

ВИРУС

- это одна из величайших загадок биологии



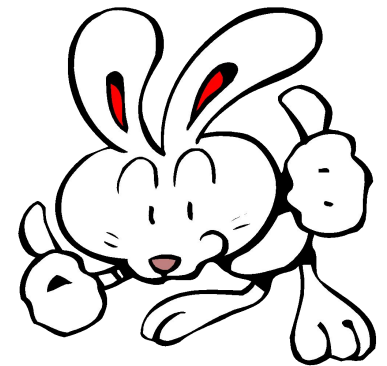
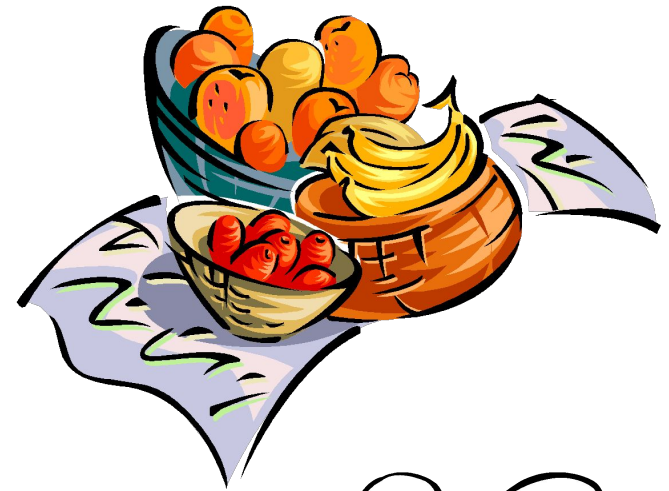
Вирус



- это нечто... имеющее ничтожно малые размеры, способное проникать в организм и вызывать заболевание почти у всех живых существ и размножающееся только в живых клетках.

Источники заражения вирусами

- Насекомые животные
- загрязненная пища
- Контакт с больным
- Зараженная пища
- Зараженная вода





Как противостоять вирусам

Прививки

Вакцина





- Это небольшие программы, которые путешествуют из одного компьютера в другой, оставаясь при этом незамеченными, приписывают себя в конец исполняемых файлов или «поселяется» в загрузочном секторе диска.

Как выглядят компьютерные вирусы



Phishing1



Phishing2



Phishing9



Netsky



Virut



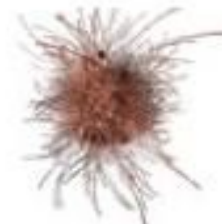
Parite / Netsky



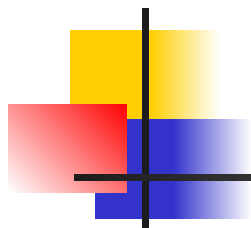
Russian3



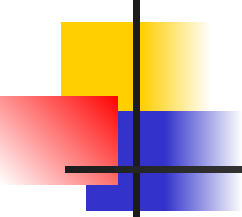
Degreesdiplomas



Scamfraud4198



- сам вирус невелик – его размер редко измеряется килобайтами. Однако натворить эта «КРОХА» может немало. В тот момент когда вы ничего не подозревая, запускаете на своем ПК зараженную программу или открываете документ вирус активизируется и заставляет компьютер следовать не вашим, а его вируса, инструкциям. И прости – прощай ваша информация!

- 
- Сегодня науке известно около 50 тысяч компьютерных вирусов – маленьких вредоносных программ, следующих в своей жизни только трем заповедям-

- ПЛОДИТЬСЯ! ПРЯТАТЬСЯ!
- ПОРТИТЬ!



Компьютерные вирусы

- Программы написанные хулиганами и вредителями или даже террористами



Наиболее известные разновидности вирусов.

