

Антивирус – это программа для защиты компьютера или мобильного устройства от вредоносных программ. Термин «вредоносные программы» включает в себя все возможные виды опасных программ, таких, как вирусы, черви, трояны и вирусы-шпионы.



Работа антивируса

Говоря о системах Майкрософт, следует знать, что обычно антивирус действует по схеме:

поиск в базе данных антивирусного ПО сигнатур вирусов.

если найден инфицированный код в памяти (оперативной и/или постоянной), запускается процесс «карантина», и процесс блокируется.

зарегистрированная программа обычно удаляет вирус, незарегистрированная просит регистрации и оставляет систему уязвимой.



Базы антивирусов

- Для использования антивирусов необходимы постоянные обновления так называемых баз антивирусов. Они представляют собой информацию о вирусах — как их найти и обезвредить. Поскольку вирусы пишут часто, то необходим постоянный мониторинг активности вирусов в сети. Для этого существуют специальные сети, которые собирают соответствующую информацию. После сбора этой информации производится анализ вредоносности вируса, анализируется его код, поведение, и после этого устанавливаются способы борьбы с ним. Чаще всего вирусы запускаются вместе с операционной системой. В таком случае можно просто удалить строки запуска вируса из реестра, и на этом в простом случае процесс может закончиться. Более сложные вирусы используют возможность заражения файлов. Например, известны случаи, как некие даже антивирусные программы, будучи зараженными, сами становились причиной заражения других чистых программ и файлов. Поэтому более современные антивирусы имеют возможность защиты своих файлов от изменения и проверяют их на целостность по специальному алгоритму. Таким образом, вирусы усложнились, как и усложнились способы борьбы с ними. Сейчас можно увидеть вирусы, которые занимают уже не десятки килобайт, а сотни, а порой могут быть и размером в пару мегабайт. Обычно такие вирусы пишут в языках программирования более высокого уровня, поэтому их легче остановить. Но по-прежнему существует угроза от вирусов, написанных на низкоуровневых машинных кодах наподобие ассемблера. Сложные вирусы

Антивирусы для сайтов

- Их можно поделить условно на несколько типов:
- Серверный — устанавливается на веб-сервер. Поиск вирусов, в этом случае, происходит в файлах всего сервера.
- Скрипт или компонент CMS — выполняющие поиск вредоносного кода, непосредственно в файлах сайта.
- [SaaS](#) сервис — система централизованного управления, позволяющая управлять файлами, базами данных, настройками и компонентами веб-ресурсов на VDS и DS удаленно.

Специальные антивирусы

- В ноябре 2014 года международная правозащитная организация [Amnesty International](#) выпустила антивирусную программу [Detect](#), предназначенную для выявления вредоносного ПО, распространяемого государственными учреждениями для слежки за гражданскими активистами и политическими оппонентами. Антивирус выполняет более глубокое сканирование жёсткого диска, нежели обычные антивирусы.

Лжеантивирусы

- В 2009 началось активное распространение лжеантивирусов — программного обеспечения, не являющегося антивирусным (то есть не имеющего реальной функциональности для противодействия вредоносным программам), но выдающим себя за таковое. По сути, лжеантивирусы могут являться как программами для обмана пользователей и получения прибыли в виде платежей за «лечение системы от вирусов», так и обычным вредоносным программным обеспечением. В настоящий момент это распространение приостановлено.

Какие бывают виды антивирусных программ?

- Kaspersky
- AVG AntiVirus FREE
- Avast! Free Antivirus
- Dr.Web Antivirus
- Microsoft Security Essentials
- NANO Антивирус
- Panda Cloud Antivirus
- Zillya! Антивирус
- 360 Total Security

Kaspersky Internet Security



- Kaspersky Internet Security для всех устройств — это надежное и удобное решение для защиты вашей жизни в интернете.
- Оптимальный набор защитных функций
- Безопасность ваших данных в интернете
- Защита детей в интернете на любом устройстве
- Конфиденциальность личности и защита общения
- Управление защитой всей семьи

Avast! Free Antivirus.



- **Avast Free Antivirus** - бесплатный антивирус, который предлагает самую современную и эффективную защиту от всех типов вирусов и вредоносного ПО.
- Антивирус доступен с расширенным пакетом функций – включающим, помимо прочего, сканирование системы в одно нажатие и отстранение нежелательных панелей инструментов из браузера.
- Уникальный модуль сканирования домашней сети теперь обнаруживает на 12 типов уязвимостей роутера больше, а новый встроенный менеджер паролей позволяет хранить все ваши пароли в зашифрованном виде.
- Устанавливая версию Avast Free, вы получаете больше, чем просто бесплатный антивирус: это бесплатная защита для вас, вашего компьютера и вашей домашней сети.

360 Total Security



- **360 Total Security** предлагает комплексную защиту от всех видов вредоносных программ и онлайн угроз.
- Бесплатный антивирус от Qihoo 360 использует защиту в реальном времени с антивирусными движками Avira и Bitdefender, проактивным QVM II и облачным 360 Cloud, а также "Исправление системы" для комплексной оценки и быстрого восстановления аномальных изменений операционной системы Windows.
- Когда вы делаете онлайн-покупки, загружаете файлы, посещаете веб-страницы различных ресурсов в Интернете, 360 Total Security в реальном времени защищает вас от угроз. Кроме этого, вы можете использовать функцию очистки "в один клик" для оптимизации работы компьютера.
- Используемые технологии защиты от цифровых угроз обеспечивают непревзойденный уровень надежности и безопасности - онлайн и оффлайн, сохраняя высокую производительность и быстродействие системы.

Dr.Web Antivirus



- Возможность установки на зараженную машину.
- Обнаружение и лечение сложных полиморфных, зашифрованных вирусов и руткитов.
- Возможность настройки копирования важных данных в защищённое хранилище позволяет пользователям версии Dr.Web для Windows самостоятельно восстанавливать поврежденные данные без необходимости обращения в службу технической поддержки «Доктор Веб».
- Поддержка большинства существующих форматов упакованных файлов и архивов, в том числе многотомных и самораспаковывающихся архивов.
- Компактная вирусная база и небольшой размер обновлений. Одна запись в вирусной базе позволяет определять до тысячи подобных вирусов.
- Обновления вирусных баз производятся немедленно по мере выявления новых вирусов, до нескольких раз в час. Разработчики антивирусного продукта отказались от выпуска обновлений вирусных баз по какому-либо графику, поскольку вирусные эпидемии не подчиняются таковому.
- Кроссплатформенность — используется единая вирусная база и единое ядро антивирусного сканера на разных платформах ОС.
- Низкое влияние на производительность системы. Благодаря технологиям оптимизации, заведомо чистые файлы не проверяются компонентами Dr.Web, что снижает нагрузку на систему.