Компьютерные вирусы. Антивирусные программы.

Что такое компьютерные 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.

Отличительные особенностями компьютерных вирусов

- маленький объем
- самостоятельный запуск
- многократное копирование кода
- создание помех для корректной работы компьютера

Классификация вирусов

- Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности.
- В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:

По поражаемым объектам

Файловые вирусы

Загрузочные вирусы

Сценарные вирусы

Макровирусы

Вирусы, поражающие исходный код

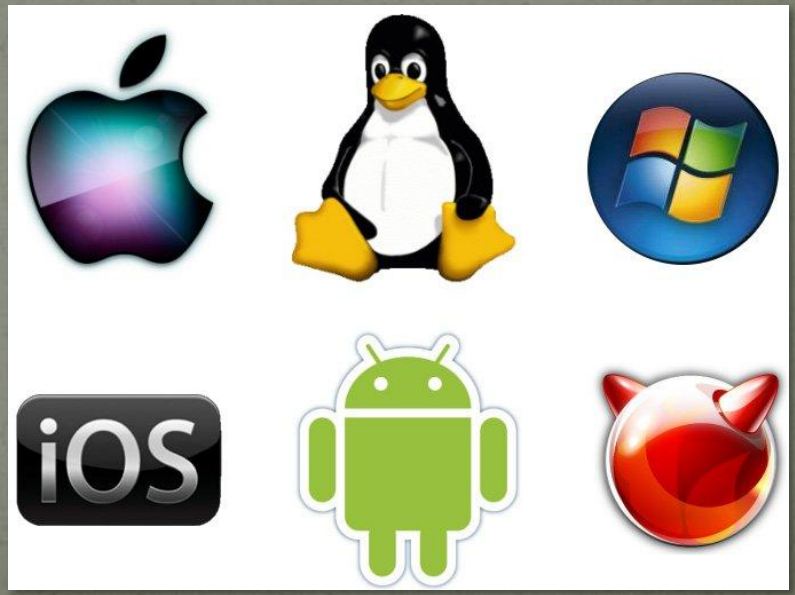
По поражаемым операционным системам и платформам

