МИНИСТЕРСТВО ВОДНОГО И СЕЛЬСКОГО ХОЗЯЙСТВА РЕСПУБЛИКИ УЗБЕКИСТАН
САМАРКАНДСКИЙ СЕЛЬСКОХОЗЯЙСТВЕННЫЙ ИНСТИТУТ

КАФЕДРА «ВЫСШАЯ МАТЕМАТИКИ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

КУРСОВАЯ РАБОТА

Курсовая работа на тему:

«Компьютерные сети и телекоммуникации»

Выполнила: Абулқосимова Зебинисо Давроновна
Специальность: технология хранения и первичной обработки сельскохозяйственной продукции.
Группа 16

Проверил: Акбаров Х.У

Самарканд 2015

СОДЕРЖАНИЕ

ВВЕДЕНИЕ....3
КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ....4
ТОПОЛОГИЯ ПОСТРОЕНИЯ ЛВС....13
МЕТОДЫ ДОСТУПА К ПЕРЕДАЮЩЕЙ СРЕДЕ В ЛВС....16
КОРПОРАТИВНАЯ СЕТЬ ИНТЕРНЕТ....29
ПРИНЦИПЫ, ТЕХНОЛОГИИ, ПРОТОКОЛЫ ИНТЕРНЕТ....30
ТЕНДЕНЦИИ РАЗВИТИЯ ИНТЕРНЕТ....32
ОСНОВНЫЕ КОМПОНЕНТЫ WWW, URL, HTML....34
ЗАКЛЮЧЕНИЕ....41
СПИСОК ЛИТЕРАТУРЫ....42

ВВЕДЕНИЕ

За последние годы глобальная сеть Интернет превратилась в явление мирового масштаба. Сеть, которая до недавнего времени использовалась ограниченным кругом ученых, государственных служащих и работников образовательных учреждений в их профессиональной деятельности, стала доступной для больших и малых корпораций и даже для индивидуальных пользователей.

Изначально Интернет представляла собой достаточно сложную систему для рядового пользователя. Как только Интернет стал доступен для коммерческих фирм и частных пользователей, началась разработка программного обеспечения для работы с различными полезными сервисами Интернет, такими, как FTP, Gopher, WAIS и Telnet. Специалисты также создали совершенно новый вид услуг, например, World Wide Web - систему, позволяющую интегрировать текст, графику и звук.

В данной работе я рассмотрю структуры Сети, ее инструментов и технологий и применения Интернет. Изучаемый мной вопрос крайне актуален потому, что Интернет сегодня переживает период взрывного роста.

1.КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Сети компьютеров имеют множество преимуществ перед совокупностью отдельных систем, в их числе следующие:

- Разделение ресурсов.
- Повышение надежности функционирования системы.
- Распределение загрузки.
- Расширяемость.

Разделение ресурсов.

Пользователи сети могут иметь доступ к определенным ресурсам всех узлов сети. В их числе, например, наборы данных, свободная память на удаленных узлах, вычислительная мощность удаленных процессоров и т.д. Это позволяет экономить значительные средства за счет оптимизации использования ресурсов и их динамического перераспределения в процессе работы.

Повышение надежности функционирования системы.

Поскольку сеть состоит из совокупности отдельных узлов, то в случае сбоя на одном или нескольких узлах другие узлы смогут взять на себя их функции. При этом пользователи могут даже и не заметить этого-перераспределение задач возьмет на себя программное обеспечение сети.

Распределение загрузки.

В сетях с переменным уровнем загруженности имеется возможность перераспределять задачи с одних узлов сети (с повышенной нагрузкой) на другие, где имеются свободные ресурсы. Такое перераспределение может производиться динамически в процессе работы, более того, пользователи могут даже и не знать об особенностях планирования задач в сети. Эти функции может брать на себя программное обеспечение сети.

Расширяемость.

Сеть может быть легко расширена за счет добавления новых узлов. При этом архитектура практически всех сетей позволяет легко адаптировать сетевое программное обеспечение к изменениям конфигурации. Более того, это может производиться автоматически.

Однако с точки зрения безопасности эти достоинства превращаются в уязвимые места, порождая серьезные проблемы.

Особенности работы в сети определяются ее двойственным характером: с одной стороны, сеть следует рассматривать как единую систему, а с другой, - как совокупность независимых систем, каждая из которых выполняет свои функции; имеет своих пользователей. Эта же двойственность проявляется в логическом и физическом восприятии сети: на физическом уровне взаимодействие отдельных узлов осуществляется с помощью сообщений различного вида и формата, которые интерпретируются протоколами. На логическом уровне (т.е. сточки зрения протоколов верхних уровней) сеть представляется как совокупность функций, распределенных по различным узлам, но связанных в единый комплекс.

Сети подразделяются:

1. По топологии сети (классификация по организации физического уровня).

Общая шина.

Все узлы соединены с общей высокоскоростной шиной передачи данных. Они одновременно настроены на прием сообщения, но каждый узел может принять только то сообщение, которое предназначено ему. Адрес идентифицируется контроллером сети, при этом в сети может быть только один узел с заданным адресом. Если два узла одновременно заняты передачей сообщения (столкновение пакетов), то один из них или они оба ее прекращают, ожидают случайный интервал времени, затем возобновляют попытку передачи (метод разрешения конфликтов). Возможен другой случай

— в момент передачи каким-либо узлом сообщения по сети, другие узлы начать передачу не могут (метод предотвращения конфликтов). Такая топология сети является очень удобной: все узлы являются равноправными, логическое расстояние между любыми двумя узлами равно 1, скорость передачи сообщений велика. Впервые организация сети «общая шина» и соответствующие протоколы нижних уровней были разработаны совместно компаниями DIGITAL и Rank Xerox, она получила название Ethernet.

Кольцо.

Сеть построена в виде замкнутого контура однонаправленных каналов между станциями. Каждая станция принимает сообщения по входному каналу, в начале сообщения содержится адресная и управляющая информация. На основании ее станция принимает решение сделать копию сообщения и убрать его из кольца либо передать по выходному каналу на соседний узел. Если в настоящий момент не передается никакого сообщения, станция сама может передать сообщение.

В кольцевых сетях используется несколько различных способов управления:

- гирляндная — управляющая информация передается по отдельным совокупностям (цепям) компьютеров кольца;

- управляющий маркер — управляющая информация оформляется в виде определенного битового шаблона, циркулирующего по кольцу; только при получении маркера станция может выдать сообщение в сеть (наиболее известный способ, получивший название token ring);

- сегментная — по кольцу циркулирует последовательность сегментов. Обнаружив пустой, станция может поместить в него сообщение и передать в сеть;

- вставка регистров — сообщение загружается в регистр сдвига и передается в сеть когда кольцо свободно.

