'Презентация подготовлена для конкурса
'Интернешка" *http://interneshka.org/*"

Презентация на тему*:*
«Компьютерные вирусы. Антивирусные программы.»

Выполнил ученик *10*-А класса
МБОО «Лицей № *2*» г. Буинска
Сафиуллин Булат

Руководитель*:*

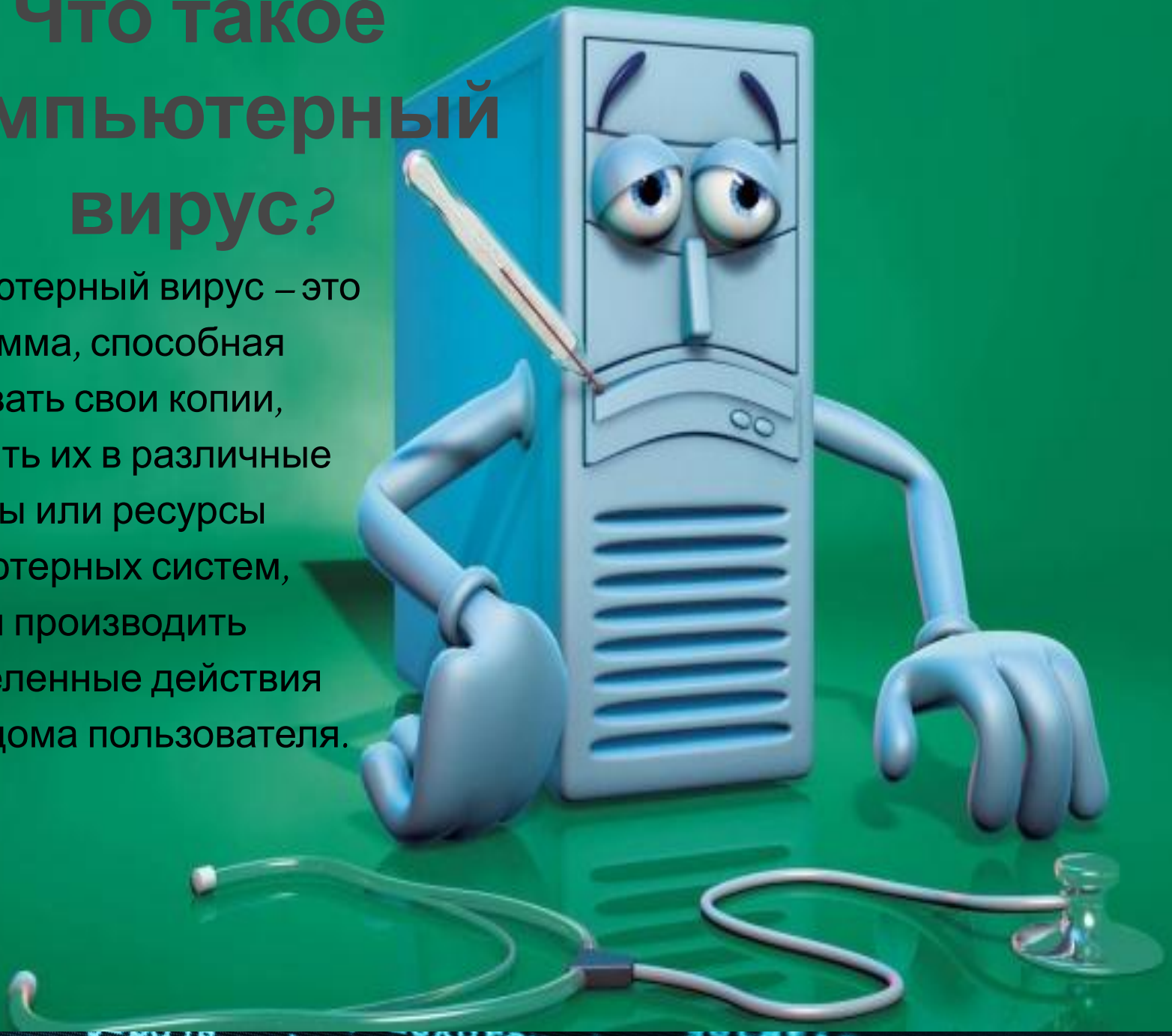
Мулеева Анастасия Юрьевна

учитель информатики.

Компьютерные вирусы

Что такое компьютерный вирус?

Компьютерный вирус – это программа, способная Создавать свои копии, внедрять их в различные объекты или ресурсы компьютерных систем, сетей и производить определенные действия без ведома пользователя.



Первые компьютерные вирусы

В *1971* году появился на свет первый компьютерный вирус *Creeper*. Данный «**червь**» был написан сотрудником компании в *1971* году, эта компания начинала заниматься обслуживанием *ARPANET* - сети, которая была создана в *1969* году Агентством министерства обороны США по перспективным исследованием и она предшествовала Интернету.

Creeper не являлся полноценным вирусом, он занимался поиском по сети компьютеров, затем мог самостоятельно скопировать на них и вывести на терминале сообщение: Я Крипер, поймай меня, если сможешь! (*«I'm the creeper, catch me if you can!»*). В том случае, если *Creeper* уже обнаружил на машине существующую копию самого себя, то «перепрыгивал» на другую машину.

В *1982* году появился другой опасный вирус - *Elk Cloner*. Данного «червя», который проникал на машины через дискеты, смог разработать *15*-летний подросток. Вирус *Jerusalem* был создан в *1987* году, он удалял любые программы на системе, которая была заражена вирусом, каждую пятницу *13* числа.