DOS

Microsoft Windows

Unix

Linux



По технологиям, используемым вирусом

Полиморфные вирусы

Стелс-вирусы

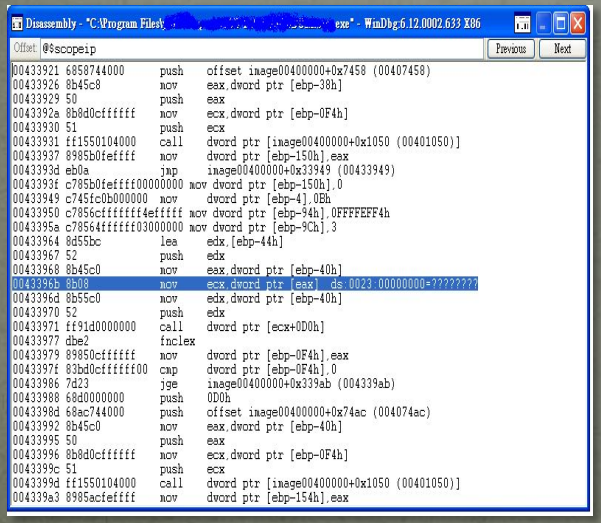
Руткиты

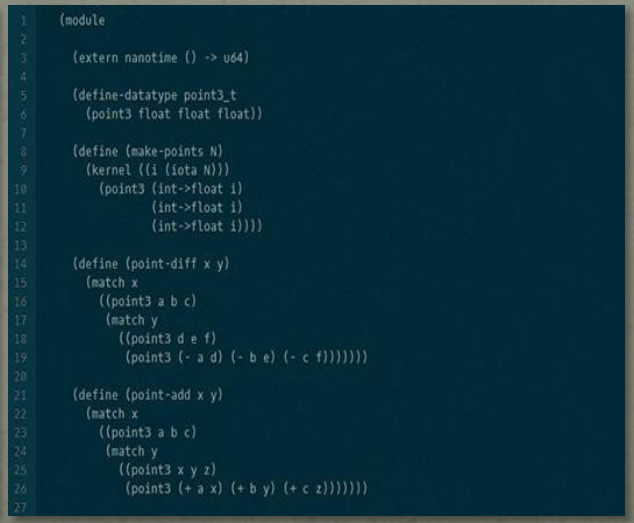
По языку, на котором написан вирус

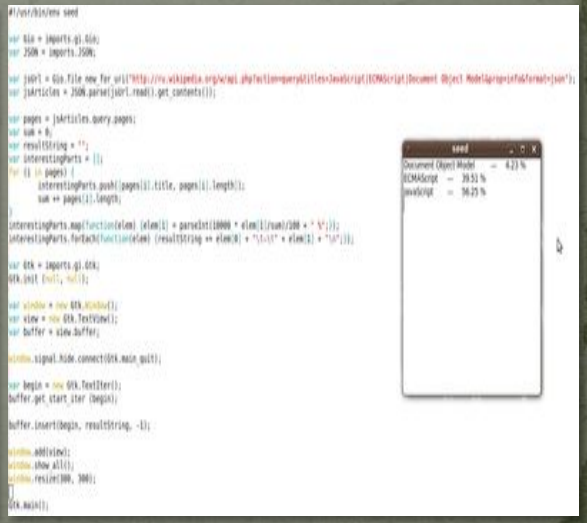
ассемблер

высокоуровневый язык программирования

сценарный язык







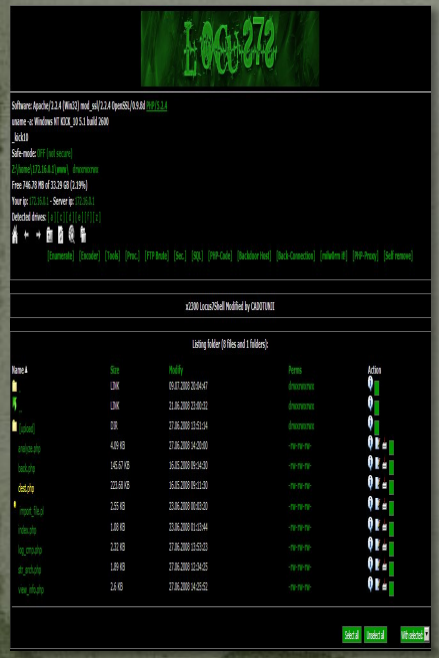
По дополнительной вредоносной функциональности

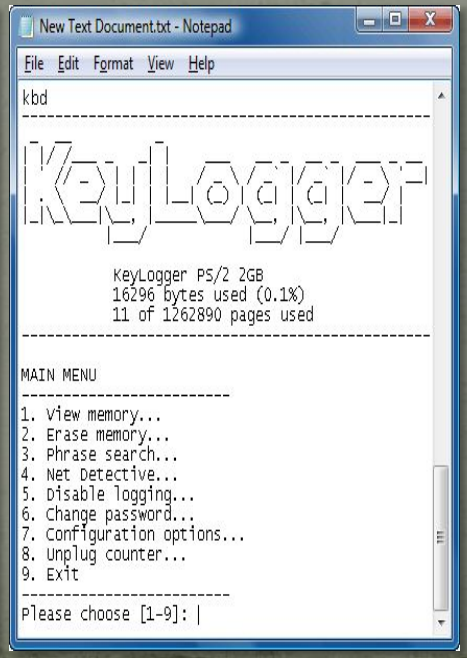
бэкдоры

кейлоггеры

шпионы

ботнеты





Что такое антивирус?

- **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.

