

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
1 ОБЗОР ЛИТЕРАТУРЫ	5
1.1 Технологии построения локальных сетей	5
1.2 VLAN	6
1.3 Web-сервер	7
1.4 ADSL2+	7
1.5 Способы обеспечения безопасности в отношении учетных записей пользователей	8
2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ	10
3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ	13
3.1 Создание виланов в сети	13
3.2 Обоснование выбора программного обеспечения для пользовательских станций	13
3.3 Обоснование выбора производителя сетевого оборудования	15
3.4 Обоснование выбора активного сетевого оборудования	16
3.5 Расчет качества связи беспроводной сети	19
3.6 Обоснование выбора веб-сервер	21
3.7 Обоснование выбора сетевого шкафа	22
3.8 Обоснование выбора пользовательских станций	22
3.9 Обоснование выбора принтера и сканера	24
3.10 Обоснование выбора IP-телефонов	24
3.11 Схема адресация	25
3.13 Описание настройки компонентов локальной сети	29
3.14 Обоснование выбора пассивного оборудования	39
4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ	40
ЗАКЛЮЧЕНИЕ	41
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	42
ПРИЛОЖЕНИЕ А	43
ПРИЛОЖЕНИЕ Б	44
ПРИЛОЖЕНИЕ В	45
ПРИЛОЖЕНИЕ Г	46
ПРИЛОЖЕНИЕ Д	47
ПРИЛОЖЕНИЕ Е	48

ВВЕДЕНИЕ

Современные образовательные учреждения активно используют информационные технологии для повышения качества образовательного процесса, организации работы сотрудников и взаимодействия участников учебной деятельности. Одной из важнейших задач в этом направлении является создание локальной вычислительной сети, которая будет объединять различные устройства, обеспечивать их взаимодействие, а также предоставлять пользователям доступ к учебным и административным ресурсам.

Целью данного курсового проекта является разработка и проектирование локальной вычислительной сети для кафедры государственного университета, где проводится обучение основам программирования. Разрабатываемая сеть должна быть надёжной, производительной, безопасной и отвечать потребностям пользователей, включая преподавателей и студентов. Она должна поддерживать как стационарные рабочие места, так и мобильные устройства, обеспечивать доступ к учебным материалам и программным средствам, а также защищать конфиденциальные данные от несанкционированного доступа.

Создание такой сети требует учёта множества факторов, включая организацию рабочего пространства, расчёт необходимой пропускной способности, выбор оборудования, совместимого с современными стандартами, и обеспечение масштабируемости. Важным аспектом является внедрение современных решений для защиты информации, что особенно актуально в образовательных учреждениях, где хранится большое количество персональных данных и другой важной информации.

Кроме того, проектируемая сеть должна быть адаптирована для поддержки образовательных процессов, включая доступ к специализированным программным продуктам и платформам для обучения программированию. Это позволит повысить эффективность учебного процесса, предоставляя студентам возможность работать с современными инструментами, необходимыми для формирования их профессиональных навыков.

Проект направлен на создание инфраструктуры, которая будет способствовать развитию цифровой образовательной среды кафедры, улучшать условия для работы преподавателей и студентов, а также обеспечивать возможность дальнейшего расширения и модернизации сети.

1 ОБЗОР ЛИТЕРАТУРЫ

Обзор литературы – важная часть курсового проекта, которая помогает оценить существующие решения и выбрать оптимальные технологии для реализации. Вопросы организации сетевых сервисов, подключения к интернету и выбора сетевого оборудования имеют важное значение при проектировании компьютерных сетей, особенно в образовательных учреждениях, где необходимо поддерживать как внутренние, так и внешние сервисы с высоким уровнем надежности и безопасности.

1.1 Технологии построения локальных сетей

Локальные сети в настоящее время принято строить на основании технологии коммутируемого Ethernet. Стремятся минимизировать число используемых концентраторов и использовать преимущественно коммутаторы. В коммутаторе между приёмником и передатчиком на время соединения образуется виртуальный канал точка-точка. Такая сеть может быть рассмотрена как совокупность независимых пар приёмник-передатчик, каждая из которых использует всю полосу пропускания. Коммутатор позволяет осуществлять параллельную передачу информации. Коммутация уменьшает вероятность переполнения в сетях Ethernet.

Для отправки фрейма через коммутатор используются два метода:

1 Отправка с промежуточным хранением. Пакет должен быть принят полностью до того как будет начата его отправка.

2 Сквозной метод. Коммутатор принимает начало пакета, считывает в нём адрес пункта назначения и начинает отправлять пакет ещё до его полного получения.

Если коммутатору необходимо передать пакет на какой-то выходной порт, и этот порт занят, то пакет помещается в буферную память. Это позволяет согласовать скорости передатчиков и приёмников пакетов.

Ethernet-коммутатор узнаёт MAC адреса устройств в сети путём чтения адресов источников в принимаемых пакетах. Коммутатор запоминает в своих внутренних таблицах информацию на какие порты и с каких MAC адресов приходят пакеты.

Используя таблицу адресов и содержащийся в пришедшем пакете адрес получателя, коммутатор организует виртуальное соединение порта отправителя с портом получателя и передает пакет через это соединение.

Виртуальное соединение между портами коммутатора сохраняется в течение передачи одного пакета, т.е. для каждого пакета виртуальное соединение организуется заново на основе содержащегося в этом пакете адреса получателя.

Поскольку пакет передается только в тот порт, к которому подключен адресат, остальные устройства подключенные к коммутатору, не получают этот пакет.

Коммутаторы можно соединять друг с другом. При этом группа попарно прямо либо косвенно связанных коммутаторов образует один логический коммутатор с теоретически произвольным числом портов. То есть коммутаторы позволяют создавать теоретически сколь угодно большую локальную сеть. Правильное соединение коммутаторов, то есть выбор топологии сети составляет одну из важнейших задач проектирования локальных сетей.

Локальная сеть, созданная с помощью одних только коммутаторов представляет один домен широковещания. Уменьшить домен широковещания можно, физически разделив локальную сеть на независимые подсети (независимые группы попарно связанных коммутаторов) и соединить их в единое целое с использованием маршрутизаторов. Такую задачу можно решить только на этапе построения сети, но не в момент её эксплуатации. Здесь на помощь приходят виртуальные локальные сети VLAN (virtual local area network).

В топологии локальных сетей возможны циклы (петли). Например, уже три коммутатора соединённых друг с другом по кругу образуют цикл в топологии. Петли приводят к неоднозначности при определении пути от источника пакетов к приёмнику. Для решения этой серьёзной проблемы был разработан протокол связующего дерева STP (spanning tree protocol).

Для создания топологии связующего дерева существуют специальные фреймы, называемые модулями данных мостового протокола (bridge protocol data units, BPDU). Эти фреймы отправляются и принимаются всеми коммутаторами в сети через равные промежутки времени.

1.2 VLAN

VLAN позволяют логически разбить исходную локальную сеть на несколько независимых локальных сетей без физического обрыва сетевых соединений. Для этого администратор сети должен на каждом коммутаторе назначить, какие его порты относятся к каким VLAN. По умолчанию все порты коммутатора относятся к одной VLAN с номером 1. Максимальное число VLAN в коммутаторе равно общему числу его портов. Правильная разбивка локальной сети на VLAN составляет одну из важнейших задач проектирования.

VLAN ведут себя так же, как и физически разделённые локальные сети. То есть после разбивки сети на VLAN мы получим несколько локальных сетей, которые далее необходимо объединить в единое целое с помощью маршрутизации на третьем сетевом уровне.

Концепция VLAN, помимо решения проблемы с широковещательным трафиком даёт также ряд дополнительных преимуществ: формирование локальных сетей не по месту расположения ближайшего коммутатора, а по принадлежности компьютеров к решению той или иной производственной задачи; создание сети по типу потребляемого вычислительного ресурса и

требуемой серверной услуги (файл-сервер, сервер баз данных). VLAN позволяют вести различную политику безопасности для разных виртуальных сетей; переводить компьютер из одной сети в другую без осуществления физического перемещения или переподключения.

Для обмена информацией о VLAN коммутаторы используют магистральный (транковый) протокол. Для осуществления обмена информацией о VLAN между коммутаторами вы должны создать магистральные порты. Магистральный порт это порт, используемый для передачи информации о VLAN в другие сетевые устройства, присоединенные к этому порту. Обычные порты не рекламируют информацию о VLAN, но любой порт может быть настроен для приема/передачи информации о VLAN. Следует активизировать магистральный протокол на нужных портах, так как он выключен по умолчанию.

1.3 Web-сервер

Web-сервер – это программное и аппаратное обеспечение, которое принимает и обрабатывает HTTP-запросы от клиентов и возвращает им соответствующий контент, чаще всего в виде HTML-страниц, а также может обрабатывать другие протоколы, такие как HTTPS и FTP. Для проектирования веб-сервера, который обслуживает как внутренние, так и внешние запросы, важно учитывать безопасность, производительность и возможность масштабирования.

Оборудование для веб-сервера представляет собой хранилище файлов сайта. На нем хранятся как отдельные страницы и файлы стилей, так и мультимедийные файлы – аудио, видео, графика и др. С сервера контент попадает на компьютер, с которого был отправлен запрос, и выводится в наглядном виде через браузер.

Программная составляющая веб-сервера позволяет осуществлять управление размещенными на нем данными, обеспечивает доступ пользователей. Минимально для этого требуется HTTP-сервер, то есть программа, которая может распознавать URL-адреса и работает на протоколе HTTP, который необходим для доступа к веб-странице.

1.4 ADSL2+

ADSL (Asymmetric Digital Subscriber Line – асимметричная цифровая абонентская линия) – модемная технология, в которой доступная полоса пропускания канала распределена между исходящим и входящим трафиком асимметрично. ADSL передает данные по обычной телефонной линии (медной паре), которая используется для обеспечения широкополосного доступа в интернет при этом сохраняя возможность использования телефонной линии для голосовых вызовов.

