

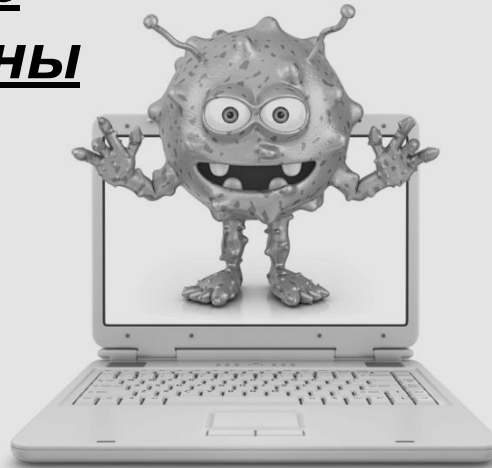
Осторожно,



Автор : Рыжков Данила Анатольевич,
учитель информатики

История
компьютерных
вирусов

Что такое
компьютерны
й вирус?



Классификац
ия
компьютерн
ых вирусов
Признаки
заражения
компьютера
вирусами

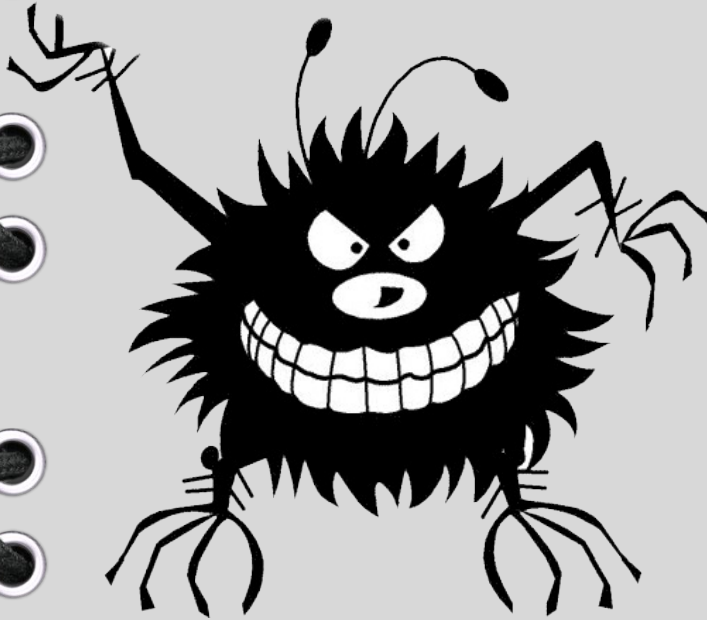
Способы
защиты от
компьютерн
ых вирусов

Каналы
распространения
компьютерных
вирусов

Что такое компьютерный вирус?

Компьютерный вирус — это разновидность компьютерной программы, отличительной особенностью которой является способность к размножению (саморепликация).

В дополнение к этому он может повреждать или полностью уничтожать данные, подконтрольные пользователю, от имени которого была запущена заражённая программа.



История компьютерных вирусов

Идея компьютерных вирусов появилась намного раньше самих персональных компьютеров. Точкой отсчета можно считать труды известного ученого Джона фон Неймана по изучению самовоспроизводящихся математических автоматов, о которых стало известно в 1940-х годах. В 1951 году он предложил способ создания таких автоматов.



История компьютерных вирусов

- **1959 г.** – на ЭВМ IBM 650 обнаружен вирус, который «съедал» часть слов.
- **1986 г.** – Первая «эпидемия» компьютерного вируса. Вирус по имени Brain (англ. «мозг») заражал дискеты персональных компьютеров.
- **1988 г.** - Роберт Моррис в США написал вирус, поразивший 2000 компьютеров.
- **В середине августа 1995 г.** в США и ряде стран Западной Европы появился вирус, который использует возможность представления информации в виде конгломерата данных и программ. Он заражал документы, подготовленные в системе MS Word – файлы типа *.doc.
- **26 апреля 1999 г.** Новым словом в вирусологии стал вирус под названием «Чернобыль» или WIN95.CIN. Данный вирус в отличие от своих собратьев в зависимости от модификации мог уничтожить MBR жесткого диска, таблицу размещения данных и не защищенную от перезаписи Flash-память. Волна эпидемии этого вируса прокатилась по всему миру. Громадный материальный ущерб был нанесен в Швеции. Пострадало большое количество пользователей и в России.



