

**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. Вариант 55»**

Выполнил(а):

Студент группы N34481

Самойлов Михаил

Борисович



Проверил преподаватель:

Попов Илья Юрьевич,

к. т. н., доцент ФБИТ

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Самойлов М.Б.

(Фамилия И.О.)

Факультет БИТ

Группа N34481

Направление (специальность) Информационная безопасность

Руководитель Попов И.Ю., к. т. н., доцент ФБИТ

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении.

Задание Цель: разработать комплекс инженерно-технической защиты информации в помещении

Краткие методические указания

Подготовить отчет по курсовой работе по образцу и презентацию для защиты

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

Рекомендуемая литература

Руководитель

(Подпись, дата)

Студент



15 октября 2023

(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Самойлов М.Б.

(Фамилия И.О.)

Факультет БИТ

Группа N34481

Направление (специальность) Информационная безопасность

Руководитель Попов И.Ю., к. т. н., доцент ФБИТ

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Создание плана курсовой работы	15.10.2023	15.10.2023	
2	Подготовка материалов для курсовой работы	23.10.23	23.10.23	
3	Анализ теоретической составляющей работы	03.11.23	03.11.23	
4	Разработка комплекса инженерно-технической защиты информации в заданном помещении	10.11.23	10.11.23	
5	Подготовка отчета по курсовой работе	25.11.23	25.11.23	
6	Представление выполненной курсовой работы	19.12.23	19.12.23	

Руководитель _____

(Подпись, дата)

Студент _____

18 декабря 2023

(Подпись, дата)

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

Студент Самойлов М.Б.

(Фамилия И.О.)

Факультет БИТ

Группа N34481

Направление (специальность) Информационная безопасность

Руководитель Попов И.Ю., к. т. н., доцент ФБИТ

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы

Предложены студентом



Сформулированы при участии студента



Определены руководителем



Цель работы - повышение защищенности рассматриваемого помещения. Задачами являются 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

В работе представлены существующие и потенциальных каналы утечки информации в защищаемых в рамках курсовой работы помещениях, схемы помещения, возможные средства обеспечения защиты от утечек, выбраны и расставлены средства защиты информации.

4. Выводы

В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель

(Подпись, дата)

Студент



18 декабря 2023

(Подпись, дата)

« 18 » декабря 2023 г.

Содержание

Введение.....	6
1. Анализ технических каналов утечек информации.....	8
2. Нормативно-правовая база.....	12
3. Анализ защищаемых помещений	14
4. Анализ рынка.....	22
4.1 Акустический и виброакустический каналы утечки информации	22
4.2 Электрический, акустоэлектрический и электромагнитный каналы утечки информации	26
4.3 Оптические каналы утечки информации	29
5. Описание расстановки технических средств защиты.....	31
Заключение	34
Список литературы	35
Приложение А	36
Приложение Б.....	37

Введение

Утечка информации представляет собой значительную угрозу для различных организаций, влекущую за собой серьезные последствия. Этот риск может возникнуть как результат злонамеренных действий третьих лиц, так и из-за неосторожных действий сотрудников. Злонамеренная утечка информации может быть направлена на нанесение ущерба государству, обществу или конкретному предприятию, что является характерным проявлением кибертерроризма. Также причиной утечки информации может быть стремление получить конкурентное преимущество в бизнесе.

Непреднамеренная утечка информации, в свою очередь, обычно происходит из-за невнимательности сотрудников организации, но даже такие случаи могут иметь серьезные и негативные последствия. Эффективная защита информационных активов от потери требует профессионального подхода и использования передовых технических средств. Это включает в себя не только понимание возможных каналов утечки, но и умение блокировать эти каналы, а также соответствие требованиям современных систем безопасности. Поэтому для построения эффективной системы противодействия утечке информации, первостепенной задачей является выявление потенциальных и реальных угроз технического проникновения в защищаемый объект, а также определение возможных каналов для несанкционированного доступа и утечки конфиденциальной информации. Основной фокус данной работы направлен на оценку каналов утечки информации и выборе мер защиты информации.

Эффективное выявление потенциальных угроз на этапе предпроектной разработки системы противодействия промышленному шпионажу позволяет последующим образом выбирать оптимальные меры и средства защиты. При анализе технических каналов утечки информации необходимо учесть все аспекты системы защиты, включая основное оборудование для обработки информации, соединительные линии, распределительные и коммутационные устройства, системы электропитания, вентиляции и прочее.

В дополнение к основным техническим средствам, прямо связанным с обработкой и передачей конфиденциальной информации, важно учитывать вспомогательные технические средства и системы (ВТСС), такие как средства связи, системы сигнализации, электрификации и другие. Особое внимание следует уделить вспомогательным средствам, имеющим линии, выходящие за пределы контролируемой зоны.

Для успешной борьбы с рисками утечки информации важно иметь систему защиты, которая учитывает различные аспекты, такие как человеческий фактор, технические уязвимости и требования соблюдения стандартов безопасности. Организации должны инвестировать в проактивные меры, такие как обучение сотрудников по вопросам

безопасности, регулярное обновление систем безопасности и мониторинг активности, чтобы оперативно выявлять и предотвращать возможные утечки информации.

Оценка защищенности объекта включает в себя анализ режима работы и охраны объекта, с целью моделирования действий по скрытному проникновению на них (неконтролируемому пребыванию) посторонних лиц. Режим работы специалистов сторонних организаций, приобретение, установка и ремонт мебели, оргтехники и т.п. Т.е. всю совокупность условий, позволяющих внедрить на объект специальные закладные устройства перехвата информации (микропередатчики, возможность установки миниатюрных микрофонов с подключением к внешним линиям и т.д.). А также определение наиболее эффективных, для использования на разных уровнях проникновения, средств технической разведки. Большое, а иногда решающее, значение при оценке угрозы может иметь знание наиболее вероятного противника, его финансовых и оперативных возможностей, знание личностных качеств постоянного персонала, временных работников и другая дополнительная информация.

В современном информационном обществе, где данные играют ключевую роль в бизнес-процессах, поддержание высокого уровня защиты информации становится неотъемлемой частью успешного управления предприятием.

Целью курсовой работы является разработка комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно»

Задачи, решаемые в ходе выполнения курсовой работы:

- произвести анализ технических каналов утечки информации;
- составить перечень управляющих документов;
- произвести анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств;
- произвести анализ рынка технических средств защиты информации разных категорий;
- разработать схемы расстановки выбранных технических средств в защищаемом помещении.

1. Анализ технических каналов утечек информации

Утечка информации – это ее утрата при распространении по каналам связи и физическому пространству по всем типам причин, включая и перехват, и перенаправление. Намеренно созданная утечка информации по техническим каналам предполагает установку на пути ее распространения различных устройств, осуществляющих ее перехват.

Этот термин применяется чаще в профессиональной сфере, на практике под данным определением понимаются все типы утечек, основанные и на человеческом, и на техническом факторе. Неправомерный акт записи сведений, содержащих охраняемую законом тайну, на внешний носитель и вынос его за пределы корпоративного пространства является наиболее распространенным способом хищения. Современные DLP-системы настраиваются сейчас в основном на опасности, исходящие от корпоративного пользователя, а не от внешнего проникновения.