сетевые черви

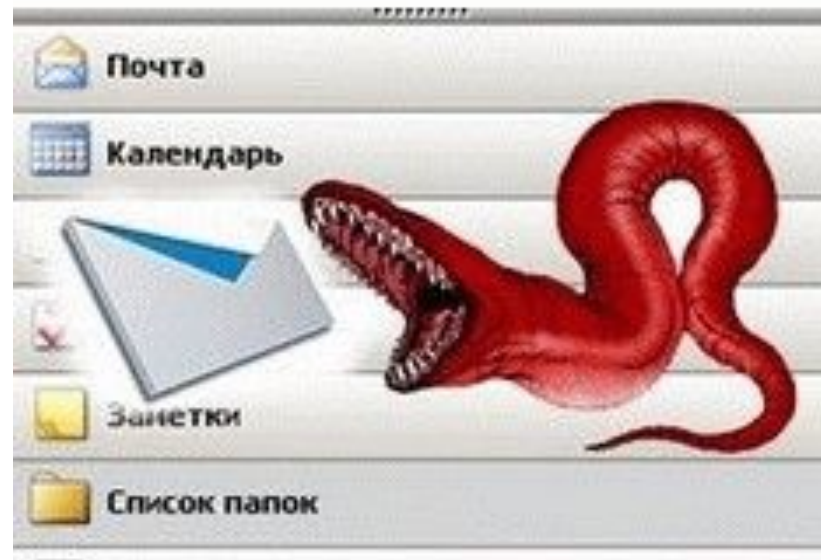
Троянские программы

Классические вирусы



Сетевые «Черви»

- В основном распространяются в виде вложений в электронные письма. Заразив компьютер, автоматически рассылают себя по всем адресам из вашей адресной книги.
- Также могут портить или удалять файлы определенных типов.



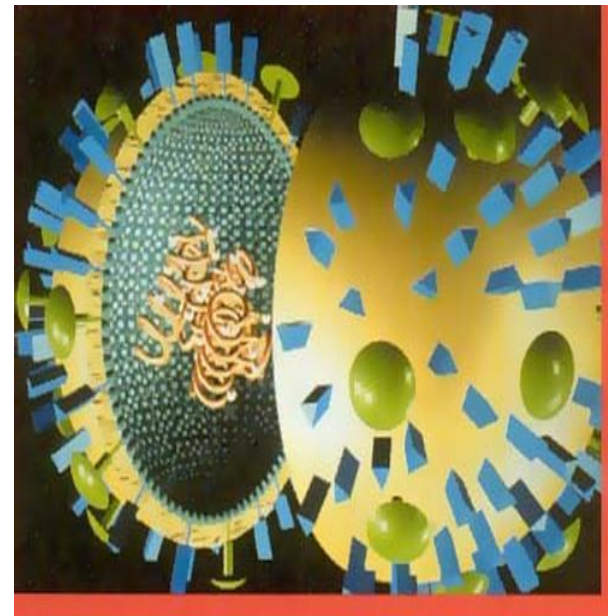
«Троянские программы»

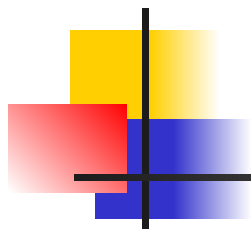


- Сравнительно молодая категория программ, которые чаще всего даже не относят к «классическим» вирусам. «Троянцы» занимаются не порчей, а воровством информации. Заразив ваш компьютер, эти программы могут отсылать на адрес своего создателя сведения о посещенных вами сайтах Сети, пароли для доступа, номера кредитных карточек и другое.

Классические вирусы

- Паразитируют на файлах определенных типов, например программах, или документах Microsoft Office(макровирусы). При открытии зараженного документа или программы заражают или уничтожают все остальные файлы этого типа на вашем ПК или в локальной сети.





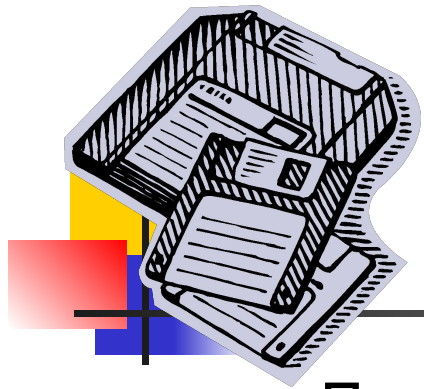
Основные классы вирусов

- Вирусы – спутники.
- Файловые вирусы.
- Загрузочные вирусы.
- Вирусы DIR.
- Макровирусы.



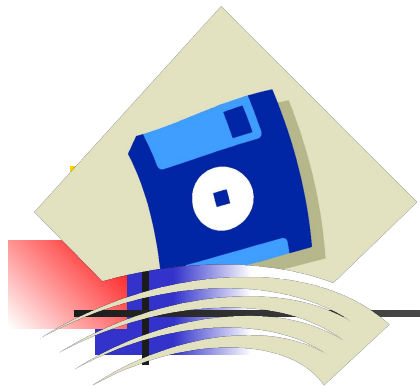
Вирусы - спутники

- наиболее примитивный тип вирусов.
- Для каждого файла с расширением .exe создают тот же файл с тем же именем, но с расширением .com, содержащий тела вируса. При запуске файла операционная система вначале ищет .com файлы, а потом .exe файлы. Поэтому вначале управление получает вирус, а затем он уже сам вызывает необходимый .exe файл.



