

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

«Инженерно-технические средства защиты информации»

На тему:

**«Проектирование инженерно-технической системы защиты информации на
предприятии. Вариант 134»**

Выполнил:

Казаков М.В., студент
группы N34521



(подпись)

Проверил преподаватель:

Попов И.Ю., к.т.н., доцент
ФБИТ

(подпись)

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Казаков М.В.
	(Фамилия И.О.)
Факультет	Безопасности информационных технологий
Группа	N34521
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	Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 134
Задание	Проектирование системы защиты от утечки информации по различным каналам.

Краткие методические указания

Содержание пояснительной записки

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

Рекомендуемая литература

Руководитель	
	(Подпись, дата)
Студент	
	(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Казаков М.В.

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34511

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 Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 134

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Заполнение задания на курсовую работу	18.10.2023	18.10.2023	
2	Анализ материалов	20.10.2023	20.10.2023	
3	Написание курсовой работы	26.10.2023	26.10.2023	
4	Подготовка презентации	30.10.2023	30.10.2023	
5	Защита курсовой работы	19.12.2023	19.12.2023	

Руководитель _____
(Подпись, дата)

Студент 

(Подпись, дата)

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

Студент Казаков М.В.

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34511

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 Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 134

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы

☐ Предложены студентом

☒ Сформулированы при участии студента

☐ Определены руководителем

2. Характер работы

☐ Расчет

☐ Конструирование

☐ Моделирование

☒ Другое: Отчет

3. Содержание работы

Введение, анализ технических каналов утечки информации, руководящие документы, анализ защищаемых помещений, анализ рынка технических средств, описание расстановки технических средств, заключение, список литературы.

4. Выводы

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

Руководитель

(Подпись, дата)

Студент



(Подпись, дата)

«18» октября 2023 г

СОДЕРЖАНИЕ

Введение	6
1 Анализ технических каналов утечки информации.....	7
1.1 Физические каналы утечки информации	8
1.2 Технические каналы утечки информации.....	9
1.2.1 Акустические технические каналы утечки информации.....	9
1.2.2 Визуально – оптические технические каналы утечки информации	10
1.2.3 Электромагнитные технические каналы утечки информации	10
1.2.4 Материально-вещественные технические каналы утечки информации	10
1.3 Информационные каналы утечки информации.....	11
2 Руководящие документы.....	12
3 Анализ защищаемых помещений.....	14
3.1 Описание помещений.....	17
3.2 Анализ возможных утечек информации	18
3.3 Выбор средств защиты информации	18
4 Анализ технических средств защиты информации.....	20
4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации	20
4.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации	23
4.3 Защита от ПЭМИН	24
4.4 Защита от утечек по оптическому каналу	25
5 Описание расстановки технических средств	26
Заключение.....	29
Список использованных источников.....	30

ВВЕДЕНИЕ

Деятельность любого современного предприятия основана на обладании и управлении информацией. В связи с этим защита информации становится предметом пристального внимания, так как повсеместно внедряемые технологии и компоненты без соответствующих предосторожностей быстро становятся источниками проблем.

Средства защиты информации (СЗИ) обеспечивают защиту информации в информационных системах, по сути, представляющих собой совокупность хранимой в базах данных информации, информационных технологий, обеспечивающих ее обработку, и технических средств. Они позволяют предотвратить несанкционированный доступ злоумышленника к ресурсам и данным предприятия, тем самым снизив риск несанкционированных утечки, утраты, искажения, уничтожения, копирования и блокирования информации и, как следствие, нанесения экономического, репутационного или других видов ущерба предприятию. Разработка эффективного комплекса мер для выполнения данной задачи является одной из наиболее актуальных современных проблем. Технические средства защиты информации являются важной частью комплекса мер по обеспечению режима конфиденциальности на предприятии.

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

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечкой информации считают неправомерное распространение набора сведений, выходящее за пределы круга доверенных лиц или организаций, которые хранили эти сведения. Утечкой называют противоправное овладение чужой информацией вне зависимости от того, каким способом достигается получение данных. Утечка информации происходит при сопутствующих условиях, которые допускают ее возникновение:

- некомпетентность сотрудников, которые занимаются защитой данных, их непонимание важности процесса и халатное отношение к информации;
- использование нелегальных средств или не прошедших сертификацию программ по защите конфиденциальной информации;
- низкая степень контроля над средствами охраны сведений;
- постоянная смена сотрудников, которые занимаются защитой конфиденциальной информации.