Особенностью ADSL является асимметричность, скорость передачи данных в сторону пользователя значительно выше, чем от пользователя. Это удобно для большинства пользователей, которые скачивают больше данных, чем загружают. Вторая особенность это возможность доступа в Интернет одновременно с телефонными вызовами без взаимных помех.

1.5 Способы обеспечения безопасности в отношении учетных записей пользователей

Обеспечение безопасности учетных записей пользователей является важной частью проектирования современных информационных систем, включая сети образовательных учреждений. Учетные записи пользователей – это основной канал доступа к конфиденциальной информации и ресурсам, таким как электронные библиотеки, административные системы, и внутренние сервисы. Защита этих учетных записей от несанкционированного доступа, взлома и утечек данных важна для обеспечения надежности системы и конфиденциальности пользователей.

Одним из самых эффективных методов защиты учетных записей является использование многофакторной аутентификации (MFA). В отличие от традиционной однофакторной аутентификации, которая требует только пароля, MFA добавляет дополнительные уровни проверки, такие как одноразовый код, отправленный на мобильный телефон, или использование биометрических данных (например, отпечатков пальцев или распознавания лиц).

Для обеспечения конфиденциальности и безопасности паролей пользователей необходимо использовать криптографические методы хранения паролей. Важнейший принцип – это хеширование паролей с использованием современных алгоритмов (например, bcrypt, Argon2 или PBKDF2). Хеширование позволяет хранить пароли в виде неизвлекаемых строк, что защищает их от утечек в случае взлома базы данных.

Следует установить и поддерживать строгие политики паролей, включая требования к их сложности и регулярной смене. Политика может включать требования к длине пароля (не менее 8-12 символов), использованию символов разных типов (буквы, цифры, специальные символы), а также запрещать использование слабых паролей, таких как «123456» или «password». Это помогает предотвратить использование простых и легко угадываемых паролей.

Мониторинг учетных записей пользователей – еще один необходимый компонент безопасности. Система должна регистрировать все попытки доступа к учетным записям и фиксировать события, связанные с изменением учетных данных. В случае подозрительной активности (например, попытки входа с нового устройства или географического положения) система должна автоматически инициировать дополнительные проверки или блокировать учетную запись до выяснения обстоятельств.

Для защиты от атак методом подбора пароля и кражи паролей используются защита от повторных попыток входа в систему. В случае многократных неудачных попыток входа, система может блокировать учетную запись на определенный срок, требовать CAPTCHA или отправлять уведомление пользователю о попытке взлома. Эти методы усложняют жизнь злоумышленникам и помогают предотвратить автоматизированные атаки.

Использование современных протоколов аутентификации, таких как OAuth2, OpenID Connect и SAML, также играет важную роль в усилении безопасности учетных записей. Эти протоколы позволяют обеспечить безопасную передачу данных и управлять правами доступа, минимизируя риски утечек и атак на аутентификацию.

При использовании мобильных технологий необходимо обеспечить безопасность учетных записей пользователей, которые могут работать с мобильных устройств. Для этого используются VPN (Virtual Private Network) и шифрование данных, которые позволяют контролировать доступ к корпоративным сервисам с мобильных устройств и защищать их от взлома.

Усиленная безопасность учетных записей пользователей представляет из себя комплексный подход, включающий многофакторную аутентификацию, надежное хранение паролей, мониторинг и защиту от атак. Применение современных методов и технологий позволяет минимизировать риски утечек данных и атак, обеспечивая высокий уровень защиты для учреждений.

2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе будет представлено структурное проектирование локальной сети для кафедры государственного университета, где проводится обучение основам программирования.

Кафедра расположена на двух этажах университетского здания – 3 и 9 этажах, с площадью каждого этажа по 240 квадратных метров. Сеть будет включать 60 стационарных подключений, из которых 55 – это стационарные пользователи, к которым подключатся периферийные устройства, такие как принтеры и IP-телефоны, что необходимо для поддержки как административных, так и учебных процессов. Кроме того, сеть должна поддерживать до 10 мобильных подключений, позволяя студентам и преподавателям использовать ноутбуки и другие мобильные устройства для доступа к ресурсам и взаимодействия.

На кафедре государственного университета будут следующие кабинеты: несколько кабинетов для студентов, кабинет заведующего кафедрой, несколько кабинетов для преподавателей и кабинет для системного администратора.

Структурная схема устройства приведена в приложении А.

2.1 Интернет

Блок интернета в структуре сети кафедры государственного университета играет ключевую роль, обеспечивая подключение локальной сети к глобальной сети. Этот узел предоставляет студентам и преподавателям доступ к внешним образовательным ресурсам, облачным платформам и другим цифровым системам, которые активно используются в учебном процессе.

Интернет соединен с модемом, который преобразует внешний сигнал и передает его на маршрутизатор, выполняя роль промежуточного устройства для подключения к провайдеру.

2.2 Модем

Модем служит связующим звеном между интернетом и маршрутизатором, обеспечивая преобразование сигнала для последующей передачи данных в локальную сеть. Модем принимает входящий сигнал от провайдера и передает его маршрутизатору, который далее управляет распределением трафика внутри сети.

2.3 Блок маршрутизации

Маршрутизатор является центральным звеном в управлении трафиком между локальной сетью кафедры и глобальной сетью интернет. Он выполняет не только маршрутизацию, но и такие важные функции, как фильтрация

данных, предотвращение нежелательного трафика и распределение нагрузки между подключенными устройствами. Кроме того, маршрутизатор обеспечивает возможность настройки приоритетов для определенных типов данных, например, для учебных процессов. Использование современных маршрутизаторов с поддержкой расширенных функций безопасности позволяет защитить локальную сеть от потенциальных угроз.

2.4 Блок коммутации

Коммутатор объединяет сетевые устройства кафедры, такие как IP-телефоны, персональные компьютеры, принтеры, точки доступа и Web-сервер, обеспечивая обмен данными между ними. Он подключен к маршрутизатору, что позволяет устройствам внутри сети иметь доступ к интернету и к локальным ресурсам.

2.5 Web-сервер

Web-сервер предоставляет доступ к учебным материалам и внутренним ресурсам кафедры. Благодаря подключению к коммутатору, сервер будет доступен для всех устройств внутри локальной сети, включая персональные компьютеры и мобильные устройства. Он используется для хранения образовательных ресурсов и выполнения запросов от студентов и преподавателей.

2.6 Персональные компьютеры

Персональные компьютеры составляют основную часть инфраструктуры кафедры и используются для выполнения учебных, административных и исследовательских задач. Они подключены к локальной сети через коммутатор, что позволяет пользователям взаимодействовать с сервером, отправлять документы на печать, использовать интернет и подключаться к образовательным платформам. Кроме того, ПК оснащены необходимым программным обеспечением для обучения программированию и других технических дисциплин, что делает их незаменимым инструментом в образовательном процессе.

2.7 Принтеры

Принтеры являются периферийными устройствами, подключенными к персональным компьютерам пользователей в локальной сети. Они предоставляют возможность печати документов, отчетов, графических изображений и других материалов, необходимых для работы рекламного агентства.

2.8 IP-телефоны

IP-телефоны соединены с коммутатором, обеспечивая внутреннюю связь в пределах кафедры. IP-телефон – устройства или программы, использующих технологию голосовой связи по интернет-протоколу (VoIP). Технология IP-телефонии позволяет пользователю совершать голосовые вызовы через широкополосное интернет-соединение, а не по традиционному аналоговому подключению.

2.9 Беспроводные точки доступа и мобильные устройства

Беспроводные точки доступа подключены к коммутатору, предоставляя возможность подключения мобильных устройств к локальной сети кафедры. Точка доступа – это беспроводная базовая станция, предназначенная для обеспечения беспроводного доступа к уже существующей сети или создания совершенно новой беспроводной сети. Беспроводная связь осуществляется посредством технологии Wi-Fi.

3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе описывается и проводится функциональное проектирование заданной локальной компьютерной сети. Здесь даётся более подробное описание функционирования программной и аппаратной составляющих разрабатываемой сети, а именно: обоснование выбранного оборудования, схема адресации, конфигурационная настройка всех устройств.

Функциональная схема разработанной сети находится в приложении Б.

3.1 Создание виланов в сети

Для правильной работы кафедры сеть разделена на виланы. В рамках данного проекта сеть кафедры будет разделена на 7 виртуальных сетей:

1. VLAN № 2 – административный влан.
2. VLAN № 3 – вилан для беспроводного подключения.
3. VLAN № 4 – вилан лаборатории на третьем этаже.
4. VLAN № 5 – вилан лаборатории на девятом этаже.
5. VLAN № 6 – вилан для преподавателей.
6. VLAN № 7 – вилан для IP-телефонов.
7. VLAN № 8 – вилан для заведующего.

3.2 Обоснование выбора программного обеспечения для пользовательских станций

На сегодняшний день существует три популярных операционных системы: Windows, macOS и Linux. У каждой из них есть свои сильные и слабые стороны, но для использования на кафедре программирования наиболее целесообразным вариантом является Windows.

Windows – это наиболее привычная и понятная система для большинства пользователей. Она обладает широким набором инструментов и поддерживает практически все программные продукты, необходимые для обучения программированию. Windows также предоставляет удобный интерфейс, понятный даже тем, кто не имеет опыта работы с компьютером, и предлагает простой доступ к настройкам и системным функциям. Большинство программ, необходимых для разработки, совместимы с этой ОС, что упрощает учебный процесс и снижает количество потенциальных технических проблем.

macOS – это операционная система, известная своей стабильностью и высоким уровнем безопасности. Она часто используется профессиональными разработчиками, особенно в сфере программного обеспечения и дизайна. Однако устройства Apple довольно дороги, что делает массовую установку macOS на кафедре затратной и не всегда оправданной в рамках учебного процесса.

