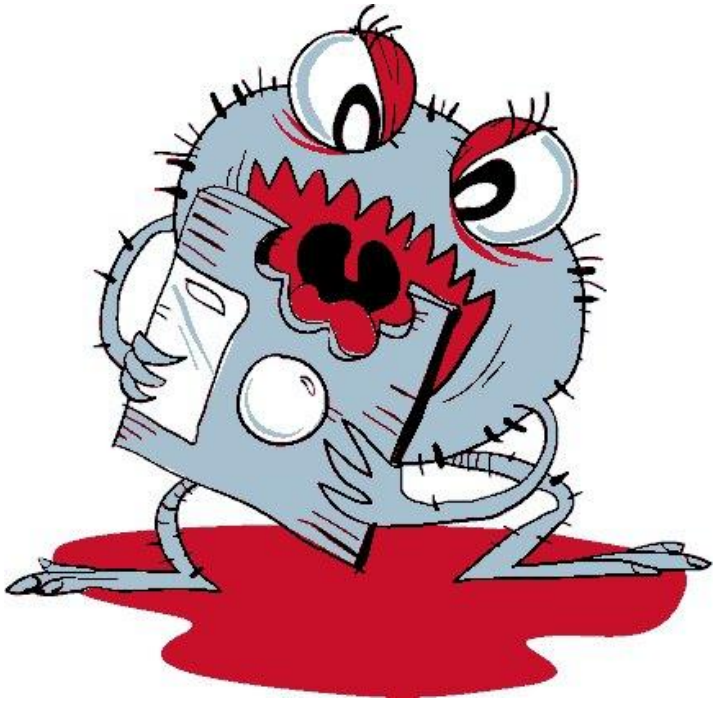
Компьютерные вирусы.

Работу выполнила
ученица 10б класса
Железникова Наташа
Учитель: Лузгина Н.Г.

Содержание:

Что такое компьютерные вирусы?

- Компьютерные вирусы - это класс программ способных к саморазмножению и самомодификации в работающей вычислительной среде и вызывающих нежелательные для пользователей действия. Действия могут выражаться в нарушении работы программ, выводе на экран посторонних сообщений или изображений, порче записей, файлов, дисков, замедлении работы ЭВМ и др.



Первые вирусы.

Первыми известными вирусами являются **Virus 1,2,3** и **Elk Cloner** для **ПК Apple II**. Оба вируса очень схожи по функциональности и появились независимо друг от друга с небольшим промежутком во времени в 1981 году.

С появлением первых персональных компьютеров Apple в 1977 году и развитием сетевой инфраструктуры начинается новая эпоха истории вирусов. Появились первые программы-вандалы, которые под видом полезных программ выкладывались на **BBS**, однако после запуска уничтожали данные пользователей. В это же время появляются троянские программы-вандалы, проявляющие свою деструктивную сущность лишь через некоторое время или при определённых условиях.

Классификация компьютерных вирусов.

В зависимости от среды обитания вирусы можно разделить на:

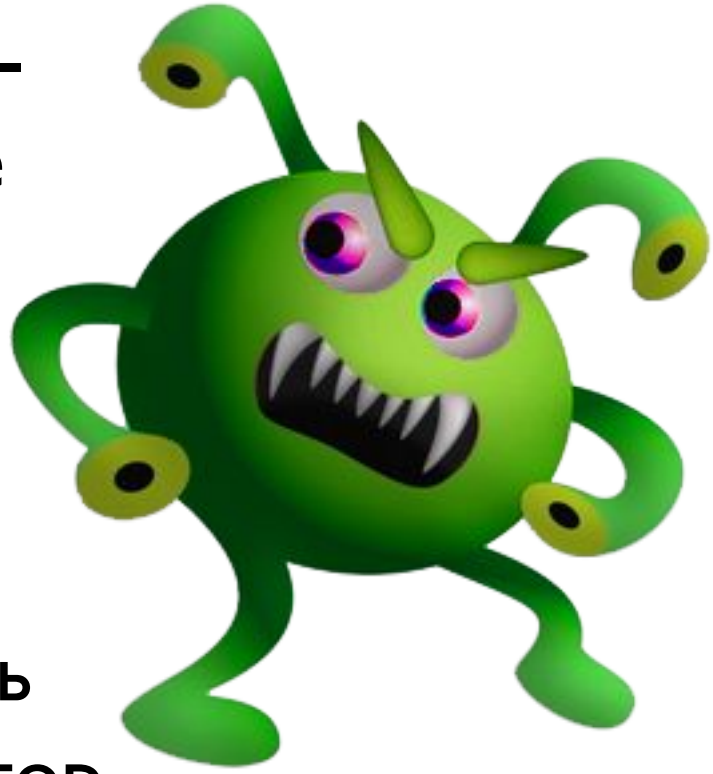
- ***файловые;***
- ***загрузочные;***
- ***макровирусы;***
- ***сетевые.***

Файловые вирусы

Либо различными способами внедряются в выполняемые файлы (наиболее распространённый тип вирус), либо создают файлы-двойники (вирусы-компаньоны), либо используют особенности организации файловой системы (link-вирусы).

