МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ВОЛЖСКИЙ ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ (ФИЛИАЛ)
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

А.А. Силаев

Компьютерные технологии и телекоммуникации

Электронное учебно-методическое пособие

Волгоград
2017

УДК : 004.7

Р е ц е н з е н т ы :

Кандидат физико-математических наук,
доцент кафедры «Автоматизации технологических процессов»
филиала МЭИ г. Волжский
Е.В. Капля,
кандидат технических наук,
доцент кафедры «Автоматизации производственных процессов» ВолгГТУ
А.Г. Алёхин

Печатается по решению редакционно-издательского совета
Волгоградского государственного технического университета

Силаев, А.А.
Компьютерные технологии и телекоммуникации [Электронный ресурс]: учебно-методическое пособие / А. А. Силаев ; ВПИ (филиал) ВолгГТУ. – Электрон. текстовые дан. (1 файл: 2,6 МБ). – Волгоград, 2017. - Режим доступа: http://lib.volpi.ru. – Загл. с титул. экрана.
ISBN 978-5-9948-2707-9

В пособие рассмотрены основные понятия и определения компьютерных сетей и телекоммуникаций.

Учебно-методическое пособие представляет собой конспект лекций, дополненный примерами применения компьютерных технологий в человеческом обществе.

Предназначено для студентов технических ВУЗов обучающихся по направлению бакалавриата «Автоматизация технологических процессов и производств» всех форм обучения.

ISBN 978-5-9948-2707-9

Содержание

Введение

В настоящее время компьютерные технологии и телекоммуникации прочно обосновались в жизни людей. Действительно сложно найти хотя бы одну отрасль деятельности, в которой не используются информационные технологии в той или иной мере. Компьютеры помогли людям сделать грандиозный прорыв в развитии науки и техники. И с каждым годом появляется всё больше вещей и техник, использующих информационные технологии. Количество пользователей сети Интернет увеличивается постоянно, при этом пользователями сети становятся не только люди, но и вещи. А информационные процессы происходят не только между людьми, но и неодушевлёнными предметами.

Сегодня скорость технологического развития растет в геометрической прогрессии. В целях поддержания конкурентного преимущества организациям следует принимать во внимание это развитие. Существуют три основных принципа, или закона, которые могут помочь организациям и экспертам распланировать свои технологические потребности.

– ***Закон Мура*** — этот закон был предложен в 1965 году Гордоном Е. Муром, сооснователем корпорации Intel. Согласно этому закону количество транзисторов в интегральных микросхемах удваивается каждые два года, что повышает вычислительную мощность.

– ***Закон Меткалфа*** – создание этого закона приписывают Роберту Меткалфу. Согласно этому закону ценность отдельно взятой сети пропорциональна квадрату количества подключенных к ней пользователей. Закон Меткалфа рассчитывает количество уникальных подключений в сети узлов, которое выражается математически в виде формулы n(n–1)/2. Таким образом, ценность, описываемая в этом законе, пропорциональна n^2.

– ***Закон Рида*** – этот закон предложил Дэвид Рид. Согласно этому закону ценность сети растет в геометрической прогрессии путем сложения групп, которые могут сформироваться из двух пользователей, трех пользователей и т. д. Данный закон рассчитывается по формуле 2^n и нагляднее всего демонстрируется на примере социальных сетей.

В целом можно сказать, что компьютерные технологии базируются на четырех составляющих:

– люди и вещи – это участники сбора и обмена информацией между собой;

– данные – это непосредственно сама информация, которая выступает как важнейший ресурс человеческого общества;

– информационные процессы – процессы, происходящие в ходе получения, обработки и передачи информации между участниками.

А основой всего этого является компьютерная сеть. Именно сети дали возможность создавать единое информационное пространство для взаимодействия.

В пособие рассмотрены основные понятия и определения компьютерных сетей и телекоммуникаций:

классификация сетей;

устройства сетей;

среды передачи данных;

базовая модель TCP/IP;

прикладные протоколы;

адресация в компьютерных сетях;

система доменных имён;

основы безопасности;

программирование.

Учебно-методическое пособие представляет собой конспект лекций, дополненный примерами применения компьютерных технологий в человеческом обществе.

Данное учебно-методическое пособие предназначено для студентов бакалавриата, обучающихся по направлению «Автоматизация технологических процессов и производств» при изучении дисциплины «Компьютерные технологии и телекоммуникации».

1 Введение в информационные технологии

Компьютерные технологии тесно связаны с понятиями «информация» и «информационные технологии».

Информационные технологии — это комплекс взаимосвязанных, научных, технологических, инженерных дисциплин, изучающих:

методы эффективной организации труда людей, занятых обработкой и хранением информации;

вычислительную технику и методы организации и взаимодействия с людьми и производственным оборудованием, их практические приложения, а также связанные со всем этим социальные, экономические и культурные проблемы.

Любая деятельность человека представляет собой процесс сбора и переработки информации, принятие на её основе решений и их выполнения. С появлением современных средств компьютерной техники информация стала выступать в качестве одного из важнейших ресурсов человеческого общества.

Свойства информации:

– ***релевантность*** — способность информации соответствовать нуждам (запросам) потребителя;

– ***полнота*** — свойство информации исчерпывающе (для данного потребителя) характеризовать отображаемый объект и / или процесс;

– ***своевременность*** — способность информации соответствовать нуждам потребителя в нужный момент времени;

– ***достоверность*** — свойство информации не иметь скрытых ошибок;

– ***доступность*** – свойство информации, характеризующее возможность её получения данным потребителем;

– ***защищённость*** — свойство, характеризующее невозможность несанкционированного использования или изменения;

– ***эргономичность*** — свойство, характеризующее удобство формы или объёма информации с точки зрения потребителя.

С понятием информации тесно связаны такие понятия, как сигнал, сообщение и данные.

Сигнал — представляет собой любой процесс, несущий информацию (например, опрос датчика).

Сообщение — это информация, представленная в определенной форме и предназначенная для передачи.

Данные — это информация, представленная в формализованном виде и предназначенная для обработки её техническими средствами, например, ЭВМ.

Различают две формы представления информации – непрерывную и дискретную.

Если эта функция непрерывна, то передаваемая информация называется аналоговой. Её источником обычно являются различные природные объекты (температура, давление, влажность воздуха и т.д.), объекты технологических процессов (нейтронный поток в реакторе, давление и температура теплоносителя и пр.) и др.

Если функция U(t) дискретна, то информация имеет характер дискретных сообщений (сигналы тревоги, языковые сообщения письменные, звуковые или на языке жестов и т.д.)

Для преобразования аналогового сигнала в цифровой сигнал требуется провести дискретизацию во времени и квантование по уровню.

Дискретизация — замена непрерывного (аналогового) сигнала последовательностью отдельных во времени отсчетов этого сигнала. Наиболее распространена равномерная дискретизация, в основе которой лежит теорема Котельникова.

На рисунке 1 схематично показан процесс преобразования аналогового сигнала в цифровой сигнал.

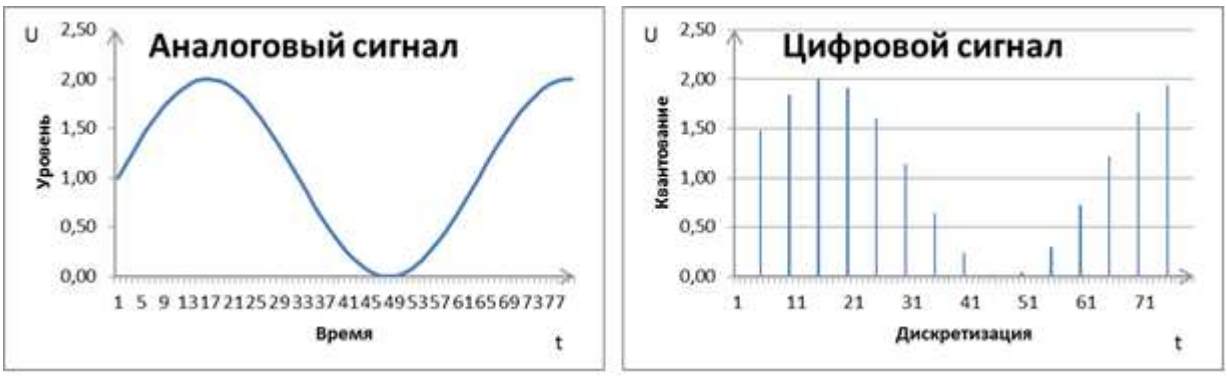

Рисунок 1 – Дискретизация аналогового сигнала.

Качество аналого-цифрового преобразования характеризует параметр, называемый разрешением. ***Разрешение*** — это количество уровней квантования, используемых для замены непрерывного аналогового сигнала цифровым сигналом. Восьмиразрядная выборка позволяет получить только 256 различных уровней квантования цифрового сигнала, а шестнадцатиразрядная выборка — 65536 уровней.

Еще один показатель качества трансформации непрерывного сигнала в цифровой сигнал — это ***частота дискретизации*** — количество преобразований аналог-цифра (выборок), производимое устройством в одну секунду. Этот показатель измеряют килогерцами (килогерц — тысяча выборок в секунду). Типичное значение частоты дискретизации аудиосигнала — 44,1 кГц.

Именно возможность представления информации в дискретном (цифровом) виде дала мощнейший толчок к развитию компьютерной техники.

Примеры использования компьютерных технологий в обществе.

Управление автоматизированным производством — возможность управлять технологическим процессом удалённо с помощью персонального компьютера (см. рисунок 2).

Рисунок 2 – Управление автоматизированным производством.

Технология «Умный дом» — возможность удалённого слежения за домом с помощью мобильных устройств. Сбор и получение данных об основных параметрах системы жизнеобеспечения (см. рисунок 3).

Рисунок 3 – Технология «Умный дом».

1.1 Форма восприятия и представления информации

Форма восприятия и представления информации определяет основной способ конечного их использования в той или иной сфере деятельности и предполагает один из следующих вариантов:

– текстовая информация;

– аудиоинформация (звуковая);

– видеоинформация (визуальная).

Текстовая информация — это различные виды письменной речи или представления данных с помощью систем специальных знаков (математические и химические формулы, тексты программ и т. п.).

Аудиоинформация — это устная речь, музыка, звуки естественного или искусственного происхождения, системы звуковых сигналов различного назначения.

Видеоинформация — это различного вида образы, воспринимаемые органами зрения (рисунки, схемы, карты, фильмы и т. п.).

1.2 Формы адекватности информации

При работе с информацией всегда имеется ее источник и потребитель (получатель). Пути и процессы, обеспечивающие передачу сообщений от источника информации к ее потребителю, называются информационными коммуникациями.

Для потребителя информации очень важной характеристикой является ее адекватность.

Адекватность информация — это уровень соответствия образа, создаваемого с помощью полученной информации, реальному объекту, процессу, явлению и т. п.

В реальной жизни вряд ли возможна ситуация, когда вы сможете рассчитывать на полную адекватность информации. Всегда присутствует некоторая степень неопределенности. От степени адекватности информации

реальному состоянию объекта или процесса зависит правильность принятия решений человеком.

Адекватность информации может выражаться в трех формах:

– синтаксической,

– семантической,

– прагматической.

Синтаксическая адекватность. Она отображает формально структурные характеристики информации и не затрагивает ее смыслового содержания. На синтаксическом уровне учитываются тип носителя и способ представления информации, скорость передачи и обработки, размеры кодов представления информации, надежность и точность преобразования этих кодов и т.п. Информацию, рассматриваемую только с синтаксических позиций, обычно называют данными, так как при этом не имеет значения смысловая сторона. Эта форма способствует восприятию внешних структурных характеристик, т.е. синтаксической стороны информации.

Семантическая (смысловая) адекватность. Эта форма определяет степень соответствия образа объекта и самого объекта. Семантический аспект предполагает учет смыслового содержания информации. На этом уровне анализируются те сведения, которые отражает информация, рассматриваются смысловые связи. В информатике устанавливаются смысловые связи между кодами представления информации. Эта форма служит для формирования понятий и представлений, выявления смысла, содержания информации и ее обобщения.

Прагматическая (потребительская) адекватность. Она отражает отношение информации и ее потребителя, соответствие информации цели управления, которая на ее основе реализуется. Проявляются прагматические свойства информации только при наличии единства информации, пользователя и цели управления. Прагматический аспект связан с ценностью, полезностью использования информации при выработке потребителем решения для

достижения своей цели. С этой точки зрения анализируются потребительские свойства информации. Эта форма адекватности непосредственно связана с практическим использованием информации.

2 Компьютерные сети. Назначение, характеристики и типы сетей

Компьютерная сеть — это совокупность узлов (компьютеров, терминалов, периферийных устройств: сетевых дисков и принтеров), имеющих возможность информационного взаимодействия друг с другом с помощью специального коммуникационного оборудования (специальная сетевая карта, осуществляющая связь между системной шиной компьютера и сетевым кабелем) и программного обеспечения (сетевая операционная система).

Основное назначение компьютерных сетей — это совместное использование ресурсов и осуществление интерактивной связи (режим реального времени, обратная связь).

Использование компьютерных сетей позволяет:

а) повысить эффективность работы;

б) снизить затраты за счет совместного использования данных, дорогостоящих периферийных устройств и программных средств (приложений).

Ресурсы — представляют собой данные (в том числе корпоративные базы данных и знаний), приложения (в том числе различные сетевые программы), а также периферийные устройства, такие как принтер, сканер, диск и т. д.

2.1 Основные характеристики компьютерных сетей

Операционные возможности сети характеризуются такими условиями, как:

− предоставление доступа к прикладным программным средствам, БД, БЗ, и т. д.;

− удаленный ввод заданий;

− передача файлов между узлами сети;

− доступы к удаленным файлам;

− выдача справок об информационных и программных ресурсах;

− распределенная обработка данных на нескольких ЭВМ и т. д.

Временные характеристики сети определяют продолжительность обслуживания запросов пользователей:

− среднее время доступа, которое зависит от размеров сети, удаленности пользователей, загрузки и пропускной способности каналов связи и т. д.;

− среднее время обслуживания.

Надежностные характеристики определяют надежность, как отдельных элементов сети, так и сеть в целом:

− время безотказной работы;

− частота отказов и т. д.

Производительность характеризуется:

– пропускная способность сети — скорость передачи данных;

– количество обрабатываемых данных;

– количество пользователей.

Стоимость оборудования и программного обеспечения.

2.2 Типы сетей

По широте охвата принято деление сетей на несколько типов.

Локальные сети (Local Area Networks LAN) — сети компьютеров, сосредоточенные на небольшой территории (обычно в одном помещении). В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации. Из-за коротких расстояний в локальных сетях имеется возможность использования высококачественных линий связи. Локальные сети получили широкое распространение из-за небольшой сложности и невысокой стоимости. Они используются при автоматизации коммерческой, банковской деятельности, а также для создания распределенных, управляющих и информационно-справочных систем.

Особенности локальных сетей:

– самая высокая скорость передачи данных;

– малое количество компьютеров в сети;

– ограниченное количество ресурсов и серверов.