Исходя из вышеприведенных критериев защищаемых данных, различаются несколько типов субъектов предпринимательского оборота, находящихся в основной зоне риска утечки информации. Это:

- коммерческие и некоммерческие, научные и иные организации, работающие со сведениями, составляющими государственную тайну, например, выполняющие государственный заказ;
- организации, работающие на рынке финансовых услуг, обладающие данными о счетах и финансах своих клиентов, номерах их банковских карт;
- организации, работающие с большими массивами персональных данных, которые часто становятся добычей хакеров и поступают на открытый рынок;

Всем им необходимо в максимальной степени использовать доступные способы предотвращения утечки информации, так как ущерб в этом случае может быть причинен не только непосредственно юридическому лицу, но и неопределенно широкому кругу лиц. В ряде случаев за непринятие мер защиты компания может быть привлечена к ответственности. Каждый канал утечки информации должен быть проанализирован с точки зрения определения его безопасности и максимально защищен.

Выделяются четыре основных группы технических способов организации утечки информации:

- визуальные, 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;
- материальные, связанные с анализом предметов, документов и отходов, возникших в результате деятельности компании.



Рисунок 1 – Классификация каналов утечки информации

В каждом случае использования технического канала утечки конкурентами применяются самые современные способы получения и обработки сведений, и само знание о наличии таких возможностей должно помочь снизить уровень риска. Для полного снятия опасности необходима коммуникация с профессионалами, которые смогут определить наиболее ценные массивы данных, являющиеся целью для возможных атак, предложить полный комплекс средств защиты.

Если экран монитора или часть лежащих на столе документов можно увидеть через окно офиса, возникает риск утечки. Любой световой поток, исходящий от источника информации, может быть перехвачен. Для борьбы с этим способом необходимо применять в большинстве случаев простые технические средства:

- снижение отражательных характеристик и уменьшение освещенности объектов;
- установка различных преград и маскировок;
- использование светоотражающих стекол;
- расположение объектов так, чтобы свет от них не попадал в зону возможного

перехвата.

Но существует и более типичный риск утечки видовой информации: вынос документов из помещения для их фотографирования, иные формы копирования, скрины экранов баз данных, содержащих важные сведения, и другие способы. Основные меры борьбы с этими рисками относятся исключительно к административно-организационной сфере, хотя существуют программные средства, которые, например, не дают возможности сделать скрин данных, выводимых на экран монитора.

Информация, существующая в форме звука, наиболее незащищена от перехвата и утечки. Звук, который находится в ультрадиапазоне (более 20 тысяч герц), легко распространяется. Если на его пути окажется преграда, звуковая волна вызовет в ней колебания, и они будут считаны специальными устройствами. Это свойство звука должно быть учтено уже на стадии проектировки здания или офиса, где расположение помещений архитекторами должно продумываться так, чтобы исключить утечку информации. Если этот способ нереализуем, необходимо обратиться к техническим средствам и использовать для отделки помещения звукоотражающие материалы, например, пористую штукатурку. Для оценки степени защищенности используются стетоскопы.

Если не удастся добиться максимального звукопоглощения, могут быть применены генераторы шума, которые можно установить по периметру не защищенных от прослушивания основных стен здания или в переговорных.

Утечка акустической информации возможна также с использованием диктофонов при проведении переговоров. Для выявления их наличия используются специальные устройства. Установка приборов снятия голосового сигнала на телефонные аппараты (жучков) сейчас практически не применяется, используется перехват цифрового трафика другим способом, в том числе через телефонного оператора или через Интернет-провайдера. Эту степень риска тоже стоит учитывать, возможно, путем создания специальных инструкций о той конфиденциальной информации, которая может быть обсуждаема в телефонных переговорах.

Представляет опасность также перехват информации, содержащейся в побочных электромагнитных излучениях. Электромагнитные волны, распространяясь в пределах электромагнитного поля на небольшом расстоянии, также могут быть перехвачены. Они могут исходить:

- от микрофонов телефонов и переговорных устройств;
- от основных цепей заземления и питания;

- от аналоговой телефонной линии;
- от волоконно-оптических каналов связи;
- из других источников.

Перехватить и расшифровать их не представляет сложности для современных технических средств.

Технологии позволяют подключать закладные устройства ПЭМИН (термин расшифровывается как «побочные электромагнитные излучения и наводки») непосредственно к цепям питания или же установить в мониторе или корпусе компьютера, при этом они через внутренние подсоединения к платам могут перехватывать данные:

- выводимые на экран монитора;
- вводимые с клавиатуры;
- выводимые через провода на периферийные устройства (принтер);
- записываемые на жесткий диск и иные устройства.

Способами борьбы в этом случае станут заземление проводов, экранирование наиболее явных источников электромагнитного излучения, выявление закладок или же использование специальных программных и аппаратных средств, позволяющих выявить закладки.

Обыкновенный мусор или производственные отходы могут стать ценным источником данных. Химический анализ отходов, покидающих пределы контролируемой зоны, может стать источником получения важнейших сведений о составе продукции или о технологии производства. Для разработки системы борьбы с этим риском необходимо комплексное решение с использованием в том числе и технологий переработки отходов.

Все вышеперечисленные способы утечки информации (кроме материально-вещественного) требуют территориальной доступности источника для похитителя, зона работы обычного устройства перехвата звуковой или визуальной информации не превышает нескольких десятков метров. Установка закладных устройств для съема электромагнитных излучений и акустических колебаний должна потребовать прямого проникновения на объект. Также необходимо знание его планировки, это может потребовать вербовки сотрудника. При том, что большинство помещений оснащено камерами видеонаблюдения, эти способы сейчас применяются в крайне редких случаях.

Наиболее же серьезную опасность несут современные способы хищения с использованием возможностей сети Интернет и доступа с ее помощью к архивам данных или голосовому трафику.

2. Нормативно-правовая база

Документами Российской Федерации в области защиты информации и предотвращения утечки информации по техническим каналам связи являются:

- Закон Российской Федерации «О государственной тайне» от 21.07.1993 г. №5485–1;
- Указ президента «Вопросы защиты государственной тайны» от 30.03.1994 г. №614;
- Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г.;
- Указ Президента РФ «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203;
- Указ Президента РФ №1286 "Вопросы Межведомственной комиссии по защите государственной тайны" от 6 октября 2004 г.;
- Указ Президента РФ №188 «Об утверждении Перечня сведений конфиденциального характера» от 13.07.2015;
- Указ Президента РФ №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016;
- Положение "О государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам" Постановление Совета Министров –Правительства Российской Федерации от 15 сентября 1993 г. №921–51;
- 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";
- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644;
- «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) 13 оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. №333;
- «О сертификации средств защиты информации» от 26 июня 1995 г, №608.

Распорядительные, нормативные и методические документы и подготовленные проекты документов ФСТЭК по технической защите информации:

- СТР Специальные требования и рекомендации по защите информации,

составляющей государственную тайну, от утечки по техническим каналам;

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

3. Анализ защищаемых помещений

Компания специализируется на создании инфраструктуры киберзащиты для крупных корпораций, государственных учреждений и объектов государственной охраны на базе импортозамещённого оборудования и ПО. Они предоставляют комплексные решения включая многоуровневые системы мониторинга, анализа угроз и автоматизированные средства реагирования на кибератаки.

