

**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

Чан Куанг Линь



(подпись)

Проверил:

преподаватель

Попов Илья Юрьевич

(подпись)

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Чан Куанг Линь

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34491

Направление (специальность) 10.03.01. - Технологии защиты информации

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

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

Задание Разработка комплекса инженерно-технической защиты информации в помещении

Краткие методические указания

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 Попов Илья Юрьевич

(Подпись, дата)

Студент Чан Куанг Линь

(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Чан Куанг Линь

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34491

Направление (специальность) 10.03.01. - Технологии защиты информации

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

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	10.11.2023	10.11.2023	
2	Анализ теоретической составляющей	19.11.2023	19.11.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	23.11.2023	23.11.2023	
4	Представление выполненной курсовой работы	19.12.2023	19.12.2023	

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Чан Куанг Линь

(Подпись, дата)

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент Чан Куанг Линь

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34491

Направление (специальность) 10.03.01. - Технологии защиты информации

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

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

- 1. Цель и задачи работы**
- ☐ Предложены студентом ☐ Сформулированы при участии студента
☒ Определены руководителем

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**
- ☐ Расчет ☒ Конструирование
☐ Моделирование ☐ Другое:

3. Содержание работы

Курсовая работа содержит введение, анализ технических каналов утечки информации, руководящие документы, анализ защищаемых помещений, анализ рынка технических средств, описание расстановки технических средств, заключение, 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 Попов Илья Юрьевич

(Подпись, дата)

Студент Чан Куанг Линь

(Подпись, дата)

«__» _____ 2023г.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	6
1. АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕКИ ИНФОРМАЦИИ	7
2. РУКОВОДЯЩИЕ ДОКУМЕНТЫ	10
3. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	12
4. АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ	17
5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ	25
ЗАКЛЮЧЕНИЕ	28
ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА	29

ВВЕДЕНИЕ

Наряду с непрерывным развитием информационных технологий крайне важно обеспечение информационной безопасности на предприятиях. В каждой организации, вне зависимости от ее размеров, штата, сферы деятельности и иных факторов, консолидируются малые или крупные информационные массивы, нуждающиеся в защите. Требования к конфиденциальности устанавливаются как федеральным законодательством, регуляторами, так и внутренней политикой конкретного предприятия, заинтересованного в охране коммерческой и других видов тайн.

Компьютеризация и развитие интернет-технологий ускорили и оптимизировали бизнес-процессы. Однако современные технические средства используют также в целях промышленного шпионажа и недобросовестной конкуренции. Наличие инженерно-технической защиты информации стало необходимым требованием для безопасной работы многих предприятий. Комплексная система защиты приобрела ведущую роль в предотвращении утечек важных технических данных.

В данной курсовой работе будут рассмотрены способы защиты от утечки информации по техническим каналам с помощью инженерно-технических средств защиты информации.

Инженерно-технические средства защиты информации – это совокупность технических средств и мероприятий, нацеленных на предотвращение утечек, разглашения информации, и несанкционированного доступа в сетевые ресурсы организации.

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

1. АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕКИ ИНФОРМАЦИИ

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

Под техническим каналом утечки информации (ТКУИ) понимают совокупность источника информации (передатчика), линии связи (физической среды – канал с шумами), по которой распространяется информационный сигнал, и технических средств перехвата информации (приемника).

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

Технический канал содержит три основных элемента: источник сигнала, среду распространения носителя и приемник.

На вход канала поступает информация в виде первичного сигнала. Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода предыдущего канала. В качестве источника 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.

Среда распространения сигнала - физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Она характеризуется набором физических параметров, определяющих условия перемещения сигнала. Основными параметрами, которые надо 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.

Среда может быть однородная и неоднородная. Однородная - вода, воздух, металл и т.п. Неоднородная среда образуется за счет перехода сигнала из одной среды в другую, например, акустоэлектрические преобразования.

Приемник выполняет функцию, обратную функции передатчика. Он производит:

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

Основным признаком для классификации технических каналов утечки информации является физическая природа носителя. По этому признаку ТКУИ делятся на:

- оптические;
- радиоэлектронные;
- акустические;
- материально-вещественные.