Глобальные сети (Wide Area Networks WAN) — объединяют территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах. Как правило, глобальные сети принадлежат автономным организациям, таким как корпорации или правительства. Обычно скорость канала, которую обеспечивают глобальные сети между локальными сетями, ниже скорости внутри локальной сети.

Особенности глобальных сетей:

– невысокая скорость передачи данных;

– максимальное количество компьютеров в сети;

– максимальное количество ресурсов и серверов.

3 Компоненты сети

Маршрут, по которому сообщение идет от источника к месту назначения, может быть простым, как, например, один кабель, соединяющий один компьютер с другим, или сложным, как сеть, буквально охватывающая весь мир. Сетевая инфраструктура — это платформа, поддерживающая конкретную сеть, которая выполняет функцию стабильного и надежного канала для передачи данных.

Устройства и среда передачи данных — это физические элементы или аппаратное обеспечение сети. Аппаратное обеспечение зачастую является видимой частью сетевой платформы — ноутбук, ПК, коммутатор, маршрутизатор, точка беспроводного доступа или кабели, используемые для соединения устройств. Однако существуют компоненты, которые остаются скрытыми. В случае беспроводных сетей сообщения передаются с помощью незримого радиочастотного или инфракрасного излучения.

Компоненты сети используются для предоставления сервисов и процессов. Они представляют собой коммуникационные программы, называемые программным обеспечением, которые запускаются на сетевых устройствах. Сетевой сервис предоставляет данные в ответ на запрос. Сервисы включают в себя множество сетевых приложений, которые люди используют ежедневно, например, сервисы электронной почты и веб-хостинга. Процессы обеспечивают функциональность, посредством которой сообщения направляются и перемещаются в пределах сети. Процессы менее очевидны для нас, но критически важны для работы сетей.

3.1 Конечные устройства

Сетевые устройства, с которыми пользователи знакомы лучше всего, называются конечными устройствами. Все компьютеры, подключенные к сети и непосредственно участвующие в обмене данными, считаются узлами. Эти устройства образуют интерфейс между пользователями и сетью связи.

Примеры конечных устройств:

– ЭВМ (компьютеры, ноутбуки, веб-серверы);

– сетевые принтеры и диски;

– VoIP-телефоны;

– терминальные устройства;

– камеры видеонаблюдения;

– мобильные карманные устройства (смартфоны, планшетные ПК, КПК);

– датчики, например, термометры, весы и другие устройства, подключаемые к сети;

– исполнительные механизмы, как составляющие «умных вещей».

Конечное устройство — это источник или место назначения данных, передаваемых по сети. Каждому конечному устройству в сети назначается адрес, чтобы устройства можно было отличить. Если конечное устройство инициирует обмен данными, то в качестве получателя сообщения оно использует адрес конечного устройства назначения.

В сетях выделяют два обобщённых типа конечных устройств.

Сервер — это конечное устройство, на котором установлено ПО, позволяющее ему предоставлять информацию, в том числе сообщения электронной почты или веб-страницы, другим конечным устройствам в сети. Например, для работы веб-служб в сети на сервере должно быть установлено ПО веб-сервера.

Рисунок 4 – Сервер хранения данных.

Клиент — это конечное устройство, на котором установлено ПО, позволяющее запрашивать и отображать информацию, полученную от сервера. Примером клиентского программного обеспечения является веб-браузер, например Internet Explorer (см. рисунок 5).

Рисунок 5 – Примеры клиентских устройств.

В настоящее время существует много новых типов конечных устройств, которые собирают и передают данные, они являются важнейшими составляющими Интернета Вещей.

Датчик — это объект, который может измерять физические свойства и преобразовывать эту информацию в электрический или оптический сигнал. Например, датчики могут измерять температуру, вес, движение, давление и влагу.

Как правило, датчики поставляются с заранее запрограммированными инструкциями; впрочем, в некоторых датчиках можно изменить степень чувствительности или частоту отчетности. Настройки чувствительности указывают степень изменения выходных данных датчика при колебаниях измеряемой величины. Например, датчик движения можно откалибровать таким образом, чтобы он замечал только движения людей, не обращая внимания на домашних животных. Для изменения параметров датчика как локально, так и удаленно используется контроллер, который может быть оснащен графическим пользовательским интерфейсом (GUI).

Исполнительный механизм — это другое устройство, которое реализовано в рамках Интернета Вещей. Это базовый двигатель, который можно использовать для активации или контроля механизма или системы, исходя из имеющихся инструкций. Исполнительные механизмы выполняют непосредственное физическое действие, стоящее за понятием «привести в движение».

В Интернете Вещей используются три типа исполнительных механизмов:

– ***гидравлический*** — использует давление жидкости для выполнения механического движения;

– ***пневматический*** — использует сжатый под высоким давлением воздух для инициирования механического действия;

– ***электрический*** — работает благодаря электродвигателю, который преобразует электроэнергию в механические действия.

Вне зависимости от того, как исполнительный механизм инициирует движение, его базовая функция заключается в получении сигнала, исходя из которого он выполняет какое-либо действие. Как правило, исполнительные механизмы не способны обрабатывать данные. Скорее, результат выполняемого механизмом действия зависит от полученного сигнала. Действие, выполняемое механизмом, обычно инициируется сигналом со стороны контроллера.

3.2 Промежуточные сетевые устройства

Промежуточные устройства служат для соединения конечных устройств. Эти устройства обеспечивают соединение, работая «за кулисами» и осуществляя передачу данных по сети. Промежуточные устройства соединяют отдельные узлы с сетью и могут соединять несколько отдельных сетей для создания объединенной сети.

Примеры промежуточных сетевых устройств (см. рисунок 6):

– коммутаторы и точки беспроводного доступа (сетевой доступ);

– маршрутизаторы (межсетевое взаимодействие);

– межсетевые экраны (безопасность).

Рисунок 6 – Пример промежуточного устройства.

К функциям промежуточных устройств относится управление данными по мере их прохождения через сеть. Эти устройства используют адрес узла назначения и информацию о межсетевых соединениях, чтобы определить пути для отправки сообщений по сети.

Процессы, запущенные на промежуточных сетевых устройствах, выполняют следующие функции:

– регенерация и ретрансляция сигналов передачи данных;

– поддержание информации о существующих путях в сети и между сетями;

– уведомление других устройств об ошибках и сбоях связи;

– направление данных через альтернативный маршрут при выходе канала из строя;

– классификация и передача сообщений в соответствии с приоритетами качества обслуживания (QoS);

– разрешение или запрет потока данных на основании настроек безопасности.

3.3 Сетевая топология

Сетевая топология — это схема, в которой изложены различные элементы компьютерной сети. Сеть может быть представлена двумя типами топологии: физической и логической.

Физическая топология отображает расположение и местонахождение всех устройств в сети. Физическая топология описывает фактические соединения между устройствами посредством проводов и кабелей.

При определении физической топологии необходимо учесть следующие аспекты.

– Местоположение компьютеров пользователей.

– Расположение сетевого оборудования, в том числе коммутаторов, маршрутизаторов и точек беспроводного доступа.

– Расположение контроллеров и серверов.

– Расположение датчиков и исполнительных механизмов.

– Возможность расширения сети в будущем.

Логическая топология основана на принципах работы протоколов связи и представляет сеть иначе, чем физические топологии. Логическая топология отображает пути, по которым данные передаются по сети. Она описывает, как устройства обмениваются данными с пользователями сети. Неотъемлемой частью логической топологии является схема адресации.

Все сети строятся на основе трех базовых топологий:

− шина (bus);

− звезда (star);

− кольцо (ring).

3.3.1 Шинная топология

При помощи кабеля каждая рабочая станция соединяется с другими рабочими станциями и с файловым сервером. Кабель проходит от узла к узлу, последовательно соединяя все рабочие станции и все файловые серверы. На каждом конце кабеля подключается согласующая нагрузка (терминатор) для исключения эхоотражений (см. рисунок7).

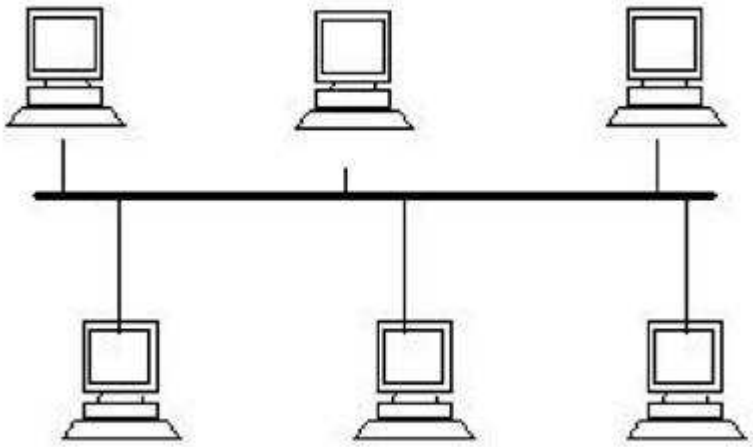

Рисунок 7 – Шинная топология.

Шинная топология использует состязательный метод доступа. Это означает, что информацию принимает только тот компьютер, адрес которого соответствует адресу получателя, зашифрованному в передаваемых сигналах. Остальные компьютеры отбрасывают сообщение. Перед передачей данных компьютер должен ожидать освобождения шины. В каждый момент времени отправлять сообщение может только один компьютер, поэтому число подключенных к сети машин значительно влияет на ее быстродействие.

Преимущества шинной топологии:

– надежно работает в небольших сетях, проста в использовании;

– требует меньше кабеля для соединения компьютеров и потому дешевле, чем другие схемы соединении;

– легко расширяется за счет состыковки кабельных сегментов с помощью цилиндрического соединителя и использования повторителей.

Недостатки шинной топологии:

– интенсивный сетевой трафик снижает производительность сети. При большом числе компьютеров в сети станции часто прерывают друг друга, и немалая часть полосы пропускания теряется понапрасну. При добавлении компьютеров к сети резко падает производительность;

– цилиндрические соединители ослабляют электрический сигнал, и большое их число вызывает нарушения в передаче информации по шине;

– разрыв кабеля или неправильное функционирование одной из станций может привести к нарушению работоспособности всей сети. Сеть трудно диагностировать.

3.3.2 Кольцевая топология

В сети с кольцевой топологией каждый компьютер соединяется со следующим компьютером, ретранслирующим ту информацию, \ он получает от первой машины. Благодаря такой ретрансляции сеть является активной, и в ней не возникают проблемы потери сигнала, как в сетях с шинной топологией.

Кроме того, поскольку «конца» в кольцевой сети нет, никаких оконечных нагрузок не нужно (см. рисунок 8).

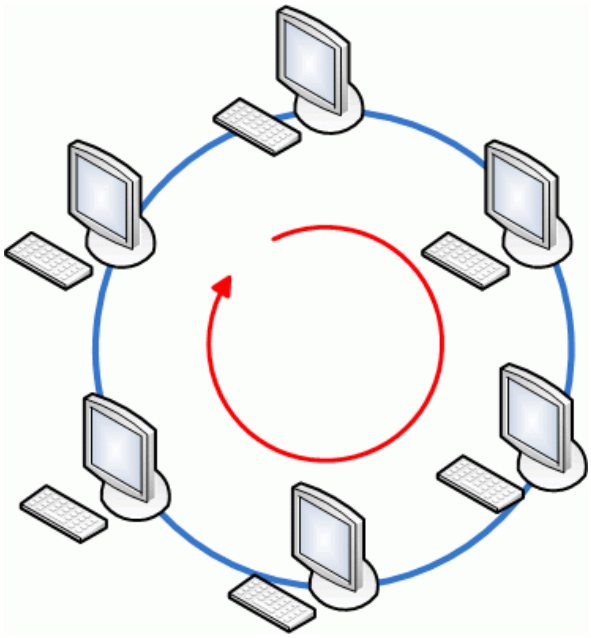

Рисунок 8 – Кольцевая топология.

Некоторые сети с кольцевой топологией используют метод доступа к среде на основе маркера (метод эстафетной передачи). Специальное короткое сообщение-маркер циркулирует по кольцу пока компьютер не пожелает передать информацию другому узлу. Он модифицирует маркер, добавляет электронный адрес и данные, а затем отправляет его по кольцу. Каждый из компьютеров последовательно получает данный маркер с добавленной информацией и передает его соседней машине, пока электронный адрес не совпадет с адресом компьютера-получателя, или маркер не вернется к отправителю. Получивший сообщение компьютер возвращает отправителю ответ, подтверждающий, что послание принято. Тогда отправитель создает еще один маркер и отправляет его в сеть, что позволяет другой станции перехватить маркер и начать передачу. Маркер циркулирует по кольцу, пока какая-либо из станций не будет готова к передаче и не захватит его.

Такая структура способствует восстановлению сети в случае возникновения отказов.

Преимущества сети с кольцевой топологией:

– поскольку всем компьютерам предоставляется равный доступ к маркеру, никто из них не сможет монополизировать сеть;

– справедливое совместное использование сети обеспечивает постепенное снижение ее производительности в случае увеличения числа пользователей и перегрузки (лучше, если сеть будет продолжать функционировать, хотя и медленно, чем сразу откажет при превышении пропускной способности).

Недостатки сети с кольцевой топологией:

– отказ одного компьютера в сети может повлиять на работоспособность всей сети;

– кольцевую сеть трудно диагностировать;

– добавление или удаление компьютера вынуждает разрывать сеть.

3.3.3 Звездообразная топология

Звездообразная топология — базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу (обычно коммутатор), образуя физический сегмент сети. Весь обмен информацией идет исключительно через центральный компьютер, на который таким способом возлагается очень большая нагрузка, поэтому ничем другим, кроме сети, он заниматься не может. Как правило, именно центральный компьютер является самым мощным, и именно на него возлагаются все функции по управлению сетью (см. рисунок 9).

Рисунок 9 – Звездообразная топология.

Активный концентратор регенерирует электрический сигнал и посылает его всем подключенным компьютерам. Такой тип концентратора часто называют многопортовым повторителем (multiport repeater). Для работы активных концентраторов и коммутаторов требуется питание от сети.

Преимущества звездообразной топологии:

– центральный концентратор звездообразной сети удобно использовать для диагностики;

– отказ одного компьютера не обязательно приводит к останову всей сети;

– добавления новых узлов не уменьшает скорость передачи данных в сети;

– в одной сети допускается применение нескольких типов кабелей (если их позволяет использовать концентратор).

Недостатки сети со звездообразной топологией:

– при отказе центрального концентратора вся сеть становится неработоспособной;

– все компьютеры должны соединяться с центральной точкой, это увеличивает расход кабеля, следовательно, такие сети обходятся дороже, чем сети с иной топологией.

4 Среды передачи данных

Передача данных в сети осуществляется через определенную среду, например, кабель или воздух. Такая среда упрощает передачу данных от источника к получателю.

В современных сетях в основном используются три типа сред, связывающих устройства и предоставляющих путь, по которому передаются данные:

– металлические провода внутри кабелей;

– стеклянные или пластиковые волокна (волоконно-оптический кабель);

– беспроводная среда передачи данных.

