Федеральное агентство по образованию

Нижегородский Государственный Технический Университет

Кафедра: «Вычислительные системы и технологии»

Операционные системы

**Лабораторная работа №2**

**Настройка и оптимизация ОС Microsoft Windows**

Выполнил:

Студент группы 14-В-2

Носов А.В.

Проверил:

Кочешков А. А.

Нижний Новгород

2017

1. **Средства управления системой**

***1.1 Знакомство с Центром справки и поддержки Windows XP.***

Откроем Центр справки и поддержки с помощью клавиши *F1* или из меню *Пуск\Справка и поддержка.*

Произведем поиск интересующей нас информации, для этого введем в разделе поиск ключевые слова. Например: *Дефрагментация диска*. Разделы справки, удовлетворяющие, критериям запроса отобразятся в результатах.

Служебные программы вызываются:

- В разделе Центра справки и поддержки: Выбор задания – Использование служебных программ

для просмотра информации о компьютере и диагностике неполадок.

- В меню *Пуск\Программы\Стандартные\Служебные.*

- В разделе *Сервис*, апплета «Конфигурация системы» (msconfig.exe)

**Сведения о системе.** (msinfo32.exe) из состава Windows XP может использоваться для сбора сведений о компьютере, для определения неполадок в системе или доступа к другим средствам, входящим в состав Windows XP. Средство «Сведения о системе» собирает данные об устройствах, установленных на компьютере, о загруженных драйверах устройств и другую системную информацию, а также содержит меню для вызова связанных разделов о системе. Это средство может быть использовано для диагностики неполадок компьютера. Средство «Сведения о системе» содержит журнал драйверов устройств, установленных на компьютере. Используя данное средство, можно узнать о последних изменениях в системе. Если какое-либо из устройств работает неправильно и в журнале содержатся сведения о недавнем обновлении драйвера, необходимо установить исходный драйвер и проверить работу устройства. При помощи средства «Сведения о системе» можно выбрать другие средства, используемые для устранения неполадок в компьютере.

Сведения о системе подразделяются на категории:

|  |  |
| --- | --- |
|  | * Сведения о системе |
|  | * Ресурсы аппаратуры |
|  | * Программная среда |
|  | * Параметры обозревателя |
|  |  |

**Восстановление системы.** Эту опцию можно использовать для отмены из­менений в конфигурации системы и восстановления прежних пара­метров.

**Удаленный помощник.** Сервис обращения за помощью к другому удален­ному пользователю, которому вы доверяете. В этом случае другой пользо­ватель с вашего разрешения может общаться с вами, а также видеть ваш экран и работать удаленно с вашим компьютером.

**Предложение удаленной помощи.** Сервис оказания помощи другим поль­зователям в локальной сети или через Интернет.

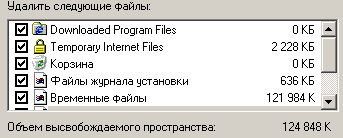
**Диагностика сети.** Сбор информации об оборудовании (модемы и сетевые платы) и сетевых подключениях (к локальной сети и Интернету).

**Очистка диска.** (cleanmgr.exe) Программа очистки дискового пространства для Windows. Программа очистки диска помогает освободить дополни­тельное свободное место на диске. Она проверяет диск и выводит список временных файлов, файлов кэша Интернета и ненужных про­граммных файлов, которые можно удалить.

До очистки диска:



Проведем очистку диска:



После очистки диска:



**Дефрагментация диска.** Программа дефрагментации объединяет разделен­ные (фрагментированные) файлы и папки на жестком диске компьютера. В результате работы программы все файлы и папки занимают на диске непрерывное пространство, что ускоряют работу с ними.

Defrag позволяет вернуть утраченную производительность рабочих станций Windows.

Мы можем добиться оптимальной производительности жестких дисков в системах под управлением Windows.

Проведем дефрагментацию диска:

C:\Documents and Settings\os>defrag C:

Программа дефрагментации дисков Windows

(C) Корпорация Майкрософт и Executive Software International Inc., 2001.

Отчет об анализе

9,99 ГБ Всего, 8,08 ГБ (80%) Свободно, 10% Фрагментировано (20% файл фрагментации)

Отчет о дефрагментации

9,99 ГБ Всего, 8,08 ГБ (80%) Свободно, 0% Фрагментировано (0% файл фрагментации)

Теперь операции по считыванию и записи информации будут выполняться быстрее, что положительно отразится на производительности системы в целом.

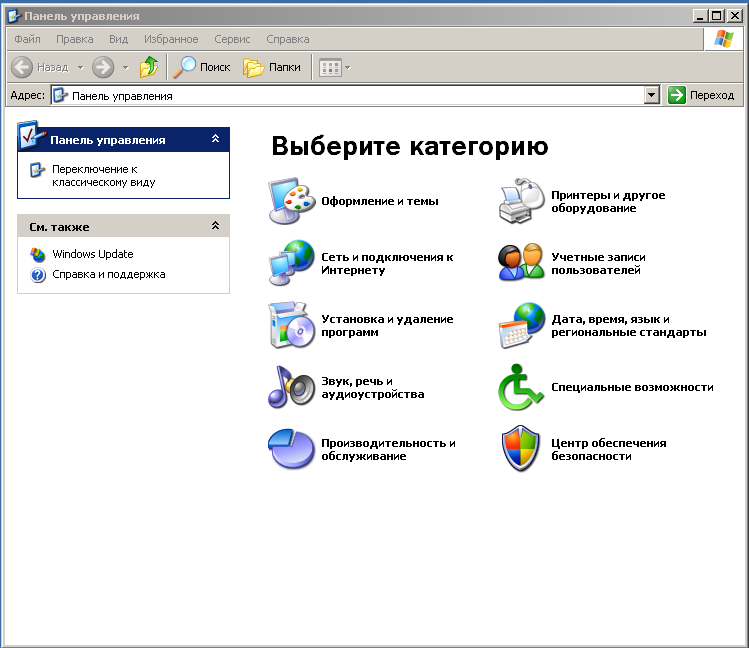
**Архивация данных.** Программа NTBackup создает копии важных файлов с учетом параметров настройки (например, копию папки Мои документы или Из­бранное). С помощью программы можно выполнить полную архи­вацию данных и создать диск автоматического восстановления системы в случае аварийного отказа.

**Конфигурация системы. (**msconfig.exe) управляет запуском служб программ, компонентов.

**Новые средства командной строки**. Список новых команд с описаниями.

***1.2 Управление компонентами системы с помощью средств панели управления.***

Основным назначением панели управления в Windows XP является конфигурирование системы.



***Состав панели управления:***

* Панель задач и меню "Пуск" (Taskbar and Start Menu).
* Экран (Display).
* Свойства панки (Folder Options)

*Сеть и подключения к Интернет***.**

Подключение к Интернету, настройка домашней или офисной локальной сети, конфигурирование установок сетевой карты, модема и телефона. Состав:

* Свойства обозревателя (Internet Options).
* Сетевые подключения (Network Connections).

*Установка и удаление программ.*

Установка и удаление программ и компонентов Windows.

*Звук, речь и аудиоустройства.*

Выбор звуковой схемы компьютера, настройка звуковоспроизводящих и записы­вающих устройств. Состав:

* Звуки и аудиоустройства (Sound and Audio Devices).
* Речь (Speech).

*Производительность и обслуживание****.***

На­стройка и конфигурирование параметров работы, монито­ринг производительности системы.

* Администрирование (Administrative Tools).
* Система (System).
* Назначенные задания (Scheduled Tasks).
* Электропитание (Power Options).

*Принтеры и другое оборудование.*

Настройка и конфигурирование параметров принтеров, клавиатуры, мыши, цифро­вой камеры и другого подключаемого оборудования.

* Игровые устройства (Game Controllers).
* Мышь (Mouse).
* Сканеры и камеры (Scanners and Cameras).
* Клавиатура (Keyboard).
* Принтеры и факсы (Printers and Faxes).
* Телефон и модем (Phone and Modem Options).

*Учетные записи пользователей.*

Создание и конфигуриро­вание пользовательских учетных записей.

*Дата, время, язык и региональные стандарты****.***

Настройка региональных опций и параметров много­язычной поддержки. Состав:

* Дата и время (Date and Time).
* Язык и региональные стандарты (Regional and Language Options).

