ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет безопасности информационных технологий

Дисциплина:

«Инженерно-технические средства защиты информации»

ОТЧЕТ ПО КУРСОВОЙ РАБОТЕ

«Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 135»

Выполнили:

студент группы N34521

Мариненков Максим Денисович

(подпись)

Проверил:

к.т.н., доцент ФБИТ

Попов Илья Юрьевич

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Мариненков Максим Денисович
(Фамилия И.О)

Факультет Безопасность информационных технологий

Группа N34521

Направление (специальность) Эксплуатация транспортно-технологических машин и комплексов

Руководитель Попов Илья Юрьевич
(Фамилия И.О)

Должность, ученое звание, степень Доцент ФБИТ, кандидат технических наук

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 135

Задание Проектирование инженерно-технической системы защиты информации на предприятии

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

Пояснительная записка включает разделы: введение, анализ технических каналов утечки информации, перечень руководящих документов, анализ защищаемых помещение, анализ рынка технических средств, описание расстановки технических средств, заключение, список литературы

Рекомендуемая литература

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Мариненков Максим Денисович
(Подпись, дата)

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

Студент Мариненков Максим Денисович
(Фамилия И.О)

Факультет Безопасность информационных технологий

Группа N34521

Направление (специальность) Эксплуатация транспортно-технологических машин и комплексов

Руководитель Попов Илья Юрьевич
(Фамилия И.О)

Должность, ученое звание, степень Доцент ФБИТ, кандидат технических наук

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 135

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1.	Разработка и утверждение задание и календарного плана на курсовую работу	20.09.2023	20.09.2023	
2.	Анализ теоретической составляющей	15.11.2023	15.11.2023	
3.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	10.12.2023	10.12.2023	
4.	Представление выполненной курсовой работы	19.12.2023	19.12.2023	

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Мариненков Максим Денисович
(Подпись, дата)

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент Мариненков Максим Денисович
(Фамилия И.О)

Факультет Безопасность информационных технологий

Группа N34521

Направление (специальность) Эксплуатация транспортно-технологических машин и комплексов

Руководитель Попов Илья Юрьевич
(Фамилия И.О)

Должность, ученое звание, степень Доцент ФБИТ, кандидат технических наук

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 135

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы Целью работы является повышение защищенности Рассматриваемого помещения. Задачами является анализ защищаемого помещения, анализ и оценка каналов утечки информации, и выбор мер пассивной и активной защиты информации

2. Характер работы Конструирование

3. Содержание работы 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 Мариненков Максим Денисович
(Подпись, дата)

«__» _____20__г.

Содержание

ЦЕЛИ И ЗАДАЧИ РАБОТЫ

Цель работы

Повышение защищенности рассматриваемого помещения.

Задачи работы

1. Проанализировать защищаемые помещения;
2. Оценить каналы утечки информации;
3. Выбрать меры пассивной и активной защиты информации;
4. Рассчитать стоимость применяемых мер

ВВЕДЕНИЕ

В настоящее время деятельность любого современного предприятия основана на обладании и управлении ресурсом информации. Из-за ценности этого ресурса он становится предметов внимания злоумышленников, которые пользуются широким перечнем устройств для получения несанкционированного доступа. Поэтому проблема утечки конфиденциальной информации является наиболее актуальной в области информационной безопасности

Средства защиты информации обеспечивают защиту информации в информационных системах, по сути, представляющих собой совокупность хранимой в базах данных информации, информационных технологий, обеспечивающих ее обработку, и технических средств. Они позволяют предотвратить несанкционированный доступ злоумышленника к ресурсам и данным предприятия, тем самым снизив риск несанкционированных утечки, утраты, искажения, уничтожения, копирования и блокирования информации и, как следствие, нанесения экономического, репутационного или других видов ущерба предприятию.

Объектом исследования являются защищаемые помещения.

Предметом исследования является безопасность информации ограниченного доступа.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно». Защищаемый объект состоит из одиннадцати помещений и представляет собой офис предприятия со следующими помещениями:

- комната охраны,
- кабинет директора,
- серверная,
- место отдыха,
- туалет,
- 4 офисных помещения,
- переговорная,
- общий зал.

Данная работа состоит из пяти глав. В первой главе произведен анализ технических каналов утечки информации. Во второй приведён перечень управляющих 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. Пятая глава посвященаразработке схем расстановки выбранных технических средств в защищаемом помещении.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечка информации — это неконтролируемое распространение информации за пределы организации, помещения, здания, какой-либо территории, а также определенного круга лиц, которые имеют доступ к этой информации. В случае обнаружения утечки важно своевременно ее ликвидировать, но лучше всего заранее принять превентивные меры по защите информации с ограниченным доступом.

