

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

«Инженерно-технические средства защиты информации»

На тему:

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

Выполнил:

Кондакова Карина Андреевна, студентка группы N34461



(подпись)

Проверил:

к.т.н., доцент ФБИТ

Попов Илья Юрьевич

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Кондакова Карина Андреевна
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34461
Направление (специальность)	10.03.01. - Технологии защиты информации
Руководить	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	Разработка комплекса инженерно-технической защиты информации в помещении
Задание	Разработка комплекса инженерно-технической защиты информации в помещении

Краткие методические указания

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	Кондакова Карина Андреевна
	(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Кондакова Карина Андреевна

(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)

Дисциплин 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	Заполнение задания на курсовую работу и аннотации	15.11.2023	15.11.2023	
2	Изучение теоретического материала	30.11.2023	30.11.2023	
3	Написание основного текста курсовой работы	19.12.2023	19.12.2023	
4	Защита курсовой работы	22.01.2024	22.01.2024	

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Кондакова Карина Андреевна

(Подпись, дата)

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент Кондакова Карина Андреевна
(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 Разработка комплекса инженерно-технической защиты информации в помещении

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

**1. Цель и
задачи работы**

☐ Предложены
студентом

☐ Сформулированы при участии студента
☒ Определены руководителем

Цель данной работы – исследовать способы предотвращения утечек конфиденциальной информации через технические каналы связи.

**2. Характер
работы**

☐ Расчет

☐ Конструирование

☐ Моделирование

☒ Другое

3. Содержание работы

1. Введение. 2. Анализ технических каналов утечки информации. 3. Руководящие документы 4. Анализ защищаемых помещений. 5. Описание расстановки технических средств. 7. Заключение. 8. Список литературы.

4. Выводы

В результате выполнения работы был проведён анализ каналов утечки информации, были изучены активные и пассивные методы защиты информации, проведена классификация технических каналов утечки информации, предложены меры защиты информации от утечек по техническим каналам.

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Кондакова Карина Андреевна

(Подпись, дата)

«___» _____ 2023 г

Содержание

ВВЕДЕНИЕ	6
1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ	7
2 НОРМАТИВНО-ПРАВОВЫЕ АКТЫ.....	13
3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	15
3.1 Описание информационных потоков	17
3.2 Описание помещений	18
3.3 Анализ возможных утечек информации	18
3.4 Выбор средств защиты информации.....	19
4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ	20
4.1 Устройства противодействия утечке информации по оптическому каналу.....	23
4.2 Устройства противодействия утечке по электромагнитным и электрическим каналам.....	23
5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ.....	25
ЗАКЛЮЧЕНИЕ.....	27
ИСТОЧНИКИ	28

ВВЕДЕНИЕ

Проектирование системы защиты от утечки информации по различным каналам является очень актуальным вопросом в настоящее время. С развитием информационных технологий и увеличением количества данных, которые хранят и обрабатывают компании, вопрос безопасности информации становится все более критическим.

Утечка информации может происходить через различные каналы, включая сеть интернет, электронную почту, физические носители данных и даже социальные инженерные методы. Проектирование системы защиты от утечки информации направлено на предотвращение таких утечек и минимизацию возможных последствий.

Актуальность данной проблемы очевидна из множества случаев нарушения информационной безопасности, которые происходят ежедневно. Утечки данных могут привести к значительным финансовым потерям, ущербу репутации компании, а также нарушению конфиденциальности клиентов и партнеров. Поэтому необходимо создание системы защиты, которая будет обеспечивать полную безопасность информации и минимизировать риски утечки.

Проектирование такой системы требует комплексного подхода, включающего анализ уязвимостей, разработку политики безопасности, установку специального программного обеспечения и обучение персонала. Кроме того, важно обновлять и совершенствовать систему в соответствии с изменяющимися требованиями и новыми угрозами безопасности.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно» на объекте информатизации.

Цель работы – исследовать способы предотвращения утечек конфиденциальной информации через технические каналы связи.

Для достижения поставленной цели необходимо решить следующие задачи:

- провести классификацию технических каналов утечки информации;
- провести анализ защищаемого помещения;
- изучить пассивные и активные способы защиты;
- провести анализ рынка инженерно-технических средств защиты

информации;

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Для передачи информации носителями в виде полей и микрочастиц по любому техническому каналу (функциональному или каналу утечки) последний должен содержать три основных элемента: *источник сигнала, среду распространения носителя и приемник*. Обобщенная типовая структура канала передачи информации приведена на рис. 1.



