Лабораторная работа №7.
Утилиты Sysinternals

Цель и задачи лабораторной работы

Целью работы является практическое изучение возможностей утилит Windows Sysinternals на примере характерных операций.

Задачами работы является освоение следующих навыков:

- управление процессами
- мониторинг процессов
- управление рабочими столами
- масштабирование экрана

Windows Sysinternals

Комплект программ **Windows Sysinternals** включает несколько десятков *утилит*, дополняющих возможности ОС **Windows**. Эти утилиты распространяются бесплатно как **freeware**.

Утилиты можно скачать на компьютер или запустить непосредственно с веб сайта:

http://live.sysinternals.com.

Задания

- Прочитайте статью **Утилита** на **Википедии**
- Прочитайте статью **Freeware** на **Википедии**
- Прочитайте статью **Sysinternals** на **Википедии**
- Зайдите на сайт:

http://technet.microsoft.com/ru-ru/sysinternals

- Прочитайте описание пакета **Sysinternals**
- Запишите названия разделов **Инструменты**
- Зайдите на сайт: **http://live.sysinternals.com**.
- Определите число файлов: скопируйте в буфер ► **Word** ► **Сервис** ► **Статистика** ► **Строк**

PROCESS EXPLORER

Запуск утилиты

Process Explorer – утилита для управления процессами.

После запуска программы появляется значок с графиком загрузки процессора на **Панели задач** в правой нижней части

экрана (рис.7.1). При наведении курсора на значок появляется всплывающая подсказка:

- загрузка процессора
- процесс, который больше всего загружает процессор

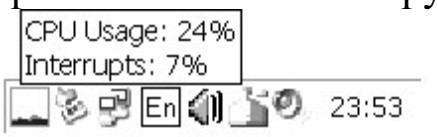

Рис.7.1. Значок **Process Monitor** на панели задач

Задания

- Прочитайте статью **Процесс (информатика)** на **Википедии**
- Прочитайте начало статьи **Процессор** на **Википедии**
- Прочитайте описание **Process Explorer** на сайте **Sysinternals**
- Запустите **Process Explorer**
- Наведите курсор на значок **Process Explorer**
- Запишите информацию из всплывающей подсказки

Дерево процессов

Отношения процессов «родитель-потомок» изображаются в виде дерева. Процессы-потомки расположены ниже и правее родительского процесса (рис. 7.2). Например, процесс **FreeCommander.exe** является родительским для процессов **WINWORD.EXE** и **procexp.exe**. Чтобы свернуть или развернуть ветку дерева, щелкните по значку **[–]** или **[+]** слева от имени процесса.

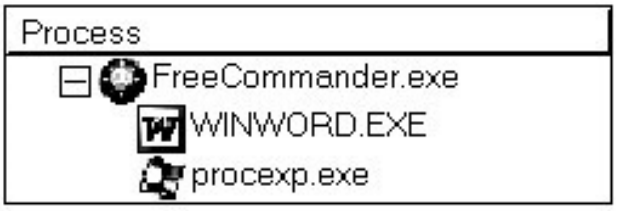

Рис.7.2. Дерево процессов

Чтобы завершить выполнение процесса или дерева процессов, вызовите контекстное меню (рис.7.3) и выберите:

- **Kill Process**
- **Kill Process Tree**

Для экспериментов с деревом процессов будем использовать командное окно, в котором введем команду **start cmd**. При этом создается дочерний процесс – новое командное окно. После создания

нового процесса вызовите в **Process Explorer** контекстное меню **Properties** (рис.7.4). Определите идентификатор процесса **PID** и время его запуска **Started**.

