

**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 системы защиты информации на
предприятии. Вариант 102»

Выполнил:

Цыдыпов Артур Олегович
студент группы N34501



(подпись)

Проверил:

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

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

Студент Цыдыпов Артур Олегович
(Фамилия И.О.)
Факультет Безопасности Информационных Технологий
Группа N34501
Направление (специальность) 10.03.01. - Технологии защиты информации
Руководитель Канжелев Юрий Алексеевич, к.т.н., с.н.с., доцент ФБИТ Университета ИТМО
(Фамилия И.О., должность, ученое звание, степень)
Дисциплина Инженерно-технические средства защиты информации
Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

Задание Проанализировать всевозможные каналы утечки данных в помещении, провести анализ рынка технических средств защиты информации разных категорий, разработать схему расстановки выбранных технических средств в защищаемом помещении

Краткие методические указания

Рекомендуемая литература

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Цыдыпов Артур Олегович



(Подпись, дата)

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

Студент Цыдыпов Артур Олегович

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34501

Направление (специальность) 10.03.01. - Технологии защиты информации

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

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

Дисциплина Инженерно-технические средства защиты информации

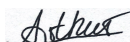
Наименование темы Проектирование инженерно-технической системы защиты
информации на предприятии

| № п/п | Наименование этапа | Дата завершения | | Оценка и подпись руководителя |
|----------|---------------------------------|-----------------|-------------|----------------------------------|
| | | Планируемая | Фактическая | |
| 1 | Создание плана КР | 20.11.2023 | 20.11.2023 | |
| 2 | Анализ литературы | 24.11.2023 | 24.11.2023 | |
| 3 | Составление основного текста КР | 2.12.2023 | 2.12.2023 | |

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Цыдыпов Артур Олегович



(Подпись, дата)

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

| | |
|-----------------------------|---|
| Студент | Цыдыпов Артур Олегович |
| | (Фамилия И.О.) |
| Факультет | Безопасности Информационных Технологий |
| Группа | N34501 |
| Направление (специальность) | 10.03.01. - Технологии защиты информации |
| Руководитель | Попов Илья Юрьевич, к.т.н., доцент ФБИТ университета ИТМО |
| | (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)

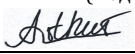
1. Цель и задачи работы ☒ Предложены студентом ☐ Сформулированы при участии студента
☐ Определены руководителем

2. Цель задач: разработать инженерно-техническую систему защиты информации на предприятии, обеспечивающую надежную защиту данных и минимизацию рисков утечки, повреждения или несанкционированного доступа к информации.

3. Задачи: рассмотреть организационную структуру предприятия; обосновать необходимость защиты информации; провести анализ защищаемых помещений; выбрать инженерно-технические средства защиты информации в соответствии с существующим рынком предлагаемых решений; спроектировать систему защиты информации на основе выбранных средств.

4. Характер работы ☐ Расчет ☐ Конструирование
☐ Другое ☒ Моделирование

5.

| | |
|--------------|--|
| Руководитель | Попов Илья Юрьевич |
| | (Подпись, дата) |
| Студент | Цыдыпов Артур Олегович  |
| | (Подпись, дата) |

«___» _____ 20__ г

СОДЕРЖАНИЕ

| | |
|--|----|
| ВВЕДЕНИЕ | 6 |
| 1. ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ | 8 |
| 2. ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ | 11 |
| 3. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ | 14 |
| 3.1 План помещений предприятия | 14 |
| 3.2 Описание помещений | 18 |
| 3.3 Анализ потенциальных каналов утечек информации..... | 19 |
| 3.3 Выбор средств защиты информации..... | 20 |
| 4. АНАЛИЗ РЫНКА ПРЕДЛАГАЕМЫХ РЕШЕНИЙ..... | 22 |
| 4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации..... | 23 |
| 4.2 Устройства для перекрытия акустического и виброакустического каналов утечки информации..... | 25 |
| 4.3 Устройства для перекрытия визуально-оптического канала утечки информации | 27 |
| 5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ | 29 |
| ВЫВОДЫ | 33 |
| СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ..... | 34 |

ВВЕДЕНИЕ

В настоящее время, в условиях стремительного развития информационных технологий и все большей зависимости организаций от электронной обработки, хранения и передачи данных, обеспечение безопасности информации становится одной из наиболее актуальных и важных задач. Особенно это касается предприятий, которые работают с конфиденциальной и важной информацией, включая персональные данные клиентов, финансовые отчеты, коммерческие секреты и другие конфиденциальные данные. В этом контексте проектирование инженерно-технической системы защиты информации на предприятии играет фундаментальную роль в обеспечении безопасности данных и предотвращении различных угроз.

В работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации на объекте: государственная тайна с уровнем «совершенно секретно». Объект имеет 16 помещений, в которые входят кабинет директора, несколько переговорных, кабинки работников, кухня и брифинг-комната.

Цель работы – разработать инженерно-техническую систему защиты информации на предприятии, обеспечивающую надежную защиту данных и минимизацию рисков утечки, повреждения или несанкционированного доступа к информации.

Для достижения поставленной цели необходимо решить следующие задачи:

- Рассмотреть организационную структуру предприятия;
- Обосновать необходимость защиты информации;
- Провести анализ защищаемых помещений;
- Выбрать инженерно-технические средства защиты информации в соответствии с существующим рынком предлагаемых решений;

– Спроектировать систему защиты информации на основе выбранных средств.

1. ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

Предприятие – объект, обрабатывающий материальные или информационные потоки. Организационная структура предприятия – это формальная система, которая определяет, как управляются и координируются различные функциональные направления, подразделения и индивиды в организации. Схема организационной структуры защищаемого предприятия представлена на рисунке 1.

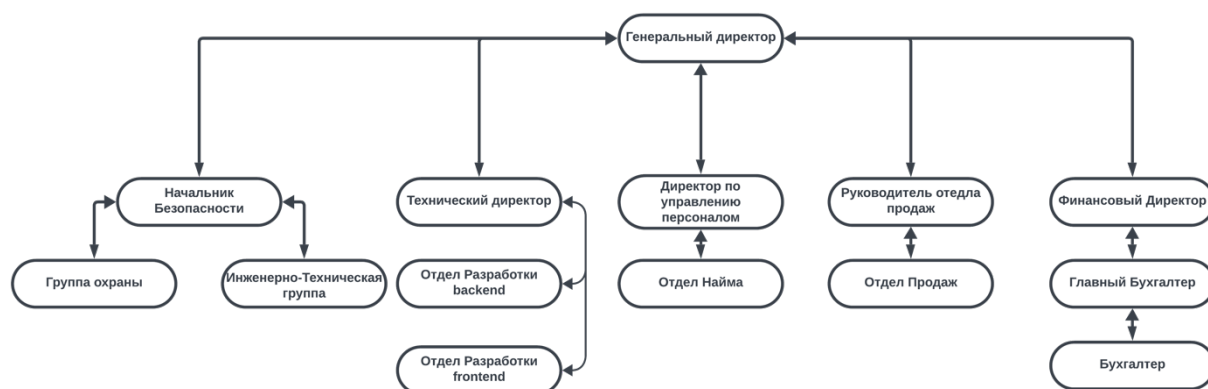


Рисунок 1 – организационная структура предприятия

Информационные потоки представляют собой ключевую составляющую системы передачи данных в организации или процессе. Схема информационных потоков позволяет визуализировать и описать обмен информацией между различными участниками системы. Она помогает выявить и проанализировать все этапы передачи и обработки информации, идентифицировать узкие места и возможные проблемы в потоке данных, а также оптимизировать процессы коммуникации и обработки информации. Схема информационных потоков предприятия представлена на рисунке 2.

