Вьюгин Данила (8А класс)
МОУ «Средняя общеобразовательная школа №1», Г.о. Саранск, Республики Мордовия

Компьютерные вирусы и Антивирусные программы

Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/

Компьютерный вирус

Целью вируса является нарушение работы программно-аппаратных комплексов:

- удаление файлов,
- приведение в негодность структур размещения данных,
- блокирование работы пользователей
- приведение в негодность аппаратных комплексов компьютера
- занять место на накопителях информации

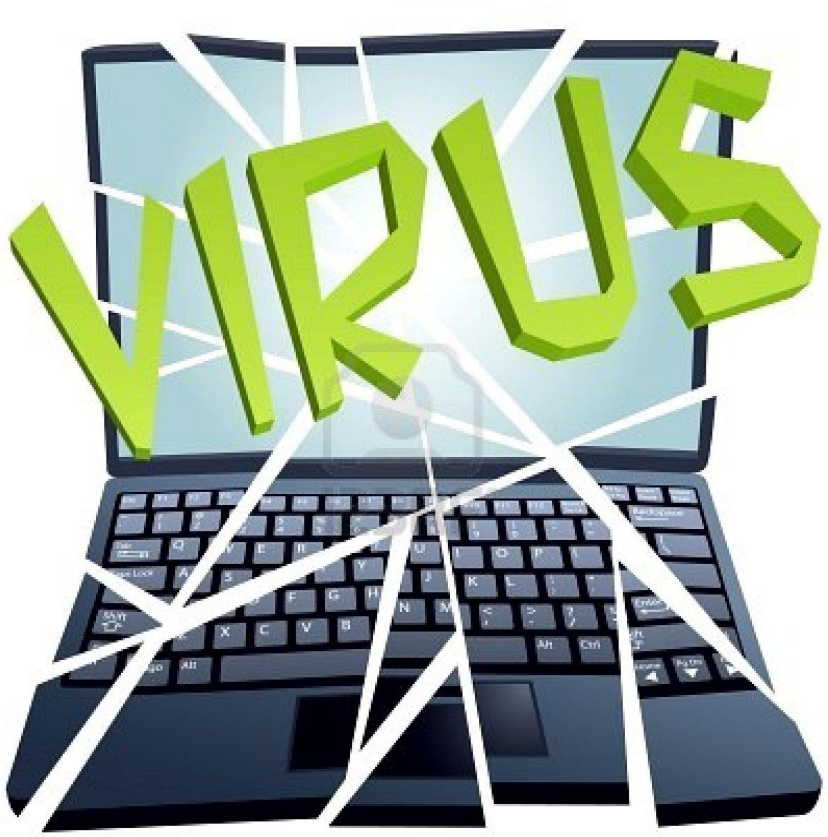
Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные сектора, а также распространять свои копии по разнообразным каналам связи.

История

ГОД	Событие
1981	Первые известные вирусы: Virus 1,2,3 и Elk Cloner для ПК Apple II
1984 (зима)	Появились первые антивирусные утилиты — CHK4BOMB и BOMBSQAD авторства Энди Хопкинса
1985	Ги Вонг написал программу DPROTECT — первый резидентный антивирус
1986—1989	Первые вирусные эпидемии: Brain.A (распространялся в загрузочных секторах дискет, вызвал крупнейшую эпидемию)
13 мая 1988	Появление Jerusalem (уничтожая программы при их запуске),червь Морриса (свыше 6200 компьютеров, большинство сетей вышло из строя на срок до пяти суток), DATACRIME (около 100 тысяч зараженных ПЭВМ только в Нидерландах).
1992	Появились первый конструктор вирусов для PC — VCL (для Amiga конструкторы существовали и ранее), а также готовые полиморфные модули (MtE, DAME и TPE) и модули шифрования для встраивания в новые вирусы.

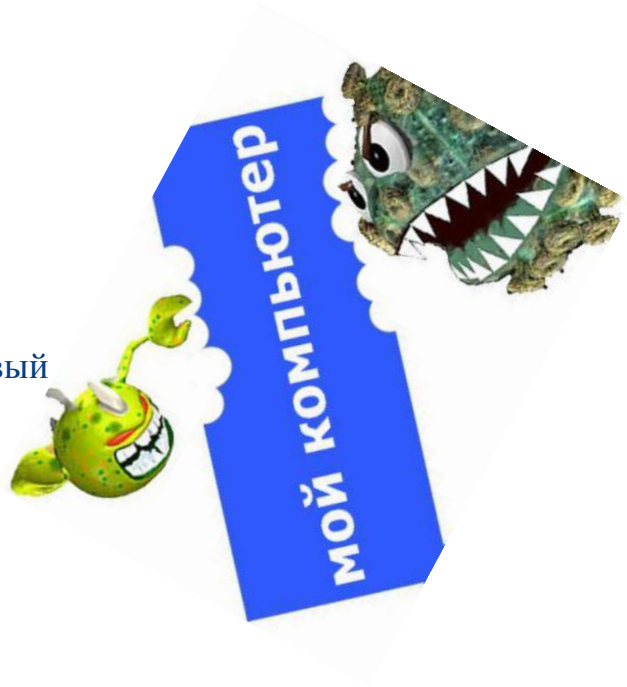
Этимология названия

* **Компьютерный вирус** назван по аналогии с биологическими вирусами за сходный механизм распространения.
* Впервые слово «вирус» по отношению к программе было употреблено Грегори Бенфордом в фантастическом рассказе «Человек в шрамах», опубликованном в журнале Venture в мае 1970 года.