Рисунок 1 – Структура технического канала передачи информации

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 или побочные электромагнитные излучения;
- приемо-передатчик функционального канала связи и сам канал связи;
- закладное устройство;
- источник опасного сигнала;
- источник акустических волн, модулированных информацией. Указанные на рис. 1 стрелками пути входа и выхода информации обозначают вход и выход первичных сигналов с информацией. Так как информация от источника поступает на вход канала на языке источника (в виде буквенно-цифрового текста, символов, знаков, звуков, сигналов и т. д.), то передатчик преобразует эту форму представления информации в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения.

Кроме того, он выполняет следующие функции:

- создает (генерирует) поля (акустическое, электромагнитное) или электрический ток, которые переносят информацию;
- осуществляет запись информации на носитель (модуляцию

информационных параметров носителя);

- усиливает мощность сигнала (носителя с информацией);
- обеспечивает передачу (излучение) сигнала в среду распространения в заданном секторе пространства.

Информация записывается путем изменения параметров носителя в соответствии с уровнем первичного сигнала, поступающего на вход. Если носителями информации являются субъекты и материальные тела (макрочастицы), то передатчик соответствует первоначальному смыслу этого слова – передавать или переносить, т. е. выполняет функцию носителя. В случае, когда информацию переносят сигналы (поля, электрический ток и элементарные частицы), передатчики являются их источниками.

Источниками сигналов могут быть как источники функциональных каналов связи, так и опасных сигналов. К последним относятся сигналы с конфиденциальной информацией, появление которых является для источника информации случайным событием и им не контролируется.

Среда распространения носителя – часть пространства, в которой перемещается носитель. Она характеризуется набором физических параметров, определяющих условия перемещения носителя информации. Из них основными параметрами, которые надо учитывать при анализе среды распространения носителя, являются следующие:

- физические препятствия для субъектов и материальных тел;
- мера ослабления (или пропускания энергии) сигнала на единицу длины;
- частотная характеристика (неравномерность ослабления частотных составляющих спектра сигнала);
- вид и мощность помех для сигнала.

Приемник выполняет функции, обратные функциям передатчика. Он осуществляет:

- выбор (селекцию) носителя с нужной получателю информацией;
- усиление принятого сигнала до значений, обеспечивающих съем информации; съем информации с носителя (демодуляцию, декодирование);
- преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и его усиление до значений, необходимых для безошибочного восприятия информации получателем.

Если получатель информации человек, то информация с выхода приемника должна быть представлена на языке общения людей; если техническое устройство, то форма

представления информации должна быть ему понятна. Например, если получатель – ЭВМ, то с выхода приемника на ЭВМ подается двоичная последовательность в кодах, например таблицы ASCII.

– Канал утечки информации отличается от функционального канала передачи получателем информации. Если получатель санкционированный, то канал функциональный, в противном случае – канал утечки. Классификация каналов утечки информации дана на рис. 2.

Физическая природа носителя является основным классификационным признаком технических каналов утечки информации. По этому признаку они делятся:

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

Носитель информации в оптическом канале – электромагнитное поле в диапазоне 0,46 – 0,76 мкм (видимый свет) и 0,76 – 13 мкм (инфракрасные излучения).

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по проводникам из меди, железа, алюминия. Диапазон колебаний этого вида носителя чрезвычайно велик: от звукового диапазона до десятков ГГц. Часто этот канал называют электромагнитным, что представляется недостаточно корректным, так как носителями информации в оптическом канале являются также электромагнитные поля, но в более высокочастотном диапазоне. Кроме того, широко используется в качестве носителя информации модулированный поток электронов (электрический ток). Объединяя эти два носителя информации в канале одного вида, целесообразно назвать его «радиоэлектронный» (электромагнитное поле в радиодиапазоне и электроны электрического тока).



Рисунок 2 – Классификация каналов утечки информации

Носителями информации в акустическом канале являются механические акустические волны в инфразвуковом (менее 16 Гц), звуковом (16 – 20 кГц) и ультразвуковом (свыше 20 кГц) диапазонах частот, распространяющиеся в атмосфере, воде и твердой среде.

В материально-вещественном канале утечка информации возможна через несанкционированное распространение за пределы организации вещественных носителей с секретной или конфиденциальной информацией, прежде всего выбрасываемых черновиков документов и использованной копировальной бумаги, забракованных деталей и узлов, демаскирующих веществ. Последние в виде твердых, жидких и газообразных отходов или промежуточных продуктов содержат химические элементы, по которым в принципе можно определить состав, структуру и свойства новых материалов или восстановить технологию их получения.

Когда речь идет о распространении за пределы организации отходов производства в широком смысле, то следует отличать технический канал утечки от агентурного, в рамках которого носитель информацией выносится проникшим к источнику злоумышленником, завербованным сотрудником организации или сотрудником, стремящимся продать информацию любому ее покупателю. Граница между каналами достаточно условна, однако при утечке информации в агентурном канале переносчиком информации является лицо, сознающее противоправные действия, а в техническом материально-вещественном канале носители вывозятся из организации с целью освобождения ее от отходов или отходы распространяются в результате действия природных сил. В качестве таких сил могут быть воздушные потоки, разносящие газообразные отходы, или водные потоки рек или водоемов, куда сбрасываются недостаточно очищенные жидкие или взвешенные в воде твердые частицы демаскирующих веществ.