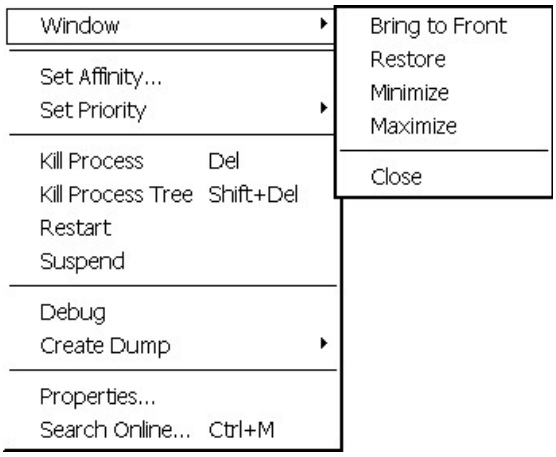

Рис.7.3. Контекстное меню процесса

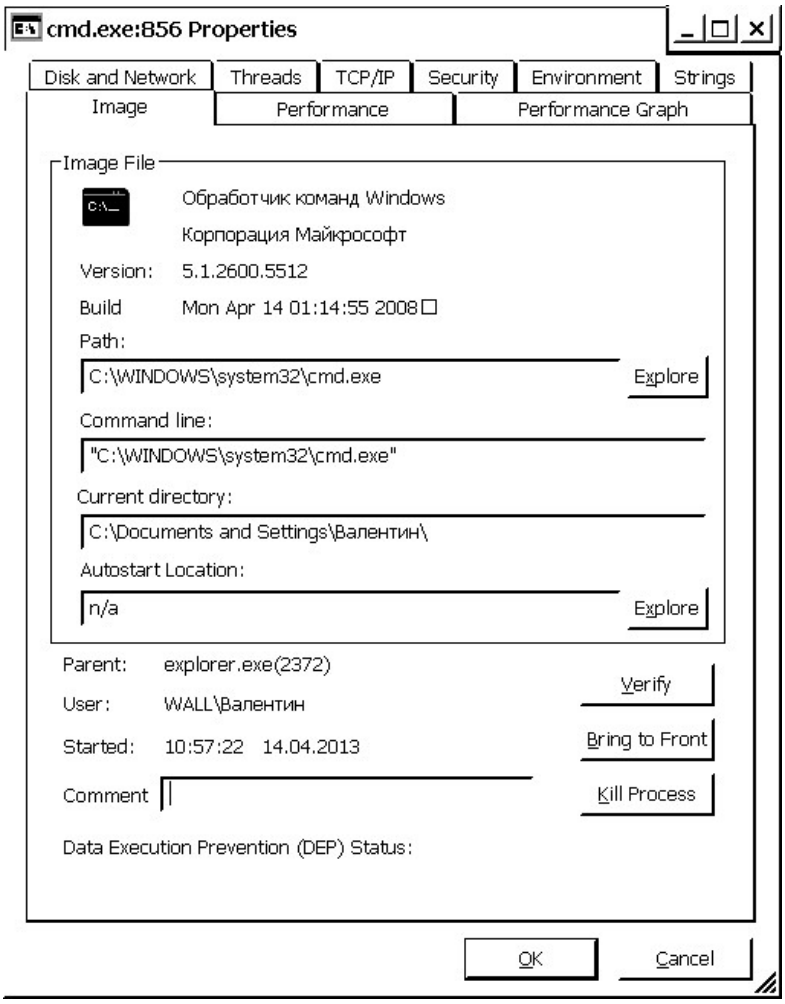

Рис.7.4. Свойства процесса

ОС хранит информацию только о *непосредственном родителе*: **Parent** (рис.7.4). Когда родительский процесс завершает работу, его

дочерние процессы становятся «сиротами». Процессы-сироты выводятся по левому краю списка процессов.

Задания

- Разверните окно **Process Explorer** во весь экран
- Запустите командную строку: **Пуск ► Выполнить ► cmd**
- Сверните все деревья
- Разверните дерево процесса **explorer.exe**
- Создайте дерево процессов (рис.7.5): **start cmd**

