

**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:

студент группы N34461
Шмыга Максим Сергеевич


(подпись)

Проверил:

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

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Шмыга М.С. (Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34461
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

- 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.
- Список литературы.

Рекомендуемая литература

Руководитель	 (Подпись, дата)
Студент	 20.12.2023 (Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Шмыга М.С.

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34461

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	20.12.2023	20.12.2023	

Руководитель

(Подпись, дата)

Студент

20.12.2023

(Подпись, дата)

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

Студент Шмыга М.С.

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34461

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.

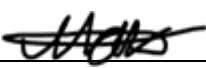
3. Выводы

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 _____


20.12.2023
(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	9
3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	10
3.1 Схема помещения	10
3.2 Описание помещений	11
3.3 Анализ возможных каналов утечки информации.....	12
4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ	14
4.1 Выбор средств защиты	14
4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам	14
4.3 Защита от утечки информации по (вибро-) акустическим каналам	16
4.4 Защита от ПЭМИН	18
4.5 Защита от утечек информации по оптическим каналам	19
5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ	19
ЗАКЛЮЧЕНИЕ.....	24
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	25

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.

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 “ИнфоТехника”. Область деятельности: разработка программного обеспечения.

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 информационных потоков организации представлена на Рисунке 1. Стрелочки, выделенные красным цветом, являются закрытыми потоками, зеленые – открытыми.

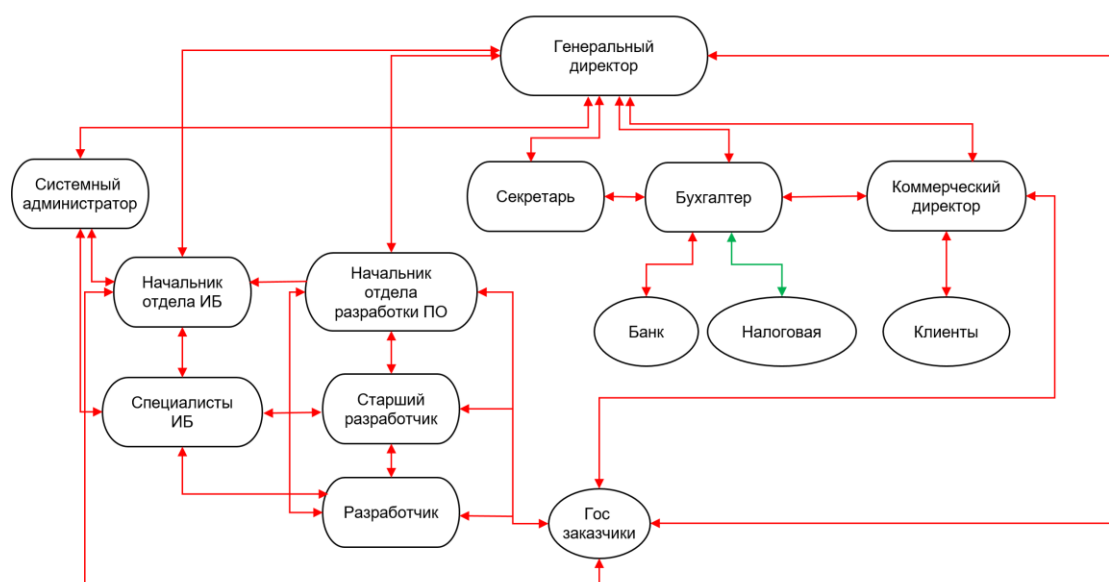


Рисунок 1 – Схема информационных потоков на предприятии

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. На рисунке 4 представлены изображения, описанные в плане.

