

**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»**

**Выполнил:**

Студент группы N34461  
Фомин Олег Максимович



**Проверил преподаватель:**

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

Санкт-Петербург

2023 г.

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

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

|                                    |   |
|------------------------------------|---|
| <b>Студент</b>                     | Фомин Олег Максимович   |
|                                    | (Фамилия И.О.)  |
| <b>Факультет</b>                   | Безопасности информационных технологий  |
| <b>Группа</b>                      | N34461  |
| <b>Направление (специальность)</b> | 10.03.01. - Технологии защиты информации                                      |
| <b>Руководитель</b>                | Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО                     |
|                                    | (Фамилия И.О.,<br>должность, ученое звание, степень)                          |
| <b>Дисциплина</b>                  | Инженерно-технические средства защиты информации                              |
| <b>Наименование темы</b>           | Проектирование системы защиты от утечки информации по<br>различным<br>каналам |
| <b>Задание</b>                     | Разработка системы инженерно-технической защиты информации в помещении        |

**Краткие методические указания**

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

**Содержание пояснительной записки**

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

## Рекомендуемая литература

---

Руководитель

---

(Подпись, дата)

Студент



---

(Подпись, дата)

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

## ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

**Студент**      Фомин Олег Максимович  
(Фамилия И.О.)

---

**Факультет**      Безопасности информационных технологий

---

**Группа**      N34461

---

**Направление (специальность)**      10.03.01. - Технологии защиты информации

---

**Руководитель**      Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО  
(Фамилия И.О., должность, ученое звание, степень)

---

**Дисциплина**      Инженерно-технические средства защиты информации

---


**Наименование темы**      Проектирование системы защиты от утечки информации по различным каналам

---

| №<br>п/п | Наименование этапа              | Дата завершения |             | Оценка и подпись<br>руководителя |
|----------|---------------------------------|-----------------|-------------|----------------------------------|
|          |                                 | Планируемая     | Фактическая |                                  |
| 1        | Создание плана КР               | 24.11.2023      | 24.11.2023  |                                  |
| 2        | Анализ литературы               | 3.12.2023       | 3.12.2023   |                                  |
| 3        | Составление основного текста КР | 15.12.2023      | 10.12.2023  |                                  |
| 4        | Защита курсовой работы          | 26.12.2023      | 26.12.2023  |                                  |

**Руководитель**      Попов Илья Юрьевич  
(Подпись, дата)

---

**Студент**        
(Подпись, дата)

---

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

|                             |   |
|-----------------------------|---|
| Студент                     | Фомин Олег Максимович   |
| Факультет                   | Безопасности информационных технологий                                  |
| Группа                      | N34461  |
| Направление (специальность) | 10.03.01. - Технологии защиты информации                                |
| Руководитель                | Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО               |
| Дисциплина                  | Инженерно-технические средства защиты информации                        |
| Наименование темы           | Проектирование системы защиты от утечки информации по различным каналам |

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

**1. Цель и задачи работы**

Предложены студентом ☒                      Сформулированы при участии студента ☐

Определены руководителем ☐

Цель - Разработать инженерно-техническую систему защиты информации для предприятия

**2. Характер работы**

Расчет ☐    ☐    Конструирование ☐

Моделирование ☐    Другое ☒

**3. Содержание работы**

Анализ защищаемого помещения, оценка каналов утечки информации, выбор средств и методов защиты информации.

**4. Выводы**

По итогам проделанной работы была разработана система инженерно-технической защиты информации от утечек, повышающей защищенность информации, обрабатываемой в организации

Руководитель      Попов Илья Юрьевич

(Подпись, дата)

Студент



(Подпись, дата)

« 12 » декабря 2023 г.

## **СОДЕРЖАНИЕ**

|   |    |
|---|----|
| ВВЕДЕНИЕ .....                                  | 7  |
| 1 ОПИСАНИЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ .....      | 8  |
| 2 РУКОВОДЯЩИХ ДОКУМЕНТОВ .....                  | 15 |
| 3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ .....             | 17 |
| 4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ .....        | 23 |
| 5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ..... | 30 |

## **ВВЕДЕНИЕ**

В современном информационном обществе защита информации является одной из ключевых задач предприятий и организаций. Учитывая постоянно возрастающую угрозу кибератак, важность реализации эффективной инженерно-технической системы защиты информации на предприятии становится очевидной.

Инженерно-техническая защита (ИТЗ)— это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации. Средства защиты информации (СЗИ) обеспечивают защиту информации в информационных системах, по сути, представляющих собой совокупность хранимой в базах данных информации, информационных технологий, обеспечивающих ее обработку, и технических средств. Они позволяют предотвратить несанкционированный доступ злоумышленника к ресурсам и данным предприятия, тем самым снизив риск несанкционированных утечки, утраты, искажения, уничтожения, копирования и блокирования информации и, как следствие, нанесения экономического, репутационного или других видов ущерба предприятию

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну на объекте информатизации. Защищаемый объект состоит из десяти помещений и представляет собой офис предприятия с переговорной, кабинетом директора, серверной, двумя санузлами, 3 кабинетами отдела разработки, главным холлом, и кухней.

## 1 ОПИСАНИЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Под каналами утечки информации понимаются методы и способы получения закрытой информации. Категории и группы каналов утечки информации представлены на рисунке 1.