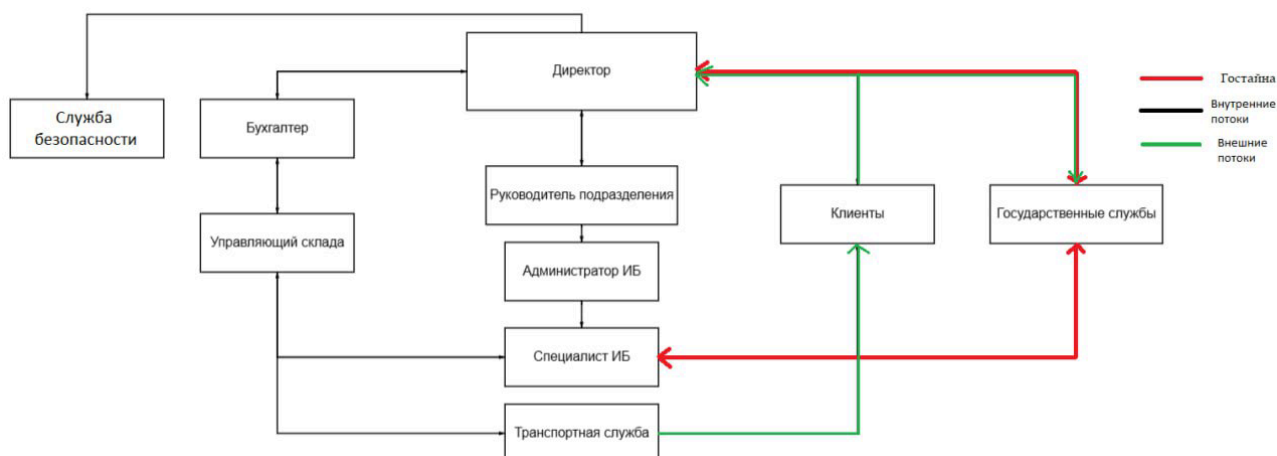


Рисунок 2 – Информационные потоки организации

- коды и алгоритмы защитного программного обеспечения;
- разработки и патенты по новым методам киберзащиты;
- исследования по обнаружению и предотвращению кибератак;
- серверы и сетевое оборудование;
- коммуникационные каналы и криптографические ключи;
- конфигурации фаерволлов и средств обнаружения вторжений;
- личные данные клиентов и пользователей;
- конфиденциальные данные о киберугрозах и событиях безопасности;
- средства мониторинга, анализа, реагирования безопасности;
- информация о партнерах и клиентах, включая гостайну;
- детали о сотрудничестве и обмене информацией с другими организациями по кибербезопасности.

Согласно требованиям к режимным помещениям и их оборудованию, содержащимся в «Типовых нормах и правилах 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 №199. Для степени «секретно» следует соблюсти следующие требования:

- стены или перегородки между обычными и защищенными помещениями должны быть бетонными, железобетонными или металлическими с толщиной стен — от 10 см, или кирпичными с толщиной стен от 12 см;
- в помещениях для работы с гостайной 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;
- обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании;
- 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;
- все режимные помещения оборудуются аварийным освещением;
- вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.

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.

Класс защищенности у рассматриваемой организации 1В, так как в ней обрабатывается секретная информация и предприятие является многопользовательской АС, где не все пользователи имеют права доступа ко всей информации

Таблица 1 – Классы защищенности автоматизированных систем

Описание класса	Обозначение	Уровень конфиденциальности
Первая группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право	1А	В случае обработки секретной информации с грифом «особая важность»
	1Б	В случае обработки секретной информации с грифом не выше «совершенно секретно»
	1В	В случае обработки секретной

доступа ко всей информации АС)		информации с грифом не выше «секретно»
	1Г	АС, в которых циркулирует служебная информация
	1Д	АС, в которых циркулируют персональные данные
Вторая группа (АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности)	2А	Информация, составляющая гостайну
	2Б	Служебная тайна или персональные данные
Третья группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)	3А	Информация, составляющая гостайну
	3Б	Служебная тайна или персональные данные

План помещения представлен на рисунке 3.

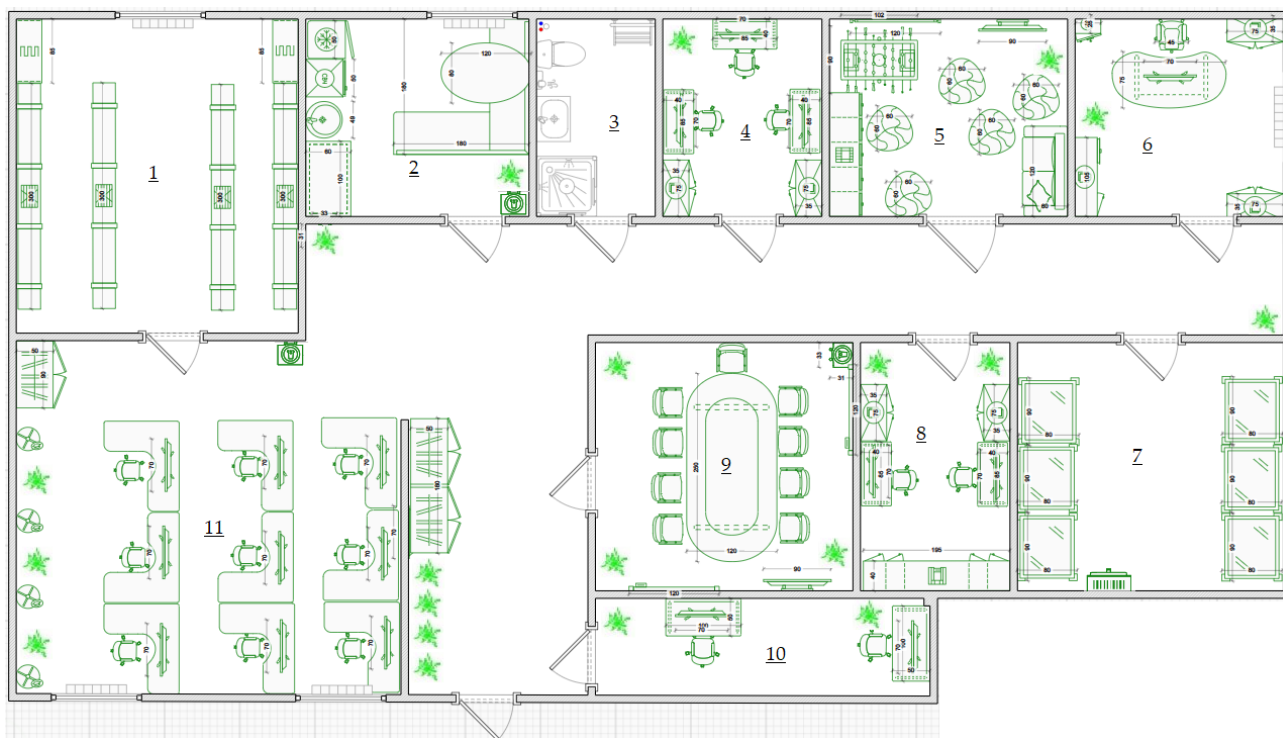

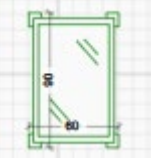







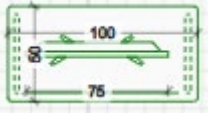

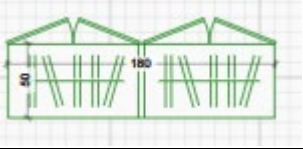

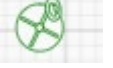
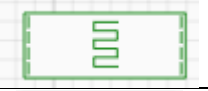

