

# КОМПЬЮТЕРНЫЕ ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ



**Ученица 9Б класса школы 54  
Г. Новоуральска  
Хасанова Анэлла**

- ▶ **Компьютерный вирус** – вид вредоносного программного обеспечения, способный создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а так же распространять свои копии по разнообразным каналам связи, с целью нарушения работы программно-аппаратных комплексов, удаления.



## *По масштабу вредных воздействий компьютерные вирусы делятся на:*

- \* ***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 потере программ и данных (изменение, удаление), форматированию винчестера и тд.

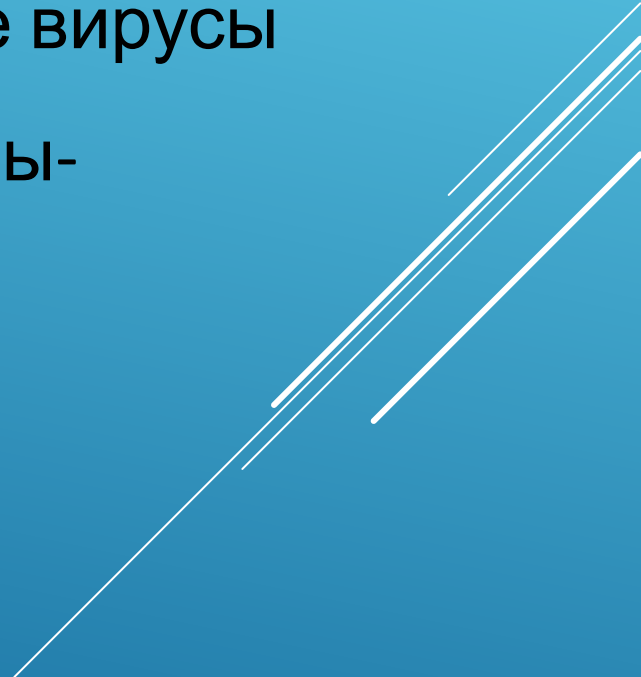
## Признаками появления вируса являются:

- замедление работы компьютера;
- невозможность загрузки операционной системы;
- частые зависания и сбои в работе компьютера;
- увеличение количества файлов на диске и их размеров;
- изменение времени и даты создания файлов;
- периодическое появление на экране монитора неуместных сообщений и т.п.



## ► Классификация компьютерных вирусов

*По среде обитания* различаются загрузочные вирусы (внедряются в сектор, содержащий программу загрузки системного диска), файловые вирусы (внедряются в основном в исполняемые файлы с расширением COM и EXE), сетевые вирусы (обитают в компьютерных сетях), системные вирусы (проникают в системные модули, поражают программы-интерпретаторы).

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.

► По степени воздействия вирусы подразделяются на:

неопасные вирусы – они не разрушают файлы, но могут переполнять оперативную и дисковую память, выводить на экран различные графические эффекты;

опасные вирусы – приводят к различным нарушениям в работе компьютера;

очень опасные вирусы – это вирусы разрушительные, они приводят к стиранию информации, полному или частичному нарушению работы прикладных программ.

## *По способу заражения вирусы подразделяются на:*

Резидентные вирусы – при заражении компьютера они оставляют в оперативной памяти свою резидентную часть, которая затем при каждом обращении к операционной системе и к другим объектам внедряется в них и выполняет свои разрушительные действия до выключения или перезагрузки компьютера;

Нерезидентные вирусы – не заражают оперативную память.



# ***По алгоритмической сущности* вирусы подразделяются на:**

вирусы -“черви” - распространены в компьютерных сетях;

вирусы-невидимки – перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо них незараженные объекты;

вирусы-мутанты – самовоспроизводясь, воссоздают копии, явно отличающиеся от оригинала;

вирус-“троянский конь” - это программа, которая, маскируясь под полезную программу, выполняет дополнительные функции, о которых пользователь не догадывается.



# ПРИМЕРЫ ВИРУСОВ

## Creeper

- ▶ Первый сетевой вирус Creeper появился в начале 70-х годов в военной компьютерной сети Arpanet, прототипе Интернета. Программа была в состоянии самостоятельно выйти в сеть через модем и сохранить свою копию на удаленной машине. На зараженных системах вирус обнаруживал себя сообщением: I'M THE CREEPER: CATCH ME IF YOU CAN. В целом, вирус был безобидным, но раздражал персонал.

# ПРИМЕРЫ ВИРУСОВ

## Brain

- ▶ Brain (1986) — первый вирус для IBM-совместимых компьютеров, вызвавший глобальную эпидемию. Он был написан двумя братьями-программистами — Баситом Фаруком и Амжадом Алви (Basit Farooq Alvi и Amjad Alvi) из Пакистана. Его отличительной чертой была функция подмены в момент обращения к нему зараженного сектора незараженным оригиналом. Это дает право назвать Brain первым известным стелс-вирусом.

# ПРИМЕРЫ ВИРУСОВ

## **Virdem**

- ▶ Немецкий программист Ральф Бюргер (RalfBurger) в 1986 г. открыл возможность создания программой своих копий путем добавления своего кода к выполняемым DOS-файлам формата COM. Опытный образец программы, получившей название Virdem, был продемонстрирован на форуме компьютерного андеграунда — ChaosComputerClub (декабрь, 1986, Гамбург, ФРГ). Это послужило толчком к написанию сотен тысяч компьютерных вирусов, частично или полностью использовавших описанные автором идеи. Фактически, данный вирус положил начало массовым заражениям.