Звезда.

Сеть состоит из одного узла-концентратора и нескольких соединенных с ним терминальных узлов, непосредственно между собой несвязанных. Один или несколько терминальных узлов могут являться концентраторами другой сети, в этом случае сеть приобретает древовидную топологию.

Управление сетью полностью осуществляется концентратором; терминальные узлы могут связываться между собой только через него. Обычно на терминальных узлах выполняется лишь локальная обработка данных. Обработка данных, имеющих отношение ко всей сети, осуществляется на концентраторе. Она носит название централизованной. Управление сетью обычно осуществляется с помощью процедуры опроса: концентратор через определенные промежутки времени опрашивает по очереди терминальные станции - есть ли для него сообщение. Если есть - терминальная станция передает сообщение на концентратор, если нет - осуществляется опрос следующей станции. Концентратор может передать сообщение одному или нескольким терминальным станциям в любой момент времени.

2. По размерам сети:

- Локальные.
- Территориальные.

Локальные.

Сеть передачи данных, связывающая ряд узлов в одной локальной зоне (комната, организация); обычно узлы сети комплектуются однотипным аппаратным и программным обеспечением (хотя это и необязательно). Локальные сети обеспечивают высокие скорости передачи информации.

Локальные сети характеризуются короткими (не более нескольких километров) линиями связи, контролируемой рабочей средой, низкой вероятностью ошибок, упрощенными протоколами. Для связи локальных сетей с территориальными используются шлюзы.

Территориальные.

Отличаются от локальных большей протяженностью линий связи (город, область, страна, группа стран), которые могут обеспечиваться телекоммуникационными компаниями. Территориальная сеть может связывать несколько локальных сетей, отдельные удаленные терминалы и ЭВМ и может быть соединена с другими территориальными сетями.

Территориальные сети редко используют какие-либо типовые топологические конструкции, так как они предназначены для выполнения других, обычно специфических задач. Поэтому они как правило строятся в соответствии с произвольной топологией, управление осуществляется с помощью специфических протоколов.

3. По организации обработки информации (классификация на логическом уровне представления; здесь под системой понимается вся сеть как единый комплекс):

Централизованная.

Системы такой организации наиболее широко распространены и привычны. Они состоят из центрального узла, реализующего весь комплекс выполняемых системой функций, и терминалов, роль которых сводится к частичному вводу и выводу информации. В основном периферийные устройства играют роль терминалов, с которых осуществляется управление процессом обработки информации. Роль терминалов могут выполнять дисплейные станции или персональные компьютеры, как локальные, так и удаленные. Любая обработка (в том числе связь с другими сетями) выполняется через центральный узел. Особенностью таких систем является

высокая нагрузка на центральный узел, в силу чего там должен быть высоконадежный и высокопроизводительный компьютер. Центральный узел является наиболее уязвимой частью системы: выход его из строя выводит из строя всю сеть. В тоже время задачи обеспечения безопасности в централизованных системах решаются наиболее просто и фактически сводятся к защите центрального узла.

Другой особенностью таких систем является неэффективное использование ресурсов центрального узла, а также неспособность гибкой перестройки характера работы (центральный компьютер должен работать все время, а значит какую-то его часть он может работать вхолостую). В настоящее время доля систем с централизованным управлением постепенно падает.

Распределенная.

Практически все узлы этой системы могут выполнять сходные функции, причем каждый отдельный узел может использовать оборудование и программное обеспечение других узлов. Основной частью такой системы является распределенная ОС, которая распределяет объекты системы: файлы, процессы (или задачи), сегменты памяти, другие ресурсы. Но при этом ОС может распределять не все ресурсы или задачи, а только часть их, например, файлы и свободную память на диске. В этом случае система все равно считается распределенной, количество ее объектов (функций, которые могут быть распределены по отдельным узлам) называется степенью распределенности. Такие системы могут быть как локальными, так и территориальными. Говоря математическим языком, основной функцией распределенной системы является отображение отдельных задач во множество узлов, на которых происходит их выполнение [4, с.49]. Распределенная система должна обладать следующими свойствами: [6]

1. Прозрачностью, то есть система должна обеспечить обработку информации вне зависимости от ее местонахождения.

2. Механизмом распределения ресурсов, который должен выполнять следующие функции: обеспечивать взаимодействие процессов и удаленный вызов задач, поддерживать виртуальные каналы, распределенные транзакции и службу имен.

3. Службой имен, единой для всей системы, включая поддержку единой службы директорий.

4. Реализацией служб гомогенных и гетерогенных сетей.

5. Контролем функционирования параллельных процессов.

6. Безопасностью. В распределенных системах проблема безопасности переходит на качественно новый уровень, поскольку приходится контролировать ресурсы и процессы всей системы в целом, а также передачу информации между элементами системы. Основные составляющие защиты остаются теми же - контроль доступа и информационных потоков, контроль трафика сети, аутентификация, операторский контроль и управление защитой. Однако контроль в этом случае усложняется.

Распределенная система обладает рядом преимуществ, не присущих никакой другой организации обработки информации: оптимальностью использования ресурсов, устойчивостью к отказам (выход из строя одного узла не приводит к фатальным последствиям - его легко можно заменить) и т.д. Однако при этом возникают новые проблемы: методика распределения ресурсов, обеспечение безопасности, прозрачности и др. В настоящее время все возможности распределенных систем реализованы далеко не полностью.

В последнее время все большее признание получает концепция обработки информации клиент-сервер. Данная концепция является переходной от централизованной к распределенной и одновременно

объединяющей обе последних. Однако клиент-сервер - это не столько способ организации сети, сколько способ логического представления и обработки информации.

Клиент-сервер - это такая организация обработки информации, при которой все выполняемые функции делятся на два класса: внешние и внутренние. Внешние функции состоят из поддержки интерфейса пользователя и функций представления информации на уровне пользователя. Внутренние касаются выполнения различных запросов, процесса обработки информации, сортировки и др.

Сущность концепции клиент-сервер заключается в том, что в системе выделяются элементы двух уровней: серверы, выполняющие обработку данных (внутренние функции), и рабочие станции, выполняющие функции формирования запросов и отображения результатов их обработки (внешние функции). От рабочих станций к серверу идет поток запросов, в обратном направлении - результаты их обработки. Серверов в системе может быть несколько и они могут выполнять различные наборы функций нижнего уровня (серверы печати, файловые и сетевые серверы). Основной объем информации обрабатывается на серверах, которые в этом случае играют роль локальных центров; информация вводится и выводится с помощью рабочих станций.

