**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:**

**«*Разработка комплекса инженерно-технической защиты информации в помещении*»**

**Выполнила:**

студентка группы N34471

Слесарева Анастасия Викторовна

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Проверил преподаватель:**

Попов Илья Юрьевич \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Отметка о выполнении:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Санкт-Петербург 2023 г.

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Студент** | Слесарева Анастасия Викторовна | | | | | |  |
|  |  |  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Безопасности Информационных Технологий | | | | | |
| **Группа** | N34471 | | |  |  |  |  |
| **Направление (специальность)** | | | | | | 10.03.01. - Технологии защиты информации | |
| **Руководитель** | | Попов Илья Юрьевич, к.т.н., доцент ФБИТ | | | | | |
| (Фамилия И.О., должность, ученое звание, степень) | | | | | | | |
| **Дисциплина** | | Инженерно-технические средства защиты информации | | | | | |
| **Наименование темы** | | | | Разработка комплекса инженерно-технической защиты информации в помещении | | | |
| **Задание** | Разработка комплекса инженерно-технической защиты информации в помещении | | | | | | |
|  | | | | | | | |
| **Краткие методические указания** | | | | | | | |
| Курсовая работа выполняется в рамках изучения дисциплины «Инженерно-технические средства | | | | | | | |
| защиты информации». Объект исследований курсовой работы ограничивается заданным помещением. | | | | | | | |
|  | | | | | | | |
|  | | | | | | | |
| **Содержание пояснительной записки** | | | | | | |  |
| 1. Введение.  2. Анализ технических каналов утечки информации.  3. Руководящие документы  4. Анализ защищаемых помещений  5. Анализ рынка технических средств  6. Описание расстановки технических средств  7. Заключение  8. Список литературы | | | | | | | |
| **Рекомендуемая литература** | | | | | | | |
| Руководитель | | Попов Илья Юрьевич | | | | | |
|  |  |  |  |  |  |  | (Подпись, дата) |
| Студент | Слесарева Анастасия Викторовна | | | | | |  |
|  |  |  |  |  |  |  | (Подпись, дата) |

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Студент** | Слесарева Анастасия Викторовна | | | | |
|  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Безопасности Информационных Технологий | | | |
| **Группа** | N34471 | | |  |  |
| **Направление (специальность)** | | | | | 10.03.01. - Технологии защиты информации |
| **Руководитель** | | Попов Илья Юрьевич, к.т.н., доцент ФБИТ | | | |
| (Фамилия И.О., должность, ученое звание, степень) | | | | | |
| **Дисциплина** | | Инженерно-технические средства защиты информации | | | |
| **Наименование темы** | | | | Разработка комплекса инженерно-технической защиты информации в помещении | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п/п** | **Наименование этапа** | **Дата завершения** | | **Оценка и подпись**  **руководителя** |
| **Планируемая** | **Фактическая** |
| 1 | Анализ теоретической составляющей | 18.10.2022 | 18.10.2022 |  |
| 2 | Создание плана КР | 18.10.2022 | 18.10.2022 |  |
| 3 | Составление основного текста КР | 18.10.2022 | 18.10.2022 |  |
| 4 | Представление выполненной курсовой работы | 29.12.2022 | 19.12.2022 |  |

|  |  |  |
| --- | --- | --- |
| Руководитель | | Попов Илья Юрьевич |
|  |  | (Подпись, дата) |
| Студент | Слесарева Анастасия Викторовна | |
|  |  | (Подпись, дата) |

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Студент** | Слесарева Анастасия Викторовна | | | | |
|  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Безопасности Информационных Технологий | | | |
| **Группа** | N34471 | | |  |  |
| **Направление (специальность)** | | | | | 10.03.01. - Технологии защиты информации |
| **Руководитель** | | Попов Илья Юрьевич, к.т.н., доцент ФБИТ | | | |
| (Фамилия И.О., должность, ученое звание, степень) | | | | | |
| **Дисциплина** | | Инженерно-технические средства защиты информации | | | |
| **Наименование темы** | | | | Разработка комплекса инженерно-технической защиты информации в помещении | |

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

1. **Цель и задачи работы**

Предложены студентом Сформулированы при участии студента

Определены руководителем

Цель данной работы – повышение защищенности рассматриваемого помещения. Задачами является

анализ защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и

активной защиты информации.



1. **Характер работы**

Расчет

Моделирование

Конструирование Другое

1. **Содержание работы**

1. **Выводы**

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

|  |  |  |
| --- | --- | --- |
| Руководитель | | Попов Илья Юрьевич |
|  |  | (Подпись, дата) |
| Студент | Слесарева Анастасия Викторовна | |
|  |  | (Подпись, дата) |

« » 2022г.

# ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 7](#_Toc1)

[3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ 14](#_Toc2)

[**3.1 Описание помещений** 19](#_Toc3)

[3.2 Анализ возможных утечек информации 20](#_Toc4)

[3.3 Выбор средств защиты информации 20](#_Toc5)

[4. АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ 23](#_Toc6)

[**4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации**  23](#_Toc7)

[**4.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации**  26](#_Toc8)

[**4.3 Защита от ПЭМИН**  29](#_Toc9)

[**4.4 Защита от утечек по оптическому каналу** 29](#_Toc10)

[ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ 30](#_Toc11)

[ВЫВОДЫ 33](#_Toc12)

ВВЕДЕНИЕ

Деятельность любого современного предприятия основана на обладании и управлении информацией. В связи с этим защита информации становится предметом пристального внимания, так как повсеместно внедряемые технологии и компоненты без соответствующих предосторожностей быстро становятся источниками проблем.

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. Разработка эффективного комплекса мер для выполнения данной задачи является одной из наиболее актуальных современных проблем. Технические средства защиты информации являются важной частью комплекса мер по обеспечению режима конфиденциальности на предприятии.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно» на объекте информатизации. Защищаемый объект состоит из семи помещений и представляет собой научную биолабораторию с архивом, двумя кабинетами бухгалтера, двумя кабинетами для ученых, комнатой отдыха, холлом и санузлом.

Данная работа состоит из пяти глав. В первой главе произведен анализ технических каналов утечки информации. Во второй приведён перечень управляющих документов, в третьей – анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств. Четвертая глава представляет собой анализ рынка 7 технических средств защиты информации разных категорий, и пятая глава посвящена разработке схем расстановки выбранных технических средств в защищаемом помещении

# АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕКИ ИНФОРМАЦИИ

Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена. Утечка информации может осуществляться по различным каналам. Каналом утечки информации называют канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.

Существует три формы утечки информации:

* разглашение информации;
* несанкционированный доступ к информации;
* утечка информации по техническим каналам

Согласно теме данной работы, рассматриваться будет только утечка информации по техническим каналам.

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

Утечка - бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Утечка (информации) по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Источниками сигнала могут быть:

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

Далее полученная информация преобразуется в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. Среда распространения сигнала - физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Она характеризуется набором физических параметров, определяющих условия перемещения сигнала. Приемник после этого снимает информацию с носителя, обрабатывает полученный сигнал (усиление) и преобразует информацию в форму сигнала, доступную получателю (человеку или техническому устройству).

По физической природе носителя и виду канала связи ТКУИ делятся на:

* оптические;
* радиоэлектронные;
* электрические;
* электромагнитные;
* индукционные;
* акустические;
* акустоэлектрические;
* виброакустические;
* материально-вещественные.

Носителем информации в оптическом канале является электромагнитное поле (фотоны). Снятие информации возможно с помощью наблюдения, например, через подсматривание в окно или приоткрытую дверь. Альтернативой является использование закладного устройства с возможностью фото или видеозаписи. Данный канал утечки актуален для графической формы представления информации, защита осуществляется методом установки жалюзи или другой формой непрозрачного покрытия на все просматриваемые снаружи поверхности (окна, стеклянные двери и т. д.), а также использованием доводчиков для дверей.

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

Электромагнитный ТКУИ связан с перехватом электромагнитных излучений на частотах работы передатчиков систем и средств связи. Используется для перехвата информации, передаваемой по каналам радио-, радиорелейной, спутниковой связи. Напряженность электрического поля в точке приема (перехвата) будет прямо пропорциональна величине мощности передатчика, высоте приемной и передающей антенн и обратно пропорциональна расстоянию. Данный канал утечки актуален при наличии в помещении электронной вычислительной техники, компьютеров или других средств обработки информации. Создаваемое при работе технических устройств электромагнитное излучение называют побочным электромагнитным излучением и наводками (ПЭМИН); защита осуществляется посредством специальных технических устройств, создающих электромагнитный шум, скрывающий это электромагнитное излучение.

Электрический ТКУИ связан со съемом информации путем контактного подключения аппаратуры злоумышленника к кабельным линиям связи. Электрические колебания, появляющиеся при работе электрических приборов, содержат информацию о подключенных устройствах. Защита осуществляется посредством специальных фильтров для сетей электропитания, которые скрывают электрические колебания, вызываемые вычислительной техникой.