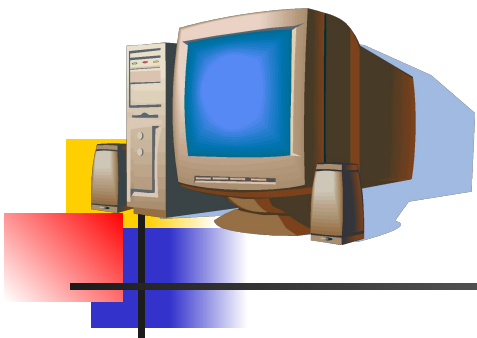
Файловые вирусы

- Поражают файлы с расширением .com, .exe. Эти вирусы дописывают свое тело в начало, середину или конец файла и изменяют его таким образом, чтобы первыми получить управление. Некоторые из этих вирусов не заботятся о сохранении заражаемого файла. В результате чего он оказывается неработоспособным; и что самое печальное, такой файл восстановить нельзя. Часть этих вирусов после запуска остается в памяти резидентно.



Загрузочные вирусы

- Поражают загрузочные сектора дисков. Инфицирование новых дисков происходит в тот момент, когда в зараженный компьютер вставляют новую дискету и начинают с ней работать.
- Часто вирус не помещается целиком в загрузочной записи, туда пишется только его начало, а продолжение тела вируса сохраняется в другом месте диска. После запуска остаются в памяти резидентно.



Вирусы DIR.

- Интересный класс вирусов появившийся недавно. Эти вирусы изменяют файловую систему диска очень хитрым образом. В таблице размещения файлов (FAT) для всех исполняемых файлов ссылки на начало заменяются ссылками на тело вируса. Адреса же начала файлов в закодированном виде помещаются в неиспользуемые элементы директории. В результате как только вы запускаете любую программу. Управление автоматически получает вирус. Он остается в памяти резидентно и при работе восстанавливает правильные ссылки на начала файлов. Если диск зараженный этим вирусом попадает на чистый компьютер, считать с него данные становится невозможным. При попытке протестировать файловую систему на экран выдается сообщение об огромном количестве ошибок, но стоит запустить хоть одну программу с зараженного диска, как файловая система тут же «восстанавливается». На самом деле происходит инфицирование еще одного компьютера.

