

**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:**

Семенов Владислав Дмитриевич,  
студент группы N34501

\_\_\_\_\_  
(подпись)

**Проверил преподаватель:**

Попов И.Ю., к.т.н.

**Отметка о выполнении:**

\_\_\_\_\_

Санкт-Петербург

2023 г.

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

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

Студент	Семенов Владислав Дмитриевич
	(Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34501
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
Задание	Разработать системы инженерно-технической защиты информации на предприятии

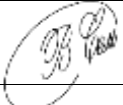
**Краткие методические указания**

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

**Содержание пояснительной записки**

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

**Рекомендуемая литература**

Руководитель		(Подпись, дата)
Студент		16.11.2023
		(Подпись, дата)

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

**Студент**    Семенов Владислав Дмитриевич

(Фамилия И.О.)

**Факультет**    Безопасность информационных технологий

**Группа**    N34501

**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
		Планируема я	Фактически я	
1	Разработка и утверждение задания и календарного плана на курсовую работу	24.10.2023	24.10.2023	
2	Анализ теоретической составляющей	26.10.2023	26.10.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	27.10.2023	27.11.2023	
4	Представление выполненной курсовой работы	16.11.2023	16.11.2023	

**Руководитель** \_\_\_\_\_

(Подпись, дата)

**Студент** \_\_\_\_\_

16.11.2023

(Подпись, дата)

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

Студент Семенов Владислав Дмитриевич

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34501

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 ☐ Сформулированы при участии студента  
☒ Определены руководителем

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

**2. Характер  
работы**

- ☐ Расчет ☒ Конструирование  
☐ Моделирование Другое \_\_\_\_\_

**Содержание работы**

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

**3. Выводы**

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

Руководитель \_\_\_\_\_

(Подпись, дата)

Студент \_\_\_\_\_

16.11.2023

(Подпись, дата)

«\_\_» \_\_\_\_\_ 20\_\_ г

## СОДЕРЖАНИЕ

Введение .....	6
1    Организационная структура предприятия.....	7
1.1    Информационные потоки .....	7
1.2    Структура информационных потоков на предприятии .....	7
2    Обоснование защиты информации .....	10
3    Анализ защищаемых помещений .....	11
3.1    Схема помещения .....	11
3.2    Описание помещений.....	14
3.3    Анализ возможных каналов утечки информации.....	15
4    Анализ рынка технических средств .....	16
4.1    Выбор средств защиты.....	16
4.2    Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам.....	17
4.3    Защита от утечки информации по (вибро-) акустическим каналам.....	18
4.4    Защита от ПЭМИН .....	21
4.5    Защита от утечек информации по оптическим каналам.....	22
5    Описание расстановки технических средств .....	23
Заключение.....	27
Список использованных источников .....	28

## 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 21 помещений и представляет собой офис предприятия с переговорной, кабинетом бухгалтерии, кабинетом директора, коворкингами, 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**

## **1.1    Информационные потоки**

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.

Информационные потоки могут быть классифицированы по различным критериям. Согласно цели данной работы информационные потоки будут разделены на две основные категории: открытые и закрытые.

Открытые информационные потоки представляют собой те, которые доступны сотрудникам и другим заинтересованным сторонам в пределах предприятия без специальных ограничений. Они включают в себя информацию, не содержащую чувствительных данных и не требующую дополнительных уровней доступа. Примеры открытых информационных потоков включают в себя общие отчеты, обновления проектов и новости компании. Открытые информационные потоки способствуют эффективному внутреннему обмену информацией и содействуют открытости и прозрачности внутри организации.

Закрытые информационные потоки содержат конфиденциальную, чувствительную информацию, которая требует высокого уровня защиты. Эти потоки могут включать в себя финансовые данные, персональные записи, интеллектуальную собственность и другие данные, которые, если попадут в неправильные руки, могут нанести ущерб предприятию.

Защита закрытых информационных потоков включает в себя установление строгих политик доступа, шифрование данных, мониторинг активности и другие меры безопасности.

## **1.2    Структура информационных потоков на предприятии**

Наименование организации: ООО “РосГосБез”. Область деятельности: разработки в области ИТ.

Организация-подрядчик. Выполняет заказы государственных организаций на разработку программного обеспечения для работы с государственной тайной.

Защищаемая информация:

1. коммерческая тайна - сведения о заключенных договорах и контрактах, данные о партнерах и клиентах компании, информация о ценовой политике и финансовых операциях;
2. техническая информация конфиденциального характера - состав и структура баз данных, содержащих информацию клиентов, конфигурации используемого серверного и сетевого оборудования, сведения об архитектуре и настройках корпоративных информационных систем;
3. государственная тайна - проекты для государственных учреждений или оборонных организаций, информация о разработке систем защиты от киберугроз, криптографии или технологий, обеспечивающих конфиденциальность данных.

Схема организации представлена на Рисунке 1.

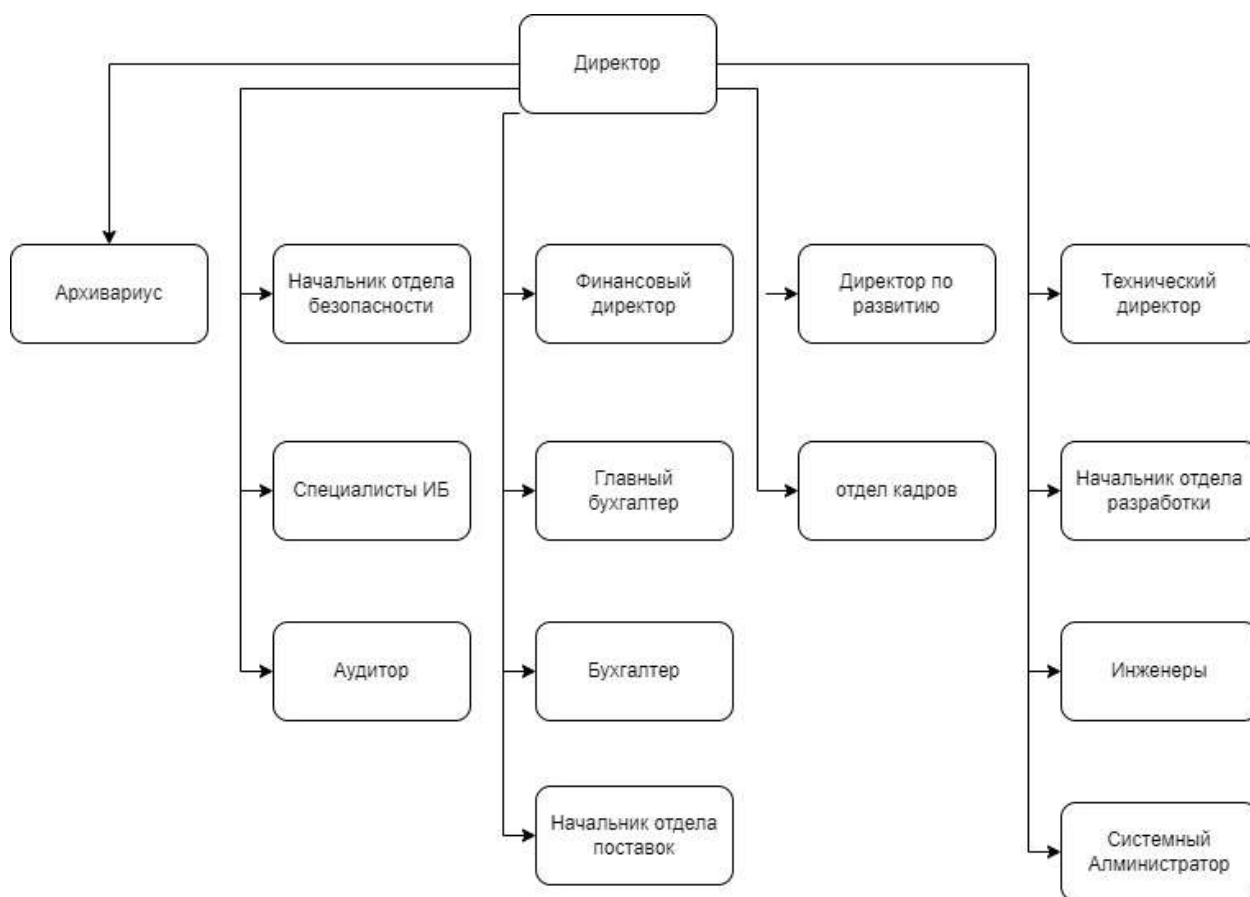


Рисунок 1 – Структура организации



The diagram illustrates the organizational structure and information flow of the Federal Scientific Center of Information Security (VNIIS). It is divided into an internal perimeter (Внутренний периметр) and external entities.