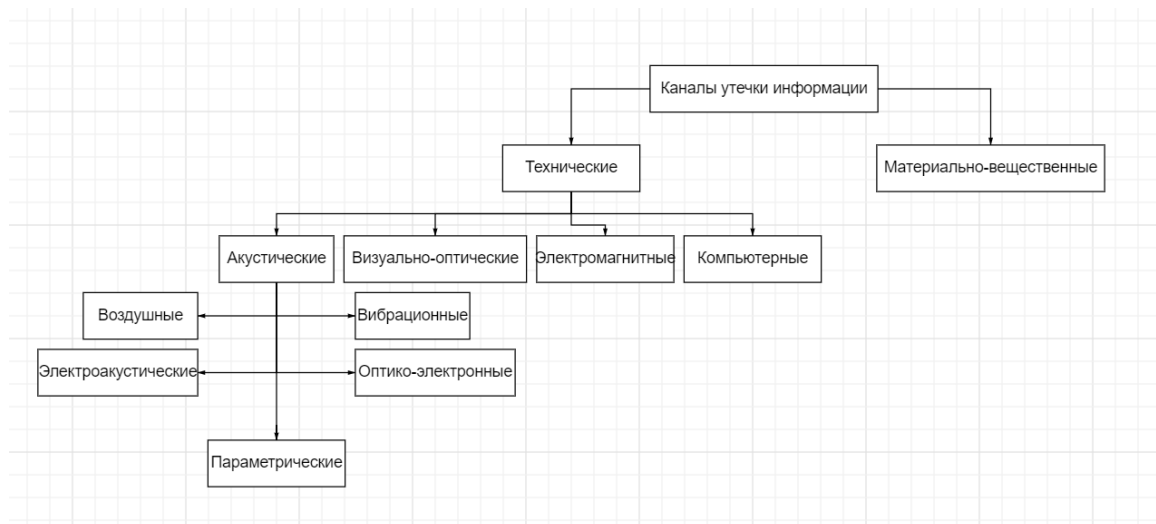


Рисунок №1. Категории и группы каналов утечки информации

### 1.1 Описание технических каналов утечки информации

#### 1.1.1 Акустические каналы утечки информации

В зависимости от среды распространения акустических колебаний, способов их перехвата и физической природы возникновения информационных сигналов, технические каналы утечки акустической информации подразделяются на воздушные, вибрационные, электроакустические, оптико-электронные и параметрические.

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух и для их перехвата используются миниатюрные высокочувствительные и направленные микрофоны, которые соединяются с диктофонами или специальными микропередатчиками. Подобные автономные устройства, объединяющие микрофоны и передатчики, обычно называют акустическими закладками. Перехваченная этими устройствами акустическая информация может передаваться по радиоканалу, по сети переменного тока, соединительным линиям, посторонним проводникам, трубам и т.п.

| Методы съема информации | Способы съема информации | Методы и средства защиты информации |
|-------------------------|--------------------------|-------------------------------------|
|-------------------------|--------------------------|-------------------------------------|



|  |   |  |
|--|---|--|
| <ul style="list-style-type: none"> <li>• установка радио-закладок в стенах и мебели;</li> <li>• съем информации по системе вентиляции;</li> <li>• съем информации направленным микрофоном</li> </ul> | <ul style="list-style-type: none"> <li>• подслушивание;</li> <li>• диктофон;</li> <li>• микрофон (направленный микрофон)</li> </ul> | <ul style="list-style-type: none"> <li>• шумовые генераторы;</li> <li>• поиск закладок (установление контрольных проверок);</li> <li>• система контроля доступа</li> </ul> |
|--|---|--|

*Таблица №1. Методы и способы съема информации на акустическом канале.*

В вибрационных каналах (структурных каналах) утечки информации средой распространения акустических сигналов является конструкция зданий (стены, потолки, полы), трубы водоснабжения и теплоснабжения, канализации и другие твердые тела.

| <b>Методы съема информации</b>   | <b>Способы съема информации</b>   | <b>Методы и средства защиты информации</b>   |
|--|---|--|
| <ul style="list-style-type: none"> <li>• за счет структурного звука в стенах и перекрытиях;</li> <li>• утечка по сети отопления</li> </ul> | <ul style="list-style-type: none"> <li>• вибродатчики;</li> <li>• инфракрасные датчики</li> </ul> | <ul style="list-style-type: none"> <li>• соблюдения требований при строительстве (реконструкции) целевых помещений;</li> <li>• защитные фильтры</li> </ul> |

*Таблица №2. Методы и способы съема информации на вибрационном канале.*

Электроакустические каналы утечки информации обычно образуются за счет преобразования акустических сигналов в электрические по двум основным направлениям: путем «высокочастотного навязывания» и путем перехвата через вспомогательные технические средства и системы. Технический канал утечки информации путем «высокочастотного навязывания» образуется при несанкционированном контактном введении токов высокой частоты от ВЧ-генератора в линии, имеющие функциональные связи с элементами вспомогательных технических средств и систем, на которых происходит модуляция ВЧ-сигнала. Наиболее часто подобный канал утечки информации используют для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны. С другой стороны, вспомогательные технические средства и системы могут сами содержать электроакустические преобразователи. К таким вспомогательным техническим средствам и системам относятся некоторые датчики пожарной сигнализации, громкоговорители ретрансляционной сети и т.д. Используемый в них эффект обычно называют «микрофонным эффектом».

| Методы съема информации   | Способы съема информации   | Методы и средства защиты информации  |
|---|--|--|
| <ul style="list-style-type: none"> <li>• съем информации за счет наводок и «навязывания»;</li> <li>• съем информации за счет использования «телефонного уха»;</li> <li>• утечка по охранно-пожарной сигнализации</li> </ul> | <ul style="list-style-type: none"> <li>• подключение к вспомогательным техническим средствам и системам (телефон, датчики пожарной сигнализации, громкоговорители ретрансляционной сети).</li> </ul> | <ul style="list-style-type: none"> <li>• использование специальных устройств;</li> <li>• отключение телефонных аппаратов от линии при введении в помещении конфиденциальных разговоров;</li> <li>• установка в телефонной линии специального устройства защиты, автоматически (без участия оператора) отключающего телефонный аппарат от линии при положенной телефонной трубке;</li> <li>• использование метода «выжигания» закладных устройств или их блоков питания путем подачи в линию высоковольтных импульсов;</li> <li>• поиск закладок (установление контрольных проверок)</li> </ul> |

*Таблица №3. Методы и способы съема информации на электроакустическом канале.*

При облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей, таких как стекла окон, зеркал, картин и т.п., создается оптико-электронный (лазерный) канал утечки акустической информации. Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация. Для перехвата речевой информации по данному каналу используются локационные системы, работающие,

как правило, в ближнем инфракрасном диапазоне и известные как «лазерные микрофоны». Дальность перехвата составляет несколько сотен метров.