Файлы типа \*.cpl - это компоненты панели управления. Хранятся они в каталоге Windows/system32.

access.cpl - Специальные возможности   
appwiz.cpl - Установка и удаление программ   
deck.cpl - Свойства: Экран   
hdwwiz.cpl - Мастер установки оборудования   
inet.cpl - Свойства: Интернет   
intl.cpl - Язык и региональные стандарты   
joy.cpl - Игровые устройства   
main.cpl - Свойства: Мышь   
mmsys.cpl - Свойства: Звуки и аудиоустройства   
ncpa.cpl - Сетевые подключения   
nusrmgr.cpl - Учетные записи пользователей   
odbccp32.cpl - Администратор источников данных odbs   
powercfg.cpl - Свойства: Электропитание   
sysdm.cpl - Свойства системы   
telephon.cpl - Телефон и модем   
timedate.cpl - Свойства даты и времени

***1.3 Использование консоли управления MMC.***

Консоль управления Microsoft Management Console - это основа администрирования и управления системы Windows. Это средство операционной системы, которое предоставляет своим встроенным (интегрированным) компонентам или, другими словами, системным приложениям, удобный для использования графический интерфейс.

ММС не содержит средств администрирования, но она позволяет в любой момент добавлять новые интегрированные компоненты и координировать работу уже установленных. Консоль управления ММС работает на любой платформе Win32 (например, Windows 2000, Windows NT 4.0, Windows 9x). Разработчики Microsoft почти все инструменты управления Windows XP встроили в систему в виде "оснасток" (snap-ins) MMC.

С помощью MMC существует возможность объединять встроенные в систему (интегрированные) компоненты, создавая собственные надежные средства управления компьютерами предприятия. Созданные таким образом управляющие системы можно сохранить в файлах с расширением .msc (Management Saved Console - сохраненная консоль управления) и распространять их в пределах всей системы (например, задавая к ним доступ с помощью ярлыков или элементов меню Start, отправляя их по почте или размещая на страницах Web).

Одно из достоинств ММС заключается в том, что собранную информацию можно сохранять выборочно и рационально, однако эта возможность доступна не для всех объектов. Сохраненный текстовый файл можно в дальнейшем распечатать. Можно, например, распечатать занятые прерывания IRQ компьютера (или любую другую информацию, которая должна быть всегда под рукой) и присоединить этот список на всякий случай к файлу.

Отметим очень полезный инструмент MMC, который позволяет работать с интегрируемыми компонентами в простом для пользователя интерфейсе - Функция панели задач (Taskpad View). Мастер New Taskpad View Wizard позволяет настроить параметры отображения элементов интегрируемых объектов и задач (или, иными словами, ярлыков команд, программ и проч.).

Перед тем как консольный файл будет сохранен и предоставлен в общее пользование, нужно установить некоторые ограничения. В окне ММС следует выбрать элемент Параметры (Options) меню Консоль.

Теперь нужно выбрать один из описанных ниже режимов выпадающего меню:

*- Авторский режим - предоставляет все права.*

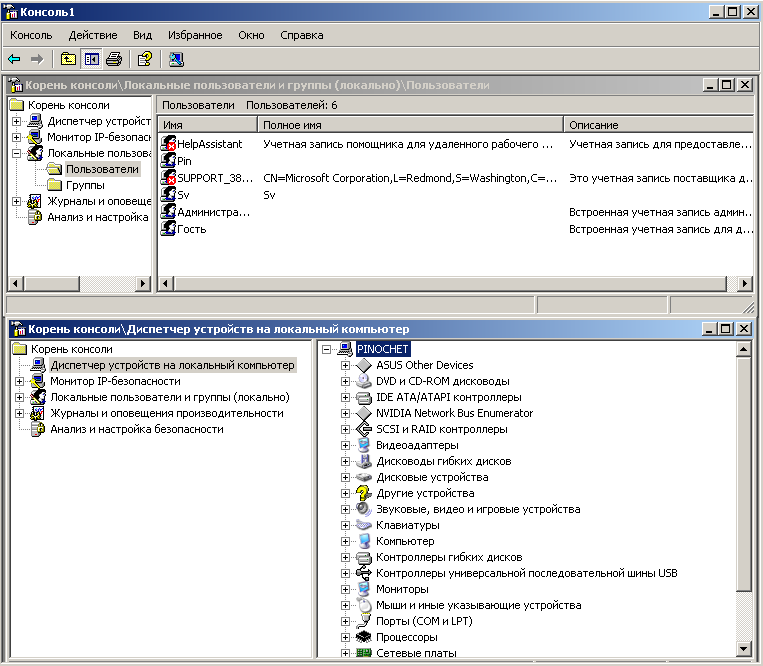
- *Пользовательский режим - полный доступ* - предоставляет пользователям доступ ко всем управляющим элементам ММС всех объектов дерева консоли. Однако пользователь лишен возможности добавлять или удалять интегрируемые компоненты и изменять параметры файла консоли.

*- Пользовательский режим - ограниченный доступ, многооконный*, - не позволяет открывать в консоли новые окна. В этом режиме пользователям не разрешается работать в тех ветвях дерева консоли, которые не были раскрыты при сохранении файла консоли.

*- Пользовательский режим - ограниченный доступ, однооконный,* - активизирует те же ограничения, что и режим Пользовательский режим - ограниченный доступ, многооконный. Разница заключается в том, что открывается только одно окно, и пользователь при этом лишается доступа к элементам управления, разрешающим работу с множественными окнами.

MMC позволяет создать свой собственный интерфейс управления, и значительно упрощает работу с системой.

Результат создания «своей» консоли:



1. **Управление устройствами**

***2.1 Процедуры установки устройств. Технология Plug and Play. Назначение INF файлов.***

При установке самонастраивающихся (Plug and Play) устройств необходимо физически подсоединить устройство, запустить windows, который автоматически должен обнаружить новое устройство и установить драйверы. При принудительной установке установка производится через мастер, либо вызов диспетчера устройств поддерживающего Plug and Play. При ручной установке необходимо указать inf-файл в апплете установки оборудования для драйвера устройства.

Plug and Play (сокр. PnP), дословно переводится как «включил и играй» — технология, предназначенная для быстрого определения и конфигурирования устройств в [компьютере](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80). Разработана фирмой [Microsoft](http://ru.wikipedia.org/wiki/Microsoft) при содействии других компаний. Важными составляющими PnP являются:

*PNP BIOS* — расширения BIOS для работы с PnP устройствами.

*Plug and Play Device ID* — индификатор PnP устройства имеет вид PNPXXXX, где XXXX — специальный код, работающий в связке с арбитром устройств.

*Plug and Play* - это стандарт компьютерной индустрии для автоматизации процесса добавления новых возможностей к вашему компьютеру. Технология PnP основана на использовании объектно-ориентированной архитектуры, ее объектами являются внешние устройства и программы. ОС автоматически распознает объекты и вносит изменения в конфигурацию системы, важными свойствами PnP являются относительная совместимость с уже установленными устройствами и независимость от аппаратных средств и ОС.

Аппаратные средства Plug and Play - это множество устройств компьютера, которые автоконфигурируемы системой Plug and Play. Аппаратные средства Plug and Play обычно состоят из адаптеров или эквивалентных схем на материнской плате компьютера; однако принтеры, внешние модемы и другие устройства, связанные с последовательными (COM) и параллельными (LPT) портами компьютера, так же могут поддерживаться Plug and Play.

Компьютеры, поддерживающие технологию Plug and Play и оборудованные Plug and Play-адаптерами, не требуют файлов config.sys и autoexec.bat. Каждый раз, когда вы загружаете ОС, она проверяет, какие адаптеры и периферийное оборудование, такое как принтеры, видеоадаптеры, инсталлированы на вашем компьютере. Далее она присваивает каждой карте свои собственные параметры: прерывания (IRQ), канал прямого доступа к памяти (DMA) и адреса портов. Наконец, стартовый процесс загружает только те драйверы, которые поддерживают установленные аппаратные средства.

Plug and Play обходится без переключателей и программ конфигурирования; вставляйте Plug and Play-адаптер, и Plug and Play-совместимый компьютер заработает с первого раза. Как только вы дважды щелкните по значку New Device (Новое устройство) в Control Panel (Панели управления), появиться окно New Device Installation Wizard (Мастера установки новых устройств). В Windows XP поддержку стандарта PnP можно установить с помощью средства панели управления «Установка и удаление программ». Если поддержка стандарта PnP установлена, то при добавлении в сеть универсального устройства Plug and Play компьютер под управлением Windows выполняет функцию контрольной точки для этого устройства. При этом на панели задач появляется уведомление о том, что доступно новое устройство.

*INF-файлы* - текстовые файлы, позволяющие управлять установкой драйвером или приложений. INF файлы содержат информацию для установки драйверов и программ. Формат INF файлов аналогичен формату INI файлов.

INF-файлы выполняют следующие задачи:

- Создание элементов реестра

- Определение параметров инициализации

- Копирование файлов дистрибутива и размещение их в системе.

- Инсталляция драйвера.

- Конфигурирование опций устройств

- Управление другими INF файлами

Назначение INF файлов на примере какого-либо устройства - в INF файле содержится информация для установки драйверов устройства, о производителе, о конкретных типах устройств.

