|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Федеральное государственное бюджетное образовательное учреждение высшего образования**  **«Российский биотехнологический университет (РОСБИОТЕХ)»** | | | | | | | | | | | | | | |
|  |  | |  |  | |  |  |  | |  | |  | |  |
| **Кафедра** | | | **Информатика и вычислительная техника пищевых производств** | | | | | | | | | | | |
|  |  | |  |  | |  |  |  | |  | |  | |  |
| **Направление (Специальность)** | | | **Информатика и вычислительная техника** | | | | | | | | | | | |
|  |  | |  |  | |  |  |  | |  | |  | |  |
| **Профиль** | | | **Искусственный интеллект** | | | | | | | | | | | |
|  |  | |  |  | |  |  |  | |  | |  | |  |
|  |  | |  |  | |  |  | **К ЗАЩИТЕ** | | | | | | |
|  |  | |  |  | |  |  | **(РЕКОМЕНДОВАНО / НЕ РЕКОМЕНДОВАНО)** | | | | | | |
|  |  | |  |  | |  |  | **зав. кафедрой** | | | | | | |
|  |  | |  |  | |  |  | **к.ф.-м.н., доцент** | | | | | | |
|  |  | |  |  | |  |  | ***(ученая степень, ученое звание)*** | | | | | | |
|  |  | |  |  | |  |  |  | | |  | | **Т.А. Санаева** | |
|  |  | |  |  | |  |  | ***(подпись)*** | | |  | | ***(И.О. Фамилия)*** | |
|  |  | |  |  | |  |  | **« » 20   г.** | | | | | | |
|  |  | |  |  | |  |  |  | |  | |  | |  |
| **КУРСОВАЯ РАБОТА** | | | | | | | | | | | | | | |
| ***по дисциплине*** | | | | | | | | | | | | | |  |
| ***«Информационные системы и технологии»*** | | | | | | | | | | | | | |  |
|  |  | |  |  | |  |  |  | |  | |  | |  |
| **на тему:** | |  | | | | | | | | | | | | |
|  |  |
|  |  | ***(тема курсовой работы)*** | | | | | | | | | | | | |
|  |  |  |  |  | |  |  |  | |  | |  | |  |
| **Обучающийся:** | | |  | | **« » \_ 20\_\_ г.** | | | | **Агаметов Ш.И.** | | | | | |
|  |  |  | ***(подпись)*** | |  |  |  |  | ***(инициалы, фамилия)*** | | | | | |
|  |  | |  |  | |  |  |  | |  | |  | |  |
|  | | | |  |  | | | **группа** | | |  | |  | |
|  |  | |  |  |  | | |  | | |  | | ***(шифр группы)*** | |
| **Руководитель** | | |  | | **« » \_ 20\_\_ г.** | | | | **доц, к.т.н, Т.В. Ящун** | | | | | |
|  |  | | ***(подпись)*** | |  |  |  |  | ***(уч. степень, уч. звание, инициалы, фамилия)*** | | | | | |

Москва, 2025 г.

**Содержание**

Введение

1. Анализ локальной вычислительной сети

1.1 Выбор технологии и топологии

1.2 Выбор кабельной среды

2. Анализ характеристик и выбор оборудования

2.1 Анализ и выбор рабочей станции

2.2 Выбор подходящего программного обеспечения

2.3 Обоснования выбора оборудования

3. Анализ и настройка сети для данной организации

3.1 Разбиение сети на под сети

3.2 Построение логической схемы сети

3.3 Настройка адресов и подключение устройств

4. Настройка файлового и веб серверов

4.1 Настройка Веб Сервера

5. Настройка маршрутизаторов,списков доступа,статической маршрутизации

5.1 Настройка ACL

5.2 Настройка статической маршрутизации

6. Построение физической модели сети

Заключение

Список сокращенных слов

Список использованных источников

Введение

С началом массового использования компьютеров стало возможным крайне быстро передавать информацию на расстоянии, совместно используя периферийные устройства. Однако ещё больше выросла производительность работы с объединением компьютеров в компьютерные сети, особенно в 90-е годы XX века стала бурно развиваться и использоваться сеть Интернет. Объединение компьютеров в единую сеть стало толчком к развитию научно-технического прогресса.