# ПРИМЕРЫ ВИРУСОВ

## Jerusalem

- ▶ Самая известная модификация вирусного семейства резидентных файловых вирусов Suriv (1987) — творения неизвестного программиста из Израиля, Jerusalem, стала причиной глобальной вирусной эпидемии, первой настоящей пандемией, вызванной MS-DOS-вирусом. Таким образом, именно с данного вируса начались первые компьютерные пандемии (от греч. *pandemía* — весь народ) — эпидемии, характеризующиеся распространением на территорию многих стран мира.

# ПРИМЕРЫ ВИРУСОВ

## Червь Морриса

- ▶ Червь Морриса (ноябрь, 1988) — первый сетевой червь, вызвавший эпидемию. Он написан 23-летним студентом Корнельского университета (США) Робертом Моррисом, использовавшим ошибки в системе безопасности операционной системы Unix для платформ VAX и SunMicrosystems. С целью незаметного проникновения в вычислительные системы, связанные с сетью Arpanet, использовался подбор паролей (из списка, содержащего 481 вариант). Общая стоимость ущерба оценивается в 96 млн долл. Ущерб был бы гораздо больше, если бы червь изначально создавался с разрушительными целями.

# ПРИМЕРЫ ВИРУСОВ

## Chameleon

- ▶ Chameleon (начало 1990 г.) — первый полиморфный вирус. Его автор, Марк Уошбурн (Mark Washburn), за основу для написания программы взял сведения о вирусе Vienna из книги Computer Viruses. The Disease of High Technologies Ралфа Бюргера и добавил к ним усовершенствованные принципы самошифрации вируса Cascade — свойство изменять внешний вид как тела вируса, так и самого расшифровщика.

# ПРИМЕРЫ ВИРУСОВ

## Concept

- ▶ Concept (август, 1995) — первый макровирус, поражающий документы Microsoft Word. Именно в 1995 г. стало понятно, что заражаться могут не только исполняемые файлы, но и файлы документов.

# ПРИМЕРЫ ВИРУСОВ

## Win95.CIH

- ▶ В июне 1998 г. был обнаружен вирус тайваньского происхождения Win95.CIH, содержащий логическую бомбу для уничтожения всей информации на жестких дисках и порчи содержимого BIOS на некоторых системных платах. Дата срабатывания программы (26 апреля) совпадала с датой аварии на Чернобыльской атомной электростанции, вследствие чего вирус получил второе имя — «Чернобыль» (Chernobyl). Именно данный вирус показал уязвимость систем перезаписи BIOS. Таким образом, вдруг оказалось, что опасное ПО может вывести из строя не только информацию, но и компьютерное «железо».



## Профилактические меры

- v Не использовать сомнительные диски и другие носители информации
- v Ограничить доступ к файлам программ, устанавливая для них, когда возможно, статус «только для чтения»
- v При работе в сети, по возможности, не вызывайте программы из памяти других компьютеров.
- v Храните программы и данные в архивах на дисках и в разных подкаталогах жесткого диска.
- v Не копируйте программы для собственных нужд со случайных копий.
- v Обязательно иметь антивирусную программу

## Для защиты от компьютерных вирусов необходимо использовать:

- общие средства защиты информации, которые полезны для защиты не только от вирусов, но и от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.



**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 вируса. Если лечение невозможно, то зараженный файл удаляется целиком.

Типы антивирусных программ – полифаги, ревизоры, блокировщики, сторожа, вакцины и пр.



## *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

# Антивирусные программы

## *Антивирус Касперского*

Антивирус Касперского Personal предназначен для антивирусной защиты персональных компьютеров от всех известных вирусов, включая потенциально опасное ПО. Программа осуществляет постоянный контроль всех источников проникновения вирусов – электронной почты, интернета, дискет, компакт-дисков и т.д.

[HTTP://WWW.KASPERSKY.RU/ANTIVIRUS](http://www.kaspersky.ru/antivirus)



## **AVAST**

Антивирусная программа avast! v. home edition 4.7 (бесплатная версия) русифицирована и имеет удобный интерфейс, содержит резидентный монитор, сканер, средства автоматического обновление баз и т.д.

[HTTPS://WWW.AVAST.RU/INDEX](https://www.avast.ru/index)



## *Norton AntiVirus*

Состоит из одного модуля, который постоянно находится в памяти компьютера и осуществляет такие задачи как мониторинг памяти и сканирование файлов на диске. Доступ к элементам управления и настройкам программы выполняется с помощью соответствующих закладок и кнопок.

[HTTP://RU.NORTON.COM/ANTIVIRUS/](http://ru.norton.com/antivirus/)



# Антивирус Касперского 7.0

это классическая защита компьютера от вирусов, троянских и шпионских программ, а также от любого другого вредоносного ПО.

▶ [HTTP://WWW.KASPERSKY.RU/ANTIVIRUS](http://www.kaspersky.ru/antivirus)





# СПАСИБО ЗА ВНИМАНИЕ!