Классификация компьютерных вирусов

* ПО ПОРАЖАЕМЫМ ОБЪЕКТАМ (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);
* ПО МЕХАНИЗМУ ЗАРАЖЕНИЯ: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.
* ПО ПОРАЖАЕМЫМ ОПЕРАЦИОННЫМ СИСТЕМАМ И ПЛАТФОРМАМ (DOS, Microsoft Windows, Unix, Linux);
* ПО ТЕХНОЛОГИЯМ, ИСПОЛЬЗУЕМЫМ ВИРУСОМ (полиморфные вирусы, стелс-вирусы, руткиты);
* ПО ЯЗЫКУ, НА КОТОРОМ НАПИСАН ВИРУС (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);
* ПО ДОПОЛНИТЕЛЬНОЙ ВРЕДОНОСНОЙ ФУНКЦИОНАЛЬНОСТИ (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).



Целевые платформы антивирусного ПО

Антивирусное программное обеспечение разрабатывается

- Windows
- Windows Mobile
- Linux
- Apple Ios
- UNIX
- Android
- Mac OS X
- Windows Phone 7

Пользователи устройств на данных ОС подвержены риску заражения вредоносным программным обеспечением

Классификация антивирусных продуктов

ПО ИСПОЛЬЗУЕМЫМ ТЕХНОЛОГИЯМ АНТИВИРУСНОЙ ЗАЩИТЫ:

- Классические антивирусные продукты (продукты, применяющие только сигнатурный метод детектирования, продукты, применяющие только проактивные технологии антивирусной защиты);
- Комбинированные продукты

ПО ФУНКЦИОНАЛУ ПРОДУКТОВ:

- Антивирусные продукты (продукты, обеспечивающие только антивирусную защиту)
- Комбинированные продукты (продукты, обеспечивающие не только защиту от вредоносных программ, но и фильтрацию спама, шифрование и резервное

ПО ОБЪЕКТАМ ЗАЩИТЫ:

- Антивирусные продукты для защиты рабочих станций
- Антивирусные продукты для защиты файловых и терминальных серверов
- Антивирусные продукты для защиты почтовых и Интернет-шлюзов
- Антивирусные продукты для защиты серверов виртуализации

Схема работы антивируса

1. Поиск в базе данных антивирусного ПО сигнатур вирусов.
2. если найден инфицированный код в памяти (оперативной и/или постоянной), запускается процесс «карантина», и процесс блокируется.
3. Зарегистрированная программа обычно удаляет вирус, незарегистрированная просит регистрации и оставляет систему уязвимой.

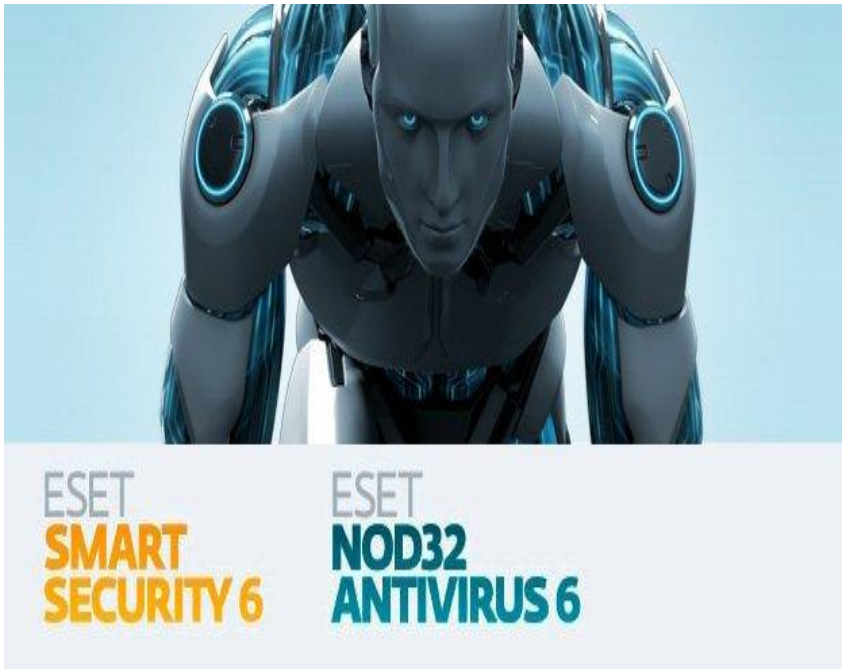
Dr.Web

* **Dr.Web** (рус. ***Доктор Веб***) — общее название семейства программного антивирусного ПО для различных платформ (Windows, OS X, Linux, мобильные платформы) и линейки программно-аппаратных решений (Dr.Web Office Shield), а также решений для обеспечения безопасности всех узлов корпоративной сети (Dr.Web Enterprise Suite). Разрабатывается компанией «Доктор Веб».