Основная цель создания компьютерных сетей является совместное использование ресурсов и осуществление интерактивной связи как внутри одной фирмы, так и за её пределами. Компьютерные сети обеспечивают:

 совместное использование ресурсов, т.е. если в организации имеется несколько компьютеров и эпизодически возникает потребность в печати текста, то достаточно иметь один сетевой принтер для всех вычислительных машин;

 повышение надёжности работы вычислительной техники. Здесь если отказ может вызвать катастрофические последствия, то устанавливаются вычислительные машины, которые соединены друг с другом и в случае выхода из строя можно заменить другой вычислительной машиной;

 для общения пользователей. Сотрудники могут общаться между собой с помощью электронных писем, видео звонков и тому подобное;

 сохранение данных. На данный момент времени очень важно регулярно производить резервное копирование данных в компьютере. С помощью сети легче осуществлять резервное копирование всех данных компании с использованием одного устройства.

Но существует главный фактор, как территориальное размещение сети. Оно делится на:

 локальные сети, они обеспечивают наивысшую скорость обмена информацией между компьютерами, и типичная локальная сеть занимает пространство в одно или несколько зданий;

 глобальные сети, позволяют организовать взаимодействие между компьютерами на больших расстояниях;

 городские сети эти сети предназначены для обслуживания территории крупного города-мегаполиса.;

Но сети не так надёжный как кажется на первый взгляд, их основными недостатками являются:

 вопросы безопасности. Одним из основных недостатков компьютерных сетей вопросам безопасности. Если компьютер находится в сети, хакер может получить несанкционированный доступ с помощью различных инструментов;

 вирусы и вредоносные программы. Если хотя бы один компьютер подвергся атаки вируса, то возможна угроза для других систем, так как все компьютеры объединены в одну сеть. Вирусы довольно легко могут распространяются по сети.

Компьютерные сети развиваются со стремительной скоростью, что-то модернизируется, создаётся. И главным толчком в развитии стало появление беспроводной передачи данных. Сегодня существует большое число беспроводных телекоммуникационных систем, из которых наиболее распространенными являются системы широковещания, такие как радио или телевидение. Беспроводная среда, для которой сегодня в основном используется микроволновый диапазон, отличается высоким уровнем помех, которые создают внешние источники излучения.

На сегодняшний день наиболее широко используемой спецификацией является стандарт 802.11b. Это модификация Wi-Fi технологии, которая используется часто, но на данный момент ему на смену приходят стандарты с высокой скоростью. Традиционная схема сети с технологией Wi-Fi содержит как минимум одну точку доступа и одного клиента. Возможна коммутация двух абонентов в режиме точка-точка. При этом точка доступа отсутствует, а клиенты соединяются напрямую через сетевые адаптеры.

Как узнали ранее безопасность компьютерных сетей постоянно находиться под угрозой, ежедневно около тысячи компьютеров подвергаются атаками вирусов. Многие компании борются с ними, но с каждым днём создаются всё более опасные вирусы. Вирусы подразделяют на несколько видов (начиная с COM-вирусов до макровирусов)

Исходя из этого будет рассматриваться компания по безопасности компьютерных сетей и разработка софта для обеспечения безопасности компьютерных сетей под названием ООО “Fil Industries”. В этом проектировании будет отображаться логическая схема сети, физическая схема сети, подбор оборудования для компании.

Передо мной стоит цель построить компьютерную сеть для данной организации. Сеть в ней нужна для объединения компьютеров сотрудников и связи между ними, и доступа в локальную сеть.

