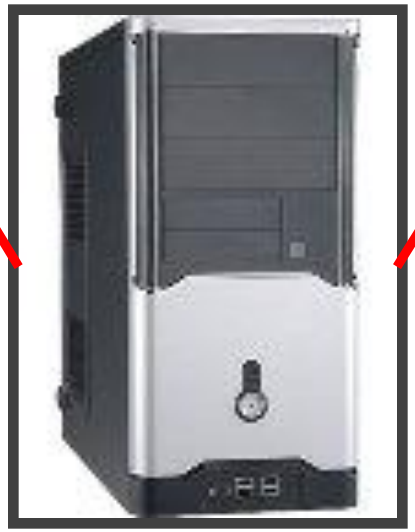
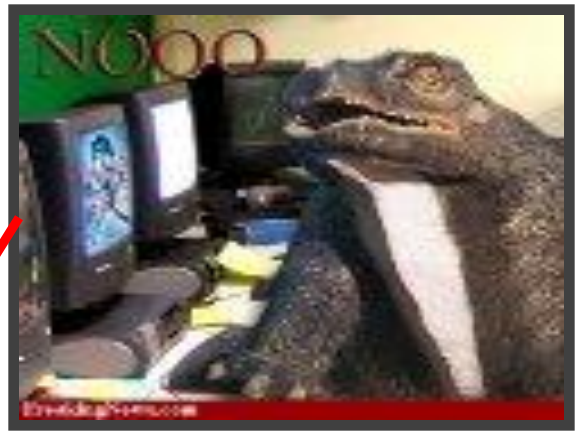
Компьютерные вирусы и антивирусные программы

Компьютерный вирус – *это* небольшая ***программа,*** способная записывать свои копии в компьютерные программы, расположенные в исполняемых файлах, драйверах или «поселяется» в загрузочном секторе диска, причем эти копии сохраняют возможность к «размножению».





Проявление вирусов:

- сильное замедление работы компьютера;
- неожиданное появление на экране посторонних фраз;
- появление различных видеоэффектов;
- пропадание информации с экрана;
- генерация различных звуков;
- некоторые программы перестают работать, а другие ведут себя очень странно;
- на дисках появляется большое количество испорченных файлов данных, текстовых файлов;
- рушится вся файловая система на одном из дисков;
- произвольно изменяется длина отдельных файлов;
- невозможность загрузки операционной системы;
- изменение даты и времени модификации файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- частые зависания и сбои в работе компьютера.

Авторы: Кто и почему ?

1 группа: студенты и школьники, которые только что изучили язык программирования, хотели попробовать свои силы, но не смогли найти для них более достойного применения.

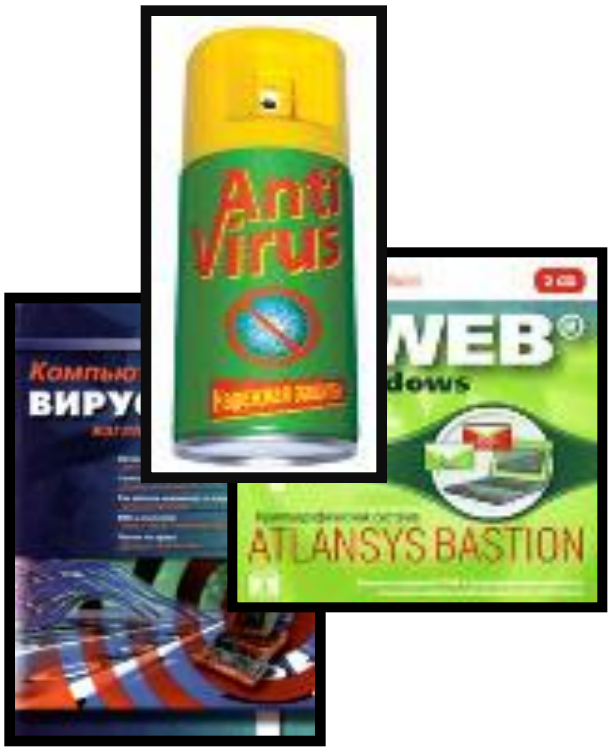
2 группа: наиболее опасная, которая создает и запускает в мир «профессиональные» вирусы. Эти тщательно продуманные и отлаженные программы создаются профессиональными, часто очень талантливыми программистами.

