Компьютерные вирусы
Антивирусные программы

Презентация подготовлена для конкурса «Интернешка» http://intrneshka.org/
Студенткой Кузнецкого филиала Пензенского многопрофильного колледжа группа 14КФ15
Китовой Натальей

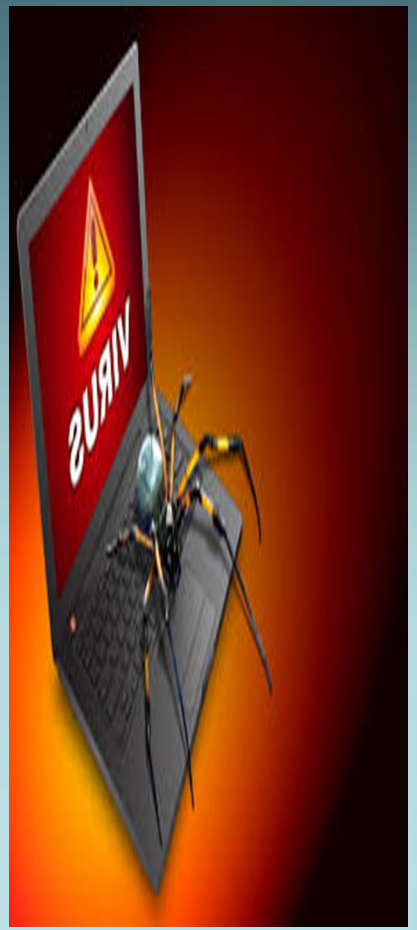
Понятие компьютерного вируса

- Массовое использование ПК в автономном и сетевом режиме, включая выход в глобальную сеть Интернет, породило проблему заражения их компьютерными вирусами.
- **Компьютерным вирусом** принято называть специально написанную, небольшую по размерам программу. Способную самопроизвольно присоединяться к другим программам (т.е. заражать их), создавать свои копии и внедрять их в файлы, системные области компьютера и в другие, объединенные с ним компьютеры с целью нарушения нормальной работы программ, порчи файлов и каталогов, создания различных помех при работе на компьютере.

Признаки появления вирусов

К признакам появления вируса можно отнести:

- • замедление работы компьютера;
- • невозможность загрузки операционной системы;
- • частые «зависания» и сбои в работе компьютера;
- • прекращение работы или неправильная работа ранее успешно функционировавших программ;
- • увеличение количества файлов на диске;
- • изменение размеров файлов;
- • периодическое появление на экране монитора неуместных системных сообщений;
- • уменьшение объема свободной оперативной памяти;
- • заметное возрастание времени доступа к жесткому диску;
- • изменение даты и времени создания файлов;
- • разрушение файловой структуры (исчезновение файлов, искажение каталогов и др.);
- • загорание сигнальной лампочки дисковода, когда к нему
- нет обращения.



Классификация вирусов

- *В зависимости от среды обитания вирусы классифицируются на загрузочные, файловые, системные, сетевые, файлово -загрузочные.*
- *Загрузочные вирусы внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска.*
- *Файловые вирусы внедряются в основном в исполняемые файлы с расширением .COM и .EXE.*
- *Системные вирусы проникают в системные модули и драйверы периферийных устройств, поражают программы-интерпретаторы.*
- *Сетевые вирусы обитают в компьютерных сетях; файлово-загрузочные поражают загрузочные сектора дисков и файлы прикладных программ.*
- *Резидентные вирусы при заражении компьютера оставляют в оперативной памяти свою резидентную часть, которая затем при каждом обращении к операционной системе и к другим объектам внедряется в них и выполняет свои разрушительные действия до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают оперативную память.*

- ***Алгоритмическая особенность построения вирусов оказывает влияние на их проявление и функционирование. Так, репликаторные программы благодаря своему быстрому воспроизводству приводят к переполнению основной памяти, при этом уничтожение программ-репликаторов усложняется, если воспроизводимые программы не являются точными копиями оригинала. В компьютерных сетях распространены программы-«черви». Они вычисляют адреса сетевых компьютеров и «записываются по ним», поддерживая между собой связь. В случае прекращения существования «червя» на каком-либо ПК оставшиеся отыскивают свободный компьютер и внедряют в него такую же программу***

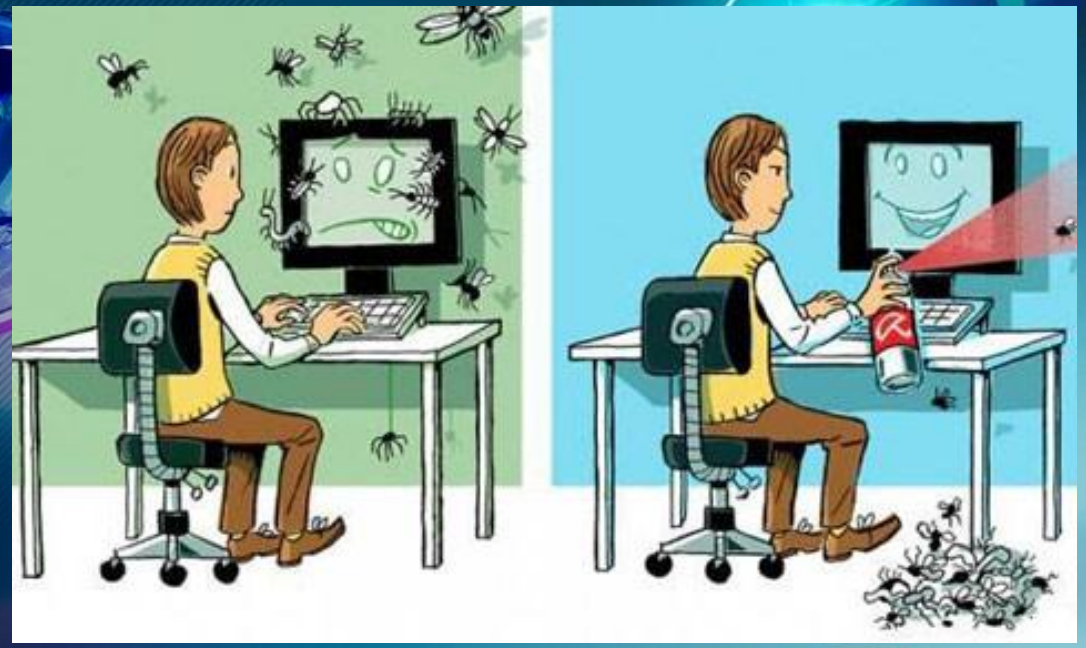
- ***" Троянский конь" - это программа, которая, маскируясь под полезную программу, выполняет дополнительные функции, о чем пользователь и не догадывается (например, собирает информацию об именах и паролях, записывая их в специальный файл, доступный лишь создателю данного вируса), либо разрушает файловую систему.***

- ***Логическая бомба - это программа, которая встраивается в большой программный комплекс. Она безвредна до наступления определенного события, после которого реализуется ее логический механизм. Например, такая вирусная программа начинает работать после некоторого числа запусков прикладной программы, комплекса, при наличии или отсутствии определенного файла или записи файла и т.д.***

- *Программы-мутанты, самовоспроизводясь, воссоздают копии, которые явно отличаются от оригинала.*
- *Вирусы-невидимки перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо них незараженные объекты.*
- *По степени воздействия на ресурсы компьютерных систем и сетей выделяются безвредные, опасные и разрушительные вирусы.*
- *Безвредные вирусы не разрушают файлы, но могут переполнять оперативную и дисковую память, выводить на экран графические эффекты и т.д.*

Антивирусные программы

Антивирусная программа (антивирус)- программа которая пытается обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы с зараженного компьютера, а так же служит для профилактики- предотвращения заражения файлов вирусами. Первые антивирусные программы появились практически сразу после появления первых вирусов. Современные антивирусные программы могут обнаруживать десятки тысяч вирусов.