Каждый из технических каналов имеет свои особенности, которые необходимо знать и учитывать для обеспечения эффективной защиты информации от утечки или ее предпосылок.

По информативности каналы утечки делят на информативные, малоинформативные и неинформативные (информативность канала оценивается ценностью передаваемой по нему информации). По времени проявления – на постоянные, периодические и эпизодические. В постоянном канале утечка информации носит достаточно регулярный характер. Например, наличие в кабинете источника опасного сигнала может привести к передаче из кабинета речевой информации до момента обнаружения этого источника. Периодический канал утечки может возникнуть во время пролетов разведывательных космических аппаратов, при условии, например, размещения во дворе неукрытой продукции, демаскирующие признаки которой составляют тайну. К эпизодическим относят каналы, утечка информации в которых имеет разовый, случайный характер.

Канал утечки информации, состоящий из передатчика, среды распространения и приемника, является одноканальным. Однако возможны варианты, когда утечка информации происходит более сложным путем – по нескольким последовательным или параллельным каналам. При этом используется свойство информации переписываться с одного носителя на другой. Например, если в кабинете ведется конфиденциальный разговор, то утечка возможна не только по акустическому каналу через стены, двери, окна, но и по оптическому – путем съема информации лазерным лучом со стекла окна или по радиоэлектронному с использованием установленной в кабинете радиозакладки. В двух последних вариантах образуется составной канал, образованный из последовательно соединенных акустического и оптического (на лазерном луче) или акустического и радиоэлектронного (радиозакладка – среда распространения – радиоприемник) каналов. Для повышения дальности канала утечки может также использоваться ретранслятор, совмещающий функции приемника одного канала утечки информации и передатчика следующего канала. Например, для повышения дальности подслушивания с использованием радиозакладки можно разместить ретранслятор в портфеле, сдаваемом в камеру хранения закрытого предприятия.

Как любой канал связи, канал утечки информации характеризуется следующими основными показателями:

- пропускной способностью;
- дальностью передачи информации.

Пропускная способность канала связи оценивается количеством информации, передаваемой по нему в единицу времени с определенным качеством. В теории связи пропускная способность канала в бодах (битах в секунду) определяется по формуле

$$C = \Delta F \log_2 (1 + P_c/P_n),$$

где ΔF – ширина полосы пропускания канала связи; P_c и P_n – мощность сигнала и помехи (в виде белого шума) в полосе пропускания канала соответственно.

Следовательно, пропускная способность канала связи является интегральной характеристикой, учитывающей как ширину полос частот сигнала, которую пропускает канал, так и его энергетику. Чем меньше отношение мощностей сигнала и помехи, тем больше ошибок в принятом сообщении и тем меньше количество переданной информации.

По ширине полосы частот пропускания каналы делят на узко- и широкополосные. Стандартный телефонный канал для передачи речевой информации имеет полосу 300 – 3400 Гц и относится к узко-полосным, а канал для передачи телевизионных сигналов шириной 8 МГц – к широкополосным. Чем шире канал, тем больше информации можно передать за единицу времени. Так как для добывания информации с требуемым качеством необходимо обеспечить на входе приемника канала минимально допустимое для каждого вида информации и носителя отношение сигнал/помеха, то это отношение достигается на различном удалении от источника сигнала в зависимости от мощности сигнала и помехи, а также величины (коэффициента) ослабления (затухания) сигнала в канале. Носители информации существенно отличаются по величине затухания в среде распространения: в наибольшей степени уменьшается энергия акустической волны, в наименьшей – электромагнитная волна в длинноволновом диапазоне частот.

2 НОРМАТИВНО-ПРАВОВЫЕ АКТЫ

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».
- 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 21.01.2011 г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними”;
- СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации;
- Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров;
- Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации;
- Временный порядок аттестации объектов информатизации по требованиям безопасности информации;
- Руководящий документ. Защита от НСД. Термины и определения;
- Руководящий документ. СВТ. Защита от НСД. Показатели защищенности от

несанкционированного доступа к информации;

- Руководящий документ. Автоматизированные системы. Защита от НСД. Классификация автоматизированных систем и требования по защите информации;

- Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;

- Руководящий документ Гостехкомиссии России. Защита от НСД. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей;

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

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

На рисунке 3 представлен план защищаемого помещения.