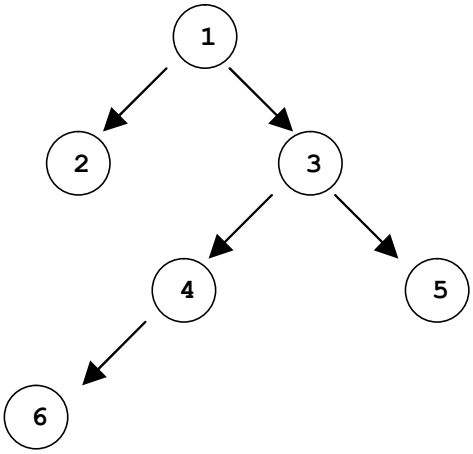

Рис.7.5. Задание: структура дерева

- Ознакомьтесь с деревом **cmd.exe**
- Сделайте зарисовку дерева, указав для каждого процесса:
  - идентификатор
  - время запуска
- Завершите *первый* процесс (рис.7.3) через контекстное меню:
  - **Kill Process**
- Ознакомьтесь с изменением в структуре дерева
- Завершите дерево *третьего* процесса (рис.7.3)
  - **Kill Process Tree**
- Прочитайте статью **Процесс-сирота** на **Википедии**
- Ознакомьтесь с изменением в структуре дерева
- Найдите процесс-сироту
- Завершите *второй* процесс
- Выберите в списке **Process Explorer**
- Выясните имя файла и расположение программы **Process Explorer**

Переменные окружения

Каждый процесс получает значения переменных окружения от операционной системы. Дочерний процесс наследует значения переменных родительского процесса на момент создания. После создания дочернего процесса, изменения окружения родительского процесса не влияют на окружение дочернего процесса.

Задания

- Запустите командное окно **Пуск ► Выполнить ► cmd**
- Запустите в командном окне **start cmd**
- Перейдите в **Process Explorer**
- Дважды щелкните по значку родительского процесса **cmd**
- На вкладке **Environment** ознакомьтесь с переменными
- Закройте окно **Properties**
- В контекстном меню вызовите **Window ► Bring to Front**
- В командном окне введите **set var=myvar**
- На вкладке **Environment** ознакомьтесь с переменными:
  - для родительского процесса
  - для дочернего процесса
- Переключитесь в родительское окно **cmd**
- Запустите команду **start cmd**
- На вкладке **Environment** ознакомьтесь с переменными:
  - для нового дочернего процесса

Верхняя и нижняя панели

Окно **Process Explorer** включает верхнюю и нижнюю панели (рис.7.6).

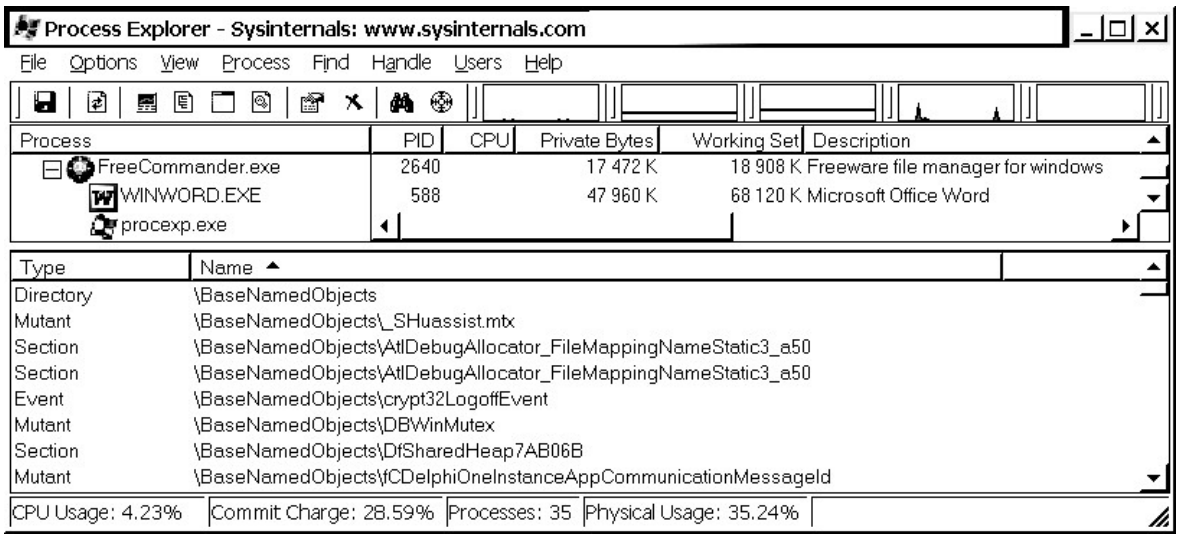

Рис.7.6. Две панели **Process Explorer**

Верхняя информационная панель содержит список процессов.

