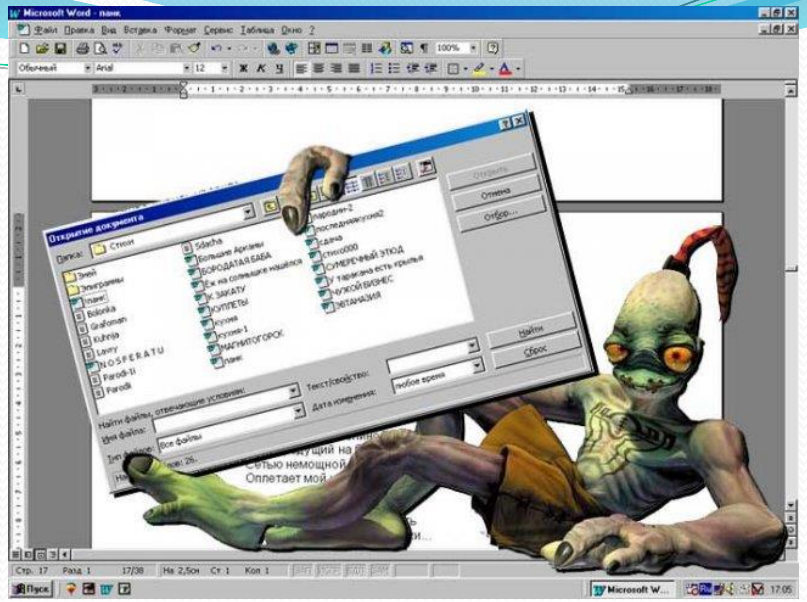
«Компьютерные вирусы и средства борьбы с ними»

Преподаватель:
Сыроватский К.Б.

Оглавление:



- Вирус
  - Что такое вирус?
  - Классификация вирусов
- Антивирусные программы
  - Что такое антивирусная программа?
  - Некоторые её параметры
  - Виды антивирусных программ

Классификация:

Что такое вирус???

- *Прежде всего, вирус – это программа, которая может «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.*

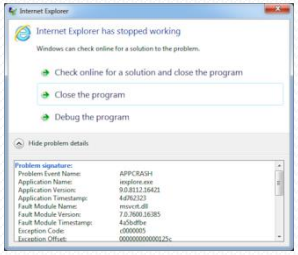
- *Активизация компьютерного вируса может вызвать уничтожение программ и данных, и даже уничтожение составляющих компьютера (системного блока).*

200 - 5000 байт

более 50 тыс. вирусов

Назад

Признаки появления вирусов:



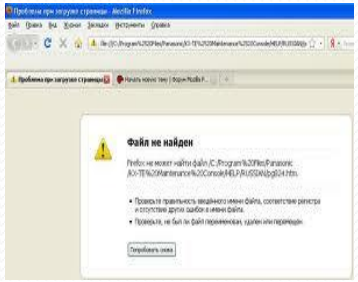
- **Неправильная работа нормально работающих программ**

- **Частые зависания и сбои в работе ПК**

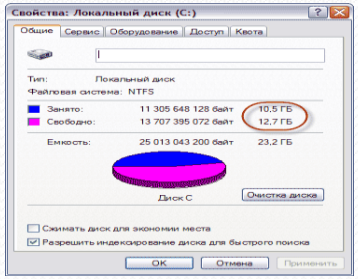
- **Медленная работа ПК**

- **Изменение размеров файлов**

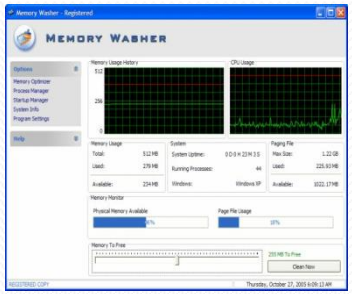
Признаки появления вирусов:



- Исчезновение файлов и каталогов

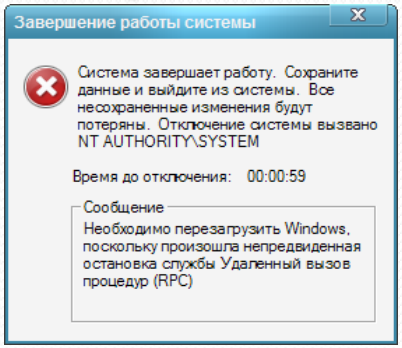


- Неожиданное увеличение количество файлов на диске

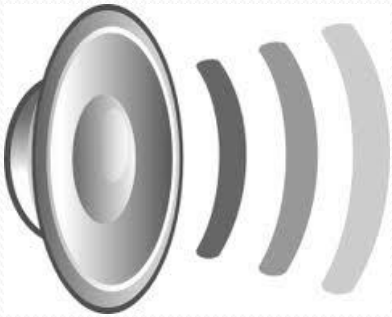


- Уменьшение размеров свободной оперативной памяти

Признаки появления вирусов:



- ***Вывод на экран неожиданных сообщений и изображений***



- ***Подача непредусмотренных звуковых сигналов***

- ***Невозможность загрузки Операционной Системы***

Что заражают вирусы?

Для того, чтобы вирус смог выполнить какие-то действия, он должен оказаться в памяти в виде **программного кода** и получить управление.

Вирусы

заражают

- программы – `*.exe, *.com`
- загрузочные сектора дисков и дискет
- командные файлы – `*.bat`
- драйверы – `*.sys`
- библиотеки – `*.dll`
- документы с макросами – `*.doc, *.xls, *.mdb`
- *Web*-страницы со скриптами

не заражают

- текст – `*.txt`
- рисунки – `*.gif, *.jpg, *.png, *.tif`
- звук (`*.wav, *.mp3, *.wma`)
- видео (`*.avi, *.mpg, *.wmv`)
- любые данные (без программного кода)

Стоимость нанесенного вреда

КЛАССИФИКАЦИЯ ВИРУСОВ

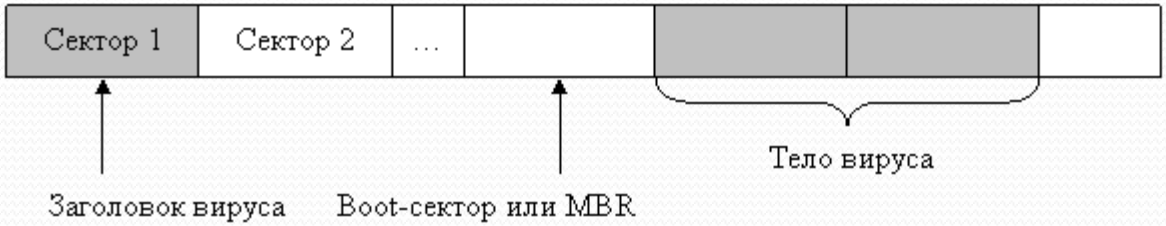
- Загрузочные вирусы
- Файловые вирусы
- Макро-вирусы
- Сетевые вирусы

Назад

Загрузочные вирусы

заражают загрузочный сектор гибкого диска или винчестера.

При заражении дисков загрузочный вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не программному коду загрузчика операционной системы, а коду вируса.



