

**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»

Выполнила:

Чан Тхю Нга, студентка группы N34481

(подпись)

Проверил:

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

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

| | |
|-----------------------------|--|
| Студент | Чан Тхю Нга |
| | (Фамилия И.О.) |
| Факультет | Безопасность информационных технологий |
| Группа | N34481 |
| Направление (специальность) | 10.03.01 (Технологии защиты информации 2020) |
| Руководитель | Попов Илья Юрьевич, к.т.н., доцент факультета безопасности информационных технологий |
| | (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

| | |
|--------------|--|
| Руководитель | |
| | (Подпись, дата) |
| Студент |  10.12.2023 |
| | (Подпись, дата) |

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Чан Тхю Нга

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34481

Направление (специальность) 10.03.01 (Технологии защиты информации 2020)

Руководитель Попов Илья Юрьевич, к.т.н., доцент факультета безопасности
информационных технологий

(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 | Разработка и утверждение задания и календарного плана на курсовую работу | 21.11.2023 | 21.11.2023 | |
| 2 | Анализ теоретической составляющей | 05.12.2023 | 05.12.2023 | |
| 3 | Разработка комплекса инженернотехнической защиты информации в заданном помещении | 10.12.2023 | 10.12.2023 | |
| 4 | Представление выполненной курсовой работы | 19.12.2023 | 19.12.2023 | |

Руководитель

(Подпись, дата)

Студент

Nga

10.12.2023

(Подпись, дата)

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

Студент Чан Тхю Нга
(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34481

Направление (специальность) 10.03.01 (Технологии защиты информации 2020)

Руководитель Попов Илья Юрьевич, к.т.н., доцент факультета безопасности информационных технологий
(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. Цели 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

3. Содержание работы

Введение; Анализ технических каналов утечки информации; Перечень руководящих документов; Анализ защищаемого помещения; Анализ технических средств защиты информации; Расстановка технических средств; Заключение; Список использованных источников

4. Выводы

В процессе выполнения задачи осуществлен полный анализ потенциальных технических путей утечки информации в предоставленных помещениях, а также предложены меры для пассивной и активной защиты данных.

Руководитель _____
(Подпись, дата)

Студент Nga 10.12.2023
(Подпись, дата)

СОДЕРЖАНИЕ

| | |
|--|----|
| Содержание | 5 |
| Введение | 6 |
| 1 Анализ технических каналов утечки информации..... | 7 |
| 1.1 Акустический канал | 8 |
| 1.2 Акустоэлектрический канал | 8 |
| 1.3 Виброакустический канал (телефонный)..... | 9 |
| 1.4 Оптический канал..... | 9 |
| 1.5 Электрический канал..... | 9 |
| 1.6 Электромагнитный канал..... | 10 |
| 2 Перечень руководящих документов | 11 |
| 3 Анализ защищаемого помещения | 13 |
| 3.1 Общая информация о предприятии | 13 |
| 3.2 Описание помещения | 13 |
| 3.3 Анализ возможных утечек информации | 16 |
| 4 Анализ технических средств защиты информации..... | 17 |
| 4.1 Анализ СЗИ для акустического и виброакустического каналов | 17 |
| 4.2 Анализ СЗИ для электрического, электромагнитного, акустоэлектрического каналов | 19 |
| 4.3 Анализ СЗИ для оптического канала..... | 20 |
| 5 Расстановка технических средств | 21 |
| Заключение..... | 24 |
| Список использованных источников..... | 25 |

ВВЕДЕНИЕ

В современном информационном обществе, где цифровые технологии играют ключевую роль в бизнес-процессах, обеспечение надежной защиты информации на предприятии становится стратегической необходимостью. Дисциплина "Инженерно-технические средства защиты информации" занимает важное положение в контексте создания эффективных мер безопасности, направленных на предотвращение утечек, а также гарантирование целостности и конфиденциальности информационных ресурсов.

