

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

**Выполнил:**

студент группы N34481

Васильева Арина Артемовна



---

(подпись)

**Проверил:**

Попов Илья Юрьевич

---

(отметка о выполнении)

---

(подпись)

Санкт-Петербург

2023г.

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

<b>Студент</b>	Васильева Арина Артемовна (Фамилия И.О)
<b>Факультет</b>	Безопасность информационных технологий
<b>Группа</b>	N34481
<b>Направление (специальность)</b>	10.03.01 (Технологии защиты информации 2020)
<b>Руководитель</b>	Попов Илья Юрьевич (Фамилия И.О)
<b>Дисциплина</b>	Инженерно-технические средства защиты информации
<b>Наименование темы</b>	Разработка комплекса инженерно-технической защиты информации в помещении
<b>Задание</b>	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**

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**


1. 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.

<b>Руководитель</b>	 (Подпись, дата)
<b>Студент</b>	 (Подпись, дата)

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

<b>Студент</b>	Васильева Арина Артемовна
	(Фамилия И.О)
<b>Факультет</b>	Безопасность информационных технологий
<b>Группа</b>	N34481
<b>Направление (специальность)</b>	10.03.01 (Технологии защиты информации 2020)
<b>Руководитель</b>	Попов Илья Юрьевич
	(Фамилия И.О)
<b>Дисциплина</b>	Инженерно-технические средства защиты информации
<b>Наименование темы</b>	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	21.09.2023	21.09.2023	
2.	Создание плана КР	22.09.2023	22.09.2023	
3.	Анализ теоретической составляющей	23.09.2023	23.09.2023	
4.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	26.10.2023	26.10.2023	
5.	Представление выполненной курсовой работы	19.12.2023	19.12.2023	


<b>Руководитель</b>	
	(Подпись, дата)
<b>Студент</b>	
	(Подпись, дата)

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

<b>Студент</b>	Васильева Арина Артемовна
	(Фамилия И.О)
<b>Факультет</b>	Безопасность информационных технологий
<b>Группа</b>	N34481
<b>Направление (специальность)</b>	10.03.01 (Технологии защиты информации 2019)
<b>Руководитель</b>	Попов Илья Юрьевич
	(Фамилия И.О)
<b>Дисциплина</b>	Инженерно-технические средства защиты информации
<b>Наименование темы</b>	Разработка комплекса инженерно-технической защиты информации в помещении

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

1. Цель и задачи работы	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	Конструирование
3. Содержание работы	<ol style="list-style-type: none"> <li>1. Введение.</li> <li>2. Анализ технических каналов утечки информации.</li> <li>3. Руководящие документы</li> <li>4. Анализ защищаемых помещений</li> <li>5. Анализ рынка технических средств</li> <li>6. Описание расстановки технических средств</li> <li>7. Заключение</li> <li>8. Список литературы</li> </ol>
4. Выводы	В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

<b>Руководитель</b>	(Подпись, дата)
<b>Студент</b>	 (Подпись, дата)

«\_\_» \_\_\_\_\_ 20\_\_ г.

## СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ .....	9
ВВЕДЕНИЕ .....	11
ОСНОВНАЯ ЧАСТЬ .....	12
1     Организационная структура предприятия.....	14
2     Обоснование защиты информации .....	19
3     Анализ рынка технических средств защиты информации .....	21
3.1   Устройства противодействия утечке информации по акустическому и виброакустическому каналам .....	21
3.2   Устройства противодействия утечке информации по оптическому каналу.....	23
3.3   Устройства противодействия утечке по электромагнитным и электрическим каналам.....	23
4     Описание расстановки технических средств .....	26
ЗАКЛЮЧЕНИЕ.....	28
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....	29

## 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).

## **ВВЕДЕНИЕ**

Цель работы – повышение защищенности рассматриваемого помещения.

