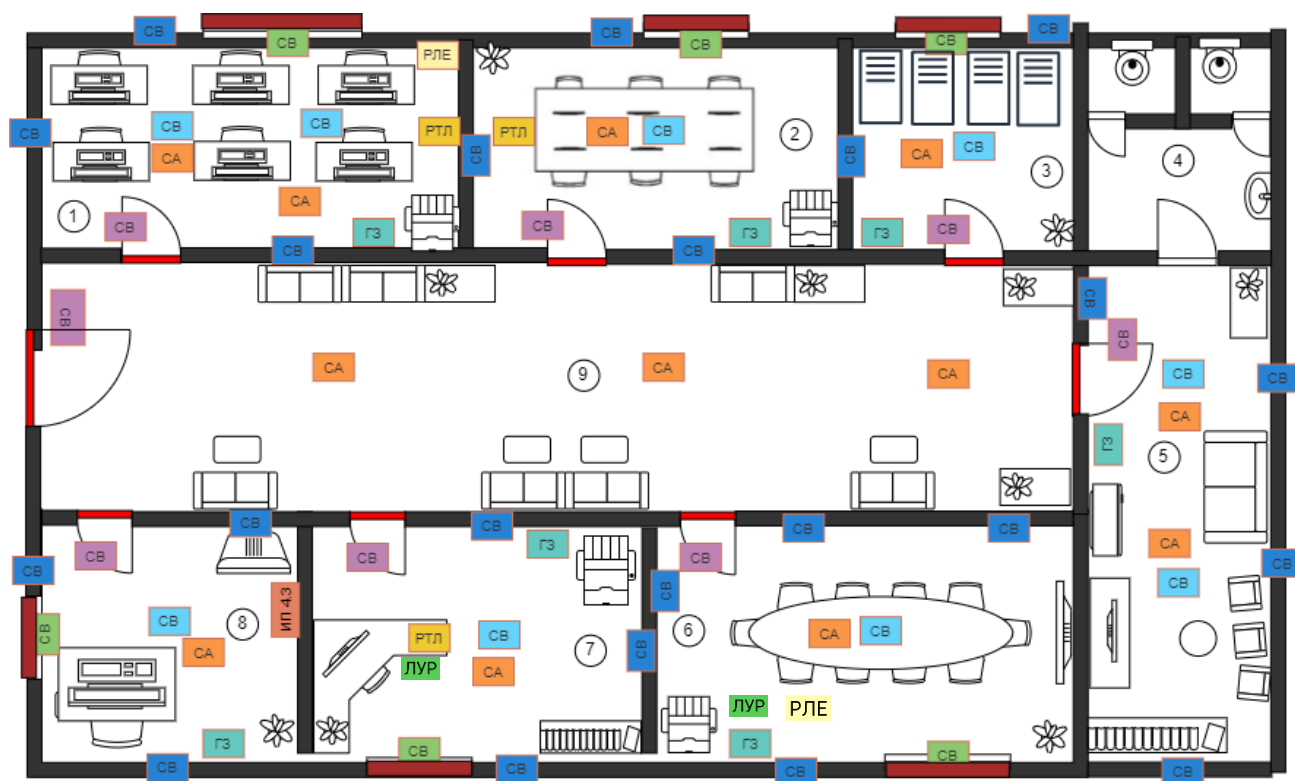


Рисунок 4 – План помещения после расстановки технических средств

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной курсовой работы был проведен анализ технических каналов утечки информации, включая оптико-визуальные, аудиоинформационные, электромагнитные, а также каналы утечки материалов и информации. Исследование позволило изучить современные методы предотвращения утечки информации и разработать схему установки устройств, направленных на предотвращение потенциальных угроз.

Практическая часть работы включала составление схемы установки устройств по предотвращению утечки информации в офисном здании компании, а также подробный расчет затрат. Полученные результаты были представлены в документе в виде комплексного анализа возможных технических каналов утечки информации и предложениями по внедрению мер пассивной и активной защиты информации.

В итоге данной работы выявлены основные угрозы и уязвимости, а также предложены конкретные шаги по обеспечению безопасности помещений компании. Разработанные рекомендации могут служить основой для эффективного внедрения системы защиты информации, минимизируя риски утечки и обеспечивая надежную защиту конфиденциальных данных компании "SEVA".

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Организационно-правовое и методическое обеспечение информационной безопасности / Н.С. Кармановский, О.В. Михайличенко, С.В. Савков. / Учебное пособие. – СПб: НИУ ИТМО, 2013. – 148 с.
2. Государственный реестр сертифицированных средств защиты информации // ФСТЭК РОССИИ [Электронный ресурс] (дата обращения: 28.11.2022).
3. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
4. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия РФ, 1998. 320с
5. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. – экз
6. Мещеряков Р. В., Шелупанов А. А., Зайцев А. П. Технические средства и методы защиты информации. – 2007.