**Internal Perimeter (Внутренний периметр):**

- Генеральный директор (General Director):** The central authority, receiving reports (Отчетность) from the Fire Inspection (Пожарная инспекция), Suppliers (Поставщики), and the Department of Supplies (Отдел поставок). He provides information (Информация о ГТ) to the FSB (ФСБ) and information (Информация о поставках) to the Suppliers. He also provides information (Информация о покупках) to the Archive (Архив) and information (Информация о сотрудниках) to the HR Department (Отдел кадров).
- Отдел поставок (Department of Supplies):** Reports (Отчетность) to the General Director and the Ministry of Defense (Министерство Обороны). It provides information (Информация о сотрудниках + документы на допуск) to the HR Department and contracts (Договоры) to the Accounting Department (Бухгалтерия).
- Отдел кадров (HR Department):** Reports (Отчетность) to the General Director and the Ministry of Defense. It provides information (Информация о сотрудниках) to the General Director, the Department of Supplies, and the Accounting Department. It also manages personnel and wages (Кадры и ЗП).
- Бухгалтерия (Accounting):** Reports (Отчетность) to the General Director and the Ministry of Defense. It provides information (Информация о сотрудниках) to the General Director and the HR Department. It also handles deductions and taxes (Отчисления и налоги) to the Tax Authority (Налоговая).
- Архив (Archive):** Reports (Отчетность) to the General Director and the System Administrator (Системный администратор). It provides information (Информация о сотрудниках) to the General Director and instructions (Инструкции по архивации) to the Development Department (Отдел разработки).
- Системный администратор (System Administrator):** Reports (Отчетность) to the General Director and the Archive. He provides instructions (Инструкции) to the Development Department.
- Отдел разработки (Development Department):** Reports (Отчетность) to the General Director and the Information Security Department (Отдел Информационной безопасности). He provides instructions (Инструкции) to the Information Security Department.
- Отдел Информационной безопасности (Information Security Department):** Reports (Отчетность) to the General Director and the Development Department. He provides instructions (Инструкции) to the Development Department.

**External Entities:**

- Пожарная инспекция (Fire Inspection):** Reports (Отчетность) to the General Director.
- Поставщики (Suppliers):** Reports (Отчетность) to the General Director and provides information (Информация о поставках) to the General Director.
- ФСБ (FSB):** Receives information (Информация о ГТ) from the General Director.
- Заказчики (Clients):** Receives orders (Заказы) from the Department of Supplies.
- Министерство Обороны (Ministry of Defense):** Receives reports (Отчетность) from the Department of Supplies and the HR Department.
- Налоговая (Tax Authority):** Receives deductions and taxes (Отчисления и налоги) from the Accounting Department.

9

## **2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ**

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «совершенно секретно». Согласно требованиям «Типовых норм и правил проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденных Решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199, защита рассматриваемых помещений должна удовлетворять следующим критериям:

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 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

#### 3.1 Схема помещения

Необходимо провести анализ защищаемого помещения, чтобы разместить технические средства защиты на объекте. План помещения предприятия офисного типа представлен на рисунке 3. В таблице 3 представлены описание обозначений, изображенных на плане.

