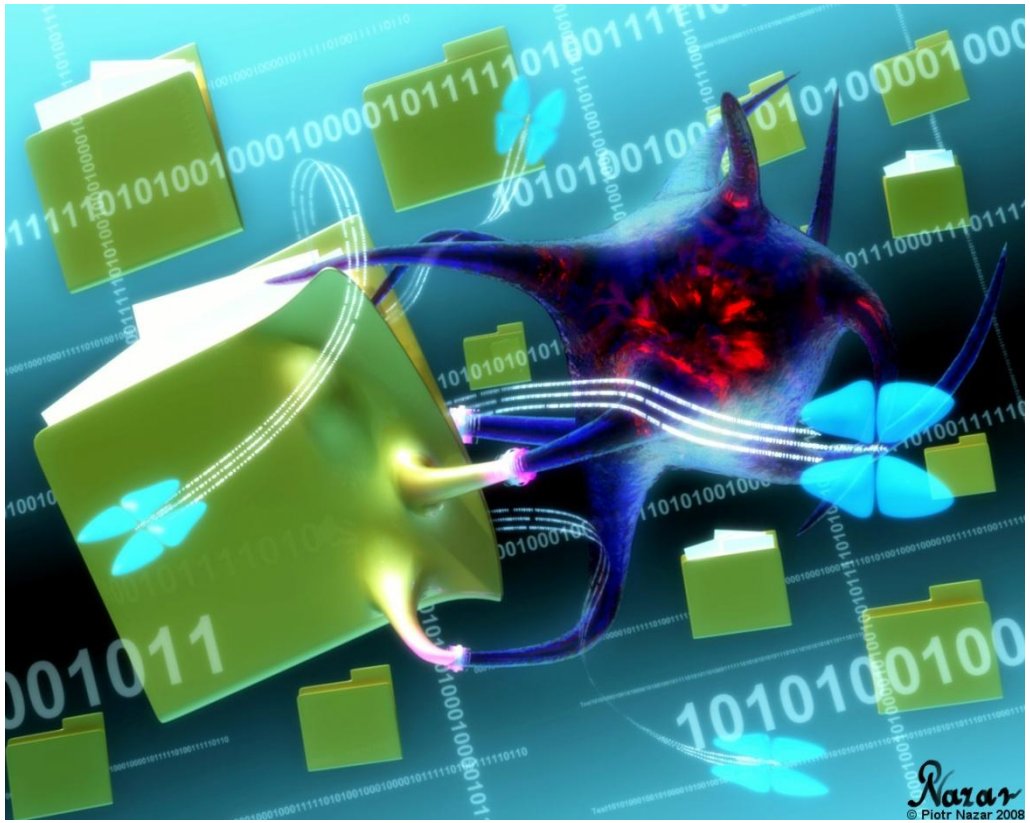
Научно- практическая работа

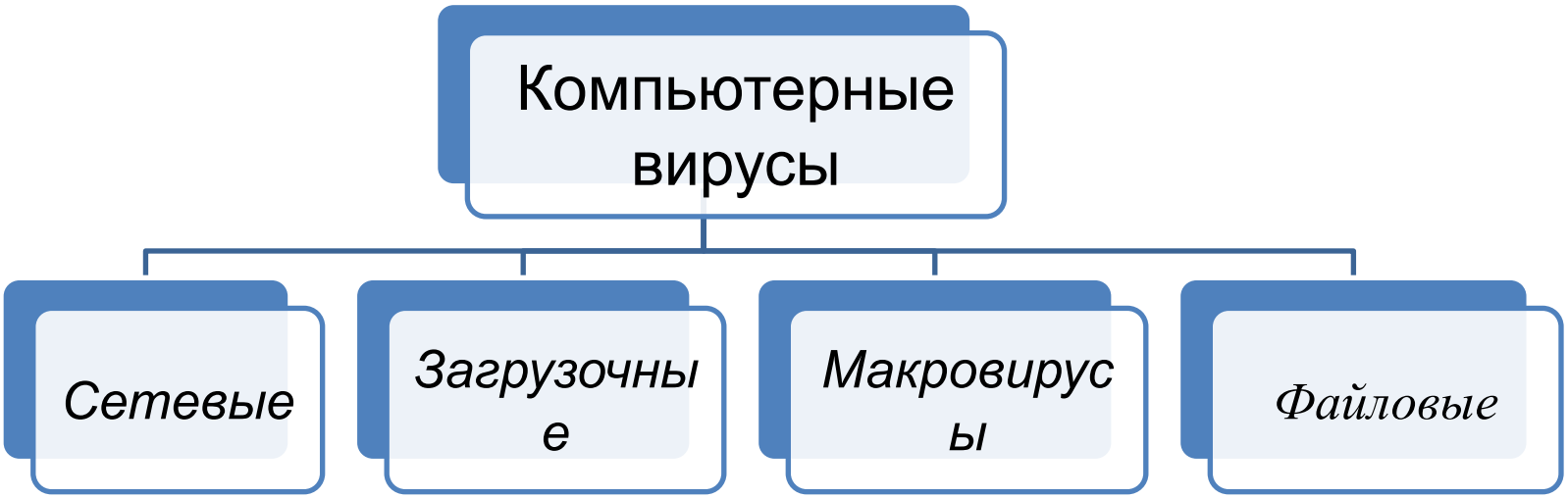
КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ

КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ



Компьютерные вирусы – это программа, которая способна создавать свои копии и внедрять их в различные объекты или ресурсы компьютерных, систем и т.д. без ведома пользователя.

КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ



ФАЙЛОВЫЕ ВИРУСЫ

Файловые вирусы различными способами внедряются в исполняемые файлы (программы) и обычно активизируются при их запуске. После запуска зараженной программы вирус находится в оперативной памяти компьютера и является активным (то есть может заражать другие файлы) вплоть до момента выключения или перезагрузки операционной системы.

При этом файловые вирусы не могут заразить файлы данных (например, файлы, содержащие изображение и звук).

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

ЗАГРУЗОЧНЫЕ ВИРУСЫ

Загрузочные вирусы записывают себя в загрузочный сектор диска. При загрузке операционной системы с заражённого диска вирусы внедряются в оперативную память компьютера. В дальнейшем загрузочный вирус ведёт себя так же как и файловый, то есть может заражать файлы при обращении к ним компьютера.

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

МАКРОВИРУСЫ

Макровирусы заражают файлы документов Word и электронных таблиц Excel. Макровирусы являются фактически макрокомандами (макросами), которые встраиваются в документ .

После загрузки заражённого документа в приложение макровирусы постоянно присутствуют в памяти компьютера и могут заражать другие документы. Угроза заражения прекращается только после закрытия приложения.

Профилактическая защита от макровирусов состоит в предотвращении запуска вируса. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов (потенциальных вирусов) и предлагается запретить их загрузку. Выбор запрета на загрузку макросов защитит ваш компьютер от заражения макровирусами, однако и может отключить полезные макросы, содержащиеся в документе

