

# 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

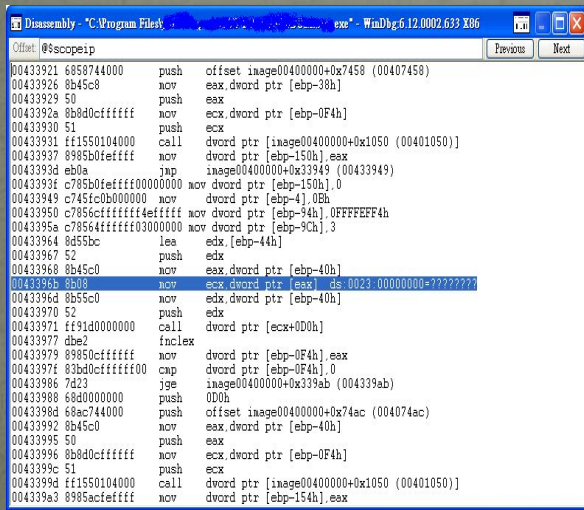


# По языку, на котором написан вирус

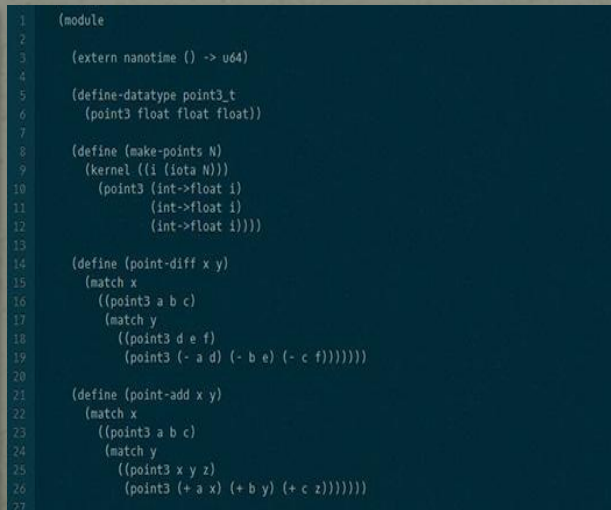
ассемблер

высокоуровневый язык  
программирования

сценарный язык



```
Disassembly - "C:\Program Files\...\.exe" - WinDbg.6.12.0002.633 X86
Offset: @$scope:ip
00433921 6858744000  push  offset inage00400000+0x7458 (00407458)
00433926 8b45c8      mov    eax,dword ptr [ebp-38h]
00433929 50         push  eax
0043392a 8b8d0cffff  mov    ecx,dword ptr [ebp-0F4h]
00433930 51         push  ecx
00433931 ff1550104000  dword ptr [inage00400000+0x1050 (00401050)]
00433937 8985b0ffff  mov    dword ptr [ebp-150h],eax
0043393d ebd0      jmp    inage00400000+0x33949 (00433949)
0043393e c785b0ffff00000000 00000000  mov  dword ptr [ebp-150h],0
00433949 c745fc0b000000  mov  dword ptr [ebp-4],0bh
00433950 c785cfffff4efffff 00000000  mov  dword ptr [ebp-94h],0FFFFFFF4h
0043395a c78564ffff03000000 00000000  mov  dword ptr [ebp-9Ch],3
00433964 8d55bc     lea   edx,[ebp-44h]
00433967 52         push  edx
00433968 8b45c0     mov    eax,dword ptr [ebp-40h]
00433969 8b08      mov    ecx,dword ptr [eax],ds:0023:00000000+?2????2?
0043396d 8b55c0     mov    edx,dword ptr [ebp-40h]
00433970 52         push  edx
00433971 ff91d0000000  call  dword ptr [ecx+0D0h]
00433977 db2       fnclex
00433979 89850cffff  mov    dword ptr [ebp-0F4h],eax
0043397f 83bd0cffff00  cmp    dword ptr [ebp-0F4h],0
00433986 7d23      jge   inage00400000+0x339ab (004339ab)
00433988 68d0000000  push  00h
0043398d 88ac744000  push  offset inage00400000+0x74ac (004074ac)
00433992 8b45c0     mov    eax,dword ptr [ebp-40h]
00433995 50         push  eax
00433996 8b8d0cffff  mov    ecx,dword ptr [ebp-0F4h]
0043399c 51         push  ecx
0043399d ff1550104000  call  dword ptr [inage00400000+0x1050 (00401050)]
004339a3 8985acffff  mov    dword ptr [ebp-154h],eax
```



