

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

**Факультет безопасности информационных технологий**

**КУРСОВАЯ РАБОТА**

**По дисциплине:**

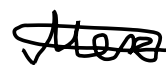
***«Инженерно-технические средства  
защиты  
информации»***

**На тему:**

**«Проектирование инженерно-технической защиты информации на  
предприятии»**

**Выполнил(а):**

Студент группы N34491  
Механиков Д. И.



**Проверил преподаватель:**

Попов И. Ю., к. т. н., доцент  
ФБИТ

**Отметка о выполнении:**

г. Санкт-Петербург  
2023

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

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

Студент	Механиков Данила Игоревич (Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34491
Направление (специальность)	Информационная безопасность
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ (Фамилия И.О., должность, учено звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии
Задание	Разработать системы инженерно-технической защиты информации на предприятии

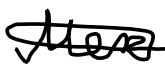
**Краткие методические указания**

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

**Содержание пояснительной записки**

- Введение.
- Организационная структура предприятия.
- Обоснование защиты информации.
- Анализ защищаемых помещений.
- Анализ рынка технических средств.
- Описание расстановки технических средств.
- Заключение.

**Рекомендуемая литература**

Руководитель		(Подпись, дата)
Студент		21 декабря 2023 (Подпись, дата)

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

Студент      Механиков Данила Игоревич

(Фамилия И.О.)

Факультет      Безопасность информационных технологий

Группа      N34491

Направление (специальность)      Информационная безопасность

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

(Фамилия И.О., должность, ученое  
звание, степень)

Дисциплина      Инженерно-технические средства защиты информации


Наименование темы      Проектирование инженерно-технической системы защиты информации на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируе мая	Фактичес кая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	18.12.2023	18.12.2023	
2	Анализ теоретической составляющей	19.12.2023	20.12.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	21.12.2023	21.12.2023	
4	Представление выполненной курсовой работы	21.12.2023	21.12.2023	

Руководитель

(Подпись, дата)

Студент



21 декабря 2023

(Подпись, дата)

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

Студент	Механиков Данила Игоревич
	(Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34491
Направление (специальность)	Информационная безопасность
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

**1. Цель и задачи работы**

Предложены студентом	<input checked="" type="checkbox"/>	Сформулированы при участии студента	<input type="checkbox"/>
		Определены руководителем	<input type="checkbox"/>

**2. Характер работы**

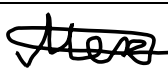
Расчет	<input type="checkbox"/>	Моделирование	<input type="checkbox"/>
		Конструирование	<input type="checkbox"/>
		Другое: Исследовательская работа	<input checked="" type="checkbox"/>

**3. Содержание работы**

В ходе работы мы познакомимся с рынком инженерно-технических средств защиты информации а также разработаем инженерно-техническую систему защиты информации

**4. Выводы**

В результате выполнения курсовой работы я спроектировал инженерно-техническую систему защиты информации для предприятия «Тракт». Также научился выделять организационную структуру, провёл анализ рынка решений, а также разработал итоговый план предприятия.

Руководитель		(Подпись, дата)
Студент	 21 декабря 2023	
	(Подпись, дата)	

« 21 » декабря 2023 г.

## Содержание

ВВЕДЕНИЕ .....	5
1     Организационная структура предприятия .....	6
2     Обоснование защиты информации .....	8
3     Рассмотрение плана .....	16
4     Анализ способов утечки информации .....	17
5     Анализ рынка технических средств .....	18
5.1    Акустический и виброакустический каналы .....	18
5.2    Оптический канал .....	20
5.3    Электрический, электромагнитный и акустоэлектрический каналы .....	20
5.4    Побочное электромагнитное излучение и наводки (ПЭМИН) .....	22
6     Итоговый план .....	25
ЗАКЛЮЧЕНИЕ .....	26
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....	27

## ВВЕДЕНИЕ

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 объекте информатизации. Защищаемый объект состоит из десяти помещений и представляет собой офис предприятия с переговорной, кабинетом директора, серверной, двумя санузлами, 3 кабинетами отдела разработки, главным холлом, серверной и кухней.

