



КОМПЬЮТЕРНЫЕ ВИРУСЫ

АНТИВИРУСНЫЕ ПРОГРАММЫ



Выполнила:
ученица 8 В класса
МАОУ лицея №21
Спиридонова Ольга
Учитель: Молькова Е.О
«Презентация
подготовлена для конкурса
«Интернешка»

ЧТО ТАКОЕ КОМПЬЮТЕРНЫЙ ВИРУС?

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

В обиходе «вирусами» называют всё вредоносное ПО, хотя на самом деле это лишь один его вид.



ЦЕЛЬ КОМПЬЮТЕРНОГО ВИРУСА:

Цель вируса: нарушение работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера.

Вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы.



КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Принято разделять вирусы:

- 1) по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);
- 2) файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.
- 3) по поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, Linux);
- 4) по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
- 5) по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);
- 6) по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

КАНАЛЫ ЗАРАЖЕНИЯ КОМПЬЮТЕРНЫМИ ВИРУСАМИ

Флеш-накопители (флешки). Большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, портативные цифровые плееры, мобильные телефоны, особенно смартфоны (появились мобильные вирусы).

Электронная почта. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код.



КАНАЛЫ ЗАРАЖЕНИЯ КОМПЬЮТЕРНЫМИ ВИРУСАМИ

Системы обмена мгновенными сообщениями. Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

Веб-страницы. Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компонент.

Интернет и локальные сети (черви). Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» в программном обеспечении операционных систем, чтобы проникнуть на компьютер.



ЧТО ТАКОЕ АНТИВИРУСНЫЕ ПРОГРАММЫ?

Антивирусная программа (антивирус) — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.



КЛАССИФИКАЦИЯ АНТИВИРУСНЫХ ПРОГРАММ

По используемым технологиям антивирусной защиты:

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

Комбинированные продукты (продукты, применяющие как сигнатурные методы защиты, так и проактивные)

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 копирование данных и другие функции)

КЛАССИФИКАЦИЯ АНТИВИРУСНЫХ ПРОГРАММ

По целевым платформам:

Антивирусные продукты для ОС семейства Windows

Антивирусные продукты для ОС семейства *NIX (к данному семейству относятся ОС BSD, Linux и др.)

Антивирусные продукты для ОС семейства MacOS

Антивирусные продукты для мобильных платформ (Windows Mobile, Symbian, iOS, BlackBerry, Android, Windows Phone 7 и др.)

Антивирусные продукты для корпоративных пользователей можно также классифицировать 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

РАБОТА АНТИВИРУСА

Говоря о системах Майкрософт, следует знать, что обычно антивирус действует по схеме:

поиск в базе данных антивирусного ПО сигнатур вирусов.

если найден инфицированный код в памяти (оперативной и/или постоянной), запускается процесс «карантина», и процесс блокируется.

зарегистрированная программа обычно удаляет вирус, незарегистрированная просит регистрации и оставляет систему уязвимой.



ПОПУЛЯРНЫЕ АНТИВИРУСЫ

Антивирус

Касперского

Eset NOD32

Dr. Web

Trend Micro Internet Security

Avast! Professional Edition

BitDefender Antivirus

Panda Antivirus

McAfee VirusScan

Avira AntiVir

Symantec Norton Anti-Virus