

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

Факультет безопасности информационных технологий

Дисциплина:

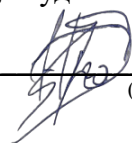
«Инженерно-технические средства защиты информации»

КУРСОВОЙ ПРОЕКТ

«Проектирование системы защиты от утечки информации по различным каналам»

Выполнили:

Дрокин Никита Сергеевич, студент группы N34501


_____ (подпись)

Проверил:

Попов Илья Юрьевич, 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	Дрокин Никита Сергеевич (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34501
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич (Фамилия И.О)
Должность, ученое звание, степень	к.т.н., доцент ФБИТ
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование системы защиты от утечки информации по различным каналам
Задание	Проектирование системы защиты от утечки информации по различным каналам


Краткие методические указания

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

Содержание пояснительной записки

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	 (Подпись, дата)
Студент	 (Подпись, дата)

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

Студент Дрокин Никита Сергеевич
(Фамилия И.О)

Факультет Безопасность информационных технологий

Группа N34501

Направление (специальность) 10.03.01 (Технологии защиты информации 2020)


Руководитель Попов Илья Юрьевич
(Фамилия И.О)


Должность, ученое звание, степень к. т. н., доцент ФБИТ

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.	Разработка и утверждение задания и календарного плана на курсовую работу	21.10.2023	21.10.2023	
2.	Анализ теоретической составляющей	23.11.2023	23.11.2023	
3.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	16.12.2023	16.12.2023	
4.	Представление выполненной курсовой работы	19.12.2023	19.12.2023	

Руководитель  (Подпись, дата)



Студент  (Подпись, дата)

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

Студент	Дрокин Никита Сергеевич (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34501
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич (Фамилия И.О)
Должность, ученое звание, степень	к. т. н., доцент ФБИТ
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 Целью работы является повышение защищенности рассматриваемого помещения. Задачами является анализ защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.
2. Характер работы Конструирование
3. Содержание работы
 - 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
4. Выводы В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель	 (Подпись, дата)
Студент	 (Подпись, дата)

СОДЕРЖАНИЕ

Введение	6
1 Проектирование системы защиты от утечки информации по различным каналам	7
1.1 Анализ технических каналов утечки информации	7
1.2 Общие сведения об организации на территории помещения	11
1.3 Руководящие документы	12
1.4 Анализ защищаемых помещений	13
1.4.1 План помещения и описание присутствующей мебели	13
1.4.2 Описание помещений	15
1.4.3 Анализ способов утечки информации	16
1.4.4 Выбор необходимых средств защиты информации	17
1.5 Анализ рынка технических средств	17
1.5.1 Акустический и виброакустический каналы	17
1.5.2 Оптический канал	19
1.5.3 Электрический, электромагнитный и акустоэлектрический каналы	19
1.5.1 Побочное электромагнитное излучение и наводки (ПЭМИН)	20
1.6 Описание расстановки технических средств	22
1.6.1 Размещение устройств	23
Заключение	25
Список использованных источников	26

ВВЕДЕНИЕ

Средства защиты информации (СЗИ) обеспечивают защиту информации в информационных системах, представляющих собой совокупность хранимой в базах данных информации, информационных технологий, обеспечивающих ее обработку, и технических средств. Их целью является предотвращение несанкционированного доступа злоумышленников к ресурсам и данным предприятия, что снижает риск утечек, утраты, искажения, уничтожения, копирования и блокирования информации. Это, в свою очередь, помогает избежать экономических, репутационных и других видов ущерба для предприятия. Разработка эффективного комплекса мер для достижения этой цели является одной из наиболее актуальных задач современности.

В данной работе рассмотрен процесс создания комплекса инженерно-технической защиты информации, составляющей является государственной тайной с уровнем «совершенно секретно» на объекте информатизации. Объект защиты включает в себя шесть помещений: кабинет директора, переговорную, офис для сотрудников, кухню/зону отдыха, коридор и архив.