Индукционный ТКУИ связан с бесконтактным съемом информации с кабельных линий связи. Возможность такого съема информации возникает за счет эффекта возникновения вокруг кабеля связи электромагнитного поля, модулированного информационным сигналом. Это поле перехватывается специальным индукционным датчиком, далее усиливается и демодулируется на аппаратуре злоумышленника. Следует отметить, что бесконтактные закладные устройства обнаружить труднее всего, так как они не изменяют характеристик канала связи. Защита осуществляется посредством использования специальных программных и аппаратных средств, позволяющих выявить закладки.

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Снятие информации возможно либо с помощью подслушивания из-за пределов помещения (при отсутствии звукоизоляции), либо с помощью закладных устройств с функциями аудиозаписи. Данный канал утечки актуален при передаче информации в звуковой форме (диалог, совещание, др.); защита осуществляется посредством использования звукоизолирующих материалов, мешающих звуку выйти за пределы помещения, а также использованием специальных программных и аппаратных средств, позволяющих выявить закладки.

В акустоэлектрическом канале информация представлена в виде акустических колебаний, которые далее воздействую на сети электропитания, вызывая электрические колебания. При снятии этих колебаний есть возможность восстановить исходный акустический сигнал. Данный канал утечки информации актуален, когда в контролируемом помещение есть электрические сети, связанные с внешней территорией. Например, телефонная сеть – подав небольшое напряжение на входящую телефонную линию и сняв его на входе, мы сможем получить распространяющуюся в помещение звуковую информацию. Защита осуществляется посредством использования специальных фильтры для сетей электропитания, скрывающих колебания, вызванные воздействием на электрические сети.

В виброакустическом канале информация изначально представлена в виде акустических колебаний, которые воздействуют на некоторую твердую поверхность, превращаясь в вибрационные колебания. Данный канал утечки информации актуален практически всегда, так как связан с наличием твёрдых поверхностей в контролируемом помещении, в т. ч. стен, потолка и пола, батарей отопления, оконных стёкол. Защита осуществляется путём использования специальных технические устройства, которые передают на защищаемую твердую поверхность белый шум, который скрывает вибрационные колебания, вызванные акустическими волнами.

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных носителей с защищаемой информацией. В качестве вещественных носителей чаще всего выступают черновики документов и использованная копировальная бумага, портативные носители информации (HHD, SSD, проч. карты памяти). С кражей или копированием 12 информации, зафиксированной на материальных носителях, борются в первую очередь организационными мерами, вводя строгий порядок учета и работы с данными видами носителей.

Помимо вышеперечисленного, также выделяют оптико-электронные ТКУИ, связанные с перехватом акустических сигналов путём лазерного зондирования оконных стекол.

Отдельной угрозой является возможность проникновения злоумышленника на территорию охраняемого помещения, так что не менее актуальным вопросом является рассмотрение контроля доступа на охраняемую территорию.

# 2 РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Основными документами в области защиты информации являются:

* Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
* Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».
* Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
* Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».
* Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне».
* Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации».
* Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
* Постановление Правительства 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".

Также на сайте ФСТЭК существует отдельный раздел, содержащий специальные нормативно-технические документы ФСТЭК России – нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации:

* СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам.
* СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации.
* Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров.
* Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации.
* Временный порядок аттестации объектов информатизации по требованиям безопасности информации.
* Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения.
* Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
* Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
* Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.
* Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.
* Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования.
* Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.
* Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

На рисунке 1 представлен план защищаемого помещения. А в таблице 1 указаны все предметы, которые присутствуют в помещении.

