

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

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Инженерно-технические средства защиты информации»

**КУРСОВАЯ РАБОТА**

**на тему**

«Проектирование инженерно-технической системы защиты информации на предприятии»

**Выполнила:**

Чыонг Тан Зыонг, студентка группы N34471

\_\_\_\_\_  
(подпись)

**Проверил:**

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

\_\_\_\_\_  
(отметка о выполнении)

\_\_\_\_\_  
(подпись)

Санкт-Петербург

2023 г.

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

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

**Студент** Чыонг Тан Зыонг

(Фамилия И.О.)

**Факультет** Безопасность информационных технологий

**Группа** N34471

**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**

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**

Чыонг Тан Зыонг

(Подпись, дата)

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

**Студент** Чыонг Тан Зыонг

(Фамилия И.О.)

**Факультет** Безопасность информационных технологий

**Группа** N34471

**Направление (специальность)** 10.03.01 (Технологии защиты информации 2020)

**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

| №<br>п/п | Наименование этапа   | Дата завершения |             | Оценка и подпись<br>руководителя |
|----------|--|-----------------|-------------|----------------------------------|
|          |  | Планируемая     | Фактическая |                                  |
| 1        | Разработка и утверждение задания и календарного плана на курсовую работу         | 15.11.2023      | 15.11.2023  |                                  |
| 2        | Анализ теоретической составляющей  | 01.12.2023      | 01.12.2023  |                                  |
| 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** Попов Илья Юрьевич

(Подпись, дата)

**Студент**

Чыонг Тан Зыонг

(Подпись, дата)

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

Студент Чыонг Тан Зыонг

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34471

Направление (специальность) 10.03.01 (Технологии защиты информации 2020)

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 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 рынка технических средств; Расстановка технических средств; Заключение;

Список использованных источников

4. Выводы

В результате работы была предложена защита от утечек информации по акустическому, оптико-виброакустическому, оптическому, акустоэлектрическому, электрическому, электромагнитному, электронному техническим каналам защиты информации, обеспечена защита от ПЭМИН.

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент

Чыонг Тан Зыонг

(Подпись, дата)

## СОДЕРЖАНИЕ

|  |    |
|--|----|
| Содержание .....   | 6  |
| Введение .....   | 7  |
| 1     АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ.....                | 8  |
| 1.1    Визуально-оптические .....                                      | 9  |
| 1.2    Акустические .....  | 9  |
| 1.3    Электромагнитные.....   | 10 |
| 1.4    Материально-вещественные.....                                   | 11 |
| 2     ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ.....                             | 12 |
| 3     АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ .....                                | 14 |
| 3.1    Общая информация о предприятии .....                            | 14 |
| 3.2    Описание помещения .....  | 14 |
| 3.3    Анализ возможных утечек информации и выборы СЗИ .....           | 17 |
| 4     АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ.....                | 19 |
| 4.1    Анализ СЗИ для акустического и виброакустического каналов ..... | 20 |
| 4.2    Анализ СЗИ для визуально-оптического канала .....               | 23 |
| 4.3    Анализ СЗИ для электромагнитного каналов.....                   | 23 |
| 5     РАССТАНОВКА ТЕХНИЧЕСКИХ СРЕДСТВ .....                            | 26 |
| Заключение.....  | 29 |
| Список литературы.....   | 30 |

## **ВВЕДЕНИЕ**

В процессе строительства, развития и утверждения позиции на рынке каждая компания хранит много информации по разным вопросам. Среди них есть информация, которую компания публикует для общественного доступа, но также есть информация, которую необходимо абсолютно сохранять в секрете из-за ее конфиденциальности, которая прямо влияет на интересы компании и многих ее сотрудников.

Информационная безопасность обеспечивает безопасность передачи информации в конкретной области с использованием различных передовых методов, избегая негативных воздействий угроз. Таким образом, информационная безопасность в предприятии заключается в сохранении информации, напрямую связанной с существованием и развитием предприятия, в определенном, защищенном пространстве. Это имеет крайне важное значение для выживания каждой компании.

Информационная безопасность в предприятии должна обеспечивать абсолютную целостность, доступность и аутентичность информации. Предприятие реализует меры информационной безопасности через действия, такие как предотвращение утечки внутренних данных, обеспечение конфиденциальности взаимодействия с партнерами или клиентами, поддержание строгой тайны персональной информации о сотрудниках, стратегий развития и так далее. Реализация эффективной и успешной информационной безопасности требует грамотного сочетания реальных инструментов с применением технологий и надежной команды сотрудников. Это подчеркивает сложность и важность обеспечения информационной безопасности в предприятии.