Linux, в свою очередь, является бесплатной и открытой операционной системой, которая активно используется в технической и научной среде. Она предоставляет множество инструментов для разработки и позволяет глубоко настроить систему под конкретные задачи. Однако Linux может быть сложной для освоения, особенно для начинающих пользователей, и не поддерживает многие популярные коммерческие программы. Использование Linux потребует дополнительных усилий на обучение студентов базовым операциям в этой системе.

Сравнительная характеристика выбора программного обеспечения для пользовательских станций приведена ниже в таблице 3.1.

Таблица 3.1 – Сравнительная характеристика выбора программного обеспечения для пользовательских станций

Характеристика	Windows	macOS	Linux
Простота освоения	Высокая. Понятный интерфейс даже для новичков.	Средняя. Понятен, но требует привыкания.	Низкая. Сложен для начинающих пользователей.
Стоимость	Средняя	Высокая	Бесплатная
Совместимость с программами	Широкая. Поддерживает большинство популярных программ.	Ограниченная. Преимущественно поддерживает ПО от Apple.	Средняя. Не поддерживает многие коммерческие программы.
Безопасность	Средняя. Требуется антивирусное ПО.	Высокая. Защита встроена в систему.	Высокая. Защита настраивается вручную.
Подходит для программирования	Отлично. Поддерживает большинство инструментов.	Отлично. Используется профессионалами.	Хорошо. Предоставляет множество инструментов.

Таким образом, Windows представляется оптимальным выбором для кафедры программирования, сочетая в себе удобство использования, совместимость с большинством учебных и профессиональных программ и доступность по стоимости. Важно также правильно выбрать версию операционной системы. Для учебных целей лучше всего подойдет версия Windows 10 или Windows 11, так как они обеспечивают хороший баланс между функциональностью, стабильностью и производительностью. Windows 10 может быть предпочтительнее для тех, кто работает с более старым оборудованием, в то время как Windows 11 предлагает более современный интерфейс и новые функции, которые могут быть полезны для работы с новыми технологиями.

В итоге, была выбрана операционная система Windows 10 по той причине, что она обеспечивает стабильную работу на различных типах оборудования, легко совместима с большинством учебных и профессиональных программ, а также обладает хорошей производительностью. Эта версия системы имеет широкую поддержку и подходит для использования на устройствах с разными техническими характеристиками, что делает её оптимальным вариантом для кафедры программирования, особенно при наличии более старых компьютеров.

3.3 Обоснование выбора производителя сетевого оборудования

При проектировании данной локальной сети было учтено требование заказчика в области финансов – бюджетная сеть. При выборе сетевого оборудования необходимо опираться на размер проектируемой локальной сети, на поддержку оборудованием технологий, необходимых для настройки локальной компьютерной сети, на наличие поддержки оборудования со стороны производителя и на требования заказчика к производителю закупаемого оборудования.

В настоящей ситуации заказчик не уверен в производителе закупаемого сетевого оборудования. Из доступного на рынке оборудования в данный момент можно выделить следующих самых распространенных производителей: Cisco, Mikrotik, D-Link и TP-Link.

Оборудование от Cisco имеет запределённую стоимость даже в рамках бюджета, выделяемого на полноценную коммерческую сеть: маршрутизаторы данного производителя по стоимости начинаются от 2000 BYN и могут достигать 130000 BYN. По вышеописанным причинам выбор данного производителя является нерациональным.

Оборудование от Mikrotik хорошо справляется со своими задачами, однако само по себе оборудование от данного производителя является чем-то средним между бюджетным оборудованием от производителей D-Link и TP-Link и оборудованием от таких лидеров рынка, как Cisco, Juniper, Huawei. На базе оборудования от данного производителя уже намного целесообразнее проектировать корпоративные сети с средними нагрузками без жестких требований к бесперебойной работе сети. Однако во внимание стоит принимать тот факт, что оборудование Mikrotik имеет сложности при настройке и ограниченный функционал.

Оборудование от производителей D-Link и TP-Link самое дешевое и доступное среди всех предложенных производителей. Данное оборудование предназначено для сегмента бюджетных сетей и отдельных пользователей. При более тщательном анализе, выбор в пользу D-Link будет более обоснован.

TP-Link славится своей доступностью и простотой в использовании, что делает его хорошим выбором для домашнего использования или небольших офисов. Однако в контексте учебного заведения, где могут возникать

потребности в немного более сложной настройке и управлении сетью, TP-Link может ограничивать возможности.

D-Link, в свою очередь, предлагает устройства с хорошим соотношением цены и качества, а также с более гибкими возможностями для настройки и управления. Эти устройства могут быть полезны для учебных заведений, где потребуется немного больше функционала для создания стабильной и управляемой сети.

Для проектируемой сети учебного заведения, учитывая бюджет и функциональные требования заказчика, оптимальным выбором являются маршрутизатор и коммутаторы от компании D-Link. Они предлагают хороший баланс цены, функциональности и удобства настройки, что делает их идеальными для создания стабильной и управляемой сети.

3.4 Обоснование выбора активного сетевого оборудования

Активное сетевое оборудование – это устройства, которые обеспечивают передачу, управление и обработку данных в сети. Включает в себя маршрутизаторы, коммутаторы, точки доступа, системы безопасности и другие элементы, необходимые для функционирования сети. Эти устройства играют ключевую роль в обеспечении стабильности, производительности и безопасности локальной сети. Правильный выбор активного сетевого оборудования особенно важен в образовательных учреждениях, где требования к сети могут варьироваться от базовых до более сложных в зависимости от задач.

Для проектируемой сети кафедры университета было принято решение использовать оборудование производителя D-Link. Этот выбор обусловлен несколькими факторами, такими как доступность продукции в Беларуси, разумная стоимость и хорошее соотношение цены и качества. Оборудование D-Link будет эффективно работать для образовательной сети, обеспечивая стабильное соединение и требуемые функции для работы с учебными ресурсами и коммуникациями.

3.4.1 Обоснование выбора маршрутизатора

Для выбора оптимального маршрутизатора для сети кафедры государственного университета, где проводится обучение основам программирования были рассмотрены два беспроводных маршрутизатора от компании D-Link – DSL-245GR/R1A и DSL-2640U/RB/U2B. Эти модели обладают схожими характеристиками, но имеют и различия, которые могут повлиять на конечный выбор.

Маршрутизаторы D-Link DSL-245GR/R1A и DSL-2640U/RB/U2B являются моделями, подходящими для построения домашней или малой офисной сети. Оба устройства поддерживают ADSL и VDSL, обеспечивая стабильное подключение к интернету через телефонную линию. Оба

маршрутизатора имеют встроенные механизмы защиты, включая фаерволы и другие средства безопасности.

Сравнительная характеристика выбора маршрутизатора приведена ниже в таблице 3.2.

Таблица 3.2 – Сравнительная характеристика маршрутизаторов

Характеристика	D-Link DSL-245GR/R1A	D-Link DSL-2640U/RB/U2B
Тип устройства	беспроводной DSL-маршрутизатор	беспроводной DSL-маршрутизатор
Стандарты беспроводной сети	802.11ac (Wi-Fi 5)	802.11n (Wi-Fi 4)
Протоколы безопасности беспроводной сети	WEP, WPA, WPA2-PSK, WPA2-RADIUS	WEP, WPA, WPA2-PSK
Диапазон частот	2.4 ГГц, 2.5 ГГц	2.4 ГГц
Стоимость	290 BYN	190 BYN

Исходя из сравнительных характеристик и требований к сети кафедры, выбор будет сделан в пользу D-Link DSL-245GR/R1A.

Этот маршрутизатор обеспечивает более высокую производительность благодаря поддержке стандарта Wi-Fi 5, что позволяет достигать более высоких скоростей передачи данных, а также двухдиапазонному подключению, что улучшает стабильность связи в условиях большой нагрузки. Дополнительные функции безопасности, такие как поддержка WPA2-RADIUS, обеспечивают защиту сети, что важно для образовательной среды. Несмотря на более высокую цену, его возможности и качество оправдывают инвестиции, особенно в контексте использования на кафедре программирования, где требуется стабильная и безопасная сеть для доступа к онлайн-ресурсам и обучению.

3.4.2 Обоснование выбора коммутатора

Для организации проводной сети на кафедре для сравнения были выбраны два коммутатора от компании D-Link: D-Link DGS-1100-24 и D-Link DES 1210-28P. Оба устройства являются управляемыми коммутаторами второго уровня, которые обеспечивают надежную и гибкую работу образовательной сети, поддерживая такие функции, как VLAN, а также различные протоколы безопасности. Эти коммутаторы идеально подходят для управления трафиком и сегментации сети, что позволяет разделить различные части сети и эффективно изолировать данные.

Сравнительная характеристика выбора коммутатора приведена ниже в таблице 3.3.

Таблица 3.3 – Сравнительная характеристика коммутаторов

Характеристики	D-Link DGS-1100-24	D-Link DES 1210-28P
Тип устройства	управляемый коммутатор 2-го уровня	управляемый коммутатор 2-го уровня
Количество портов	24 порта 10/100/1000BASE-T, 4 гигабитных порта SFP	24 порта 10/100Base-TX, 2 порта 10/100/1000BaseT, 2 комбинированных порта 100/1000Base-T/SFP
Безопасность	ACL, SSH, SSL	ACL, SSH, SSL
Управление устройством	веб-интерфейс, SNMP, CLI	Веб-интерфейс, SNMP, CLI
Стоимость	944 BYN	1748 BYN

Сравнение коммутаторов D-Link DGS-1100-24 и D-Link DES 1210-28P позволяет сделать вывод, что D-Link DGS-1100-24 является более выгодным выбором для образовательной сети с базовыми потребностями. Его стоимость значительно ниже, и он предоставляет все необходимые функции для управления трафиком и безопасности. Этот вариант будет идеальным для кафедры с ограниченным бюджетом.