Канал утечки информации (или технический канал утечки) – это путь информации, который она может пройти от источника информации до приемника/получателя в процессе случайной утечки или целенаправленного несанкционированного получения закрытой информации. Если меры по защите информации не были приняты заранее, то могут быть задействованы любые каналы утечки. Если же защита информации предусмотрена – то будет задействован наиболее слабозащищенный канал.

В природе существуют только 4 средства переноса информации – это световые лучи, звуковые волны, электромагнитные волны, а также материальные носители (бумага, фото, магнитные носители и т.д.). Эти средства являются составляющими любой системы связи, в которой помимо них обязательно присутствуют:

- Источник информации;
- Передатчик;
- Канал передачи информации;
- Приемник;
- Получатель сведений.

Непосредственно сам человек может стать инициатором (намеренным или случайным) утечки информации, используя одно или несколько вышеназванных средств переноса информации. Поэтому работу некоторых систем связи необходимо контролировать, чтобы, с одной стороны, обеспечить безопасную, надежную и точную передачу информации, а с другой, защитить ее от незаконного доступа. И если канал должным образом не защищен, и передача информации из исходной точки в другую происходит без ведома источника, то такой канал можно называть каналом утечки информации.

Выделяются четыре основные группы утечки информации:

- визуально-оптические, позволяющие перехватывать или копировать сведения, отражающиеся в визуальной форме, это документы, информация, выведенная на экран монитора компьютера;

- акустические, позволяющие перехватывать ведущиеся в помещении переговоры или разговоры по телефонам;
- электромагнитные, позволяющие получать данные, выраженные в виде излучения электромагнитных волн, их дешифровка может также дать необходимые сведения;
- материально-вещественные, связанные с анализом предметов, документов и отходов, возникших в результате деятельности компании.

Защита от утечки информации требует проведения обязательных организационных и технических мер, которые позволят выявить вероятные технические каналы утечки информации, чтобы избежать их возможного использования. Рассмотрим более подробно каждую группу технических способов организации утечки информации.

1.1 Визуально-оптические каналы

Если экран монитора или часть лежащих на столе документов можно увидеть через окно офиса, возникает риск утечки. В качестве защиты от утечки информации по визуально-оптическому каналу следует снизить освещенность защищаемого объекта и его отражательные свойства, использовать различные пространственные ограждения (ширмы, экраны, шторы, ставни, темные стекла), применять специальную маскировку и средства сокрытия защищаемых объектов (аэрозольные завесы, сетки, краски, укрытия).

1.2 Акустические каналы

В акустических каналах утечки информации средой распространения речевых сигналов является воздух, и для их перехвата используются высокочувствительные микрофоны и специальные направленные микрофоны. Микрофоны соединяются с портативными звукозаписывающими устройствами или специальными миниатюрными передатчиками.

Автономные устройства, конструктивно объединяющие микрофоны и передатчики, называют закладными устройствами (ЗУ) перехвата речевой информации.

Перехваченная ЗУ речевая информация может передаваться по радиоканалу, сети электропитания, оптическому (ИК) каналу, соединительным линиям, посторонним проводникам, инженерным коммуникациям в ультразвуковом (УЗ) диапазоне частот, телефонной линии с вызовом от внешнего телефонного абонента.

Прием информации, передаваемой ЗУ, осуществляется, как правило, на специальные приемные устройства, работающие в соответствующем диапазоне длин волн. Однако существуют исключения из этого правила. Так, в случае передачи информации по

телефонной линии с вызовом от внешнего абонента прием можно осуществлять с обычного телефонного аппарата.

1.3 Электромагнитные каналы

Представляет опасность также перехват информации, содержащейся в побочных электромагнитных излучениях и наводках (ПЭМИН). Электромагнитные волны могут исходить от любого электрического прибора, установленного в помещении.

Ключевым способом защиты от утечки информации по электромагнитным каналам считается экранирование аппаратуры и ее элементов. Электростатическое, магнитостатическое и электромагнитное экранирование позволяет предохранить объект от воздействия и электромагнитных, и акустических сигналов. Таким образом, оно обеспечивает надежную защиту информации от утечки по ПЭМИН.