## **1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ**

Каналы утечки информации существуют в любом информационном пространстве. Под каналом утечки в самом общем смысле понимают неконтролируемый способ передачи информации. В результате злоумышленник может получить несанкционированный доступ к нужным ему конфиденциальным данным компании.

Утечка относится к:

- раскрытие данных лицами, имеющими доступ к секретной информации;
- потеря флэш-накопителей и других типов носителей информации, на которых хранилась конфиденциальная информация;
- умышленное хищение секретной информации с использованием шпионажа за открытыми каналами ее утечки.

Как правило, факт утечки конфиденциальной информации проявляется не сразу. В результате, например, получения коммерческой тайны предприятия конкурент может долгое время не выдавать себя и не распространять данные. Однако факт хищения «выявляется» со временем, что выражается в виде серьезных финансовых или материальных потерь для организации.

Согласно общепринятой классификации существующие каналы утечки информации могут быть косвенными или прямыми. Когда речь идет о непрямых каналах, то подразумевают, что злоумышленник имеет прямой доступ к технической среде конкретной системы защиты информации.

Примеры косвенных утечек:

- Утеря флэш-носителя или его умышленная кража.
- Поиск конфиденциальных данных путем попыток исследовать мусор, выброшенные документы и т. д.
- Чтение паразитного электромагнитного излучения и помех.
- Попытка хищения информации оптическими средствами: фотографирование объектов информационной системы, прослушивание помещений.

При взаимодействии с прямыми каналами злоумышленник получает доступ к оборудованию и информации, которая используется в информационной системе.

Ярким примером прямого канала утечки является деятельность инсайдеров. Сами сотрудники компании в большинстве случаев становятся средством передачи информации злоумышленнику. Это может произойти намеренно или случайно. В первом случае

сотрудник сознательно устраивается на работу в организацию с целью дальнейшего выведывания тайны, во втором – непреднамеренное раскрытие происходит в неформальной обстановке.

Прямое копирование информации еще называют утечками по прямым каналам.

Для защиты данных в компаниях чаще всего задействована одна основная автоматизированная система, поэтому важно учитывать все технические каналы утечки, предполагающие варианты хищения данных с использованием физических свойств системы.

### **1.1 Визуально-оптические**

Визуально-оптические каналы, предполагает передачу конфиденциальной информации с использованием визуальных средств и оптических технологий. Проблемы включают в себя риск незаконного наблюдения за действиями или информацией на экране, а также опасения по поводу несанкционированной записи или видеозаписи. Чтобы свести к минимуму риски, рекомендуется принять такие меры, как контроль видимого диапазона, использование защитных пленок для экрана, управление рабочими пространствами, обучение персонала и применение вспомогательных технологий, таких как оптические фильтры.

### **1.2 Акустические**

Одним из значительных вызовов в области информационной безопасности является опасность утечки чувствительной информации через аудиопротоколы. Угроза может произойти из различных источников и требует строгих профилактических мер для обеспечения безопасности информации. Вот некоторые подробности по этому вопросу:

**Основные Угрозы:**

- **Неправильная Запись Звука:** Неправильное выполнение процесса записи звука может привести к нежелательному раскрытию чувствительной информации.
- **Дальнейшая Запись Звука:** Современные технологии позволяют записывать звук с дистанции, увеличивая риск упущенных предупреждений.

**Средства Атаки:**

- **Использование Ультразвука:** Применение технологии ультразвука может позволить доступ к информации, которую человеческий слух не воспринимает.

**Профилактические Меры:**



- Контроль Записывающих Устройств: Установка и строгое следование политикам контроля за использованием устройств записи в предприятии.
- Контроль Окружающего Звука: Использование технологии для мониторинга и контроля окружающего звука, особенно в местах, где требуется обеспечить безопасность информации.
- Минимизация Уровня Шума: Применение методов для минимизации уровня шума с целью улучшения защиты чувствительной информации.
- Обучение Сотрудников: Проведение обучения сотрудников относительно конкретных рисков и мер безопасности, связанных с информационной безопасностью через звуковые протоколы.

Для защиты важной информации организации важно понимать риски и реализовывать эффективные меры информационной безопасности для предотвращения утечек данных через аудиопотоки.

### **1.3 Электромагнитные**

Представляет опасность также перехват информации, содержащейся в побочных электромагнитных излучениях и наводках (ПЭМИН). Электромагнитные волны могут исходить от любого электрического прибора, установленного в помещении, например: – от микрофонов телефонов и переговорных устройств; – от основных цепей заземления и питания; – от аналоговой телефонной линии; – от волоконно-оптических каналов связи. Технологии позволяют подключать закладные устройства ПЭМИН непосредственно к цепям питания или же установить в мониторе или корпусе компьютера для перехвата следующих данных:

- выводимых на экран монитора;
- вводимых с клавиатуры или другого периферийного устройства;
- выводимых через провода на периферийные устройства;
- записываемых на жесткий диск и иные устройства.