Тема настоящей курсовой работы, посвященной проектированию инженерно-технической системы защиты информации на предприятии, выдвигает перед исследователем сложную задачу создания комплексного подхода к обеспечению безопасности данных. Основные этапы работы включают в себя анализ технических каналов утечки информации, изучение руководящих документов, анализ характеристик защищаемого помещения, а также оценку предложений рынка технических средств.

В рамках курсовой работы предстоит провести детальный анализ существующих технических каналов, которые могут стать источниками потенциальных угроз для безопасности информации на предприятии. Также будут рассмотрены и проанализированы руководящие документы, регламентирующие требования к системам защиты информации.

Цель настоящей работы заключается в разработке инженерно-технической системы, которая, сочетая в себе передовые технологии и лучшие практики в области защиты информации, обеспечит надежное функционирование предприятия в условиях постоянно меняющейся киберугрозы.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечки информации — неправомерная передача конфиденциальных сведений (материалов, важных для различных компаний или государства, персональных данных граждан), которая может быть умышленной или случайной. Информация утекает в результате бесконтрольного распространения секретов за пределы кабинета, здания, предприятия. Несоблюдение правил защиты и хранения данных влекут за собой их утечку и распространение в общедоступных местах, таких как сеть «Интернет».

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.

Каналы утечки информации можно разделить по физическим свойствам и принципам функционирования:

- акустические — запись звука, подслушивание и прослушивание;
- акустоэлектрические — получение информации через звуковые волны с дальнейшей передачей её через сети электропитания;
- виброакустические — сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;
- оптические — визуальные методы, фотографирование, видеосъемка, наблюдение;
- электромагнитные — копирование полей путём снятия индуктивных наводок;
- радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съёма речевой информации «закладных устройств», модулированные информативным сигналом;
- материальные — информация на бумаге или других физических носителях информации.

Технические каналы утечки информации можно разделить на естественные и специально создаваемые.

Естественные каналы утечки информации возникают при обработке информации техническими средствами (электромагнитные каналы утечки информации) за счет побочных электромагнитных излучений, а также вследствие наводок информационных сигналов в линиях электропитания технического средства обработки информации,

соединительных линиях вспомогательных технических средств и систем (ВТСС) и посторонних проводниках (электрические каналы утечки информации).

К специально создаваемым каналам утечки информации относятся каналы, создаваемые путем внедрения в техническое средство обработки информации электронных устройств перехвата информации (закладных устройств) и путем высокочастотного облучения технического средства обработки информации.

1.1 Акустический канал

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, т. е. первичные сигналы, прошедшие по электроакустическим трактам связи и вещания и соответственно видоизмененные по своим параметрам.

1.2 Акустоэлектрический канал

Акустоэлектрический канал утечки информации, особенностями которого являются:

- удобство применения (электросеть есть везде);
- отсутствие проблем с питанием у микрофона;
- возможность съёма информации с питающей сети не подключаясь к ней (используя электромагнитное излучение сети электропитания). Прием информации от таких «жучков» осуществляется специальными приёмниками, подключаемыми к силовой сети в радиусе до 300 метров от «жучка» по длине проводки или до силового трансформатора, обслуживающего здание или комплекс зданий;

- возможные помехи на бытовых приборах при использовании электросети для передачи информации, а также плохое качество передаваемого сигнала при большом количестве работы бытовых приборов.

Предотвращение: трансформаторная развязка является препятствием для дальнейшей передачи информации по сети электропитания.

1.3 Виброакустический канал (телефонный)

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 подается 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).

1.4 Оптический канал

В оптическом канале получение информации возможно путём:

- визуального наблюдения,
- фото-видеосъемки,
- использования видимого и инфракрасного диапазонов для передачи информации от скрыто установленных микрофонов и других датчиков.

В качестве среды распространения в оптическом канале утечки информации выступают:

- безвоздушное пространство;
- атмосфера;
- оптические световоды.

1.5 Электрический канал

Причины появления каналов утечки информации следующие:

- наводки электромагнитных излучений системы на соединительные линии и посторонние проводники;
- просачивание сигналов информации в связи электропитания системы;
- попадание информационных сигналов в цепи заземления системы.

