**UAC или User Account Control на страже системы**

Наиболее сильно недооцененной и не понятой функцией в Windows Vista является **User Account Control (UAC)**. А зря, это очень важная и полезная функция. Долгие годы пользователи были богами в своих системах и работали от имени учетной записи администратора. Так было в Windows 95, 98, ME и даже в 2000 и XP, когда все предупреждают, что это опасно для системы. В конкурирующих системах, например в ОС Linux, запрещено входить в графическую оболочку от имени администратора (root). Если необходимо выполнить действия от имени администратора, пользователь должен переключиться в консоли на учетную запись администратора, но запускать целую оболочку от администратора не нужно.

Компания Microsoft не стала вводить такой категорический запрет ради удобства пользователей и ради большого количества программ, которые могут потребовать выполнения привилегированных операций, но безопасность важнее, поэтому в Windows Vista для нашей защиты была внедрена User Account Control. Не советую ее отключать, ибо это реальная защита, и если какая-то программа не работает корректно с UAC, то это не Windows плохой, это программа не умеет работать в безопасном окружении и я бы не стал работать с такой программой ради собственной безопасности. Такое отношение есть в любой безопасной системе и теперь так есть и скорей всего будет в Windows.

Технология UAC позволяет пользователям работать от имени стандартного пользователя и контролировать выполнение привилегированных операций. Когда программе необходимо выполнить операцию, требующую административных прав, система запрашивает у нас подтверждение на выполнение этих действий. Пользователь может контролировать процесс, и если он действительно уверен, что программа заслуживает доверия и ей можно доверить доступ к привилегированным возможностям.

Административные права могут потребоваться, когда вы устанавливаете программу, и она производит копирование файлов в директории Program Files, Windows или производит запись в реестр HKLM (HKEY\_LOCAL\_MACHINE).

Не имея администраторских прав, пользователь не сможет случайно или специально изменить критические данные. Когда приложение запущено от имени не привилегированного пользователя, пользователь может избежать тяжелых последствий зловредного кода, а у этого кода остается меньшее поле для деятельности.

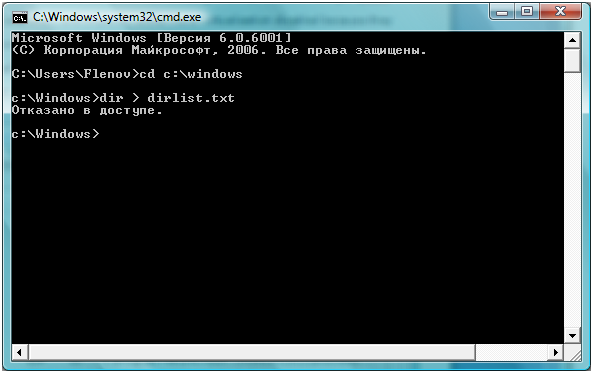
**Виртуализация**

Помимо контроля доступа к запрещенным ресурсам, UAC может виртуализировать работу с критически важными данными. Если программа обращается к важным данным, то UAC создает видимость реального доступа (виртуализирует доступ). Программа даже не будет подозревать, что реального доступа нет.

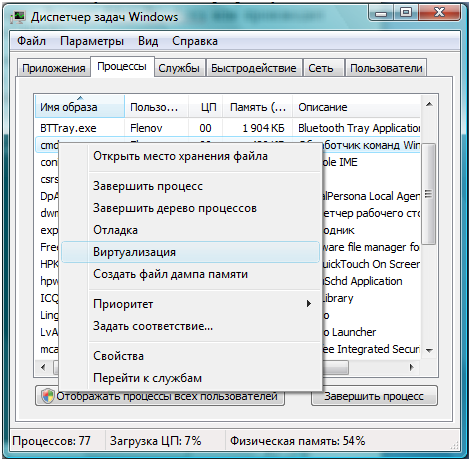
Давайте рассмотрим это на примере. Запустите командную строку и перейдите в папку Windows. Эта системная папка и ее защищает UAC. Я надеюсь, он у вас включен? Иначе вы не только в большей безопасности, но и не увидите результат примера. В директории Windows выполните какую-нибудь команду по созданию файла. Например, можно попытаться сохранить в текстовый файл список файлов текущей директории командой:

dir > myfile.txt

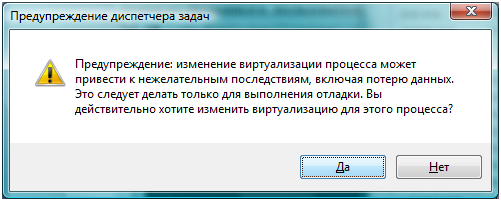
Это делать запрещено из под стандартного пользователя, поэтому в результате вы увидите сообщение об отказе в доступе:



Запустите диспетчер задач и найдите там свой процесс cmd.exe. Если у вас запущен только один интерпретатор, то это не сложно. Щелкните правой кнопкой по процессу и из выпадающего меню выберите Виртуализация:



Перед вами появиться предупреждение о том, что данные могут быть потеряны приложением. Сейчас мы увидим эту потерю на практике и чтобы увидеть, виртуализация должна быть включена, поэтому давите Да.



Теперь повторите команду создания файла. Ни единой ошибки. На этот раз программа выполнила все успешно и сохранила результат в файл. А сохранила ли? Проверьте директорию Windows, там вашего файла не будет!!! На самом деле, его нет нигде. Если включена виртуализация, то система создала видимость доступа, но не дала его реально, поэтому файла не будет. Программа думала, что она работает с системой, но UAC не дал сделать этого.

Таким образом, если программа не умеет по человечески работать в стандартном пользовательском режиме и зачем-то лезет в защищенную зону, но вы не хотите дозволить это (а вы и не должны позволять), можно включить для программы виртуализацию и она будет работать прекрасно.