Презентация на тему: «Компьютерные Вирусы»

Выполнили студенты группы 9кс-104:
Бакутин Артем,
Пасичников Сергей,
Чижков Денис.

Проверил преподователь:
Музика Т.В.

2012-2013 уч. год

Содержание

Что такое компьютерный вирус?

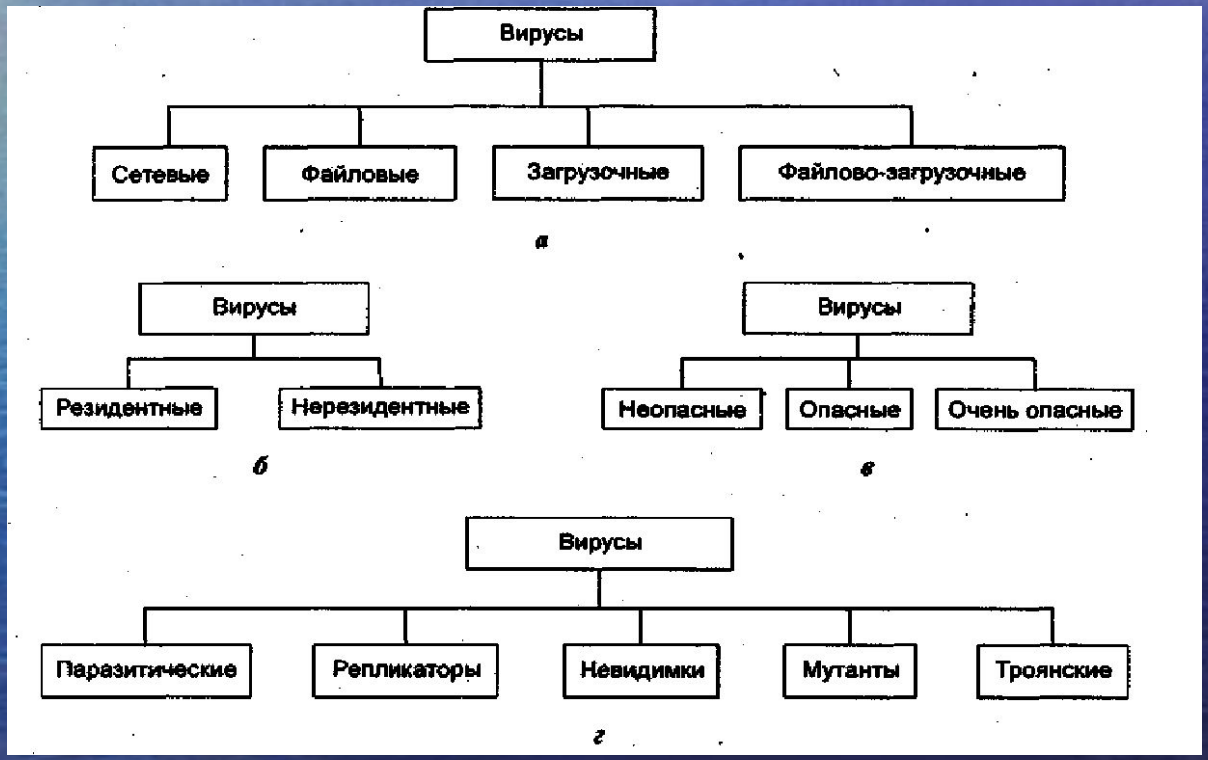
Компьютерный вирус – разновидность компьютерных программ, отличительной особенностью которых является способность к размножению (саморепликация). В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю или компьютеру. По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

Основные признаки проявления вирусов

- Прекращение работы или неправильная работа ранее успешно функционировавших программ
- Медленная работа компьютера
- Невозможность загрузки операционной системы
- Исчезновение файлов и каталогов или искажение их содержимого
- Изменение даты и времени модификации файлов
- Изменение размеров файлов
- Частые зависания и сбои в работе компьютера
- Неожиданное значительное увеличение количества файлов на диске
- Существенное уменьшение размера свободной оперативной памяти
- Вывод на экран непредусмотренных сообщений или изображений
- Подача непредусмотренных звуковых сигналов

Классификация компьютерных вирусов

а - по среде обитания; б - по способу заражения; в - по степени воздействия; г - по особенностям алгоритмов



По среде обитания:

- **Сетевые вирусы** используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.
- **Файловые вирусы** либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы)
- **Загрузочные вирусы** записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.

По способу заражения:

- Резидентные (такой вирус при инфицировании ПК оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение ОС к объектам заражения и поражает их. Резидентные вирусы живут до первой перезагрузки ПК)
- Нерезидентные (не заражают оперативную память и могут быть активными ограниченное время)

По степени воздействия:

- **Неопасные** (как правило эти вирусы забивают память компьютера путем своего размножения и могут организовывать мелкие пакости – проигрывать заложенную в них мелодию или показывать картинку);
- **Опасные** (эти вирусы способны создать некоторые нарушения в функционировании ПК – сбои, перезагрузки, глюки, медленная работа компьютера и т. д.);
- **Очень опасные** (опасные вирусы могут уничтожить программы, стереть важные данные, убить загрузочные и системные области жесткого диска, который потом можно выбросить)

По особенностям алгоритма:

- **Паразитические** (меняют содержимое файлов и секторов диска. Такие вирусы легко вычисляются и удаляются);
- **Мутанты** (их очень тяжело обнаружить из-за применения в них алгоритмов шифрования. Каждая следующая копия размножающегося вируса не будет похожа на предыдущую);
- **Репликаторы** (вирусы-репликаторы, они же сетевые черви, проникают через компьютерные сети, они находят адреса компьютеров в сети и заражают их);
- **Троянский конь** (один из самых опасных вирусов, так как трояны не размножаются, а воруют ценную (порой очень дорогую) информацию – пароли, банковские счета, электронные деньги и т. д.);
- **Невидимки** (это трудно обнаружимые вирусы, которые перехватывают обращения ОС к зараженным файлам и секторам дисков и подставляют вместо своего незараженные участки.

ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

- Глобальная сеть Глобальная сеть Internet
- Электронная почта
- Локальная сеть
- Компьютеры «Общегопользования»
- Пиратское программное обеспечение
- Ремонтные службы
- Съемные накопители

ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

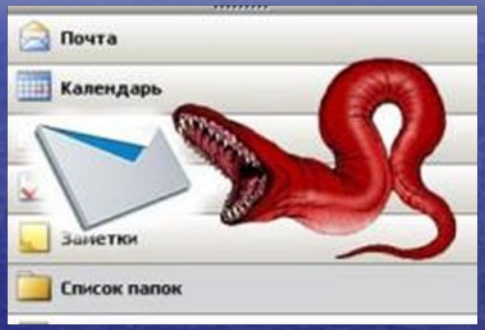
Глобальная сеть Интернет

Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Возможно заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта, а ничего не подозревающие пользователи зайдя на такой сайт рискуют заразить свой компьютер.

ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

Электронная почта

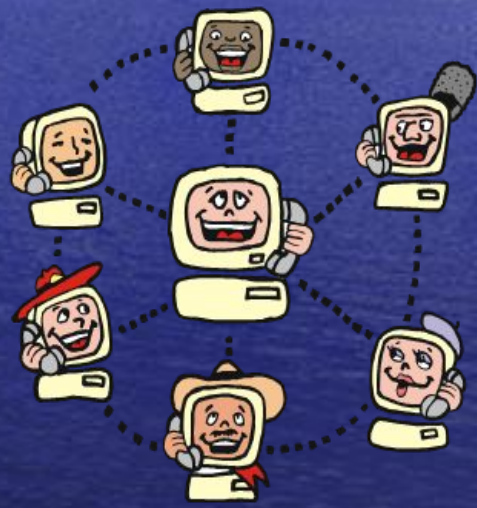
Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.



ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

Локальные сети

Третий путь «быстрого заражения» — локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере .



На следующий день пользователи при входе в сеть запускают зараженные файлы с сервера, и вирус, таким образом, получает доступ на компьютеры пользователей.

ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

Персональные компьютеры «общего пользования»

Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из учащихся принес на своих носителях вирус и заразил какой-либо учебный компьютер, то очередную «заразу» получат и носители всех остальных учащихся, работающих на этом компьютере.

То же относится и к домашним компьютерам, если на них работает более одного человека.

ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

Пиратское программное обеспечение

Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных «зон риска».Часто пиратские копии на дисках содержат файлы, зараженные самыми разнообразными типами вирусов.

ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

Ремонтные службы

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре. Ремонтники — тоже люди, и некоторым из них свойственно наплевательское отношение к элементарным правилам компьютерной безопасности.

ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

Съемные накопители

В настоящее время большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны.

Как защититься от вирусов

- установите на свой ПК современную антивирусную программу.
- перед просмотром информации принесенной на флэш-карте (дискете) с другого компьютера проверьте носитель антивирусом;
- после разархивирования архивных файлов сразу проверьте их на вирусы (не все антивирусные программы могут искать вредоносный код в архивах или могут делать это не корректно);
- периодически проверяйте компьютер на вирусы (если активно пользуетесь Интернетом – запускайте раз в неделю, а то и чаще);
- как можно чаще делайте резервные копии важной информации (backup);
- используйте совместно с антивирусной программой файервол (firewall) если компьютер подключен к Интернет;
- настройте браузер (программа просмотра Интернет страниц – IE, Opera и т.д.) для запрета запуска активного содержимого html-страниц.

Что такое Антивирус?

Антивирусная программа (антивирус) — специализированная 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) файлов или операционной системы вредоносным кодом.

Виды антивирусных программ:

- Программы-детекторы
- Программы-доктора
- Программы-ревизоры
- Программы вакцины

Программы-детекторы

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них вирусов

Программы-доктора

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них вирусов

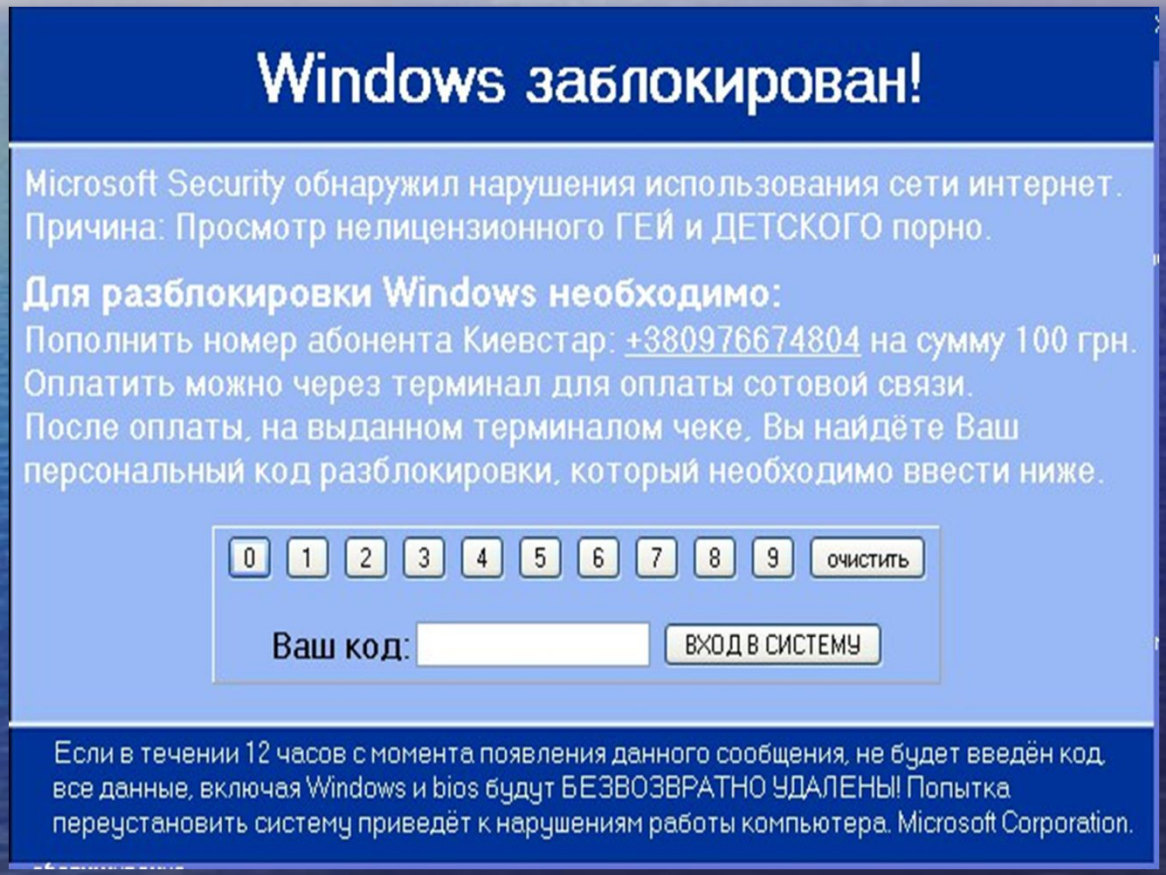
Программы-ревизоры

Принцип их работы состоит в подсчете контрольных сумм для присутствующих на диске файлов/системных секторов. Эти суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

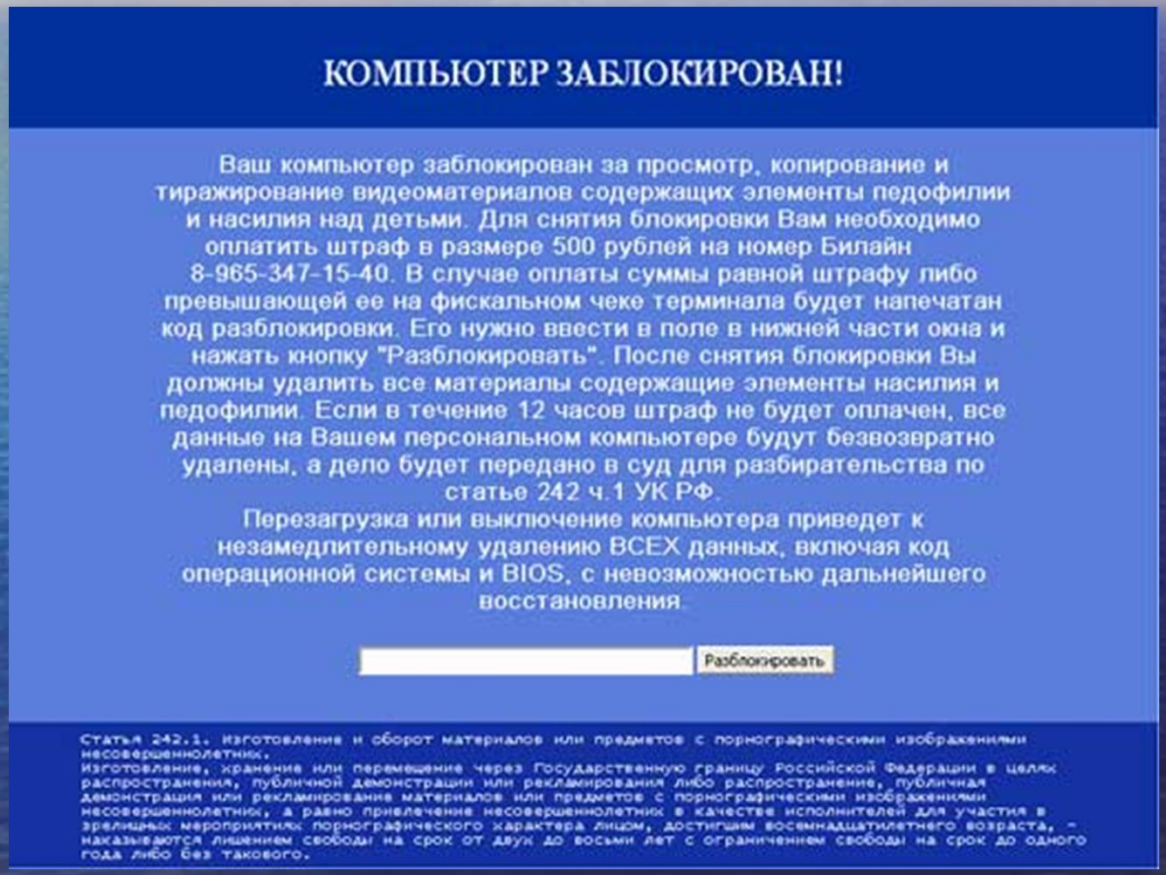
Программы-вакцины

Программы-вакцины, или иммунизаторы, модифицируют программы и диски такимобразом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Сообщения на дисплее при блокировке компьютера вирусами



Сообщения на дисплее при блокировке компьютера вирусами



Сообщения на дисплее при блокировке компьютера вирусами