Отличительные особенности систем, построенных по принципу клиент-сервер, следующие:

- наиболее оптимальное использование ресурсов;

- частичное распределение процесса обработки информации в сети;

- прозрачный доступ к удаленным ресурсам;

- упрощенное управление;

- пониженный трафик;

- возможность более надежной и простой защиты;

- большая гибкость в использовании системы в целом, а также разнородного оборудования и программного обеспечения;

- централизованный доступ к определенным ресурсам,

Отдельные части одной системы могут строится по различным принципам и объединяться с использованием соответствующих согласующих модулей. Каждый класс сетей имеет свои специфические особенности как в плане организации, так и в плане защиты.

2.ТОПОЛОГИЯ ПОСТРОЕНИЯ ЛВС

Термин "топология сети" относится к пути, по которому данные перемещаются по сети. Существуют три основных вида топологий: "общая шина", "звезда" и "кольцо".

Рисунок 1. Шинная (линейная) топология.

Топология "общая шина" предполагает использование одного кабеля, к которому подключаются все компьютеры сети (рис. 1). В случае "общая шина" кабель используется совместно всеми станциями по очереди. Принимаются специальные меры для того, чтобы при работе с общим кабелем компьютеры не мешали друг другу передавать и принимать данные.

В топологии "общая шина" все сообщения, посылаемые отдельными компьютерами, подключенными к сети. Надежность здесь выше, так как выход из строя отдельных компьютеров не нарушит работоспособности сети в целом. Поиск неисправностей в кабеле затруднен. Кроме того, так как используется только один кабель, в случае обрыва нарушается работа всей сети.

Рисунок 2. Топология типа "звезда".

На рис. 2 показаны компьютеры, соединенные звездой. В этом случае каждый компьютер через специальный сетевой адаптер подключается отдельным кабелем к объединяющему устройству.

При необходимости можно объединять вместе несколько сетей с топологией "звезда", при этом получаются разветвленные конфигурации сети.

С точки зрения надежности эта топология не является

наилучшим решением, так как выход из строя центрального узла приведет к остановке всей сети. Однако при использовании топологии "звезда" легче найти неисправность в кабельной сети.

Используется также топология "кольцо" (рис. 3). В этом случае данные передаются от одного компьютера к другому как бы по эстафете. Если компьютер получит данные, предназначенные для другого компьютера, он передает их дальше по кольцу. Если данные предназначены для получившего их компьютера, они дальше не передаются.

Локальная сеть может использовать одну из перечисленных топологий. Это зависит от количества объединяемых компьютеров, их взаимного

расположения и других условий. Можно также объединить несколько локальных сетей, выполненных с использованием разных топологий, в единую локальную сеть. Может, например, древовидная топология.

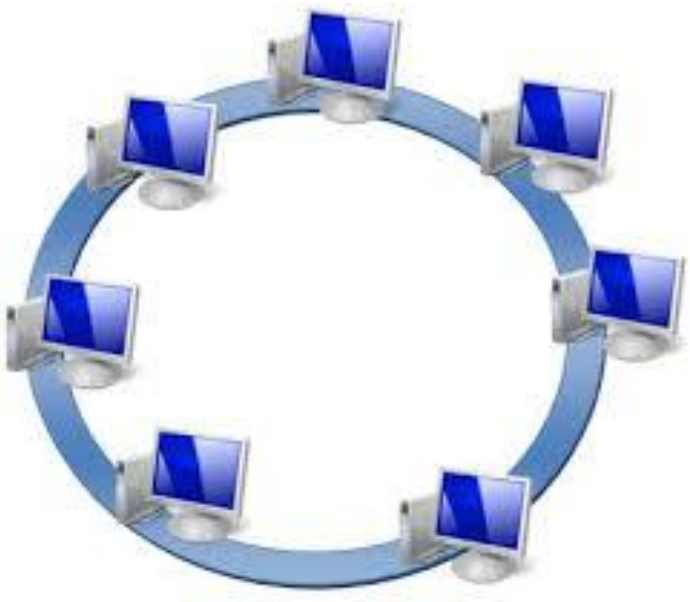

Рисунок 3. Кольцевая топология.

3.МЕТОДЫ ДОСТУПА К ПЕРЕДАЮЩЕЙ СРЕДЕ В ЛВС

Несомненные преимущества обработки информации в сетях ЭВМ оборачиваются немалыми сложностями при организации их защиты. Отметим следующие основные проблемы:

Разделение совместно используемых ресурсов.

В силу совместного использования большого количества ресурсов различными пользователями сети, возможно находящимися на большом расстоянии друг от друга, сильно повышается риск НСД - в сети его можно осуществить проще и незаметнее.

Расширение зоны контроля.

Администратор или оператор отдельной системы или подсети должен контролировать деятельность пользователей, находящихся вне пределов его досягаемости, возможно, в другой стране. При этом он должен поддерживать рабочий контакт со своими коллегами в других организациях.

Комбинация различных программно-аппаратных средств.

Соединение нескольких систем, пусть даже однородных по характеристикам, в сеть увеличивает уязвимость всей системы в целом. Система настроена на выполнение своих специфических требований безопасности, которые могут оказаться несовместимы с требованиями на других системах. В случае соединения разнородных систем риск повышается.

Неизвестный периметр.

Легкая расширяемость сетей ведет к тому, что определить границы сети подчас бывает сложно; один и тот же узел может быть доступен для пользователей различных сетей. Более того, для многих из них не всегда

можно точно определить сколько пользователей имеют доступ к определенному узлу и кто они.

Множество точек атаки.

В сетях один и тот же набор данных или сообщение могут передаваться через несколько промежуточных узлов, каждый из которых является потенциальным источником угрозы. Естественно, это не может способствовать повышению защищенности сети. Кроме того, ко многим современным сетям можно получить доступ с помощью коммутируемых линий связи и модема, что во много раз увеличивает количество возможных точек атаки. Такой способ прост, легко осуществим и трудно контролируем; поэтому он считается одним из наиболее опасных. В списке уязвимых мест сети также фигурируют линии связи и различные виды коммуникационного оборудования: усилители сигнала, ретрансляторы, модемы и т.д.

Сложность управления и контроля доступа к системе.

Многие атаки на сеть могут осуществляться без получения физического доступа к определенному узлу - с помощью сети из удаленных точек. В этом случае идентификация нарушителя может оказаться очень сложной, если не невозможной. Кроме того, время атаки может оказаться слишком мало для принятия адекватных мер.

По своей сути проблемы защиты сетей обусловлены двойственным характером последних: об этом мы говорили выше. С одной стороны, сеть есть единая система с едиными правилами обработки информации, а с другой, - совокупность обособленных систем, каждая из которых имеет свои собственные правила обработки информации. В частности, эта двойственность относится и к проблемам защиты. Атака на сеть может осуществляться с двух уровней (возможна их комбинация):

1. Верхнего - злоумышленник использует свойства сети для проникновения на другой узел и выполнения определенных

несанкционированных действий. Предпринимаемые меры защиты определяются потенциальными возможностями злоумышленника и надежностью средств защиты отдельных узлов.