| <b>Методы съема информации</b>   | <b>Способы съема информации</b>  | <b>Методы и средства защиты информации</b>  |
|--|--|---|
| <ul style="list-style-type: none"> <li>• лазерный съем акустической информации с окон</li> <li>• снятие оптических сигналов</li> </ul> | <ul style="list-style-type: none"> <li>• с помощью «лазерных микрофонов»;</li> <li>• оптические приемники;</li> <li>• фотодетекторы</li> </ul> | <ul style="list-style-type: none"> <li>• звукоизоляция окон;</li> <li>• установка на стекла окон «виброгенераторов»</li> <li>• установка оптических усилителей</li> </ul> |

*Таблица №4. Методы и способы съема информации на оптико-электронном канале.*

Параметрический канал утечки акустической информации образуется в результате воздействия акустического поля на элементы высокочастотных генераторов и изменения взаимного расположения элементов схем, проводов, дросселей и т.п., что приводит к изменениям параметров сигнала, например, модуляции его информационным сигналом. Промодулированные высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы соответствующими средствами. Параметрический канал утечки акустической информации может быть создан и путем высокочастотного облучения помещения, где установлены полуактивные закладные устройства, имеющие элементы, параметры которых (добротность, частота и т.п.) изменяются по закону изменения акустического (речевого) сигнала.

| <b>Методы съема информации</b>  | <b>Способы съема информации</b>  | <b>Методы и средства защиты информации</b>   |
|---|--|--|
| <ul style="list-style-type: none"> <li>• анализ электромагнитных излучений;</li> <li>• тепловизионное наблюдение</li> </ul> | <ul style="list-style-type: none"> <li>• детекторы электромагнитных излучений;</li> <li>• тепловизоры</li> </ul> | <ul style="list-style-type: none"> <li>• шумовые генераторы;</li> <li>• не устанавливать элементы высокочастотных генераторов в целевых помещениях;</li> <li>• поиск закладок (установление контрольных проверок)</li> </ul> |

*Таблица №5. Методы и способы съема информации на параметрическом канале.*

### **1.1.2 Визуально-оптические каналы утечки информации**

Визуально-оптические каналы утечки графической информации реализуются техническими средствами и предоставляют информацию в виде изображений объектов или копий документов, получаемых 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, для чего используются фотографические и телевизионные средства, соответствующие условиям съемки. Для снятия копий документов используются электронные и специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют видео закладки, либо осуществляют видеосъемку из зданий, расположенных по близости.

| <b>Методы съема информации</b>  | <b>Способы съема информации</b>  | <b>Методы и средства защиты информации</b>   |
|---|--|--|
| <ul style="list-style-type: none"> <li>• наблюдение;</li> <li>• фотографирование;</li> <li>• видеосъемка объекта</li> </ul> | <ul style="list-style-type: none"> <li>• съем информации с использованием видео-закладок;</li> <li>• использование закамуфлированной техники (фотоаппарата, видеокамеры);</li> <li>• наблюдение за объектом вне его зоны (из соседних зданий)</li> </ul> | <ul style="list-style-type: none"> <li>• экранировка помещения;</li> <li>• использование жалюзи или штор;</li> <li>• поиск закладок (установление контрольных проверок)</li> </ul> |

*Таблица №6. Методы и способы съема информации на визуально-оптическом канале.*

### **1.1.3 Электромагнитные каналы утечки информации**

Для электромагнитных каналов утечки информации характерными являются побочные электромагнитные излучения и наводки различных технических средств за счет распространения электромагнитных волн в воздушном пространстве и направляющих системах.

Носителем информации является электрический ток, сила которого, напряжение, частота или фаза изменяются по закону информационного сигнала. В результате воздействия информационного сигнала на элементах генераторов наводятся электрические сигналы, которые могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов и излучение в окружающее пространство.

| Методы съема информации  | Способы съема информации  | Методы и средства защиты информации   |
|--|---|---|
| <ul style="list-style-type: none"> <li>• утечка за счет побочного излучения терминала;</li> <li>• съем информации с дисплея;</li> <li>• утечка по цепям заземления;</li> <li>• утечка по трансляционной цепи и громко говорящей связи;</li> <li>• утечка по охранно-пожарной сигнализации;</li> <li>• утечка по сети электропитания</li> </ul> | <ul style="list-style-type: none"> <li>• электромагнитный датчик;</li> <li>• акустические датчики</li> <li>•</li> </ul> | <ul style="list-style-type: none"> <li>• экранирование.</li> <li>• система контроля доступа;</li> <li>• поиск закладок (установление контрольных проверок)</li> </ul> |

Таблица №7. Методы и способы съема информации на электромагнитном канале.

#### 1.1.4 Компьютерные каналы утечки информации

Компьютерный канал утечки информации представляет собой тип утечки информации, который может происходить через различные технические средства, включая компьютеры, их периферийные устройства, сетевое оборудование и окружающие устройства.

| Методы съема информации  | Способы съема информации   | Методы и средства защиты информации  |
|--|--|--|
| <ul style="list-style-type: none"> <li>• программно-аппаратные закладки;</li> <li>• компьютерные вирусы, логические бомбы, троянские кони и т.п.;</li> </ul> | <ul style="list-style-type: none"> <li>• физический доступ;</li> <li>• сетевой мониторинг и перехват;</li> <li>• шпионское ПО</li> </ul> | <ul style="list-style-type: none"> <li>• использование сертифицированного ПО;</li> <li>• установка FireWall'ов;</li> <li>• установка антивирусного программного обеспечения</li> </ul> |

| <b>Методы съема информации</b>  | <b>Способы съема информации</b> | <b>Методы и средства защиты информации</b> |
|---|---------------------------------|--|
| <ul style="list-style-type: none"> <li>• подключение к удаленному компьютеру</li> </ul> |                                 |  |

*Таблица №8. Методы и способы съема информации на компьютерном канале.*

## **2.2 Материально-вещественные каналы утечки информации**

К материально-вещественным каналам утечки информации относится снятие информации непосредственно с носителей информации.

