

**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»

ОТЧЕТ ПО КУРСОВОЙ РАБОТЕ

«Проектирование инженерно-технической системы защиты информации на предприятии.

Вариант 39»

Выполнили:

Чан Нгок Хуан, студент группы N34471


(подпись)

Проверил:

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

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023г.

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

Студент	Чан Нгок Хуан (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34471
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. Вариант 39.
Задание	Проектирование инженерно-технической системы защиты информации на предприятии.

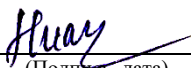
Краткие методические указания

1. Курсовая работа выполняется в рамках изучения дисциплины «Инженерно-технические средства защиты информации».
2. Порядок выполнения и защиты курсовой работы представлен в методических указаниях, размещенных на коммуникационной площадке дисциплины.
3. Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

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

Рекомендуемая литература

Руководитель	Попов Илья Юрьевич (Подпись, дата)
Студент	Чан Нгок Хуан  (Подпись, дата)

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

Студент Чан Нгок Хуан
(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34471

Направление (специальность) 10.03.01 Технологии защиты информации (2020)

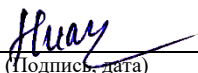
Руководитель Попов Илья Юрьевич, к.т.н., доцент факультета безопасности информационных технологий
(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 39.

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1.	Разработка и утверждение задания и календарного плана на курсовую работу	21.11.2023	21.11.2023	
2.	Анализ теоретической составляющей	09.12.2023	09.12.2023	
3.	Разработка комплекса инженернотехнической защиты информации в заданном помещении	15.12.2023	16.12.2023	
4.	Представление выполненной курсовой работы	19.12.2023	19.12.2023	

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Чан Нгок Хуан 
(Подпись, дата)

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

Студент	Чан Нгок Хуан	
	(Фамилия И.О)	
Факультет	Безопасность информационных технологий	
Группа	N34471	
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. Вариант 39.	

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы ☐ Предложены студентом ☐ Сформулированы при участии студент работы ☒ 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 ☐ Расчёт ☒ Конструирование
☐ Моделирование ☐ Другое

3. Содержание работы

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

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

Руководитель	Попов Илья Юрьевич
	(Подпись, дата)
Студент	Чан Нгок Хуан
	(Подпись, дата)

СОДЕРЖАНИЕ

Содержание	5
Введение	6
1 Анализ технических каналов утечки информации.....	7
1.1 Визуально-оптические каналы утечки	8
1.2 Радиоэлектронные каналы утечки	8
1.3 Акустические каналы утечки	9
1.4 Материально-вещественные каналы утечки.....	9
2 Анализ нормативной базы	10
3 Анализ защищаемых помещений.....	11
3.1 Анализ плана(Объекта).....	11
3.2 Информационные потоки предприятия	14
3.3 Анализ возможных утечек информации	14
3.4 Выбор средств защиты информации	15
4 Анализ технических средств защиты информации.....	16
4.1 Требования к средствам и мерам защиты информации.....	16
4.2 Устройства для перекрытия акустического и виброакустического каналов утечки информации	17
4.3 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации	19
4.4 Средства защиты от утечки по ПЭМИН	20
4.5 Устройства для защиты по оптическому каналу	21
5 Описание расстановки технических средств	22
Заключение.....	25
Список использованных источников.....	26

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 настоящей работе рассмотрен процесс разработки комплекса средств ИТЗ информации на объекте, в помещениях которого хранятся и обрабатываются данные, составляющие государственную тайну с грифом «совершенно секретно».

Цель работы – Повышение защищенности рассматриваемого помещения.

Для достижения поставленной цели необходимо решить следующие задачи:

- проанализировать защищаемые помещения;
- изучить нормативно-правовую базу;
- оценить каналы утечки информации;
- проанализировать средства защиты информации;
- разработать систему защиты информации на основе выбранных средств.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

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

Канал утечки информации(КУИ) – совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя. Одним из основных свойств канала является месторасположение средства выделения информации из сигнала или носителя, которое может быть в пределах контролируемой зоны, охватывающей систему, или вне ее.

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

Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация. На вход канала поступает информация в виде первичного сигнала.

Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода предыдущего канала. Так как информация от источника поступает на вход канала на языке источника (в виде буквенноцифрового текста, символов, знаков, звуков, сигналов и т. д.), то передатчик производит преобразование этой формы представления информации в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения.