2. Нижнего - злоумышленник использует свойства сетевых протоколов для нарушения конфиденциальности или целостности отдельных сообщений или потока в целом. Нарушение потока сообщений может привести к утечке информации и даже потере контроля за сетью. Используемые протоколы должны обеспечивать защиту сообщений и их потока в целом.

Защита сетей, как и защита отдельных систем, преследует три цели: поддержание конфиденциальности передаваемой и обрабатываемой в сети информации, целостности и доступности ресурсов и компонентов сети.

Эти цели определяют действия по организации защиты от нападений с верхнего уровня. Конкретные задачи, встающие при организации защиты сети, обуславливаются возможностями протоколов высокого уровня: чем шире эти возможности, тем больше задач приходится решать. Действительно, если возможности сети ограничиваются пересылкой наборов данных, то основная проблема защиты заключается в предотвращении НСД к наборам данных, доступным для пересылки. Если же возможности сети позволяют организовать удаленный запуск программ, работу в режиме виртуального терминала, то необходимо реализовывать полный комплекс защитных мер.

Защита сети должна планироваться как единый комплекс мер, охватывающий все особенности обработки информации. В этом смысле организация защиты сети, разработка политики безопасности, ее реализация и управление защитой подчиняются общим правилам, которые были рассмотрены выше. Однако необходимо учитывать, что каждый узел сети должен иметь индивидуальную защиту в зависимости от выполняемых функций и от возможностей сети. При этом защита отдельного узла должна

являться частью общей защиты. На каждом отдельном узле необходимо организовать:

- контроль доступа ко всем файлам и другим наборам данных, доступным из локальной сети и других сетей;

- контроль процессов, активизированных с удаленных узлов;

- контроль сетевого графика;

- эффективную идентификацию и аутентификацию пользователей, получающих доступ к данному узлу из сети;

- контроль доступа к ресурсам локального узла, доступным для использования пользователями сети;

- контроль за распространением информации в пределах локальной сети и связанных с нею других сетей.

Однако сеть имеет сложную структуру: для передачи информации с одного узла на другой последняя проходит несколько стадий преобразований. Естественно, все эти преобразования должны вносить свой вклад в защиту передаваемой информации, в противном случае нападения с нижнего уровня могут поставить под угрозу защиту сети. Таким образом, защита сети как единой системы складывается из мер защиты каждого отдельного узла и функций защиты протоколов данной сети.

Необходимость функций защиты протоколов передачи данных опять же обуславливается двойственным характером сети: она представляет собой совокупность обособленных систем, обменивающихся между собой информацией с помощью сообщений. На пути от одной системы к другой эти сообщения преобразуются протоколами всех уровней. А поскольку они являются наиболее уязвимым элементом сети, протоколы должны предусматривать обеспечение их безопасности для поддержки

конфиденциальности, целостности и доступности информации, передаваемой в сети.

Сетевое программное обеспечение должно входить в состав сетевого узла, в противном случае возможно нарушение работы сети и ее защиты путем изменения программ или данных. При этом протоколы должны реализовывать требования по обеспечению безопасности передаваемой информации, которые являются частью общей политики безопасности. Ниже приводится классификация угроз, специфических для сетей (угрозы нижнего уровня):

1. Пассивные угрозы (нарушение конфиденциальности данных, циркулирующих в сети) — просмотр и/или запись данных, передаваемых по линиям связи:

- просмотр сообщения - злоумышленник может просматривать содержание сообщения, передаваемого по сети;

- анализ графика - злоумышленник может просматривать заголовки пакетов, циркулирующих в сети и на основе содержащейся в них служебной информации делать заключения об отправителях и получателях пакета и условиях передачи (время отправления, класс сообщения, категория безопасности и т.д.); кроме того, он может выяснить длину сообщения и объем графика.

2. Активные угрозы (нарушение целостности или доступности ресурсов сети) — несанкционированное использование устройств, имеющих доступ к сети для изменения отдельных сообщений или потока сообщений:

- отказ служб передачи сообщений - злоумышленник может уничтожать или задерживать отдельные сообщения или весь поток сообщений;

- «маскарад» — злоумышленник может присвоить своему узлу или ретранслятору чужой идентификатор и получать или отправлять сообщения от чужого имени;

- внедрение сетевых вирусов — передача по сети тела вируса с его последующей активизацией пользователем удаленного или локального узла;

- модификация потока сообщений — злоумышленник может выборочно уничтожать, модифицировать, задерживать, переупорядочивать и дублировать сообщения, а также вставлять поддельные сообщения.

Совершенно очевидно, что любые описанные выше манипуляции с отдельными сообщениями и потоком в целом, могут привести к нарушениям работы сети или утечке конфиденциальной информации. Особенно это касается служебных сообщений, несущих информацию о состоянии сети или отдельных узлов, о происходящих на отдельных узлах событиях (удаленном запуске программ, например) — активные атаки на такие сообщения могут привести к потере контроля за сетью. Поэтому протоколы, формирующие сообщения и ставящие их в поток, должны предпринимать меры для их защиты и неискаженной доставки получателю.

Решаемые протоколами задачи аналогичны задачам, решаемым при защите локальных систем: обеспечение конфиденциальности обрабатываемой и передаваемой в сети информации, целостности и доступности ресурсов (компонентов) сети. Реализация этих функций осуществляется с помощью специальных механизмов. К их числу следует отнести:

- Механизмы шифрования, которые обеспечивают конфиденциальность передаваемых данных и/или информации о потоках данных. Используемый в данном механизме алгоритм шифрования может использовать секретный или открытый ключ. В первом случае предполагается наличие механизмов управления и распределения ключей. Различают два способа шифрования:

канальное, реализуемое с помощью протокола канального уровня, и оконечное (абонентское), реализуемое с помощью протокола прикладного или, в некоторых случаях, представительного уровня.

В случае канального шифрования защищается вся передаваемая по каналу связи информация, включая служебную. Этот способ имеет следующие особенности:

- вскрытие ключа шифрования для одного канала не приводит к компрометации информации в других каналах;

- вся передаваемая информация, включая служебные сообщения, служебные поля сообщений с данными, надежно защищена;

- вся информация оказывается открытой на промежуточных узлах - ретрансляторах, шлюзах и т.д.;

- пользователь не принимает участия в выполняемых операциях;

- для каждой пары узлов требуется свой ключ;

- алгоритм шифрования должен быть достаточно стоек и обеспечивать скорость шифрования на уровне пропускной способности канала (иначе возникнет задержка сообщений, которая может привести к блокировке системы или существенному снижению ее производительности);

- предыдущая особенность приводит к необходимости реализации алгоритма шифрования аппаратными средствами, что увеличивает расходы на создание и обслуживание системы.