1.6 Электромагнитный канал

Электромагнитный канал утечки информации – физический путь от источника побочных электромагнитных излучений и наводок различных технических средств к злоумышленнику за счёт распространения электромагнитных волн в воздушном пространстве и направляющих системах.

Переносчиком информации являются электромагнитные волны в диапазоне от сверхдлинных с длиной волны 10 000 м (частоты менее 30 Гц) до субмиллиметровых с длиной волны 1 - 0,1 мм (частоты от 300 до 3000 ГГц). Каждый из этих видов электромагнитных волн обладает специфическими особенностями распространения как по дальности, так и в пространстве. Длинные волны, например, распространяются на весьма большие расстояния, миллиметровые — наоборот, на удаление лишь прямой видимости в пределах единиц и десятков километров. Кроме того, различные телефонные и иные провода и кабели связи создают вокруг себя магнитное и электрическое поля, которые также выступают элементами утечки информации за счет наводок на другие провода и элементы аппаратуры в ближней зоне их расположения.

2 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ

Указы Президента Российской Федерации:

- "Об утверждении Перечня сведений конфиденциального характера" от 06.03.1997 N 188 (ред. от 13.07.2015);
- "Об утверждении Перечня сведений, отнесенных к государственной тайне" от 30 ноября 1995 г. N 1203.

Постановления Правительства Российской Федерации:

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

На веб-сайте Федеральной службы по техническому и экспортному контролю (ФСТЭК) также существует отдельный раздел, включающий в себя специальные нормативно-технические документы. Эти документы представляют собой нормативные правовые акты, организационно-распорядительные документы, а также нормативные и методические материалы, включая разрабатываемые проекты документов в области технической защиты 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. 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. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

3 АНАЛИЗ ЗАЩИЩАЕМОГО ПОМЕЩЕНИЯ

3.1 Общая информация о предприятии

Объектом защиты является фирма ООО «Alpha», занимающаяся предоставлением услуг по разработке веб-сайтов.

Основные информационные процессы и потоки в организации.

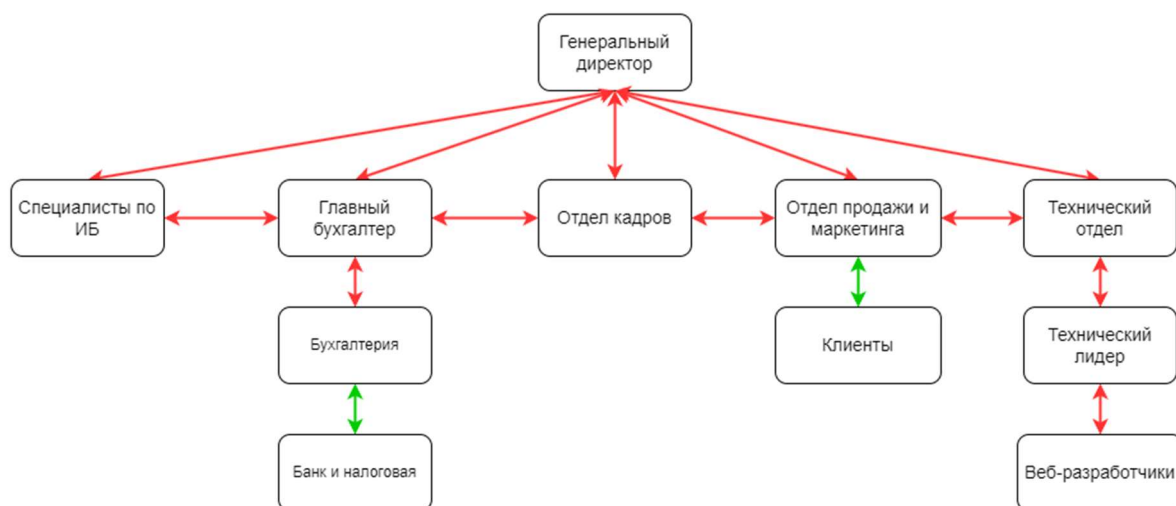


Рисунок 1 – Информационные потоки

3.2 Описание помещения

На рисунке 3 представлен план защищаемого помещения с учетом мебелировки, а в таблице 1 приведены обозначения объектов в каждом помещении и их краткое описание.