Способами борьбы в этом случае станут заземление проводов, экранирование наиболее явных источников электромагнитного излучения, выявление закладок или же использование специальных программных и аппаратных средств, позволяющих выявить закладки.

Все вышеперечисленные способы утечки информации требуют территориальной доступности источника для похитителя, зона работы обычного устройства перехвата звуковой или визуальной информации не превышает нескольких десятков метров. Установка закладных устройств для съема электромагнитных излучений и акустических колебаний должна потребовать прямого проникновения на объект. Наиболее же серьезную опасность несут современные способы хищения с использованием возможностей сети Интернет и доступа с ее помощью к архивам данных или голосовому трафику.

Система инженерно-технической безопасности должна проектироваться комплексно, поэтому ее элементы должны составлять единую систему, контроль над работоспособностью, которой должен быть возложен на компетентных сотрудников. При этом комплексное применение всего диапазона методов защиты может быть избыточным, поэтому для организации систем защиты информации в конкретной компании нужно создавать собственный проект, который окажется оптимальным с ресурсной точки зрения..

#### **1.4 Материально-вещественные**

Материально-вещественными каналами утечки информации это область исследования, касающаяся способов утечки или сбора информации через физические элементы и материалы в окружающей среде. Меры безопасности включают в себя управление документами, правильное уничтожение чувствительных материалов и использование материалов, сопротивляющихся методам сбора информации.

## **2 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ**

Основными указами Президента Российской Федерации в области предотвращения утечки информации по техническим каналам являются:э

- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644.
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.

Основными постановлениями Правительства Российской Федерации в области предотвращения утечки информации по техническим каналам являются:

- 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»;

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.

### 3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

#### 3.1 Общая информация о предприятии

Объектом защиты является фирма ООО «Square» предоставляет услуги, связанные с продажей недвижимости, включая услуги такие как брокерские услуги по недвижимости, управление недвижимостью и оценка стоимости недвижимости.

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа (рисунок 1).

Условные обозначения:

- Красная стрелка: совершенно секретная информация;
- Зеленая стрелка: открытый поток.