3 группа: «исследователи», довольно сообразительные программисты, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т. д.

4 группа: хакеры-одиночки или группы хакеров.

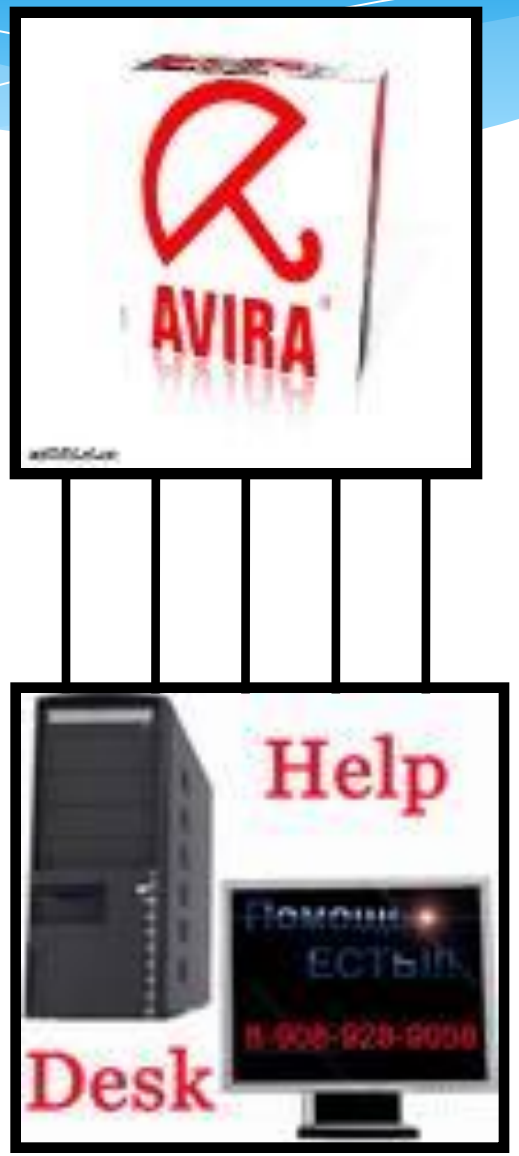
Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются ***антивирусными***.
Различают следующие виды антивирусных программ:

- ***программы-детекторы;***
- **программы-доктора или фаги;**
- ***программы-ревизоры;***
- **программы-фильтры;**
- ***программы-вакцины или иммунизаторы.***



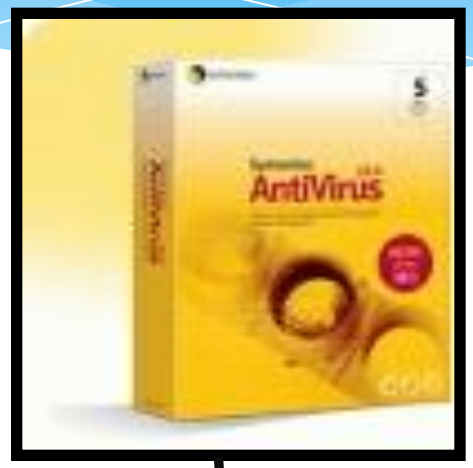
Программы-детекторы

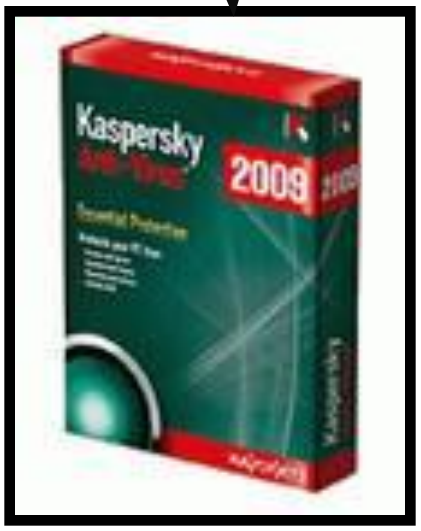
-осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.