Номера на плане здания соответствуют следующим помещениям:

- 1 - Приёмная: 20м²
- 2 - Туалет: 20м²
- 3 - пространство для отдыха: 35м²
- 4 - офис: 70м². Расположены 16 столов, 16 стульев, 16 АРМ.
- 5 - кабинет директора: 25м²
- 6 - переговорная: 45м²
- 7 - серверное помещение: 12м². Расположены 2 сервера.
- 8 - помещение охраны: 20м²
- 9 - коридор

Помещение расположено на втором этаже малоэтажного здания, окна выходят в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными

лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

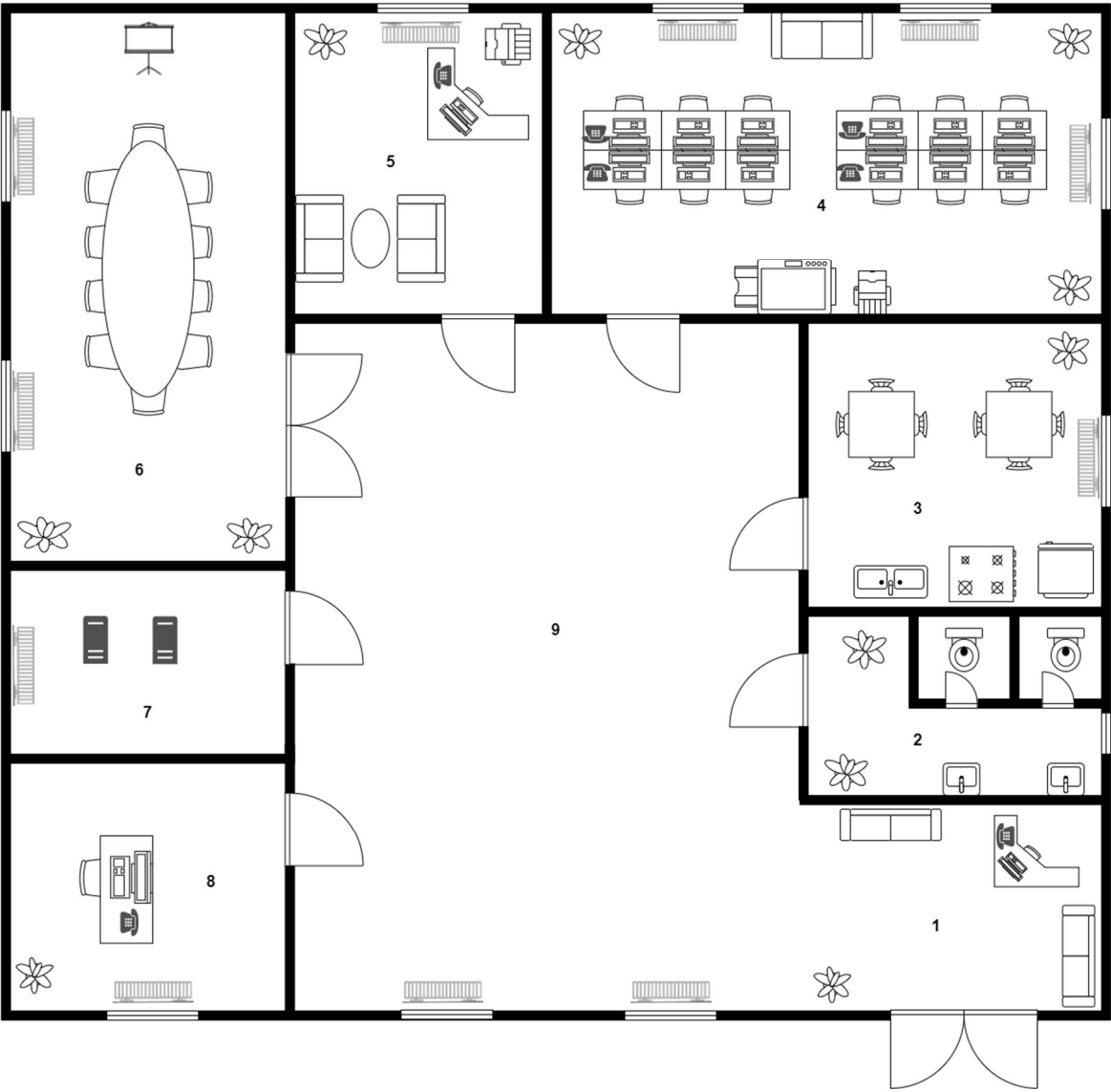
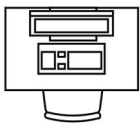