Среда распространения сигнала - физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Она характеризуется набором физических параметров, определяющих условия перемещения сигнала.

Среда может быть однородная и неоднородная. Однородная - вода, воздух, металл и т.п. Неоднородная среда образуется за счет перехода сигнала из одной среды в другую, например, акустоэлектрические преобразования. Приемник выполняет функцию, обратную функции передатчика.

Таким образом, описание ТКУИ должно включать в себя:

- источник угрозы (приемник информативного сигнала);
- среда передачи информационного сигнала;
- источник (носитель) информации.



Рисунок 1 – Структура технического канала утечки информации

Основным признаком для классификации технических каналов утечки информации является физическая природа носителя. По этому признаку ТКУИ делятся на:

- визуально-оптические;
- радиоэлектронный;
- акустические;
- материально-вещественные.

1.1 Визуально-оптические каналы утечки

Каналы утечки графической информации, реализуются техническими средствами. И предоставляют информацию в виде изображений объектов или копий документов, получаемых путем наблюдения за объектом, съемки объекта и съемки (копирования) документов. В зависимости от условий наблюдения обычно используются соответствующие технические средства, в том числе: оптика (бинокли, подзорные трубы, телескопы, монокуляры), телекамеры, приборы ночного видения, тепловизоры и т.п. Для документирования результатов наблюдения проводится съемка объектов, для чего используются фотографические и телевизионные средства, соответствующие условиям съемки. Для снятия копий документов используются электронные и специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют видеозакладки, либо осуществляют видеосъемку из зданий расположенных по близости.

1.2 Радиоэлектронные каналы утечки

Носителем информации в радиоэлектронном КУИ являются электромагнитные поля, а также электрический ток. Электромагнитные каналы утечки информации – это методы перехвата и получения конфиденциальной информации путем анализа электромагнитных излучений, которые генерируются различными устройствами.

Диапазон передачи радиоэлектронного КУИ подразделяется на:

- низкочастотный (30–300 кГц);
- среднечастотный (300 кГц–3 МГц);
- высокочастотный (3–30 МГц);
- ультравысокочастотный (30–300 МГц);
- сверхвысокочастотный (до 30 ГГц).

В зависимости от диапазона используются различные средства съема и передачи информации, а также различные каналы их передачи (проводные или беспроводные).

Множество устройств, таких как компьютеры, мобильные телефоны, планшеты и другие электронные устройства, генерируют электромагнитные волны в процессе своей работы. Эти волны могут быть перехвачены и анализированы злоумышленниками для получения информации, которая должна быть конфиденциальной.

1.3 Акустические каналы утечки

Акустические каналы утечки информации основаны на использовании звуковых волн для передачи и перехвата конфиденциальной информации. Звуковые волны могут быть созданы различными источниками, такими как голосовые разговоры, звуки клавиатуры, вентиляторы и другие устройства.

Злоумышленники могут использовать специальное оборудование или программное обеспечение для перехвата и анализа звуковых волн, создаваемых компьютером или другими устройствами.

1.4 Материально-вещественные каналы утечки

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных носителей с защищаемой информацией. В качестве вещественных носителей чаще всего выступают черновики документов и использованная копировальная бумага.

2 АНАЛИЗ НОРМАТИВНОЙ БАЗЫ

Основными документами, регулирующими деятельность в области защиты информации, являются:

- 1) Федеральный закон Российской Федерации от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- 2) Закон Российской Федерации от 21.07.1993 N 5485-1 «О государственной тайне»;
- 3) Указ Президента РФ от 06.03.1997 N 188 «Об утверждении Перечня сведений конфиденциального характера»;
- 4) Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- 5) Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»;
- 6) Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Основными руководящими документами в области ИТЗИ и средств ИТЗ являются:

- 1) СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации;
- 2) Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации;
- 3) Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации;
- 4) Временный порядок аттестации объектов информатизации по требованиям безопасности информации;
- 5) Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения;
- 6) Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;
- 7) Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Анализ плана(Объекта)

Объект представляет собой компанию, занимающуюся научно-исследовательской и опытно-конструкторской работой в стратегически важных для Российской Федерации областях.

