Методы атак

Владимир Борисович Лебедев

ТТИ ЮФУ

Программа

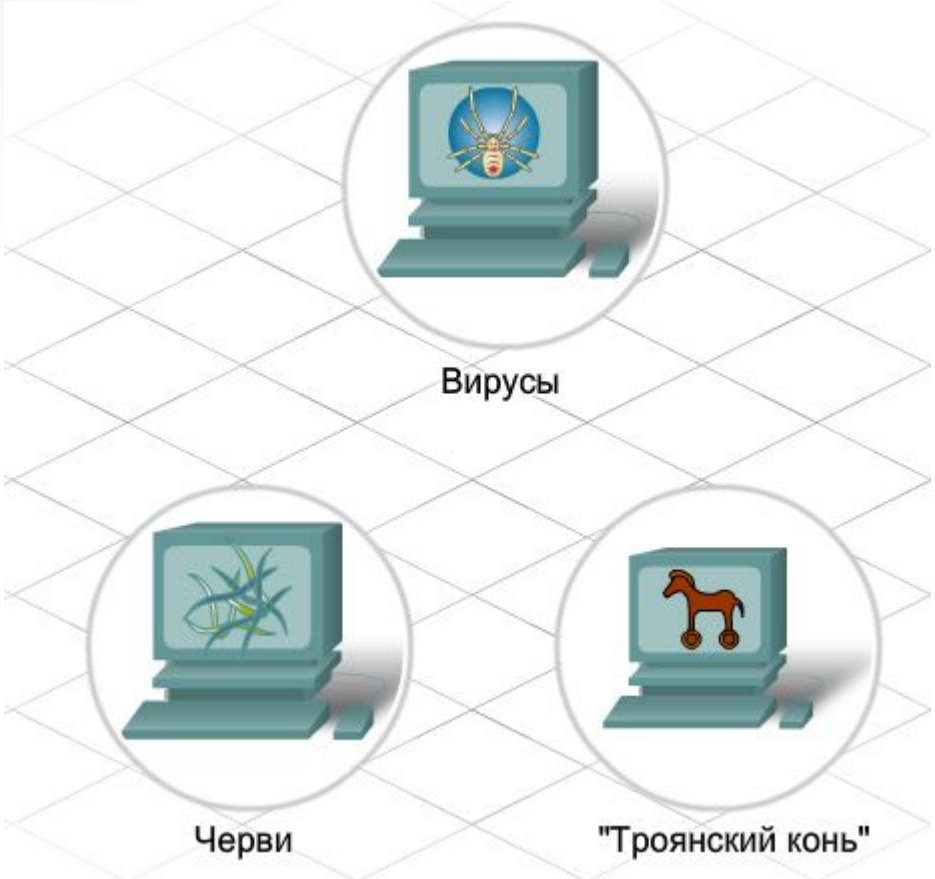
- Вирусы, черви и "троянские кони"
- Отказ в обслуживании и атаки методом грубой силы
- Шпионское ПО, сеансовые идентификаторы, рекламное ПО и всплывающие окна
- Спам

Вирусы, черви и "троянские кони"

Социотехника – распространенный фактор опасности, предполагающий эксплуатацию психологических слабостей для получения требуемых результатов.

Помимо социотехники существуют и другие виды атак, которые направлены уже на уязвимости в компьютерном ПО. К ним относятся вирусы, черви и "троянские кони". Их общим свойством является проникновение вредоносного ПО на узел. Вредоносное ПО может вывести из строя систему, уничтожить данные и нарушить доступ к сетям, системам и сервисам. Кроме того, незаметно для пользователей оно может привести к попаданию важной информации и личных данных в руки преступников. Во многих случаях вредоносные программы самопроизвольно распространяются по другим узлам сети.

Иногда эти технологии используются параллельно с социотехникой: неподозревающим пользователем манипулируют так, что он становится инициатором атаки.