1.4 Материально-вещественные каналы

Материально-вещественные каналы также нуждаются в защите, так как различные материальные носители могут содержать в себе важнейшую секретную информацию. К примеру, любое производственное предприятие имеет отходы, в которых могут содержаться различные испорченные документы, бракованные детали, жидкости или газообразные вещества, и часто они бесконтрольно отправляются за пределы контролируемой зоны. Основные меры борьбы с этими рисками относятся исключительно к административно-организационной сфере, хотя существуют программные средства, которые не дают возможности сделать скриншот данных, выводимых на экран монитора.

2 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ

Перечень основных руководящих документов в области защиты информации включает в себя:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

3. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

4. Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;

5. Приказ ФСТЭК «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644;

6. Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;

7. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

8. Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;

9. Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»;

10. Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1;

11. 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:

1. СТР. Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам;

2. СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации;

3. Временный порядок аттестации объектов информатизации по требованиям безопасности информации;

4. РД. Защита от несанкционированного доступа к информации. Термины и определения;

5. РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;

6. РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации;

7. РД. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации;

8. РД. Защита информации. Специальные защитные знаки. Классификация и общие требования;

9. РД Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей;

10. РД. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

3 АНАЛИЗ ЗАЩИЩЕМЫХ ПОМЕЩЕНИЙ

3.1 План помещений и информационные потоки предприятия

Перед началом проектирования инженерно-технической защиты помещений необходимо изучить все открытые и закрытые информационные потоки.

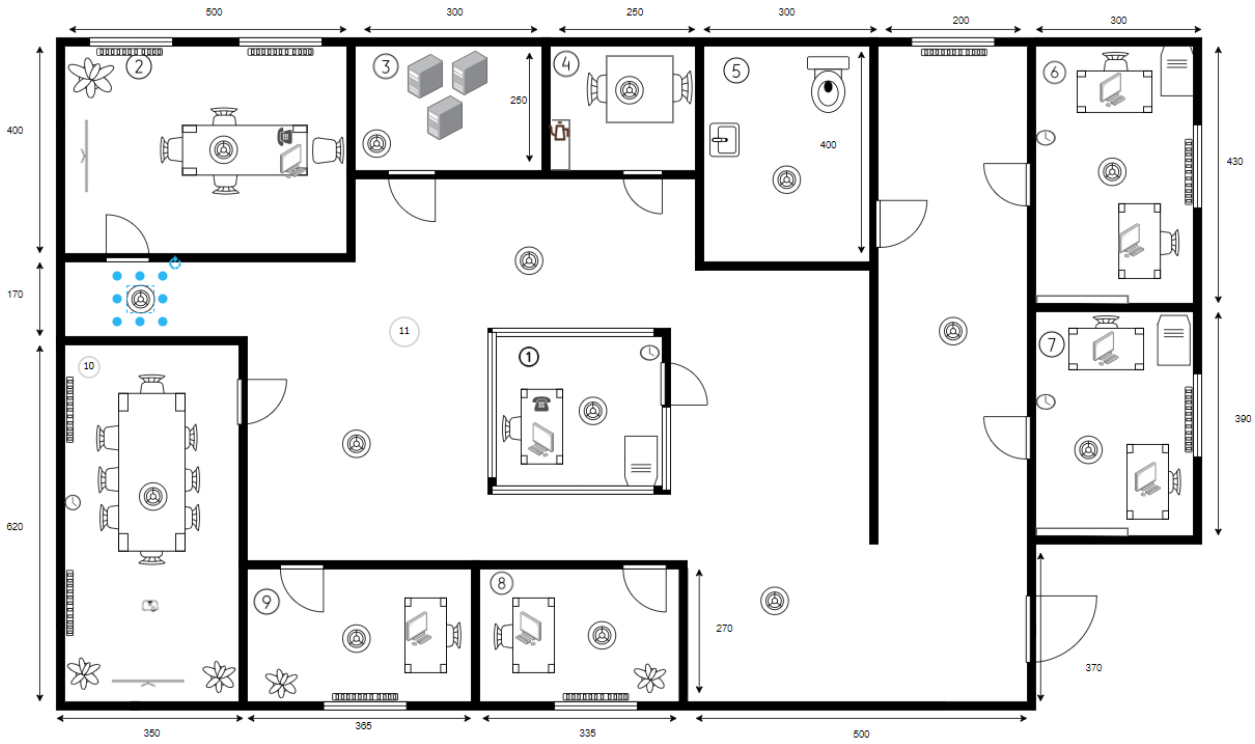

Рисунок 1 – План защищаемого помещения

Рисунок 2 – Легенда защищаемого помещения

Составим схему информационных потоков Организации.

