

**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:

 Рашидов М.-И.М.-Б.,
студент группы N34501

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 | Рашидов Мир Исмаил Мир Бахтиярович (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

- 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 | | 07.11.2023 |
| | | (Подпись, дата) |

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Рашидов Мир Исмаил Мир Бахтиярович

(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 | 25.10.2023 | 25.10.2023 | |
| 3 | Разработка комплекса инженерно-технической защиты информации в заданном помещении | 26.10.2023 | 27.11.2023 | |
| 4 | Представление выполненной курсовой работы | 07.11.2023 | 07.11.2023 | |

Руководитель



(Подпись, дата)

Студент

07.11.2023

(Подпись, дата)

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

Студент Рашидов Мир Исмаил Мир Бахтиярович
(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 _____
Студент _____
(Подпись, дата) 07.11.2023
(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..... | 8 |
| 3 Анализ защищаемых помещений | 9 |
| 3.1 Схема помещения | 9 |
| 3.2 Описание помещений | 12 |
| 3.3 Анализ возможных каналов утечки информации..... | 13 |
| 4 Анализ рынка технических средств | 13 |
| 4.1 Выбор средств защиты | 13 |
| 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 | 20 |
| 5 Описание расстановки технических средств..... | 20 |
| 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. 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

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

На рисунке 1.1 зеленым цветом обозначены открытые потоки, а красным цветом - закрытые потоки.

К информации, передающейся по открытым потокам, относятся бухгалтерская и финансовая отчетность, налоговые сведения.

К защищаемой информации, передающейся по закрытым потокам, относятся

персональные данные клиентов и сотрудников, служебная тайна, коммерческая тайна и сведения о разрабатываемом программном продукте (программный код, назначение и т. д.).

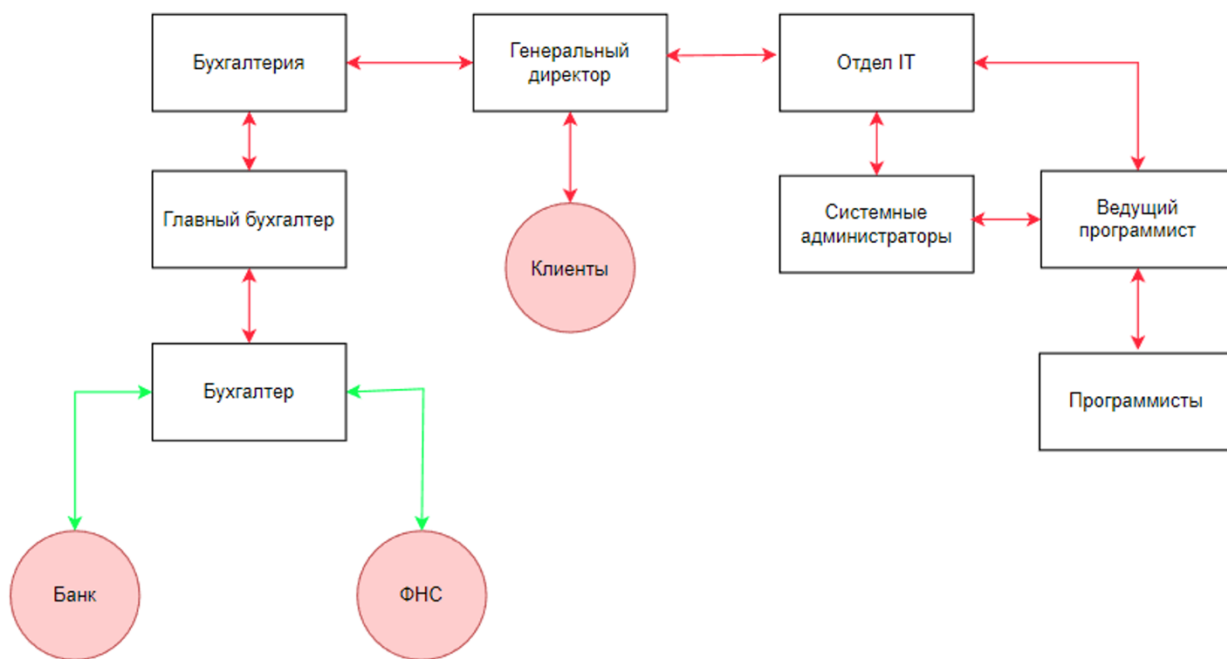


Рисунок 1.1 – Схема информационных потоков на предприятии

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 3.1. В таблице 3.1 представлены описание обозначений, изображенных на плане.

