Компьютерные вирусы. Антивирусные программы

21 декабря 201

Фрэд Коэн

«Компьютерный вирус есть программа, способная заражать другие программы путем добавления в них собственной копии».

Компьютерные вирусы

это специально созданная небольшая программа, предназначенная для нарушений работы компьютера

Записываясь в системные области диска или приписываясь к файлам и производит различные нежелательные действия, которые, зачастую, ают катастрофические последствия.

Univac 1108

«Pervading Animal»

Первая программа, выполнявшая не те действия, которых ожидал от нее оператор, и пытающаяся создавать свои копии.

Elk Cloner 1981г.

распространяющийся на дискетах для Apple II

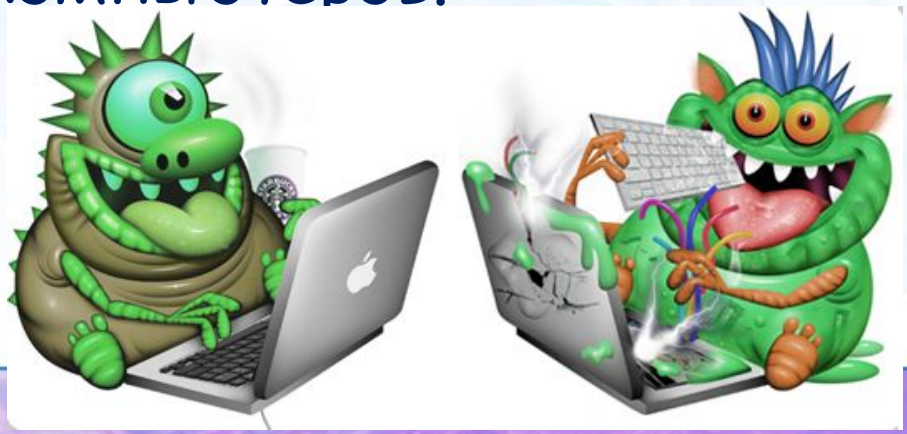
```
Elk Cloner:
The program with a personality

    It will get on all your disks
      It will infiltrate your chips
        Yes it's Cloner!

    It will stick to you like glue
      It will modify ram too
        Send in the Cloner!
```

Из истории создания вирусов

- **1959 год** - на ЭВМ IBM 650 обнаружен вирус, который «съедал» часть слов.
- Первая «эпидемия» компьютерного вируса произошла в **1986 году**, когда вирус по имени **Brain** (англ. «мозг») заражал дискеты персональных компьютеров
- **1988 год** - Роберт Моррис в США написал вирус, поразивший 2000 компьютеров.



История создания

1993 год - «PS-MPC» активность вирусов проявляется при активности пользователя.

1995 год – Выход Windows 95.

Вирус: «Concept»

В настоящее время известно более **50 тысяч** вирусов, заражающих компьютеры и распространяющихся по компьютерным сетям. К концу **1989 г.** в ряде стран (США, Великобритания, ФРГ) находятся на рассмотрении законы, предусматривающие для разработчиков компьютерных вирусов значительные сроки тюремного заключения. (В США до 15 лет).

Отличительные особенности компьютерных вирусов:

- Малый объем
- Самостоятельный запуск
- Многократное копирование
- Создание [illegible] работы

Масштаб вредных воздействий

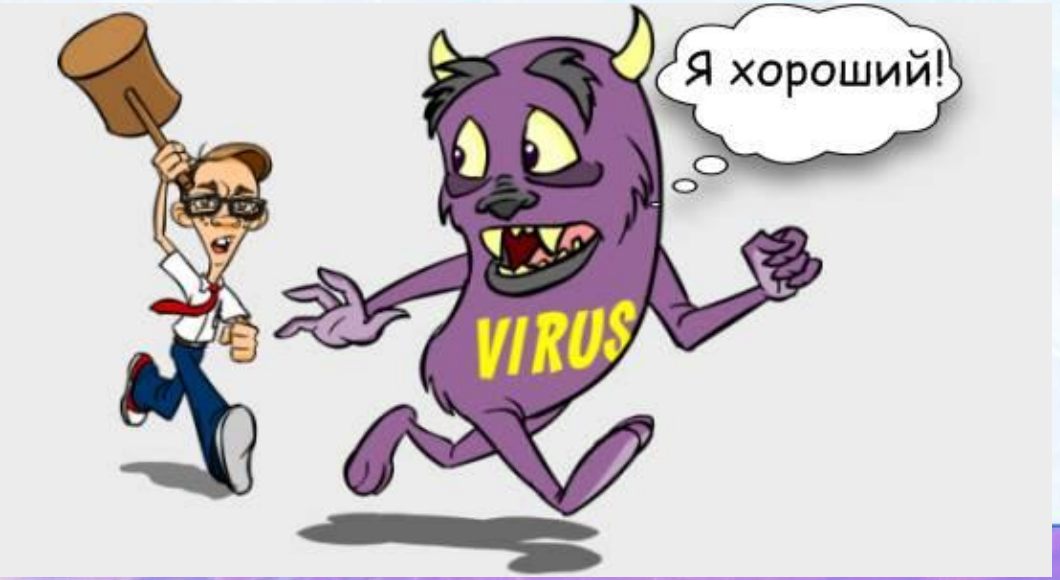
- Безвредные
- Неопасные
- Опасные
- Очень опасные

