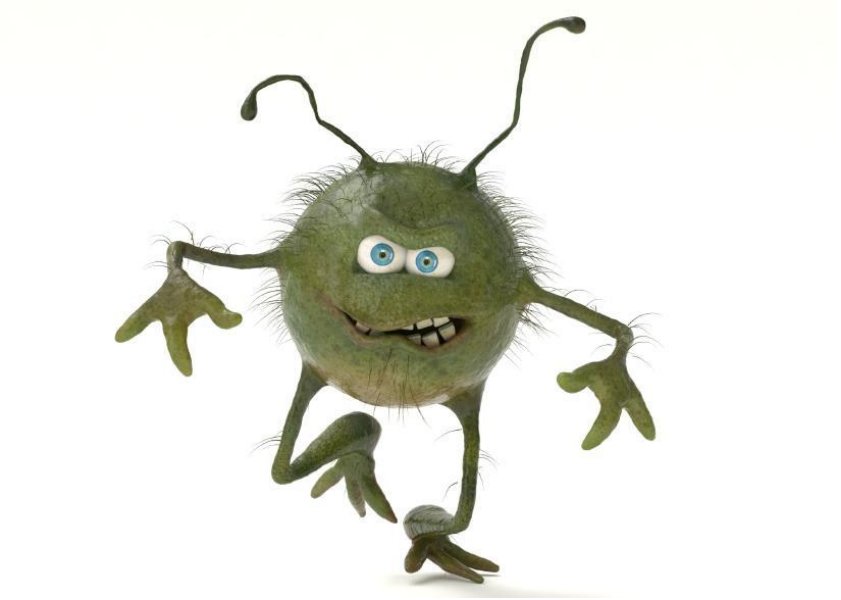
Компьютерные вирусы

Антивирусные программы

Работу выполнила:
ученица ГБОУ СОШ №10
10 класса
Гусенкова Мария

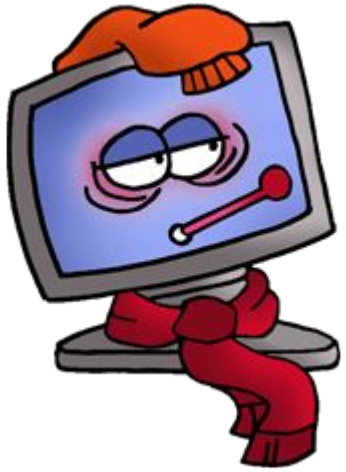
Компьютерные вирусы-

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.



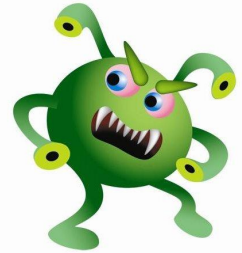
Цель вируса

является нарушение работы программно-аппаратных комплексов:



- удаление файлов
- приведение в негодность структур размещения данных
- блокирование работы пользователей
- приведение в негодность аппаратных комплексов компьютера

Признаки того, что



заразил ваш компьютер:

- Программы стали загружаться медленнее.
- Файлы появляются или исчезают.
- Размер программы или объекта изменяются по непонятным причинам.
- На экране появляется необычный текст или изображения.
- Элементы экрана выглядят нечеткими, размытыми.
- Сам по себе уменьшается объем свободного места на жестком диске.
- Команды CHKPSK и SCANDISK возвращают некорректные значения.
- Имена файлов изменяются без видимых причин.
- Нажатия клавиш сопровождаются странными звуками.
- Доступ к жесткому диску запрещен.

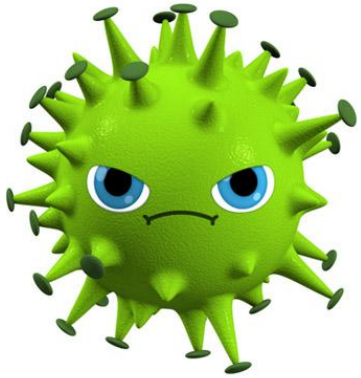
Какие же бывают вирусы…

Червь (программа, которая делает копии самой себя. Ее вред заключается в захламлении компьютера, из-за чего он начинает работать медленнее.)

Троянская программа (маскируется в других безвредных программах. Троянская программа может нанести различный ущерб для компьютера. В основном трояны используются для кражи, изменения или удаления данных.)