Кодирование сигналов, которое необходимо для передачи, осуществляется по-разному в зависимости от типа среды. В металлических проводах данные кодируются в виде электрических импульсов, соответствующих определенным шаблонам. Передача в оптоволоконных сетях происходит в виде импульсов света, в диапазоне инфракрасного излучения или видимого света. При беспроводной передаче для описания разных значений битов используются шаблоны электромагнитного излучения.

Разные типы сред передачи данных отличаются характерными функциями и преимуществами. Критерии выбора среды передачи данных:

– расстояние передачи сигнала в рамках среды;

– условия реализации среды передачи данных;

– объем данных и требуемая скорость их передачи;

– стоимость носителей и их развертывания.

4.1 Кабельные линии связи

Кабельные линии связи имеют довольно сложную структуру. Кабель состоит из проводников, заключенных в несколько слоев изоляции. В компьютерных сетях используются три типа кабелей:

– коаксиальный кабель;

– витая пара;

– волоконно-оптический кабель.

4.1.1 Коаксиальный кабель

Коаксиальный кабель — электрический кабель, состоящий из центрального проводника и экрана, расположенных соосно и разделённых изоляционным материалом или воздушным промежутком. Используется для передачи радиочастотных электрических сигналов.

Коаксиальный кабель (см. рисунок 10) состоит из следующих компонент:

– оболочка — служит для изоляции и защиты от внешних воздействий, изготавливается из светостабилизированного изоляционного материала;

– внешний проводник в виде оплетки, фольги из меди, медного или алюминиевого сплава;

– изоляция, выполненная в виде диэлектрического заполнения, обеспечивающая постоянство взаимного расположения (соосность) внутреннего и внешнего проводников;

– внутренний проводник в виде одиночного прямолинейного или многожильного скрученного провода.

Рисунок 10 – Устройство коаксиального кабеля.

На сегодняшний день сети, построенные на основе коаксиального кабеля, встречаются крайне редко, так как они обладают весьма низкой пропускной способностью. Используется в основном для передачи видео и аудио сигналов.

4.1.2 Кабель витая пара

Витая пара (twisted pair) — разновидность электрического кабеля, используемого при создании телекоммуникационных сетей. Используется в телекоммуникациях и в компьютерных сетях в качестве физической среды передачи сигнала во многих технологиях, таких как Ethernet, Arcnet, Token ring, USB. Кабель представляет из себя некоторое количество изолированных проводников, скрученных между собой попарно для повышения помехоустойчивости. Все пары заключены в общую пластиковую оболочку (см. рисунок 11).

Свивание проводников производится с целью повышения степени связи между собой проводников одной пары (электромагнитные помехи одинаково влияют на оба провода пары) и последующего уменьшения электромагнитных помех от внешних источников, а также взаимных наводок при передаче сигналов. Для снижения связи отдельных пар кабеля провода пары свиваются с различным шагом.

На сегодняшний день витая пара является самым распространенным решением для построения локальных проводных сетей, так как имеет невысокую стоимость и легка в монтаже.

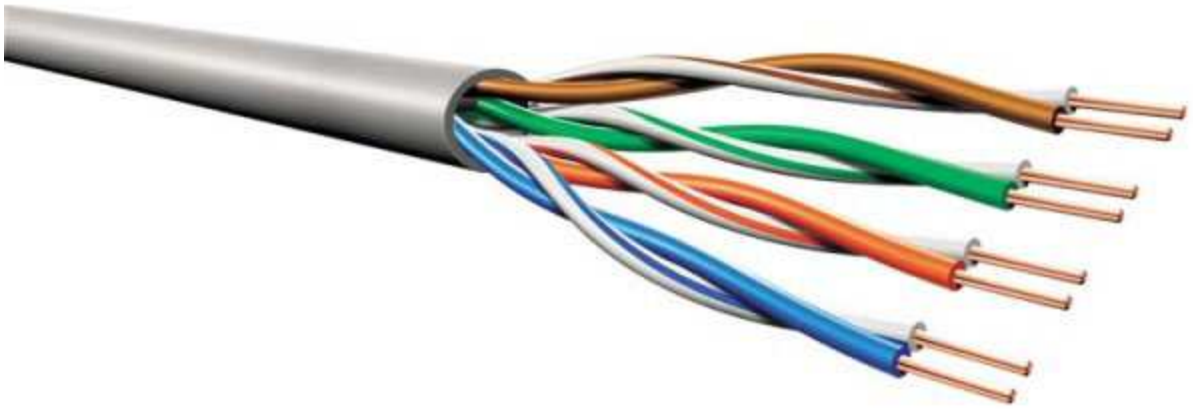

Рисунок 11 – Кабель витая пара.

Витая пара бывает неэкранированная (UTP) и экранированная (STP). Последняя покрыта дополнительным защитным алюминиевым или полиэстеровым экраном.

Существуют различные категории витой пары, различающиеся эффективным пропускаемым частотным диапазоном и нумеруемые от 1 до 7 (CAT1-7). Эти категории подробно описываются в стандарте EIA/TIA 568.

Пропускная способность сети на основе неэкранированной витой пары — от 1 Мбит/с до 1 Гбит/с, на основе экранированной витой пары — до 500 Мбит/с. Максимальная длина сегмента в обоих случаях не должна превышать 100 м.

4.1.3 Волоконно-оптический кабель

Волоконно-оптический кабель — кабель на основе оптоволоконных нитей, предназначенный для передачи оптических сигналов в линиях связи.

Структура волоконно-оптического кабеля (см. рисунок 12) похожа на структуру коаксиального электрического кабеля, только вместо центрального медного провода здесь используется тонкое (диаметром 1-10 мкм) стекловолокно, а вместо внутренней изоляции — стеклянная или пластиковая

оболочка, не позволяющая световому лучу выходить за пределы стекловолокна. Принцип действия основан на эффекте полного внутреннего отражения света от границы двух веществ с разными коэффициентами преломления (у стеклянной оболочки коэффициент преломления значительно ниже, чем у центрального волокна). Металлическая оплетка кабеля обычно отсутствует, так как экранирование от внешних электромагнитных помех здесь не требуется. Иногда ее применяют для механической защиты от внешних воздействий (такой кабель иногда называют броневым, он может объединять под одной оболочкой несколько оптоволоконных кабелей).

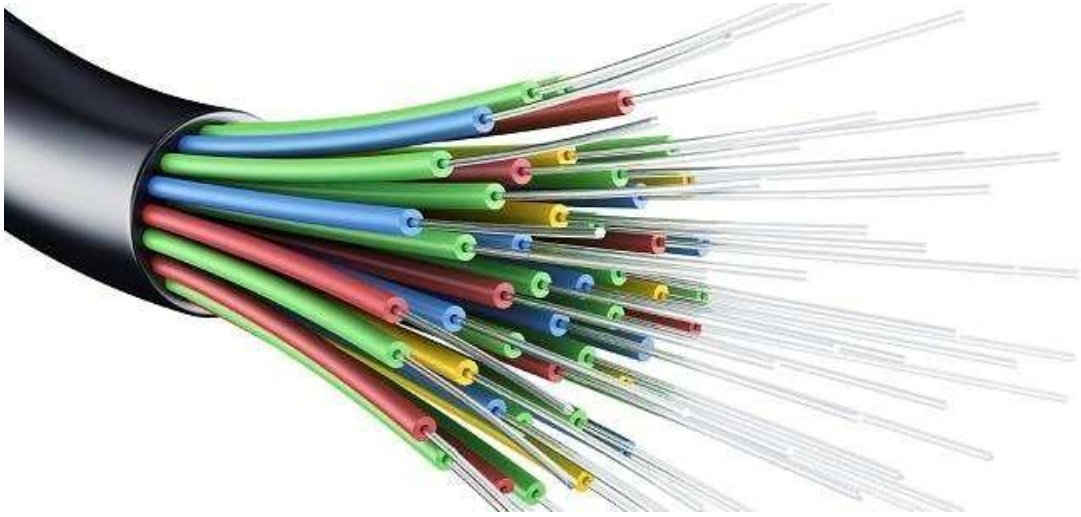

Рисунок 12 – Волоконно-оптический кабель.

Существуют два различных типа оптоволоконных кабелей:

– многомодовый;

– одномодовый.

Основные различия между этими типами связаны с разными режимами прохождения световых лучей в кабеле.

В одномодовом кабеле практически все лучи проходят один и тот же путь, в результате чего все они достигают приемника одновременно, и форма сигнала практически не искажается. Одномодовый кабель имеет диаметр центрального волокна около 1,3 мкм и передает свет только с такой же длиной волны. Дисперсия и потери сигнала при этом очень незначительны, что позволяет

передавать сигналы на значительно большее расстояние, чем в случае применения многомодового кабеля. Для одномодового кабеля применяются лазерные приемопередатчики, использующие свет исключительно с требуемой длиной волны.

В многомодовом кабеле траектории световых лучей имеют заметный разброс, в результате чего форма сигнала на приемном конце кабеля искажается. Центральное волокно имеет диаметр 62,5 мкм, а диаметр внешней оболочки - 125 мкм (это иногда обозначается как 62,5/125). Для передачи используется обычный (не лазерный) светодиод, что снижает стоимость и увеличивает срок службы приемопередатчиков по сравнению с одномодовым кабелем[9].

Волоконно-оптические кабели широко используются в телекоммуникациях, так как позволяют передавать данные на большие расстояния и с очень высокой скоростью (до нескольких Гбит/с и более). Оптоволоконные кабели не подвержены действию электромагнитных помех, сигнал, передаваемый по ним, невозможно перехватить.

4.2 Беспроводные линии связи

Беспроводная среда передачи данных характеризуется отсутствием необходимости в применении каких-либо кабелей. Для передачи информации могут использоваться радиоволны, а также инфракрасное, оптическое или лазерное излучение.

4.2.1 Инфракрасная связь

Инфракрасная связь — группа стандартов, описывающая протоколы физического и логического уровня передачи данных с использованием инфракрасного диапазона световых волн в качестве среды передачи данных. В компьютерной технике обычно используется для связи компьютеров с периферийными устройствами (например, инфракрасный порт IrDA).

Инфракрасный порт (IrDA) содержит в себе передатчик (специальный светодиод) и приемник (фотодиод), которые работают в инфракрасном диапазоне. Инфракрасное излучение не способно проникать сквозь преграды, поэтому для установления связи между устройствами их необходимо располагать в условиях прямой видимости относительно друг друга. См. рисунок 13. Основные характеристики представлены в таблице 1.

Таблица 1 – Основные характеристики технологии инфракрасный порт.

Название	**Стандарт**	**Назначение**	**Скорость передачи данных**	**Радиус действия**
Инфракрасный порт	IrDa	Персональная локальная сеть	до 16 Мбит/с	от 5 до 50 см, односторонняя связь — до 10 метров

Рисунок 13 – Инфракрасный порт.

Этот тип связи получил распространение в современных фотовспышках и синхронизаторах. Он используется для дистанционного запуска дополнительных вспышек и обмена данными между TTL-экспонометром фотоаппарата и микропроцессорами, управляющими мощностью импульсного освещения.

4.2.2 Беспроводная локальная связь Wi-Fi

Беспроводная локальная связь Wi-Fi — это семейство протоколов для беспроводных сетей на базе стандарта IEEE 802.11 в зоне частотных диапазонов 0,9; 2,4; 3,6 и 5 ГГц.

Таким образом, данный стандарт является наиболее приемлемым при построении беспроводных сетей (см. рисунок 14).

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка, когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с — наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi даёт клиенту полную свободу при выборе критериев для соединения.

Рисунок 14 – Использование беспроводной сети Wi-Fi.

Однако стандарт не описывает всех аспектов построения беспроводных локальных сетей Wi-Fi. Поэтому каждый производитель оборудования решает эту задачу по-своему, применяя те подходы, которые он считает наилучшими с той или иной точки зрения. Поэтому возникает необходимость классификации способов построения беспроводных локальных сетей.

По способу объединения точек доступа в единую систему можно выделить:

автономные точки доступа (называются также самостоятельные, децентрализованные, умные)

точки доступа, работающие под управлением контроллера.

Основные характеристики представлены в таблице 2.

Таблица 2 – Основные характеристики технологии Wi-Fi.

Название	**Стандарт**	**Назначение**	**Скорость передачи данных**	**Радиус действия**	**Частота**
Wi-Fi	802.11a	Локальная сеть	до 54 Мбит/с	до 100 метров	5,0 ГГц
Wi-Fi	802.11ac	Локальная сеть	до 3.39 Гбит/с	до 100 метров	2.4+5.0 ГГц
Wi-Fi	802.11b	Локальная сеть	до 11 Мбит/с	до 100 метров	2,4 ГГц
Wi-Fi	802.11g	Локальная сеть	до 54 Мбит/с	до 100 метров	2,4 ГГц
Wi-Fi	802.11n	Локальная сеть	до 300 Мбит/с	до 100 метров	2,4–2,5 или 5,0 ГГц

4.2.3 Беспроводная персональная связь Bluetooht

Bluetooth — технология беспроводных персональных сетей. Bluetooth обеспечивает обмен информацией между такими устройствами, как ноутбуки, мобильные телефоны, принтеры, цифровые фотоаппараты, мышки, клавиатуры, джойстики, наушники, гарнитуры на надёжной, бесплатной, повсеместно доступной радиочастоте для ближней связи. Bluetooth позволяет этим устройствам сообщаться, когда они находятся в радиусе до 10 м друг от друга (дальность сильно зависит от преград и помех), даже в разных помещениях (см. рисунок 15).

Рисунок 15 – Использование беспроводной сети Bluetooth.

Принцип действия основан на использовании радиоволн. Радиосвязь Bluetooth осуществляется в ISM-диапазоне, который используется в различных бытовых приборах и беспроводных сетях (свободный от лицензирования диапазон 2,4-2,4835 ГГц). В Bluetooth применяется метод расширения спектра со скачкообразной перестройкой частоты. Метод FHSS прост в реализации, обеспечивает устойчивость к широкополосным помехам, а оборудование недорогое.

Согласно алгоритму FHSS, в Bluetooth несущая частота сигнала скачкообразно меняется 1600 раз в секунду[7] (всего выделяется 79 рабочих частот шириной в 1 МГц, а в Японии, Франции и Испании полоса уже — 23 частотных канала). Последовательность переключения между частотами для каждого соединения является псевдослучайной и известна только передатчику и приёмнику, которые каждые 625 мкс (один временной слот) синхронно перестраиваются с одной несущей частоты на другую. Таким образом, если рядом работают несколько пар приёмник-передатчик, то они не мешают друг другу. Этот алгоритм является также составной частью системы защиты конфиденциальности передаваемой информации: переход происходит по псевдослучайному алгоритму и определяется отдельно для каждого соединения. При передаче цифровых данных и аудиосигнала (64 кбит/с в обоих направлениях) используются различные схемы кодирования: аудиосигнал не повторяется (как правило), а цифровые данные в случае утери пакета информации будут переданы повторно.

Протокол Bluetooth поддерживает не только соединение «точка-точка», но и соединение «мультиточка»[7].

Основные характеристики представлены в таблице 3.

Таблица 3 – Основные характеристики технологии Bluetooth.