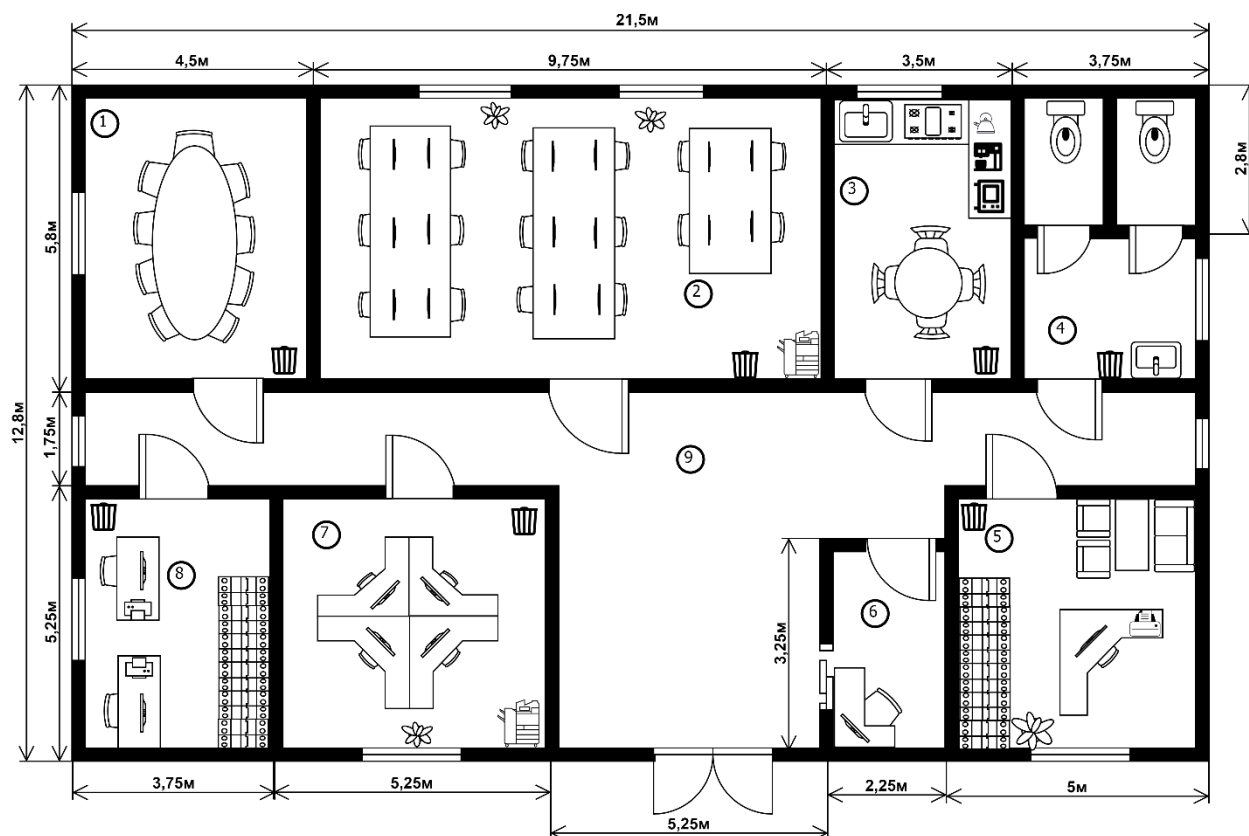


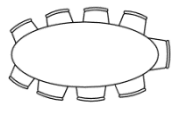
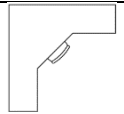
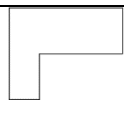


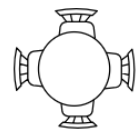

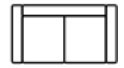

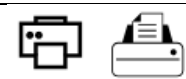
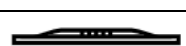
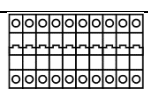









Рисунок 2 – План помещения

Таблица 1 – Условные обозначения плана помещений объекта

Обозначение	Количество	Наименование обозначаемого объекта
	10	Окно
	1	Окошко охраны
		Стена
	10	Дверь
	1	Двойная дверь