Задачи:

- Проанализировать защищаемое помещение;
- Оценить каналы утечки информации;
- Проанализировать рынок;
- Выбрать меры пассивной и активной защиты информации;
- Представить результат работы в виде схемы с установленными средствами

защиты.



## ОСНОВНАЯ ЧАСТЬ

Чтобы построить эффективную систему предотвращения утечки информации в первую очередь необходимо определить потенциальные и реальные угрозы технологического проникновения на защищаемый объект, несанкционированного доступа и утечки защищаемой информации.

Эта работа основывается на знании физической природы возникающих технологических каналов утечки информации и методов технологической разведки. Правильная идентификация потенциальных угроз на предварительных этапах проекта по созданию системы защиты от промышленного шпионажа позволит в дальнейшем выбрать наиболее подходящие контрмеры и защитные меры.

При выявлении технических путей утечки информации необходимо комплексно рассмотреть основное оборудование технических средств обработки информации, соединительные линии, силовые распределительные и коммутационные устройства, системы электроснабжения, системы вентиляции и другие элементы защиты.

Помимо основных технических средств, непосредственно связанных с обработкой и передачей конфиденциальной информации, необходимо учитывать вспомогательные технические средства и системы (ВТС), такие как технические средства открытой телефонной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часовые системы, электроприборы и другие. Наибольшее внимание следует уделять вспомогательным средствам, линии которых находятся за пределами контролируемой зоны, а также посторонним линиям и кабелям, проходящим через помещения, где установлено основное и вспомогательное техническое оборудование, металлические трубы, системы отопления, водоснабжения и другие токопроводящие металлические конструкции.

При оценке защищенности объекта от утечек аудиоинформации следует учитывать возможность подслушивания с соседних объектов или улиц. Следует оценить возможность разведки с помощью лазерных микрофонов. Интерес могут представлять каналы утечки из-за вибрации, вызванной звуковым давлением твердых тел (заборы, трубы и т.д.).

Цель защиты информации от шпионажа техническими средствами на конкретном объекте разведки определяется конкретным перечнем потенциальных угроз. В общем случае цели защиты информации могут быть сформулированы следующим образом:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Эффективность защиты информации определяется своевременностью, активностью, непрерывностью и комплексностью. Крайне важно реализовать комплексные меры защиты, то есть перекрыть все опасные каналы утечки информации. Следует помнить, что эффективность системы защиты снижается при наличии хотя бы одного не закрытого канала утечки.

## 1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

Наименование организации: ООО «Кинжал»

Область деятельности: оказание услуг по созданию сайтов, принимает заказы в том числе от гос. компаний, поэтому происходит работа со сведениями, представляющими государственную тайну.

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа:

Основные информационные процессы:

1. Публикация предложения услуг.
2. Предоставление пользователям инструментов для заказа услуги и создания учётной записи на сайте.
3. Техническое сопровождение оказания услуги.
4. Предоставление консультаций пользователям.
5. Удаление данных по завершении сотрудничества.
6. Ведение бухгалтерского учёта организации, взаимодействие внутренних отделов с бухгалтерией.
7. Хранение, обработка, передача, утилизация персональных данных пользователей.

Информация ограниченного доступа:

1. Персональные данные сотрудников (ПД)
2. Персональные данные клиентов (ПД)
3. Техническая информация (ТИ)
4. Коммерческая тайна (КТ)
5. Государственная тайна (ГТ)

На рисунке 1 представлена организационная структура предприятия.



Рисунок 1 – Организационная структура предприятия

Основные информационные потоки, циркулирующие в организации, можно увидеть на рисунке 2.