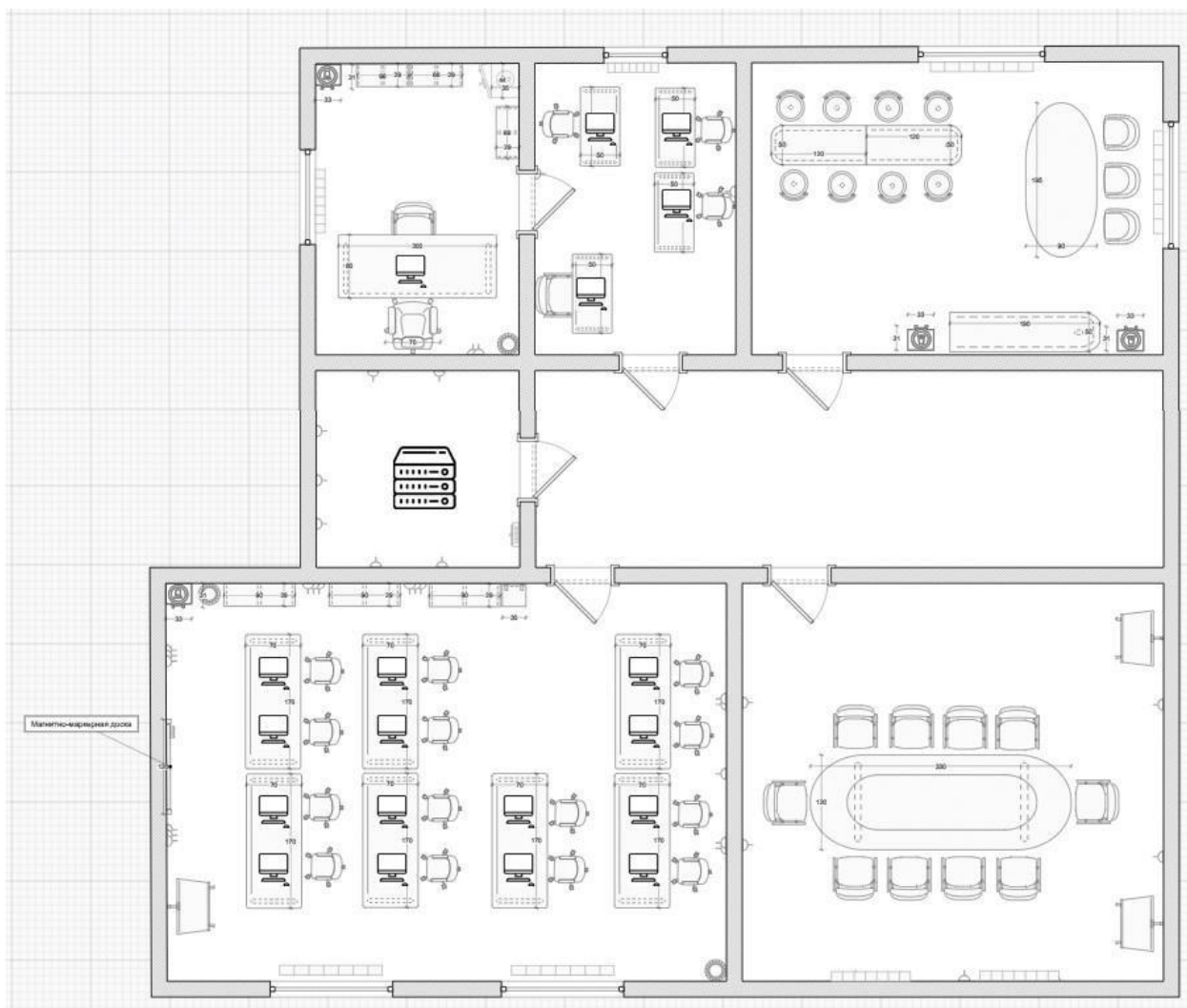




Рисунок 3 – План защищаемого помещения

Таблица 1 – Используемые обозначения

Обозначения	Описание
	Кресло руководителя
	АРМ



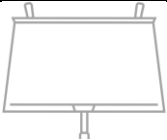







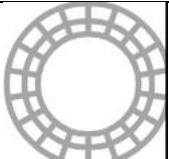

	Кресло для переговорной
	Офисное кресло
	Флипчарт
	Обеденный стол
	Барная стойка
	Кулер
	Офисный стол
	Барный стул
	Шкаф для бумаг
	Сейф
	Урна
	Тумбочка

Схема информационных потоков представлена на рисунке 4.