**Пример части файла \inf\battery.inf:**

*[Version]*

*Signature="$WINDOWS NT$"*

*Class=Battery*

*ClassGuid={72631e54-78a4-11d0-bcf7-00aa00b7b32a}*

*Provider=%MSFT%*

*LayoutFile=layout.inf*

*DriverVer=07/01/2001,5.1.2535.0*

*[class\_copyfiles]*

*batt.dll*

*[DestinationDirs]*

*class\_copyfiles= 11*

*DefaultDestDir = 12*

*[ControlFlags]*

*;*

*; Exclude all devices from Select Device list*

*;*

*ExcludeFromSelect = \**

*[ClassInstall32]*

*AddReg=System\_Class\_Addreg*

*CopyFiles = class\_copyfiles*

*[System\_Class\_Addreg]*

*HKR,,,%REG\_SZ%,%BatteryClassName%*

*HKR,,Icon,%REG\_SZ%,"2"*

*HKR,,Installer32,%REG\_SZ%,"Batt.dll,BatteryClassInstall"*

*HKR,,NoInstallClass,,1*

*HKLM,SYSTEM\CurrentControlSet\Services\BattC,MofImagePath,%REG\_EXPAND\_SZ%,"System32\Drivers\battc.sys"*

*HKLM,SYSTEM\CurrentControlSet\Control\CoDeviceInstallers,{72631e54-78a4-11d0-bcf7-00aa00b7b32a},%REG\_APPEND\_MULTI\_SZ%,"Batt.dll,BatteryClassCoInstaller"*

***2.2 Использование диспетчера устройств. Получение информации и конфигурирование параметров устройств.***

Узел диспетчер устройств представляет одноименную оснастку, которая отображает в виде дерева все аппаратные устройства, установленные на локальном компьютере, и показывает их состояние, версии программных драйверов, используемые ресурсы (порты ввода/вывода, адреса памяти и IRQ). Данная оснастка позволяет изменять конфигурацию элементов, а также механизм их взаимодействия с ЦП. Диспетчер устройств позволяет:

Выяснить, корректно ли работает аппаратное обеспечение компьютера. Изменить конфигурационные настройки оборудования

Идентифицировать драйверы устройств, которые загружены для каждого устройства, и получить информацию о драйверах всех устройств

Изменить дополнительные установки и параметры устройств. Инсталлировать обновленные драйверы устройств. Отключать и активизировать устройства

Идентифицировать конфликты устройств и вручную конфигурировать установки ресурсов

Распечатать суммарную информацию об устройствах, установленных на компьютере

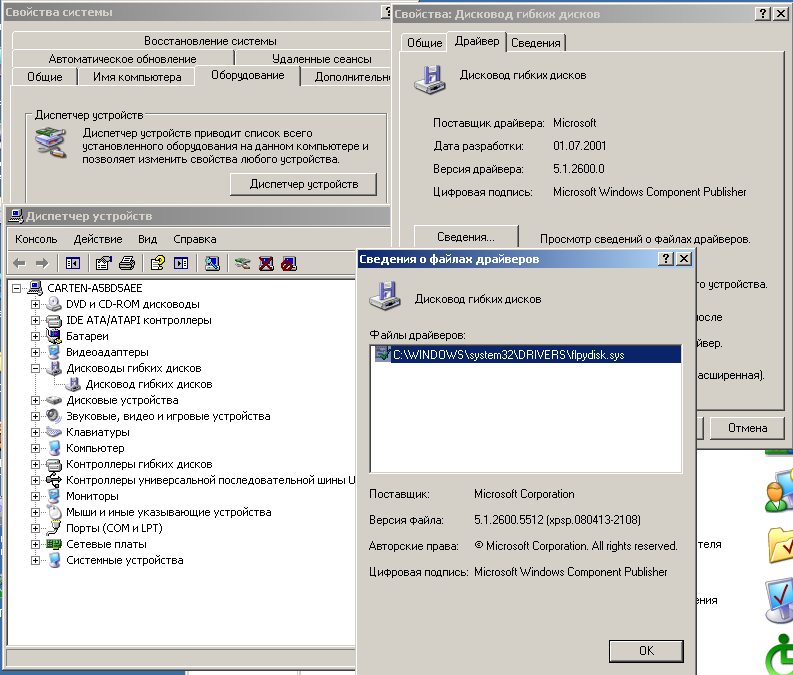
Диспетчер устройств преимущественно используется для проверки состояния аппаратного обеспечения и обновления драйверов устройств на компьютере. Диспетчер устройств можно использовать для управления устройствами только на локальном компьютере. На удаленном компьютере данная оснастка будет работать только в режиме просмотра.

Для каждого устройства на компьютере выделяется уникальный набор системных ресурсов для обеспечения корректной работы устройства. В число этих ресурсов входят:

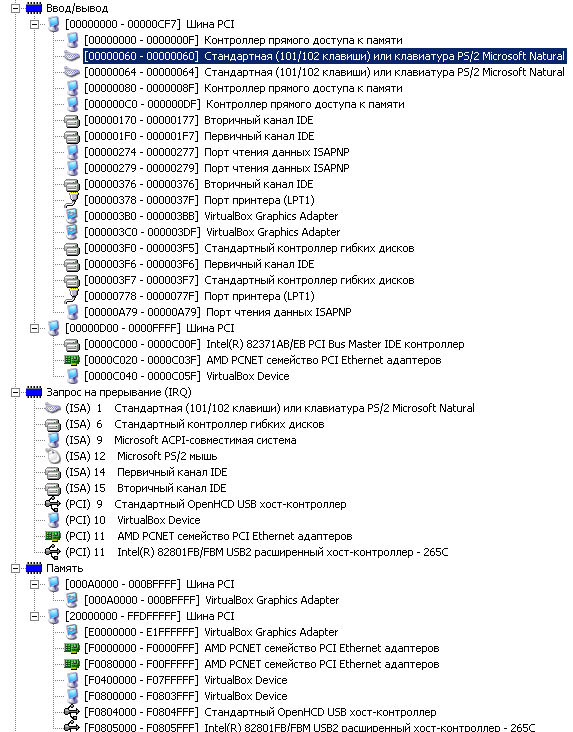
* *Номера запросов на прерывание (Interrupt Request, IRQ)*
* *Каналы прямого доступа к памяти (Direct Memory Access, DMA)*
* *Адреса портов ввода/вывода (Input/Output, I/O)*
* *Диапазоны адресов памяти*

Механизм Plug and Play системы Windows производит выделение данных ресурсов автоматически в ходе установки всех устройств, которые поддерживают данный механизм. Если два устройства обращаются к одним ресурсам, то возникает аппаратный конфликт. В этом случае необходимо вручную изменить установки ресурсов для обеспечения их уникальности для каждого устройства. Диспетчер устройств позволяет отключать и удалять устройства из системной конфигурации компьютера. При отключении устройства физическое устройство остается подключенным к компьютеру, но производятся соответствующие изменения в системном реестре, так что драйверы устройства не, будут загружены при следующем запуске системы. Отключение устройств полезно, если необходимо иметь несколько аппаратных конфигураций или если работа ведется на портативном компьютере, используемом вместе со станцией расширения.

Таким образом, мы можем определить ресурсы соответствующие реально существующим устройствам. Через вкладку Ресурсы мы можем определить диапазон I/O, ресурсы IRQ, диапазон памяти, DMA, используемые данным устройством. Также можно узнать размещение данных ресурсов.

**

***Распределение ресурсов:***

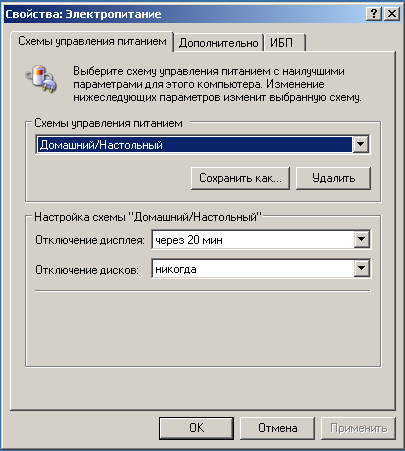


***2.3 Работа устройств в различных режимах энергосбережения.***

С помощью параметров питания в Windows XP можно сократить потребление электроэнергии некоторыми устройствами компьютера или системой в целом. Для этого нужно выбрать схему управления питанием, которая представляет собой набор параметров, определяющих использование электроэнергии компьютером. Можно также создать собственную схему управления питанием или использовать схемы, поставляемые с Windows.

Кроме того, в Windows поддерживаются два режима работы, которые можно использовать для неактивного компьютера, – *Ждущий режим* и *Спящий режим*.

Чтобы открыть окно параметров электропитания, щелкните правой кнопкой мыши на любой свободной области рабочего стола и выберите параметр *Свойства*. Затем перейдите на вкладку *Заставка* и щелкните на кнопке *Питание*.