Признаки, указывающие на заражение компьютера вирусами

- Неправильная работа программ.
- Медленная работа компьютера.
- Невозможность загрузки операционной системы.
- Исчезновение файлов.
- Изменение даты, времени создания файла или его размера.
- Вывод на экран непредусмотренных. сообщений или изображений.
- Частые зависания компьютера.

Активизация вируса может быть связана с различными событиями:

- Наступлением определённой даты или дня недели;
- Запуском программы;
- Открытием документа и т.д.



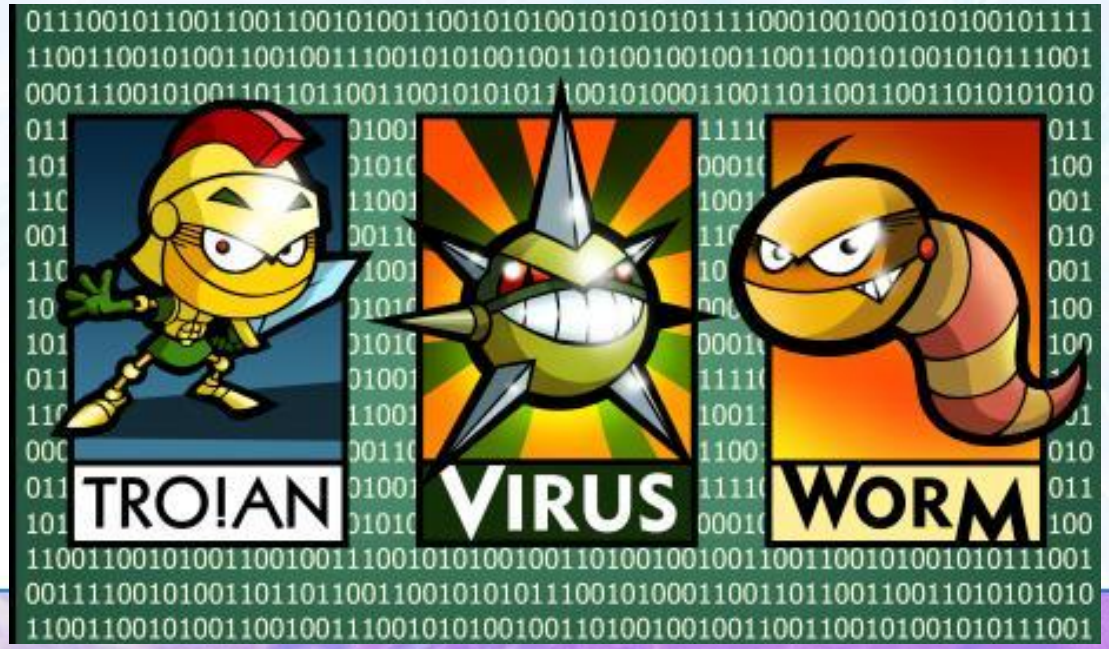
Типы вирусов по среде обитания:

ВИРУСЫ

- файловые
- макровирусы
- сетевые

Файловые вирусы

- Внедряются в программу и активизируются при их запуске.
- Могут заражать другие файлы до момента выключения компьютера.