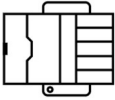



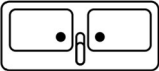
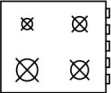

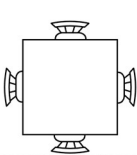
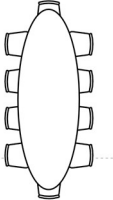
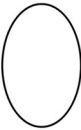






Рисунок 2 – План здания с учетом мебелировки помещений

Таблица 1 – Описание выбранных объектов при мебелировке помещения

| Объект | Обозначение |
|---|-----------------------|
|  | Рабочее место с АРМом |

| | |
|---|--------------------------------|
|  | Телефон |
|  | Сканер |
|  | Принтер |
|  | Диван |
|  | Санузел |
|   | Раковина |
|  | Электрическая плита |
|  | Холодильник |
|   | Стол и стулы |
|  | Стол |
|  | Экран для проектора |
|  | Сервер |
|  | Батарея центрального отопления |
|  | Живое растение |

3.3 Анализ возможных утечек информации

В помещениях существует множество путей для возможной утечки информации, включая стены, электрическое оборудование (например, принтеры, компьютеры) и другие элементы. В каждом помещении имеются розетки, сетевые устройства. Типы каналов утечки информации, которые могут происходить в помещениях: электрический канал и электромагнитный канал, акустический канал, виброакустический канал, акустоэлектрический канал и оптический канал. В таблице 2 представлена подробная информация о каналах утечки информации.

Таблица 2 – Активная и пассивная защита информации

| Канал утечки | Источники | Пассивная защита | Активная защита |
|-----------------------------------|--|--|---|
| Акустический, акустоэлектрический | Окна, двери, электрические сети, проводка и объекты, которые могут скрыть подслушивающие устройства. | Использование звукоизоляции для предотвращения утечки звука. | Устройства акустического зашумления |
| Виброакустический | Батарей и все твердые поверхности помещений | Использование материалов с амортизацией для уменьшения вибраций. | Устройства вибрационного зашумления |
| Оптический | Стекол окон, двери | Шторы на окнах, тонирующие пленки на окна, доводчики на дверях | Бликующие устройства |
| Электромагнитный, электрический | Розетки, компьютер, принтеры, бытовая техника | Фильтры для сетей электропитания | Устройство электромагнитного зашумления |

4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «совершенно секретно». Согласно требованиям «Типовых норм и правил проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденных Решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 N199, 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 Анализ СЗИ для акустического и виброакустического каналов

Пассивная защита: усиленные звукоизоляционные двери SWEDOOR by Jeld-Wen Sound 201DB (23 500 руб.).

Активная защита: в следующей таблице сравниваются и анализируются характеристики некоторых устройств, используемых для активной защиты.

