

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

Факультет безопасности информационных технологий

Дисциплина:

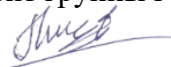
«Инженерно-технические средства защиты информации»

ОТЧЕТ ПО КУРСОВОЙ РАБОТЕ

«Разработка комплекса инженерно-технической защиты информации в помещении»

Выполнили:

Нгуен Куанг Туан, студент группы N34511



(подпись)

Проверил:

Попов И.Ю., К.т.н., доцент ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

Студент Нгуен Куанг Туан

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34511

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 Разработка комплекса инженерно-технической защиты информации в помещении

Задание Разработка комплекса инженерно-технической защиты информации в помещении

Краткие методические указания

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

Содержание пояснительной записки

Пояснительная записка включает разделы: введение, анализ технических каналов утечки информации, перечень руководящих документов, анализ защищаемых помещений, анализ рынка технических средств, расстановка технических средств, заключение, список использованных источников.

Рекомендуемая литература

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Нгуен Куанг Туан

(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Нгуен Куанг Туан

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34511

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 Разработка комплекса инженерно-технической защиты информации в помещении

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	15.11.2023	15.11.2023	
2	Анализ теоретической составляющей	02.12.2023	02.12.2023	
3	Разработка комплекса инженернотехнической защиты информации в заданном помещении	11.12.2023	11.12.2023	
4	Представление выполненной курсовой работы	25.12.2023	25.12.2023	

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Нгуен Куанг Туан

(Подпись, дата)

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

Студент Нгуен Куанг Туан

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34511

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 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

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

**2. Характер
работы**

☐ Расчет

☒ Конструирование

☐ Моделирование

☐ Другое

3. Содержание работы

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

4. Выводы

В результате работы 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 Нгуен Куанг Туан

(Подпись, дата)

СОДЕРЖАНИЕ

Содержание	4
Введение	5
1 Анализ технических каналов утечки информации.....	6
1.1 Акустические каналы утечки информации.....	7
1.2 Материально-вещественные каналы утечки информации	8
1.3 Визуально-оптические каналы утечки информации.....	8
1.4 Электромагнитные каналы утечки информации	8
2 Перечень руководящих документов	10
3 Анализ защищаемых помещений.....	12
3.1 План помещений и информационные потоки предприятия.....	12
3.2 Описание помещений.....	15
3.3 Анализ возможных утечек информации	16
3.4 Выбор средств защиты информации	16
4 Анализ технических средств защиты информации.....	18
4.1 Требования к защите помещений	18
4.2 Анализ СЗИ для акустического и виброакустического каналов	19
4.3 Анализ СЗИ для визуально-оптического канала	20
4.4 Анализ СЗИ для электромагнитного, электрического каналов	20
5 Расстановка 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 данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем “совершенно секретно” на предприятии. Защищаемый объект состоит из кабинета директора, переговорной, офисов, серверного помещения.

Данная работа состоит из пяти глав. В первой главе произведен анализ технических каналов утечки информации. Во второй приведён перечень управляющих документов, в третьей – анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств. Четвертая глава представляет собой анализ рынка технических средств защиты информации разных категорий, и пятая глава посвящена разработке схем расстановки выбранных технических средств в защищаемом помещении.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечка информации – неконтролируемый выход конфиденциальных сведений за пределы предприятия, помещения, здания, какой-либо территории или круга лиц, которым доверили хранение информации ограниченного круга лиц. Утечка происходит по каналам передачи данных. Неконтролируемые каналы нарушают безопасность систем защиты.

Для похищения сведений о новаторских технологиях, секретных разработках и других конфиденциальных данных злоумышленники стремятся получить доступ к каналам утечки информации. При этом они пользуются различными средствами аппаратной разведки, предназначенной для перехвата речевой и визуальной информации.

Технический канал утечки информации (ТКУИ) – это путь информации, который она может пройти от источника информации до приемника/получателя в процессе случайной утечки или целенаправленного несанкционированного получения закрытой информации. Если меры по защите информации не были приняты заранее, то могут быть задействованы любые каналы утечки. На рисунке 1 представлена общая структурная схема любого канала утечки информации.



