

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ 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 в помещении»

Выполнил(а):

Филатова П., студент группы N34501



(подпись)

Проверил преподаватель:

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

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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


Студент	Филатова Полина
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34501
Направление (специальность)	10.03.01. - Технологии защиты информации
Руководитель	Попов И. Ю., доцент, к. т. н.
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы 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.

Рекомендуемая литература

Н.С. Кармановский, О.В. Михайличенко, С.В. Савков - Организационно-правовое и методическое обеспечение информационной безопасности

Руководитель	Попов И. Ю., доцент, к. т. н.
	(Подпись, дата)
Студент	Филатова Полина
	 (Подпись, дата)

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

Студент Филатова Полина
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34501

Направление (специальность) 10.03.01. - Технологии защиты информации

Руководитель Попов И. Ю., доцент, к. т. н
(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Создание плана КР	31.10.2023	31.10.2023	
2	Анализ литературы	10.11.2023	10.11.2023	
3	Составление основного текста КР	15.11.2023	15.11.2023	
4	Создание презентации	10.12.2023	10.12.2023	
5	Презентация КР перед аудиторией	15.12.2023	15.12.2023	

Руководитель Попов И. Ю., доцент, к. т. н.
(Подпись, дата)

Студент Филатова Полина
(Подпись, дата)

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

Студент	Филатова Полина
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34501
Направление (специальность)	10.03.01. - Технологии защиты информации
Руководитель	Попов И. Ю., доцент, к. т. н.
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

**1. Цель и задачи
работы**

- ☒ Предложены студентом ☐ Сформулированы при участии студента
☐ Определены руководителем

Цель данной работы – разработать инженерно-техническую систему защиты информации в помещении

**2. Характер
работы**

- ☐ Расчет ☐ Конструирование
☐ Моделирование ☒ Другое

3. Содержание работы

В работе представлен результат анализа рынка инженерно-технических средств защиты информации и на его основе разработана инженерно-техническая система защиты информации в помещении

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 И. Ю., доцент, к. т. н.
	(Подпись, дата)
Студент	Филатова Полина
	(Подпись, дата)

«___» _____ 20__ г

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	2
1.1. Термины и определения.....	3
1.2 Основная часть.....	5
1.3 Руководящие документы.....	10
2. АНАЛИЗ ЗАЩИЩАЕМОГО ПОМЕЩЕНИЯ.....	12
2.1. Комплексная безопасность.....	18
3. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ.....	19
3.1. Устройства противодействия утечке информации по акустическому и виброакустическому каналам	20
3.2 Устройства противодействия утечке информации по оптическому каналу.....	23
3.3. Устройства противодействия утечке по электромагнитным и электрическим каналам.....	24
4. ОПИСАНИЕ СРЕДСТВ ЗАЩИТЫ И РАССТАНОВКА ВЫБРАННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ.....	26
ВЫВОД.....	28
6. Используемая литература.....	29

ВВЕДЕНИЕ

Цель работы – повышение защищенности рассматриваемого помещения.

Задачи:

1. Проанализировать защищаемое помещение;
 2. оценить каналы утечки информации;
 3. проанализировать рынок;
 4. выбрать меры пассивной и активной защиты информации;
- представить результат работы в виде схемы с установленными средствами защиты.

1.1. Термины и определения

Коммерческая тайна – информация конфиденциального характера из любой сферы производственной и управленческой деятельности государственного или частного предприятия, разглашение которой может нанести материальный или моральный ущерб ее владельцам или пользователям (юридическим лицам). Охрана коммерческой тайны осуществляется ее владельцем на основе государственных законодательных актов. Коммерческая тайна включает в себя также подробности коммерческой деятельности, состав партнеров, источники сырья, технологию сбыта продукции.

Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена. Утечка информации может осуществляться по различным каналам. Каналом утечки информации называют канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.

Промышленная тайна – это новые технологии, открытия, изобретения, применяемые в процессе производства продукции, и т. д.

Финансовая тайна - бухгалтерские и финансовые документы, деловая переписка и т. д.

Личная тайна – это сведения конфиденциального характера, разглашение которых может нанести материальный ущерб отдельному (физическому) лицу. Охрана личной тайны осуществляется ее владельцем. Государство не несет ответственность за сохранность личных тайн.

