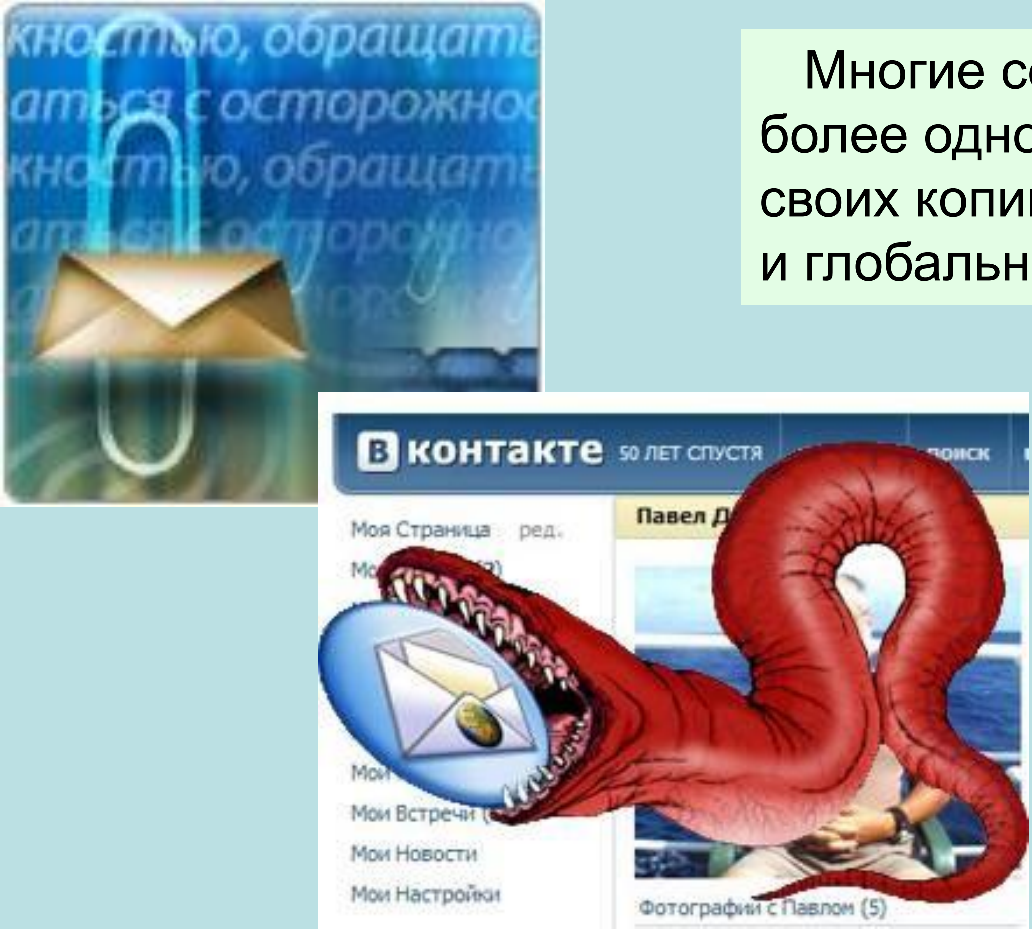
Сетевые черви и защита от них

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.