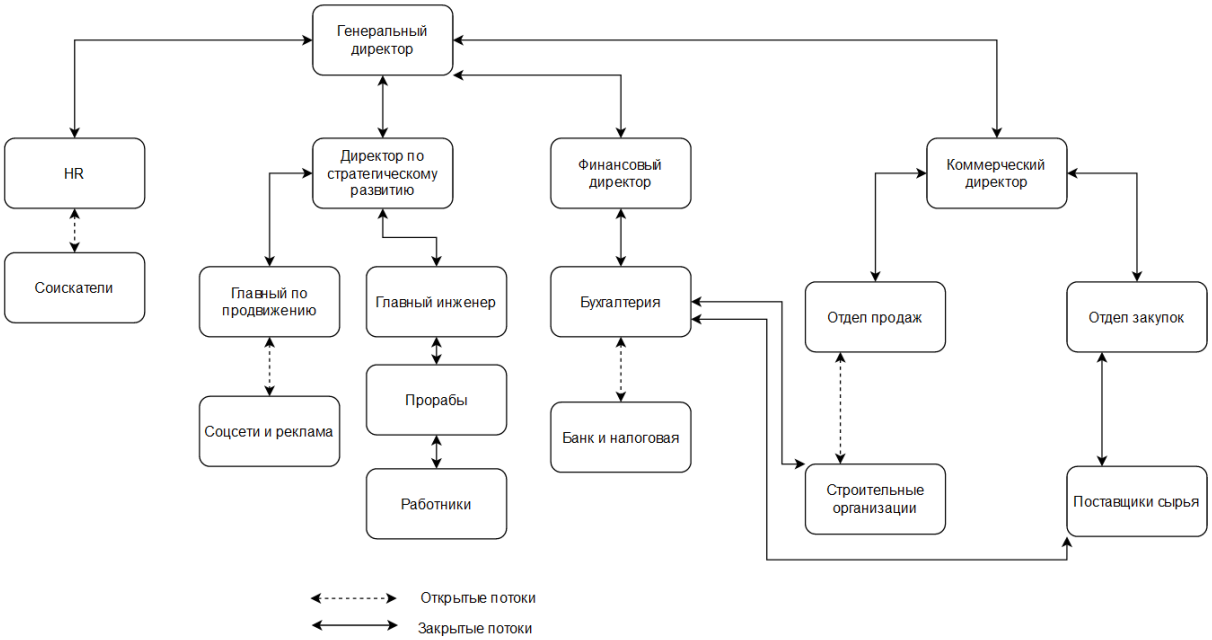

Рисунок 3 – Информационные потоки организации

Государственную тайну в Организации представляют информационные потоки между директором по стратегическому развитию и главным инженером, а также данные о поставщиках сырья. Компания выполняет оборонные заказы, поэтому поставщики и технологии производства остаются засекреченными.

3.2 Описание помещений

Защите подлежат следующие помещения

- Кабинет директора, 5м × 4м (20м^2);
- Переговорная, 6.2м × 3.5м (21.7м^2);
- Офис 8, 3.65м × 2.7м (9.8м^2);
- Офис 9, 3.35м × 2.7м (9м^2);
- Серверная, 3м × 2.5м (7.5м^2);
- Комната охраны, 3.5м × 3.5м (12.25м^2);

В кабинете директора расположены стол, четыре стула, растение, телефон, компьютер, телевизор. В помещении есть два окна, две батареи и одно вентиляционное отверстие в потолке.

В переговорной расположен стол, 8 стульев, часы, два растения, проектор и телевизор. Окон в помещении нет. Есть две батареи и одно вентиляционное отверстие в потолке.

В офисе 9 расположен стол, стул, компьютер, растение. В помещении есть одно окно, одна батарея и вентиляционное отверстие в потолке.

В офисе 8 расположен стол, стул, компьютер, растение. В помещении есть 1 окно, 1 батарея и одно вентиляционное отверстие в потолке.

В серверной расположено 3 сервера. Окон в помещении нет. Есть вентиляционное отверстие в потолке.

Комната охраны представляет собой стойку регистрацией, есть стол, стул, телефон, шкаф. Окон в помещении нет. Есть вентиляционное отверстие в потолке.

Офис расположен на втором этаже двухэтажного 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. Защищаемые помещения размещены в «непроходной» 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.

3.3 Анализ возможных утечек информации

В помещениях присутствуют декоративные элементы, батареи и вентиляция, в которых можно спрятать закладное устройство. В каждом помещении имеются розетки, сетевые устройства, а значит, актуальны электрический и электромагнитный каналы 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 информационной безопасности 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 (Таблица 1).

