# КОМПЬЮТЕРНЫЕ

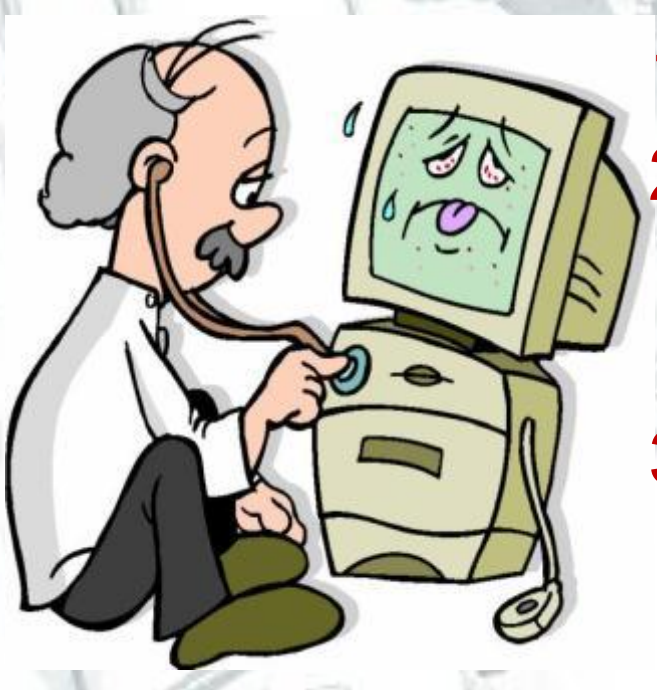
# ВИРУСЫ

ПОСЛУШАЙ

# МЕНЮ

1. Компьютерные вирусы.
2. Из истории компьютерных вирусов.
3. Опасность компьютерных вирусов.
4. Классификация компьютерных вирусов.

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



**Имеет:**

1. Способность к размножению.
2. Вред для здоровья человека и нежелательные действия для компьютера.
3. Скрытность, т.к. вирусы имеют инкубационный период.

# ИЗ ИСТОРИИ КОМПЬЮТЕРНЫХ ВИРУСОВ

**Первая «эпидемия»** компьютерного вируса произошла в 1986 году, когда вирус по имени Brain (англ. «мозг») «заражал» дискеты персональных компьютеров. В настоящее время известно несколько десятков тысяч вирусов, заражающих компьютеры и распространяющихся по компьютерным сетям.

Первый прототип вируса появился еще в 1971г. 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. Правда эта программа не саморазмножалась, не наносила ущерба.

Первые исследования саморазмножающихся искусственных конструкций проводилась в середине прошлого столетия учеными Джоном фон Нейманом и Норбертом Винером.

Джон фон Нейман

(1903 - 1957)

Норберт Винер

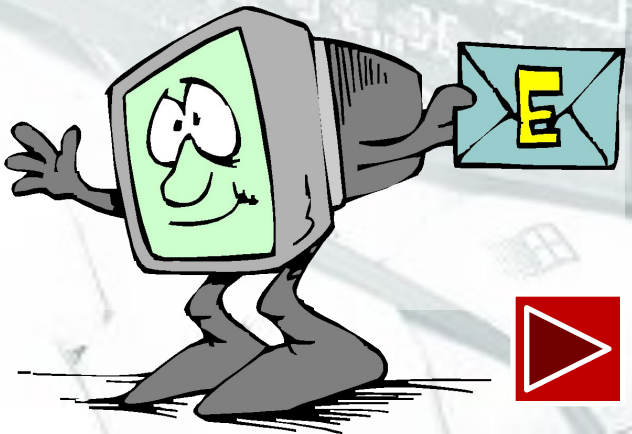
(1894 - 1964)

