Содержание

[Введение 4](#_Toc198725025)

[1. Аналитический раздел 5](#_Toc198725026)

[1.1 Требования к сети веб-офиса 5](#_Toc198725027)

[1.2 Анализ и выявление недостатков сетевых решений 6](#_Toc198725028)

[1.3 Постановка задачи и формирование требований сети 8](#_Toc198725029)

[2. Конструкторский раздел 10](#_Toc198725030)

[2.1 Построение логической схемы сети 10](#_Toc198725031)

[2.2 Построение физической схемы сети 13](#_Toc198725032)

[2.3 Выбор аппаратного и программного обеспечения 15](#_Toc198725033)

[2.4 Проведение настройки сетевой инфраструктуры 18](#_Toc198725034)

[2.5 Расчет технических характеристик 21](#_Toc198725035)

[2.6 Алгоритмы работы сети 22](#_Toc198725036)

[Заключение 25](#_Toc198725037)

[Список источников и литературы 26](#_Toc198725038)

# Введение

В современную цифровую эпоху локальная вычислительная сеть (ЛВС) является критически важным элементом IT-инфраструктуры для компаний, занимающихся веб-разработкой. Специфика работы веб-студий, включающая обработку больших объемов данных, требования к низкой задержке, активное использование облачных сервисов и постоянный доступ к Интернету, предъявляет высокие требования к производительности и надежности сети. Более того, развитие технологий, возрастающие киберугрозы и переход к гибридным формам работы делают вопросы проектирования, безопасности и гибкости сети особенно актуальными. Неоптимальная или устаревшая сеть может серьезно снизить продуктивность и создать угрозы безопасности.

Данная работа посвящена проектированию и настройке локальной сети для офиса веб-разработки с учетом этих факторов. Для достижения цели поставлены следующие задачи:

1. Проанализировать современные требования к ЛВС и выявить основные проблемы.
2. Выполнить сравнительный анализ существующих типовых решений.
3. Сформулировать технические требования к проектируемой сети.
4. Разработать логическую схему сети.
5. Разработать физическую схему сети.
6. Обосновать выбор аппаратного и программного обеспечения.
7. Описать основные шаги по настройке ключевых элементов сети.
8. Произвести расчеты технических характеристик сети.

# 1. Аналитический раздел

## 1.1 Требования к сети веб-офиса

Специфика веб-разработки требует от локальной сети (ЛВС) особой производительности, надежности и безопасности. Это напрямую влияет на эффективность работы, сроки проектов и защиту данных. На основе типовых задач веб-разработки формулируются следующие ключевые требования к ЛВС:

1. Производительность и пропускная способность:
   * Высокоскоростная внутренняя сеть (LAN): Необходим Gigabit Ethernet (1000 Мбит/с) для рабочих станций. Для серверов (файловых, баз данных, контроля версий, тестовых) требуется 1 Гбит/с с возможностью агрегации или 10 Гбит/с для обработки высоких нагрузок.
   * Быстрый и стабильный доступ в Интернет: Требуется надежный канал 500 Мбит/с+, оптимально 1 Гбит/с+. Важны низкая задержка (latency) и минимальные потери пакетов. Критически необходим резервный интернет-канал, желательно от другого провайдера.
   * Низкая задержка (Latency): Архитектура сети должна минимизировать задержки, особенно при доступе к локальным серверам и тестовым средам. Задержка внутри VLAN не должна превышать 1-2 мс.
2. Надежность и отказоустойчивость:
   * + Надежное сетевое оборудование корпоративного класса.
     + Резервирование критически важных узлов (коммутаторы, шлюзы).
     + Резервирование интернет-канала.
     + Системы бесперебойного питания (ИБП) для всего активного оборудования.
3. Безопасность:
   * + Защита периметра: Межсетевой экран нового поколения (NGFW) с функциями IDS/IPS, контроля приложений.
     + Сегментация сети: Логическое разделение сети на VLAN (рабочие станции, серверы, гостевой Wi-Fi и т.д.) со строгими правилами доступа между ними.
     + Защита беспроводной сети: Использование WPA3/WPA2-Enterprise (802.1X) для корпоративной сети и изолированной гостевой сети.
     + Безопасный удаленный доступ: Доступ только через VPN-соединения (IPsec, OpenVPN и др.) с обязательной многофакторной аутентификацией (MFA).
     + Контроль доступа: Принцип минимальных привилегий, доступ на основе ролей, желательно с интеграцией со службой каталогов (Active Directory, LDAP).
     + Защита от вредоносного ПО: Использование антивирусных решений и функций NGFW.
4. Масштабируемость и гибкость:
   * Возможность легкого расширения: Архитектура сети (например, иерархическая), модульное/стекируемое оборудование должны позволять просто добавлять рабочие места и серверы. Необходимо заложить запас портов (15-25%). Структурированная кабельная система (СКС) должна быть не ниже Категории 6/6A и иметь запас портов для будущего расширения и увеличения скоростей.

## 1.2 Анализ и выявление недостатков сетевых решений

На основе требований к ЛВС офиса веб-разработки, необходимо рассмотреть существующие подходы к построению сетей. Анализ их преимуществ и недостатков поможет выбрать оптимальное решение, избежав типичных ошибок.

