

Презентация подготовлена для конкурса "Интернешка" <http://interneshka.org/>

# Компьютерные вирусы и антивирусные программы



**Автор:** Глухова Кристина, 9Б класс,  
**Руководитель:** Боженкина Н.Н., учитель информатики  
МБОУ Идринская СОШ, с.Идринское, Идринский район, Красноярский край

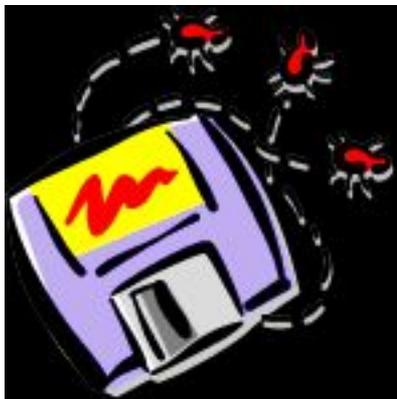
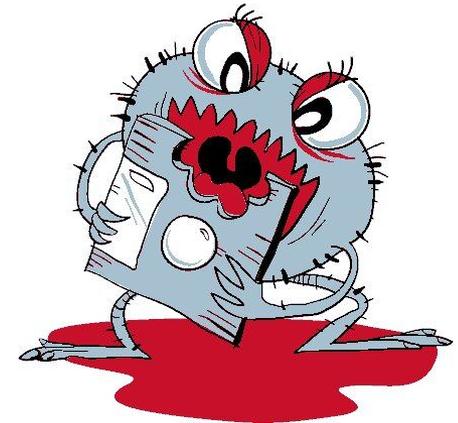
*Компьютерный вирус – специально созданная небольшая программа, способная к саморазмножению, засорению компьютера и выполнению других нежелательных действий*



# История компьютерных вирусов

**1971г.** - первый прототип вируса.

Программист Боб Томас, пытаясь решить задачу передачи информации с одного компьютера на другой, создал программу **Creeper**, самопроизвольно «перепрыгивавшую» с одной машины на другую в сети компьютерного центра. Эта программа не саморазмножалась, не наносила ущерба.



**1986г.** - первая «эпидемия» компьютерного вируса. Вирус по имени **Brain** «заражал» дискеты персональных компьютеров.

# Чем опасен компьютерный вирус

После заражения компьютера вирус может активизироваться и начать выполнять вредные действия по уничтожению программ и данных.

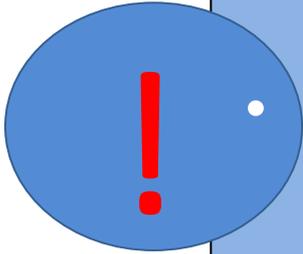
Активизация вируса может быть связана с различными событиями:

- наступлением определённой даты или дня недели
- запуском программы
- открытием документа



# Признаки заражения

- *общее замедление работы компьютера и уменьшение размера свободной оперативной памяти;*
- *некоторые программы перестают работать или появляются различные ошибки в программах;*
- *на экран выводятся посторонние символы и сообщения, появляются различные звуковые и видеоэффекты;*
- *размер некоторых исполнимых файлов и время их создания изменяются;*
- *некоторые файлы и диски оказываются испорченными;*
- *компьютер перестает загружаться с жесткого диска.*



# Классификация вирусов

---

**ФАЙЛОВЫЕ**

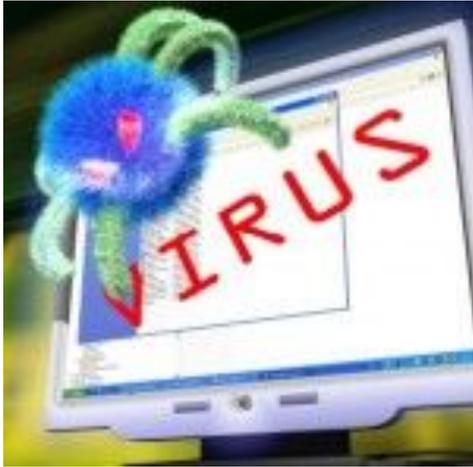
**МАКРОВИРУСЫ**

**СЕТЕВЫЕ ВИРУСЫ**



# Файловые вирусы

---



*Внедряются в программы и активизируются при их запуске. После запуска заражённой программой могут заражать другие файлы до момента выключения компьютера или перезагрузки операционной системы.*

Не рекомендуется запускать на исполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами.