Оптический канал утечки информации реализуется непосредственным восприятием глазом человека окружающей обстановки путем применения специальных технических средств, расширяющих возможности органа зрения по видению в условиях недостаточной освещенности, при удаленности объектов наблюдения и недостаточности углового разрешения. Это и обычное подглядывание из соседнего здания через бинокль, и регистрация излучения различных оптических датчиков в видимом или ИК-диапазоне, которое может быть модулировано полезной информацией. При этом очень часто осуществляют документирование зрительной информации с применением фотопленочных или электронных носителей. Наблюдение дает большой объем ценной информации, особенно если оно сопряжено с копированием документации, чертежей, образцов продукции и т. д.

Радиоэлектронный канал утечки информации — канал, в котором носителем информации служит электромагнитное поле и электрический ток. Радиоэлектронный канал относится к наиболее информативным каналам утечки в силу следующих его особенностей:

- независимость функционирования канала от времени суток и года, существенно меньшая зависимость его параметров по сравнению с другими

каналами от метеоусловий;

- высокая достоверность добываемой информации, особенно при перехвате ее в функциональных каналах связи (за исключением случаев де информации);
- большой объем добываемой информации;
- оперативность получения информации вплоть до реального масштаб времени;
- скрытность перехвата сигналов и радиотеплового наблюдения.

В радиоэлектронном канале производится перехват радио и электрических сигналов, радиолокационное и радиотепловое наблюдение. Следовательно, в рамках этого канала утечки добывается семантическая информация видовые и, сигнальные демаскирующие признаки. Радиоэлектронные каналы утечки информации используют радио, радиотехническая, радиолокационная и радиотепловая разведка.

Под техническим каналом утечки акустической (речевой) информации понимают совокупность объекта разведки (выделенного помещения), технического средства акустической (речевой) разведки, с помощью которого перехватывается речевая информация, и физической среды, в которой распространяется информационный сигнал. В зависимости от физической природы возникновения информационных сигналов, среды их распространения технические каналы утечки акустической (речевой) информации можно разделить на: прямые акустические (воздушные), акустовибрационные (вибрационные), акустооптические (лазерные), акустоэлектрические и акустоэлектромагнитные (параметрические).

Материально-вещественные каналы – каналы утечки информации, возникающие за счет неконтролируемого выхода за пределы контролируемой зоны различных материалов и веществ, в которых может содержаться конфиденциальная информация.

2. РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Основными документами в области защиты информации являются:

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

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

- СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам.
- СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации.
- Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров.

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

3. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

Наименование организации: САО «РЕСО-Гарантия».

Область деятельности: страхование.

Закрытые информационные потоки (красный): взаимодействие с отделом безопасности, бухгалтерии, маркетинга, взаимодействие с отделом по работе с клиентами (финансы), банковская информация, клиентская база, а также взаимодействие с администратором предприятия.

Открытые информационные потоки (зеленый): взаимодействие с Федеральной Налоговой Службой, договоры с клиентами, взаимодействие с отделом по работе с клиентами (служба поддержки)

Перечень защищаемых информационных активов:

- Персональные данные сотрудников;
- Персональные данные клиентов;
- Конфиденциальная информация, содержащая коммерческую тайну;
- Исходный код разработанного веб приложения

На рисунке 1 представлены информационные потоки предприятия:

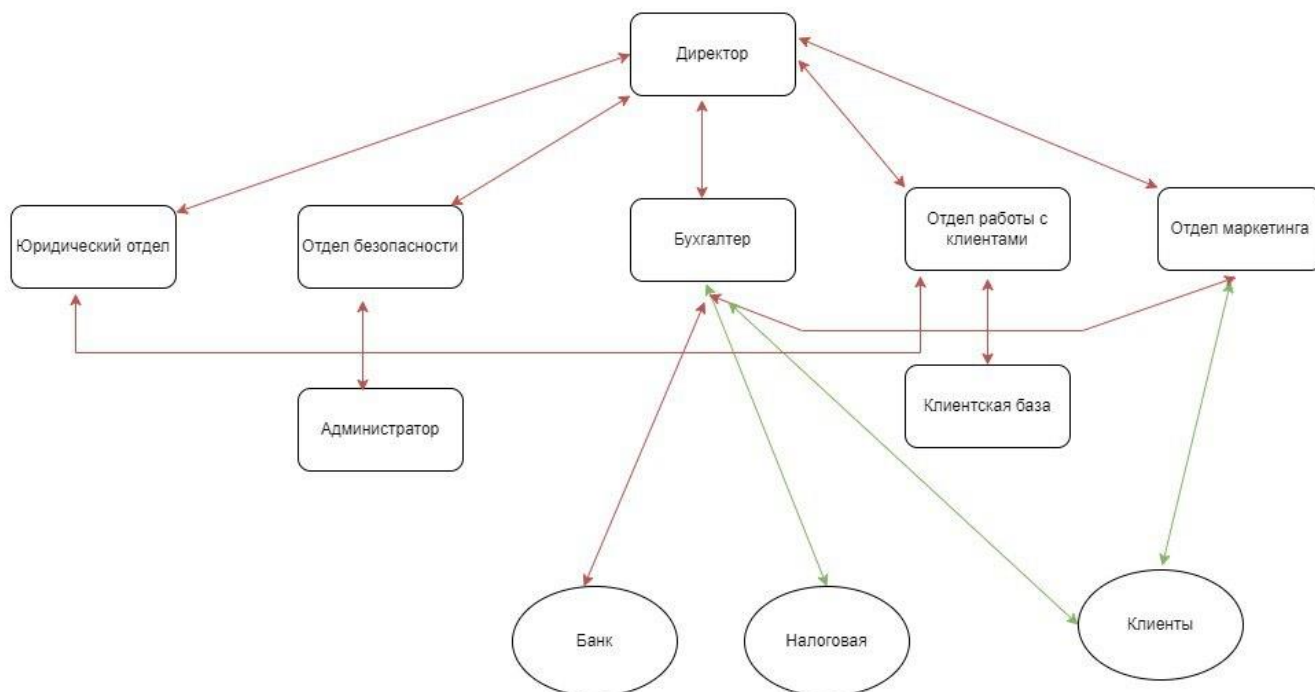


Рисунок 1 – информационные потоки

На рисунке представлен план защищаемого помещения.