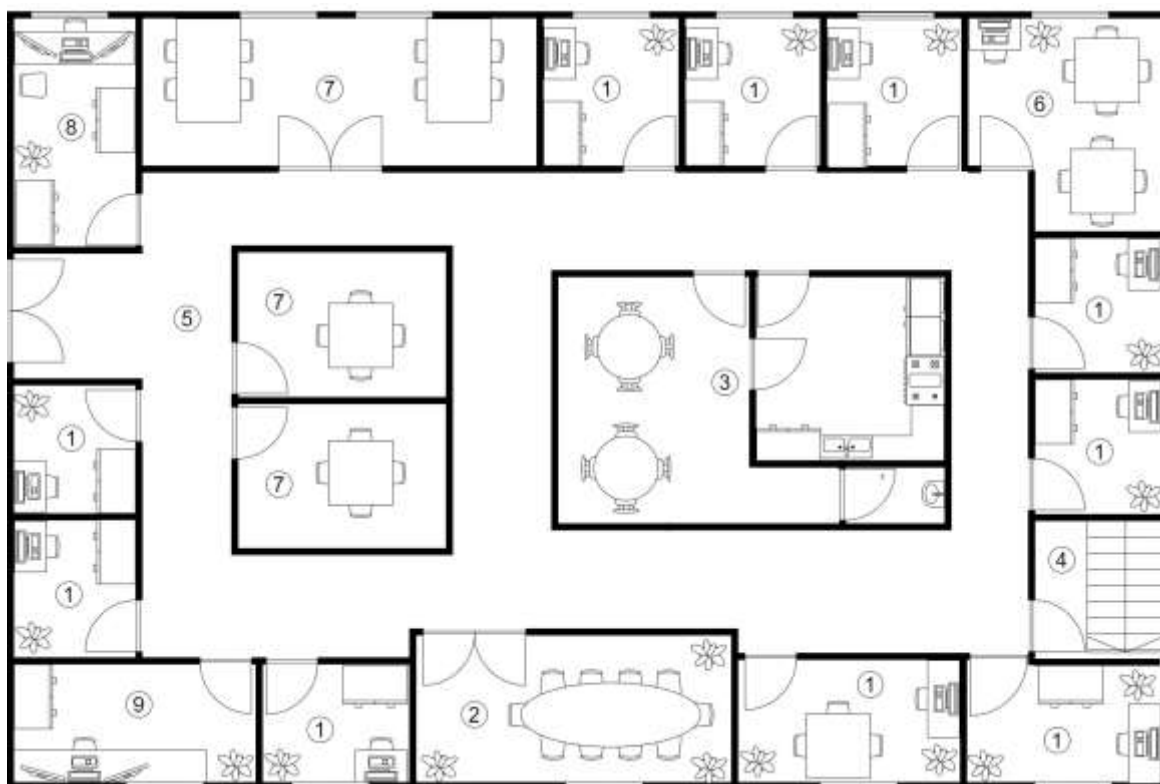


Рисунок 3 – План защищаемого помещения

Таблица 1 – Описание обозначений

Обозначение	Описание
	Кресло
	Офисный стул
	Стул руководителя
	Компьютерный стол
	Стол переговоров
	Журнальный стол
	Кухонный стол
	Компьютер
	Интерактивная доска с проектором
	Мусорное ведро для бумаги

Продолжение таблицы 1

Обозначение	Описание
	Книжный шкаф
	Шкаф для документов
	Радиатор отопления
	Кулер для воды
	Туалет
	Раковина
	СВЧ-печь
	Кофемашина
	Чайник
	Комнатное растение

### 3.2 Описание помещений

На рассматриваемом предприятии в рамках курсовой работы имеются следующие помещения, подлежащие инженерно-технической защите:

- 1) офисное помещение (15,9 м<sup>2</sup>);
- 2) переговорная комната (30,2 м<sup>2</sup>)(защищаемое помещение);
- 3) кухня (25,0 м<sup>2</sup>);
- 4) серверная комната (14,4 м<sup>2</sup>)(защищаемое помещение);
- 5) главный холл (47,4 м<sup>2</sup>);
- 6) бухгалтерия (30,2 м<sup>2</sup>);
- 7) Открытое рабочее пространство (30,2 м<sup>2</sup>);
- 8) Кабинет генерального директора (24,4 м<sup>2</sup>)(защищаемое помещение);
- 9) Кабинет начальника безопасности (24,4 м<sup>2</sup>)(защищаемое помещение);

Кабинет генерального директора включает в себя: один стул руководителя, один офисный стул, один компьютерный стол, один книжный шкаф, одно окно, один шкаф для документов, и одно комнатное растение, компьютер, три монитора. Данное помещение оснащено шестью розетками.

В переговорной комнате находятся девять стульев, один стол для переговоров, одно окно и три комнатных растения. Переговорная комната оснащена восьмью розетками.

Офисные помещения предназначены для сотрудников предприятия.

В каждом офисном помещении стоят: стул, компьютерный стол, один компьютер, один шкаф для документов одно окно и одно комнатное растение. В данных помещениях находятся по пять розеток.

В серверной комнате расположены 16 серверов. В данном помещении есть 16 розеток.

Кабинет начальника безопасности включает в себя один компьютерный стол, один компьютер, три монитора, одно окно, одно комнатное растение и один стул.