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 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

Организация производит различное ПО для военно-промышленного комплекса, а следовательно, имеет сведения, которые относятся к государственной тайне в соответствии с «Перечень сведений, отнесенных к государственной тайне» сведения, раскрывающие направления развития, содержание разработки вооружения, военной техники имеют степень секретности данных сведений – «секретно».

Рассмотрим информационные потоки организации (рисунок 1) и структуру организации (рисунок 2).

Информационный поток — это совокупность циркулирующих в логистической системе, между логистической системой и внешней средой сообщений, необходимых для управления, анализа и контроля логистических операций. Они играют ключевую роль в функционировании предприятия, их правильное управление и защита существенны для обеспечения конфиденциальности, целостности и доступности информации. Они могут существовать в виде бумажных, электронных документов (носителей), звука, символов и сигналов.

двусторонний закрытый информационный поток –  $\longleftrightarrow$

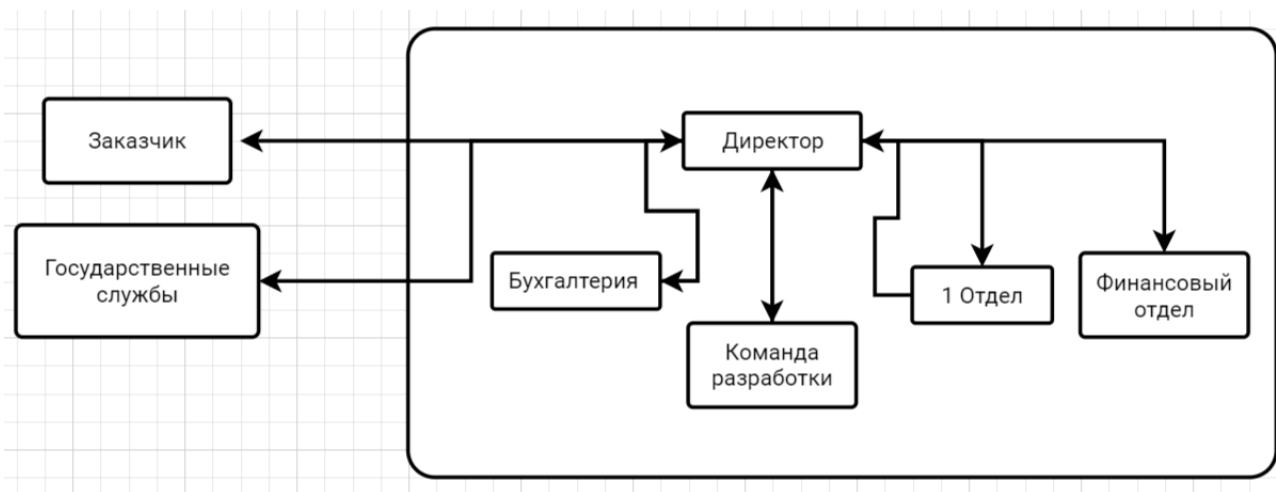


Рисунок 1 – Информационные потоки

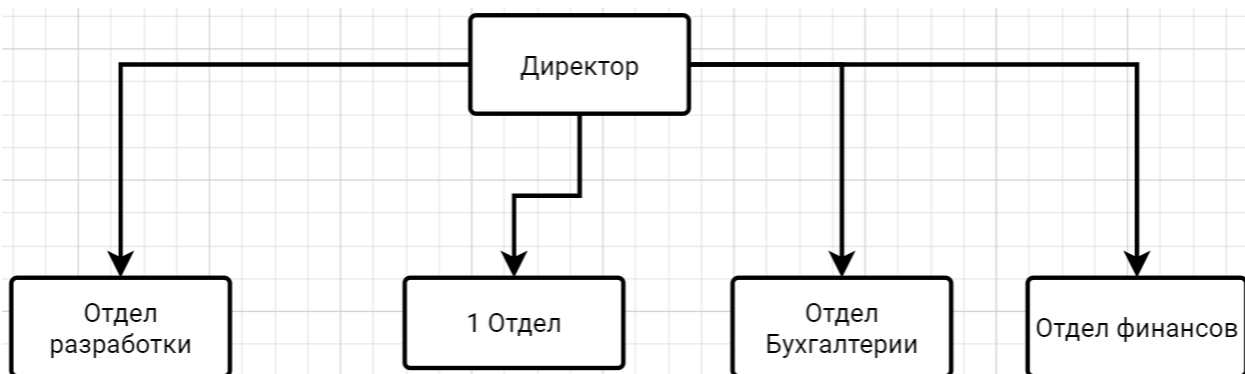


Рисунок 2 – Структура организации



## **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:

- о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;
- о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;
- о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;
- о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;
- о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2. сведения в области экономики, науки и техники:

- о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;
- об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства
- об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;
- о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

**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.**

В соответствии со статьей 4 Закона Российской Федерации "О государственной тайне" постановляю:

1. Утвердить прилагаемый перечень сведений, отнесенных к государственной тайне.
3. Правительству Российской Федерации организовать работу по приведению действующих нормативных актов в соответствие с перечнем сведений, отнесенных к государственной тайне.
4. Настоящий Указ вступает в силу со дня его подписания.

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

В соответствии с Законом Российской Федерации "О государственной тайне" постановляю:

1. Образовать Межведомственную комиссию по защите государственной тайн

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

В целях дальнейшего совершенствования порядка опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти постановляю:

Утвердить прилагаемый перечень сведений конфиденциального характера.

## **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.**

Настоящее Положение является документом, обязательным для выполнения при проведении работ по защите информации, содержащей сведения, составляющие государственную или служебную тайну.

Работы по защите информации в органах государственной власти и на предприятиях проводятся на основе актов законодательства РФ.

Защита осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного

доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путём проведения специальных работ, порядок организации и выполнения которых определяется Правительством РФ

Главными направлениями работ по защите информации являются:

- Обеспечение эффективного управления системой защиты информации
- Определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения
- Анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технически каналов утечки сведений, подлежащих защите
- Разработка организационно-технических мероприятий по защите информации и их реализация
- Организация и проведение контроля состояния защиты информации

Основными организационно-техническими мероприятиями по защите информации являются:

- Лицензирование деятельности предприятий в области защиты информации
- Аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности
- Сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам
- Введение территориальных, частотных, энергетически, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите
- Создание и применение информационных и автоматизированных систем управления в защищенном исполнении
- Разработка и внедрение технических решений и элементов защиты информации при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи
- Разработка средств защиты информации и контроля за её эффективностью (специального и общего применения) и их использование

– Применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи

**«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.**

В соответствии с Законом Российской Федерации "О государственной тайне" и в целях установления порядка допуска 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, Правительство Российской Федерации постановляет:

1. Утвердить 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 (прилагается).
3. Федеральной службе безопасности Российской Федерации, Государственной технической комиссии при Президенте Российской Федерации, Федеральному агентству правительственной связи и информации при Президенте Российской Федерации, Службе внешней разведки Российской Федерации совместно с заинтересованными министерствами и ведомствами Российской Федерации в 3-месячный срок разработать комплекс мер организационного, материально-технического и иного характера, необходимых для осуществления лицензирования деятельности предприятий, организаций и учреждений по проведению работ, связанных с использованием сведений, составляющих государственную тайну.
5. Установить, что предприятия, учреждения и организации, допущенные к моменту принятия настоящего постановления к работам, связанным с использованием сведений, составляющих государственную тайну, могут осуществлять эти работы в течение 1995 года.
7. Лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных

за защиту сведений, составляющих государственную тайну (далее именуются - руководители предприятий), и при выполнении следующих условий:

- соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;
- наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны;
- наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

**«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.**

В связи с созданием в Министерстве обороны Российской Федерации системы сертификации средств защиты информации, предусмотренной постановлением Правительства Российской Федерации от 26 июня 1995 г. N 608 "О сертификации средств защиты информации" (Собрание законодательства Российской Федерации, 1995, N 27, ст. 2579), Правительство Российской Федерации постановляет :

Дополнить абзац третий пункта 2, абзацы второй и пятый пункта 10 Положения 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, утвержденного постановлением Правительства Российской Федерации от 15 апреля 1995 г. N 333 (Собрание законодательства Российской Федерации, 1995, N 17, ст. 1540; 1996, N 18, ст. 2142), после слов: "Служба внешней разведки Российской Федерации" словами: "Министерство обороны Российской Федерации".