	1	Стол для конференций с 9 стульями
	5	Угловой компьютерный стол со стулом
	1	Угловой стол
	6	Стол
	19	Стул
	1	Кухонный стол с 4 стульями
	2	Двойной диван
	1	Диван
	2	Копировальная машина
	3	Принтеры
	24	АРМ
	2	Шкафы
	1	Чайник
	1	Кофеварка
	1	Микроволновка
	1	Индукционная плита
	4	Растение
	4	Элементы санузла
	7	Мусорная корзина

Помещения объекта состоят из:

- 1) Переговорная – 26,1м². Содержит стол для конференций с 9 стульями, оборудование для выступлений (маркерная доска, экран, проектор, микрофон, динамики), мусорную корзину, 1 окна и 1 радиатор под окном. Соединена с общим коридором;
- 2) Рабочее пространство (офис) – 56,55м². Содержит 3 больших стола, 10 стульев, 10 АРМ, 2 растения в горшках, 1 копировальный аппарат, мусорную корзину, 2 радиатора под окнами. Соединено с общим коридором;
- 3) Кухня – 20,3м². В этой комнате есть 1 раковина, 1 индукционная плита, 1 электрический чайник, 1 кофеварка, 1 микроволновка, мусорную корзину, 1 круглый стол и 4 стула.
- 4) Туалет(Санузел) – 10,5м²
- 5) Кабинет директора – 26,25м². Содержит угловой стол со стулом, 1 шкаф, АРМ, сканер, шредер, мусорную корзину, окно на восточной стороне здания и 1 радиатор под окном. Соединен с общим коридором;
- 6) Комната охраны – 7,3м². Содержит угловой стол, стул, компьютер охраны, щиток электропитания, КПУ охранной и пожарной сигнализации объекта, 1 радиатор под окнами и окно, выходящее к входной двери. Соединено с общим коридором;
- 7) Отдел разработчики – 27,6м². Содержит 4 угловых стола, 4 АРМ, 1 копировальный аппарат, 1 растение в горшке, мусорную корзину, окно на восточной стороне здания и 1 радиатор под окнами.
- 8) Бухгалтерия – 19,7м². Содержит сейф, шкаф, 2 стола, 2 стула, 2 принтера, мусорную корзину, 2 АРМ, окно на восточной стороне здания и 1 радиатор под окном. Соединена с общим коридором;
- 9) Коридор. Соединен с бухгалтерией, отделом разработчики, комнатой охраны, кабинетом директора, кухней, рабочим пространством и переговорной.

Все помещения электрифицированы, оснащены пожарной и охранной сигнализацией, системой освещения, имеют розетки.

Объект расположен на первом этаже многоэтажного здания, окна выходят в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными лестницами и элементами, с которых в помещения могут проникнуть внешние нарушители, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица.

Стены и внутренние перегородки здания железобетонные, толщиной 10 см, высотой 3 м.

3.2 Информационные потоки предприятия

На схеме информационных потоков зеленым отмечены открытые потоки, а красным – закрытые(рисунок 3).