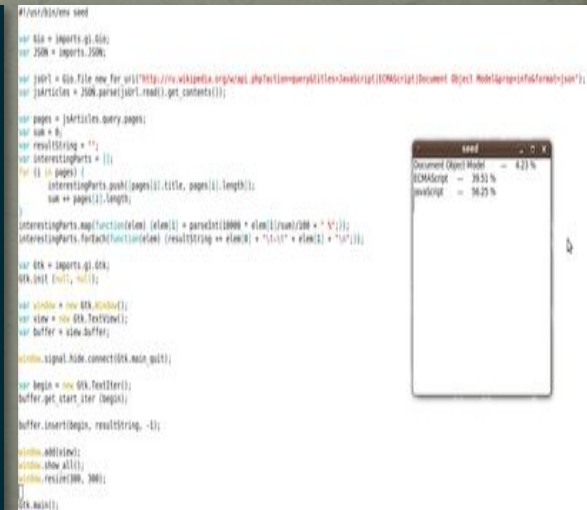
```
(module
  (extern nanotime () -> u64)

  (define-datatype point3_t
    (point3 float float float))

  (define (make-points N)
    (kernel ((i (iota N)))
            (point3 (int->float i)
                    (int->float i)
                    (int->float i))))

  (define (point-diff x y)
    (match x
      ((point3 a b c)
       (match y
         ((point3 d e f)
          (point3 (- a d) (- b e) (- c f)))))))

  (define (point-add x y)
    (match x
      ((point3 a b c)
       (match y
         ((point3 x y z)
          (point3 (+ a x) (+ b y) (+ c z)))))))
```



```
#!/usr/bin/perl

my $to = "ipnets.qj.dk";
my $port = "ipnets.2500";

my $url = "http://www.wikipedia.org/w/index.php?title=query&rlto=script&document=Object%20Not%20a%20Function%20";
my $url .= $to.$port.$url.read($_.read());

my $pages = (split($_.query.pages);
my $sum = 0;
my $resulting = "";
my $interestingParts = ();
for ($i = 0; $i < @$pages; $i++) {
  $interestingParts.push($pages[$i].$url.$pages[$i].length);
  $sum += $pages[$i].length;
}
$interestingParts.map(function($elem) { return ($elem * $pages[$i].length) / $sum; });
$interestingParts.forEach(function($elem) { $resulting += $elem["url"] . "\n"; });

my $dns = "ipnets.qj.dk";
my $url = "http://www.wikipedia.org/w/index.php?title=query&rlto=script&document=Object%20Not%20a%20Function%20";
my $url .= $to.$port.$url.read($_.read());

my $buffer = $url.$dns;

my $signal = "connect(dns.main.quit)";

my $begin = "connect(dns.main.quit)";
my $buffer = $signal.$begin.$resulting.$signal;

my $addition();
my $show = "show all()";
my $resulting = "show all()";
my $url = "http://www.wikipedia.org/w/index.php?title=query&rlto=script&document=Object%20Not%20a%20Function%20";
my $url .= $to.$port.$url.read($_.read());
```



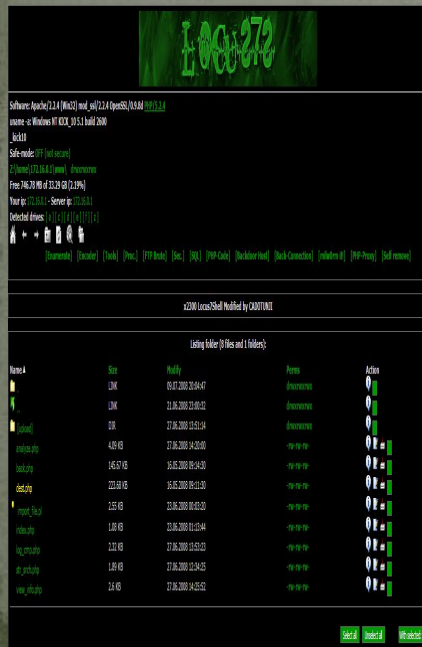
# По дополнительной вредоносной функциональности