Оконечное (абонентское) шифрование позволяет обеспечивать конфиденциальность данных, передаваемых между двумя прикладными объектами. Другими словами, отправитель зашифровывает данные, получатель - расшифровывает. Такой способ имеет следующие особенности (сравните с канальным шифрованием):

- защищенным оказывается только содержание сообщения; вся служебная информация остается открытой;

- никто кроме отправителя и получателя восстановить информацию не может (если используемый алгоритм шифрования достаточно стоек);

- маршрут передачи несущественен — в любом канале информация останется защищенной;

- для каждой пары пользователей требуется уникальный ключ;

- пользователь должен знать процедуры шифрования и распределения ключей.

Выбор того или иного способа шифрования или их комбинации зависит от результатов анализа риска. Вопрос стоит следующим образом: что более уязвимо — непосредственно отдельный канал связи или содержание сообщения, передаваемое по различным каналам. Канальное шифрование быстрее (применяются другие, более быстрые, алгоритмы), прозрачно для пользователя, требует меньше ключей. Оконечное шифрование более гибко, может использоваться выборочно, однако требует участия пользователя. В каждом конкретном случае вопрос должен решаться индивидуально.

- Механизмы цифровой подписи, которые включают процедуры закрытия блоков данных и проверки закрытого блока данных. Первый процесс использует секретную ключевую информацию, второй — открытую, не позволяющую восстановить секретные данные. С помощью секретной информации отправитель формирует служебный блок данных (например, на основе односторонней функции), получатель на основе общедоступной информации проверяет принятый блок и определяет подлинность отправителя. Сформировать подлинный блок может только пользователь, имеющий соответствующий ключ.

Механизмы контроля доступа.

Осуществляют проверку полномочий сетевого объекта на доступ к ресурсам. Проверка полномочий производится в соответствии с правилами разработанной политики безопасности (избирательной, полномочной или любой другой) и реализующих ее механизмов.

Механизмы обеспечения целостности передаваемых данных.

Эти механизмы обеспечивают как целостность отдельного блока или поля данных, так и потока данных. Целостность блока данных обеспечивается передающим и принимающим объектами. Передающий объект добавляет к блоку данных признак, значение которого является функцией от самих данных. Принимающий объект также вычисляет эту функцию и сравнивает ее с полученной. В случае несовпадения выносится решение о нарушении целостности. Обнаружение изменений может повлечь за собой действия по восстановлению данных. В случае умышленного нарушения целостности может быть соответствующим образом изменено и значение контрольного признака (если алгоритм его формирования известен), в этом случае получатель не сможет установить нарушение целостности. Тогда необходимо использовать алгоритм формирования контрольного признака как функцию данных и секретного ключа. В этом случае правильное изменение контрольного признака без знания ключа будет невозможно и получатель сможет установить, подвергались ли данные модификации.

Защита целостности потоков данных (от переупорядочивания, добавления, повторов или удаления сообщений) осуществляется с использованием дополнительных формы нумерации (контроль номеров сообщений в потоке), меток времени и т.д.

Желательными компонентами защиты сети являются следующие механизмы:

Механизмы аутентификации объектов сети.

Для обеспечения аутентификации используются пароли, проверка характеристик объекта, криптографические методы (аналогичные цифровой подписи). Эти механизмы обычно применяются для аутентификации одноуровневых сетевых объектов. Используемые методы могут совмещаться с процедурой «троекратного рукопожатия» (троекратный обмен сообщениями между отправителем и получателем с параметрами аутентификации и подтверждениями).

Механизмы заполнения текста.

Используются для обеспечения защиты от анализа графика. В качестве такого механизма может использоваться, например, генерация фиктивных сообщений; в этом случае трафик имеет постоянную интенсивность во времени.

Механизмы управления маршрутом.

Маршруты могут выбираться динамически или быть заранее заданы с тем, чтобы использовать физически безопасные подсети, ретрансляторы, каналы. Оконечные системы при установлении попыток навязывания могут потребовать установления соединения по другому маршруту. Кроме того, может использоваться выборочная маршрутизация (то есть часть маршрута задается отправителем явно - в обход опасных участков).

Механизмы освидетельствования.

Характеристики данных, передаваемые между двумя и более объектами (целостность, источник, время, получатель) могут подтверждаться с помощью механизма освидетельствования. Подтверждение обеспечивается третьей стороной (арбитром), которой доверяют все заинтересованные стороны и которая обладает необходимой информацией.

Помимо перечисленных выше механизмов защиты, реализуемых протоколами различных уровней, существует еще два, не относящихся к определенному уровню. Они по своему назначению аналогичны механизмам контроля в локальных системах:

Обнаружение и обработка событий (аналог средств контроля опасных событий).

Предназначены для обнаружения событий, которые приводят или могут привести к нарушению политики безопасности сети. Список этих событий соответствует списку для отдельных систем. Кроме того, в него могут быть включены события, свидетельствующие о нарушениях в работе перечисленных выше механизмов защиты. Предпринимаемые в этой ситуации действия могут включать различные процедуры восстановления, регистрацию событий, одностороннее разъединение, местный или периферийный отчет о событии (запись в журнал) и т.д.

Отчет о проверке безопасности (аналог проверки с использованием системного журнала).

Проверка безопасности представляет собой независимую проверку системных записей и деятельности на соответствие заданной политике безопасности.

Функции защиты протоколов каждого уровня определяются их назначением:

1. Физический уровень - контроль электромагнитных излучений линий связи и устройств, поддержка коммуникационного оборудования в рабочем состоянии. Защита на данном уровне обеспечивается с помощью экранирующих устройств, генераторов помех, средств физической защиты передающей среды.

2. Канальный уровень - увеличение надежности защиты (при необходимости) с помощью шифрования передаваемых по каналу данных. В этом случае шифруются все передаваемые данные, включая служебную информации.

3. Сетевой уровень - наиболее уязвимый уровень с точки зрения защиты. На нем формируется вся маршрутизирующая информация, отправитель и получатель фигурируют явно, осуществляется управление потоком. Кроме того, протоколами сетевого уровня пакеты обрабатываются на всех маршрутизаторах, шлюзах и др. промежуточных узлах. Почти все специфические сетевые нарушения осуществляются с использованием протоколов данного уровня (чтение, модификация, уничтожение, дублирование, переориентация отдельных сообщений или потока в целом, маскировка под другой узел и др.).

Защита от всех подобных угроз осуществляется протоколами сетевого и транспортного уровней и с помощью средств криптозащиты. На данном уровне может быть реализована, например, выборочная маршрутизация.

