

Компьютерные вирусы и защита от них

КОМПЬЮТЕРНЫЕ ВИРУСЫ

Компьютерные вирусы - это вредоносные программы, которые могут «размножаться» и скрытно внедрять свои копии **в исполнимые файлы, загрузочные секторы дисков и документы.**



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.).

КЛАССИФИКАЦИЯ ВИРУСОВ

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.)

КЛАССИФИКАЦИЯ ВИРУСОВ

По способу сохранения и исполнения своего кода:



ЗАГРУЗОЧНЫЕ

ФАЙЛОВЫЕ

МАКРО-ВИРУСЫ

СКРИПТ-ВИРУСЫ

ЗАГРУЗОЧНЫЕ ВИРУСЫ

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



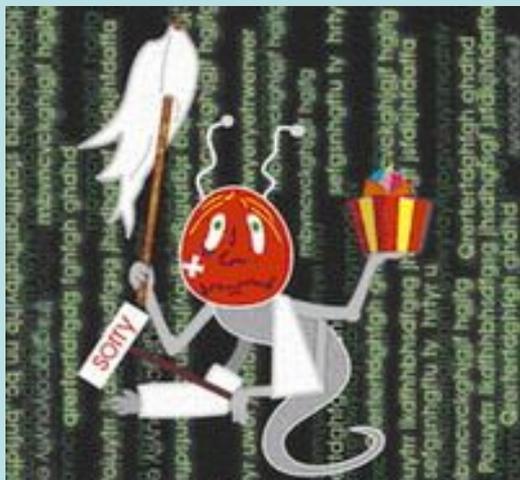
При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке системы, и передают управление не оригинальному коду загрузчика, а коду вируса.

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 от 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.

КОМПЬЮТЕРНЫЙ ПРАКТИКУМ

Защита от компьютерных вирусов

Задание. С помощью антивирусной программы *AntiVir Personal Edition*:

- настроить параметры антивирусного монитора (*Guard*) и антивирусного сканера (*Scanner*),
- проверить компьютер на наличие вирусов и при их обнаружении вылечить или удалить зараженные файлы.

The image displays four screenshots of the Avira AntiVir Personal Edition Classic software interface, illustrating the configuration steps for the Guard and Scanner modules. Blue arrows indicate the flow of the configuration process.

- Top-left screenshot:** The main interface with the **Configuration** button circled in red. A blue arrow points from this button to the Guard configuration window.
- Top-right screenshot:** The **Guard** configuration window. The **Expert mode** checkbox is checked and circled in red. The **Scan** section is circled in red, showing options for scan mode (Scan when reading and writing is selected), file extensions, and archive settings (Unpack runtime compressed files is checked).
- Bottom-left screenshot:** The main interface with the **Scanner** button circled in red. A blue arrow points from this button to the Scanner configuration window. The **Manual Selection** section is circled in red, showing selected drives: **Мой компьютер**, **Диск 3,5 (A:)**, and **Локальный диск (C:)**.
- Bottom-right screenshot:** The **Scanner** configuration window. The **Scanner** button is circled in red. The **Files** section is circled in red, showing options for file extensions and additional settings (Scan boot sectors of selected drives, Scan master boot sectors, Scan memory, Ignore offline files, and Search for Rootkits before scan are checked).