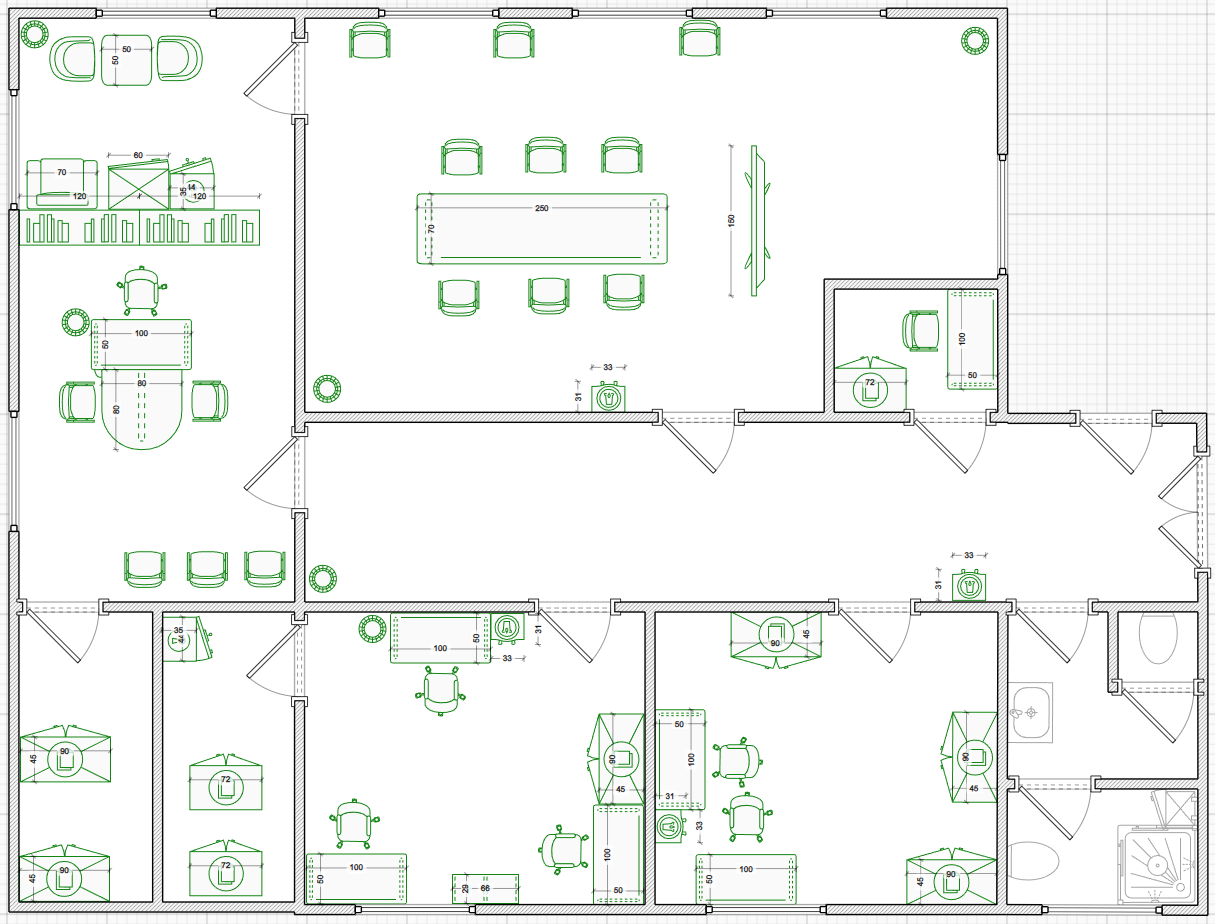


Рисунок 1 – План защищаемого помещения

Таблица 1

|  |  |
| --- | --- |
| Обозначения | Описание |
|  | Проектор |
|  | Стулья |
|  | Рабочий стол |
|  | Комнатное растение |
|  | Диван |
|  | Туалет |
|  | Сейф |
|  | Книжный шкаф |
|  | Шкаф |
|  | Кулер |
|  | Раковина |
|  | Душевая |
|  | Серверный шкаф |
|  | Шкаф для бумаг |

Схема информационных потоков представлена на Рисунке 2.

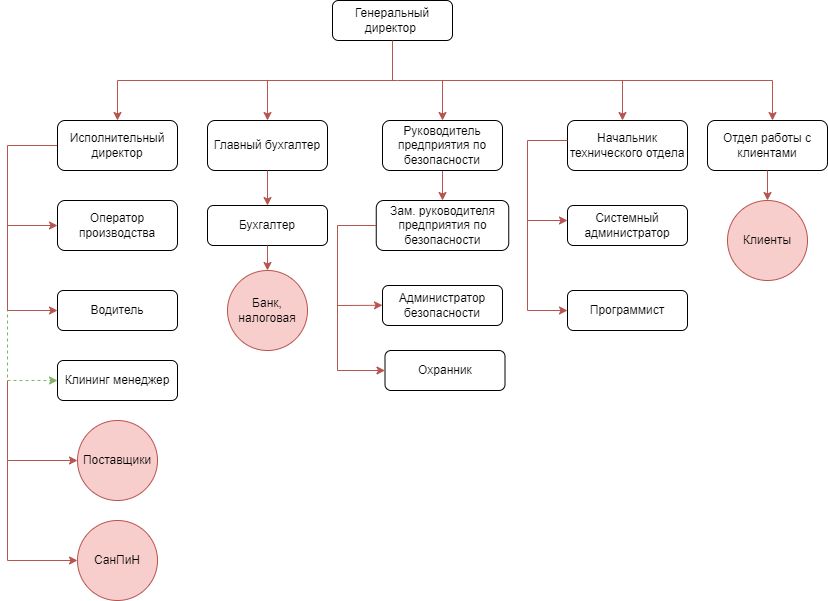


Рисунок 2 – Информационные потоки Организации

**Описание информационных потоков**

Открытые потоки:

1. Исполнительный директор – менеджер (вопросы, связанные с организацией)

Закрытые потоки:

1. Ген.директор – Исполнительный директор (вопросы, связанные с подбором персонала, организацией работы)
2. Ген.директор – Главный бухгалтер (вопросы, связанные с налоговыми отчислениями, организацией закупок и другими финансовыми вопросами)
3. Ген.директор – Руководитель предприятия по безопасности (Вопросы по обеспечению ИБ)
4. Ген.директор – Начальник технического отдела (Технические вопросы, поддержка сайта, работоспособность техники)
5. Ген.директор – Отдел работы с клиентами (Вопросы по ценообразованию, работе с клиентами)
6. Исполнительный директор – Оператор производства (Вопросы технологии и сроков производства)
7. Исполнительный директор – Водитель (Вопросы доставки товара до Клиентов)
8. Исполнительный директор – Поставщики (Вопросы поставки сырья)
9. Исполнительный директор – СанПиН
10. Главный бухгалтер – Бухгалтер (вопросы, связанные с налоговыми отчислениями,
11. организацией закупок и другими финансовыми вопросами)
12. Главный бухгалтер – Банк, налоговая (Отчетность)
13. Руководитель предприятия по безопасности – Зам. руководителя предприятия по безопасности (Распределение ролей, отчетность)
14. Зам. руководителя предприятия по безопасности – Администратор безопасности (Вопросы обеспечения информационной безопасности предприятия)
15. Зам. руководителя предприятия по безопасности – Охранник (Организация физической защиты территории)
16. Начальник технического отдела –  Системный администратор (Организация настройки и поддержки сети компании)
17. Начальник технического отдела – Программист (Технические вопросы, поддержка сайта)
18. Отдел работы с клиентами – Клиенты (персональные данные клиентов, договоры и обслуживание клиентов)

Информация ограниченного доступа:

1. Персональные данные сотрудников –представлены в электронной форме, владельцем является руководитель отдела.
2. Персональные данные клиентов - представлены в электронной форме, владельцем является сотрудники отдела технической поддержки с необходимым уровнем доступа, отдел работы с клиентами
3. Техническая информация (логины, пароли, данной локальной сети и т. д.) - представлены в электронной форме, владельцем являются сотрудники отдела технической поддержки с необходимым уровнем доступа.
4. Коммерческая тайна (данные о производстве) – представлен в электронной форме, владельцем является Организации.
5. Государственная тайна (уровень секретно) – разработки лаборатории: достижения науки, научно-исследовательские, о проектные работы, имеющие важное оборонное или экономическое значение, влияющих на безопасность государства.

**3.1 Описание помещений**

Защите подлежат следующие помещения:

* архив 3.88м2
* Серверная 3.82м2
* Кабинет руководителя 16.1м2
* Переговорная 25м2
* Кабинет 1 9.96м2
* Кабинет 2 10.02м2
* Охранная комната 2м2
* Уборная 1 3.02м2
* Уборная 2 2.21м2
* Холл 16м2

В комнате архива нет окон. В нем находится два серверных секретера.

В серверной так же нет окон. В ней находится два серверных шкафа и сейф с документами IT-отдела.

В кабинете руководителя три окна. Площадь разделена на две части: рабочую и отдыха. В рабочей зоне находится стол руководителя, шесть стульев, два книжных шкафа и цветок. В зоне отдыха складной цветок, диван, два шкафа общего пользования, стол и два стула.

В первом кабинете 3 рабочие зоны с столом и креслом, а так же два шкафа для документов, кулер и цветок.

Во втором кабинете 2 рабочие зоны с столом и креслом, и 3 шкафа для документов, а так же кулер.

В переговорной установлен большой монитор для проекции информации, стол, 9 стульев, 2 цветка и кулер для воды.

В комнате охраны расположен стол с монитором для просмотра камер, а так же шкаф для документов.

В Уборной 1 раковина и унитаз, в уборной 2 унитаз, душевая и подвесной шкафчик.

Защищаемое помещение расположено на первом этаже 5-этажного здания. Здание является жилым домом с первым этажом, выделенным под коммерческие организации:

* Сверху расположены жилые помещения.
* Снизу расположен помещение с трубопроводом (подвал).
* Со стороны нижней стены расположен магазин “Улыбка радуги”.
* Со стороны верхней стены расположен выход на улицу.
* Со стороны левой стены выход на улицы с интенсивным пешеходным и транспортным движением.
* Со стороны правой стены расположен общий подъезд.