3.4.3 Обоснование выбора точки доступа

Для обеспечения стабильного и эффективного покрытия Wi-Fi на всей территории кафедры были выбраны точки доступа D-Link DWL-6610AP и D-Link DAP-2680. Оба устройства поддерживают современные стандарты Wi-Fi 5 (802.11ac), обеспечивая высокоскоростное подключение, что особенно важно для учебных помещений с большим количеством пользователей. Эти точки доступа подходят для высоконагруженных сетей, что делает их хорошими кандидатами для учебных заведений, где одновременно могут быть подключены десятки и сотни мобильных устройств.

Сравнительная характеристика выбора точек доступа приведена ниже в таблице 3.4.

Таблица 3.4 – Сравнительная характеристика точек доступа

Характеристика	D-Link DWL-6610AP	D-Link DAP-2680
1	2	3
Тип устройства	Точка доступа, управление через облако	Точка доступа, управление через облако
Частотные диапазоны	2.4ГГц, 5ГГц	2.4ГГц, 5ГГц
Класс скорости Wi-Fi	867 mbps	1300 mbps

Продолжение таблицы 3.4.

1	2	3
Стандарты беспроводной связи	802.11ac (Wi-Fi 5)	802.11ac (Wi-Fi 5)
Протоколы безопасности беспроводной сети	WEP, WPA, WPA2-PSK, WPA2-RADIUS	WEP, WPA, WPA2-PSK, WPA2-RADIUS
Стоимость	720 BYN	784 BYN

Сравнение этих точек доступа позволяет сделать вывод, что D-Link DWL-6610AP является более выгодным вариантом с точки зрения цены, при этом он поддерживает все необходимые функциональные возможности. Это устройство будет отлично подходить для образовательной сети с большим количеством пользователей.

3.5 Расчет качества связи беспроводной сети

Беспроводная сеть должна обеспечивать подключение до 56 устройств и покрывать всю площадь помещений.

Чтобы определить количество точек доступа на этаж и на все здание, необходимо рассчитать покрытие беспроводной сетью всех помещений в организации. Расчет будет производиться при условии, что соседние здания находятся на расстоянии, достаточном для того, чтобы беспроводные сети, организованные в них, не влияли на разрабатываемую сеть.

Для расчёта затухания радиоволн в беспрепятственной воздушной среде будет использована упрощенная формула:

$$L = 32,44 + 20 \lg(F) + 20 \lg(D), \text{ дБ}, \quad (3.1)$$

где F – частота сигнала в ГГц, D – расстояние в метрах от точки доступа.

Здание имеет т-образную форму. В одной части здания находятся лестница и лифты. Предполагается, что эта зона не обязательно должна покрываться сетью. Исходя из этого, зона, которая обязательно должна быть покрыта сетью, имеет прямоугольную форму. Для минимизации расстояния для всех возможных пользователей, точка размещается в центре этой зоны, на потолке.

Учитывая высоту потолка 2,5 метра и расстояние до стен – 5 и 8 метров, формула нахождения максимального расстояния от центра зоны до стены будет выглядеть так:

$$D = \sqrt{l^2 + w^2 + h^2} = \sqrt{2,5^2 + 5^2 + 8^2} = 9,75 \text{ м}, \quad (3.2)$$

где l – длина, w – ширина, h – высота.

Затухание радиоволн $L_{2,4}$ для частоты 2,4 ГГц L_5 для частоты 5 ГГц рассчитывается по формуле (3.1):

$$L_{2,4} = 32,44 + 20 \lg(2,4) + 20 \lg(9,75) = 59,8 \text{ дБ}, \quad (3.3)$$

$$L_5 = 32,44 + 20 \lg(5) + 20 \lg(9,75) = 66,2 \text{ дБ}. \quad (3.4)$$

Так как внутренние стены являются кирпичными, что придает зданию дополнительную пожарную безопасность, то наиболее серьёзное препятствие для распространения сигнала представляется в виде двух кирпичных стен. Таким образом, затухание радиоволн при прохождении через стены: $L_{2,4 \text{ макс. ст.}} = 2 * 4,44 = 8,88 \text{ дБ}$, $L_{5 \text{ макс. ст.}} = 2 * 14,62 = 29,24 \text{ дБ}$. Также необходимо учесть возможное затухание за счёт взаимного размещения оборудования $L_{\text{обор.}} = 5 \text{ дБ}$.

Учитывая данные факторы, максимальное затухание сигнала в помещениях составляет:

$$L_{2,4 \text{ макс.}} = L_{2,4} + L_{2,4 \text{ макс. ст.}} + L_{\text{обор.}} = 59,8 + 8,88 + 5 = 73,68 \text{ дБ}, \quad (3.5)$$

$$L_{5 \text{ макс.}} = L_5 + L_{5 \text{ макс. ст.}} + L_{\text{обор.}} = 66,2 + 29,24 + 5 = 100,44 \text{ дБ}. \quad (3.6)$$

С учётом мощности излучения точки доступа, равной $S_{\text{т.д.}} = 16 \text{ дБм}$ для частоты 2.4 ГГц, $S_{\text{т.д.}} = 18 \text{ дБм}$ для частоты 5 ГГц, минимальная мощность сигнала в самой удаленной точке помещения будет равна:

$$S_{2.4 \text{ мин.}} = S_{\text{т.д.}} - L_{2,4 \text{ макс.}} = 16 - 73,68 = -57,68 \text{ дБм}, \quad (3.7)$$

$$S_{5 \text{ мин.}} = S_{\text{т.д.}} - L_{5 \text{ макс.}} = 18 - 100,44 = -82,44 \text{ дБм}. \quad (3.8)$$

Качество обслуживания беспроводных клиентов напрямую зависит от мощности сигнала в точке обслуживания и может быть оценена по следующей шкале:

- до -50 дБм – отличный уровень сигнала, устройства работают хорошо;
- от -50 до -60 дБм – сигнал высокого качества, устройства работают нормально;
- от -60 до -80 дБм – низкое качество, подходит не для всех задач;
- от -80 дБм – минимальная мощность сигнала, практически непригодна для использования.

Таким образом, минимальной мощности Wi-Fi сигнала на этаже при размещении единственной точки доступа в середине этажа будет недостаточно для кафедры программирования, так как преподавателям и студентам нужен идеальный уровень сигнала. Но, так как минимальной мощности одной точки почти достаточно, двух точек доступа на этаж хватит для кафедры.

3.6 Обоснование выбора веб-сервер

Основное требование, которое предъявляется к аппаратной платформе для веб-сервера – высокая скорость работы, которая показывает минимальное время отклика у накопителя, хранящего запрашиваемые данные.

Для достижения высокой производительности и надежности было выбрано оборудование с твердотельными накопителями (SSD), которые позволяют значительно уменьшить время отклика по сравнению с традиционными жесткими дисками (HDD). Такой выбор критичен для работы образовательных и исследовательских порталов, где доступность данных и минимизация задержек играют важную роль.

Для обоснования выбора серверного оборудования были выбраны два современных варианта: HPE ProLiant DL380 Gen9 24SF и HPE ProLiant DL380 Gen10. Эти серверы предоставляют высокую производительность, масштабируемость и подходят для использования в образовательных учреждениях.

Сравнительная характеристика выбора веб-сервера приведена ниже в таблице 3.5.

Таблица 3.5 – Сравнительная характеристика веб-сервера

Характеристика	HP ProLiant DL380 Gen9 24SF	HP ProLiant DL380 Gen10 8SF
Процессоры	До 2x Intel Xeon E5-2600 v3/v4	До 2x Intel Xeon Scalable
ОЗУ	до 3 ТБ DDR4	До 3 ТБ DDR4 с поддержкой Persistent Memory
Сетевые интерфейсы	4x 1GbE	4x 1GbE, возможность установки 10GbE карт
Количество слотов памяти	24	24
Максимальное количество оперативной памяти	768 GB	3073 GB
Стоимость	4231 BYN	9543 BYN

HP ProLiant DL380 Gen9 является отличным выбором для задач, требующих высокой производительности и хранения данных, благодаря своим широким возможностям масштабирования и надежности. Для текущих нужд кафедры, где важна производительность и стоимость, HP ProLiant DL380 Gen9 выглядит наиболее оптимальным вариантом, предоставляя отличное соотношение цены и возможностей.

3.7 Обоснование выбора сетевого шкафа

Для размещения серверов и коммутаторов в телекоммуникационных шкафах на кафедре были выбраны шкафы TC6401-06G, соответствующие размерам и требованиям оборудования. В шкафу на третьем этаже будет расположен сервер HP ProLiant DL380 Gen9 24SF, который имеет компактный форм-фактор и поддерживает достаточно большое количество устройств. Этот сервер будет обеспечивать необходимую вычислительную мощность и место для хранения данных. В шкафу на девятом этаже разместится дополнительный коммутатор D-Link DGS-1100-24, который обеспечивает эффективное подключение всех рабочих станций и периферийных устройств.

Для оптимальной организации пространства и безопасности оборудования, шкафы TC6401-06G обладают хорошей вентиляцией и достаточно прочной конструкцией для размещения и надежной работы сетевых устройств. Размеры шкафа позволяют разместить до нескольких устройств, в том числе серверы и коммутаторы, с возможностью дальнейшего расширения при необходимости.

Основные характеристики сетевого шкафа:

- тип крепления: настенный;
- высота: 370 мм;
- ширина: 600 мм;
- глубина: 450 мм;
- материал: сталь, окрашенная порошковой краской;
- вентиляция: предусмотрены вентиляционные отверстия для обеспечения циркуляции воздуха и предотвращения перегрева оборудования;
- вес: около 10-12 кг (в зависимости от комплектации);
- максимальная нагрузка: до 30-50 кг;
- стоимость: 290BYN.

3.8 Обоснование выбора пользовательских станций

Для обеспечения комфортной и продуктивной работы сотрудников и студентов кафедры университета потребовалось подобрать компьютеры, которые соответствуют определенным требованиям. Основными задачами сотрудников и студентов кафедры являются работа с виртуальными учебными средами, программирование, а также управление сетевой инфраструктурой и её настройка. Исходя из этих требований, необходимо оборудование с высокой вычислительной мощностью, большим объемом памяти и удобным интерфейсом.

