# *ВВЕДЕНИЕ*

*Курсовой проект представляет собой работу, основанную на построение двух зданий, проведении в них локальной вычислительной сети (ЛВС) и подсчете затрат.*

*Локальная вычислительная сеть — компьютерная сеть, которая обычно покрывает относительно небольшую территорию или небольшую группу зданий. Ее задача состоит в том, чтобы обрабатывать, хранить и передавать данные. Представляет собой кабельную систему здания или группы зданий. На данный момент трудно представить работу современного офиса без локальной вычислительной сети, а без информационно-вычислительной сети сейчас не обходится ни одно предприятие.*

*Структурированная кабельная сеть – физическая основа инфраструктуры здания, позволяющая свести в общую систему множество сетевых информационных сервисов разного назначения: локальные вычислительные сети и телефонные сети, системы безопасности, видеонаблюдения и т.д. В нее входит набор кабелей и коммутационного оборудования, и методика их совместного использования, которая позволяет создавать структуры связей в локальных сетях разного назначения.[1]*

*Локальная вычислительная система позволяет организовать общий доступ в интернет без, настроить сервер или установить программу для обмена мгновенными сообщениями. Так же локальная система предоставляет возможность сотрудникам совместно трудиться над документами и проектами на сервере, не создавая дубликатов и копий. Компания, в свою очередь, экономит на стоимости расходных материалов, приобретая сетевой принтер или сканер.*

*Компьютеры соединяются между собой, используя различное оборудование: медные проводники (витая пара), оптические проводники (оптические кабели) и через радиоканал (беспроводные технологии). Проводные, оптические связи устанавливаются посредством “Ethernet”. Отдельная локальная вычислительная сеть может иметь связь и с другими локальными сетями с использованием шлюзов, а также быть частью и иметь доступ к глобальной сети Интернет.*

*Создание и проектирование структурированной кабельной сети – это разработка документации, где описана структура сети и ее топология, имеются схема расположения конечных устройств пользователей, компьютерных розеток и характеристики оборудования для построения ЛВС.*

*Принципами проектирования локальной вычислительной сети являются обеспечение высокой скорости и безопасности передачи данных. Учитывая необходимые требования, инженеры-проектировщики выбирают максимально подходящее сетевое оборудование и операционная система для сервера и пользовательских устройств.*

# *ЗАКЛЮЧЕНИЕ*

*При проектировании основной задачей является разработка инженерных решений и подготовка инфраструктуры помещений, включающая в себя подготовку кабельных трасс для установки структурированных кабельных систем. Проектирование сети является сложным и трудоемким процессом, который требует инженерного мышления и творческого подхода.*

*Анализ выполненной работы позволил достичь следующих целей:*

* *Выбранная схема расположения рабочих мест соответствует стандартам и может быть легко изменена.*
* *В проекте предусмотрены рекомендации по защите рабочих мест, которые могут быть изменены системным администратором. Использование программируемого коммутатора позволяет эффективно управлять сетью и повысить ее производительность.*

*Сам проект включает чертежи зданий с расположением рабочих мест и трассировкой по этажам, моделирование компьютерной сети с использованием Cisco Packet Tracer и соответствующую документацию. Все расчеты в проекте выполнены с высокой точностью, исключая риск неправильной оценки стоимости.*

*В результате был создан проект, реализующий поставленную задачу. Были спроектированы подсистема рабочего места, горизонтальная и административная подсистемы. Выполнены расчеты необходимого оборудования и материалов, обоснован выбор активного оборудования, топологии сети, используемых протоколов и размещения рабочих мест. Учтены правила пожарной безопасности.*

1. ***ПОСТАНОВКА ТЕХНИЧЕСКОГО ЗАДАНИЯ***
   1. *Описание предметной области*

*Локальная вычислительная сеть (ЛВС) представляет собой группу компьютеров и других устройств, объединенных в пределах ограниченной территории для совместного использования ресурсов и обмена данными. Такие сети широко применяются в офисах, образовательных учреждениях, промышленных предприятиях и даже в домашних условиях. Основное назначение ЛВС — обеспечение эффективного взаимодействия между устройствами, повышение производительности работы и оптимизация использования ресурсов.*

*Для функционирования локальной сети требуется совокупность аппаратных и программных компонентов. Рассмотрим их подробнее.*

*Аппаратные компоненты:*

* *Абонентские устройства: компьютеры (рабочие станции), серверы, принтеры, сканеры и другие периферийные устройства.*
* *Сетевое оборудование: сетевые адаптеры (NIC), обеспечивающие подключение устройств к сети.*
* *Коммутаторы (switches), которые соединяют устройства внутри одного сегмента сети.*
* *Маршрутизаторы (routers), отвечающие за передачу данных между различными сетями.*
* *Концентраторы (hubs) и мосты (bridges), используемые для объединения сегментов сети.*
* *Коммуникационные каналы: кабели (например, витая пара или оптоволокно) и беспроводные технологии (Wi-Fi).*

*Программные компоненты:*

* *Сетевые операционные системы (например, Windows Server, Linux).*
* *Протоколы передачи данных (TCP/IP, FTP, HTTP).*
* *Сетевые службы, такие как DHCP, DNS и файловые серверы.*

*Локальные сети классифицируются по нескольким признакам:*

*По архитектуре:*

* *Одноранговые сети: все устройства равноправны и могут выступать как клиентами, так и серверами.*
* *Сети с выделенным сервером: один или несколько серверов управляют всей сетью и предоставляют ресурсы клиентам.*

*По способу подключения:*

* *Проводные сети: используют кабели для передачи данных.*
* *Беспроводные сети: основаны на технологиях Wi-Fi или Bluetooth.*

*По топологии:*

* *Звезда: все устройства подключены к центральному узлу (коммутатору или маршрутизатору).*
* *Шина: устройства подключены к общему каналу передачи данных.*
* *Кольцо: данные передаются по замкнутому контуру.*
* *Древовидная или смешанная топология: комбинация нескольких схем.*

