

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

Факультет безопасности информационных технологий

Дисциплина:

«Инженерно-технические средства защиты информации»

КУРСОВАЯ РАБОТА

на тему

«Проектирование инженерно-технической системы защиты информации на предприятии»

Выполнила:

Нгуен Хонг Хань, студентка группы N34481

(подпись)

Проверил:

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

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Нгуен Хонг Хань

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34481

Направление (специальность) 10.03.01 (Технологии защиты информации 2020)

Руководитель Попов Илья Юрьевич, к.т.н., доцент факультета безопасности информационных технологий

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

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 помещений, анализ рынка технических средств, расстановка технических средств, заключение, список использованных источников.

Рекомендуемая 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

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Нгуен Хонг Хань

(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Нгуен Хонг Хань

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34481

Направление (специальность) 10.03.01 (Технологии защиты информации 2020)

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

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	15.11.2023	15.11.2023	
2	Анализ теоретической составляющей	01.12.2023	01.12.2023	
3	Разработка комплекса инженернотехнической 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 Нгуен Хонг Хань

(Подпись, дата)

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

Студент Нгуен Хонг Хань

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34481

Направление (специальность) 10.03.01 (Технологии защиты информации 2020)

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

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

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

Введение; Анализ технических каналов утечки информации; Перечень руководящих документов; Анализ защищаемого помещения; Анализ рынка технических средств; Расстановка технических средств; Заключение;

Список использованных источников

4. Выводы

В результате работы была предложена защита от утечек информации по акустическому, оптико-виброакустическому, оптическому, акустоэлектрическому, электрическому, электромагнитному, электронному техническим каналам защиты информации, обеспечена защита от ПЭМИН.

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Нгуен Хонг Хань

(Подпись, дата)

«__» _____ 20
____ г.

СОДЕРЖАНИЕ

Введение	7
1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ.....	8
1.1 Визуально-оптические	9
1.2 Акустические	9
1.3 Электромагнитные.....	9
1.4 Материально-вещественные.....	10
2 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ.....	11
3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	13
3.1 Общая информация о предприятии	13
3.2 Описание помещения	13
3.3 Анализ возможных утечек информации и выборы СЗИ	16
4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ.....	18
4.1 Анализ СЗИ для акустического и виброакустического каналов	19
4.2 Анализ СЗИ для визуально-оптического канала	22
4.3 Анализ СЗИ для электромагнитного каналов.....	23
4.3.1 Экранирование электромагнитных волн	23
4.3.2 Заземление технических систем.....	24
4.3.3 Разделительные трансформаторы и помехоподавляющие фильтры.	24
4.3.4 Пространственное и линейное зашумление.....	25
5 РАССТАНОВКА ТЕХНИЧЕСКИХ СРЕДСТВ	28
Заключение.....	31
Список литературы.....	32

ВВЕДЕНИЕ

В современном информационном обществе защита информации является одной из первостепенных задач для любого предприятия. Утечка или несанкционированный доступ к конфиденциальным данным может привести к серьезным негативным последствиям, включая финансовые потери, утрату репутации и нарушение законодательных требований. В связи с этим, проектирование и разработка инженерно-технической системы защиты информации становятся критически важными задачами для предприятий.

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

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

В рамках работы проведен анализ технических каналов утечки информации, где проводится детальный анализ различных каналов, через которые информация может быть украдена или раскрыта несанкционированным образом. Этот анализ позволяет определить уязвимости и потенциальные угрозы информационной безопасности. Во второй главе приводится обзор основных нормативных актов, которые регулируют область защиты информации на предприятии. Анализ защищаемого помещения осуществляется в третьей главе. Далее проводится обзор существующих технических средств и решений, доступных на рынке, которые могут быть использованы для защиты информации в рассматриваемом помещении. В последней главе определяются места и способы размещения выбранных технических средств в помещении, чтобы обеспечить наибольшую эффективность и защиту информации.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Технический канал утечки информации (ТКУИ) - совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка - бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

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

Существуют определенные условия, при которых возможно образование системы передачи информации из одной точки в другую независимо от желания объекта и источника. При этом, естественно, такой канал в явном виде не должен себя проявлять. По аналогии с каналом передачи информации такой канал называют каналом утечки информации. Он также состоит из источника сигнала, физической среды его распространения и приемной аппаратуры на стороне злоумышленника. Движение информации в таком канале осуществляется только в одну сторону — от источника к злоумышленнику. На рис. 1 приведена структура технического канала утечки информации.



Рисунок 1 – Структура технического канала утечки информации

Применительно к практике с учетом физической природы образования каналы утечки информации можно разделить на следующие группы:

- визуально-оптические;
- акустические (включая и акустико-преобразовательные);
- электромагнитные (включая магнитные и электрические);
- материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида — твердые, жидкие, газообразные).

Каждому виду каналов утечки информации свойственны свои специфические особенности.

1.1 Визуально-оптические

Визуально-оптические каналы — это, как правило, непосредственное или удаленное (в том числе и телевизионное) наблюдение. Переносчиком информации выступает свет, испускаемый источником конфиденциальной информации или отраженный от него в видимом, инфракрасном и ультрафиолетовом диапазонах.