| <b>Методы съема информации</b>   | <b>Способы съема информации</b>  | <b>Методы и средства защиты информации</b>  |
|--|--|---|
| <ul style="list-style-type: none"> <li>• несанкционированное размножение, копирования или хищения носителей информации;</li> <li>• визуальный съем информации с дисплея или документов;</li> <li>• использование производственных и технологических отходов</li> </ul> | <ul style="list-style-type: none"> <li>• наблюдение;</li> <li>• обработка мусора;</li> <li>• копирование документов;</li> <li>• хищение носителей информации</li> <li>•</li> </ul> | <ul style="list-style-type: none"> <li>• система контроля доступа;</li> <li>• использование «уничтожителей документов»;</li> <li>• физическая защита</li> </ul> |

*Таблица №9. Методы и способы съема информации на материально-вещественном канале.*

## 2 РУКОВОДЯЩИХ ДОКУМЕНТОВ

Основными документами в области защиты информации являются:

- ФЗ Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;
- Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;
- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
- ПП РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»;
- ФЗ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- ПП РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1;
- Межведомственная комиссия по защите государственной тайны решение № 199 от 21.01.2011г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними";
- 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 НСД. Термины и определения;
- Руководящий документ. СВТ. Защита от НСД. Показатели защищенности от несанкционированного доступа к информации;

- Руководящий документ. Автоматизированные системы. Защита от НСД. Классификация автоматизированных систем и требования по защите информации;
- Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;
- Руководящий документ Гостехкомиссии России. Защита от НСД. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей;
- Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.



### 3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

#### 3.1 Схема помещения

Необходимо провести анализ защищаемого помещения, чтобы разместить технические средства защиты на объекте. План помещения предприятия офисного типа представлен на рисунке №2. В таблице 10 представлены описание обозначений, изображенных на плане.

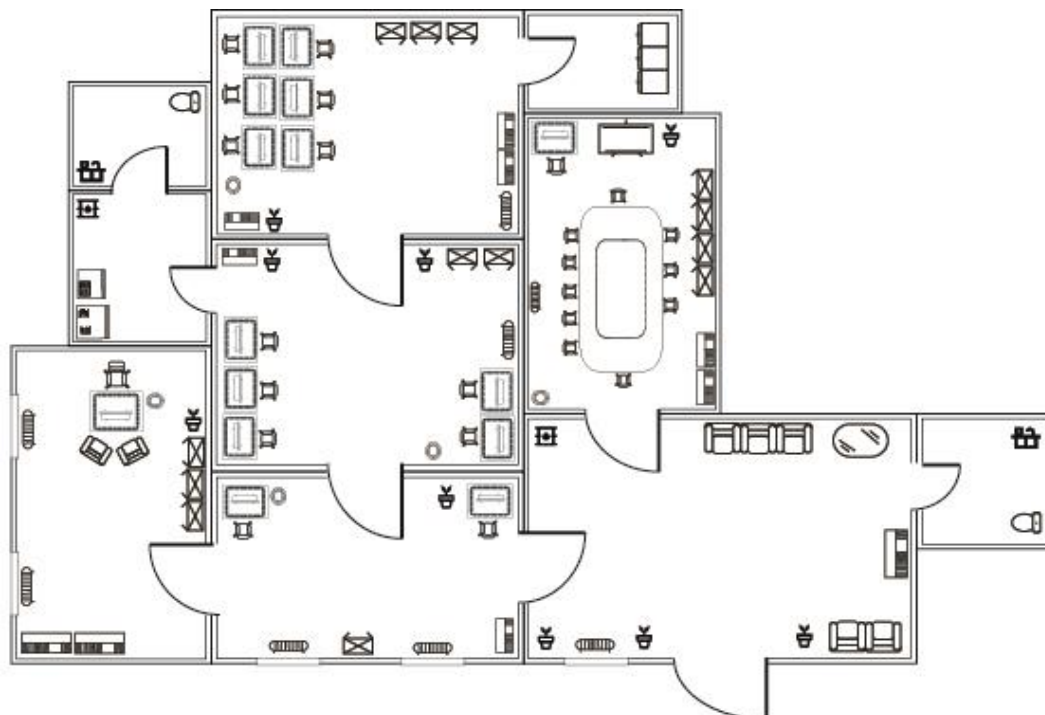



Рисунок №2. План защищаемого помещения

Таблица №10 – описание обозначений

| Обозначение   | Описание          |
|---|-------------------|
|  | Кресло            |
|  | Офисный стул      |
|  | Стул руководителя |

|   |                                  |
|---|----------------------------------|
|    | Компьютерный стол                |
|    | Стол переговоров                 |
|    | Журнальный стол                  |
|   | Кухонный стол                    |
|  | Компьютер                        |
|  | Интерактивная доска с проектором |
|  | Мусорное ведро для бумаги        |

Продолжение таблицы 10

| Обозначение   | Описание            |
|---|---------------------|
|    | Книжный шкаф        |
|    | Шкаф для документов |
|    | Радиатор отопления  |
|    | Кулер для воды      |
|   | Туалет              |
|  | Раковина            |
|  | Кофемашина          |
|  | Цветок<br>комнатный |

На рисунке № 3 обозначены информационные потоки организации: сплошной зеленой линией обозначены открытые потоки, а красным пунктиром обозначены закрытые потоки.

Информация ограниченного доступа:

- персональные данные сотрудников;
- коммерческая тайна (данные о производстве);
- финансовые данные;

- техническая информация;
- информация о новых разработках/улучшениях.

По открытым потокам передается:

- информация о продаже товаров;
- информация о состоянии платежей;
- юридическая информация для клиентов.