бэкдоры

кейлоггеры

шпионы

ботнеты



# Что такое антивирус?

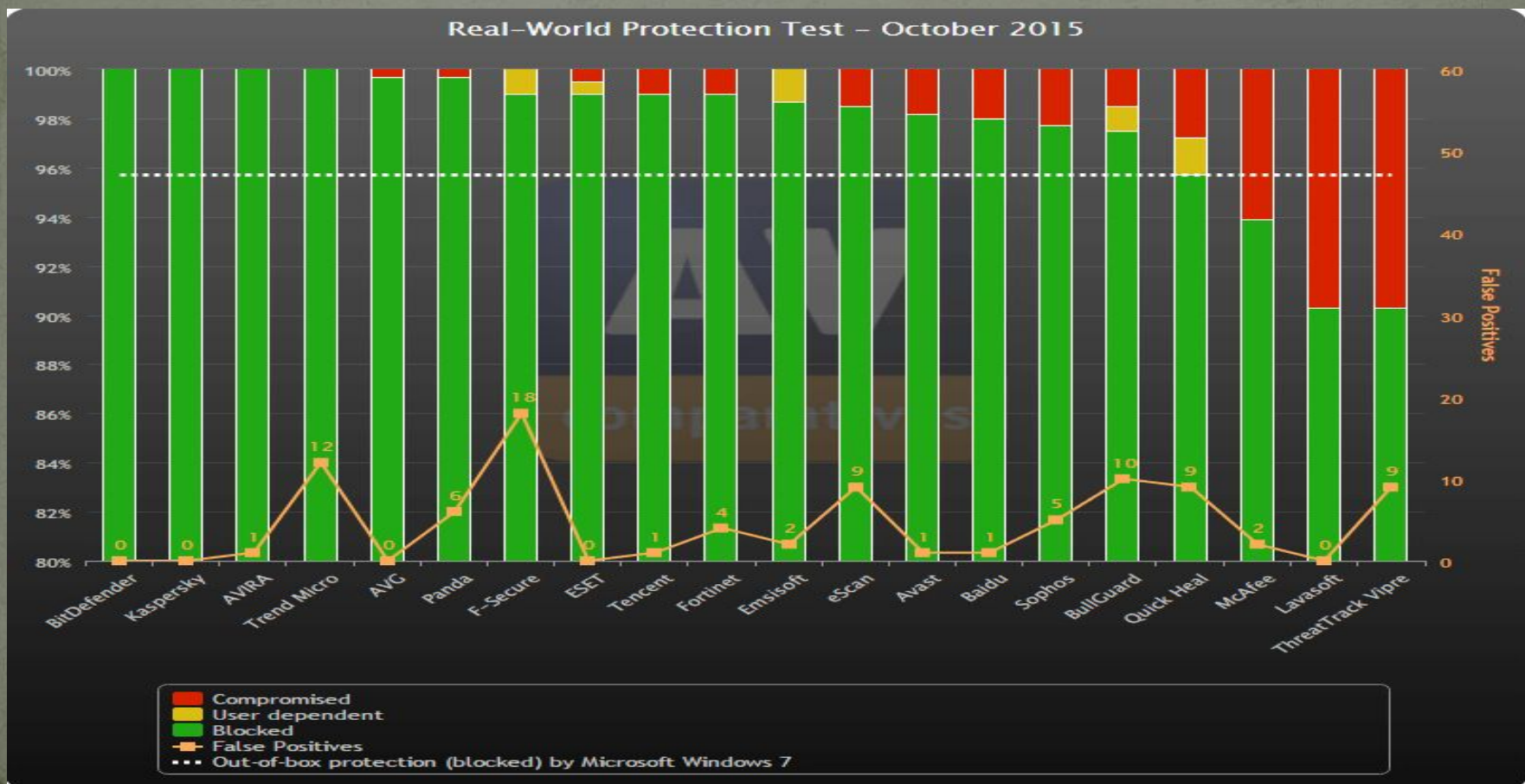
- **Антивирусная программа (антивирус)** — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (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.).