1.2 Акустические

Для человека слух является вторым по информативности после зрения. Поэтому одним из довольно распространенных каналов утечки информации является акустический канал. В акустическом канале переносчиком информации выступает звук, лежащий в полосе ультра (более 20 000 Гц), слышимого и инфразвукового диапазонов. Диапазон звуковых частот, слышимых человеком, лежит в пределах от 16 до 20 000 Гц, и содержащихся в человеческой речи — от 100 до 6000 Гц.

Когда в воздухе распространяется акустическая волна, частицы воздуха приобретают колебательные движения, передавая колебательную энергию друг другу. Если на пути звука нет препятствия, он распространяется равномерно во все стороны. Если же на пути звуковой волны возникают какие-либо препятствия в виде перегородок, стен, окон, дверей, потолков и т. п., звуковые волны оказывают на них соответствующее давление, приводя их также в колебательный режим. Эти воздействия звуковых волн и являются одной из основных причин образования акустического канала утечки информации.

Различают определенные особенности распространения звуковых волн в зависимости от среды. Это прямое распространение звука в воздушном пространстве, распространение звука в жестких средах (структурный звук). Под структурным звуком понимают механические колебания в твердых средах. Механические колебания стен, перекрытий или трубопроводов, возникающие в одном месте, передаются на значительные расстояния, почти не затухая. Опасность такого канала утечки состоит в неконтролируемой дальности распространения звука.

1.3 Электромагнитные

Электромагнитный канал утечки информации — физический путь от источника побочных электромагнитных излучений и наводок различных технических средств к злоумышленнику за счёт распространения электромагнитных волн в воздушном пространстве и направляющих системах.

Переносчиком информации являются электромагнитные волны в диапазоне от сверхдлинных с длиной волны 10 000 м (частоты менее 30 Гц) до субмиллиметровых с длиной волны 1 - 0,1 мм (частоты от 300 до 3000 ГГц). Каждый из этих видов электромагнитных волн обладает специфическими особенностями распространения как по дальности, так и в пространстве. Длинные волны, например, распространяются на весьма большие расстояния, миллиметровые — наоборот, на удаление лишь прямой видимости в пределах единиц и десятков километров. Кроме того, различные телефонные и иные провода и кабели связи создают вокруг себя магнитное и электрическое поля, которые также выступают элементами утечки информации за счет наводок на другие провода и элементы аппаратуры в ближней зоне их расположения.

1.4 Материально-вещественные

Материально-вещественными каналами утечки информации выступают самые различные материалы в твердом, жидком и газообразном или корпускулярном (радиоактивные элементы) виде. Очень часто это различные отходы производства, бракованные изделия, черновые материалы и другое.

2 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ

Основными указами Президента Российской Федерации в области предотвращения утечки информации по техническим каналам являются:э

- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644.
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.

Основными постановлениями Правительства Российской Федерации в области предотвращения утечки информации по техническим каналам являются:

- Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»;
- Постановление Правительства РФ от 1 ноября 2012 г. No 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

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.

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Общая информация о предприятии

Объектом защиты является фирма ООО «Vagrant», занимающаяся предоставлением услуг по ИБ (включая услуги тестирования на проникновение, услуги аудита ИБ, консультационные ИБ услуги). Организация имеет вторую степень секретности информации («совершенно секретно»).

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа (рисунок 2).