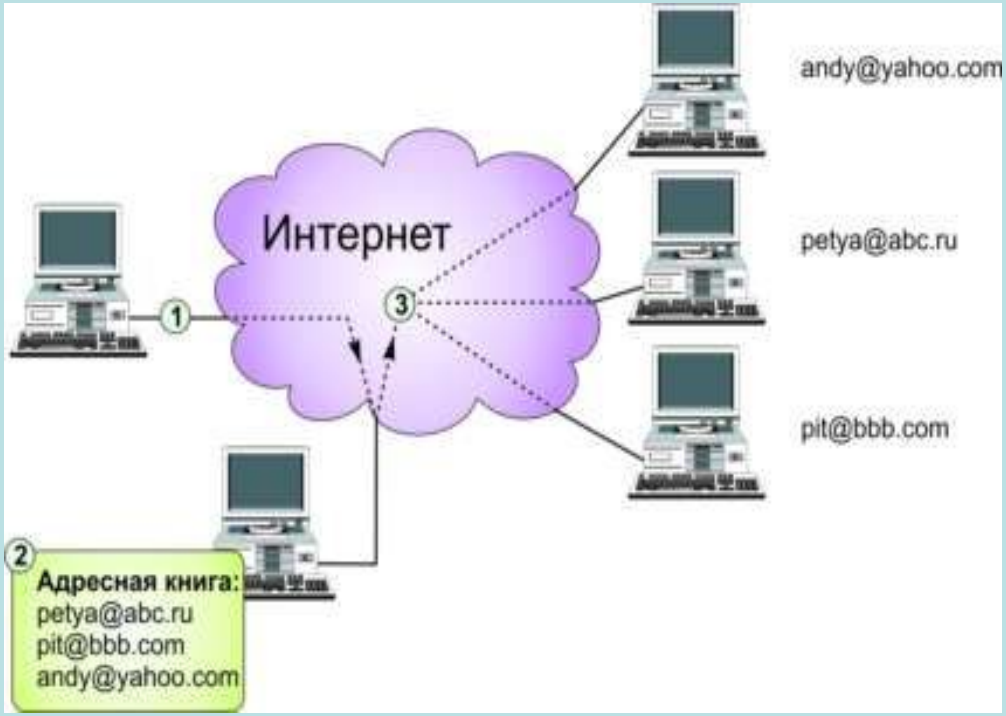


Многие сетевые черви используют более одного способа распространения своих копий по компьютерам локальных и глобальных сетей.

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.

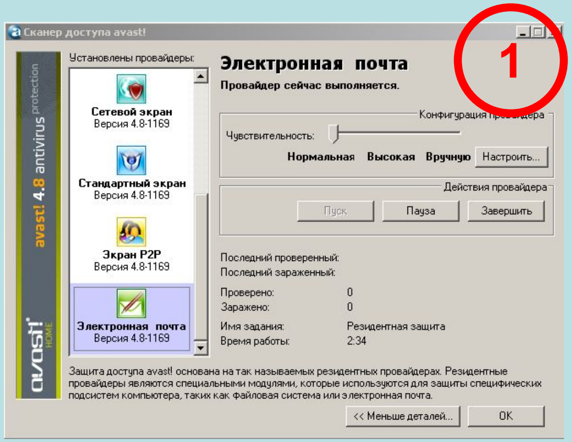
В 2001 году стал стремительно распространяться сетевой червь «Nimda», который атаковал компьютеры сразу несколькими способами: через сообщения электронной почты, через открытые ресурсы локальных сетей, а также используя уязвимости в системе безопасности операционной системы серверов Интернета.

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

КОМПЬЮТЕРНЫЙ ПРАКТИКУМ

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

Установлены провайдеры:

- Сетевой экран Версия 4.8-1169
- Стандартный экран Версия 4.8-1169
- Экран P2P Версия 4.8-1169
- Электронная почта Версия 4.8-1169

Электронная почта

Провайдер сейчас выполняется.

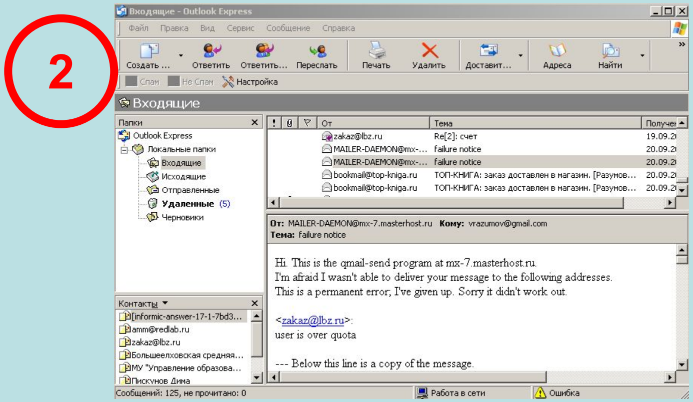
Конфигурация провайдера

Чувствительность: Нормальная Высокая Вручную

Последний проверенный:
Последний зараженный:
Проверено: 0
Заражено: 0
Имя задания: Резидентная защита
Время работы: 2:34