Нижняя информационная панель выводит сведения о ресурсах, которые использует процесс, выбранный в верхней панели. Нижнюю панель можно включать и выключать:

- **View ► Show Lower Pane**
- **View ► Lower Pane View ► DLLs**
- **View ► Lower Pane View ► Handles**

Объекты в панелях подсвечены разными цветами:

- зеленый – новые объекты
- красный – объекты, завершающие работу

Скорость обновления информации устанавливается в верхнем меню программы: **View ► Update Speed**.

Задания

- Запустите **cmd**
- Наблюдайте за изменением списка процессов
- Завершите **cmd**
- Наблюдайте за изменением списка процессов
- Установите скорость обновления 5 секунд
- Включите нижнюю панель
- Прочитайте статью **DLL** на **Википедии**
- Выясните, как расшифровать сокращение **DLL**
- Обратите внимание на описание явления **DLL hell**
- Установите режим просмотра **DLLs**
- Запустите **cmd**
- Наблюдайте за изменением верхней и нижней панелей
- Выберите **cmd** в списке процессов
- Запишите, сколько библиотек **DLL** использует процесс **cmd**
- Откройте страницу **Википедии**
  - **http://en.wikipedia.org**
- Откройте статью
  - **Handle (computing)**
- Запишите и переведите первый абзац статьи
- Найдите и запишите подходящий перевод компьютерного термина **Handle** на сайте **Яндекс.Словари**
- Прочитайте статью:

    - **http://exelab.ru/faq/Handle**
- Установите режим просмотра **Handles**
- Запишите, сколько объектов ОС использует процесс **cmd**
- Завершите **cmd**
- Наблюдайте за изменением верхней и нижней панелей
- Запустите текстовый редактор **WORD**
- Выберите процесс **WORD** в списке
- Просмотрите список **Handles**
- Запишите виды объектов ОС, используемых процессом
- Переведите названия видов объектов

Поиск

С помощью поиска можно выяснить, каким приложением открыт файл, какие библиотеки загружены дескриптором.

Для поиска выберите в верхнем меню **Find ► Find Handle or DLL**. В диалоговом окне **Process Explorer Search** введите имя файла и нажмите кнопку **Search**.

Задания

- Найдите сведения о файле **normal.dot**
- Прочитайте статью **Семафор (информатика)** на **Википедии**
- Найдите сведения об объектах **semaphore**
- Выясните, какой процесс использует больше всего семафоров
- Прочитайте статью **мьютекс** на **Википедии**
- Найдите сведения об объектах **mutex**
- Выясните, какой процесс использует больше всего **мьютексов**

Настройка таблицы

Пользователь может настроить вид списка процессов. Чтобы выбрать колонки таблицы, укажите на заголовок таблицы и вызовите **Select Columns** в контекстном меню. Колонки выбираются в нескольких вкладках. После выбора колонок можно изменить их порядок в таблице путем перетаскивания заголовков колонок.

Задания

- Настройте вывод информации следующим образом:
    - **Process Image:**
        - **Description**

        - **Company Name**
        - **Window Title**
    - **Process Memory**
        - **Убрать все поля**
    - **Handle**
        - **Type**
        - **Name**
        - **Handle Value**
    - **DLL**
        - **Description**
        - **Version**
        - **Name**
        - **Path**
        - **Company Name**
    - **Status Bar**
        - **CPU Usage**
        - **Number of Processes**
        - **Physical Memory Usage**
        - **Number of Threads**
    - **Process Performance**
        - **CPU Usage**
        - **Start Time**
        - **Threads**
        - **CPU Time**
    - **Process I/O**
        - **Read Bytes**
        - **Write Bytes**
- Убедитесь в изменении настроек
- Настройте порядок колонок:
    - **Process**
    - **PID**
    - **Threads**
    - **CPU**
    - **Start Time**
    - **Windows Title**
- Запустите командное окно: **[Win + R] ► cmd**