Работа состоит из 6 глав. В первой главе произведен анализ технических каналов утечки. Во второй приведены общие сведения об организации. В третьей приведен перечень управляющих документов. В четвертой анализ защищаемых помещений. В пятой анализ рынка технических средств защиты информации разных категорий. И шестая глава разработка схем расстановки выбранных технических средств в защищаемом помещении.

1 ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО РАЗЛИЧНЫМ КАНАЛАМ

1.1 Анализ технических каналов утечки информации

Утечка информации — это незаконное получение или передача 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;
- несанкционированный доступ к информации;
- получение конфиденциальной 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.



Рисунок 1 – Структура технического канала утечки информации.

На рисунке 1 представлена структуры технического канала утечки информации. На вход ТКУИ поступает информация в виде первичного сигнала. Первичный сигнал

представляет собой носитель с информацией от её источника или с выхода предыдущего канала.

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.

Информация от источника поступает на вход канала на языке источника, передатчик производит преобразование этой формы представления информации в форму, обеспечивающую запись её на носитель информации. Среда передачи сигнала — это физическая среда, через которую информационный сигнал может распространяться и быть зарегистрированным приемником. Она описывается набором физических параметров, которые определяют условия передвижения сигнала. После этого приемник извлекает информацию с носителя, обрабатывает полученный сигнал (путем усиления) и преобразует информацию в форму сигнала, доступную для восприятия получателю (человеку или техническому устройству).

Согласно физическим свойствам носителя и характеру канала связи технические средства коммуникации и информации делятся на следующие категории:

- Оптические;
- Радиоэлектронные;
- Электрические;
- Электромагнитные;
- Индукционные;
- Акустические;
- Акустоэлектрические;
- Вибро-акустические;
- Материально-вещественные.

Оптические. Возможность похищения данных реализуется с помощью оптических датчиков, улавливающих световые излучения в видимом или инфракрасном диапазоне. Для получения видовой конфиденциальной информации используются приборы дневного и ночного видения со специальными объективами, позволяющими увеличивать изображение и менять угол обзора.

Проводится съемка объектов информации с помощью портативных камер, способных вести видеозапись на большом удалении. Для фотографирования используются миниатюрные аппараты, четко фиксирующие видовую информацию с расстояния 100 м, не требующие настройки резкости и других параметров. Информация может быть перехвачена с помощью тепловизоров, улавливающих тепловое ИК излучение, а также оптико-волоконных систем видеонаблюдения;

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 охватывает полосу частот от десятков ГГц до звукового.

Электромагнитный ТКУИ связан с перехватом электромагнитных излучений на частотах работы передатчиков систем и средств связи. Этот метод используется для перехвата информации, передаваемой по каналам радио-, радиорелейной, спутниковой связи. Напряженность электрического поля в точке приема (перехвата) пропорциональна мощности передатчика, высоте антенн, и обратно пропорциональна расстоянию. Этот канал утечки актуален в наличии электронной вычислительной техники, компьютеров или других средств обработки информации в помещении. Электромагнитное излучение, создаваемое при работе технических устройств, известно как побочное электромагнитное излучение и наводки (ПЭМИН); защита осуществляется с использованием специальных технических устройств, создающих электромагнитный шум, чтобы скрыть это излучение.

Электрический ТКУИ связан с возможностью съема информации через контактное подключение аппаратуры злоумышленника к кабельным линиям связи. Электрические колебания, генерируемые в процессе работы электрических устройств, содержат данные о подключенных устройствах. Защита осуществляется с использованием специальных фильтров для электросетей, которые маскируют электрические колебания, порождаемые вычислительной техникой.

Индукционный ТКУИ связан с бесконтактным съемом информации с кабельных линий связи. Эта возможность основана на эффекте образования вокруг кабеля электромагнитного поля, модулированного информационным сигналом. Данное поле перехватывается специальным индукционным датчиком, затем усиливается и демодулируется на аппаратуре злоумышленника. Следует отметить, что обнаружение бесконтактных закладных устройств представляет трудность, поскольку они не изменяют характеристики канала связи. Защита осуществляется с применением специальных программных и аппаратных средств, способных выявлять подобные закладки.