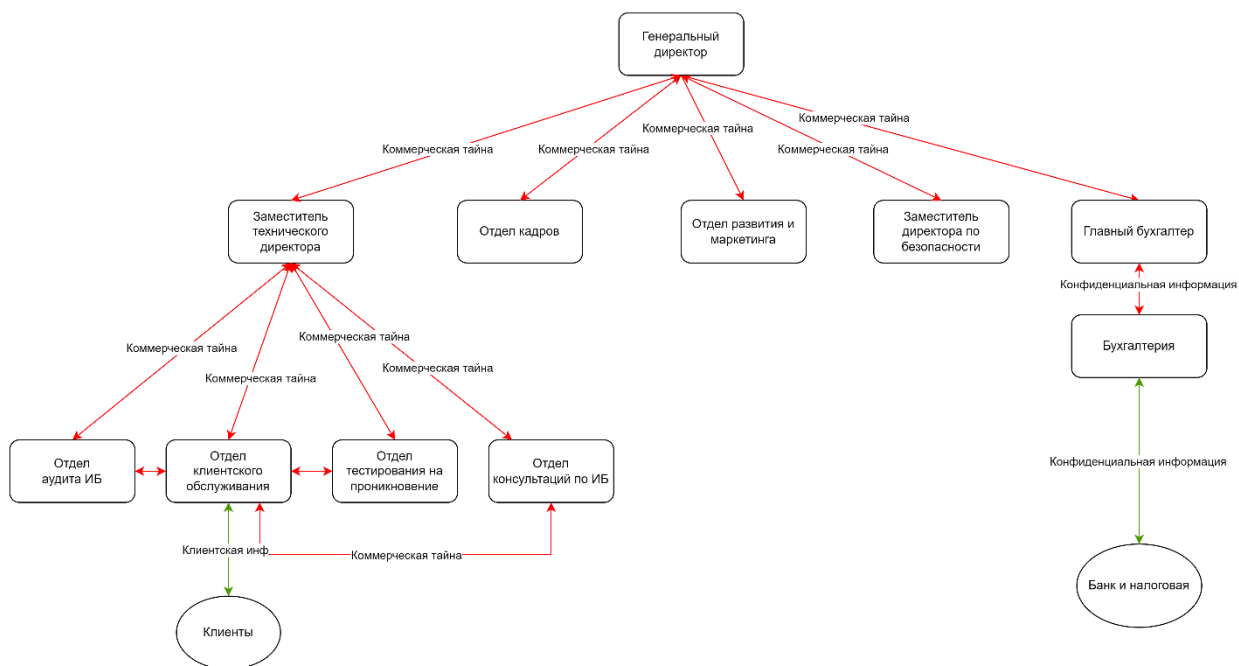


Рисунок 2 – Информационные потоки

3.2 Описание помещения

На рисунке 3 представлен план защищаемого помещения с учетом мебелировки, а в таблице 1 приведены обозначения объектов в каждом помещении и их краткое описание. Номера на плане здания соответствуют следующим помещениям:

1 – приёмная

2 – помещение охраны

3 – серверное помещение: 18 м². В серверном помещении расположены 4 серверов.

Окон в помещении нет.

4 – кабинет заместителя технического директора 18 м². В помещении есть одно окно. Кабинет директора имеет диван, рабочее место с ПК и стелляж.

5 – кабинет директора: 18 м². В помещении есть два окна. Кабинет директора имеет диван для посетителей, кресло, рабочее место с ПК и стелляж.

6 – переговорная: 25 м². В помещении есть 2 окна. Там находятся стол для переговоров и стулья вокруг него, экран для проектора, проектор.

7 – офис 1, 8 – офис 2, 9 – офис 3: 32 м². В помещении есть 1 окно. В каждом офисе располежны 10 столов, 10 стульев, 10 АРМ.

10 – туалет

11 – кухня

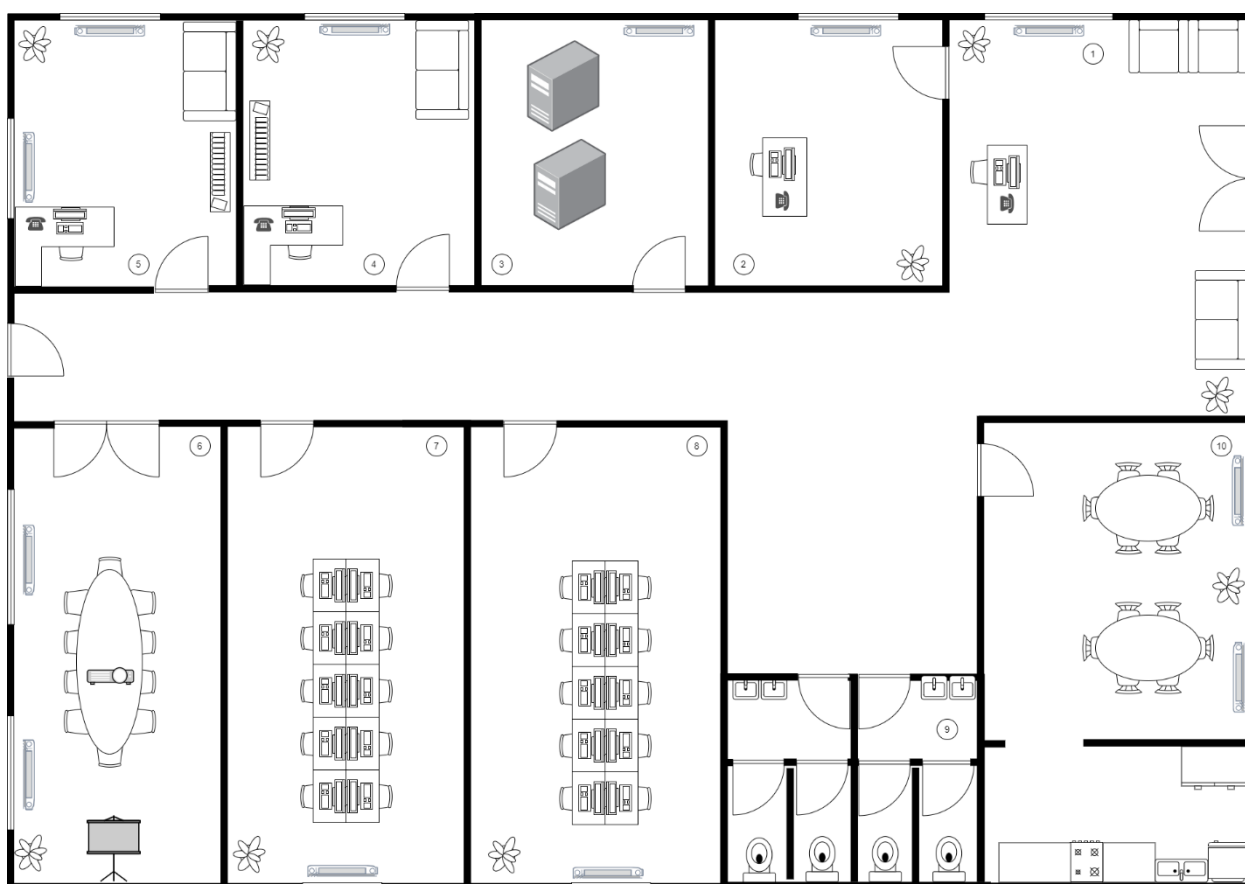
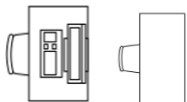