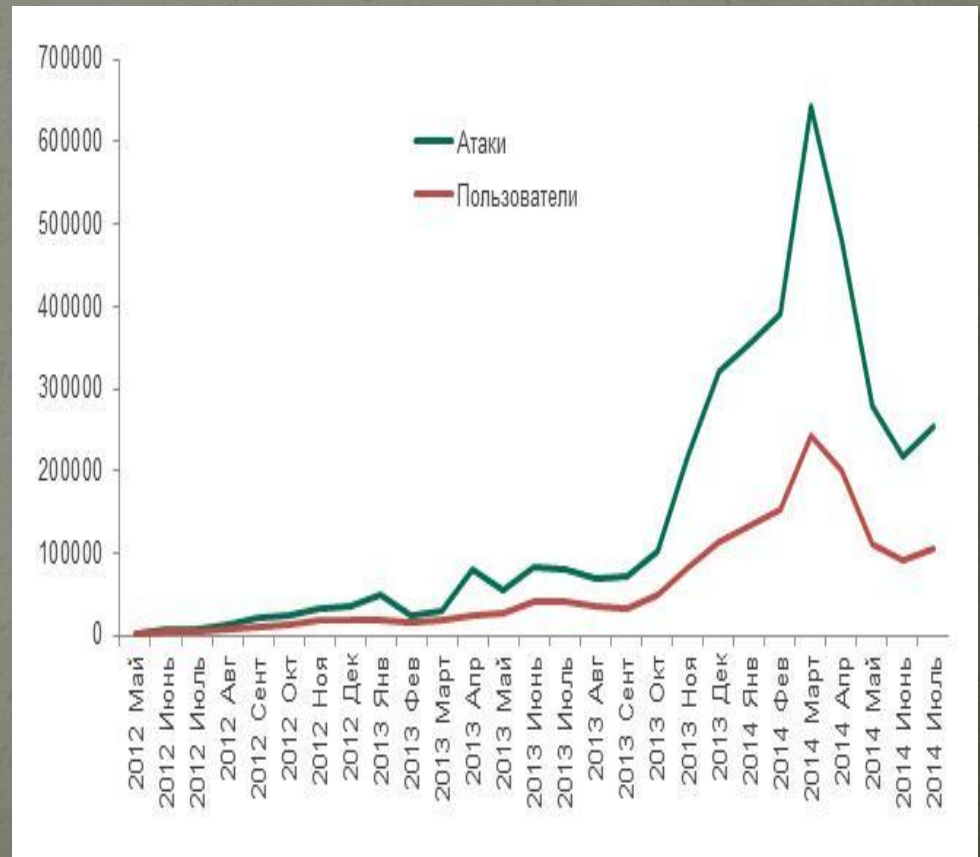
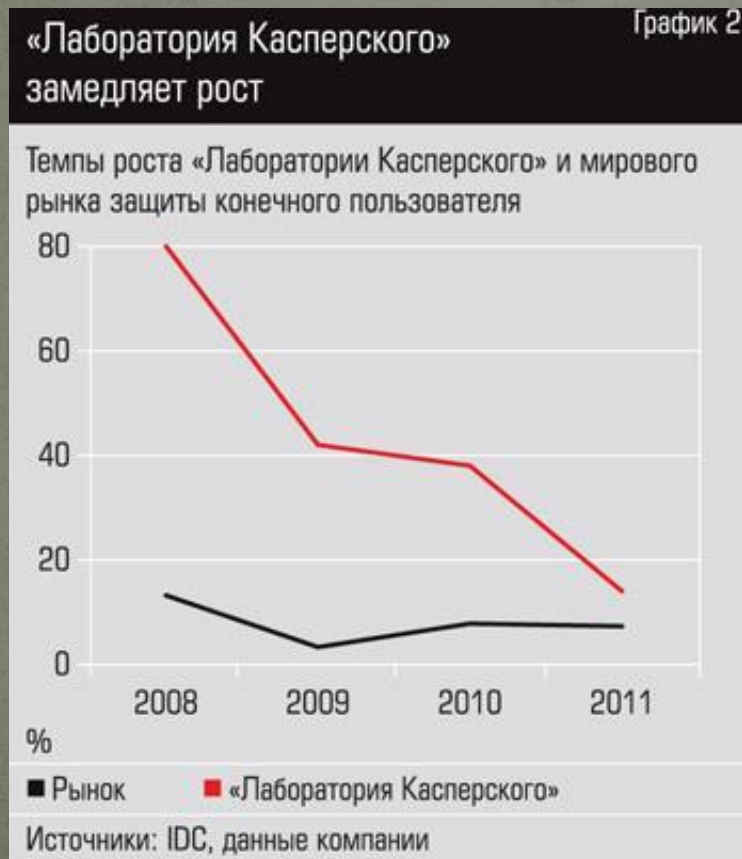