*Функции компонентов ЛВС*

* *Серверы:*

*Серверы являются ключевыми элементами в сетях с выделенным сервером. Они выполняют такие задачи как хранение данных и управление доступом к ним, обеспечение работы приложений и баз данных, управление периферийными устройствами.  
Серверы размещаются в специально оборудованных помещениях – дата-центрах – или в офисах с подключением к источникам бесперебойного питания.*

* *Маршрутизаторы:  
  Маршрутизаторы обеспечивают связь между различными сетями, включая доступ к Интернету. Они используют таблицы маршрутизации для выбора оптимального пути передачи данных.*
* *Коммутаторы:  
  Коммутаторы объединяют устройства внутри одного сегмента сети, обеспечивая передачу данных между ними без коллизий.*
* *Клиентские устройства:  
  Рабочие станции пользователей подключаются к ЛВС для доступа к общим ресурсам – файлам, принтерам, базам данных.*
  1. *Обоснование необходимости проектирования ЛВС*

Проектирование локальной вычислительной сети (ЛВС) является важным этапом в создании эффективной и безопасной информационной инфраструктуры компании. ЛВС предоставляет возможность значительно повысить уровень безопасности корпоративных данных. Системный администратор может настроить индивидуальные уровни доступа для каждого сотрудника в зависимости от его должностных обязанностей и потребностей. Это позволяет ограничить доступ к конфиденциальной информации и минимизировать риски утечек данных или несанкционированного доступа.

*Еще одним важным преимуществом ЛВС является снижение затрат на программное обеспечение и его лицензирование. Вместо установки и обновления приложений на каждом компьютере, они могут быть централизованно размещены на сервере. Сотрудники получают доступ к этим программам через сеть, что упрощает управление программным обеспечением, ускоряет процесс обновлений и сокращает расходы компании.*

*Современные ЛВС также позволяют интегрировать облачные технологии для хранения данных и резервного копирования. Это обеспечивает надежную защиту информации, а также снижает вероятность потери данных в случае аппаратных сбоев или других непредвиденных обстоятельств. Использование облачных решений делает сеть более устойчивой и безопасной.*

*Однако, несмотря на преимущества, ЛВС имеет и определенные недостатки. Например, работа сети может быть нарушена в случае выхода из строя сервера или возникновения проблем с подключением.*

*Кроме того, локальные сети требуют регулярного технического обслуживания, модернизации оборудования и обновления программного обеспечения для обеспечения их стабильной работы.*

*Для успешного функционирования ЛВС необходим квалифицированный специалист — системный администратор.*

*Он отвечает за настройку сети, установку оборудования (таких как маршрутизаторы, коммутаторы, точки доступа и принтеры), а также за ее обслуживание. Системный администратор также занимается устранением возникающих проблем и обеспечивает бесперебойную работу сети.*

*Настройка и поддержка ЛВС представляет собой сложный процесс, требующий учета множества факторов. Среди них:*

* *Общее количество устройств, которые будут подключены к сети.*
* *Типы приложений, которые планируется использовать.*
* *Уровень безопасности данных, необходимый для защиты корпоративной информации.*
* *Пропускная способность сети для обеспечения стабильной работы всех пользователей.*

*Таким образом, необходимость проектирования ЛВС обусловлена не только стремлением оптимизировать использование ресурсов компании, но и обеспечением высокой надежности, безопасности и производительности информационной инфраструктуры. Правильно спроектированная локальная сеть становится основой для эффективной работы организации.*

1. ***Разработка конфигурации локальной вычислительной сети***
   1. *Обзор существующих топологий локальных вычислительных сетей*

*Под топологией сети понимается описание ее физического расположения, а именно, как компьютеры соединены друг с другом в сети, и с помощью каких устройств входят в физическую топологию. Существуют четыре основных топологии: шина (Bus), кольцо (Ring), звезда (Star) и ячеистая топология (Mesh). Другие топологии обычно являются комбинацией двух и более главных типов. Выбор топологии основывается на множестве факторов, в число которых входят цена, расстояния, вопросы безопасности, предполагаемая сетевая операционная система, а также будет ли новая сеть использовать существующее оборудование, проводку и т. п.*

*Физическая топология "шина" состоит из единственного кабеля, к которому присоединены все компьютеры сегмента. Сообщения посылаются по линии всем подключенным станциям вне зависимости от того, кто является получателем. Каждый компьютер проверяет каждый пакет в проводе, чтобы определить получателя пакета. Если пакет предназначен для другой станции, компьютер отвергнет его. Шинная топология – это хороший способ быстрого построения временной сети. Это обычно лучший выбор для малых сетей (не более 10 компьютеров).*

*Топология "кольцо" (Ring) обычно используется в сетях Token Ring и FDDI (волоконно-оптических). В физической топологии Ring линия передачи данных фактически образует логическое кольцо, к которому подключены все компьютеры сети. В отличие от шинной топологии, которая использует конкурентную схему, чтобы позволить станциям получать доступ к сетевому носителю, доступ к носителю в кольце осуществляется посредством логических знаков - “маркеров”, которые пускаются по кругу от станции, к станции, давая им возможность переслать пакет, если это нужно. Компьютер может посылать данные только тогда, когда владеет маркером. Однако из-за того, что все маркеры пускаются по кругу, с течением времени могут образовываться «блуждающие» сигналы, загрязняющие сеть.*

*В топологии "звезда" (Star) все компьютеры в сети соединены друг с другом с помощью центрального концентратора. Все данные, которые посылает станция, направляются прямо на концентратор, который затем пересылает пакет в направлении получателя. Как и при шинной топологии, компьютер в сети типа "звезда" может пытаться послать данные в любой момент. Однако на деле только один компьютер может в конкретный момент времени производить посылку. Если две станции посылают сигналы на концентратор точно в одно время, обе посылки окажутся неудачными и каждому компьютеру придется подождать случайный период времени, прежде чем снова пытаться получить доступ к носителю. Сети с топологией Star обычно лучше масштабируются, чем другие типы.*

