

Компьютерные вирусы.

Антивирусные программы.



Компьютерные вирусы

- 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.



Виды компьютерных вирусов

- Червь,
Троянская программа (троянский конь, троян),
Программы – шпионы,
Зомби,
Программы – блокировщики
(баннеры)

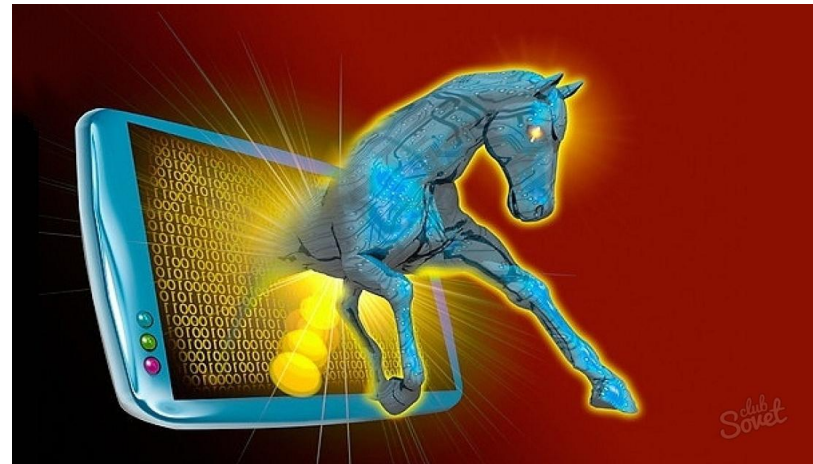
Червь

- Червь – программа, которая делает копии самой себя. Ее вред заключается в захламлении компьютера, из-за чего он начинает работать медленнее. Отличительной особенностью червя является то, что он не может стать частью другой безвредной программы.



Троянская программа (троянский конь, троян)

- Троянская программа маскируется в других безвредных программах. До того момента как пользователь не запустит эту самую безвредную программу, троян не несет никакой опасности. Троянская программа может нанести различный ущерб для компьютера. В основном трояны используются для кражи, изменения или удаления данных. Отличительной особенностью трояна является то, что он не может самостоятельно размножаться.

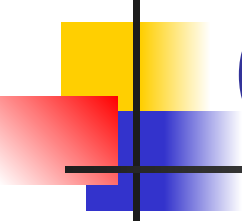




Зомби

- Зомби позволяют злоумышленнику управлять компьютером пользователя. Компьютеры – зомби могут быть объединены в сеть и использоваться для массовой атаки на сайты или рассылки спама. Пользователь может не догадываться, что его компьютер зомбирован и используется злоумышленником

Программы – блокировщики (баннеры)



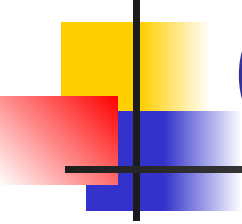
- Это программа, которая блокирует пользователю доступ к операционной системе. При загрузке компьютера появляется окно, в котором пользователя обвиняют в скачивание нелицензионного контента или нарушение авторских прав. И под угрозой полного удаления всех данных с компьютера требуют отослать смс на номер телефона или просто пополнить его счет. Естественно после того как пользователь выполнит эти требования банер никуда не исчезнет.

Программы – шпионы

- Шпионы собирают информацию о действиях и поведении пользователя. В основном их интересует информация (адреса, пароли).



Антив́ирусная програ́мма (антив́ирус)



- — 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.

Виды антивирусных программ

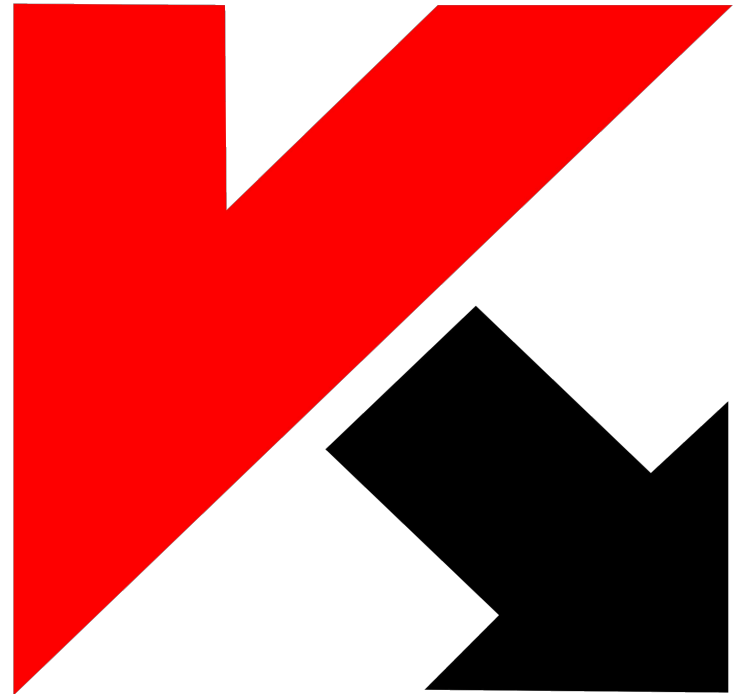


- — программы-детекторы;
- программы-доктора, или фаги;
- программы-ревизоры;
- программы-фильтры;
- программы-вакцины, или иммунизаторы.



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

- 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. Среди фагов выделяют полифаги, т. е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

Dr.WEB®





Программы-ревизоры

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. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом



AVIRA AntiVir®



Программы-фильтры

- представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов



Вакцины или иммунизаторы

- 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.