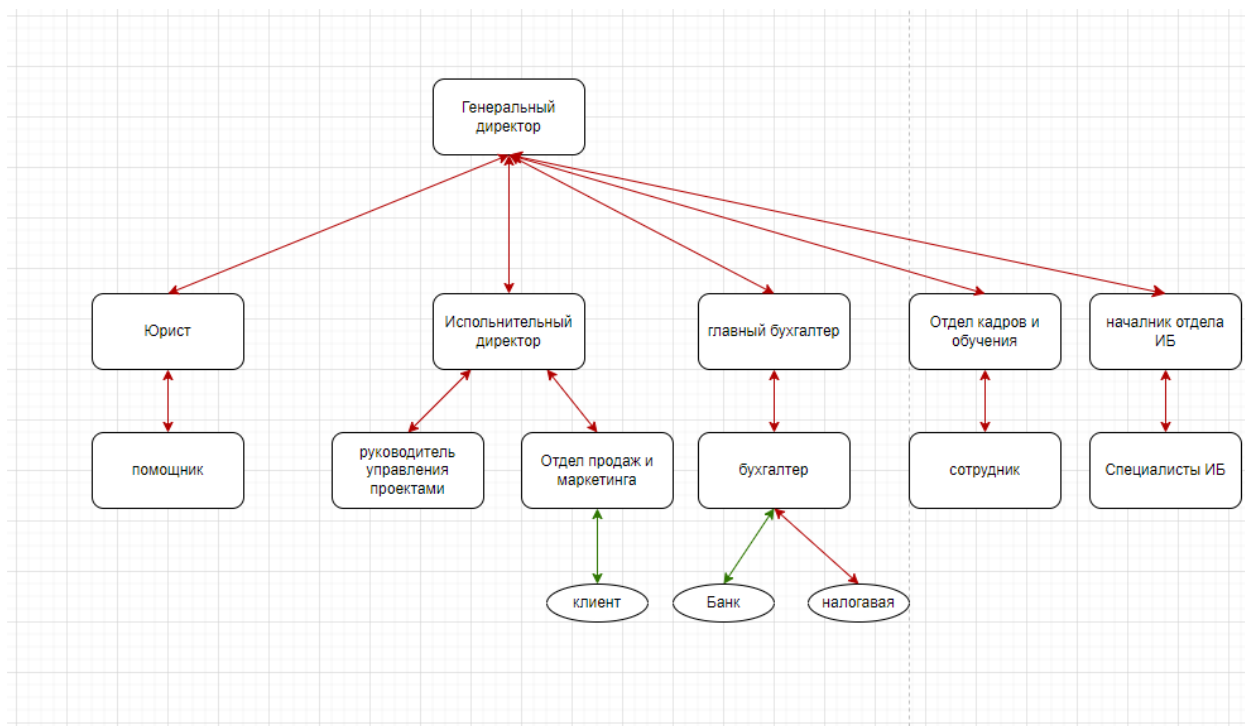


Рисунок 1 – Открытые и закрытые информационные потоки предприятия

#### 3.2 Описание помещения

На рисунке 2 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 – переговорная: Там находятся стол для переговоров и стулья вокруг него, экран для проектора, проектор и шкаф

2 – Офис управления недвижимостью. В комнате 2 окна. В офисе есть письменный стол с компьютером и шкаф..

3 – кабинет заместителя директора: В помещении есть два окна. В офисе есть письменный стол с компьютером и шкаф.

4 – Кабинет директора: В помещении есть два окна. В офисе есть письменный стол с компьютером и шкаф.

5 – кухня

6 – приёмная

7 – офис, В офисе располежны 16 столов, 16 стульев, 16 АРМ.

8 – помещение охраны

9 – туалет

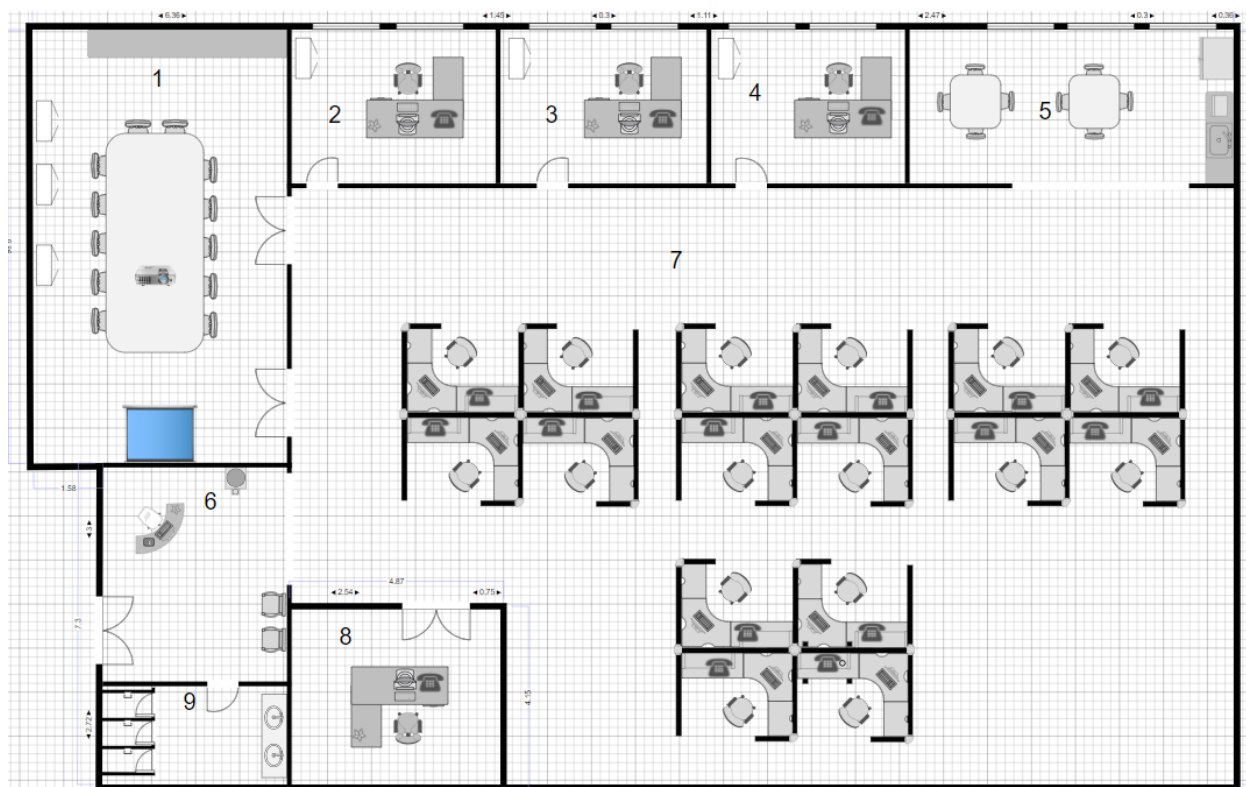
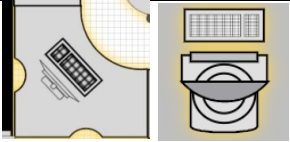
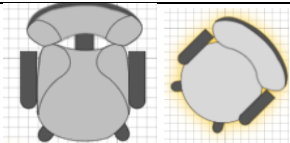

