

Windows7

- Многозадачная ОС (вытесняющая/приоритетная многозадачность)
 - Разделение процессорного времени между потоками происходит по принципу «карусели». Ядро операционной системы выделяет квант времени каждому из потоков по очереди при условии, что все потоки имеют одинаковый приоритет. Поток может отказаться от выделенного ему кванта времени. В этом случае система перехватывает у него управление (даже если выделенный квант времени не закончен) и передаёт управление другому потоку. При передаче управления другому потоку система сохраняет состояние всех регистров процессора в особой структуре в оперативной памяти. Структура контекста потока. Сохранения контекста потока достаточно для последующего возобновления его работы.
- Многопользовательская система
- Средства локальной безопасности:
 - 1) механизмы разграничения прав доступа пользователей к системе.
 - 1.1) Администратор. Пользователи учетных записей администраторов имеют полный доступ ко всем файлам и папкам на диске, а также вправе изменять любые параметры системы. Кроме того, администраторы обладают возможностью создавать, редактировать и удалять учетные записи других пользователей.
 - 1.2) Обычный доступ. Пользователи учетных записей данного типа существенно ограничены в доступе к «недрам» системы. Они могут беспрепятственно работать с разрешенными файлами и папками, с программами, однако устанавливать и удалять приложения, оборудование, менять настройки системы, которые могут затронуть и других пользователей, а также работать с их

личными файлами и папками права не имеют. При попытке совершить одно из вышеперечисленных действий появится окно UAC, в котором будет предложено ввести пароль учетной записи администратора. Если он известен пользователю, то дальнейшее продолжение действия будет возможно

2) шифрование диска – BitLocker To Go, предназначенный для шифрования любых съемных накопителей - USB-дисков, карт памяти и пр.

3) защита от нежелательного ПО – интегрированная программа – Защитник Windows. Использование антивируса.

4) встроенные средства автоматического обновления Windows.

- Средства сетевой безопасности.

1) программы, препятствующие проникновению через сеть на компьютер вредоносных приложений

1.1) Ashampoo Firewall

Принцип работы фаервола следующий: для каждого приложения должно быть сформировано разрешающее или запрещающее правило, которое обрабатывается фаерволом.

В случае попытки приложением, для которого не назначено правило, установить соединение, фаервол предупреждает пользователя – предлагая создать правило.

Данное утверждение справедливо, когда фаервол работает в режиме обучения. При отключении этого режима, приложения для которых не назначены правила – будут блокироваться в автоматическом режиме.

Не совместим с некоторыми антивирусами; отсутствуют обновления.

1.2) PC Tools Firewall Plus

Программа имеет удобное управление сетевым трафиком, позволяет создавать новые правила, скрывать присутствие

компьютера в сети, присутствует возможность защиты настроек паролем.

Фаервол устанавливается без ввода каких-либо паролей или прохождения регистрации.

Создание правил для доступа приложений происходит в ручном режиме.

Рекомендуем не откладывать эту процедуру на потом, т.к. после установки Ashampoo Firewall может запомнить некоторые приложения и программы, как непроверенные, вследствие чего последние могут некорректно работать или не работать вообще.

Отсутствуют обновления; отсутствует русскоязычный интерфейс; настройка в ручном режиме.

1.3) И т.п.

- 2) Брандмауэр Windows 7 — специальная служебная программа, предназначенная для контроля за сетевыми интерфейсами, контролирует выход программ в интернет, является своего рода защитой от проникновения вирусов и предотвращает их распространение.