Таблица 1 – Виды уязвимых каналов и применяемые меры по защите

Каналы	Источники	Пассивная защита	Активная защита
Акустический	Окна, двери, электрические сети, проводка	Звукоизоляция помещений, фильтры для сетей ЭП	Устройства акустического зашумления
Вибрационный, виброакустический	Батареи и все твердые поверхности помещений	Изоляция поверхностей с помощью дополнительных обшивок	Устройства вибрационного зашумления
Оптический	Окна, двери	Жалюзи на окнах, доводчики на дверях	Маскирующие средства сокрытия объектов
Электромагнитный, электрический	Розетки, АРМ, любая техника	Фильтры для сетей питания, экранирующие материалы, помехоподавляющие фильтры	Устройство ЭМ зашумления

4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

4.1 Требования к защите помещений

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
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.

4.2 Анализ СЗИ для акустического, вибрационного и виброакустического каналов

В качестве пассивной защиты от утечки информации по виброакустическим каналам утечки информации были выбраны усиленные звукоизоляционные двери, а также

дополнительная звукоизоляционная отделка переговорного помещения и кабинета директора.

Активная защита представляет собой систему виброакустического зашумления. Для защиты помещения для работы с государственной тайной уровня «секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1В. Проведем сравнительный анализ подходящих средств активной защиты помещений по виброакустическому каналу (Таблица 2).

Таблица 2 – Сравнительные анализ средств активной защиты от утечки по виброакустическому каналу

Устройство	Цена	Описание	Назначение
Система «Кабинет»	30 000	Система состоит из генератора шума с независимой регулировкой уровня сигнала в октавных полосах 250, 500, 1000, 2000 и 4000 Гц, блоков расширения, обеспечивающих независимую регулировку АЧХ спектра шумового сигнала и суммирование его (опция) с дополнительным шумовым сигналом со спектром до 10 кГц, и подключаемых к генератору и блокам расширения стенных и оконных вибраторов, а также акустических систем.	Система предназначена для предотвращения утечки информации из защищаемых помещений по акустическому и виброакустическому канала
Система виброакустической защиты ШТОРМ-7	32 000	Состав системы: трехканальный прибор виброакустической защиты SI - 3010 электромагнитные излучатели TRN -2000 для формирования помехи в стенах и перекрытиях помещения виброакустические преобразователи ВД-1 для	Система спроектирована с учетом многолетнего опыта производства приборов виброакустического зашумления и предназначена для защиты выделенных

		формирования помехи в оконных стеклах, системе отопления и вентиляции помещения акустические излучатели OMS-2000	помещений 1-й категории.
Соната АВ-4Б	40 000	Изделия "Соната-АВ" модель 4Б является построение по принципу "единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)". Состав: Блоки электропитания и управления – Соната-ИП4.1, Соната-ИП4.2, Соната-ИП4.3; Генераторы-акустоизлучатели – СА-4Б, СА-4Б1; Генератор-вибровозбудитель – СВ-4Б Размыкатель телефонной линии – Соната-ВК4.1; Размыкатель слаботочной линии – Соната-ВК4.2; Размыкатель линии Ethernet – Соната-ВК4.3; Пульт управления – Соната-ДУ4.3; Блоки сопряжения с внешними устройствами – Соната-СК4.1, Соната-СК4.2; Техническое средство защиты речевой информации от утечки по оптико-электронному (лазерному) каналу – "Соната-АВ4Л": Генераторный блок "АВ-4Л" + вибровозбудитель "СП-4Л"; Аксессуары – фиксатор труба, фиксатор стена, кабель.	Система защиты речевой информации от утечки по техническим каналам "Соната-АВ" модель 4Б, предназначена для защиты речевой информации в выделенных помещениях, от утечки по акустическим, виброакустическим, акустоэлектрическим и оптико-электронным (лазерным) каналам.

В результате проведенного анализа средств защиты в качестве системы виброакустической защиты была выбрана «Соната АВ-4Б». Данная система имеет сертификат ФСТЭК, достаточную комплектацию и приемлемую стоимость. Улучшенная аппаратная настройка элементов модели «Соната АВ-4Б» позволяет связывать источник электропитания с другими для обмена информацией. Это дает возможность создать гибкую систему с меньшими затратами на электропитание.

4.3 Анализ СЗИ для электромагнитного, электрического каналов

В качестве пассивной защиты от утечки информации по электромагнитным каналам утечки информации могут быть выбраны сетевые помехоподавляющие фильтры.