Название	**Стандарт**	**Назначение**	**Скорость передачи данных**	**Радиус действия**	**Частота**
Bluetooth v. 1.1	802.15.1	Персональная локальная сеть	до 0,7 Мбит/с	до 10 метров	2,4 ГГц
Bluetooth v. 2.0	802.15.3	Персональная локальная сеть	до 3 Мбит/с	до 100 метров	2,4 ГГц
Bluetooth v. 3.0	802.11	Персональная локальная сеть	от 3 Мбит/с до 24 Мбит/с	до 100 метров	2,4 ГГц

4.2.4 Беспроводная персональная связь ZigBee

ZigBee — стандарт для набора высокоуровневых протоколов связи, использующих небольшие, маломощные цифровые приёмопередатчики, основанный на стандарте IEEE 802.15.4 для беспроводных персональных сетей, таких как, беспроводные наушники. ZigBee предназначен для радиочастотных устройств, где необходима длительная работа от батареек и безопасность передачи данных по сети[3].

Рисунок 16 — Умный дом с технологией ZigBee.

Области применения стандарта (см. рисунок 16):

домашняя автоматизация;

рациональное использование энергии (ZigBee Smart Energy 1.0/2.0);

автоматизация коммерческого строительства;

телекоммуникационные приложения;

медицинское оборудование;

беспроводные игрушки.

Существуют три различных типа устройств ZigBee.

Координатор ZigBee (ZC) — наиболее ответственное устройство, формирует пути древа сети и может связываться с другими сетями. В каждой сети есть один координатор ZigBee. Он хранит информацию о настройках сети, выступает как доверенный центр и хранит ключи безопасности.

Маршрутизатор ZigBee (ZR) — может выступать в качестве промежуточного маршрутизатора, передавая данные с других устройств.

Конечное устройство ZigBee (ZED) — предназначено для обмена информацией только с материнским узлом (координатором, или маршрутизатором), поэтому не может получать данные с других устройств. Это позволяет ему большую часть времени пребывать в спящем состоянии, что позволяет экономить энергоресурс батарей. ZED требует минимальное количество памяти и поэтому стоит дешевле в производстве, чем ZR или ZC.

Основные характеристики представлены в таблице 4.

Таблица 4 – Основные характеристики технологии ZigBee.

Название	**Стандарт**	**Назначение**	**Скорость передачи данных**	**Радиус действия**	**Частота**
ZigBee	802.15.4	Персональная локальная сеть	от 20 до 250 Кбит/с	1—100 м	2,4 ГГц (16 каналов), 915 МГц (10 каналов), 868 МГц (один канал)

4.2.5 Сотовая связь

Сотовая связь — это вид радиосвязи, в основе которого лежит сотовая сеть. Ключевая особенность заключается в том, что общая зона покрытия делится на ячейки (соты), определяющиеся зонами покрытия отдельных базовых станций. Соты частично перекрываются и вместе образуют сеть. На идеальной (ровной и без застройки) поверхности зона покрытия одной базовой станции представляет собой круг, поэтому составленная из них сеть, имеет вид шестиугольных ячеек (сот).

Сеть составляют разнесённые в пространстве приёмопередатчики, работающие в одном и том же частотном диапазоне, и коммутирующее оборудование, позволяющее определять текущее местоположение подвижных абонентов и обеспечивать непрерывность связи при перемещении абонента из зоны действия одного приёмопередатчика в зону действия другого (см. рисунок 17).

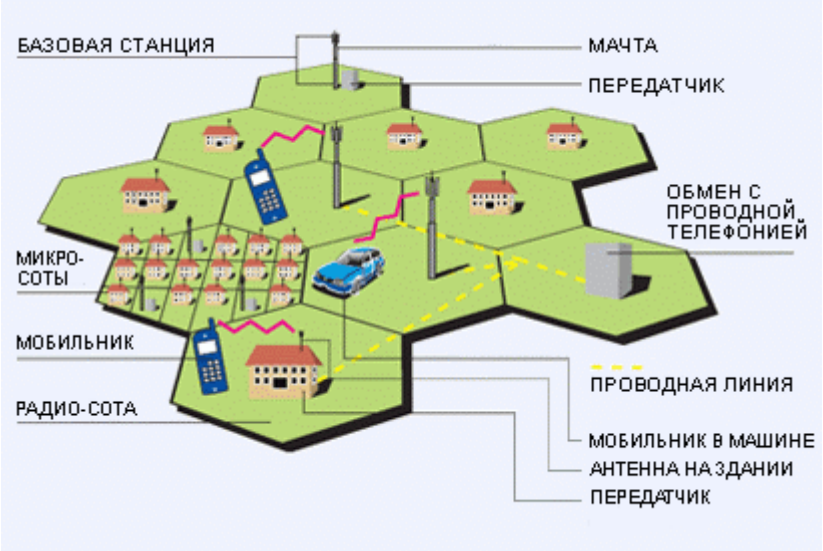

Рисунок 17 – Организация сотовой связи.

Стандарты сотовой связи для беспроводных сетей.

LTE — стандарт беспроводной высокоскоростной передачи данных для мобильных телефонов и других терминалов, работающих с данными. Он основан на GSM/EDGE и UMTS/HSPA сетевых технологиях, увеличивая пропускную способность и скорость за счёт использования другого радиоинтерфейса вместе с улучшением ядра сети[1].

Радиус действия базовой станции LTE зависит от мощности излучения и теоретически не ограничен, а максимальная скорость передачи данных зависит от радиочастоты и удалённости от базовой станции. Теоретический предел для скорости в 1 Мбит/сек — от 3,2 км (2600 МГц) до 19,7 км (450 МГц).

Диапазон 1800 МГц — наиболее используемый в мире, он сочетает в себе высокую емкость и относительно большой радиус действия (6,8 км).

Спецификация LTE позволяет обеспечить скорость загрузки до 326,4 Мбит/с, скорость отдачи до 172,8 Мбит/с, а задержка в передаче данных может быть снижена до 5 миллисекунд. LTE поддерживает полосы пропускания частот от 1,4 МГц до 20 МГц и поддерживает как частотное разделение каналов, так и временное разделение.

WiMAX — телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях

для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов).

WiMAX сети состоят из следующих основных частей: базовых и абонентских станций, а также оборудования, связывающего базовые станции между собой, с поставщиком сервисов и с Интернетом.

Для соединения базовой станции с абонентской используется высокочастотный диапазон радиоволн от 1,5 до 11 ГГц. В идеальных условиях скорость обмена данными может достигать 70 Мбит/с, при этом не требуется обеспечения прямой видимости между базовой станцией и приёмником.

Между базовыми станциями устанавливаются соединения (прямой видимости), использующие диапазон частот от 10 до 66 ГГц, скорость обмена данными может достигать 140 Мбит/с. При этом, по крайней мере, одна базовая станция подключается к сети провайдера с использованием классических проводных соединений. Однако, чем большее число БС подключено к сетям провайдера, тем выше скорость передачи данных и надёжность сети в целом.

Структура сетей семейства стандартов IEEE 802.16 имеет схожесть с традиционными GSM сетями (базовые станции действуют на расстояниях до десятков километров, для их установки не обязательно строить вышки — допускается установка на крышах домов при соблюдении условия прямой видимости между станциями)[6].

5 Взаимодействия в сетях

5.1 Типы подключения

Процессы способствуют взаимодействию между людьми, устройствами и данными. Выделяют три типа подключений.

5.1.1 Подключения M2M

Подключения «машина-машина» (M2M) происходят, когда данные передаются по сети от одного устройства к другому. К устройствам относятся:

– датчики,

– роботы,

– компьютеры и мобильные устройства.

Часто подключения M2M называют интернетом вещей.

Наиболее известный тип связи M2M — это телеметрия, используемая для передачи показателей производительности, собранных путем мониторинга аппаратуры в удаленных местах. Продукты со встроенными функциями коммуникации M2M нередко заявлены как «интеллектуальные».

Например, подключенный автомобиль, который отправляет сигнал о том, что водитель скоро прибудет домой, чтобы домашняя сеть отрегулировала температуру и освещение в доме, — это подключение M2M.

5.1.2 Подключения M2P

Подключения «машина-человек» (M2P) происходят, когда информация передается между машиной (например, компьютером, мобильным устройством или цифровым знаком) и человеком. Если человек получает информацию от базы данных или руководит комплексным анализом, то это подключение M2P. Подключения M2P способствуют перемещению, управлению и отчетности данных от устройств, чтобы люди принимали обоснованные решения. Действия, выполняемые людьми, исходя из обоснованных решений, завершают петлю обратной связи.

Существуют разные технологии M2P — от автоматизированных систем оповещения клиентов, основанных на определённых критериях срабатывания, до усовершенствованных панелей мониторинга, которые способствуют визуализации аналитических сведений. Также люди могут выполнять более сложные операции типа M2P, в том числе изучать и анализировать полученные данные, а также определять способ представления информации сотрудникам, ответственным за принятие решений.

5.1.3 Подключения P2P

Подключения «человек-человек» (P2P) происходят, когда информация передается от одного человека другому. Все чаще подключения P2P осуществляются посредством видео, мобильных устройств и социальных сетей. Зачастую такие подключения P2P называют совместной работой.

Подключения P2P характеризуются совместными решениями, которые задействуют новые и существующие сетевую инфраструктуру, устройства и приложения. Эти оптимизированные и безопасные сетевые платформы обеспечивают передачу голоса, видео и данных в едином представлении между любыми конечными и мобильными устройствами в обоих направлениях.

5.2 Архитектура компьютерных систем

5.2.1 Архитектура «клиент-сервер»

Чтобы понять принципы передачи данных по сети, необходимо изучить принципы построения сетевые соединений.

С начала эпохи Интернета для обработки данных чаще всего использовали модель типа «клиент-сервер». Рассмотрим типичный способ организации файловых серверов. Конечные пользователи внутри организации могут хранить на файловом сервере любое количество файлов и документов, благодаря чему у конечных устройств остается больше памяти и вычислительной мощности для локальных приложений. За счет хранения файлов на центральном файловом сервере другие пользователи внутри организации без труда получают доступ к

нужным файлам, что способствует взаимодействию и совместному использованию информации. Наконец, благодаря централизованным сервисам (например, файловым серверам), организации могут реализовывать централизованные процедуры безопасности и резервирования для защиты ресурсов (см. рисунок 18).

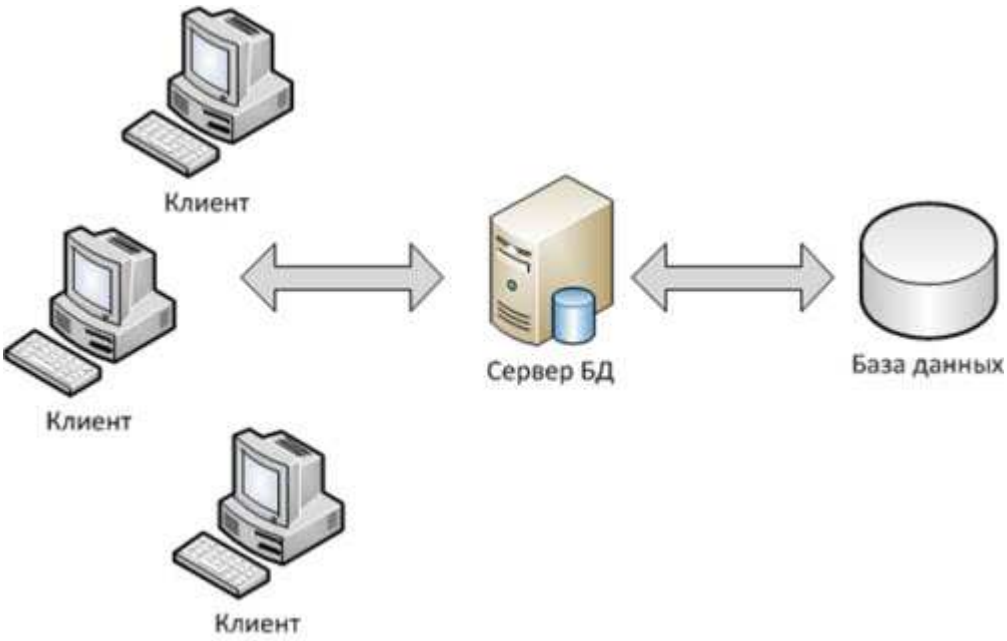

Рисунок 18 – Архитектура «клиент-сервер».

Вследствие расширения Интернета и увеличения количества пользователей мобильных устройств модель типа «клиент-сервер» не всегда является наиболее эффективным вариантом. Поскольку все больше людей подключаются издалека, централизованного сервера может быть недостаточно. Пользователи, находящиеся слишком далеко от сервера, могут испытывать большие задержки и трудности с получением доступа к информации. Эти изменения в требованиях для организаций и рядовых пользователей привели к появлению облачных вычислений.

5.2.2 Архитектура облачных вычислений

Облачные вычисления отличаются от модели типа «клиент-сервер» тем, что серверы и сервисы рассредоточены по всему миру в распределенных центрах обработки данных. С приходом облачных вычислений сильно изменились

рабочие нагрузки. Облачные вычисления позволяют конечным пользователям обращаться к приложениям на серверах, расположенных в облаке, не требуя наличия клиентского ПО на конечном устройстве (см. рисунок 19).

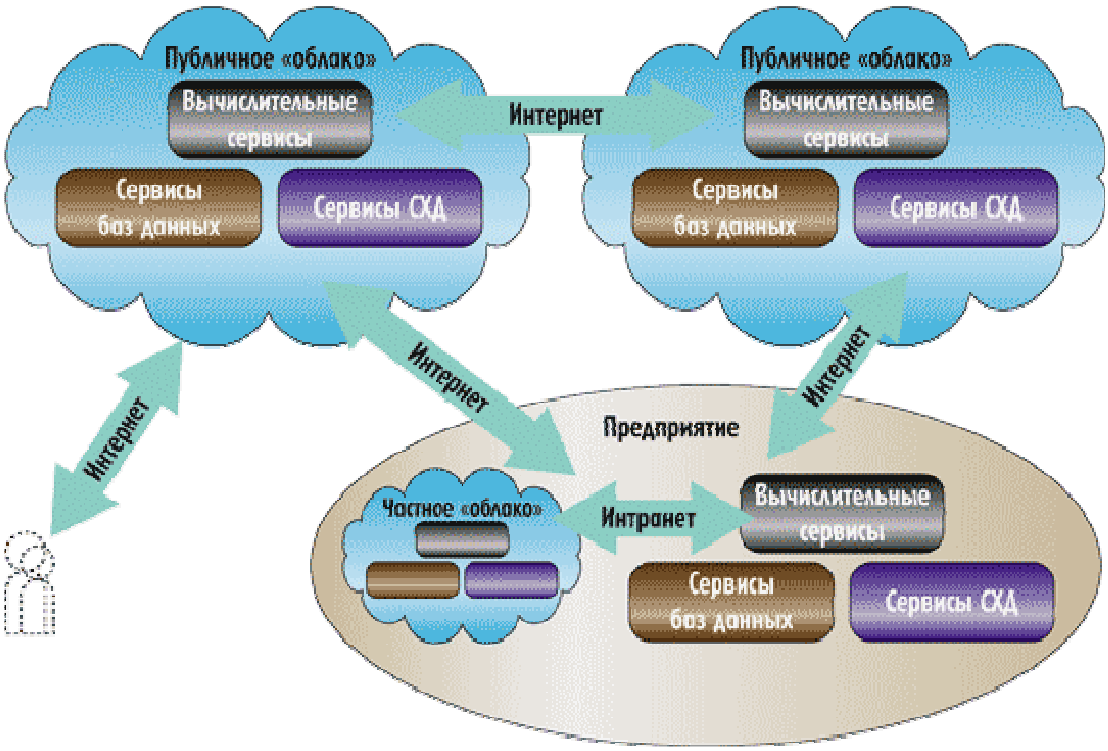

Рисунок 19 – Архитектура облачных вычислений.