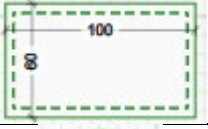




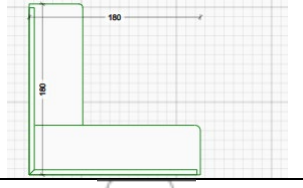





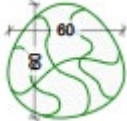
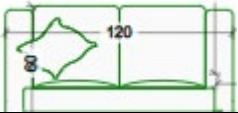
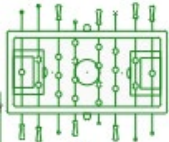


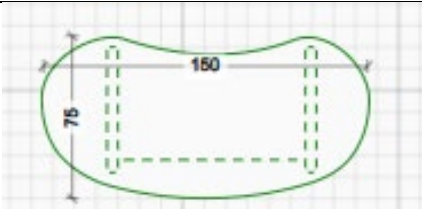




Рисунок 3 – План помещения

Таблица 2 – Условные обозначения

Обозначение	Описание
	Стеллаж
	Сервер
	Шкаф с замком
	Шкаф-стенка
	Офисное кресло
	Стул для переговорной
	Магнитно-маркерная доска
	Кулер
	Стол для переговоров

Обозначение	Описание
	Стол с АРМ
	Горшок с цветком
	Шкаф гардеробный двойной
	Телевизор на кронштейне
	Вешалка-стойка
	Шкаф-стеллаж в замком
	Радиатор
	Столешница
	Круглая мойка
	Шкаф-пенал с СВЧ
	Холодильник
	Стол-эллипс
	Диван угловой
	Унитаз
	Раковина
	Полотенцесушитель
	Сушилка для рук

Обозначение	Описание
	Душевая кабинка
	Кресло-мешок
	Диван
	Кикер
	Шкаф-стенка
	Сейф
	Стол руководителя
	Кресло руководителя
	Электроплитовая

Рассматриваемые помещения имеют следующую площадь:

1. склад для технического оборудования 18м²;
2. кухня 12м²;
3. ванная/туалет 7м²;
4. Первый отдел 9 м²;
5. комната отдыха 15м²;
6. кабинет директора 9м²;
7. серверная 14м²;
8. кабинет бухгалтеров 8м²;
9. переговорная комната 14м²;
10. комната охраны 8м²;
11. опенспейс 64м².

1. Первое помещение является складом для технического оборудования, сертифицированного ФСТЭК. Здесь размещается оборудование, которое затем настраивается и отправляется заказчикам. Содержит 2 шкафа для хранения и учет лицензий оборудования, 4 стеллажа, на которых размещается запакованное оборудование, 2 розетки, 1 кондиционер, 1 радиатор, 1 окно.

2. Второй помещение является кухней, на которой расположены 1 большой обеденный стол, 1 угловой диван, 1 столешница, 1 раковина, 1 холодильник, 1 шкаф со встроенной микроволновой печкой, 1 радиатор, 1 горшок с цветками, 5 розеток, 1 окно.

3. Третье помещение является ванной/туалетом. Содержит 1 душевую кабинку, 1 унитаз, 1 раковину, 1 полотенцесушитель, 1 сушилку рук, 2 розетки.

4. Четвертое помещение является Первым отделом. Здесь расположен 2 шкафа, 3 кресла, 3 АРМ, 1 горшок с цветами, 5 розеток.

5. Пятое помещение является комнатой отдыха. Здесь расположен 1 большой стеллажный шкаф, 1 магнитно-маркерная доска, 5 кресел-мешков, 1 стол для кикера, 1 диван, 1 телевизор, 2 горшка с цветами, 3 розетки.

6. Шестое помещение это кабинет директора, в котором расположены 1 кресло начальника, 1 круглый стол начальника с АРМ, 1 шкаф для одежды, 2 тумбочки под вещи, 1 горшок с цветком, 1 сейф, 1 радиатор, 3 розетки, 1 окно.

7. Седьмое помещение это серверная, в которой расположены 6 серверов, 2 кондиционера, 26 розеток.

8. Восьмое помещение это кабинет бухгалтеров, где расположены 2 стола с АРМ, 2 рабочих кресла, 1 шкаф под документы с замком, 1 шкаф под одежду, 1 стеллаж под вещи, 2 горшка с цветами, 6 розеток.

9. Девятое помещение — это переговорная комната, в которой расположен 1 большой стол для переговоров, 9 мягких кресел, 1 магнитно-маркерная доска, 1 телевизор, 1 кулер, 2 цветка, 1 кондиционер, 1 настенные часы, 3 горшка с цветами, 2 розетки

10. Десятое помещение это комната охраны, в которой расположены 2 стола с АРМ и мониторами, 2 офисных кресла, 2 горшка с цветами, 4 розетки.

11. Одиннадцатое помещение это опенспейс, в которой расположены 9 рабочих мест с АРМ, 30 розеток, 4 вешалки под одежду, 1 шкаф под вещи, 2 гардеробных шкафа, 1 кулер, 9 офисных кресел, 9 горшков с цветами, 2 радиатора, 2 окна.

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. Помещения сгруппированы в тупиковой части здания, которая редко используется сотрудниками при выполнении служебных обязанностей, не связанных с доступом к государственной тайне. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10см.

Множество помещений оборудованы розетками, отсюда возникает уязвимость к угрозе утечки информации по электромагнитным каналам связи; декоративные и крупногабаритные элементы могут использоваться для того, чтобы спрятать там закладные устройства. Также есть угроза снятия информации по оптическому и акустическому каналам.

Материально-вещественный канал утечки информации регулируется политикой компании в отношении физических носителей информации, и в рамках данной курсовой работы не рассматривается.

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «совершенно секретно» требуется оснастить помещение средствам защиты, приведенными в таблице 3.

Таблица 3 – Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
Акустический/ акустоэлектрический	Проводка, окна, двери	Сетевые фильтры, звукоизоляция переговорной и кабинета директора	Устройства акустического зашумления
Вибрационный/ виброакустический	Батареи и трубы, стены, пол, окна, двери, все твердые поверхности помещения	Изолирующие звук и вибрацию материалы стен	Устройства вибрационного зашумления
Оптический	Окна, двери	Жалюзи/шторы на окнах, доводчики на двери, пленки на окна	Блокирующие обзор устройства, бликующие устройства
Электромагнитный/ электрический	АРМ, бытовые приборы и техника, телевизоры, розетки	Сетевые фильтры	Устройства электромагнитного зашумления

4. Анализ рынка

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 Акустический и виброакустический каналы утечки информации

Активная и пассивная защита информации в акустическом и виброакустическом каналах связи — это методы обеспечения безопасности передачи звуковой информации.