Канал утечки информации – совокупность источника сигнала, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя.

При выявлении каналов утечки информации необходимо рассматривать всю совокупность элементов системы, включающую основное оборудование технических средств обработки информации, оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей информации, необходимо учитывать и вспомогательные технические средства и системы, такие как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др.

Канал утечки данных, которыми владеет компания, может быть физическим, техническим или информационным.

Физический канал возникает из-за недостаточной защиты бумажных или электронных носителей информации в процессе их перевозки, хранения, использования для работы. Появление такого канала позволяет злоумышленникам подслушивать служебные разговоры, скрытно изучать и копировать информацию ограниченного доступа.

Техническим называют канал, в котором источниками информации служат шумовые сигналы, излучения и вибрации, исходящие от интересующих объектов. Распространение

сигналов происходит через определенную физическую среду (волновую или электрическую). Для улавливания и расшифровки информационных сигналов используется специальная техника.

В информационных каналах происходит потеря компьютерных данных. Угрозы перехвата могут возникать из-за несоблюдения правил обработки, хранения и передачи информации или в результате использования слабозащищенного программного обеспечения.

1.1 Физические каналы утечки информации

Физическими называют каналы утечки информации, возникающие из-за слабой организации физической защиты данных от несанкционированного изучения и копирования, а также от похищения.

Канал подобных утечек может возникать в процессе:

- передачи сотрудникам документов из хранилища, обмена данными между работниками, знакомства клиентов и поставщиков с деятельностью предприятия;
- распечатки и тиражирования данных с помощью устройств общего пользования;
- перевозки документов без должной охраны;
- размещения документов в архивах и хранилищах;
- уничтожения данных с несоблюдением правил и требований безопасности.

Каналы утечки информации могут появиться из-за непродуманной организации рабочих мест сотрудников (тесного расположения столов, отсутствие перегородок между ними, хранения документации не в сейфах, а в обычных шкафах).

Причиной утечки графической информации может быть использование в дизайне помещений стеклянных перекрытий, сквозь которые можно визуально проследить за работой сотрудников и изучить обрабатываемые данные.

Для утечки акустической информации достаточно подслушивания разговоров между сотрудниками. Злоумышленники могут подслушать разговоры сотрудников, в которых оглашается конфиденциальная информация. Нередко происходят ситуации, в которых сотрудники обсуждают рабочие проблемы, находясь в общественных местах, провоцируя случайную утечку важной коммерческой информации.

1.2 Технические каналы утечки информации

Происхождение технического канала утечки информации (ТКУИ) может быть естественным и искусственным.

Естественный технический канал утечки информации появляется в результате способности физических объектов излучать тепло и свет, производить шумы, испускать радиоактивные лучи. Информация об интересующем объекте может быть получена путем косвенного изучения его физических характеристик и состава.

Искусственный канал утечки создается путем внедрения в линии связи закладных устройств, установки в рабочих помещениях малогабаритных приборов перехвата. ТКУИ подразделяют на:

- акустические;
- виброакустические;
- оптические;
- электромагнитные;
- материально-вещественные.

1.2.1 Акустические технические каналы утечки информации

Акустическими называют ТКУИ, которые образуются при прохождении звуковых волн через воздух, жидкие или твердые материалы.

Выделяют следующие разновидности акустического канала утечки информации:

- воздушный (перехват речевой информации производится с помощью чувствительных направленных микрофонов);
- виброакустический (злоумышленники используют устройства для улавливания вибрационных колебаний, вызываемых давлением звуковых волн на строительные конструкции зданий);
- электроакустический (утечка информации происходит из-за преобразования звукового сигнала в электрический при прохождении акустических волн через ВТСС);
- параметрический (поле, создаваемое источником акустического сигнала, может изменять параметры электромагнитных устройств, используемых злоумышленниками);
- оптико-акустический (причиной потери данных является «микрофонный» эффект).