Вирусы, черви и "троянские кони"

Вирусы

Вирус – программа, которая функционирует и распространяется путем изменения других программ и файлов. Вирус не запускается сам – он должен быть активирован. После активации действия вируса могут ограничиться простым размножением и распространением. Даже такие вирусы при всей своей простоте опасны, поскольку они способны быстро заполнить всю свободную память и остановить работу системы. Более серьезные вирусы могут быть запрограммированы на удаление или повреждение конкретных файлов перед дальнейшим распространением. Вирусы могут распространяться через вложения в электронной почте, загружаемые из Интернета файлы, системы мгновенного обмена сообщениями, а также через дискеты, компакт-диски и USB-устройства

Черви

Червь аналогичен вирусу, но, в отличие от вируса, он не присоединяется к существующей программе. Червь рассылает копии самого себя по сети на все подключенные узлы. Черви могут функционировать независимо и интенсивно распространяться. Для их работы не требуется ни активация, ни вмешательство человека. Ущерб от саморазмножающихся сетевых червей может значительно превышать последствия одного вируса. Черви способны быстро поражать значительную часть Интернета.

"Троянские кони”

"Троянским конем" называют неразмножающуюся программу, представляющую собой инструмент для атаки, замаскированный под некоторую легитимную программу. Успешное выполнение троянского коня зависит от успешности его маскировки под программу, которую пользователь согласится запустить. Троянские кони могут быть сравнительно безвредными или могут содержать код, способный повредить файлы на жестком диске пользователя. Некоторые "троянские кони" также открывают "черный ход" в систему для хакера.

Отказ в обслуживании и атаки методом грубой силы

В некоторых случаях злоумышленник заинтересован воспрепятствовать нормальному функционированию сети. Этот вид атак обычно выполняется с целью нарушить работу организации.

Отказ в обслуживании (DoS)-атаки

DoS-атаки представляют собой агрессивные атаки с отдельных компьютеров или групп компьютеров, препятствующие обслуживанию легитимных пользователей. DoS-атаки могут быть нацелены на пользовательские системы, серверы, маршрутизаторы и сетевые соединения.

Обычно DoS-атаки предполагают следующие вредоносные действия:
заполнение системы или сети посторонним трафиком, блокирующим доставку легитимного трафика;
нарушение соединения клиента с сервером для предотвращения доступа к сервису.