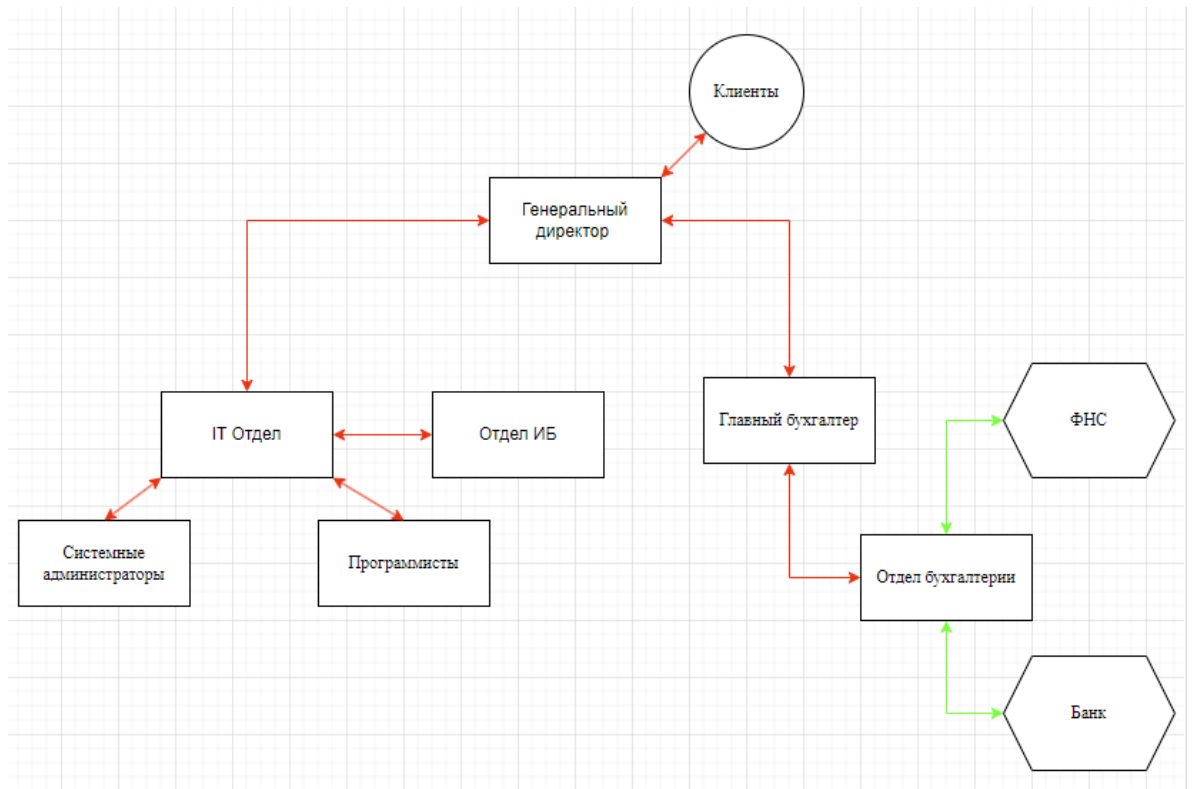


Рисунок №3. Схема информационных потоков на предприятии

### 3.2 Описание помещений

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

- кабинет директора (18 м<sup>2</sup>);
- переговорная комната (28 м<sup>2</sup>);
- офис 1 (17 м<sup>2</sup>);
- офис 2 (17,2 м<sup>2</sup>);
- офис 3 (15,7 м<sup>2</sup>);
- серверная комната (8 м<sup>2</sup>);

- кухня (12 м<sup>2</sup>);
- главный холл (35 м<sup>2</sup>).
- два санузла (18 м<sup>2</sup>)

Кабинет директора включает в себя: один стул руководителя, два стула, один компьютерный стол, два книжных шкафа, три шкафа для документов, одно мусорное ведро, два радиатора отопления, два окна и одно комнатное растение.

В переговорной комнате находятся одиннадцать стульев, один стол для переговоров, один компьютерный стол, один компьютер, четыре шкафа для документов, два книжных шкафа, одно мусорное ведро, один радиатор отопления и одно комнатное растение.

Офис 1, офис 2 и офис 3 предназначены для сотрудников предприятия.

В офисе 1 стоят два стула, два компьютерных стола, два компьютера, один книжный шкаф, один шкаф для документов, одно мусорное ведро для бумаги, один радиатор отопления, два окна и одно комнатное растение.

В офисе 2 есть пять стульев, пять компьютерных столов, пять компьютеров, один книжный шкаф, два шкафа для документов, одно мусорное ведро для бумаги, один радиатор отопления и два комнатных растения.

В офисе 3 находятся шесть компьютерных столов, шесть компьютеров, три книжных шкафа, три шкафа для документов, одно мусорное ведро, один радиатор отопления и одно комнатное растение.

В серверной комнате расположены три сервера.

В кухне есть кулер для воды и кухонный стол, на котором находятся одна кофемашина и одна микроволновая печь.

Главный холл предназначен для сотрудников предприятия и посетителей. В нем находятся пять кресел, два комнатных растения, один журнальный стол, книжный шкаф и кулер для воды.

Окна помещения выходят в закрытый двор, который находится под постоянным наблюдением и не имеет смежности с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и другими элементами, которые могли бы использоваться посторонними лицами для доступа в помещение. Помещения сгруппированы в «непроходной» (тупиковой) части здания, которая редко используется сотрудниками при выполнении служебных обязанностей, не связанных с доступом к государственной тайне.

Стены и внутренние перегородки здания выполнены из железобетона и имеют толщину не менее 13 см.

### **3.3 Анализ возможных каналов утечки информации**

В каждом помещении существуют потенциальные пути для нежелательной утечки информации, связанные с электромагнитными и электрическими утечками информации, то есть с использованием компьютеров и розеток. Декоративные элементы, такие как комнатные растения, могут использоваться для установки закладных устройств, которые могут использоваться для передачи информации через акустический канал.

Существуют также риски утечки информации через оптические каналы, например, из-за незакрытых окон и незащищенных дверей. Важно учитывать также виброакустический канал, который может быть использован для передачи информации из-за наличия твердых поверхностей, таких как стены или батареи отопления.

Вещественно-материальный канал утечки информации возможен ввиду наличия вещественных носителей информации, однако он не перекрывается техническими средствами защиты.

