КОМПЬЮТЕРНЫЕ ВИРУСЫ И ЗАЩИТА ОТ НИХ

Информатика и ИКТ 10 класс

КОМПЬЮТЕРНЫЕ ВИРУСЫ

- Компью́терные ви́русы — разновидность самовоспроизводящихся компьютерных программ, которые распространяются, внедряя себя в исполняемый код других программ или в документы специального формата, содержащие макрокоманды, такие, как MS Word и Excel. Многие вирусы вредят данным на заражённых компьютерах, хотя иногда их единственной целью является лишь заражение как можно большего количества компьютеров.

- В общем словоупотреблении к компьютерными вирусами причисляют все вредоносные программы, такие как сетевые и файловые черви, троянские кони, программы-шпионы.

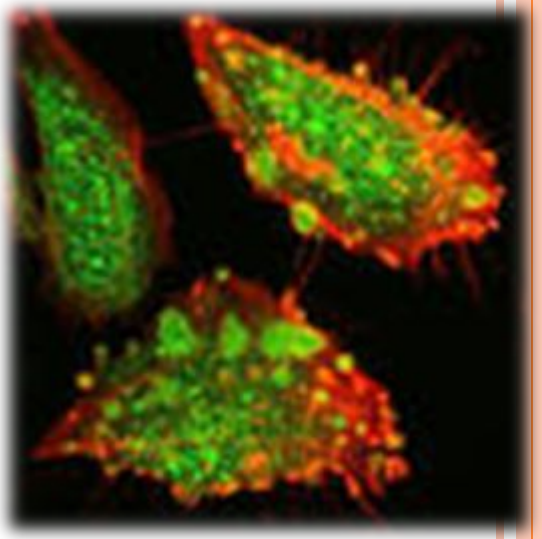
Классификация

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году).

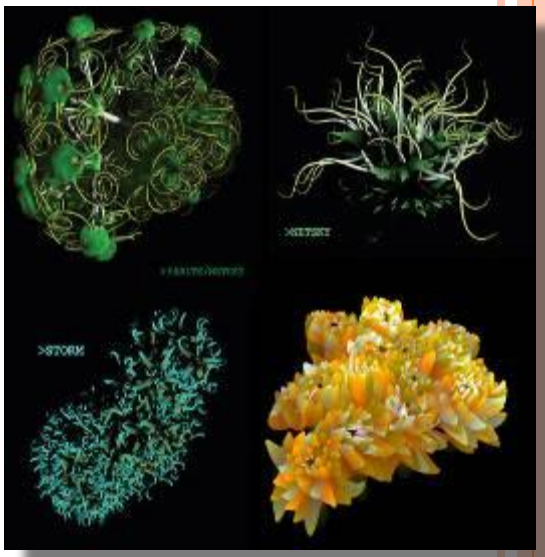
Принято разделять вирусы:

- по поражаемым объектам (файловые вирусы, загрузочные вирусы, скриптовые вирусы, сетевые черви),
- по поражаемым операционным системам и платформам (DOS, Windows, Unix, Linux, Java и другие),
- по технологиям используемым вирусом (полиморфные вирусы, стелс-вирусы),
- по языку на котором написан вирус (ассемблер, высокоуровневый язык программирования, скриптовый язык и др.).

