

**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
Ризаев Никита Сергеевич



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


Студент	Ризаев Н.С. <div>(Фамилия И.О.)</div>
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 <div>(Фамилия И.О., должность, ученое звание, степень)</div>
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 <div>(Подпись, дата)</div>
Студент	Ризаев Никита Сергеевич  <div>(Подпись, дата)</div>

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

Студент Ризаев Н.С.
(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 Ризаев Никита Сергеевич 
(Подпись, дата)

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

Студент	Ризаев Н.С.
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 Ризаев Никита Сергеевич

(Подпись, дата)

« 12 » декабря 2023 г.

ВВЕДЕНИЕ.....	7
1 Анализ технических каналов утечки информации.....	8
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.....	16
4.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации.....	18
4.3 Защита от утечек по оптическому каналу.....	20
5 Описание расстановки технических средств.....	21

Сокращения

АРМ	–	автоматизированное рабочее место
АСО	–	активное сетевое оборудование
АСУ	–	автоматизированная система управления
ИБ	–	информационная безопасность
ИБП	–	источник бесперебойного питания
ИС	–	информационная система
ЛВС	–	локальная вычислительная сеть
ТП	–	технологический процесс
ТС	–	техническое средство
КСПД	–	корпоративная сеть передачи данных
ТСПД	–	транспортная сеть передачи данных
ЦОД	–	центр обработки данных
ЛУС	–	локальный узел связи
ОИ	–	объект информатизации
ОТСС	–	основные технические средства и системы
УБИ	–	угрозы безопасности информации

ВВЕДЕНИЕ

Цель работы: повышение защищенности рассматриваемого помещения.

Задачи:

- анализ Защищаемого помещения;
- оценка каналов утечки информации;
- выбор мер пассивной и активной защиты информации.

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.

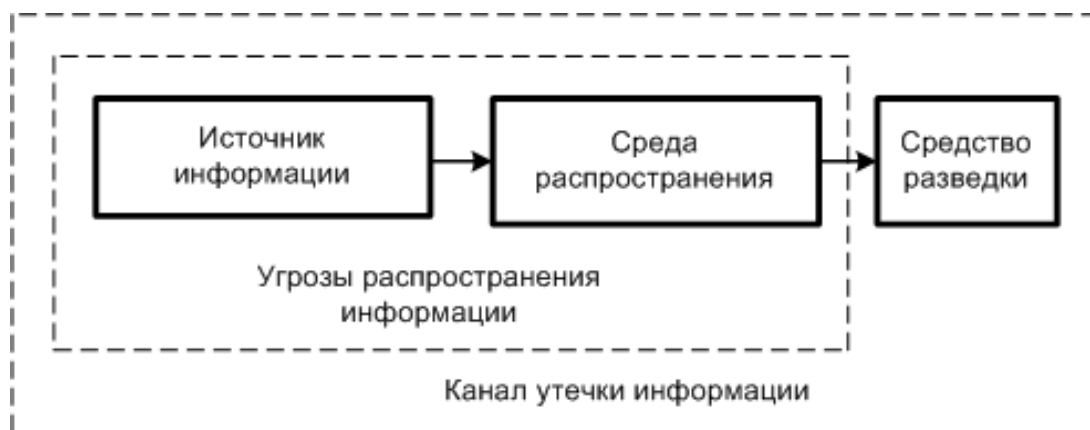


Рисунок 1 – Общая структурная схема канала утечки информации

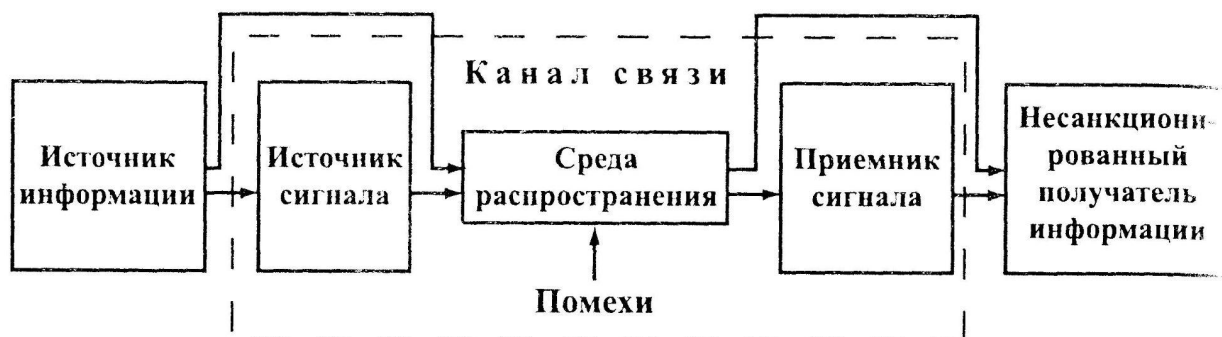


Рисунок 2 – Структура технического канала утечки информации

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

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 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 недекларированных 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 десяти помещений и представляет собой офис организации, который включает в себя:

- коридор;
- кабинет директора;
- переговорную;
- столовую;
- серверную;
- санузел;
- офисные помещения для сотрудников.