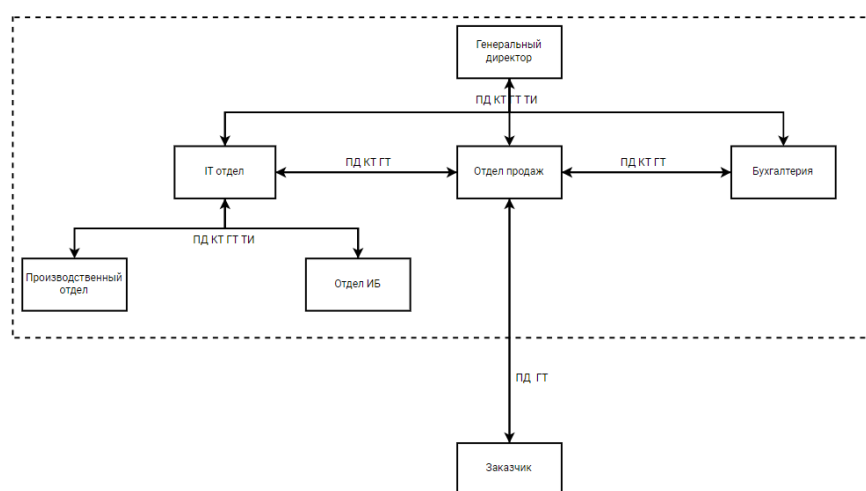


Рисунок 2 – Основные информационные потоки

На рисунке 3 представлен общий план защищаемого помещения.

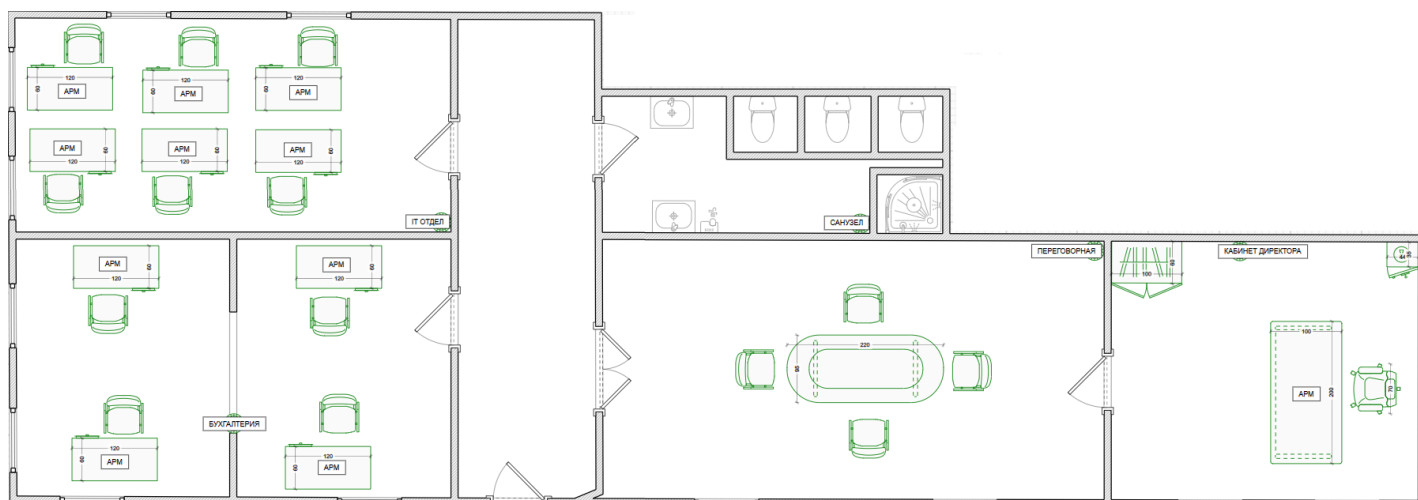
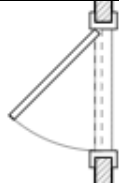
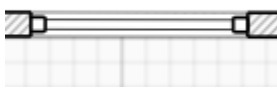
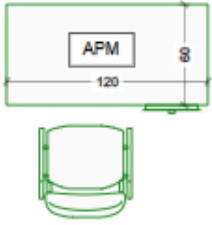
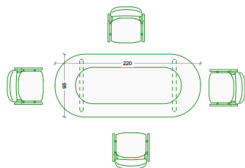
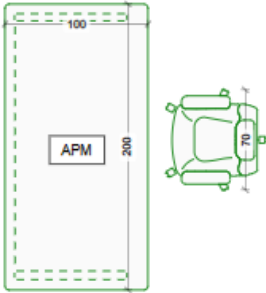