1.2.2 Визуально – оптические технические каналы утечки информации

В оптических ТКУИ производится перехват видовой информации с помощью оптических приборов.

По способу перехвата информации визуально-оптические ТКУИ подразделяют на оптические каналы:

- визуального наблюдения (невооруженным глазом или через бинокль);
- фотографирования и видеосъемки;
- перехвата видимого и ИК-излучения, исходящего от объекта информации, с помощью скрытно установленных датчиков.

1.2.3 Электромагнитные технические каналы утечки информации

Источниками информационных сигналов в электромагнитном канале утечки информации могут быть:

- устройства передачи радиочастотных сигналов, установленные в функциональных каналах связи;
- побочные электромагнитные излучения и наводки;
- аппараты, испускающие тепловые электромагнитные волны;
- объекты, способные отражать радиосигналы.

В данном канале электромагнитные волны проходят сквозь воздух или распространяются по волноводам.

Выделяют следующие виды электромагнитного канала утечки информации:

- электрический (телефонные линии, с которых ведется перехват данных с помощью закладок);
- электромагнитный (для улавливания радиочастотных сигналов используются портативные разведывательные устройства);
- индукционный (производится бесконтактный перехват электромагнитных сигналов с использованием специальных датчиков).

1.2.4 Материально-вещественные технические каналы утечки информации

В материально-вещественных ТКУИ источниками информации становятся материальные объекты, выносимые за пределы рабочей зоны.

Материально-вещественные ТКУИ классифицируют, учитывая:

- физическое состояние информационных объектов (твердое, жидкое или газообразное);
- природу объектов перехвата (химическую, биологическую, радиоактивную, механическую);
- виды носителей (воздух, земля, вода).

1.3 Информационные каналы утечки информации

Информационный канал может быть разделен на следующие каналы:

- канал коммутируемых линий связи;
- канал выделенных линий связи;
- канал локальной сети;
- канал машинных носителей информации;
- канал терминальных и периферийных устройств.

В последнее время наиболее динамично развиваются методы съема компьютерной информации. В этом направлении используются:

- аппаратные закладки;
- вредоносные программы.

Основные возможности несанкционированного доступа связаны с использованием специального математического обеспечения, включающего в себя такие составляющие, как компьютерные вирусы, «логические бомбы», «троянские кони», программные закладки и т. п.

В настоящее время известно большое количество программных закладок, основные функции которых следующие:

- слежение за пользователем;
- раскрытие паролей, ключей;
- изучение обрабатываемой информации.

2 РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Основными документами в области защиты информации являются:

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

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

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

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

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

Перед проектированием технических средств защиты на объекте проведем анализ защищаемых помещений (Рисунок 1).