*Ячеистая топология (Mesh) соединяет все компьютеры попарно. Сети ячеистой топологии используют значительно большее количество кабеля, чем любая другая топология, что делает их дороже. Кроме того, такие сети значительно сложнее устанавливать, чем другие топологии. Однако ячеистая топология устойчива к сбоям. Устойчивость к сбоям заключается в способности работать при наличии повреждений. В сети с поврежденным сегментом это означает обход сегмента. Каждый компьютер имеет множество возможных путей соединения с другим компьютером по сети, так что отдельный обрыв кабеля не приведет к потере соединения между любыми двумя компьютерами.*

* 1. *Описание используемой топологии проектируемой компьютерной сети*

***Топология дерева: определение, структура и функциональные особенности***

*Дерево представляет собой топологию сетей, в которой каждый узел более высокого уровня соединен со своим множеством дочерних узлов посредством звездообразной связи. Такая структура формирует иерархическую систему, где ключевое звено – корневой узел – становится отправной точкой для распространения сигналов, контроля и управления сетью. Каждый следующий уровень сети организован по принципу «родитель–дочерний», где родительские узлы объединяют группу устройств или подсетей, действуя как концентраторы для управления трафиком и распределения ресурсов. Таким образом, топология дерева фактически представляет собой комбинацию двух известных схем: звезды и шины, что позволяет использовать сильные стороны каждой из них в одном решении.*

*Подобная организация сети получила свое название из теории графов, где корневой узел выбирается первым, а последующие уровни получают имена родительских и дочерних. Каждый дочерний узел, обладая возможностью подключения к еще более низким уровням, одновременно становится родительским для своей группы. Такая стратификация особенно важна для крупных корпоративных сетей, где необходимо обеспечить логическую сегментацию и управляемость сложных систем. Благодаря своему иерархическому устройству, дерево позволяет разделить сеть на независимые подсети, упростить диагностику неисправностей и четко распределить нагрузку между узлами.*

***Преимущества топологии дерева***

1. ***Масштабируемость и расширяемость***

*Одним из главных достоинств топологии дерева является ее легкая масштабируемость. При появлении новых пользователей или устройств сеть можно расширять, просто добавляя дополнительные уровни или ветви. Такое решение позволяет избежать полного пересмотра архитектуры сети, что существенно снижает затраты и временные ресурсы при модернизации системы. Каждая новая ветвь сети интегрируется в существующую структуру, сохраняя общую иерархическую схему и делая обслуживание более предсказуемым.*

1. ***Упрощенное управление и модульность***

*Благодаря наличию четко структурированных уровней, можно внедрить централизованные системы контроля и мониторинга. В случае возникших проблем или сбоев достаточно локализовать неисправность в определенном сегменте, не затрагивая всю сеть. Такой подход облегчает работу специалистов по техническому обслуживанию и позволяет проводить диагностику, ремонт или модернизацию с минимальным воздействием на остальную часть системы.*

1. ***Логическая сегментация и безопасность***

*Иерархическая структура позволяет разделить сеть на отдельные подсети или сегменты, что особенно важно для крупных организаций. Каждая подсеть может иметь свои политики безопасности, разграничение прав доступа и специализированные параметры работы. Такое разделение помогает не только повысить безопасность, но и повысить производительность за счет уменьшения количества конфликтов и избыточного трафика между независимыми сегментами.*

1. ***Удобство при реализации конечных устройств***

*При использовании активных узлов, таких как компьютеры, в роли участников сети, топология дерева позволяет обеспечить высокую степень распределенного управления. Каждый узел работает не только как передатчик данных, но и как элемент контроля, что позволяет сделать сеть более динамичной. При этом благодаря звездообразному распределению сигналов, легко организовать резервирование и построение отказоустойчивых цепочек передачи данных.*

***3.1 Оценочный расчет количества и размещение рабочих мест в помещениях зданий с учётом санитарных норм и правил***

*Санитарно-гигиенические нормы и правила организации рабочих мест устанавливаются соответствующими нормативными документами (СанПиН, СНиП и ведомственными регламентами). В них прописаны требования к обеспечению благоприятного микроклимата, освещённости, уровню шума, а также к параметрам планировки, размещения мебели и техники. Особое значение при этих требованиях уделяется адекватной площади рабочего места, поскольку пространство напрямую влияет на возможность правильного расположения компьютера, периферийных устройств и средств для коррекции осанки. Нормативными документами предусмотрены разные значения минимальной площади в зависимости от технологических особенностей оборудования: при использовании плоских ЖК-мониторов минимальная площадь может составлять около 4,5 м2, тогда как для более массивных ЭЛТ-мониторов стандарты требуют до 6 м2 на одного сотрудника.*

*Организация рабочего места должна учитывать не только размеры поверхности стола, но и свободное пространство для перемещения сотрудника. Согласно нормативам, рабочее место с компьютером должно предусматривать:*

* *Достаточную площадь стола для расположения системного блока, монитора, клавиатуры, мыши, а также дополнительного оборудования;*
* *Свободную рабочую поверхность, позволяющую размещать документы и другие необходимые предметы без стеснения движений;*
* *Зону, обеспечивающую возможность правильной посадки за столом, а также свободное перемещение рук и ног.*

*Дополнительные требования к пространству касаются не только общей площади, но и правильной расстановки оборудования:*

* *Компьютерный монитор должен располагаться на расстоянии, обеспечивающем комфортное восприятие изображения, что требует соблюдения горизонтальных и вертикальных параметров (на уровне глаз и на расстоянии 50-70 см от глаз);*
* *Между рабочими местами должно быть обеспечено расстояние, позволяющее не создавать неудобства и «заставлять» сотрудника пересекать рабочие зоны коллег;*
* *Углы наклона монитора, высота стола и кресла подбираются таким образом, чтобы минимизировать нагрузку на глаза, спину и шею, а в совокупности с поверхностью рабочего места это позволяет создать благоприятное для труда пространство.*