В облачных вычислениях данные синхронизируются между несколькими серверами, чтобы серверы из разных центров обработки данных содержали одну и ту же информацию. Организации просто подписываются на различные сервисы в одном облаке. Отдельным организациям больше не нужно отвечать за поддержку обновлений, систем безопасности и резервирования для приложения. Теперь за это отвечает организация, предлагающая облачный сервис.

Microsoft Outlook — это система типа «клиент-сервер», которая, как правило, устанавливается для определенной организации. Конечные пользователи подключаются к серверу электронной почты с помощью локально установленного почтового клиента.

Gmail — это программа, основанная на облачных вычислениях, которая предоставляет своим пользователям из любой точки мира доступ в учетную запись Gmail. Пользователь может создавать, открывать и изменять электронные письма из любого места, где есть подключение к Интернету, с помощью различных устройств и операционных систем. Пользователям больше не нужно следить за обновлением своих почтовых клиентов или устанавливать новые функции, поскольку все обновления выполняются на сервере автоматически.

Различают четыре типа моделей развертывания облачных вычислений:

– частная;

– общедоступная;

– коллективная;

– гибридная.

Частное облако создается исключительно для одной организации. Физически инфраструктура может находиться на территории предприятия или за ее пределами, а также принадлежать отдельному поставщику. Частное облако предоставляет услуги только сотрудникам данной организации.

Общедоступное облако создается для всеобщего использования. Физически инфраструктура расположена на территории поставщика, но может принадлежать одной или нескольким организациям, среди которых могут быть компании, учебные учреждения или правительства.

Коллективное облако создается для эксклюзивного использования конкретным сообществом. Сообщество состоит из нескольких организаций, разделяющих общие интересы (например, одна цель, одинаковые требования к безопасности, политика и соображения совместимости). Физически инфраструктура может находиться на территории предприятия или за ее пределами, может принадлежать отдельному поставщику или одной, или нескольким организациям в сообществе. Различия между общедоступным облаком и коллективным облаком заключаются в функциональных

потребностях, настроенных для сообщества. Например, медицинские учреждения должны соблюдать политики и законы, которые требуют особой аутентификации и конфиденциальности. Организации могут вместе стремиться к реализации этих требований в общем развертывании облака.

Инфраструктура ***гибридного облака*** состоит из двух и более отдельных элементов — облачных инфраструктур (частных, общедоступных или принадлежащих сообществам). Эти элементы соединяются вместе посредством технологий, обеспечивающих переносимость данных и приложений. Благодаря переносимости организации могут поддерживать одну сторону облачного решения, одновременно используя преимущества, предлагаемые различными поставщиками облачных услуг. Поставщики могут отличаться друг от друга географическим местоположением, пропускной способностью, требованиями политики или закона, системой безопасности и стоимостью. Гибридное облако предлагает гибкость, позволяющую по необходимости подстраиваться под различные услуги поставщиков.

5.2.3 Архитектура туманных вычислений

Облачные вычисления помогли решить много проблем традиционной модели типа «клиент-сервер». Однако облачные вычисления могут и не быть оптимальным вариантом для приложений, чувствительных к задержкам, которые требуют немедленного локального ответа.

Помимо работы с учётом местоположения и минимизации задержки, растущая популярность Интернета Вещей требует поддержки мобильной связи и территориального распределения. Устройства в Интернете Вещей потребуют данных реального времени и механизмов обеспечения качества обслуживания. Интернет Вещей охватывает практически безграничное количество устройств с поддержкой IP, которые могут контролировать или измерять почти что угодно. Но при этом все эти устройства разбросаны по земному шару (см. рисунок 20).

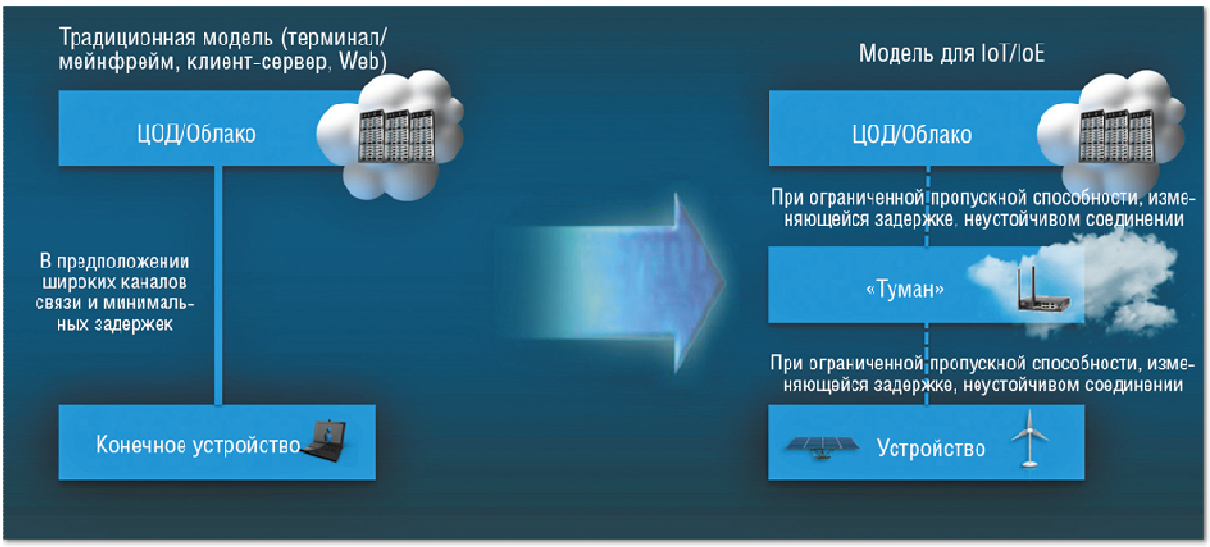

Рисунок 20 – Архитектура туманных вычислений.

Это может повлечь за собой некоторые проблемы, одна из которых заключается в создании каналов между этими устройствами и центров обработки данных, где эти данные можно будет анализировать, как показано на рисунке. Эти устройства могут производить большие объемы данных. Например, всего за 30 минут реактивный двигатель может создать 10 терабайт данных о производительности и состоянии. Отправлять все эти данные от устройств Интернета Вещей в облако для анализа и дальнейшей передачи решений на периметр не очень эффективно. Вместо этого часть анализа должна происходить на границе, например, на маршрутизаторах промышленного стандарта, созданных для работы в полевых условиях.

Туманные вычисления создают инфраструктуру распределенных вычислений рядом с границей сети, где выполняются простые задачи, требующие быстрого ответа. Это уменьшает загрузку сетей данными, улучшает отказоустойчивость за счет работы устройств Интернета Вещей во время потери сетевых подключений, а также повышает уровень безопасности, благодаря хранению чувствительных данных в пределах границы, где они необходимы.

5.3 Набор протоколов

Когда два устройства обмениваются данными по сети, сначала им необходимо согласовать определенный набор предустановленных правил (или протоколов). Протоколом называются правила общения, используемые устройствами и определяющие характеристики этого общения. При ежедневном личном общении правила для обмена данными по одному средству связи, например, по телефону, не обязательно совпадают с протоколом для использования другого средства связи, например, при отправке письма.

Протоколы определяют способ передачи и получения сообщений. Каждый язык, на котором общаются люди, имеет свод правил. Также и протоколы указывают, по каким правилам должны обмениваться данными устройства.

Группа взаимосвязанных протоколов, необходимых для выполнения функции связи, называется набором протоколов. Наборы протоколов позволяют обеспечить совместимость между сетевыми устройствами. Некоторые протоколы в наборе могут быть проприетарными (proprietary) и определяться конкретным поставщиком (vendor-specific). «Проприетарный» в данном контексте означает, что описание протокола и принципы его работы диктуются какой-то одной конкретной компанией. Некоторые проприетарные протоколы могут использоваться и другими организациями с разрешения владельца, а некоторые могут быть реализованы только на оборудовании, производимом поставщиком.

Наборы сетевых протоколов описывают следующие процессы.

– Формат или структура сообщения.

– Метод, посредством которого сетевые устройства обмениваются данными о каналах с другими сетями.

– Способ и время передачи сообщений об ошибках или системные сообщения между устройствами.

– Запуск и прекращение сеансов передачи данных.

Наборы протоколов могут быть реализованы аппаратно, программно или в сочетании этих двух способов. Каждый уровень отвечает за часть процесса по подготовке данных к передаче через сеть.

5.4 Семиуровневая модель открытых систем OSI

В 1978 году Международная организация по стандартизации (International Standards Organization ISO) выпустила набор спецификаций, описывающих архитектуру сети с неоднородными устройствами. В 1984 году ISO выпустила новую версию своей модели, названной эталонной моделью взаимодействия открытых систем (Open system Interconnection reference model, OSI). И с 1984 года эта версия стала международным стандартом.

Сетевая модель OSI (базовая эталонная модель взаимодействия открытых систем, англ. Open Systems Interconnection Basic Reference Model) — абстрактная сетевая модель для коммуникаций и разработки сетевых протоколов. Представляет уровневый подход к сети. Каждый уровень обслуживает свою часть процесса взаимодействия. Благодаря такой структуре совместная работа сетевого оборудования и программного обеспечения становится гораздо проще и прозрачнее.

Модель делит все функции сети на 7 уровней. Каждый уровень имеет заранее заданный набор функций, которые он должен выполнить для проведения связи.

5.4.1 Прикладной уровень

Прикладной уровень (уровень 7) – это самый близкий к пользователю уровень OSI. Он отличается от других уровней тем, что не обеспечивает услуг ни одному из других уровней OSI. Он обеспечивает услугами прикладные процессы, лежащие за пределами масштаба модели OSI. Примерами таких прикладных процессов могут служить процессы передачи речевых сигналов, базы данных, текстовые процессоры и т.д.

Прикладной уровень идентифицирует и устанавливает наличие предполагаемых партнеров для связи, синхронизирует совместно работающие прикладные процессы, а также устанавливает и согласовывает процедуры устранения ошибок и управления целостностью информации. Прикладной уровень также определяет, имеется ли в наличии достаточно ресурсов для предполагаемой связи.

5.4.2 Представительный уровень

Представительный уровень (уровень 6) отвечает за то, чтобы информация, посылаемая из прикладного уровня одной системы, была читаемой для прикладного уровня другой системы. При необходимости представительный уровень осуществляет трансляцию между множеством форматов представления информации путем использования общего формата представления информации.

Представительный уровень занят не только форматом и представлением фактических данных пользователя, но также структурами данных, которые используют программы. Поэтому кроме трансформации формата фактических данных (если она необходима), представительный уровень согласует синтаксис передачи данных для прикладного уровня.

5.4.3 Сеансовый уровень

Сеансовый уровень (уровень 5) устанавливает, управляет и завершает сеансы взаимодействия между прикладными задачами. Сеансы состоят из диалога между двумя или более объектами представления. Сеансовый уровень синхронизирует диалог между объектами представительного уровня и управляет обменом информации между ними.

Кроме того, сеансовый уровень предоставляет средства для отправки информации, класса услуг и уведомления в исключительных ситуациях о проблемах сеансового, представительного и прикладного уровней.

5.4.4 Транспортный уровень

Транспортный уровень (уровень 4) Граница между сеансовым и транспортным уровнями может быть представлена как граница между протоколами высших (прикладных) уровней и протоколами низших уровней. В то время как прикладной, представительный и сеансовый уровни заняты прикладными вопросами, четыре низших уровня решают проблемы транспортировки данных.

Транспортный уровень обеспечивает услуги по транспортировке данных, что избавляет высшие слои от необходимости вникать в ее детали. Функцией транспортного уровня является надежная транспортировка данных через сеть. Предоставляя надежные услуги, транспортный уровень обеспечивает механизмы для установки, поддержания и упорядоченного завершения действия каналов, систем обнаружения и устранения неисправностей транспортировки и управления информационным потоком (с целью предотвращения переполнения системы данными из другой системы).

5.4.5 Сетевой уровень

Сетевой уровень (уровень 3) – это комплексный уровень, который обеспечивает возможность соединения и выбор маршрута между двумя конечными системами.

Поскольку две конечные системы, желающие организовать связь, может разделять значительное географическое расстояние и множество подсетей, сетевой уровень является доменом маршрутизации. Протоколы маршрутизации выбирают оптимальные маршруты через последовательность соединенных между собой подсетей. Традиционные протоколы сетевого уровня передают информацию вдоль этих маршрутов.

5.4.6 Канальный уровень

Канальный уровень (уровень 2) (формально называемый информационно-канальным уровнем) обеспечивает надежный транзит данных через физический

канал. Выполняя эту задачу, канальный уровень решает вопросы физической адресации (в противоположность сетевой или логической адресации), топологии сети, линейной дисциплины (каким образом конечной системе использовать сетевой канал), уведомления об ошибках, упорядоченной доставки блоков данных и управления потоком информации.

5.4.7 Физический уровень

Физический уровень (уровень 1) определяет электротехнические, механические, процедурные и функциональные характеристики установления, поддержания и разъединения физического канала между конечными системами. Спецификации физического уровня определяют такие характеристики, как величины напряжений, параметры синхронизации, скорость передачи физической информации, максимальные расстояния передачи информации, физические соединители и другие аналогичные характеристики.

Физической средой в различных телекоммуникационных системах могут быть самые разнообразные средства от простейшей пары проводов до сложной системы передачи синхронной цифровой иерархии. Данный курс лекций посвящен рассмотрению именно физических сред и физического уровня эталонной модели взаимодействия открытых систем.

5.5 Стек протоколов TCP/IP

Один из наиболее распространенных наборов сетевых протоколов известен как протокол управления передачи/интернет-протокол (TCP/IP). Все устройства, которые обмениваются данными по Интернету, должны использовать набор протоколов TCP/IP. В частности, все они должны использовать протокол IP из интернет-уровня стека, поскольку он позволяет отправлять и получать данные через Интернет.

Модель TCP/IP в большей степени ориентируется на обеспечение сетевых взаимодействий. Для этой цели она признает важность иерархической

структуры функций, и предоставляет проектировщикам протоколов достаточную гибкость в реализации.

Стек протоколов TCP/IP включает в себя четыре уровня:

– прикладной уровень (application layer),

– транспортный уровень (transport layer),

– сетевой уровень (Internet layer),

– канальный уровень (link layer).