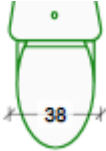
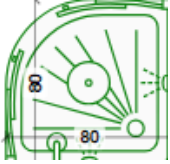
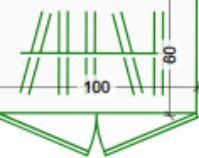



Рисунок 3 – План помещения

В таблице 1 приведены обозначения компонентов плана.

Таблица 1 – обозначения

Обозначение	Описание
	Дверь
	Окно
	РМ сотрудника
	Стол для переговоров
	РМ директора
АРМ	Компьютер
	Раковина
	Унитаз

	Душевая кабина
	Шкаф
	Сейф

Помещения, требующие защиты:

- Переговорная: 6м на 12м – 72м<sup>2</sup>
- Кабинет директора: 6м на 6м – 36м<sup>2</sup>
- Санузел: 8 м на 3м - 24м<sup>2</sup>
- Бухгалтерия: 6м на 8м – 48м<sup>2</sup>
- IT отдел: 5м на 8м – 48м<sup>2</sup>

Для ведения переговоров предназначено помещение (переговорная). В переговорной находятся: стол, 4 стула, 3 розетки. В кабинете директора: стол, стул, компьютер, 2 розетки, сейф, шкаф. В IT отделе: 6 рабочих мест с АРМ, 12 розеток. В комнате бухгалтерии 4 стола, 4 стула и 4 АРМ. Помещение расположено на 1 этаже трехэтажного здания, окна выходят в закрытый контролируемый двор. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

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

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

Таблица 2 – Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
акустический акустоэлектрический	Проводка, двери, окна	Сетевые фильтры, звукоизоляция	Акустическое зашумление
вибрационный виброакустический	Батареи и трубы, стены, пол, окна, двери	Изолирующие звук и вибрацию материалы стен	Вибрационное зашумление
оптический	Окна, двери	Жалюзи/шторы на окнах, доводчики на двери	Блокирующие обзор устройства
электромагнитный электрический	АРМ, ноутбуки, бытовые приборы, телевизоры, розетки	Сетевые фильтры	Электромагнитное зашумление

## **2       ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ**

Для обоснования защиты информации мы проведём анализ существующих РПД. Так как наше предприятие работает с государственной тайной, то рассмотрим документы, которые относятся к гос. тайне.

### **1. Законы Российской Федерации:**

«О государственной тайне» от 21 июля 1993 г. N 5485–1 (последняя редакция).

Настоящий Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Государственную тайну составляют:

- сведения в военной области
- сведения в области экономики, науки и техники

Статья 27. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.

### **Статья 30. Контроль за обеспечением защиты государственной тайны**

Контроль за обеспечением защиты государственной тайны осуществляют Президент Российской Федерации, Правительство Российской Федерации в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

### **2. Указы Президента Российской Федерации:**

«Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203.



«О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. №1108.

«Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.

### 3. Постановления Правительства Российской Федерации:

Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам  
Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. №921-51.

«О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. №333.

«О внесении дополнения в Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 30 апреля 1997 г. №513.

«Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870.

«О сертификации средств защиты информации» от 26 июня 1995 г, №608.