*Эти требования продиктованы не только санитарными нормами, но и современными стандартами эргономики, которые учитывают специфику длительной работы за компьютером.*

*Данные, используемые в таблице 3.1, были выбраны в соответствии с этими нормами.*

*3.2 Размещение рабочих мест в помещениях зданий*

*Санитарно-гигиенические нормы и правила для организации рабочих мест регулируются различными нормативными документами, такими как СанПиН, СНиП и ведомственные регламенты. Эти документы содержат требования к созданию благоприятного микроклимата, уровню освещения и шума, а также к планировке и размещению мебели и техники. Существенным аспектом является адекватная площадь рабочего места, так как она напрямую влияет на правильное расположение компьютера, периферийных устройств и средств для коррекции осанки.*

*Минимальная площадь рабочего места зависит от типа оборудования: для плоских ЖК-мониторов она составляет около 4,5 м², а для более громоздких ЭЛТ-мониторов требуется до 6 м² на одного сотрудника. При организации рабочего места необходимо учитывать не только размеры стола, но и свободное пространство для передвижения. Рабочее место с компьютером должно обеспечивать достаточную площадь стола для размещения системного блока, монитора, клавиатуры, мыши и дополнительного оборудования. Также важно предусмотреть свободную рабочую поверхность для документов и других необходимых предметов, а также зону, позволяющую правильно сидеть за столом и свободно перемещать руки и ноги.*

***3.3 Проектирование горизонтальной подсистемы***

*Горизонтальная подсистема сети представляет собой физическое соединение между телекоммуникационными разъемами на рабочих местах и телекоммуникационными помещениями в здании. Она играет ключевую роль в локальной вычислительной сети, обеспечивая передачу данных между компьютерами и другими устройствами внутри здания.*

*Эта подсистема включает горизонтальные кабели, розетки, патч-корды и патч-панели. Обычно она соединяется с магистральной подсистемой через серверные помещения.*

*При расчете подсистем важно учитывать основные характеристики зданий в соответствии с санитарными нормами. Необходимо принять во внимание следующие параметры: высота коммутационного шкафа (КШ) должна составлять 1,8 м; высота коммутационной стойки (КС) — 0,7 м; высота установки розеток — 0,4 м; глубина кабеля в напольной розетке — 0,1 м; расстояние между двумя напольными розетками — 0,4 м.*

*Для расчета длины кабеля в горизонтальной подсистеме, использующей витую пару, к итоговому результату добавляется 10% в качестве запаса на случай необходимости удлинения кабеля.*

*3.4 Проектирование вертикальной подсистемы*

*Вертикальная подсистема играет важную роль в обеспечении связи между различными уровнями сети, начиная от корневого узла и заканчивая конечными устройствами. Она функционирует как логическое продолжение горизонтальной интеграции, что позволяет объединять несколько горизонтальных подсистем (например, этажей) в единую сеть, увеличивая ее масштабируемость и оптимизируя маршрутизацию данных.*

*Процесс разработки вертикальной подсистемы начинается с анализа эксплуатационных требований. Это включает в себя необходимую пропускную способность, уровень надежности, возможность масштабирования и приоритет обработки трафика. Корневой узел, который является центром управления, должен агрегировать потоки, поступающие с распределительных уровней, и одновременно поддерживать связь с внешними каналами. Эффективная работа горизонтальной подсистемы, обеспечивающей локальную маршрутизацию и сегментацию трафика, способствует наладке вертикального взаимодействия между уровнями сети.*

*3.5 Проектирование магистральной подсистемы*

*Магистральная подсистема играет ключевую роль в информационной системе, соединяя горизонтальные и вертикальные уровни сети в единую инфраструктуру. Её основная функция заключается в обеспечении надежной и высокоскоростной передачи данных между различными узлами сети, а также в организации централизованного управления трафиком. Это становится особенно важным при увеличении числа подключенных рабочих мест и объёмов передаваемой информации.*

*Магистраль должна эффективно агрегировать информационные потоки от рабочих мест и распределительных узлов, обеспечивая стабильное соединение для выполнения различных задач. Оптимизация маршрутов передачи данных позволяет уменьшить задержки в сети, что особенно критично для видеоконференций, облачных сервисов и приложений, работающих в реальном времени.*

*Для магистральной подсистемы необходимо использовать высокопроизводительные маршрутизаторы и коммутаторы, которые способны работать на скоростях 10 Гбит/с и выше. Применение оптоволоконных линий связи гарантирует надежную передачу данных на большие расстояния. Рекомендуется выбирать устройства, поддерживающие протоколы динамической маршрутизации, такие как OSPF и BGP, для автоматизированного управления маршрутами и балансировки нагрузки.*

**4. СЕТЕВЫЕ УСТРОЙСТВА: ТИПЫ СЕТЕВЫХ УСТРОЙСТВ И ИХ ФУНКЦИИ**

**4.1 Пассивное сетевое оборудование**

Пассивное сетевое оборудование представляет собой базовые элементы сети, функционирующие без необходимости электропитания. В отличие от активных устройств, оно не обрабатывает и не преобразует сигналы, а служит физической основой для их передачи между компонентами сети. Главная задача таких компонентов – обеспечить надежное соединение с минимальными потерями данных, не влияя на характеристики сигнала.

Основу пассивной инфраструктуры составляют кабельные системы, включающие витую пару, оптоволоконные и коаксиальные кабели. Эти элементы выступают в роли магистралей для передачи информации между устройствами. Для их соединения используются различные типы разъемов – RJ-45 для медных кабелей, LC и SC для оптических линий. Особое место занимают готовые коммутационные шнуры (патч-корды), которые упрощают подключение оборудования в серверных стойках и распределительных узлах.

Важным компонентом структурированных кабельных систем являются патч-панели, позволяющие организовать порядок в коммутационных узлах и обеспечить удобное подключение активного оборудования. Для ручного управления соединениями применяются кросс-панели, а для защиты и правильной прокладки кабелей – специальные лотки и короба.

