

# АНТИВИРУС

Что это такое?

# Основное понятие

## №1

- Компьютерный вирус – это программный код, встроенный в другую программу или документ, или в определённые области носителя данных и предназначенный для выполнения несанкционированных действий на несущем компьютере.

# Какие бывают вирусы...



# Важно знать!

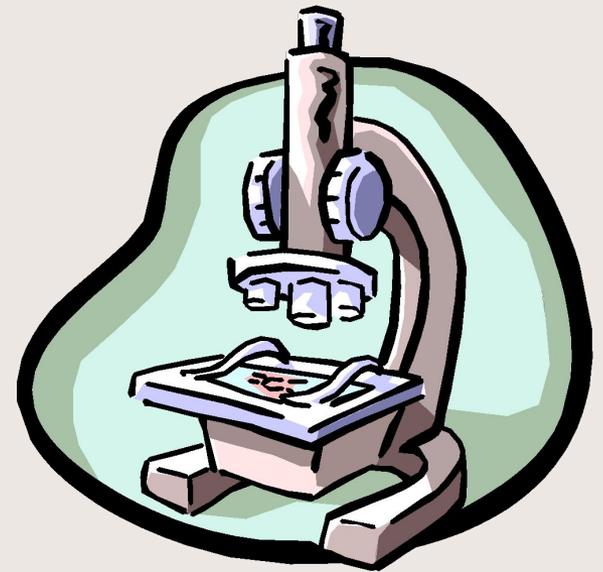
- **Программные вирусы** – это блоки программного кода, целенаправленно внедрённые внутрь других прикладных программ.





- **Загрузочный вирус** – это блок программного кода, поражающий не программные файлы, а определённые системные области магнитных носителей.

- **Макровирусы** – это особая разновидность вирусов поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения макрокоманд.



# Основное понятие

## №2

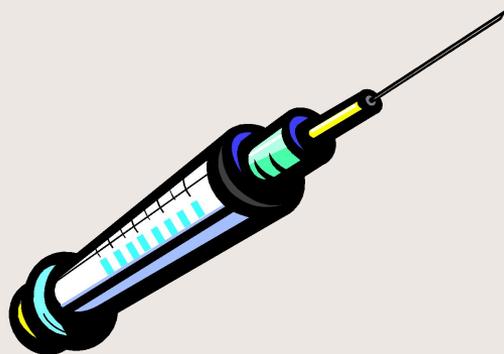
- Антивирус – это специализированная программа, которая предназначена для поиска и уничтожения компьютерных вирусов, а также для предохранения от заражения вирусом.

# Методы защиты от вирусов

---

- Общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей.

- Профилактические меры позволяющие уменьшить вероятность заражения вирусом.



- Для защиты от вирусов обычно используются: специализированные программы для защиты от вирусов.

# Выделяют:

- Программы-детекторы
- Программы-доктора (фаги)
- Программы-ревизоры
- Доктора-ревизоры
- Программы-фильтры
- Программы-вакцины (иммунизаторы)

# Дополнения:

- Программы-детекторы позволяют обнаруживать файлы зараженные одним из известных вирусов.
- Программы-доктора, или фаги лечат зараженные программы или диски, выкусывая из зараженных программ тело вируса, т.е. восстанавливая программу в то состояние, в котором она находилась до заражения вируса.

- Программы-ревизоры сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходными. При появлении несоответствий об этом сообщается пользователю.



- Доктора-ревизоры это гибриды ревизоров и докторов, т.е. программ, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменения вернуть их в исходное состояние.



- Программы-фильтры располагаются резидентно в оперативной памяти компьютера и перехватывают те сообщения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них соответствующей операции. Пользователь может разрешить или запретить выполнение соответствующей операции.

- Программы-вакцины или иммунизаторы модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус против которого производится вакцинация, считает эти программы или диски уже зараженными. На данный момент эти программы крайне не эффективны.

## Антивирусные средства позволяют:

- ✓ обнаружить вирусы в передаваемых файлах и вложениях писем;
- ✓ проверять архивированные файлы;
- ✓ Осуществлять автоматическую установку и обновление версий и баз данных по вирусам;
- ✓ отслеживать в реальном времени все записываемые и открываемые файлы;
- ✓ использовать сканирующие и резидентные модули;

- ✓ сканировать диски, когда компьютер простаивает, или по расписанию;
- ✓ проверять входящий/исходящий трафик посредством установки на Firewall;
- ✓ осуществлять удалённое администрирование и оповещение в случае выявления вирусов.

# Парад лучших антивирусов (в алфавитном порядке)

---

- Aladdin Knowledge Systems eSafe
- Command AntiVirus
- Computer Associates InoculateIT
- Doctor Web
- Eset NOD 32
- F-Secure Anti-Virus
- Kaspersky Antivirus
- Network Associates McAfee VirusScan
- Norman Virus Control
- Panda Antivirus Platinum
- Symantec Norton AntiVirus