Документ – представленная на материальном носителе информация с идентификатором, позволяющим установить характер документа и его собственника.

Источник речевой информации - разговоры в помещениях и системы звукоусиления и звуковоспроизведения.

Носитель видовой информации объекта - сам объект, а также его фото- и видеоизображения на материальных носителях информации.

Политическая разведка - деятельность по добыванию сведений внутриполитического и внешнеполитического характера в стране, являющейся объектом разведки, организует действия по подрыву политического строя государства.

Экономическая разведка - сбор сведений, раскрывающих экономический потенциал определенной страны.

Военная разведка - сбор сведений о военном потенциале интересующего ее государства, о новейших образцах военной техники.

Научно-техническая разведка – сбор сведений по новейшим теоретическим и практическим разработкам в области науки и техники.

Агентурная разведка - добывание информации и проведения диверсионных акций специально подобранных, завербованных и профессионально подготовленных агентов.

Легальная разведка-добыча информации при различных официальных связях и контактах с нашей страной, из легальных источников информации.

Техническая разведка - сбор информации с использованием технических разведывательных средств.

Воздушные каналы - каналы утечки информации, в которых средой распространения акустических сигналов является воздух, а для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны.

Вибрационные каналы - каналы утечки информации, в которых средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твёрдые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы).

Акустоэлектрические каналы - каналы утечки информации, в которых утечка происходит за счет преобразований акустических сигналов в электрические различными радиоэлектронными устройствами. Перехват акустических колебаний осуществляется через ВТСС, обладающие «микрофонным эффектом», а также путем «высокочастотного навязывания».

Гидроакустический канал - канал, который образуется в водной среде и позволяет добывать акустическую информацию с использованием гидрофонов (сонаров).

Оптико-электронный канал - каналы утечки информации, в которых утечка образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол, окон, картин, зеркал и т. д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация).

Параметрические каналы - канал, в котором в результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСПИ и ВТСС.

1.2 Основная часть

Для того, чтобы построить эффективную систему противодействия утечке информации, необходимо в первую очередь определить потенциальные и реальные угрозы технического проникновения на защищаемый объект, возможные каналы для несанкционированного доступа и утечки защищаемой информации.

Курсовая работа базируется на знании физической природы возникновения технических каналов утечки информации и методов ведения технической разведки. Правильное определение потенциальных угроз на предпроектном этапе построения системы противодействия промышленному шпионажу позволит в дальнейшем выбрать наиболее оптимальные меры и средства защиты.

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

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей конфиденциальной информации, необходимо учитывать и вспомогательные технические средства и системы (ВТСС), такие, как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др. Наибольшее внимание следует уделить вспомогательным средствам, имеющие линии, выходящие за пределы контролируемой зоны.

В качестве каналов утечки больше внимания следует уделить вспомогательным средствам, имеющим линии, выходящие за пределы контролируемой зоны, а также посторонним проводам и кабелям, проходящим через помещения, где установлены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

При оценке защищенности помещений от утечки речевой информации необходимо учитывать возможность ее прослушивания как из соседних помещений, так и с улицы. Следует проводить оценку возможности ведения разведки с использованием лазерных микрофонов. Интерес могут вызывать каналы утечки за счет вибраций, возникающих под давлением акустических волн, в твердых телах (ограждениях, трубах и т.п.).

Оценка защищенности объекта включает в себя:

1. анализ режима работы и охраны объекта,
2. моделирование действий по скрытному проникновению на них (неконтролируемому пребыванию) посторонних лиц;
3. режим работы специалистов сторонних организаций,
4. приобретение, установка и ремонт мебели, оргтехники и т.п.,
5. совокупность условий, позволяющих внедрить на объект специальные закладные
6. устройства перехвата информации (микропередатчики, возможность установки
7. миниатюрных микрофонов с подключением к внешним линиям и т.д.),
8. определение наиболее эффективных, для использования на разных уровнях проникновения, средств противодействия промышленному шпионажу.

Большое, а иногда решающее, значение при оценке угрозы может иметь знание конкурента, его финансовых и оперативных возможностей, знание личностных качеств постоянного персонала, временных работников и другая дополнительная информация.

Источник сигнала формирует конкретный вид технического канала. Существует следующая классификация.