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

Таблица 3 – Сравнительные анализ средств активной защиты информации для электромагнитного и электрического каналов

Устройство	Цена	Описание	Назначение
SEL 111 «Шифон»	64 000	Сертификат ФСБ Применение теплового источника шума с цифровой обработкой позволяет получить равномерный линейный спектр шумового сигнала во всем диапазоне частот. Раздельные регулировки выходного уровня шума по диапазонам позволяет оптимальным образом сформировать «защитную помеху», снижая уровни паразитных электромагнитных излучений (соблюдение норм ГКРЧ, СанПин, требований по ЭМС). Цифровое автономное (защищённое паролем) управление и контроль за настройками системы с выводом информации на встроенный ЖК экран. Возможность удалённого управления по сети Ethernet позволяет объединять	Средство активной защиты информации от утечки за счёт ПЭМИН

		устройства в единую сеть для формирования распределенной системы защиты информации любого объекта. Наличие встроенного счётчика суммарного времени наработки генератора помех с регистрацией значений в защищённой энергонезависимой памяти. Распределённая система контроля и индикации нормального режима работы или возникновения аварийной ситуации в элементах системы (визуальная, звуковая, текстовая). Применение одной плоской сверхширокополосной антенны SEL SP-111RA позволяет существенно сократить время установки и настройки системы. Предусмотрена возможность как горизонтального, так и настенного крепления генераторного блока и антенн.	
Система «Стикс-4»	44 000	Система осуществляет защиту информации от утечек за счет: побочных электромагнитных излучений путем создания в диапазоне частот 0,01 - 1800 МГц электромагнитного поля маскирующего шума вокруг технических средств и подключенных к ним периферийных устройств, цепей электропитания и кабелей передачи данных; за счет наведения шумового маскирующего электрического сигнала в отходящие от СЗИ «Стикс-4» линии электропитания и заземления, а также в	предназначена для активной защиты объектов вычислительной техники от утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН) на объектах до 2-ой категории включительно.

		токопроводящие линии и инженерно-технические коммуникации в диапазоне частот 0,01 - 400 МГц.	
SEL SP-44	24 000	Цифровое автономное управление и контроль за настройками с защитой от несанкционированного доступа и выводом информации на встроенный жидкокристаллический экран. Применение двух некоррелируемых формирователей шума для цепей «фаза»-«земля» и «ноль»-«земля» позволяет исключить возможность съёма информационного сигнала как для противофазной, так и для синфазной схем подключения.	предназначено для защиты информации, обрабатываемой техническими средствами и системами, путём формирования шумового сигнала маскирущих помех в цепях электропитания и заземления.
Соната Р3.1	33 120	"Соната-Р3.1" может комплектоваться следующими дополнительными опциями: Антенна "Веер" (применяется для повышения уровней электромагнитного поля шума (ЭМПШ) в диапазоне частот 0,01…200 МГц) (рис. 3); (индивидуальный) пульт управления "Соната-ДУ4.4" Изделие может быть включено в состав комплекса ТСЗИ. В этом случае управление его работой и контроль режима работы (исправности) будет осуществляться от пульта управления "Соната-ДУ4.3" в комплексе с блоком питания "Соната-ИП4.х" (Комплекс 3095, Комплекс 3109).	Средство активной защиты информации "Соната-Р3.1" предназначено для защиты информации от утечки за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и токоведущие проводные коммуникации.

			"Соната-Р3.1" обеспечивает защиту путем излучения в окружающее пространство электромагнитного поля шума, а также инжекции шумовых токов в линии сети электропитания и заземления.

В результате проведенного анализа в качестве средства защиты от утечки по электрическому каналу была выбрана «СОНАТА-Р3.1». Данное средство имеет сертификат ФСТЭК и приемлемую стоимость. ПЭМИН «Соната-Р3.1» обеспечивает защиту информации от утечки за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума, а также наводок на линии сети электропитания и заземления путем индуцирования в них маскирующих шумовых напряжений.

4.4 Анализ СЗИ для визуально-оптического канала

В качестве пассивной защиты визуально-оптического канала были выбраны средства преграждения или значительного ослабления отраженного света, то есть шторы, жалюзи, темные стекла и др. Более удобны в эксплуатации рулонные шторы или жалюзи полного перекрытия проникновения света (ткани BlackOut).

Были выбраны рулонные шторы с технологией BlackOut 80 см * 250 см 1845 руб/шт.