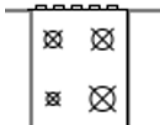

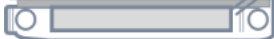


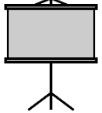


Рисунок 3 – План здания с учетом мебелировки помещений

Таблица 1 – Описание выбранных объектов при мебелировке помещения

Объект	Обозначение
	Рабочее место с АРМом и без АРМа
	Диван
	Сервер
	Живое растение
	Санузел
	Раковины
	Электрическая плита
	Круглый стол
	Батарея центрального отопления
	Телефон
	Проектор
	Экран для проектора

Офис расположен на третьем этаже малоэтажного 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. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

3.3 Анализ возможных утечек информации и выборы СЗИ

Акустические каналы утечки информации образуются:

- за счет распространения акустических (механических) колебаний в свободном воздушном пространстве: переговоры на открытом пространстве, открытые окна, двери, форточки, вентиляционные каналы
- за счет воздействия звуковых колебаний на элементы и конструкции зданий, вызывая их вибрации: стены, потолки, полы, окна, двери, короба вентиляционных систем, трубы водоснабжения, отопления, кондиционирования и др.
- за счет воздействия звуковых колебаний на технические средства обработки информации: микрофонный эффект, акустическая модуляция волоконно-оптических линий передачи информации.

В помещениях присутствуют декоративные элементы, 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. В таблице 2 приведено описание всех элементов, изображенных на плане помещения.

Таблица 2 – Активная и пассивная защита информации

Канал утечки	Источники	Пассивная защита	Активная защита
Акустический	Окна, двери, электрические сети, проводка и розетки	Звуко-изоляция, звуко-поглощение	Звуко-подавление, защищенные акустические системы
Вибрационный виброакустический	Батареи и все твердые поверхности помещений	максимальное снижение уровня перехватываемого сигнала	Создание помех
Визуально-оптический	Незащищенные окна, двери	Снизить освещенность защищаемого	Средства сокрытия защищаемых объектов

		объекта и его отражательные свойства	
ПЭМИН	Розетки, АРМы, бытовая техника	Экранирование, заземление, фильтрация, развязка	Зашумление

4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «совершенно 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 Анализ СЗИ для акустического и виброакустического каналов

Защита информации от утечки по акустическому каналу — это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей.

Организационно-технические меры предусматривают использование звукопоглощающих средств. Пористые и мягкие материалы типа ваты, ворсистые ковры, пенобетон, пористая сухая штукатурка являются хорошими звукоизолирующими и звукопоглощающими материалами — в них очень много поверхностей раздела между воздухом и твердым телом, что приводит к многократному отражению и поглощению звуковых колебаний.

Для облицовки поверхностей стен и потолков широко используются специальные герметические акустические панели, изготавливаемые из стекловаты высокой плотности и различной толщины (от 12 до 50 мм). Такие панели обеспечивают поглощение звука и исключают его распространение в стеновых конструкциях. Степень звукопоглощения α , отражения и пропускания звука преградами характеризуется коэффициентами звукопоглощения, отражения R , пропускания t .

Устраивать звукоизолирующие покрытия стен целесообразно в небольших по объему помещениях, так как в больших помещениях звуковая энергия максимально поглощается, еще не достигнув стен. Известно, что воздушная среда обладает некоторой звукопоглощающей способностью и сила звука убывает в воздухе пропорционально квадрату расстояния от источника.

Итак, защита от утечки по акустическим каналам реализуется:

- применением звукопоглощающих облицовок, специальных дополнительных тамбуров дверных проемов, двойных оконных переплетов;
- использованием средств акустического зашумления объемов и поверхностей;
- закрытием вентиляционных каналов, систем ввода в помещения отопления, электропитания, телефонных и радиосвязей;
- использованием специальных аттестованных помещений, исключающих появление каналов утечки информации.

Пассивная защита:

Цель пассивной защиты состоит в том, чтобы уменьшить шум из окружающей среды, поэтому выбор звукоизолирующих дверей является подходящим вариантом.

Активная защита:

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. В следующей таблице сравниваются и анализируются характеристики некоторых устройств, используемых для активной защиты.

Ниже в таблице 3 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому каналу.