В бухгалтерии один компьютерный стол, два письменных стола, 9 офисных стульев, одно окно и одно комнатное растение.

В кухне есть два кухонных стола, две раковины одна плита, полки для посуды и два холодильника. Данное помещение включает в себя пять розеток.

Комнаты для коворкинга включают в себя столы и стулья.

Окна помещения выходят в закрытый двор и на улицу. Двор находится под постоянным наблюдением и не имеет смежности с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и другими элементами, которые могли бы использоваться посторонними лицами для доступа в помещение.

Помещения сгруппированы в «непроходной» (тупиковой) части здания, которая редко используется сотрудниками при выполнении служебных обязанностей, не связанных с доступом к государственной тайне. Стены и внутренние перегородки здания выполнены из железобетона и имеют толщину не менее 13 см.

### **3.3 Анализ возможных каналов утечки информации**

В каждом помещении существуют потенциальные пути для нежелательной утечки информации, связанные с электромагнитными и электрическими утечками информации, то есть с использованием компьютеров и розеток. Декоративные элементы, такие как комнатные растения, могут использоваться для установки закладных устройств, которые могут использоваться для передачи информации через акустический канал.

Существуют также риски утечки информации через оптические каналы, например, из-за незакрытых окон и незащищенных дверей. Важно учитывать также виброакустический канал, который может быть использован для передачи информации из-за наличия твердых поверхностей, таких как стены или батареи отопления.

Вещественно-материальный канал утечки информации возможен ввиду наличия вещественных носителей информации, однако он не перекрывается техническими средствами защиты.

Акустический, вибро-акустический и электроакустический. Акустический канал утечки информации формируется из трех элементов:

- источника — голоса при разговоре в помещении с коллегами или по телефону;
- среды распространения — воздуха для акустического сигнала, металлических конструкций и стекол для виброакустического;
- приемника — электронного закладного устройства, совмещающего функции снятия информации и передачи ее по радиосигналу.

Электрический (электромагнитный) - Он разделяет способы перехвата данных на:

- перехват побочных электромагнитных излучений;
- перехват побочных электромагнитных излучений на частотах работы высокочастотных генераторов;
- перехват побочных электромагнитных излучений на частотах самовозбуждения усилителей низкой частоты.

## **4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ**

### **4.1 Выбор средств защиты**

Для обеспечения высокого уровня комплексной безопасности информации, которая отнесена к категории «совершенно секретно» в зависимости от её типа, требуется оснащение помещения специальными средствами и устройствами, перечисленными в таблице 2. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки такой конфиденциальной информации.

Таблица 2 – Активная и пассивная защита информации

<b>Каналы</b>	<b>Источники</b>	<b>Пассивная защита</b>	<b>Активная защита</b>
Визуально-оптический	Окна, стеклянные, отражающие поверхности, двери	Защитные экраны, жалюзи	Бликующие устройства
Акустический Электроакустический	Стены, двери, окна, электрические сигналы	Защитные экраны и фильтры для сетей электропитания, изоляция особо важных помещений, шумоподавление	Устройства акустического зашумления,
Вибро-акустический	Стекла, стены и иные твердые поверхности	Изоляция переговорной, использование антивибрационных материалов и звукозащитных экранов	Устройства вибрационного зашумления
Электрический Электромагнитный	Компьютеры, сервера, бытовая техника, розетки	Защитные экраны и фильтры для сетей электропитания	Устройства электромагнитного зашумления



## 4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам

Пассивная защита включает себя размещение фильтров в электропитании всех помещений.

Активная защита заключается в использовании системы белого шума в сети, которая создает фоновый шум, маскирующий колебания, вызванные звуковыми волнами или работой электронных устройств. Модели устройств, относительно которых будет идти дальнейший анализ, и их характеристики представлены в таблице 3.

Таблица 3 – Активная защита от утечек информации по электрическим каналам

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	Диапазон частот 10 кГц – 400 МГц. Диапазон регулировки уровня выходного шумового сигнала не менее 20 дБ. Мощность, потребляемая от сети не более 45 ВА.	Сетевой генератор шума. Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.
Соната- РС1	16 520	Диапазон частот до 1 ГГц, регулировка уровня шума в 1 частотной полосе. Напряжение 220 В.	Возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus)
Генератор шума Покров	32 800		

Продолжение таблицы 3

Модель	Цена, руб.	Характеристики	Особенности
		<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 позволяют установить достаточное количество подобных устройств в помещениях. Кроме того, этот выбор был обоснован самым широким диапазоном частот.