# ОПАСНОСТЬ КОМПЬЮТЕРНОГО ВИРУСА

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…*



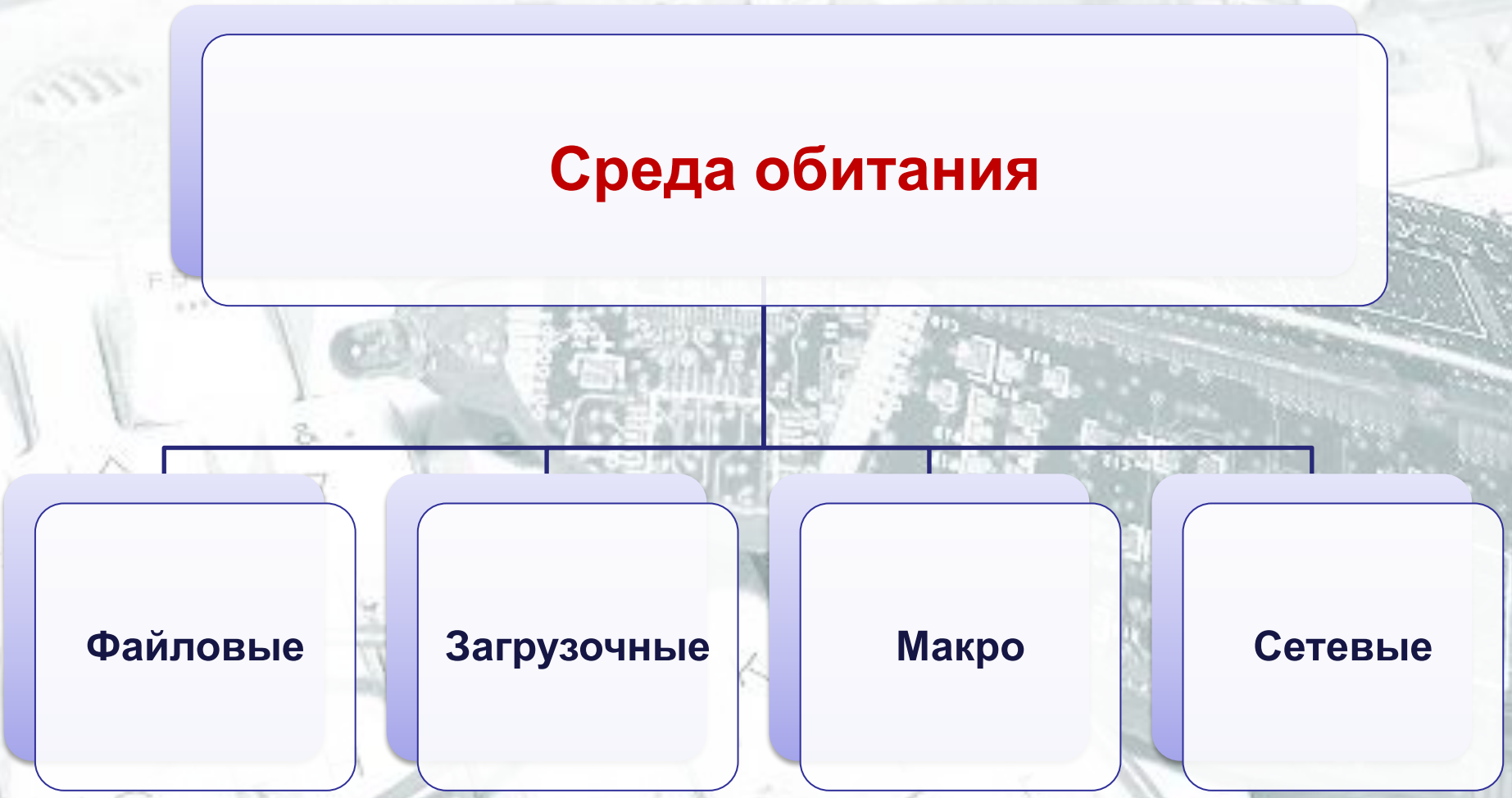
- *общее замедление работы компьютера и уменьшение размера свободной оперативной памяти;*
- *некоторые программы перестают работать или появляются различные ошибки в программах;*
- *на экран выводятся посторонние символы и сообщения, появляются различные звуковые и видеоэффекты;*
- *размер некоторых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

# КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

ПОСМОТРИ

# ПРИЗНАКИ КЛАССИФИКАЦИИ

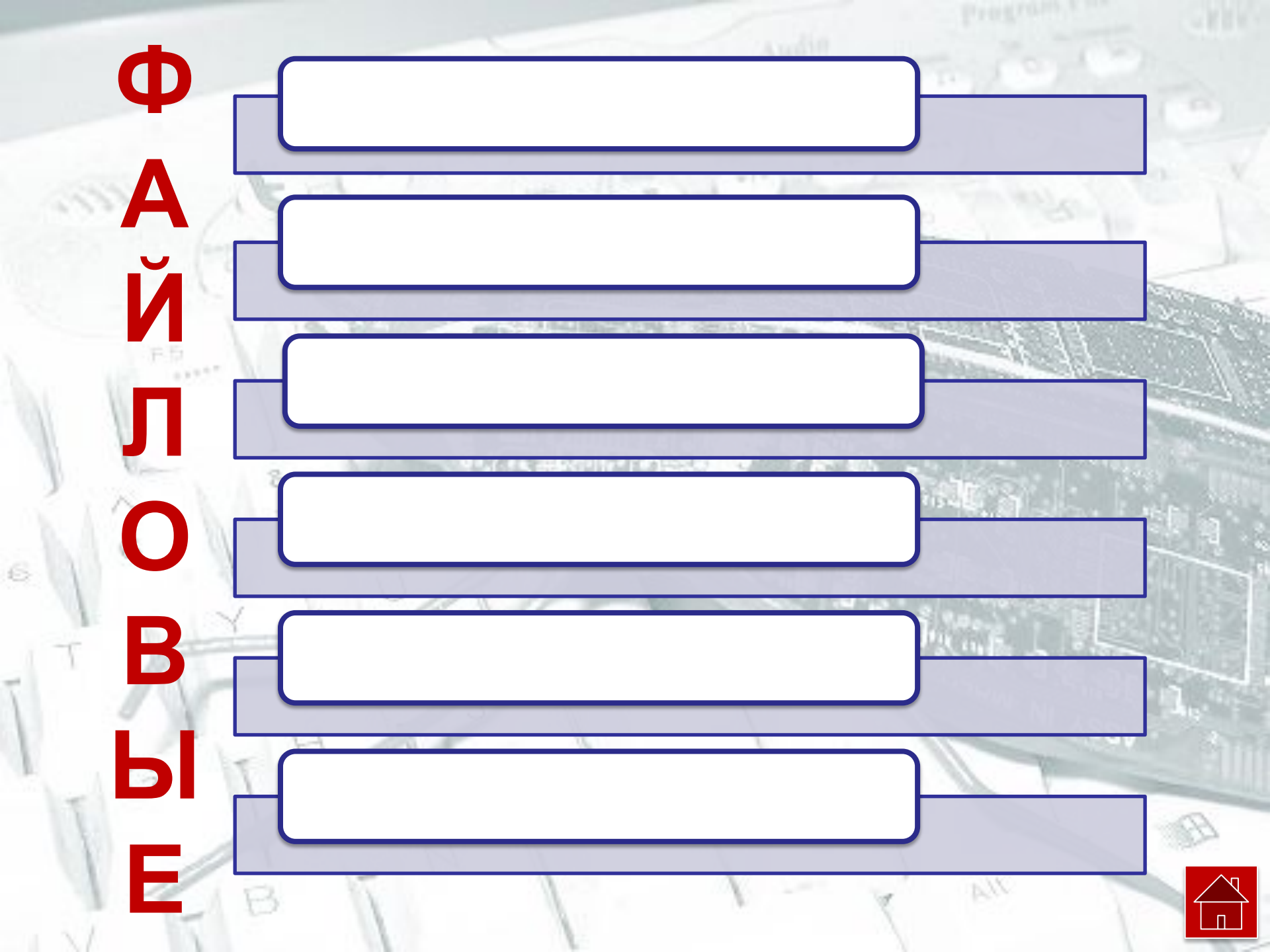
- Среда обитания
- Особенности алгоритма работы
- Операционная система
- Деструктивные возможности


Среда обитания
Файловые
Загрузочные
Макро
Сетевые

# 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.

# ФАЙЛОВЫЕ



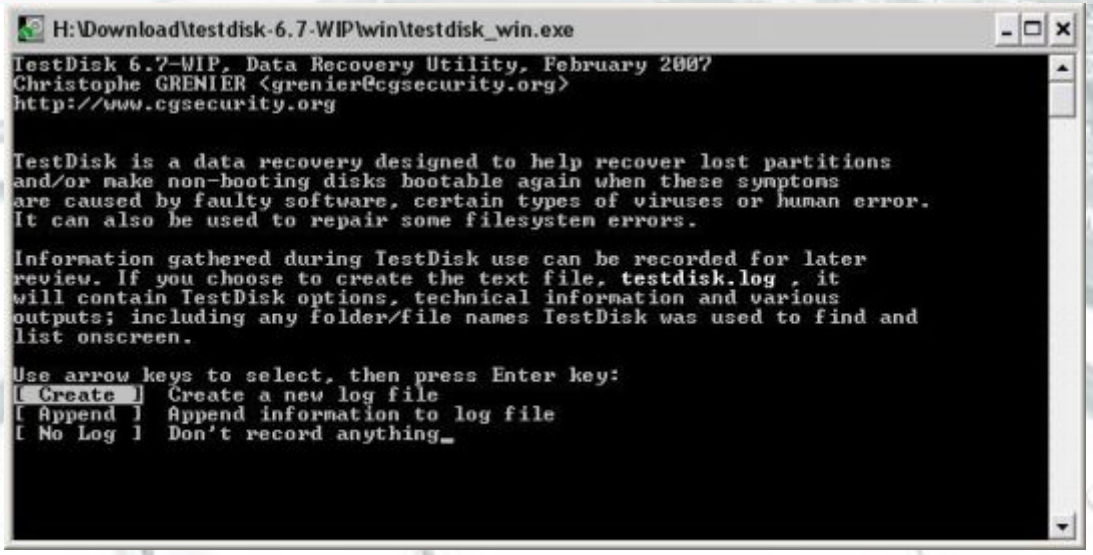
# Справочник:

1. Перезаписывающие вирусы. Записывают свое тело вместо кода программы, не изменяя название исполняемого файла, вследствие чего программа перестает запускаться.
2. Вирусы-компаньоны. Создают свою копию на месте заражаемой программы, но не уничтожают оригинальный файл, а переименовывают его или перемещают. При запуске программы вначале выполняется код вируса, а затем управление передается оригинальной программе.
3. Файловые черви создают собственные копии с привлекательными для пользователя названиями в надежде, что он их запустит.

