

# Вирусы и антивирусные программы



*Коляда Татьяна Александровна*

# Компьютерный вирус -

Компьютерный вирус — это специально созданная программа, которая приписывается другой программе или устройству.



— это специально созданная программа, которая приписывается другой программе или устройству.

# Первый вирус

Первая «эпидемия» компьютерного вируса произошла в 1986 году, когда вирус по имени Brain (англ. «мозг») заразил дискеты персональных компьютеров.



# Россия вышла в мировые лидеры по распространению компьютерных вирусов



Аналитики PC Tools уверяют, что по масштабам распространения компьютерных вирусов, вредоносного и шпионского программного обеспечения Россия давно опередила таких "гигантов" в этой области, как Китай и США. По оценкам аналитиков PC Tools - американского производителя средств защиты от нежелательного ПО – на долю РФ приходится **27,89%** вредоносных программ в мире, Китая - **26,52%**, США - **9,98%**

# Классификация вирусов по среде обитания

- Загрузочные вирусы
- Файловые вирусы
- Макро - вирусы
- Сетевые вирусы



# Загрузочные вирусы

- Загрузочные вирусы заражают загрузочный (boot) сектор флорпи-дисков, жестких дисков и винчестера. Их распространение основано на алгоритмах, которые выполняются при включении компьютера (например, тестирование оборудования, загрузка BIOS и т.д.). Программа, заражающая загрузочный сектор, получает первый контроль над системой при загрузке (например, BIOS Setup) и управляет процессом загрузки. Такие вирусы "подставляют" себя, получая управление, и "заставляют" компьютер загрузить память и отдать управление не оригинальному коду загрузчика, а коду вируса.





# Файловые вирусы

- К данной группе относятся вирусы, которые используют для размножения файлы или папки. Они используют файлы с расширениями .COM, .EXE, .SYS, и т.д.
- Могут быть как резидентными, так и не резидентными. Резидентные вирусы остаются в памяти компьютера, а не резидентные — нет.
- Практически все файлы с расширениями .COM, .EXE, .SYS, и т.д. являются файлами-вирусами. резидентные



# Макро-вирусы

- Макро-вирусы (macro viruses) являются программами на языках (макро-языках), встроенных в некоторые системы обработки электронных таблицы. Такие вирусы используют их помощи переноса (документа или табл
- На сегодня, системы, для которых Excel, MS Office и получают зараженного файла, где функции и затем за вирусом либо образ идет обращение. макро-вирусов резидентные.





# Сетевые вирусы

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей.

Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. "Полноценные" сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, "подтолкнуть" пользователя к запуску зараженного файла.



# По особенностям алгоритма вирусы имеют большое разнообразие

**Простейшие вирусы** – не изменяют содержимое файлов, могут быть легко обнаружены и уничтожены

**Черви** – распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и рассылают свои копии по этим адресам

**Вирусы – невидимки** – трудно обнаружить и обезвредить, подставляют вместо своего тела незараженные участки диска

**Вирусы-мутанты** – содержат алгоритмы шифровки / расшифровки, наиболее трудно обнаружить

**Трояны** – маскируются под полезную программу, разрушают загрузочный сектор и файловую систему

# Другие вредоносные программы

## Троянские кони (логические бомбы)

К троянским коням относятся программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от каких-либо условий выполняющие уничтожающую систему и т.п. информацию.

Большинство троянских коней являются программами, которые "под видом" полезных программ, дополнения к станциям или вирусам распространяются по BBS-сетям. По сравнению с вирусами они имеют более широкий спектр причин - они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем.



# Другие вредоносные программы

## Intended-вирусы

К таким вирусам относятся программы, которые на первый взгляд являются полезными, но не являются таковыми. Например, вирус, который копирует файлы и записывает их в неправильном формате, прерывает работу и закрывает программы.



К категории Intended-вирусов относятся вирусы, которые по своей природе являются полезными, но только один раз - из "авторского" экземпляра. Если файл, они теряют способность к дальнейшему размножению.