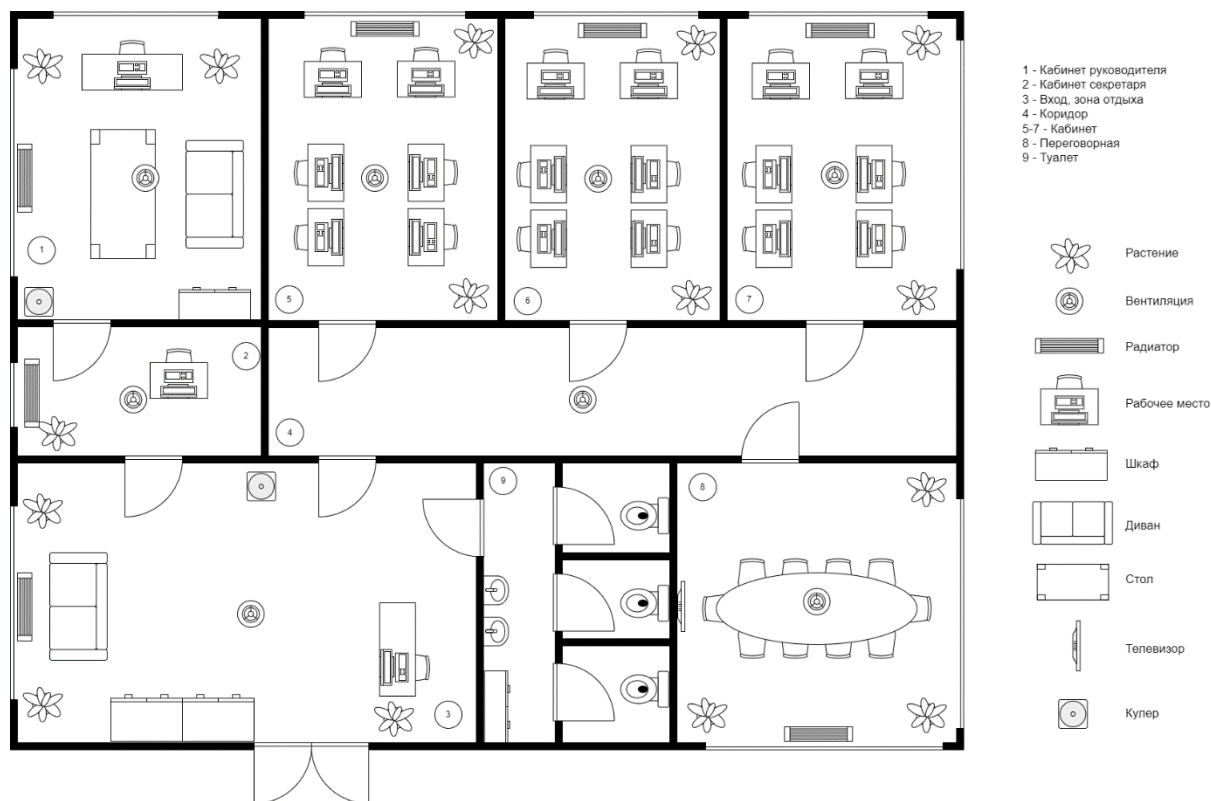


Рисунок 1 – План защищаемого помещения

Составим схему информационных потоков Организации (Рисунок 2).