Программы – шпионы (собирают информацию о действиях и поведении пользователя. В основном их интересует информация (адреса, пароли).)

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) (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.)

Вредоносная программа (Malware) (любое программное обеспечение, созданное для получения несанкционированного доступа к компьютеру и его данным, с целью хищения информации или нанесению вреда. Термин “Вредоносная программа” можно считать общим для всех типов компьютерных вирусов, червей, троянских программ и тд.)

Как же защитить свой компьютер от вирусов?

Антивирусные программы-

любая 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) файло

в или операци-онной системы вредоносным кодом.

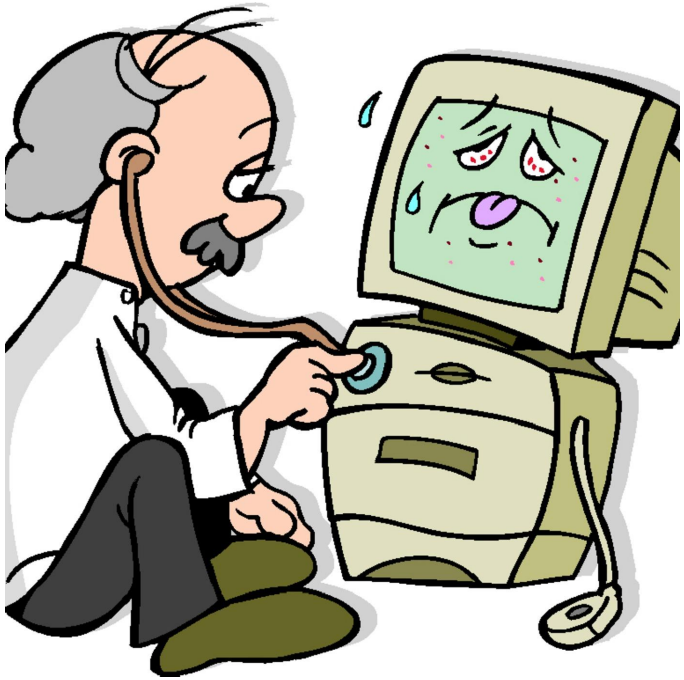
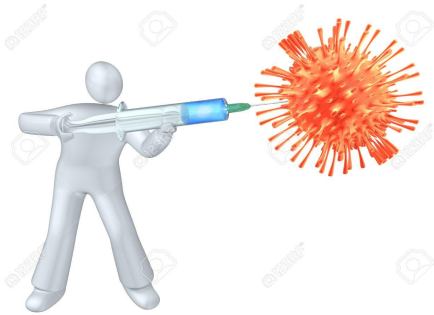


Схема действий антивируса:

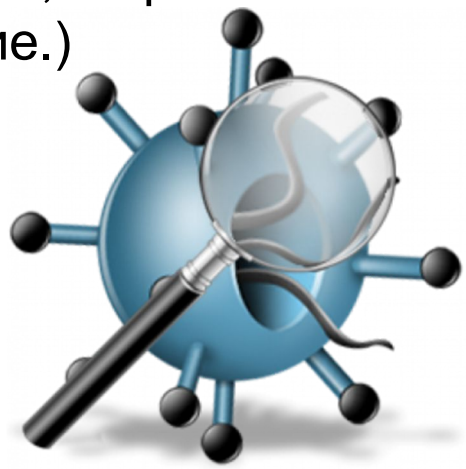
- поиск в базе данных антивирусного ПО сигнатур вирусов.
- если найден инфицированный код в памяти (оперативной и/или постоянной), запускается процесс «карантина», и процесс блокируется.
- зарегистрированная программа обычно удаляет вирус, незарегистрированная просит регистрации и оставляет систему уязвимой.

Классификация антивирусов

Вакцины (программы, предназначенные для предотвращения заражения файлов от какого-либо одного, конкретного вируса. Вакцины применяются, если отсутствуют программы, способные обезвредить данный вирус.)



«Детекторы» или **«сканеры»** (программы, которые осуществляют поиск характерной для конкретного вируса сигнатуры, в оперативной памяти компьютера или в файлах на жестком диске, и при обнаружении, выдают соответствующее сообщение.)