Минимальные требования для компьютеров:

- шестиядерный процессор или выше для многозадачности;
- не менее 16 ГБ оперативной памяти, желательно 32 ГБ для работы с виртуализацией и ресурсоемкими приложениями;
- SSD объемом от 512 ГБ для быстрого доступа к данным;

- дискретная видеокарта с хорошей производительностью, так как задачи могут включать в себя анализ данных, их визуализация и другие;
- монитор с разрешением не ниже Full HD для удобной работы с текстом и визуальными элементами;
- наличие USB, HDMI, и Ethernet для подключения периферийных устройств и сетевых кабелей.

Сравнив несколько подходящих моделей, были выбраны следующие сборки:

Таблица 3.6 – Сравнительная характеристика пользовательских станций

Параметры	TGPC Action 82774 A-X	TGPC Action 5 85577 I-X
Процессор	AMD Ryzen 5 5600	Intel Core i5 3400F
Количество ядер	6	10
Оперативная память	16 ГБ	32 ГБ
Емкость накопителя	1000 ГБ	1000 ГБ
Видеокарта	NVIDIA GeForce RTX 4060	NVIDIA GeForce RTX 4060
Стоимость	2680 BYN	3707 BYN

Выбор был сделан в пользу модели TGPC Action 5 85577 I-X благодаря лучшим параметрам по количеству ядер и увеличенному объему оперативной памяти, что позволит сотрудникам кафедры и студентам работать с более сложными задачами.

Для комфортной работы за компьютером также потребовались мониторы с хорошей цветопередачей и частотой обновления экрана.

Были рассмотрены следующие модели:

Таблица 3.7 – Сравнительная характеристика мониторов

Параметры	Монитор LG 24MR400-B	Монитор Philips 241V8L/01	Монитор Samsung LS24C310EAIXCI
Разрешение	1920x1080	1920x1080	1920x1080
Плотность пикселей	93 ppi	91 ppi	92 ppi
Частота обновления экрана	100 Гц	75 Гц	75 Гц
Яркость экрана	250 кд/м2	250 кд/м2	144 кд/м2
Цветовой охват sRGB	99%	-	72%
Стоимость	347 BYN	422,37 BYN	399 BYN

Был выбран монитор Монитор LG 24MR400-B, так как он имеет лучшую частоту обновления и цветовой охват, что делает его хорошим вариантом для выполнения задач, требующих высокой четкости и точности изображения.

Для работы за компьютером выбраны также мышь и клавиатура. Офисный набор Logitech MK120 920-002561 стоимостью 76,67 BYN обеспечивает комфорт и долговечность, что идеально подходит для повседневных задач.

Общая стоимость рабочей станции: 4130,67BYN.

3.9 Обоснование выбора принтера и сканера

Для обеспечения печати документов, учебных материалов и других рабочих заданий на кафедре, требуется надежный и функциональный принтер, который сможет справляться с разными объемами печати и обеспечивать качество, подходящее для учебных и административных нужд. Основные требования к выбору принтера включают высокую скорость печати, низкие эксплуатационные затраты, возможность сетевого подключения, а также поддержку монохромной и цветной печати для разнообразных задач.

Сравнительная характеристика принтеров представлена в таблице 3.8.

Таблица 3.8 – Сравнительная характеристика принтеров

Параметры	HP LaserJet Pro M479fdw	Xerox B225DNI
Скорость ч/б печати (A4)	27 стр/мин	34 стр/мин
Наличие сканера	да	да
Ресурс ч/б картриджа в комплекте	2 400 стр	1 500 стр
Wi-Fi	802.11n, 802.11g, 802.11b	802.11n, 802.11g, 802.11b
Вес	23.4 кг	10 кг
Стоимость	2518,99 BYN	783,40 BYN

В данном случае выбор пал на Xerox B225DNI, так как он имеет лучшие характеристики по скорости печати в ч/б формате и выгодно выделяется по стоимости по сравнению с аналогом за большую цену.

3.10 Обоснование выбора IP-телефонов

Для обеспечения эффективной внутренней и внешней связи на кафедре были выбраны IP-телефоны, которые позволяют осуществлять звонки через интернет-соединение, обеспечивая качество передачи голоса и широкие возможности по интеграции с корпоративной сетью. IP-телефоны, в отличие от аналоговых телефонов, имеют гибкие настройки и возможности, такие как

передача вызовов, конференц-связь и интеграция с различными программами для связи, что особенно важно в образовательной и административной среде.

Для удовлетворения данных требований был выбран IP-телефон Yealink SIP-T31P. Эта модель оптимально сочетает доступную цену с функциональностью, необходимой для рабочего процесса на кафедре.

Стоимость устройства: 186,30BYN.

3.11 Схема адресация

3.11.1 Внешняя адресация

Согласно требованиям заказчика, непосредственное подключение к провайдеру отсутствует, то есть сеть соединена только с общей сетью здания.

Согласно варианту, дается выбор из 10 подсетей, где можно выбрать одну подсеть и назначить внешний статический IPv4-адрес организации из неё. Предлагаемые подсети, их маски и доступные диапазоны адресов приведены в таблице 3.9.

Таблица 3.9 – Предлагаемые по варианту подсети

№	Адрес подсети	Маска подсети	Количество хостов
1	3.233.112.0	255.255.248.0 2048	510
2	34.74.224.0	255.255.224.0 8192	8,190
3	93.239.0.0	255.255.0.0	65536
4	100.144.144.0	255.255.255.0	256
5	131.204.56.0	255.255.255.224	32
6	148.85.172.0	255.255.255.248	8
7	168.176.70.64	255.255.255.192	64
8	183.208.191.128	255.255.248.0	2048
9	199.63.46.24	255.255.224.0	8192
10	204.31.94.0	255.255.0.0	65536

Предположим, что зданием используется шестая подсеть 148.85.172.0, имеющая 8 адресов.

3.11.2 Внутренняя адресация IPv4

Согласно требованиям заказчика, для внутренней IPv4 адресации должны быть использованы приватные адреса. Следовательно для доступа в интернет на роутере должен быть настроен NAT. Для компании выберем подсеть 192.168.0.0/24.

Требуется разделение сети на подсети для каждого из VLAN, при этом должно быть учтено различие количества, относящегося к данным VLAN, хостов. Схема IPv4 адресации приведена в таблице 3.10.

Таблица 3.10 – Схема внутренней IPv4 адресации

Назначение	№ VLAN	Адрес подсети	Маска подсети в битах	Хосты
Административный	2	192.168.0.0	28	14
Для беспроводное подключения	3	192.168.0.16	27	30
Для третьего этажа	4	192.168.0.48	27	30
Для девятого этажа	5	192.168.0.80	27	30
Для преподавателей	6	192.168.0.112	28	14
Для IP-телефонов	7	192.168.0.128	29	6
Для заведующего	8	192.168.0.136	29	6

Административный VLAN подразумевает назначение статических адресов, схема адресации данной подсети приведена в таблице 3.11. Так как все устройства находятся в одной подсети, все их адреса имеют одинаковую маску: 255.255.255.240.

Таблица 3.11 – Схема IPv4 адресации административного VLAN (2)

Устройство	Позиционное обозначение	Адрес
Маршрутизатор	RT1	192.168.0.1
Коммутатор	SW1	192.168.0.2
Коммутатор	SW2	192.168.0.3
Коммутатор	SW3	192.168.0.4
Коммутатор	SW4	192.168.0.5
Административная пользовательская станция	PC1	192.168.0.6
Web-сервер	Server1	192.168.0.7

IPv4-адреса мобильным подключениям будут выдаваться по протоколу Dynamic Host Configuration Protocol (DHCP) из промежутка 192.168.0.17-46/27 за исключением 192.168.0.17, 192.168.0.43-46 по причине того, что данные IP-адреса будут зарезервированы для маршрутизатора и для точек доступа.

IPv4-адреса стационарным пользователям будут выдаваться по протоколу Dynamic Host Configuration Protocol (DHCP) из промежутков подсетей 192.168.0.49-78/27 и 192.168.0.81-110/27 за исключением 192.168.0.49 и 192.168.0.81 по причине того, что данные IP-адреса будут зарезервированы для маршрутизатора.

IPv4-адреса для преподавателей были установлены статическими по причине их малого количества (6 штук) и отсутствия фактора частой смены на кафедре. IPv4-адреса преподавателей приведены в таблице 3.12.

Таблица 3.12 – Схема IPv4 адресации преподавателей

Устройство	Позиционное обозначение	Адрес/маска
Маршрутизатор	RT1	192.168.0.113
ПК преподавателя 1	PC3.1	192.168.0.114
ПК преподавателя 2	PC3.2	192.168.0.115
ПК преподавателя 3	PC3.3	192.168.0.116
ПК преподавателя 4	PC9.1	192.168.0.117
ПК преподавателя 5	PC9.2	192.168.0.118
ПК преподавателя 6	PC9.3	192.168.0.119

IPv4-адреса IP-телефонов были установлены статическими по причине их малого количества (2 штуки) и отсутствия фактора частой смены на кафедре. IPv4-адреса IP-телефонов приведены в таблице 3.13.

Таблица 3.13 – Схема IPv4 адресации IP-телефонов

Устройство	Позиционное обозначение	Адрес/маска
Маршрутизатор	RT1	192.168.0.129
Телефон заведующего	IpPhone 1	192.168.0.130
Телефон сотрудника	IpPhone 2	192.168.0.131

IPv4-адрес для станции заведующего был установлен статическими 192.168.0.138.

IPv4-адреса точкам доступа были установлены статическими в промежутке 192.168.0.43/7 – 192.168.0.46/27.