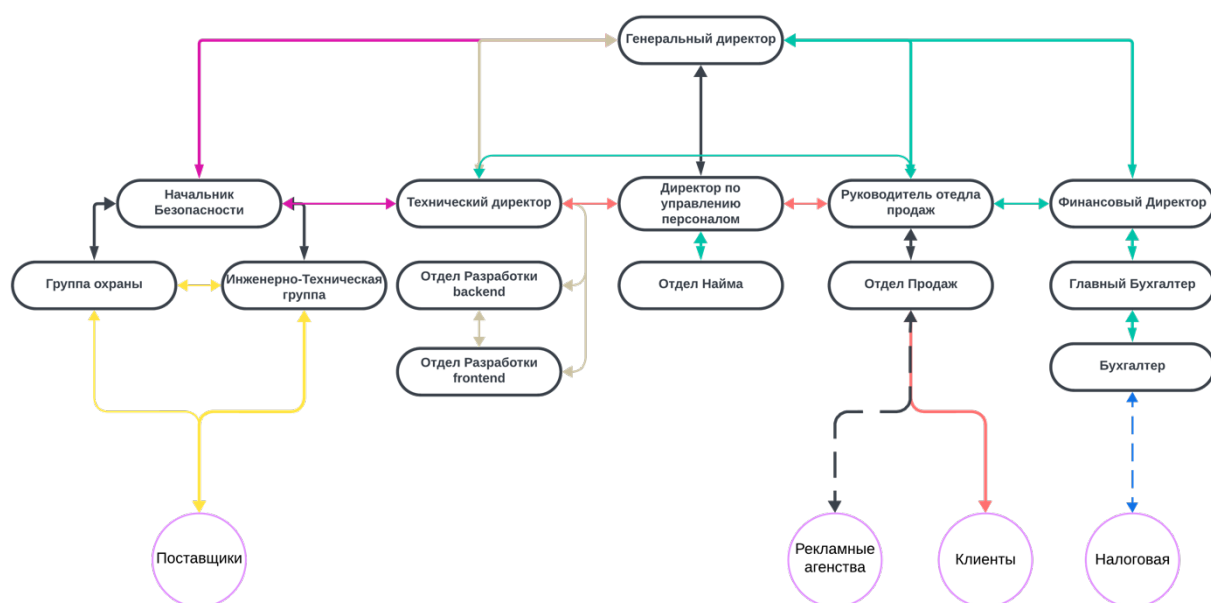






Рисунок 2 – информационные потоки предприятия

Пояснения к цветовым обозначения на схеме информационных потоков предприятия представлены в таблице 1.

| Обозначение | Значение |
|-------------|--|
| | Внешние субъекты информационного обмена |
| | Внутренний субъект информационного объекта |
| | Открытый информационный поток |
| | Закрытый информационный поток |
| | Информация о поставках |
| | Информация о клиентах |

| | |
|---|--------------------------------------|
|  | Открытая финансовая информация |
|  | Информация о инцидентах безопасности |
|  | Закрытая финансовая информация |
|  | Информация о разработке |

2. ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Государственная безопасность – система гарантий государства от угроз извне и основам конституционного строя внутри страны. Для реализации этих гарантий в стране создана и функционирует система защищаемых законом тайн. Под тайной понимается нечто скрываемое от других, известное не всем, секрет. Существует большое число охраняемых законом тайн.

В информации, хранящейся и обрабатываемой защищаемым объектом, содержатся сведения, содержащие:

1. Коммерческую тайну – информацию, которая относится к бизнес-операциям, процессам, методологиям и стратегиям предприятия, и которая дает ей конкурентное преимущество на рынке. Это могут быть конфиденциальные данные о продуктах, клиентах, партнерах, сделках, финансовых показателях, исследованиях и разработках.
2. Персональные данные – предприятие обрабатывает персональные данные сотрудников, клиентов и сторонних лиц, работающих с проектами. Это может включать личную информацию, такую как имена, адреса, номера телефонов, электронные адреса, финансовые данные, данные о физической и медицинской характеристиках и другие личные сведения.
3. Государственную тайну – это сведения политического, экономического, военного и научно-технического характера, утрата или разглашение которых создает угрозу безопасности и независимости государства или наносит ущерб его интересам.

Подробнее остановимся на государственной тайне. Установлены три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений.

К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

В рассматриваемом предприятии фигурируют сведения второй степени секретности (гриф «совершенно секретно»). Предприятие занимается разработкой программного обеспечения, обеспечивающего шифрование данных.

На основании представленной выше информации, требования к защите информации определяют следующие руководящие документы:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

4. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
5. Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;
6. Приказ ФСТЭК «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644;
7. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
8. Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
9. Закон РФ «О государственной тайне» от 21.07.1993 N 5485–1;
10. Межведомственная комиссия по защите государственной тайны решение № 199 от 21.01.2011 г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними";
11. СТР. Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам;
12. СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации.

3. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 План помещений предприятия

Перед началом проектирования инженерно-технической защиты подробно рассмотрим план помещений с меблировкой предприятия (рисунок 3).