1. Канал побочных электромагнитных излучений и наводок (ПЭМИН).

При обработке информации в компьютере возникают колебания электромагнитного поля, которые могут быть перехвачены закладным устройством и преобразованы в читаемый вид. До 61 % утечек данных по техническим каналам связаны именно с ПЭМИН;

Наибольший риск утраты информации прослеживается при использовании именно этого канала. Еще в 1985 году на одной из международных выставок, посвященных кибербезопасности, посетителям продемонстрировали, с какой легкостью перехваченные электромагнитные сигналы преобразовываются в изображение и текст, выведенные на экран монитора.

Каналы ПЭМИН имеют собственную классификацию:

- Электромагнитные. Среда распространения — эфир;
- Электрические каналы. Среда распространения — эфир, линии электропитания, заземления, оптоволоконные и другие кабели связи.

В электромагнитных каналах утечки информации данные переносятся посредством электромагнитных излучений, генерируемых в процессе обработки данных техническими средствами. Побочные электромагнитные излучения (ПЭМИ) — нежелательные (паразитные), в процессе работы средств обработки информации они создают риск ее утечки.

Во время работы компьютера большинство элементов его архитектуры становится источником генерации и утечки ПЭМИН:

- процессор;
- электрические цепи питания;
- все контроллеры;
- модули памяти;
- шина данных;
- видеокарты;
- все типы портов;
- адаптеры для локальных сетей.

Информация снимается:

- с монитора. С ранних мониторов телевизионного типа данные снимались за сотни метров, с современных жидкокристаллических — за десятки;
- с клавиатуры, даже беспроводной, но сигнал с проводной клавиатуры может быть перехвачен за десятки метров, с беспроводной — за единицы;
- при записи информации на жесткий диск или съемное устройство;
- в режиме общения по голосовым мессенджерам.

Отдельные риски утечки информации по техническим каналам связи создают наводки — под ними понимается передача электрических сигналов из одного устройства в другое, не предусмотренная конструктивными решениями или схемой прокладки проводов. Между устройствами или кабелями возникают паразитные связи. Наводки порождают риск

утечки модулированного информационным сигналом электромагнитного импульса за пределы охраняемой зоны.

Информативными считаются высокочастотные сигналы, информацией — изображение, выводимое на экран монитора, данные, обрабатываемые на устройствах ввода-вывода. Неинформативные не раскрывают суть обрабатываемой информации, они только дают представление о работе технического средства обработки.

2. Оптический канал.

Это видовая информация — документы, изображения на мониторе, оборудование, новые модные коллекции, все, что можно увидеть или сфотографировать.

3. Модифицированный оптический канал

Это оптико-электронный канал утечки речевой информации. Перехват ведется при помощи лазерного луча, испускаемого от лазерных акустических систем разведки (ЛАСР), а также трипель-призм (промежуточных элементов конструкции систем разведки, отражающих лазерный луч под определенным углом) на расстоянии до 500 метров;

4. Акустический канал.

При анализе акустических каналов утечки информации отдельно выделяются телефонные каналы связи, которые несут несколько рисков:

- прослушку переговоров, ведущихся по городским телефонным сетям;
- прослушку переговоров по мобильным устройствам;
- удаленную активацию мобильного телефона (с внешнего устройства управления) или микрофона компьютера (при помощи вредоносных программ) для записи разговоров или трансляции злоумышленнику последних разговоров, зафиксированных в памяти.

Мощный направленный микрофон перехватит сигнал на расстоянии до 100—150 м. Закладные устройства — микрофоны, скрытые видеокамеры, эндовибраторы, не имеющие источника питания и действующие по принципу отражения сигнала от аналога зеркала, аудиотранспондеры.

5. Виброакустический

При использовании данного канала перехватываются и преобразуются в данные колебания твердых сред — стекол, труб, строительных конструкций, вызываемые механическим воздействием звуковых волн. Стетоскоп позволяет прослушивать через стены толщиной до 1м;

6. Акустоэлектрические преобразования речевого сигнала.

Возникает в результате преобразования акустических сигналов в электрические, которые являются объектом перехвата. Перехват информации осуществляется за пределами контролируемых помещений и зон. Дальность перехвата электромагнитного сигнала от закладки-преобразователя — 100 м.