3.11.3 Внутренняя адресация IPv6

По требованию заказчика адресация IPv6 будет использоваться для взаимодействия внутри сети. Для этих целей задействованы адреса IPv6 формата Unique Local Unicast. Global ID выбран случайным образом, а в Subnet ID старшие биты обозначают номер соответствующего VLAN, с заполнением оставшихся бит нулями. Это обеспечивает интуитивно понятную структуру адресов и гибкость для адаптации. Длина префикса подсети составит 64 бита во всех случаях. Схема внутренней IPv6-адресации организации представлена в таблице 3.14.

Таблица 3.14 – Схема внутренней IPv6 адресации организации

Название подсети	№ VLAN	Адрес подсети
1	2	3
Административный	2	2001:3456:789a:0002::/64
Для беспроводное подключения	3	2001:3456:789a:0003::/64

Продолжение таблицы 3.14.

1	2	3
Для третьего этажа	4	2001:3456:789a:0004::/64
Для девятого этажа	5	2001:3456:789a:0005::/64
Для преподавателей	6	2001:3456:789a:0006::/64
Для IP-телефонов	7	2001:3456:789a:0007::/64
Для заведующего	8	2001:3456:789a:0008::/64

IPv6-адреса административного VLAN приведена в таблице 3.15.

Таблица 3.15 – Схема IPv6 адресации административного VLAN (2)

Устройство	Позиционное обозначение	Адрес
Маршрутизатор	RT1	2001:3456:789a:0002::1/64
Коммутатор	SW1	2001:3456:789a:0002::2/64
Коммутатор	SW2	2001:3456:789a:0002::3/64
Коммутатор	SW3	2001:3456:789a:0002::4/64
Коммутатор	SW4	2001:3456:789a:0002::5/64
Административная пользовательская станция	PC1	2001:3456:789a:0002::6/64
Web-сервер	Server1	2001:3456:789a:0002::7/64

IPv6-адреса мобильным подключениям будут выдаваться по протоколу Dynamic Host Configuration Protocol v6(DHCPv6) из промежутка 2001:3456:789a:0003::17-46/64 за исключением 2001:3456:789a:0003::17/64, 2001:3456:789a:0003::43-46/64 по причине того, что данные IP-адреса будут зарезервированы для маршрутизатора и для точек доступа.

IPv6-адреса стационарным пользователям будут выдаваться по протоколу Dynamic Host Configuration Protocol v6(DHCPv6) из промежутков подсетей 2001:3456:789a:0004::49-78/64 и 2001:3456:789a:0005::81-110/64 за исключением 2001:3456:789a:0004::49 и 2001:3456:789a:0005::81 по причине того, что данные IP-адреса будут зарезервированы для маршрутизатора.

IPv6-адреса для преподавателей были установлены статическими по причине их малого количества (6 штук) и отсутствия фактора частой смены на кафедре. IPv6-адреса преподавателей приведены в таблице 3.16.

Таблица 3.16 – Схема IPv4 адресации преподавателей

Устройство	Позиционное обозначение	Адрес/маска
1	2	3
Маршрутизатор	RT1	2001:3456:789a:0006::113
ПК преподавателя 1	PC3.1	2001:3456:789a:0006::114
ПК преподавателя 2	PC3.2	2001:3456:789a:0006::115

Продолжение таблицы 3.16.

1	2	3
ПК преподавателя 3	PC3.3	2001:3456:789a:0006::116
ПК преподавателя 4	PC9.1	2001:3456:789a:0006::117
ПК преподавателя 5	PC9.2	2001:3456:789a:0006::118
ПК преподавателя 6	PC9.3	2001:3456:789a:0006::119

IPv6-адреса IP-телефонов были установлены статическими по причине их малого количества (2 штуки) и отсутствия фактора частой смены на кафедре. IPv6-адреса IP-телефонов приведены в таблице 3.17.

Таблица 3.17 – Схема IPv6 адресации IP-телефонов

Устройство	Позиционное обозначение	Адрес/маска
Маршрутизатор	Router1	2001:3456:789a:0007::129/64
Телефон заведующего	IpPhone 1	2001:3456:789a:0007::130/64
Телефон сотрудника	IpPhone 2	2001:3456:789a:0007::131/64

IPv6-адрес для станции заведующего был установлен статическими 2001:3456:789a:0008::138.

IPv6-адреса точкам доступа были установлены статическими в промежутке 2001:3456:789a:0003::43/64 – 2001:3456:789a:0003::46/64.

3.13 Описание настройки компонентов локальной сети

3.13.1 Настройка маршрутизатора

Настройка и управление маршрутизатором DSL-245GR выполняется с помощью встроенного web-интерфейса. Web-интерфейс доступен в любой операционной системе, которая поддерживает web-браузер.

Перед настройкой маршрутизатора, необходимо включить питание и подключиться к одному из портов LAN. Далее необходимо убедиться, что Ethernet-адаптер компьютера настроен на автоматическое получение IP-адреса. Как только вы получили по DHCP конфигурацию, можно переходить к web-интерфейсу.

В адресной строке web-браузера введем доменное имя маршрутизатора (по умолчанию – dlinkrouter.local) с точкой в конце и нажмем клавишу Enter. Вы также можете ввести IP-адрес устройства (по умолчанию – 192.168.0.1).

Если устройство еще не было настроено или ранее были восстановлены настройки по умолчанию, при обращении к web-интерфейсу открывается страница изменения настроек по умолчанию.

Необходимо ввести пароль администратора в поля «Новый пароль» и «Подтверждение пароля» (рисунок 3.1). После авторизации будет предложено изменить настройки по умолчанию.

Рисунок 3.1 – Смена настроек по умолчанию

После того, как мы оказались авторизованы в web-интерфейсе, можно приступать к конфигурированию.

Подключение к интернету осуществляется через ADSL2+. Выбранный маршрутизатор поддерживает стандарты ADSL2+ и имеет порт DSL с разъёмом RJ-11. Подключаем телефонный кабель к DSL-порту маршрутизатора и порту MODEM сплиттера (сплиттер идёт в комплекте с маршрутизатором), затем кабель от телефонной розетки к порту LINE сплиттера.

Чтобы подключить устройство к ADSL-линии, на странице «Режим работы устройства» в списке «Способ подключения» выбираем значение ADSL. В этом режиме далее настроим WAN-соединение.

Рисунок 3.2 – Выбор режима работы устройства

По заданию, непосредственного подключения к провайдеру нет. В этом случае требуется добавить статическое IPv4 соединение в маршрутизатор и указать публичный IP-адрес, который используется в здании, маску подсети, IP-адрес шлюза и DNS.

Чтобы настроить WAN-соединение нужно перейти в «Настройка соединений WAN», затем нажать кнопку «ДОБАВИТЬ» и выставить нужный

тип соединения. Ставим статический IPv4 адрес, в разделе интерфейс выбираем DSL-порт маршрутизатора.

IP-адрес*

Маска подсети*

IP-адрес шлюза*

Первичный DNS*

Вторичный DNS

Рисунок 3.3 – Настройка WAN

Главные настройки

Тип соединения
Статический IPv4

Интерфейс
Добавить новый ATM PVC

Имя соединения*
statip_80

☒ Включить соединение

☒ NAT

☐ Ping

☐ RIP

Рисунок 3.4 – Добавления соединения типа Статический IPv4

Далее перейдём на вкладку IPv6, чтобы добавить локальный IPv6-адрес маршрутизатора. Нажимаем кнопку «ДОБАВИТЬ». В отобразившейся строке вводим IPv6-адрес, а также через косую черту указываем десятичное значение длины префикса.

Локальный IPv6

Например: fd00::1/64

Имя устройства
dlinkrouter.local

Рисунок 3.5 – Настройка IPv6 на маршрутизаторе

Также необходимо настроить межсетевой экран на маршрутизаторе, чтобы ограничить доступ к административному VLAN извне, но предоставить доступ к серверу. Переходим в раздел «Межсетевой экран».

Рисунок 3.6 – Страница Межсетевой экран / IP-фильтры

Вводим IP-адрес подсети для VLAN 2 в поле «IP-адрес назначения», в поле «IP-адрес источника» выбираем «WAN», и в поле «Действие» выбираем «Запретить» и нажимаем кнопку «Применить».

Для разрешения доступа к Web-серверу открываем раздел «Межсетевой экран» (рисунок 3.6). Вводим IP-адрес Web-сервера поле «IP-адрес назначения», в поле «IP-адрес источника» выбираем «WAN», и в поле «Действие» выбираем «Разрешить» и нажимаем кнопку «Применить».

3.13.2 Настройка коммутаторов

Для корректной работы сети в первую очередь необходимо настроить VLAN. Для этого используем WebUi коммутатора.

Для того чтобы зайти в WebUi подключаем компьютер к коммутатору через Ethernet, заходим в веб-браузер и вводим IP-адрес коммутатора по

умолчанию (10.90.90.90). После этого открывается окно авторизации где требуется ввести логин и пароль.



Рисунок 3.7 – Окно авторизации WebUi

Для создания VLAN переходим в «VLAN/VLAN Configuration Wizard». Вводим нужный VID и нажимаем «Next». Появляется окно где происходит дальнейшая настройка. Вводим VLAN Name, выбираем порты которые будет использовать данный VLAN, порты для окончечных устройств ставим в access, порт идущий на маршрутизатор ставим в trunk. Нажимаем «Apply».

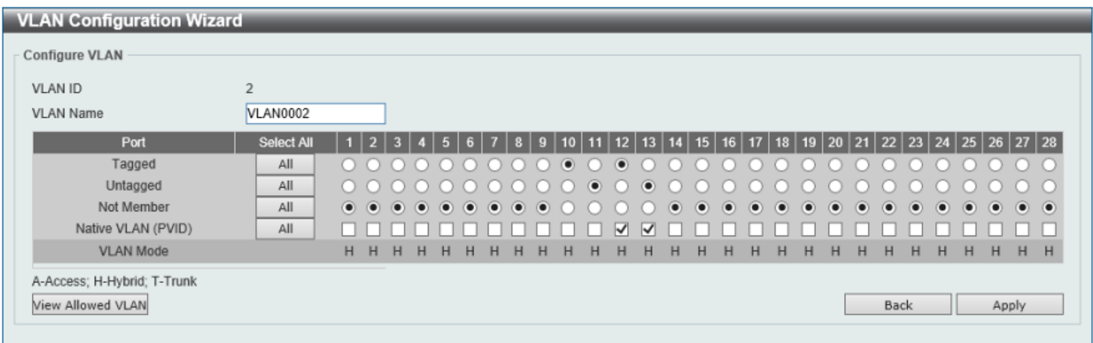


Рисунок 3.8 – Создание VLAN

Заходим в «VLAN/802.1Q VLAN» и видим созданный и сконфигурированный новый VLAN.

