

# Защита от вредоносных программ

## Общие сведения

Все знают, что для защиты от вредоносных программ нужно использовать антивирусы. Но в то же время нередко можно услышать о случаях проникновения вирусов на защищенные антивирусом компьютеры. В каждом конкретном случае причины, по которым антивирус не справился со своей задачей могут быть разные, например:

- Антивирус был отключен пользователем
- Антивирусные базы были слишком старые
- Были установлены слабые настройки защиты
- Вирус использовал технологию заражения, против которой у антивируса не было средств защиты
- Вирус попал на компьютер раньше, чем был установлен антивирус, и смог обезвредить антивирусное средство
- Это был новый вирус, для которого еще не были выпущены антивирусные базы

**Антивирус** – это программное обеспечение для комплексной защиты компьютера от вредоносных программ, поступающих в нее из сети Интернет, флеш-накопителей, съемных носителей информации.

Основные задачи:

- 1) Не допускать заражения
- 2) Обнаружить вредоносные программы
- 3) Удалить вредоносные программы и данные

Методы поиска:

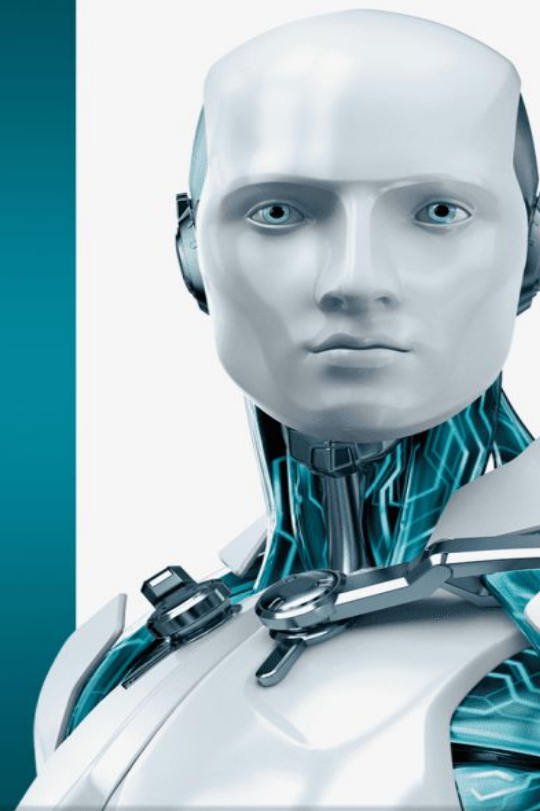
- 1) Поиск сигнатурных вирусов
- 2) Эвристика

**Примеры:**

Условно-бесплатные:

Бесплатные: Microsoft Security Essentials, Avast Home, Avira, AVG Free.

Свободные: ClamAV.

The ESET logo consists of the word "eset" in a lowercase, bold, sans-serif font. The letters "e" and "s" are white and are contained within a dark teal rounded rectangular shape. The letters "e" and "t" are dark teal and are positioned to the right of the rounded shape. A registered trademark symbol (®) is located at the top right of the logo.The text "NOD32 ANTIVIRUS" is displayed in a large, white, bold, sans-serif font. "NOD32" is on the top line and "ANTIVIRUS" is on the bottom line. The text is centered on a dark teal background.

**Антивирусный монитор** – это часть антивируса, предназначенная для непрерывного контроля ситуаций, при которых может произойти заражение вредоносной программой. Антивирусный монитор должен работать постоянно и в режиме реального времени, отслеживая такие потенциально опасные операции, как:

- загрузка веб-страниц и программ из интернета
- изменение файлов
- создание новых файлов
- модификация системного реестра
- обмен файлами и сообщениями электронной почты
- изменение загрузочных областей жесткого диска.

Главный недостаток - значительное замедление работы системы

**Брандмауэр** (или **Firewall**) – это программный комплекс, который служит для защиты компьютера от взлома хакерами, а также всевозможных вирусов и «троянов». Благодаря данной системе повышается степень безопасности работы в сети и отражаются многие атаки на компьютер за счёт фильтрации некоторых информационных пакетов. Именно поэтому настоятельно рекомендуется не отключать брандмауэр. Если пользователя не устраивает стандартный брандмауэр, то его в любой момент можно поменять на сторонний. Однако полностью отключать его весьма опасно.



## Меры безопасности при работе за компьютером:

- 1) Регулярное создание резервных копий важных данных на дисках CD/DVD или флеш-дисках .
- 2) При работе в сети включать антивирус-монитор и брандмауэр.
- 3) Проверять новые файлы с помощью антивируса-сканера.
- 4) Не открывать подозрительные сообщения электронной почты и переходить по ссылкам из недостоверных источников.
- 5) При заражении компьютера – отключить его от компьютерной сети и запустить антивирус-сканер.