1.3 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 (ред. от 13.07.2015) «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 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне».
- Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации».
- Федеральный закон от 27 июля 2006 г. No 152-ФЗ «О персональных данных».
- 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»
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1.
- 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.
- 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.

2. АНАЛИЗ ЗАЩИЩАЕМОГО ПОМЕЩЕНИЯ

Ниже приведена примерная схема защищаемого помещения.

Защищаемое помещение — офис одного из филиалов компании ООО «Информационная Опасность». Офис располагается на третьем этаже бизнес-центра.

Деятельность компании заключается в проведении тестирования на проникновение и организации защиты внешнего и внутреннего периметра компаний-заказчиков. ООО «Информационная Опасность» так же участвует в тендерах и принимает заказы от гос.компаний и банков. На рисунке 1 показаны информационные потоки в компании, на рисунке 2 показана общая схема офиса ООО «Информационная Опасность», в таблице 1 приведен перечень наименований мебели и используемой техники.

Основные информационные процессы в компании:

- публикация предложения услуг;
- предоставление пользователям инструментов для заказа услуги и создания учётной записи на сайте;
- технологическое сопровождение оказания услуги;
- предоставление консультаций пользователям;
- удаление данных по завершении сотрудничества;
- ведение бухгалтерского учёта организации, взаимодействие внутренних отделов с бухгалтерией;
- хранение, обработка, передача, утилизация персональных данных пользователей.

Информация ограниченного доступа:

- персональные данные сотрудников;
- персональные данные клиентов;
- техническая информация;
- коммерческая тайна;
- государственная тайна.