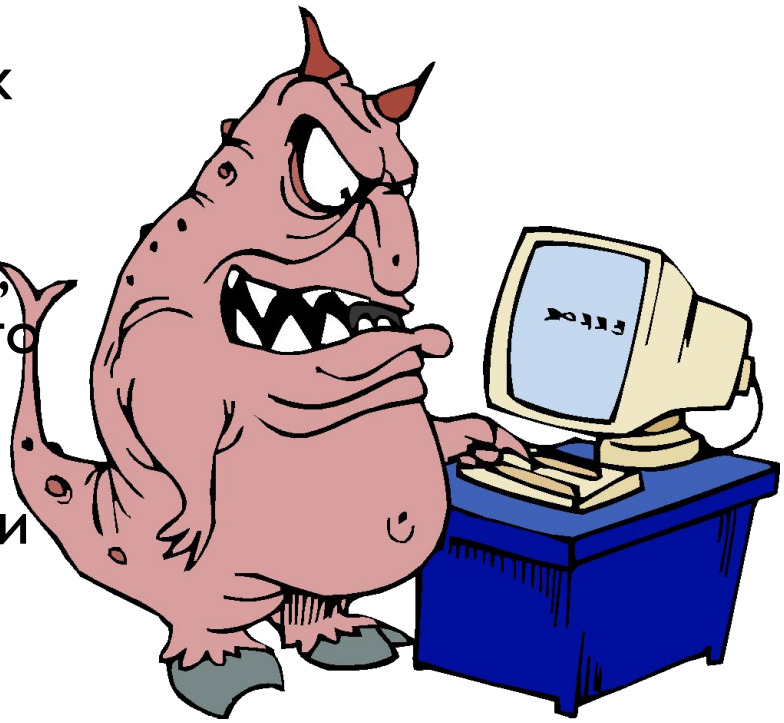
Загрузочные вирусы

- *Загрузочные вирусы* - заражают загрузочные сектора дисков (boot-сектор), либо главную загрузочную запись (Master Boot Record), либо меняют указатель на активный boot-сектор.



Макровирусы

Макровирус — это разновидность компьютерных вирусов, разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office. Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносятся из одного зараженного файла в другие. Большая часть таких вирусов написана для MS Word.



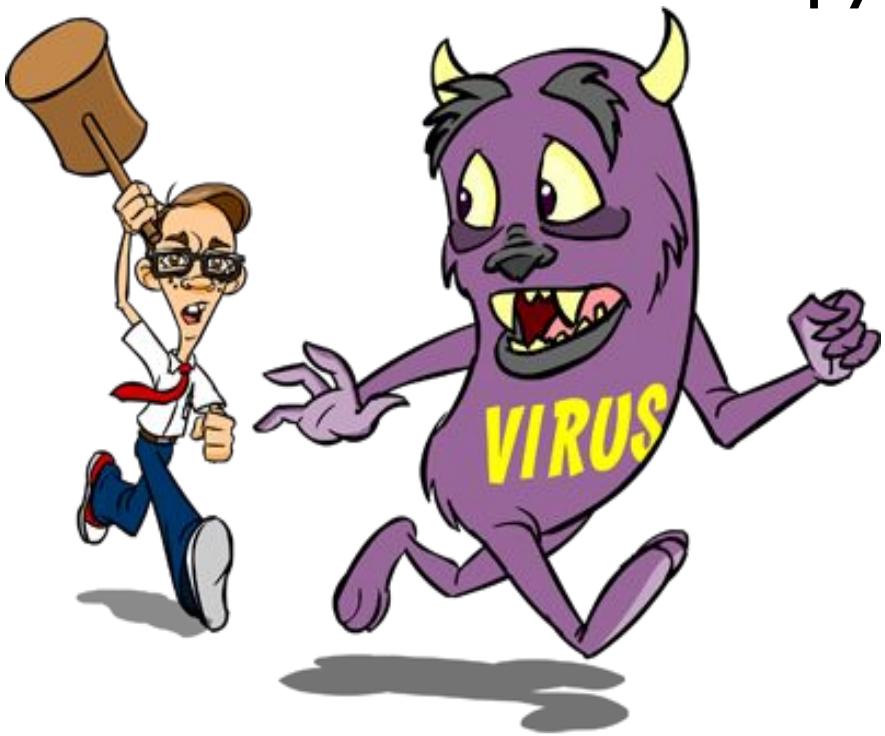
Сетевые вирусы.

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. "Полноценные" сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, "подтолкнуть" пользователя к запуску зараженного файла.

Обнаружение и удаление компьютерных вирусов.

Способы противодействия компьютерным вирусам можно разделить на:

- Профилактику вирусного заражения.
- Использование антивирусных программ



Виды антивирусных программ.

- *Сторожа или детекторы* – предназначены для обнаружения файлов зараженных известными вирусами, или признаков указывающих на возможность заражения;
- *Доктора* – предназначены для обнаружения и устранения известных им вирусов, удаляя их из тела программы и возвращая ее в исходное состояние;
- *Ревизоры* – они контролируют уязвимые и поэтому наиболее атакуемые компоненты компьютера, запоминают состояние служебных областей и файлов, а в случае обнаружения изменений сообщают пользователю;
- *Резидентные мониторы или фильтры* – постоянно находятся в памяти компьютера для обнаружения попыток выполнить несанкционированные действия. В случае обнаружения подозрительного действия выводят запрос пользователю на подтверждение операций;
- *Вакцины* – имитируют заражение файлов вирусами. Вирус будет воспринимать их зараженными и не будет внедряться.

Правила защиты.

- Применение комплекса антивирусных программ;
- Необходимо периодическое обновление антивирусных программ;
- Проверка информации поступающей из вне;
- Периодическая проверка всего компьютера;
- Осторожность с незнакомыми файлами, их действия могут не соответствовать названию.