Телекоммуникационные шкафы и стойки служат для компактного и безопасного размещения как активного, так и пассивного оборудования. В беспроводных сетях используются пассивные антенны, которые усиливают сигнал без дополнительного питания.

Качество пассивных компонентов напрямую влияет на стабильность и производительность сети. Они не требуют сложной настройки или обслуживания, но являются фундаментом, от которого зависит долговечность и надежность всей инфраструктуры. Правильно спроектированная пассивная система позволяет минимизировать помехи, обеспечить высокую скорость передачи данных и упростить масштабирование сети в будущем.

Дополнительно стоит отметить, что при выборе пассивного оборудования важно учитывать стандарты качества и совместимость с активными компонентами сети. Современные решения предлагают улучшенные характеристики, такие как повышенная помехозащищенность кабелей или удобство монтажа патч-панелей, что в итоге снижает затраты на эксплуатацию и повышает отказоустойчивость системы.

Кроме того, пассивное оборудование играет ключевую роль в обеспечении безопасности сети. Например, экранированные кабели и разъемы помогают снизить влияние электромагнитных помех, а качественные монтажные решения предотвращают повреждение кабелей при длительной эксплуатации. При проектировании сети также важно учитывать будущие потребности, такие как возможность добавления новых линий связи или увеличение пропускной способности без замены всей инфраструктуры.

Еще одним важным аспектом является соответствие международным стандартам, таким как TIA/EIA, ISO/IEC и другим, что гарантирует совместимость оборудования и его надежность. Использование сертифицированных компонентов минимизирует риски возникновения неисправностей и обеспечивает стабильную работу сети на протяжении многих лет.

Таким образом, пассивное сетевое оборудование, хотя и не требует питания и сложного управления, является критически важным элементом любой ИТ-инфраструктуры. Его правильный выбор, монтаж и обслуживание позволяют создать устойчивую, производительную и масштабируемую сеть, способную поддерживать современные технологии передачи данных.

**4.2 Выбор пассивного сетевого оборудования используемого при проектировании локальной вычислительной сети**

В рамках данного курсового проекта в качестве кабельных сегментов вертикальной подсистемы был выбран кабель UTP Cat5e, обеспечивающий высокоскоростной доступ в интернет. Максимальная скорость передачи данных достигает 1000 Мбит/с. Кабель содержит 4 пары проводников и не является экранированным. Материал проводника – алюминий, а наружная оболочка выполнена из поливинилхлорида. В проекте используется кабель U/UTP Cat5e 4х2х24AWG CCA.

Расположение розеток будет осуществляться в соответствии с заранее подготовленным планом размещения рабочих мест. Для подключения будут использоваться информационные розетки Schneider Electric W59 RSI-152K5E-5-86. Связь между компьютерами и розетками будет осуществляться с помощью патч-кордов UTP Cat5e длиной 1 метр.

**4.3 Типы активного сетевого оборудования**

Активные сетевые устройства представляют собой интеллектуальную основу современных компьютерных сетей, обеспечивая не только передачу данных, но и их обработку, анализ и оптимальное распределение. В отличие от пассивного оборудования, эти устройства требуют электропитания и обладают программной начинкой, позволяющей выполнять сложные функции управления сетевым трафиком. Современные активные устройства сочетают в себе высокую производительность, расширенные функции безопасности и гибкие возможности масштабирования, что делает их незаменимыми компонентами любой сетевой инфраструктуры.

Коммутаторы (свитчи) являются ключевыми элементами локальных сетей, обеспечивающими эффективную передачу данных между узлами на канальном уровне модели OSI. Современные управляемые коммутаторы обладают широким функционалом, включая поддержку VLAN, QoS, агрегирование каналов и мониторинг трафика. Многоуровневые коммутаторы (L3) дополнительно выполняют функции базовой маршрутизации, что позволяет оптимизировать работу средних и крупных сетей. Важной особенностью современных коммутаторов является поддержка технологий PoE (Power over Ethernet), позволяющих питать подключенные устройства через сетевой кабель.

Маршрутизаторы выполняют критически важную функцию соединения различных сетей и сетевых сегментов, работая на сетевом уровне модели OSI. Современные маршрутизаторы оснащены мощными процессорами, способными обрабатывать десятки тысяч пакетов в секунду, и поддерживают сложные протоколы динамической маршрутизации (OSPF, BGP). Дополнительно они обеспечивают функции межсетевого экранирования, VPN-туннелирования и балансировки нагрузки. Корпоративные маршрутизаторы часто включают в себя встроенные системы предотвращения вторжений (IPS) и защиты от DDoS-атак.

Беспроводные точки доступа (Wi-Fi) стали неотъемлемой частью современной сетевой инфраструктуры. Современные модели поддерживают стандарты 802.11ac Wave 2 и 802.11ax (Wi-Fi 6), обеспечивая скорость передачи данных до нескольких гигабит в секунду. Корпоративные точки доступа обладают функциями централизованного управления, поддержкой нескольких SSID с разными политиками безопасности, а также возможностью работы в кластерном режиме. Особое внимание уделяется системам роуминга и балансировке нагрузки между точками доступа.

Межсетевые экраны (файрволы) обеспечивают защиту сети от внешних угроз, анализируя и фильтруя проходящий трафик на основе сложных правил. Современные UTM-решения (Unified Threat Management) объединяют в себе функции файрвола, системы предотвращения вторжений, антивирусной защиты, фильтрации контента и VPN. Особую важность приобретают системы нового поколения (NGFW), способные анализировать трафик на уровне приложений и выявлять сложные угрозы.

Серверы доступа и контроллеры обеспечивают централизованное управление сетевыми услугами, включая аутентификацию пользователей (RADIUS), распределение IP-адресов (DHCP) и разрешение имен (DNS). В крупных сетях используются специализированные системы управления сетью (NMS), позволяющие мониторить состояние всех сетевых устройств, анализировать трафик и оперативно реагировать на возникающие проблемы.