### **3 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

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.	15 600
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	25 220
SI-3030 Виброакустический шумогенератор	Спектр шумовой помехи 125 Гц - 6,3 кГц	Предназначен для защиты помещений от прослушивания через строительные элементы конструкции.	28 500
"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.	18 000
«БУБЕН» - генератор акустической помехи	Диапазон рабочих частот 400...18000 Гц	Используется для защиты конфиденциальных переговоров по принципу создания акустических помех. Вид помех: речеподобная, "белый шум".	15 000
Упрощенный вариант генератора ГШ-111У	В комплект поставки входит генератор ГШ-111У и ПО конфигурирования системы / Дополнительно к генератору можно приобрести: Антенна 6 ГГц активная АА-6000,	Упрощённый вариант генератора шума без кнопочной клавиатуры и ЖКИ. Управление, регулировка и контроль осуществляются только через компьютер по сети Ethernet.	75 000

	Антенна 3 ГГц пассивная двухкомпонентная ПА-111		
Система активной акустической и вибрационной защиты акустической речевой информации "Соната-АВ" модель 4Б	Диапазон частот до 2 ГГц, диапазон регулировки	Генератор шума. Регулировка уровня шума в 3 частотных полосах. Индикация нормального/аварийного режима работы.	23 000

В результате анализа был выбран генератор акустического шума ЛГШ-304. Генератор 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 нам подходит за свою цену.

### **3.2 Устройства противодействия утечке информации по оптическому каналу**

Для обеспечения защиты помещения от визуального наблюдения, необходимо установить на окно жалюзи или шторы. С точки зрения удобства содержания 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» оснащено счетчиком учета времени наработки,	44200 руб.

		<p>учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех. Конструкция Изделия «ЛГШ-503» обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.</p> <p>Изделие «ЛГШ-503» имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».</p>	
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.	57 000
Генератор виброакустического шума SEL SP-157G	Принцип действия основан на формировании широкополосных акустических и виброакустических маскирующих шумовых помех (аналоговый белый шум или смешанный с цифровой речеподобной помехой).	Фильтр сетевой помехоподавляющий ФСПК-40-220-99-УХЛ4 предназначен для защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания. В общем случае защитное устройство может применяться как сетевой фильтр для улучшения параметров качества сети.	70 500

	Система состоит из центрального генераторного блока и подключаемых к нему по проводам пассивных электромагнитных (вибрационных) или электродинамических (акустических) преобразователей (излучателей).		
ЛРЧФ-100-1Ф	Диапазон рабочих частот 0,15 - 40 000 МГц	Изделие «ЛРЧФ-100-1Ф» предназначено для исключения или затруднения получения иностранной радио-, радиотехнической разведкой охраняемых параметров образцов вооружения и военной техники (ВиВТ) на технологических рабочих местах путем ограничения электромагнитной энергии опасного сигнала внутри замкнутых экранов в линиях электропитания напряжением до 380 В. Изделие «ЛРЧФ-100-1Ф» является пассивным техническим средством противодействия иностранной радио-, радиотехнической разведке.	83 200

По результатам анализа была выбран генератор шума ЛГШ-503. Из-за невысокой цены и достаточного функционала.



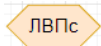





#### 4 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

Выбранные средства защиты информации включают в себя:

- Усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей прокладкой на металлическом каркасе – 4 шт., в переговорную, кабинет директора, бухгалтерию и IT отдел.
- «ЛГШ-304» - генератор акустической помехи
- «ЛГШ-503»
- ФСП-1Ф-7А Фильтр сетевой помехоподавляющий
- РАЗМЫКАТЕЛЬ СОНАТА-ВК 4.1 для защиты телефонной линии

Общие трудозатраты описаны в таблице 5.