Пассивная защита:

- использование материалов и технологий для уменьшения передачи вибраций через твердые объекты;
- использование усиленных дверей и сетевых фильтров.

Активная защита:

- использование методов активной маскировки для создания фоновых шума или искажения передаваемого сигнала, чтобы затруднить его перехват и анализ.
- изменение частотных характеристик звукового сигнала для усложнения его перехвата и декодирования.
- применение технологий для подавления эха, что может предотвратить анализ сигнала.
- использование устройств для создания вибраций, маскирующих передаваемую информацию.
- применение экранирующих материалов для уменьшения передачи вибрации через объекты.

Обеспечение безопасности в акустическом и виброакустическом каналах требует комплексного подхода, включая как пассивные, так и активные методы защиты, чтобы предотвратить несанкционированный доступ, перехват и анализ звуковой информации.

Таблица 4 – Сравнительный анализ средств активной защиты

Устройство	Характеристики	Предназначение/состав	Цена, руб
Портативный генератор акустического шума ЛГШ-303	Диапазон рабочих частот 180 ÷ 11 300 Гц	Для защиты речевой информации от перехвата по прямому акустическому каналу	15 600р
Генератор акустического шума ЛГШ-304	Диапазон рабочих частот 175 ÷ 11 200 Гц	Сертификат ФСТЭК РОССИИ по 2 классу защиты; может устанавливаться в ВП до 2 категории.	25 300р
«БУБЕН» - генератор акустической помехи	Диапазон рабочих частот 400...18000 Гц	Используется для защиты конфиденциальных переговоров по принципу создания акустических помех. Вид помех: Речеподобная, «белый шум».	25 000р
Фотон-М –	Скорость	Устройство защиты акустической	395 000р

устройство защиты оптоволоконной линии от утечки акустической информации	передачи данных в сетях по технологии Ethernet до 100 Мбит/с	речевой информации от утечки по волоконно-оптической линии связи (ВОЛС).	
SI-3030 Виброакустический шумогенератор	Спектр шумовой помехи 125 Гц – 6,3 кГц	Предназначен для защиты помещений от прослушивания через строительные элементы конструкции. Имеет три независимых канала, в приборе используются три некоррелированные источника шума, исключающие возможность восстановления речи методами адаптивной фильтрации.	28 500р
Система постановки виброакустических и акустических помех «ЛГШ-404»	Диапазон рабочих частот 175-11200 Гц	Изделие соответствует требованиям документа «Требования к средствам активной акустической и вибрационной защиты акустической речевой информации» (ФСТЭК России, 2015) - по 2 классу защиты. Изделие «ЛГШ-404» может устанавливаться в выделенных помещениях до 2 категории включительно. В состав входят: - «ЛГШ-404»; - Вибровозбудитель «ЛВП-10» - для установки на стены, трубы и окна; - Акустический излучатель «ЛВП-2а» - для возбуждения маскирующих акустических помех; - Виброэкран «ЛИСТ-1» - для защиты от налблюдения и акустических микрофонов; - Размыкатель «ЛУР» - для размыкания слаботочных линий.	44 000р
Буран	Частота, Гц	Является средством активной	35 000р

	100 – 11 200 Гц	акустической и вибрационной защиты акустической речевой информации типа А. Имеет четыре канала формирования помех, к каждому из которых могут подключаться вибропреобразователи пьезоэлектрического или электромагнитного типа, а также акустические системы, обеспечивающие преобразование электрического сигнала, формируемого прибором, в механические колебания в граждающих конструкциях защищаемого помещения, а также в акустические колебания воздуха	
Соната «АВ» модель 4Б	Диапазон рабочих частот 175-11200 Гц	Блок электропитания и управления, генератора акустоизлучатель, генератор вибровозбудитель, размыкатель телефонной линии, размыкатель слаботочной линии, размыкатель линии Ethernet, пульт управления, блок сопряжения с внешними устройствами, техническое средство защиты речевой информации от утечки по оптикоэлектронному (лазерному) каналу.	44 000р
Буран-2	Диапазон рабочих частот не менее 180-11200 Гц	Является средством активной акустической и вибрационной защиты акустической речевой информации типа А, имеет сертификат ФСБ. Имеет четыре канала формирования помех, к каждому из которых могут подключаться вибропреобразователи пьезоэлектрического или электромагнитного типа, а также акустические системы, обеспечивающие преобразование	81 000р

		электрического сигнала, формируемого прибором, в механические колебания в гражданских конструкциях защищаемого помещения, а также в акустические колебания воздуха	
--	--	--	--

На основании информации из таблицы 4, в качестве средства активной защиты был выбран Буран, так как он имеет сертификат ФСТЭК, его цена средняя, а по характеристикам не сильно отличается от Буран-2, цена которого выше на 13 500р. Благодаря особенностям конструкции можно эффективно и экономично укомплектовать объекты вычислительной техники с большим числом вычислительных средств. Также полезным будет «БУБЕН» - генератор акустической помехи, который используется для защиты конфиденциальных переговоров по принципу создания акустических помех – речеподобных помехи либо «белый шум».

4.2 Электрический, акустоэлектрический и электромагнитный каналы утечки информации

Технические средства, не являющиеся радиопередающими устройствами, являются источниками нежелательных электромагнитных излучений. Такие излучения называются побочными электромагнитными излучениями.

К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений технических средств приема, обработки, хранения и передачи информации (ПЭМИ) ТСПИ:

- излучений элементов ТСПИ;
- излучений на частотах работы высокочастотных (ВЧ) генераторов технических средств приема, обработки, хранения и передачи информации (ТСПИ);
- излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Электрические каналы утечки информации возникают за счет:

- наводок электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;
- просачивания информационных сигналов в линии электропитания и цепи заземления ТСПИ;
- использования закладных устройств.

В цепях различных устройств протекают переменные электрические токи, порождающие электромагнитные поля, излучаемые в окружающее пространство. Структура и параметры электромагнитных полей, создаваемых токоведущими элементами,

определяются конструктивными особенностями систем и средств информатизации и связи, а также условиями их размещения и эксплуатации.

Такие электромагнитные излучения являются потенциальными носителями опасного сигнала.

Технические средства различного назначения могут иметь в своем составе устройства, которые для выполнения своих основных функций генерируют электромагнитные колебания (эталонные и измерительные генераторы, генераторы тактовых частот).