## 4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

### 4.1 Выбор средств защиты

Для обеспечения высокого уровня комплексной безопасности информации, которая отнесена к категории «совершенно секретно» в зависимости от её типа, требуется оснащение помещения специальными средствами и устройствами, перечисленными в таблице 11. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки такой конфиденциальной информации.

Таблица №11. Активная и пассивная защита информации

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

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

Пассивная защита включает себя размещение фильтров в электропитании всех помещений.

Активная защита заключается в использовании системы белого шума в сети, которая создает фоновый шум, маскирующий колебания, вызванные звуковыми волнами или работой

электронных устройств. Модели устройств, относительно которых будет идти дальнейший анализ, и их характеристики представлены в таблице №12.

*Таблица №12. Активная защита от утечек информации по электрическим каналам*

| <b>Модель</b>            | <b>Цена, руб.</b> | <b>Характеристики</b>   | <b>Особенности</b>   |
|--------------------------|-------------------|---|--|
| Соната-РС3               | 32 400            | Работа от сети<br>~220 В +10%/-15%, 50<br>Гц.<br>Потребляемая<br>мощность – 10Вт.<br>Продолжительность<br>работы не менее 8<br>часов.   | Звуковая и световая<br>индикация<br>работы. Возможно<br>дистанционное<br>управление<br>посредством<br>проводного пульта.   |
| ЛГШ-221                  | 36 400            | Диапазон частот<br>10 кГц – 400 МГц.<br>Диапазон регулировки<br>уровня выходного<br>шумового сигнала<br>не менее 20 дБ.<br>Мощность,<br>потребляемая от сети<br>не более 45 ВА. | Сетевой генератор<br>шума.<br>Устройство оснащено<br>световым<br>и звуковым<br>индикаторами<br>работы. Возможность<br>управления<br>устройством с<br>помощью пульта ДУ.  |
| Соната- РС1              | 16 520            | Диапазон частот до 1<br>ГГц, регулировка<br>уровня шума в 1<br>частотной полосе.<br>Напряжение 220 В.   | Возможность<br>локального проводного<br>управления в случае<br>использования в<br>составе комплекса<br>ТСЗИ (встроенный<br>модуль Rebus)   |
| Генератор<br>шума Покров | 32 800            | Диапазон частот 10<br>кГц – 6000 МГц.<br>Мощность 15 Вт.<br>Наработка на отказ<br>5000 часов.   | Централизованное<br>управление и контроль<br>по Ethernet (для<br>исполнения 2), для<br>применения в системах<br>пространственного<br>зашумления.<br>Независимая<br>регулировка уровней<br>электромагнитного<br>поля<br>шумового сигнала и<br>шумового сигнала в<br>линии электропитания<br>и заземления. |

На основании анализа, проведенного в таблице №11 был выбран генератор шума «Покров». Оптимальный вариант по соотношению цена и качество позволяют установить



достаточное количество подобных устройств в помещениях. Кроме того, этот выбор был обоснован самым широким диапазоном частот.

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

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

Активные меры безопасности представляют собой систему виброакустической маскировки. Для обеспечения безопасности помещения, в котором обрабатывается информация, отнесенная к категории «совершенно секретно», рассматриваются технические средства активной защиты информации для объектов информатизации, имеющих категорию не ниже 1Б.

*Таблица №13. Активная защита от утечек информации по (вибро-)акустическим каналам*

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

|                       |        |   |  |
|-----------------------|--------|---|--|
|                       |        |   | комплекте  |
| Шорох 5Л              | 21 500 | Максимальное количество излучателей – 40.<br>Электропитание 220 (+10% - 15%) В (есть возможность работы системы от источника питания 12В).<br>Количество октавных полос для регулировки уровня мощности шума – 7. | Сетевой генератор шума.<br>Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.  |
| SEL SP-157<br>Шагрень | 47 400 | Диапазон воспроизводимого шумового сигнала 90–11200 Гц.<br><br>Максимальное количество излучателей – 64.<br>Электропитание 220В/50Гц.   | Защита паролем настроек системы.<br>Отсчёт времени наработки генерации шума по каждому каналу с выводом на экран. Непрерывный контроль состояния системы и каждого отдельного излучателя.  |
| Соната<br>АВ-4Б       | 44 200 | Диапазон воспроизводимого шумового сигнала 175–11200 Гц.<br><br>Выходное напряжение В 12,5 ± 0,5.<br><br>Электропитание сеть ~220 В/50 Гц.  | Комплект состоит из блоков электропитания и управления, генераторов-акустоизлучателей, генераторов-вибровозбудителей, размыкателя телефонной линии, размыкателя слаботочной линии, размыкателя линии Ethernet,<br><br>пульта управления, блоков сопряжения из внешних устройств. Технического средства защиты речевой информации от утечки по опто-электронному (лазерному) каналу и прочих аксессуаров. |

#### 4.4 Защита от ПЭМИН

Таблица №14. Активная защита от ПЭМИН

| Модель      | Цена, руб. | Характеристики   | Особенности  |
|-------------|------------|--|--|
| ЛГШ 503     | 44 200     | Диапазон частот 10 кГц – 1800 МГц.<br>Уровень шума от -26 дБ (мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц).<br>Мощность – 45 Вт. | Оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа).<br>Оснащен счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы в режиме формирования маскирующих помех.<br>Прибор имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно аппаратный комплекс «Паутина». |
| Соната-РЗ.1 | 39 000     | Электропитание – 220 В +10%/-15%, 50 Гц.<br>Мощность – 10 Вт.<br>Продолжительность непрерывной работы не менее 8 ч   | Обеспечивает защиту информации от утечки за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума, а также наводок на   |

|                           |        |  |   |
|---------------------------|--------|--|---|
|                           |        |  | линии сети электропитания и заземления путем индуцирования в них маскирующих шумовых напряжений.  |
| ЛГШ-513                   | 33 120 | Диапазон частот 10 кГц – 1800 МГц. Уровень шума от -18 дБ(мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц).<br>Мощность – не более 45 ВА.<br>Режим работы – круглосуточно. | Изделие «ЛГШ-513» оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Изделие «ЛГШ-513» оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех. |
| Генератор шума<br>Пульсар | 24 525 | Диапазон частот 10 кГц – 6 ГГц.<br>Электропитание – однофазная сеть переменного тока 187–242 В.<br>Мощность – 50 ВА.                                       | Имеет защиту регулятора уровня выходного шумового сигнала от нелегального доступа (и сигнализирует об этом).<br>Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук).  |

В качестве средства активной защиты от ПЭМИН был выбран генератор шума «ЛГШ-503». Этот выбор обоснован широким диапазоном частот (от 10 кГц до 1800 МГц) и круглосуточным режимом работы. Кроме того, данный прибор поддерживает возможность подключения проводного дистанционного управления и контроля, для чего может быть использован программно-аппаратный комплекс «Паутина».