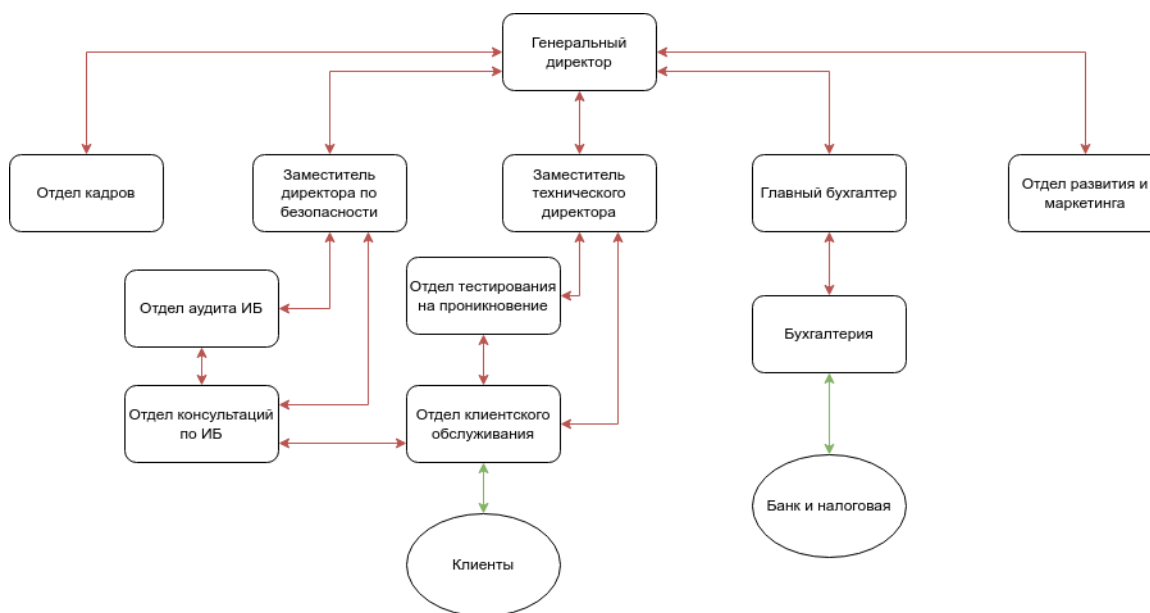


Рисунок 4 – Схема информационных потоков

3.1 Описание информационных потоков

Информация ограниченного доступа:

1. Персональные данные сотрудников – является информационным активом, представлены в электронной форме, владельцем является руководитель службы безопасности, отдел информационной безопасности.
2. Персональные данные клиентов - является информационным активом, представлены в электронной форме, владельцем являются сотрудники отдела по работе с клиентами с необходимым уровнем доступа
3. Конфигурация ПО клиентов - является информационным активом, представлена в электронной форме, владельцем являются сотрудники IT-отдела.
4. Техническая информация (логины, пароли, данной локальной сети и т. д.) - является информационным активом, представлены в электронной форме, владельцем являются сотрудники IT-отдела с необходимым уровнем доступа.
5. Коммерческая тайна (данные о производстве) – представлен в электронной форме, владельцем является владелец Организации.
6. Финансовые данные, данные о состоянии счетов, доходов и расходов – являются информационным активом, представлены в электронной форме, владельцем является главный бухгалтер.

Система имеет классификацию «секретно», т.е. к ней относятся все сведения, не

относящиеся к сведениям с грифом «особой важности» и «совершенно секретно», но составляющие государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-разыскной области деятельности.

3.2 Описание помещений

Защите подлежат следующие помещения:

- кабинет директора 9,49 м²;
- офис 9,39 м²;
- переговорная комната 26,84 м²;
- кофе-пойнт 19,28 м²;
- open space 35,68 м²;
- серверная 6,5 м²;
- коридор 20,05 м².

В переговорной комнате нет окон и средств вычислительной техники. Вход в кабинет директора осуществляется через бухгалтерию. В серверной нет окон.

В опенспейсе есть 7 рабочих столов, магнитно-маркерная доска, 14 офисных кресел, 2 окна с батареями центрального отопления, 17 розеток, есть 3 шкафа для бумаг, кулер, тумба, 2 мусорных корзины. Из средств вычислительной техники в помещении установлены ПЭВМ, включённые в локальную сеть. В кофепойнте есть 2 окна с батареями центрального отопления, 3 барных стола, 8 барных стульев, обеденный стол, 3 обеденных стула, кофемашина и кулер.

В бухгалтерии есть 1 окно с радиатором центрального отопления, 4 рабочих стола, 4 компьютерных стула, 4 ПЭВМ.

В кофепойнте есть 3 барных стойки, 8 барных стульев, обеденный стол, 3 обеденных стула, 2 кулера, 2 окна с радиаторами центрального отопления.

3.3 Анализ возможных утечек информации

Из-за расположения помещения на втором этаже возможен просмотр его извне, как с улицы, так и со стороны жилого дома с использованием оптических приборов, что создает потенциальную возможность утечки видовой информации.