Таблица 3 – Анализ средств активной защиты от утечки информации

| Наименование средства | Система активной акустической и вибрационной защиты акустической речевой информации СОНАТА-АВ модель 4Б | Система постановки виброакустических помех ЛГШ-402 | Генератор акустического шума ЛГШ-304 |
|-----------------------|---|--|---|
| Характеристики | <ul style="list-style-type: none"> - Сертификат ФСТЭК - Диапазон частот 175-11200 Гц - Система активной акустической и вибрационной защиты акустической речевой информации "Соната-АВ" модель 4Б, предназначена для защиты речевой информации в выделенных помещениях, от утечки по акустическим, виброакустическим и акустоэлектрическим каналам. | <ul style="list-style-type: none"> - Сертификат ФСТЭК - Диапазон частот 175-11200 Гц - Изделие предназначено для защиты акустической речевой информации, циркулирующей в помещениях, предназначенных для обсуждения или воспроизведения, а также проведения мероприятий с обсуждением информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки информации по виброакустическому и акустическому каналам. | <ul style="list-style-type: none"> - Сертификат ФСТЭК - Диапазон частот 175-11200 Гц - Защиты акустической речевой информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, циркулирующей (обрабатываемой) в помещениях, путем формирования акустических маскирующих шумовых помех. |
| Цена (руб.) | 44 200 | 18 200 | 25 220 |

На основании проведенного анализа и сравнения характеристик нескольких устройств, было принято решение выбрать модель "СОНАТА-АВ 4Б" для системы активной акустической и вибрационной защиты акустической речевой информации. Эта модель обладает рядом выдающихся характеристик:

– Увеличение стойкости защиты: Реализовано многогенераторное независимое возбуждение заградительной помехи в нескольких точках, что существенно повышает эффективность защиты. Исключение электроакустического преобразования в излучателях способствует дополнительному укреплению системы.

– Снижение стоимости комплексов: Предельная безизбыточность комплексов защиты обеспечивает гибкость в выборе сочетаний излучателей. Возможность комбинирования различных сочетаний на одном питающем шлейфе способствует экономии средств.

Выбор модели "СОНАТА-АВ 4Б" основан на эффективности ее характеристик, таких как увеличение стойкости защиты за счет многогенераторного возбуждения и снижение стоимости комплексов виброакустической защиты благодаря безизбыточности комплексов.

4.2 Анализ СЗИ для электрического, электромагнитного, акустоэлектрического каналов

Пассивная защита представляет собой фильтры 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.

Таблица 4 – Анализ средств активной защиты от утечки информации

| Наименование средства | Генератор зашумления Соната РС2 | Генератор шума Соната Р3.1 | Двухканальный генератор Зашумления SEL SP-44 |
|-----------------------|---|--|--|
| Характеристики | <ul style="list-style-type: none"> - Диапазон частот до 2 ГГц - Предназначен для активной защиты объектов ВТ (объектов вычислительной техники) или, другими словами, переговорных помещений от утечки информации через линии электропитания и заземления. | <ul style="list-style-type: none"> - Диапазон частот 0,01...200 МГц - Предназначено для защиты информации от утечки информации за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и | <ul style="list-style-type: none"> - Диапазон частот от 0,01МГц до 2000МГц - SEL SP- 44 является генератором шума по электросети и техническим средством защиты информации от утечки по сети электропитания, а также устройством подавления устройств несанкционированного съёма информации, |

| | | | |
|-------------|--------|--------------------------------------|--|
| | | токоведущие инженерные коммуникации. | использующих электросеть в качестве канала передачи. |
| Цена (руб.) | 23 600 | 33 120 | 24 000 |

В результате проведенного сравнительного анализа мы приняли решение о выборе системы СОНАТА-21 РС.2. Основными преимуществами данной системы являются возможность регулировки уровня шума в трех частотных полосах и доступность удаленного управления. Эти характеристики делают систему подходящей как для автономного использования, так и в составе комплекса технических средств защиты информации (ТСЗИ).

Дополнительно, для защиты от перехвата электромагнитных излучений (ПЭМИН) была выбрана СОНАТА-РЗ.1. Эта система обеспечивает эффективную защиту от утечек информации, создавая в окружающем пространстве электромагнитное поле шума и индуцируя маскирующие шумовые напряжения на линиях сети электропитания и заземления.

Одним из ключевых факторов при выборе было также совпадение производителя обеих систем, что значительно упрощает интеграцию и снижает временные и финансовые затраты на подключение оборудования.







