

ЗАЩИТА ИНФОРМАЦИИ,
АНТИВИРУСНАЯ ЗАЩИТА.



КОМПЬЮТЕРНЫЙ ВИРУС

программа способная самопроизвольно внедряться и внедрять свои копии в другие программы, файлы, системные области компьютера и в вычислительные сети, с целью создания всевозможных помех работе на компьютере.

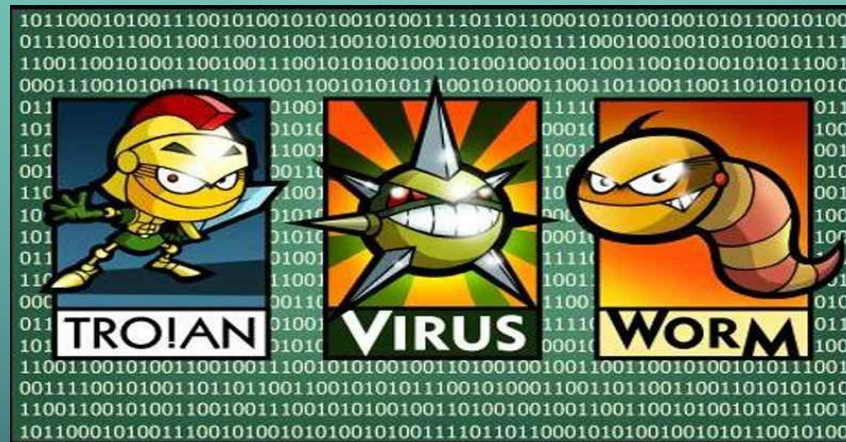


ПРИЗНАКИ ЗАРАЖЕНИЯ:

- прекращение работы или неправильная работа ранее функционировавших программ
- медленная работа компьютера
- невозможность загрузки ОС
- исчезновение файлов и каталогов или искажение их содержимого
- изменение размеров файлов и их времени модификации
- уменьшение размера оперативной памяти
- непредусмотренные сообщения, изображения и звуковые сигналы
- частые сбои и зависания компьютера и др.



КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ



ПО СРЕДЕ ОБИТАНИЯ:

- *Сетевые* – распространяются по различным компьютерным сетям
- *Файловые* – внедряются в исполняемые модули (COM, EXE)
- *Загрузочные* – внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска
- *Фалово-загрузочные* – внедряются и в загрузочные сектора и в исполняемые модули

По способу заражения:

- *Резидентные* – при заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения
- *Нерезидентные* – не заражают оперативную память и активны ограниченное время

По воздействию:

- *Неопасные* – не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках
- *Опасные* – приводят к различным нарушениям в работе компьютера
- *Очень опасные* – могут приводить к потере программ, данных, стиранию информации в системных областях дисков

По особенностям алгоритма:

- *Паразиты* – изменяют содержимое файлов и секторов, легко обнаруживаются
- *Черви* – вычисляют адреса сетевых компьютеров и отправляют по ним свои копии
- *Стелсы* – перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области
- *Мутанты* – содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую
- *Трояны* – не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему



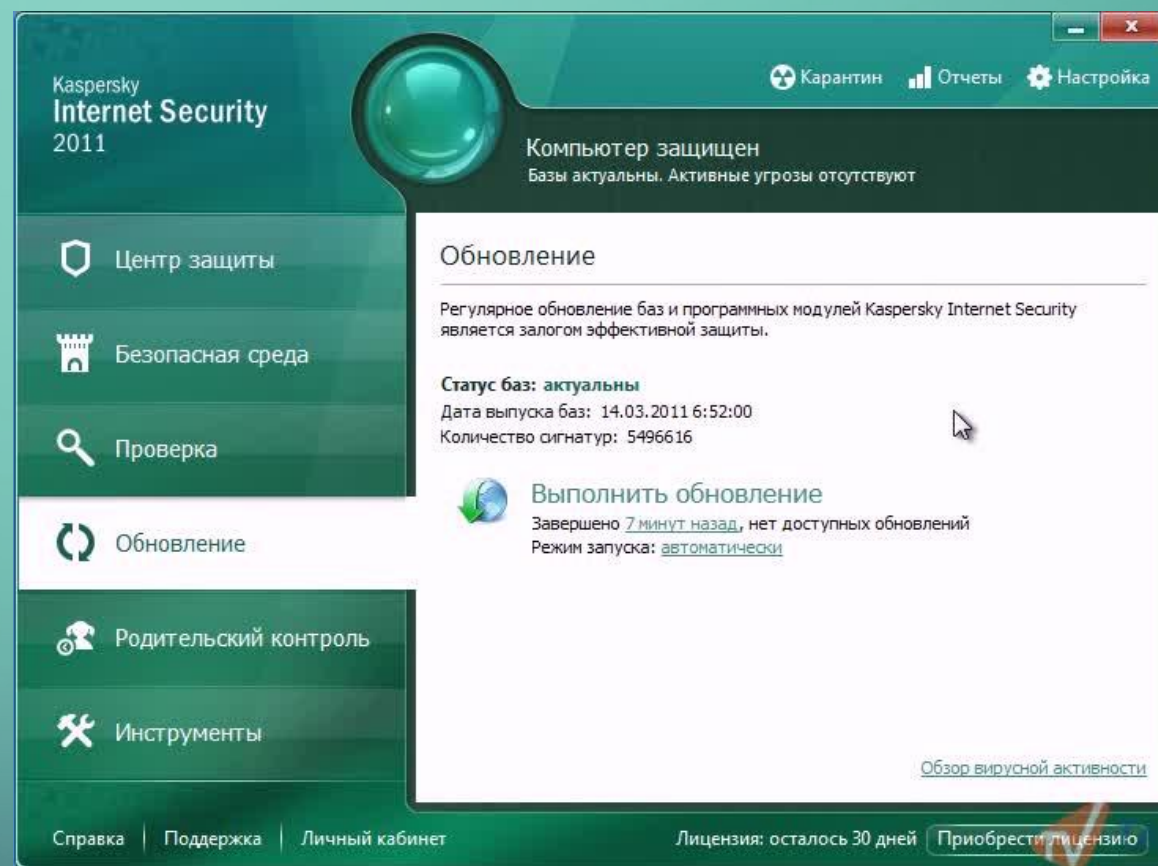
ОСНОВНЫЕ МЕРЫ ПО ЗАЩИТЕ ОТ ВИРУСОВ



Оснастите свой компьютер одной из современных антивирусных программ: Doctor Weber, Norton Antivirus, AVG, Kaspersky.



Постоянно обновляйте антивирусные базы



Делайте архивные копии ценной для Вас информации (гибкие диски, CD)



КЛАССИФИКАЦИЯ АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Сканеры (детекторы). Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов.



Мониторы. Это целый класс антивирусов, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. С помощью монитора можно остановить распространение вируса на самой ранней стадии.

Ревизоры. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Для определения наличия вируса в системе программы-ревизоры проверяют созданные ими образы и производят сравнение с текущим состоянием





СПАСИБО ЗА ВАШЕ
ВНИМАНИЕ