5 РАССТАНОВКА ТЕХНИЧЕСКИХ СРЕДСТВ

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

- Усиленные двери (толще 4мм), обшитые металлом (не менее 2 мм) со звукоизолирующей прокладкой на металлическом каркасе.
- Соната АВ-4Б
- Соната Р3-1
- BlackOut жалюзи на окна.

Было решено установить 5 усиленных дверей (переговорная, кабинет директора, серверная, офис 8 и 9), 4 рулонных шторы на каждое окно в нужные помещения. Также была использована звукоизоляционная отделка для 4 помещений (кабинет директора, переговорная, офис 8 и 9) общей площадью стен 180.6 $м^2$, следовательно, необходимо выделить 25 рулонов отделки.

Перейдём к оценке количества компонентов и расстановке выбранных технических средств. «Соната АВ-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 $м^2$ 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 «СВ-4Б1» можно предварительно оценить из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8–12 $м^3$ надпотолочного пространства или других пустот.

По результатам выбора средств защиты информации от утечки составим смету (Таблица 4).

Таблица 4 – Смета

Мера защиты	Цена, руб.	Количество, шт.	Стоимость, руб.
Блок электропитания и управления «Соната-ИП4.3»	21 600	1	21 600
Генератор-акустоизлучатель «СА-4Б1»	7 440	7	52 080
Генератор-вибровозбудитель «СВ-4Б1»	7 440	16	119 040
Пульт управления «Соната-ДУ4.3»	7 700	1	7 700
Генераторный блок «АВ-4Л»	10 320	1	10 320
Размыкатель телефонной линии «Соната-ВК4.1»	6 000	2	12 000
Размыкатель Слаботочной линии «Соната-ВК4.2»	6 000	1	6 000
Размыкатель линии Ethernet "Соната-ВК4.3"	6 000	2	12 000
Средство активной защиты информации от утечки за счет ПЭМИН "Соната-Р3.1"	33 120	1	33 120
Жалюзи BlackOut	1845	4	7 380

Усиленные двери «КД-3»	72 900	5	364 500
Звукоизоляционная отделка	390	25	9750
Итого			655 490