Таблица 3 – Сравнительный анализ средств активной защиты по виброакустическому каналу

Наименование средства	Система активной акустической и вибрационной защиты акустической речевой информации Соната «АВ» модель 4Б	Система постановки виброакустических помех ЛГШ-402	Генератор маскирующего шума «Камертон- 5»
Характеристики	<ul style="list-style-type: none"> - Сертификат ФСТЭК - Диапазон частот 175 – 11200 Гц - Система активной акустической и вибрационной защиты акустической речевой информации "Соната-АВ" модель 4Б, предназначена для защиты речевой информации в выделенных помещениях, от утечки по акустическим, виброакустическим и акустоэлектрическим каналам. 	<ul style="list-style-type: none"> - Сертификат ФСТЭК - Диапазон частот 175 – 11200 Гц - Изделие предназначено для защиты акустической речевой информации, циркулирующей в помещениях, предназначенных для обсуждения или воспроизведения, а также проведения мероприятий с обсуждением информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки информации по виброакустическому и акустическому каналам. 	<ul style="list-style-type: none"> - Сертификат ФСТЭК - Диапазон частот 90 - 11200 Гц - Предназначен для обеспечения защиты акустической речевой информации от утечки по акустическому и вибрационному каналам, за счет акустоэлектрических преобразований во вспомогательных технических средствах и системах, блокирует применение направленных и лазерных микрофонов
Цена (руб.)	44200	18200	46000

По результатам проведенного анализа средств защиты, в качестве системы виброакустической защиты была выбрана «Соната АВ-4Б».

Данное средство имеет сертификат ФСТЭК и обладает следующими преимуществами:

- возможность построения системы автоматического контроля всех элементов
- снижение трудозатрат на конфигурирование и тестирование системы при инсталляции и контроле
- возможность изменения настроек генераторов-излучателей
- снижение затрат на создание единого комплекса ТСЗИ

4.2 Анализ СЗИ для визуально-оптического канала

С целью защиты информации от утечки по визуально-оптическому каналу рекомендуется:

- располагать объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника (пространственные ограждения);
- уменьшить отражательные свойства объекта защиты;
- уменьшить освещенность объекта защиты (энергетические ограничения);
- использовать средства преграждения или значительного ослабления отраженного света: ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды;
- применять средства маскирования, имитации и другие с целью защиты и введения в заблуждение злоумышленника;
- использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражательного или излученного света и других излучений;

Для защиты информации от наблюдения применяют методы энергетического скрывания путем увеличения затухания среды распространения. Для обеспечения скрытности защиты применять пленку надо на всех окнах, по крайней мере, этажа, а лучше здания. Наиболее приемлемый вариант защиты — применение жалю-зи на окнах. Они не только исключают возможность наблюдения через окно, но и эффективны по основному назначению — защите от солнечных лучей. Для предотвращения наблюдения через приоткрытую дверь применяют доводчик двери, который плавно закрывает дверь после ее открытия.

4.3 Анализ СЗИ для электромагнитного каналов

Защита информации от утечки осуществляется с применением пассивных и активных методов и средств. Цель пассивных и активных методов защиты – уменьшение отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки противника опасного информационного сигнала. В пассивных методах защиты уменьшение отношения сигнал/шум достигается путем уменьшения уровня опасного сигнала, в активных методах – путем увеличения уровня шума.

Пассивные методы защиты информации направлены на: ослабление побочных электромагнитных излучений на границе контролируемой зоны; ослабление наводок побочных электромагнитных излучений в посторонних проводниках, соединительных линиях, цепях электропитания и заземления, выходящих за пределы контролируемой зоны; исключение или ослабление просачивания информационных сигналов в цепи электропитания и заземления, выходящие за пределы контролируемой зоны.

Ослабление опасного сигнала необходимо проводить до величин, обеспечивающих невозможность его выделения средством разведки на фоне естественных шумов.

К пассивным методам защиты относятся: применение разделительных трансформаторов и помехоподавляющих фильтров; экранирование; заземление всех устройств, как необходимое условие эффективной защиты информации.

Активные методы защиты информации направлены на: создание маскирующих пространственных электромагнитных помех; создание маскирующих электромагнитных помех в посторонних проводниках, соединительных линиях, цепях электропитания и заземления. К активным методам защиты относятся пространственное и линейное зашумление.

4.3.1 Экранирование электромагнитных волн

Виды экранирования: электростатическое экранирование – подавление емкостных паразитных связей; магнитостатическое экранирование – подавление индуктивных паразитных связей; электромагнитное экранирование – подавление электромагнитного поля.

Сущность электростатического экранирования заключается в замыкании электростатического поля на поверхность металлического экрана и отводе электрических зарядов на землю (корпус прибора) с помощью контура заземления. Применение металлических экранов весьма эффективно и позволяет полностью устранить влияние электростатического поля.

Магнитостатическое экранирование (экранирование шунтированием магнитного поля) используется для наводок низкой частоты в диапазоне от 0 до $3 \dots 10$ Гц. Оно основано на применении экранов из ферромагнитных материалов с большой магнитной проницаемостью.