Стек является независимым от физической среды передачи данных, благодаря чему, в частности, обеспечивается полностью прозрачное взаимодействие между проводными и беспроводными сетями.

5.5.1 Прикладной уровень

Прикладной уровень является интерфейсом между приложением (участником информационного обмена, источником данных) и средой передачи данных. На прикладном уровне работает большинство сетевых приложений. Эти программы имеют свои собственные протоколы обмена информацией, например, HTTP для WWW, FTP (передача файлов), SMTP (электронная почта), SSH (безопасное соединение с удалённой машиной), DNS (преобразование символьных имён в IP-адреса) и многие другие.

В массе своей эти протоколы привязаны к определённому порту, например, HTTP на TCP-порт 80 или 8080. Эти порты определены Агентством по выделению имен и уникальных параметров протоколов.

5.5.2 Транспортный уровень

Протоколы транспортного уровня могут решать проблему негарантированной доставки сообщений («дошло ли сообщение до адресата?»), а также гарантировать правильную последовательность прихода данных. В стеке TCP/IP транспортные протоколы определяют, для какого именно приложения предназначены эти данные.

Протоколы автоматической маршрутизации, логически представленные на этом уровне:

TCP — «гарантированный» транспортный механизм с предварительным установлением соединения, предоставляющий приложению надёжный поток данных, дающий уверенность в безошибочности получаемых данных, перезапрашивающий данные в случае потери и устраняющий дублирование данных. TCP позволяет регулировать нагрузку на сеть, а также уменьшать время ожидания данных при передаче на большие расстояния. Более того, TCP гарантирует, что полученные данные были отправлены точно в такой же последовательности. В этом его главное отличие от UDP.

UDP — протокол передачи датаграмм без установления соединения. Также его называют протоколом «ненадёжной» передачи, в смысле невозможности удостовериться в доставке сообщения адресату, а также возможного перемешивания пакетов. UDP обычно используется в таких приложениях, как потоковое видео и компьютерные игры, где допускается потеря пакетов, а повторный запрос затруднён или не оправдан, либо в приложениях вида запрос-ответ (например, запросы к DNS), где создание соединения занимает больше ресурсов, чем повторная отправка.

И TCP, и UDP используют для определения протокола верхнего уровня число, называемое портом.

5.5.3 Сетевой уровень

Сетевой уровень изначально разработан для передачи данных из одной сети в другую. С развитием концепции глобальной сети в уровень были внесены дополнительные возможности по передаче из любой сети в любую сеть, независимо от протоколов нижнего уровня, а также возможность запрашивать данные от удалённой стороны.

Пакеты сетевого протокола IP могут содержать код, указывающий, какой именно протокол следующего уровня нужно использовать, чтобы извлечь данные из пакета. Это число — уникальный IP-номер протокола.

5.5.4 Канальный уровень

Канальный уровень описывает, каким образом передаются пакеты данных через физический уровень, включая кодирование (то есть специальные последовательности бит, определяющих начало и конец пакета данных). Ethernet, например, в полях заголовка пакета содержит указание того, какой машине или машинам в сети предназначен этот пакет.

Кроме того, канальный уровень описывает среду передачи данных (будь то коаксиальный кабель, витая пара, оптическое волокно или радиоканал), физические характеристики такой среды и принцип передачи данных (разделение каналов, модуляцию, амплитуду сигналов, частоту сигналов, способ синхронизации передачи, время ожидания ответа и максимальное расстояние).

5.6 Сравнение эталонных моделей OSI и TCP/IP

У моделей OSI и TCP имеется много общих черт. Обе модели основаны на концепции стека независимых протоколов. Функциональность уровней также во многом схожа. Например, в обеих моделях уровни, начиная с транспортного и выше, предоставляют сквозную, не зависящую от сети транспортную службу для процессов, желающих обмениваться информацией. Эти уровни образуют поставщика транспорта. Также в каждой модели уровни выше транспортного являются прикладными потребителями транспортных сервисов.

Несмотря на это фундаментальное сходство, у этих моделей имеется и ряд отличий. Для модели OSI центральными являются три концепции:

– службы;

– интерфейсы;

– протоколы.

Вероятно, наибольшим вкладом модели OSI стало явное разделение этих трех концепций. Каждый уровень предоставляет некоторые сервисы для расположенного выше уровня. Сервис определяет, что именно делает уровень,

но не то, как он это делает и каким образом сущности, расположенные выше, получают доступ к данному уровню.

Интерфейс уровня определяет способ доступа к уровню для расположенных выше процессов. Он описывает параметры и ожидаемый результат. Он также ничего не сообщает о внутреннем устройстве уровня.

Наконец, равноранговые протоколы, применяемые в уровне, являются внутренним делом самого уровня. Для выполнения поставленной ему задачи (то есть предоставления сервиса) он может использовать любые протоколы. Кроме того, уровень может менять протоколы, не затрагивая работу приложений более высоких уровней.

Эти идеи очень хорошо соответствуют современным идеям объектно-ориентированного программирования. Уровень может быть представлен в виде объекта, обладающего набором методов (операций), к которым может обращаться внешний процесс. Семантика этих методов определяет набор служб, предоставляемых объектом. Параметры и результаты методов образуют интерфейс объекта. Внутреннее устройство объекта можно сравнить с протоколом уровня. За пределами объекта оно никого не интересует и никому не видно.

Изначально в модели TCP/IP не было четкого разделения между службами, интерфейсом и протоколом, хотя и производились попытки изменить это, чтобы сделать ее более похожей на модель OSI. Так, например, единственными настоящими сервисами, предоставляемыми межсетевым уровнем, являются SEND IP PACKET (послать IP-пакет) и RECEIVE IP PACKET (получить IP-пакет).

В результате в модели OSI протоколы скрыты лучше, чем в модели TCP/IP, и при изменении технологии они могут быть относительно легко заменены. Возможность проводить подобные изменения — одна из главных целей многоуровневых протоколов.

Эталонная модель OSI была разработана прежде, чем были изобретены протоколы для нее. Такая последовательность событий означает, что эта модель не была настроена на какой-то конкретный набор протоколов, что сделало ее универсальной. Обратной стороной такого порядка действий было то, что у разработчиков было мало опыта в данной области и не было четкого представления о том, какие функции должен выполнять каждый уровень.

Например, уровень передачи данных изначально работал только в сетях с передачей от узла к узлу. С появлением широковещательных сетей в модель потребовалось ввести новый подуровень. Когда же на базе модели OSI начали строить реальные сети с использованием существующих протоколов, обнаружилось, что они не соответствуют требуемым спецификациям служб. Поэтому в модель пришлось добавить подуровни для устранения несоответствия. Наконец, изначально ожидалось, что в каждой стране будет одна сеть, управляемая правительством и использующая протоколы OSI, поэтому никто и не думал об объединении различных сетей. В действительности все оказалось не так.

С моделью TCP/IP было все наоборот: сначала появились протоколы, а уже затем была создана модель, описывающая существующие протоколы. Таким образом, не было проблемы с соответствием протоколов модели. Они ей соответствовали прекрасно. Единственной проблемой было то, что модель не соответствовала никаким другим стекам протоколов. В результате она не использовалась для описания каких-нибудь других сетей, отличных от TCP/IP.

Если взглянуть на эти две модели поближе, то, прежде всего, обратит на себя внимание различие в количестве уровней: в модели OSI семь уровней, в модели TCP/IP — четыре. В обеих моделях имеются межсетевой, транспортный и прикладной уровни, а остальные уровни различные.

Еще одно различие между моделями лежит в сфере возможности использования связи на основе соединений и связи без установления соединения. Модель OSI на сетевом уровне поддерживает оба типа связи, а на

транспортном уровне — только связь на основе соединений (поскольку транспортные службы являются видимыми для пользователя). В модели TCP/IP на сетевом уровне есть только один режим связи (без установления соединения), но на транспортном уровне он поддерживает оба режима, предоставляя пользователям выбор. Этот выбор особенно важен для простых протоколов «запрос — ответ».

6 Протоколы прикладного уровня

6.1 HTTP протокол

HTTP (англ. HyperText Transfer Protocol — «протокол передачи гипертекста») — протокол прикладного уровня передачи данных (изначально в виде гипертекстовых документов в формате «HTML», в настоящий момент используется для передачи произвольных данных). В работе использует 80 порт.

Основой HTTP является технология «клиент-сервер», то есть предполагается существование:

– клиентов, которые инициируют соединение и посылают запрос;

– серверов, которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом (см. рисунок 21).

Рисунок 21 – Сетевое взаимодействие по протоколу http.

HTTP в настоящее время повсеместно используется в сети Интернет для получения информации с веб-сайтов.

Основным объектом работы в HTTP является ресурс, на который указывает URI (Uniform Resource Identifier) в запросе клиента. Обычно такими ресурсами являются хранящиеся на сервере файлы, но ими могут быть логические объекты или что-то абстрактное. Особенностью протокола HTTP является возможность указать в запросе и ответе способ представления одного и того же

ресурса по различным параметрам: формату, кодировке, языку и т. д. (в частности, для этого используется HTTP-заголовок). Именно благодаря возможности указания способа кодирования сообщения, клиент и сервер могут обмениваться двоичными данными, хотя данный протокол является текстовым.

Особенностью протокола HTTP является то, что он не сохраняет своего состояния. Это означает отсутствие сохранения промежуточного состояния между парами «запрос-ответ». Компоненты, использующие HTTP, могут самостоятельно осуществлять сохранение информации о состоянии, связанной с последними запросами и ответами (например, «куки» на стороне клиента, «сессии» на стороне сервера). Браузер, посылающий запросы, может отслеживать задержки ответов. Сервер может хранить IP-адреса и заголовки запросов последних клиентов. Однако сам протокол не осведомлён о предыдущих запросах и ответах, в нём не предусмотрена внутренняя поддержка состояния, к нему не предъявляются такие требования.

Основные свойства HTTP протокола:

– Глобальные URI. HTTP основывается на механизме именования URI. HTTP использует URI во всех транзакциях для идентификации ресурсов в сети.

– Обмен по схеме запрос-ответ. HTTP-запросы отправляются клиентами, получая затем ответы от серверов. Направление потока — от клиента к серверу; сервер не инициирует сетевой трафик.

– Отсутствие сохранения состояния. Состояние между запросами и ответами клиентами и серверами не сохраняется. Каждая пара запрос-ответ трактуется как независимый обмен сообщениями.

– Метаданные ресурсов. Информация о ресурсах часто включается в Web-транзакции и может быть использована различными способами.

6.2 FTP протокол

FTP (англ. File Transfer Protocol) — протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к

серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами.

Отличительной особенностью FTP является использование двух TCP соединений для передачи данных.

1) ***Управляющее соединение*** устанавливается как обычное соединение клиент-сервер. Сервер осуществляет пассивное открытие на заранее известный порт FTP (21) и ожидает запроса на соединение от клиента. Клиент осуществляет активное открытие на TCP порт 21, чтобы установить управляющее соединение. Управляющее соединение существует все время, пока клиент общается с сервером. Это соединение используется для передачи команд от клиента к серверу и для передачи откликов от сервера.

2) ***Соединение данных*** открывается каждый раз, когда осуществляется передача файла между клиентом и сервером, а также при получении клиентом списка файлов (см. рисунок 22).

Рисунок 22 – Сетевое взаимодействие по протоколу ftp.

Обмен данными в FTP происходит по TCP-каналу. Обмен построен на технологии «клиент-сервер». FTP не может использоваться для передачи конфиденциальных данных, поскольку не обеспечивает защиты передаваемой информации и передает между сервером и клиентом открытый текст. FTP-сервер может потребовать от FTP-клиента аутентификации (т.е. при

присоединении к серверу FTP-пользователь должен будет ввести свой идентификатор и пароль). Однако пароль, и идентификатор пользователя будут переданы от клиента на сервер открытым текстом.

6.3 SMTP протокол

SMTP (англ. Simple Mail Transfer Protocol) — это сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.

Протокол SMTP поддерживает передачу сообщений электронной почты между произвольными узлами сети Интернет. Для работы через протокол SMTP клиент создаёт двухстороннее TCP соединение с сервером через порт 25. Затем клиент и SMTP сервер обмениваются информацией пока соединение не будет закрыто или прервано. Он служит для достоверной и надежной передачи сообщений между хостами сети Интернет (см. рисунок 23).

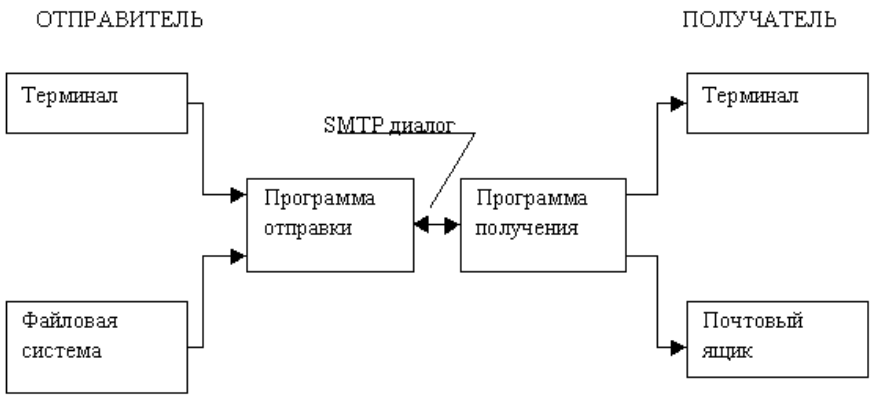

Рисунок 23 – Сетевое взаимодействие по протоколу smtp.

SMTP — протокол прикладного уровня, поэтому обычно над модулем SMTP располагается почтовая служба организаций. SMTP представляет собой независимый от транспортной подсистемы протокол, для работы которого необходим только транспортный канал передачи потока данных. Собственные механизмы промежуточного хранения почты и механизмы повышения надежности доставки позволяют протоколу SMTP использовать для работы различные транспортные службы. SMTP может работать по любому

транспортному каналу, удовлетворяющему требованиям передачи данных SMTP через различные сети или группы сетей.

Протокол SMTP обеспечивает как передачу сообщений на адрес одного получателя, так и тиражирование нескольких копий сообщения для передачи на разные адреса. Протокол SMTP может передавать не только текстовые сообщения, но и двоичную информацию, такую как рисунки, исполняемые файлы и др. Двоичная информация, находящаяся в сообщении, перед отправкой определенным образом форматируется и, как правило, кодируется в 7-битный вид, хотя современные расширения протокола SMTP — ESMTP позволяют передавать данные в 8-битном виде. Форматирование и кодирование разнородной пользовательской информации производится почтовым клиентом, обеспечивающим доступ к сервису электронной почты.

6.4 POP3 протокол

POP3 — это простейший протокол для работы пользователя с содержимым своего почтового ящика. Он позволяет только забрать почту из почтового ящика сервера на рабочую станцию клиента и удалить ее из почтового ящика на сервере. Всю дальнейшую обработку почтовое сообщение проходит на компьютере клиента. Этот протокол позволяет рабочим станциям динамически получать доступ к своим почтовым ящикам, расположенным на сервере, предназначенном для обслуживания электронной почты в данной организации.