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Съем информации возможен как через подслушивание извне помещения (в случае отсутствия звукоизоляции), так и с использованием закладных устройств с функцией аудиозаписи. Этот метод утечки актуален при передаче информации в звуковой форме (диалоги, совещания и др.). Защита осуществляется с использованием звукоизолирующих материалов, предотвращающих распространение звука за пределы помещения, а также с использованием специальных программных и аппаратных средств, способных выявлять подобные закладные устройства.

В акустоэлектрическом канале информация представлена в форме акустических колебаний, которые воздействуют на электрические сети, вызывая электрические колебания. Сняв эти колебания, можно восстановить исходный акустический сигнал. Этот метод утечки информации актуален в случае наличия электрических сетей, связанных с внешней территорией в контролируемом помещении. Например, в телефонной сети, подав небольшое напряжение на входящую телефонную линию и сняв его на входе, можно получить распространяющуюся в помещение звуковую информацию. Защита осуществляется с использованием специальных фильтров для сетей электропитания, которые скрывают колебания, вызванные воздействием на электрические сети.

В виброакустическом канале информация изначально представлена акустическими колебаниями, которые воздействуют на твердую поверхность, преобразуясь в вибрационные колебания. Этот метод утечки информации актуален практически всегда, так как связан с наличием твердых поверхностей в контролируемом помещении, включая стены, потолок, пол и другие поверхности. Защита осуществляется с использованием специальных технических устройств, передающих на защищаемую твердую поверхность

белый шум, который скрывает вибрационные колебания, вызванные акустическими волнами.

В материально-вещественном канале для перехвата информации используются материальные объекты. Такими объектами могут быть отходы производства, черновики и записи, случайно оказавшиеся в мусорной корзине, забракованные изделия и макеты. Для получения секретной информации перехватываются источники, оказавшиеся за пределами контролируемой зоны. Их свойства и состав изучаются с помощью различных приборов и технических устройств. Против кражи или копирования информации, зафиксированной на материальных носителях, предпринимаются организационные меры, включая введение строгого контроля и учета этих видов носителей данных.


В дополнение к вышеупомянутому, стоит выделить оптико-электронные ТКУИ, связанные с перехватом акустических сигналов при помощи лазерного зондирования оконных стекол. Отдельной угрозой также является возможность проникновения злоумышленника на охраняемую территорию, что делает не менее актуальным вопрос обеспечения контроля доступа к этой территории.

1.2 Общие сведения об организации на территории помещения

Организация производит различное ПО для военно-промышленного комплекса, а следовательно, имеет сведения, которые относятся к государственной тайне в соответствии с «Перечень сведений, отнесенных к государственной тайне» сведения, раскрывающие направления развития, содержание разработки вооружения, военной техники имеют степень секретности данных сведений – «секретно».

Рассмотрим информационные потоки организации (рисунок 2).

Информационный поток — это совокупность циркулирующих в логистической системе, между логистической системой и внешней средой сообщений, необходимых для управления, анализа и контроля логистических операций. Они играют ключевую роль в функционировании предприятия, их правильное управление и защита существенны для обеспечения конфиденциальности, целостности и доступности информации. Они могут существовать в виде бумажных, электронных документов (носителей), звука, символов и сигналов.