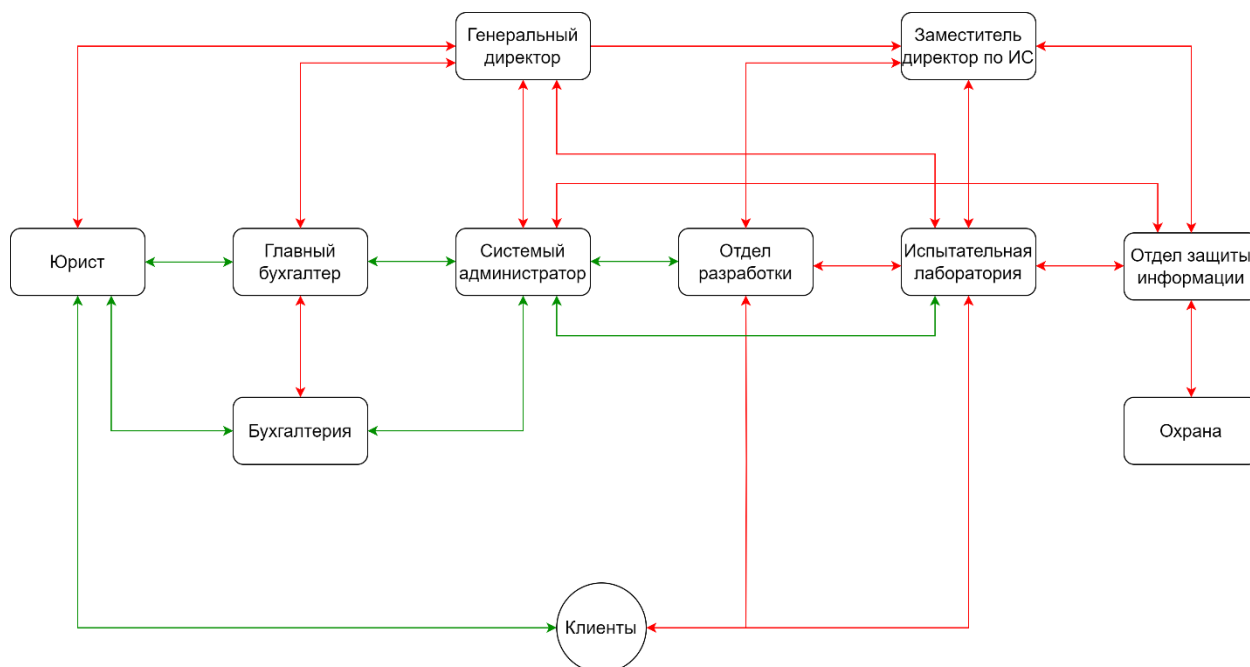


Рисунок 3 – Схема информационных потоков предприятия

3.3 Анализ возможных утечек информации

В помещениях присутствуют элементы, где можно спрятать закладное устройство, такие как: шкафы, растения. Окна помещений не защищены, поэтому актуальны акустический (при открытом окне), в частности, виброакустический, оптический каналы утечки информации. В каждом помещении имеются розетки, а значит, актуальны электрического и электромагнитного каналов утечки информации. Стены, пол, потолки, радиатор не защищены от съема акустической информации, генераторы фонового шума не используются, поэтому актуален акустический, в частности, виброакустический канал утечки информации.

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

3.4 Выбор средств защиты информации

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

Таблица 2 – Активная и пассивная защита информации

Канал передачи	Источник	Пассивная защита	Активная защита
Акустический	Окна, двери	Звукоизоляция помещения	Устройства акустического зашумления
Акустоэлектрический	Сети электропитания	Сетевые фильтры	Устройства акустического зашумления
Вибрационный, виброакустический	Стены, пол, потолок, двери, другие твердые поверхности	Изоляция стен, дверей в виде дополнительных обшивок	Устройств Авибрационного зашумления
Оптический	окна, двери	жалюзи на окнах, доводчики на дверях	Бликующие устройства
Радиоэлектронный	Розетки, электрические приборы, АРМ, сети передачи информации	Сетевые фильтры, экранирование проводов	Сетевые фильтры, экранирование проводов

4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

4.1 Требования к средствам и мерам защиты информации

Согласно заданию курсовой работы, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «совершенно секретно». Исходя из требований «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 № 199, защита рассматриваемых помещений должна удовлетворять следующим критериям:

- В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие и звукоизоляцию. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри – звукоизоляционный материал, сама дверь должна иметь толщину не менее 4,5 см. Дверь устанавливается на металлический каркас, для надежного крепления;
- По требованиям безопасности режимных помещений, если окна в комнатах и хранилищах 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;
- 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;
- Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании;
- Все режимные помещения оборудуются аварийным освещением;
- Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

4.2 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита представляет собой:

- установка усиленных дверей;
- установка фильтров для сетей электропитания;
- установка жалюзи на окна;
- дополнительная отделка переговорной звукоизолирующими материалами.