Таблица 5 – Смета

Устройство	Цена, руб	Кол-во	Обозначение	Стоимость, руб
Усиленные звукоизолирующие двери Ultimatum PP	75 283	4		301 132
«ЛГШ-304»	25 220	2		50 440
Вибропреобразователь «ЛВП-2с»	3640	8		29 120
РАЗМЫКАТЕЛЬ СОНАТА-ВК 4.1 телефонных линий	6000	1		6000
РАЗМЫКАТЕЛЬ СОНАТА-ВК 4.3 ethernet	6000	1		6000
Генератор шума "Гамма-ГШ18"	31 500	4		126 000
"ЛГШ-503"	44 200	4		176 800
ФСП-1Ф-7А Фильтр сетевой помехоподавляющий	15 300	3		45 900
ИТОГО				654 349

На рисунке 6 представлен план защищенного помещения.

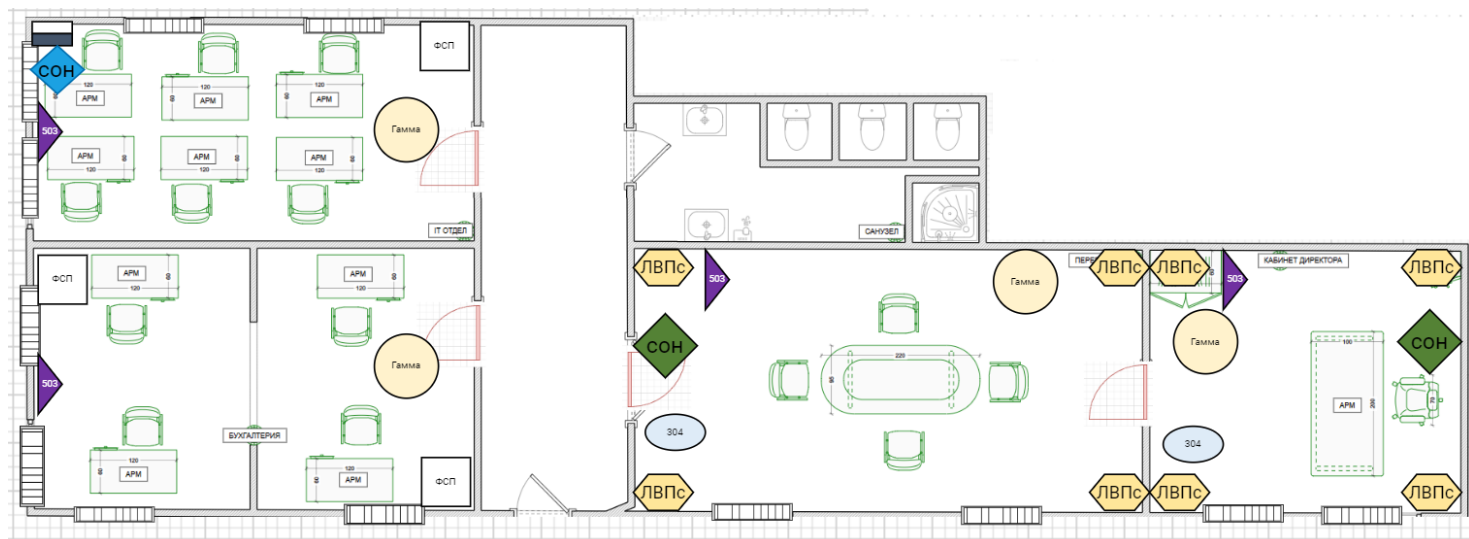


Рисунок 4 – Схема расстановки устройств



## **ЗАКЛЮЧЕНИЕ**

В ходе данной работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении и описаны необходимые меры их защиты. Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для нашего объекта. Был разработан план установки и произведен расчет сметы затрат. В результате была предложена защита от утечек информации по акустическому, виброакустическому, оптическому, акустоэлектрическому, электрическому, электромагнитному техническим каналам защиты информации, обеспечена защита от ПЭМИН.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. 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.
2. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — №3 (107). — С. 69–72. — URL: <https://moluch.ru/archive/107/25842/> (дата обращения: 19.01.2022).
3. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.
4. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: <https://intuit.ru/studies/courses/3649/891/info> (дата обращения: 15.01.2022)