# Другие вредоносные программы

## Конструкторы вирусов

Конструкторы вирусов — это утилита, предназначенная для создания и управления новыми вредоносными программами. Известны такие конструкторы, как VirusShare, DOS, Windows и Macro-Generator, которые позволяют генерировать исходный код вирусов (ASM-файлы), объектные модули, и/или непосредственно зараженные файлы.

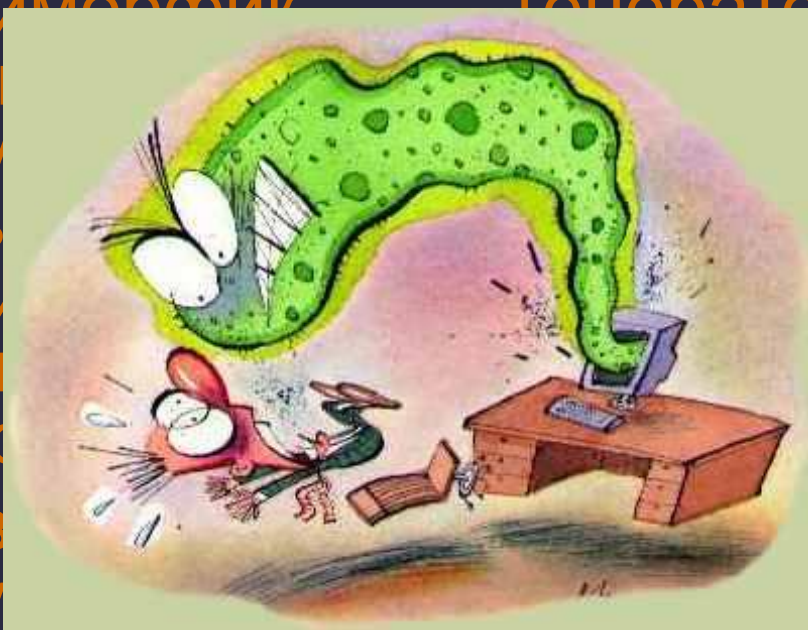




# Другие вредоносные программы

## Полиморфные генераторы

Полиморфные генераторы, как и вирусы, являются вредоносными программами. Это слово, происходящее от греческого слова, означающего «разнообразие», описывает способность этих программ изменять свой код при каждом запуске. Это позволяет им избежать обнаружения антивирусными программами. Они могут изменять свои функции, например, скрывать файлы, удалять данные, красть информацию, читать и изменять файлы, а также повреждать данные. Главной задачей полиморфных генераторов является создание нового вида вредоносных программ. Они делают это путем изменения структуры тела вируса и генерация соответствующего расшифровщика.



# Примеры вирусов

## KeyKut 4.0 (Trojan-Spy.Win32.Banker.ckl)

Бразильский троян для кражи персональной информации, написан на Delphi. Имеет размер более 2Мб.



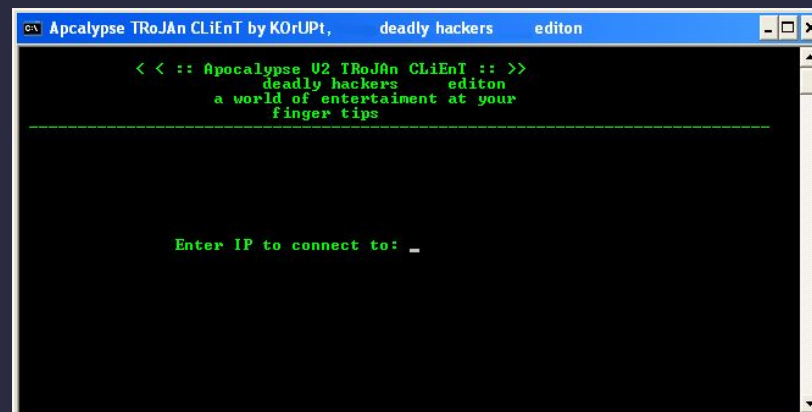
# Примеры вирусов

## Аpocalypse Trojan v2

Троян-бекдор, не обнаруживаемый антивирусами.