Принцип действия электромагнитного (динамического) экранирования заключается в том, что переменное магнитное поле ослабляется по мере проникновения в металл, так как внутренние слои экранируются вихревыми токами обратного направления, возникающими в слоях, расположенных ближе к поверхности. Экранирующее действие вихревых токов определяется двумя факторами:

обратным полем, создаваемым токами, протекающими в экране,
поверхностным эффектом в материале экрана.

4.3.2 Заземление технических систем

При реализации электромагнитного экранирования необходимо заземление экрана источника ПЭМИ, под которым понимается преднамеренное электрическое соединение экрана с заземляющим устройством. Кроме того, правильное заземление устройств является одним из важных условий защиты информации от утечки по цепям заземления.

Защитное действие заземления основано на двух принципах:

уменьшение до безопасного значения разности потенциалов между заземляемым проводящим предметом и другими проводящими предметами, имеющими естественное заземление;

отвод тока утечки при контакте заземляемого проводящего предмета с фазным проводом.

4.3.3 Разделительные трансформаторы и помехоподавляющие фильтры.

Разделительные (разделяющие) трансформаторы обеспечивают разводку первичной и вторичной цепей по сигналам наводки. То есть наводки первичной обмотки трансформатора не должны попадать во вторичную.

Помехоподавляющие (развязывающие) фильтры – это устройство, ограничивающее распространение помехи по проводам, являющимся общими для источника и приемника наводки.

В качестве помехоподавляющих фильтров используются фильтры, которые ослабляют нелинейные сигналы в разных участках частотного диапазона. Основное назначение фильтров – пропускать без значительного ослабления сигналы с частотами, лежащими в заданной (рабочей) полосе частот, и подавлять (ослаблять) сигналы за пределами этой полосы. В соответствии с расположением полосы пропускания фильтра относительно полосы помехоподавления в частотном спектре различают четыре класса помехоподавляющих фильтров, амплитудно-частотные характеристики которых показаны на рис. 7.

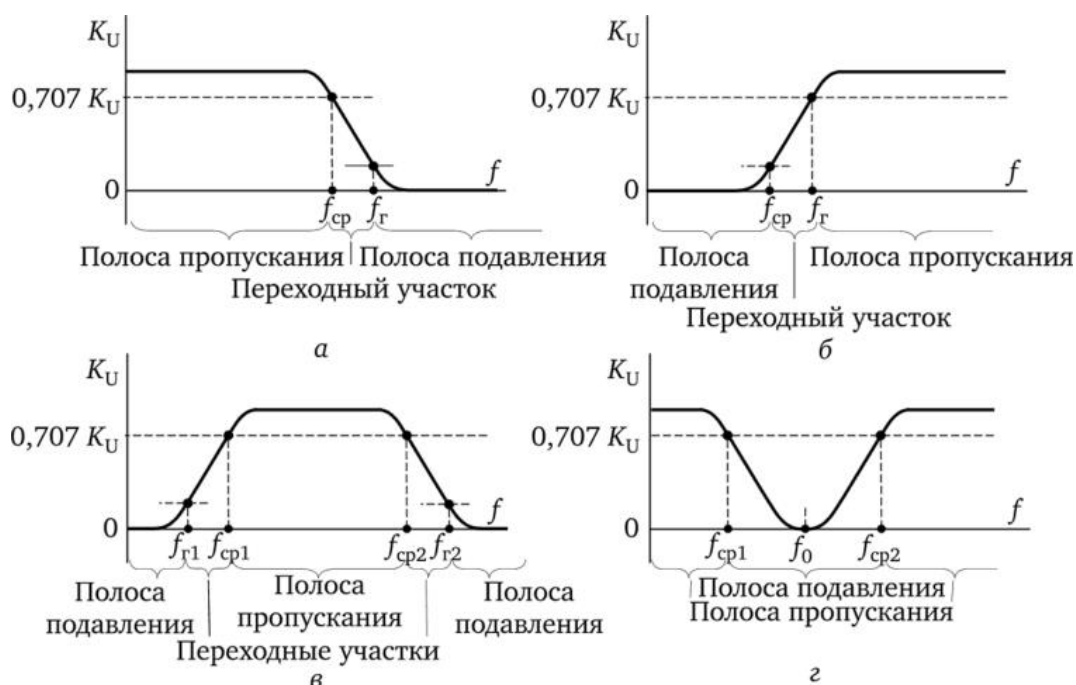


Рисунок 4 – Амплитудно-частотные характеристики помехоподавляющих фильтров: фильтра нижних частот (а), фильтра верхних частот (б), полосового фильтра (в), режекторного фильтра (г), соответственно

4.3.4 Пространственное и линейное зашумление

Пространственное зашумление предполагает создание маскирующих помех в окружающем пространстве и используется для исключения перехвата ПЭМИН по электромагнитному каналу. Цель пространственного зашумления считается достигнутой, если отношение опасный сигнал/шум на границе контролируемой зоны не превышает некоторого допустимого значения, рассчитываемого по специальным методикам для

каждой частоты информационного (опасного) побочного электромагнитного излучения. В системах пространственного зашумления в основном используются помехи типа «белого шума» или «синфазные помехи».

