Презентация подготовлена для конкурса «Интернешка»
http://interneshka.org

Компьютерные вирусы. Антивирусные программы

Автор: Меша Мария, 10 класс,
Руководитель: Александрова З.В., учитель
МБОУ СОШ №5 пгт Печенга, Мурманская обл.

Цель работы: ***исследование компьютерных вирусов, поиск наилучших способов защиты от них .***

Содержание

- Определение компьютерного вируса.
- История создания компьютерного вируса.
- Диагностика заражения компьютера.
- Симптомы заражения компьютера.
- Антивирусные программы.

Понятие компьютерного вируса

Компьютерный вирус — разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (саморепликация). В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру. По этой причине вирусы относят к вредоносным программам.

История создания компьютерного вируса

Вирусы появились приблизительно 30 лет назад. Именно тогда, в конце 60-х, когда о ПК можно было прочитать лишь в фантастических романах, в нескольких «больших» компьютерах в США, обнаружились очень необычные программы. Они не выполняли распоряжения человека, а действовали сами по себе. Причем, своими действиями они сильно замедляли работу компьютера, но при этом ничего не портили и не размножались. Но продлилось это недолго.

Уже в 70-х годах были зарегистрированы первые настоящие вирусы, способные к размножению. А появление и распространение ПК породило настоящую эпидемию – счет вирусов пошел на тысячи. Правда, термин «компьютерный вирус» появился только в 1984 г.

История создания компьютерного вируса

Первые компьютерные вирусы были простыми и неприхотливыми – от пользователей не скрывались, «скрашивали» свое разрушительное действие (удаление файлов, разрушение логической структуры диска) выводимыми на экран картинками и «шутками» («Назовите точную высоту горы Килиманджаро в миллиметрах! При введении неправильного ответа все данные на вашем винчестере будут уничтожены!»). Выявить такие вирусы было не трудно.
Позднее вирусы стали прятать свой программный код так, что ни один антивирус не мог его обнаружить. Такие вирусы назывались «невидимками» (stealth).

В течение 1998-1999 гг. мир потрясли несколько разрушительных вирусных атак: в результате деятельности вирусов Melissa, Win95.CIH и Chernobyl были выведены из строя около миллиона компьютеров во всех странах мира.

Классификация вредоносных программ

Класификация вирусов

Типы вирусов

ФАЙЛОВЫМ ВИРУСОМ называют вирус, который внедряется в выполняемые файлы.Это означает, что код программы-вируса находится в каком-то выполняемом файле. Файл, в теле которого присутствует код программы-вируса, называется зараженным (инфицированным) файлом.

ЗАГРУЗОЧНЫМ ВИРУСОМ (бутовым) называют вирус, который внедряется в загрузочный сектор диска (Boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record).В данном случае код программы-вируса (или его часть) размещен в загрузочном секторе или в главной загрузочной записи. Диск, загрузочный сектор которого поражен вирусом, называется зараженным, или инфицированным диском.

СЕТЕВЫМ ВИРУСОМ называют вирус, который распространяется по различным компьютерным сетям.

Группы вирусов по способам заражения

РЕЗИДЕНТНЫЙ ВИРУС размещает себя или некоторую свою часть в оперативной памяти компьютера, получая возможность перехватывать обращения операционной системы к дискам и файлам. При обращении операционной системы к этим объектам вирус внедряется в них. Резидентный вирус находится в оперативной памяти и является активным (т.е., способным заражать все новые и новые объекты) вплоть до выключения или перезагрузки компьютера. Резидентными являются все загрузочные вирусы.

НЕРЕЗИДЕНТНЫЙ ВИРУС не заражает оперативную память компьютера, то есть, не размещает свой код в оперативной памяти. Он является активным только во время работы зараженной программы.

Группы вирусов по особенностям алгоритма

ПАРАЗИТИЧЕСКИЕ - это вирусы, изменяющие содержимое файлов и секторов диска, они могут быть достаточно легко обнаружены.