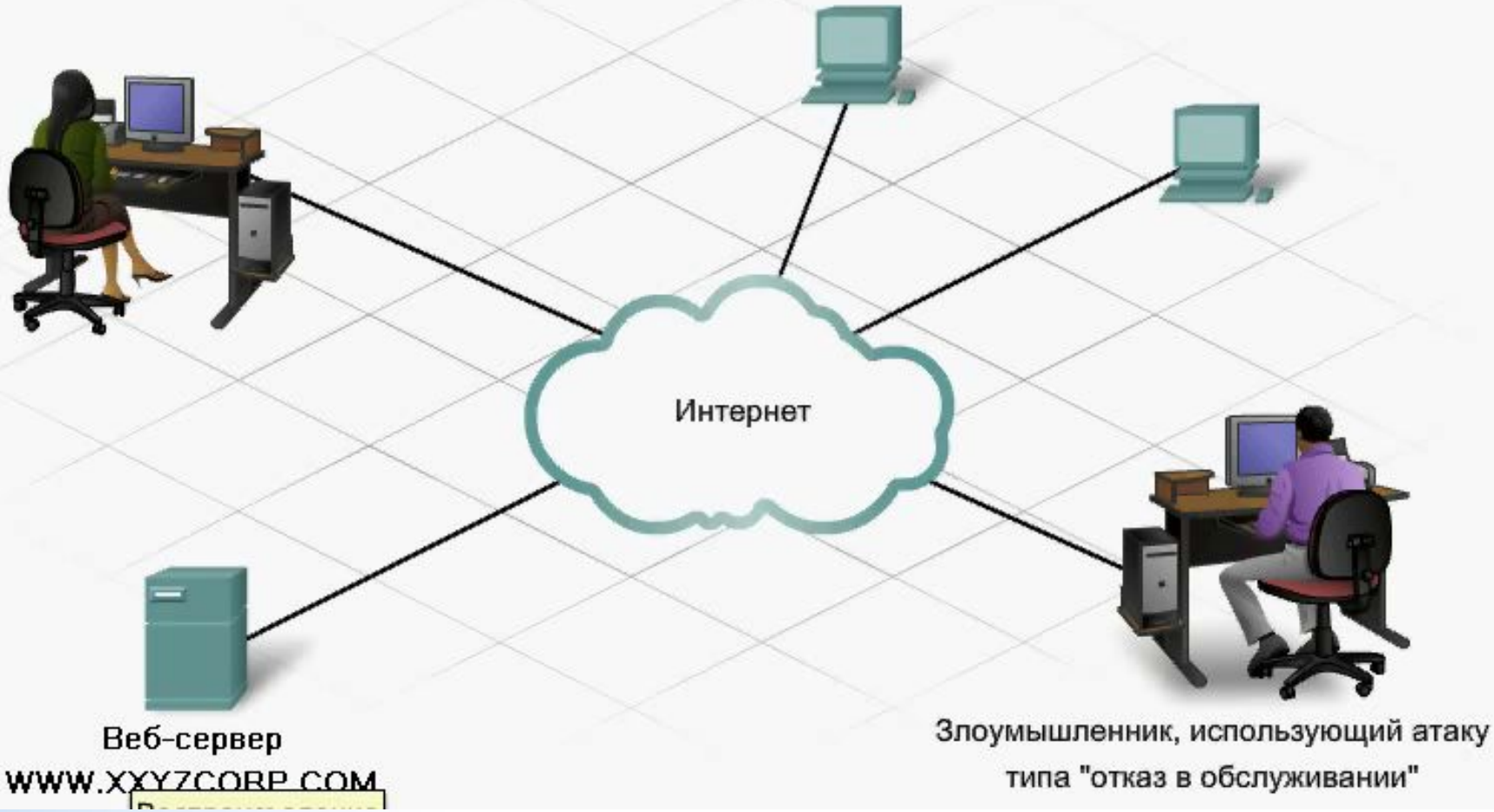
DoS-атаки подразделяются на несколько видов. Администраторы, отвечающие за вопросы безопасности, должны знать о видах DoS-атак, которые угрожают их сетям, и обеспечить защиту сетей. Два наиболее распространенных вида DoS-атак:

Насыщение пакетами синхронизации (SYN Flood) – к серверу направляется поток пакетов от клиента, запрашивающего установление соединения. Пакеты содержат неверные IP-адреса источников. Сервер, занятый обработкой этих фиктивных запросов, теряет способность обрабатывать легитимные запросы.

Деструктивный эхо-запрос (Ping of Death) – устройству направляется пакет эхо-запроса, размер которого превышает максимум, предусмотренный протоколом IP (65 535 байт), что может привести к сбою системы-приемника.

Тип атаки «Отказ в обслуживании»

mov



Отказ в обслуживании и атаки методом грубой силы

Распределенная DoS-атака (DDoS)

DDoS представляет собой развитие DoS-атаки со значительно большим вредоносным потенциалом. Цель состоит в насыщении и переполнении сетевых каналов бесполезными данными, но DDoS действует в гораздо большем масштабе, чем простые DoS-атаки. Жертва обычно становится получателем громадного потока трафика от сотен тысяч источников атаки. Источниками могут быть компьютеры неподозревающих пользователей, на которые ранее проникло вредоносное ПО, открывающее DDoS-атаку на целевой сайт после получения определенного сигнала.