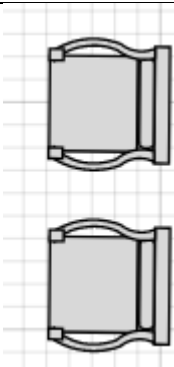
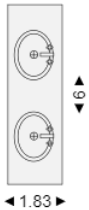
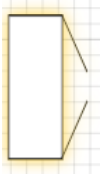

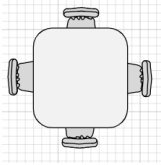





Рисунок 2 – План здания с учетом мебелировки помещений

Таблица 1 – Описание выбранных объектов при мебелировке помещения

| Объект | Обозначение |
|--------|-------------|
|--------|-------------|

|   |                                    |
|---|------------------------------------|
|    | Рабочее место с АРМо               |
|    | вращающееся кресло с подлокотником |
|    | Живое растение                     |
|    | стул для ожидания                  |
|  | Раковины                           |
|  | шкаф                               |
|  | Электрическая плита                |
|  | Круглый стол                       |
|  | Телефон                            |

|   |                            |
|---|----------------------------|
|  | <p>Проектор</p>            |
|  | <p>Экран для проектора</p> |

Офис расположен на третьем 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.

### **3.3 Анализ возможных утечек информации и выборы СЗИ**

Каналы утечки звука могут возникнуть по разным причинам, и основные факторы зависят от окружающей среды и способа организации или развертывания системы. Вот несколько основных причин:

- **Использование Нелегальных Аудиозаписывающих Устройств:** Использование скрытых устройств для записи звука может быть размещено в стратегических местах для сбора информации без ведома других.
- **Небезопасные Проведение Совещаний:** На важных совещаниях, если не принимаются меры по обеспечению безопасности звука, несанкционированные лица могут записывать информацию, к которой они не должны иметь доступ.
- **Не Безопасные Системы Звука:** Если система звука не правильно защищена, существует риск несанкционированного доступа или утечки информации.
- **Отсутствие Понимания Вопросы Защиты Звука:** Организации могут не осознавать, что звук также является важной формой информации и требует защиты.
- **Технические Средства Противостояния Звуку:** Технологии, такие как использование аппаратных средств противостояния, могут помочь хакерам записывать звук на расстоянии, не имея непосредственного доступа к источнику звука.



– Не Контролируемая Окружающая Среда: Если окружающая среда не контролируется, звук может легко просачиваться. Это может включать в себя звуки из телефонных разговоров, разговоры на рабочем месте или даже голосовые разговоры в открытом пространстве.

– Технически Продвинутое Техники Хакеров: Хакеры могут использовать сложные техники, такие как анализ звука, чтобы извлечь информацию из звуковых волн.

В помещениях присутствуют декоративные элементы, в которых можно спрятать закладное устройство. В каждом помещении имеются розетки, сетевые устройства, а значит, актуальны электрический и электромагнитный каналы утечки информации. Также есть угроза снятия информации по вибрационному и оптическому каналам. В таблице 2 приведено описание всех элементов, изображенных на плане помещения.

Таблица 2 – Активная и пассивная защита информации

| Канал утечки                   | Источники   | Пассивная защита  | Активная защита                                   |
|--------------------------------|---|---|---|
| Акустический                   | Окна, двери, электрические сети, проводка и розетки | Звуко-изоляция, звуко-поглощение                                      | Звуко-подавление, защищенные акустические системы |
| Вибрационный виброакустический | Батареи и все твердые поверхности помещений         | максимальное снижение уровня перехватываемого сигнала                 | Создание помех                                    |
| Визуально-оптический           | Незащищенные окна, двери                            | Снизить освещенность защищаемого объекта и его отражательные свойства | Средства сокрытия защищаемых объектов             |
| ПЭМИН                          | Розетки, АРМы, бытовая техника                      | Экранирование, заземление, фильтрация, развязка                       | Зашумление  |

#### **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 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 Анализ СЗИ для акустического и виброакустического каналов**

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.

Архитектурно-планировочные меры предусматривают выполнение определенных требований при проектировании или реконструкции помещений с целью исключения или ослабления неконтролируемого распространения звука. Например – особое расположение помещений или оборудование их элементами акустической безопасности (тамбуры, ориентирование окон в сторону контролируемой зоны).

Режимные меры – строгий контроль пребывания в контролируемой зоне сотрудников и посетителей.

