МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное агентство по образованию

Государственное образовательное учреждение высшего профессионального образования

«ЮЖНО-РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (НОВОЧЕРКАССКИЙ ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ)»

ФАКУЛЬТЕТ ОИТ и У \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

КАФЕДРА Информационные и управляющие системы

СПЕЦИАЛЬНОСТЬ 23020165 Информационные системы и технологии

ОТЧЕТ

по лабораторным работам

по дисциплине \_\_\_\_\_\_

Студент \_IV курс, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

курс, группа фамилия, и.о.

Преподаватель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

должность, звание фамилия, и.о.

Отчет принят \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

дата подпись

Волгодонск, 2010 г.

Содержание

1 Ключи реестра

2 Счетчики производительности

3 Скрипт

Используемая литература

1 Ключи реестра

Рассмотрим ключи реестра, разбив их на четыре группы.

В первую группу объединим ключи, которые служат для ограничения возможностей пользователя.

Операции с контекстным меню Проводника

Чтобы сделать недоступным контекстное меню, вызываемое на файле в проводнике необходимо в HKEY CURRENT USER\Software\Microsoft\Windows\Current Version\Polices\Explorer создать параметр NoViewContextMenu=1 типа DWORD.

Тем не менее, даже при отключении контекстного меню доступ к дискам ПК сохраняется. Например, если воспользоваться командой Файл – Создать – Ярлык на экране отображается окно мастера создания ярлыка в котором с помощью кнопки «Обзор» открывается доступ к локальным и сетевым дискам. Чтобы перекрыть этот доступ, достаточно в системном реестре удалить или переименовать раздел HKEY CLASSES ROOT\.lnk\Shellnew в результате чего возможность создания ярлыка остается, но без помощи мастера.

Удаление меню Файл

Меню Файл удаляется из главного меню Проводника, а также из других окон использующих оболочку Windows. Для этого необходимо создать параметр NoFileMenu=1 типа DWORD в разделе HKEY CURRENT USER\Software\Microsoft\Windows\Current Version\Polices\Explorer.

Ко второй группе отнесем ключи позволяющие изменить пути к системным и специальным папкам. Поменять из расположение можно обычным способом, но после перезагрузки ПК они будут восстановлены на прежнем месте. Это связано с тем, что пути к ним прописаны в системном реестре – в разделах HKEY CURRENT USER\Software\Microsoft\Windows\Current Version\Explorer\Shell Folders либо HKEY CURRENT USER\Software\Microsoft\Windows\Current Version\Explorer\User Shell Folders. Поэтому чтобы перенести какую – либо из системных папок, нужно сначала прописать путь к ней в реестре и лишь затем поместить ее по указанному адресу.

В третей группе рассмотрим ключи с помощью которых можно ограничить право пользователя редактировать системные настройки.

Панель управления

При необходимости можно удалить из меню кнопки Пуск функцию Панель Управления. Для этого необходимо создать параметр NoControlPanel=1 типа DWORD в разделе реестре HKEY CURRENT USER\Software\Microsoft\Windows\Current Version\Polices\Explorer. Отображением функции Панель Управления можно также управлять в разделе HKEY CURRENT USER\Software\Microsoft\Windows\Current Version\Explorer\Advanced с помощью параметра Start\_ShowControlPanel типа DWORD. Возможны следующие значения этого параметра:

=0 функция Панель Управления будет исключена из меню Пуск;

=1 функция Панель Управления отображается как ссылка;

=2 функция Панель Управления отображается как подменю.

В четвертой группе рассмотрим управление файлом подкачки. Его особенностью является то, что после завершения работы на ПК в нем может содержатся конфиденциальная информация. Поэтому целесообразно производить очистку файла подкачки по окончании работы. Для этого в разделе HKEY Local Machine\System\CurrentControlSet\Control\SessionManager\Memory Management создается параметр ClearPageFileAtShutdown = 1 типа DWORD. Запущенные системные драйверы и пользовательские коды, которые не помещаются в памяти, по умолчанию сбрасываются в файл подкачки на диске. При наличии большлго объема памяти данный режим можно отключить. HKEY Local Machine\System\CurrentControlSet\Control\SessionManager\Memory Management параметр DisablePagigExecutive =1 типа DWORD.

2 Счетчики производительности

Проблема: жалобы пользователя на зависание ПК.

Одним из первых действий администратора является проверка Диспетчера задач. В нем возможно наблюдение за количеством работающих процессов, а также за процентом загруженности процессора. Далее с помощью счетчиков производительности: % работы в пользовательском режиме и % работы в привилегированном режиме, устанавливается какого рода деятельность занимается процессор. При одновременном просмотре результатов счетчиков и диспетчера задач возможно установить соответствие процесса пику на графике производительности (рис. 1).

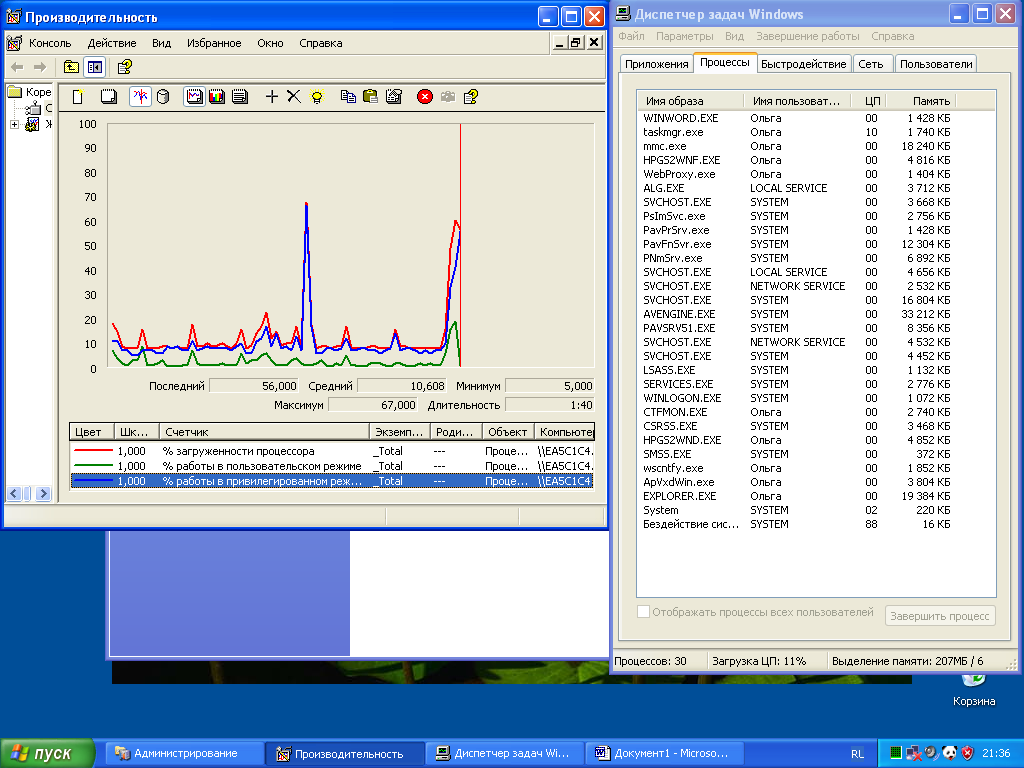


Рис. 1. Окно консоли Производительность

Если пику счетчика % процент загруженности процессора соответствует пик счетчика % работы в пользовательском режиме, то в этом случае необходимо рассмотреть работающее пользовательское приложение, которое может быть слишком мощным для данного ПК.

Если пику счетчика % процент загруженности процессора соответствует пик счетчика % работы в привилегированном режиме, то в диспетчере задач необходимо отследить системный процесс, который активен во время пика счетчика % работы в привилегированном режиме. Зная процесс устанавливается служба которой он соответствует, после этого решается вопрос нужно ли активизировать эту службу в автоматическом режиме.

Если же процесс не является системным, то прояснения ситуации можно воспользоваться счетчиками чтения/записи на диск (рис. 2).

меню файл компьютер драйвер

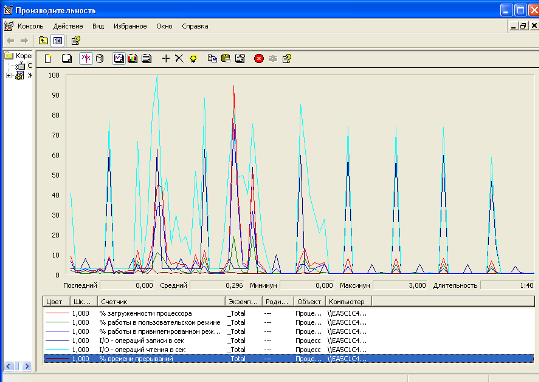


Рис. 2. Окно консоли Производительность

3 Скрипт

strComputer = "." 'задание имени локального компьютера

Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")

Set colMonitoredProcesses=objWMIService.ExecNotificationQuery("select \* from \_\_instancecreationevent " & " within 1 where TargetInstance isa 'Win32\_Process'")

i = 0

Do While i = 0

Set objLatestProcess = colMonitoredProcesses.NextEvent

Wscript.Echo objLatestProcess.TargetInstance.Name

Loop

В результате работы этого скрипта сразу после запуска какого-либо процесса на экран монитора выдается сообщение, в котором указывается имя этого процесса.

Этот скрипт будет полезен для ознакомления и изучения процессов при использовании ПК, а также при слежении за активностью процессов и выявлении подозрительной активности.

В данном скрипте используется средства Windows Management Instrumentation.

Используемая литература

1. Библиотека MSDN
2. Z:\Преподаватели\ИиУС\Виниченко С.М\МАТЕРИАЛЫ\WSH советы\