#### 4.3 Защита от утечки информации по (вибро-) акустическим каналам

Пассивные меры безопасности включают в себя создание тамбурной зоны перед переговорной комнатой и установку усиленных дверей. Для обеспечения звукоизоляции переговорной комнаты и кабинета руководителя используются специальные материалы для звукоизоляции стен.

Активные меры безопасности представляют собой систему виброакустической маскировки. Для обеспечения безопасности помещения, в котором обрабатывается информация, отнесенная к категории «совершенно секретно», рассматриваются технические средства активной защиты информации для объектов информатизации, имеющих категорию не ниже 1Б (Таблица 4).

Таблица 4 – Активная защита от утечек информации по (вибро-)акустическим 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.	Вариативность количества подключаемых к генераторному блоку преобразователей. К двухканальному виброакустическому генератору шума ЛГШ-404 можно одновременно подключить до 20 ЛВП-10 и до 20 ЛВП-2А. Счетчик времени наработки и световая индикация режима работы. Проводной пульт дистанционного управления в комплекте
Шорох 5Л	21 500	Максимальное количество излучателей – 40. Электропитание 220 (+10% - 15%) В (есть возможность работы системы от источника питания 12В). Количество октавных полос для регулировки уровня мощности шума – 7.	Сетевой генератор шума. Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.
SEL SP-157 Шагрень	47 400	Диапазон воспроизводимого шумового сигнала 90–11200 Гц. Максимальное количество излучателей – 64. Электропитание 220В/50Гц.	Защита паролем настроек системы. Отсчёт времени наработки генерации шума по каждому каналу с выводом на экран. Непрерывный контроль состояния системы и каждого отдельного излучателя.

Продолжение таблицы 4

Соната АВ-4Б	44 200	<p>Диапазон воспроизводимого шумового сигнала 175–11200 Гц.</p> <p>Выходное напряжение В 12,5 ± 0,5.</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>
-----------------	--------	---	--

Исходя из анализа, представленного в таблице 4, было принято решение о выборе системы «СОНАТА АВ-4Б». По сравнению с альтернативными системами, предназначенными для защиты от утечек информации через акустические и вибрационные каналы, данная система считается наиболее востребованной и получила множество положительных отзывов. 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.

#### 4.4 Защита от ПЭМИН

Таблица 5 – Активная защита от ПЭМИН

Модель	Цена, руб.	Характеристики	Особенности
ЛГШ 503	44 200	<p>Диапазон частот 10 кГц - 1800 МГц.</p> <p>Уровень шума от -26 дБ (мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц).</p> <p>Мощность – 45 Вт.</p>	<p>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 программно-аппаратный комплекс «Паутина».</p>
Соната-РЗ.1	39 000	<p>Электропитание – 220 В +10%/-15%, 50 Гц.</p> <p>Мощность – 10 Вт.</p> <p>Продолжительность непрерывной работы не менее 8 ч</p>	<p>Обеспечивает защиту информации от утечки за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума, а также наводок на линии сети электропитания и заземления путем индуцирования в них маскирующих шумовых напряжений.</p>

Продолжение таблицы 5

Модель	Цена, руб.	Характеристики	Особенности
ЛГШ-513	33 120	<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>Мощность – не более 45 ВА.</p> <p>Режим работы – круглосуточно.</p>	<p>Изделие «ЛГШ-513» оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Изделие «ЛГШ-513» оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех.</p>
Генератор шума Пульсар	24 525	<p>Диапазон частот 10 кГц - 6 ГГц.</p> <p>Электропитание – однофазная сеть переменного тока 187–242 В.</p> <p>Мощность – 50 ВА.</p>	<p>Имеет защиту регулятора уровня выходного шумового сигнала от нелегального доступа (и сигнализирует об этом). Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук).</p>

В качестве средства активной защиты от ПЭМИН был выбран генератор шума «ЛГШ-503». Этот выбор обоснован широким диапазоном частот (от 10 кГц до 1800 МГц) и круглосуточным режимом работы. Кроме того, данный прибор поддерживает возможность подключения проводного дистанционного управления и контроля, для чего может быть использован программно-аппаратный комплекс «Паутина».