Рисунок 1 – Структура технического канала утечки информации

Защита от утечки информации требует проведения административно-организационных и инженерно-технических мер, которые выявляют вероятные технические каналы утечки информации (ТКУИ), чтобы избежать их возможного использования.

Выделяются четыре основных группы технических способов организации утечки информации (рисунок 2):

- акустические, позволяющие перехватывать ведущиеся в помещении переговоры или разговоры по телефонам;
- материально-вещественные, связанные с анализом предметов, документов и отходов, возникших в результате деятельности компании;

- визуально-оптические, позволяющие перехватывать или копировать сведения, отражающиеся в визуальной форме, это документы, информация, выведенная на экран монитора компьютера;
- электромагнитные, позволяющие получать данные, выраженные в виде излучения электромагнитных волн, их дешифровка может также дать необходимые сведения.

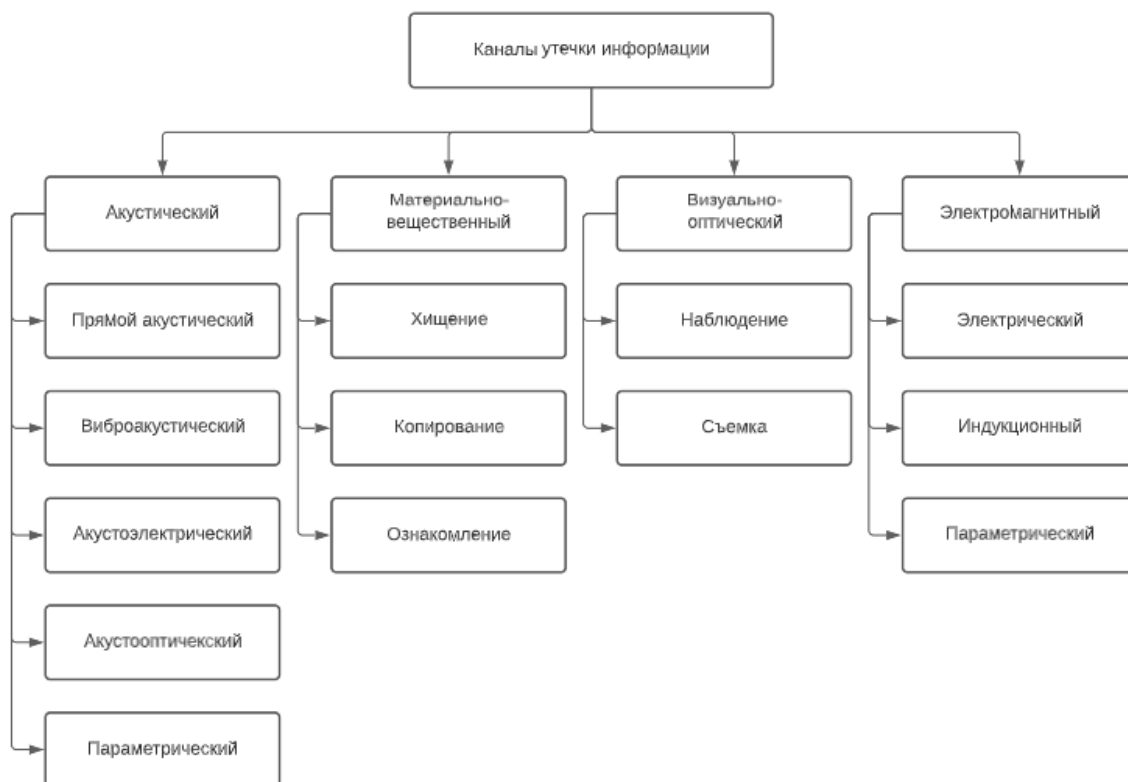


Рисунок 2 – Классификация ТКУИ

1.1 Акустические каналы утечки информации

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

Перехват акустической информации может происходить не только в помещении или в транспорте, существуют риски утечки даже при разговоре на улице. Шум оживленной трассы или включение воды в номере гостиницы не подавят сигнал, нужны специальные устройства, снижающие риск передачи данных в воздушной среде по каналам утечки акустической информации.