POP3-сервер не отвечает за отправку почты, он работает только как универсальный почтовый ящик для группы пользователей. Когда пользователю необходимо отправить сообщение, он должен установить соединение с каким-либо SMTP-сервером и отправить туда свое сообщение по SMTP протоколу.

POP3-сервис, как правило, устанавливается на 110-й TCP-порт сервера, который будет находиться в режиме ожидания входящего соединения. Когда клиент хочет воспользоваться POP3-сервисом, он просто устанавливает TCP-соединение с портом 110 этого хоста. После установления соединения сервис

POP3 отправляет подсоединившемуся клиенту приветственное сообщение. После этого клиент и сервер начинают обмен командами и данными. По окончании обмена POP3-канал закрывается.

7 Классификация адресов в компьютерных сетях

Каждый компьютер в сети TCP/IP имеет адреса трех уровней:

Локальный адрес (MAC адрес);

IP-адрес;

Символьное имя.

7.1 Локальный адрес

Локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети, — это MAC-адрес сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта – идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.

Таким образом, глобально администрируемый MAC-адрес устройства глобально уникален и обычно «зашит» в аппаратуру.

7.2 IP-адрес

IP-адрес, состоящий из 4 байт, например, 109.26.17.100 или 6 байт, например, 2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов.

В исходном варианте — IP версии 4 (IPv4) — используются 32-разрядные

двоичные адреса. IP-адреса обычно записываются в виде четырех десятичных чисел, разделенных точками (так называемая десятичная запись с точечным разделением). Каждый компонент IP-адреса представляется одним октетом, то есть 8-разрядным двоичным числом. Двоичная запись удобна для

машинной обработки, но не для пользователей, поэтому сетевые адреса обычно записываются в более понятной десятичной форме. По этой причине необходимо хорошо понимать различия между десятичной и двоичной системами счисления, поскольку на них базируется вся схема адресации IP[11].

IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Интернет (Network Information Center, NIC), если сеть должна работать как составная часть Интернет. Обычно провайдеры услуг Интернет получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами.

Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла гибкое, и граница между этими полями может устанавливаться весьма произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Есть два способа определения того, сколько бит отводится на маску подсети, а сколько — на IP-адрес:

– классовая адресация, зависит от класса сети.

– бесклассовая адресация, при которой количество адресов в сети определяется маской подсети.

Введение в протоколе IPv6 поля «Метка потока» позволяет значительно упростить процедуру маршрутизации однородного потока пакетов. Поток — это последовательность пакетов, посылаемых отправителем определённому адресату. При этом предполагается, что все пакеты данного потока должны быть подвергнуты определённой обработке. Характер данной обработки задаётся дополнительными заголовками.

7.3 Символьное имя

Символьный идентификатор — имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем.

7.3.1 Система доменных имен DNS.

DNS (Domain Name System, система доменных имён) — иерархическая, распределенная в сети система баз данных, предоставляющая пользователям сети дополнительный сервис, по автоматическому преобразованию запросов, оформленных в удобном для человека текстовом формате, например, http://www.ipipe.ru, в цифровой IP адрес компьютера, например, 123.222.111.88, где находиться искомый ресурс. Единицей измерения этой системы является домен.

Домен — это область (зона) пространства иерархических имен сети Интернет, которая обслуживается набором серверов доменных имен (DNS) и централизованно администрируется. Домен идентифицируется именем домена (доменным именем).

Доменное имя (от англ. domain name) — аналог IP-адреса. Доменное имя представляет собой сочетание символов, разделенных точками. Доменное имя позволяет идентифицировать компьютер или любой информационный ресурс в сети Интернет. Например, petya_elkin.7-a.125shkola.edu.

Поддомен (англ. subdomain) — имя подчинённой зоны (например, wikipedia.org — поддомен домена org, а ru.wikipedia.org — домена wikipedia.org). Теоретически такое деление может достигать глубины 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина вместе с точками не достигнет 254 символов. Но на практике регистраторы доменных имён используют более строгие ограничения.

DNS-сервер — специализированное ПО для обслуживания DNS. DNS-сервер может быть ответственным за некоторые зоны и/или может перенаправлять запросы вышестоящим серверам.

DNS-клиент — специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.

DNS-запрос (англ. DNS query) — запрос от клиента (или сервера) серверу. Запрос может быть рекурсивным или нерекурсивным.

Нерекурсивный запрос либо возвращает данные о зоне, которая находится в зоне ответственности DNS-сервера (который получил запрос) или возвращает адреса корневых серверов (точнее, адрес любого сервера, который обладает большим объёмом информации о запрошенной зоне, чем отвечающий сервер).

В случае рекурсивного запроса сервер опрашивает серверы (в порядке убывания уровня зон в имени), пока не найдёт ответ или не обнаружит, что домен не существует. На практике поиск начинается с наиболее близких к искомому DNS-серверов, если информация о них есть в кеше и не устарела, то сервер может не запрашивать DNS-серверы. Рекурсивные запросы требуют больше ресурсов от сервера (и создают больше трафика), так что обычно принимаются от «известных» владельцу сервера узлов (например, провайдер предоставляет возможность делать рекурсивные запросы только своим клиентам, в корпоративной сети рекурсивные запросы принимаются только из локального сегмента). Нерекурсивные запросы обычно принимаются ото всех узлов сети.

Иерархию DNS чаще всего представляют в виде древовидной структуры

В основе этого дерева находиться корневой домен "." (root), далее идут домены первого уровня TLD (top level domains). За доменами первого уровня не закреплено никаких IP-адресов, они предназначены для создания на их основе (в их зонах) доменов второго уровня, с последующим закреплением за ними IP адресов. В настоящее время существует 2 вида доменов первого уровня:

– родовые (Generic Top Level Domains) — указывают на род деятельности владельца доменного имени, размещенного в той или иной доменной зоне (таблица 1).

– региональные (Country Code Top Level Domains) — указывают на принадлежность доменной зоны той или иной стране. Например, .ru - Россия, .us - США, .ua - Украина.

Процессом распределения IP-адресов и доменных имен управляет неправительственная, некоммерческая организация ICANN - The Internet Corporation for Assigned Names and Numbers (Интернет-корпорация по распределению адресов и имен). Примеры родовых доменов приведены в таблице 5

Таблица 5 – Примеры родовых доменов.

Домен первого уровня	**Для каких ресурсов предназначен (описание зоны)**
.aero	Для ресурсов мирового авиационного сообщества
.biz	Для бизнес-ресурсов
.com	Для коммерческих ресурсов
.coop	Для ресурсов кооперативных организаций
.info	Для информационных ресурсов
.museum	Для ресурсов о музеях и все что с ними связано
.name	Для индивидуальных ресурсов
.net	Для сетевых ресурсов
.org	Для общественных организаций

Примеры региональных доменов приведены в таблице 6.

Таблица 6 – Примеры региональных доменов.

Имя	**Страна**
.ae	ОАЭ
.bg	Болгария
.br	Бразилия
.cu	Куба
.cz	Чехия
.de	Германия
.fr	Франция

Имя	Страна
.gb	Великобритания
.it	Италия
.kz	Казахстан
.mx	Мексика
.na	Намибия
.ru	Россия
.рф	Россия
.us	США

Каждый DNS-сервер отвечает за свою зону иерархического пространства доменных имен. Информация эта постоянно обновляется. Сервера, которые поддерживают домены первого уровня, например, .ru, содержат информацию (IP адреса) о серверах доменных имен второго уровня, например, ipipe.ru. Сервера второго уровня содержат информацию (IP адреса) о доменах второго уровня, а также IP адреса DNS серверов, которые поддерживают домены 3 уровня и т.д. DNS сервера не существуют в единственном экземпляре. У каждого DNS сервера (еще называют первичным DNS сервером) есть свой «брат-близнец» (вторичный DNS сервер). Вся информация, записанная на первичном сервере, периодически копируется на вторичный. Это дает возможность нормальной работы системы DNS в случае выхода первичного DNS сервера из строя[4].

7.3.2 Алгоритм работы DNS

DNS работает в режиме вопрос/ответ. Допустим, Вы ввели в строке своего браузера volpi.ru. Рассмотрим работу DNS пошагово:

Шаг 1. Ваш браузер об IP адресе ipipe.ru ничего не знает и с запросом IP адреса volpi.ru через специальную программу resolver обращается к локальному серверу имен. Локальный DNS сервер – это сервер имен Вашей локальной сети или DNS сервер Вашего Интернет провайдера (если вы используете DialUp). Откуда браузеру известно о существовании этого локального DNS? Спросите Вы. Все очень просто: при настройках сетевого подключения Вы прописываете

IP адреса DNS серверов (предпочитаемого и/или альтернативного), один из которых будет отвечать на запросы, посылаемые Вашим браузером через resolver, – это и есть локальный или местный сервер Вашей сети. Для Вас местным сервером имен будет DNS сервер Вашего провайдера. IP адрес этого сервера также будет прописан в настройках сетевого подключения, независимо от того, как осуществлялась настройка (вручную или автоматически). Вы всегда сможете посмотреть IP адрес Вашего локального DNS сервера. Для этого достаточно посмотреть свойства сетевого подключения, используемого на Вашем компьютере.

Шаг 2. Запрос на IP адрес volpi.ru доходит до местного сервера имен. Этот сервер об этом IP адресе ничего не знает, и посылает запрос одному из корневых серверов «.» (root).

Шаг 3. Корневой сервер отдает локальному серверу IP адрес сервера, который поддерживает зону .ru.

Шаг 4. Далее по полученному адресу локальный сервер имен обращается к DNS серверу, который поддерживает .ru.

Шаг 5. Этот DNS сервер по полученному запросу отдает IP адрес сервера, который поддерживает зону volpi.ru.

Шаг 6. Местный DNS сервер с запросом IP адреса volpi.ru обращается к DNS серверу зоны volpi.ru.

Шаг 7. Локальный сервер имен получает IP адрес volpi.ru от DNS сервера зоны volpi.ru.

Шаг 8. Получив адрес volpi.ru локальный DNS сервер сообщает его Вашему браузеру.

Теперь браузер знает IP адрес volpi.ru и напрямую обращается к серверу, на котором расположен сайт volpi.ru.

8 Организация безопасности в сетях

Увеличение числа подключенных устройств и объемов, производимых ими данных, повышает спрос на безопасность этих данных.

Хакерские атаки происходят ежедневно, и кажется, что ни у одной организации нет от этого иммунитета. Учитывая, насколько легко в современном мире злоумышленники могут украсть и использовать информацию в своих целях, беспокойство о сетевой безопасности людей, процессов, данных и вещей, подключенных к Интернету, вполне естественно. Например, проблема взлома автомобиля.

8.1 Стратегия безопасности

Чем больше размеры и интеграция сети Интернет, тем более децентрализованной становится сеть. Это обеспечивает еще больше точек доступа в сеть, что подразумевает много уязвимостей. Очень много устройств, подключенных друг к другу, будут обмениваться данными из незащищенных местоположений, но этот процесс должен быть защищен. Однако из-за большого количества датчиков, интеллектуальных объектов и устройств, подключенных к сети, обеспечение безопасности — задача не из легких. Основной проблемой для специалистов по обеспечению безопасности являются потенциальные риски, связанные с предоставлением доступа к сети организации для незащищенных устройств.

В настоящее время тактика опережения угроз является основной стратегией системы сетевой безопасности. Подобно тому, как врачи пытаются предотвратить новые болезни, борясь с текущим диагнозом пациента, специалисты сетевой безопасности стремятся предупредить возможные угрозы, сводя к минимуму последствия от удавшихся атак.

Система безопасности должна быть повсеместной. Подход к обеспечению безопасности должен быть:

– последовательным и автоматизированным, а также достигать защищенных границ других организаций;

– динамичным для улучшенного распознавания угроз безопасности с помощью упреждающего анализа в реальном времени;

– интеллектуальным для обеспечения полного контроля всех подключений и элементов инфраструктуры;

– масштабируемым для удовлетворения потребностей растущей организации;

– адаптивным и способным реагировать на угрозы в реальном времени;

– комплексным, полноценным решением.

Решение повсеместной системы безопасности позволяет избежать изолированных средств защиты, которые сложны в управлении и требуют большого штата и обширных технических знаний.

8.2 Архитектура безопасности

При обеспечении безопасности сетей нельзя ограничиться лишь защитой отдельных устройств. Здесь важнее реализовать комплексное решение безопасности.

По всей сети должно быть развернуто решение безопасности, которое обеспечивает защиту с централизованным управлением политик и их распределенным применением. Для сбора и сопоставления данных по подключенной среде необходим непрерывный мониторинг деятельности в сети с последующим использованием полученных сведений и применением необходимых мер. Эти инструменты и системы работают сообща для получения сведений, применимых в обеспечении безопасности практически в реальном времени. При этом сеть может реагировать и перестраиваться в ответ на угрозы безопасности как самостоятельно, так и с незначительным вмешательством сотрудников.

8.3 Устройства обеспечения безопасности

К устройствам архитектуры безопасности, которые можно использовать для контроля доступа, проверки содержимого и соблюдения политик, относятся следующие:

– Межсетевые экраны — создают барьер между двумя сетями. На основании запрограммированных в него правил, межсетевой экран анализирует сетевой трафик с целью определить, допустим ли он для передачи между двумя сетями.

– Системы предотвращения вторжений (IPS) — отслеживают действия в сети и определяют, являются ли они вредоносными. IPS пытается предотвратить атаку, отклоняя трафик от вредоносного устройства или прерывая соединение.

8.4 Безопасность, ориентированная на приложения

По мере переключения организаций к средам, ориентированным на приложения, традиционные решения по обеспечению безопасности теряют свою актуальность. Решения по обеспечению безопасности защищают среды посредством полной интеграции настроенных технологий безопасности для защиты конкретного приложения. Решениями по обеспечению безопасности можно управлять, как пулом ресурсов, подключенных к приложениям и операциям с помощью центрального контроллера. Это решение может автоматически масштабироваться по запросу, что обеспечивает целостную систему безопасности на основе политик.

8.5 Безопасность беспроводной сети

Обеспечить безопасность беспроводной сети еще сложнее, чем защитить проводную сеть. В диапазоне действия точки доступа беспроводная сеть открыта для всех, кто обладает соответствующими учетными данными.

Система безопасности беспроводных сетей часто реализуется в точке доступа или в месте, где осуществляется беспроводное подключение к сети. Базовая система безопасности беспроводных сетей включает в себя следующие параметры.

– Настройка надежных протоколов аутентификации со стойкими паролями.

– Настройка защиты административного доступа.

– Включение шифрования.

– Изменение всех настроек по умолчанию.

– Своевременное обновление микропрограмм.

Однако, даже несмотря на применение указанных выше настроек, хакер с доступом к беспроводному устройству и знанием технологий взлома может взломать как сеть отдельного пользователя, так и организации. Кроме того, многие новые устройства с поддержкой беспроводной связи, подключающиеся к Интернету, не обладают функциями защиты беспроводной сети.