Лучший антивирус

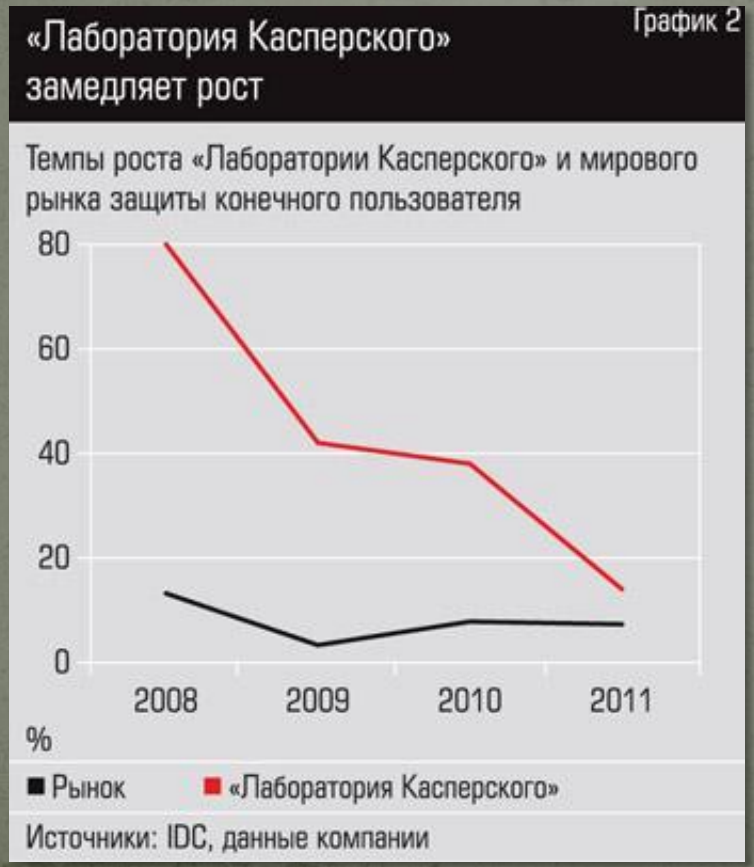
Динамическое тестирование (Real World Protection Test) антивирусов от AV-Comparatives является наиболее полным и комплексным из доступных сравнительных тестов, в котором используется большое количество тестовых образцов.

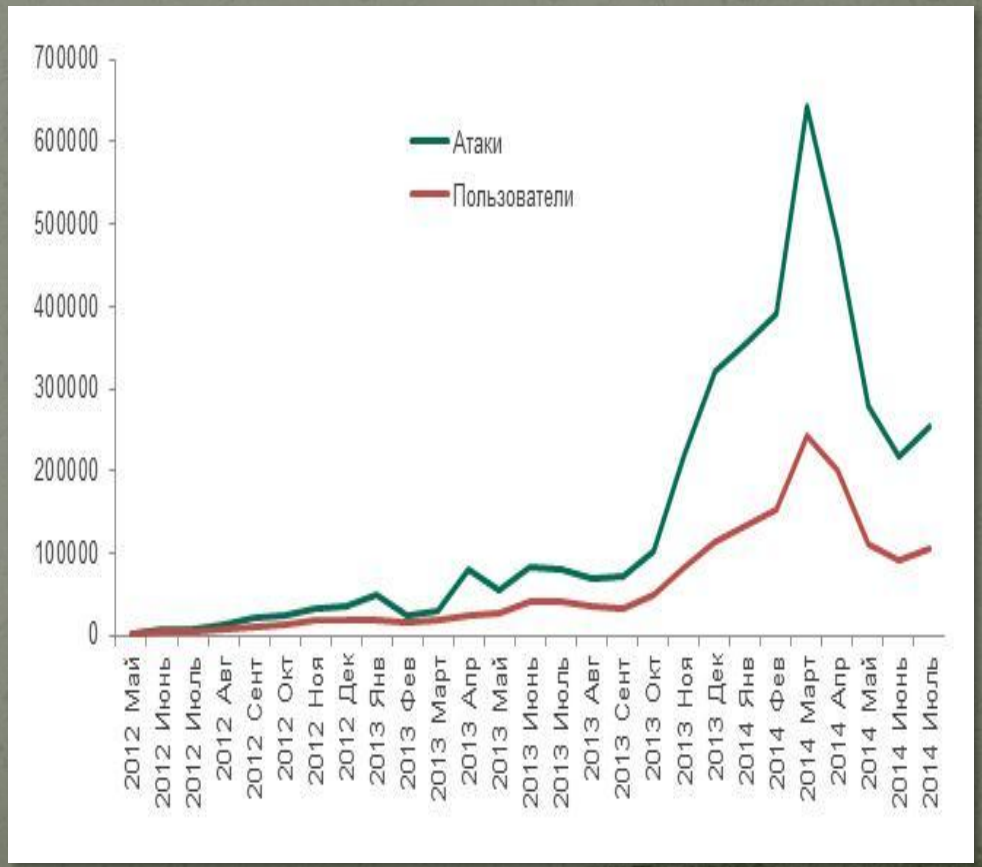
В 2015 году тестирование проводится на платформе с ОС Microsoft Windows 7 Home Premium 64-bit SP1 с установленными актуальными (обновленными на момент тестирования) сторонними приложениями (например, Adobe Flash, Adobe Acrobat Reader, Java и т.д.).