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

Таблица 3 – Сравнительный анализ активной защиты виброакустического канала

Наименование средства	Характеристики	Состав	Финальная стоимость(руб.)
Соната АВ-4Б	Сертификат ФСТЭК, диапазон воспроизводимого шумового сигнала: 175-11200 Гц. Максимальное количество излучателей: 239шт.	В комплект входят акустоизлучатели, вибровозбудители, размыкатель телефонной линии, размыкатель слаботочной линии, размыкатель линии Ethernet, блок сопряжения с внешними устройствами и т.д.	44200
Барон-S1	Диапазон частот: 60-16000Гц	Кабель для подключения к ПЭВМ, сетевой шнур, техническое описание; дополнительно устройство контроля эффективности помех Барон-К, Барон-ДК, устройство дистанционного включения Барон-В	33500

Камертон-5	Сертифицированн ФСТЭК, диапазон рабочих частот 90 - 11200 Гц.	В комплект входит блок управления и контроля системой, блок генерации и генератор маскирующих шумов, виброизлучатели, акустоизлучатели, размыкатели проводных линий, виброшторы.	46000
SEL SP-157 ШАГРЕНЬ	Диапазон воспроизводимого шумового сигнала: 90-11200Гц. Максимальное количество излучателей: 64шт.	Содержит два независимых канала генерации с семиполосным эквалайзером и двумя параллельными выходами на нагрузку, автоматическая диагностика генератора, электронный счётчик времени наработки в режиме генерации отдельно по каждому каналу, в комплект входит блок питания, вибровозбудители, акустические излучатели.	47400

По результатам анализа таблицы 3 была выбрана система НПО «Анна» Соната «АВ» модель 4Б. Кроме того, что она является наиболее популярным решением для этого класса защиты (отмечена как «хит продаж» на нескольких сайтах-агрегаторах), она сочетает в себе умеренную стоимость с большим диапазоном регулирования уровня шума.

Из преимуществ системы — существенное увеличение стойкости защиты за счет многогенераторного независимого возбуждения заградительной помехи в нескольких точках и вследствие исключения электроакустического преобразования в излучателях, а также существенное снижение стоимости комплексов виброакустической защиты вследствие предельной безизбыточности комплексов защиты (возможно комбинирование на одном питающем шлейфе любых сочетаний излучателей).

4.3 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.

Для этого необходимо разобрать устройства для создания подобного зашумления (электрического):

Таблица 4 – Средства защиты от утечек по электрическим каналам

Наименование средства	Характеристики	Состав	Финальная стоимость(руб.)
ЛГШ-513	Сертификат ФСТЭК. Диапазон частот: 10кГц-1800 МГц	Генератор шума по цепям электропитания, заземления и ПЭМИН. Возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».	39000
SEL SP-44	Сертификат ФСТЭК. Диапазон частот: 10кГц-400МГц.	Генератор шума; активная защита конфиденциальных сведений от утечки по проводам электропитания; возможность регулировки уровня ВЧ и НЧ шумов; функция самодиагностики для оперативного выявления неисправностей и сбоев в работе.	26000
СОНАТА-РСЗ	Сертифицировано ФСТЭК.	Устройства для защиты линий электропитания, заземления от	32400

		утечки информации(Генератор шума). Возможно дистанционное управление посредством проводного пульта;	
Гном 3М	Сертификат ФСТЭК. Создает полосу помех в диапазоне частот 150кГц-1800МГц.	Имеет 4 выхода для подключения к цепям электропитания и к антенным контурам; система контроля функционирования генераторов.	57200

На основании анализа, приведенного в таблице 4, был выбран генератор шума Соната-РС3. Генератор шума СОНАТА-РС3 – средство активной защиты конфиденциальной информации от утечки по проводам электросети. Это устройство предназначено для использования в помещениях, в которых на электронно-вычислительных машинах обрабатываются данные, являющиеся коммерческой либо государственной тайной. Он имеет характеристики, сравнимые с конкурентами:

- 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.

4.4 Средства защиты от утечки по ПЭМИН

Для определения активной защиты от ПЭМИН необходимо разобрать устройства для создания подобного зашумления:

Таблица 5 – Активная защита от ПЭМИН

Наименование средства	Характеристики	Состав	Финальная стоимость, руб.
SEL 111 «ШИФОН»	Сертификат ФСБ. Диапазон частот: 10кГц – 3000МГц.	Генератор шума от ПЭМИН; управление с панели, проводное ДУ, по сети Ethernet 10/100 МБт; индикация светодиодная, текстовая и звуковая	64000

ЛГШ-504	Сертификат ФСБ России. Диапазон частот: 0,009 - 1000 МГц.	Генератор шума от ПЭМИН; ПАК Паутина по Ethernet	156000
СОНАТА-РЗ.1	Сертификат ФСТЭК. Диапазон частот шумового сигнала 0,01 – 200 МГц.	Генератор шума от ПЭМИН; пульт управления «Соната-ДУ4.1» в комплексе с блоком питания и управления «Соната-ИП4.х»; пульт управления «Соната-ДУ4.2»	33120