Именно поэтому трафик от интеллектуальных и мобильных устройств с поддержкой беспроводной связи, а также трафик от датчиков и встроенных объектов должен проходить через устройства обеспечения безопасности и контекстно-осведомленные приложения сети.

8.6 Избыточность и высокая степень доступности

При наличии столь большого количества подключений к сети важно обеспечить ее доступность и надежность.

Избыточность требует дополнительных компонентов сетевой инфраструктуры, каналов связи и элементов питания для резервирования основных ресурсов на случай их сбоя. Также избыточность поддерживает распределение нагрузки ресурсов, предоставляя высоко доступную структуру системы, которая обеспечивает соответствие заранее установленному уровню эксплуатационных показателей во время периода измерения, согласованного в договоре.

Помимо избыточных подключений и оборудования также необходимо резервирование данных. Безопасные резервы архивируют данные в зашифрованном формате, что предотвращает несанкционированный доступ к хранящемуся архиву.

8.7 Люди – это самое слабое звено

Некоторые люди преследуют злые цели, в то время как остальные допускают ошибки и не обеспечивают достаточный уровень безопасности, что подвергает риску их оборудование и данные. Для защиты активов должны быть применены правила и нормы, регулирующие поведение пользователей, определены допустимые и запрещенные действия, а также способ доступа к системам и данным.

8.8 Политика безопасности

Политика безопасности определяет все правила, нормы и процедуры, которым необходимо следовать для защиты организации, ее сотрудников и систем. Политику безопасности можно разделить на множество различных областей, направленных на борьбу с конкретными типами угроз.

Обучение пользователей — это самая важная составляющая политики безопасности. Сотрудники, действия которых регулируются политикой безопасности, должны не просто знать о ней, но и понимать ее, а также полностью следовать этой политике, чтобы обеспечить безопасность людей, данных и вещей.

8.9 Личные данные и Интернет

Организации могут собирать все виды личных данных. Однако между доступом и конфиденциальностью всегда есть противоречия в вопросах законности и этики. Блоки данных дополняются метаданными, которые содержат информацию о месте создания, авторе и пункте назначения данных. Таким образом, данные становятся собственностью, которой можно

обмениваться. Это изменение позволит контролировать информацию в целях соблюдения политик и законов в случае возникновения проблем.

8.10 Функции брандмауэров

Ключевым компонентом сетевой безопасности является ***брандмауэр*** (firewall) — компьютер, который обеспечивает взаимодействие сети и Интернетом, уделяя основное внимание безопасности.

Брандмауэр выполняет несколько функций:

– Сокращение количества точек доступа к сети до минимума.

– Предотвращение несанкционированного доступа к сети.

– Принудительная отправка трафика в Интернет через защищенные точки.

– Предотвращение атак типа отказа от обслуживания.

– Ограничение возможных действий в сети со стороны пользователей Интернета.

Брандмауэры не ограничиваются подключениями сети к Интернету, они также используются на серверах удаленного (модемного) доступа и при объединении сетей. Принцип работы брандмауэра заключается в направлении всего входящего и исходящего трафика по каналу, настройка которого обеспечивает контроль за службами и доступом.

Одним из ключевых аспектов настройки брандмауэра является принятие решений о том, какие службы следует пропускать через интерфейс сети с Интернетом, а какие следует запретить. Хотите ли вы разрешить подключения из сети к внешним компьютерам через FTP? А как насчет запросов web-страниц?

Администратор разрешает или запрещает отдельные службы, руководствуясь требованиями безопасности своей сети.

Многие брандмауэры по умолчанию разрешают служб:

– электронная почта (SMTP);

– HTTP;

– FTP;

– DNS (разрешение имен хостов).

8.11 Прокси-серверы

Прокси-сервер находится между сетью и Интернетом, принимает запросы к службам, анализирует их и, если сочтет запрос допустимым, передает для дальнейшей обработки. Фактически прокси-сервер предоставляет промежуточную точку, через которую должно производиться подключение к службе. Например, если вы находитесь внутри сети и хотите воспользоваться службой Telnet для подключения к интернет-хосту, прокси-сервер примет запрос, решит, стоит ли разрешить такое подключение, и затем создаст сеанс Telnet между собой и сервером Telnet. Прокси-сервер находится между пользователем и сервером Telnet, скрывает часть информации от пользователя, а все взаимодействие со службой осуществляется через него. Прокси-серверы работают со службами и приложениями, поэтому их часто называют «шлюзами уровня приложения».

Для чего нужны прокси-серверы? Представьте, что вы работаете над секретным проектом и хотите скрыть от Интернета всю информацию, относящуюся к вашей сети, — IP-адреса, учетные данные пользователей и т. д. При создании сеанса Telnet с удаленным хостом по Интернету ваш IP-адрес будет передан в пакетах. По адресу хакер может определить размер сети, особенно если мимо него проходят пакеты с разными IP-адресами. Прокси-сервер заменяет ваш IP-адрес своим собственным и использует внутреннюю таблицу для распределения входящего и исходящего трафика между нужными сторонами. За пределами сети виден только один IP-адрес, принадлежащий прокси-серверу. Иначе говоря, из-за специфики своей работы прокси-сервер также выполняет функции преобразования сетевых адресов (NAT).

Прокси-серверы всегда реализуются на программном уровне. Они не обязаны быть частью программного обеспечения брандмауэра, но обычно

выбирается именно этот вариант. Многие коммерческие брандмауэры также обладают функциями прокси-сервера. С другой стороны, многие программные прокси-серверы не ограничиваются выполнением посреднических функций; они также контролируют состав используемых приложений и блокируют некоторые входящие/исходящие данные.

9 Программирование

Все конечные и промежуточные устройства для правильного обмена данными должны быть запрограммированы, поэтому для работы с компьютерными технологиями важны навыки программирования.

9.1 Определение базовых возможностей программирования

Компьютерная программа — это набор инструкций, отправляемых компьютеру для выполнения в определенном порядке. Поскольку компьютеры не понимают человеческие языки, были созданы специальные компьютерные языки программирования. Эти языки позволяют людям писать инструкции таким образом, чтобы они были понятны компьютерам. Хотя существует несколько различных языков программирования, все они основаны на логических структурах.

Наиболее распространенные логические структуры в языках программирования.

– ***Оператор условия*** (If/Then/Else) — одна из наиболее распространенных структур программирования. Она используется для введения выполнения условного кода. Набор инструкций, следующий за ключевым словом THEN, выполняется, только если данное условие соответствует истине. Если условие ошибочно, то будет выполнена инструкция после оператора Else (см. рисунок 24).

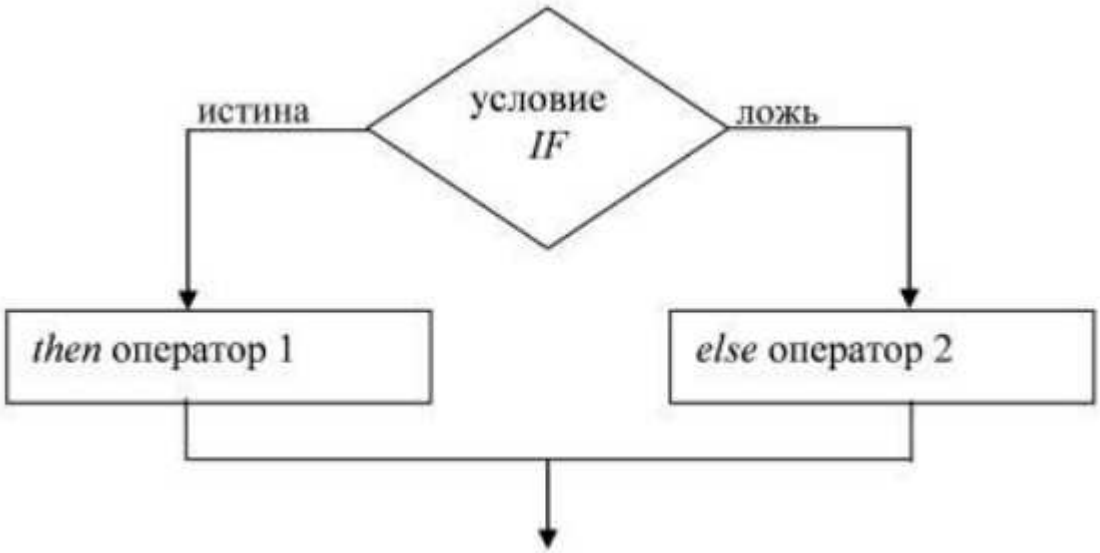

Рисунок 24 – Структура оператора if.

Например:

IF password = 12345,

THEN display “password correct.”

Этот код отобразит сообщение password correct (верный пароль) только в том случае, если будет введен пароль 12345.

– ***Оператор цикл*** (For/Do) — эта логическая структура используется для создания управляемых циклов. Набор инструкций выполняется столько раз, сколько определено в выражении. Если выражение уже не соответствует истине, то цикл заканчивается, и компьютер переходит к следующей инструкции (см. рисунок 25).

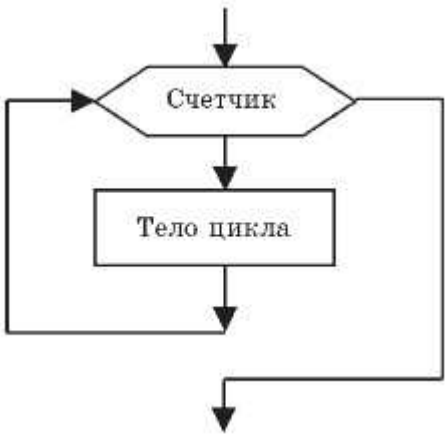

Рисунок 25 – Структура оператора for.

Например:

FOR count<=10 DO

display “not 10 yet!”

Программа проверяет значение переменной под названием count. Когда значение этой переменной меньше или равно 10, на экране будет отображено not 10 yet! (еще не равно 10!). Когда значение превысит 10, компьютер оставляет эту структуру и переходит к следующей строке кода.

Оператор цикл с условием (While/Do) — логическая структура WHILE тоже используется для контроля циклов, но немного по-другому. WHILE выполняет инструкции, пока условие соответствует истине. Когда условие больше не соответствует истине, компьютер оставляет эту структуру и переходит к следующей строке кода (см. рисунок 26).

Рисунок 26 – Структура оператора while.

Например:

WHILE temperature sensor> 80 DO

show “temperature too high!” on screen.

Сообщение temperature too high! (слишком высокая температура!) будет непрерывно отображаться, пока значение датчика температуры не сравняется с 80 или не опустится ниже этого уровня.

Подобные логические условия позволяют выстроить компьютерные программы.

9.2 Типы программ

Различные программы выполняют разные задачи. Например, бывают программы для измерения и отображения температуры, программы для управления светофорами и программы, которые позволяют нам взаимодействовать с компьютерами и устройствами.

Иногда категория программ становится настолько распространенной, что получает собственное название. Существуют следующие категории.

– ***Микропрограмма*** (прошивка, firmware) — содержит инструкции, которым следует устройство во время загрузки. Такая программа может быть единственной на устройстве или же содержать инструкции по загрузке более надежной операционной системы.

Например, микропрограммы используются в таких устройствах, как часы, принтеры, телевизоры, датчики, сотовые телефоны, маршрутизаторы и коммутаторы. Обычно микропрограмма не может похвастаться большим набором функций, и поэтому она не занимает много пространства.

– ***Операционные системы*** — эти программы помогают людям взаимодействовать с компьютером. К примерам операционных систем относятся Windows, MAC OS, Linux, Apple iOS, Android и Cisco IOS.

– ***Приложения*** — эти программы разрабатываются и пишутся для выполнения определенной задачи или услуги. Текстовые редакторы, программы для редактирования изображений, редакторы электронных таблиц, программы для обеспечения совместной работы, инструменты для анализа и мониторинга данных — все это приложения.

Заключение

Компьютерные технологии задействованы во всех областях человеческой деятельности.

Вычислительные сети постоянно развиваются и появляются новые стандарты передачи данных между узлами.

Наборы стандартных прикладных протоколов стека TCP/IP используются людьми повсеместно.

Поэтому важно понимать принципы работы сетей, чтобы быстрее осваивать новые технологии.

Ещё раз обратим внимание, что компьютерные технологии базируются на четырех составляющих:

– люди и вещи — это участники сбора и обмена информацией между собой;

– данные — это непосредственно сама информация, которая выступает как важнейший ресурс человеческого общества;

– информационные процессы — процессы, происходящие в ходе получения, обработки и передачи информации между участниками.

При этом не стоит забывать про безопасность работы в сети. Так как, расширяющееся число устройств и функций, увеличивает число внешних угроз для атаки злоумышленниками.

Технология «Интернет вещей», рассмотренная в данном пособии может стать основой для разработки проектных решений в учебном процессе.

Материал, изложенный в учебно-методическом пособии, понадобится студентам для изучения таких дисциплин, как «Вычислительные машины, системы и сети» и «Основы технических измерений».

Список литературы

1. 3GPP LTE Encyclopedia (точка доступа url: https://sites.google.com/site/lteencyclopedia/home)
2. IEEE 802.15.4 web site (точка доступа url: http://www.ieee802.org/15/pub/TG4.html)
3. Zigbee Alliance homepage (точка доступа url: http://www.zigbee.org/)
4. Альбитц, П., DNS и BIND. - Пер. с англ. - СПб. Символ-Плюс, 2002 - 696 с.
5. Б. Кришнамурти, Web-протоколы. Теория и практика. — М.: ЗАО «Издательство БИНОМ», 2002 г. - 592 с.
6. В.Вишневский, Энциклопедия WiMax. Путь 4G. /В. Вишневскй, С.Портной, И.Шахнович — М.: Техносфера, 2009 г. — 472 с.
7. Вишневский и др. Широкополосные беспроводные сети передачи данных. — М.: Техносфера, 2005. — 592 с.
8. Курс сетевой академии Cisco Introduction to the Internet of Everything - Russian - 1.1.
9. Оптоволоконные кабели, виды и характеристики. (точка доступа url: http://rostech.info/optovolokonnye-kabeli-vidy-i-harakteristiki)
10. Сети ЭВМ и телекоммуникации. Методические указания к лабораторным работам. /Сост. Д.Н. Лясин, С.Г. Саньков; Волгоград.гос.техн.ун-т.- Волгоград, 2003. – 54 с.
11. TCP/IP. Для профессионалов. 3-е изд. / Т. Паркер, К. Сиян. — СПб.: Питер, 2004.— 859 с.

Электронное учебное издание

Алексей Александрович **Силаев**

Компьютерные технологии и телекоммуникации

Учебно-методическое пособие

Электронное издание сетевого распространения

Редактор Н.И. Матвеева
И.Н. Горбунова

Темплан 2017 г. Поз. № 45
Подписано к использованию 26.12.2017 г. Формат 60×84 1/16.
Гарнитура Times. Усл. печ. л. 5,0.

Волгоградский государственный технический университет
400005, г. Волгоград, пр. Ленина, 28, корп. 1.

ВПИ (филиал) ВолгГТУ
404121, г. Волжский, ул. Энгельса, 42а.