Автономные устройства, конструктивно объединяющие микрофоны и передатчики, называют закладными устройствами (ЗУ) перехвата речевой информации. Для внедрения ЗУ в 90% случаев необходима возможность проникнуть в офис. Введение пропускного режима и электронных замков поможет минимизировать риски утечки информации по каналам акустического типа, но они останутся. Среди актуальных для большинства организаций носителей угрозы оказываются работники, которые могут быть подкуплены конкурентами.

1.2 Материально-вещественные каналы утечки информации

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, использованная копировальная бумага, различные отходы производства, бракованные изделия, черновые материалы и другое.

1.3 Визуально-оптические каналы утечки информации

Если экран монитора или часть лежащих на столе документов можно увидеть через окно офиса, возникает риск утечки. Для борьбы с этим способом необходимо применять в большинстве случаев простые технические средства:

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

1.4 Электромагнитные каналы утечки информации

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

- от микрофонов телефонов и переговорных устройств;
- от основных цепей заземления и питания;
- от аналоговой телефонной линии;
- от волоконно-оптических каналов связи.

Технологии позволяют подключать закладные устройства ПЭМИН непосредственно к цепям питания или же установить в мониторе или корпусе компьютера для перехвата следующих данных:

- выводимых на экран монитора;
- вводимых с клавиатуры или другого периферийного устройства;
- выводимых через провода на периферийные устройства;
- записываемых 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.

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

Система инженерно-технической безопасности должна проектироваться комплексно, поэтому ее элементы должны составлять единую систему, контроль над работоспособностью, которой должен быть возложен на компетентных сотрудников.

При этом комплексное применение всего диапазона методов защиты может быть избыточным, поэтому для организации систем защиты информации в конкретной компании нужно создавать собственный проект, который окажется оптимальным с ресурсной точки зрения.

2 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ

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 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Постановление Правительства РФ от 1 ноября 2012 г. No 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;
- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1;
- Приказ ФСТЭК «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. No644;
- Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»;
- Межведомственная комиссия по защите государственной тайны решение No 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.

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 План помещений и информационные потоки предприятия

Перед началом проектирования инженерно-технической защиты помещений необходимо изучить все открытые и закрытые информационные потоки, которые фигурируют на предприятии ООО «NQT».

В соответствии с заданием курсовой работы система имеет вторую степень секретности информации (гриф «совершенно секретно»). В соответствии с классификацией «совершенно секретно» к сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации.

Закрытые информационные потоки: взаимодействие с отделом продаж, отделом разработки и дизайна, финансовым отделом, юридическая консультация на предприятии, а также взаимодействие с администратором предприятия.

Открытые информационные потоки: взаимодействие с внешним отделом (специалист по рекламе, работа с соцсетями и рекламой), работа HR-специалиста (набор персонала и организация его работы), взаимодействие с внешними предприятиями (банк и налоговая).

Перечень защищаемых информационных активов:

- Персональные данные сотрудников;
- Персональные данные клиентов;
- Секретные сведения, содержащие государственную тайну;
- Конфиденциальная информация, содержащая коммерческую тайну;
- Техническая конфигурация программного обеспечения.

На рисунке 4 представлены информационные потоки предприятия.