Системы линейного зашумления применяются для маскировки наведенных опасных сигналов в линиях, если они имеют выход за пределы контролируемой зоны.

В простейшем случае система линейного зашумления представляет собой генератор шумового сигнала, формирующий шумовое маскирующее напряжение с заданными спектральными, временными и энергетическими характеристиками. Генератор гальванически подключается в линию, которую необходимо зашумить (например, посторонний проводник).

Ниже в таблице 4 приведен сравнительный анализ подходящих средства активной защиты помещений от ПЭМИН. В результате анализа был выбран генератор шума «Соната РЗ». Данный выбор обоснован особенностями конструкции устройства, которые позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники.

Дополнительно был выбран маскиратор электромагнитных излучений Маис-М2, так как оно обладает лучшими характеристиками по сравнению с другими средствами пассивной защиты от ПЭМИН.

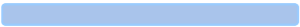
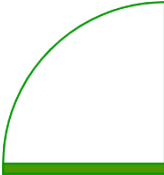



Таблица 4 – Сравнительный анализ средств активной защиты от ПЭМИН

Наименование средства	«Соната-ФС10.1»	«Соната-РЗ»	«Маис-М2»
Характеристики, достоинства и недостатки	<ul style="list-style-type: none"> - Сертифицирован ФСТЭК. - Стандартная комплектация включает заделанные в заводских условиях вводный и отводящий отрезки кабелей. Подключение кабелей к Изделию силами заказчика технически возможна. Длина может быть увеличена по заявке. - Дорогой 	<ul style="list-style-type: none"> - Сертифицирован ФСТЭК. - Возможность, в случае необходимости, дополнительного повышения уровня излучаемого электромагнитного поля шума в диапазоне частот 0,01...200 МГц за счет применения опционально поставляемой дополнительной антенны; возможность удаленного управления изделием как в случае автономного использования (непосредственно пультом "Соната-ДУ4.4"), так и в случае использования в составе комплекса ТСЗИ; - Возможность воздействия на другие электронные устройства при неправильной установке и калибровке 	<ul style="list-style-type: none"> - Сертифицирован ФСТЭК. - Диапазон рабочих частот: 0,01 - 3000 МГц - Простой в использовании. эксплуатация не требует вмешательства персонала, специального обучения и квалификации; управление сводится к подключению к источнику питания перед включением основных технических средств (систем) и отключению после их выключения.
Цена (руб.)	50400	33120	39500

5 РАССТАНОВКА ТЕХНИЧЕСКИХ СРЕДСТВ

В таблице 5 ниже описано, где разместить оборудование, а также количество оборудования и стоимость его оснащения.

Таблица 5 – Описание расстановок технических средств на помещении и расчет стоимости оснащения

Средство ЗИ	Обозначение	Место расположение	Цена (руб.)	Количество (шт)	Стоимость
1	2	3	4	5	6
Рулонные шторы		На каждом окне	2970	11	32670
Звукоизоляционные двери		На двери	61020	3	183060
Соната-ИП4.3 Блок электронного управления		У стен	21600	1	21600
Генератор вибровозбудителей СВ-4Б		- стены - один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;	7440	64	476160
		- потолок , пол - один на каждые 15...25 м2 перекрытия;			

	ВВ	- окна - один на окно (при установке на оконный переплет);			
	ВВ	- двери - один на дверь (при установке на верхнюю перекладину дверной коробки);			
Генератор акустоизлучателей СА-4Б1	АИ	- один на каждый вентиляционный канал или дверной тамбур; - один на каждые 8...12 м3 надпотолочного пространства или др. пустот.	3 540	15	53100
Размыкатели Соната-ВК4.2	РТЛ	Около каждого телефона	6000	4	24000
Соната-РЗ.1	ГШ	подключена напрямую к «Соната-ИП4.3»	33120	1	33120
«Маил-М2»	ГШ	подключена к системе электроснабжения согласно рекомендациям производителя	39500	1	39500
					863210