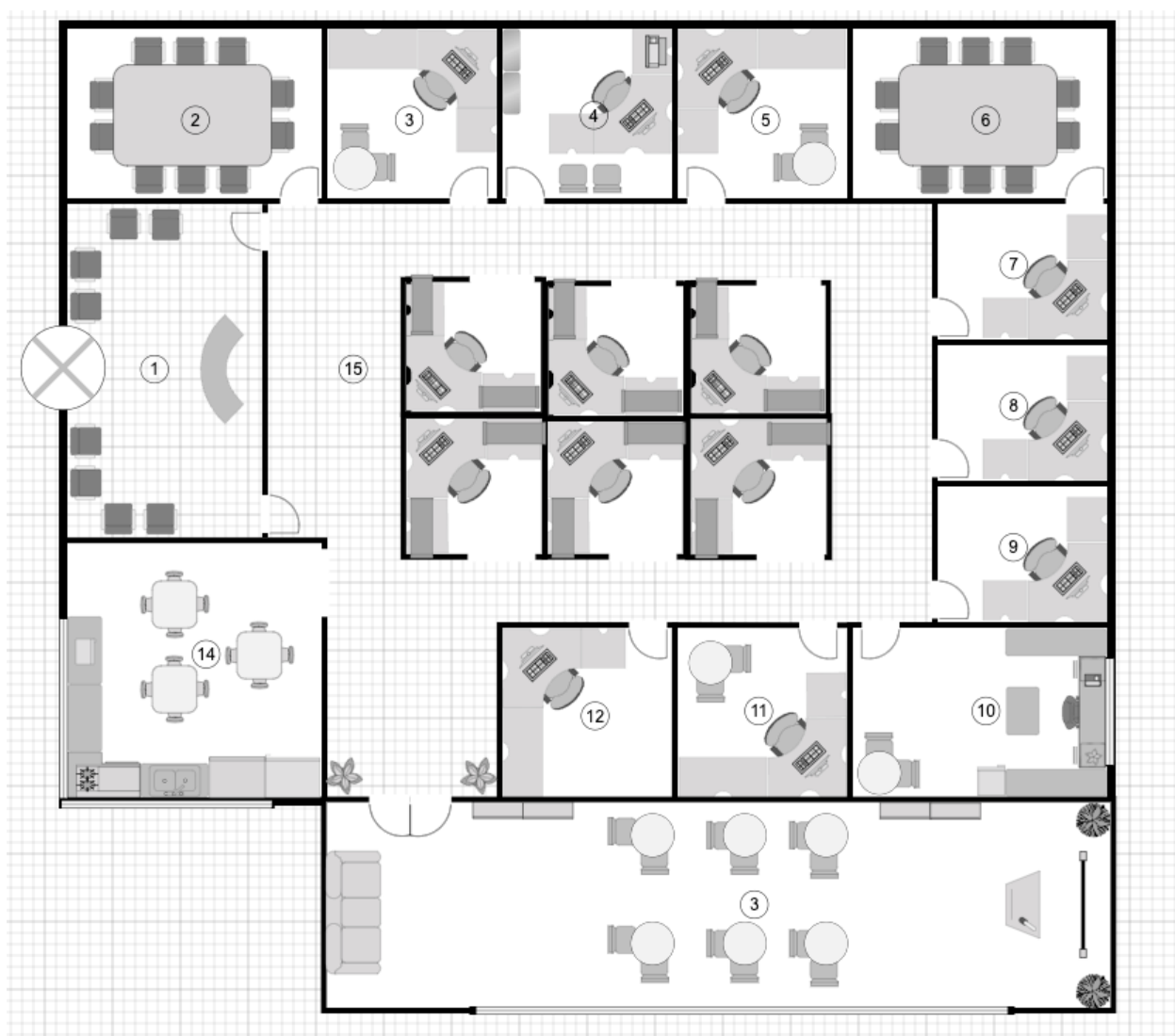
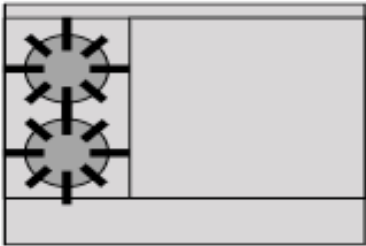

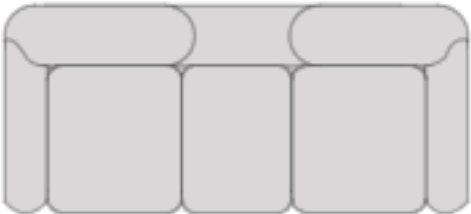

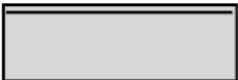



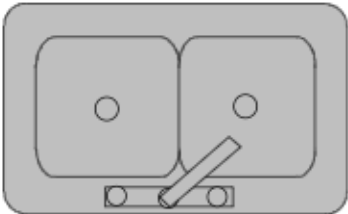




Рисунок 3 – план защищаемого помещения







На таблице 2 приведен список мебели, установленной в помещении.