4. Вирусы-звенья не изменяют код программы, а заставляют ОС выполнить свой код, изменяя адрес местоположения на диске зараженной программы, на собственный адрес.
5. Паразитические вирусы изменяют содержимое файла, добавляя в него свой код. При этом зараженная программа сохраняет полную или частичную работоспособность. Код может внедряться в начало, середину или конец программы.
6. Вирусы, поражающие исходный код программы. Вирусы данного типа поражают исходный код программы или ее компоненты (.OBJ, .LIB, .DCU). После компиляции программы оказываются встроенными в неё.

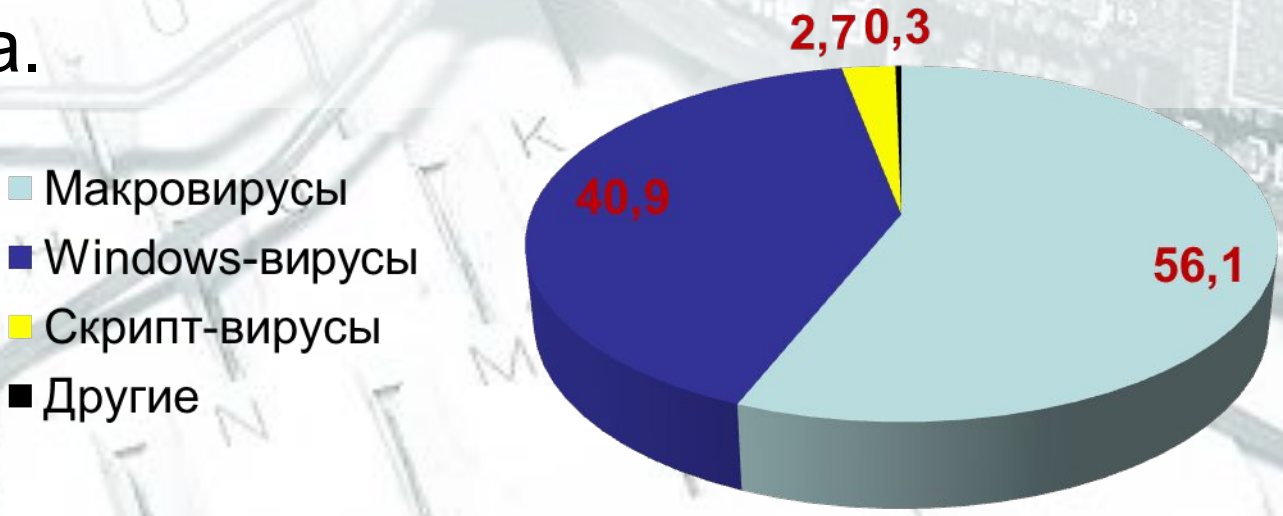
# ЗАГРУЗОЧНЫЕ ВИРУСЫ

Загрузочный вирус (англ. Boot viruses) — компьютерный вирус, записывающийся в первый сектор гибкого или жесткого диска и выполняющийся при загрузке компьютера. При включении или перезагрузки компьютера Boot-вирус заменяет собой загрузочный код



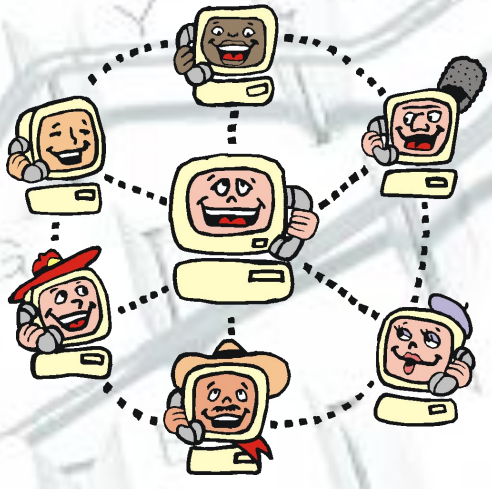
# МАКРОВИРУСЫ

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.



# СЕТЕВЫЕ ВИРУСЫ

Могут передавать по компьютерным сетям свой программный код и запускать его на компьютерах, подключённых к этой сети. Заражение сетевым вирусом может произойти при работе с электронной почтой или при «путешествиях» по Всемирной паутине.



# СЕТЕВЫЕ

- черви
- троян
- хакер