Окно свойств электропитания содержит несколько вкладок, которые рассматриваются далее.

Вкладка *Схема управления питанием* содержит раскрывающееся меню *Схемы управления питанием*, в котором можно выбрать такие варианты энергосбережения:

* Домашний/Настольный;
* Портативная;
* Презентационная;
* Включен постоянно;
* Диспетчер энергосбережения;
* Экономия батарей.

Выберите тот режим энергосбережения, который соответствует используемому вами компьютеру. Например, схемы *Портативная* и *Экономия батарей* предназначены для ноутбуков и портативных компьютеров, а схемы *Презентационная* и *Включен постоянно* – для систем, работающих без перерыва в течение суток.

В области окна *Настройка схемы* можно настроить такие параметры.

* Параметр *Отключение дисплея*. Период времени, по истечении которого монитор автоматически отключится (при отсутствии пользовательской активности).
* Параметр *Отключение дисков*. Период времени, по истечении которого жесткий диск или жесткие диски автоматически отключатся (также при отсутствии пользовательской активности).
* Параметр *Ждущий режим*. Находясь в ждущем режиме, компьютер переключается в режим с низким потреблением электроэнергии, в котором отключаются жесткие диски и монитор. При возобновлении работы компьютер быстро выходит из ждущего режима, и рабочий стол полностью восстанавливается.
* Параметр *Спящий режим*. В спящем режиме все содержимое оперативной памяти сохраняется на жестком диске, отключаются монитор и жесткие диски, и компьютер выключается. При перезапуске компьютера рабочий стол полностью восстанавливается. Выход из спящего режима занимает больше времени, чем выход из ждущего режима.

*Для использования спящего режима необходимо установить соответствующий флажок на вкладке Спящий режим.*

На вкладке *ИБП* можно настроить параметры работы источника бесперебойного питания. Это устройство позволит сохранить ваши данные и обеспечить стабильную работу компьютера в условиях перебоев в поставке электроэнергии или полного отключения света. Параметры вкладки доступны только в том случае, если ИБП подключен к вашему компьютеру.

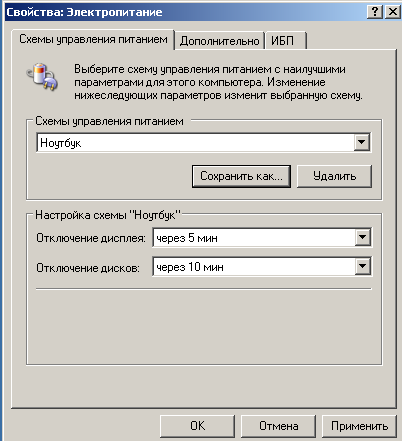
На вкладке *Дополнительно* можно настроить следующие параметры.

* Установите флажок *Всегда отображать значок на панели задач*, чтобы индикатор электропитания был размещен на панели задач Windows. Это может понадобиться, например, для ноутбуков и других портативных компьютеров.
* Установите флажок *Запрашивать пароль при выходе из спящего режима*, чтобы при выводе компьютера из данного режима у пользователя запрашивался пароль. Это позволяет, например, обеспечить защиту компьютера в офисе, когда сотрудник может отойти от своего рабочего места.

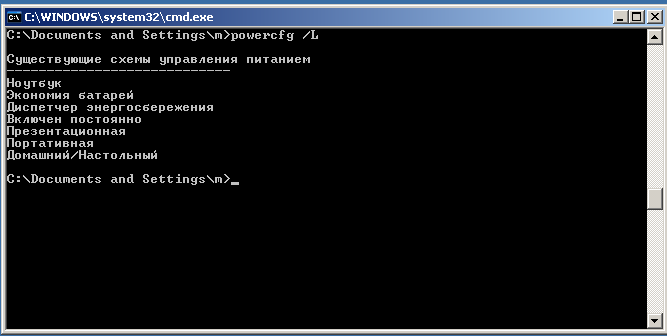
В поле *Кнопки питания* можно выбрать то, каким образом компьютер будет реагировать на нажатие кнопки питания на корпусе компьютера и кнопки перехода в ждущий режим, расположенной на клавиатуре.

***Создания своего плана энергопотребления***

Я создал собственный план энергопотребления, изменив параметры “Отключение дисплея” и “Отключение дисков”, назвав его как “Ноутбук”



***Возможности команды powercfg***



Утилита командной строки POWERCFG предназначена для управления параметрами электропитания в командной строке Windows в соответствии со спецификацией ACPI. ACPI (Advanced Configuration and Power Interface - усовершенствованный интерфейс управления конфигурацией и электропитанием) - открытый промышленный стандарт, впервые выпущенный в декабре 1996 года и разработанный совместно компаниями HP, Intel, Microsoft, Phoenix и Toshiba, который определяет общий интерфейс для программного управления электропитанием . Стандарт ACPI определяет возможности управления электропитанием компьютерного оборудования со стороны операционных систем. Получить более подробную информацию о программе и ее параметрах можно через команду powercfg /?

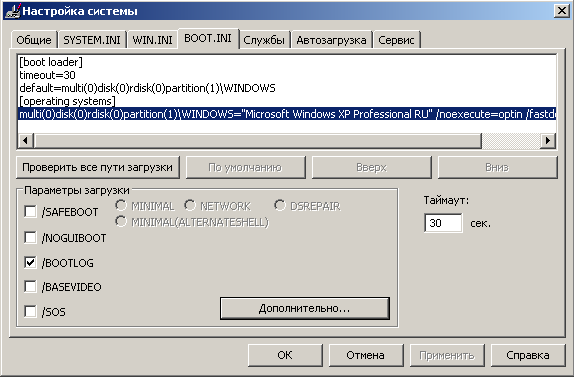
**Примеры:**

* Отобразить текущую конфигурацию схемы электропитания: powercfg /Q
* Включение функции гибернации: powercfg /hibernate on
* Получения информации о поддерживаемых состояниях спящего режима: powercfg /a

1. **Реестр и файлы инициализации**

***3.1 MSConfig. Основные установки системных файлов конфигурации.***

Программу настройки системы msconfig можно запустить с помощью команды msconfig из пункта "Выполнить". После загрузки появляется окно с семью вкладками:



*- Общие - позволяет управлять параметрами запуска системы.  
- System.ini.- редактирование файла System.ini.*

SYSTEM.INI - содержит информацию о конфигурации системы, ее аппаратных средств и драйверов. В отличии от WIN.INI не имеет значений по умолчанию.

[Boot] – драйверы и модули Windows

Shell = программа – графическая оболочка (обычно Explorer.exe)

[386Enh] – параметры защищенного режима (управление памятью процессами, диском, шрифтом и т.д.)

32bitDiskAccess = On/Off

Имеет параметры настройки DOS программ для управления EMS памятью, шрифтами, обращением программ к COM портам, работой клавиатуры.

Global = имя\_устройства –в памяти устанавливается копия драйвера, доступная VDM.

MinTimeSlice = 20 – квант времени в мс

[NonWindowsApp] – информация о TSR DOS программах, которые должны быть скопированы в каждую VDM.

[Drivers] – определяет состав имен драйвера

*- Win.ini - редактирование файла Win.ini*

WIN.INI содержит информацию о среде и параметрах.

[Windows] – содержит общие параметры (отображение курсора, скринсейвер вкл./выкл., загружаемые программы).

[Intl] – управление числами, датой, временем

[Fonts] – шрифты

[Ports] – перечисление COM и LPT портов

имя\_порта = скорость, четность, длина слова, стоп\_биты [,p]

[Color] – цветовые схемы

компонент = цвет (красный%, зеленый%, синий%)

[Embedding] – связка с OLE. Определяются классы объектов, которые могу внедряться в приложения-клиенты

*- Boot.ini - редактирование файла Boot.ini*

В Boot.ini задан выбор одной из нескольких ОС. Boot.ini используется при загрузке ОС.

*- Службы* – здесь перечислены все работающие системные службы.  
*- Автозагрузка* - здесь перечислены все программы, которые запускаются при загрузке системы.

Программа настройки системы (msconfig.exe) позволяет отключить загрузку любой программы или выполнение строки одного из перечисленных файлов, не правя ничего вручную, просмотреть и отключить некоторые файлы и службы. При этом комментарии будут расставлены автоматически, а программы, запускаемые из реестра, например, из раздела "Run", будут перенесены в раздел "Run-" (в конце соответствующего раздела добавляется символ "-"), т.е. благодаря msconfig.exe не нужно самостоятельно разыскивать необходимую информацию в реестре и файлах, чтобы посмотреть, что загружается на компьютере.

***3.2 Regedit. Главные ключи реестра.***

Системный реестр Windows - иерархически построенная, централизованная база данных в составе ОС Windows, содержащая сведения, которые используются для конфигурации ОС для работы с пользователями, программными продуктами и устройствами.Windows XP в отличие от своих предшественниц не имеет ограничения по размеру реестра.