Назад

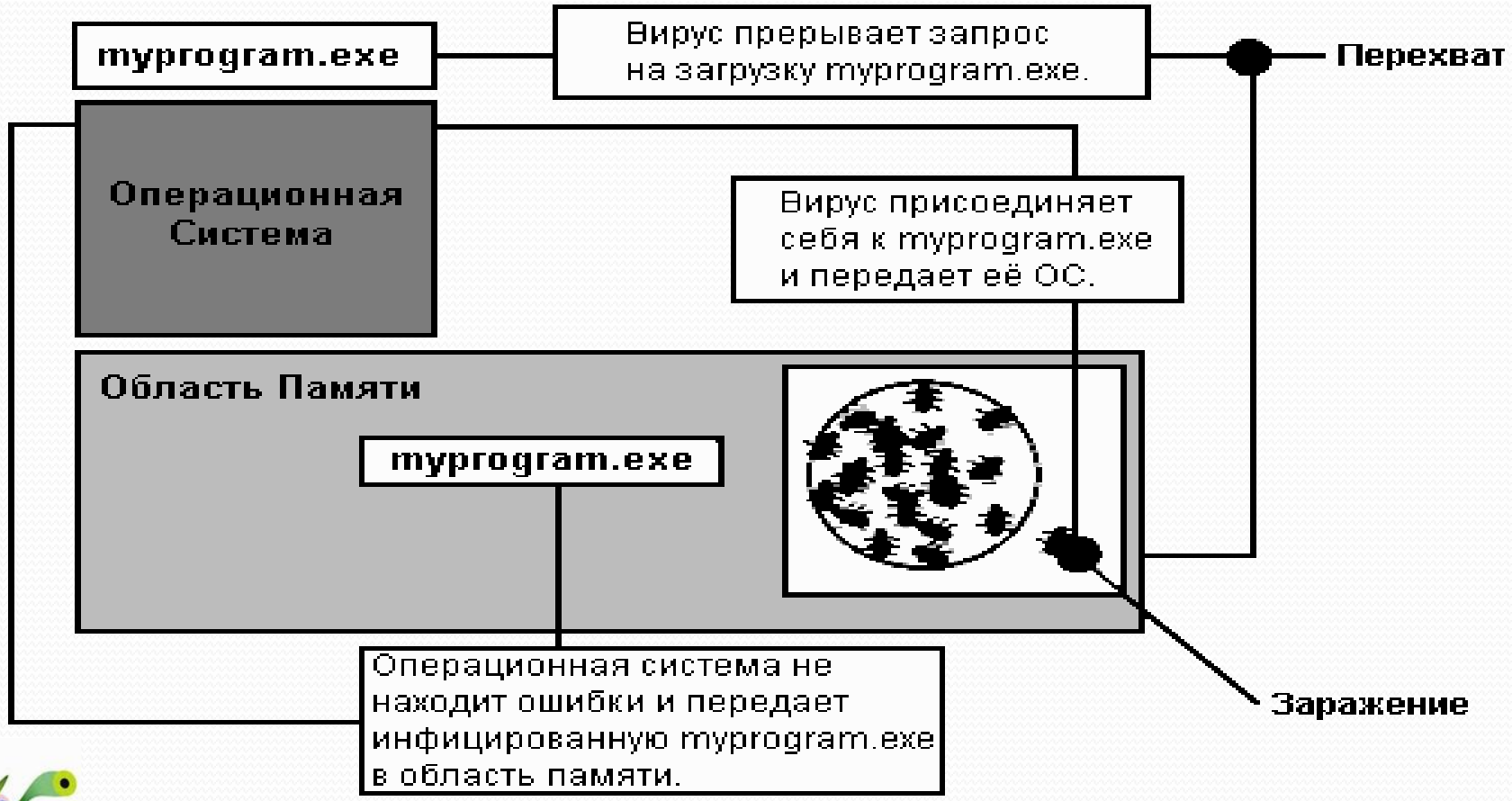
Файловые вирусы

при своем размножении тем или иным способом используют файловую систему операционной системы.