Организационно — технические меры – использование звукопоглощающих средств. Пористые и мягкие материалы типа ваты, ворсистые ковры, пенобетон, пористая сухая штукатурка являются хорошими звукоизолирующими и звукопоглощающими материалами — в них очень много поверхностей раздела между воздухом и твердым телом, что приводит к многократному отражению и поглощению звуковых колебаний (звукопоглощение, отражение и пропускание звука).

Для определения эффективности защиты звукоизоляции используются шумомеры. Шумомер — это измерительный прибор, который преобразует колебания звука в числовые показания. Измерения акустической защищенности реализуются методом образцового источника звука (с заранее известным уровнем мощности на определенной частоте).

Имея образцовый источник звука и шумомер, можно определить поглощающие возможности помещения. Величина акустического давления образцового источника звука известна. Принятый с другой стороны стены сигнал замерен по показаниям шумомера. Разница между показателями и дает коэффициент поглощения

В тех случаях, когда пассивные меры не обеспечивают необходимого уровня безопасности, используются активные средства. К активным средствам относятся генераторы шума — технические устройства, вырабатывающие шумоподобные сигналы. Эти сигналы подаются на датчики акустического или вибрационного преобразования.

Акустические датчики предназначены для создания акустического шума в помещениях или вне их, а вибрационные — для маскирующего шума в ограждающих конструкциях.

Вибрационные датчики приклеиваются к защищаемым конструкциям, создавая в них звуковые колебания.

Генераторы шума позволяют защищать информацию от утечки через стены, потолки, полы, окна, двери, трубы, вентиляционные коммуникации и другие конструкции с достаточно высокой степенью надежности.

Таблица 3 – Сравнительный анализ средств активной защиты по виброакустическому каналу

| Наименование средства | Вуаль – Генератор акустических и виброакустических помеховых сигналов (средство активной защиты)  | Генератор маскирующего шума «Камертон5»  | «Соната АВ- 4Б»   |
|-----------------------|---|--|---|
| Характеристики        | <ul style="list-style-type: none"> <li>- сертификат соответствия ФСТЭК России № 2636 на генератор «Вуаль»</li> <li>- Диапазон частот 100 – 11200 Гц</li> <li>-Генератор акустических и виброакустических помеховых сигналов «Вуаль» в совокупности с акустическими и вибропреобразователями является средством активной защиты и используется для защиты выделенных помещений от утечки речевой информации по акустическому и виброакустическому каналам</li> </ul> | <ul style="list-style-type: none"> <li>- Сертификат ФСТЭК</li> <li>- Диапазон частот 90 - 11200 Гц</li> <li>- Предназначен для обеспечения защиты акустической речевой информации от утечки по акустическому и вибрационному каналам, за счет акустоэлектрических преобразований во вспомогательных технических средствах и системах, блокирует применение направленных и лазерных микрофонов</li> </ul> | <ul style="list-style-type: none"> <li>- Сертифицировано ФСТЭК</li> <li>- Диапазон рабочих частот 175 - 11200 Гц</li> <li>- Система защиты речевой информации от утечки по техническим каналам "Соната- АВ" модель 4Б, предназначена для защиты речевой информации в выделенных помещениях, от утечки по акустическим, виброакустическим, акустоэлектрическим и оптико-электронным (лазерным) каналам.</li> </ul> |
| Цена (руб.)           | <b>44 730</b>   | 46000  | 44,200  |

По результатам проведенного анализа средств защиты, в качестве системы виброакустической защиты была выбрана «Соната АВ-4Б».

Данное средство имеет сертификат ФСТЭК и обладает следующими преимуществами:

- возможность построения системы автоматического контроля всех элементов
- снижение трудозатрат на конфигурирование и тестирование системы при инсталляции и контроле
- возможность изменения настроек генераторов-излучателей
- снижение затрат на создание единого комплекса ТСЗИ

#### 4.2 Анализ СЗИ для визуально-оптического канала

Необходимую и достаточную защиту обеспечивают жалюзи. Они выбраны в связи с простотой и эффективностью в эксплуатации.

Были выбраны рулонные шторы Роллайт 2 с технологией BlackOut 100 см \* 150 см 3190 руб/шт.

#### 4.3 Анализ СЗИ для электромагнитного каналов

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 представлены в Таблице 4.