В реестре хранятся данные, необходимые для правильного функционирования Windows. К ним относятся профили всех пользователей, сведения об установленном ПО и типах документов, которые могут быть созданы каждой программой, информация о свойствах папок и значках приложений, а также установленном оборудовании и используемых портах. Системный реестр заменяет собой большинство текстовых INI-файлов, которые использовались в ранних версиях Windows, а также файлы конфигурации MS-DOS (Autoexec.bat и Config.sys). Версии реестра для разных версий ОС семейства Windows имеют определенные различия. Данные реестра хранятся в двоичных файлах. Ключ реестра— некая переменная, которой присвоено определенное значение.

Куст (основной раздел) — раздел реестра, отображаемый как файл на жестком диске. Куст является набором разделов, подчиненных разделов и параметров и имеет корни на верхнем уровне иерархии реестра. По умолчанию большинство файлов кустов (Default, SAM, Security и System) сохраняются в папке %SystemRoot%System32Config. Папка %SystemRoot%Profiles содержит профили (настройки) каждого пользователя.Поскольку куст представляет собой файл, его можно перемещать из одной системы в другую.  
   
Реестр Windows XP состоит из следующих основных разделов (корневых ключей):

*HKEY\_CLASSES\_ROOT* — это ссылка на раздел HKEY\_LOCAL\_MACHINE SoftwareClasses. Хранящиеся здесь сведения обеспечивают запуск необходимой программы при открытии файла с помощью проводника. Этот раздел содержит связи между приложениями и типами файлов, а также информацию об OLE.

*HKEY\_CURRENT\_USER* — это ссылка на определенный подраздел HKEY\_USERS. Настройки соответствуют, активному пользователю, выполнившему вход в систему.   
*HKEY\_LOCAL\_MACHINE* — раздел содержит настройки, относящиеся к вашему компьютеру и действительные для всех пользователей, а также информацию об аппаратной конфигурации и установленном программном обеспечении.

*HKEY\_USERS* — этот раздел содержит настройки для всех пользователей компьютера.

*HKEY\_CURRENT\_CONFIG* — это ссылка на HKEY\_LOCAL\_MACHINE SYSTEM

CurrentControlSet Hardware ProfilesCurrent. Раздел содержит сведения о настройках оборудования, используемых при запуске системы, инф. о текущей конфигурации.

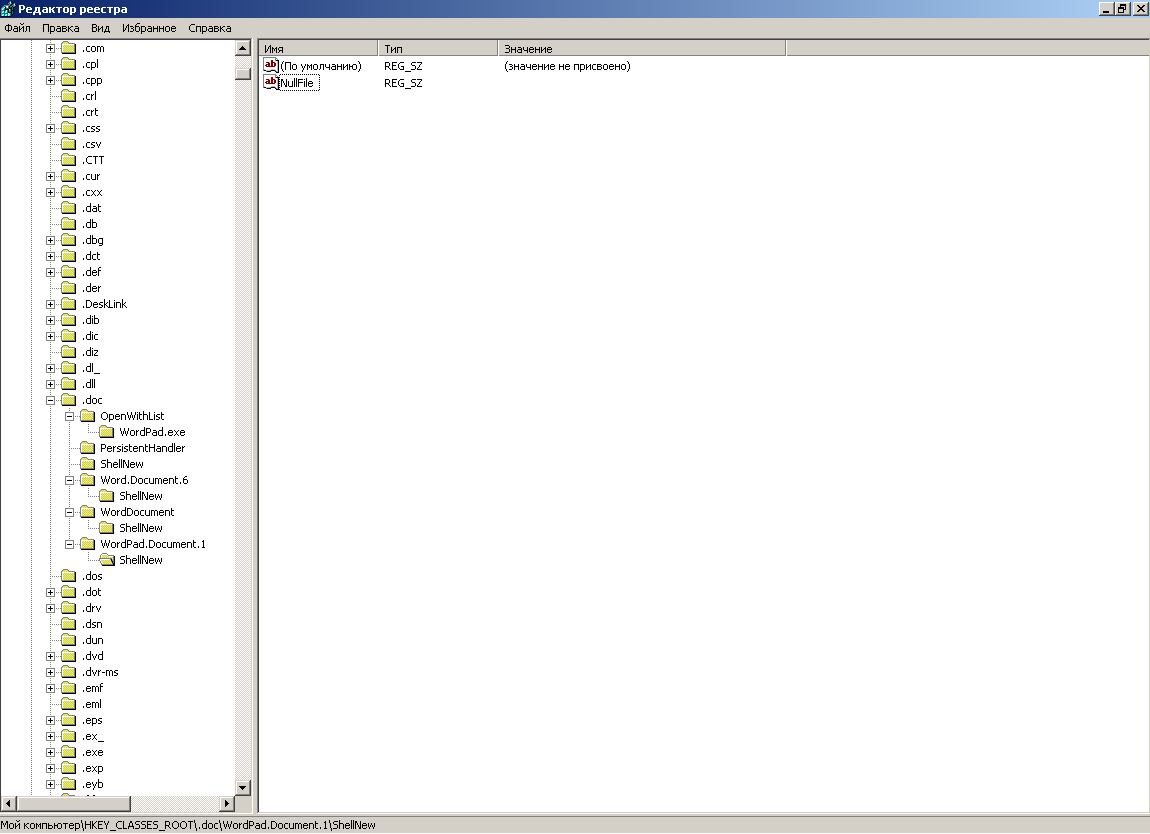
Вышеуказанные основные, стандартные разделы невозможно удалить или переименовать. Некоторые разделы реестра являются энергозависимыми (volatile) и не хранятся в каком-либо файле. ОС создает и управляет этими разделами полностью в памяти, поэтому они являются временными по своей природе. Система создает энергозависимые разделы каждый раз при начальной загрузке.

*HKEY\_LOCAL\_MACHINE HARDWARE* — раздел реестра, который хранит информацию по физическим устройствам и назначенным им ресурсам. Назначение ресурса и аппаратное обнаружение происходят каждый раз при загрузке системы, поэтому логично, что эти данные не записываются на диск.

Сердце системного реестра — это раздел HKEY\_LOCAL\_MACHINE SYSTEM.

Раздел HKEY\_USERS содержит все активные загруженные параметры пользователя.

*Regedit.exe* — это редактор конфигурации Windows (изменение базы данных конфигурации (реестра) Windows ). Программа позволяет просматривать и редактировать реестр Windows . Каждый корневой раздел реестра (куст) представлен в отдельном окне, разделенном на две части. Слева в виде папок отображаются разделы реестра, а справа — параметры, которые входят в состав выбранного раздела. Программа Regedit обладает очень мощными функциями — Некорректное использование редактора системного реестра может привести операционную систему в неработоспособное состояние, в результате чего потребуется полная переустановка.



* 1. ***Ключи аппаратной конфигурации, установленных программ, автозапуска, ассоциации типов файлов.***

*Описание текущей конфигурации в ключе HKEY\_LOCAL\_MACHINE:*

На текущую конфигурацию в HKLM указывает HKEY\_CURRENT\_CONFIG.

Пример изменения параметров:

1) При изменении разрешения экрана соответственно изменяется значение Resolution под ключом HKCC\Display\Settings.

2) При изменении используемого по умолчанию принтера изменяется значение Default под

ключом HKCC\System\CurrentControlSet\Control\Print\Printers.

3) Результат команды cpuid хранится в значении VendorIdentifier под ключом HKLM\Hardware\Description\System\CentralProcessor\0 и обновляется при загрузке системы.

4) При изменении размера кэша для cd-rom изменяются значения под ключом HKLM\System\CurrentControlSet\Control\FileSystem\CDFS

Поиск соответствующих ключей:

*1. Ключи установленных программ, аппаратной конфигурации:*

HKLM\System\SOFTWARE – далее в данном подразделе расположены ключи всех установленных программ (информация обо всех программах).

HKLM\System\HARDWARE – соответственно информация о аппаратной конфигурации.