двусторонний закрытый информационный поток - 

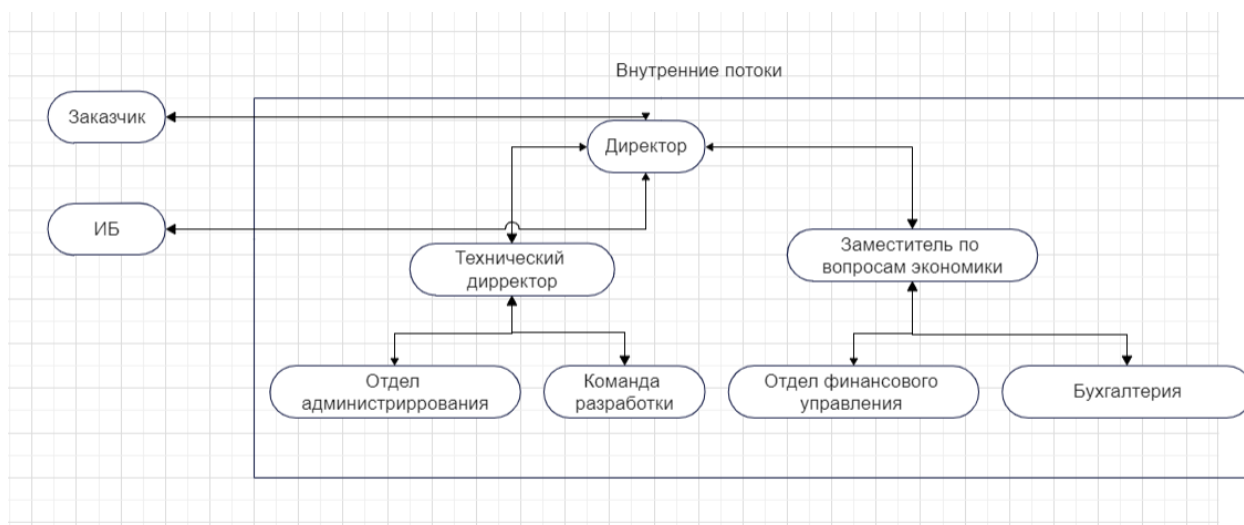


Рисунок 2 – Информационные потоки

1.3 Руководящие документы

- 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 недеklarированных возможностей;
- Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам;

1.4 Анализ защищаемых помещений

1.4.1 План помещения и описание присутствующей мебели

Теперь перейдем к анализу помещений, для которых требуется защита от утечек (рисунок 3).