4. Транспортный уровень - осуществляет контроль за функциями сетевого уровня на приемном и передающем узлах (на промежуточных узлах протокол транспортного уровня не функционирует). Механизмы транспортного уровня проверяют целостность отдельных пакетов данных, последовательности пакетов, пройденный маршрут, время отправления и доставки, идентификацию и аутентификацию отправителя и получателя и др. функции. Все активные угрозы становятся видимыми на данном уровне.

Гарантом целостности передаваемых данных является криптозащита данных и служебной информации. Никто кроме имеющих секретный ключ получателя и/или отправителя не может прочитать или изменить информацию таким образом, чтобы изменение осталось незамеченным.

Анализ графика предотвращается передачей сообщений, не содержащих информацию, которые, однако, выглядят как настоящие. Регулируя интенсивность этих сообщений в зависимости от объема передаваемой информации можно постоянно добиваться равномерного графика. Однако все эти меры не могут предотвратить угрозу уничтожения, переориентации или задержки сообщения. Единственной защитой от таких нарушений может быть параллельная доставка дубликатов сообщения по другим путям.

5. Протоколы верхних уровней обеспечивают контроль взаимодействия принятой или переданной информации с локальной системой. Протоколы сеансового и представительного уровня функций защиты не выполняют. В функции защиты протокола прикладного уровня входит управление доступом к определенным наборам данных, идентификация и аутентификация определенных пользователей, а также другие функции, определяемые конкретным протоколом. Более сложными эти функции являются в случае реализации полномочной политики безопасности в сети.

4.КОРПОРАТИВНАЯ СЕТЬ ИНТЕРНЕТ

Корпоративная сеть представляет собой частный случай корпоративной сети крупной компании. Очевидно, что специфика деятельности предъявляет жесткие требования к системам защиты информации в компьютерных сетях. Не менее важную роль при построении корпоративной сети играет необходимость обеспечения безотказной и бесперебойной работы, поскольку даже кратковременный сбой в ее работе может привести к гигантским убыткам. И, наконец, требуется обеспечить быструю и надежную передачу большого объема данных, поскольку многие прикладные программы должны работать в режиме реального времени.

Требования к корпоративной сети

Можно выделить следующие основные требования к корпоративной сети:

- Сеть объединяет в структурированную и управляемую замкнутую систему все принадлежащие компании информационные устройства: отдельные компьютеры и локальные вычислительные сети (LAN), хост-серверы, рабочие станции, телефоны, факсы, офисные АТС.
- В сети обеспечивается надежность ее функционирования и мощные системы защиты информации. То есть, гарантируется безотказная работа системы как при ошибках персонала, так и в случае попытки несанкционированного доступа.
- Существует отлаженная система связи между отделениями разного уровня (как с городскими, так и с иногородними отделениями).
- В связи с современными тенденциями развития появляется потребность в специфичных решениях. Существенную роль приобретает организация оперативного, надежного и безопасного доступа удаленного клиента к современным услугам.

5.ПРИНЦИПЫ, ТЕХНОЛОГИИ, ПРОТОКОЛЫ ИНТЕРНЕТ

Основное, что отличает Internet от других сетей - это ее протоколы - TCP/IP. Вообще, термин TCP/IP обычно означает все, что связано с протоколами взаимодействия между компьютерами в Internet. Он охватывает целое семейство протоколов, прикладные программы, и даже саму сеть. TCP/IP - это технология межсетевого взаимодействия, технология internet. Сеть, которая использует технологию internet, называется "internet". Если речь идет о глобальной сети, объединяющей множество сетей с технологией internet, то ее называют Internet.

Свое название протокол TCP/IP получил от двух коммуникационных протоколов (или протоколов связи). Это Transmission Control Protocol (TCP) и Internet Protocol (IP). Несмотря на то, что в сети Internet используется большое число других протоколов, сеть Internet часто называют TCP/IP-сетью, так как эти два протокола, безусловно, являются важнейшими.

Как и во всякой другой сети в Internet существует 7 уровней взаимодействия между компьютерами: физический, логический, сетевой, транспортный, уровень сеансов связи, представительский и прикладной уровень. Соответственно каждому уровню взаимодействия соответствует набор протоколов (т.е. правил взаимодействия).

Протоколы физического уровня определяют вид и характеристики линий связи между компьютерами. В Internet используются практически все известные в настоящее время способы связи от простого провода (витая пара) до волоконно-оптических линий связи (ВОЛС).

Для каждого типа линий связи разработан соответствующий протокол логического уровня, занимающийся управлением передачей информации по каналу. К протоколам логического уровня для телефонных линий относятся

протоколы SLIP (Serial Line Interface Protocol) и PPP (Point to Point Protocol). Для связи по кабелю локальной сети - это пакетные драйверы плат ЛВС.

Протоколы сетевого уровня отвечают за передачу данных между устройствами в разных сетях, то есть занимаются маршрутизацией пакетов в сети. К протоколам сетевого уровня принадлежат IP (Internet Protocol) и ARP (Address Resolution Protocol).

Протоколы транспортного уровня управляют передачей данных из одной программы в другую. К протоколам транспортного уровня принадлежат TCP (Transmission Control Protocol) и UDP (User Datagram Protocol).

Протоколы уровня сеансов связи отвечают за установку, поддержание и уничтожение соответствующих каналов. В Internet этим занимаются уже упомянутые TCP и UDP протоколы, а также протокол UUCP (Unix to Unix Copy Protocol).

Протоколы представительского уровня занимаются обслуживанием прикладных программ. К программам представительского уровня принадлежат программы, запускаемые, к примеру, на Unix-сервере, для предоставления различных услуг абонентам. К таким программам относятся: telnet-сервер, FTP-сервер, Gopher-сервер, NFS-сервер, NNTP (Net News Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP2 и POP3 (Post Office Protocol) и т.д.

К протоколам прикладного уровня относятся сетевые услуги и программы их предоставления.

6.ТЕНДЕНЦИИ РАЗВИТИЯ ИНТЕРНЕТ

В 1961 году DARPA (Defence Advanced Research Agensy) по заданию министерства обороны США приступило к проекту по созданию экспериментальной сети передачи пакетов. Эта сеть, названная ARPANET, предназначалась первоначально для изучения методов обеспечения надежной связи между компьютерами различных типов. Многие методы передачи данных через модемы были разработаны в ARPANET. Тогда же были разработаны и протоколы передачи данных в сети - TCP/IP. TCP/IP - это множество коммуникационных протоколов, которые определяют, как компьютеры различных типов могут общаться между собой.

Эксперимент с ARPANET был настолько успешен, что многие организации захотели войти в нее, с целью использования для ежедневной передачи данных. И в 1975 году ARPANET превратилась из экспериментальной сети в рабочую сеть. Ответственность за администрирование сети взяло на себя DCA (Defence Communication Agency), в настоящее время называемое DISA (Defence Information Systems Agency). Но развитие ARPANET на этом не остановилось; протоколы TCP/IP продолжали развиваться и совершенствоваться.