Состоит из одного файла

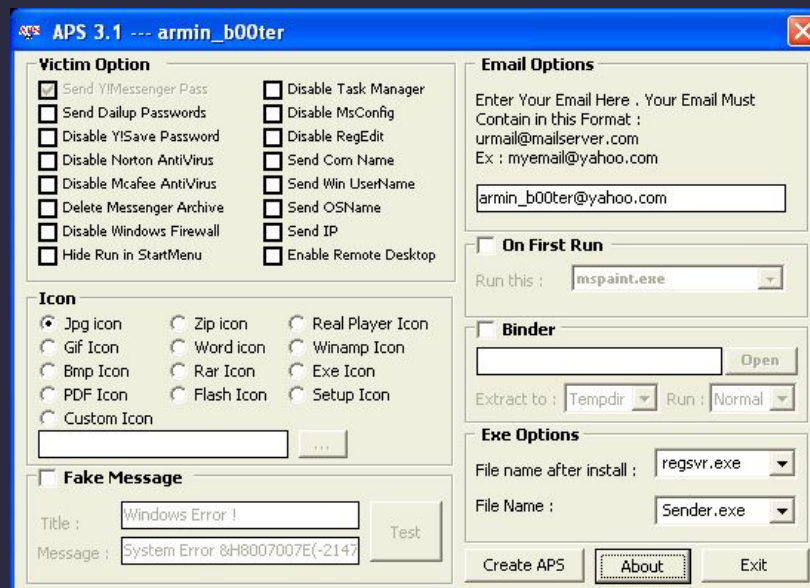
c:\WINDOWS\system32\ntoskrnl32.exe  
размером 534 кб.



```
Apocalypse TRoJAn CLiEnT by KOrUP1, deadly hackers editon
< < :: Apocalypse U2 TRoJAn CLiEnT :: >>
  deadly hackers    editon
  a world of entertainment at your
  finger tips
-----
Enter IP to connect to: _
```

# Примеры вирусов

**APS 3.1**  
**(Trojan.Win32.VB.akr)**  
Многофункциональный  
иранский троян,  
способный отключать  
различные средства  
защиты компьютера.  
Серверная часть  
состоит из одного  
файла  
c:\WINDOWS\system32\  
regsvr.exe размером  
23,203 байт.



# Признаки, указывающие на поражение программ вирусом:

- *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 и т.д.*



# Антивирусные программы



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

Антивирусное программное обеспечение состоит из подпрограмм, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другое вредоносное программное обеспечение.