*2. Ключи автозапуска, профиля пользователя и др.:*

Все ключи, соответствующие профилю текущего пользователя, расположены в разделе HKEY\_CURRENT\_USER (ссылка на определенный подраздел HKEY\_USERS. Настройки соответствуют, активному пользователю, выполнившему вход в систему). Когда пользователь регистрируется в системе, Windows копирует информацию из его профиля в раздел реестра HKEY\_CURRENT\_USER. Когда пользователь выходит из системы или завершает работу, Windows заменяет информацию в разделе, соответствующему данному пользователю, информацией из раздела HKEY\_CURRENT\_USER. Раздел HKEY\_CURRENT\_USER содержит множество настроек программного обеспечения, в которых хранится информация о конфигурации рабочего стола и клавиатуры. Кроме того, в этом разделе есть информация о параметрах меню Пуск. Здесь - все настройки, специфичные для пользователя.  
Раздел HKEY\_CURRENT\_USER полностью посвящен настройкам текущего пользователя, т.е. того пользователя, который в настоящий момент зарегистрирован в системе. Это отличается от пользовательской конфигурационной информации, которая хранится в других разделах реестра. Информация в этом разделе является динамической; информация в других разделах, которая относится к пользовательским настройкам, - статическая. Реестр копирует содержимое одного из подразделов из HKEY\_USERS в данный раздел и по окончании работы обновляет раздел HKEY\_USERS. В HKEY\_CURRENT\_USER Windowsполучает новую информацию о настройках системы, а также сюда помещаются любые изменения. Все, что здесь хранится, служит только для настройки системы для нужд пользователя, но никогда не содержит системной информации (например, описание драйвера устройства).

Для настройки автозапуска в реестре Windows предназначено несколько ключей:

Первая группа находится в ключе HKCU\Software\Microsoft\Windows\CurrentVersion, все ключи, относящиеся к автозагрузке, начинаются с Run. Эти программы запускаются только при входе в систему текущего пользователя. В зависимости от операционной системы это могут быть ключи:

Run - основной ключ автозапуска

RunOnce - служебный ключ для программ, которым требуется запуститься только один раз

RunServices - ключ для запуска служб в Windows 98/Me\*

Другая группа находится в ключе HKLM\Software\Microsoft\Windows\CurrentVersion, т. е. в аналогичном ключе, но в настройках, относящихся к компьютеру в целом, а значит, ко всем пользователям. Имена ключей такие же: RunServicesOnce - служебный ключ для служб, которым требуется однократный запуск

Run

RunOnce

RunServices

RunServicesOnce

Каждая запись в ключе автозапуска соответствует одной запускаемой программе. Запись состоит из имени записи, типа записи (для параметров автозапуска тип записи - строковый, обозначается как REG\_SZ) и значения, которое и является строкой запуска, т. е. включает имя исполняемого файла и параметры командной строки.

Например, представленная на [рисунке](http://www.intuit.ru/department/security/antiviruskasp/3/4.html#image.3.5#image.3.5) ниже запись "internat.exe" служит для автозапуска одноименной программы internat.exe. Эта программа является системной утилитой Windows, отвечающей за переключение раскладки (языка) клавиатуры.

Стандартными для Windows являются следующие строки запуска:

|  |  |
| --- | --- |
| Имя | Значение |
| KernelFaultCheck | %systemroot%\system32\dumprep 0 -k |
| Synchronization Manager | mobsync.exe /logon |
| LoadPowerProfile | Rundll32.exe powrprof.dll,LoadCurrentPwrScheme |
| ScanRegistry | C:\WINDOWS\scanregw.exe /autorun |
| SystemTray | SysTray.Exe |
| TaskMonitor | C:\WINDOWS\taskmon.exe |
| CTFMON.EXE | C:\WINDOWS\system32\ctfmon.exe |

В зависимости от настроек Windows и установленных программ ключи автозапуска могут содержать множество различных строк для запуска различных программ. Поэтому все на первый взгляд подозрительные файлы нужно перепроверять - они могут оказаться вполне обычными программам.

Настроить автозапуск программ можно и в системных файлах Windows - system.ini и win.ini. Эти файлы используются (преимущественно, использовались) в Windows 3.x, 9x, Me для хранения системных настроек. В Windows NT, 2000, XP аналогичные настройки перенесены в системный реестр, но старые конфигурационные файлы сохранены в целях обеспечения совместимости со старыми же программами.

Конфигурационные файлы win.ini и system.ini разбиты на секции. Название каждой секции заключено в квадратные скобки, например, [boot] или [windows].

В файле win.ini строки запуска программ выглядят так:

Load=<строка запуска>

Run=>строка запуска>

Анализируя такие строки можно понять, какие файлы запускаются при старте компьютера.

***Ассоциация типов файлов***

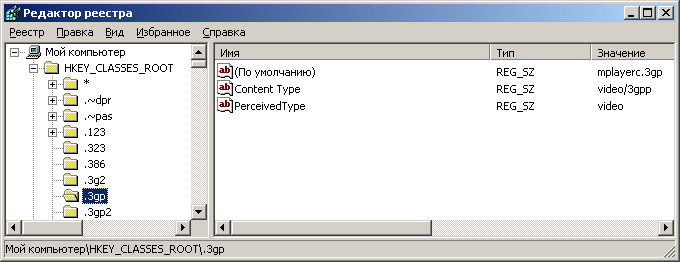
Корневой раздел реестра *HKEY\_CLASSES\_ROOT* - используется для ассоциации между приложениями и расширениями файлов. Другими словами, содержимое данного раздела, определяет, какие приложения, и каким образом, обрабатывают файлы с определенными расширениями. Например, при установленном пакете Microsoft Office, файлы с расширением .doc отображаются в проводнике с иконкой ассоциированного с данным типом файлов приложения Microsoft Word, а двойной щелчок на ярлыке такого файла вызовет его открытие для редактирования в Word.

Для просмотра и изменения ассоциаций файлов и приложений можно воспользоваться меню

Панель управления - Свойства папки - Типы файлов

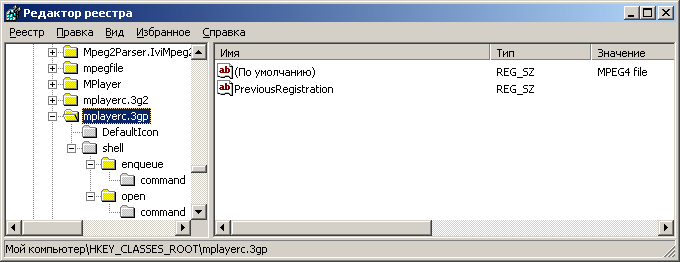
При создании ассоциаций выполняется запись определенных данных в раздел HKCR, что позволяет сопоставить определенному типу файла нужное для его обработки приложение и соответствующую ему иконку. В качестве примера возьмём записи в *HKEY\_CLASSES\_ROOT*, относящиеся к файлам с расширением .3gp

Отрываем раздел *HKEY\_CLASSES\_ROOT\.3gp*



Первый строковый параметр (Параметр по умолчанию) определяет имя раздела в *HKEY\_CLASSES\_ROOT*, данные которого, описывают приложение, сопоставленное расширению файла .3gp. Остальные параметры не обязательны, и описывают тип содержимого для файлов .3gp.

В данном случае, раздел реестра для ассоциации приложения с типом файлов .3gp - *HKEY\_CLASSES\_ROOT\mplayerc.3gp*



Количество и содержание подразделов и отдельных ключей определяется особенностями конкретных типов файлов и ассоциируемых с ними приложений, однако практически всегда присутствуют

DefaultIcon - параметр по умолчанию указывает на файл, содержащий иконку, сопоставленную файлам с данным расширением. В данном примере для открытия файлов с расширением .3gp используется приложение Media Player Classic , набор иконок которого хранится в библиотеке mpciconlib.dll в каталоге программы. Значение строкового параметра

*"C:\Program Files\K-Lite Codec Pack\Media Player Classic\mpciconlib.dll",*28

Где 28 - порядковый номер иконки. Одно и то же приложение может быть ассоциировано с несколькими типами файлов, и иметь несколько разных вариантов отображаемых иконок.

Shell - раздел определяет набор возможных действий над файлом данного типа.

Подраздел Open раздела Shell определяет действие при открытии файла .3gp

Подраздел Command раздела Open задает команду, выполняемую при открытии файлов .3gp. В данном случае:

*"C:\Program Files\K-Lite Codec Pack\Media Player Classic\mplayerc.exe" "%1"*

Т.о. при открытии файла с расширением .3gp, например, двойным щелчком мышки, будет запущен проигрыватель Media Player Classic, и в качестве входного параметра ему будет передано имя проигрываемого файла ("%1" в строке команды).

В ветви *HKEY\_CLASSES\_ROOT* есть раздел с именем "\*". Параметры, задаваемые в данном разделе определяют действия, выполняемые по отношению ко всем расширениям файлов, в том числе и не зарегитрированным. Действия по отношению к папкам определяются содержимым раздела *HKEY\_CLASSES\_ROOT\Folder*.

1. **Управление пользователями**

***4.1 Состав и основные свойства локального профиля пользователя.***

Windows XP использует понятие профиля пользователя, который хранит все личные данные и настройки. В этой операционной системе есть возможность использования разными пользователями компьютера различных профилей, а данные профиля надежно защищены от других пользователей.

*Профиль пользователя* - специальная папка на локальном компьютере, в которой хранятся файлы и настройки конкретного пользователя. По умолчанию приложения, совместимые с Windows XP, сохраняют свои данные и настройки пользователя в одну из папок профиля пользователя.