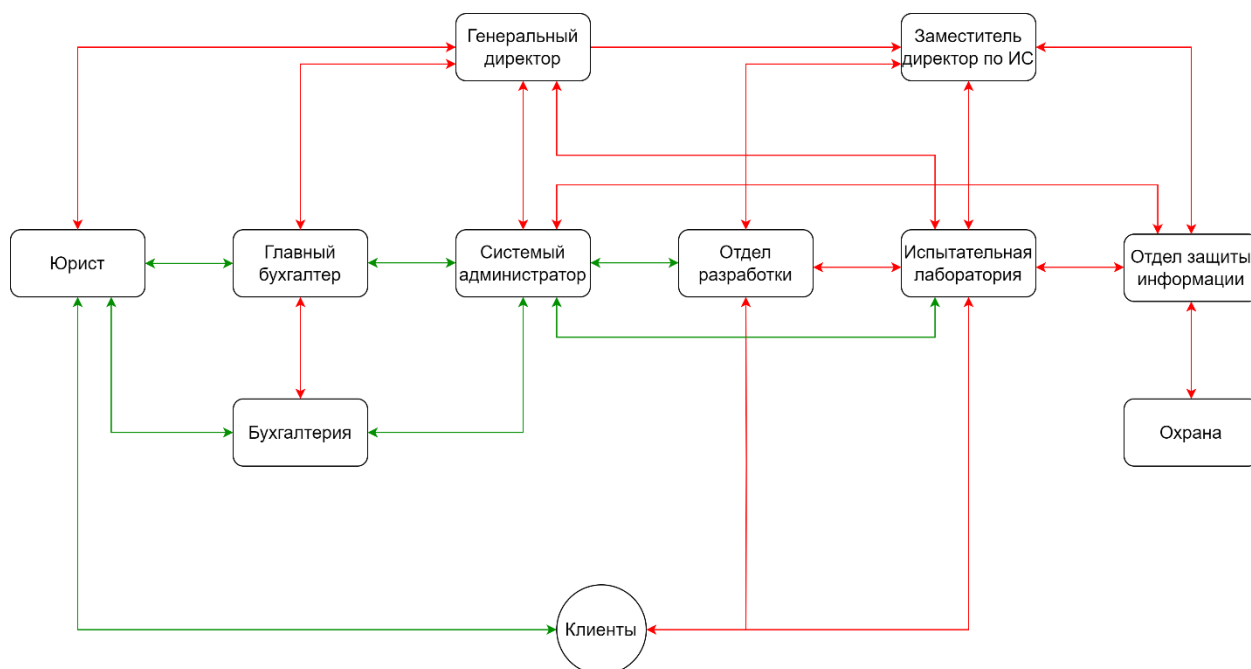


Рисунок 4 - Открытые и закрытые информационные потоки предприятия

Также на рисунке 5 представлен план защищаемого помещения с учетом мебелировки, а в таблице 1 приведены обозначения объектов в каждом помещении и их краткое описание. Номера на плане здания соответствуют следующим помещениям:

- 1) Кабинет директора;
- 2) Переговорная;
- 3) Офис 1;
- 4) Зона отдыха;
- 5) Коридор;
- 6) Офис 2;
- 7) Серверное помещение;
- 8) Уборная.