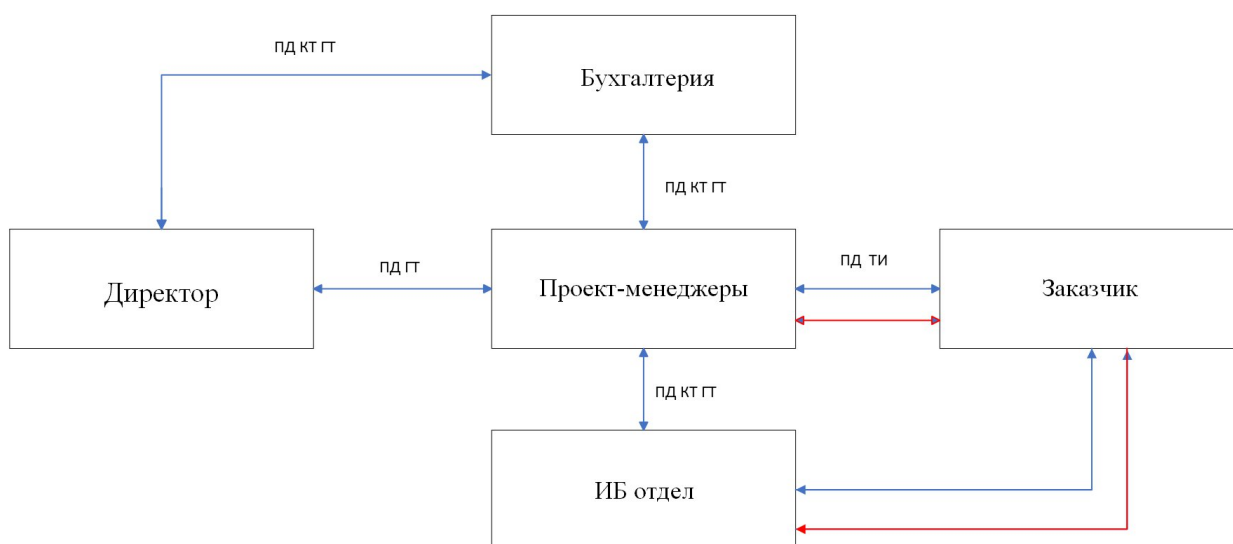


Рисунок 1 — Информационные потоки в офисе

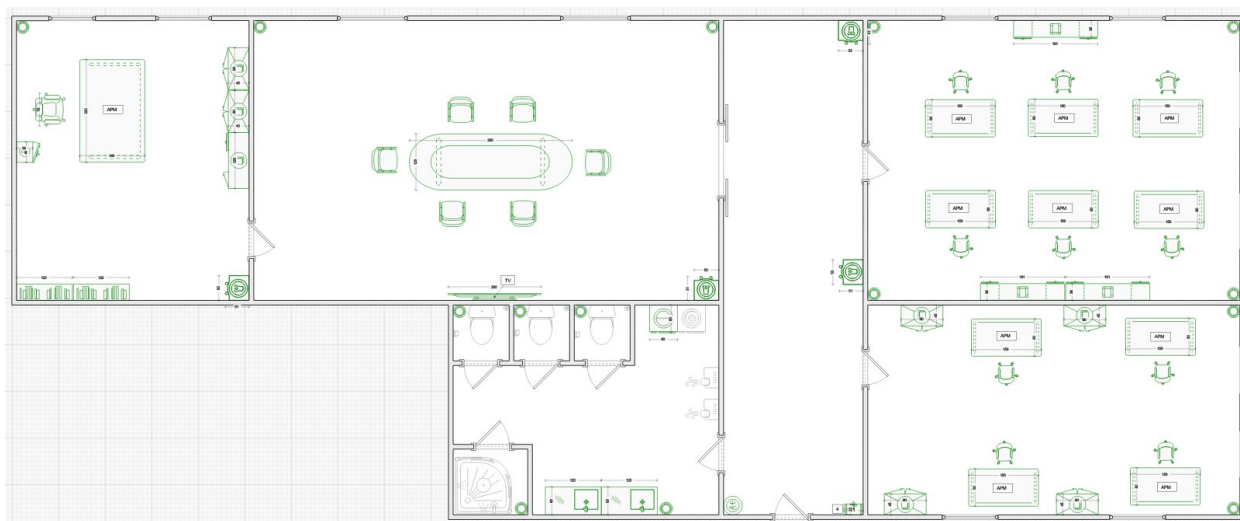
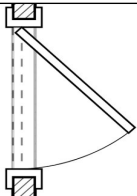


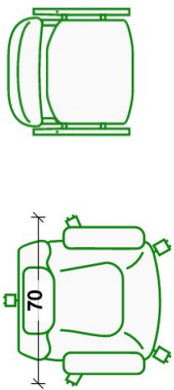
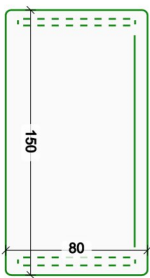
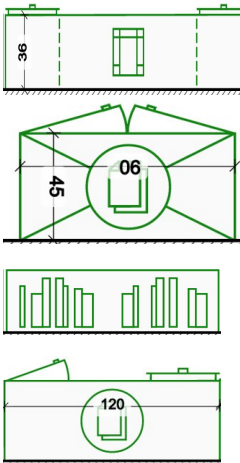
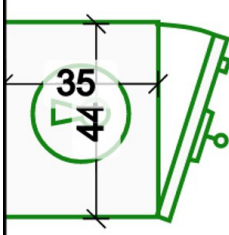



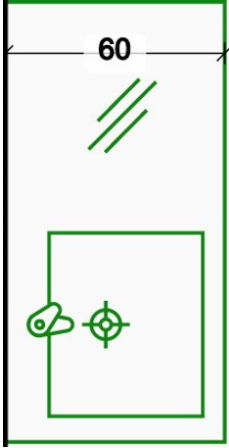


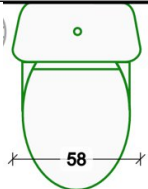
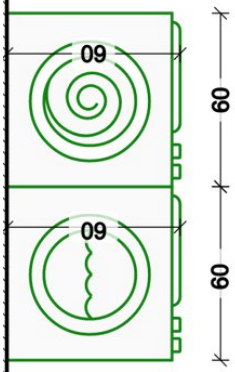

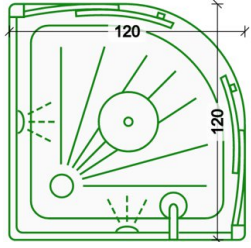
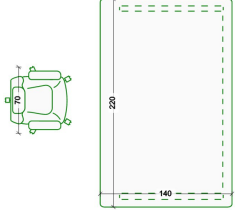
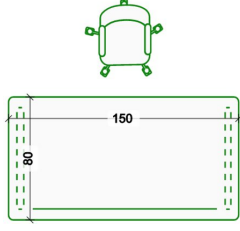
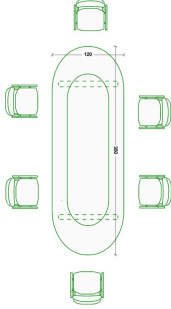
Рисунок 2 — План офиса