Таблица 5 – Сравнительный анализ средств активной защиты

Устройство	Характеристики	Предназначение/состав	Цена, руб
«Соната-РСЗ» – устройство для защиты линий электропитания и заземления от утечки информации	Диапазон частот до 2 ГГц	Изделия рассчитаны на подключение к 3-проводной сети энергоснабжения и обеспечивают формирование несинфазных токов и синфазных и паразитных составляющих шумового напряжения во всех проводниках. Возможность регулирования уровня излучаемых электромагнитных шумов; возможность блокировки прибора от несанкционированного доступа; световой и звуковой индикаторы работы и контроля уровня излучения; совместимость с проводными пультами ДУ линейки СОНАТА	32 400р
Генератор шума Покров, исполнение 1	Диапазон шумового сигнала - для электрической составляющей 0,01 – 6000 МГц - для магнитной составляющей 0,01 –	Предназначен для защиты информации от утечки по техническим каналам за счет ПЭМИН путем излучения в окружающее пространство электромагнитного поля шумового сигнала и наводок на	32 800р

	30 МГц -для электрических сигналов, наведённых на цепи электропитания 0,01 – 400 МГц	линии электропитания и заземления. Имеется сертификат ФСТЭК России №4324 от 18.11.2020, действителен до 18.11.2025	
Двухканальный генератор зашумления SEL SP-44	Спектральная плотность напряженности электрического поля шума 0,01 – 1 МГц 90дБ / 1 – 10 МГц 70 дБ / 10 – 100 МГц 50 дБ / 100 – 300 МГц 35 дБ	Диапазон частот 10 кГц – 400 МГц, диапазон регулировки уровня шума не менее 20 ДБ. Индикация нормального/ аварийного режима работы. Электропитание от сети переменного тока 220В 50 Гц. Устройство имеет высший классустойчивости к импульсным помехам и допускает длительную работу в условиях эквивалентного короткого замыкания.	24 000р
Сетевой генератор шума ЛГШ-221	Спектральная плотность напряжения шумового сигнала в диапазоне частот 10 ÷ 500 кГц, дБ(мкВ/√кГц) – 10 ÷ 50 / в диапазоне частот 0,5 ÷ 30 МГц, дБ(мкВ/√кГц) – 10 ÷ 58 / в диапазоне частот 30 ÷ 400 МГц, дБ(мкВ/√кГц) – 10 ÷ 47	Сертификат ФСТЭК России по 2 классу защиты. Может устанавливаться в ВП до 2 категории. Диапазон частот 10 кГц – 400 МГц, диапазон регулировки уровня шума не менее 20 ДБ. Световой индикатор работы в стандартном режиме; световая и звуковая сигнализация в случае отказа и перехода в аварийный режим работы; счетчик отработанных часов; возможность интеграции в программно-аппаратный комплекс ДУ и контроля «Паутина»	36 400р
Фильтр сетевой	Номинальный	Принцип действия – подавление	267 000р

помехоподавляющий ФСПК-100	рабочий ток не более 100 А. Режим работы устройство допускает непрерывную круглосуточную работу в течение длительного времени (не менее 1 года)	(фильтрация) помех в частотном диапазоне от 0,1 до 1000 МГц. Фильтр обеспечивает электромагнитную развязку в цепях электропитания электросетей объектов промышленного и непромышленного назначения, и различной вычислительной и радиоэлектронной техники. Каждый полукомплект состоит из: <ul style="list-style-type: none"> - металлического основания; - двух токонесущих латунных (медных) шин с устройствами подключения; - шести цилиндрических корпусов - двенадцати конденсаторов по 10 мкФ каждый. 	
-------------------------------	---	---	--

На основании проведенного анализа средств активной защиты в электрических, акустоэлектрических и электромагнитных каналах утечки информации, принял решение использовать двухканальный генератор зашумления SEL SP-44, имеющий низкую стоимость по сравнению с конкурентами и большой диапазон частот, также имеет высший класс устойчивости к импульсным помехам. В дополнение для защиты от ПЭМИН буду использовать генератор шума Покров, исполнение 1, который выполнен в виде сетевого удлинителя с 5 розетками и сертифицирован ФСТЭК.

4.3 Оптические каналы утечки информации

Для предотвращения утечек информации через окна в кабинете директора и окнах опенспейса, в которых видно работу специалистов ИБ для обеспечения защиты помещения от оптических каналов утечки информации, вариантами решения были установка на окна жалюзи и установка на окна штор.

Шторы — это тканевое покрытие, которое используется для прикрытия окон или других открытых проемов. Они выполняют несколько функций, включая регулирование уровня света, обеспечение конфиденциальности. В контексте обеспечения защиты от

оптических каналов утечки информации, шторы могут предоставить визуальный барьер и помешать прямому взгляду извне.:

Жалюзи представляют собой систему горизонтальных или вертикальных ламелей, которые можно регулировать для изменения уровня освещения и приватности. Жалюзи обеспечивают более тонкое регулирование освещения по сравнению с шторами и могут предоставить дополнительный уровень защиты от внешних взглядов и оптических утечек информации.

Доводчики — это устройства, установленные на дверях или окнах, чтобы контролировать их открытие и закрытие. Они могут автоматически закрывать двери или окна после их открытия или медленно закрываться, предотвращая резкие удары. Доводчики могут использоваться для предотвращения нежелательного оставления дверей или окон открытыми, что могло бы создать возможность для визуального наблюдения извне.

Комбинация этих элементов может существенно улучшить уровень безопасности помещения и снизить возможность нежелательного сбора информации через оптические каналы. Для удобства эксплуатации и содержания мной было выбрано использовать жалюзи, а также на двери устанавливать доводчики, чтобы препятствовать утечкам информации по оптическим каналам утечки информации.

5. Описание расстановки технических средств защиты

Список всех выбранных технических средств защиты, полученных и выбранных путем анализа предыдущих пунктов, приведен ниже:

- Виброакустический генератор "Буран" - средство активной акустической и вибрационной защиты акустической речевой информации;
- "БУБЕН" - генератор акустической помехи;
- SEL SP-44 -генератор зашумления;
- Генератор шума Покров, исполнение 1;
- Дверь взломостойкая 4 класс, укрепленная Bronedver - дверное полотно и коробка - сталь 2 мм. Толщина полотна от 65 до 85 мм;
- Рулонные жалюзи Blackout;
- Вибропреобразователь для стен «Молот» с креплением;
- Вибропреобразователь для коммуникаций(труб) «Сerp-T» с креплением;
- Вибропреобразователь для рам «Сerp-P» с креплением;
- Вибропреобразователь для окон «Копейка» с креплением на раму окна;
- Преобразователь акустический «Рупор»;
- Модуль дистанционного управления по проводному каналу «Буран-ДУ».

Необходимое количество аудиоизлучателей можно предварительно оценить из следующих норм:

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





Основным критерием, который необходимо учитывать при выборе расположения передатчиков в каждом конкретном помещении, является обеспечение максимального уровня вибрационного и акустического шума в предполагаемом канале утечки информации, при этом поддерживая приемлемый уровень помех от звукового воздействия в защищаемом помещении.