#### **4.5 Защита от утечек информации по оптическим каналам**

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

## 5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В предыдущей главе был проанализирован рынок инженерно-технических средств и были выбраны лучшие средства защиты информации из них, которые включает в себя:

- сетевой генератор шума «Покров»;
- система виброакустической защиты «Соната АВ-4Б»;
- генератор шума «ЛГШ-503» от ПЭМИН
- жалюзи на семь окон;
- три усиленные двери с толщиной 4 мм, обшитые металлическим листом не

менее 2 мм, внутри – звукоизоляционный материал.

Для каждого помещения оптимальное количество акустоизлучателей и вибровозбудителей зависит от различных факторов, таких как звукоизоляция, форма, материалы стен, местоположение, уровень фонового шума и другие подобные аспекты. Согласно информации на официальном веб-сайте производителя НПО «АННА» для выбранной системы виброакустической защиты, предварительную оценку необходимого количества вибровозбудителей «Соната СВ-4Б» можно провести, руководствуясь следующими стандартами:

- стены – один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- потолок, пол – один на каждые 15...25 м<sup>2</sup> перекрытия;
- окна – один на окно (при установке на оконный переплет);
- двери – один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Предварительная оценка необходимого количества акустоизлучателей «Соната СВ-4Б» может быть выполнена из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8...12 м<sup>3</sup> надпотолочного пространства или других пустот.

В таблице №15 содержится список мер защиты, предназначенных для применения во всех помещениях, а также конечная стоимость.

*Таблица №15. Необходимое оборудование*

| Меры защиты                     | Цена, руб | Количество, шт. | Итоговая стоимость |
|---------------------------------|-----------|-----------------|--------------------|
| Сетевой генератор шума «Покров» | 32 800    | 1               | 32 800             |

|   |        |    |         |
|---|--------|----|---------|
| Генератор шума «ЛГШ-503»                              | 44 200 | 1  | 44 200  |
| Блок электропитания и управления «Соната-ИП4.3»       | 21 600 | 1  | 21 600  |
| Генератор-акустоизлучатель «Соната СА-4Б1»            | 3 540  | 15 | 53100   |
| Генератор-вибровозбудитель «Соната СА-4Б»             | 7 440  | 63 | 468720  |
| Рызмыкатель телефонной линии «Соната ВК4.1»           | 6 000  | 2  | 12 000  |
| Рызмыкатель слаботочной линии «Соната ВК4.2»          | 6 000  | 1  | 6 000   |
| Рызмыкатель линии «Ethernet» «Соната ВК4.1»           | 6 000  | 1  | 6 000   |
| Пульт управления «Соната-ДУ 4.3»                      | 7 680  | 1  | 7 680   |
| Шторы-плиссе Blackout                                 | 4 900  | 5  | 24500   |
| Усиленные звукоизолирующие двери «Ultimatum Next ПВХ» | 83 619 | 3  | 250 857 |
| Итого   |        |    | 927457  |

В трех помещениях установлены усиленные звукоизолирующие двери, как показано на рисунке №4. На каждом окне установлены шторы. Системы «Соната СА-4Б1» и «Соната СВ-4Б» размещены в соответствии с указаниями производителя. «ЛГШ-221» и «ЛГШ-503» находятся рядом с «Соната-ИП4.3» и подключены к ней. Все выключатели установлены в соответствии с рекомендациями производителя. В таблице №15 приведены описание обозначений устройств.

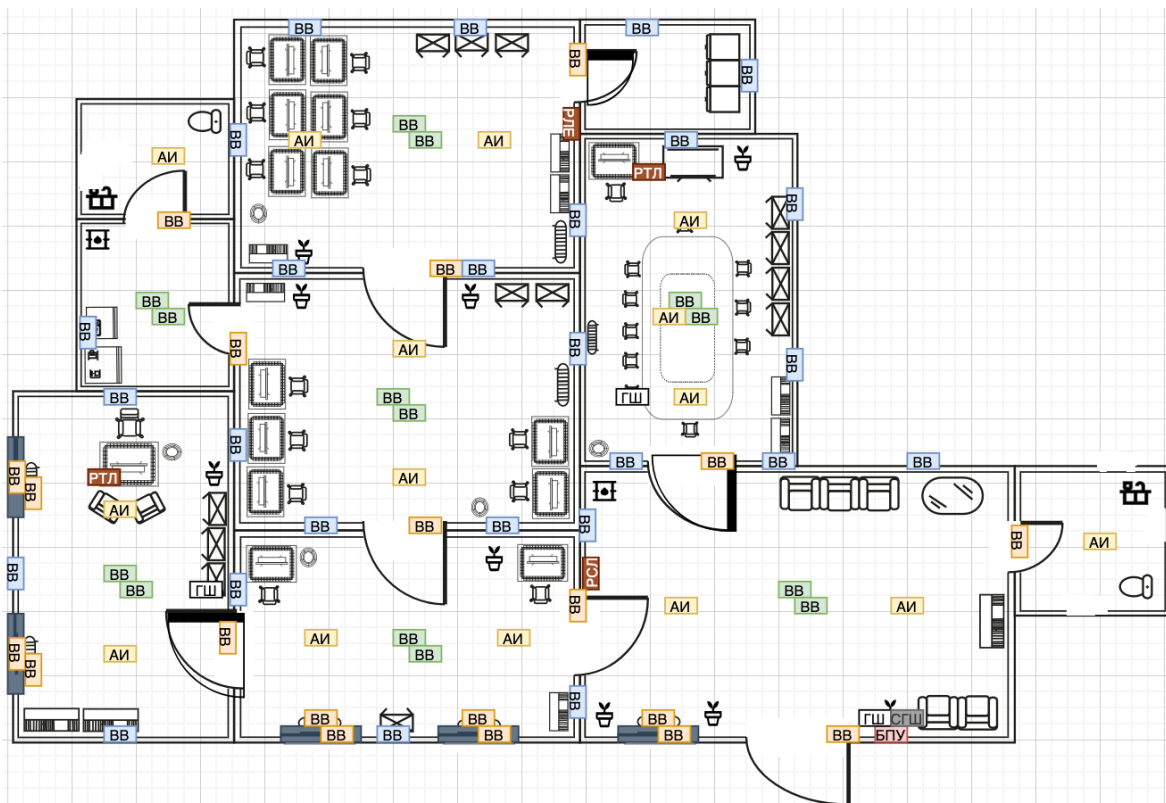
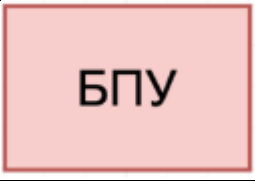
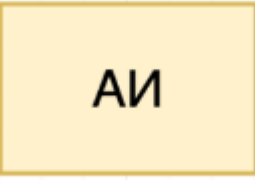
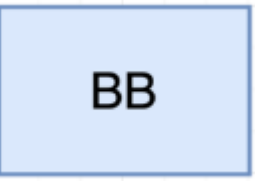