При построении сетевой инфраструктуры крайне важно учитывать не только текущие потребности, но и перспективы развития. Современные тенденции включают переход на программно-определяемые сети (SDN), виртуализацию сетевых функций (NFV) и конвергентные архитектуры. Особое внимание следует уделять вопросам резервирования критически важных компонентов, регулярного обновления программного обеспечения и грамотной настройки всех параметров работы сети. Комплексный подход к проектированию и эксплуатации активного сетевого оборудования позволяет создать надежную, безопасную и высокопроизводительную сетевую инфраструктуру, способную удовлетворять растущие потребности современных организаций.

**4.4 Выбор активного сетевого оборудования и его технические характеристики**

Активные сетевые устройства являются основой современных компьютерных сетей, обеспечивая не только передачу данных, но и их обработку, анализ и оптимальное распределение. В отличие от пассивного оборудования, активные устройства требуют электропитания и имеют программное обеспечение, позволяющее им выполнять сложные функции управления сетевым трафиком. Современные активные устройства сочетают высокую производительность, расширенные функции безопасности и гибкие возможности масштабирования, что делает их незаменимыми в любой сетевой инфраструктуре.

Коммутаторы (свитчи) играют ключевую роль в локальных сетях, обеспечивая эффективную передачу данных на канальном уровне модели OSI. Управляемые коммутаторы обладают широкими функциональными возможностями, включая поддержку VLAN, QoS, агрегирование каналов и мониторинг трафика.

**5. РАСЧЕТ СТОИМОСТИ ОБОРУДОВАНИЯ ПРИ ПРОЕКТИРОВАНИИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ**

**5.1 Расчет количества пассивного оборудования, материалов и их стоимости**

При проектировании локальной сети важно учитывать не только активное, но и пассивное оборудование. Грамотный расчет необходимого количества и характеристик таких материалов позволяет не только спрогнозировать бюджет, но и обеспечить стабильную и долговечную работу сети.

Для точного определения объема пассивного оборудования необходимо проанализировать специфику проекта, включая площадь помещений, количество подключаемых устройств и их тип. Кроме того, стоимость пассивных компонентов существенно влияет на общие затраты. Корректный расчет помогает оптимизировать проект, повысив его надежность и экономическую эффективность.

Итоговая стоимость пассивного оборудования указана в приложении.

**5.2 Расчет количества активного оборудования и его стоимости**

Для обеспечения стабильного и эффективного функционирования сети было проведено тщательное проектирование и подбор активного сетевого оборудования, полностью соответствующего требованиям технического задания. При выборе устройств учитывался широкий спектр факторов, включая не только их технические характеристики, такие как пропускная способность, надежность, масштабируемость и энергопотребление, но и экономическая составляющая, выраженная в стоимости оборудования, а также его совместимость с уже развернутой инфраструктурой. Это позволило создать сбалансированное решение, обеспечивающее высокую производительность сети при оптимальных финансовых затратах.

Особое внимание уделялось подбору коммутаторов, маршрутизаторов и другого активного оборудования, способного обеспечить бесперебойную работу сети даже в условиях пиковых нагрузок. Каждое устройство было выбрано с учетом его функциональных возможностей, таких как поддержка современных стандартов передачи данных, возможность управления трафиком, а также интеграция с системами мониторинга и безопасности. Кроме того, учитывались перспективы дальнейшего расширения сети, чтобы избежать необходимости полной замены оборудования при увеличении нагрузки или изменении топологии.

Финансовая составляющая проекта также играла важную роль, поэтому при расчете стоимости активного оборудования проводился детальный анализ рыночных предложений, что позволило выбрать оптимальные по цене и качеству решения. В результате была сформирована итоговая стоимость всех необходимых устройств, которая подробно отражена в приложении к проектной документации. Этот подход обеспечил не только выполнение технических требований, но и соблюдение бюджета проекта, что является важным аспектом при реализации любых сетевых решений.

Итоговая стоимость активного оборудования приведена в приложении.

**6. НАСТРОЙКА СЕТЕВОГО ОБОРУДОВАНИЯ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

**6.1 Разбиение сети на подсети с выбором IP адресов**

Разбиение единой сети на изолированные подсети является ключевым этапом построения эффективной локальной инфраструктуры. Этот процесс приобретает особую значимость в крупных корпоративных средах, где критически важно грамотно распределять сетевые ресурсы и контролировать потоки данных. Основная цель такого разделения заключается в создании безопасной и управляемой сетевой архитектуры, обеспечивающей стабильную работу всех подключенных устройств.

Формирование отдельных сетевых сегментов дает возможность рационально использовать доступный диапазон IP-адресов, минимизировать ненужный трафик и устанавливать четкие правила коммуникации между различными отделами или службами организации. При проектировании адресного пространства необходимо учитывать назначение специальных адресов: начальный адрес диапазона идентифицирует саму подсеть, а конечный используется для широковещательных запросов. Для упрощения администрирования рекомендуется создавать подсети с количеством адресов, кратным степеням двойки, что соответствует естественной бинарной логике работы сетевых протоколов.

В рамках решения поставленной задачи было осуществлено логическое разделение адресного пространства между основными сетями и их внутренними подсетями. Распределение IP-адресов выполнено сбалансированно, с учетом необходимости резервирования служебных адресов в каждом сегменте. Размеры подсетей оптимизированы согласно стандартным сетевым практикам, что обеспечивает корректную работу всех сетевых устройств и сервисов. Такой подход гарантирует гибкость масштабирования сети и простоту дальнейшего администрирования инфраструктуры.Детальная информация о распределении IP-адресов представлена в таблице, размещенной в приложении.

**6.2 Настройка сетевого серверного программного обеспечения в программе Cisco Pocket Tracer**

В ходе реализации проекта была проведена комплексная настройка локальной сети с применением программного обеспечения Cisco Packet Tracer. Архитектурное решение предполагало разделение на две основные сети, каждая из которых состояла из пяти подсетей, что обеспечило логичную структуру и эффективное управление сетевыми ресурсами. Основу инфраструктуры составили маршрутизаторы и коммутаторы, настроенные для стабильной и производительной работы всей системы.