Независимо от типа профиля в момент работы пользователя на компьютере профиль хранится в папке Documents and Settings\%username%. Для доступа к этой папке также может использоваться переменная среды %userprofile%. Обычно папка Documents and Settings располагается на том же диске, что и операционная система.

Папка профиля пользователя обычно доступна администраторам компьютера, операционной системе и самому пользователю. Другие пользователи не имеют прав для просмотра, а тем более изменения данных, хранящихся в профиле.

Профиль всех пользователей предназначен для хранения данных и настроек, общих для всех пользователей компьютера. Профиль хранится в папке Documents and Settings\All Users. Для доступа к этой папке также может использоваться переменная среды %allusersprofile%.

Этот профиль по своей структуре идентичен профилю обычного пользователя, однако не содержит многих папок, предназначенных для хранения данных пользователя. Изменения в профиль всех пользователей могут вносить только члены локальных групп

|  |  |
| --- | --- |
| Папка | Описание |
| Application Data | Различные данные, сохраняемые приложениями для всех пользователей компьютера |
| Desktop | Значки, расположенные на рабочих столах всех пользователей |
| Favorites | Общие элементы папки Избранное Microsoft Internet Explorer |
| Documents | Общие элементы папки Мои документы . Главным образом файлы примеров |
| Start Menu | Структура подменю Программы меню Пуск общая для всех пользователей |
| Templates | Шаблоны файлов, создаваемых с помощью меню Создать файл |

Профиль пользователя по умолчанию абсолютно идентичен профилю обычного пользователя, за исключением того, что этот профиль не может быть использован ни одним пользователем компьютера. Профиль пользователя по умолчанию используется при создании профиля нового пользователя: при регистрации нового пользователя, ранее не использовавшего компьютер, его профиль создается путем копирования профиля пользователя по умолчанию. Поэтому, если вы хотите включить какие-либо файлы в профиль каждого пользователя, но не можете это сделать при помощи профиля всех пользователей, скопируйте эти файлы в профиль пользователя по умолчанию. Например, скопировав нужные значки в папку NetHood, вы добьетесь их появления в папке Мое сетевое окружение каждого нового пользователя.

Профиль пользователя по умолчанию хранится в папке %homedrive%\Documents and Settings\Default User. Изменения в профиль пользователя по умолчанию могут вносить только члены локальной группы Администраторы.

Windows XP поддерживает также так называемые локальные профили.  
Локальный профиль является единственным типом профилей, на работу с которыми ориентирован компьютер. При использовании остальных типов профилей (перемещаемый, обязательный) все равно создается и используется локальный профиль (они создаются на сервере).   
Локальный профиль обладает следующими свойствами:

хранится на конкретном компьютере; при перемещении пользователя на другой компьютер все его настройки и файлы остаются на старом компьютере;

не замедляет загрузку компьютера, т.к. хранится на одном из дисков компьютера;

данные профиля всегда соответствуют набору программного обеспечения, установленного на компьютере; профиль может использоваться только одним пользователем.

Локальный профиль пользователя хранится на компьютере в папке, имя которой совпадает с именем данного пользователя, находящейся в папке Documents and Settings на загрузочном томе. Если для данного пользователя не существует сконфигурированный перемещаемый (находящийся на сервере) профиль, то при первой регистрации пользователя в компьютере для него создается индивидуальный профиль. Содержимое папки Default User копируется в папку нового профиля пользователя. Информация профиля, вместе с содержимым папки All Users, используется при конфигурации рабочей среды пользователя. При завершении пользователем работы на компьютере все сделанные им изменения настроек рабочей среды, выбираемых по умолчанию, записываются в его профиль. Содержимое папки Default User остается неизменным. Если пользователь имеет отдельную учетную запись на локальном компьютере и в домене, для каждой из них создается свой профиль пользователя, поскольку регистрация на компьютере происходит с помощью различных учетных записей. При завершении работы все сделанные изменения также записываются в соответствующий данной учетной записи профиль.

Как уже говорилось, при создании профиля пользователя используется профиль, назначаемый по умолчанию, находящийся в папке Default User. Папка Default User, папки профилей индивидуальных пользователей, а также папка All Users, находятся в папке Documents and Settings корневого каталога. В папке Default User находятся файл NTuser.dat и список ссылок на объекты рабочего стола.

В таблице ниже перечислены подпапки, находящиеся внутри папки локального профиля пользователя, и описано их содержимое.

**Структура папки профиля**

По умолчанию каждый профиль пользователя имеет структуру файлов и папок, описанную ниже. Различные приложения могут добавлять свои файлы и папки в профиль, однако описанная структура остается неизменной, т.к. используется операционной системой для работы.

|  |  |
| --- | --- |
| Папка | Описание |
| Application Data | Различные данные, сохраняемые приложениями. По стандартам Microsoft приложения, совместимые с Windows должны сохранять настройки пользователя в системном реестре или в этой папке. Большинство приложений Microsoft, в частности Microsoft Office, сохраняют дополнительные файлы, шаблоны и т.п. в этой папке |
| Cookies | Файлы cookies, сохраняемые Microsoft Internet Explorer |
| Desktop | Значки и файлы, расположенные на рабочем столе пользователя |
| Favorites | Папка Избранное Microsoft Internet Explorer |
| Local Settings | Данные, хранимые только на локальном компьютере. При использовании перемещаемых профилей (см. ниже) содержимое этой папки не копируется на сервер |
| Local Settings\Application Data | Данные, сохраняемые приложениями, которые специфичны для данного компьютера и не должны копироваться в перемещаемый профиль |
| Local Settings\History | История посещения сайтов Microsoft Internet Explorer |
| Local Settings\Temp | Папка для хранения временных файлов, создаваемых приложениями и операционной системой во время работы |
| Local Settings\Temporary Internet Files | Папка для кэширования файлов Microsoft Internet Explorer |
| My Documents | Папка Мои документы |
| NetHood | Пользовательские значки, добавленные в папку Мое сетевое окружение |
| PrintHood | Пользовательские значки, добавленные в папку Принтеры |
| Recent | Ссылки на недавно открывавшиеся файлы |
| SendTo | Пользовательские значки, добавленные в меню Отправить |
| Start Menu | Структура подменю Программы меню Пуск пользователя |
| Templates | Шаблоны файлов, создаваемых с помощью меню Создать файл |
| UserData | Информация об адресах, набиравшихся в Microsoft Internet Explorer |
| ntuser.dat | Куст системного реестра HKEY\_CURRENT\_USER пользователя |
| ntuser.dat.log | Журнал транзакций куста системного реестра пользователя |
| ntuser.ini | Дополнительные параметры профиля пользователя. Например, список папок профиля, не копируемых при использовании перемещаемого профиля |

Перемещаемый профиль является расширением локального профиля и предназначен для использования пользователями, не имеющими постоянного рабочего места. При регистрации на компьютере пользователя с перемещаемым профилем операционная система выполняет следующие действия:

Если для пользователя не был создан локальный профиль, то он создается на основе профиля пользователя по умолчанию. Это необходимо для того, чтобы не вызвать сбоев в работе приложений, хранящих свои данные в профиле пользователя;

перемещаемый профиль пользователя синхронизируется с локальным профилем на компьютере. Копируются только те файлы, которые были изменены с момента последнего использования профиля пользователем;

осуществляется процедура загрузки профиля, как локального профиля.

Перемещаемый профиль обладает следующими свойствами:

хранится на конкретном компьютере и на сервере. Обычно копия профиля на сервере является самой свежей. При перемещении пользователя на другой компьютер все его настройки и файлы сохраняются;

существенно замедляет загрузку компьютера, даже если пользователь всегда использует один и тот же компьютер;

существенно замедляет завершение сеанса пользователя;

данные профиля не всегда соответствуют набору программного обеспечения, установленного на компьютере, что может привести к появлению неработающих значков или невозможности открыть некоторые файлы;

профиль может совместно использоваться несколькими пользователями, хотя это не рекомендуется.

**4.2 Конфигурирование пользовательской среды.**

Пользовательский профиль включает в себя настройки дисплея, параметры сетевых подключений, региональные параметры, подключения ВУ, содержит соответствующие файлы и каталоги, и другие индивидуальные параметры.Настройка пользовательской среды может выполняться через редактор реестра, либо через вкладки, меню и утилиты Windows.Через каталог \Documents and Settings\Администратор\LocalSettings\Application Data\ Identities\…\Microsoft\Outlook Express можно провести быструю настройку вашей (пользовательской) почты Outlook Express.

Через каталог \Documents and Settings\Администратор\Local Settings\History можно получить список ссылок на сайты в Интернете, посещаемые пользователем (журнал Internet Explorer).

Через \Documents and Settings\Администратор\Application Data\Microsoft\Internet Explorer\ Quick Launch можно провести настройку панели быстрого вызова.