Таблица 2 – Условные обозначения на плане защищаемого помещения

| Графическое изображение | Наименование |
|---|-------------------|
|  | Дверь |
|  | Вращающаяся дверь |
|  | Окно |
|  | Кафедра |
|  | Маленький цветок |
|  | Стол ресепшена |

| | |
|---|-----------------------|
|  | <p>Газовая плита</p> |
|  | <p>Холодильник</p> |
|  | <p>Диван</p> |
|  | <p>Средний цветок</p> |
|  | <p>Книжная полка</p> |

| | |
|---|------------------|
|  | Кресла и стулья |
|  | Раковина |
|  | Стол переговоров |
|  | Стол |
|  | Рабочий стол |
|  | Обеденный стол |

| | |
|---|----------------------------------|
|  | Автоматизированное рабочее место |
|  | Принтер |
|  | Шкаф |
|  | Интерактивная доска |
|  | Тумба |
|  | Телефон |

3.2 Описание помещений

На плане обозначено 15 комнат, из них подлежат защите помещения под следующими номерами:

1. Переговорная (2), 8м x 6м (48м²)
2. Переговорная (6), 8м x 6м (48м²)
3. Бриффинг-комната (3), 16м x 6м (96м²)
4. Кабинет директора (10) 6.4м x 6м (38.4м²)

В двух переговорных расположены: стол, стулья.

В бриффинг комнате расположены: 12 стульев, 6 столов, кафедра, интерактивная доска, 4 книжных полки, 2 средних цветка, диван и большое панорамное окно.

В кабинете директора расположены: окно, телефон, маленький цветок, рабочий стол, рабочее кресло, два стула, 2 стола, тумба.

Офис расположен на первом этаже многоэтажного здания, окна выходят во двор с ограниченным доступом. Окна не соседствуют с пожарными или эвакуационными лестницами, крышами пристроек, балконами и иными прочими выступами, с которых в помещение могут проникнуть посторонние лица. Стенды здания и внутренние перегородки железобетонные, толщиной не менее 300 мм.

3.3 Анализ потенциальных каналов утечек информации

В интерьерах данного объекта имеются декоративные элементы, которые могут служить укрытием для размещения скрытых устройств для передачи информации. В каждой комнате присутствуют электрические розетки, сетевые устройства и в некоторых из них — телефонная аппаратура, что означает потенциальную возможность утечек через электрические и электромагнитные каналы. Кроме того, существует угроза извлечения информации через вибрационные (включая вибро-акустические), оптические и акустические (включая акустоэлектрические) каналы. Однако физические методы передачи информации не рассматриваются в данном исследовании, поскольку их защита регулируется внутренней политикой информационной безопасности компании.

3.4 Выбор средств защиты информации

Для обеспечения всесторонней безопасности в соответствии с уровнем конфиденциальности информации, такой как государственная тайна «совершенно секретно», необходимо оснастить помещения специальными средствами инженерно-технической защиты (см. таблицу 3).

1. Акустический, акустоэлектрический

- Источники: Окна, двери, электрическая сеть, проводка, вентиляция.
- Пассивная защита: Звукоизоляция помещений, акустические экраны, фильтры для цепей электропитания.
- Активная защита: Акустические извещатели, звукопоглощающие экраны, фильтры для защиты от акустоэлектрического шпионажа.

2. Вибрационный, виброакустический

- Источники: Радиаторы отопления, любые твердые поверхности в помещениях.
- Пассивная защита: Изоляция поверхностей от вибраций, дополнительная обшивка для уменьшения вибрации.
- Активная защита: Вибрационные извещатели, дополнительная обшивка для уменьшения вибрации.

3. Оптический

- Источники: Окна, двери, преграждения.
- Пассивная защита: Средства для подавления отраженного света, доводчики на дверях.
- Активная защита: Маскирующие средства, преграждения от отраженного света.

4. Электромагнитный, электрический

- Источники: Розетки, любые электрические приборы.

- Пассивная защита: Фильтры для цепей электропитания, экранирование металлом для подавления шума.
- Активная защита: Системы защиты от электромагнитных помех, электромагнитные защитные экраны.

4. АНАЛИЗ РЫНКА ПРЕДЛАГАЕМЫХ РЕШЕНИЙ

В соответствии с требованиями задания к курсовой работе, система защиты информации разрабатывается для обеспечения безопасности сведений, составляющих государственную тайну уровня «совершенно секретно». Согласно нормам и правилам проектирования помещений для хранения и работы с государственной тайной, утвержденным Решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 №199, следует удовлетворить следующие критерии безопасности:

1. Установка усиленных дверей в помещениях для работы с государственной тайной и хранилищах секретных документов. Двери должны обшиваться металлическим листом толщиной не менее 2 мм с обеих сторон, внутри должен быть звукоизоляционный материал. Толщина двери должна быть не менее 4 см. Дверь должна быть установлена на металлический каркас.
2. Обязательное наличие противопожарного перекрытия между блоком режимных помещений и другими комнатами в здании.
3. Оснащение всех режимных помещений аварийным освещением.
4. Перед вводом в эксплуатацию необходимо провести проверку выделенных режимных помещений и других секретных зон на предмет обнаружения "жучков" или других устройств для несанкционированного сбора информации. В дальнейшем рекомендуется проводить такие проверки периодически для исключения возможности утечки информации.