Информационные потоки организации представлены на рисунке 3, красными линиями обозначены закрытые потоки, в которых передается информация ограниченного доступа, а зелеными – открытые потоки.

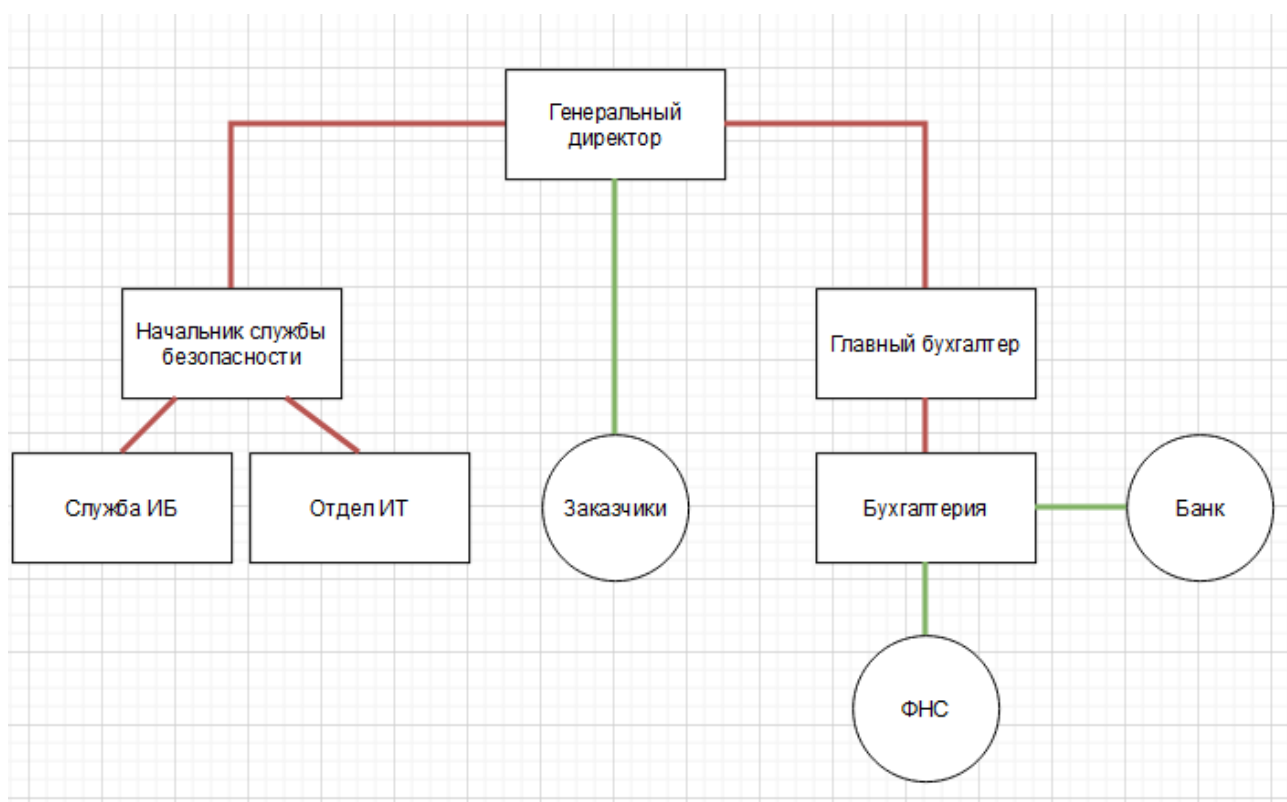


Рисунок 3 – Информационные потоки организации

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 4 представлен план защищаемого помещения.

