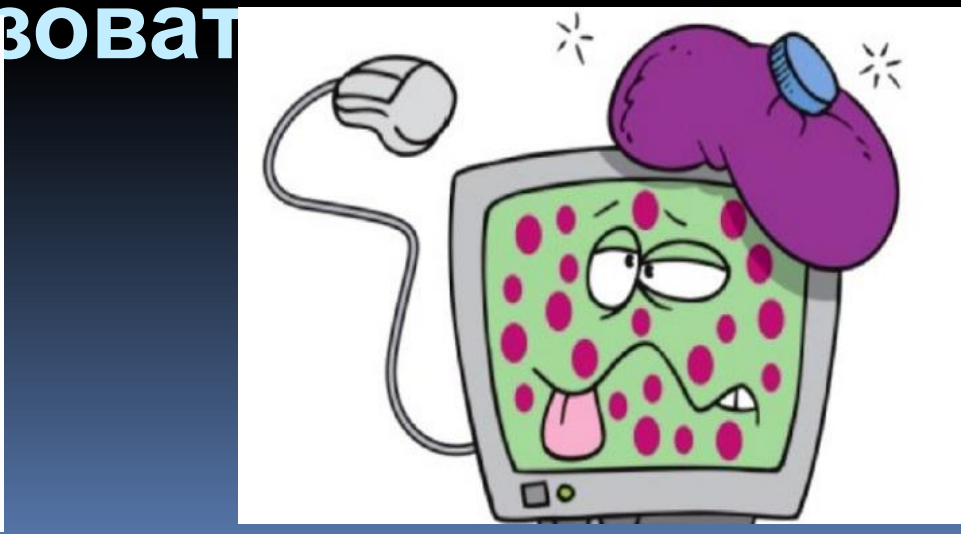
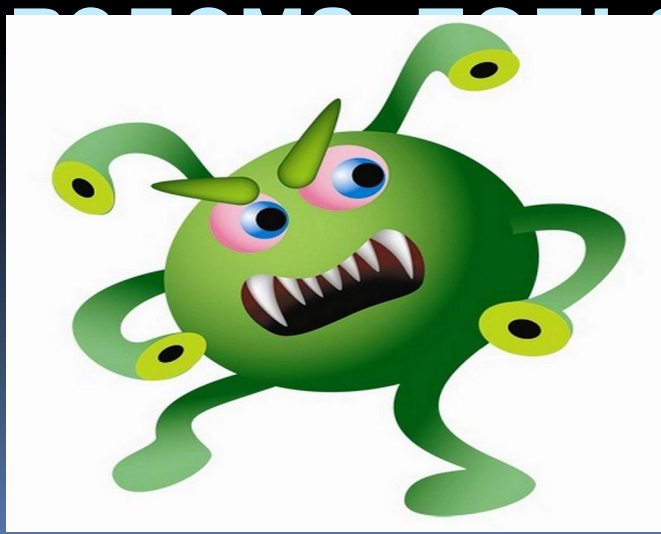




# **ВИРУСЫ** **И АНТИВИРУСНЫЕ** **ПРОГРАММЫ**

Выполнила: Сагитова Л.И.

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



Вirusy mogu razmnozhatsya, i skryto vnedryat svoi kopii v fayly, zagruzochnye sektora diskov i dokumenty. Aktivizatsiya virusa mozhety vyzvaty unichtozheniye programm i dannykh.. Perwaya epidemiyay proizoshla v 1986g (virus «Brain» - mozg po angl.) Vsemyrnayay epidemiyay zarazheniyay pochtovyym virusom nachalasy 5 mayay 2000g, kogdaya kompyutyery po seti Internet poluchily soobshcheniya «Yay tebyay lyublyu» s vlozhenным файлом, kotoryy i sodержал virus.

Отличительными особенностями компьютерных вирусов являются:

- 1) маленький объем;
- 2) самостоятельный запуск;
- 3) многократное копирование кода;
- 4) создание корректной работы



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,

## По среде обитания компьютерные вирусы бывают:

\* Файловые вирусы способны внедряться в программы и активизируются при их запуске. Из ОП вирусы заражают другие программные файлы (.com, .exe, .sys) меняя их код вплоть до момента выключения ПК. Передаются с нелегальными копиями популярных программ, особенно компьютерных игр. Но не могут заражать файлы данных (изображения, звук)

\* Загрузочные вирусы передаются через зараженные загрузочные сектора при загрузке ОС и внедряется в ОП, заражая другие файлы. Правила защиты: 1) Не рекомендуется запускать файлы сомнительного источника (например, перед загрузкой с диска А -

**\*Макровирусы** - заражают файлы документов Word и Excel. Эти вирусы являются фактически макрокомандами (макросами) и встраиваются в документ, заражая стандартный шаблон документов. Угроза заражения прекращается после закрытия приложения. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов и предлагается запретить их загрузку. Выбор запрета на макросы предотвратит загрузку от зараженных, но и отключит возможность использования полезных макросов в документе

**\* Сетевые вирусы** – распространяются по компьютерной сети.

При открытии почтового сообщения обращайтесь

**Антивирусная программа** - программа, предназначенная для борьбы с компьютерными вирусами.

В своей работе эти программы используют различные принципы для поиска и лечения зараженных файлов.

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

вируса.  
заражен



ТО  
М.



## 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

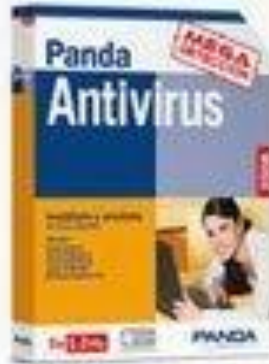
Полифаги – самые универсальные и эффективные антивирусные программы. Проверяют файлы, загрузочные сектора дисков и ОП на поиск новых и неизвестных вирусов.

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

# Рынок антивирусных программ довольно разнообразен





Спасибо за внимание!