4.3 Анализ СЗИ для оптического канала





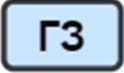

Для обеспечения защиты от визуального наблюдения было принято решение установить на окна жалюзи. В качестве выбора были предпочтены жалюзи "Inspire" по цене 1450 рублей за штуку. Общая стоимость установки жалюзи для данного помещения составила 14 500 рублей.

5 РАССТАНОВКА ТЕХНИЧЕСКИХ СРЕДСТВ

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

Таблица 5 – Описание расстановок технических средств на помещении и расчет стоимости оснащения

| Наименование СЗИ | Обозначение | Место расположение | Цена (руб.) | Количество (шт) | Стоимость |
|---|---|--|-------------|-----------------|-----------|
| Звукоизоляционные двери SWEDOOR by JELD-WEN Sound 201DB |  | На каждой двери | 23 500 | 5 | 117 500 |
| Блок электропитания и управления «Соната- ИП4.3» |  | У стен | 21 600 | 1 | 21 600 |
| Генератор акустоизлучатель «Соната-СА-4Б1» |  | - стены - один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения; | 3 540 | 53 | 187 620 |
| |  | - 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); | | | |
| Генератор Вибровозбудитель «Соната-СВ-4Б» |  | - один на каждый вентиляционный канал или дверной тамбур; - один на каждые 8...12 м3 надпотолочного пространства или др. пустот. | 7 440 | 12 | 89 280 |
| Размыкатели Соната-ВК4.1 |  | | 6 000 | 1 | 6000 |
| Размыкатели Соната-ВК4.2 |  | Около каждого телефона | 6 000 | 7 | 42 000 |
| Размыкатели Соната-ВК4.3 |  | | 6 000 | 1 | 6000 |
| Генератор шума «Соната-РС2» |  | Около проводников, у стен | 23 600 | 1 | 23 600 |
| Соната-РЗ.1 | - | Подключена напрямую к «Соната-ИП4.3» | 33 120 | 1 | 33 120 |
| Жалюзи Inspire |  | На каждом окне | 1 450 | 10 | 14 500 |
| Итог | | | | | 541 220 |

