Безопасность в ОС Windows

Если вы подключаетесь к Интернету, разрешаете другим людям пользоваться своим компьютером или открываете общий доступ к файлам, необходимо принять меры по защите компьютера от угроз. Почему? Потому что существуют компьютерные злоумышленники, которые атакуют компьютеры других людей. Эти преступники могут атаковать напрямую, проникая в компьютер пользователя через Интернет и воруя личные данные, или косвенно, создавая вредоносные программы, разработанные для причинения вреда компьютеру.

Защита личных данных пользователя является первостепенной задачей для всех современных операционных систем. Microsoft стремится снабдить свои операционные системы самыми передовыми средствами защиты, совершенствуя их с каждой новой своей операционной системой.

Существуют различные способы защиты компьютера от возможных угроз безопасности.

Брандмауэр

Брандмауэр защищает компьютер, предотвращая доступ к нему злоумышленников и вредоносных программ.

Защита от вирусов

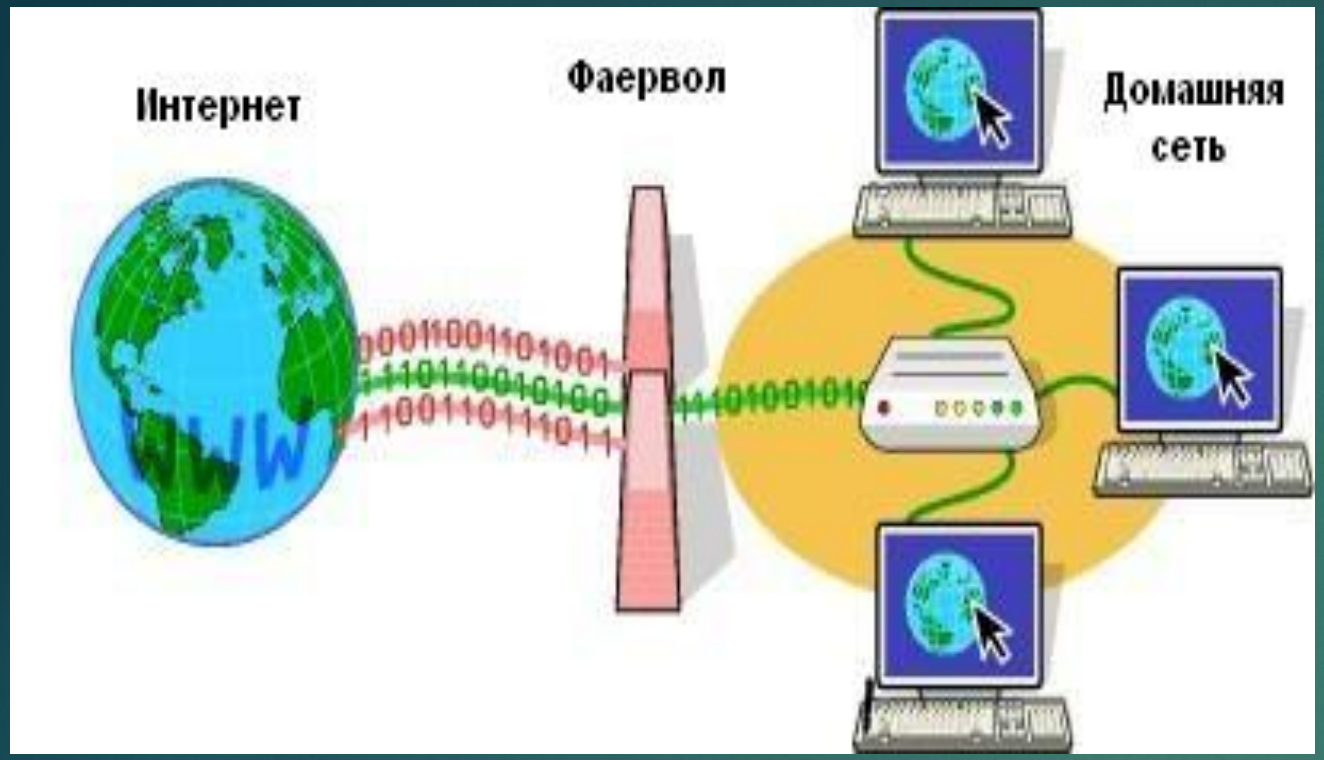
Антивирусное программное обеспечение поможет защитить компьютер от вирусов, вирусов-червей и других угроз безопасности.