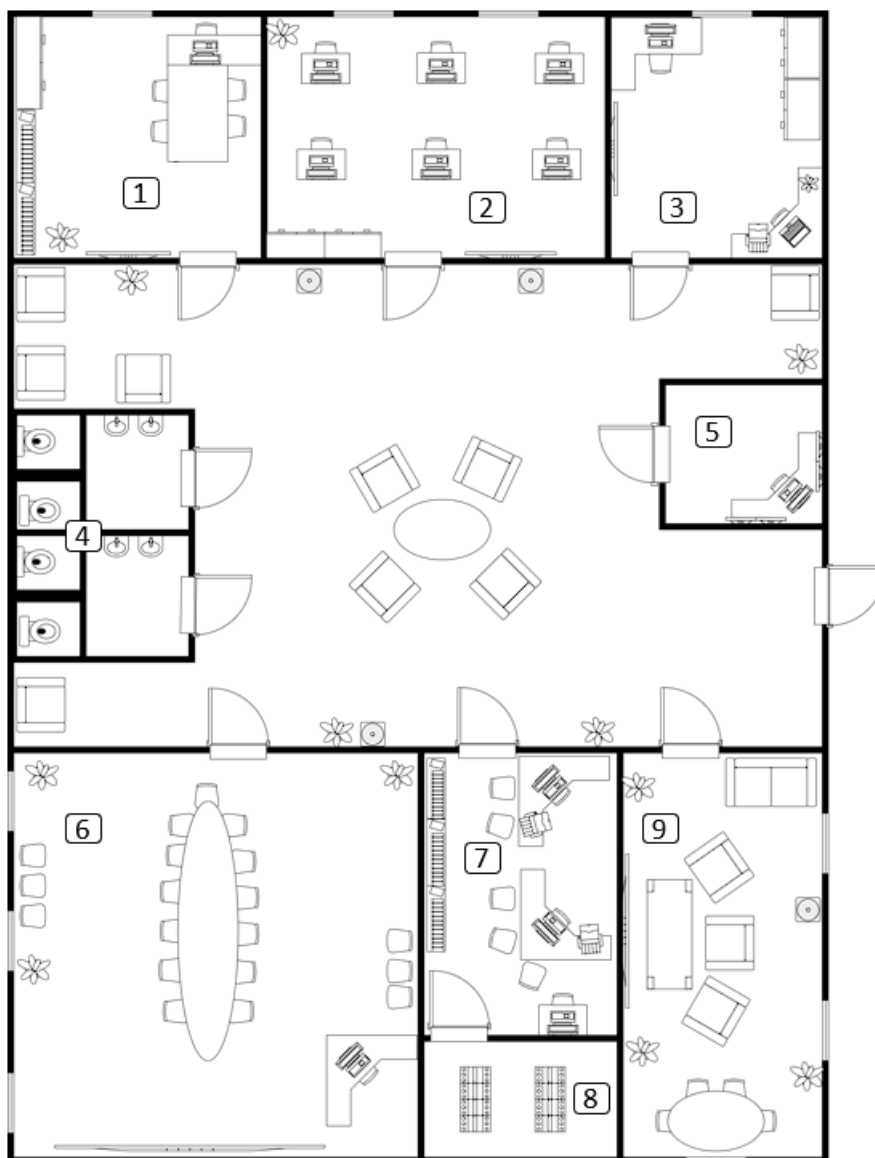


Рисунок 2 – План защищаемого помещения

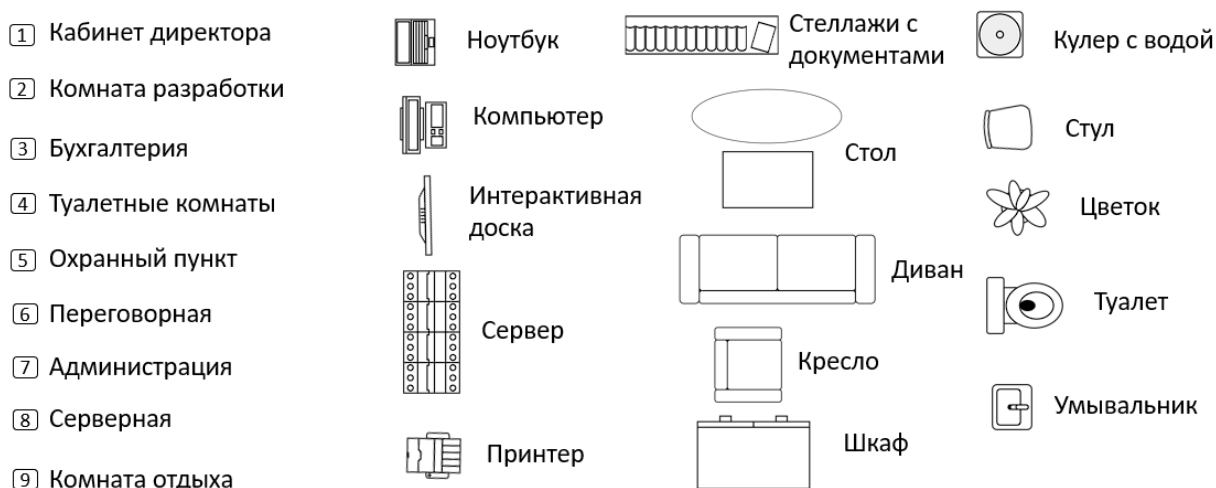


Рисунок 3 – Описание обозначений

3.2 Описание помещений

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

- кабинет директора (26 м²);
- комната разработки (36 м²);
- бухгалтерия (24, м²);
- охранный пункт (12 м²);
- туалетные комнаты (22 м²);
- переговорная (68 м²);
- администрация (25 м²);
- серверная (15 м²);
- комната отдыха (40 м²);

В кабинете директора находится 5 стульев, 2 стола, стеллажи с документами, цветок, интерактивная доска, компьютер, шкаф. В кабинете есть окно.