#### 4.5 Защита от утечек информации по оптическим каналам

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

## 5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В предыдущей главе был проанализирован рынок инженерно-технических средств и были выбраны лучшие средства защиты информации из них, которые включает в себя:

- сетевой генератор шума «Покров»;
- система виброакустической защиты «Соната АВ-4Б»;
- генератор шума «ЛГШ-503» от ПЭМИН
- жалюзи на семь окон;
- три усиленные двери с толщиной 4 мм, обшитые металлическим листом не

менее 2 мм, внутри – звукоизоляционный материал.

Для каждого помещения оптимальное количество акустоизлучателей и вибровозбудителей зависит от различных факторов, таких как звукоизоляция, форма, материалы стен, местоположение, уровень фонового шума и другие подобные аспекты.

Согласно информации на официальном веб-сайте производителя НПО «АННА» для выбранной системы виброакустической защиты, предварительную оценку необходимого количества вибровозбудителей «Соната СВ-4Б» можно провести, руководствуясь следующими стандартами:

- стены – один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- потолок, пол – один на каждые 15...25 м<sup>2</sup> перекрытия;
- окна – один на окно (при установке на оконный переплет);
- двери – один на дверь (при установке на верхнюю перекладину дверной коробки);

В таблице 6 содержится список мер защиты, предназначенных для применения во всех помещениях, а также конечная стоимость.

Таблица 6 – Необходимое оборудование

Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Сетевой генератор шума «Покров»	32 800	1	32 800
Генератор шума «ЛГШ-503»	44 200	1	44 200
Блок электропитания и управления «Соната-ИП4.3»	21 600	1	21 600

Продолжение таблицы 6

<b>Меры защиты</b>	<b>Цена, руб.</b>	<b>Количество, шт.</b>	<b>Итоговая стоимость</b>
Генератор-акустоизлучатель «Соната СА-4Б1»	3 540	34	120 360
Генератор-вибровозбудитель «Соната СА-4Б»	7 440	118	877 920
Рызмыкатель телефонной линии «Соната ВК4.1»	6 000	2	12 000
Рызмыкатель слаботочной линии «Соната ВК4.2»	6 000	1	6 000
Рызмыкатель линии «Ethernet» «Соната ВК4.1»	6 000	2	12 000
Пульт управления «Соната-ДУ 4.3»	7 680	1	7 680
Шторы-плиссе Blackout	4 900	12	58 800
Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	83 619	3	250 857
Итого			1 444 217

В трех помещениях установлены усиленные звукоизолирующие двери, как показано на рисунке 4. На каждом окне установлены шторы. Системы «Соната СА-4Б1» и «Соната СВ-4Б» размещены в соответствии с указаниями производителя. «ЛГШ-221» и «ЛГШ-503» находятся рядом с «Соната-ИП4.3» и подключены к ней. Все выключатели установлены в соответствии с рекомендациями производителя. В таблице 7 приведены описание обозначений устройств.