Программы-доктора или фаги, а также программы-вакцины

-не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов



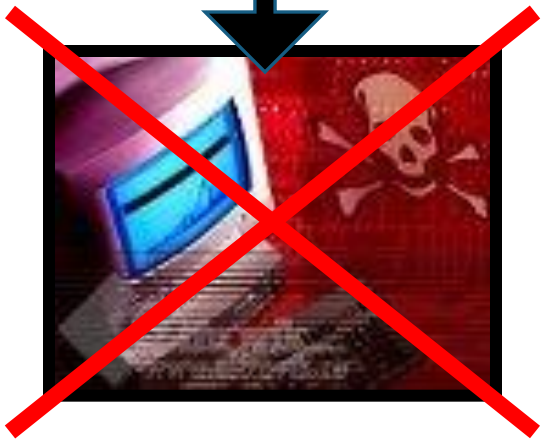


Программы-ревизоры

- относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы

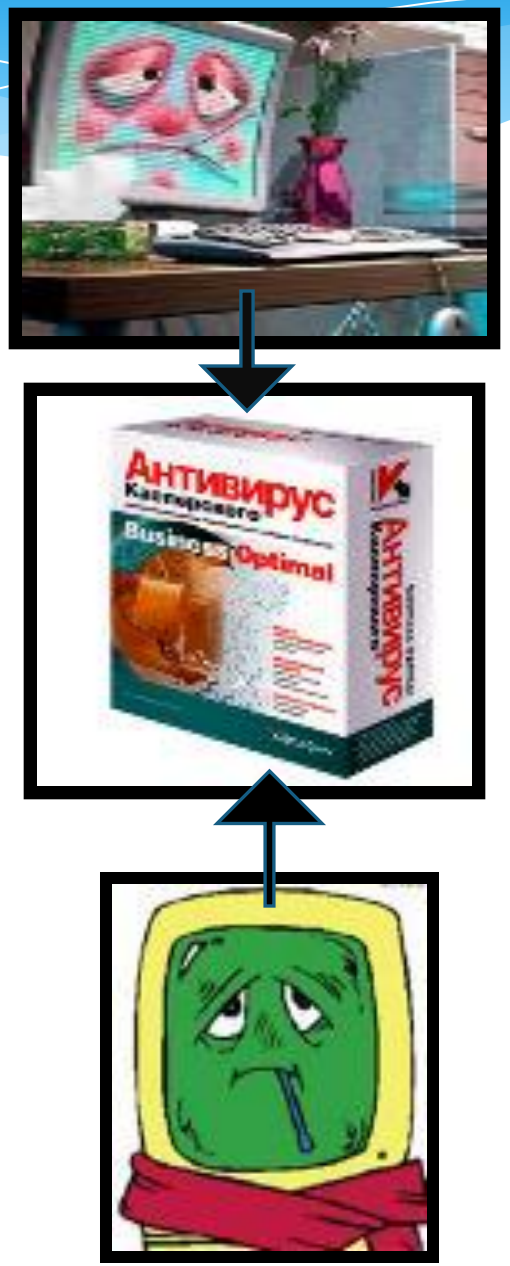
Программы-фильтры или «сторожа»

- представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако, они не «лечат» файлы и диски.



Вакцины или иммунизаторы

- это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.



Основные меры по защите от вирусов

(памятка пользователю)

- **Оснастите свой компьютер современными антивирусными программами и постоянно обновляйте их версии**
- **Перед считыванием информации с носителей, записанной на других компьютерах, всегда проверяйте их на наличие вирусов**
- **При переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске**
- **Периодически проверяйте на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков**
- **Обязательно делайте архивные копии ценной для вас информации**
- **Используйте антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей**