### Цель работы: изучить возможностей контроля, управления процессами в операционных системах Windows

**I часть:**

1. Запускаем утилиту Process Explorer
2. Изучаем программу и её возможности
3. Запускаем несколько приложений (Paint, WordPad, NotePad)
4. Описани изменений в окне процессов: В верхнем окне появляются только что открытые приложения, секунду (*настраиваемое*) подсвечиваются зеленым (*настраиваемое)*,также показаны некоторые характеристики процессов, которые мы запустили.Идентификатор процесса - PID, процент загрузки процессора - CPU, описание - Description, наименование аккаунта владельца - Owner, приоритет процесса - Priority, Handles, Windows Title.
5. Открываем стандартный диспетчер задач (Ctrl+Alt+Del –> Диспетчер задач). Сравниваем его возможности с возможностями утилиты ProcExp. К преимуществам ProcExp относится: представление полной информации по всем процессам, запущенным на компьютере, показ связей между процессами, библиотеками и ключами запуска, вывод подробной картины использования аппаратных мощностей. К недостаткам можно отнести тот факт, что для отображения некоторых полей (сетевая статистика) требуются административные привилегии, а также интерфейс может легко запутать неопытного пользователя.

**II часть:**

1. Отсортируем процессы по загрузке процессора. Для этого необходимо в верхнем окне кликнуть левой кнопкой мыши по графе CPU.
2. Рассмотрим процесс «svchost.exe», его идентификатор процесса – PID – 15968, CPU – нет (в данный момент не задействуется), компания - Microsoft Corporation, описание - Хост-процесс для служб Windows, версия 6.2.16299.15 (для просмотра версии и прочих характеристик необходимо правой кнопкой кнопки кликнуть на процесс и выбрать пункт Properties).
3. Запускаем Wordpad.
4. Определяем используемые handles:

|  |  |  |  |
| --- | --- | --- | --- |
| Name | wordpad.exe(19652): 15952 | HKCR\PackagedCom | \Device\Nsi |
| Type | Thread | Key | File |
| Description | An object that executes program code | A Registry key | A disk file, communications endpoint or driver interface. |
| Addres | 0xFFFFA186E957D700 | 0xFFFF900FF3AD7810 | 0xFFFFA186E2D77310 |

1. Принудительно завершаем созданный процесс. Выбираем процесс «wordpad.exe», правой кнопкой мыши кликаем по нему и выбираем пункт Kill process.