Задачи:

 проанализировать потребности предприятия;

 проанализировать план здания;

 спроектировать логическую карту, соответствующая поставленным целям;

 спроектировать физическую карту, соответствующая поставленным целям;

 проанализировать и выбрать оборудование исходя из потребностей компании;

 проанализировать и подобрать программное обеспечение исходя из потребностей компании;

1. Анализ локальной-вычислительной сети

Для анализа предприятия необходимо убедиться, в том что оно соответствует правилам СанПин. Первое что должно быть это размер рабочего места, в компании одно рабочее место составляет 19 м2, что соответствует минимальному размеру 4,5 м2. Второе, рабочие столы разместили таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева. Освещенность на поверхности стола в зоне размещения рабочего документа составляет 400 лк. Третье, между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора) должно быть составляет 2,5 м, а расстояние между боковыми поверхностями видеомониторов - 1,5 м. Экран видеомонитора должен находиться от глаз пользователя на расстоянии 650 мм. Высота рабочей поверхности стола для взрослых пользователей составляет 700 мм. Исходя из правил СанПин, компания соответствует правилам и готова быть размещена. Теперь нужно расположить все 256 устройств в наше здание. Для расчёта площади были взяты следующие значения:

 длина 168 м;

 ширина 107 м;

 умножим 168 107 = 18,000 м3.

Вот мы получили площадь нашего здания.

Данная локальная сеть будет разрабатываться для организации по безопасности компьютерных сетей. Это организация будет выполнять множество функций:

 обеспечение безопасности компьютерных сетей;

 разработка и внедрения программ по защите сетей;

 организация антивирусной защиты информации;

 выявление и обезвреживание угроз;

 проверка сетей на уязвимости;

 подготовка специалистов к дальнейшей работе.

Для эффективной реализации оказываемых услуг необходимо наличие:

 высокоскоростного доступа в интернет;

 грамотно построенной сети внутри организации;

 правильного построенного чертежа здания по СанПиН;

Локальная сеть будет использоваться для обеспечения доступа к сети Интернет, хранения на серверах большого объёма информации (документации, отчёты) и будет состоять из 256 устройств различного типа (компьютеры, ноутбуки, сервера, коммутаторы и так далее).

1.1 Выбор технологии и топологии

На сегодняшний день существует несколько технологий, на основе которых работает большинство локальных сетей, такие как Ethernet, Token Ring, FDDI.Для выбора технологии, сначала необходимо разобраться, какая топология будет использоваться.

Под термином топология понимают физическое расположение компьютеров, кабелей и других компонентов сети. От выбора топологии сети будет зависеть следующее:

 способ управления связью;

 устойчивость сети к неисправностям;

 лёгкость настройки сети и её конфигурации;

 уровень затрат.

В данной организации была выбрана топология кольцо. Основными преимуществами этой топологии в отличие от других является:

 простота реализации (установки);

 не требует дополнительного оборудования;

 возможность высокой скорости передачи данных, ведь для отправки пакета не требуется дожидаться отчёта о доставке;

 большая протяженность. Каждый из компьютеров выступает в роли повторителя, тем самым усиливая сигнал;

 обладает высокой устойчивостью к перегрузкам, обеспечивая эффективную работу с большими потоками передаваемой информации.

Исходя из этого, перейдём к выбору технологии. В этом случаи мы выбрали Token Ring.

Token Ring- технология локальной-вычислительной сети кольца с “маркерным доступом”. Используя специальный трёхбайтовый фрейм, который перемещается вокруг кольца. В отличие от сетей CSMA/CD (например, Ethernet), сети с передачей маркера являются детерминистическими сетями. Это означает, что можно вычислить максимальное время, которое пройдет, прежде чем любая конечная станция сможет передавать. Эта характеристика, а также некоторые характеристики надежности, делают сеть Token Ring идеальной для применений, где задержка должна быть предсказуема и важна устойчивость функционирования сети. Применяется как более дешёвая технология, получила распространение везде, где есть ответственные приложения, для которых важна не столько скорость, сколько надёжная доставка информации.