4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Для обеспечения пассивной защиты данного объекта используются следующие методы:

1. Использование усиленных дверей;
2. Установка тамбурного помещения перед зоной переговоров;
3. Дополнительная звукоизоляция переговорной за счет использования специальных звукоизолирующих материалов.

В качестве метода для активной защиты применяется система виброакустического зашумления. Для защиты помещения, предназначенного для работы с государственной тайной уровня "совершенно секретно", будет рассмотрено применение средств активной защиты информации для объектов информатизации не менее 1Б. Таблица 4 содержит сравнительный анализ решений, предложенных на современном рынке и соответствующих установленным требованиям для защиты объекта от утечек по виброакустическому каналу.

Таблица 3 – Средства активной защиты от утечек по виброакустическому каналу

| Фирма | Устройство | Цена, руб. | Характеристики |
|---------------------|-------------------|-----------------------|---|
| Детектор Системс | СОНАТА СВ-4Б | 8 100 | <ul style="list-style-type: none">• Полоса воспроизводимых частот: 175– 11200 Гц |

| | | | |
|------------------|---------------|--------|--|
| | | | <ul style="list-style-type: none"> • Диапазон регулировки: 32 дБ |
| Детектор Системс | СОНАТА СА-4Б1 | 7 440 | <ul style="list-style-type: none"> • Полоса воспроизводимых частот: 175–11200 Гц • Диапазон регулировки: 32 дБ |
| Лаборатория ППШ | ЛГШ-304 | 25 200 | <ul style="list-style-type: none"> • Полоса воспроизводимых частот: 175–11200 Гц • Диапазон регулировки: 32 дБ • Мощность: не более 10 Вт |

В результате анализа было решено использовать комбинацию аппаратуры для защиты от акустической разведки “Соната СВ-4Б” и “Соната СА-4Б1”. Этот выбор обоснован оптимальным соотношением цены и характеристик системы. Данная система позволяет автоматически контролировать все компоненты при минимальных затратах на

оборудование и установку. Она также обеспечивает возможность изменения настроек генераторов-излучателей в реальном времени, что позволяет создавать адаптивную систему виброакустической защиты с различными профилями, соответствующими требованиям безопасности при различных условиях использования помещения.

4.2 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Для пассивной защиты объекта используются сетевые фильтры, которые применяются в электропитании, и металлический материал для экранирования.

Для активной защиты используется генератор пространственного зашумления, который создает белый шум в электрической сети, скрывая колебания, возникающие от работающей электроники или воздействия звуковых волн. В таблице 4 проведено сравнение доступных на рынке решений, соответствующих требованиям защиты для предотвращения утечек через электрические каналы.

Таблица 4 – Средства активной защиты от утечек по электрическим каналам

| Фирма | Устройство | Цена, руб. | Характеристики |
|---------------------|---|-----------------------|---|
| Детектор Системс | Генератор шума Покров, исполнение 1 | 32 800 | <ul style="list-style-type: none"> • Диапазон для электрической составляющей: 0,009 – 6000 МГц • Диапазон для магнитной |

| | | | |
|------------------|--|--------|--|
| | | | <p>составляющей: 0,009 – 30 МГц</p> <ul style="list-style-type: none"> • Диапазон для электрических сигналов, наведенных на цепи электропитания: 0,009 – 400 МГц • Потребляемая мощность: не более 15 Вт |
| Детектор Системс | Соната-РЗ Средство активной защиты информации от утечки за счёт ПЭМИН | 97 200 | <ul style="list-style-type: none"> • Потребляемая мощность: не более 30 Вт |
| Сюртель | SEL SP-44, устройство защиты цепей электросети | 24 000 | <ul style="list-style-type: none"> • Диапазон частот формируемого шумового сигнала: 0,001 – 300 МГц |

| | | | |
|--|-----------------|--|---|
| | и заземления | | <ul style="list-style-type: none"> • Защищаемые линии: питание, заземление • Управление включением шумового сигнала: ручное, ДУ, RS-485 |
|--|-----------------|--|---|

В результате сравнительного анализа было решено использовать устройство защиты информации от утечки ПЭМИН "Соната-РЗ". Это устройство обеспечивает защиту от утечки информации путем генерации электромагнитного поля шума, которое скрывает побочные электромагнитные излучения и помехи. Оно также создает маскирующие шумовые напряжения для защиты от помех на линиях электропитания и заземления.