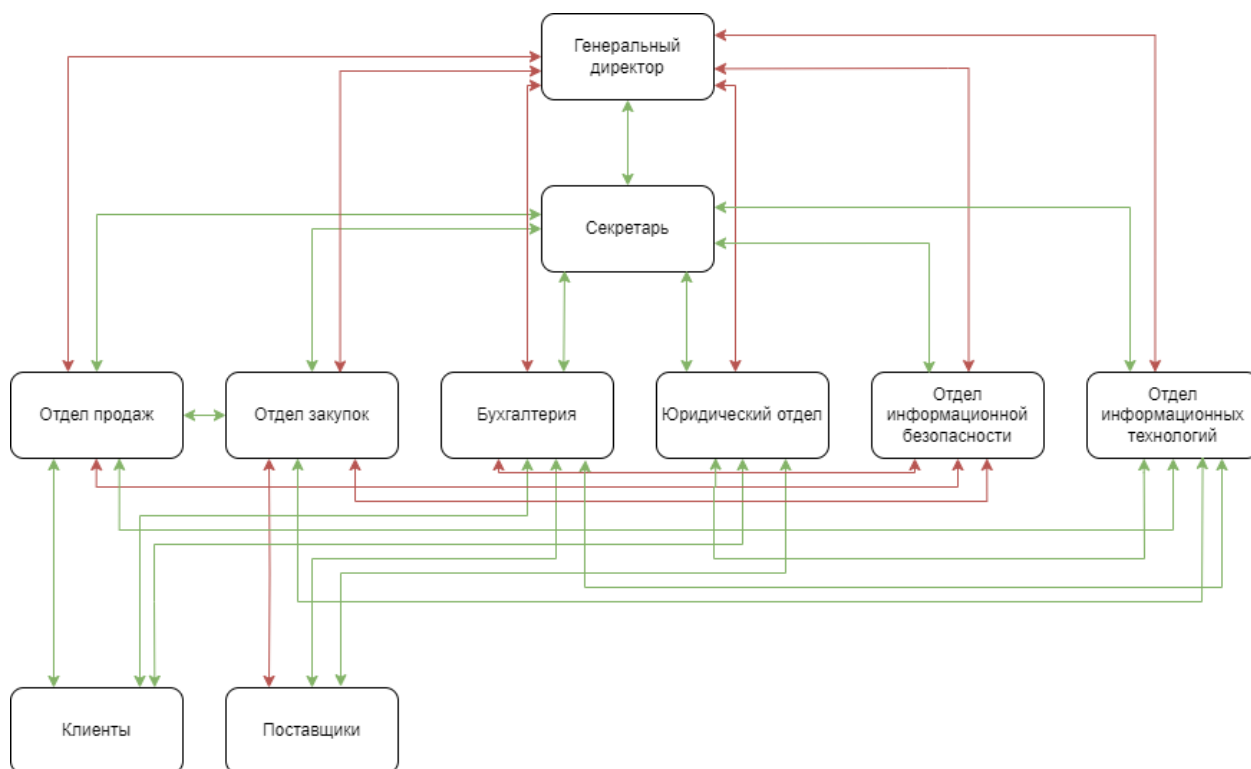


Рисунок 2 – Информационные потоки организации

Таблица 1 содержит описание закрытых двусторонних информационных потоков организации.

Таблица 1 – Закрытые информационные потоки

Стороны		Информация
Генеральный директор	Отдел продаж	Информация о продажах товаров
Генеральный директор	Отдел закупок	Информация о закупках товаров
Генеральный директор	Бухгалтерия	Информация о финансах
Генеральный директор	Юридический отдел	Юридическая информация
Генеральный директор	Отдел информационной безопасности	Информация о проводимых мероприятиях по обеспечению ИБ
Генеральный директор	Отдел информационных технологий	Информация о состоянии программного обеспечения и технических средств
Отдел продаж	Отдел информационной безопасности	Информация о проводимых мероприятиях по

		обеспечению ИБ
Отдел закупок	Поставщики	Поставщики
Отдел закупок	Отдел информационной безопасности	Информация о проводимых мероприятиях по обеспечению ИБ
Бухгалтерия	Отдел информационной безопасности	Информация о проводимых мероприятиях по обеспечению ИБ
Бухгалтерия	Юридический отдел	Финансово-юридическая информация
Юридический отдел	Отдел информационной безопасности	Информация о проводимых мероприятиях по обеспечению ИБ
Отдел информационной безопасности	Отдел информационных технологий	Информация о состоянии системы

Таблица 2 содержит описание открытых двусторонних информационных потоков организации.

Таблица 2 – Открытые информационные потоки

Стороны		Информация
Отдел продаж	Клиенты	Клиенты
Отдел продаж	Отдел закупок	Информация о наличии товаров
Отдел продаж	Отдел информационных технологий	Информация об установленном ПО и возникающих ошибках в ходе работы
Отдел закупок	Отдел информационных технологий	Информация об установленном ПО и возникающих ошибках в ходе работы
Бухгалтерия	Клиенты	Информация о платеже

Бухгалтерия	Поставщики	Информация о платеже
Юридический отдел	Клиенты	Юридическая информация
Юридический отдел	Поставщики	Юридическая информация
Юридический отдел	Отдел информационных технологий	Информация об установленном ПО и возникающих ошибках в ходе работы
Генеральный директор	Секретарь	Информация о распорядке дня директора
Юридический отдел	Секретарь	Информация о распорядке дня директора
Бухгалтерия	Секретарь	Информация о распорядке дня директора
Отдел закупок	Секретарь	Информация о распорядке дня директора
Отдел продаж	Секретарь	Информация о распорядке дня директора
Отдел информационных технологий	Секретарь	Информация о распорядке дня директора
Отдел информационной безопасности	Секретарь	Информация о распорядке дня директора

3.1 Описание помещений

Защите подлежат следующие помещения:

- кабинет руководителя, 24 кв. м;
- переговорная, 20 кв. м;
- кабинеты, 25 кв. м, 23 кв. м, 25 кв. м.

В кабинете директора расположены 2 стола, компьютер, шкаф, 2 цветка, радиатор, вентиляция, диван, кулер. В помещении также есть 2 окна.

В переговорной находятся большой стол, телевизор, 3 цветка, радиатор, вентиляция. В помещении имеется 2 окна.

В кабинетах расположены 6 столов и 6 компьютеров, 2 цветка, радиатор, вентиляция. В помещениях есть одно окно.