Классификация

компьютерных вирусов

В настоящее время нет единой классификации вирусных программ, но их можно выделить по следующим признакам:

по среде обитания

по способу заражения



по степени воздействия

по особенностям алгоритма



Классификация компьютерных вирусов по среде обитания

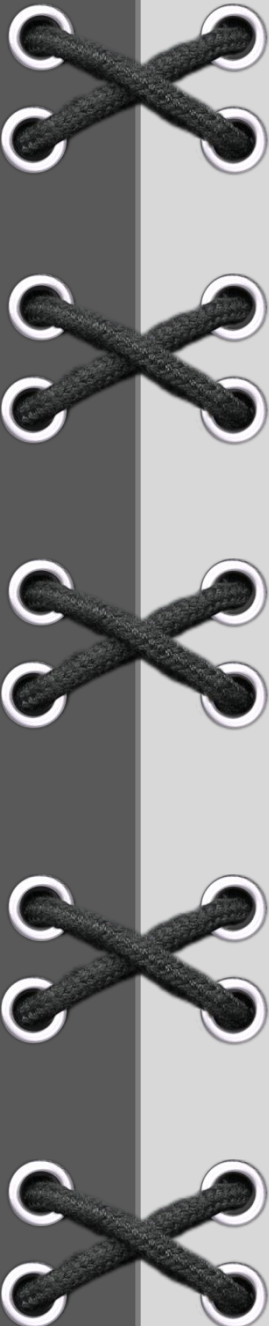
Сетевые вирусы – распространяются по различным компьютерным сетям.

Файловые вирусы – внедряются в исполняемые файлы, имеющие расширение EXE.

Загрузочные вирусы – внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска.

Файлово-загрузочные вирусы – заражают файлы и загрузочные сектора дисков.





Классификация компьютерных вирусов по способу заражения

Резидентные – при заражении оставляют в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения и внедряется в них.

Нерезидентные вирусы – не заражают память компьютера и являются активными ограниченное время.



Классификация компьютерных вирусов по особенностям алгоритма

Простейшие вирусы – не изменяют содержимое файлов, могут быть легко обнаружены и уничтожены.

Черви – распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и рассылают свои копии по этим адресам.

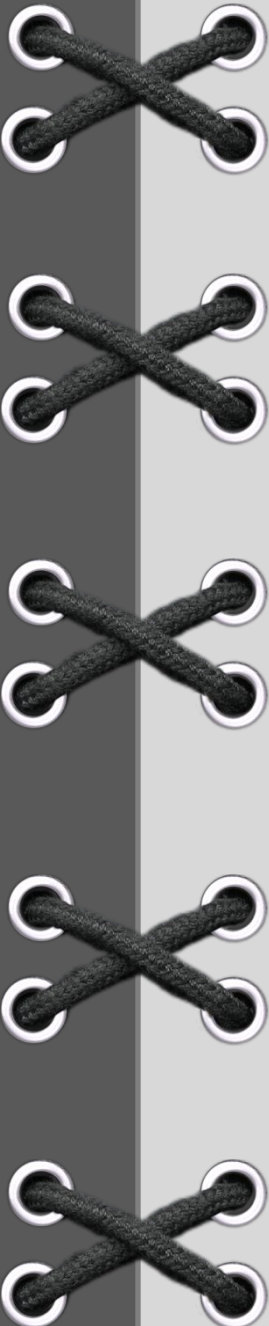
Вирусы – невидимки (стелс-вирусы) – трудно обнаружить и обезвредить, подставляют вместо своего тела незараженные участки диска.

Вирусы-мутанты – содержат алгоритмы шифровки/расшифровки, наиболее трудно обнаружить.

Трояны – маскируются под полезную программу, разрушают загрузочный сектор и файловую систему, воруют пароли.