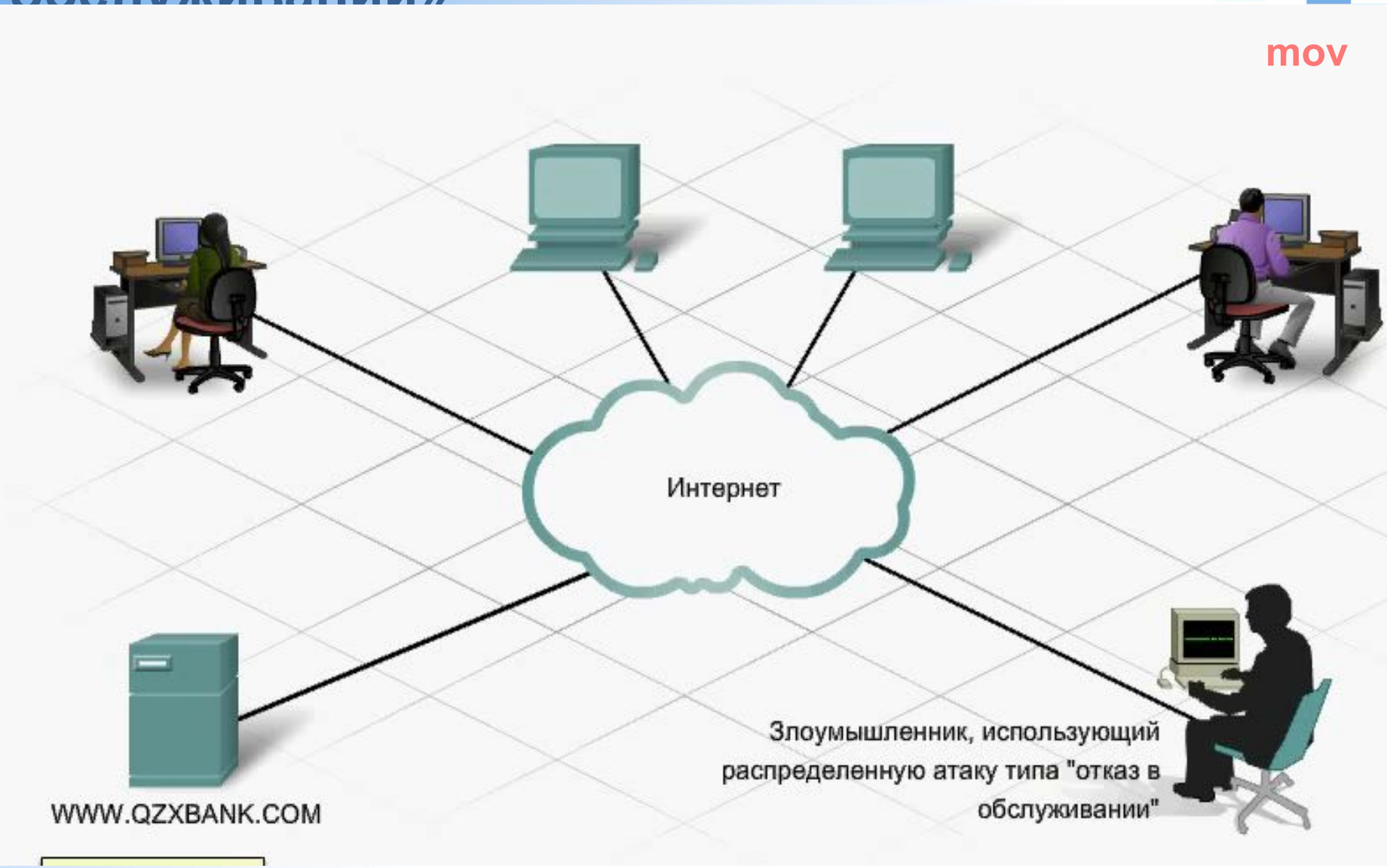
Атаки методом грубой силы

Не все атаки, приводящие к нарушению работы сети, относятся к категории DoS. Атака методом грубой силы – другой распространенный вид атак, часто приводящий к отказу в обслуживании.

В атаках методом грубой силы используется быстродействующий компьютер для подбора паролей или дешифровки. Злоумышленник активно перебирает большое число возможных вариантов для получения доступа или извлечения ключа шифрования. Атаки методом грубой силы могут стать причиной отказа обслуживания в результате перенасыщения трафиком определенного ресурса или блокирования учетной записи пользователя.