Защита от шпионских и других вредоносных программ.

Антишпионское программное обеспечение поможет защитить компьютер от шпионских и других нежелательных программ.

Центр обновления Windows.

Windows может регулярно проверять наличие обновлений для компьютера и автоматически их устанавливать.



Брандмауэр — это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет ее, либо пропускает в компьютер, в зависимости от параметров брандмауэра. Таким образом, брандмауэр помогает предотвратить атаки хакеров и вредоносных программ на компьютер. Брандмауэр Windows встроен в Windows и включается автоматически.

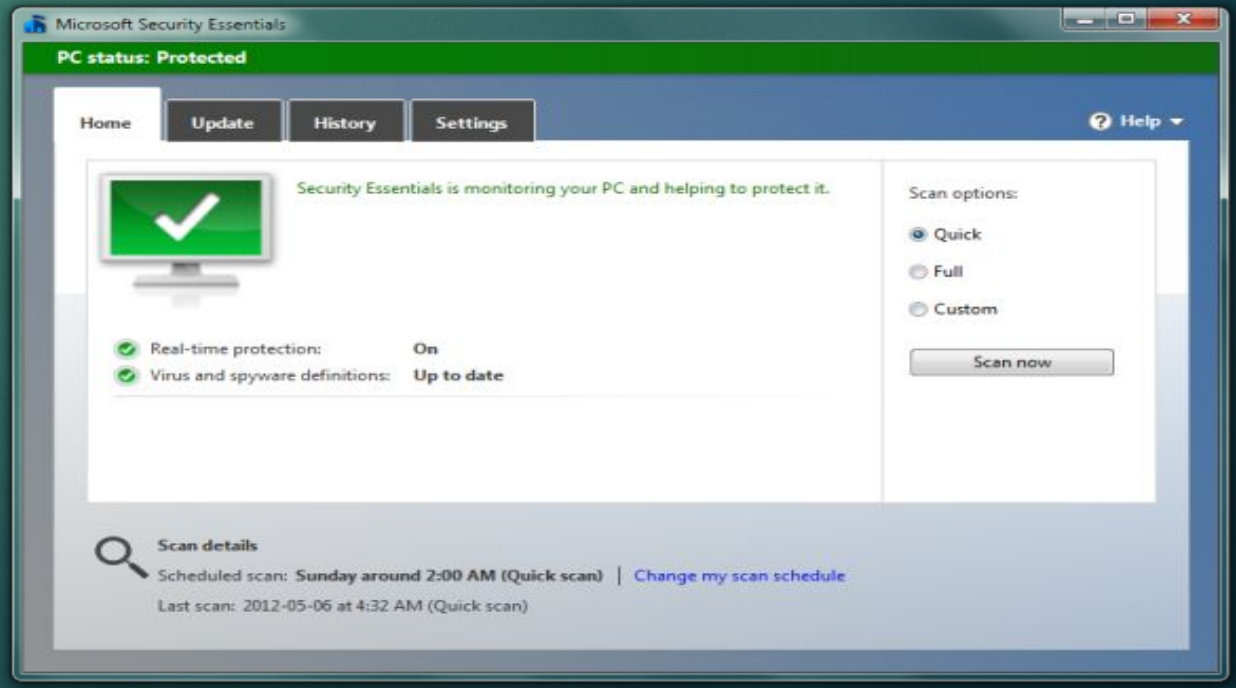
Как работает брандмауэр

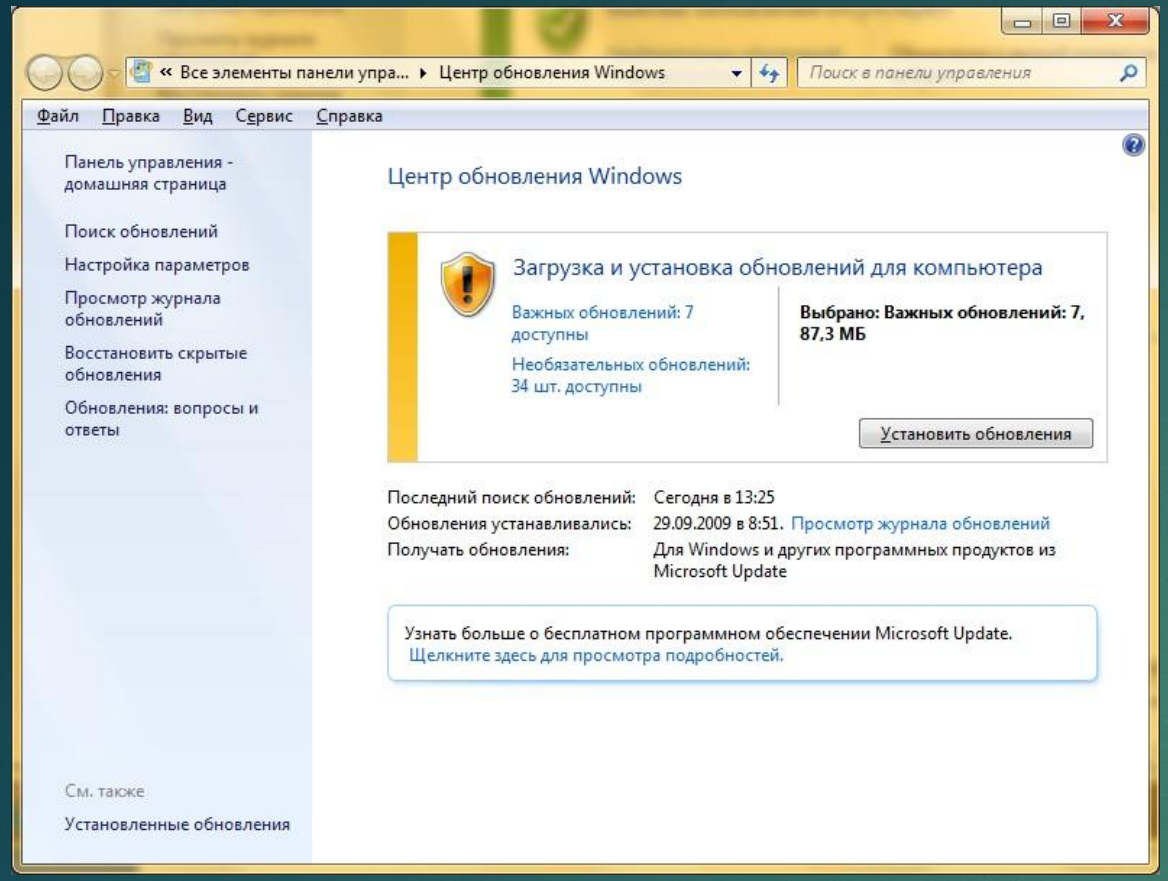
Если на компьютере используются такие программы, как программа передачи мгновенных сообщений или сетевые игры, которым требуется принимать информацию из Интернета или локальной сети, брандмауэр запрашивает пользователя о блокировании или разрешении подключения. Если пользователь разрешает подключение, брандмауэр Windows создает исключение, чтобы не тревожить пользователя запросами, когда в будущем этой программе понадобятся данные.