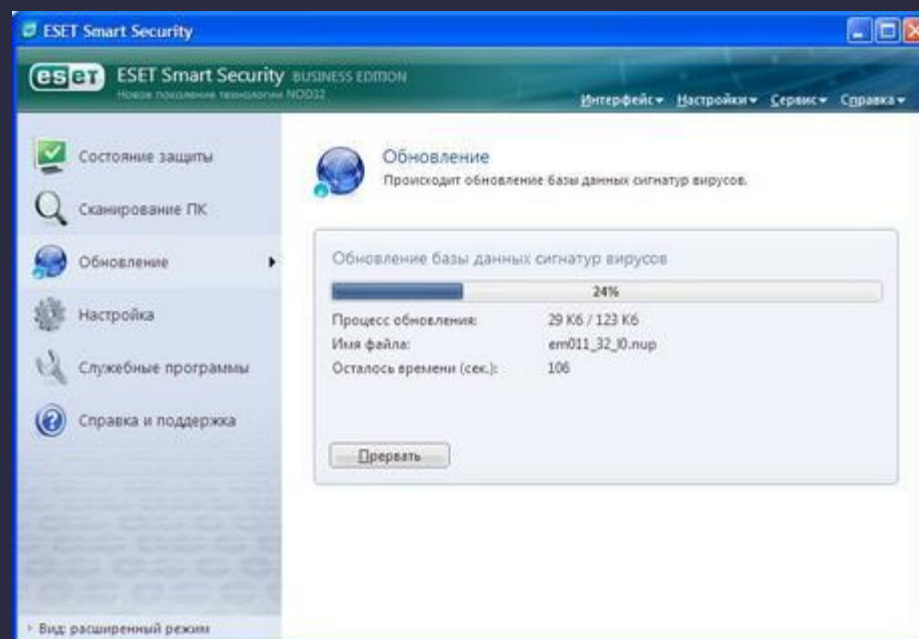


# Антивирусные программы

- [NOD 32](#)
- [Dr. Web](#)
- [Kaspersky](#)
- [Avast!](#)
- [Norton](#)
- [Panda](#)