- Введите в командном окне команду: **title 111**
- Запустите командное окно: **File ► Run ► cmd**
- Определите родительские процессы для двух запущенных **cmd**
- Введите во втором командном окне команду: **title 222**
- Убедитесь, что заголовки окон изменились
- Убедитесь, что колонка **Window Title** изменилась
- Запишите и переведите информацию в строке состояния в нижней части окна **Process Explorer**
- Сохраните настройки: **View ► Save Column Set**

Журнал

Информацию, выводимую на экран, можно записать в текстовый файл. Для этого вызовите в верхнем меню **File ► Save As**.

Задания

- Сохраните данные в файл
- Откройте файл в **Блокноте**

  Сравните содержимое файла с экраном **Process Explorer**

Замена Диспетчера задач

Утилиту **Process Explorer** можно установить взамен встроенного **Диспетчера задач**. Для этого вызовите в верхнем меню **Options ► Replace Task Manager**. После этого утилита будет запускаться при нажатии **[Ctrl + Alt + Del]**.

Задания

- Установите **Process Explorer** вместо **Диспетчера задач**.
- Завершите работу **Process Explorer**
- Нажмите комбинацию **[Ctrl + Alt + Del]**
- Снимите настройку **Replace Task Manager**
- Завершите работу **Process Explorer**
- Нажмите комбинацию **[Ctrl + Alt + Del]**
- Завершите работу **Диспетчера задач**

Потоки

Чтобы вывести дополнительную информацию о потоках в рамках процесса, выберите процесс, вызовите контекстное меню и

выберите вкладку **Threads** (рис.7.7). Щелкните по выбранной строке для получения сведений о потоке.

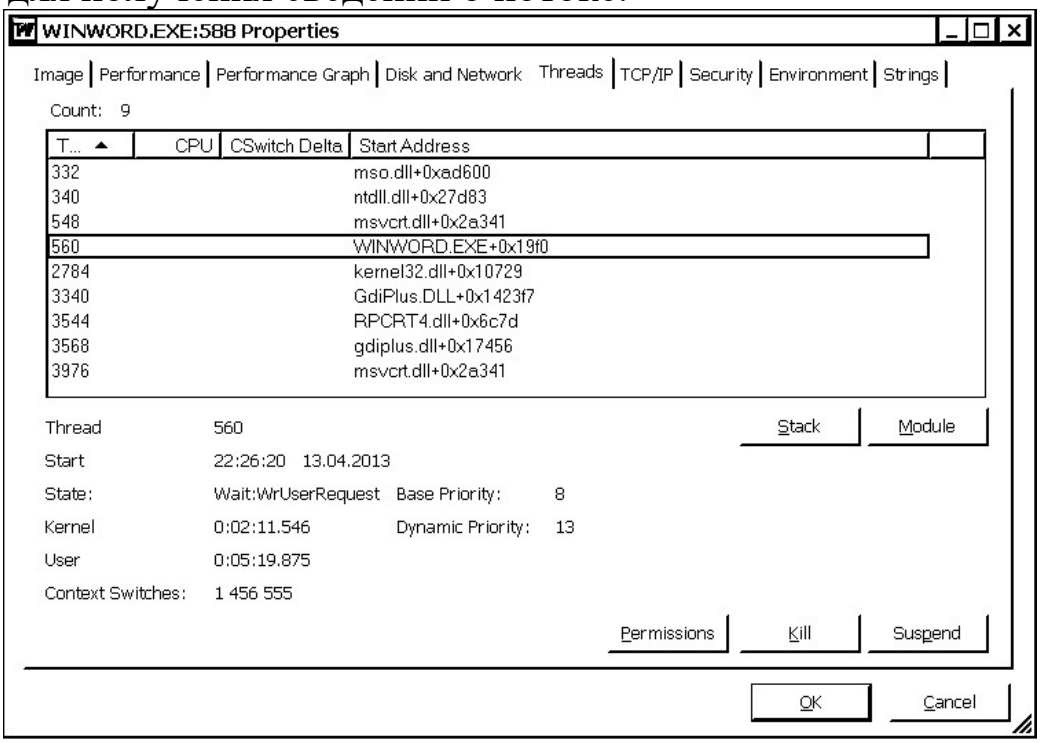

Рис.7.7. Сведения о потоках внутри процесса **WINWORD.EXE**

Задания

- Прочитайте начало статьи **Многопоточность** на **Википедии**
- Запустите редактор **WORD**
- Просмотрите информацию о потоках внутри данного процесса
- Запишите сведения о потоках
  - число потоков
  - поток, запущенный позже всех
  - идентификатор этого потока **TID**
  - время его запуска **Start**