- Результат Microsoft Security Essentials - 95.7% - не участвует в общем сравнении. На графике он показан прерывистой линией как уровень защиты самой системы Microsoft Windows.
- Комплексные антивирусы Bitdefender Internet Security, Kaspersky Internet Security, Avira Antivirus Pro и Trend Micro Internet 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.



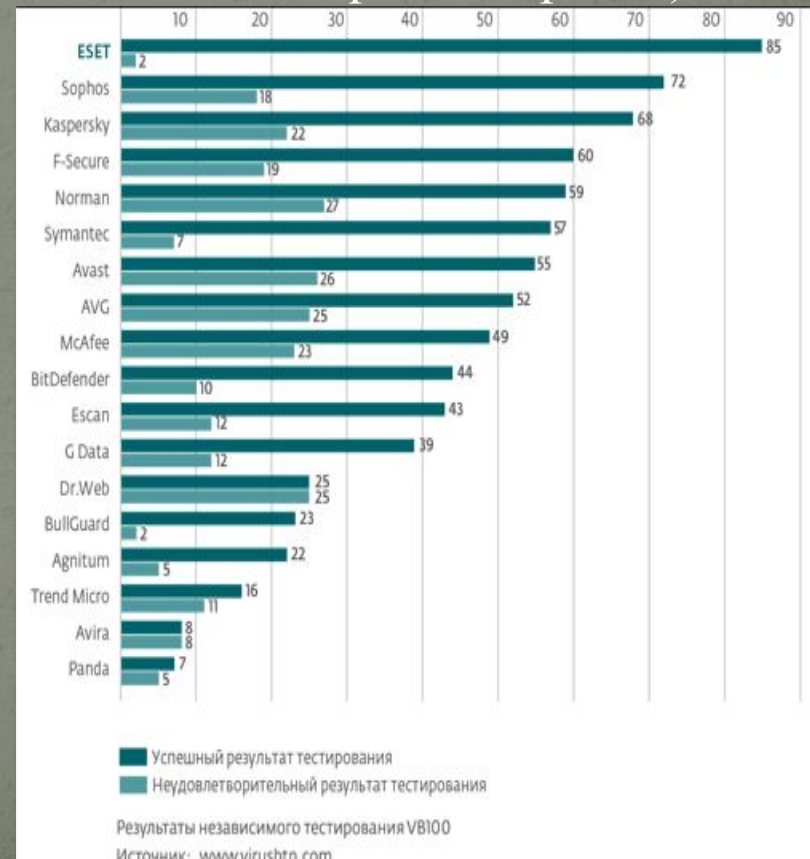
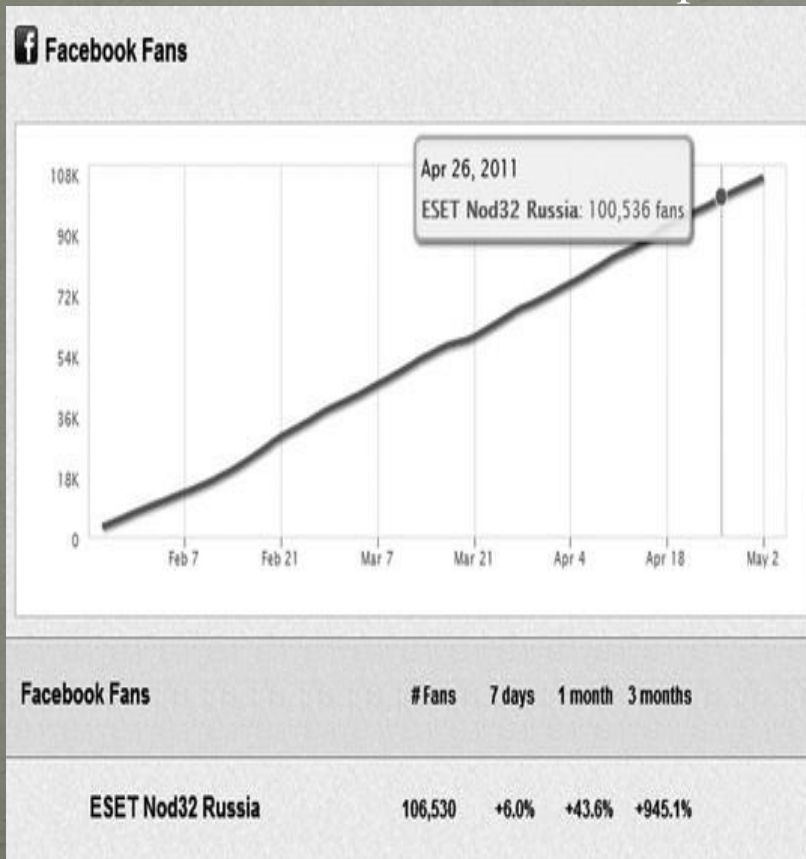
# Kaspersky Internet Security