Окна помещения оборудованы шторами и решетками, смотрят на проезжую часть и жилой дом, расположенный на расстоянии 50 метров.

Стены здания и внутренние перегородки железобетонные, толщиной не менее 15 см.

3.2 Анализ возможных утечек информации

Просмотр помещения со стороны улицы ввиду того, что помещение находится на 1 этаже возможен. А также возможен просмотр помещения извне, со стороны жилого дома с помощью оптических приборов, существует потенциальный канал утечки видовой информации.

Так как возможно прослушивание помещения, со стороны улицы и жилого дома, через открытые окна и форточки с помощью направленных микрофонов, существует потенциальный канал утечки акустический информации.

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

В помещениях присутствуют декоративные элементы и растения, где можно спрятать закладное устройство.

В каждом помещении имеются розетки, а значит, актуальны электрического и электромагнитного каналов утечки информации.

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

3.3 Выбор средств защиты информации

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

Таблица 1 – Активная и пассивная защита

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

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

1. скрытное размещение поста перехвата (для прослушивания и просмотра помещения) на улице с умеренным движением возможно, т. к. подозрительные лица, транспортные средства и т. п. не будут привлекать к себе много внимания;
2. скрытное размещение поста перехвата (для прослушивания и просмотра помещения, установки лазерного микрофона) в жилом здании, если, например, арендовать квартиру с окнами, расположенными напротив окон защищаемого помещения, вполне реализуемо.

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

4. АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «секретно». Согласно требованиям «Типовых норм и правил проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденных Решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199, защита рассматриваемых помещений должна удовлетворять следующим критериям:

1. В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри — звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 см. Дверь устанавливается на металлический каркас.
2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.
3. По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене.
4. Все режимные помещения оборудуются аварийным освещением.
5. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.
6. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

**4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации**

Пассивная защита представляет собой:

* усиленные двери,
* тамбурное помещение перед переговорной,
* дополнительная отделка переговорной звукоизолирующими материалами.

Активная защита представляет собой систему виброакустического зашумления. Для защиты помещения для работы с государственной тайной уровня «совершенно секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1Б. Ниже в таблице 2 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому каналу.

Таблица 4 – Сравнительный анализ средств активной защиты от утечки

виброакустическому каналу

|  |  |  |  |
| --- | --- | --- | --- |
| Модель | Диапазон  воспроизводимого  шумового сигнала | Состав | Цена |
| [Бекар](http://deep-electronics.ru/catalog/tekhnicheskie-sredstva-zashchity-informatsii/zashchita-informatsii-ot-utechki-po-tekhnicheskim-kanalam/po-vibroakusticheskomu-kanalu/bekar/) | 175–11200 Гц | Конструктивно СВАЗ «Бекар» состоит из блока питания «Бекар»-БП, блока контроля целостности «Бекар»-БКЦ и акустических «Бекар»-А и вибрационных «Бекар»-В излучателей. Для настройки и отладки системы акустической и вибрационной защиты при её установке используется программатор параметров «Бекар»-ПР. | 46000 руб. |
| КАМЕРТОН-5 | 90–11200 Гц | Блок управления и контроля системой; Блок генерации и генератор маскирующих шумов, создающий помехи в речевом диапазоне частот; Виброизлучатели разных типов, блокирующие вибрационные каналы утечки информации (стены, перекрытия, оконные рамы, прочие элементы строительной конструкции); Акустоизлучатели разных типов, создающие помехи в акустических каналах утечки данных (вентиляционная система, дверные проемы, трубы инженерных коммуникаций, пр.); Размыкатели проводных линий, перекрывающие утечку акустических сигналов по проводам телефонной связи, локальной компьютерной сети, пр.; Виброшторы, создающие надежную помеху для прослушки разговоров с помощью направленного микрофона через оконное стекло. | 46000 руб. |
| Соната «АВ» модель 4Б | 175–11200 Гц | Блок электропитания и управления, генератор-акустоизлучатель, генератор-вибровозбудитель, размыкатель телефонной линии, размыкатель слаботочной линии, размыкатель линии Ethernet, пульт управления, блок сопряжения с внешними устройствами, техническое средство защиты речевой информации от утечки по оптико-электронному (лазерному) каналу, генераторный блок "АВ-4Л", вибровозбудитель "СП-4Л". | 26400 руб. |
| SEL SP-157 «Шагрень» | 90–11200 Гц | Центральный генераторный блок помех SEL SP-157G, вибрационный преобразователь SEL SP-157VP , акустический излучатель SEL SP-157AS, вибрационный преобразователь повышенной мощности SEL SP-157VPS, акустический излучатель повышенной мощности SEL SP-157ASP. | 31200 руб. |

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

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

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

Благодаря этому построению проявляется высокая стойкость защиты информации.