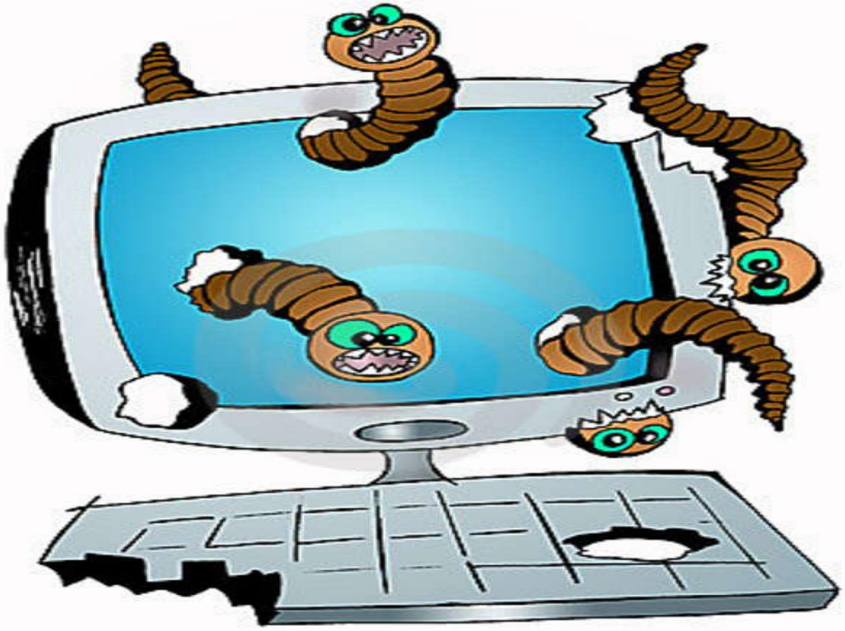
СЕТЕВЫЕ ВИРУСЫ

По компьютерной сети могут распространяться и заражать компьютеры любые обычные вирусы. Это может происходить при получении заражённых файлов с серверов файловых архивов. Однако существуют и специфические вирусы, которые используют для своего распространения электронную почту и Всемирную паутину. В частности, к ним относят:

- *Интернет- черви*
- *Троянские вирусы*
- *Скрипт- вирусы*

•Интернет черви

Интернет- черви (worm)- это вирусы, которые распространяются по компьютерной сети во вложенных в почтовое сообщение файлах. Автоматическая активизация червя и заражение компьютера могут произойти при просмотре сообщения. Опасность таких вирусов заключается в том, что они активируются по определённым датам и уничтожают файлы на дисках заражённого компьютера.



•Троянская программа (троянский вирус)

Троянская программа была названа в честь всем известного деревянного коня, с помощью которого греки захватили и уничтожили неприступную Трою. Как и троянский конь, одноименная программа выглядит безобидным и полезным подарком, а на деле оказывается коварным вирусом-сюрпризом. До установки распознать такой вирус практически невозможно. Некоторые трояны даже после установки продолжают выполнять функции программы, под которую были замаскированы. Размножаться такой вирус не может, но, запуская его, пользователь каждый раз возобновляет разрушительную деятельность в своем компьютере. Практически все вирусы этого типа состоят из клиента и сервера. Сервер внедряется в зараженную систему, а клиент используется преступникомом для управления ею.

Graphic Design by **Panda Software**

•Скрипт- вирусы

Данные вирусы, написаны на различных скрипт-языках (VBS, JS, BAT, PHP и т.д.). Они либо заражают другие скрипт-программы (командные и служебные файлы MS Windows или Linux), либо являются частями многокомпонентных вирусов. Также, данные вирусы могут заражать файлы других форматов (например, HTML), если в них возможно выполнение скриптов.

АНТИВИРУСНЫЕ ПРОГРАММЫ

Методы борьбы с вирусами и троянцами описаны во многих местах. К сожалению, единственный действенный метод -не включать компьютер вовсе.

Можно еще посоветовать ничего не устанавливать и ничего не запускать. Только тогда какой смысл иметь компьютер?

Поэтому широко используются антивирусы - программы, призванные обнаруживать и удалять известные им "нехорошие программы.

Наиболее представительными в настоящее время являются DrWeb, Eset NOD32, Kaspersky, McAfee Panda.

По способу действия выделяют следующую классификацию антивирусных программ.

- Полифаги
- Ревизоры
- Блокировщики

Рассмотрим основной принцип работы каждого типа:

Рынок антивирусных программ очень разнообразен

Полифаги

Принцип работы основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них неизвестных и новых вирусов.

Для поиска известных вирусов используются маски – некоторые последовательности программного кода, специфичные для каждого вируса. Если антивирусная программа обнаруживает такую последовательность в каком-либо файле, то программа выдает сообщение о зараженной файле и предлагает выполнить определённое действие (лечение, удаление, перемещение в карантин). Для поиска новых вирусов используется алгоритм сканирования (эвристическое сканирование) то есть анализ последовательности команд в проверяемом объекте. Если обнаруживается неизвестная последовательность, то полифаг выдаёт сообщение о возможности заражения файла. Полифаги так же могут обеспечить проверку файлов в процессе их загрузки в оперативную память. Такие программы образуют группу, называемую антивирусными мониторами.К достоинствам полифагов относится их универсальность. Однако такие программы занимают большие размеры, занимаемые антивирусными базами, содержащими информацию о максимально возможном количестве вирусов.