В 1983 году вышел первый стандарт для протоколов TCP/IP, вошедший в Military Standarts (MIL STD), т.е. в военные стандарты, и все, кто работал в сети, обязаны были перейти к этим новым протоколам. Для облегчения этого перехода DARPA обратилась с предложением к руководителям фирмы внедрить протоколы TCP/IP в Berkeley(BSD) UNIX. С этого и начался союз UNIX и TCP/IP.

Спустя некоторое время TCP/IP был адаптирован в обычный, то есть в общедоступный стандарт, и термин Internet вошел во всеобщее употребление. В 1983 году из ARPANET выделилась MILNET, которая стала

относиться к министерству обороны США. Термин Internet стал использоваться для обозначения единой сети: MILNET плюс ARPANET. И хотя в 1991 году ARPANET прекратила свое существование, сеть Internet существует, ее размеры намного превышают первоначальные, так как она объединила множество сетей во всем мире. Рисунок 4 иллюстрирует рост числа хостов, подключенных к сети Internet с 4 компьютеров в 1969 году до 8,3 миллионов в 1996. Хостом в сети Internet называются компьютеры, работающие в многозадачной операционной системе (Unix, VMS), поддерживающие протоколы TCP\IP и предоставляющие пользователям какие-либо сетевые услуги.

7.ОСНОВНЫЕ КОМПОНЕНТЫ WWW, URL, HTML

World Wide Web переводится на русский язык как “Всемирная Паутина”. И, в сущности, это действительно так. WWW является одним из самых совершенных инструментов для работы в глобальной мировой сети Internet. Эта служба появилась сравнительно недавно и все еще продолжает бурно развиваться.

Наибольшее количество разработок имеют отношение к родине WWW - CERN, European Particle Physics Laboratory; но было бы ошибкой считать, что Web является инструментом, разработанным физиками и для физиков. Плодотворность и привлекательность идей, положенных в основу проекта, превратили WWW в систему мирового масштаба, предоставляющую информацию едва ли не во всех областях человеческой деятельности и охватывающую примерно 30 млн. пользователей в 83 странах мира.

Главное отличие WWW от остальных инструментов для работы с Internet заключается в том, что WWW позволяет работать практически со всеми доступными сейчас на компьютере видами документов: это могут быть текстовые файлы, иллюстрации, звуковые и видео ролики, и т.д.

Что такое WWW? Это попытка организовать всю информацию в Internet, плюс любую локальную информацию по вашему выбору, как набор гипертекстовых документов. Вы перемещаетесь по сети, переходя от одного документа к другому по ссылкам. Все эти документы написаны на специально разработанном для этого языке, который называется HyperText Markup Language (HTML). Он чем-то напоминает язык, использующийся для написания текстовых документов, только HTML проще. Причем, можно использовать не только информацию, предоставляемую Internet, но и создавать собственные документы. В последнем случае существует ряд практических рекомендаций к их написанию.

Вся польза гипертекста состоит в создании гипертекстовых документов, если вас заинтересовал какой либо пункт в таком документе, то вам достаточно ткнуть туда курсором для получения нужной информации. Также в одном документе возможно делать ссылки на другие, написанные другими авторами или даже расположенные на другом сервере. В то время как вам это представляется как одно целое.

Гипермедиа это надмножество гипертекста. В гипермедиа производятся операции не только над текстом но и над звуком, изображениями, анимацией.

Существуют WWW-серверы для Unix, Macintosh, MS Windows и VMS, большинство из них распространяются свободно. Установив WWW-сервер, вы можете решить две задачи:

1. Предоставить информацию внешним потребителям - сведения о вашей фирме, каталоги продуктов и услуг, техническую или научную информацию.

2. Предоставить своим сотрудникам удобный доступ к внутренним информационным ресурсам организации. Это могут быть последние распоряжения руководства, внутренний телефонный справочник, ответы на часто задаваемые вопросы для пользователей прикладных систем , техническая документация и все, что подскажет фантазия администратора и пользователей. Информация, которую вы хотите предоставить пользователям WWW, оформляется в виде файлов на языке HTML. HTML - простой язык разметки, который позволяет помечать фрагменты текста и задавать ссылки на другие документы, выделять заголовки нескольких уровней, разбивать текст на абзацы, центрировать их и т. п., превращая простой текст в отформатированный гипермедийный документ. Достаточно легко создать html-файл вручную, однако, имеются специализированные редакторы и преобразователи файлов из других форматов.

Основные компоненты технологии World Wide Web

К 1989 году гипертекст представлял новую, многообещающую технологию, которая имела относительно большое число реализаций с одной стороны, а с другой стороны делались попытки построить формальные модели гипертекстовых систем, которые носили скорее описательный характер и были навеяны успехом реляционного подхода описания данных. Идея Т. Бернерс-Ли заключалась в том, чтобы применить гипертекстовую модель к информационным ресурсам, распределенным в сети, и сделать это максимально простым способом. Он заложил три краеугольных камня системы из четырех существующих ныне, разработав:

язык гипертекстовой разметки документов HTML (HyperText Markup Lan-guage);

• универсальный способ адресации ресурсов в сети URL (Universal Resource Locator);

• протокол обмена гипертекстовой информацией HTTP (HyperText Transfer Protocol).

Позже команда NCSA добавила к этим трем компонентам четвертый:

• универсальный интерфейс шлюзов CGI (Common Gateway Interface).

Идея HTML—пример чрезвычайно удачного решения проблемы построения гипертекстовой системы при помощи специального средства управления отображением. На разработку языка гипертекстовой разметки существенное влияние оказали два фактора: исследования в области интерфейсов гипертекстовых систем и желание обеспечить простой и быстрый способ создания гипертекстовой базы данных, распределенной на сети.

В 1989 году активно обсуждалась проблема интерфейса гипертекстовых систем, т.е. способов отображения гипертекстовой

информации и навигации в гипертекстовой сети. Значение гипертекстовой технологии сравнивали со значением книгопечатания. Утверждалось, что лист бумаги и компьютерные средства отображения/воспроизведения серьезно отличаются друг от друга, и поэтому форма представления информации тоже должна отличаться. Наиболее эффективной формой организации гипертекста были признаны контекстные гипертекстовые ссылки, а кроме того было признано деление на ссылки, ассоциированные со всем документом в целом и отдельными его частями.

Самым простым способом создания любого документа является его набивка в текстовом редакторе. Опыт создания хорошо размеченных для последующего отображения документов в CERN_е был - трудно найти физика, который не пользовался бы системой TeX или LaTeX. Кроме того к тому времени существовал стандарт языка разметки—Standard Generalised Markup Language (SGML).

