



# *КОМПЬЮТЕРНЫЕ ВИРУСЫ И ЗАЩИТА ОТ НИХ*

Презентация  
Ученицы 11 класса А  
ГБОУ Школы Спектр  
Рау Дарьи



После заражения компьютера вирус может начать выполнение вредоносных действий и распространение своих копий, а также заставлять компьютер выполнять какие-либо действия.



Активация компьютерного вируса может вызывать уничтожение программ и данных и может быть связана с различными событиями (наступлением определенной даты или дня недели, запуском программ, открытием документа и т.д.).

## По величине вредных воздействий:



### НЕОПАСНЫЕ

(последствия действия вирусов - уменьшение свободной памяти на диске, графические и звуковые эффекты)

### ОПАСНЫЕ

(последствия действия вирусов - сбои и «зависания» при работе компьютера)

### ОЧЕНЬ ОПАСНЫЕ

(последствия действия вирусов - потеря программ и данных форматирование винчестера и т.д.)

**По способу сохранения и исполнения своего кода:**



**ЗАГРУЗОЧНЫЕ**

**ФАЙЛОВЫЕ**

**МАКРО-ВИРУСЫ**

**СКРИПТ-ВИРУСЫ**

## ЗАГРУЗОЧНЫЕ ВИРУСЫ

**Загрузочные вирусы** заражают  
загрузочный сектор гибкого или  
жесткого диска.



- При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке системы, и отдают управление не оригинальному коду загрузчика, а коду вируса.





- В 1986 году началась первая эпидемия загрузочного вируса. Вирус-невидимка «Brain» «заражал» загрузочный сектор дискет. При попытке обнаружения зараженного загрузочного сектора вирус незаметно «подставлял» его незараженный оригинал.

- Профилактическая защита от таких вирусов состоит в отказе загрузки операционной системы с гибких дисков и установке в BIOS компьютера защиты загрузочного сектора от изменений.

# ФАЙЛОВЫЕ ВИРУСЫ

**Файловые вирусы** внедряются в **исполняемые файлы** (командные файлы **\*.bat**, программы **\*.exe**, системные файлы **\*.com** и **\*.sys**, программные библиотеки **\*.dll** и др.) и обычно активируются при их запуске.



- После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным (т.е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.
- По способу заражения файловые вирусы разделяют на перезаписывающие вирусы, вирусы-компаньоны и паразитические вирусы.

- В 1999 году началась эпидемия файлового вируса Win95.CIH, названного «Чернобыль» из-за даты активации 26 апреля. Вирус уничтожал данные на жестком диске и стирал содержание BIOS.

Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на исполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами.

# МАКРО-ВИРУСЫ

**Макро-вирусы** заражают документы, созданные в офисных приложениях.



- Макро-вирусы являются макрокомандами (макросами) на встроенном языке программирования Visual Basic for Applications (VBA), которые помещаются в документ.

Макро-вирусы являются **ограниченно-резидентными**, т.е. они находятся в оперативной памяти и заражают документ, пока он открыт.

Макро-вирусы заражают шаблоны документов.

- В 1995 году началась эпидемия первого макро-вируса «Concept» для текстового процессора Microsoft Word. Макро-вирус «Concept» до сих пор широко распространен.

Профилактическая защита от макро-вирусов состоит в предотвращении запуска вируса (запрете на загрузку макроса).



# СКРИПТ-ВИРУСЫ

**Скрипт-вирусы** – активные элементы (программы) на языках **JavaScript** или **VBScript**, которые могут содержаться в файлах Web-страниц.

Заражение локального компьютера происходит при их передаче по Всемирной паутине с серверов Интернета в браузер локального компьютера.



В 1998 году появился первый скрипт-вирус VBScript.Rabbit, заражающий скрипты Web-страниц, а в мае 2000 года грянула глобальная эпидемия скрипт-вируса «LoveLetter».

Профилактическая защита от скрипт-вирусов состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.

## ДЛЯ ЗАЩИТЫ ОТ ВИРУСОВ МОЖНО ИСПОЛЬЗОВАТЬ:

- Общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- Профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- Специализированные программы для защиты от вирусов.





# Программы-детекторы

позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны".



# Программы-ревизоры

- имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

# Программы-фильтры

располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не "ловят" подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны - они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

# Программы-вакцины (Иммунизаторы)

модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.