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

1. Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен

безопасности Российской Федерации вследствие распространения указанных сведений.

6. Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на сведения особой важности, совершенно секретные и секретные.
7. К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из указанных областей.
8. К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам государственного органа или отрасли экономики Российской Федерации в одной или нескольких из указанных областей.
9. К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-разыскной области деятельности.

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

В соответствии с Законами Российской Федерации "О государственной тайне" и "О сертификации продукции и услуг" Правительство Российской Федерации постановляет:

1. Утвердить прилагаемое Положение о сертификации средств защиты информации.
2. Государственной технической комиссии при Президенте Российской Федерации, Федеральному агентству правительственной связи и информации при Президенте Российской Федерации, Федеральной службе безопасности Российской Федерации и Министерству обороны Российской Федерации в пределах определенной законодательством Российской Федерации компетенции в 3-месячный срок разработать и ввести в действие соответствующие положения о системах сертификации, перечни средств защиты информации, подлежащих

сертификации в конкретной системе сертификации, а также по согласованию с Министерством финансов Российской Федерации порядок оплаты работ по сертификации средств защиты информации.

3. Настоящее Положение устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом.

Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных Федеральной службой безопасности Российской Федерации.

Система сертификации средств защиты информации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам (далее именуется - система сертификации).

Системы сертификации создаются Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации, Министерством обороны Российской Федерации, уполномоченными проводить работы по сертификации средств защиты информации в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации (далее именуются - федеральные органы по сертификации).



### 3 РАССМОТРЕНИЕ ПЛАНА

На рисунке 3 представлен план предприятия.

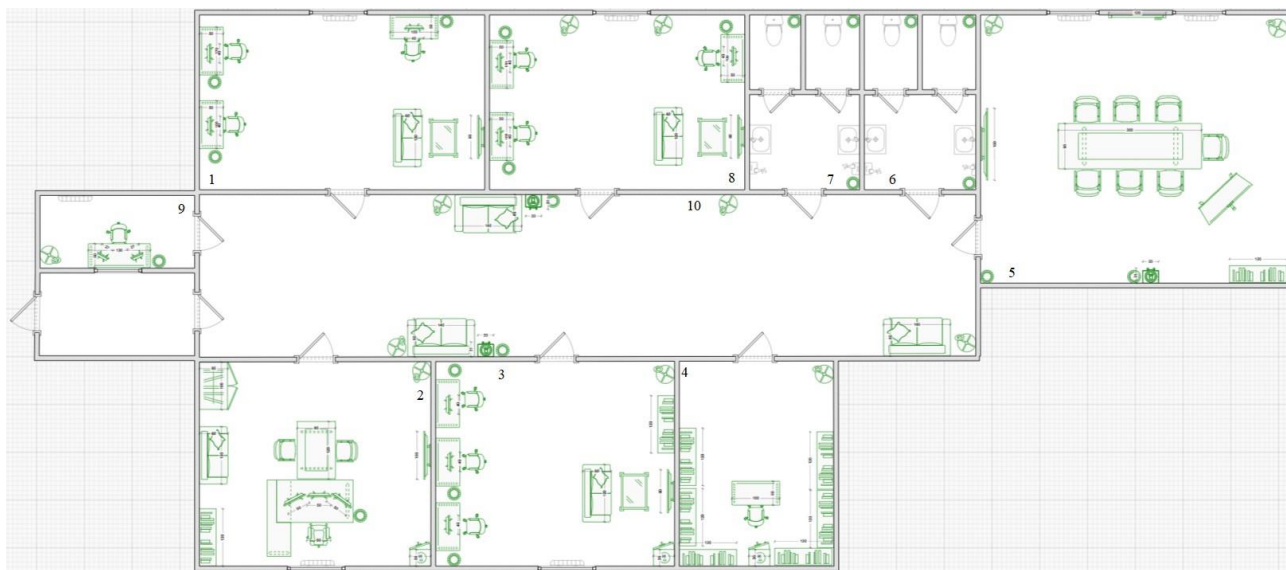


Рисунок 3 – План предприятия

Помещения:

1. Отдел разработки (гос. тайна)
2. Кабинет директора (гос. тайна)
3. 1 Отдел(гос. тайна)
4. Секретный архив
5. Переговорная
6. Мужской туалет
7. Женский туалет
8. Бухгалтерия и финансовый отдел
9. Комната охраны
10. Коридор

#### 4 АНАЛИЗ СПОСОБОВ УТЕЧКИ ИНФОРМАЦИИ

Во всех помещениях используются декоративные элементы, в которые потенциально могут быть заложены закладные устройства.

Каждое помещение, требующее защиты, оснащено розетками.

Таким образом, актуальны следующие угрозы:

- Закладное устройство;
- Электрические и электромагнитные каналы утечки;
- Вибрационные каналы утечки;
- Оптические каналы утечки;
- Акустические, виброакустические, акустоэлектрические каналы утечки.

#### Выбор необходимых средств защиты информации

Определим в таблице 1 необходимые средства защиты

Таблица 1 – Средства защиты информации

Каналы утечки	Источники утечки	Пассивная защита	Устройства активной защиты
Вибрационный и виброакустический	Твердые поверхности, радиаторы	Добавление дополнительного помещения перед переговорной	Вибрационное зашумление
Оптический	Окна, двери	Шторы, доводчики для плотного закрывания дверей	Бликующие устройства
Электромагнитный и электрический	ПК, розетки, техника	Фильтры для сетей	Электромагнитное зашумление
Акустический и акустоэлектрический	Окна, двери	Звукоизоляция, фильтры для сетей электропитания	Акустическое зашумление

## 5 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

### 5.1 Акустический и виброакустический каналы

Пассивной защитой будет выступать усиленные двери в кабинет директора и переговорную, дополнительное помещение перед переговорной.

Средствами виброакустического зашумления будет выбрано на основании сравнении компонентов таблицы 2.

Таблица 2 – Активная защита от утечек информации по виброакустическим каналам

Модель	Цена, руб.	Характеристики	Особенности
ЛГШ-404	35 100	Электропитание 220 В/50 Гц. Максимальное количество излучателей – 40. Диапазон воспроизводимого шумового сигнала 175–11200 Гц.	Одно из существенных преимуществ системы – вариативность количества подключаемых к генераторному блоку преобразователей. Уровень шумового сигнала, создаваемого генератором ЛГШ, регулируется.
SEL SP-157 Шагренъ	47 400	Диапазон воспроизводимого шумового сигнала 90–	Защита паролем настроек системы. Отсчёт времени наработки генерации
		11200 Гц. Максимальное количество излучателей – 64. Электропитание 220В/50Гц.	шума по каждому каналу с выводом на экран. Непрерывный контроль состояния системы и каждого отдельного излучателя.

Соната АВ-4Б	<p>Диапазон воспроизводимого шумового сигнала 175–11200 Гц.</p> <p>Выходное напряжение В <math>12,5 \pm 0,5</math>.</p> <p>Электропитание сеть ~220 В/50 Гц.</p>	<p>Диапазон воспроизводимого шумового сигнала 175–11200 Гц.</p> <p>Выходное напряжение В <math>12,5 \pm 0,5</math>.</p> <p>Электропитание сеть ~220 В/50 Гц.</p>	<p>Комплект состоит из блоков электропитания и управления, генераторов акустоизлучателей, генераторов-вибровозбудителей, размыкателя телефонной линии, размыкателя слаботочной линии, размыкателя линии Ethernet, пульта управления, блоков сопряжения из внешних устройств. Технического средства защиты речевой информации от утечки по оптико-электронному (лазерному) каналу и прочих аксессуаров.</p>
Шорох 5Л	21 500	<p>Максимальное количество излучателей 40.</p> <p>Электропитание 220 (+10% - 15%) В (есть возможность работы системы от источника питания 12В).</p> <p>Количество октавных полос для регулировки уровня мощности шума 7.</p>	<p>Сетевой генератор шума. Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.</p>

Исходя из анализа, представленного в таблице 2, было принято решение о выборе системы «СОНАТА АВ-4Б». Особенностью «Соната АВ-4Б» является использование

принципа «единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)», что обеспечивает высокую степень надежности в защите информации. Кроме того, усовершенствованная настройка аппаратных элементов модели

4Б позволяет интегрировать источник электропитания с другими для обмена информацией.

