**5 неделя**

**Лекция 9-10** Надежность передачи информации в Интернет. Система доменных имен. DNS – сервер.

Общение с Интернетом приносит не только пользу и удовольствие. Даже опытного пользователя подстерегает немало опасностей, способных отнять у него и нервы и время, а часто и деньги. Компьютерные злоумышленники используют Интернет для похищения информации, извлечения незаконной прибыли, причинения вреда конкурентам. Огромный вред приносит деструктивная, подчас совершенно бессмысленная деятельность хакеров и прочих сетевых хулиганов.

Самая большая напасть Интернета – компьютерные вирусы. Это программы, способные самостоятельно размножаться путем заражения других программ, то есть включения в них своего кода. Вирус может уничтожать или изменять информацию на зараженном компьютере, мешать работе. Так называемые сетевые черви создают и рассылают по сети свои бесчисленные копии, засоряя и перегружая линии связи, что иногда просто парализует работу сети.

Особой разновидностью вирусов являются троянские кони (трояны). Попадая в компьютер, они маскируют себя под безобидные программы. В определенные моменты трояны активизируются и начинают вредоносную работу – перехватывают пароли и коды доступа, пересылают информацию своему хозяину, постоянно выводят на экран рекламные сообщения и тому подобное.

Интернет представляет собой благодатную среду для распространения вирусов. Всего за несколько часов вирусная эпидемия может охватить весь земной шар, заразив миллионы компьютеров и причинив огромный ущерб.

Большую опасность прежде всего для серверов Интернета представляют хакерские атаки. Хакеры (hacker – взломщик) стремятся взломать защиту компьютера, используя слабые места операционной системы, или организуя огромное число запросов, которые сервер не в состоянии обработать.

Целью хакера является получение контроля над компьютером, похищение секретной информации, прекращение работы какого-либо сайта или порча информации на нем. Часто компьютеры взламывают из спортивного интереса или для демонстрации своего мастерства. Иногда остепенившиеся хакеры получают хорошую работу в отделах компьютерной безопасности.

Методы защиты от вирусов постоянно совершенствуются, хотя пессимисты предрекают гибель Интернета именно от расплодившихся в нем «сетевых червей» нового поколения, вышедших из под контроля создателей и захвативших власть в Сети.

Немало неприятностей пользователю приносит спам – навязчивая реклама, забивающая почтовые ящики. Спам (SPAM – фирменное название усиленно рекламировавшихся мясных консервов из некогда популярного кинофильма) представляет собой массовую рассылку по электронной почте рекламных объявлений разного характера. Списки почтовых адресов добываются всеми возможными способами, продаются, покупаются, похищаются. Существуют фирмы, целиком специализирующиеся на спамерской деятельности.

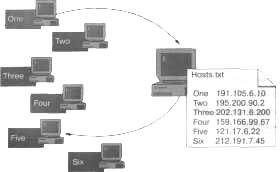
Каждый провайдер услуг электронной почты организует более-менее эффективную антиспамерскую защиту с помощью почтовых фильтров. По ряду признаков рекламные письма опознаются и помещаются в особую папку.

Неискушенный пользователь может попасться на крючок виртуальных мошенников, которые организуют в Интернете многочисленные пирамиды, лотереи, липовые магазины и распродажи.

Интернет предоставляет большую свободу распространения информации, но не все пользуются этой свободой должным образом. К числу проблем современного Интернета следует отнести нарушения авторских прав и распространение порнографии.

Доменная система имен (Domain Name System, DNS) похожа на телефонную книгу. При использовании DNS компьютер обращается к другому компьютеру по имени, а сервер имен домена преобразует имя в IP-адрес. На этом занятии Вы узнаете об архитектуре и структуре DNS.

До 1980 года сеть ARPANET состояла лишь из нескольких сотен компьютеров. Все соответствия имен и адресов компьютеров хранились в одном файле с именем Hosts.txt. Этот файл находился на компьютере центра Stanford Research Institute's Network Information Center (SRI-NIC) в Менло-Парк, штат Калифорния. Как показано на иллюстрации, остальные компьютеры сети ARPANET по мере надобности копировали из SRI-NIC файл Hosts.txt на свои узлы.