Графики

Для вывода на экран индикаторов и диаграмм выберите в верхнем меню **View ► System Information**.

Для многоядерной машины по умолчанию выводится отдельный график для каждого процессорного ядра.

Задания

- Откройте окно **System Information**.
- Перейдите на вкладку **Summary**
- Запишите и переведите названия индикаторов и их значения
- Перейдите на вкладку **CPU**

- Запишите следующие сведения
  - Загрузка процессора
  - Число процессов
  - Число потоков
- Включите и выключите установку
  - **Show one graph per CPU**
- Перейдите на вкладку **Memory**
- Запустите **Диспетчер задач**
- Сравните показания **Диспетчера** и **Process Explorer**
- Запишите следующие сведения:
  - Объем физической оперативной памяти
  - Объем использованной оперативной памяти
  - Объем незанятой оперативной памяти
  - Максимально доступный объем оперативной памяти
- Сделайте вывод о наличии и размере файла подкачки
- Прочитайте и переведите первый абзац статьи **Commit charge** на сайте **http://en.wikipedia.org**

PROCESS MONITOR

Утилита **Process Monitor** отслеживает обращение процессов к ресурсам системы. После запуска **Process Monitor** открывается окно фильтров для исключения стандартных событий из дальнейшего наблюдения. Нажимаем **[OK]**. Для дальнейшей работы может потребоваться нажать кнопку **Reset**.

Чтобы выбрать процесс для наблюдения, выберите в верхнем меню **Tool ► Process Tree** либо нажмите кнопку  в верхней панели инструментов. В диалоговом окне **Process Tree** укажите на процесс и нажмите кнопку **Include Process**, затем **Close**.

Вывод на экран сведений о наблюдаемом процессе – кнопки в верхней панели инструментов:

-  **Show Registry Activity**
-  **Show File System Activity**
-  **Show Network Activity**
-  **Show Process and Thread Activity**

Для остановки мониторинга щелкните по кнопке  **Capture** на панели инструментов. Значок становится зачеркнутым. Повторный щелчок возвращает режим перехвата системных событий.

Для вывода на экран последних событий используется автоматическая прокрутка. Чтобы включить или выключить автоскроллинг, щелкните по кнопке  **Autoscroll** в панели инструментов.

Для очистки экрана нажмите кнопку  **Clear**.

Чтобы сохранить результаты мониторинга, нажмите кнопку  **Save** или выберите **File ► Save** в верхнем меню.

Задания

- Прочитайте начало статьи **Реестр Windows** на **Википедии**
- Прочитайте статью **Process Monitor** на **Википедии**
- Запустите **Process Monitor**
- В окне фильтров нажмите **[OK]**
- Запустите командное окно: **[Win + R] ► cmd**
- Переключитесь в **Process Monitor**
- Откройте дерево процессов
- Выберите **cmd**
- Запишите идентификатор процесса **PID**
- Включите **cmd** в наблюдаемые процессы
- Включите вывод обращений к реестру
- Переключитесь в командное окно **cmd**
- Введите команду **cd**
- Вызовите окно фильтров
- Убедитесь в появлении правила по **PID**
- Закройте окно фильтров
- Щелкните по кнопке  **Capture**
- Убедитесь в изменении кнопки **Capture**
- Щелкните по кнопке  **Capture**
- Включите и выключите автоскроллинг
- Нажмите кнопку **Clear**
- Включите вывод операций с реестром
- Сохраните результаты мониторинга:
    - **Events to save ► All events**
    - **Format ► CSV**

- Откройте сохраненный файл в **EXCEL**

DESKTOPS

Утилита **Desktops** позволяет создать до четырех виртуальных рабочих столов. После запуска утилиты в области уведомлений (системном трее) в правом нижнем углу экрана появляется иконка программы  .