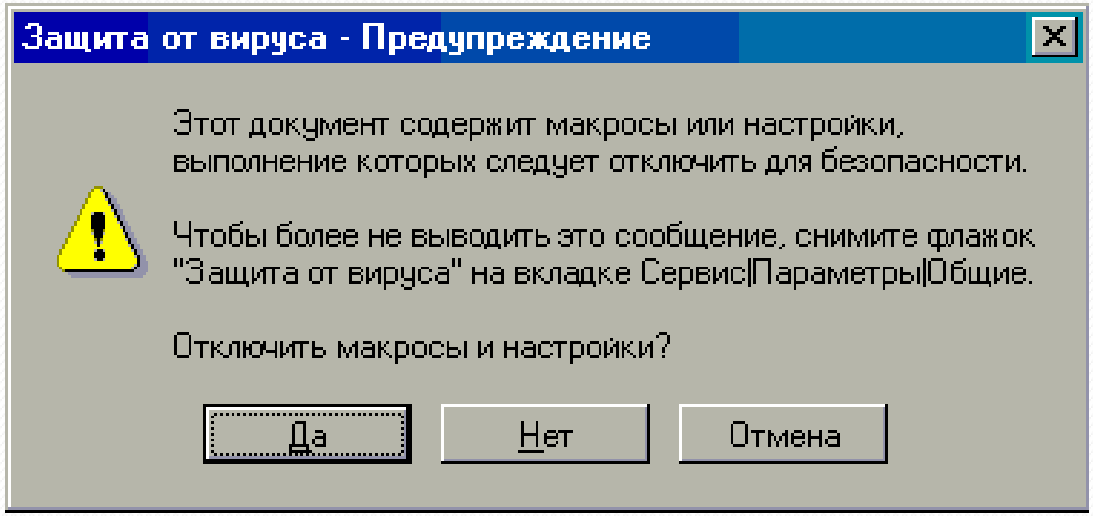
Файловые вирусы могут поражать исполняемые файлы различных типов (EXE, COM, BAT, SYS и др.).

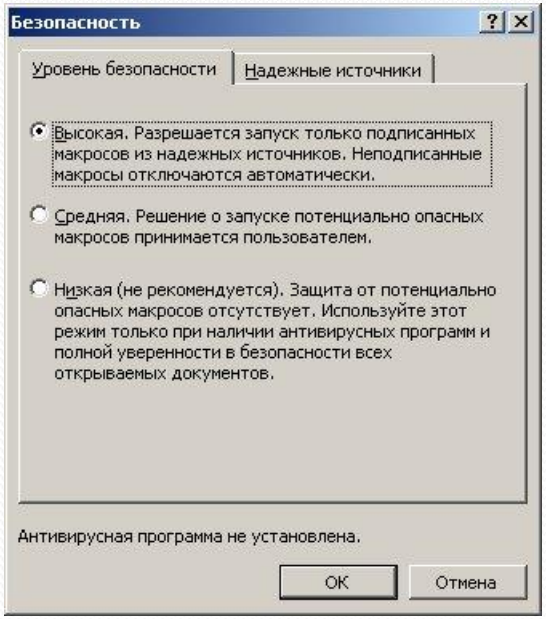
Назад

Загрузка программы в присутствии файлового вируса



Макровирусы





Являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).

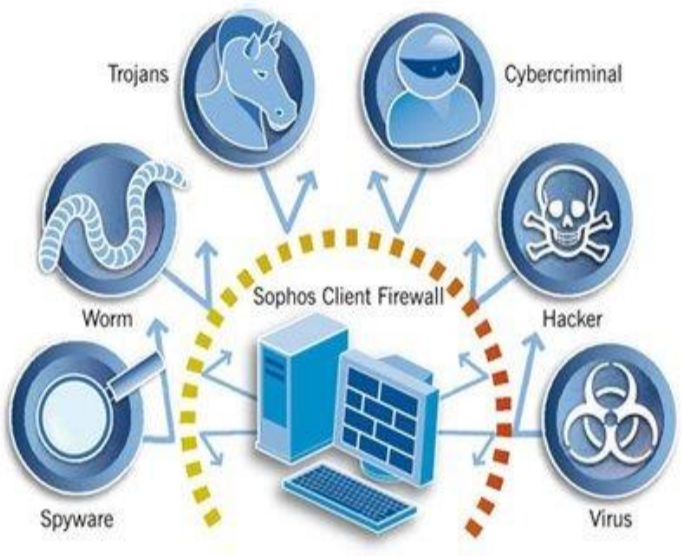
Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Назад

Сетевые вирусы

Для своего распространения используют протоколы и возможности локальных и глобальных компьютерных сетей.

Основным принципом работы сетевых вирусов является возможность передать и запустить свой код на удаленном компьютере.

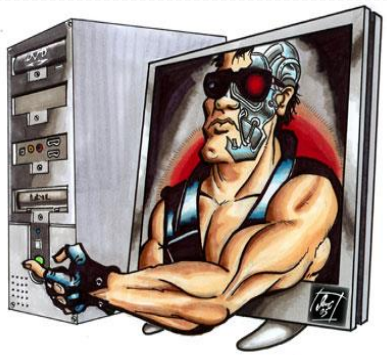


Назад

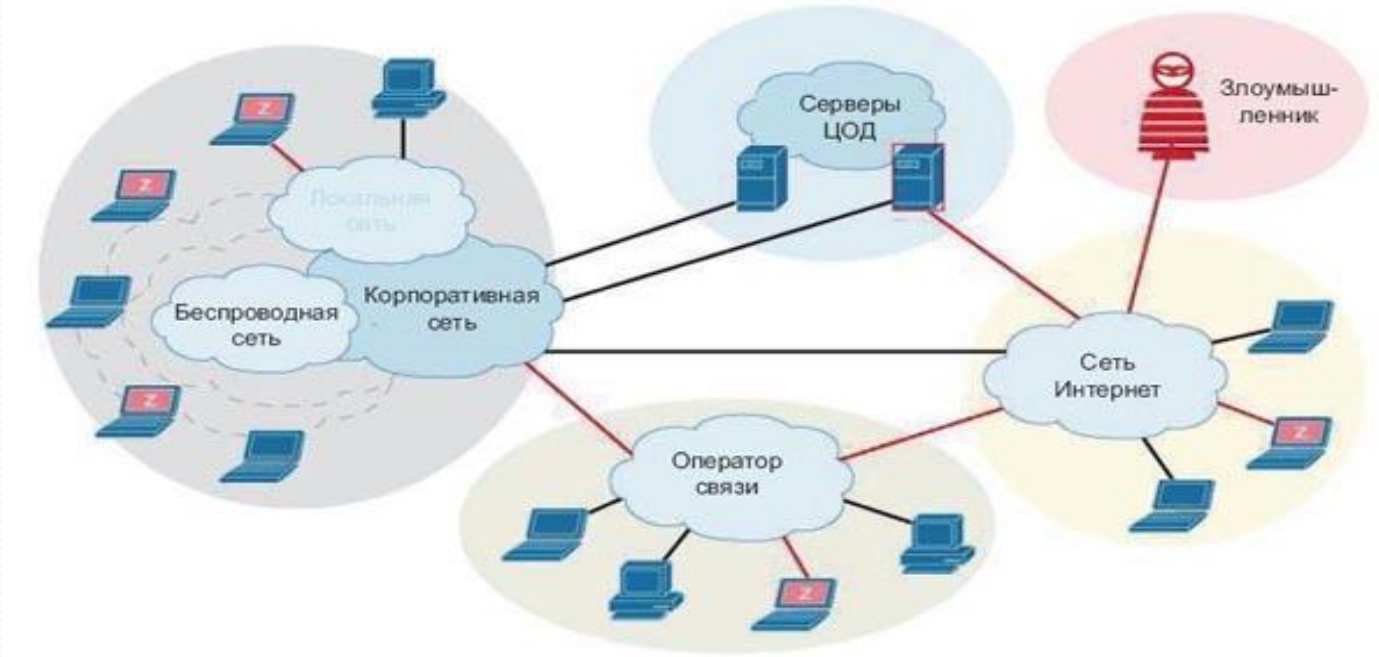
Вирусы делятся также на резидентные и нерезидентные

Первые, в отличие от нерезидентных, при получении управления загружаются в память и могут действовать не только во время работы зараженного файла.