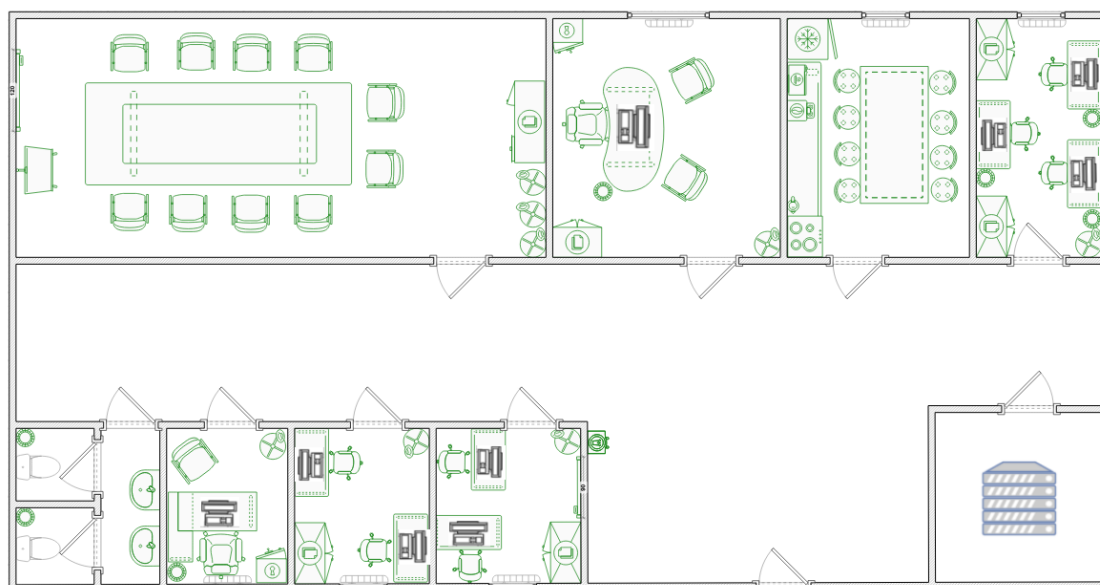


Рисунок 4 – План помещения

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 1.

Таблица 1 – Необходимые средства защиты информации

Технические каналы утечки информации	Источники	Пассивные средства защиты	Активные средства защиты
Вибрационный и виброакустический	Твердые поверхности, радиаторы	Добавление дополнительного помещения перед переговорной	Вибрационное зашумление
Оптический	Окна, двери	Шторы, доводчики для плотного закрывания дверей	Бликующие устройства
Электромагнитный и электрический	ПК, розетки, техника	Фильтры для сетей	Электромагнитное зашумление
Акустический и акустоэлектрический	Окна, двери	Звукоизоляция, фильтры для сетей электропитания	Акустическое зашумление

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

Модель	Цена, руб.	Характеристики	Особенности
ЛГШ-404	35 100	Электропитание 220 В/50 Гц. Максимальное количество излучателей – 40. Диапазон воспроизводимого шумового сигнала 175–11200 Гц.	Одно из существенных преимуществ системы – вариативность количества подключаемых к генераторному блоку преобразователей. Уровень шумового сигнала, создаваемого генератором ЛГШ, регулируется.
SEL SP-157 Шагрень	47 400	Диапазон воспроизводимого шумового сигнала 90–11200 Гц. Максимальное количество излучателей – 64. Электропитание 220В/50Гц.	Защита паролем настроек системы. Отсчёт времени наработки генерации шума по каждому каналу с выводом на экран. Непрерывный контроль состояния системы и каждого отдельного излучателя.
Соната АВ-4Б	44 200	Диапазон воспроизводимого шумового сигнала 175–11200 Гц. Выходное напряжение В $12,5 \pm 0,5$. 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, пульта управления, блоков сопряжения из внешних устройств. Технического средства защиты речевой информации от утечки по оптико-электронному (лазерному) каналу и прочих аксессуаров.

Шорох 5Л	21 500	Максимальное количество излучателей 40. Электропитание 220 (+10% - 15%) В (есть возможность работы системы от источника питания 12В). Количество октавных полос для регулировки уровня мощности шума 7.	Сетевой генератор шума. Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.
----------	--------	---	--

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

Модель	Цена, руб.	Характеристики	Особенности
Соната-РСЗ	32 400	Работа от сети ~220 В +10%/15%, 50 Гц. Потребляемая мощность – 10Вт. Продолжительность работы не менее 8 часов.	Звуковая и световая индикация работы. Возможно дистанционное управление посредством проводного пульта.

ЛГШ-513	39 000	<p>Диапазон частот 0.009-1800 МГц.</p> <p>Диапазон регулировки уровня выходного шумового сигнала не менее 20 дБ.</p> <p>Мощность, потребляемая от сети не более 45 ВА.</p>	<p>Обеспечивает защиту информации от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.</p> <p>Оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима.</p> <p>Оснащен 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>
Соната- РС1	16 520	<p>Диапазон частот до 1 ГГц,</p> <p>регулировка уровня шума в 1 частотной полосе.</p> <p>Напряжение 220 В.</p>	<p>Возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus)</p>

Генератор шума Покров	32 800	Диапазон частот 10 кГц – 6000 МГц. Мощность 15 Вт. Наработка на отказ 5000 часов.	Централизованное управление и контроль по Ethernet (для исполнения 2), для применения в системах пространственного зашумления. Независимая регулировка уровней электромагнитного поля шумового сигнала и шумового сигнала в линии электропитания и заземления.
--------------------------	--------	---	--

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 возможной фото-видеосъемки или визуального наблюдения следует установить жалюзи на окна и также воспользоваться доводчиками для дверей.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

Выбранные средства защиты информации включают в себя:

- усиленные двери;
- жалюзи;
- «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 5 – Состав изделия «Соната-АВ» модель 4Б

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	10	74 400
Размыкатель	6 000	4	24 000

телефонной линии "Соната-ВК4.1"			
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	3	117 000
Жалюзи Blackout	1 200	5	6 000
Усиленные двери Torex Super Omega PRO PP	45 000	5	225 000
ИТОГО			598 080

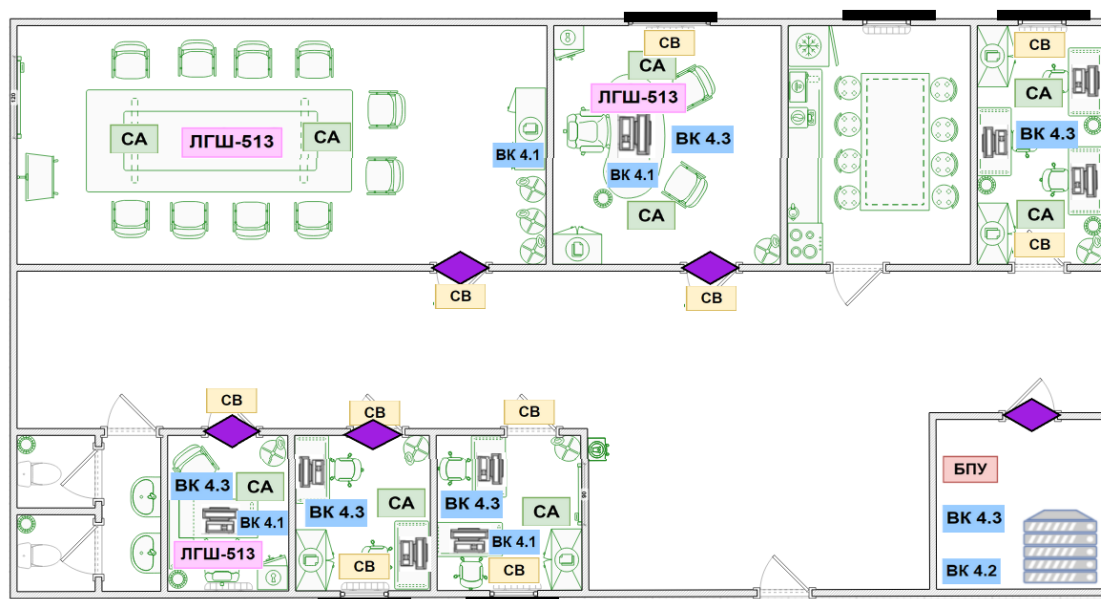

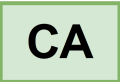
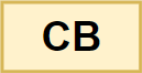

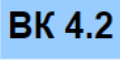
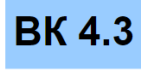
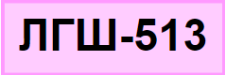
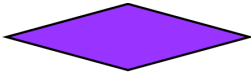



Рисунок 6 – План расстановки СЗИ

Таблица 5 – Условные обозначения

Условное обозначение	Описание
	Блок электропитания и управления "Соната-ИП4.3"
	Генератор-акустоизлучатель "СА-4Б"
	Генератор-вибровозбудитель "СВ-4Б"
	Размыкатель телефонной линии
	Размыкатель слаботочной линии
	Размыкатель линии Ethernet
	Генератор шума ЛГШ-513
	Усиленные двери
	Жалюзи

ЗАКЛЮЧЕНИЕ

В ходе данной курсовой работы был составлен план помещения, изучен теоретический материал, проведен анализ возможных каналов утечки секретной информации, описаны необходимые меры. Были выбраны меры защиты информации, проанализированы существующие средства защиты от различных утечек. Также был разработан план установки выбранных пассивных и активных средств защиты. Общая стоимость всего оборудования составила 598 080 рубля.

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)