В комнате разработки находятся 6 столов, 6 стульев, 6 компьютеров, 2 шкафа, интерактивная доска, цветок. В комнате есть 2 окна.

В бухгалтерии находятся компьютер, ноутбук, цветок, принтер, интерактивная доска, 2 шкафа, 2 стула, 2 стола. В комнате есть окно.

Охранный пункт включает в себя стол, стул, компьютер, 4 монитора. В комнате окон нет.

В переговорной находятся 20 стульев, 2 стола, компьютер, интерактивная доска, 3 цветка. В комнате есть 3 окна.

В администрации находятся стеллажи, 3 стола, 3 компьютера, 8 стульев, принтер. В данной комнате окон нет.

В серверной комнате расположены 2 сервера. В данном помещении окон нет.

В комнате отдыха находятся 3 кресла, 2 стола, диван, кулер с водой, 3 цветка, 4 стула, интерактивный экран. В комнате есть 3 окна.

В открытом пространстве находятся стол, 3 кулера, 4 цветка, 9 кресел.

Помещение находится на 7 этаже бизнес-центра. Стоит отметить наличием окон почти в каждой комнате. Окна не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Помещения сгруппированы в «непроходной» (тупиковой) части здания, которая редко используется сотрудниками при выполнении служебных обязанностей, не связанных с доступом к государственной тайне.

Стены здания и внутренние перегородки железобетонные, толщиной не менее 10см.

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 1 – Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
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 2 – 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	Диапазон частот 10 кГц – 6000 МГц. Мощность 15 Вт. Наработка на отказ 5000 часов.	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.
--	--	--	--

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 3 – 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.
Соната АВ-4Б	44 200	Диапазон воспроизводимого шумового сигнала 175–11200 Гц. Выходное напряжение В 12,5 ± 0,5. Электропитание сеть ~220 В/50 Гц.	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.

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 4 – 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-Р3.1	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</p>

			линии сети электропитания и заземления путем индуцирования в них маскирующих шумовых напряжений.
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>	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.
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>	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).

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 м² 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 5 – 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
Генератор-акустоизлучатель «Соната СА-4Б1»	3 540	39	134 550

Генератор-вибровозбудитель «Соната СА-4Б»	7 440	83	617 520
Рызмыкатель телефонной линии «Соната ВК4.1»	6 000	3	18 000
Рызмыкатель слаботочной линии «Соната ВК4.2»	6 000	1	6 000
Рызмыкатель линии «Ethernet» «Соната ВК4.1»	6 000	7	42 000
Пульт управления «Соната-ДУ 4.3»	7 680	1	7 680
Шторы-плиссе Blackout	4 900	10	49 000
Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	83 619	3	250 857
Итого			1 224 207

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.