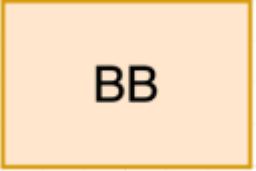


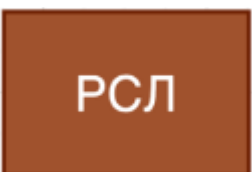
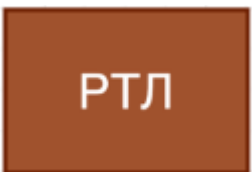
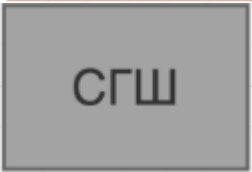

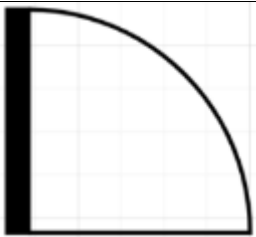



Рисунок №4. Схема расстановки устройств

Таблица №16. Необходимое оборудование

| Обозначение   | Устройство   | Количество,<br>шт. |
|---|--|--------------------|
|  | Блок электропитания и управления<br>«Соната-ИП4.3»             | 1                  |
|  | Генератор-акустоизлучатель<br>«Соната СА-4Б1»                  | 15                 |
|  | Генератор-вибровозбудитель<br>«Соната СВ-4Б» (стены)           | 24                 |
|  | Генератор-вибровозбудитель<br>«Соната СВ-4Б» (потолок,<br>пол) | 14                 |



|   |  |    |
|---|--|----|
|    | Генератор-вибровозбудитель<br>«Соната СВ-4Б» (окна,<br>двери, батареи) | 20 |
|    | Генератор-вибровозбудитель<br>«Соната СВ-4Б»<br>(трубопровод)          | 0  |
|    | Размыкатель линии<br>«Ethernet»<br>«Соната-ВК4.3»                      | 1  |
|    | Размыкатель слаботочной<br>линии<br>«Соната-ВК4.2»                     | 1  |
|   | Размыкатель телефонной<br>линии<br>«Соната-ВК4.1»                      | 2  |
|  | Сетевой генератор шума<br>«Покров»                                     | 1  |
|  | Генератор шума<br>«ЛГШ-503»  | 1  |
|  | Усиленные<br>звукоизолирующие двери<br>«Ultimatum Next ПВХ»            | 3  |
|  | Шторы-плиссе<br>BlackOut   | 5  |

## **ЗАКЛЮЧЕНИЕ**

В ходе выполнения курсовой работы был проведен анализ потенциальных каналов утечки информации в защищаемом помещении и разобраны необходимые меры их защиты. Были выбраны подходящие для защищаемого объекта средства защиты путем анализа существующих на рынке технических средств противодействия рассматриваемым каналам утечки информации. Также был разработан план установки средств защиты и подсчитана смета расходов.

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

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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.
2. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий
3. Молодой ученый. — 2016 — No 3 (107). — С. 69-72. — URL: <https://moluch.ru/archive/107/25842>
4. Мещеряков Р. В., Шелупанов А. А., Зайцев А. П. Технические средства и методы защиты информации. – 2007. - 507 с
5. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с.

## СПИСОК ЛИТЕРАТУРЫ

1. КАРМАНОВСКИЙ Н.С., МИХАЙЛИЧЕНКО О.В., САВКОВ С.В. ОРГАНИЗАЦИОННО-ПРАВОВОЕ И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. УЧЕБНОЕ ПОСОБИЕ - САНКТ-ПЕТЕРБУРГ: НИУ ИТМО, 2013. - 151 с. – экз.
2. КАТОРИН Ю. Ф., РАЗУМОВСКИЙ А. В., СПИВАК А. И. ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ. УЧЕБНОЕ ПОСОБИЕ - САНКТ-ПЕТЕРБУРГ: НИУ ИТМО, 2012. - 416 с. - экз.
3. ХОРЕВ А. А. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ: учеб. пособие для СТУДЕНТОВ ВУЗОВ. В 3-х т. Т. 1. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ. М.: НПЦ «АНАЛИТИКА», 2010.- 436
4. СПЕЦИАЛИЗИРОВАННЫЙ ХОЛДИНГ. ЛАБОРАТОРИЯ ППШ. URL: [HTTP://WWW.PPS.RU/](http://www.pps.ru/) (ДАТА ОБРАЩЕНИЯ: 20.12.2023)