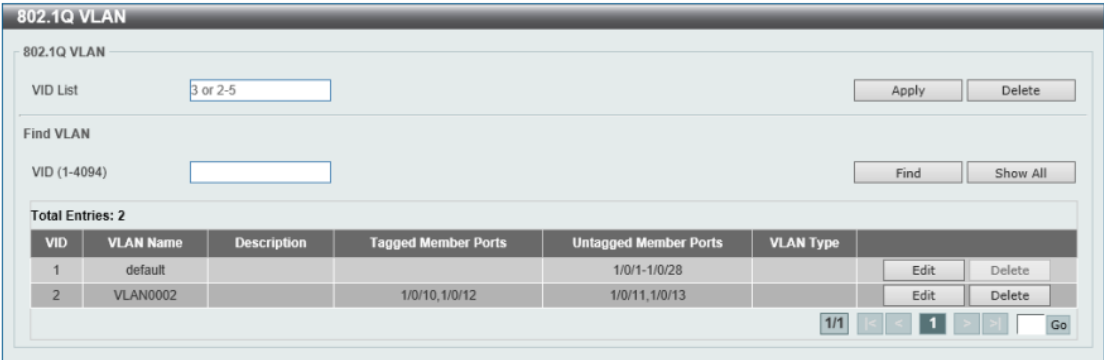


Рисунок 3.9 – Пример созданного и сконфигурированного VLAN

Configure VLAN Interface

Configure VLAN Interface

Port

VLAN Mode

Acceptable Frame

Ingress Checking

VID (1-4094)

eth1/0/2

Access

Untagged Only

☒ Enabled ☐ Disabled

1

☐ Clone

From Port

eth1/0/1

To Port

eth1/0/1

Back

Apply

По заданию, в локальной сети присутствуют IP-телефоны, а это значит что также понадобится настроить Voice VLAN. Переходим в «VLAN/Voice VLAN». Включаем Voice VLAN State, указываем VID, CoS и Aging Time.

Рисунок 3.11 – Создание Voice VLAN

Информация о системе		VLAN				
Список VLAN		Добавить Удалить				
<input type="checkbox"/>	Имя	Тип	Нетегированные порты	Тегированный порт	VLAN ID	Включено
<input type="checkbox"/>	lan	Нетегированный LAN	LAN1, LAN2, LAN3, LAN4, wifi_2G-1, wifi_5G-1	-	-	Да
<input type="checkbox"/>	wan	Нетегированный NAT	WAN	-	-	Да

34

Необходимо нажать кнопку «Добавить» и на открывшейся странице нужно ввести VID, название и выбрать подключенные порты для каждого VLAN в нашей локальной сети рисунок 3.13:

Рисунок 3.13 – Страница создания группы портов для VLAN

3.13.3 Настройка точек доступа

Настройка точек доступа выполнена после изучения руководства пользователя. На странице Device mode настраиваем режим работы (рисунок 3.14).

Рисунок 3.14 – Настройка режима работы

Далее на странице Wireless Network 2.4 GHz заполняем параметры сети (рисунок 3.15). Аналогичным образом настраиваем параметры сети 5 GHz. На странице Connections Setup / LAN выбираем IPv4 и далее во вкладке Local IP Address и вводим следующие данные в пустые поля: IP Address – 192.168.0. 43, Mask – 255.255.255.224, Gateway IP address – 192.168.0.16. Во вкладке IPv4 / Dynamic IP Addresses заполняем следующие данные (рисунок 3.16).

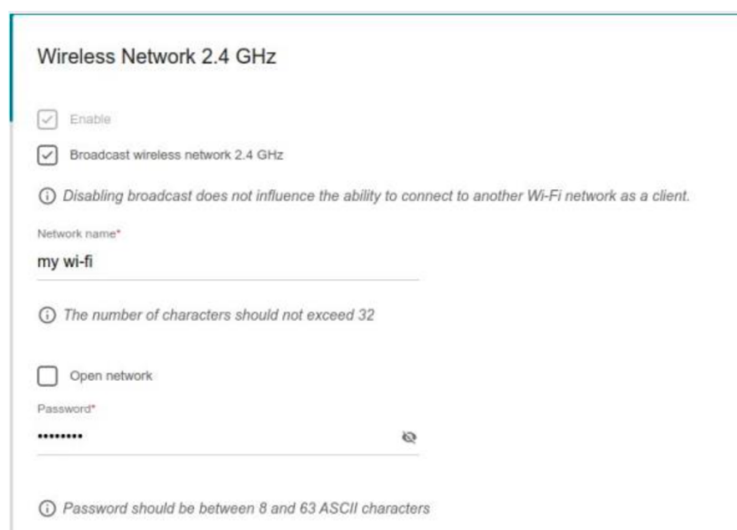


Рисунок 3.15 – Настройка сети

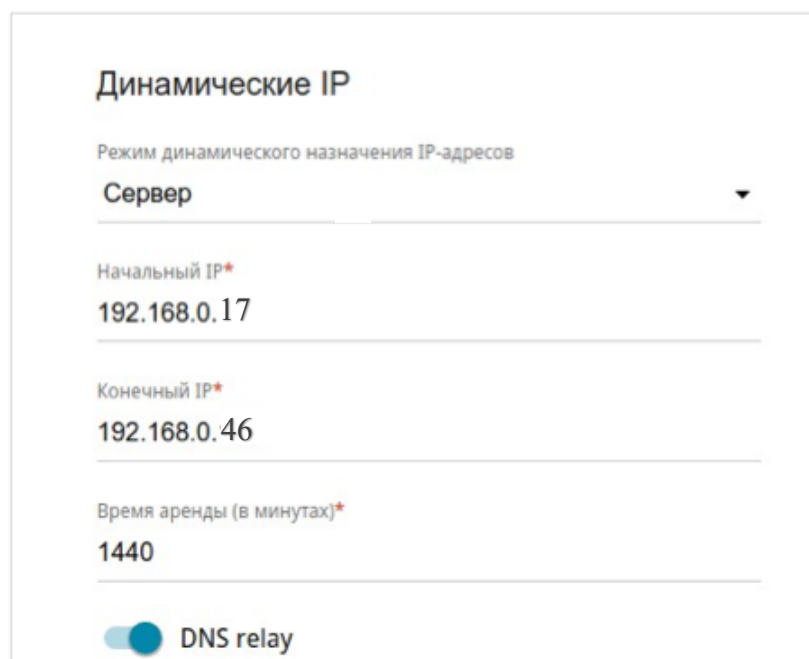


Рисунок 3.16 – Настройка DHCP

Далее на вкладке Connections Setup / LAN выбираем IPv6 и далее во вкладке Local IPv6 Address и заполняем поля: Local IPv6 Address –

2001:3456:789a:0003::43, Префикс - 64. Во вкладке IPv6 / Dynamic IPv6 Addresses заполняем следующие данные (рисунок 3.17).

Динамические IPv6

Режим динамического назначения IPv6-адресов

Stateful

(1-FFFF)*

Диапазон адресов 17 — 46 (1-FFFF)*

Время аренды (в минутах)*

5

Рисунок 3.17 - Настройка DHCPv6

3.13.4 Настройка пользовательских станций

Для настройки пользовательских станций IP-адреса назначаются автоматически через DHCP, который настроен на маршрутизаторе. Это позволяет устройствам подключаться к сети и получать параметры конфигурации, такие как IP-адрес, маска подсети, шлюз по умолчанию и адреса DNS-серверов, без необходимости ручной настройки.

Подключение станции к VLAN определяется сетевым оборудованием. Например, станции в административной подсети используют статическую настройку IP-адресов (например, для ПК администрации задается адрес 192.168.0.6), а для VLAN с беспроводным подключением и этажей 3 и 9 IP-адреса автоматически назначаются из заранее заданных диапазонов DHCP. Например, для VLAN 3 диапазон составляет 192.168.0.17–46, исключая зарезервированные адреса.

Для проверки корректности настроек пользователи могут использовать команды `ipconfig` на Windows, чтобы убедиться, что станция получила правильный IP-адрес и параметры шлюза. Завершающим этапом является тестирование подключения, например, с помощью команды `ping`, чтобы проверить доступность маршрутизатора и интернета.

Для обеспечения усиленной безопасности учетных записей пользователей в рамках настроек пользовательских станций применяются дополнительные меры. Каждой учетной записи назначается уникальный сложный пароль, соответствующий требованиям информационной безопасности университета (не менее 12 символов, использование букв разных регистров, цифр и специальных символов). Также включена двухфакторная аутентификация для учетных записей преподавателей и сотрудников, что обеспечивает дополнительный уровень защиты.

3.13.5 Настройка IP-телефонов

Для настройки IP-телефонов Yealink SIP-T31P подключаем устройства к сети через Ethernet-кабель. Телефоны могут автоматически получать IP-адреса через DHCP, но в данном случае используются статические адреса. Для телефона заведующего назначен адрес 192.168.0.130, а для телефона сотрудника – 192.168.0.131. Маска подсети для обоих устройств – 255.255.255.248, шлюз – 192.168.0.129 (адрес маршрутизатора). Чтобы вручную настроить телефон, узнаем его текущий IP-адрес через экран телефона или меню, вводим этот адрес в браузере, чтобы открыть веб-интерфейс. Авторизуемся, используя стандартные учетные данные (admin/admin), и настроим параметры SIP: адрес сервера, имя пользователя и пароль. Сохранив настройки, можно протестировать устройства, совершив пробные звонки, чтобы убедиться в их корректной работе.