Из-за возможности прослушивания помещения через открытые окна и форточки с помощью направленных микрофонов с улицы или из жилого дома, может произойти существует потенциальный акустический канал утечки информации.

При использовании лазерного микрофона в жилом доме для перехвата разговоров можно получить информацию о проводимых в помещении беседах через вибрации оконных стекол. Таким образом, существует еще один способ утечки акустической информации.

В помещениях присутствуют декоративные элементы (растения, кулер), где можно спрятать закладное устройство. В каждом помещении имеются розетки, а значит, актуальны электрического и электромагнитного каналов утечки информации. Также есть угроза снятия информации по вибрационному и оптическому каналам, а также акустическому, виброакустическому, акустоэлектрическому. Материально-вещественный канал утечки информации регулируется строгой политикой компании в отношении физических носителей информации, и в рамках курсовой работы не рассматривается.

3.4 Выбор средств защиты информации

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещение средствам защиты, приведенными в таблице 2.

Таблица 2 – Активная и пассивная защита

Канал утечки	Источники	Пассивная защита	Активная защита
Оптический	Окна, двери	Снизить освещенность защищаемого объекта и отражательные свойства	Средства сокрытия защищаемых объектов
Акустический, акустоэлектрический	Окна, двери, электрические сети, проводка и розетки	Звукоизоляция переговорной, фильтры для сетей электропитания	Звуко-подавление, защищенные акустические системы
Вибрационный, виброакустический	Батареи и все твердые поверхности помещений	Максимальное снижение уровня перехватываемого сигнала	Устройства вибрационного зашумления
Электромагнитный, электрический	Розетки, АРМы, бытовая техника	Экранирование, заземление, фильтрация, развязка	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.

Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита представляет собой:

- установка сетевых фильтров;
- установка усиленных дверей;
- дополнительную отделку переговорной комнаты и кабинета директора звукоизолирующими материалами

Активная защита представляет собой систему виброакустического зашумления. В таблице 3 приведён сравнительный анализ подходящих средства активной защиты помещений по виброакустическому каналу.

Таблица 3 – Сравнительный анализ средств активной защиты от утечки виброакустическому каналу

Модель	Диапазон воспроизводимого шумового сигнала	Характеристики	Цена, руб.
ЛГШ-403	180 ÷ 11 300 Гц	ЛГШ-403 обеспечивает защиту путем постановки широкополосной виброакустической шумовой помехи на потенциально опасные конструкции помещений. Виброакустические шумовые помехи создаются генератором и передаются на строительные конструкции через вибропреобразователи. Предусмотрена также возможность установки акустического излучателя для защиты закрытых воздушных объемов (воздуховодов, вентиляционных шахт и т.п.). ЛГШ-403 – одноканальный генератор шума.	19 400

ЛГШ-404	175 ÷ 11 200 Гц	Изделие представляет собой генератор шумовых помех и подключаемые к нему по линиям связи пассивные преобразователи – вибровозбудители «ЛВП-10» и акустические излучатели «ЛВП-2а». Генераторный блок оснащен двумя независимыми выходами, к каждому из этих выходов могут быть подключены преобразователи.	35 100
«СОНАТА-АВ» МОДЕЛЬ 4Б	175 Гц ÷ 11.2 кГц	Имеет ряд преимуществ перед "классическим" подходом - "центральный генератор + электроакустические преобразователи". Есть возможность подключения к одному питающему шлейфу. Это делает легче процесс проектирования и монтажа. Индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы. Улучшенная аппаратная настройка элементов модели 4Б позволяет связывать источник электропитания с другими для обмена информацией. Можно создать систему автоматического контроля всех элементов. Позволяет снизить время на конфигурирование и тестирование системы.	44 200

По результатам анализа была выбрана система Соната «АВ» модель 4Б, так как:

- есть возможность подключения к одному питающему шлейфу. Это делает легче процесс проектирования и монтажа;
- индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы;
- дает возможность создать систему автоматического контроля всех элементов
- имеет среднюю цену из представленных средств активной защиты, а также позволяет уменьшить затраты благодаря использованию единой линии связи и электропитания.

4.1 Устройства противодействия утечке информации 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.

4.2 Устройства противодействия утечке по электромагнитным и электрическим каналам

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. Устройства активной защиты представлены в таблице 4.