Таблица 1 — Перечень наименований мебели и используемой техники

Объект	Описание
APM	Автоматизированное рабочее место
TV	Телевизор
	Дверь
	Дверь в переговорную
	Окно
	Стул
	Стол

Д

	Шкаф
	Сейф
	Кулер
	Санитайзер
	Урна
	Раковина

	Унитаз
	Стиральная и сушильная машины
	Ершик и держатель для туалетной бумаги
	Душевая кабина
	Рабочее место руководителя
	Рабочее место сотрудника
	Стол в зале совещаний

Помещения, требующие защиты:

- Зал совещаний: 6м на 10 м, общей площадью 60м²

Зал совещаний предназначен для ведения переговоров с заказчиками и для коммуникации с остальными филиалами компании ООО «Информационная Опасность». В зале для совещаний находятся стол, 6 стульев, телевизор, кулер, 2 урны и 2 розетки.

- ИБ отдел: 8м на 6м, общей площадью 48м²

В ИБ отделе работают непосредственно ИБ и IT специалисты компании. В помещении ИБ отдела находятся 6 рабочих мест с АРМ, 3 шкафа, 4 урны и 12 розеток.

- Бухгалтерия: 8м на 4.5м, общей площадью 36м²

Отдел бухгалтерии работает с тендерами документацией. В помещении отдела находятся 4 рабочих места с АРМ, 4 шкафа, 4 урны, 8 розеток.

- Кабинет руководителя: 5м на 6м, общей площадью 30м²

В кабинете руководителя находятся 1 рабочее место с АРМ, 5 шкафов, урна, кулер, сейф и 2 розетки.

- Санузел: 4,5м на 5,4м, общей площадью 24,3м²

В санузле находятся душевая, 3 унитаза, стиральная и сушильная машины, 2 раковины, 5 урн, 3 ершика, 3 держателя для туалетной бумаги, 2 розетки и 2 сушилки для рук.

В коридоре, соединяющем все помещения, находится 2 кулера, 2 розетки и санитайзер.

Офис компании ООО «Информационная опасность» находится на 3-ем этаже бизнес-центра с собственной охраняемой территорией и внутренним двором. Все окна выходят во внутренний двор бизнес-центра.

В каждом помещении имеются розетки, что означает актуальность электрического и электромагнитного канала утечки информации. В каждом помещении, кроме сан.узла, имеются окна, что означает актуальность угрозы снятия информации по вибрационному, акустическому, виброакустическому а также оптическому каналам.

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

2.1. Комплексная безопасность

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

Таблица 2 — активная и пассивная защита информации

Канал утечки информации	Источник	Активная защита	Пассивная защита
Акустический и акустоэлектрический	Двери, окна, проводка	Сетевые фильтры, звукоизоляция	Акустическое зашумление
Вибрационный и виброакустический	Стены, пол, окна, двери, трубы, батареи	Изолирующие звук и вибрацию материалы стен	Вибрационное зашумление
Оптический	Окна и двери	Шторы, жалюзи, доводчики на двери	Блокирующие обзор устройства
Электромагнитный и электрический	АРМ, телевизоры, ноутбуки, розетки, бытовые приборы	Сетевые фильтры	Электромагнитное зашумление

3. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ

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.

3.1. Устройства противодействия утечке информации по акустическому и виброакустическому каналам

Пассивная защита представляет собой:

- усиленные двери;
- сетевые фильтры
- изолирующие звук и вибрацию материалы стен

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 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

Устройство	Характеристики	Предназначение	Цена, руб
Портативный генератор акустического шума ЛГШ-303	Диапазон рабочих частот 180 ÷ 11 300 Гц	Изделие предназначено для защиты речевой информации от перехвата по прямому акустическому каналу.	15600
Генератор акустического шума ЛГШ-304	Диапазон рабочих частот 175 ÷ 11 200 Гц	Сертификат ФСТЭК РОССИИ по 2 классу защиты; предназначен для защиты акустической речевой информации, содержащей сведения, составляющие государственную тайну	25220
«БУБЕН» - генератор акустической	Диапазон рабочих частот 400...18000 Гц	Используется для защиты конфиденциальных	15000