Дополнительные типы вирусов



Зомби (Zombie) - это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры.



Хакерские утилиты и прочие вредоносные программы

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

Каналы распространения

- ***Флеш-накопители (флешки)***
- ***Электронная почта***
- ***Системы обмена мгновенными сообщениями***
- ***Веб-страницы***

АНТИВИРУСНЫЕ ПРОГРАММЫ

- *Антивирусные блокировщики*
- *Ревизоры*
- *Полифаги*
- *Полифаги-мониторы*

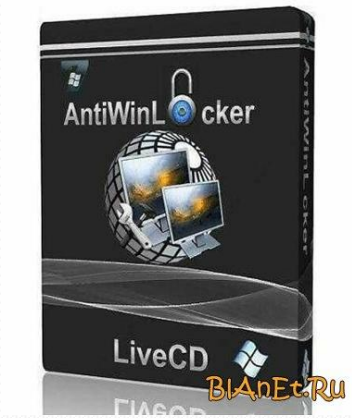
Назад

Задумайся о защите:

AntiWinLocker

Антивирусные блокировщики

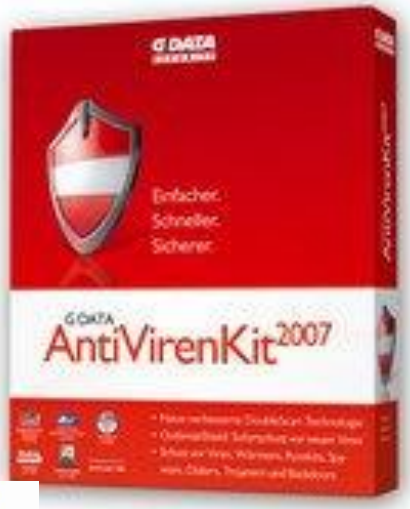
резидентные программы, которые перехватывают «вирусоопасные» ситуации и сообщают об этом пользователю. Например, «вирусоопасной» является запись в загрузочные сектора дисков, которую можно запретить с помощью программы BIOS Setup



Назад

Ревизоры

Принцип работы ревизоров основан на подсчете контрольных сумм для хранящихся на диске файлов.



Назад

Полифаги

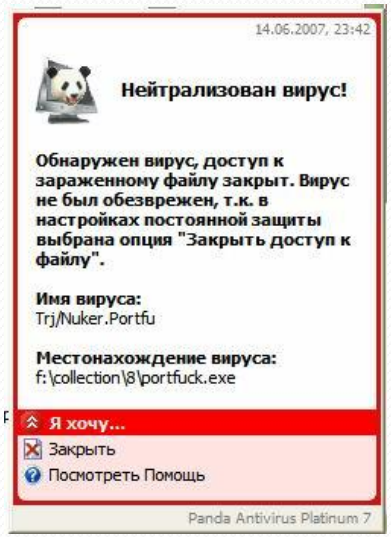
Принцип работы полифагов основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных полифагу) вирусов.

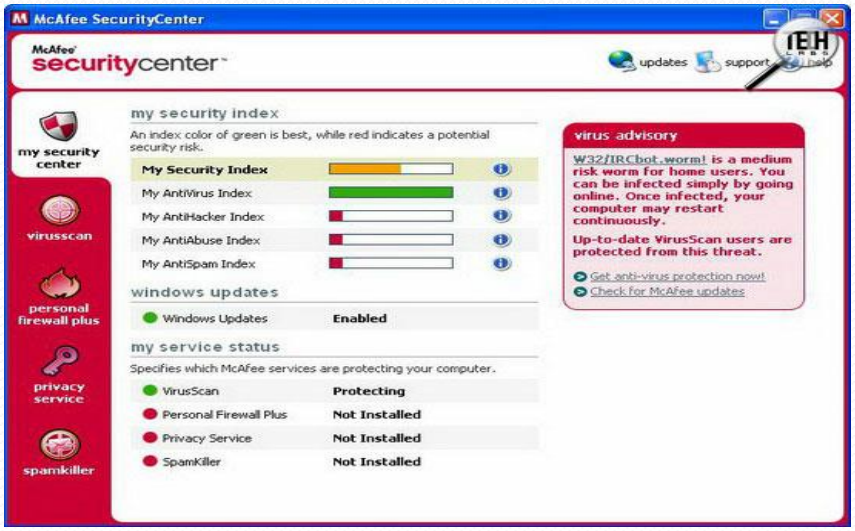
Назад

Полифаги-мониторы

постоянно находятся в оперативной памяти компьютера и проверяют все файлы в реальном режиме времени.

Полифаги-сканеры производят проверку системы по команде пользователя.





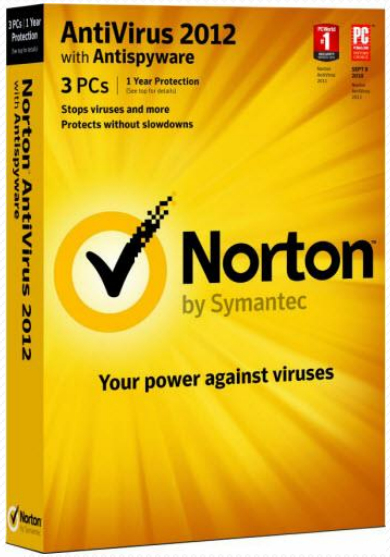
Назад

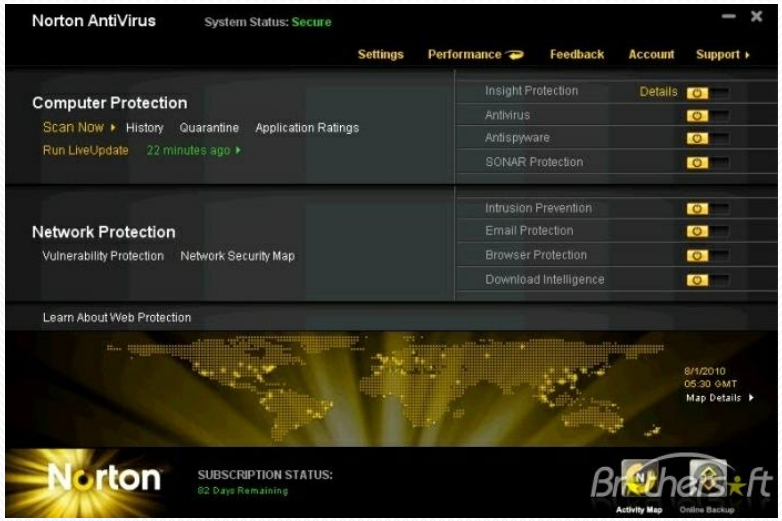
Краткий обзор антивирусных программ

Norton AntiVirus

by: invetalcom

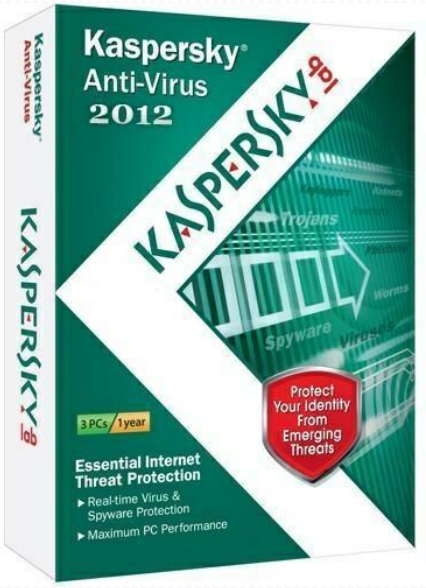
Один из известных и популярных антивирусов. Процент распознавания вирусов очень высокий (близок к 100%).