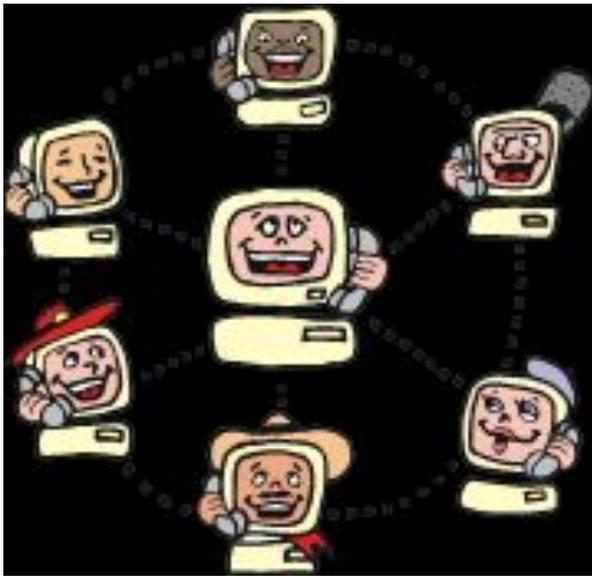
# Макровирусы



*Заражают файлы документов, например текстовых. После загрузки заражённого документа в текстовый редактор макровирус постоянно присутствует в оперативной памяти компьютера и может заражать другие документы. Угроза заражения прекращается только после закрытия текстового редактора.*

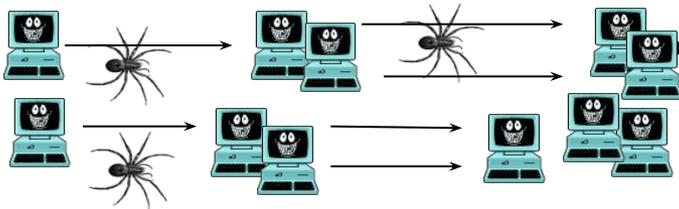
**Профилактическая защита от макро-вирусов состоит в предотвращении запуска вируса (запрете на загрузку макроса).**

# Сетевые вирусы



*Сетевые черви – программы, распространяющие свои копии по локальным или глобальным сетям с целью:*

- проникновения на удаленные компьютеры;*
- запуска своей копии на удаленном компьютере;*



*дальнейшего распространения на другие ПК*

*Передают по компьютерным сетям свой программный код и запускают его на компьютерах, подключённых к этой сети. Заражение сетевым вирусом может произойти при работе с электронной почтой, сетью Интернет.*

# Пути проникновения вирусов



*Глобальная сеть Internet*

*Электронная почта*

*Локальная сеть*

*Компьютеры «Общего назначения»*

*Пиратское программное обеспечение*

*Ремонтные службы*

*Съемные накопители*

# Методы защиты от вирусов

---



# Методы защиты от вирусов

---

- *Защита локальных сетей*
- *Использование дистрибутивного ПО*
- *Резервное копирование информации*
- *Использование антивирусных программ*
- *Не запускать непроверенные файлы*



# Антивирусные программы



*Обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ.*

# Критерии выбора антивирусных программ

---

- Надежность и удобство в работе
- Качество обнаружения вирусов
- Существование версий под все популярные платформы
- Скорость работы
- Наличие дополнительных функций и возможностей



# Разнообразие антивирусных программ

*avast! Free Antivirus*  
*Tor Browser Bundle*  
*Microsoft Security Essentials*  
*Avira Free Antivirus*  
*AVG AntiVirus Free*  
*360 Total Security*  
*Panda Free Antivirus*  
*Ad-Aware Free Antivirus+*  
*Comodo*  
*Zillya! Antivirus Free*  
*PC Tools AntiVirus Free*  
*Zillya! Antivirus Free*  
*PC Tools AntiVirus Free*  
*PC Tools ThreatFire*





## Памятка пользователю

- *Ограничить физический доступ к компьютеру, установить пароль на вход в систему и отключать доступ в Интернет, когда он не нужен;*
- *подписаться на информационные бюллетени Microsoft и регулярно обновлять операционную систему;*
- *отключить все неиспользуемые службы и закрыть порты, через которые могут осуществляться атаки;*
- *тщательно настроить все программы, работающие с Интернет, начиная с браузера например, запретить использование Java и ActiveX;*
- *установить и обновлять антивирусную программу;*
- *использовать брандмауэр;*
- *крайне аккуратно работать с почтой, а также программами для обмена сообщениями и работы с файлообменными сетями;*
- *никогда не запускать программы сомнительного происхождения, даже полученные из заслуживающих доверия источников, например, из присланного другом письма;*
- *ни при каких условиях не передавать по телефону или по почте свои персональные данные, особенно пароли;*
- *регулярно создавать резервные копии критических данных.*



**Спасибо за внимание!**