Следует также принять во внимание, что согласно своим предложениям Бернерс-Ли предполагал объединить в единую систему имеющиеся информационные ресурсы CERN, и первыми демонстрационными системами должны были стать системы для NeXT и VAX/VMS.

Обычно гипертекстовые системы имеют специальные программные средства построения гипертекстовых связей. Сами гипертекстовые ссылки хранятся в специальных форматах или даже составляют специальные файлы. Такой подход хорош для локальной системы, но не для распределенной на множестве различных компьютерных платформ. В HTML гипертекстовые ссылки встроены в тело документа и хранятся как его часть. Часто в системах применяют специальные форматы хранения данных для повышения эффективности доступа. В WWW документы—это обычные ASCII- файлы, которые можно подготовить в любом текстовом редакторе. Таким образом,

проблема создания гипертекстовой базы данных была решена чрезвычайно просто.

В качестве базы для разработки языка гипертекстовой разметки был выбран SGML (Standard Generalised Markup Language). Следуя академическим традициям, Бернерс-Ли описал HTML в терминах SGML (как описывают язык программирования в терминах формы Бекуса-Наура). Естественно, что в HTML были реализованы все разметки, связанные с выделением параграфов, шрифтов, стилей и т. п., т.к. реализация для NeXT подразумевала графический интерфейс. Важным компонентом языка стало описание встроенных и ассоциированных гипертекстовых ссылок, встроенной графики и обеспечение возможности поиска по ключевым словам.

С момента разработки первой версии языка (HTML 1.0) прошло уже пять лет. За это время произошло довольно серьезное развитие языка. Почти вдвое увеличилось число элементов разметки, оформление документов все больше приближается к оформлению качественных печатных изданий, развиваются средства описания не текстовых информационных ресурсов и способы взаимодействия с прикладным программным обеспечением. Совершенствуется механизм разработки типовых стилей. Фактически, в настоящее время HTML развивается в сторону создания стандартного языка разработки интерфейсов как локальных, так и распределенных систем.

Вторым краеугольным камнем WWW стала универсальная форма адресации информационных ресурсов. Universal Resource Identification (URI) представляет собой довольно стройную систему, учитывающую опыт адресации и идентификации e-mail, Gopher, WAIS, telnet, ftp и т. п. Но реально из всего, что описано в URI, для организации баз данных в WWW требуется только Universal Resource Locator (URL). Без наличия этой спецификации вся мощь HTML оказалась бы бесполезной. URL используется в гипертекстовых ссылках и обеспечивает доступ к распределенным

ресурсам сети. В URL можно адресовать как другие гипертекстовые документы формата HTML, так и ресурсы e-mail, telnet, ftp, Gopher, WAIS, например. Различные интерфейсные программы по разному осуществляют доступ к этим ресурсам. Одни, как например Netscape, сами способны поддерживать взаимодействие по протоколам, отличным от протокола HTTP, базового для WWW, другие, как например Chimera, вызывают для этой цели внешние программы. Однако, даже в первом случае, базовой формой представления отображаемой информации является HTML, а ссылки на другие ресурсы имеют форму URL. Следует отметить, что программы обработки электронной почты в формате MIME также имеют возможность отображать документы, представленные в формате HTML. Для этой цели в MIME зарезервирован тип “text/html”.

Третьим в нашем списке стоит протокол обмена данными в World Wide Web -HyperText Transfer Protocol. Данный протокол предназначен для обмена гипертекстовыми документами и учитывает специфику такого обмена. Так в процессе взаимодействия, клиент может получить новый адрес ресурса на сети (relocation), запросить встроенную графику, принять и передать параметры и т. п. Управление в HTTP реализовано в виде ASCII-команд. Реально разработчик гипертекстовой базы данных сталкивается с элементами протокола только при использовании внешних расчетных программ или при доступе к внешним относительно WWW информационным ресурсам, например базам данных.

Последняя составляющая технологии WWW - это уже плод работы группы NCSA -- спецификация Common Gateway Interface. CGI была специально разработана для расширения возможностей WWW за счет подключения всевозможного внешнего программного обеспечения. Такой подход логично продолжал принцип публичности и простоты разработки и наращивания возможностей WWW. Если команда CERN предложила простой и быстрый способ разработки баз данных, то NCSA развила этот

принцип на разработку программных средств. Надо заметить, что в общедоступной библиотеке CERN были модули, позволяющие программистам подключать свои программы к серверу HTTP, но это требовало использования этой библиотеки. Предложенный и описанный в CGI способ подключения не требовал дополнительных библиотек и буквально ошеломлял своей простотой. Сервер взаимодействовал с программами через стандартные потоки ввода/вывода, что упрощает программирование до предела. При реализации CGI чрезвычайно важное место заняли методы доступа, описанные в HTTP. И хотя реально используются только два из них (GET и POST), опыт развития HTML показывает, что сообщество WWW ждет развития и CGI по мере усложнения задач, в которых будет использоваться WWW-технология.

ЗАКЛЮЧЕНИЕ

Сети ЭВМ врываются в жизнь людей как в профессиональную деятельность, так и в быт - самым неожиданным и массовым образом. знания о сетях и навыки работы в них становятся необходимыми множеству людей. Использование самых современных компьютерных технологий приносит фирмам прибыли и помогает им победить в конкурентной борьбе. Совершенно очевидна роль сетевых технологий.

Сети ЭВМ породили существенно новые технологии обработки информации - сетевые технологии. В простейшем случае сетевые технологии позволяют совместно использовать ресурсы - накопители большой емкости, печатающие устройства, доступ в Internet, базы и банки данных. Наиболее современные и перспективные подходы к сетям связаны с использованием коллективного разделения труда при совместной работе с информацией - разработке различных документов и проектов, управлении учреждением или предприятием и т.д. Компьютерные сети и сетевые технологии обработки информации стали основой для построения современных информационных систем. Компьютер ныне следует рассматривать не как отдельное устройство обработки, а как «окно» в компьютерные сети, средство коммуникаций с сетевыми ресурсами и другими пользователями сетей.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1.Закирова Ф. и др. Информатика и информационные технологии. Т.: Изд-во «Aloqachi», 2007, 176 с.

2.Фаронов В.В. Турбо Paskalь 7.0. Начальный курс. Учебное пособие. М.: «Ноллидж», 1999. – 580 с.

3.Савченко Н.А. Информатика и информационные технологии. (http://www.humanities.edu.ru/db/msg/)

4.http:// ictcouncil.gov.uz

5.http://searchengine.narod.ru/archiv/se_2_250500.htm-Дидактические материалы по информатике.

6. https://ru.wikipedia.org/wiki/