1.2 Выбор кабельной среды

Для реализации технологии Token Ring будут использоваться кабели на витой паре. Витая пара представляет собой два скрученных изолированных медных провода диаметром порядка 1 мм, помещённых в защитную оболочку. Особенности витой пары:

 при скручивании проводники идут под некоторым углом друг к другу, что снижает ёмкостную и индуктивную связь между ними. Благодаря этому уменьшаются перекрёстные помехи;

 при включении по дифференциальной схеме снижается чувствительность к наводкам от внешних полей благодаря сохранению симметрии;

 для витой пары увеличивается погонное затухание кабеля и время распространения сигнала.

Различают витые пары двух видов:

 экранированные витые пары (Shielded Twisted Pair- STP)(смотри рисунок 1);



Рисунок 1 - Структура экранированной витой пары

 неэкранированные витые пары (Unshielded Twisted Pair- UTP)(смотри рис. 2);



Рисунок 2 - Структура неэкранированной витой пары

В этом случае мы будем использовать экранированную витую пару, так как экран выполнен из плетенных медных жилок или фольги и заключён в защитную изоляционную оболочку, что уменьшает влияние внешних электромагнитных помех.

Рассмотрим стандарты Fast Ethernet, которые представлены в таблице 1

Таблица 1

Основные интерфейсы Fast Ethernet

|  |  |  |  |
| --- | --- | --- | --- |
| Физический интерфейс | Порт устройства | Среда передачи | Число витых пар/волокон |
| 100Base-FX | Duplex SC | Оптическое волокно | 2 волокна |
| 100Base-TX | RJ-45 | Витая пара UTP Cat. 5 | 2 витых пары |
| 100Base-T4 | RJ-45 | Витая пара UTP Cat. 3,4,5 | 4 витых пары |

 100BASE-FX использует волоконно-оптический кабель и обеспечивает связь излучением с длиной волны 1310 нм по двум жилам - для приёма (RX) и для передачи (TX);

 100BASE-TX обеспечивает передачу данных со скоростью до 100 Мбит/с по кабелю, состоящему из двух витых пар 5-й категории;

 100BASE-T4 обеспечивает передачу данных со скоростью до 100 Мбит/с по кабелю, состоящему из четырёх витых пар 3-й категории.

Исходя из вышеуказанной информации, наиболее эффективным является использование витой пары категории 5(100BASE-TX), так как данный вид кабеля может обеспечить достаточно неплохую скорость передачи(1000Мбит/с) при использовании 4-х пар, а также прост в реализации и цена весьма невысокая.

Для разрабатываемой сети будем использовать экранированную витую пару: BION BAUI-2151 Кабель UTP indoor cat.5е 4 пары (305 м) 0.51мм

2. Анализ характеристик и выбор оборудований

2.1 Анализ и выбор рабочей станции

Для сотрудников ООО «Fil Industries», занимающихся разработкой программного обеспечения для защиты сетей, тестированием уязвимостей и обеспечением безопасности, рабочие станции должны обладать высокой производительностью, поддерживать специализированное ПО и обеспечивать стабильную работу в условиях многозадачности. Основные требования к рабочим станциям:

- Процессор : Не менее 6 ядер, частота от 3.5 ГГц (например, AMD Ryzen 5 5600X или Intel Core i5-12400F).

- Оперативная память : Минимум 16 ГБ DDR4 (рекомендуется 32 ГБ для задач, связанных с анализом сетей и симуляцией атак).

- Хранилище : SSD NVMe объемом от 512 ГБ для быстрой загрузки и работы с большими массивами данных.

- Графический адаптер : Интегрированная графика (например, Intel UHD Graphics 730) для стандартных задач или дискретная видеокарта (NVIDIA GTX 1650) для работы с визуализацией данных.

- Сетевой адаптер : Gigabit Ethernet (1000 Мбит/с) и поддержка Wi-Fi 6 для беспроводного подключения.

- Операционная система : Windows 11 Pro или специализированные дистрибутивы Linux (например, Kali Linux, Ubuntu) для задач тестирования безопасности.