Таблица 6 - Смета на выбранные средства защиты информации

Средство защиты	Цена, руб.	Количество, шт	Стоимость, руб.
Виброакустический генератор "Буран"	35 000	1	35 000
"БУБЕН" - генератор акустической помехи	25 000	1	25 000
SEL SP-44 -генератор зашумления	24 000	6	144 000
Генератор шума Покров, исполнение 1	32 800	7	229 600
Дверь взломостойкая 4 класс, укрепленная Bronedver	79 000	5	395 000

Средство защиты	Цена, руб.	Количество, шт	Стоимость, руб.
Жалюзи Blackout	2 600	5	13 000
Доводчики GEZE TS 2000/4000	1 100	10	11 000
Вибропреобразователь для стен «Молот»	3 000	17	51 000
Вибропреобразователь для коммуникаций(труб) «Серп-Т»	3 000	9	27 000
Вибропреобразователь для рам «Серп-Р»	3 000	5	15 000
Вибропреобразователь для окон «Копейка»	2 500	5	12 500
Преобразователь акустический «Рупор»	2 000	10	20 000
Размыкатель линий оповещения и сигнализации "Буран-К2"	3 400	3	10 200
Размыкатель компьютерных сетей "Буран-К3"	3 500	3	10 500
Модуль дистанционного управления по проводному каналу «Буран-ДУ»	4 500	1	4 500
Итого			1 003 300

Таблица 7 – Условные обозначения

Средство защиты	Условное обозначение	Количество, шт
Виброакустический генератор "Буран"		1
"БУБЕН" - генератор акустической помехи		1
SEL SP-44 -генератор зашумления		6
Генератор шума Покров, исполнение 1		7

Средство защиты	Условное обозначение	Количество, шт
Дверь взломостойкая 4 класс, укрепленная Bronedver		5
Вибропреобразователь для стен «Молот»		17
Вибропреобразователь для коммуникаций(труб) «Серп-Т»		9
Вибропреобразователь для рам «Серп-Р»		5
Вибропреобразователь для окон «Копейка»		5
Преобразователь акустический «Рупор»		10
Размыкатель линий оповещения и сигнализации "Буран-К2"		3
Размыкатель компьютерных сетей "Буран-К3"		3
Модуль дистанционного управления по проводному каналу «Буран-ДУ»		1

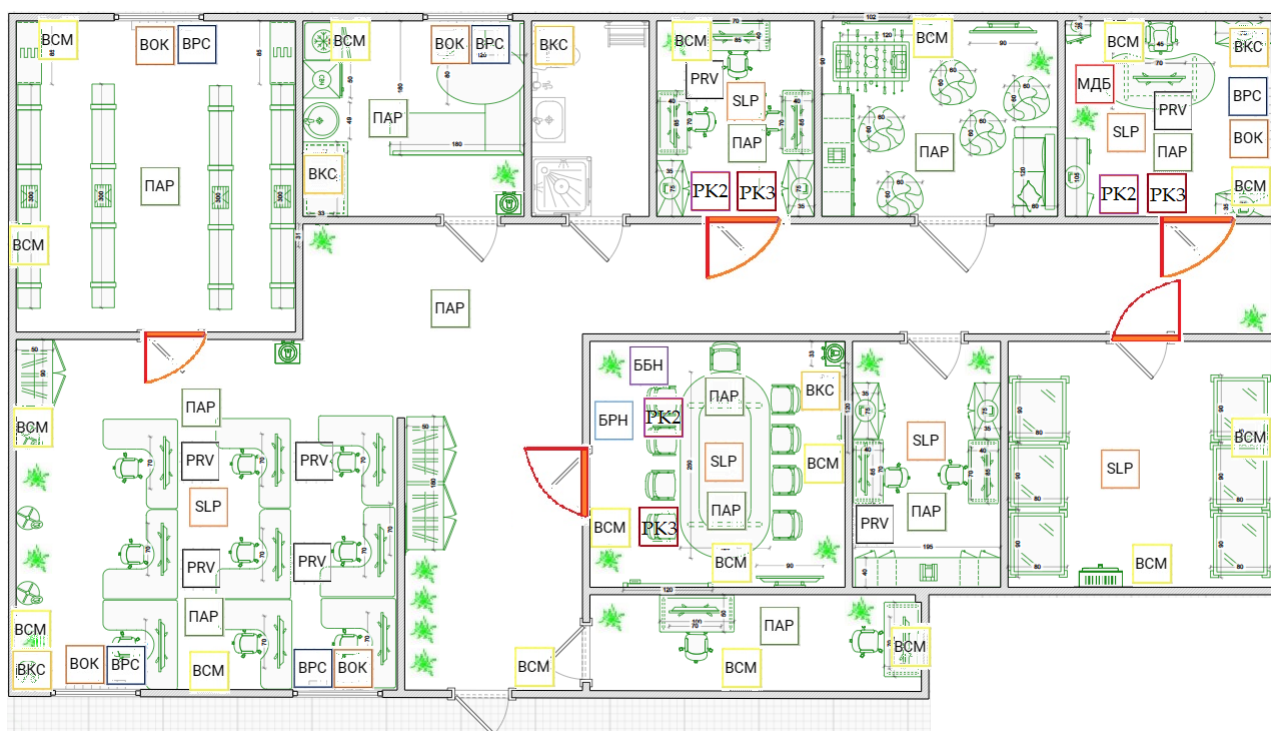


Рисунок 4 – Расстановка технических средств защиты

Заключение

В ходе данной работы был проведен анализ существующих каналов утечки информации, потенциальных каналов утечки информации в защищаемых в рамках курсовой работы помещениях и были описаны и приведены необходимые меры их защиты.

Был произведен анализ рынка существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие средства для выбранной организации.

Был разработан план помещения и план установки инженерных средств защиты информации и произведен расчет соответствующих на защиту затрат. В результате была предложена защита от утечек информации по акустическому, виброакустическому, электрическому, электромагнитному, оптико-электронному, оптическому, акустоэлектрическому каналам защиты информации и была обеспечена защита от ПЭМИН. Итоговое значение суммы затрат составило 1 003 300 рублей. Также, была нарисована схема расстановки устройств.

Цель курсовой работы была достигнута, все поставленные задачи выполнены.

Список литературы

1. Способы предотвращения утечки информации // searchinform URL: <https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sposoby-predotvrascheniya-utechki-informatsii/?ysclid=lq18z4fs2z659064915> (дата обращения: 22.10.2023).
2. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012 (23.10.2023 обращения: XXX).
3. Утечка информации компании // Ростелеком Солар URL: https://rt-solar.ru/products/solar_dozor/blog/2581/?ysclid=lq19h3eetq605163530 (дата обращения: 02.11.2023).
4. Требования к режимным помещениям и их оборудованию // КАСЛ URL: <https://licenziya-fsb.com/trebovaniya-k-rezhimnym-pomeshheniyam?ysclid=lq22t8ojgv679271593> (дата обращения: 05.11.2023).
5. Оборудование для защиты информации // INFOSECUR URL: <https://infosecur.ru/product/oborudovanie-dlya-zashchity-informatsii/> (дата обращения: 08.11.2023).