Современные офисные сети строятся с использованием различных технологий и топологий. Рассмотрим основные подходы:

1. Классическая проводная сеть (Ethernet):

* Описание: Технология Ethernet и структурированная кабельная система (СКС). Устройства (ПК, серверы) подключаются кабелем (витая пара) к коммутаторам, которые связаны с центральным оборудованием.
* Преимущества: Высокая и стабильная скорость (1 Гбит/с+), низкая задержка, высокая надежность (устойчивость к радиопомехам), повышенная безопасность (контроль физического доступа).
* Применение: Основное подключение для стационарных рабочих мест, серверов, критически важной инфраструктуры, где важны максимальная производительность и стабильность.

1. Беспроводная сеть (Wi-Fi):

* Описание: Использует радиоволны (стандарты IEEE 802.11). Точки доступа (AP) подключаются к проводной сети (часто с питанием по PoE) и обеспечивают беспроводной доступ. В корпоративных сетях используется централизованное управление точками доступа.
* Преимущества: Мобильность пользователей, гибкость развертывания, удобство для мобильных и гостевых устройств, поддержка BYOD (Bring Your Own Device).
* Применение: Подключение мобильных устройств, доступ в зонах отдыха/переговорных, гостевые сети.

1. Гибридные сети:

* Описание: Сочетает проводную (Ethernet) и беспроводную (Wi-Fi) сети. Ethernet используется для стационарных устройств и серверов, требующих высокой производительности и надежности, Wi-Fi — для мобильности и гостевого доступа.
* Преимущества: Объединяет высокую производительность и надежность проводной сети с гибкостью и мобильностью беспроводной. Позволяет удовлетворить разнообразные потребности пользователей и устройств.

Таблица 1 - Сравнение проводных, беспроводных (Wi‑Fi) и гибридных сетей

|  |  |  |  |
| --- | --- | --- | --- |
| Характеристика | Проводная сеть | Беспроводная сеть (Wi‑Fi) | Гибридная сеть |
| Инфраструктура | Кабели (витая пара, оптоволокно) | Радиоволны, без кабелей | Сочетание проводных и Wi‑Fi соединений |
| Производительность | Высокая скорость и стабильность | Скорость зависит от стандарта и помех | Оптимизация за счет разделения нагрузки |
| Надежность | Минимальные перебои | Может быть чувствительна к помехам | Резервирование критичных сегментов провода |
| Гибкость | Фиксированная, сложна в изменении топологии | Высокая мобильность | Баланс между стабильностью и мобильностью |
| Безопасность | Сложнее перехват данных | Требует шифрования и аутентификации | Усиленная, с централизованным управлением |

## 1.3 Постановка задачи и формирование требований сети

На основе анализа специфики офиса веб-разработки и обзора существующих сетевых решений сформулирована постановка задачи и детальные требования к проектируемой ЛВС.

Цель проектирования:

Создать современную, производительную, безопасную, отказоустойчивую и масштабируемую гибридную (проводную + беспроводную) локальную сеть для офиса веб-разработки, соответствующую текущим и будущим потребностям компании.

Для достижения этой цели формируются следующие ключевые требования к инфраструктуре сети:

1. Безопасность (Приоритет):
   * Многоуровневая защита: Комплексный подход (NGFW с IDS/IPS, защита конечных точек, сегментация).
   * Строгая сегментация: Логическое разделение сети на VLAN с гранулярными правилами доступа (ACLs).
   * Защищенный беспроводной доступ: WPA3-Enterprise (802.1X/RADIUS) для корпоративной сети, изолированная гостевая сеть (WPA2/WPA3-Personal).
   * Безопасный удаленный доступ: Доступ только через защищенные VPN с обязательной многофакторной аутентификацией (MFA).
   * Контроль доступа: Принцип минимальных привилегий (RBAC).
2. Производительность:
   * Высокоскоростная проводная сеть: Gigabit Ethernet (1 Гбит/с) для рабочих станций; 1/10 Гбит/с (с LACP) для серверов и аплинков.

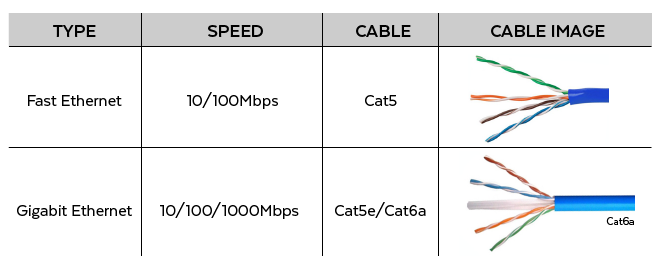


Рисунок 1 – Сравнение gigabit ethernet и fast ethernet

* + Производительный Wi-Fi: Использование стандарта Wi-Fi 6 (802.11ax).
  + Быстрый и стабильный Интернет: Канал ≥ 500 Мбит/с (оптимально 1 Гбит/с+) с низкими задержками.
  + Низкая внутренняя задержка: Минимизация задержек (< 2 мс).
  + Качество обслуживания (QoS): Приоритизация критичного трафика (VoIP, видео).

1. Отказоустойчивость:
   * Резервирование ключевых узлов: Стекирование коммутаторов или протоколы резервирования шлюза (VRRP/HSRP).
   * Резервирование каналов связи: Обязательный резервный интернет-канал от другого провайдера; резервирование внутренних соединений (LACP).
   * Бесперебойное питание: Обеспечение активного сетевого оборудования источниками ИБП.
2. Масштабируемость:
   * Гибкая архитектура: Иерархическая модель (ядро-распределение-доступ).
   * Запас ресурсов: Запас портов на коммутаторах (~20-25%), запас производительности оборудования, наличие портов SFP/SFP+.
   * Современная СКС: Категория 6/6А с запасом портов.
3. Сегментация сети (как часть безопасности и управляемости):
   * Логическое разделение: Отдельные VLAN для рабочих станций (по группам), серверов (Production, Dev/Test), управления сетью, гостевого Wi-Fi и др.
   * Контролируемое взаимодействие: Настройка правил на МЭ/маршрутизаторе для разрешения только необходимого трафика между VLAN.