Для выбора рабочего стола щелкните по значку левой кнопкой мыши (рис.7.8).

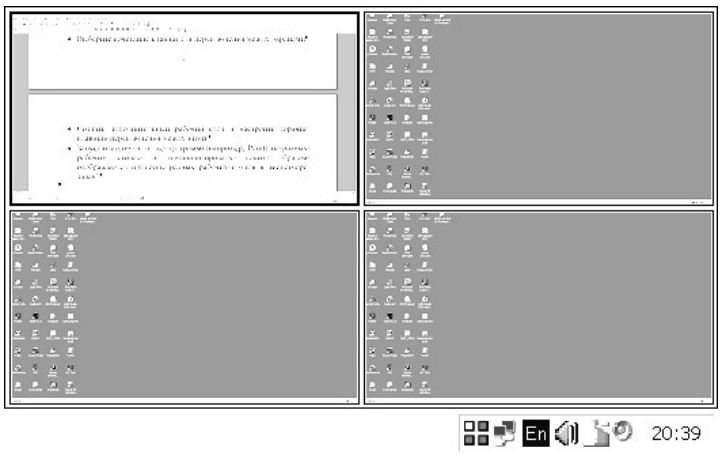

Рис.7.8. Выбор рабочего стола

Контекстное меню (рис.7.9) позволяет изменить настройки программы, включая сочетания клавиш для переключения между рабочими столами. Для автоматического запуска при входе в систему установите **Run automatically at logon**.

Задания

- Прочитайте описание **Desktops** на сайте **SysInternals**
- Прочитайте статью **Область уведомлений** на **Википедии**
- Запустите **Desktops**
- Выберите сочетание клавиш для переключения между экранами
- Запустить программу **Paint** на четырех рабочих столах
- Переключайтесь между рабочими столами
  - С помощью иконки в трее
  - С помощью комбинаций клавиш
- Запустите **Диспетчер задач**
- Найдите процессы **Paint**
- Завершите процесс **Desktops**

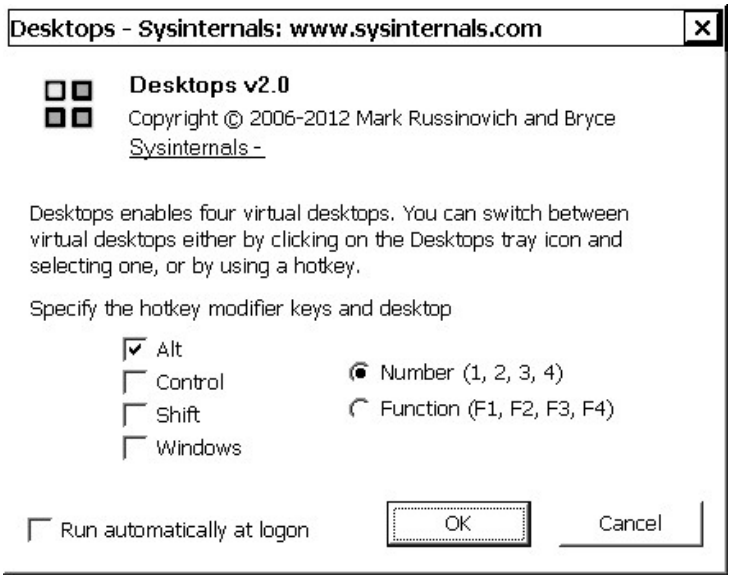

Рис.7.9. Окно настроек программы *Desktops*

ZOOMIT

Утилита **ZoomIt** позволяет увеличить область экрана и делать пометки во время доклада. Это удобно при показе презентаций и демонстрации работы программ.