Цель компьютерного вируса

Целью вируса является нарушение работы программно аппаратных комплексов:

удаление файлов, приведение в негодность структур размещения данных, блокирование работы пол иведение в негодность

аппаратных комплексов компьюте

Основные пути проникновения вирусов

- Съемные носители (съемные винчестеры, флеш-память, компакт-диски *CD* и *DVD*), на которых находятся зараженные вирусом файлы
- Компьютерные сети и их сервисы, в том числе система электронной почты и *World Wide Web*
- Жесткие диски, на которые проник вирус в результате работы с зараженными программами
- Вирус, который остался в оперативной памяти после работы предшествующего пользователя с зараженными программами

Признаки заражения ПК вирусом

- медленная работа компьютера;
- зависания и сбои в работе компьютера;
- изменение размеров файлов;
- уменьшение размера свободной оперативной памяти;
- значительное увеличение количества файлов на диске;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- частые зависания и сбои в работе компьютера;
- И другие признаки.

Профилактика вирусов

- Использовать только лицензионные программные средства
- Проверять компьютер на наличие вирусов
- Иметь последние версии антивирусных средств
- Делать архивные копии файлов
- Выбрать высокий уровень безопасности в «Свойствах обозревателя»
- Не открывать вложения электронного письма, если отправитель неизвестен
- Иметь специальный загрузочный диск
- Добавить в файл автозагрузки антивирусную программу сторож
- Проверять все поступающие данные на наличие вирусов

Классификация компьютерных вирусов

По разрушительным возможностям

По способу заражения

По среде обитания

Классификация по разрушительным возможностям

Безвредные	не влияют на работу ПК, лишь уменьшают объем свободной памяти на диске, в результате своего размножения.
Неопасные	влияние, которых ограничивается уменьшением памяти на диске, графическими, звуковыми и другими внешними эффектами.
Опасные	приводят к сбоям и зависаниям при работе на ПК.
Очень опасные	приводят к потери программ и данных (изменение, удаление), форматированию винчестера и тд.

Классификация по среде обитания

Сетевые	вирусы, которые распространяются по различным компьютерным сетям (локальным, беспроводным или через Интернет)
Файловые	вирусы, заражающие исполнительные файлы и загружающиеся после запуска зараженных программ, в которых они находятся
Загрузочные	вирусы, которые внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки ОС с системного диска
Файлово-загрузочные	вирусы, которые способны заражать и файлы, и загрузочные секторы

По способу заражения

Резидентные	вирусы, оставляющие в оперативной памяти свою резидентную (постоянную) часть, которая потом перехватывает обращения к заражаемым программам и внедряется в них
Нерезидентные	вирусы, которые не заражают оперативную память и проявляются лишь при запуске инфицированной программы.

По особенностям алгоритма работы различают:

- Простейшие вирусы (вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов, поэтому его достаточно легко обнаружить.)
- Вирусы-спутники (вирус, который не внедряется в сам исполняемый файл, а создает его зараженную копию с другим расширением.)
- Стелс-вирус «невидимка» (вирусы, скрывающие свое присутствие в зараженных объектах, подставляя вместо себя незараженные участки.)
- Полиморфные вирусы (вирусы, модифицирующие свой код таким образом, что копии одного и того же вируса не совпадали.)
- Макровирус (вирусы, которые заражают документы офисных приложений.)
- Троянская программа (программа, которая маскируется под полезные приложения (утилиты или даже антивирусные программы), но при этом производит различные шпионские действия.)
- Черви (это вредительские компьютерные программы, которые

Антивирусные программы

Антивирусная программа -

программа, предназначенная для борьбы с компьютерными вирусами.

В своей работе эти программы используют различные принципы для поиска и

лечения зараженных файлов. Для нормальной работы на ПК каждый

пользователь должен следить за обновлением антивирусов. Если антивирусная

программа обнаруживает вирус в файле, то она удаляет из него программный код

ви[illegible]но, то зараженный файл удаляется

Типы антивирусных программ

- Антивирусные сканеры – после запуска проверяют файлы и оперативную память и обеспечивают нейтрализацию найденного вируса
- Антивирусные сторожа (мониторы) – постоянно находятся в ОП и обеспечивают проверку файлов в процессе их загрузки в ОП
- Полифаги – самые универсальные и эффективные антивирусные программы. Проверяют файлы, загрузочные сектора дисков и ОП на поиск новых и неизвестных вирусов. Занимают много места, работают не быстро
- Ревизоры – проверяют изменение длины файла. Не могут обнаружить вирус в новых файлах (на дискетах, при распаковке), т.к. в базе данных нет сведений о этих файлах
- Блокировщики – способны обнаружить и остановить вирус на самой ранней стадии его развития (при записи в загрузочные сектора дисков). Антивирусные блокировщики могут входить в *BIOS Setup*

Краткий обзор антивирусных программ.

При выборе антивирусной программы необходимо учитывать не только процент обнаружения вирусов, но и способность обнаруживать новые вирусы, количество вирусов в антивирусной базе, частоту ее обновления, наличие дополнительных функций.

В настоящее время серьезный антивирус должен уметь распознавать не менее *25000* вирусов. Это не значит, что все они находятся "на воле". На самом деле большинство из них или уже прекратили свое существование или находятся в лабораториях и не распространяются. Реально можно встретить *200-300* вирусов, а опасность представляют только несколько десятков из них.

Существует множество антивирусных программ. Рассмотрим наиболее известные из них.

Антивирус Касперского 2012

KASPERSKY lab

Защита из облака

Отчеты Настройка

Компьютер защищен

- **Угрозы:** отсутствуют
- **Компоненты защиты:** включены
- **Базы:** давно не обновлялись
- **Лицензия:** осталось 52 дня

Проверка Обновление Инструменты Виртуальная клавиатура

Справка Поддержка Личный кабинет Управление лицензиями

Dr.WEB

Спасибо за внимание!!!