Макровирусы

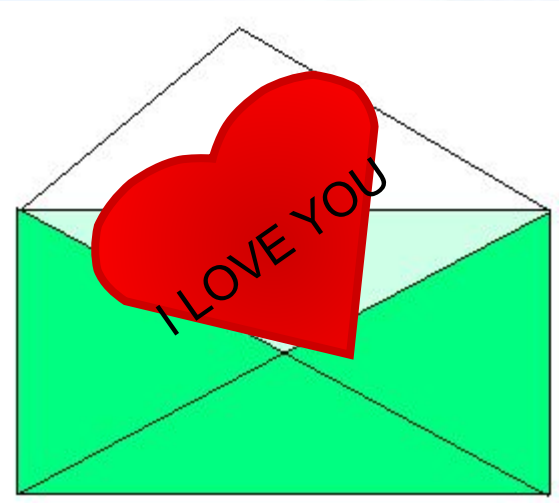
- Заражают файлы документов, например, текстовых документов.
- Угроза заражения прекращается только после закрытия текстового документа

Сетевые вирусы

- Могут передавать по компьютерным сетям свой программный код и запускать его на компьютерах, подключенных к этой сети.
- Заражение сетевым вирусом может произойти при работе с электронной почтой или при «путеше
Всемирной паутине.

5 мая 2005 года

Началась всемирная эпидемия заражения почтовым вирусом, когда десятки миллионов, подключенных к сети Интернет, получили почтовое сообщение:

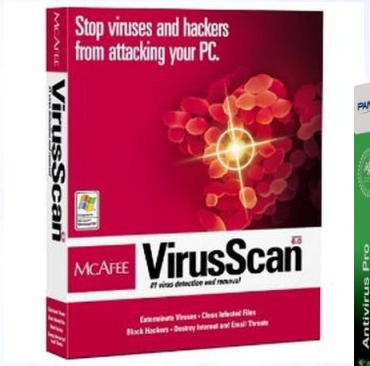


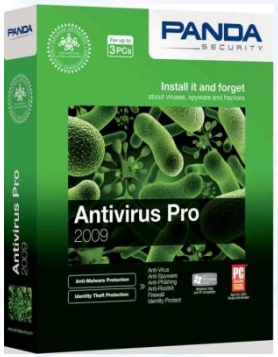
Профилактика заражения вирусами

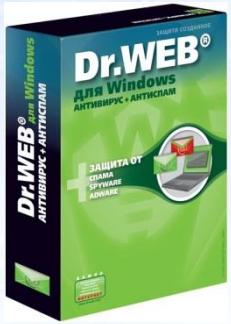
- Резервное копирование всех программ, файлов и системных областей дисков на дискеты.
- Ограничение доступа к машине путем введения пароля, администратора, закрытых дисков.
- Использование только лицензионного программного обеспечения, а не пиратских копий.
- Проверка всей поступающей извне информации на вирусы, как на дискетах, CD-ROM, так и по сети.
- Применение антивирусных программ и обновление их версий.
- Периодическая проверка компьютера на наличие вирусов при помощи антивирусных программ.

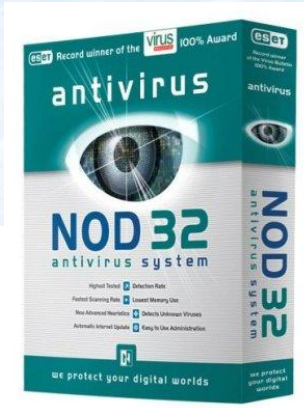
Антивирусные программы

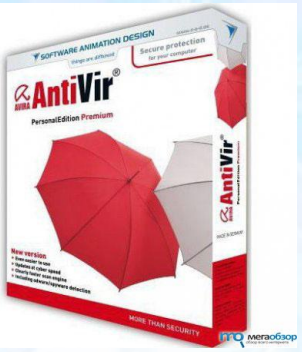
- программа, предназначенная для борьбы с компьютерными вирусами.

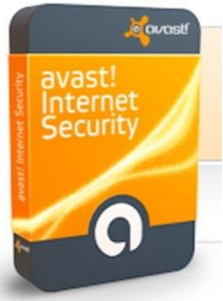












Типы антивирусных программ:

- **Антивирусные сканеры** – после запуска проверяют файлы и оперативную память и обеспечивают нейтрализацию найденного вируса
- **Антивирусные сторожа (мониторы)** – постоянно находятся в ОП и обеспечивают проверку файлов в процессе их загрузки в ОП
- **Полифаги** – самые универсальные и эффективные антивирусные программы. Проверяют файлы, загрузочные сектора дисков и ОП на поиск новых и неизвестных вирусов. Занимают много места, работают не быстро

Типы антивирусных программ:

- **Ревизоры** – проверяют изменение длины файла. Не могут обнаружить вирус в новых файлах (на дискетах, при распаковке), т.к. в базе данных нет сведений о этих файлах
- **Блокировщики** – способны обнаружить и остановить вирус на самой ранней стадии его развития (при записи в загрузочные сектора дисков). Антивирусные блокировщики могут входить в BIOS Setup.