Улучшенная аппаратная настройка элементов модели 4Б позволяет связывать источник электропитания с другими для обмена информацией. Это дает возможность:

* Создать систему автоматического контроля всех элементов
* Снизить время на конфигурирование и тестирование системы
* Изменить настройки генераторов и построить гибкую систему виброакустической защиты
* Уменьшить затраты благодаря использованию единой линии связи и электропитания

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

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

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

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

|  |  |  |  |
| --- | --- | --- | --- |
| Модель | Характеристики | Описание | Цена |
| ГНОМ-  3М-60В | Диапазон частот 150кГц-1800мГц | Гном-3М-60В используется с внешними антеннами. В данном приборе предусмотрено 4 не связанных между собой выхода для подключения к антеннам и цепи электропитания. Для 100-процентной защиты информации от утечки следует использовать 3 рамочные антенны, расположив их в 3 перпендикулярных друг другу плоскостях. | 61824 руб. |
| Соната РС2 | Диапазон частот до 2 ГГЦ | Особенности конструкции устройств позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники (СВТ). Также предусмотрена возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus).  Изделия рассчитаны на подключение к 3-проводной сети энергоснабжения ("Фаза", "Ноль" и "Защитное заземление") и обеспечивают формирование несинфазных токов и синфазных и парафазных составляющих шумового напряжения во всех проводниках. | 23600 руб. |
| ЛГШ-513 | Диапазон частот –  0,01–1800 МГц | Генератор шума ЛГШ-513 оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа).  Генератор шума ЛГШ-513 имеет встроенный счетчик учета времени наработки, учитывающий и отображающий в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех. Конструкция генератор ЛГШ-513 обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.  Генератор шума ЛГШ-513 имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина». | 39000 руб. |
| ЛГШ-503 | Диапазон частот –  10 кГц – 1,8 ГГц | Изделие «ЛГШ-503» оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех.  Конструкция Изделия «ЛГШ-503» обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.  Изделие «ЛГШ-503» имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина». | 44200 руб. |

В результате проведенного анализа средств защиты от утечки виброакустическому каналу была выбрана Соната РС2 из-за низкой стоимости и удовлетворении необходимым критериям.

Особенности конструкции устройств позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники. Также предусмотрена возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus).

**4.3 Защита от ПЭМИН**

Для реализации активной защиты от ПЭМИН было также выбрано устройство Соната РС2.

**4.4 Защита от утечек по оптическому каналу**

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

ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

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

* Усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей прокладкой на металлическом каркасе – 5 шт.;
* Соната «АВ» модель 4Б;
* Соната РС2
* Жалюзи на 4 окна.

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

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

− стены: один на каждые 3–5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;

− потолок, пол: один на каждые 15–25 м2 перекрытия;

− один на окно (при установке на оконный переплет);

− один на дверь (при установке на верхнюю перекладину дверной коробки);

− трубы систем водо-, тепло- и газоснабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

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

− один на каждый вентиляционный канал или дверной тамбур;

− один на каждые 8–12 м3 надпотолочного пространства или других пустот.