Таблица 4 – Сравнительный анализ средств активной защиты от утечки по электрическому и электромагнитному каналу утечки информации

Устройство	Характеристики	Цена (руб.)
Генератор шума СОНАТА-РС2	Предназначен для активной защиты объектов ВТ (объектов вычислительной техники) или, другими словами, переговорных помещений от утечки информации через линии электропитания и заземления. Отличается от прибора Соната-РС1 только наличием модуля ИК-управления, что позволяет дистанционное включение прибора с пульта управления. Тогда как Соната-РС1 включается только в розетку. Данный прибор больше не поставляется и заменен новой версией (Соната- РС3).	23 600




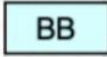

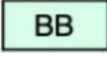
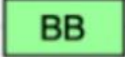
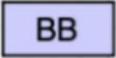

Генератор шума SEL SP-44	<p>Наличие сертификата ФСТЭК, разрешающего использование устройства в выделенных помещениях 3–1 категорий.</p> <p>2-канальный цифровой генератор шумовых сигналов в диапазоне 10кГц–400МГц.</p> <p>Активная защита конфиденциальных сведений от утечки по проводам электропитания.</p> <p>2 независимых друг от друга формирователей шума.</p> <p>Функция самодиагностики для оперативного выявления неисправностей и сбоев в работе.</p>	26 000
Генератор шума СОНАТА-РС3	<p>Устройство для активной защиты информации от утечки по сети электропитания.</p> <p>Предназначено для подключения к 3-проводной сети (энергосеть с проводом заземления).</p> <p>Звуковая и световая индикация работы.</p> <p>Возможно дистанционное управление посредством проводного пульта.</p> <p>Работа от сети 220В и 50Гц.</p> <p>Потребляемая мощность – 10Вт.</p> <p>Сертифицировано ФСТЭК.</p>	32 400
Генератор шума ЛГШ-221	<p>Сертификат ФСТЭК - «продлен до 2024 года».</p> <p>Сетевой генератор шума – средство защиты информации от утечки через электропроводку.</p> <p>Принцип работы – генерация электромагнитных помех.</p> <p>Устройство оснащено счетчиком отработанных часов.</p> <p>Устройство оснащено световым и звуковым индикаторами работы.</p> <p>Ресурс работы генератора шума – минимум 27000 часов.</p> <p>Возможность управления устройством с помощью пульта ДУ.</p>	36 400

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

По результатам сравнительного анализа в качестве средства активной защиты был выбран генератор шума Соната РС-3 из-за ее соотношения цены и качества, этот прибор является эффективным и недорогим, он имеет сертификат ФСТЭК. В качестве пассивной защиты был выбран сетевой фильтр ЛФС-10-1Ф, т.к. он имеет сертификат ФСТЭК и предназначен для работы с государственной тайной.

В таблице 5 представлена смета.

Таблица 5 – Смета

Наименование	Кол-во, шт.	Цена за единицу, руб.	Стоимость, руб	Обозначение
Рулонные жалюзи Blackout	6	1 773	10 638	
Усиленные звукоизолирующие двери Ultimatum PP	5	75 283	376 415	
Виброакустический генератор «Буран-2»	1	45 000	45 000	
Вибропреобразователь для стен «Молот» скреплением	18	3 000	54 000	
Вибропреобразователь для коммуникаций «Серп- Т» с креплением	8	3 000	24 000	
Вибропреобразователь для рам «Серп-Р» с креплением	6	3 000	18 000	
Вибропреобразователь для окон «Копейка» с креплением на раму окна	6	2 500	15 000	
Преобразователь акустический «Рупор»	4	2 000	8 000	
Модуль дистанционного управления по проводному каналу	1	4 500	4 500	

«Буран-ДУ»				
Размыкатель линий оповещения и сигнализации «Буран-К2»	1	3 400	3 400	РСЛ
Размыкатель компьютерных сетей «Буран-К3»	2	3 500	7 000	РЛЕ
Соната РС-3	4	32 400	129 600	РС3
ЛФС-10-1Ф	1	47 060	47 600	ЛФС