### FTP Five

Поначалу эта схема работала достаточно хорошо, поскольку файл Hosts.txt необходимо было обновлять один или два раза в неделю. Однако через несколько лет, когда сеть ARPANET заметно выросла, возникли проблемы:

* файл Hosts.txt стал очень большим;
* приходилось обновлять файл несколько раз в день;
* поскольку весь сетевой трафик маршрутизировался через SRI-NIC, то поддержка файла Hosts.txt стала камнем преткновения для всей сети;
* сетевой трафик через SRI-NIC стал почти неуправляемым;
* в Hosts.txt использовалось одноуровневое (flat) пространство имен, поэтому имя каждого компьютера в сети должно было быть уникальным.

Эти и другие проблемы заставили управление ARPANET искать другие способы распространения файла Hosts.txt. В результате была создана доменная система имен — DNS — распределенная база данных, использующая иерархическое (hierarchical) пространство имен.

*Примечание* Доменная система имен описана в документах RFC 1034 и 1035. Копии этих документов Вы найдете на Web-странице Course Materials прилагаемого к курсу компакт-диска.

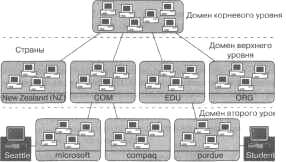
### Как работает DNS

В работе DNS участвуют три основных компонента: клиенты DNS, или программы разрешения имен (resolvers), серверы имен и пространство имен домена.

В простейшем случае DNS-клиент посылает запросы серверу имен. Сервер возвращает либо требуемую информацию, либо указание на другой сервер имен, либо сообщение об отказе, если запрос не может быть удовлетворен.

Доменная система имен — это система управления иерархической распределенной базой данных, использующая технологию клиент-сервер. DNS работает на прикладном уровне (application layer) и использует UDP и TCP/IP как нижележащие протоколы.

Задача базы данных DNS — транслировать имена компьютеров в IP-адреса, что показано на следующей иллюстрации. DNS-клиентов часто называют ресолверами (resolvers), серверы — серверами имен (name servers).



Доменная система имен похожа на телефонную книгу. Пользователь находит имя человека или название организации, с которой хочет связаться, — рядом указан телефонный номер. Аналогично, компьютер обращается к DNS, используя имя другого компьютера или домена, а сервер имен выдает соответствующий этому имени IP-адрес.

Сначала DNS-клиенты посылают серверам запросы по протоколу UDP (для повышения производительности), а переключаются на использование TCP только при потере информации.

### DNS-клиенты

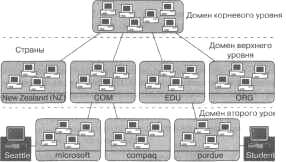
DNS-клиенты пересылают сообщения между приложениями и серверами имен. Сообщение содержит запрос, например IP-адрес Web-узла. Часто DNS-клиент встроен в приложение или работает на компьютере как библиотечная подпрограмма.

### Серверы имен

Серверы имен принимают сообщения от DNS-клиентов и преобразуют имена компьютеров (или доменов) в IP-адреса. Если сервер имен не в состоянии сам сделать это, то он может перенаправить запрос к серверу имен, который сможет разрешить его. Серверы имен сгруппированы по разным уровням — доменам (domains).

### Пространство имен домена

Это иерархически упорядоченная структура имен, напоминающая перевернутое дерево.



### Домены корневого уровня

Домены определяют различные уровни в иерархии. На самом верху — находится корневой домен (root domain). Он использует пустую метку (null lable), но ссылки на корневой домен можно задавать точкой (.).

### Домены верхнего уровня

*Вот список доменов верхнего уровня (top-level domains)\*:*

* com — коммерческие организации;
* edu — образовательные учреждения и университеты;
* org — некоммерческие организации;
* net — сети (крупные сети, входящие в Internet);
* gov — невоенные правительственные учреждения;
* mil — военные правительственные учреждения;
* num — телефонные номера;
* агра — обратный (reverse) DNS;
* хх — двухбуквенные обозначения стран.

В домены верхнего уровня могут входить узлы и домены второго уровня.

*Примечание* Комитет Сообщества Интернета (Internet Society committee) планирует ввести еще несколько доменов верхнего уровня, например .firm и .web.