Сформулированные требования являются основой для проектирования логической и физической структуры сети, выбора оборудования и конфигурации

# 2. Конструкторский раздел

## 2.1 Построение логической схемы сети

Логическая схема сети определяет взаимодействие устройств, IP-адресацию, организацию виртуальных сетей (VLAN) и маршрутизацию. Она формирует основу производительной, безопасной и управляемой сети, независимо от физической инфраструктуры.

Определение топологии сети

Выбор топологии влияет на надежность, масштабируемость и управляемость сети.

* Непригодные для современных офисов: Шина (Bus), Кольцо (Ring) из-за низкой отказоустойчивости и производительности.
* Стандарт для ЛВС: Звезда (Star), где устройства подключены к центральному коммутатору. Надежна, проста в расширении и диагностике.
* Для средних/крупных сетей: Расширенная звезда / Иерархическая модель (Extended Star / Hierarchical). Обеспечивает высокую масштабируемость и управляемость, часто строится по двухуровневой модели (Свернутое ядро/Распределение - Доступ).

Для офиса веб-разработки наиболее подходящей является иерархическая топология типа "звезда". В условиях офиса среднего размера рекомендуется двухуровневая модель:

* Уровень доступа (Access): Коммутаторы для прямого подключения конечных устройств (ПК, AP).
* Уровень ядра/распределения (Core/Distribution): Высокопроизводительный коммутатор (или стек), агрегирующий трафик, обеспечивающий маршрутизацию между VLAN и подключение к внешним сетям (Интернет).

Такая топология повышает надежность (изоляция сбоев), упрощает масштабирование и управление.

Логическая сегментация сети (VLAN)

Для повышения безопасности, управления трафиком и производительности сеть разделяется на логические сегменты – функциональные зоны, реализуемые через технологию VLAN (IEEE 802.1Q). Каждая VLAN – изолированный широковещательный домен. Взаимодействие между VLAN происходит на сетевом уровне (L3) через маршрутизатор или L3-коммутатор.

Для офиса веб-разработки предлагается выделить следующие функциональные зоны (VLAN) с соответствующими IP-подсетями:

1. VLAN 10: Серверная зона (Servers)
   * Назначение: Критически важные серверы (БД, репозитории, CI/CD, файлы).
   * Требования: Максимальная безопасность, ограниченный доступ, высокая производительность.
   * IP-подсеть: 192.168.10.0/24
2. VLAN 20: Рабочие станции сотрудников (Workstations)
   * Назначение: Компьютеры разработчиков, дизайнеров, менеджеров.
   * Требования: Выборочный доступ к серверам, доступ в Интернет.
   * IP-подсеть: 192.168.20.0/23
3. VLAN 30: Зона разработки и тестирования (Dev/Test)
   * Назначение: Изолированная среда для развертывания и тестирования.
   * Требования: Изоляция от основных сетей, контролируемый доступ.
   * IP-подсеть: 192.168.30.0/24
4. VLAN 40: Гостевая Wi-Fi сеть (Guest Wi-Fi)
   * Назначение: Доступ в Интернет для посетителей.
   * Требования: Полная изоляция от внутренней сети, доступ только в Интернет.
   * IP-подсеть: 192.168.40.0/24

Контролируемое взаимодействие между этими VLAN настраивается на межсетевом экране или маршрутизаторе уровня 3 с помощью правил доступа (ACL).

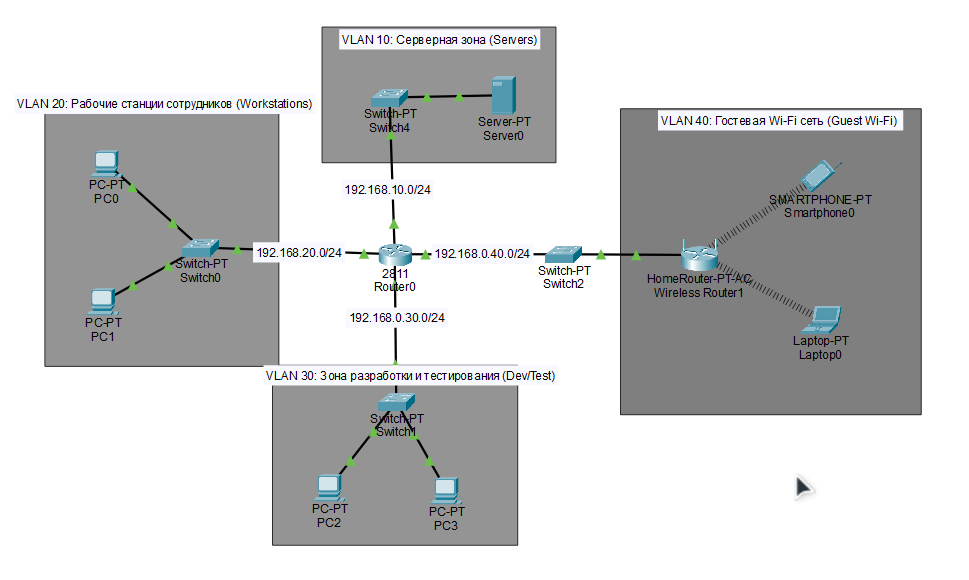


Рисунок 2 - Логичиская схема

## 2.2 Построение физической схемы сети

Физическая схема сети определяет реальное размещение оборудования и кабельной инфраструктуры. Она показывает, где устанавливаются серверы, коммутаторы, точки доступа и как прокладываются кабели. Правильное физическое проектирование критически важно для производительности, надежности и обслуживания сети.