Одним из преимуществ этого решения является возможность комбинирования нескольких устройств для потенциального увеличения уровня защиты. Также важно отметить наличие сертификата ФСТЭК и приемлемую стоимость данного устройства. Дополнительным плюсом является возможность интеграции данного устройства в систему "Соната РЗ" производства того же производителя, что также предоставляет средство защиты от акустических утечек.

4.3 Устройства для перекрытия визуально-оптического канала утечки информации

Для предотвращения утечки информации через оптический канал рекомендуется установить на окно жалюзи, шторы или тонирующие пленки.

Для предотвращения наблюдения сквозь неполностью закрытую дверь может быть использован доводчик, который плавно закрывает дверь после ее открытия.

Кроме того, для дополнительной защиты от утечек через виброакустический канал можно использовать устройство «Соната СВ-4Б», описанное в разделе 4.1.

5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

На основе данных из главы 4 были выбраны следующие технические средства для защиты информации:

1. Усиленные двери, обшитые металлом и со звукоизолирующей прокладкой на металлическом каркасе - 4 шт., установлены в двух переговорных, брифинг-комнате и кабинете директора.
2. Аппаратура защиты от акустической разведки «Соната СА-4Б1».
3. Устройство защиты объектов информатизации от утечки информации - ПЭМИН "Соната-РЗ".
4. Жалюзи на окна.

Для оценки необходимого количества компонентов были учтены спецификации модели «Соната СВ-4Б», включающие в себя генераторы-акустоизлучатели СА-4Б и генераторы-вибровозбудители СВ-4Б. Согласно данным от НПО, предполагаемое количество генераторов-вибровозбудителей СВ-4Б можно определить следующим образом:

- Для стен: один на каждые 3–5 метров периметра для капитальной стены на уровне половины высоты помещения;
- Для потолка и пола: один на каждые 15–25 м² площади;
- По одному на окно и дверь при установке на соответствующие элементы;
- Для труб систем централизованного отопления: один на каждую вертикальную трубу коммуникаций.

Необходимое количество генераторов-акустоизлучателей СА-4Б можно предположительно оценить по следующим критериям:

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

Общее количество необходимых технических средств для данного объекта защиты, а также их оценочная стоимость представлены в таблице 5.

Таблица 5 – Оценка стоимости ТСЗИ

| Наименование средства | Количество, у.е. | Цена за штуку, руб | Общая стоимость |
|--|------------------|--------------------|-----------------|
| Генератор-вибровозбудитель Соната СВ-4Б | 62 | 8 100 | 502 200 |
| Генератор-акустоизлучатель Соната СА-4Б1 | 17 | 7 440 | 126 480 |
| Жалюзи blackout | 17 | 2 000 | 34 000 |
| Пульт управления «Соната-ДУ4.4» | 1 | 7 680 | 7 680 |
| Звукоизолирующая усиленная дверь | 4 | 40 200 | 160 800 |
| Соната-РЗ.1 | 4 | 97 200 | 388 800 |
| Размыкатель Ethernet “etherCUT” | 1 | 12 400 | 12 400 |
| Размыкатель слаботочной линии “Соната-ВК4.2” | 4 | 6 000 | 24 000 |

Общая стоимость затрат на ТСЗИ: 1 255 600 рублей.