Выбор : Рабочая станция Dell OptiPlex 7090 Tower с процессором Intel Core i7-11700, 32 ГБ ОЗУ, SSD 1 ТБ и Gigabit Ethernet. Эта модель обеспечивает баланс между производительностью, надежностью и стоимостью, а также поддерживает установку специализированного ПО для анализа сетей.

2.2 Выбор подходящего программного обеспечения

Для обеспечения функциональности сети и выполнения задач компании необходимо следующее ПО:

- Операционные системы :

- Windows 11 Pro для рабочих станций сотрудников, работающих с документацией и стандартными задачами.

- Kali Linux для специалистов по тестированию уязвимостей и анализу безопасности.

- Сетевое ПО :

- Wireshark для анализа сетевого трафика.

- Nmap для сканирования сети и выявления уязвимостей.

- Cisco Packet Tracer для моделирования и тестирования сети.

- Антивирусное ПО :

- Kaspersky Endpoint Security для защиты рабочих станций и серверов от вирусов и вредоносных программ.

- Серверное ПО :

- Windows Server 2022 для файлового сервера и управления доменом.

- Apache или Nginx для настройки веб-сервера.

- ПО для резервного копирования :

- Veeam Backup & Replication для создания резервных копий данных.

Обоснование : Выбранное ПО соответствует задачам компании по обеспечению безопасности сетей, тестированию и разработке. Kali Linux и Nmap обеспечивают инструменты для пентеста, Wireshark позволяет анализировать трафик, а Kaspersky защищает от угроз. Windows Server 2022 поддерживает управление сетью и хранение данных.

2.3 Обоснование выбора оборудования

Оборудование выбрано исходя из следующих критериев:

- Производительность : Коммутаторы, маршрутизаторы и рабочие станции поддерживают высокую скорость передачи данных (до 1 Гбит/с) и многозадачность.

- Надежность : Используются устройства от проверенных производителей (Cisco, Dell), что минимизирует риски сбоев.

- Безопасность : Оборудование поддерживает функции шифрования, настройки ACL и мониторинга трафика.

- Масштабируемость : Сеть рассчитана на 256 устройств с возможностью расширения.

- Стоимость : Выбраны решения, обеспечивающие оптимальное соотношение цены и качества (например, экранированная витая пара категории 5e вместо оптоволокна).

Пример коммутатора : Cisco Catalyst 9200L с 24 портами Gigabit Ethernet, поддержкой PoE и управлением через Cisco IOS. Он подходит для подключения рабочих станций и точек доступа, обеспечивая высокую пропускную способность и безопасность.

3. Анализ и настройка сети для данной организации

3.1 Разбиение сети на подсети

Для эффективного управления сетью и повышения безопасности сеть разделяется на подсети. Общее количество устройств — 256, включая рабочие станции, серверы, коммутаторы и маршрутизаторы. Используется адресное пространство класса C (например, 192.168.0.0/24), но для поддержки 256 устройств потребуется расширение до /23 (512 адресов).

Разбиение подсетей :

- Подсеть 1 (Офисные рабочие станции) : 192.168.0.0/25 (128 адресов, 126 хостов). Для сотрудников, работающих с документацией и стандартными задачами.

- Подсеть 2 (Отдел тестирования безопасности) : 192.168.0.128/26 (64 адреса, 62 хоста). Для специалистов, использующих Kali Linux и инструменты анализа.

- Подсеть 3 (Серверы) : 192.168.0.192/27 (32 адреса, 30 хостов). Для файлового и веб-сервера.

- Подсеть 4 (Управление и сетевые устройства) : 192.168.0.224/27 (32 адреса, 30 хостов). Для коммутаторов, маршрутизаторов и точек доступа.

Обоснование : Разбиение на подсети снижает широковещательный трафик, повышает безопасность (изоляция критических систем) и упрощает управление.