Размещение оборудования

Эффективное размещение обеспечивает стабильность и удобство эксплуатации.

1. Серверная комната (или коммуникационный шкаф):
   * Назначение: Центральный узел сети. Размещаются: маршрутизатор/межсетевой экран, коммутаторы ядра/распределения, основные серверы, патч-панели.
   * Требования: Отдельное, запираемое помещение с ограниченным доступом. Обязательны: адекватное охлаждение/вентиляция, надежное электропитание (с ИБП), достаточное пространство для стоек и обслуживания.
2. Коммутаторы уровня доступа:
   * Размещение: Близко к группам пользователей/устройствам (до 90м). В небольших офисах – в серверной, в крупных – в этажных шкафах.
   * Подключение: Соединяются с коммутатором ядра/распределения (медью или оптоволокном).
   * Требование: Поддержка PoE для точек доступа Wi-Fi и IP-телефонов.
3. Точки доступа Wi-Fi (AP):
   * Размещение: Определяется по результатам радиопланирования для обеспечения наилучшего покрытия (обычно на потолке/стенах).
   * Питание: Подается по PoE от коммутаторов доступа.
   * Подключение: Кабелем витой пары к коммутатору доступа.
4. Рабочие станции и периферия:
   * Размещение: На рабочих местах.
   * Подключение: Каждое стационарное место должно иметь сетевую розетку RJ-45, подключенную к патч-панели.

Оптимизация кабельной инфраструктуры (СКС)

Структурированная кабельная система (СКС) – это основа физической сети, обеспечивающая надежность и гибкость.

1. Выбор типа кабеля:
   * Горизонтальная подсистема (от розетки до патч-панели): Минимум Категория 6 (Cat 6). Для поддержки 10 Гбит/с на 100м рекомендуется Категория 6A (Cat 6A). Cat 5e для новых инсталляций нежелателен.
   * Магистральная подсистема (между коммутационными узлами/этажами): Предпочтительно оптоволокно (многомодовое или одномодовое) для высоких скоростей и больших расстояний. Медь Cat 6A или DAC для коротких связей.
2. Организация СКС:
   * Топология: Звезда, все кабели сходятся в центральный узел.
   * Патч-панели: Терминирование всех горизонтальных кабелей для гибкости подключений к оборудованию.
   * Кабельные трассы: Прокладка в лотках/коробах для защиты и организации. Избегать силовых кабелей.
   * Кабель-менеджмент: Органайзеры в стойках для аккуратности и вентиляции.
   * Маркировка: Четкая маркировка всех элементов (кабель, порт, розетка) для администрирования.
   * Стандарты: Монтаж по международным/национальным стандартам (ISO/IEC 11801, TIA/EIA-568).

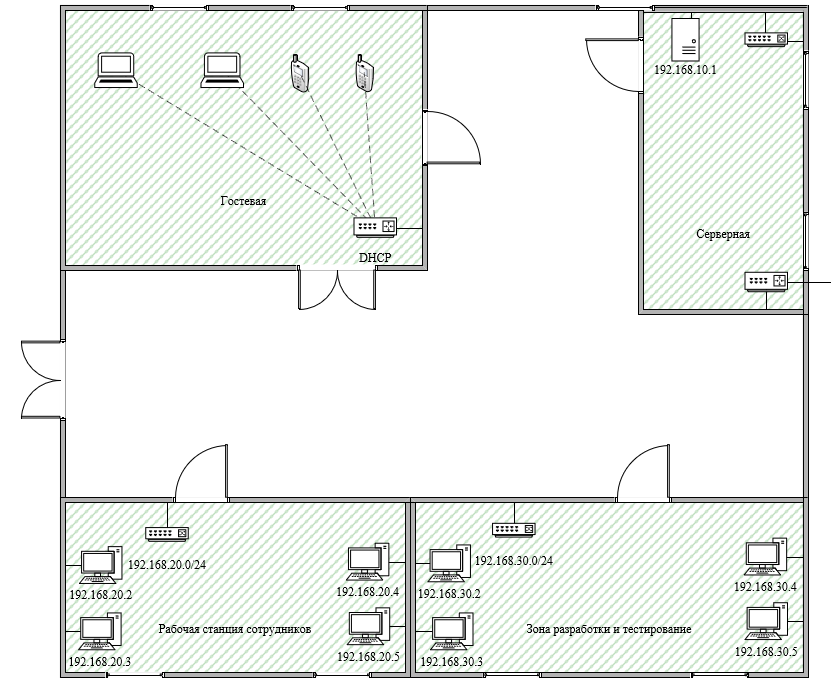


Рисунок 3 – Физичиская схема

## 2.3 Выбор аппаратного и программного обеспечения

1. Межсетевой экран: FortiGate 80F
   * Обоснование: Обеспечивает гигабитную NGFW-производительность и надежный VPN для защиты периметра и удаленного доступа.



Рисунок 4 - FortiGate 80F

1. Коммутатор Ядра/Распределения: Стек из 2-х Cisco Catalyst C9300L-48P-4G
   * Обоснование: Предоставляет отказоустойчивость (стек), L3-маршрутизацию между VLAN, 10G аплинки и PoE+ для гибкости подключения.