Защита доступа avast! основана на так называемых резидентных провайдерах. Резидентные провайдеры являются специальными модулями, которые используются для защиты специфических подсистем компьютера, таких как файловая система или электронная почта.

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


2

От	Тема	Получен
zakaz@lbz.ru	Re[2]: счет	19.09.2
MAILER-DAEMON@mx-...	failure notice	20.09.2
MAILER-DAEMON@mx-...	failure notice	20.09.2
bookmail@top-kniga.ru	ТОП-КНИГА: заказ доставлен в магазин. [Разумов...	20.09.2
bookmail@top-kniga.ru	ТОП-КНИГА: заказ доставлен в магазин. [Разумов...	20.09.2

От: MAILER-DAEMON@mx-7.masterhost.ru **Кому:** vrazumov@gmail.com
Тема: failure notice

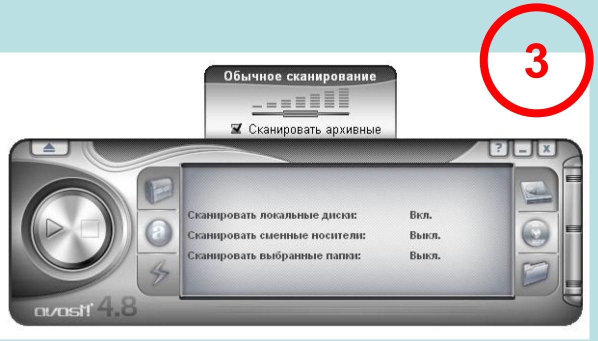
Hi. This is the qmail-send program at mx-7.masterhost.ru.
I'm afraid I wasn't able to deliver your message to the following addresses.
This is a permanent error; I've given up. Sorry it didn't work out.

<zakaz@lbz.ru>:
user is over quota

--- Below this line is a copy of the message.

[informic-answer-17-1-7bd3...
amm@redlab.ru
zakaz@lbz.ru
Большеелховская средняя...
МУ "Управление образова...
Пискунов Дима

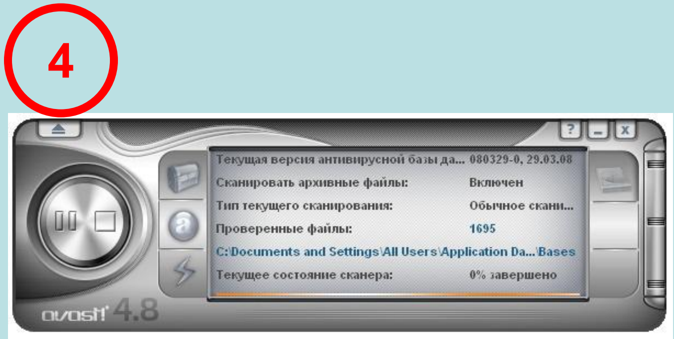
Сообщений: 125, не прочитано: 0 Работа в сети Ошибка


3

Обычное сканирование

☑ Сканировать архивные

Сканировать локальные диски: Вкл.
Сканировать сменные носители: Выкл.
Сканировать выбранные папки: Выкл.


4

Текущая версия антивирусной базы да... 080329-0, 29.03.08
Сканировать архивные файлы: Включен
Тип текущего сканирования: Обычное скани...
Проверенные файлы: 1695
C:\Documents and Settings\All Users\Application Da...\Bases
Текущее состояние сканера: 0% завершено