Общее количество подключенных устройств составило 249 единиц, для которых автоматическое распределение IP-адресов было организовано через DHCP-сервер. Такой подход позволил избежать ручного ввода параметров для каждого устройства, минимизировав вероятность ошибок и существенно упростив процесс администрирования. Автоматизация особенно актуальна в крупных сетях, где ручная настройка потребовала бы значительных временных затрат и могла привести к сбоям в работе.

Для соединения сетевых сегментов между двумя зданиями использовались два маршрутизатора – по одному на каждую сеть. К каждому маршрутизатору был подключен центральный коммутатор, выполняющий роль основного узла. Далее к нему присоединялись дополнительные коммутаторы, соответствующие пяти подсетям в рамках своей сети. Связь между главными коммутаторами и маршрутизаторами была организована через trunk-интерфейсы, что обеспечило передачу трафика нескольких VLAN по единому физическому соединению. Каждая подсеть получила уникальный идентификатор VLAN, что позволило четко разграничить зоны влияния.

Во второй сети, где количество устройств в подсетях превышало 24, для масштабируемости добавили дополнительные коммутаторы. Их включили в соответствующие VLAN, чтобы сохранить логическую структуру и избежать смешения трафика. Все порты коммутаторов перевели в режим access, ограничив их работу одной VLAN. Это повысило безопасность и исключило несанкционированный обмен данными между сегментами сети.

Настройку оборудования выполняли поэтапно. Сначала добавили необходимые компоненты: маршрутизаторы, коммутаторы, компьютеры и принтеры. Затем соединили их подходящими кабелями. На маршрутизаторах детально настроили интерфейсы для каждой VLAN, назначив IP-адреса и маски подсетей. Для связи между VLAN реализовали маршрутизацию с помощью соответствующих команд. в программе Cisco Packet Tracer представлено в приложении.

**6.3 Настройка сетевого клиентского программного обеспечения в программе Cisco**

Для обеспечения стабильной работы сети каждое подключенное устройство должно обладать уникальным IP-адресом. В целях автоматизации данного процесса был задействован протокол DHCP, который динамически распределяет IP-адреса и сопутствующие сетевые параметры (маску подсети, основной шлюз, DNS-серверы). Такой подход существенно упрощает развертывание сети, снижает риск ошибочных настроек и оптимизирует трудозатраты системного администратора.

На стороне клиентских устройств настройка сводится к активации функции автоматического получения сетевых параметров через DHCP. Данная опция включается в параметрах сетевого адаптера, после чего оборудование самостоятельно запрашивает и получает от DHCP-сервера все необходимые для работы конфигурации

Конфигурация DHCP-сервера на маршрутизаторе выполняется через специализированный интерфейс управления. Для каждой подсети создается отдельный пул адресов с четко определенными границами распределяемых IP-адресов, указанием сетевой маски, адреса шлюза и DNS-серверов. После активации этих настроек маршрутизатор начинает автоматически обслуживать все подключенные устройства, выдавая им соответствующие сетевые параметры.

Особое внимание при настройке уделяется коммутационному оборудованию. В среде Cisco Packet Tracer требуется обеспечить корректную передачу DHCP-запросов от конечных устройств к маршрутизатору. Это достигается правильной настройкой портов коммутаторов (режимы Access для конечных устройств и Trunk для магистральных соединений). Для trunk-портов обязательно активируется поддержка VLAN-тегирования по стандарту 802.1Q, что гарантирует правильную маршрутизацию запросов между различными подсетями.

При планировании DHCP-адресации важно предусмотреть резерв IP-адресов для будущего расширения сети. Одновременно из общего пула следует исключить статические адреса, закрепленные за критически важным оборудованием (серверы, сетевые принтеры, системы видеонаблюдения). Такой подход предотвращает потенциальные конфликты адресов в сети.

Верификация работоспособности сети проводится с использованием стандартных диагностических средств. Основным инструментом проверки является утилита ping, позволяющая проверить доступность сетевых узлов и качество соединения между ними. Успешный обмен пакетами между устройствами без потерь подтверждает корректность выполненной конфигурации сети. Дополнительно рекомендуется проверять журналы DHCP-сервера для контроля процесса аренды адресов и своевременного выявления возможных проблем.

Изображения этапов настройки сетевого клиентского программного обеспечения представлены в приложении

**6.4 Настройка сетевого дополнительного оборудования в ОС Windows 10**

Сетевые принтеры являются важным элементом современной офисной инфраструктуры, обеспечивая коллективный доступ к печати документов и графических материалов. Существуют различные методы интеграции печатающих устройств в локальную сеть. Наиболее распространенный подход предполагает прямое подключение принтера к сетевому оборудованию - через Ethernet-кабель или по беспроводному соединению, если модель поддерживает Wi-Fi. Альтернативным решением служит подключение устройства к рабочей станции через USB-интерфейс с последующей активацией функции общего доступа, что делает принтер видимым для всех участников сети под уникальным сетевым именем.

Процесс добавления сетевого печатающего устройства в операционной системе Windows 10 осуществляется через системные настройки. Пользователю необходимо открыть раздел "Устройства" в параметрах системы, затем перейти во вкладку "Принтеры и сканеры". Активация функции "Добавить принтер или сканер" инициирует автоматический поиск доступных устройств в пределах локальной сети. При успешном обнаружении оборудования система предложит завершить процесс установки, следуя пошаговым инструкциям на экране.

В случаях, когда автоматическое обнаружение не приносит результатов, существует возможность ручной настройки. Для этого следует выбрать опцию "Необходимый принтер отсутствует в списке" и перейти к расширенным параметрам подключения. В появившемся диалоговом окне необходимо указать тип подключения через TCP/IP-адрес или сетевое имя устройства. После ввода соответствующих сетевых реквизитов система предложит выбрать подходящий драйвер из встроенной базы или установить его вручную. Завершение процесса инсталляции драйверов делает печатающее устройство полностью готовым к работе в сетевом окружении.