Таблица 4. Сравнительный анализ средств активной защиты информации для электромагнитного и электрического каналов

| Устройство                                 | Цена, руб | Характеристики  | Описание   |
|--|-----------|---|--|
| Фильтр сетевой помехоподавляющий «ФСПК-40» | 47,000    | Напряжение питания 220/380 В $\pm$ 10%, 50 Гц                             | Фильтр сетевой помехоподавляющий ФСПК-40-220-99-УХЛ4 предназначен для защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания. В общем случае защитное устройство может применяться как сетевой фильтр для улучшения параметров качества сети. |
| Генератор шума «Соната РС2»                | 23,600    | Диапазон частот до 2 ГГц, диапазон регулировки уровня шума не менее 35 дБ | 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. Регулировка уровня шума в 3 частотных полосах. Индикация нормального/аварийного режима работы. Сертифицировано ФСТЭК. |
| «Соната-РЗ»<br>средство активной защиты информации от утечки за счет ПЭМИН | 97,200 | Световая и звуковая индикация, потребляемая мощность 30 Вт, электропитание от сети 220 В, время непрерывной работы 8 часов | Изделие может быть включено в состав комплекса ТСЗИ. В этом случае управление его работой и контроль режима работы (исправности) будет осуществляться от пульта управления "СонатаДУ4.1" в комплексе с блоком питания "СонатаИП4.х" (Комплекс 3095, Комплекс 3106, Комплекс 3109). Сертифицировано ФСТЭК.          |

Пространственное зашумление предполагает создание маскирующих помех в окружающем пространстве и используется для исключения перехвата ПЭМИН по электромагнитному каналу. Цель пространственного зашумления считается достигнутой, если отношение опасный сигнал/шум на границе контролируемой зоны не превышает некоторого допустимого значения, рассчитываемого по специальным методикам для каждой частоты информационного (опасного) побочного электромагнитного излучения. В

системах пространственного зашумления в основном используются помехи типа «белого шума» или «синфазные помехи».

Системы линейного зашумления применяются для маскировки наведенных опасных сигналов в линиях, если они имеют выход за пределы контролируемой зоны.

В простейшем случае система линейного зашумления представляет собой генератор шумового сигнала, формирующий шумовое маскирующее напряжение с заданными спектральными, временными и энергетическими характеристиками. Генератор гальванически подключается в линию, которую необходимо зашумить (например, посторонний проводник).

Ниже в таблице 4 приведен сравнительный анализ подходящих средства активной защиты помещений от ПЭМИН. В результате анализа был выбран генератор шума «Соната РЗ». Данный выбор обоснован особенностями конструкции устройства, которые позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники.

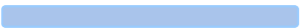
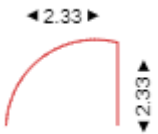


Дополнительно был выбран маскиратор электромагнитных излучений Маис-М2, так как оно обладает лучшими характеристиками по сравнению с другими средствами пассивной защиты от ПЭМИН.



## 5 РАССТАНОВКА ТЕХНИЧЕСКИХ СРЕДСТВ

В таблице 5 ниже описано, где разместить оборудование, а также количество оборудования и стоимость его оснащения.

Таблица 4 – Описание расстановок технических средств на помещении и расчет стоимости оснащения

| Средство ЗИ                               | Обозначение   | Место расположение  | Цена (руб.) | Количество (шт) | Стоимость |
|---|---|---|-------------|-----------------|-----------|
| 1   | 2   | 3   | 4           | 5               | 6         |
| Рулонные шторы                            |    | На каждом окне  | 3190        | 11              | 32670     |
| Звукоизоляционные двери                   |    | На двери  | 61020       | 4               | 244080    |
| Соната-ИП4.3 Блок электронного управления |   | У стен  | 21600       | 1               | 21600     |
| Генератор вибровозбудителей СВ-4Б         |  | - <b>стены</b> - один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения; | 7440        | 58              | 43152     |

|                                    |     |   |       |    |        |
|------------------------------------|-----|---|-------|----|--------|
|                                    | ВВ  | - <b>потолок</b> , пол - один на каждые 15...25 м2 перекрытия;  |       |    |        |
|                                    | ВВ  | - <b>окна</b> - один на окно (при установке на оконный переплет);   |       |    |        |
|                                    | ВВ  | - <b>двери</b> - один на дверь (при установке на верхнюю перекладину дверной коробки);  |       |    |        |
| Генератор акустоизлучателей СА-4Б1 | АИ  | - один на каждый вентиляционный канал или дверной тамбур;<br>- один на каждые 8...12 м3 надпотолочного пространства или др. пустот. | 3 540 | 18 | 63720  |
| Размыкатели Соната-ВК4.2           | РТЛ | Около каждого телефона  | 6000  | 4  | 24000  |
| Соната-РЗ.1                        | -   | подключена напрямую к «Соната-ИП4.3»  | 33120 | 1  | 33120  |
| «Маил-М2»                          | -   | подключена к системе электроснабжения согласно рекомендациям производителя  | 39500 | 1  | 39500  |
|                                    |     |   |       |    | 857540 |