Макровирусы – заражают файлы документов, например, текстовых документов. После загрузки заражённого документа в текстовый редактор макровирус постоянно присутствует в оперативной памяти компьютера и может заражать другие документы.





Классификация компьютерных вирусов по степени воздействия

БЕЗВРЕДНЫЕ – программы-шутки.

НЕОПАСНЫЕ – не мешают работе компьютера, но уменьшают объем оперативной памяти и памяти на дисках; действия таких вирусов проявляются в каких-либо графических или звуковых эффектах.

ОПАСНЫЕ – приводят к различным нарушениям в работе ПК.

ОЧЕНЬ ОПАСНЫЕ – их действие может привести к потере программ, уничтожению данных.



Признаки заражения компьютерными вирусами

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- Microsoft Internet Explorer "зависает" или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

Некоторые характерные признаки поражения вирусом через электронную почту:

- друзья или знакомые говорят вам о сообщениях от вас, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.



Каналы распространения компьютерных вирусов

1) *Флеш-накопители (флешки)*



2) *Электронная почта*



3) *Системы обмена мгновенными сообщениями (интернет-пейджеры)*



4) *Веб-страницы*



5) *Интернет и локальные сети*



Способы защиты от

компьютерных вирусов

Идеальный вариант - не допускать проникновения компьютерных вирусов в компьютер. Но если беда уже произошла, нужно принять оперативные меры по обнаружению и удалению вирусной инфекции.

Самым простым способом обнаружения вирусов, является обычное сканирование системы разнообразными антивирусными сканерами.

При регулярном обновлении, антивирусные программы способны показать достаточно высокий результат и выявить до 90% известных вирусов.

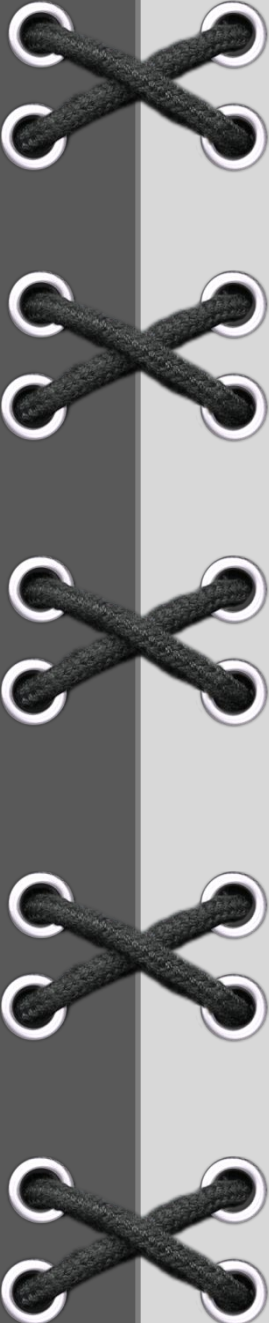


Способы защиты от

компьютерных вирусов
В качестве самых действенных мер по защите от заражения компьютерными вирусами рекомендуется:

- 1) использовать современные операционные системы, имеющие более серьезный уровень защиты от вредоносных программ;
- 2) своевременно устанавливать программы для устранения ошибок в ОС и прикладных программах, которые являются «лазейками» для вирусов;
- 3) использовать антивирусные программные продукты известных производителей с автоматическим обновлением антивирусных баз;
- 4) ограничить физический доступ к компьютеру посторонних лиц;
- 5) использовать внешние носители информации, полученные только от проверенных лиц;
- 6) не открывать компьютерные файлы, полученные из ненадежных источников (например, полученные в качестве вложения в письмо e-mail или скачанные из Интернета, без их предварительной проверки антивирусом);
- 7) отключить автозапуск со сменных носителей, что не позволит запускаться вредоносным программам, которые без ведома пользователя были туда записаны при заражении этих носителей вирусами.





Использованные источники информации

- Информатика и ИКТ: Учебник. 8 ласс. Базовый уровень/ Под редакцией Н. Д. Угринович. Бинوم. Лаборатория знаний, 2015
- Материалы сайта <http://pedsovet.su>
- Материалы сайта <http://easyen.ru>
- Материалы сайта <http://nsportal.ru>