Распределенная атака «Отказ в обслуживании»

mov



Шпионское ПО, сеансовые идентификаторы

Не все атаки ведут к ущербу или лишению легитимных пользователей доступа к ресурсам. Многие угрозы связаны со сбором сведений о пользователях, которые в дальнейшем могут использоваться для рекламы, маркетинга и анализа. Источниками таких угроз являются шпионское ПО, сеансовые идентификаторы (cookies), рекламное ПО и всплывающие окна. Не приводя к непосредственным сбоям в работе компьютера, они вторгаются в личные данные пользователя и могут раздражать своей работой.

Шпионское ПО

Шпионское ПО – программы, собирающие личные данные с компьютера пользователя без его ведома. Эти данные поступают в распоряжение рекламных агентств или других пользователей Интернета. В их числе могут оказаться пароли и банковские реквизиты.

Шпионское ПО обычно устанавливается незаметно для пользователя при загрузке файла, установке другой программы или щелчке мышью во всплывающем окне. Оно может замедлить работу компьютера и изменить внутренние параметры настройки, сделав систему более уязвимой для других угроз. Кроме того, при удалении шпионского ПО часто возникают сложности.

Сеансовые идентификаторы

Сеансовые идентификаторы (cookie) считаются одним из видов **шпионского ПО**, но не всегда являются вредоносными. Они фиксируют информацию о посещении сайтов определенным пользователем Интернета. Сеансовые идентификаторы могут быть полезны для персонализации настроек и других применений, экономящих время. Многие веб-сайты при подключении пользователя требуют, чтобы сеансовые идентификаторы были разрешены.

Шпионское ПО, сеансовые идентификаторы

Рекламное ПО и всплывающие окна

Рекламное ПО

Рекламное ПО – вид шпионского ПО для сбора сведений о пользователях, посещающих веб-сайты. Собранные сведения в дальнейшем используются для целевой рекламы. Часто рекламное ПО попадает к пользователю вместе с "бесплатным" продуктом. Когда пользователь открывает окно браузера, рекламное ПО может запустить новые копии браузера с рекламой продуктов и услуг, отражающей интересы пользователя в Интернете. Нежелательные окна браузера могут открываться неоднократно и сильно затруднить работу в Интернете, особенно при низкоскоростном подключении. Удалить рекламное ПО из системы часто бывает сложно.

Всплывающие и фоновые окна

Всплывающие и фоновые окна – это дополнительные рекламные окна, которые появляются на экране при посещении веб-сайта. В отличие от рекламного ПО, всплывающие и фоновые окна не служат для сбора сведений о пользователе и обычно связаны только с конкретным просматриваемым веб-сайтом.
Всплывающие окна: открываются перед текущим окном браузера.
Фоновые окна: отрываются за текущим окном браузера.

Они могут раздражать и обычно рекламируют продукты и услуги, не представляющие интереса.

