

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

Факультет безопасности информационных технологий

Курсовая работа

По дисциплине:

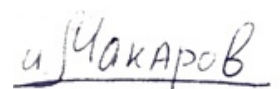
«Инженерно-технические средства защиты информации»

На тему:

«Проектирование системы защиты от утечки информации по различным каналам»

Выполнили:

Макаров Илья Евгеньевич, студент группы N34461



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**

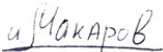
| | |
|-----------------------------|---|
| Студент | Макаров Илья Евгеньевич |
| | (Фамилия И.О.) |
| Факультет | Безопасности информационных технологий |
| Группа | N34461 |
| Направление (специальность) | 10.03.01. - Технологии защиты информации |
| Руководитель | Попов Илья Юрьевич, к.т.н., доцент 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 |
| Задание | Разработка системы инженерно-технической защиты информации в помещении |

Краткие методические указания

Содержание пояснительной записки

Пояснительная записка включает разделы – введение, анализ технических каналов утечки информации, перечень управляющих документов, анализ защищаемых помещений и технических средств защиты информации разных категорий, разработка схем расстановки выбранных технических средств в защищаемом помещении.

Рекомендуемая литература

| | |
|--------------|--|
| Руководитель | Попов Илья Юрьевич |
| | (Подпись, дата) |
| Студент | Макаров Илья Евгеньевич |
| |  (Подпись, дата) |

| | |
|-----------------------------|---|
| Студент | Макаров Илья Евгеньевич |
| | (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 |

| № п/п | Наименование этапа | Дата завершения | | Оценка и подпись руководителя |
|----------|---------------------------------|-----------------|-------------|----------------------------------|
| | | Планируемая | Фактическая | |
| 1 | Создание плана КР | 10.10.2023 | 01.11.2023 | |
| 2 | Анализ литературы | 28.11.2023 | 01.12.2023 | |
| 3 | Составление основного текста КР | 15.12.2023 | 22.12.2023 | |
| 4 | Защита курсовой работы | 19.12.2023 | 25.12.2023 | |

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Макаров Илья Евгеньевич и Макаров
(Подпись, дата)

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

| | |
|-----------------------------|---|
| Студент | Макаров Илья Евгеньевич |
| 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 данной работы – повышение уровня защиты информации от утечек.

**2. Характер
работы**


- ☐ Расчет ☐ Конструирование
☐ Моделирование ☒ Друго

1. Содержание работы

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

2. 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 | Макаров Илья Евгеньевич  |
| | (Подпись, дата) |

«25» декабря 2023 г

СОДЕРЖАНИЕ

| | |
|---|----|
| Введение | 6 |
| 1 Анализ технических каналов утечки информации..... | 7 |
| 2 Перечень руководящих документов | 11 |
| 3 Сведения об организации и анализ защищаемых помещений | 13 |
| 3.1 Сведения об организации..... | 13 |
| 3.2 Анализ защищаемых помещений..... | 14 |
| 3.3 Анализ возможных утечек информации | 14 |
| 3.4 Необходимые средства защиты информации | 15 |
| 4 Анализ рынка и выбор необходимых инженерно-технических средств защиты информации..... | 16 |
| 4.1 Устройства для перекрытия акустического и виброакустического канала утечки информации | 17 |
| 4.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации | 18 |
| 4.3 Защита от утечек по оптическому каналу | 21 |
| 5 Описание расстановки технических средств | 22 |
| Заключение..... | 26 |

ВВЕДЕНИЕ

Средства защиты информации обеспечивают защиту информации в информационных системах, позволяют предотвратить несанкционированный доступ злоумышленника к ресурсам и данным предприятия, тем самым снизив риск несанкционированных утечки, утраты, искажения, уничтожения, копирования и блокирования информации и нанесения экономического, репутационного или других видов ущерба предприятию.

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

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно» на объекте научно-технического центра (далее - НТЦ). Защищаемый объект состоит из 9 помещений и представляет собой кабинет главного конструктора, заместителя главного конструктора, переговорную, офисное помещение для сотрудников, обеденная зона и серверная.