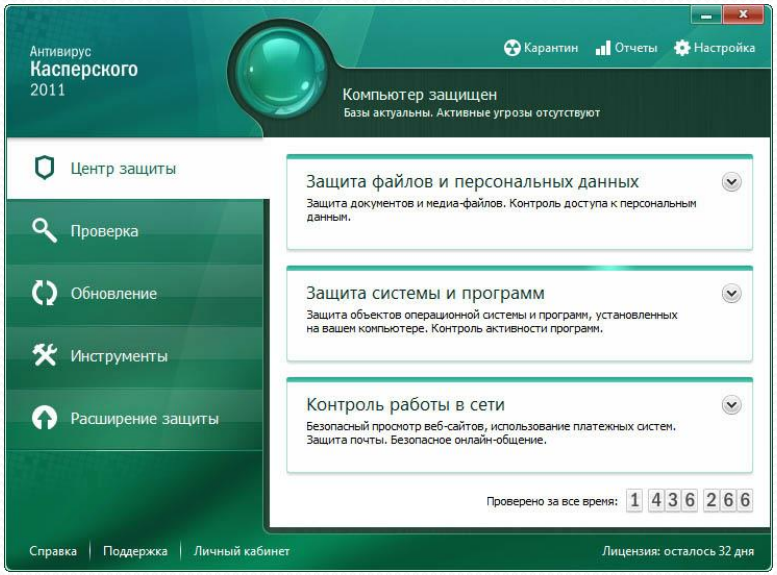




Kaspersky

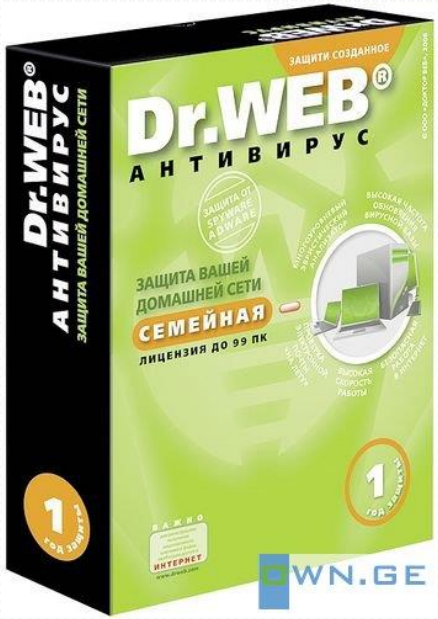
Антивирус Касперского 2012 — это решение для базовой защиты компьютера от вредоносных программ. Продукт обеспечивает защиту в режиме реального времени от основных информационных угроз — как известных, так и новых.





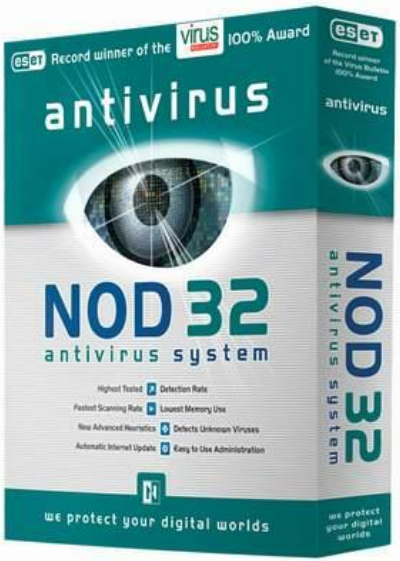
DrWeb

Популярный отечественный антивирус. Хорошо распознает вирусы, но в его базе их меньше чем у других антивирусных программ



Eset NOD32

Простое и надежное решение для базовой защиты домашнего компьютера от вирусов, червей, троянских программ, шпионского, рекламного и потенциально опасного ПО, руткитов и фишинг-атак



Репортаж о вирусах

Видео в Интернете