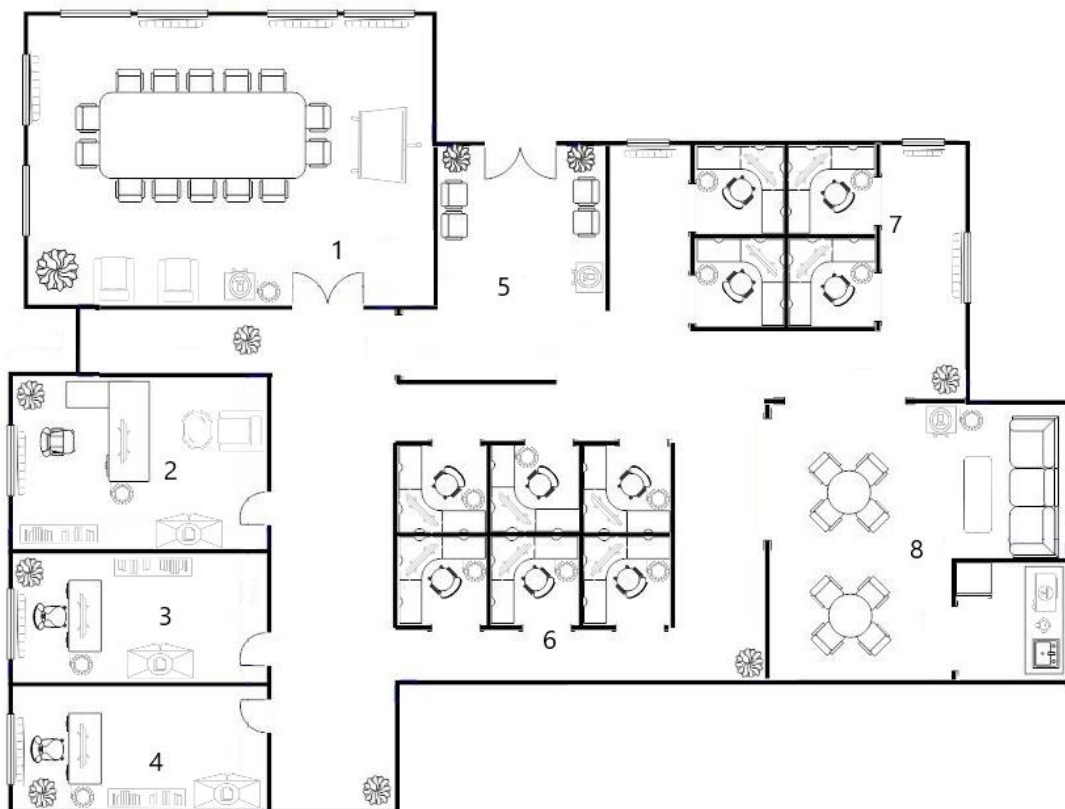


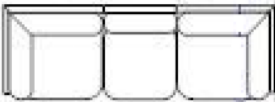
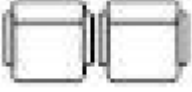



Рисунок 3 – План помещения с мебелью

Ниже приведена таблица с описанием мебели в рассматриваемом помещении

Таблица 1 - Описание мебели представлено ниже:

	Мусорное ведро
	Интерактивная доска
	Кулер
	Радиатор
	Чайник
	СВЧ-печь
	ПК
	Горшок с цветком
	Холодильник
	Стулья
	Кресло
	Стол
	Стол для совещаний
	Журнальный стол

	Стол с раковиной
	Стол с ящиками
	Диван
	Сдвоенные кресла
	Шкаф для документов

1.4.2 Описание помещений

Теперь определим защищаемые помещения.

В нашем случае это будут:

- Переговорная (7м на 4м $S = 28 \text{ м}^2$) (1 зона);
- Кабинет директора (5м на 3,5 м $S = 17,5 \text{ м}^2$) (2 зона)
- Кабинет технического директора (5м на 3м $S = 15 \text{ м}^2$) (3 зона)
- Кабинет заместителя по вопросам экономики (5м на 3м $S = 15 \text{ м}^2$) (4 зона);
- Холл (3м на 3м, $S = 9 \text{ м}^2$) (5 зона);
- Рабочая зона 1 (7м на 5м $S = 35 \text{ м}^2$) (6 зона);
- Рабочая зона 2 (6м на 4м $S = 24 \text{ м}^2$) (7 зона);
- Кухня/комната отдыха (5 м на 4 м, $S = 20 \text{ м}^2$) (8 зона).

Теперь опишем данные помещения:

Для ведения переговоров выделено обособленное помещение, в котором помимо стола и стульев имеется 1 проектор, 1 кулер, 1 мусорное ведро. В помещении есть 6 окон, 1 горшок с цветком и 4 розетки, 4 радиатора.

Для работы директора выделено помещение, в нем присутствует 1 окно, 1 рабочее место с ПК, 3 розетки, 1 радиатор, 1 мусорное ведро, 1 книжная полка, 1 горшок с цветком, 1 кресло, 1 журнальный столик, 1 шкаф для документов.

Для технического директора выделено помещение, в нем присутствует 1 окно, 1 рабочее место с персональным компьютером (стол, кресло и компьютер), 1 радиатор, 2 розетки, 1 мусорное ведро, 1 книжная полка, 1 шкаф для документов.

Для работы заместителя по вопросам экономики выделено помещение, в нем присутствует 1 окно, 1 рабочее место с персональным компьютером (стол, кресло и компьютер), 1 радиатор, 2 розетки, 1 мусорное ведро, 1 книжная полка, 1 шкаф для документов.

Для работников выделена комната с залом и кухней. В ней есть 5 розеток, 1 холодильник, 1 кулер, 1 мусорное ведро, 1 диван, 1 стол, два стола для приема пищи (4 стула на каждом), 1 СВЧ-печь, 1 чайник, 1 раковина.

Есть холл, который включает в себя 2 горшка с цветами, 1 кулер, 4 кресла для гостей.

Для работы сотрудников выделены рабочие всего 10. Каждое рабочее место представляет из себя стол, компьютер и кресло, и 1 мусорное ведро. Также там находятся 3 окна, 3 радиатора, 4 цветка.