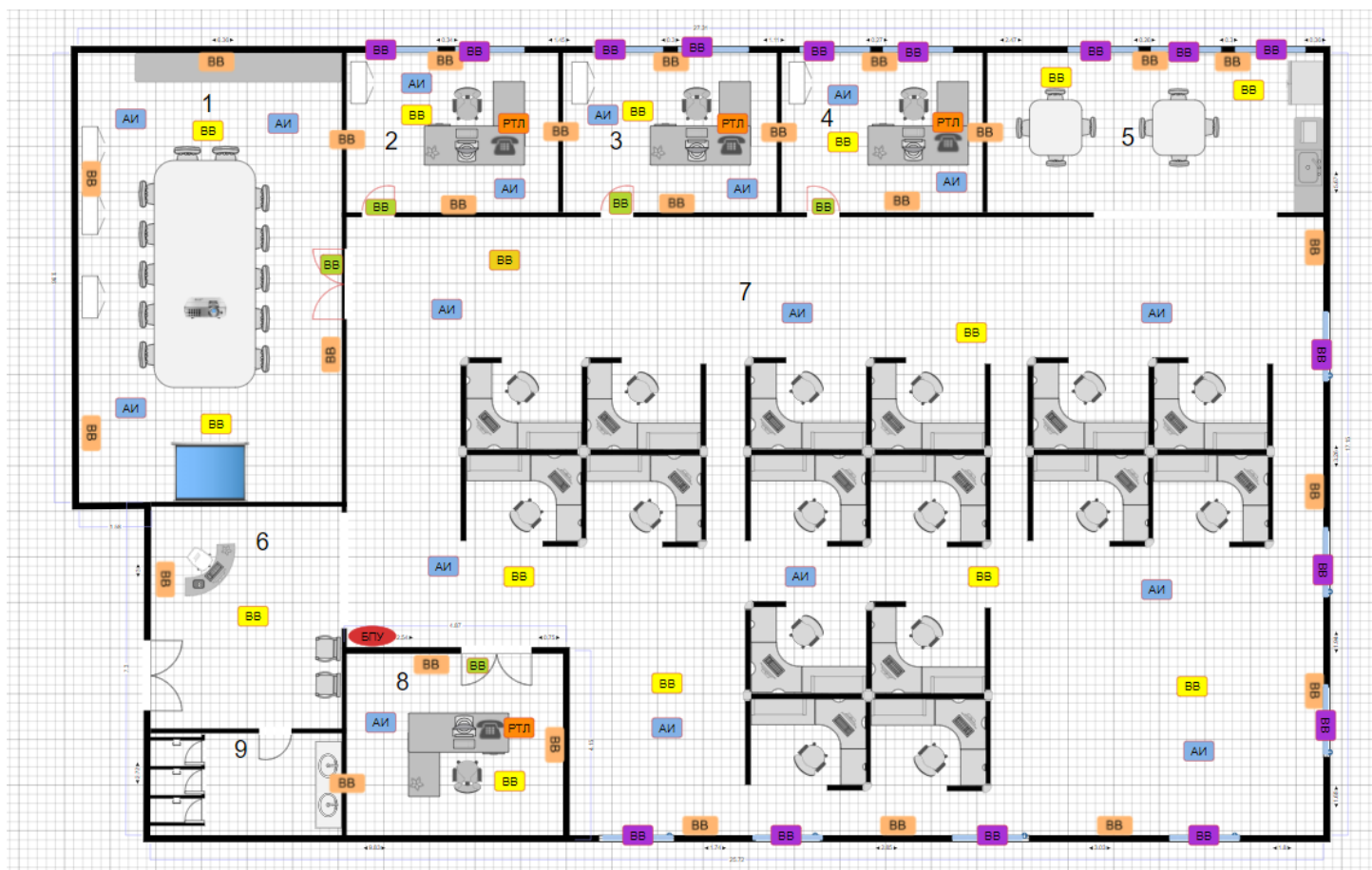


Рисунок 3 – План помещения после расстановки защитных средств

## **ЗАКЛЮЧЕНИЕ**

В ходе данной курсовой работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении, а также описаны необходимые меры их защиты. Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для объекта средства защиты. Был разработан план установки средств и произведен расчет сметы затрат. В результате работы 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. А. Торокин: «Инженерно-техническая защита информации: учебное пособие для студентов», М.: Гелиос АРВ, 2005. – 960 с.
3. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия РФ, 1998. 320 с
4. Защита информации от утечки по акустическим каналам: <https://www.anti-malware.ru/practice/methods/information-from-leakage-through-acoustic-channels-protection>
5. 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.
6. Рекомендации по определению количества и мест установки акустоизлучателей и вибровозбудителей. URL: <http://npoanna.ru/Content.aspx?name=recommendations.placement>