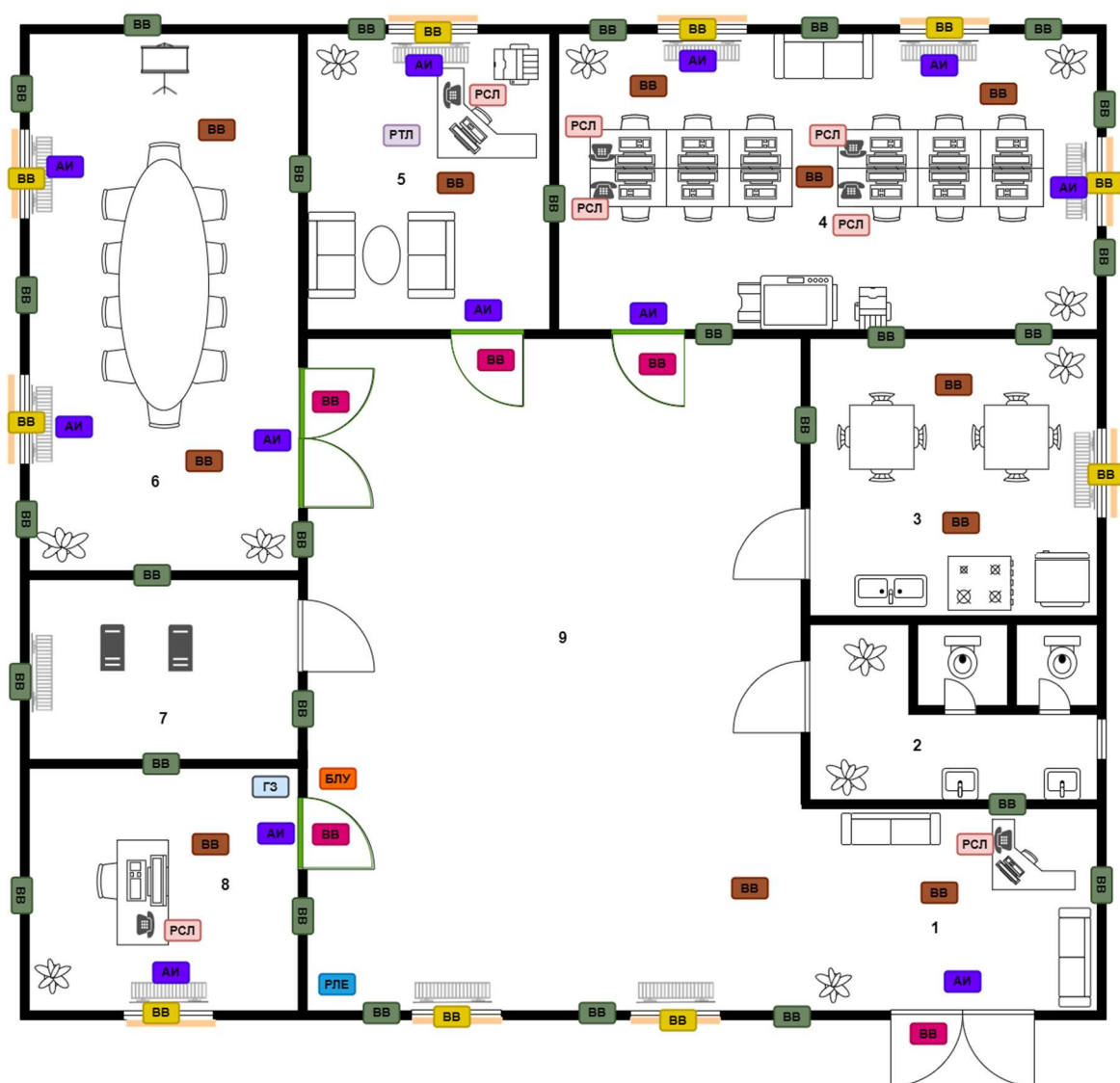


Рисунок 3 – План помещения после расстановки защитных средств

ЗАКЛЮЧЕНИЕ

В рамках проведенного анализа технических каналов утечки информации были выявлены потенциальные угрозы и уязвимости в области информационной безопасности. Этот анализ позволил разработать эффективные меры для предотвращения утечек и несанкционированного раскрытия информации. Подробный обзор защищаемого помещения дал полное представление о его физической структуре, архитектурных особенностях и системах коммуникации, что помогло выявить конкретные уязвимости и риски информационной безопасности.

На основе анализа рынка технических средств были выбраны наиболее подходящие технологии и инструменты для реализации системы защиты информации. Это позволило разработать оптимальное решение, учитывая специфические потребности и требования помещения. Размещение выбранных технических средств было осуществлено с учетом рекомендаций и требований, обеспечивая наивысшую эффективность и защиту информации.

Проведенные меры пассивной и активной защиты информации способствуют обеспечению конфиденциальности, целостности и доступности данных в помещении. Важно отметить, что защита информации является динамическим процессом, требующим постоянного обновления и совершенствования. Рекомендуется проводить регулярные аудиты и тестирования системы защиты информации для выявления новых уязвимостей и принятия соответствующих мер. Такой подход обеспечивает непрерывное улучшение уровня защиты помещения и снижение риска утечек и раскрытия конфиденциальной информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия РФ, 1998. 320 с.
2. А. Торокин: «Инженерно-техническая защита информации: учебное пособие для студентов», М.: Гелиос АРВ, 2005. – 960 с.
3. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с.
4. Евстифеев А.А., Ерошев В.И., Мартынов А.П., Николаев Д.Б., Сплюхин Д.В., Фомченко В.Н. Основы защиты информации от утечки по техническим каналам. Саров: РФРЦ-ВНИИЭФ, 2019. -267с., ил.
5. Рекомендации по определению количества и мест установки акустоизлучателей и вибровозбудителей. [Интернет-ресурс] URL:
<http://npoanna.ru/Content.aspx?name=recommendations.placement>.