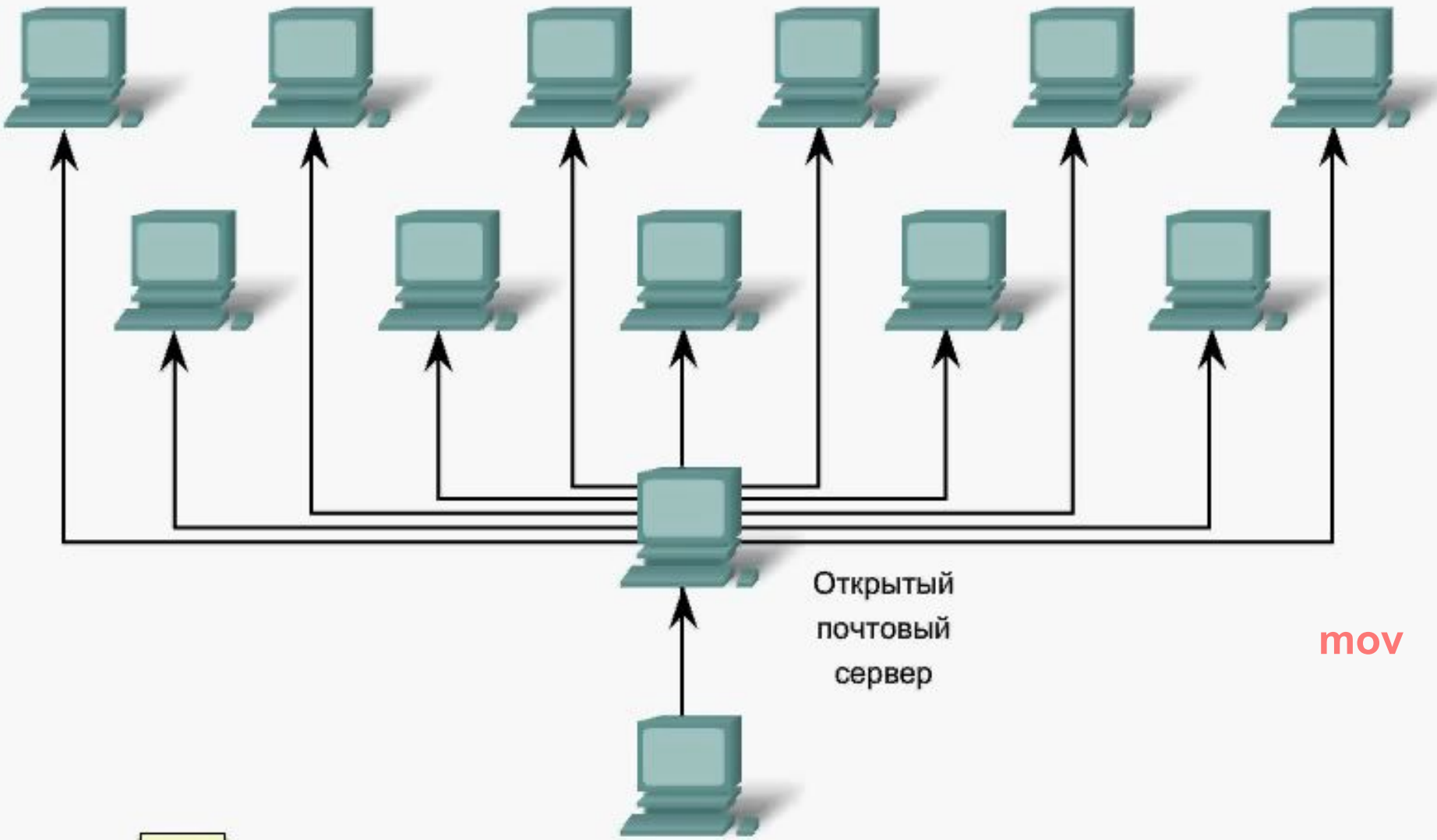
Спам

Рост значимости электронных коммуникаций сопровождается еще одним досаждающим явлением – несанкционированными массовыми рассылками по электронной почте. В некоторых случаях продавцы намеренно не прибегают к целевому маркетингу и стараются разослать рекламу товара или услуги по электронной почте максимальному числу получателей в расчете на то, что заинтересованный покупатель обязательно найдется. Этот широко распространенный подход к маркетингу в Интернете получил название спама.

Спам представляет собой существенную угрозу для сети и ведет к перегрузке Интернет-провайдеров, серверов электронной почты и отдельных пользовательских систем. Лица и организации, ведущие рассылку спама, называются спамерами. Для рассылки спамеры часто пользуются незащищенными серверами электронной почты. Спамеры могут взламывать домашние компьютеры посредством таких приемов, как вирусы, черви и троянские кони. После этого компьютеры начинают рассылать спам без ведома владельца. В последнее время помимо электронной почты спам стал распространяться посредством ПО для мгновенного обмена сообщениями.

В среднем каждый пользователь Интернета получает более 3 000 спам-сообщений за год. Спам нагружает Интернет-каналы и становится настолько серьезной проблемой, что во многих странах появились законы, регулирующие порядок проведения подобных рассылок.

Распространение спама



mov

Вопросы&Ответы

Методы атак