После запуска утилиты в области уведомлений (трее) появляется значок программы  . Для вызова контекстного меню щелкните по значку любой кнопкой мыши. Варианты действий:

- **Options** – выбор режима увеличения
- **Break Timer** – таймер
- **Draw** – рисовать на экране
- **Zoom** – выбор режима увеличения
- **Exit** – закрыть программу

Режимы увеличения экрана:

Zoom – статичное увеличение. Вращение колесика мыши регулирует масштаб. Нажатие левой кнопки мыши включает режим рисования **Draw**. Во время рисования можно изменить размер «карандаша» клавишами **[Ctrl + ↑]** и **[Ctrl + ↓]** либо вращением колесика мыши при нажатой клавише **[Ctrl]**. Нажатие правой кнопки мыши выключает увеличение. Заметки не сохраняются при выходе из режима увеличения.

LiveZoom – динамическое увеличение. Мышь остается активной, область увеличения следует за мышью. Выключение режима осуществляется той же комбинацией клавиш, как и включение. Режим поддерживается не во всех версия **Windows**.

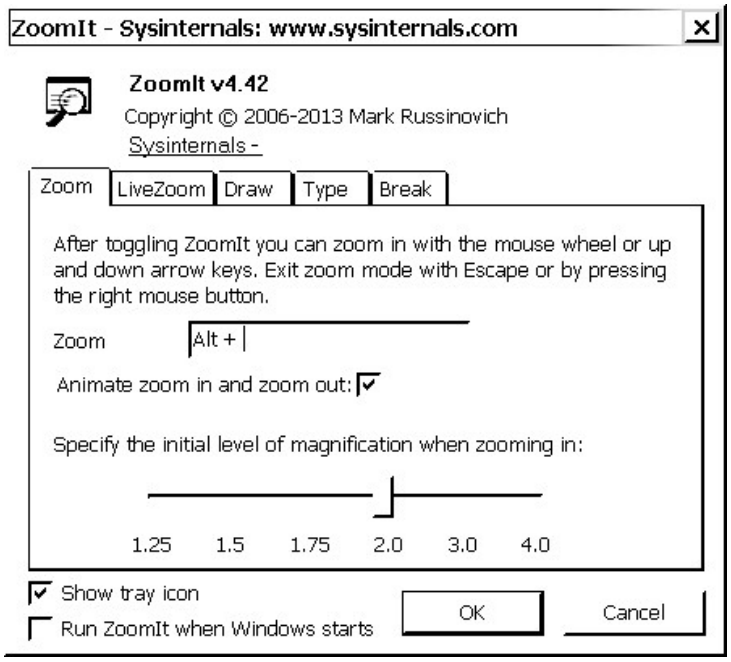

Рис.7.10. Настройка **ZoomIt**

Type – печатать текст поверх изображения экрана. В режиме рисования нажмите клавишу **[t]**. Можно печатать латинские буквы, цифры и знаки препинания. Выход – клавиша **[Esc]** или левая кнопка мыши. При выходе из режима увеличения заметки теряются.

Break Timer – включение таймера обратного отсчета. Дополнительные настройки – кнопка **Advanced**. Выход – клавиша **[Esc]** или правая кнопка мыши. Если выйти из таймера комбинацией клавиш **[Alt + Tab]**, то можно продолжить обратный отсчет, щелкнув левой кнопкой по значку в трее.

Задания

- Прочитайте описание **ZoomIt** на сайте **Sysinternals**
- Запустите утилиту **ZoomIt**
- Включите режим увеличения
- Перемещайте курсор по экрану
- Изменяйте масштаб колесиком мыши
- Сделайте пометки на экране
- Измените размер «карандаша»
- Сделайте пометки на экране
- Напечатайте комментарий
- Отключите масштабирование
- Запустите таймер через трей
- Завершите работу таймера клавишей **[Esc]**

- Измените настройки таймера:
    - Интервал 1 минута
    - Показывать время после истечения интервала
    - Положение в правом верхнем углу
    - Показывать таймер на фоне затемненного экрана
- Запустите таймер комбинацией клавиш
- Выйдите из таймера комбинацией клавиш **[Alt + Tab]**
- Продолжите обратный отсчет
- Завершите работу таймера правой кнопкой мыши
- Запишите свои предложения по использованию таймера при проведении докладов и презентаций