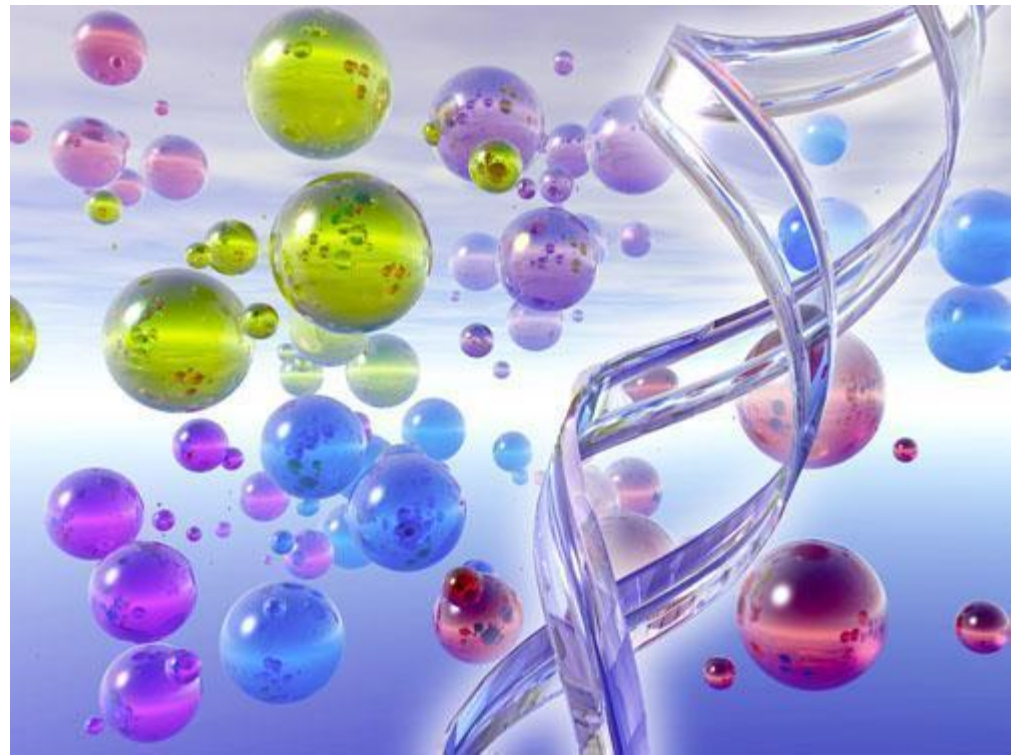


Макровирусы

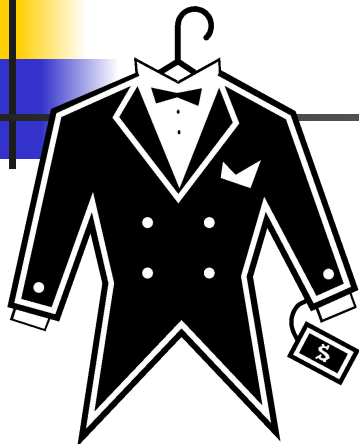
- Весьма оригинальный класс вирусов (хотя вирусами в полном смысле этого слова их даже нельзя назвать), заражающий документы, в которых предусмотрено выполнение макрокоманд (маленькие программки, некоторые из которых запускаются при загрузке файла в редактор и выполняют полезные действия по оформлению документа) вот в них и может забраться макровирус.
- Таким образом как только будет открыт зараженный документ, вирус получит управление и совершит все вредные действия, в частности найдет и заразит еще не зараженные документы.

Самомодифицирующиеся вирусы

- Вирусы которые очень трудно обнаружить



Вирусы - невидимки



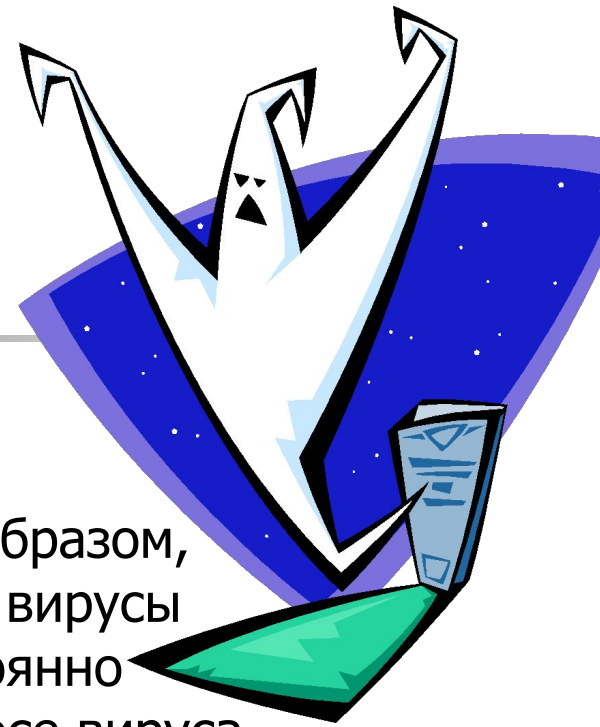
- Реализуют очень хитрый механизм, затрудняющий их обнаружение. При заражении эти вирусы остаются в памяти резидентно и при обращении к зараженным файлам и областям диска подменяют информацию так, что «заказчик» получает ее в незараженном исходном виде.



Вирусы - призраки

Маскируются с помощью другого механизма

Эти вирусы постоянно модифицируют себя таким образом, что не содержат одинаковых фрагментов. Такие вирусы хранят свое тело в закодированном виде и постоянно меняют параметры своей кодировки. При переносе вируса данного типа с одного компьютера на другой код вируса изменяется таким образом что уже не имеет ничего общего с предыдущим вариантом. А часть вирусов может самомодифицироваться и в пределах одного компьютера. Обнаружение таких вирусов весьма затруднено, хотя часть антивирусных программ пытается находить их по участкам кода, характерным для стартовой части.





Признаки появления вирусов

- Медленная работа компьютера
- Изменение даты и времени модификации файлов
- Вывод на экран непредусмотренных сообщений
- Частые зависания и сбои в работе компьютера

Случаи, когда можно заразить свой компьютер.



- Запуск исполняемой программы зараженной вирусом.
- Загрузка ПК с дискеты, содержащей загрузочный вирус.
- Подключение к системе зараженного драйвера
- Открытие документа зараженного макровирусом
- Установка на компьютере зараженной операционной системы.

