Сетевые черви
и защита от них

СЕТЕВЫЕ ЧЕРВИ

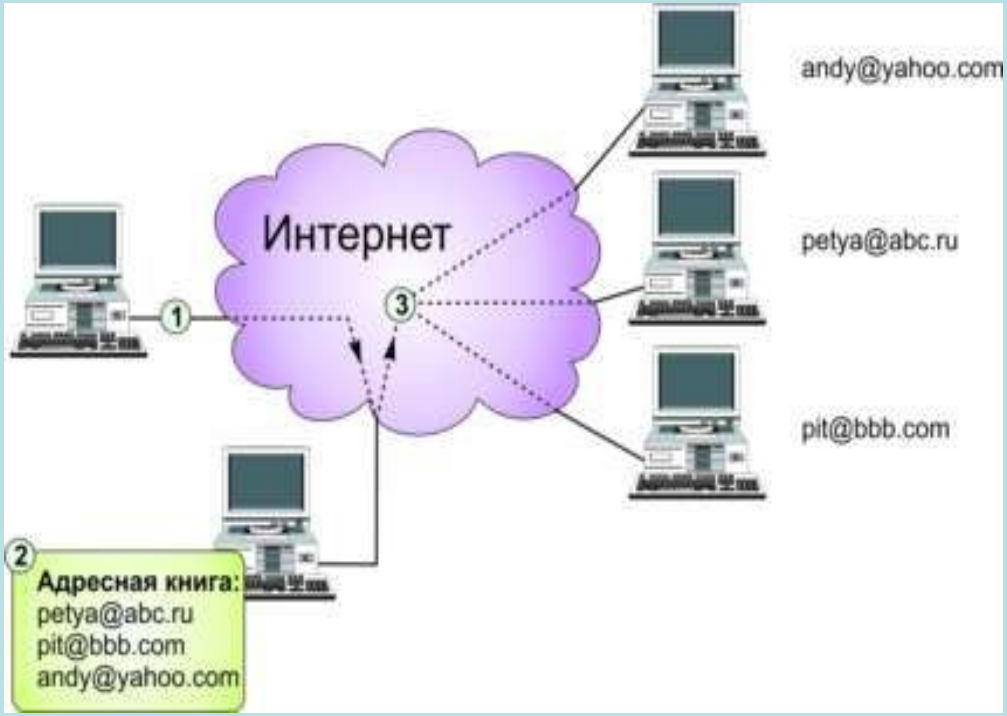
Сетевые черви - это вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей: Всемирную паутину, электронную почту, интерактивное общение, файлообменные сети и т.д.

Многие сетевые черви используют более одного способа распространения своих копий по компьютерам локальных и глобальных сетей.

Активация сетевого червя может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

ПОЧТОВЫЕ ЧЕРВИ

Почтовые черви для своего распространения используют электронную почту.



Червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе.

Код червя активируется при открытии (запуске) зараженного вложения или при открытии ссылки на зараженный файл.

Профилактическая защита от почтовых червей состоит в том, что не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников.

ЧЕРВИ, ИСПОЛЬЗУЮЩИЕ «УЯЗВИМОСТИ» ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Червь ищет в сети компьютеры, на которых используются операционная система и приложения, содержащие уязвимости.

Червь посылает на компьютер специально оформленный сетевой пакет или запрос, в результате чего код (или часть кода) червя проникает на компьютер-жертву.

Если сетевой пакет содержит только часть кода червя, он затем скачивает основной файл и запускает его на исполнение на зараженном компьютере.

Профилактическая защита от таких червей состоит в том, что рекомендуется своевременно скачивать из Интернета и устанавливать обновления системы безопасности операционной системы и приложений.

ЧЕРВИ, ИСПОЛЬЗУЮЩИЕ ФАЙЛООБМЕННЫЕ СЕТИ

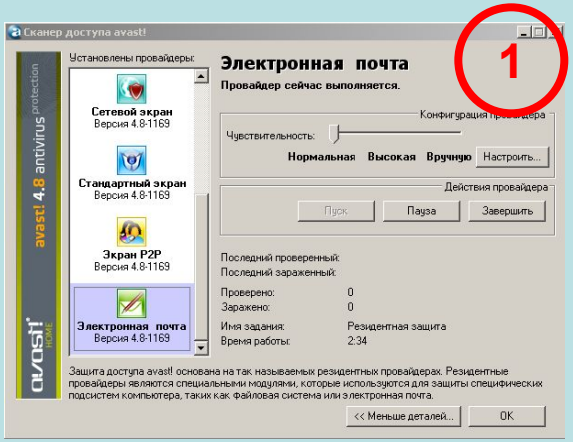
Для внедрения в файлообменную сеть червь копирует себя в папку обмена файлами на одном из компьютеров.

В 2001 году стал стремительно распространяться сетевой червь «Nimda», который атаковал компьютеры сразу несколькими способами: через сообщения электронной почты, через открытые ресурсы локальных сетей, а также используя уязвимости в системе безопасности операционной системы серверов Интернета.

Профилактическая защита от таких сетевых червей состоит в том, что рекомендуется своевременно скачивать из Интернета и обновлять антивирусную программу и вирусную базу данных.

Защита от сетевых червей

Задание. С помощью антивирусной программы avast! проверить компьютер на заражение сетевыми червями и при их обнаружении вылечить или удалить зараженные файлы.



1. *Настройка параметров антивирусного монитора (сканера доступа)*
2. *Запуск почтовой программы Outlook Express*
3. *Выбор дисков для сканирования*
4. *Проверка на вирусы выбранных дисков*