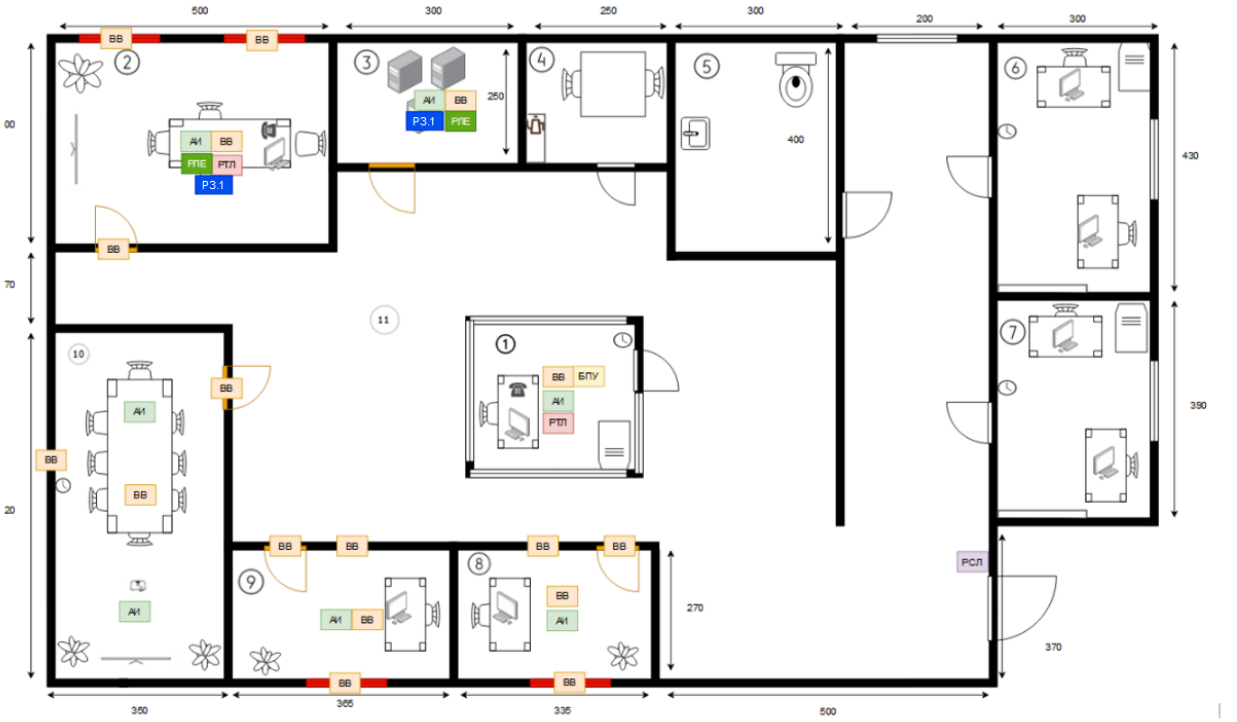

Рисунок 4 – Схема расстановки технических средств

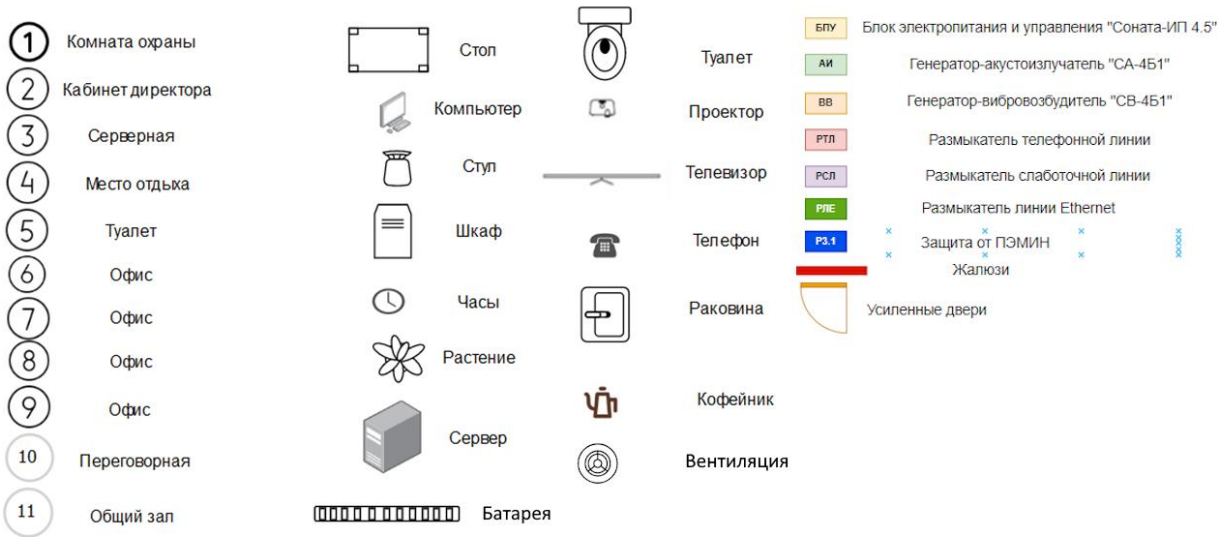

Рисунок 5 – Легенда рисунка 4

ЗАКЛЮЧЕНИЕ

В рамках данной работы был проведен теоретический обзор существующих каналов утечки информации, а также произведен анализ потенциальных каналов утечки в защищаемом помещении и описаны меры их защиты. Был проанализирован рынок технических средств для борьбы с утечками информации и выбраны наиболее подходящие для данного объекта. Был разработан план установки и рассчитана стоимость предложенных средств защиты информации. В результате была создана защита от утечек информации по различным техническим каналам, включая акустический, виброакустический, оптический, акустоэлектрический, электрический, электромагнитный и оптико-электронный, а также обеспечена защита от ПЭМИН.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Способы предотвращения утечки информации | Способы и средства защиты информации от утечки по техническим каналам - SearchInform. Дата просмотра: 20.11.2022 searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sposoby-predotvrascheniya-utechki- informatsii/.
2. Каналы утечки информации на предприятии - SearchInform. Дата просмотра: 20.11.2022 searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sluchai-utechki-informatsii/kanaly-utechki-informatsii-na-predpriyatii/.
3. Угрозы информационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности информации. Защита информации от утечки по техническим каналам. Дата просмотра: 20.11.2022
4. learn.urfu.ru/resource/index/data/resource_id/40977/revision_id/0.
5. Государственный реестр сертифицированных средств защиты информации // ФСТЭК РОССИИ [Электронный ресурс]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/15 3-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zash chity-informatsii-n-ross-ru-0001-01bi00. (дата обращения: 28.11.2022).
6. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.
7. Мещеряков Р. В., Шелупанов А. А., Зайцев А. П. Технические средства и методы защиты информации. – 2007.
8. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
9. 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.
10. 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: 28.11.2022).