Помещение расположено на первом этаже офисного здания, окна выходят в закрытый контролируемый двор. Имеется только один вход. Все окна имеют с внешней стороны решетки, а с внутренней используются шторы, плотно закрывающие видимость снаружи.

Стены здания железобетонные, толщиной не менее 13 см.

1.4.3 Анализ способов утечки информации

Во всех помещениях используются декоративные элементы, в которые потенциально могут быть заложены закладные устройства.

Каждое помещение, требующее защиты, оснащено розетками

Таким образом, актуальны следующие угрозы:

- Закладное устройство;
- Электрические и электромагнитные каналы утечки;
- Вибрационные каналы утечки;
- Оптические каналы утечки;
- Акустические, виброакустические, акустоэлектрические каналы утечки.

1.4.4 Выбор необходимых средств защиты информации

Определим в таблице 2 необходимые средства защиты

Таблица 2 – Средства защиты информации

Каналы утечки	Источники утечки	Пассивная защита	Устройства активной защиты
Вибрационный и виброакустический	Твердые поверхности, радиаторы	Добавление дополнительного помещения перед переговорной	Вибрационное шумление
Оптический	Окна, двери	Шторы, доводчики для плотного закрывания дверей	Бликующие устройства
Электромагнитный и электрический	ПК, розетки, техника	Фильтры для сетей	Электромагнитное шумление
Акустический и акустоэлектрический	Окна, двери	Звукоизоляция, фильтры для сетей электропитания	Акустическое шумление

1.5 Анализ рынка технических средств

1.5.1 Акустический и виброакустический каналы

Пассивной защитой будет выступать усиленные двери в кабинет директора и переговорную, дополнительное помещение перед переговорной.

Средствами виброакустического шумления будет выбрано на основании сравнении компонентов таблицы 3.

Таблица 3 – Активная защита от утечек информации по виброакустическим каналам

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 Шагренъ	47 400	Диапазон воспроизводимого шумового сигнала 90–	Защита паролем настроек системы. Отсчёт времени наработки генерации

		11200 Гц. Максимальное количество излучателей – 64. Электропитание 220В/50Гц.	шума по каждому каналу с выводом на экран. Непрерывный контроль состояния системы и каждого отдельного излучателя.
Соната АВ-4Б	<p>Диапазон воспроизводимого шумового сигнала 175–11200 Гц.</p> <p>Выходное напряжение В $12,5 \pm 0,5$.</p> <p>Электропитание сеть ~220 В/50 Гц.</p>	<p>Диапазон воспроизводимого шумового сигнала 175–11200 Гц.</p> <p>Выходное напряжение В $12,5 \pm 0,5$.</p> <p>Электропитание сеть ~220 В/50 Гц.</p>	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	<p>Максимальное количество излучателей – 40.</p> <p>Электропитание 220 (+10% - 15%) В (есть возможность работы системы от источника питания 12В).</p> <p>Количество октавных полос для регулировки уровня мощности шума – 7.</p>	Сетевой генератор шума. Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.

Исходя из анализа, представленного в таблице 3, было принято решение о выборе системы «СОНАТА АВ-4Б». Особенностью «Соната АВ-4Б» является использование принципа «единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)», что обеспечивает высокую степень надежности в защите информации. Кроме того, усовершенствованная настройка аппаратных элементов модели 4Б позволяет интегрировать источник электропитания с другими для обмена информацией.

1.5.2 Оптический канал

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

1.5.3 Электрический, электромагнитный и акустоэлектрический каналы

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

Выберем средство активной защиты.

Таблица 4 – Электрические и электромагнитные каналы утечки

Модель	Цена, руб.	Характеристики	Особенности
Соната-РСЗ	32 400	Работа от сети ~220 В +10%/- 15%, 50 Гц. Потребляемая мощность – 10Вт. Продолжительнос ть работы не менее 8 часов.	Звуковая и световая индикация работы. Возможно дистанционное управление посредством проводного пульта.
ЛГШ-221	36 400	Диапазон частот 10 кГц – 400 МГц. Диапазон регуливовки уровня выходного шумового сигнала не менее 20 дБ. Мощность, потребляемая от	Сетевой генератор шума. Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.