Для реализации активной защиты от ПЭМИН было выбрано устройство НПО «Анна» СОНАТА-РЗ.1. Данный выбор обоснован тем, что управление его работой и контроль режима работы может осуществляться от пульта управления «Соната-ДУ4.1» в комплексе с блоком питания «Соната-ИП4.х», т. е. устройство может быть встроено в систему СОНАТА АВ-4Б, выбранную как реализация активной защиты по виброакустическому каналу.

4.5 Устройства для защиты по оптическому каналу

Для обеспечения защиты помещения от визуального наблюдения, необходимо установить на окно жалюзи. Для данной организации было решено установить жалюзи на все окна в каждом помещении.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

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

- система виброакустической защиты СОНАТА АВ-4Б, НПО «Анна»;
- сетевой генератор шума Соната-РС3, НПО «Анна»;
- средство защиты от ПЭМИН СОНАТА-РЗ.1, НПО «Анна»;
- установка 5 усиленных дверей толщиной более 4 мм, обшитые металлом,

толщиной не менее 2 мм со звукоизолирующей прокладкой на металлическом каркасе.

Устанавливаются в кабинет директора, переговорную и 3 кабинета;

- жалюзи на все окна в офисе.

Оптимальное количество акустоизлучателей и вибровозбудителей для каждого помещения определяется множеством факторов. Согласно официальному сайту НПО «Анна», необходимое количество генераторов-вибровозбудителей СВ-4Б 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 м² перекрытия;
- один на окно (при установке на оконный переплет);
- один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Необходимое количество генераторов-акустоизлучателей СВ-4Б можно предварительно оценить из следующих норм:

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

Также размыкатели слаботочных линий «Соната-ВК4.1» предназначены для защиты информации от утечки за счет акустоэлектрических преобразований и ВЧ-навязывания по телефонным линиям, «Соната-ВК4.2» по соединительным линиям систем оповещения и сигнализации, а «Соната-ВК4.3» по линиям компьютерных сетей. Элементы комплексной системы «СОНАТА АВ-4Б» расположены на структурной схеме на Рисунке 4. «СОНАТА-РЗ.1», «СОНАТА-РС3» подключены напрямую к «Соната-ИП4.3» из системы СОНАТА АВ-4Б. Пульт управления «Соната-ДУ 4.3.» 1 шт. для всей системы.

Таблица 6 – Количество и стоимость необходимого оборудования

Средство защиты	Цена, руб.	Кол-во	Стоимость, руб.
Усиленные звукоизолирующие двери Ultimatum Nex NC-2	65632	5	328 160
Жалюзи-blackout	2150	7	15 050
СОНАТА-РЗ.1	33120	2	66 240
Генератор шума СОНАТА-РСЗ	32400	5	162 000
Размыкатель телефонной линии «Соната- ВК4.1»	6000	2	12 000
Размыкатель слаботочной линии «Соната- ВК4.2»	6000	1	6 000
Размыкатель линии Ethernet «Соната-ВК4.3»	6000	2	12 000
Блок электропитания и управления «Соната- ИП4.3»	21600	1	21 600
Пульт управления «Соната-ДУ4.3»	7680	1	7 680
Генератор-акустоизлучатель СА-4Б	7440	20	148 800
Генератор-вибровозбудитель СВ-4Б	7440	81	602 640
Итого			1 382 170

На схеме показано расположение средств защиты.

