МБОУ СОШ с.Петровское

Вирусы и Антивирусные программы

Подготовила:
Левашова Инга Александровна,
социальный педагог

***Петровское**, 2016*

Компьютерный вирус —

специально созданная компьютерная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии, внедрять их в файлы с целью нарушения работы других программ, порчи файлов и каталогов.

Признаки появления вирусов:

- неправильная работа программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов;
- изменение размеров файлов;
- неожиданное увеличение количества файлов на диске;
- уменьшение размеров свободной операционной памяти;
- вывод на экран неожиданных сообщений и изображений;
- подача непредусмотренных звуковых сигналов;
- частые «зависания» и сбои в работе компьютера.

Вирусы могут распространяться через:

- исполняемые программы;
- документы *Word, Excel;*
- программное обеспечение компьютера;
- *web*-страницы;
- файлы из Интернета;
- письма *e-mail;*
- дискеты и компакт-диски.

Классификация вирусов по масштабу вредных воздействий:

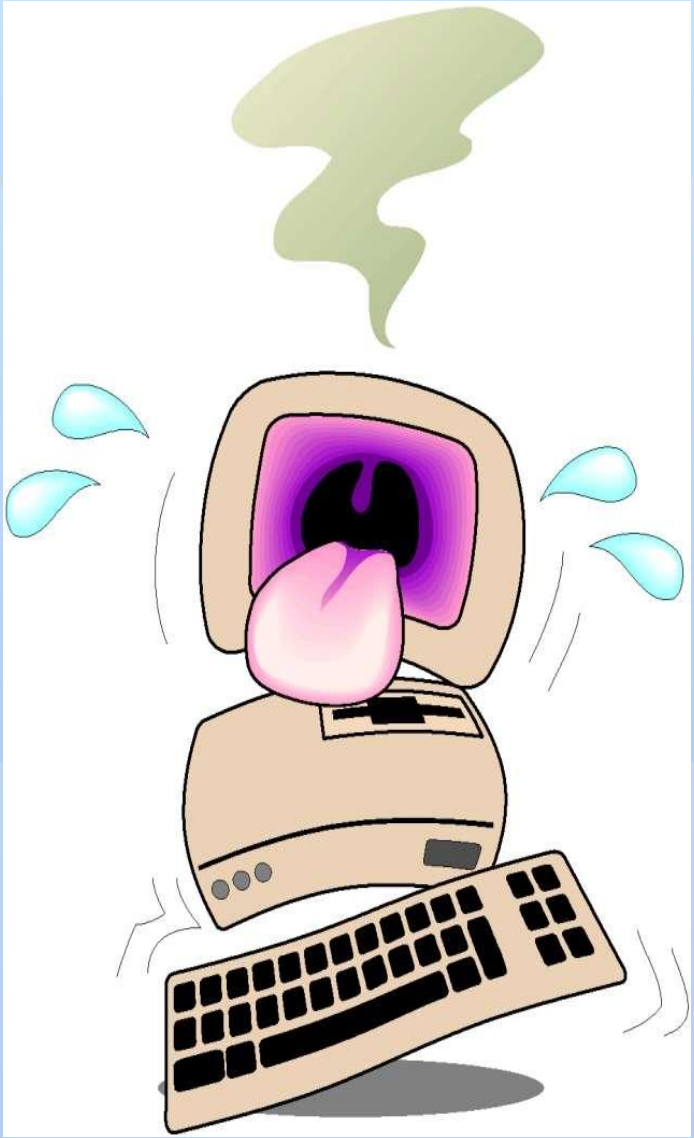
Безвредные	Уменьшают свободную память на диске за счет своего «размножения»
Неопасные	Уменьшают свободную память на диске. Вызывают появление графических, звуковых и др. внешних эффектов
Опасные	Могут привести к сбоям и зависаниям при работе компьютера
Очень опасные	Потеря программ и данных (изменение, удаление файлов и каталогов), форматирование винчестера и т.п.

Классификация вирусов по среде обитания:

Файловые	Внедряются в исполняемые файлы (программы) и активизируются при их запуске. Находятся в ОП до выключения компьютера
Загрузочные	Записывают себя в загрузочный сектор диска (в программу — загрузчик ОС). При загрузке ОС с зараженного диска внедряется в ОП и ведет себя как файловый вирус
Макровирусы	Являются макрокомандами, которые заражают файлы документов Word, Excel. Находятся в ОП до закрытия приложения
Драйверные	Заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации дополнительной строки
Сетевые	Заражают компьютер после открытия вложенного файла (вируса) в почтовое сообщение. Похищают пароли пользователей. Рассылают себя по электронным адресам

Профилактика компьютерных вирусов:

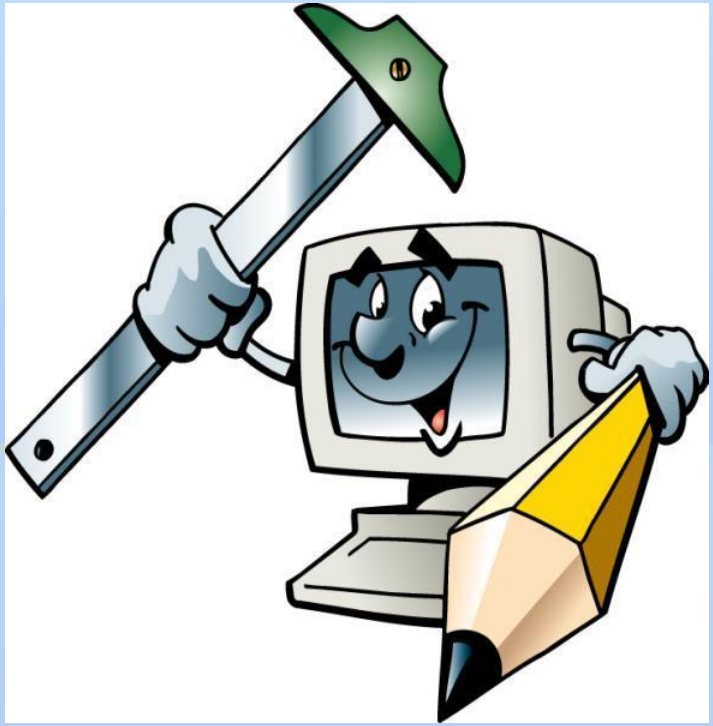
- иметь специальный загрузочный диск;
- систематически проверять компьютер на наличие вирусов;
- иметь последние версии антивирусных средств;
- проверять все поступающие данные на наличие вирусов;
- не использовать нелицензионные программные средства;
- выбирать запрет на загрузку макросов при открытии документов Word и Excel;
- выбрать высокий уровень безопасности в «Свойствах обозревателя»;
- делать архивные копии файлов;
- добавить в файл автозагрузки антивирусную программу сторож;
- не открывать вложения электронного письма, если отправитель неизвестен



Антивирусные программы — программы, которые предотвращают заражение компьютерным вирусом и ликвидируют последствия заражения.

Существуют несколько типов антивирусных программ, различающихся выполняемыми функциями:

- Полифиги;
- Ревизоры;
- Блокировщики.



ПОЛИФИГИ:

Самыми популярными и эффективными антивирусными программами являются антивирусные программы полифаги (например, Kaspersky Anti-Virus, Dr.Web).

Для поиска известных вирусов используются так называемые *маски*.

Маской вируса является некоторая постоянная последовательность программного кода, специфичная для этого конкретного вируса.

Если антивирусная программа обнаруживает такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению.

Полифаги могут обеспечивать проверку файлов в процессе их загрузки в оперативную память. Такие программы называются *антивирусными мониторами.*

К *достоинствам полифагов* относится их универсальность.

К *недостаткам* можно отнести большие размеры используемых ими антивирусных баз данных, которые должны содержать информацию о максимально возможном количестве вирусов, что, в свою очередь, приводит к относительно небольшой скорости поиска вирусов.

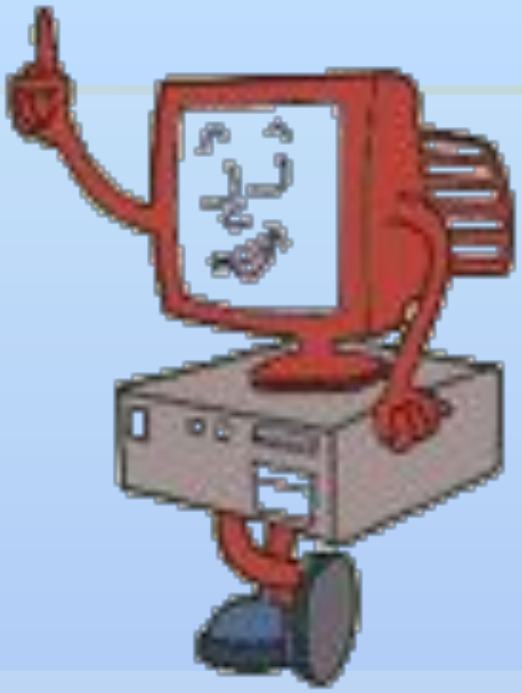
http://private-edu.narod.ru/book/polyf_swf.swf

РЕВИЗОРЫ:

- Принцип работы ревизоров (например, ADinf) основан на подсчете контрольных сумм для присутствующих на диске файлов. Эти контрольные суммы затем сохраняются в базе данных антивируса, как и некоторая другая информация: длины файлов, даты их последней модификации и пр.
- При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.

- *Недостаток ревизоров* состоит в том, что они не могут обнаружить вирус в новых файлах (на дискетах, при распаковке файлов из архива, в электронной почте), поскольку в их базах данных отсутствует информация об этих файлах.

  http://private-edu.narod.ru/book/revizzor_swf.swf



БЛОКИРОВЩИКИ

- Антивирусные блокировщики - это программы, перехватывающие "вирусоопасные" ситуации и сообщающие об этом пользователю. К таким ситуациям относится, например, запись в загрузочный сектор диска. Эта запись происходит при установке на компьютер новой операционной системы или при заражении загрузочным вирусом.
- Наибольшее распространение получили антивирусные блокировщики в BIOS компьютера. С помощью программы BIOS Setup можно провести настройку BIOS таким образом, что будет запрещена (заблокирована) любая запись в загрузочный сектор диска и компьютер будет защищен от заражения загрузочными вирусами.

- *К достоинствам блокировщиков*

относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения.

http://private-edu.narod.ru/book/block_swf.swf

СПАСИБО ЗА ВНИМАНИЕ!!!

При создании презентации использовались следующие интернет ресурсы:

1.http://ru.wikipedia.org/wiki
2. http://dpk-info.ucoz.ru/publ/kompjuternye_virusy_i_antivirusnye_programmy/32-1-0-61
3. http://private-edu.narod.ru/book/polyf_swf.swf
4. http://private-edu.narod.ru/book/revizzor_swf.swf
http://private-edu.narod.ru/book/block_swf.swf