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

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

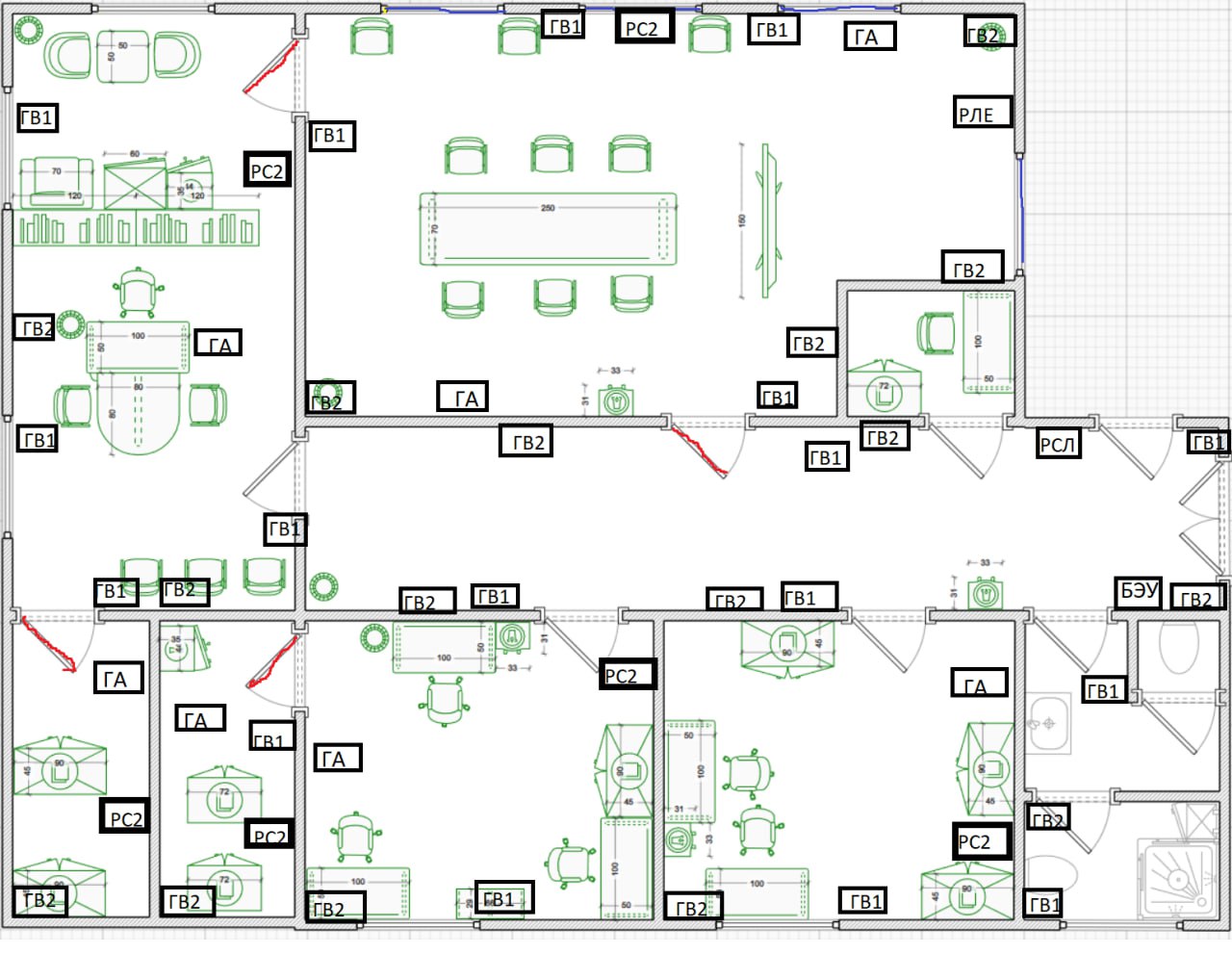


Рисунок 3 – Схема расстановки устройств

Таблица 4 – Технические средства

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Условное обозначение | Цена, руб. | Количество, шт. | Стоимость, руб. |
| Блок электропитания и управления «Соната-ИП4.3» | БЭУ | 21600 | 1 | 21600 |
| «Соната-СА-4Б1» генератор-акустоизлучатель | ГА1 | 7440 | 4 | 29760 |
| «Соната-СВ-4Б» генератор-вибровозбудитель (двери, окна) | ГА2 | 7400 | 8 | 59200 |
| «Соната-СВ-4Б» генератор-вибровозбудитель (стены) | ГВ1 | 7680 | 17 | 130560 |
| «Соната-СВ-4Б» генератор-вибровозбудитель (пол, потолок) | ГВ2 | 6000 | 5 | 30000 |
| Усиленные металлические двери Медверь |  | 6000 | 4 | 24000 |
| Жалюзи WINKER |  | 33120 | 3 | 99360 |
| Размыкатель линии Ethernet "Соната-ВК4.3" | РЛЕ | 3256 | 1 | 3256 |
| Размыкатель слаботочной линии "Соната-ВК4.2" | РСЛ | 12000 | 1 | 12000 |
| Устройства для защиты линий электропитания, заземления от утечки информации "Соната-РС1" | РС2 | 23600 | 5 | 118000 |
| ИТОГО |  |  |  | 670296 |

ВЫВОДЫ

В ходе данной работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении и описаны необходимые меры их защиты. Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для нашего объекта. Был разработан план установки и произведен расчет сметы затрат.

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

1. ПРИКАЗ ЦБ РФ ОТ 03.03.97 N 02–144 «О ВВЕДЕНИИ В ДЕЙСТВИЕ ВРЕМЕННЫХ ТРЕБОВАНИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ТЕХНОЛОГИЙ ОБРАБОТКИ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ ДОКУМЕНТОВ В СИСТЕМЕ ЦЕНТРАЛЬНОГО БАНКА РОССИЙСКОЙ ФЕДЕРАЦИИ»
2. **"**Руководящий документ "Защита от несанкционированного доступа к информации. Термины и определения".