Вирусы

Вирусы, черви и троянские кони — это программы, созданные хакерами, использующими Интернет для заражения уязвимых компьютеров. Вирусы и черви могут размножаться от компьютера к компьютеру, тогда как троянские кони попадают в компьютер, прячась в предположительно легальных программах, таких как заставки. Деструктивные вирусы, вирусы-черви и троянские программы могут стереть информацию с жесткого диска или полностью вывести компьютер из строя. Другие программы не наносят прямой урон, но ухудшают быстродействие и стабильность компьютера.
Антивирусные программы проверяют электронную почту и другие файлы компьютера на наличие вирусов, червей и троянских программ. При обнаружении вредоносной программы антивирусная программа либо отправляет вирус в карантин (изолирует), либо полностью удаляет его до нанесения ущерба компьютеру и файлам.

Изначально в ОС Windows нет антивирусного ПО, но вы можете скачать
Microsoft Security Essentials – бесплатный пакет антивирусного ПО, выпущенный Microsoft и, заменивший Windows defender





Microsoft регулярно предлагает важные обновления Windows для защиты компьютера от новых вирусов и других угроз безопасности. Для скорейшего получения обновлений включите автоматическое обновление. В этом случае не нужно волноваться, что критические обновления Windows могут быть пропущены.
Обновления загружаются в фоновом режиме при подключении к Интернету. Обновления устанавливаются в 03:00, если не задано другое время. Если пользователь выключает компьютер раньше, можно установить обновления перед выключением. В противном случае Windows установит обновления в следующий раз при запуске компьютера.

Для того, чтобы включить автоматическое обновление Windows откройте Центр обновления Windows. В группе Рекомендуемые обновления установите флажок Получать рекомендуемые **обновления** таким же образом, как и важные **обновления** и нажмите кнопку ОК.

Windows Hello

Windows Hello с биометрической альтернативой паролям поможет решить эту проблему. Вы сможете мгновенно получать защищенный доступ к устройствам с Windows 10 и онлайн-сервисам Microsoft. Windows узнает ваш отпечаток пальца или лицо и тут же приветствует по имени: вы сможете войти в систему быстро, безопасно и без всяких паролей. А благодаря бесплатным автоматическим обновлениям у вас будут новейшие функции и обновления безопасности в течение всего срока поддержки устройства.

Microsoft Edge — принципиально новый браузер, с который быстрее чем Enternet Explorer, а главное безопаснее. Благодаря ему возрастает эффективность и безопасность работы Интернете, потому что обмен данными, чтение, изучение информации и т. п. стали проще. Microsoft Edge заявлен как самый безопасный браузер Microsoft: его передовая технология «песочницы» позволяет работать в Интернете изолированно от личной информации и данных, а также от самой системы Windows.

Собирать информацию об интернет угрозах Microsoft помогает Microsoft SpyNet – онлайн сообщество, которое консультирует пользователей в вопросах безопасности, а так же осуществляет сбор информации о вредоносно ПО и останавливает распространение инфекций

Технология Microsoft SmartScreen защищает от фишинговых сайтов, пытающихся украсть ваши пароли и личные данные. Microsoft SmartScreen проверяет репутацию каждого посещаемого сайта и блокирует потенциально опасные. Эта технология также защитит вас от загрузок вредоносного ПО, навязанного вам обманным путем. Для этого используется облачный сервис репутации приложений, который непрерывно оценивает миллиарды новых образцов ПО.

Интернет-фишинг — один из способов получения обманным путем личной информации о пользователях компьютера через сообщение электронной почты или веб-сайт. Обычно интернет-фишинг начинается с сообщения электронной почты, похожего на официальное уведомление из надежного источника. В сообщении электронной почты содержится ссылка на поддельный веб-сайт, где требуется ввести личную информацию, например номер банковского счета или пароль. Эта информация впоследствии используется с целью кражи.