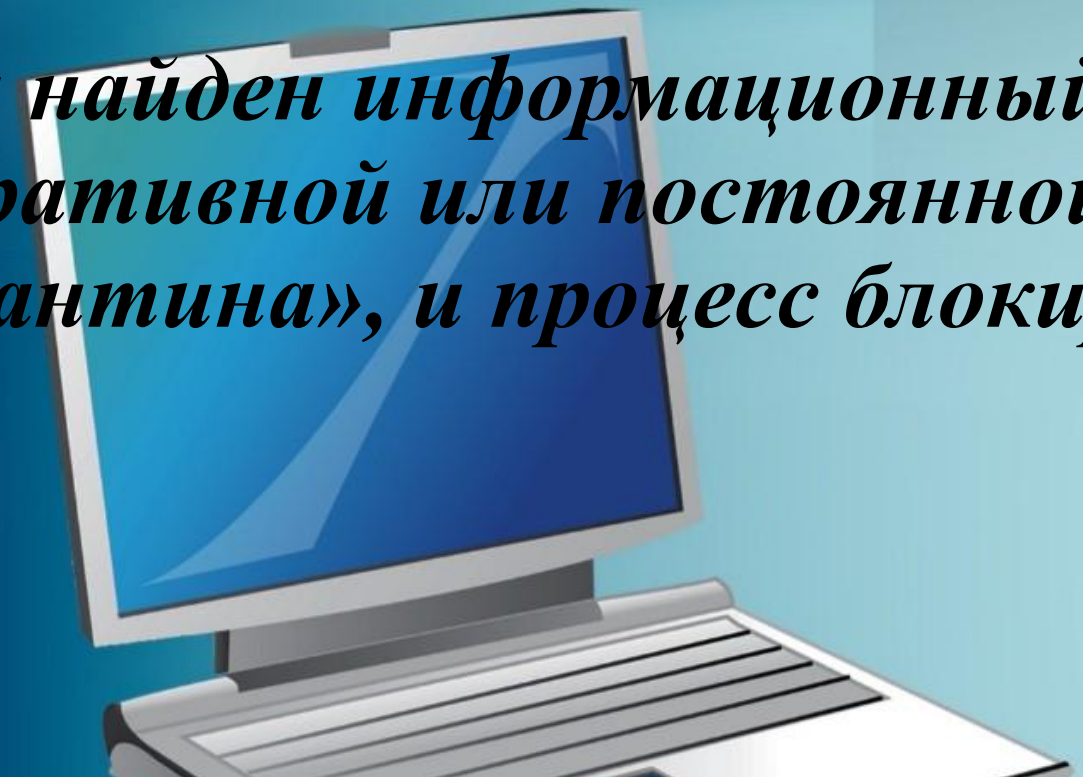


На данный момент антивирусное программное обеспечение разрабатывается в основном для операционной системы семейства Windows от компании Microsoft. Это вызвано большим количеством вредоносных программ именно на эту платформу.

Также на рынок выходят продукты и для других операционных систем, таких, к примеру, как Linux и Mac OS X. Это вызвано началом распространения компьютерных вирусов и под эти платформы, хотя Unix- подобные системы традиционно пользуются репутацией более устойчивых к воздействию вредоносных программ

ГОВОРЯ О СИСТЕМАХ MICROSOFT СЛЕДУЕТ ЗНАТЬ, ЧТО ОБЫЧНО АНТИВИРУС ДЕЙСТВУЕТ ПО СХЕМЕ:

- *Поиск по базе данных антивирусного ПО сигнатур вирусов*
- *Если найден информационный код в памяти (оперативной или постоянной), запускается процесс «карантина», и процесс блокируется*



Наиболее популярные антивирусные программы

AVG Anti-Virus

AVIRA

Профилактика

- Для того, чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:
- • оснастите свой компьютер современными антивирусными программами, например Doctor Web, Антивирус Касперского и постоянно возобновляйте их версии
- • перед считыванием с дискет информации, записанной на других компьютерах, всегда проверяйте эти дискеты на наличие вирусов, запуская антивирусные программы своего компьютера
- • при переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами
- • периодически проверяйте на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив операционную систему с защищенной от записи системной дискеты

- всегда защищайте свои дискеты от записи при работе на других компьютерах, если на них не будет производится запись информации
- • обязательно делайте архивные копии на дискетах ценной для вас информации
- • не оставляйте в кармане дисковода А дискеты при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами
- • используйте антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей
- • проверяйте e-mail даже если письмо пришло от хорошо известного вам человека (это обусловлено не тем что он хочет вам навредить а из-за того что он полный Lamer а его компьютер заражён)
- Так же следует иногда проверять автозагрузку, т.к. именно обычно закидывают загрузочные вирусы