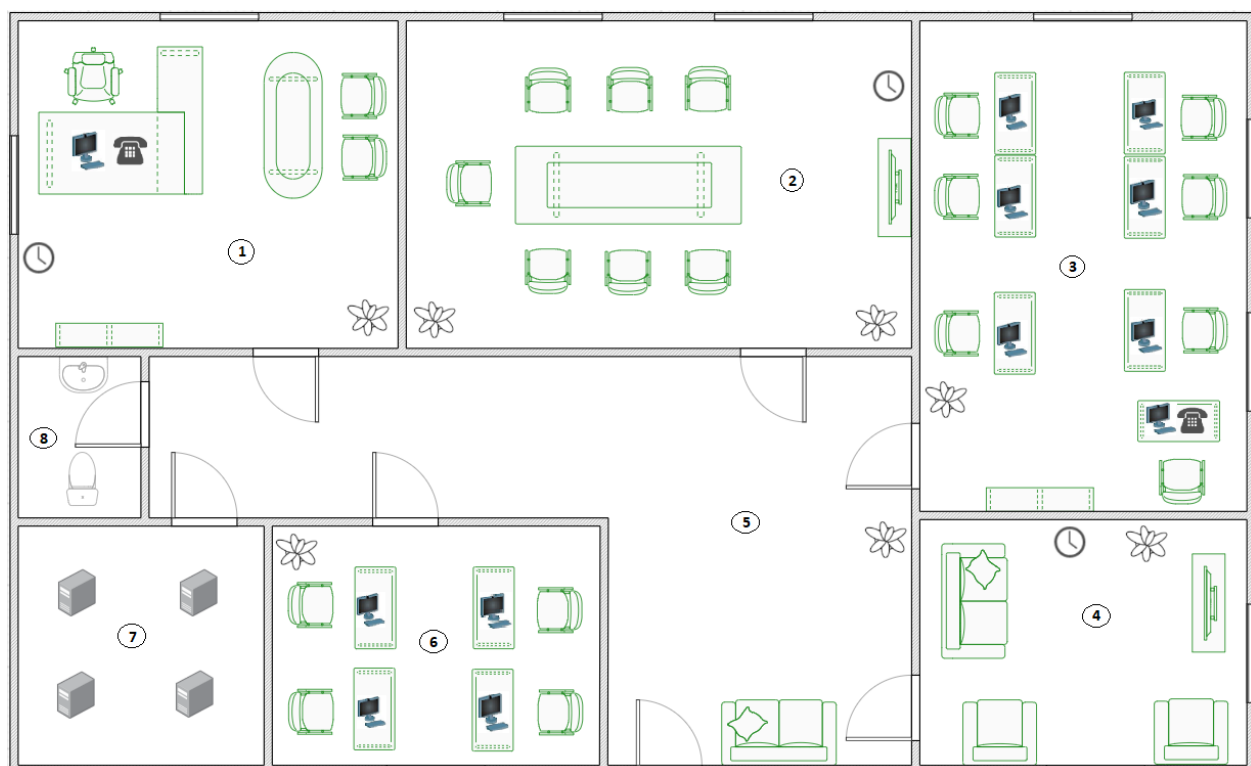










Рисунок 5 - План здания с учетом мебелировки помещений

Таблица 1. Описание выбранных объектов при мебелировке помещения

Объект	Обозначение
	Угловой стол руководителя
	Кресло руководителя
	Стул для переговорной
	Стеллаж
	Полукруглый стол
	Прямой стол
	Телевизор

	Компьютер
	Растение
	Часы
	Рабочий стол
	Мягкое кресло
	Диван
	Раковина
	Унитаз

3.2 Описание помещений

В соответствии с степенью защищенности информации защите подлежат следующие помещения:

- 1) Кабинет директора: 4 м * 4.5 м (площадь: 18 м²);
- 2) Переговорная: 4м * 6 м (площадь: 24 м²);
- 3) Офис 1: 6м * 4 м (площадь: 24 м²);
- 4) Зона отдыха: 3 м * 4 м (площадь: 12 м²);
- 5) Офис 2: 3 м * 4 м (площадь: 12 м²);
- 6) Серверное помещение: 3 м * 3 м(площадь: 9 м²);

В кабинете директора расположены 2 стола, 3 стула, стеллаж, компьютер, телефон, часы и растение. В помещении есть 2 окна.

В переговорной расположены стол, 7 стульев, телевизор, часы и растение. В помещении есть 2 окна.

В офисе 1 расположены 7 столов, 7 стульев, компьютеры, телефон и растение. В помещении есть 3 окна.

В зоне отдыха расположены диван, 2 кресла, телевизор, часы и растение. В помещении есть 2 окна.

В офисе 2 располжены 4 столов, 4 стульев, компьютеры и растение. В помещении есть 1 окно.

В серверном помещении расположены 4 серверов. Окон в помещении нет.

Офис расположен на третьем этаже трехэтажного здания, окна выходят в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

3.3 Анализ возможных утечек информации

В помещениях присутствуют декоративные элементы, в которых можно спрятать закладное устройство. В каждом помещении имеются розетки, сетевые устройства, а значит, актуальны электрический и электромагнитный каналы утечки информации. Также есть угроза снятия информации по вибрационному и оптическому каналам, а также акустическому, виброакустическому, акустоэлектрическому. Так как информации на предприятии присвоена 2 степень секретности, материально-вещественный канал утечки информации регулируется строгой политикой информационной безопасности компании в отношении физических носителей информации и в рамках курсовой работы не рассматривается.

3.4 Выбор средств защиты информации

Для реализации инженерно-технической защиты, соответствующей 2 уровню секретной информации «совершенно секретно», необходимо оборудовать помещение СЗИ, приведенными в таблице 2.

Таблица 2. Виды уязвимых каналов и применяемые меры по защите

Каналы	Источники	Пассивная защита	Активная защита
Акустический	Окна, двери, электрические сети, проводка и розетки	Звукоизоляция помещения, фильтры для акустического канала	Устройства акустического зашумления
Вибрационный, виброакустический	Батареи и все твердые поверхности помещений (стены, пол, окна, двери)	Изоляция поверхностей с помощью дополнительных обшивок	Устройства Вибрационного зашумления
Визуально- оптический	Незащищенные окна, двери	Жалюзи на окнах, доводчики на двери, уменьшение освещенности носителей информации, темные стекла	Маскирующие средства сокрытия объектов
Электромагнитный, электрический	Телевизор в зоне отдыха, розетки во всех помещениях, ПК, серверы, телефон	Фильтры для сетей питания, экранирующие материалы, помехоподавляющие фильтры	Устройства электромагнитного зашумления

4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

4.1 Требования к защите помещений

В соответствии с заданием курсовой работы предприятие работает с информацией 2 степени секретности или с информацией, представляющей государственную тайну с грифом «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:

- 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;
- 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 20 или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене;
- Все режимные помещения оборудуются аварийным освещением;
- 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;
- 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;
- Помещения, где хранятся секретные документы и носители государственной тайны, оборудуются охранной и аварийной сигнализацией.

4.2 Анализ СЗИ для акустического и виброакустического каналов

Основным пассивным методом защиты акустической информации является звукоизоляция. Выделение акустического сигнала злоумышленником возможно, если отношение сигнал/шум лежит в определенном диапазоне. Основная цель применения пассивных средств защиты информации - снижение соотношения сигнал/шум в возможных точках перехвата информации за счет снижения информативного сигнала.

В качестве пассивных средств были выбраны: шумоизоляция стен, звукоизолирующие двери.

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 и акустическому каналам.

Таблица 3. Сравнительный анализ средств активной защиты информации для виброакустического канала

Устройство	Цена, руб	Характеристики	Описание
Генератор акустического шума «ЛГШ-304»	25,220	Диапазон рабочих частот 175 - 11200 Гц	Изделие «ЛГШ-304» предназначено для защиты акустической речевой информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, циркулирующей (обрабатываемой) в помещениях, путем формирования акустических маскирующих шумовых помех. Сертифицировано ФСТЭК
Генератор маскирующего шума «Камертон-5»	46,000	Диапазон рабочих частот 90 - 11200 Гц	Комплекс технических средств для защиты речевой информации от несанкционированного съема через виброакустические каналы. Гарантирует невозможность прослушки разговоров посредством лазерных и направленных микрофонов через окна, инженерные коммуникации, вентиляцию, межкомнатные перегородки, пр.

			Сертифицировано ФСТЭК.
«Соната АВ-4Б»	44,200	Диапазон рабочих частот 175 - 11200 Гц	Система защиты речевой информации от утечки по техническим каналам "Соната- АВ" модель 4Б, предназначена для защиты речевой информации в выделенных помещениях, от утечки по акустическим, виброакустическим, акустоэлектрическим и оптико- электронным (лазерным) каналам. Сертифицировано ФСТЭК.

По результатам 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 изменить настройки генераторов и построить гибкую систему виброакустической.

4.3 Анализ СЗИ для визуально-оптического канала

Необходимую и достаточную защиту обеспечивают жалюзи. Они выбраны в связи с простотой и эффективностью в эксплуатации.

Были выбраны рулонные шторы Роллайт 2 с технологией BlackOut 100 см * 150 см 3190 руб/шт.

4.4 Анализ СЗИ для электромагнитного, электрического каналов

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. Устройства активной защиты представлены в Таблице 4.

Таблица 4. Сравнительный анализ средств активной защиты информации для электромагнитного и электрического каналов

Устройство	Цена, руб	Характеристики	Описание
Фильтр сетевой	47,000	Напряжение питания 220/380 В ± 10%, 50 Гц	Фильтр сетевой помехоподавляющий ФСПК-40-220-99-УХЛ4 предназначен для защиты информации от утечки за счет побочных

помехоподавляющий «ФСПК-40»			электромагнитных наводок на линии электропитания. В общем случае защитное устройство может применяться как сетевой фильтр для улучшения параметров качества сети.
Генератор шума «Соната РС2»	23,600	Диапазон частот до 2 ГГц, диапазон регулировки уровня шума не менее 35 дБ	Устройство для защиты линий электропитания, заземления от утечки информации "Соната-РС2" (сертифицировано ФСТЭК) предназначены для защиты объектов вычислительной техники от утечки информации за счет наводок на линии электропитания и заземления и может использоваться в выделенных помещениях до 1 категории включительно. Регулировка уровня шума в 3 частотных полосах. Индикация нормального/аварийного режима работы. Сертифицировано ФСТЭК.
«Соната-Р3» средство активной защиты информации от утечки за счет ПЭМИН	97,200	Световая и звуковая индикация, потребляемая мощность 30 Вт, электропитание от сети 220 В, время непрерывной работы 8 часов	Изделие может быть включено в состав комплекса ТСЗИ. В этом случае управление его работой и контроль режима работы (исправности) будет осуществляться от пульта управления "Соната-ДУ4.1" в комплексе с блоком питания "Соната-ИП4.х" (Комплекс 3095, Комплекс 3106, Комплекс 3109). Сертифицировано ФСТЭК.

В результате анализа был выбран генератор шума «Соната РС2». Данный выбор обоснован особенностями конструкции устройства, которые позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники.

Дополнительно был выбран «Соната-Р3» средство активной защиты информации от утечки за счет ПЭМИН, так как оно обладает лучшими характеристиками по сравнению с другими средствами пассивной защиты от ПЭМИН.

5 РАССТАНОВКА ТЕХНИЧЕСКИХ СРЕДСТВ

На основании таблиц 3 и 4 были выбраны следующие средства защиты информации:

- Система активной акустической и вибрационной защиты акустической речевой информации «Соната-АВ» модель 4Б;
- Генератор шума «Соната РС2»;
- «Соната-РЗ» средство активной защиты информации от утечки за счет ПЭМИН;
- Рулонные шторы Роллайт 2 с технологией BlackOut 100 см * 150 см;
- Усиленные звукоизоляционные двери Phoenix (звукоизоляционная прокладка с металлической сеткой: толщина 10 мм, обшивка: металл 3 мм, устройство для опечатывания);
- Звукоизоляционная отделка помещений Шуманет Комби 5 мм 1 м * 10 м.

Пассивная защита

Было решено установить 5 усиленные двери (в переговорную комнату, кабинет директора, 2 офиса и серверное помещение, так как двери оснащены устройством для опечатывания), 10 рулонных штор на каждое окно в каждое помещение. Также была использована звукоизоляционная отделка для 5 помещений (переговорная комната, кабинет директора, 2 офиса и серверное помещение) общей площадью стен 135 м², следовательно, необходимо выделить 14 рулон отделки.

Активная защита

Соната «АВ» 4Б содержит генераторы-акустоизлучатели СА-4Б1 и генераторы-вибровозбудители СВ-4Б.

1) Генераторы-акустоизлучатели СА-4Б1

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

2) Генераторы-вибровозбудители СВ-4Б

- 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.

3) Блок электропитания и управления «Соната-ИП 4.3» устанавливается в количестве 1 шт. на 1-15 генераторных блока для управления одной системой защиты для выбранных помещений.

4) 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.

5) Пульт управления «Соната-ДУ 4.3» 1 шт. для всей системы.

6) Генератор шума «Соната-РС2» подключена к системе электроснабжения согласно рекомендациям производителя, на схеме отдельно не обозначена.

7) Средство активной защиты информации от утечки за счет ПЭМИН «Соната-Р3»

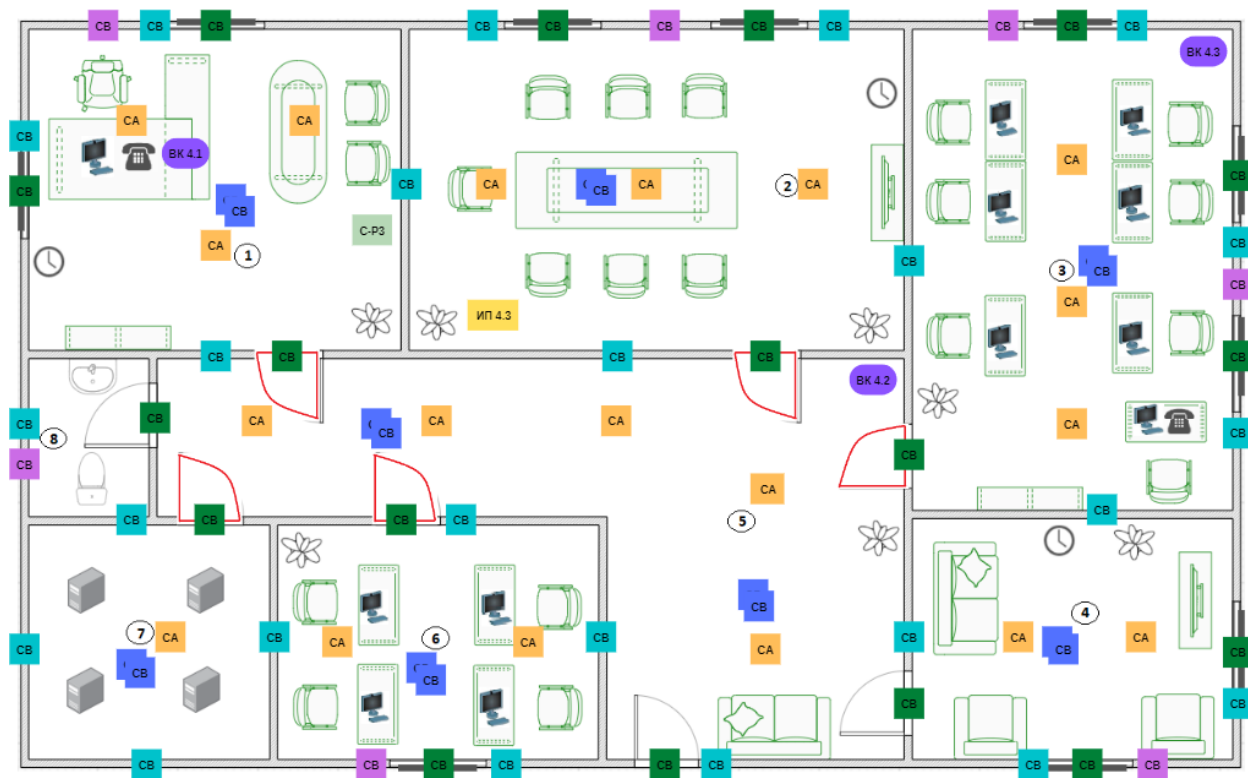














Рисунок 6 - План помещений с внедренными СЗИ

Таблица 5. Смета и условные обозначения СЗИ

СЗИ	Условное обозначение	Цена, руб	Количество, шт	Стоимость, руб
Усиленные звукоизоляционные двери Phoenix		89,990	5	449,950
Звукоизоляционная отделка помещений Шуманет Комби	-	390	14	5,460
Рулонные шторы Роллайт 2 с технологией BlackOut		3,190	10	31,900
Генераторы-акустоизлучатели СА-4Б1		7,440	19	141,360
Генераторы-вибровозбудители СВ-4Б (стены)		7,440	24	178,560
Генераторы-вибровозбудители СВ-4Б (пол, потолок)		7,440	16	119,040
Генераторы-вибровозбудители СВ-4Б (двери, окна)		7,440	18	133,920
Генераторы-вибровозбудители СВ-4Б (трубопровод)		7,440	7	52,080
Блок электропитания и управления «Соната-ИП 4.3»		21,600	1	21,600
Размыкатель «Соната-ВК 4.1»		6,000	1	6,000
Размыкатель «Соната-ВК 4.2»		6,000	1	6,000
Размыкатель «Соната-ВК 4.3»		6,000	1	6,000
Пульт управления «Соната-ДУ 4.3»	-	7,680	1	7,680
Генератор шума «Соната-РС2»	-	23,600	1	23,600
Средство активной защиты информации от утечки за счет ПЭМИН «Соната-РЗ»		97,200	1	97,200
ИТОГ				1,280,350

ЗАКЛЮЧЕНИЕ

В ходе данной курсовой работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении, а также 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. Государственный реестр сертифицированных средств защиты информации // ФСТЭК РОССИИ [Электронный ресурс] (дата обращения: 28.11.2022).
2. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.
3. Мещеряков Р. В., Шелупанов А. А., Зайцев А. П. Технические средства и методы защиты информации. – 2007.
4. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
5. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.