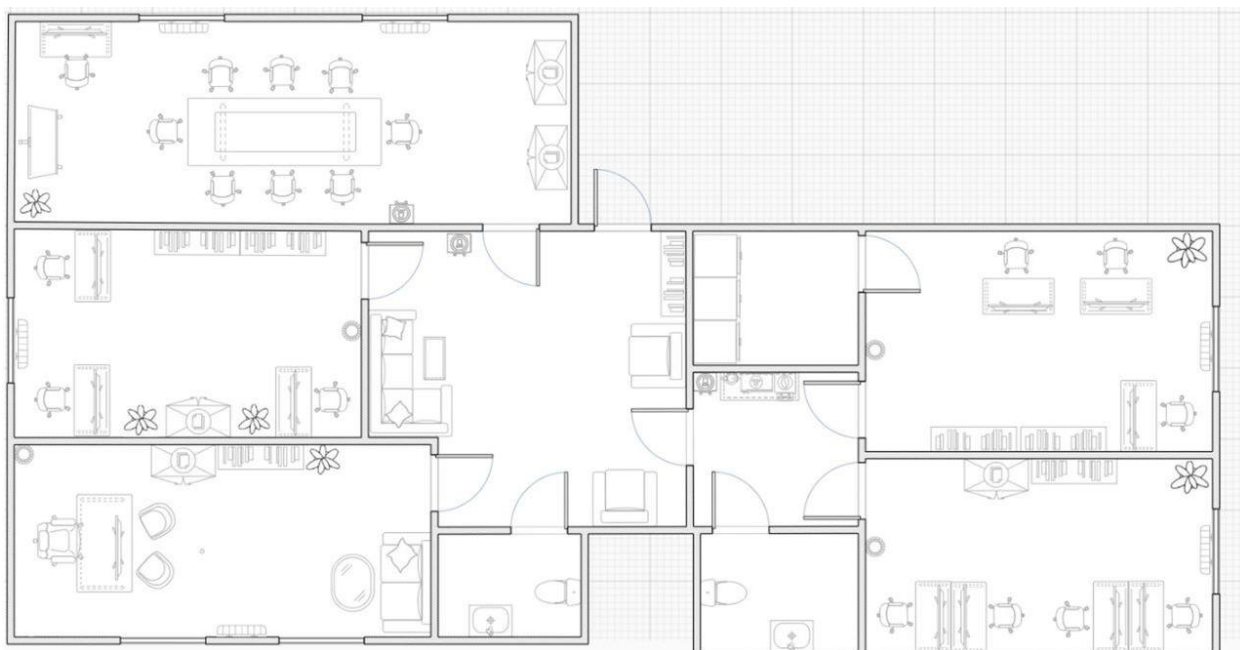


Рисунок 3.1 – План защищаемого помещения

Таблица 3.1 – 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 3.1

| 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:

- кабинет директора (15,9 м²);
- переговорная комната (22,2 м²);
- офис 1 (15,2 м²);
- офис 2 (13,3 м²);
- офис 3 (14,3 м²);
- серверная комната (4,4 м²);
- кухня (5,0 м²);
- главный холл (17,4 м²).

Кабинет директора включает в себя: один стул руководителя, два стула, два офисных кресла (совмещенных), один компьютерный стол, один журнальный стол, один книжный шкаф, один шкаф для документов, один сейф, одно мусорное ведро для бумаги, один радиатор отопления, два окна и одно комнатное растение. Данное помещение оснащено шестью розетками.

В переговорной комнате находятся девять стульев, один стол для переговоров, один компьютерный стол, один компьютер, два шкафа для документов, одна интерактивная доска с проектором, один кулер для воды, два радиатора отопления, два окна и одно комнатное растение. Переговорная комната оснащена восьмью розетками.

Офис 1, офис 2 и офис 3 предназначены для сотрудников предприятия.