- Результат Microsoft Security Essentials - 95.7% - не участвует в общем сравнении. На графике он показан прерывистой линией как уровень защиты самой системы Microsoft Windows.
- Комплексные антивирусы Bitdefender Internet Security, Kaspersky Internet Security, Avira Antivirus Pro и Trend Micro Internet Security показали максимальный уровень обнаружения, не пропустив ни одной угрозы. При этом решения Bitdefender и Kaspersky прошли испытание без ложных срабатываний, антивирус Avira допустил 1 ложное срабатывание, а Trend Micro - 12 ложных срабатываний.
- Ближайшие преследователи AVG Internet Security и Panda Free Antivirus пропустили 0.3% угроз. AVG прошел тестирование без ложных срабатываний, бесплатный антивирус Panda показал 6 ложных срабатываний.
- Решения F-Secure Internet Security и Emsisoft Anti-Malware хотя и не пропустили ни одной угрозы, но 1% и 1.3% обрабатываемых вредоносных образцов требовали решения пользователя. Поэтому показатель обнаружения специалистами лаборатории AV-Comparatives засчитан на уровне 99% и 98.7% соответственно.
- В AV-Comparatives отмечают, что даже если некоторые продукты показывают 100% уровень защиты в тестировании, это не значит, что эти антивирусные программы всегда будут защищать от всех угроз в интернете. Это просто означает, что они в состоянии заблокировать 100% распространенных вредоносных образцов, используемых в данном конкретном тесте.
- Мы рассмотрим самые популярные в России антивирусы: Kaspersky Internet Security, ESET NOD32, Dr.WEB.

Kaspersky Internet Security

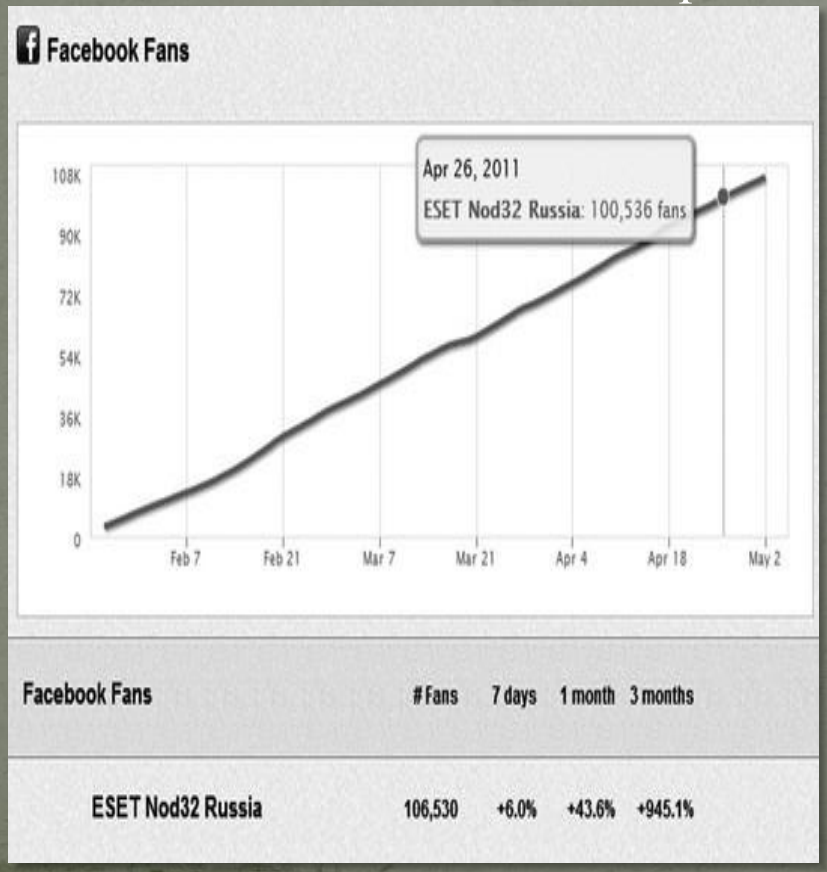
- **Kaspersky Internet Security** (KIS) — линейка программных продуктов, разработанная компанией «Лаборатория Касперского» на базе линейки продуктов Антивирус Касперского, для комплексной защиты домашних персональных компьютеров в реальном времени от известных и новых современных угроз.