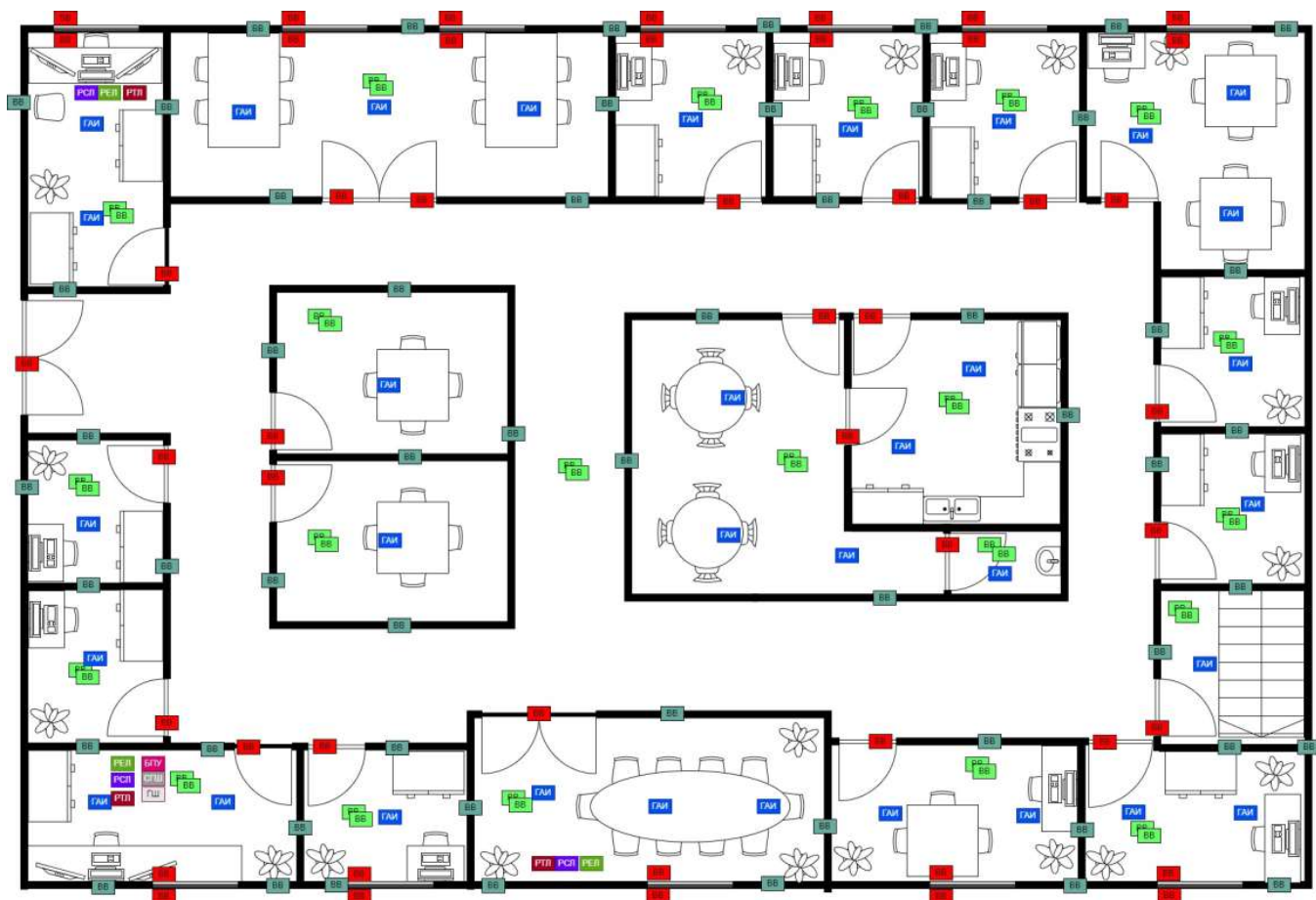


Рисунок 4 – Схема расстановки устройств

Таблица 7 – Описание обозначений устройств

Обозначение	Устройство	Количество, шт.
	Блок электропитания и управления «Соната-ИП4.3»	1
	Генератор-акустоизлучатель «Соната СА-4Б1»	17
	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)	23
	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)	16
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)	23

Продолжение таблицы 7

Обозначение	Устройство	Количество, шт.
	Размыкатель линии «Ethernet» «Соната-ВК4.3»	1
	Размыкатель слаботочной линии «Соната-ВК4.2»	1
	Размыкатель телефонной линии «Соната-ВК4.1»	2
	Сетевой генератор шума «Покров»	1
	Генератор шума «ЛГШ-503»	1
	Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	3
	Шторы-плиссе BlackOut	7

## **ЗАКЛЮЧЕНИЕ**

В процессе написания данной курсовой работы был проведен анализ как открытых, так и закрытых информационных потоков на предприятии. Также было проведено обоснование защиты информации, составляющей государственную тайну уровня «совершенно секретно» на предприятии. Далее, был проведен анализ уровня защищенности помещений, в результате чего были выявлены актуальные каналы утечки информации. На основе этого анализа были выбраны соответствующие средства защиты информации, которые были выбраны с учетом данных рынка. Затем был разработан план размещения технических средств защиты информации, и были произведены расчеты стоимости его внедрения.

Как результат данной работы был создан план по защите помещения от потенциальных каналов утечки информации, включая ПЭМИН и электрические, акустоэлектрические, электромагнитные, акустические, виброакустические и оптические пути передачи информации.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.
2. Хорев А. А. Техническая защита информации: учебное пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010. — 436 с.
3. Detector Systems: Системы комплексной безопасности [Электронный ресурс]. – Режим доступа: <https://detsys.ru/> (дата обращения: 01.11.2023).