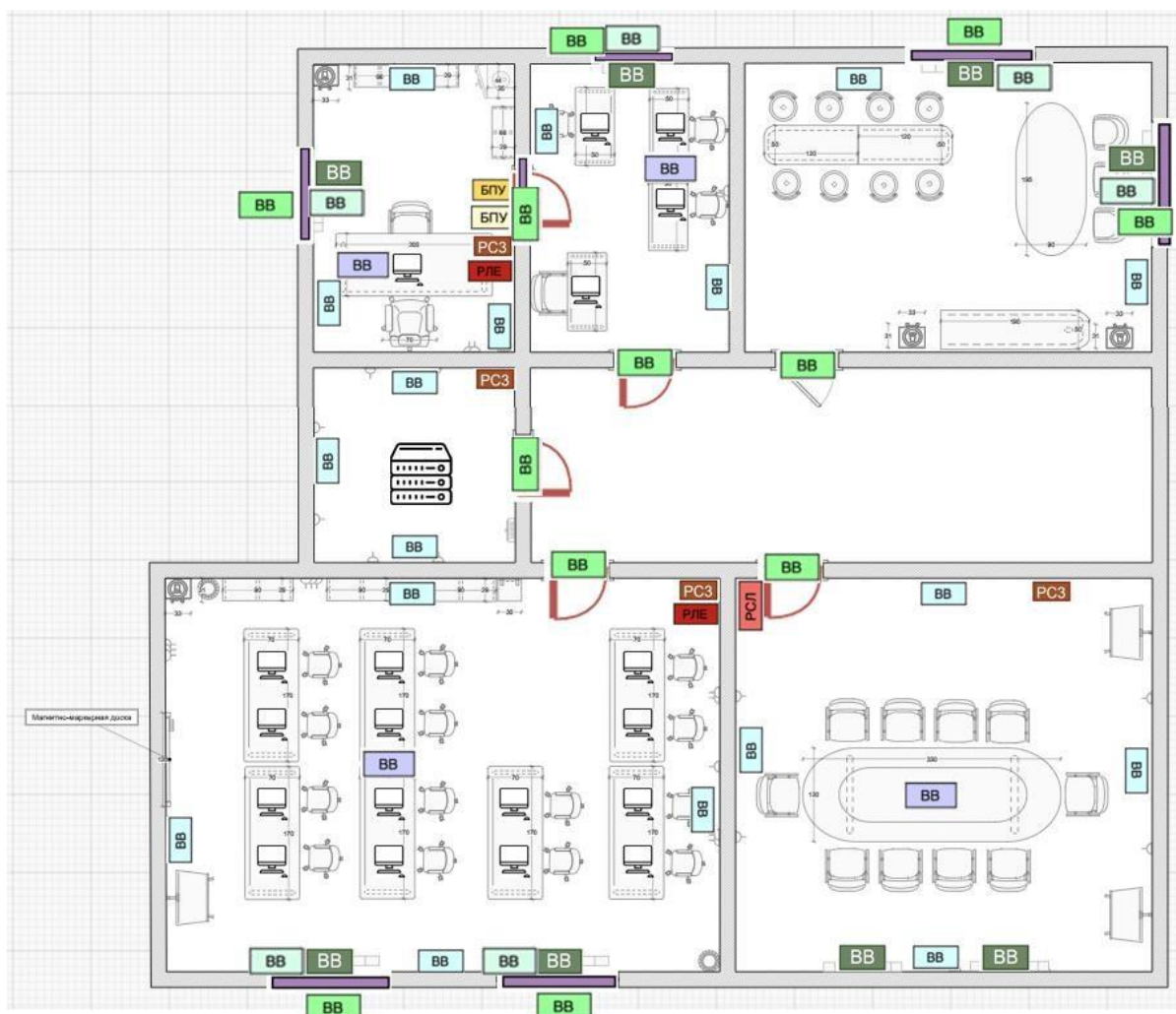


Рисунок 5 – Размещение средств защиты

ЗАКЛЮЧЕНИЕ

В результате выполнения данной работы был проведен теоретический анализ технических каналов утечки информации. Были рассмотрены такие технические каналы утечки связи, как оптический, акустический, радиоэлектронный и материально-вещественный. Далее были определены руководящие документы, а также проведен анализ защищаемых помещений для организации ООО «Sicurezza», проведена оценка каналов утечки информации и выбраны меры пассивной и активной защиты информации.

По итогам работы была составлена смета на основе действующих цен на технические средства защиты информации, итоговое значение суммы затрат составило 743 153 рубля. Кроме того, была нарисована схема расстановки устройств (рисунок 5).

ИСТОЧНИКИ

1. Утечки данных в России// Tadviser — URL: tadviser.ru/index.php/ Статья:Утечки_данных_в_России (дата обращения: 25.11.2023).
2. Утечки информации ограниченного доступа в мире 2022 г. // InfoWatch — URL: <https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichenogo-dostupa-v-mire-2022-g> (дата обращения: 01.12.2023).
3. Хорев А. А. Классификация и характеристика технических каналов утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи // Спецтехника. — 2018. — № 2. — С. 17-22.
4. Соколов, А. И. Технические средства защиты информации: технические каналы утечки информации : учеб. пособие /А. И. Соколов, М. Ю. Монахов ; Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2006 – 71 с. (Комплексная защита объектов информатизации. Кн. 13 / под ред. М. Ю. Монахова).
5. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения — URL: <https://docs.cntd.ru/document/1200075565> (дата обращения: 27.11.2023).
6. Виброакустический канал утечки информации // SearchInform — URL: <https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sluchai-utechki-informatsii/vibroakusticheskij-kanal-utechki-informatsii/> (дата обращения: 30.11.2023).
7. Хорев А. А. Способы защиты объектов информатизации от утечки информации по техническим каналам: защита цепей электропитания средств вычислительной техники // Спецтехника. — 2013. — № 1. — С. 30-37.