В офисе 1 стоят три стула, три компьютерных стола, три компьютера, два книжных шкафа, один шкаф для документов, одно мусорное ведро для бумаги, один радиатор отопления, одно окно и два комнатных растения. В данном помещении находятся шесть розеток.

В офисе 2 есть четыре стула, четыре компьютерных стола, четыре компьютера, один книжный шкаф, один шкаф для документов, одно мусорное ведро для бумаги, один радиатор отопления, одно окно и одно комнатное растение. Данное помещение оснащено восьмью розетками.

В офисе 3 находятся три компьютерных стола, три компьютера, два книжных шкафа, одно мусорное ведро для бумаги, один радиатор отопления, одно окно и одно комнатное растение. Офис 3 оснащен шестью розетками.

В серверной комнате расположены три сервера. В данном помещении есть девять розеток.

В кухне есть кулер для воды и кухонный стол, на котором находятся одна

кофемашина, одна микроволновая печь и один чайник. Данное помещение включает в себя пять розеток.

Главный холл предназначен для сотрудников предприятия и посетителей. В нем находятся четыре кресла (совмещенных), два кресла, один журнальный стол, книжный шкаф и кулер для воды.

Окна помещения выходят в закрытый двор, который 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.

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 4.1. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки такой конфиденциальной информации.

Таблица 4.1 – Активная и пассивная защита информации

| Каналы | Источники | Пассивная защита | Активная защита |
|-------------------------------------|---|--|---|
| Электрический Электромагнитный | Компьютеры, сервера, бытовая техника, розетки | Защитные экраны и фильтры для сетей электропитания | Устройства электромагнитного зашумления |
| Акустический Электроакустический | Стены, двери, окна, электрические сигналы | Защитные экраны и фильтры для сетей электропитания, изоляция особо важных помещений | Устройства акустического зашумления |
| Виброакустический | Стекла, стены и иные твердые поверхности | Изоляция переговорной, использование антивибрационных материалов и звукозащитных экранов | Устройства вибрационного зашумления |
| Визуально- оптический | Окна и стеклянные поверхности, двери | Защитные экраны и фильтры для сетей электропитания | Жалюзи, бликующие устройства |

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 4.2.

Таблица 4.2 – 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 4.1, 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 4.3 – 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 |

Продолжение таблицы 4.3

| Модель | Цена, руб. | Характеристики | Особенности |
|-----------------------|---------------|---|---|
| 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 Шагренъ | 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 4.2, 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 4.4 – 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> |

Продолжение таблицы 4.4

| Модель | Цена, руб. | Характеристики | Особенности |
|------------------------------|---------------|--|---|
| Соната-РЗ.1 | 39 000 | Электропитание – 220 В +10%/-15%, 50 Гц. Мощность – 10 Вт. Продолжительность непрерывной работы не менее 8 ч | 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. |
| ЛГШ-513 | 33 120 | Диапазон частот 10 кГц - 1800 МГц. Уровень шума от -18 дБ(мкА/м* $\sqrt{\text{кГц}}$) до 50 дБ(мкВ/м* $\sqrt{\text{кГц}}$). Мощность – не более 45 ВА. Режим работы – круглосуточно. | 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 | Диапазон частот 10 кГц - 6 Гц. Электропитание – однофазная сеть переменного тока 187–242 В. Мощность – 50 ВА. | 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);

– трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Предварительная оценка необходимого количества акустоизлучателей «Соната СВ-4Б» может быть выполнена из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8...12 м³ надпотолочного пространства или других пустот.

В таблице 5.1 содержится список мер защиты, предназначенных для применения во всех помещениях, а также конечная стоимость.

Таблица 5.1 – 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 | 17 | 60 180 |
| Генератор-вибровозбудитель «Соната СА-4Б» | 7 440 | 66 | 491 040 |
| 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 | 1 | 6 000 |
| Пульт управления «Соната-ДУ 4.3» | 7 680 | 1 | 7 680 |
| Шторы-плиссе Blackout | 4 900 | 7 | 34 300 |
| Усиленные звукоизолирующие двери «Ultimatum Next ПВХ» | 83 619 | 3 | 250 857 |
| Итого | | | 966 657 |

В трех помещениях установлены усиленные звукоизолирующие двери, как показано на рисунке 5.1. 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 5.1 приведены описание обозначений устройств.