помехи		переговоров по принципу создания акустических помех. Вид помех: речеподобная, "белый шум".	
"ANG-2200" генератор шума	- Диапазон акустического шума 250 Гц...5 кГц	Генератор шума для акустического зашумления помещения и его защиты от утечки информации по вибро каналам (250...5000 Гц). Сертификат Гостехкомиссии.	18000
SI-3030 Виброакустический шумогенератор	Спектр шумовой помехи 125 Гц - 6,3 кГц	Предназначен для защиты помещений от прослушивания через строительные элементы конструкции.	28500
Упрощенный вариант генератора ГШ-111У	В комплект поставки входит генератор ГШ- 111У и ПО конфигуратора системы	Упрощённый вариант генератора шума без кнопочной клавиатуры и ЖКИ. Управление, регулировка и контроль осуществляются только через компьютер по сети Ethernet.	75000
Система активной акустической и	Диапазон частот до 2 ГГц, диапазон	Генератор шума. Регулировка уровня	23000

вибрационной защиты акустической речевой информации "Соната-АВ" модель 4Б	регулировки	шума в 3 частотных полосах. Индикация нормального/аварийн ого режима работы.	
---	-------------	---	--

В результате анализа различных устройств был выбран генератор акустического шума ЛГШ-304.

Генератор акустического шума ЛГШ-304 предназначен 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. Данный генератор подходит нам согласно сертификату ФСТЭК России и имеет оптимальную цену для филиала компании ООО «Информационная Опасность»

3.2 Устройства противодействия утечке информации по оптическому каналу

Для обеспечения защиты помещения от визуального наблюдения, необходимо установить доводчики на двери, а так же жалюзи или шторы на окна. С точки зрения удобства обслуживания были выбраны жалюзи.

3.3. Устройства противодействия утечке по электромагнитным и электрическим каналам

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

Устройство	Характеристики	Предназначение	Цена, руб
Генератор шума ЛГШ-503	Диапазон частот – 10 кГц – 1,8 ГГц	Изделие «ЛГШ-503» предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.	44200
Генератор виброакустического шума SEL SP-157G	Принцип действия основан на формировании широкополосных акустических и виброакустических маскирующих	Фильтр сетевой помехоподавляющий ФСПК-40-220-99-УХЛ4 предназначен для защиты информации от утечки за счет побочных электромагнитных наводок	70500

	шумовых помех (аналоговый белый шум или смешанный с цифровой речеподобной помехой).	на линии электропитания.	
Генератор шума ГНОМ-3М-60В	Диапазон частот 150кГц-1800мГц	Гном-3М-60В используется с внешними антеннами. В данном приборе предусмотрено 4 не связанных между собой выхода для подключения к антеннам и цепи электропитания. Для 100 процентной защиты информации от утечки следует использовать 3 рамочные антенны, расположив их в 3 перпендикулярных друг другу плоскостях.	57000

В результате анализа различных устройств был выбран генератор шума ЛГШ-503. Его функционал достаточен для обеспечения надежной защиты филиала компании ООО «Информационная Опасность» и имеет сравнительно невысокую цену.




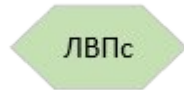
4. ОПИСАНИЕ СРЕДСТВ ЗАЩИТЫ И РАССТАНОВКА ВЫБРАННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

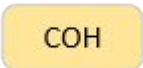



Выбранные средства для защиты офиса филиала компании ООО «Информационная Опасность» включают в себя:

1. Усиленные двери с повышенной шумоизоляцией Sigma Prestige Smart — цельногнутое П-образное полотно из стали толщиной 1,8 мм, защита от всех видов взлома, МДФ плита 12 мм, шумоизоляция +/- 42 дБ;
2. Генератор акустической помехи «ЛГШ-304»;
3. Генератор шума «ЛГШ-503»;
4. Генератор шума «ГАММА-ГШ18»;
5. Сетевой помехоподавляющий фильтр ФС-32М;
6. Для защиты телефонной линии размыкатель СОНАТА-ВК-4.1;
7. Вибропреобразователь «ЛВП-2с» для окон.