Изображения этапов настройки подключения сетевых принтеров представлены в приложении

**7 ПЛАНИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ**

**7.1 Общие принципы безопасности**

Сетевая безопасность представляет собой комплекс взаимосвязанных мер защиты, которые являются важной составляющей общей системы информационной безопасности организации. Для реализации этих мер привлекаются различные структурные подразделения компании и применяется специализированное техническое оборудование и программное обеспечение.

Эффективность функционирования компьютерной сети в значительной степени зависит от уровня защиты передаваемой и обрабатываемой информации. Под безопасностью информации понимается ее способность противостоять различным видам угроз на всех этапах работы с данными - от момента их получения и обработки до хранения, передачи и конечного использования.

Актуальность вопросов сетевой безопасности постоянно возрастает в связи с повсеместным внедрением компьютерных технологий во все сферы деятельности современного общества, а также в результате перехода от использования выделенных каналов связи к общедоступным сетевым ресурсам.

При разработке системы информационной безопасности сети необходимо учитывать ряд фундаментальных принципов. В первую очередь требуется разработать и внедрить комплексную политику безопасности, которая будет устанавливать четкие правила, процедуры и стандарты работы с информацией для всех сотрудников организации. Особое внимание следует уделить вопросам управления доступом, включая разработку эффективных механизмов аутентификации, авторизации и учета пользователей.

Обязательным требованием является использование современных методов шифрования данных при их передаче по сети, что позволяет обеспечить необходимый уровень конфиденциальности информации. Для этого применяются специальные криптографические протоколы, такие как IPsec, которые обеспечивают защиту сетевого трафика.

Не менее важным аспектом является поддержание программного обеспечения в актуальном состоянии путем регулярного обновления. Это позволяет своевременно устранять обнаруженные уязвимости и предотвращать их использование злоумышленниками.

Особое внимание следует уделить обучению персонала основам информационной безопасности, так как человеческий фактор остается одним из наиболее уязвимых мест в системе защиты. Регулярное проведение обучающих мероприятий и информирование сотрудников о потенциальных угрозах значительно повышает общий уровень безопасности сети.

Крайне важным элементом защиты данных является организация надежной системы резервного копирования и разработка четкого плана восстановления информации после возможных сбоев. Это позволяет минимизировать последствия непредвиденных ситуаций и обеспечить непрерывность бизнес-процессов.

Соблюдение этих принципов позволяет создать сбалансированную систему безопасности, в которой каждый сотрудник получает необходимый для работы уровень доступа, но при этом ограничивается от выполнения потенциально опасных операций, которые могут нарушить работу всей сети. Грамотное распределение прав пользователей должно основываться на принципах информационной безопасности и полностью соответствовать корпоративным политикам организации, что позволяет минимизировать риски внутренних угроз.

**7.2 Оценка вероятных угроз**

Локальная вычислительная сеть (ЛВС) постоянно находится под угрозой различных факторов, способных нарушить её стабильную работу. Одной из распространённых проблем является заражение системы вредоносным программным обеспечением через съемные носители. Флеш-накопители, внешние жёсткие диски и другие портативные устройства могут стать источником вирусов, червей или троянских программ. Попадая в сеть, такие вредоносные агенты быстро распространяются, заражая компьютеры и нанося значительный ущерб данным и производительности системы.

Не менее серьёзную опасность представляют внутренние угрозы, связанные с действиями сотрудников или других пользователей сети. Несанкционированный доступ к конфиденциальной информации, нарушение политик безопасности или небрежное обращение с данными могут привести к утечкам и компрометации критически важных ресурсов. Особую опасность усугубляет отсутствие чётко настроенных прав доступа и недостаточный контроль за действиями пользователей, что создаёт благоприятные условия для злоупотреблений.

Помимо цифровых рисков, существует также угроза физического вмешательства. Неограниченный доступ к серверам, рабочим станциям или сетевому оборудованию позволяет злоумышленникам напрямую изменять настройки, повреждать технику или подключать посторонние устройства. Это может быть как действия недобросовестных сотрудников, так и проникновение посторонних лиц в помещения, где расположена инфраструктура сети.

Ещё одним фактором риска является отказ оборудования, вызванный техническими неисправностями, ошибками в настройках или некорректным обновлением программного обеспечения. Аппаратные сбои, перегревы, неправильная конфигурация сетевых устройств или сбои в работе серверов способны привести к частичной или полной недоступности ресурсов, а также к потере важных данных.

Таким образом, локальная вычислительная сеть подвержена множеству угроз, каждая из которых способна нанести серьёзный урон. Однако наибольшую опасность, как показывает практика, представляет человеческий фактор – будь то неосторожность, злой умысел или недостаточная компетентность пользователей и администраторов. Это подчёркивает необходимость комплексного подхода к безопасности, включающего как технические, так и организационные меры защиты.

**7.3 Распределение прав пользователей**

Одним из основных аспектов информационной безопасности в локальной вычислительной сети (ЛВС) является правильное распределение прав доступа между пользователями. Неправильное назначение полномочий, особенно когда у неподготовленных сотрудников есть избыточные привилегии, может привести к серьёзным сбоям, утечкам данных и даже полному нарушению работы сети. Чтобы минимизировать такие риски, необходимо чётко определить роли и зоны ответственности каждого участника сети.

Пользователи в организации должны делиться на категории в зависимости от своих функций и уровня доверия. Например, администраторы имеют максимальные права для управления сетью, в то время как рядовые сотрудники получают доступ только к необходимым ресурсам. Временные пользователи, такие как гости и подрядчики, должны иметь строго ограниченные права, чтобы избежать случайных или умышленных нарушений. Такой подход повышает безопасность и упрощает администрирование.

Принцип наименьших привилегий должен лежать в основе распределения прав. Это означает, что каждый пользователь получает только тот уровень доступа, который необходим для выполнения его обязанностей. Например, бухгалтеру не нужны права на изменение системных настроек, а инженеру технической поддержки – доступ к финансовым документам. Соблюдение этого принципа снижает риски, связанные с человеческим фактором.