		сети не более 45 ВА.	
Соната- РС1	16 520	Диапазон частот до 1 ГГц, регулировка уровня шума в 1 частотной полосе. Напряжение 220 В.	Возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus)
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.

На основании анализа, проведенного в таблице 4, был выбран генератор шума «Покров». Оптимальный вариант по соотношению цена и качество.

1.5.4 Побочное электромагнитное излучение и наводки (ПЭМИН)

Проведем анализ в таблице 4 активную защиту от ПЭМИН

Таблица 4 – Активная защита от ПЭМИН

Модель	Цена, руб.	Характеристики	Особенности
ЛГШ 503	44 200	<p>Диапазон частот 10 кГц - 1800 МГц.</p> <p>Уровень шума от -26 дБ (мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц).</p> <p>Мощность – 45 Вт.</p>	<p>Оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Оснащен счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы в режиме формирования маскирующих помех. Прибор имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».</p>
	39000	<p>Диапазон частот 10 кГц - 1800 МГц</p> <p>Уровень шума от -18 дБ(мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц)</p> <p>Электропитание однофазная сеть переменного тока 187 В-242 В</p> <p>Мощность не более 45 ВА</p> <p>Режим работы круглосуточно</p>	<p>Оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа).Оснащен счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы в режиме формирования маскирующих помех. Прибор имеет возможность подключения проводного дистанционного управления и контроля, в</p>

			качестве которого может использоваться программно-аппаратный комплекс «Паутина».
Генератор шума Покров	32 800	Диапазон частот 10 кГц – 6000 МГц. Мощность 15 Вт. Нарботка 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.

Средством ПЭМИН было выбрано входящее в состав ЛГШ-513. Модификация ЛГШ-513Ф соответствует требованиям ФСБ России к средствам активной защиты информации, обрабатываемой техническими средствами от утечки за счет ПЭМИН.

1.6 Описание расстановки технических средств

Выбранные нами средства защиты:

- система виброакустической защиты «Соната АВ-4Б»;
- сетевой генератор шума «Покров»;
- Генератор шума ЛГШ-513;
- Дверные доводчики – 7 шт. (По одному доводчику на одиночную дверь и по два доводчика на двойные);
- жалюзи на семь окон;
- Усиленные двери – 4 шт.

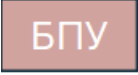


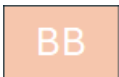

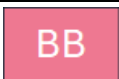
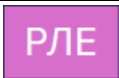

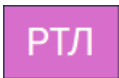

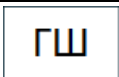
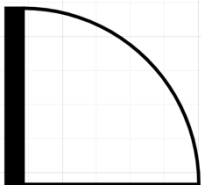

1.6.1 Размещение устройств



Рисунок 4 – Схема размещения устройств

Ниже в таблице 5 приведены обозначения средств защиты.

Таблица 5 – Обозначение средств защиты

Обозначение	Устройство
	Блок электропитания и управления «Соната-ИП4.3»
	Генератор-акустоизлучатель «Соната СА-4Б1»
	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)
	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)
	Генератор-вибровозбудитель «Соната СВ-4Б» (трубопровод)
	Размыкатель линии «Ethernet» «Соната-ВК4.3»
	Размыкатель слаботочной линии «Соната-ВК4.2»
	Размыкатель телефонной линии «Соната-ВК4.1»
	Сетевой генератор шума «Покров»
	Генератор шума «ЛГШ-513»
	Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»
	Шторы-плиссе BlackOut

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.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.
2. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.
3. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.
4. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст : непосредственный // Молодой ученый. — 2016. — № 3 (107). — С. 69-72. — URL: <https://moluch.ru/archive/107/25842/> (дата обращения: 17.12.2022).