Приложение А

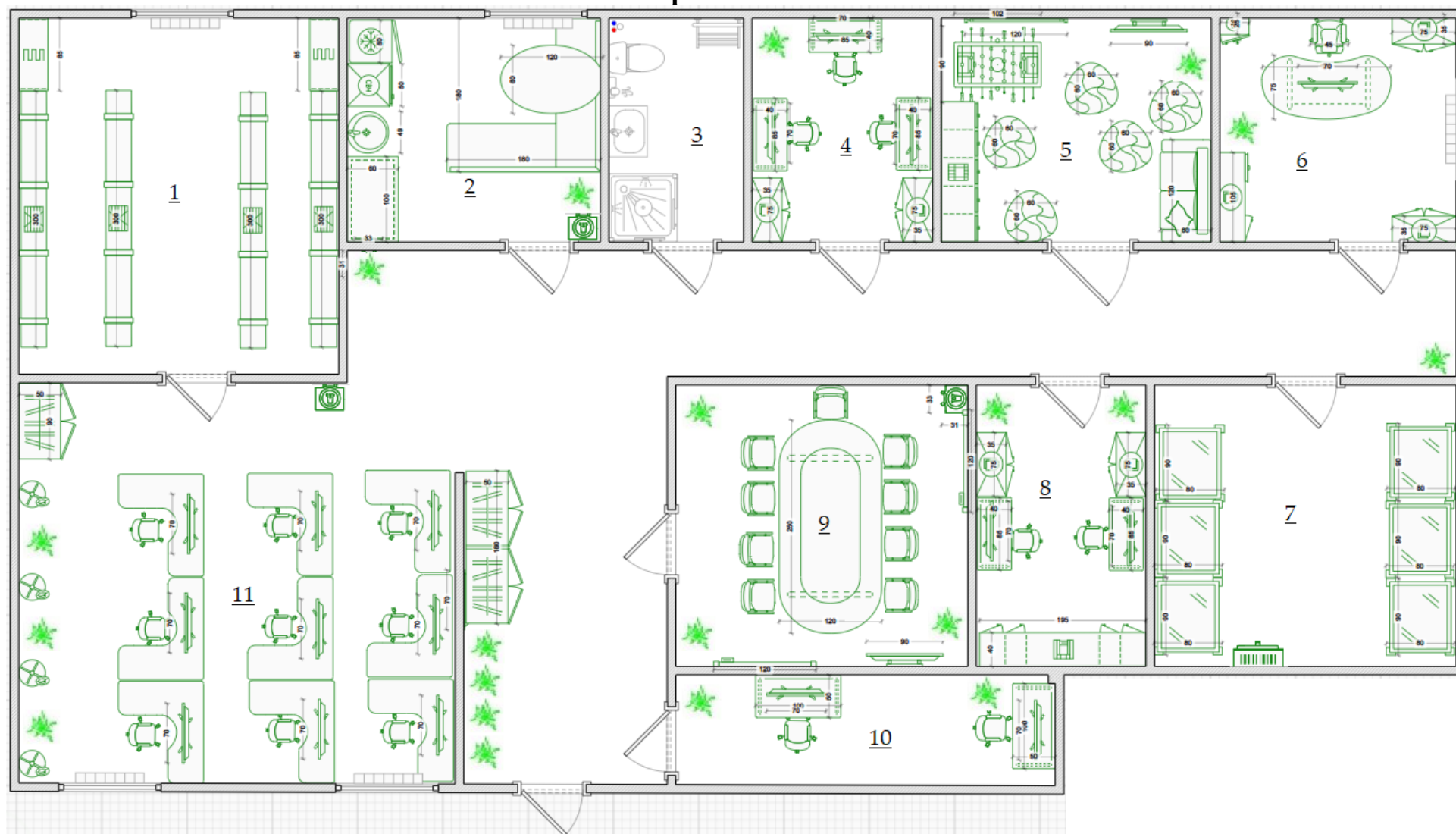


Рисунок 1А – План помещения

Приложение Б

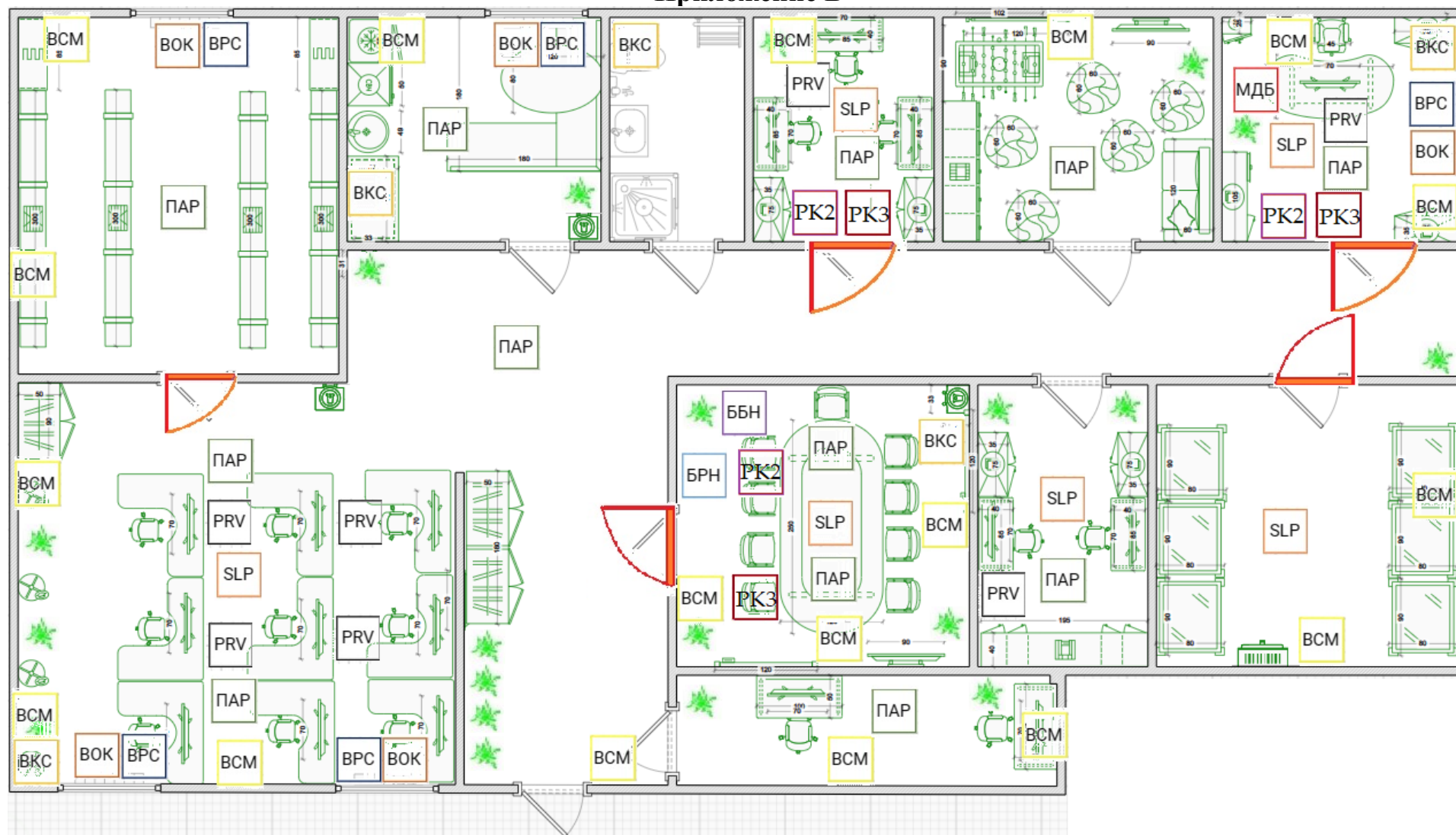


Рисунок 1Б – Схема расстановки устройств