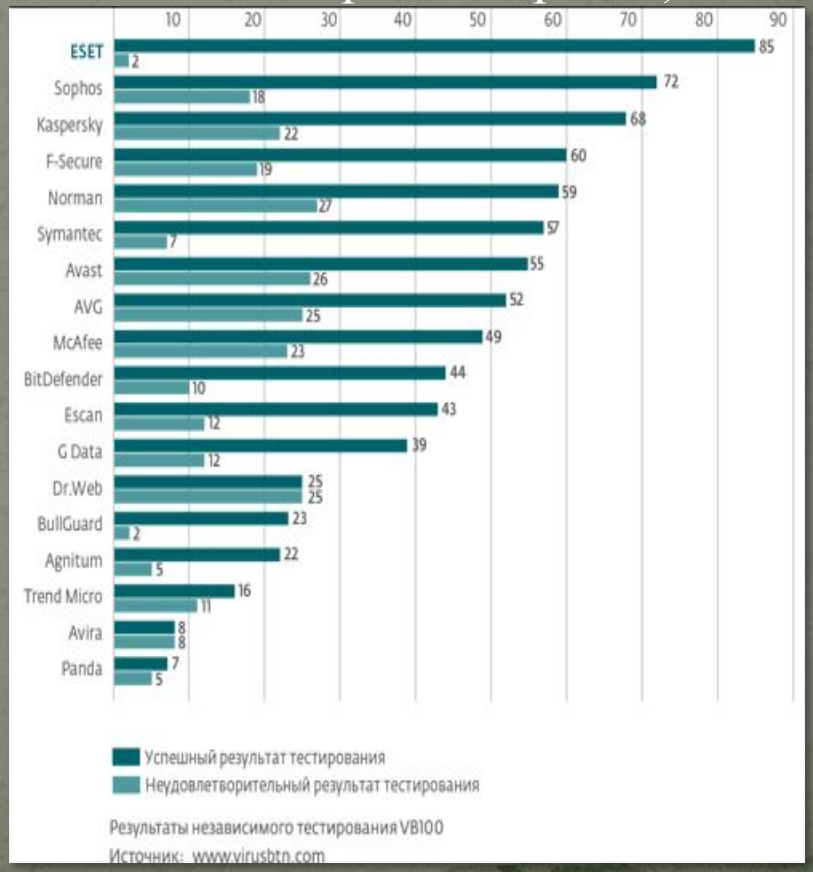




ESET NOD32

- **ESET NOD32** — антивирусный пакет, выпускаемый словацкой фирмой ESET. Первая версия была выпущена в конце 1987 года. Название изначально расшифровывалось как «Nemocnica na Okraji Disku» («Больница на краю диска», перефраз названия популярного тогда в Чехословакии телесериала «Больница на окраине города»).





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».