3.2 Построение логической схемы сети

Логическая схема сети отражает структуру взаимодействия устройств и подсетей. Основные элементы:

- Маршрутизатор (Router) : Cisco ISR 4331, соединяющий подсети и обеспечивающий доступ в Интернет.

- Коммутаторы : 4 коммутатора Cisco Catalyst 9200L, каждый обслуживает одну подсеть.

- Точки доступа : 4 точки доступа Cisco Aironet 2800 для беспроводного подключения.

- Серверы : Файловый сервер (Windows Server 2022) и веб-сервер (Nginx).

- Рабочие станции : Подключены к коммутаторам через кабели витой пары.

Логическая схема :

```

Интернет

|

[Маршрутизатор Cisco ISR 4331]

|

[Коммутатор 1] - [Подсеть 1: Офис]

| [Рабочие станции]

[Коммутатор 2] - [Подсеть 2: Тестирование]

| [Рабочие станции с Kali Linux]

[Коммутатор 3] - [Подсеть 3: Серверы]

| [Файловый сервер, Веб-сервер]

[Коммутатор 4] - [Подсеть 4: Управление]

| [Точки доступа, сетевые устройства]

```

3.3 Настройка адресов и подключение устройств

Настройка IP-адресов :

- Маршрутизатор: 192.168.0.1 (шлюз по умолчанию).

- Подсеть 1: 192.168.0.2–192.168.0.126 (динамическое распределение через DHCP).

- Подсеть 2: 192.168.0.129–192.168.0.190 (статические IP для тестовых станций).

- Подсеть 3: 192.168.0.193–192.168.0.222 (статические IP для серверов).

- Подсеть 4: 192.168.0.225–192.168.0.254 (статические IP для сетевых устройств).

Подключение :

- Рабочие станции подключаются к коммутаторам через кабели витой пары (UTP Cat.5e).

- Коммутаторы соединены с маршрутизатором через порты Gigabit Ethernet.

- Точки доступа подключены к коммутатору 4 и настроены на SSID «FilIndustries\_WiFi» с WPA3-шифрованием.

4. Настройка файлового и веб-серверов

4.1 Настройка веб-сервера

Оборудование : Сервер Dell PowerEdge T140 с Windows Server 2022.

ПО : Nginx 1.24.

Настройка :

1. Установить Nginx через официальный установщик.

2. Настроить конфигурационный файл `nginx.conf`:

```nginx

server {

listen 80;

server\_name filindustries.local;

root /www/data;

index index.html;

}

```

3. Создать директорию `/www/data` и разместить тестовую страницу `index.html`.

4. Настроить фаервол для разрешения трафика на порт 80.

5. Перезапустить службу: `systemctl restart nginx`.

Проверка : Открыть браузер и ввести `http://192.168.0.193` для доступа к веб-странице.

4.2 Настройка файлового сервера

Оборудование : Тот же сервер Dell PowerEdge T140.

ПО : Windows Server 2022 с ролью «Файловый сервер».

Настройка :

1. Установить роль «Файловые службы и службы хранения» через Server Manager.

2. Создать общую папку `SharedDocs` на диске D:.

3. Настроить права доступа:

- Полный доступ для группы «Администраторы».

- Чтение/запись для группы «Сотрудники».

4. Настроить SMB-протокол для доступа к папке по пути `\\192.168.0.193\SharedDocs`.

5. Включить резервное копирование с помощью Veeam Backup.

Проверка : Подключиться к папке с рабочей станции, введя `\\192.168.0.193\SharedDocs`.

5. Настройка маршрутизаторов, списков доступа, статической маршрутизации

5.1 Настройка ACL

Цель : Ограничить доступ к подсети серверов (192.168.0.192/27) только для подсети управления (192.168.0.224/27).

Оборудование : Маршрутизатор Cisco ISR 4331.

Настройка :

```cisco

access-list 101 permit ip 192.168.0.224 0.0.0.31 192.168.0.192 0.0.0.31

access-list 101 deny ip any 192.168.0.192 0.0.0.31

interface GigabitEthernet0/0/1

ip access-group 101 in

```

Объяснение : ACL 101 разрешает трафик от подсети управления к серверам и блокирует доступ для остальных.