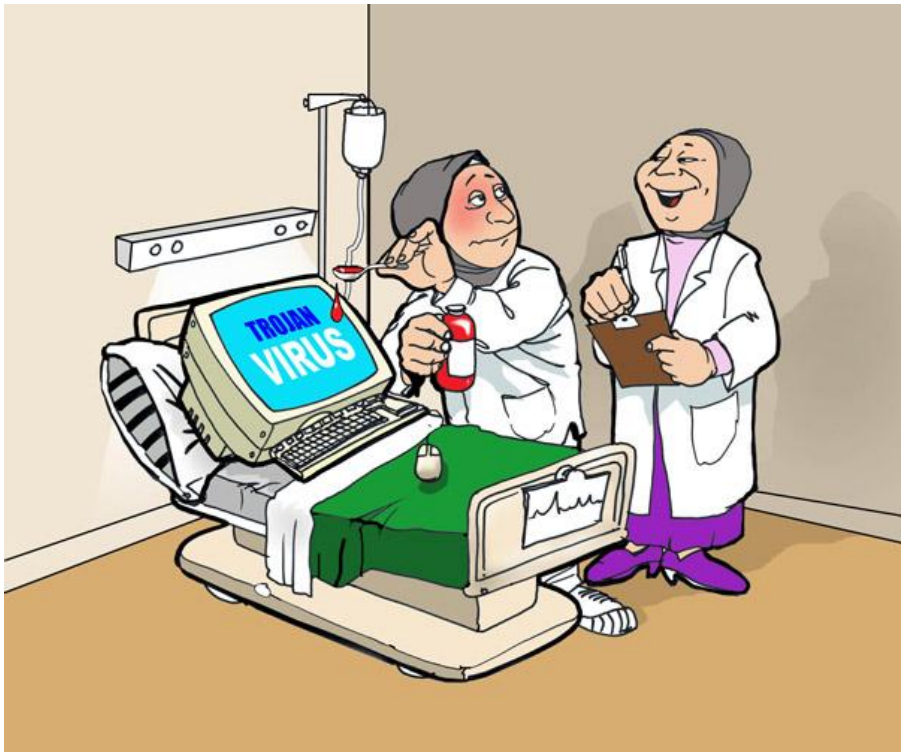
РЕПЛИКАТОРЫ - называемые червями, они распространяются по компьютерным сетям, вычисляя адреса сетевых компьютеров, они записывают по этим адресам свои копии.

НЕВИДИМКИ - называемые стелс-вирусами, их трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.

МУТАНТЫ – это вирусы, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

ТРОЯНСКИЕ – это квазивирусные программы, которые хотя и неспособны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Вирусы портили жесткий диск и уничтожали BIOS материнской платы. Нет сомнения, что вирусные атаки буду продолжаться и впредь. Поэтому пользователям компьютеров остается только обзавестись хорошей антивирусной программой.



Диагностика заражения компьютера

Когда ПК или ноутбук начинает барахлить или перестает работать вовсе и его требуется привести в исправное состояние, сначала нужно выяснить, в чем именно состоит причина возникшей проблемы. Для этого мастерами Сервис03.Ру производится диагностика неисправности компьютера. Нередко бывает так, что одна поломка влечет за собой другие, и поэтому требуется определить и устранить их все. Задача эта — не из легких, и зачастую нашими специалистами используется специальная программа для диагностики компьютера, существенно упрощающая и облегчающая ее решение.

Диагностика заражения компьютера

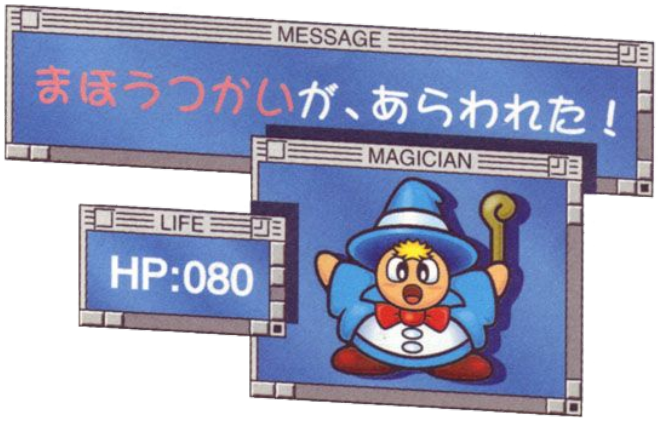
Качественная и всесторонняя диагностика и ремонт компьютеров предполагает проверку как их аппаратной части, так и программного обеспечения. Первая включает в себя следующие этапы:

- *Проверку работоспособности и исправности блока питания*
- *Проверку работоспособности и исправности системной (материнской) платы*
- *Диагностику ЦП (центрального процессора)*
- *Проверку работоспособности и исправности оперативной памяти*
- *Проверку работоспособности и исправности видеоадаптера*
- *Проверку работоспособности, исправности и стабильности работы дисковых накопителей*
- *Проверку исправности и работоспособности оптических приводов*
- *Проверка исправности и работоспособности сетевой карты*

Диагностика заражения компьютера

В тех случаях, когда выясняется, что с аппаратной частью компьютера все в порядке, наши специалисты производят диагностику его программного обеспечения. Она включает в себя следующие этапы:

- ***Проверку файловой системы с целью обнаружения ошибок***
- ***Проверку реестра на наличие ошибок***
- ***Проверку ПО на вирусные заражения***



Симптомы заражения компьютеров

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- прекращение работы или неправильная работа ранее
- успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- изменение даты и времени модификации файлов;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений и т.д.

Три

1. ВИРУСЫ НЕ ВОЗНИКАЮТ САМИ СОБОЙ - ИХ СОЗДАЮТ НЕХОРОШИЕ ПРОГРАММИСТЫ-ХАКЕРЫ И РАССЫЛАЮТ ПО СЕТИ ПЕРЕДАЧИ ДАННЫХ ИЛИ ПОДКИДЫВАЮТ НА КОМПЬЮТЕРЫ ЗНАКОМЫХ.

2. ВИРУС НЕ МОЖЕТ САМ СОБОЙ ПОЯВИТЬСЯ НА ВАШЕМ КОМПЬЮТЕРЕ - ЛИБО ЕГО ПОДСУНУЛИ НА ДИСКЕТАХ ИЛИ ДАЖЕ НА КОМПАКТ-ДИСКЕ, ЛИБО ВЫ ЕГО СЛУЧАЙНО СКАЧАЛИ ИЗ КОМПЬЮТЕРНОЙ СЕТИ, ЛИБО ВИРУС ЖИЛ У ВАС В КОМПЬЮТЕРЕ С САМОГО НАЧАЛА, ЛИБО (ЧТО САМОЕ УЖАСНОЕ) ПРОГРАММИСТ-ХАКЕР ЖИВЕТ У ВАС В ДОМЕ.

3. КОМПЬЮТЕРНЫЕ ВИРУСЫ ЗАРАЖАЮТ ТОЛЬКО КОМПЬЮТЕР И НИЧЕГО БОЛЬШЕ, ПОЭТОМУ НЕ НАДО БОЯТЬСЯ - ЧЕРЕЗ КЛАВИАТУРУ И МЫШЬ ОНИ НЕ ПЕРЕДАЮТСЯ.

Полезные

1. ПРИМЕНЕНИЕ КОМПЛЕКСА АНТИВИРУСНЫХ ПРОГРАММ.

2. НЕОБХОДИМО ПЕРИОДИЧЕСКОЕ ОБНОВЛЕНИЕ АНТИВИРУСНЫХ ПРОГРАММ

3. ПРОВЕРКА ИНФОРМАЦИИ ПОСТУПАЮЩЕЙ ИЗ ВНЕ.

4. ПЕРИОДИЧЕСКАЯ ПРОВЕРКА ВСЕГО КОМПЬЮТЕРА.

5. ОСТОРОЖНОСТЬ С НЕЗНАКОМЫМИ ФАЙЛАМИ. ИХ ДЕЙСТВИЯ МОГУТ НЕ СООТВЕТСТВОВАТЬ НАЗВАНИЮ

Антивирусные программы

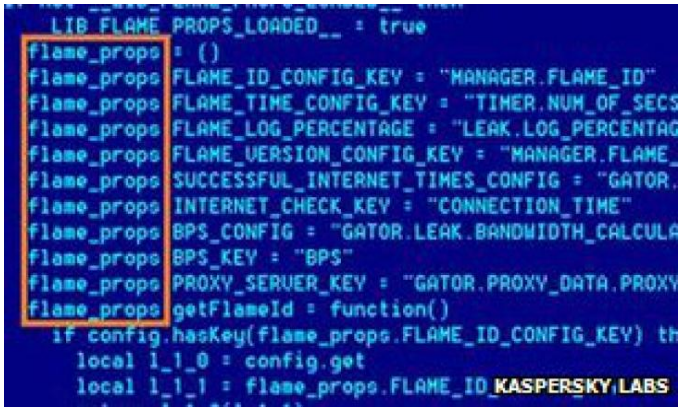
Антивирусные программы – программы, которые предотвращают заражение компьютерным вирусом и ликвидируют последствия заражения

Антивирус Касперского

Антивирус Касперского – мощное средство для борьбы с вредоносными программами. Антивирус предоставляет базовую защиту и имеет достаточно мощные функциональные возможности для защиты компьютера от всех видов вирусов. Пожалуй единственный минус этой программы это то, что он платный.