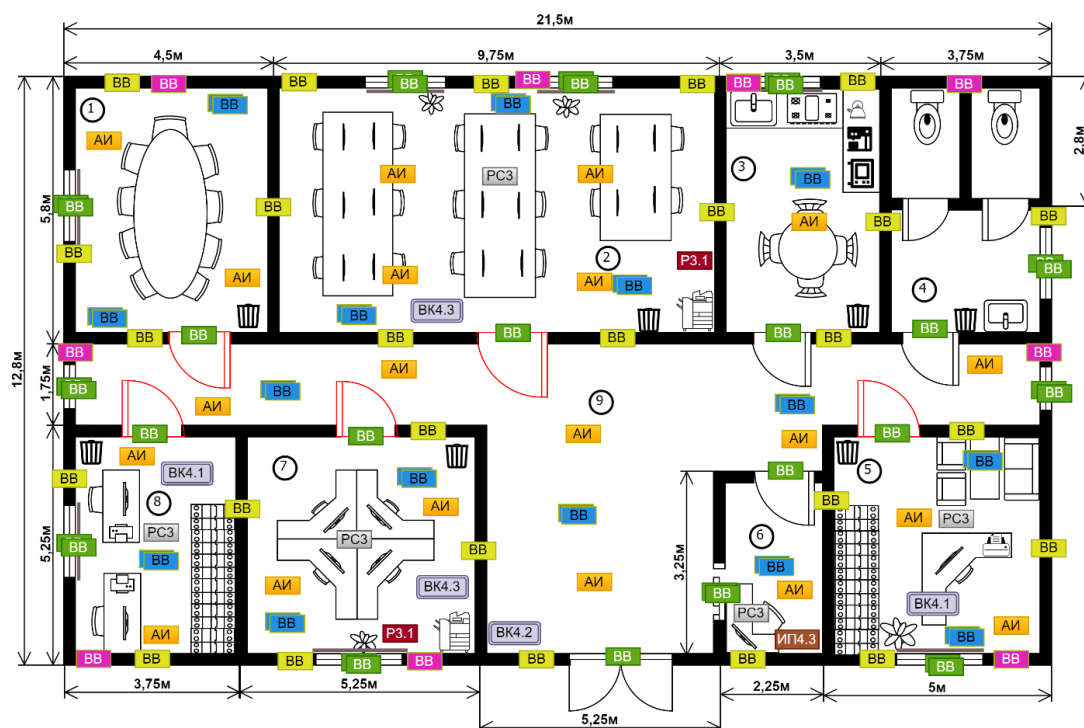








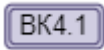

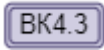




Рисунок 4 – Схема расстановки средств защиты

Таблица 7 – Условные обозначения схемы расстановки устройств

Средство защиты	Условное обозначение
Усиленные звукоизолирующие двери	
Жалюзи–blackout	
Генератор–акустоизлучатель СА-4Б	
Генераторы-вибровозбудители СВ-4Б (двери, окна, батареи)	
Генераторы-вибровозбудители СВ-4Б (стены)	
Генераторы-вибровозбудители СВ-4Б (пол, потолок)	
Генераторы-вибровозбудители СВ-4Б (трубопровод)	
Блок электропитания и управления «Соната-ИП4.3»	
Размыкатель телефонной линии «Соната-ВК4.1»	
Размыкатель слаботочной линии «Соната-ВК4.2»	
Размыкатель линии Ethernet «Соната-ВК4.3»	
Генератор шума Соната-РС3	
СОНАТА-РЗ.1	

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации на защищаемом объекте. Также сделано описание необходимых мер защиты от соответствующих утечек. Помимо этого был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации. Исходя из анализа, были выбраны подходящие для обзореваемого объекта. План установки технических средств разработан, расчеты сметы затрат отражены в 5 главе работы. В результате предложена защита от утечек информации по акустическому, виброакустическому, акустоэлектрическому, электрическому, электромагнитному, оптико-электронному и оптическому техническим каналам защиты информации, обеспечена защита от ПЭМИН. Затраты на обеспечение защиты составляют 1 382 170 руб., что можно считать оправданной суммой для объекта, который содержит информацию, составляющую государственную тайну уровня «совершенно секретно».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1) Средства защиты переговоров. – Текст : электронный // Detector Systems : [сайт]. – URL: <https://detsys.ru/catalog/> (дата обращения: 14.12.2023).
- 2) Технические каналы утечки информации. – Текст : электронный // ИРС : [сайт]. – URL: <https://intuit.ru/studies/courses/3649/891/lecture/32330> (дата обращения: 14.12.2023).
- 3) Каторин Ю. Ф. Защита информации техническими средствами : Учебное пособие / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак. – Санкт-Петербург : НИУ ИТМО, 2012. – 417 с. — Текст : электронный // ИРС : [сайт]. – URL: <https://books.ifmo.ru/file/pdf/975.pdf> (дата обращения: 14.12.2023).