**

Рисунок 5 - Cisco Catalyst C9300L-48P-4G

1. Коммутаторы Доступа: Cisco Catalyst C9200L-24P-4G
   * Обоснование: Предлагают гигабитные порты доступа с PoE+ для питания точек доступа и телефонов, базовую безопасность и подключение к ядру по SFP.

**

Рисунок 6 - Cisco Catalyst C9200L-24P-4G

1. Точки Доступа Wi-Fi: Ubiquiti UniFi 6 Pro (U6-Pro)
   * Обоснование: Поддерживают современный стандарт Wi-Fi 6 для высокой производительности и плотности клиентов по разумной цене.



Рисунок 7 - Ubiquiti UniFi 6 Pro

1. Сервер: Dell PowerEdge R650 (1 или 2 шт.)
   * Обоснование: Надежная и производительная платформа для виртуализации всех необходимых сервисов (веб, БД, Git, CI/CD, AD и т.д.).

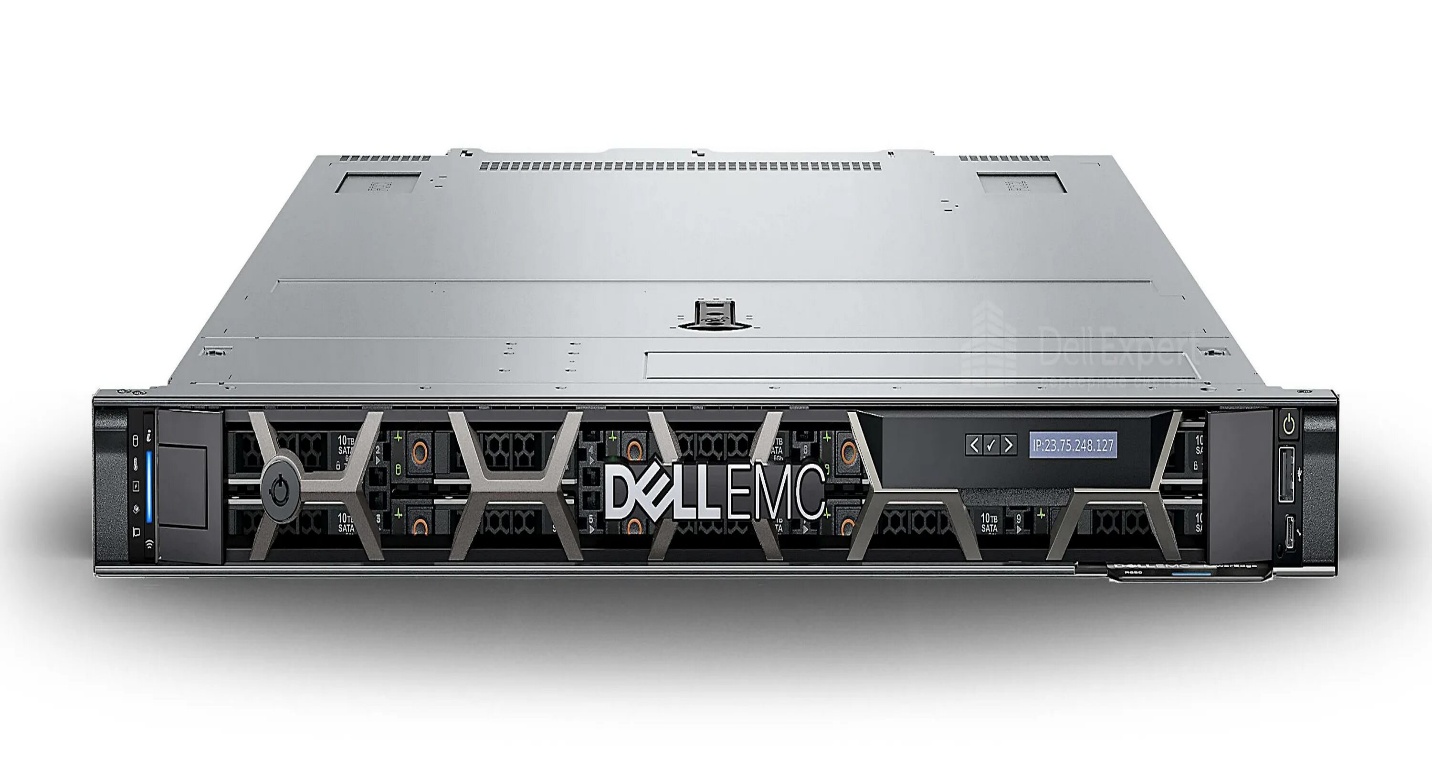


Рисунок 8 - Dell PowerEdge R650

Программное обеспечение:

Для реализации функционала сети и обеспечения работы сервисов выбрано следующее программное обеспечение:

1. ОС Серверов: Ubuntu Server 22.04 LTS и Windows Server 2022 Standard.
2. Виртуализация: VMware vSphere Essentials Kit.
3. Система Мониторинга: Zabbix.
4. Endpoint Security: Microsoft Defender for Business.
5. Резервное Копирование: Veeam Backup & Replication Community Edition.
6. Служба Каталогов / RADIUS: Microsoft Active Directory / NPS на Windows Server.

## 2.4 Проведение настройки сетевой инфраструктуры

После выбора оборудования и разработки логических/физических схем выполняется настройка сетевых устройств для реализации запланированного функционала и требований безопасности. Этот этап включает конфигурацию сегментации сети (VLAN), беспроводного доступа и базовых механизмов безопасности.

Настройка сегментации сети (VLAN, подсети, маршрутизация)

1. Создание VLAN**:** На коммутаторах ядра/распределения (Cisco Catalyst 9300L) и доступа (Cisco Catalyst 9200L) создаются VLANы: 10 (Серверы), 20 (Рабочие станции), 30 (Dev/Test), 40 (Гости).

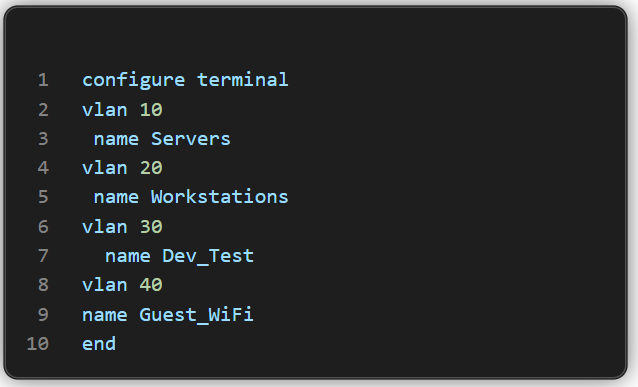


Рисунок 9 - Настройка сегментации сети VLAN

1. Настройка портов коммутаторов:
   * Access Ports: Порты для конечных устройств привязываются к соответствующей VLAN (например, порт ПК сотрудника – VLAN 20).

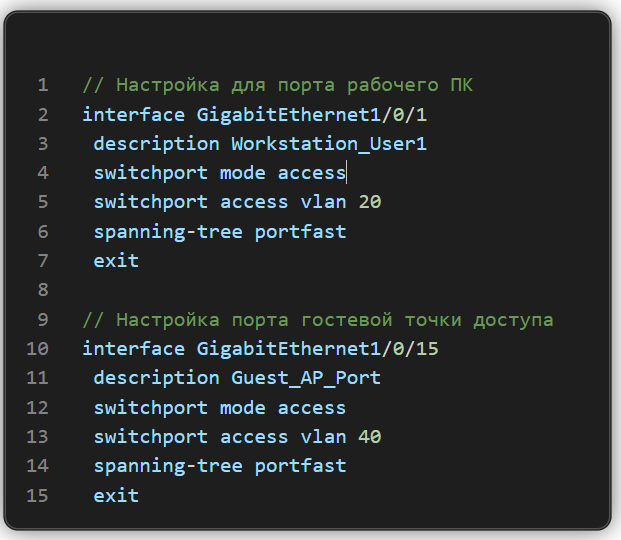


Рисунок 10 - Настройка Access Port

* + Trunk Ports: Порты между коммутаторами и порт к FortiGate настраиваются как транки, разрешающие прохождение всех используемых VLAN (10, 20, 30, 40).

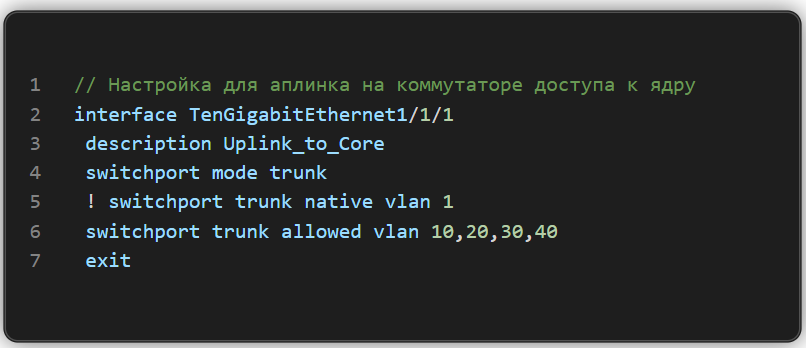


Рисунок 11 - Настройка Trunk Ports

1. Настройка маршрутизации между VLAN: Выполняется на L3-коммутаторе (стек Catalyst 9300L).
   * Создаются виртуальные интерфейсы (SVI) для внутренних VLAN (10, 20, 30) с назначением IP-адресов (шлюзов по умолчанию).
   * Шлюз и DHCP для гостевой VLAN 40 настраиваются на FortiGate для полной изоляции.

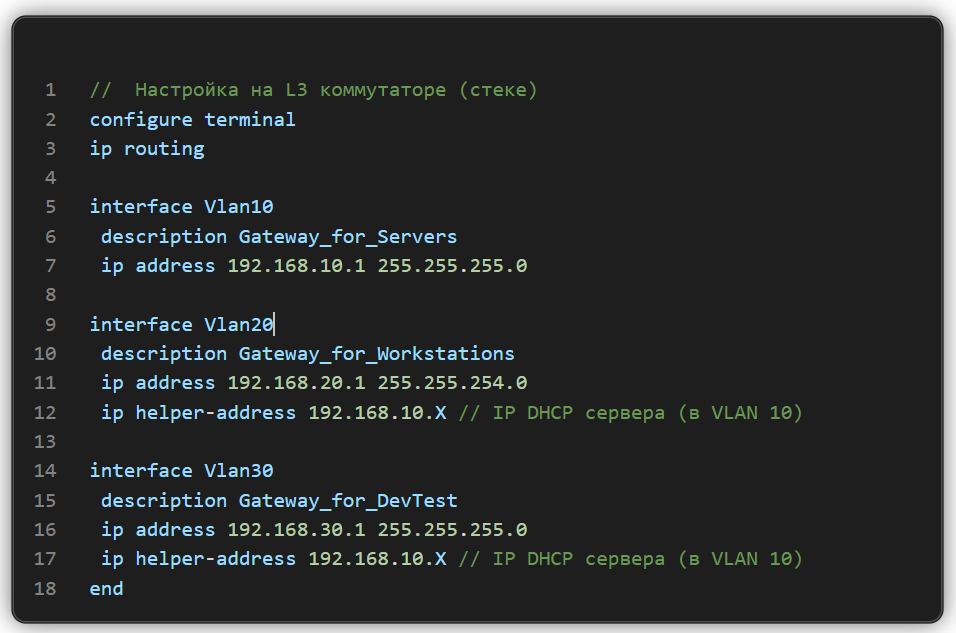


Рисунок 12 - Настройка маршрутизации между VLAN

Настройка сегментации сети (VLAN, подсети, маршрутизация)

1. Создание VLAN: На коммутаторах ядра/распределения (Cisco Catalyst 9300L) и доступа (Cisco Catalyst 9200L) создаются VLANы: 10 (Серверы), 20 (Рабочие станции), 30 (Dev/Test), 40 (Гости).
2. Настройка портов коммутаторов:
   * Access Ports: Порты для конечных устройств привязываются к соответствующей VLAN (например, порт ПК сотрудника – VLAN 20).
   * Trunk Ports: Порты между коммутаторами и порт к FortiGate настраиваются как транки, разрешающие прохождение всех используемых VLAN (10, 20, 30, 40).
3. Настройка маршрутизации между VLAN: Выполняется на L3-коммутаторе (стек Catalyst 9300L).
   * Создаются виртуальные интерфейсы (SVI) для внутренних VLAN (10, 20, 30) с назначением IP-адресов (шлюзов по умолчанию).
   * Шлюз и DHCP для гостевой VLAN 40 настраиваются на FortiGate для полной изоляции.

Настройка беспроводной сети (Гостевой Wi-Fi)

Настройка выполняется через контроллер UniFi Network Application.

1. Создание Беспроводной Сети (SSID):
   * Создается SSID "WebDev-Guest", привязанный к VLAN 40.
   * Включается режим гостевой сети (Guest Policy), обеспечивающий изоляцию клиентов на уровне L2.
2. Конфигурация Точек Доступа (UniFi AP):
   * Точки доступа регистрируются на контроллере.
   * SSID "WebDev-Guest" назначается на точки доступа с указанием VLAN 40.

Настройка сетевой безопасности (FortiGate 80F)

1. Настройка интерфейсов: Конфигурируются WAN-интерфейс, внутренний интерфейс (подключенный к L3-коммутатору) и VLAN-интерфейс для VLAN 40 (с назначенным IP 192.168.40.1/24 и включенным DHCP).
2. Настройка Политик Межсетевого Экрана: Определяются правила трафика между сегментами:
   * Доступ в Интернет для VLAN 20 и VLAN 30 (с применением профилей безопасности).
   * Доступ в Интернет для VLAN 40 (только WAN-доступ, с веб-фильтром и возможным ограничением скорости).
   * Доступ к серверам (VLAN 10) из VLAN 20 и VLAN 30 (только необходимый трафик, с применением IPS).
   * Явное правило ЗАПРЕТА трафика из VLAN 40 во все внутренние VLAN (10, 20, 30), размещенное выше разрешающих правил для гостей.

## 2.5 Расчет технических характеристик

На этапе проектирования проводится оценка пропускной способности и нагрузки, планирование резервных решений и расчет энергопотребления.

1. Оценка пропускной способности и нагрузки:
   * Пропускная способность: Сеть спроектирована с доступом 1 Гбит/с (проводной) и Wi-Fi 6 (беспроводной), ядром/аплинками 10 Гбит/с и интернет-каналом 1 Гбит/с.
   * Ожидаемая нагрузка: Интенсивный трафик веб-разработки (Git, CI/CD, ВМ, БД), передача медиа, облачные сервисы, гостевой доступ.
   * Вывод: Выбранная архитектура (1/10 Гбит/с Ethernet, Wi-Fi 6) обеспечивает достаточную пропускную способность для текущих и прогнозируемых нагрузок.
2. Планирование резервных решений:
   * Оборудование: Используется стекирование коммутаторов ядра (Cisco StackWise) и резервные БП для критичного оборудования.
   * Каналы: Предусмотрен резервный интернет-канал (управляемый FortiGate) и агрегация каналов (LACP) для важных соединений.
   * Питание: Все активное оборудование в стойке обеспечивается источниками бесперебойного питания (ИБП, например, APC Smart-UPS Online).
   * Цель: Минимизация времени простоя сети.
3. Энергопотребление и теплоотвод:
   * Энергопотребление: Ориентировочная суммарная пиковая мощность оборудования в серверной составляет 2-4 кВт (требует точного расчета).
   * Теплоотвод: Соответствует энергопотреблению (~7000-14000 BTU/час).
   * Требования: Мощность ИБП (например, APC SRT 3000VA ~2700W) должна покрывать нагрузку с запасом. Система кондиционирования серверной должна обеспечивать отвод соответствующего тепла.

## 2.6 Алгоритмы работы сети

Для обеспечения высокой производительности, безопасности и непрерывности работы сети используются следующие алгоритмы и механизмы:

1. Алгоритмы балансировки нагрузки и резервирования каналов:
   * Резервирование интернет-каналов: На межсетевом экране FortiGate настраивается SD-WAN или Link Failover для автоматического переключения на резервный канал при сбое основного или распределения трафика.
   * Агрегация внутренних каналов (LACP): Протокол Link Aggregation Control Protocol объединяет несколько физических портов в один логический канал для увеличения пропускной способности и отказоустойчивости критически важных внутренних соединений (между коммутаторами, к серверам).
2. Алгоритмы сетевой безопасности:
   * Аутентификация пользователей:
     + Гостевой Wi-Fi: WPA2/WPA3-Personal (PSK).
     + VPN (удаленный доступ): Аутентификация через Active Directory/RADIUS с обязательной многофакторной аутентификацией (MFA) на FortiGate.
   * Контроль доступа:
     + Межсетевой экран (FortiGate): Основной инструмент. Политики безопасности (Firewall Policies) с применением профилей (IPS, Web Filter, AV) регулируют трафик между сегментами (VLAN, WAN, VPN).
     + Списки контроля доступа (ACL): Могут применяться на L3-коммутаторе (Catalyst 9300L) для дополнительной фильтрации трафика между внутренними VLAN.
     + Изоляция на уровне коммутатора: Функции Port Security, DHCP Snooping, ARP Inspection для защиты на уровне доступа.
3. Механизмы автоматического восстановления работы при сбоях:
   * Отказоустойчивость ядра: Технология Cisco StackWise обеспечивает автоматическое переключение на резервный коммутатор в стеке при отказе.
   * Предотвращение петель коммутации: Протоколы Spanning Tree (STP, RPVST+, MSTP) блокируют избыточные пути в L2-сети, предотвращая штормы и обеспечивая автоматическое переключение при обрыве основного пути.
   * Резервирование интернет-шлюза: Механизм FortiGate SD-WAN/Link Failover обеспечивает автоматическое переключение на резервный интернет-канал.
   * Бесперебойное питание (ИБП): Источники бесперебойного питания обеспечивают работу оборудования при сбоях электросети.

# Заключение

В рамках данной курсовой работы проведен анализ требований к сети современного офиса веб-разработки и разработан детальный проект локальной вычислительной сети.

1. Выводы по проделанной работе:  
   Проанализированы специфические требования офиса веб-разработки. Обоснована и выбрана иерархическая архитектура сети с логической сегментацией на базе VLAN. Подобраны конкретные модели оборудования от ведущих производителей (Cisco, Fortinet, Ubiquiti) с учетом производительности, безопасности и стоимости. Разработаны физическая и логическая схемы, а также основные этапы настройки.
2. Достижение целей:  
   Основная цель работы – создание проекта производительной, безопасной и отказоустойчивой ЛВС – успешно достигнута. Спроектированное решение отвечает всем заявленным требованиям: обеспечивает высокие скорости (1/10 Гбит/с Ethernet, Wi-Fi 6), реализует многоуровневую безопасность (NGFW, изоляция сегментов), гарантирует непрерывность работы (стекирование, резервирование каналов и питания) и предусматривает потенциал для масштабирования.
3. Перспективы модернизации:  
   Спроектированная сеть является гибкой основой с потенциалом для дальнейшего развития. Основные направления модернизации включают: внедрение контроля доступа на портах (802.1X/NAC), переход на Multi-Gigabit Ethernet, расширение Wi-Fi (включая корпоративный сегмент с WPA3-Enterprise), интеграцию с SIEM-системами для безопасности и использование средств сетевой автоматизации (Ansible).

# Список источников и литературы

* IEEE Std 802.1Q™-2018: IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks. 1-е изд. – New York: IEEE Press, 2018 – 285 с.
* IEEE Std 802.11ax™-2021: IEEE Standard for Information Technology – Enhancements for High-Efficiency WLAN. 1-е изд. – New York: IEEE Press, 2021 – 392 с
* IEEE Std 802.3™-2018: IEEE Standard for Ethernet. 1-е изд. – New York: IEEE Press, 2018 – 34 с.
* RFC 1918: Address Allocation for Private Internets. 1-е изд. – New York: IETF Publications, 1996 – 132 с.
  + Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. 6-е изд. – СПб.: Питер, 2020. – 1008 с.
  + Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – СПб.: Питер, 2019. – 960 с.
  + Ламмл Т. CCNA. Учебное руководство Cisco. – М.: Лори, 2019. - 1184 с.
  + Cisco Catalyst 9300 Series Switches Data Sheet // Cisco Systems. [Электронный ресурс] URL: [https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.html](https://www.google.com/url?sa=E&q=https%3A%2F%2Fwww.cisco.com%2Fc%2Fen%2Fus%2Fproducts%2Fcollateral%2Fswitches%2Fcatalyst-9300-series-switches%2Fdatasheet-c78-738977.html).
  + Fortinet FortiGate 80F Series Data Sheet // Fortinet, Inc. [Электронный ресурс] URL: [https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-80f-series.pdf](https://www.google.com/url?sa=E&q=https%3A%2F%2Fwww.fortinet.com%2Fcontent%2Fdam%2Ffortinet%2Fassets%2Fdata-sheets%2Ffortigate-80f-series.pdf)
  + Ubiquiti UniFi 6 Pro Access Point Datasheet // Ubiquiti Inc. [Электронный ресурс]. URL: <https://dl.ui.com/ds/u6-pro_ds.pdf>
  + Настройка VLAN на коммутаторах Cisco Catalyst // Блог системного администратора [Электронный ресурс] URL: <https://blog.bissquit.com/nastroyka-vlan-na-kommutatorah-cisco-catalyst/>