- **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

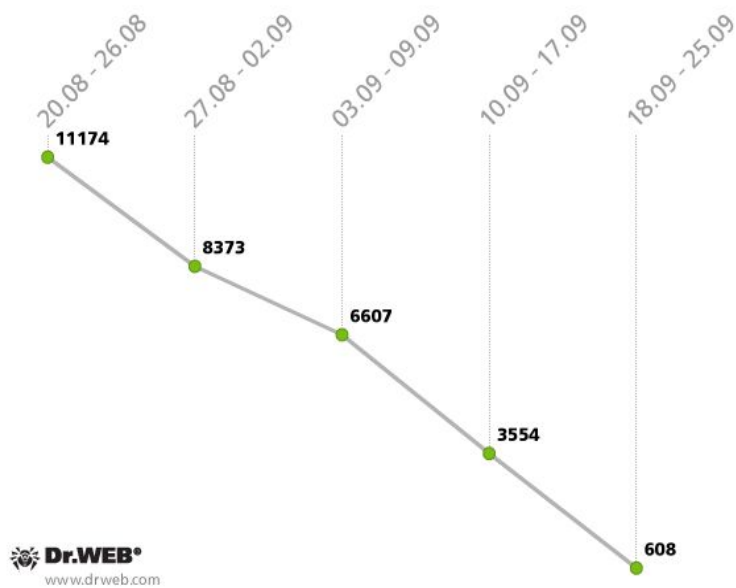
- **ESET NOD32** — антивирусный пакет, выпускаемый словацкой фирмой ESET. Первая версия была выпущена в конце 1987 года. Название изначально расшифровывалось как «Nemocnica na Okraji Disku» («Больница на краю диска», перефраз названия популярного тогда в Чехословакии телесериала «Больница на окраине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

Изменение количества заражений троянцем Trojan.Mayachok.1



Время, затраченное на проверку