### Домены второго уровня

В домены второго уровня входят узлы и другие домены, называемые поддоменами (subdomains). Так, в домен фирмы Microsoft microsoft.com включены как отдельные   
*\* В настоящее время список доменов верхнего уровня расширяется. — Прим. перев.*

компьютеры, HanpviMepftp.microsoft.com, так и поддомены, например dev.microsoft.com. В последние также могут входить узлы, например ntserver.dev.microsoft.com.

### Имена узлов

Имена узлов обычно справа дополняются именем домена. Такая запись называется полностью определенным доменным именем (fully qualified domain name, FQDN). Например, узел flleserver в домене microsoft.com будет иметь FQDN-имя вида file-server, т icrosoft. com.

### Зоны ответственности

Зона ответственности (zone of authority) — это часть пространства имен домена, за которую отвечает конкретный сервер имен. Сервер имен хранит IP-адреса для всех имен из зоны его ответственности и обслуживает все запросы клиентов к этим именам.

Зона ответственности сервера имен охватывает, как минимум, один домен, который называют корневым доменом зоны (zone root domain). Зона ответственности может включать и поддомены корневого домена этой зоны. Однако в одну зону не обязательно входят все поддомены, расположенные ниже корневого домена этой зоны.

На приведенной далее иллюстрации домен microsoft.com не укладывается в одной зоне. Часть домена выделена в отдельную зону dev.microsoft.com. Разбиение домена на несколько зон необходимо для раздельного управления группами в домене или для эффективного тиражирования данных.

Один DNS-сервер может управлять несколькими зонами. Каждая зона подчинена конкретному домену, который называют корневым доменом зоны.



### Роли DNS-серверов

DNS-серверы могут выполнять разные задачи. Они могут хранить и поддерживать свои базы данных различными способами. Далее описаны разные способы хранения данных своей зоны.

### Основной сервер имен

Основной сервер имен извлекает информацию из локальных файлов. Изменения в параметрах зоны, например добавление узла или домена, выполняются на основном сервере имен.

### Резервный сервер имен

Резервный сервер имен получает информацию о своей зоне от других серверов, которые ответственны за данную зону. Такой способ получения информации через сеть называют зонной передачей (zone transfer).

Существует три основные причины, по которым следует создавать резервные серверы имен.

 Избыточность — Вам необходимы, как минимум, один основной и один резерв- ный сервер имен на каждую зону. Компьютеры должны быть как можно более независимы.

 Ускоренный доступ для удаленных клиентов — если у Вас есть несколько удален- ных клиентов, то наличие резервных серверов имен (или других основных серверов имен в поддоменах) освободит их от использования низкоскоростных линий при распознавании имен.

 Снижение нагрузки — резервные серверы имен уменьшают загруженность основ- ных серверов.

Поскольку информация о разных зонах хранится в разных файлах, то разделение серверов на основные и резервные значимо только в пределах зоны. Другими словами, данный DNS-сервер может быть основным по отношению к одной зоне и резервным по отношению к другой.

### Главный сервер имен

При определении DNS-сервера на роль резервного сервера имен в данной зоне Вы должны указать DNS-сервер, от которого будет поступать зонная информация. Источник такой информации для резервного сервера имен в иерархии DNS называют главным сервером имен (master name server). Главный сервер имен может быть как основным, так и резервным DNS-сервером в своей зоне. При запуске резервный DNS-сервер связывается со своим главным сервером имен и запрашивает зонную передачу.

### Котирующий DNS-сервер

Все DNS-серверы кэшируют запросы, на которые они отвечают. Каптирующие — это DNS-серверы, которые только перенаправляют запросы, кэшируют ответы и возвращают результаты. Другими словами, они не отвечают ни за какие домены (на них информация о зонах не хранится), а содержат лишь информацию, которая попала в > кэш из ответов на запросы.

Обдумывая целесообразность использования такого DNS-сервера в Вашей организации, обратите внимание на то, что при начальном запуске кэш не содержит информации — она накапливается при обслуживании запросов. При этом отсутствует зональная передача и сильно снижается объем сетевого трафика. Это важно, если Вы работаете с низкоскоростными линиями связи.