Антивирус Касперского (англ. Kaspersky Antivirus, KAV) — антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского.

ЗАО «Лаборатория Касперского»



Евгений Валентинович Касперский (4 октября 1965, Новороссийск) — российский программист, специалист по антивирусной защите, один из основателей, ведущий разработчик и крупнейший акционер ЗАО «Лаборатория Касперского». Лауреат Государственной премии в области науки и технологий за 2008 год.

Функции

Базовая защита

- Защита от вирусов, троянских программ и червей
- Защита от шпионских и рекламных программ
- Проверка файлов в автоматическом режиме и по требованию
- Проверка почтовых сообщений (для любых почтовых клиентов)
- Проверка интернет-трафика
- Защита интернет-пейджеров
- Проактивная защита от новых вредоносных программ
- Проверка Java
- Предотвращение угроз
- Поиск уязвимостей в ОС и установленном ПО
- Анализ и устранение уязвимостей в браузере Internet Explorer
- Блокирование ссылок на зараженные сайты
- Распознавание вирусов по способу их упаковки
- Глобальный мониторинг угроз (Kaspersky Security Network)
- Восстановление системы и данных

- Возможность установки программы на зараженный компьютер
- Функция самозащиты программы от выключения или остановки
- Восстановление корректных настроек системы после удаления вредоносного ПО
- Наличие инструментов для создания диска аварийного восстановления
- Защита конфиденциальных данных
- Блокирование ссылок на фишинговыесайты
- Удобство использования
- Автоматическая настройка программы в процессе установки
- Готовые решения (для типичных проблем)
- Наглядное отображение результатов работы программы
- Информативные диалоговые окна для принятия пользователем обоснованных решений
- Возможность выбора между простым (автоматическим) и интерактивным режимами работы
- Круглосуточная техническая поддержка
- Автоматическое обновление баз

Avira Free Antivirus

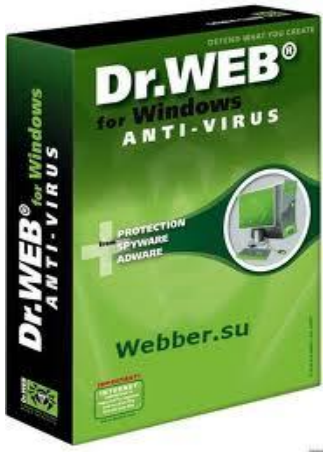
Avira Free Antivirus сканер системы защищает вас от всех типов вредоносных программ, дополнительная панель инструментов обеспечивает защиту вашей личной информации, включая в себя функции консультанта по вопросам репутации, который оценивает безопасность веб-сайтов, найденных в ходе поиска.

Avast Free Antivirus предлагает быстрый антивирус и его мощные экраны для защиты от вредоносного ПО, инструмент для очистки браузера от нежелательных плагинов / надстроек и интеллектуальный комплексный сканер, который способен в одном сеансе проверить всю систему на наличие вредоносного ПО и устаревших версий программ, требующих обновления, оценить состояние безопасности домашней сети и уровень производительности ПК

Panda Antivirus, Доктор Web

Panda Antivirus предлагает самую простую в использовании и наиболее интуитивно понятную защиту для компьютера.
Просто установите его и забудьте о вирусах, шпионах, руткитах, хакерах и онлайн-мошенниках.
Общайтесь в чатах, обменивайтесь фотографиями и видео, работайте с Интернет-банками и осуществляйте покупки в онлайн-магазинах, читайте Ваши любимые блоги или путешествуйте в Интернете с чувством полного спокойствия и без проблем.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Антивирусная защита Dr.Web позволяет информационным системам клиентов эффективно противостоять любым, даже неизвестным угрозам.



Теперь вы знаете, как вылечить компьютер от вирусов!