3.13.6 Настройка Web-сервера

Для настройки Web-сервера необходимо выполнить несколько шагов. Первым этапом будет установка операционной системы Linux, которая обеспечит стабильную и безопасную платформу для работы сервера. После установки Linux, нужно установить Apache HTTP Server, который является популярным веб-сервером, поддерживающим множество функций для хостинга веб-сайтов и приложений.

Для установки Apache HTTP Server выполним следующие команды:

```
sudo apt update
sudo apt install apache2
```

После успешной установки сервера необходимо настроить сетевой интерфейс. Для этого нужно настроить IP-адрес для интерфейса, который будет использоваться для подключения к сети. Настройка статического IPv4 и IPv6 адреса для интерфейса eth1:

```
ifconfig eth1 192.168.0.7 netmask 255.255.255.240
ifconfig eth1 inet6 static address 2001:3456:789a:0002::7
netmask 64
```

После этого сервер Apache будет готов к использованию.

3.13.7 Настройка принтеров

Для настройки принтеров Xerox B225DNI, которые находятся на 3-м этаже у заведующего и сотрудников, а также на 9-м этаже у сотрудников, выполним ряд следующих действий. Подключаем принтеры к сети через Ethernet или Wi-Fi в зависимости от их расположения. Дальше нужно зайти в

панель управления, выбрать раздел «Устройства и принтеры» и нажать на кнопку «Добавить устройство». Выполнится поиск принтеров, после чего появится нужный принтер. Нужно нажать на него, тогда выполнится автоматическая настройка и установка принтера. После этих манипуляций принтер будет готов к работе.

3.14 Обоснование выбора пассивного оборудования

Пассивное сетевое оборудование включает в себя устройства, не требующие подключения к электрической сети и не выполняющие преобразование сигналов, но обеспечивающие их передачу, усиление и защиту. К таким устройствам относятся кабели, информационные розетки, телекоммуникационные стойки и другие элементы.

В данном проекте используется кабель категории 5е, который обеспечивает поддержку скорости передачи данных до 1 Гбит/с, что идеально подходит для большинства подключений в сети. Этот кабель соответствует стандартам 10/100/1000BASE-T и имеет максимальную длину передачи до 100 метров при использовании 1000BASE-T. Для удовлетворения требований заказчика по повышенной пожарной безопасности был выбран кабель U/UTP REXANT CAT 5е ZH нг(А)-HF 4PR 24AWG. Маркировка ZH нг(А)-HF указывает на отсутствие галогенов в оболочке кабеля и на его низкую горючесть, что значительно снижает риск распространения огня и токсичных газов при возгорании.

Для прокладки кабелей, учитывая диаметр проводников (24AWG), выбраны кабельные короба следующих размеров: 25х16 для прокладки между этажами и 60х40 для подключения к розеткам. Эти короба произведены из огнестойкого ПВХ и эффективно изолируют проводники, защищая их от механических повреждений и предотвращая короткие замыкания. Для монтажа использованы коннекторы Geplink GL4701 RJ45 и информационные розетки PST00 39047, которые обеспечивают надежное подключение и соответствуют стандартам безопасности.

Для обеспечения пожарной безопасности на объекте выбраны кабельные короба Ecoplast INSTA 60х40, E15-E110 и Ecoplast 25х16, E15-E110, которые имеют повышенные характеристики огнестойкости и эффективно защищают кабели в случае пожара.

4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

При проектировании локальной сети для объекта с повышенными требованиями пожарной безопасности необходимо учитывать особенности размещения и монтажа кабельной системы. Основой системы является прокладка кабелей, обеспечивающих соединение оборудования и устройств, с соблюдением требований безопасности и эксплуатационной надежности.

Для данного проекта используется кабель категории UTP (витая пара) с огнестойким покрытием. Кабели прокладываются в металлических кабель-каналах с огнеупорным исполнением, которые монтируются вдоль стен на высоте 30 см от потолка. Это обеспечивает защиту от механических повреждений и соответствуют нормам пожарной безопасности. При необходимости пересечения стен используются специальные огнестойкие вводы, заполненные герметикам, препятствующим распространению огня.

Информационные розетки устанавливаются на высоте 30 см от пола. Кабель подводится к ним вертикально от основного канала. Все соединения внутри розеток и шкафов выполняются с использованием негорючих компонентов.

Кабельные трассы между этажами организуются через специально выделенные шахты с огнезащитными уплотнителями. Это предотвращает распространение огня и дыма между этажами. Для Wi-Fi точек доступа, размещаемых по две на каждом этаже, кабели проводятся над фальш-потолком в металлических лотках с защитным покрытием.

Серверное оборудование, маршрутизатор и коммутаторы размещаются в телекоммуникационных шкафах с противопожарной защитой. Шкафы оборудуются системой контроля температуры и дымоудаления, что минимизирует риск возгорания. Шкафы устанавливаются на высоте 150 см от пола для удобства обслуживания.

Рабочие станции и принтеры подключаются к розеткам через кабели, также выполненные в огнестойком исполнении. Все участки сети маркируются для упрощения обслуживания и быстрого реагирования в случае чрезвычайной ситуации.

Со схемой плана этажа можно ознакомиться в приложении В, Г.

ЗАКЛЮЧЕНИЕ

В рамках курсового проекта была разработана локальная сеть для кафедры университета, предназначенная для обучения студентов основам программирования. Для обеспечения стабильной и эффективной работы сети был проведен анализ рынка сетевых устройств, на основе которого было выбрано оборудование, соответствующее потребностям образовательного учреждения.

Процесс выбора включал оценку различных характеристик и возможностей устройств, таких как маршрутизаторы, коммутаторы и точки доступа, с акцентом на их производительность, масштабируемость, надежность и безопасность. Учитывались такие факторы, как поддержка современных стандартов связи, возможность сегментации сети, а также удобство управления и настройки оборудования.

В результате был выбран оптимальный набор устройств, который обеспечивает необходимую скорость передачи данных, стабильность работы и поддержку большого числа пользователей. Выбор оборудования также был обоснован его долговечностью, доступностью и возможностью модернизации в будущем, что позволит обеспечить долгосрочную эксплуатацию сети.

Проектирование и создание локальной сети для кафедры не только улучшает текущие условия работы, но и закладывает фундамент для будущих технологических решений. Разработанная сеть станет неотъемлемой частью образовательной инфраструктуры, поддерживая эффективный обмен данными, доступ к онлайн-ресурсам и удаленным сервисам. В перспективе сеть может быть расширена с учетом новых образовательных технологий и научных исследований, что будет способствовать росту и развитию кафедры в целом.

Таким образом, реализованный проект по созданию локальной сети на кафедре университета отвечает современным требованиям и создает условия для качественного образовательного процесса, обеспечивая студентов и преподавателей надежными инструментами для работы и коммуникации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- [1] Вычислительные машины, системы и сети: дипломное проектирование (методическое пособие) [Электронный ресурс]. – 2019 – Режим доступа: <https://www.bsuir.by/m/121002291136308.pdf> – Дата доступа: 17.09.2024.
- [2] Таненбаум, Э. Компьютерные сети. 6-е издание / Э.Таненбаум, Н. Фимстер, Д. Уэзеролл – Спб: Питер, 2023. – 1174 с.
- [3] Виртуальные локальные сети [Электронный ресурс]. – Режим доступа: <https://www.ibm.com/docs/ru/aix/7.2?topic=cards-virtual-local-area-networks/> – Дата доступа: 20.09.2024.
- [4] D-Link DSL-245GR R1A. Руководство пользователя [Электронный ресурс]. – Режим доступа: https://ftp.dlink.ru/pub/ADSL/DSL-245GR/Data_sh/DSL-245GR_R1_DS_4.0.2_27.12.21_RU.pdf.
- [5] Сервер HP ProLiant DL380 Gen9. Описание оборудования [Электронный ресурс]. – Режим доступа: <https://forpro.by/product/server-hp-proliant-dl380-gen9-24sff-2xxeon-e5-2699v422-core-2-2-3-6-ghz-96gt-s-512gb-p440-2x800w>.
- [6] Yealink SIP-T31P. Описание IP-телефонов [Электронный ресурс]. – Режим доступа: <https://www.yealink.com/website-service/attachment/product/documents/20230906/2023090602445121815cb7eb748cfa8f6490431981595.pdf>.
- [7] D-Link DWL-6610AP. Руководство пользователя [Электронный ресурс]. – Режим доступа: https://ftp.dlink.ru/pub/Wireless/DWL-6610AP/Data_sh/DS_DWL-6610AP_B1_A1_RUS.pdf
- [8] D-Link DGS-1100-24PV2. Коммутатор уровня 2 [Электронный ресурс]. – Режим доступа: <https://www.dlink.ru/ru/products/1366/2462.html>.
- [9] Документация для принтеров Xerox B225DNI [Электронный ресурс]. – Режим доступа: https://download.support.xerox.com/pub/docs/B225/userdocs/any-os/ru/xerox_b225_bB235_mfp_qrg_ru-RU.pdf
- [10] Классификация компьютерных сетей [электронный ресурс]. – Режим доступа: http://dit.isuct.ru/IVT/sitanov/Literatura/InformLes/Pages/Glava5_2.htm.
- [11] UTP [электронный ресурс]. Режим доступа: https://its.dlink.co.in/assets/patt_1529307287.pdf.

ПРИЛОЖЕНИЕ А
(обязательное)

Схема СКС структурная

ПРИЛОЖЕНИЕ Б
(обязательное)

Схема СКС функциональная

ПРИЛОЖЕНИЕ В
(обязательное)

План этажа

ПРИЛОЖЕНИЕ Г
(обязательное)

План этажа

ПРИЛОЖЕНИЕ Д
(обязательное)

Перечень оборудования

ПРИЛОЖЕНИЕ Е
(обязательное)

Ведомость документов