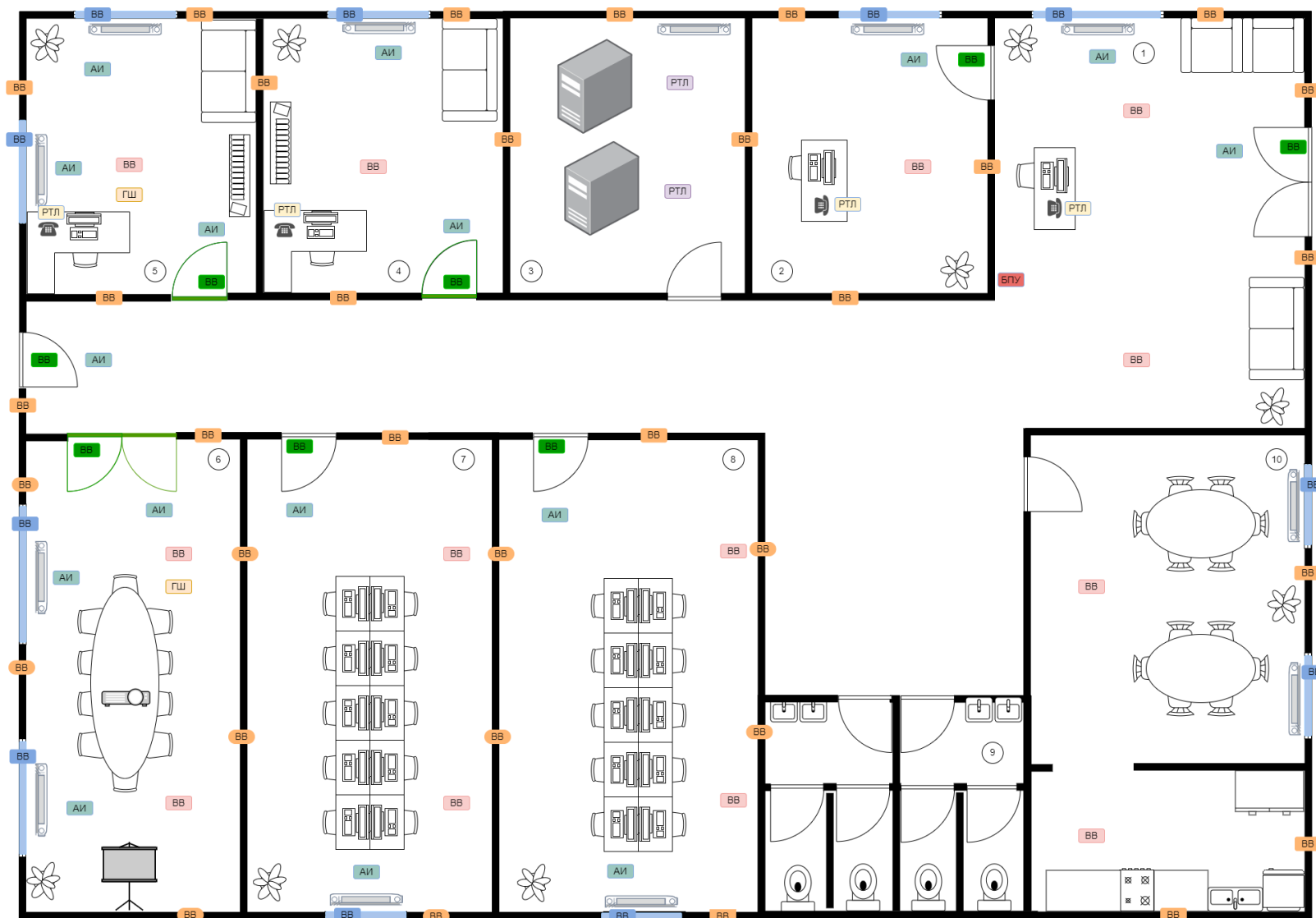


Рисунок 5 – План помещения после расстановки защитных средств

ЗАКЛЮЧЕНИЕ

В рамках работы был проведен анализ технических каналов утечки информации, что позволило выявить потенциальные уязвимости и угрозы информационной безопасности. Это позволило разработать эффективные меры для предотвращения утечек и несанкционированного раскрытия информации. Выполненный анализ защищаемого помещения позволил получить полное представление о его физической структуре, архитектурных особенностях и системах коммуникации. Это позволило определить конкретные уязвимости и риски информационной безопасности, с которыми необходимо было справиться. Был проведен анализ рынка технических средств и выбраны наиболее подходящие и эффективные технологии и инструменты для реализации системы защиты информации. Это позволило разработать оптимальное решение, учитывая специфические потребности и требования рассматриваемого помещения. Расстановка технических средств была осуществлена с учетом рекомендаций и требований, чтобы обеспечить наибольшую эффективность и защиту информации. Были определены места и способы размещения выбранных технических средств в помещении. В целом, выполнение поставленных задач позволило достичь повышения уровня защищенности рассматриваемого помещения и снизить риск утечки и раскрытия информации. Реализация предложенных мер пассивной и активной защиты информации способствует обеспечению конфиденциальности, целостности и доступности данных в помещении.

Однако следует отметить, что защита информации является динамическим процессом, и требует постоянного обновления и совершенствования. Рекомендуется проводить регулярные аудиты и тестирования системы защиты информации, чтобы обнаружить новые уязвимости и принять соответствующие меры.

СПИСОК ЛИТЕРАТУРЫ

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012.- 416 с. - экз
2. А. Торокин: «Инженерно-техническая защита информации: учебное пособие для студентов», М.: Гелиос АРВ, 2005. – 960 с.
3. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия РФ, 1998. 320 с
4. Евстифеев А.А., Ерошев В.И., Мартынов А.П., Николаев Д.Б., Сплюхин Д.В., Фомченко В.Н. Основы защиты информации от утечки по техническим каналам. Саров: РФРЦ-ВНИИЭФ, 2019. -267с., ил.
5. Рекомендации по определению количества и мест установки акустоизлучателей и вибровозбудителей. URL: <http://npoanna.ru/Content.aspx?name=recommendations.placement>