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

3.2 Анализ возможных утечек информации

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

3.3 Выбор средств защиты информации

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещение средствам защиты (Таблица 3).

Таблица 3 – Активная и пассивная защита информации

Канал утечки	Источник	Пассивная защита	Активная защита
Акустический, акустоэлектрический	Окна, двери, электрические сети, проводка	Звукоизоляция переговорной, фильтры для сетей электропитания	Звукоизоляция переговорной, фильтры для сетей электропитания
Вибрационный, виброакустический	Все твердые поверхности помещения, батареи	Дополнительное помещение перед переговорной, изолирующие звук и вибрацию обшивки	Устройства вибрационного зашумления

		стен	
Оптический	Окна, двери	Жалюзи на окнах, доводчики на дверях	Бликующие устройства
Электромагнитный, электрический	Розетки, АРМ, бытовая техника	Фильтры для сетей электропитания	Устройства электромагнитного защумления

4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

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

1. В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри – звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 см. Дверь устанавливается на металлический каркас.

2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.

3. По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене.

4. Все режимные помещения оборудуются аварийным освещением.

5. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.

6. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита представляет собой:

- усиленные двери,

- тамбурное помещение перед переговорной,
- жалюзи,
- дополнительная отделка переговорной звукоизолирующими материалами.

Активная защита представляет собой систему виброакустического зашумления. Для защиты помещения для работы с государственной тайной уровня «секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1В. Проведем сравнительный анализ подходящих средств активной защиты помещений по виброакустическому каналу (Таблица 4).

Таблица 4 – Сравнительный анализ средств активной защиты от утечки по виброакустическому каналу

Модель	Цена, руб.	Характеристики	Состав
ЛГШ-404	35100	Диапазон рабочих частот 175–11200 Гц	Изделие «ЛГШ-404» – генератор шума; 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 наблюдения и акустических микрофонов; Размыкатель «ЛУР» – для размыкания слаботочных линий.
Соната АВ-4Б	44200	Диапазон воспроизводимого шумового сигнала 175–11200 Гц	Блоки электропитания и управления – Соната-ИП4.1, Соната-ИП4.2, СонатаИП4.3; Генераторы-акустоизлучатели – СА-4Б, СА-4Б1; Генераторвибровозбудитель – СВ-4Б Размыкатель телефонной линии – Соната-ВК4.1; Размыкатель слаботочной линии – Соната-ВК4.2; Размыкатель линии Ethernet – Соната-ВК4.3; Пульт управления – Соната-ДУ4.3; Блоки сопряжения с

			<p>внешними устройствами – Соната-СК4.1, Соната-СК4.2; Техническое средство защиты речевой информации от утечки по оптикоэлектронному (лазерному) каналу – "Соната-АВ4Л":</p> <p>Генераторный блок "АВ-4Л" + вибровозбудитель "СП-4Л";</p> <p>Аксессуары – фиксатор труба, фиксатор стена, кабель.</p>
SEL SP-157 ШАГРЕНЬ	47400	<p>Диапазон воспроизводимого шумового сигнала 90–11200 Гц</p>	<p>Генератор SEL SP – 157G /БПК-155С; Вибропреобразователь SEL SP-57VP; Вибропреобразователь SEL SP-157VPS; Акустоизлучатель SEL SP-157AS; Регулятор выносной SEL SP-157P; Кабель электропитания; Разъем для подключения преобразователей; Комплект крепежа; Предохранитель 2А; Проводное ДУ SP 810; Руководство по эксплуатации; Формуляр (паспорт).</p>
КАМЕРТОН-5	46000	<p>Диапазон воспроизводимого шумового сигнала 90–11200 Гц</p>	<p>Система виброакустической защиты "Камертон-5"; Генератор маскирующего шума «Камертон-5» (ГМШ); Виброизлучатель ВП-4; Виброизлучатель ВД-микро; Виброизлучатель ВД-60; Виброизлучатель ВД-80; Виброизлучатель ВД-120; Акустоизлучатель АС-Ш; Акустоизлучатель АСП; Размыкатель сигнальных и линий оповещения Р-4С; Размыкатель</p>

			телефонных линий Р-4Т; Размыкатель локальной сети Р-8И; Размыкатель локальной сети Р-8И; Распределительная коробка РК-1; Виброштора ВШ-1; Виброштора Ш-2.
--	--	--	--

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

- создать систему автоматического контроля всех элементов;
- изменить настройки генераторов и построить гибкую систему виброакустической защиты;
- уменьшить затраты благодаря использованию единой линии связи и электропитания.

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

Пассивная защита основывается на установке фильтров для сетей электропитания во всех помещениях. Активная защита основывается на создании в сети белого шума, который скрывает колебания, порождаемые воздействием звуковой волны или работающей электрической техникой.

Таблица 5 – Сравнительный анализ средств активной защиты от утечки по электрическому каналу

Модель	Цена, руб.	Характеристики	Состав
ЛГШ-501	29900	Регулировка уровня шума – есть, диапазон регулировки уровня выходного шумового сигнала не менее 20 дБ;	Генератор шума по цепям электропитания, заземления и ПЭМИ

		Диапазон частот – 0,01–1800 МГц	
ГНОМЗМ-60В	61824	Регулировка уровня шума – нет; Диапазон частот – 0,15–1800 МГц	Генератор шума для защиты информации от утечки по каналам ПЭМИН, сети электропитания и контуру заземления
ЛГШ-513	39000	Регулировка уровня шума – есть; Диапазон частот 0,01–1800 МГц	Генератор шума по цепям электропитания, заземления и ПЭМИН
СОНАТАР-3.1	33120	Регулировка уровня шума – есть	Предназначено для защиты информации от утечки информации за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и токоведущие инженерные коммуникации

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

4.3 Защита от ПЭМИН

По результатам сравнительного анализа проведенного в 4.2 в качестве средства защиты от ПЭМИН была также выбрана «СОНАТА-РЗ.1».

4.4 Защита от утечек по оптическому каналу

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

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

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

- Усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей прокладкой на металлическом каркасе – 2 шт.;
- «Соната АВ-4Б»;
- «Соната-РЗ.1»;
- Жалюзи на 8 окон.

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

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

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

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

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

По результатам выбора средств защиты информации от утечки составим смету (Таблица 6).

Таблица 6 – Смета

Мера защиты	Цена, руб.	Количество, шт.	Стоимость, руб.
Блок электропитания и управления «Соната-ИП4.3»	21600	1	21600

Генераторакустоизлучатель "СА-4Б1"	7440	25	186000
Генераторвибровозбудитель "СВ-4Б1"	7440	47	349680
Пульт управления "Соната-ДУ4.3"	7680	1	7680
Генераторный блок "АВ-4Л"	10320	1	10320
Размыкатель телефонной линии "Соната-ВК4.1"	6000	2	12000
Размыкатель слаботочной линии "Соната-ВК4.2"	6000	1	6000
Размыкатель линии Ethernet "СонатаВК4.3"	6000	5	30000
Средство активной защиты информации от утечки за счет ПЭМИН "СонатаРЗ.1"	33120	1	33120
Жалюзи «Изолайт»	2990	8	23920
Усиленные двери «КД-3 правая»	72900	2	145800
Итого			820120

Элементы комплексной системы «Соната АВ-4Б» расположены согласно рисунку 3. «Соната-РЗ.1» подключена к блоку питания и управления и на схеме не обозначена.



Рисунок 3 – Схема расстановки технических средств

ЗАКЛЮЧЕНИЕ

В ходе курсовой работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении и описаны необходимые меры их защиты. Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для объекта средства защиты. Был разработан план установки средств и произведен расчет сметы затрат.

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

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хорев А. А. Техническая защита информации: учебное пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010. – 436 с.
2. Каналы утечки информации на предприятии - SearchInform. Дата просмотра: 22.10.2023 searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sluchai-utechkiinformatsii/kanaly-utechki-informatsii-na-predpriyatii/.
3. Угрозы информационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности информации. Защита информации от утечки по техническим каналам. Дата просмотра: 22.10.2023 learn.urfu.ru/resource/index/data/resource_id/40977/revision_id/0.
4. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.