Продукты предоставляют защиту от вирусов, троянского, шпионского и рекламного ПО, червей, руткитов, хакерских утилит, программ-шуток, а также неизвестных угроз с помощью различных технологий реального времени и превентивной защиты.

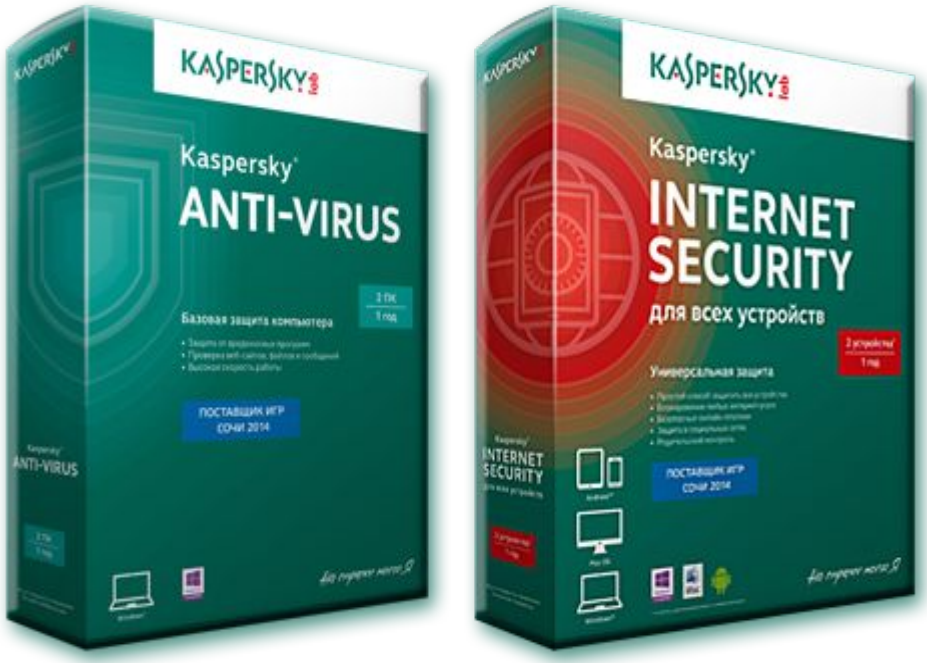
ESET NOD32

* **ESET NOD32** — антивирусный пакет, выпускаемый словацкой фирмой ESET. Первая версия была выпущена в конце 1987 года. Название изначально расшифровывалось как «Nemocnica na Okraji Disku».
* ESET NOD32 — это комплексное антивирусное решение для защиты в реальном времени. ESET NOD32 обеспечивает защиту от вирусов, а также от других угроз, включая троянские программы, черви, spyware, adware, фишинг-атаки. В ESET NOD32 используется патентованная технология ThreatSense, предназначенная для выявления новых возникающих угроз в реальном времени путём анализа выполняемых программ на наличие вредоносного кода, что позволяет предупреждать действия авторов вредоносных программ.



Антивирус Касперского

* **Антивирус Касперского** (англ. *Kaspersky Antivirus, KAV*) — антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS (только для старших версий, именуемых «Kaspersky Internet Security 2009+, где '+' — порядковый номер предыдущего регистра, ежегодно увеличиваемый на единицу в соответствии с номером года, следующим за годом выпуска очередной версии антивируса»). Первоначально, в начале 1990-х, именовался **-V**, затем — **AntiViral Toolkit Pro**.



Avast!

* **Avast!** — антивирусная программа для операционных систем Windows, Linux, Mac OS, а также для КПК на платформе Palm, Android и Windows CE.
* Разработка компании AVAST Software, основанной в 1991 году в Чехословакии. Главный офис компании расположен в Праге. Для дома выпускается в виде нескольких версий: платной (Pro Antivirus, Internet Security и Premier) и бесплатной (Free Antivirus) для некоммерческого использования. Также существуют версии для среднего и большого бизнеса (Endpoint Protection, Endpoint Protection Plus, Endpoint Protection Suite и Endpoint Protection Suite Plus) и версии для серверов (File Server Security и Email Server Security). Продукт сертифицирован ICSA Labs.

Спасибо за внимание!