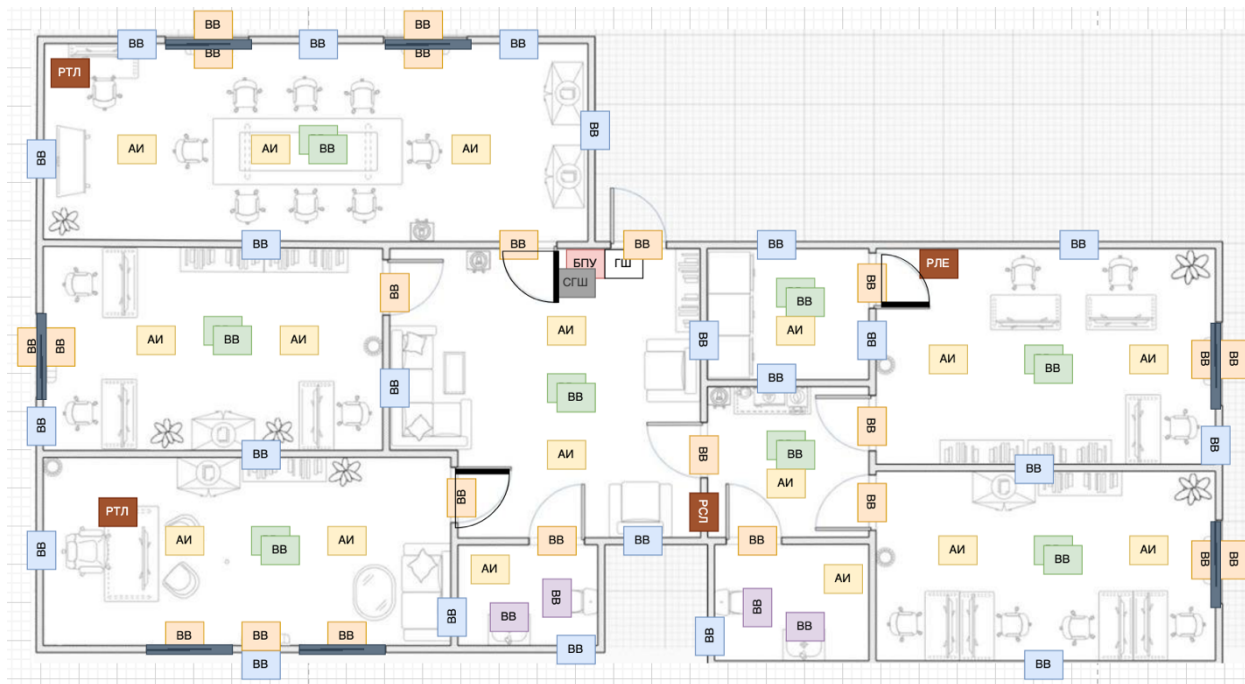

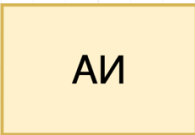
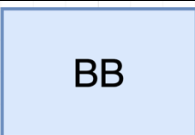

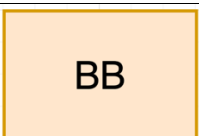
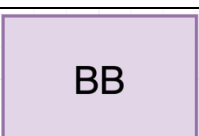

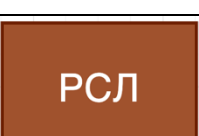

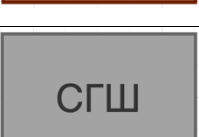
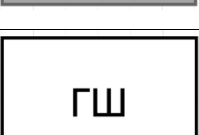
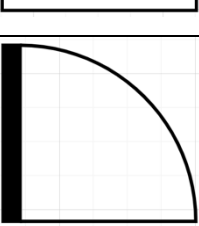



Рисунок 5.1 – Схема расстановки устройств

Таблица 5.1 – 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 |

Продолжение таблицы 5.1

| Обозначение | Устройство | Количество, шт. |
|---|---|--------------------|
|  | Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол) | 16 |
|  | Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи) | 23 |
|  | Генератор-вибровозбудитель «Соната СВ-4Б» (трубопровод) | 4 |
|  | 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).