5.2 Настройка статической маршрутизации

Цель : Обеспечить маршрутизацию между подсетями.

Настройка :

```cisco

ip route 192.168.0.0 255.255.255.0 GigabitEthernet0/0/0

ip route 0.0.0.0 0.0.0.0 203.0.113.1

```

Объяснение : Первый маршрут направляет трафик внутри сети, второй — в Интернет через внешний шлюз (203.0.113.1).

6. Построение физической модели сети

Физическая модель сети описывает размещение оборудования в здании компании (168 м × 107 м, площадь 18 000 м², два этажа).

Размещение :

- Первый этаж :

- Коммутатор 1 (офисные станции): серверная комната, стойка 1.

- Коммутатор 2 (тестирование): лаборатория безопасности, стойка 2.

- Точки доступа: 2 единицы, установлены в холле и переговорной.

- Второй этаж :

- Коммутатор 3 (серверы): серверная комната, стойка 3.

- Коммутатор 4 (управление): комната администраторов, стойка 4.

- Точки доступа: 2 единицы, установлены в офисе и зоне отдыха.

- Маршрутизатор : Серверная комната, стойка 1, соединен с коммутаторами через кабели UTP Cat.5e.

- Кабельная система : Экранированная витая пара BION BAUI-2151 (Cat.5e) проложена через кабель-каналы в стенах и потолке.

Схема (упрощенное описание):

```

[Интернет] - [Маршрутизатор (Серверная)]

| |

[Коммутатор 1] - [Коммутатор 3]

| |

[Рабочие станции] [Серверы]

| |

[Коммутатор 2] - [Коммутатор 4]

| |

[Тестовые станции] [Точки доступа]

```

Меры безопасности :

- Серверная комната оснащена системой контроля доступа и охлаждения.

- Кабели защищены от физических повреждений кабель-каналами.

- Электропитание обеспечено ИБП (APC Smart-UPS 1500).

Заключение

В рамках курсового проекта была спроектирована локальная вычислительная сеть для ООО «Fil Industries», занимающейся обеспечением безопасности компьютерных сетей. Выполнены следующие задачи:

- Проанализированы потребности компании и план здания.

- Выбрана топология «кольцо» и технология Token Ring для надежной передачи данных.

- Подобрано оборудование (коммутаторы Cisco, маршрутизаторы, рабочие станции Dell) и кабельная среда (UTP Cat.5e).

- Спроектированы логическая и физическая схемы сети.

- Настроены подсети, серверы, ACL и статическая маршрутизация.

- Обеспечена безопасность сети через WPA3, ACL и антивирусное ПО.

Сеть рассчитана на 256 устройств, соответствует требованиям СанПиН и обеспечивает высокую производительность, безопасность и масштабируемость. Проект может быть использован как основа для реального внедрения сети в организации.

Список сокращенных слов

- ACL — Access Control List (список контроля доступа).

- DHCP — Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста).

- OSI — Open Systems Interconnection (модель взаимодействия открытых систем).

- POE — Power over Ethernet (питание по Ethernet).

- SMB — Server Message Block (протокол обмена данными).

- SSID — Service Set Identifier (идентификатор беспроводной сети).

- UTP — Unshielded Twisted Pair (неэкранированная витая пара).

- WPA — Wi-Fi Protected Access (защищенный доступ Wi-Fi).

Список использованных источников

1. Олифер В.Г., Олифер Н.А.

Рисунок 1

Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Питер, 2020.

2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. — М.: Питер, 2019.

3. Cisco Networking Academy. CCNA Routing and Switching. — Cisco Press, 2022.

4. СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы.

5. Официальный сайт Cisco: https://www.cisco.com

6. Документация Nginx: https://nginx.org

7. Стандарты IEEE 802: https://www.ieee802.org