## 5.2 Оптический канал

Для обеспечения защиты помещения от возможной фото-видеосъемки или визуального наблюдения следует установить жалюзи на окна и также воспользоваться доводчиками для дверей.

## 5.3 Электрический, электромагнитный и акустоэлектрический каналы

Пассивная защита основывается на установке фильтров для сетей электропитания во всех помещениях.

Выберем средство активной защиты.

Таблица 3 – Электрические и электромагнитные каналы утечки

Модель	Цена, руб.	Характеристики	Особенности
Соната-РС3	32 400	Работа от сети ~220 В +10%/15%, 50 Гц. Потребляемая мощность – 10Вт. Продолжительность работы не менее 8 часов.	Звуковая и световая индикация работы. Возможно дистанционное управление посредством проводного пульта.

ЛГШ-221	36 400	<p>Диапазон частот 10 кГц – 400 МГц.</p> <p>Диапазон регулировки уровня выходного шумового сигнала не менее 20 дБ.</p> <p>Мощность, потребляемая от сети не более 45 ВА.</p>	<p>Сетевой генератор шума.</p> <p>Устройство оснащено световым и звуковым индикаторами работы.</p> <p>Возможность управления устройством с помощью пульта ДУ.</p>
Соната- РС1	16 520	<p>Диапазон частот до 1 ГГц,</p> <p>регулировка уровня шума в 1 частотной полосе.</p> <p>Напряжение 220 В.</p>	<p>Возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus)</p>
Генератор шума Покров	32 800	<p>Диапазон частот 10 кГц – 6000 МГц.</p> <p>Мощность 15 Вт.</p> <p>Наработка на отказ 5000 часов.</p>	<p>Централизованное управление и контроль по Ethernet (для исполнения 2), для применения в системах пространственного зашумления. Независимая регулировка уровней электромагнитного поля шумового сигнала и шумового сигнала в линии электропитания и заземления.</p>

На основании анализа, проведенного в таблице 3, был выбран генератор шума «Покров». Оптимальный вариант по соотношению цена и качество.

#### 5.4 Побочное электромагнитное излучение и наводки (ПЭМИН)

Проведем анализ в таблице 4 активную защиту от ПЭМИН

Таблица 4 – Активная защита от ПЭМИН

Модель	Цена, руб.	Характеристики	Особенности
ЛГШ 503	44 200	Диапазон частот 10 кГц - 1800 МГц. Уровень шума от -26 дБ (мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц). Мощность – 45 Вт.	Оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Оснащен счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы в режиме формирования маскирующих помех. Прибор имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программноаппаратный комплекс «Паутина».

ЛГШ 513	39000	<p>Диапазон частот 10 кГц - 1800 МГц</p> <p>Уровень шума от -18 дБ(мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц)</p> <p>Электропитание однофазная сеть переменного тока 187 В-242 В</p> <p>Мощность не более 45 ВА</p> <p>Режим работы круглосуточно</p>	<p>Оснащен визуальной системой индикации</p> <p>нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа).Оснащен счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы в режиме формирования маскирующих помех. Прибор имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программноаппаратный комплекс «Паутина».</p>
Генератор шума Покров	32 800	<p>Диапазон частот 10 кГц – 6000 МГц.</p> <p>Мощность 15 Вт. Нарботка на отказ 5000 часов.</p>	<p>Централизованное управление и контроль по Ethernet (для исполнения 2), для применения в системах пространственного зашумления. Независимая регулировка уровней электромагнитного поля шумового сигнала и шумового сигнала в линии электропитания и заземления.</p>

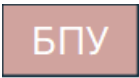

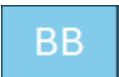
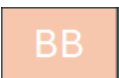

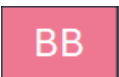
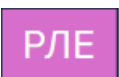
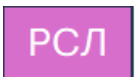
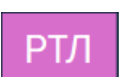

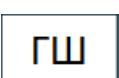

Средством ПЭМИН было выбрано входящее в состав ЛГШ-513. Модификация ЛГШ-513Ф соответствует требованиям ФСБ России к средствам активной защиты информации, обрабатываемой техническими средствами от утечки за счет ПЭМИН.