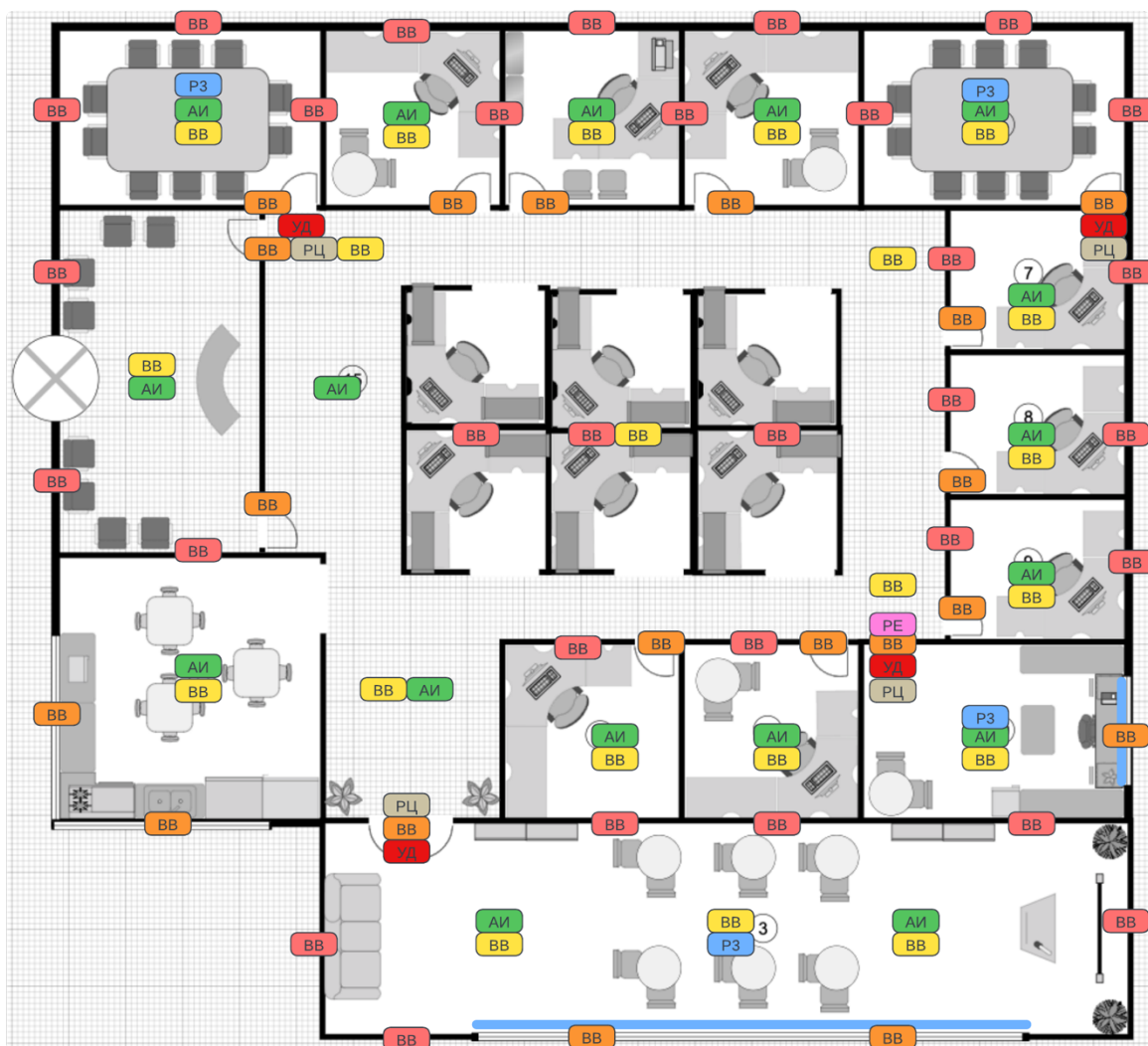










Рисунок 4 – план защищаемого помещения с ТЦСИ

Условные обозначения, используемые в рисунке 4, указаны в следующей таблице.

Таблица 6 – Средства активной защиты от утечек по электрическим каналам

| Обозначение | Средство |
|---|--|
|  | редство активной защиты информации от утечки за счёт ПЭМИН «Соната-Р3» |
|  | Генератор-вибровозбудитель СВ-4Б на стены |
|  | Генератор-вибровозбудитель СВ-4Б на двери и окна |
|  | Генератор-вибровозбудитель СВ-4Б на потолок и пол |
|  | Генератор-акустоизлучатель СА-4Б |
|  | Звукоизолирующая усиленная дверь |
|  | Размыкатель слаботочной линии |
|  | Размыкатель Ethernet |
|  | Жалюзи-blackout |

ВЫВОДЫ

В ходе выполнения курсовой работы был осуществлен теоретический обзор потенциальных технических каналов утечки информации, проведен анализ структуры защищаемого предприятия, включая подробное описание его помещений и информационных каналов.

Для выбора соответствующих средств технической защиты информации был проанализирован рынок существующих решений, нацеленных на противодействие выявленным каналам утечки. На основе этого анализа были выбраны оптимальные решения, наиболее подходящие для данного объекта. На основе этих средств был разработан план установки и проведен расчет финансовых затрат, которые описаны в разделе 5 данной работы.

В результате работы была предложена система защиты от утечек информации по различным каналам, включая акустический, виброакустический, оптический, акустоэлектрический, электрический, электромагнитный и оптико-электронный. Общие затраты на обеспечение этой защиты оцениваются в сумму 1 219 600 рублей, что является обоснованным вложением для объекта, обрабатывающего и хранящего сведения, отнесенные к государственной тайне с грифом уровня «совершенно секретно».

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Рагозин, Ю. Н. Инженерно-техническая защита информации: учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2018. — 168 с.— ISBN 978-5-4383-0161-5. - Текст: электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/103203> (дата обращения: 01.12.2023). — Режим доступа: для авториз. пользователей
2. 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. — Текст: электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/43579> (дата обращения: 01.12.2023). — Режим доступа: для авториз. пользователей.