«Ревизоры» (программы, которые относятся к самым надёжным средствам защиты от вирусов. Они построены на принципе, обратном принципу построения сканеров. Ревизоры не знают в лицо конкретные вирусы, но они запоминают информацию о каждом конкретном логическом диске и по изменению этой информации, позволяют надежно обнаруживать как известные, так и новые, неизвестные вирусы.)

«Сторожа» (небольшие резидентные программы, предназначенные для обнаружения подозрительных действий, возникающих при работе пользователя на компьютере, и характерных для вирусов.)

«Мониторы» (или программы-фильтры) (антивирусные программы, основанные по принципу полифага, и использующие для обнаружения вирусов базу данных их сигнатур. Антивирусный монитор располагается резидентно в памяти компьютера, и проверяет на наличие вирусов только те программы, над которыми производит какие-либо манипуляции пользователь, или операционная система.)

«Полифаги» (программы, которые способны благополучно удалить вирус и восстановить работоспособность испорченных программ.)

Эвристические анализаторы (программы, выполняющие под своим контролем, проверяемые программы и обнаруживающие действия, характерные для вирусов.)

Какие же антивирусные программы выбрать?

На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене (от весьма дорогих до абсолютно бесплатных), так и по своим функциональным возможностям. Наиболее мощные (и как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способных при совместном их использовании поставить заслон практически любому виду зловредных программ.

Какие функции они должны выполнять:

- сканирование памяти и содержимого дисков;
- сканирование в реальном режиме времени с помощью резидентного модуля;
- распознавание поведения, характерного для компьютерных вирусов;
- блокировка и/или удаление выявленных вирусов;
- восстановление зараженных информационных объектов;
- принудительная проверка подключенных к корпоративной сети компьютеров;
- удаленное обновление антивирусного программного обеспечения и баз данных через Интернет;
- фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;
- выявление потенциально опасных Java-апплетов и модулей ActiveX;
- ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты.

Наиболее мощные и популярные в России антивирусные пакеты:

Антивирус NOD32

Очень быстро работающая антивирусная программа, эффективно защищающая от всех видов вирусов и "шпионских" программ. NOD32 обладает всеми возможностями, характерными для современных средств защиты компьютера, причем по некоторым очень важным параметрам NOD32 превосходит абсолютное большинство популярных антивирусных программ.

Антивирус Касперского

Антивирус Касперского - одна из популярнейших и наиболее качественных антивирусных программ. За счет специального алгоритма работы у нее очень высокий процент определения вирусов, в том числе и еще не известных.

Антивирус Dr.Web

Доктор Веб - одна из самых известных и популярных отечественных антивирусных программ. Имеет эвристический анализатор, позволяющий с большой долей вероятности обнаруживать неизвестные вирусы.

Norton AntiVirus

Norton AntiVirus - одна из самых известных в мире антивирусных программ. Производится американской компанией Symantec. Данный антивирус находит и удаляет вирусы и программы-шпионы, автоматически блокирует программы-шпионы, не позволяет рассылать зараженные письма, автоматически распознает и блокирует вирусы, программы-шпионы и троянские компоненты, обнаруживает угрозы, скрытые в операционной системе, выполняет функцию защиты от интернет-червей, функцию просмотра электронной почты.

Panda Antivirus

Panda Antivirus делает защиту вашего ПК максимально простой: антивирус автоматически блокирует и уничтожает все типы вирусов и шпионов, так что можно пользоваться Интернетом и электронной почтой без риска для безопасности.

McAfee VirusScan AsaP

McAfee VirusScan AsaP - средство защиты от вирусов, представляющее собой удобное решение для всех пользователей персональных компьютеров, желающих снять с себя бремя борьбы с вирусами. Новая версия этого антивируса защищает от антивирусных атак не только настольные компьютеры, но и серверы.

Антивирус Avast!

Антивирус Avast! содержит все возможности, которые необходимы профессиональной антивирусной программе. Он имеет простой пользовательский интерфейс, подходящий для новичков или неопытных пользователей, он также имеет расширенный интерфейс (доступен только в версии Professional Edition), который даёт возможность пользователю, обращаться к любой настройке и полностью контролировать Avast!

Спасибо за внимание!

"Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/"