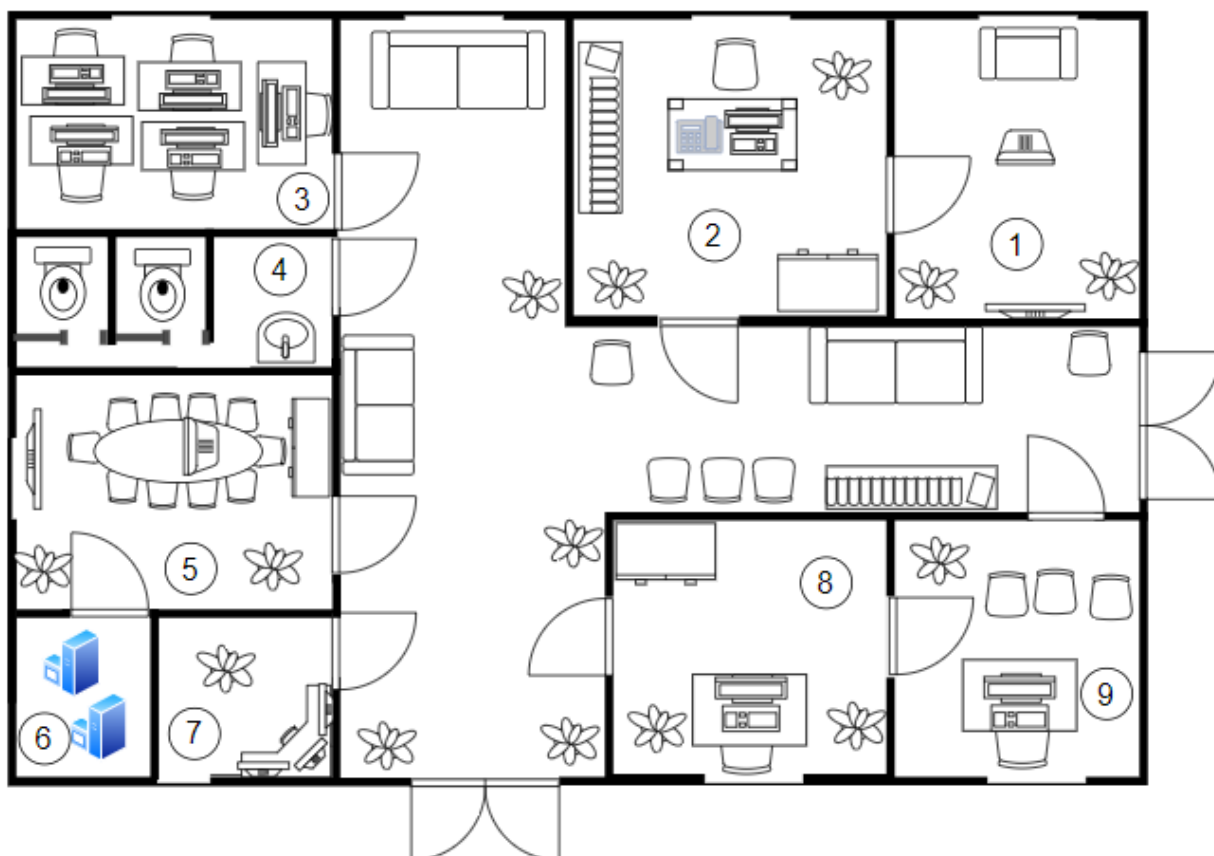


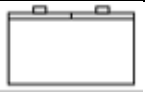

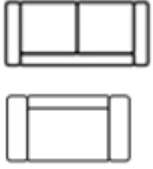

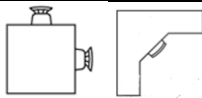
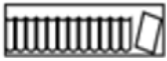

















Рисунок 2 – План защищаемого помещения

Обозначения	Описание
	Экран
	Компьютер
	Шкаф
	Комнатное растение
	Диваны

	Туалет
	Офисные столы
	Книжный шкаф
	Сервер
	Телефон
	Раковина
	Стул
	Проектор
	Двери
	Личный кабинет директора с проектором
	Кабинет директора
	Компьютерный зал
	Туалет
	Переговорная
	Серверная
	Охранная
	Бухгалтерская
	Отдел работы с клиентами

3.1 Описание помещений

Защите подлежат следующие помещения:

- Кабинет директора: 6м на 6м, площадь 36 м2;
- Личный кабинет директора с проектором: 4м на 5м, площадь 20 м2;
- Переговорная: 7 м на 5 м, площадь 35 м2;
- Компьютерная: 7 м на 4.5 м, площадь 31.5 м2;
- Бухгалтерская: 5 м на 4 м, площадь 20 м2;
- Отдел работы с клиентами: 4.5 м на 4 м, площадь 18 м2.

Помещение состоит из 9 комнат и коридора. Необходимо защищать 6 комнат, содержащих информацию ограниченного доступа. Переговоры вводятся в кабинетах директора и переговорной. В кабинете директора находятся стол, стул, диван, 2 шкафа, персональный компьютер, телефон, проектор, экран, 4 живых растения, батарея центрального отопления, 6 розеток, 2 окна. В переговорной находится стол со стульями, шкаф, проектор, экран для проектора, 2 живых растения, 4 розетки, батарея центрального отопления, окно. В компьютерной располагаются 5 столов, 5 стульев, 5 персональных компьютеров, 10 розеток, батарея центрального отопления, окно. В бухгалтерской располагается шкаф, стол, стул, компьютер, 4 розетки, батарея центрального отопления, окно, 2 живых растения. В отделе работы с клиентами располагается стол с стульями, компьютер и растение.

Офис находится на третьем этаже пятиэтажного здания, окна выходят в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Помещения сгруппированы в «непроходной» (тупиковой) части здания, которая редко используется сотрудниками при выполнении служебных обязанностей, не связанных с доступом к государственной тайне. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

3.2 Анализ возможных утечек информации

В помещении располагаются декоративные элементы, в которые могут быть подложены закладные устройства. Также существует возможность утечки информации с помощью электрического и электромагнитного каналов через розетки. Возможно снятие информации по вибрационному, оптическому каналам, акустическому, виброакустическому и акустоэлектрическому. Материально-вещественный канал утечки информации регулируется строгой политикой компании в отношении физических носителей информации, и в рамках курсовой работы не рассматривается.

3.3 Выбор средств защиты информации

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – требуется оснастить помещение средствами защиты, приведенными в таблице 1.

Таблица 1 – Активная и пассивная защита

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

4. АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

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

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

4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита представляет собой:

- усиленные двери;

- тамбурное помещение перед переговорной;
- дополнительная отделка переговорной звукоизолирующими материалами.

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

Таблица 2 – Сравнительный анализ средств активной защиты от утечки виброакустическому каналу

Модель	Диапазон воспроизводимого шумового сигнала	Предназначение	Цена
SEL SP-157 «Шагрень»	90–11200 Гц	Генераторный блок SEL SP-157G конструктивно содержит два независимых канала генерации с семи полосным (октавный) эквалайзером и двумя параллельными выходами на нагрузку. Каждый канал формирует электрический широкополосный шумовой сигнал маскирующей помехи, состоящий из аналогового белого шума и речеподобной помехи (преобразованной из цифровой).	31 200 руб.
ЛГШ-303	180 - 11 300 Гц	Изделие «ЛГШ-303» мобильно и предназначено для работы в помещениях, (автомобилях) и других местах не требующих стационарных средств защиты информации по прямому акустическому каналу и не оборудованных стационарными источниками питания.	15 600
КАМЕРТОН-5	90–11200 Гц	Предназначено для обеспечения защиты акустической речевой информации от утечки по	46 000 руб.

		<p>акустическому и вибрационному каналам. Включает : Блок управления и контроля системой; Блок генерации и генератор маскирующих шумов, создающий помехи в речевом диапазоне частот; Виброизлучатели разных типов, блокирующие вибрационные каналы утечки информации (стены, перекрытия, оконные рамы, прочие элементы строительной конструкции); Акустоизлучатели разных типов, создающие помехи в акустических каналах утечки данных (вентиляционная система, дверные проемы, трубы инженерных коммуникаций, пр.); Размыкатели проводных линий, перекрывающие утечку акустических сигналов по проводам телефонной связи, локальной компьютерной сети, пр.; Виброшторы, создающие надежную помеху для прослушки разговоров с помощью направленного микрофона через оконное стекло.</p>	
Соната «АВ» модель 4Б	175–11200 Гц	Генератор шума. Регулировка уровня шума в 3 частотных полосах. Индикация нормального/аварийного режима работы.	26 400 руб.
"ANG-2200" генератор шума	250 Гц - 5 кГц	Для защиты помещений от возможного прослушивания через проводные микрофоны, радиомикрофоны и стетоскопы,	18 000 руб.

		блокирования лазерного съема акустической информации с окон, создания помех звукозаписывающей аппаратуре.	
Буран-2	180 - 11200 Гц	Система акустических и виброакустических помех «Буран-2» является средством активной акустической и вибрационной защиты акустической речевой информации, соответствует требованиям ФСБ России к разработке, производству, сертификации и эксплуатации технических средств защиты особо важных и выделенных помещений органов государственной власти по виброакустическому каналу утечки речевой информации и может использоваться для защиты акустической речевой информации, содержащей сведения, составляющие государственную тайну, циркулирующей в выделенных помещениях до 2 категории включительно.	81 000 руб.
SEL-310 «КОМАР»	24 - 26 кГц	Количество излучателей 10 шт; Дальность подавления диктофонов, до 4 м. Предназначен для полного подавления полезного звукового сигнала при попытке записи.	60 000 руб.

В результате проведенного анализа средств защиты в качестве системы виброакустической защиты была выбрана «Соната АВ» модель 4В, так как достаточно широкий диапазон и не дорогая стоимость. «Соната-АВ» модель 4Б является комплексом

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

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

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

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

Таблица 3 – Сравнительный анализ средств активной защиты от утечки по электрическому каналу

Модель	Характеристики	Описание	Цена
ЛГШ-503	Диапазон частот – 10 кГц – 1,8 ГГц	Изделие «ЛГШ-503» оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех. Конструкция Изделия «ЛГШ-503» обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним. Изделие «ЛГШ-503» имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».	44 200 руб.
ГНОМ-3М-60В	Диапазон частот 150кГц-1800мГц	Гном-3М-60В используется с внешними антеннами. В данном	61 824 руб.

		приборе предусмотрено 4 не связанных между собой выхода для подключения к антеннам и цепи электропитания. Для 100-процентной защиты информации от утечки следует использовать 3 рамочные антенны, расположив их в 3 перпендикулярных друг другу плоскостях.	
Фильтр сетевой помехоподавляющий ФСП-1Ф-7А	Диапазон частот 0,15-1000 МГц	Вносимое затухание по напряжению в каждом проводе двухпроводной сети не менее 60 дБ; Допустимый ток нагрузки 7 А. Предназначен для защиты радиоэлектронных устройств и средств вычислительной техники от утечки информации по цепям электропитания с напряжением 220В с током нагрузки до 7А.	33 264 руб.
Соната РС2	Диапазон частот до 2 ГГц	Особенности конструкции устройств позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники (СВТ). Также предусмотрена возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus). Изделия рассчитаны на подключение к 3-проводной сети энергоснабжения ("Фаза", "Ноль" и "Защитное заземление") и обеспечивают	23 600 руб.

		формирование несинфазных токов и синфазных и парафазных составляющих шумового напряжения во всех проводниках.	
ЛГШ-513	Диапазон частот – 0,01–1800 МГц	<p>Генератор шума ЛГШ-513 оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа).</p> <p>Генератор шума ЛГШ-513 имеет встроенный счетчик учета времени наработки, учитывающий и отображающий в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех. Конструкция генератор ЛГШ-513 обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.</p> <p>Генератор шума ЛГШ-513 имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».</p>	39 000 руб.
Фильтр сетевой	Ток 6 А; Частотный диапазон	Предназначен для защиты информации на различных устройствах типа вычислительной техники и прочих радиоэлектронных	13 824

помехопода- яющий ФСШК-2	от 0,01 до 1000 МГц; Затухание 40 до 70Дб	устройствах, где возможна утечка посредством наводок по электрическим цепям.	
--------------------------------	--	--	--

В результате проведенного анализа средств защиты от утечки электрическими, акустоэлектрическим и электромагнитными каналами была выбрана Соната РС2 из-за низкой стоимости и удовлетворении необходимым критериям.

4.3 Защита от ПЭМИН

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

4.4 Защита от утечек по оптическому каналу

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

5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

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

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

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

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

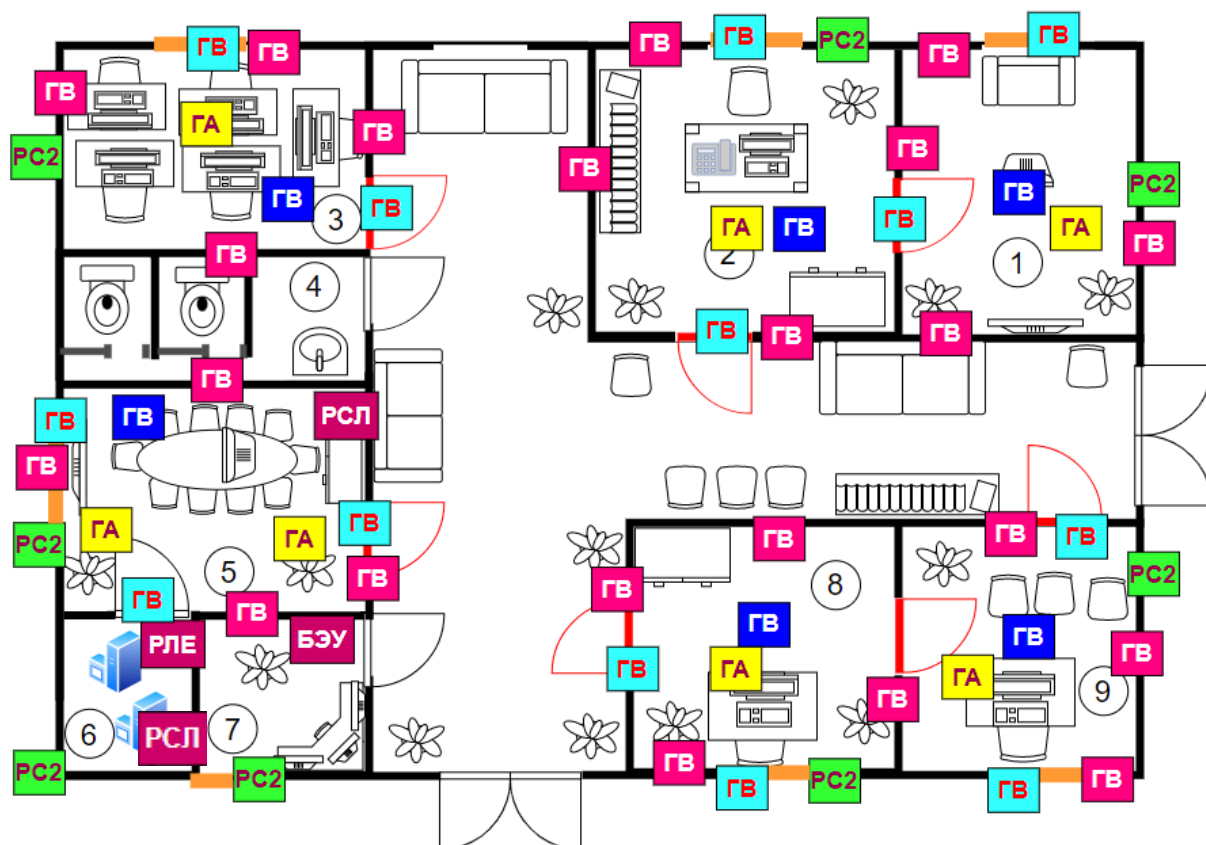
- стены: один на каждые 3–5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- потолок, пол: один на каждые 15–25 м² перекрытия;
- один на окно (при установке на оконный переплет);
- один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо-, тепло- и газоснабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

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

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

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

По результатам выбора средств защиты информации от утечки построим схему









расстановки устройств (Рисунок 3)

Рисунок 3 – Схема расстановки устройств

Таблица 4 – Технические средства

Устройство	Условное обозначение	Цена, руб.	Количество, шт.	Стоимость, руб.
Блок электропитания и управления «Соната-ИП4.3»	БЭУ	21600	1	21 600
«Соната-СА-4Б1» генератор-акустоизлучатель	ГА	3450	7	24 150
«Соната-СВ-4Б» генератор-вибровозбудитель (двери, окна)	ГВ	7400	13	96 200
«Соната-СВ-4Б» генератор-вибровозбудитель (стены)	ГВ	7680	22	168 960

«Соната-СВ-4Б» генератор-вибровозбудитель (пол, потолок)		6000	6	36000
Усиленные металлические двери Медверь		6000	7	42 000
Жалюзи Inspire		514	7	3598
Размыкатель линии Ethernet "Соната-ВК4.3"		6000	1	6000
Размыкатель слаботочной линии "Соната-ВК4.2"		6000	1	6000
Устройства для защиты линий электропитания, заземления от утечки информации "Соната-РС2"		23600	8	188 800
ИТОГО				593 308

ЗАКЛЮЧЕНИЕ

В ходе данной работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении и описаны необходимые меры их защиты. был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для нашего объекта. был разработан план установки и произведен расчет сметы затрат. Таким образом, была предложена защита от утечек информации по акустическому, виброакустическому, оптическому, акустоэлектрическому, электрическому, электромагнитному, оптико-электронному техническим каналам защиты информации и обеспечена защита от ПЭМИН.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

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. Приказ цб рф от 03.03.97 n 02–144 «О введении в действие временных требований по обеспечению безопасности технологий обработки электронных платежных документов в системе центрального банка Российской Федерации».
3. "Руководящий документ "Защита от несанкционированного доступа к информации. Термины и определения".
4. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.