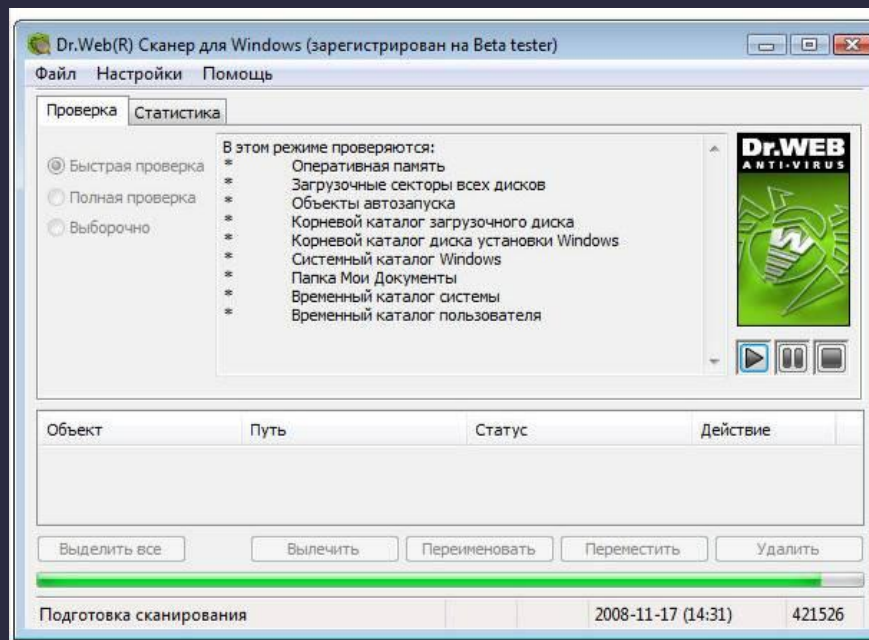
# NOD 32



<http://www.esetnod32.ru/>



# Dr. Web



<http://www.drweb.com/>



# Kaspersky Antivirus



<http://www.kaspersky.ru/>







# Norton AntiVirus

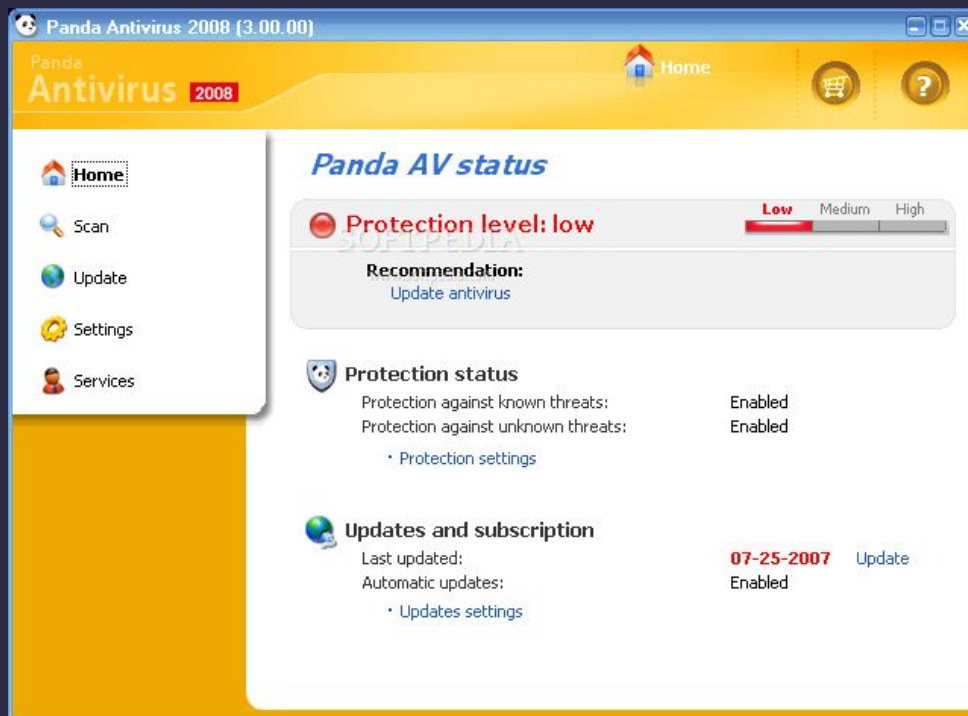


A screenshot of the Norton AntiVirus user interface. The interface is dark-themed with yellow and green accents. At the top, it says "Norton AntiVirus" and includes links for "Leave Feedback", "Norton Account", and "Help &amp; Support". A large green checkmark icon indicates the system is "Secure". Below this, there are sections for "Computer" and "Network" settings, each with a "Settings" link. The "Computer" section shows "Insight Protection", "Antivirus", "Antispyware", and "SONAR Protection", all with "On" status and information icons. The "Network" section shows "Intrusion Prevention", "Email Protection", "Browser Protection", and "Download Intelligence", also with "On" status and information icons. On the left, there are "Norton Tasks" and "Application Ratings" sections, including a bar chart comparing "CPU" (100%) and "Norton" (88%) performance. At the bottom, the Norton logo "from symantec" is visible, along with a "Learn About Web Protection" link and a trial expiration notice "Your trial period expires in 1" followed by the URL "www.izone.ru".

<http://www.symantec.com/norton/antivirus>



# Panda Antivirus



<http://www.pandasecurity.com/russia/>



# Правила защиты от компьютерных вирусов

- Регулярно тестируйте компьютер на наличие вирусов с помощью антивирусных программ
- Перед считыванием информации со съемных носителей проверяйте их на наличие вирусов
- Всегда защищайте свои носители информации от записи при работе на других компьютерах
- Делайте архивные копии ценной для вас информации
- Не используйте программы, поведение которых непонятно
- Регулярно обновляйте антивирусные программы

# Источники информации

- Компьютерные вирусы
- Компьютерный вирус
- Антивирусная программа





# Резидентность

Под термином "резидентность" (DOS'овский термин TSR - Terminate and Stay Resident) понимается способность вирусов оставлять свои копии в операционной системе, перехватывать некоторые события (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов).

Таким образом, резидентные вирусы активны не только в момент работы зараженной программы, но и после того, как программа закончила свою работу. Резидентные копии таких вирусов остаются жизнеспособными вплоть до очередной перезагрузки, даже если на диске уничтожены все зараженные файлы. Часто от таких вирусов невозможно избавиться восстановлением всех копий файлов с дистрибутивных дисков или backup-копий. Резидентная копия вируса остается активной и заражает вновь создаваемые файлы.

То же верно и для загрузочных вирусов - форматирование диска при наличии в памяти резидентного вируса не всегда вылечивает диск, поскольку многие резидентные вирусы заражают диск повторно после того, как он отформатирован.