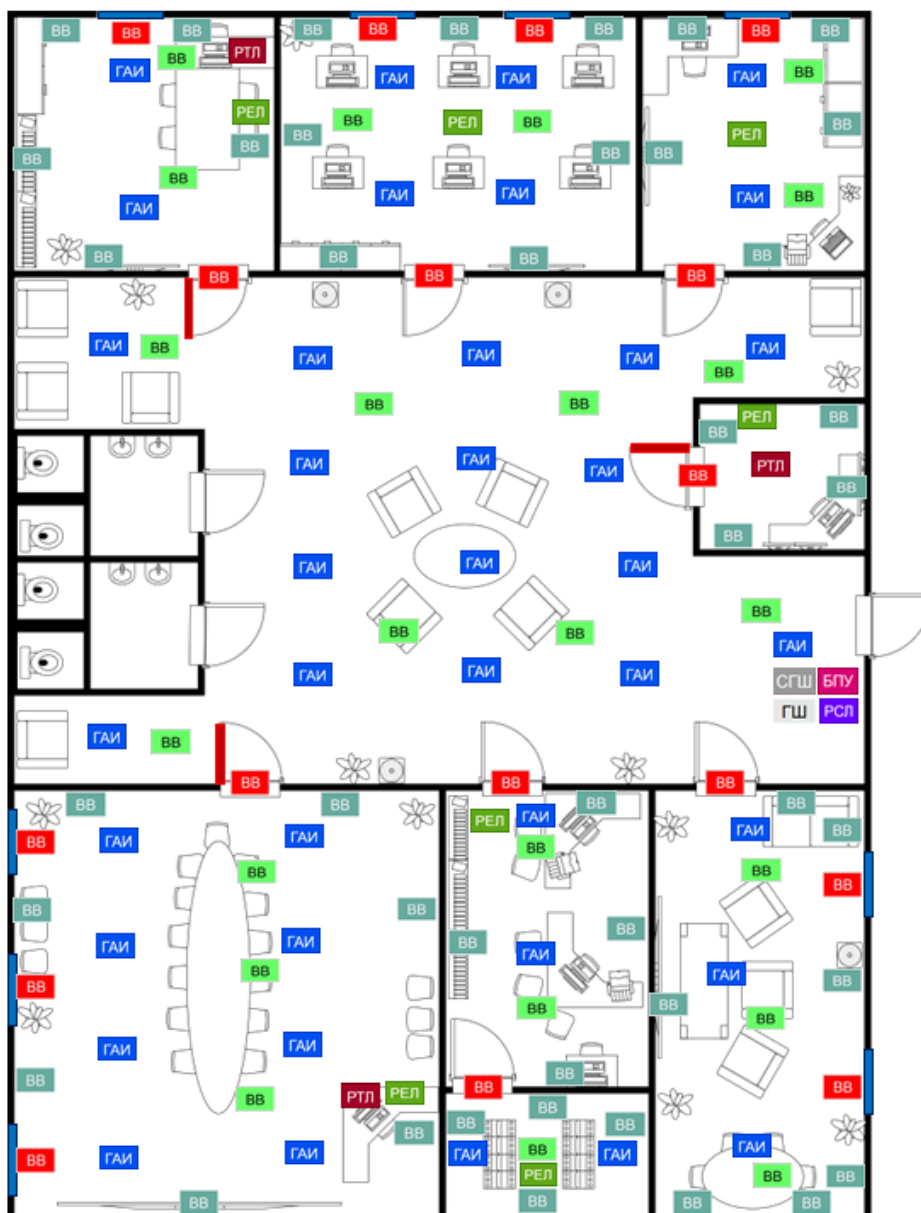





Рисунок 4 – Схема расстановки устройств

Таблица 6 – Описание обозначений устройств

Обозначение	Устройство	Количество, шт.
	Блок электропитания и управления «Соната-ИП4.3»	1
	Генератор-акустоизлучатель «Соната СА-4Б1»	39
	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)	43

	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)	23
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)	17
	Размыкатель линии «Ethernet» «Соната-ВК4.3»	7
	Размыкатель слаботочной линии «Соната-ВК4.2»	1
	Размыкатель телефонной линии «Соната-ВК4.1»	3
	Сетевой генератор шума «Покров»	1
	Генератор шума «ЛГШ-503»	1
	Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	3
	Шторы-плиссе BlackOut	10

ЗАКЛЮЧЕНИЕ

В процессе написания данного курсового проекта был проведен анализ информационных потоков на предприятии, включая как открытые, так и закрытые источники. Также было осуществлено обоснование необходимости защиты информации, отнесенной к государственной тайне уровня "совершенно секретно". Далее был проведен анализ степени безопасности помещений, выявлены актуальные потенциальные каналы утечки данных. На основе этого анализа были выбраны средства защиты информации, учитывая текущее положение на рынке. Затем был разработан план размещения технических средств защиты информации, включая расчеты стоимости их внедрения.

В результате выполненной работы был создан план по обеспечению защиты помещения от потенциальных каналов утечки информации, охватывающий ПЭМИН и различные электрические, акустоэлектрические, электромагнитные, акустические, виброакустические и оптические пути передачи данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности: учебное пособие / Н. С. Кармановский, О. В. Михайличенко, С. В. Савков. — Санкт-Петербург: НИУ ИТМО, 2013. — 148 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. Каторин Ю. Ф. Защита информации техническими средствами : Учебное пособие / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак. — Санкт-Петербург : НИУ ИТМО, 2012. — 416 с. — Текст : непосредственный.