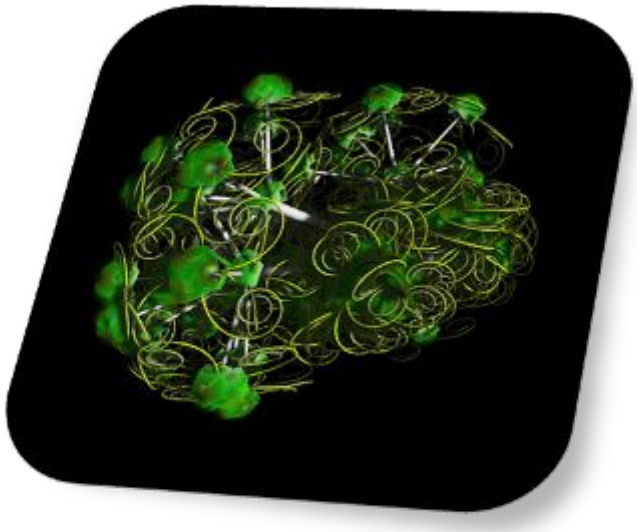
КЛАССИФИКАЦИЯ ФАЙЛОВЫХ ВИРУСОВ ПО СПОСОБУ ЗАРАЖЕНИЯ



- По способу заражения файловые вирусы (вирусы, внедряющие свой код в исполняемые файлы: командные файлы, программы, драйверы, исходный код программ и др.)разделяют на перезаписывающие, паразитические, вирусы-звенья, вирусы-черви, компаньон-вирусы, а так же вирусы, поражающие исходные тексты программ и компоненты программного обеспечения (VCL, LIB и др.).
- *Перезаписывающие вирусы*
- Вирусы данного типа записывают свое тело вместо кода программы, не изменяя названия исполняемого файла, вследствие чего исходная программа перестает запускаться. При запуске программы выполняется код вируса, а не сама программа.
- *Вирусы-компаньоны*
- Компаньон-вирусы, как и перезаписывающие вирусы, создают свою копию на месте заражаемой программы, но в отличие от перезаписываемых не уничтожают оригинальный файл, а переименовывают или перемещают его. При запуске программы вначале выполняется код вируса, а затем управление передается оригинальной программе.
- Возможно существование и других типов вирусов-компаньонов, использующих иные оригинальные идеи или особенности других операционных систем. Например, PATH-компаньоны, которые размещают свои копии в основном каталоге Windows, используя тот факт, что этот каталог является первым в списке PATH, и файлы для запуска Windows в первую очередь будет искать именно в нем. Данными способом самозапуска пользуются также многие компьютерные черви и троянские программы.
- *Файловые черви*
- Файловые черви создают собственные копии с привлекательными для пользователя названиями (например Game.exe, install.exe и др.) в надежде на то, что пользователь их запустит.



- *Вирусы-звенья*
- Как и компаньон-вирусы, не изменяют код программы, а заставляют операционную систему выполнить собственный код, изменяя адрес местоположения на диске зараженной программы, на собственный адрес. После выполнения кода вируса управление обычно передается вызываемой пользователем программе.
- *Паразитические вирусы*
- Паразитические вирусы — это файловые вирусы изменяющие содержимое файла добавляя в него свой код. При этом зараженная программа сохраняет полную или частичную работоспособность. Код может внедряться в начало, середину или конец программы. Код вируса выполняется перед, после или вместе с программой, в зависимости от места внедрения вируса в программу.
- *Вирусы, поражающие исходный код программ*
- Вирусы данного типа поражают или исходный код программы, либо её компоненты (OBJ-, LIB-, DCU- файлы) а так же VCL и ActiveX компоненты. После компиляции программы оказываются в неё встроенными. В настоящее время широкого распространения не получили.



АНТИВИРУСНАЯ ПРОГРАММА

- Антивирусная программа (антивирус) — программа для обнаружения и лечения программ, заражённых компьютерным вирусом, а также для предотвращения заражения файла вирусом (например, с помощью вакцинации).
- Первые наиболее простые антивирусные программы появились почти сразу после появления вирусов. Сейчас разработкой антивирусов занимаются крупные компании. Как и у создателей вирусов, в этой сфере также сформировались оригинальные приёмы — но уже для поиска и борьбы с вирусами. Современные антивирусные программы могут обнаруживать десятки тысяч вирусов.
- К сожалению, конкуренция между антивирусными компаниями привела к тому, что развитие идёт в сторону увеличения количества обнаруживаемых вирусов (прежде всего для рекламы), а не в сторону улучшения их детектирования (идеал — 100%-е детектирование) и алгоритмов лечения заражённых файлов.
- Антивирусное программное обеспечение состоит из компьютерных программ, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы.

Спасибо
за
внимание!