В таблице 5 приведена примерная смета на обеспечение безопасности офиса компании ООО «Информационная Опасность», на рисунке 3 показана схема расстановки устройств.

Таблица 5 — смета

Средство защиты	Цена, руб	Кол-во	Обозначение	Конечная стоимость, руб
Двери Sigma Prestige Smart	51900	5		259500
«ЛГШ-304»	25220	2		50440
«ЛГШ-503»	44200	4		176800
Вибропреобразователь «ЛВП-2с»	3600	8		28800

Размыкатель СОНАТА-БК-4.1	6000	1		6000
Генератор шума «ГАММА-ГШ18»	31500	2		63000
ФСП-32М	46000	2		92000
Размыкатель Ethernet etherCUT	12400	1		12400
Итоговая сумма	688940			

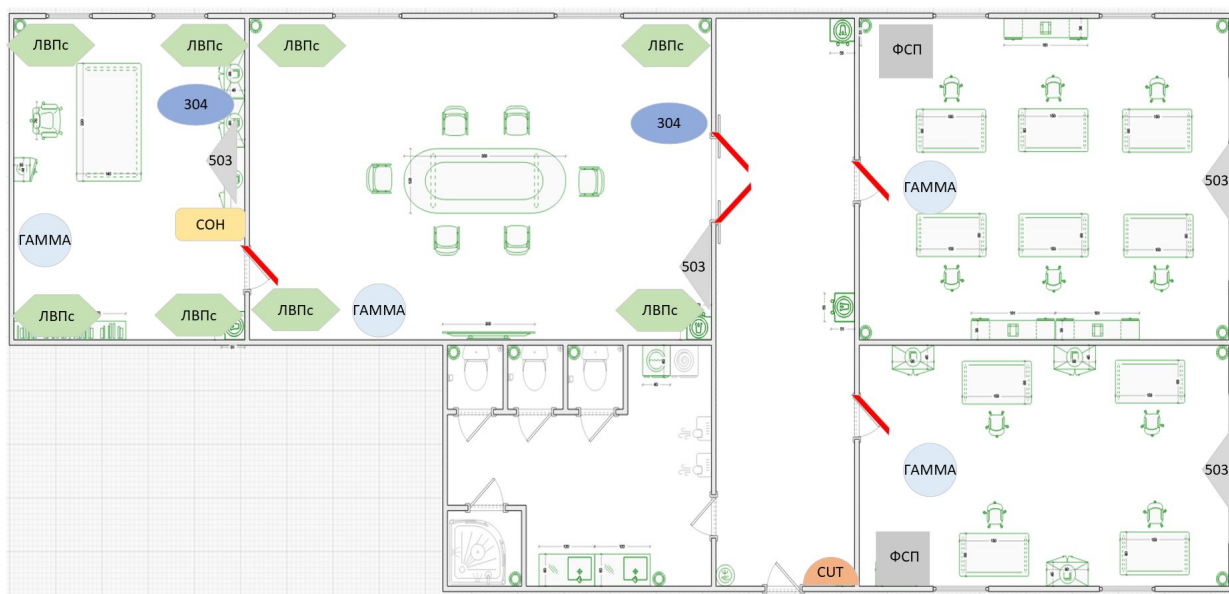


Рисунок 3 — схема расстановки устройств

ВЫВОД

В ходе данной курсовой работы был произведен теоретический обзор существующих каналов утечки информации и анализ потенциальных угроз каналов утечки информации в защищаемом помещении и описаны минимальные необходимые меры защиты.

Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и подобраны подходящие технические средства для рассматриваемого в ходе курсовой работы помещения.

В результате была предложена защита от утечки информации по акустическому, виброакустическому, акустоэлектрическому, электрическому, электромагнитному, оптическому каналам, а так же обеспечена защита от ПЭМИН.

6. ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА.

1. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. Текст: непосредственный // Молодой ученый. — 2016. — No3 (107). — С. 69–72. — URL: <https://moluch.ru/archive/107/25842/> (дата обращения: 19.01.2022).
2. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов.
3. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: <https://intuit.ru/studies/courses/3649/891/info> (дата обращения: 15.01.2022)
4. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.
5. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.