Компьютер не может быть заражен, если:

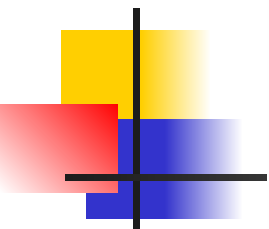


- На него переписывались текстовые и графические файлы, файлы данных и информационные файлы (за исключением файлов, предусматривающих выполнение макрокоманд).
- На нем производилось копирование с одной дискеты на другую при условии, что ни один файл с дискет не запускался.
 - На компьютере производится обработка принесенных извне текстовых и графических файлов
 - Переписывание на компьютер зараженного вирусом файла еще не означает заражения его вирусом. Чтобы заражение произошло, нужно либо запустить зараженную программу, либо открыть зараженный документ(либо, естественно загрузиться с зараженной дискеты)

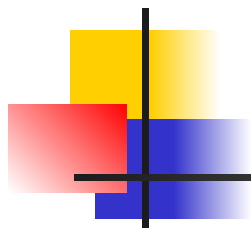
Правила которые необходимо соблюдать



- Эти правила нужно соблюдать всегда.
- Нарушив их всего один раз, вы рискуете заразить свой компьютер,
- А гораздо проще предотвратить заболевание, чем заниматься потом его лечением.



Профилактические меры.



- Все важные программы и данные необходимо иметь вне компьютера: сохранять на дискетах, дисках и т.д.
- Это позволит в случае порчи вирусом или из – за сбоев в работе оборудования быстро восстановить потерянную информацию.
- Любые программы и драйверы которые вы собираетесь использовать на ПК перед первым запуском, обязательно необходимо проверить на наличие вирусов программами – детекторами (эти программы позволяют проверить файлы на инфицированность их вирусом.)

Современные антивирусные программы - детекторы



- Обычно состоят из нескольких модулей, каждый из которых занимается своим специфическим делом.

Типы модулей, составляющих антивирусы.

- Антивирусный монитор (сторож)
- Антивирусный сканер
- Модуль автоматического обновления
- Программа – планировщик
- Модуль защиты электронной почты
- Модуль защиты документов Microsoft Office
- Центр управления.



Как работать с антивирусами

- **Выключить(включить) постоянную защиту** – для тех, кто включает антивирусный монитор только на время работы в Интернете.
- **Открыть антивирус** - появляется окно центра управления, откуда можно запустить любые операции и настроить любые режимы.
- **Обновить антивирусные базы**- запускается скачивание самых свежих данных о вирусах
- **Проверить мой компьютер на вирусы**- запускается полная проверка всех дисков.





Антивирус Касперского

- Самый популярный и умелый из отечественных вирусов
- Способен дать хороший отпор вирусам
- По всем параметрам Касперский идеальная программа для домашнего пользователя.



Doctor Web

- Позволяет обезвредить не только уже известные программе и занесенные в базу данных, но и новые еще не опознанные вирусы
- Эта программа работает значительно быстрее всех своих громоздких конкурентов



Norton Anti Virus

обладатель самой большой базы вирусов

Идеология программы – тотальный контроль
практически без участия пользователя

Недостаток – очень медлительный и занимает много
места



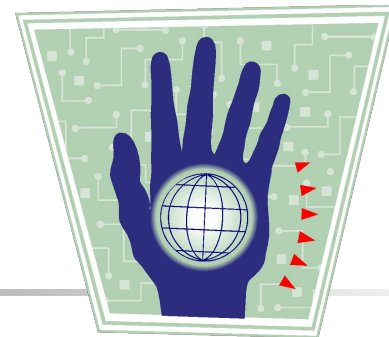
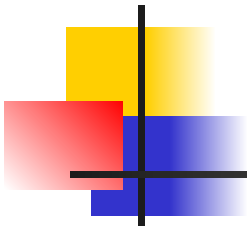


Внимание!!!



правила безопасности

- Поставьте антивирус и почаще обновляйте его антивирусную базу, это можно делать через Интернет или у фирмы – продавца.
- Каждую неизвестную программу надо проверять.
- Не перекачивайте с Сети программы, которые находятся в сомнительных местах
- Ни шагу в Интернете без антивирусного монитора.
- Обязательно установите себе программу – брандмауэр(программа для контроля за передачей информации из Сети) и внимательно читайте ее сообщения.
- Никогда не ставьте два антивируса сразу, они будут страшно мешать друг другу и всем остальным программам.



- Берегите ваш компьютер от инфицирования вирусом и он вам прослужит много лет.
- Предупреждать заболевание легче чем лечить!!