По ходу работы произведен анализ технических каналов утечки информации, приведен перечень управляющих документов, анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств, анализ рынка технических средств защиты информации разных категорий и разработка схем расстановки выбранных технических средств в защищаемом помещении.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечка конфиденциальной информации — это неконтролируемое разглашение конфиденциальной информации за пределами организации или компании, которым доверено обслуживание или которые известны во время работы. Утечка может быть вследствие разглашения конфиденциальной информации, ухода по каналам связи, несанкционированного доступа к конфиденциальной информации различными методами.

В курсовой работе рассматриваться только утечку 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 информации по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

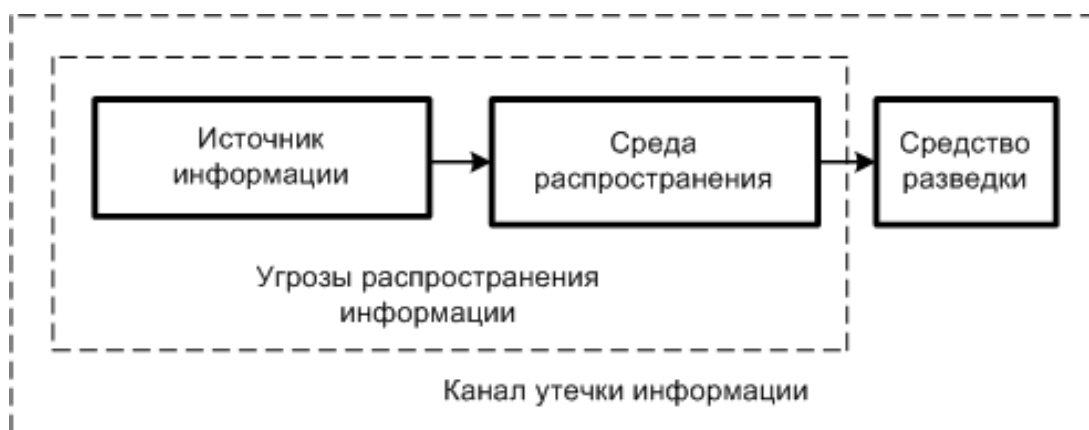


Рисунок 1 – Общая структурная схема канала утечки информации

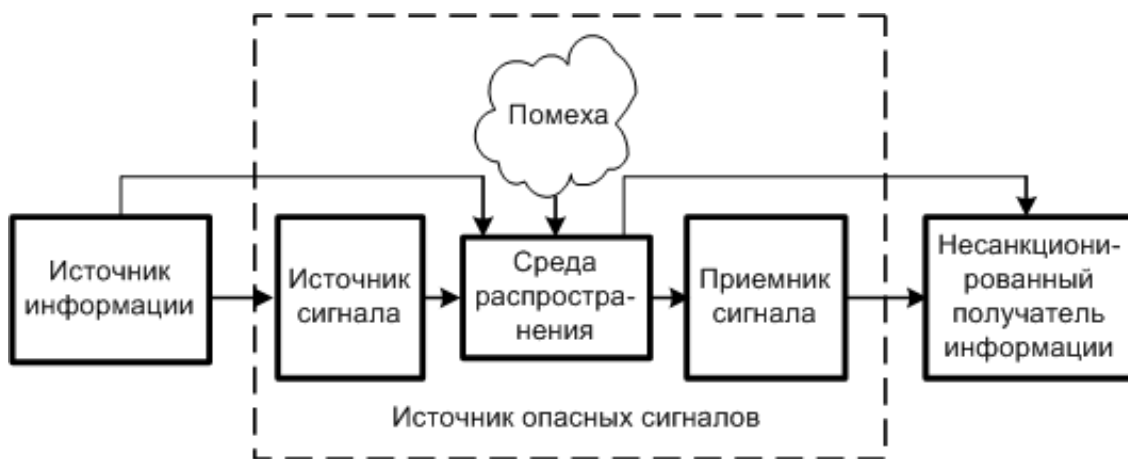


Рисунок 2 – Структура технического канала утечки информации

На вход ТКУИ поступает информация в виде первичного сигнала, представляющего собой носитель с информацией от её источника.

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.

Поскольку информация из источника передается на вход канала на исходном языке, передатчик преобразует полученную информацию в формат, который записывает ее на носитель, подходящий для среды распространения.

Среда распространения сигнала – это физическая среда, в которой информационные сигналы могут распространяться и записываться приемником. Он характеризуется набором физических параметров, которые определяют условия движения сигнала.

Основными параметрами, которые следует учитывать при описании среды распространения, являются:

- физические препятствия для субъектов и материальных тел;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;

- вид и мощность помех для сигнала.

Приемник после этого производит следующие действия:

- усиление принятого сигнала до значений, обеспечивающих съем информации;
- съем информации с носителя;
- преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

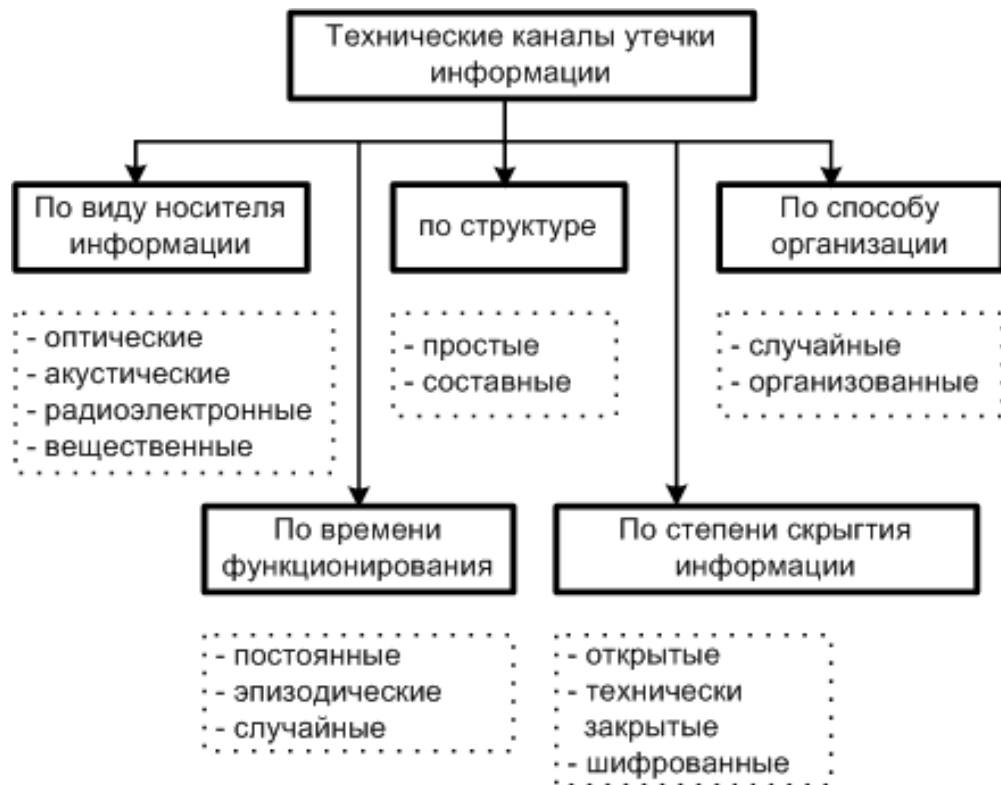


Рисунок 3 – Классификация технических каналов утечки информации

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** и **визуально-оптическом** канале является электромагнитное поле. Снятие информации возможно с помощью наблюдения через подсмотренное в окно или приоткрытую дверь. В качестве защиты от утечки информации следует снизить освещенность защищаемого объекта и его отражательные свойства, использовать различные пространственные ограждения (экраны, шторы, темные стекла), применять специальную маскировку и средства сокрытия защищаемых объектов (сетки, краски, укрытия).

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

В **электромагнитном** канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Способом защиты от утечки информации по электромагнитным каналам считается экранирование аппаратуры и ее элементов. Электростатическое, магнитостатическое и электромагнитное экранирование позволяет предохранить объект от воздействия и электромагнитных, и акустических сигналов. Таким образом, обеспечивает надежную защиту информации от утечки по ПЭМИН.

Материально-вещественные каналы также нуждаются в защите, так как различные материальные носители могут содержать в себе важнейшую секретную информацию. Для защиты материально-вещественных каналов от утечки информации разрабатывается целый комплекс организационных мер.

2 ПЕРЕЧЕНЬ 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 СВЕДЕНИЯ ОБ ОРГАНИЗАЦИИ И АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Сведения об организации

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей третий тип – уровень «секретно». Защищаемый объект состоит из девяти помещений и представляет собой офис организации с кабинетом директора НТЦ, заместителя главного конструктора, переговорной, столовой, бухгалтерией, офисным помещением для сотрудников.

Информационные потоки организации представлены на рисунке 2, красными стрелками обозначены закрытые потоки, в которых передается информация ограниченного доступа, а зелеными – открытые потоки. Закрытые потоки в схеме разделены на информацию конфиденциального характера – красная сплошная линия, информацию с грифом «секретно» - красная пунктирная линия.

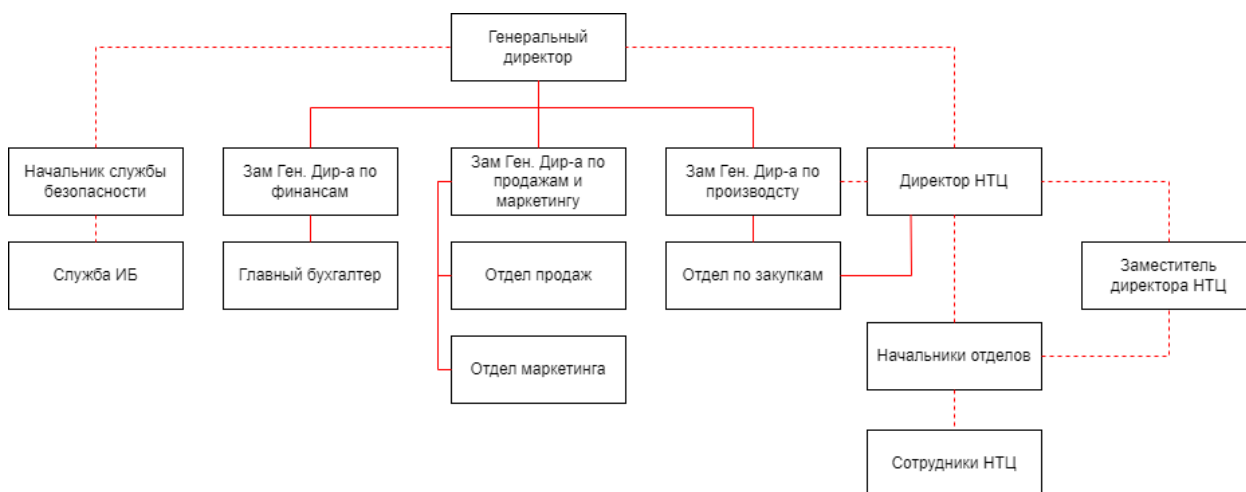


Рисунок 4 – Информационные потоки организации

Информация ограниченного доступа:

- персональные данные сотрудников;
- коммерческая тайна (данные о производстве);
- финансовые данные;
- техническая информация;
- информация о новых разработках/улучшениях;
- информация о закупках для нужд разработки.

3.2 Анализ защищаемых помещений

На рисунке 5 представлен план защищаемого помещения.

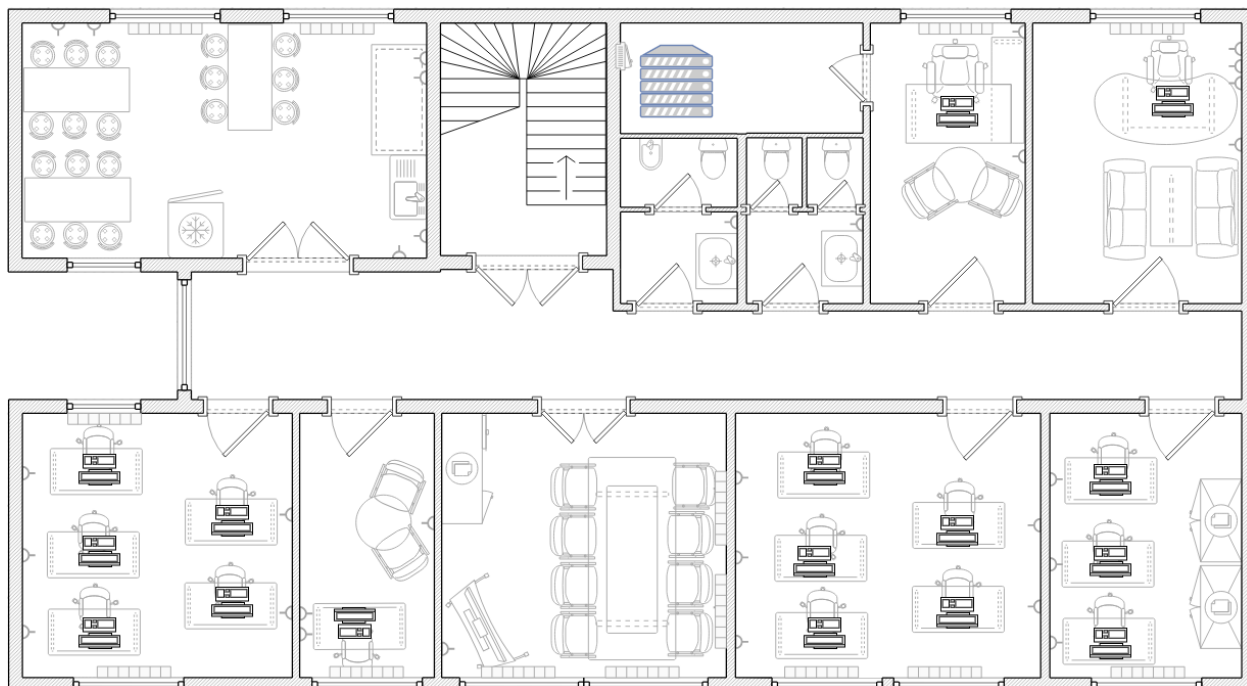


Рисунок 5 – План НТЦ

3.3 Анализ возможных утечек информации

Неправомерный доступ к конфиденциальной информации и информации, составляющей государственную тайну, может осуществляться злоумышленником путем прослушивания разговоров через окна, двери, стены, а также с помощью использования закладных устройств в декоративных элементах помещения. В помещениях есть электрические розетки и персональные компьютеры, которые могут быть использованы для перехвата передаваемой информации.

Таким образом, на объекте актуальны акустические, акустоэлектрические, виброакустические, визуально-оптические, электромагнитные и электрические каналы утечки информации. Материально-вещественный канал утечки информации регулируется организационно-правовыми методами организации.

3.4 Необходимые средства защиты информации

Согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещение средствами защиты, которые приведены в таблице 2.

Таблица 1 – Необходимые средства защиты информации

| Технические каналы утечки информации | Источники | Пассивные средства защиты | Активные средства защиты |
|--------------------------------------|--|--------------------------------------|--|
| Акустический, акустоэлектрический | Окна, двери, электрические провода, кабели | Звукоизоляция | Устройства акустического зашумления |
| Виброакустический | Твердые поверхности помещения | Звукоизоляция | Устройства виброакустического зашумления |
| Визуально-оптический | Окна, двери | Жалюзи на окнах, доводчики на дверях | Блокирующие устройства |
| Электрический, электромагнитный | ПК, электрические приборы, розетки | Сетевые фильтры | Устройства электромагнитного зашумления |

4 АНАЛИЗ РЫНКА И ВЫБОР НЕОБХОДИМЫХ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к режимным помещениям и их оборудованию содержатся в Решении Межведомственной комиссии по защите государственной тайны №199 от 21.01.2011г. "О типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".

Для уровня секретности "секретно" должны быть соблюдены следующие требования:

- в помещениях устанавливаются усиленные двери, обеспечивающие надежное закрытие и звукоизоляцию. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри;
- звукоизоляционный материал, сама дверь должна иметь толщину не менее 4,5 см.;
- по требованиям безопасности режимных помещений, если окна в комнатах и хранилищах 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;
- оборудование помещений, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений;
- обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании;
- все режимные помещения оборудуются аварийным освещением;
- перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации.

4.1 Устройства для перекрытия акустического и виброакустического канала утечки информации

Пассивная защита обеспечивается установкой усиленных дверей, обеспечивающих надежное закрытие и звукоизоляцию, отделкой переговорной комнаты и директорского кабинета, используя материалы со звукоизолирующими свойствами.

Активная защита обеспечивается устройствами виброакустического зашумления. Устройства должны быть сертифицированы для защиты выделенных помещений не ниже 3 категории, что соответствует обработке в помещениях информации, составляющей государственную тайну уровня «секретно».

Таблица 2 – Средства активной защиты информации акустического и виброакустического канала

| Наименование | Описание | Цена, руб. |
|--------------------------|---|------------|
| «Соната-АВ» модель 4Б | Диапазон частот: 90-11200 Гц Количество каналов: 1 Количество логических каналов: 239 Высокая стойкость защиты информации. Есть возможность подключения к одному питающему шлейфу, что делает легче процесс проектирования и монтажа. Индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы. Имеет сертификат соответствия ФСТЭК. | 44 200 |
| ЛГШ-404 | Диапазон частот: 175-11200 Гц Количество каналов: 2 Предусмотрена возможность регулировки уровня шумового сигнала и частотной коррекции сигнала для каждого выхода в отдельности, а также возможность дистанционного включения и выключения при помощи проводного пульта | 35 100 |

| | | |
|---------|--|--------|
| | <p>дистанционного управления.</p> <p>Имеет сертификат соответствия ФСТЭК.</p> | |
| «БУРАН» | <p>Диапазон частот: 100-11200 Гц</p> <p>Количество каналов: 3</p> <p>Вывод информации о состоянии работы системы на жидкокристаллический индикатор.</p> <p>Оптимальное использование мощности каналов за счет мониторинга уровня их нагрузки.</p> <p>Возможность дистанционного включения системы по проводному каналу.</p> <p>Имеет сертификат соответствия ФСТЭК</p> | 50 000 |
| «Барон» | <p>Диапазон частот: 100-11200 Гц</p> <p>Количество выходных каналов: 4</p> <p>Полностью цифровое управление;</p> <p>интеллектуальное меню, гибкая система конфигурирования; возможность формирования помехового сигнала от различных внутренних и внешних источников и их комбинаций наличие четырех независимых выходных каналов с отдельными регулировками для оптимальной настройки помехового сигнала для различных защищаемых поверхностей и каналов утечки;</p> <p>Имеет сертификат соответствия ФСТЭК</p> | |

По результатам анализа в качестве средства виброакустической защиты был выбран система «Соната-АВ» модель 4Б.

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

Пассивная защита обеспечивается фильтрации для сетей электропитания во всех помещениях.

Активная защита заключается в создании и передаче по каналам связи белого шума, не позволяющий выделить из перехваченного сигнала полезную информацию.

Таблица 3 – Активная защита от утечек информации по электрическим, акустоэлектрическим и электромагнитным каналам

| Наименование | Описание | Цена, руб. |
|--------------|--|------------|
| ЛГШ-503 | <p>Диапазон частот: 0.01–1800 МГц. Система представляет собой генератор шума по цепям электропитания, заземления и ПЭМИН.</p> <p>Обеспечивает защиту информации от утечки по каналам ПЭМИН путем создания на границе контролируемой зоны широкополосной шумовой электромагнитной помехи, которая зашумляет побочные излучения защищаемого объекта.</p> <p>Оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима.</p> <p>Оснащено счетчиком учета времени наработки, учитывающим и отображающим суммарное время работы в режиме формирования маскирующих помех.</p> <p>Обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.</p> | 44 200 |
| СОНАТА-РСЗ | <p>Диапазон частот: 0.01-2000 МГц</p> <p>Предназначены для защиты объектов вычислительной техники от утечки информации за счет наводок на линии электропитания и заземления.</p> <p>Обеспечивает формирование не синфазных токов и синфазных и паразитных составляющих шумового напряжения во всех проводниках.</p> | 32 400 |

| | | |
|-----------|--|--------|
| ЛГШ-513 | <p>Диапазон частот: 0.009-1800 МГц</p> <p>Система представляет собой генератор шума по цепям электропитания, заземления и ПЭМИН.</p> <p>Обеспечивает защиту информации от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.</p> <p>Оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима.</p> <p>Оснащено счетчиком учета времени наработки, учитывающим и отображающим суммарное время работы в режиме формирования маскирующих помех</p> <p>Обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.</p> | 39 000 |
| SEL SP-44 | <p>Наличие сертификата ФСТЭК.</p> <p>2-канальный цифровой генератор шумовых сигналов в диапазоне 10кГц-400МГц.</p> <p>Активная защита конфиденциальных сведений от утечки по проводам электропитания.</p> <p>2 независимых друг от друга формирователей шума.</p> <p>Возможность регулировки уровня ВЧ и НЧ шумов.</p> <p>Световая и текстовая индикация работы.</p> <p>Звуковой сигнал при переходе в аварийный режим.</p> <p>Функция самодиагностики для оперативного выявления неисправностей и сбоев в работе.</p> | 26 000 |

По результатам анализа в качестве средства защиты было выбрано ЛГШ-513, так как оно имеет приемлемую цену и наиболее широкий диапазон частот и защищает от электрического, электромагнитного каналов, а также ПЭМИН.

4.3 Защита от утечек по оптическому каналу

Для обеспечения защиты помещения от утечки по оптическим каналам необходимо установить жалюзи на окна также используются доводчики для плотного закрывания дверей. Для данной организации было решено установить жалюзи на все окна в помещении, а также установить доводчики на двери.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

Выбранные средства защиты информации включают в себя:

- усиленные двери (переговорная, кабинет директора, кабинет заместителя директора);
- жалюзи на 9 окон;
- «Соната-АВ» модель 4Б;
- генератор шума «ЛГШ-513».

| Базовый элемент | Тип базового элемента |
|--|--|
| Блок электропитания и управления | "Соната-ИП4.1" , "Соната-ИП4.2" , "Соната-ИП4.3" |
| Генератор-акустоизлучатель | "СА-4Б" , "СА-4Б1" |
| Генератор-вибровозбудитель | "СВ-4Б" |
| Размыкатель телефонной линии | "Соната-ВК4.1" |
| Размыкатель слаботочной линии | "Соната-ВК4.2" |
| Размыкатель линии Ethernet | "Соната-ВК4.3" |
| Пульт управления | "Соната-ДУ4.3" |
| Блок сопряжения с внешними устройствами | "Соната-СК4.1" , "Соната-СК4.2" |
| Техническое средство защиты речевой информации от утечки по оптико-электронному (лазерному) каналу | "Соната-АВ4Л" : Генераторный блок "АВ-4Л", вибровозбудитель "СП-4Л" |
| Техническое средство защиты речевой информации от утечки по виброакустическому каналу | "Соната-АВ4М" : Генераторный блок "АВ-4М", вибровозбудитель "ВИ-4.1" |
| Сервисное программное обеспечение "Камертон" | Руководство по эксплуатации |

Рисунок 6 – Состав изделия «Соната-АВ» модель 4Б

Необходимое количество генераторов-вибровозбудителей "СВ-4Б" 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 газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Необходимое количество генераторов-акустоизлучателей "СА-4Б"/"СА4Б1" можно предварительно оценить из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8-12 м³. надпотолочного пространства или др. пустот.

Таблица 4 – Оценка итоговой стоимости средств защиты информации

| Базовый элемент | Цена, руб./1 шт. | Количество | Стоимость, руб. |
|--|------------------|------------|-----------------|
| Блок электропитания и управления "Соната-ИП4.3" | 21 600 | 1 | 21 600 |
| Генератор-акустоизлучатель "СА-4Б" | 7 440 | 9 | 66 960 |
| Генератор-вибровозбудитель "СВ-4Б" | 7 440 | 17 | 126 480 |
| Размыкатель телефонной линии "Соната-ВК4.1" | 6 000 | 4 | 24 000 |
| Размыкатель слаботочной линии "Соната-ВК4.2" | 6 000 | 1 | 6 000 |
| Размыкатель линии Ethernet "Соната-ВК4.3" | 6 000 | 6 | 36 000 |
| Пульт управления "Соната-ДУ4.3" | 7 680 | 1 | 7 680 |
| Блок сопряжения с внешними устройствами "Соната-СК4.2" | 13 440 | 1 | 13 440 |
| «ЛГШ-513» | 39 000 | 4 | 156 000 |

| | | | |
|---|--------|---|---------|
| Жалюзи Blackout | 1 200 | 9 | 10 800 |
| Усиленные двери TorexSuper Omega PRO PP | 45 000 | 4 | 180 000 |
| ИТОГО | | | 648 960 |

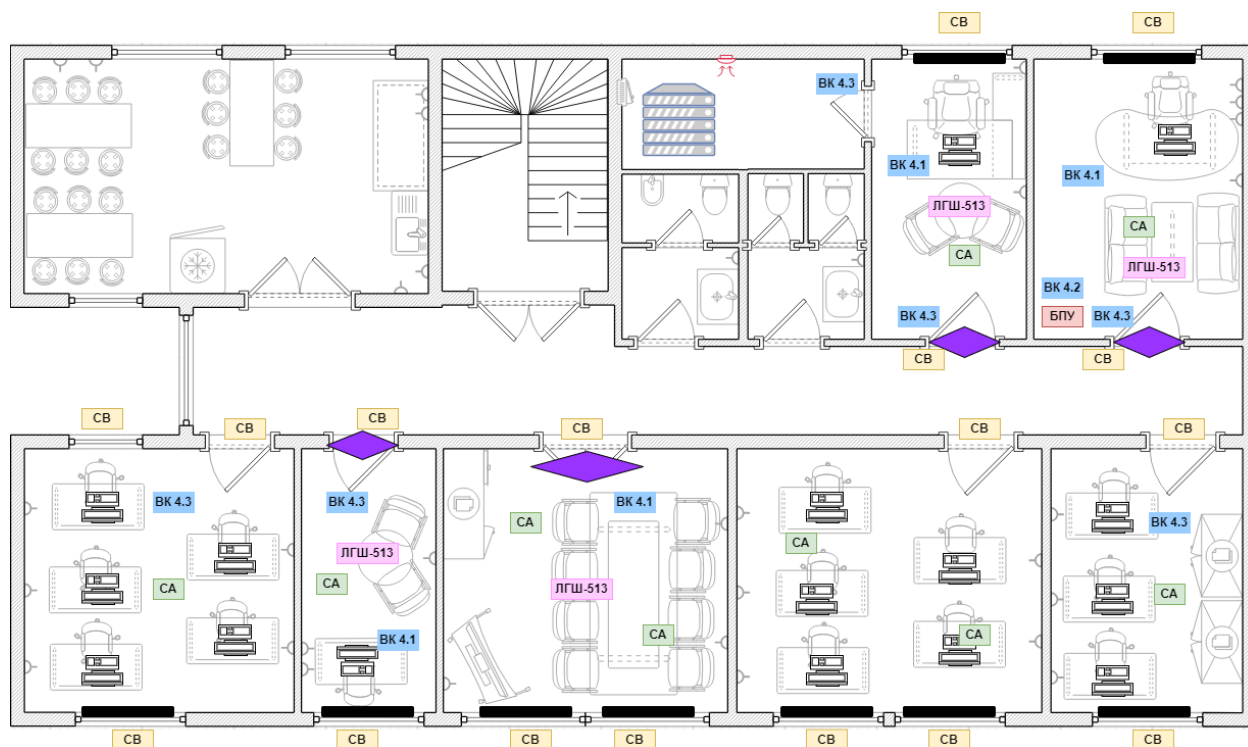


Рисунок 7 – План расстановки СЗИ

Таблица 5 – Условные обозначения

| Условное обозначение | Описание |
|----------------------|--|
| БПУ | Блок электропитания и управления "Соната-ИП4.3" |
| СА | Генератор-акустоизлучатель "СА-4Б" |
| СВ | Генератор-вибровозбудитель "СВ-4Б" |
| ВК 4.1 | Размыкатель телефонной линии |
| ВК 4.2 | Размыкатель слаботочной линии |

| | |
|---|----------------------------|
| БК 4.3 | Размыкатель линии Ethernet |
| ЛГШ-513 | Генератор шума ЛГШ-513 |
|  | Усиленные двери |
|  | Жалюзи |

ЗАКЛЮЧЕНИЕ

В ходе написания данной работы были проанализированы существующие каналы утечки информации, потенциальные каналы утечки информации на защищаемом объекте и описаны необходимые меры их защиты. А также проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны наиболее подходящие для выбранного объекта. На основании выбранных средств защиты был разработан план установки и произведен расчет сметы затрат.

В результате работы была разработана система инженерно-технической защиты, предназначенная для предотвращения утечек конфиденциальной информации и информации, составляющей государственную тайну уровня «секретно», по всем актуальным каналам утечки информации. Общая стоимость всего оборудования составила 648 960 рубля.

СПИСОК ИСПОЛЬЗОВАННОЙ 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. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — No 3 (107). — С. 69–72. — URL: <https://moluch.ru/archive/107/25842>.
3. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. ВЗ-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.