По результатам анализа рынка я выбрал средства защиты представленные в таблице

5.



Таблица 5 – Средства технической защиты.

Обозначение	Устройство
	Блок электропитания и управления «Соната-ИП4.3»
	Генератор-акустоизлучатель «Соната СА-4Б1»
	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)
	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)
	Генератор-вибровозбудитель «Соната СВ-4Б» (трубопровод)
	Размыкатель линии «Ethernet» «Соната-ВК4.3»
	Размыкатель слаботочной линии «Соната-ВК4.2»
	Размыкатель телефонной линии «Соната-ВК4.1»
	Сетевой генератор шума «Покров»
	Генератор шума «ЛГШ-513»
	Шторы BlackOut

## 6 ИТОГОВЫЙ ПЛАН

В данном разделе мы спроектировали инженерно-техническую систему защиты информации на предприятии «Тракт».

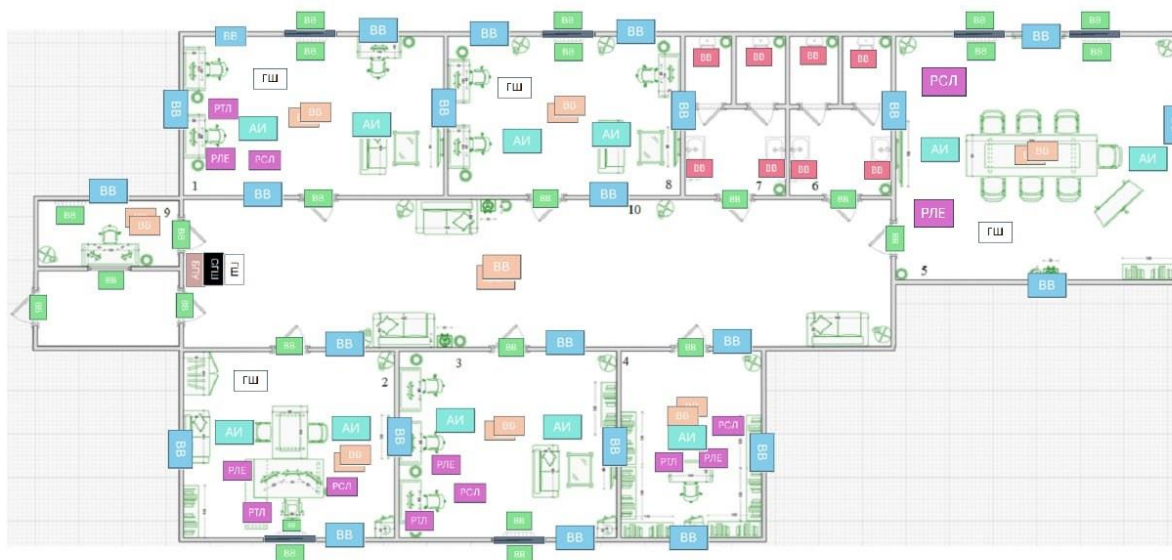


Рисунок 4 – Инженерно-техническая система защиты информации

## **ЗАКЛЮЧЕНИЕ**

В ходе данной курсовой работы был составлен план помещения, изучен теоретический материал, проведен анализ возможных каналов утечки секретной информации, описаны необходимые меры. Были выбраны меры защиты информации, проанализированы существующие средства защиты от различных утечек. Также был разработан план установки выбранных пассивных и активных средств защиты.

## 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. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.
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. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст :непосредственный // Молодой ученый. — 2016. — No 3 (107). — С. 69-72. — URL: <https://moluch.ru/archive/107/25842/> (дата обращения: 17.12.2022).