Стоит отметить, что в каталог \Documents and Settings\Администратор\Local Settings\Application Data\ записывают информацию те программы, которые имеют какие-либо различные параметры для разных пользователей (либо подразумевают такую возможность.) Некоторые программы при установке (Client LotusNotes) “спрашивают” для какого пользователя установить программу (т.е. куда записывать различные файлы).

**4.3 Компоненты реестра определяющие профиль пользователя.**

Поддерево HKEY\_CURRENT\_USER содержит профиль пользователя для текущего зарегистрированного пользователя, включая системные переменные, персональные группы программ, установки рабочего стола (desktop), сетевые соединения, принтеры и приложения.

Поддерево HKEY\_USERS - содержит профили всех пользователей компьютера, а также профиль по умолчанию. Пользователи, обращающиеся к серверу дистанционно, в этом ключе на сервере не имеют профилей, их профили загружаются в реестр на их собственных компьютерах.

HKEY\_CURRENT\_USER является ссылкой на определенный подраздел куста HKEY\_USERS. Это значит, что все изменения в разделах, подразделах и ключах куста HKEY\_CURRENT\_USER автоматически тут же отображаются в определенном подразделе HKEY\_USERS, соответствующем активному пользователю. То есть пользователю, выполнившему процедуру входа.   
Ч тобы знать в каком же именно разделе HKEY\_USERS проводятся изменения вы должны узнать свой SID. Тогда искомый раздел будет именоваться, например, так: HKEY\_USERS\S-1-5-21-117609710 -1606980848-839522115-500. Где цифровая часть, вместе с буквой S, и есть SID.

Идентификатор безопасности ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Security Identifier (SID)) — структура данных переменной длины, которая идентифицирует учетную запись пользователя, группы, домена или компьютера (в [Windows](http://ru.wikipedia.org/wiki/Windows) на базе технологии NT ([NT4](http://ru.wikipedia.org/wiki/Microsoft_Windows_NT), [2000](http://ru.wikipedia.org/wiki/Microsoft_Windows_2000), [XP](http://ru.wikipedia.org/wiki/Microsoft_Windows_XP), [2003](http://ru.wikipedia.org/wiki/Microsoft_Windows_Server_2003), [Vista](http://ru.wikipedia.org/wiki/Microsoft_Windows_Vista)). SID ставится в соответствие каждой учетной записи в момент её создания. Система оперирует с SID'ами учетных записей, а не их именами. В контроле доступа пользователей к защищаемым объектам (файлам, ключам [реестра](http://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B5%D1%81%D1%82%D1%80) и т.п.) участвуют также только SID'ы. Каждая учетная запись в сети имеет уникальный SID. Внутренние процессы в Windows обращаются к SID для получения учетной записи пользователя или имени группы.

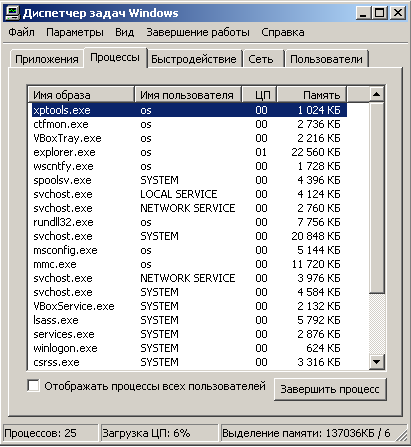
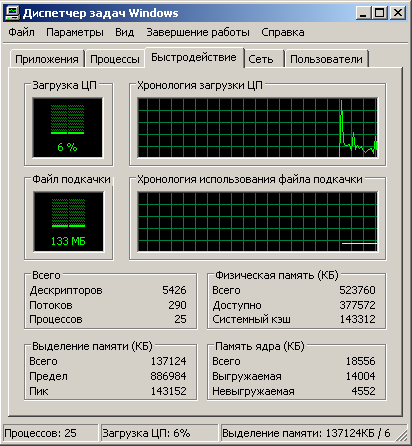
Идентификаторы безопасности для [встроенных учетных записей](http://ru.wikipedia.org/w/index.php?title=%D0%92%D1%81%D1%82%D1%80%D0%BE%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D1%83%D1%87%D0%B5%D1%82%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D1%8C&action=edit&redlink=1) (таких, как например Администраторы или Гости) одинаковы в каждом экземпляре установленной Windows и не зависят от ее версии (будь то Windows 2000 или Vista). Это позволяет администраторам сетей применять [шаблоны безопасности](http://ru.wikipedia.org/w/index.php?title=%D0%A8%D0%B0%D0%B1%D0%BB%D0%BE%D0%BD_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8&action=edit&redlink=1) и политики безопасности, а также управлять доступом удаленных пользователей в сети без доменов.

Открыв редактор реестра Regedit по ключу:

HKLM\SOFTWARE\ Microsoft\WindowsNT\CurrentVersion\ProfileList. Выберите SID и посмотрите ProfileImagePath. В конце строки найдете имя пользователя.   
Увидеть все SID, относящиеся к пользователям компьютера, вы можете раскрыв раздел HKEY\_USERS. Но в большинстве случаев знать SID не обязательно.

1. **Настройка производительности**

***5.1 Использование Task Manager для управления процессами. Наблюдение за использованием аппаратных ресурсов.***

**

Диспетчер задач предоставляет информацию о программах и процессах, запущенных на компьютере, и отображает наиболее общие показатели производительности процессов.

Диспетчер задач можно использовать для отслеживания индикаторов производительности вашего компьютера. Можно быстро отслеживать статус запущенных программ и завершать приложения, которые перестали отвечать на запросы системы. С помощью диспетчера задач можно отслеживать активность запущенных процессов по различным параметрам и просматривать графики использования процессора и памяти. В режиме реального времени можно отслеживать выполняющиеся приложения и процессы.

В вкладке Процессы в виде списка представлены все выполняющиеся в системе процессы. Процессом называется часть приложения, выполняющая определенные функции, т.е. некая программа на стадии выполнения. Приложение может состоять из нескольких процессов/потоков, а может состоять только из одного процесса. Для каждого процесса выводятся его параметры: имя образа (может не совпадать с именем запускаемого файла), имя пользователя, от чьего имени был запущен процесс, загрузка этим процессом процессора и объем занимаемой им оперативной памяти.

В современных компьютерах одновременно выполняется много приложений и еще больше процессов. Так как через определенные малые промежутки времени процессор переключается от одного процесса к другому, кажется, что программы работают одновременно.

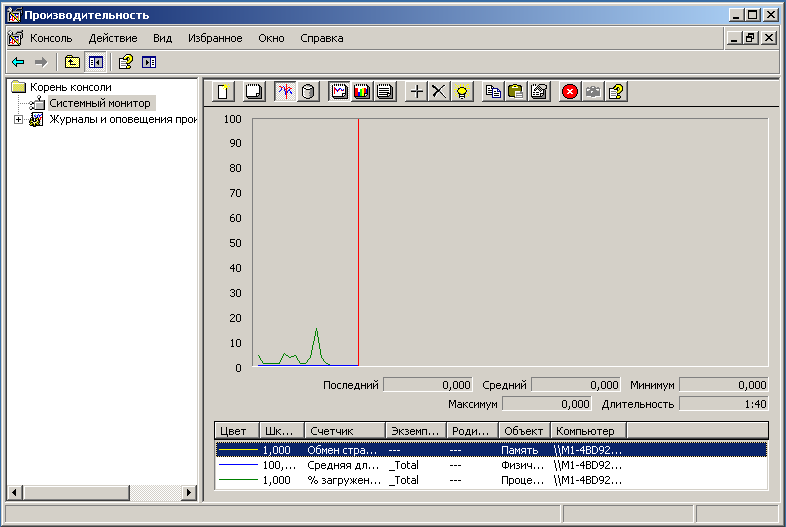
Приоритет представляет собой общий показатель того, как часто это процесс будет получать в свое распоряжение ресурсы компьютера, и, следовательно, как быстро будет работать. Подняв приоритет процессу, вы можете ускорить его работу, а опустив приоритет - наоборот, замедлить его работу. Установив флаг в нижней части диалогового окна, вы можете наблюдать состояние не только своих процессов, но и процессов других пользователей, если они работают в системе.

Возможно отсортировать все процессы по использованию ресурсов процессора и памяти. Для этого нажмите на заголовок поля ЦП или память.

В виде графика, рисуется журнал использования измеряемых параметров за прошедшее время. Любые всплески на графиках должны по времени соответствовать неким действиям, например запуску требовательной к ресурсам программы.

В вкладке Сеть выводится информация, показывающая использование сетевых возможностей компьютера. В виде графика рисуется история загрузки сети, отображается количество переданных и принятых по сети байт информации.

***Монитор ресурсов***

****

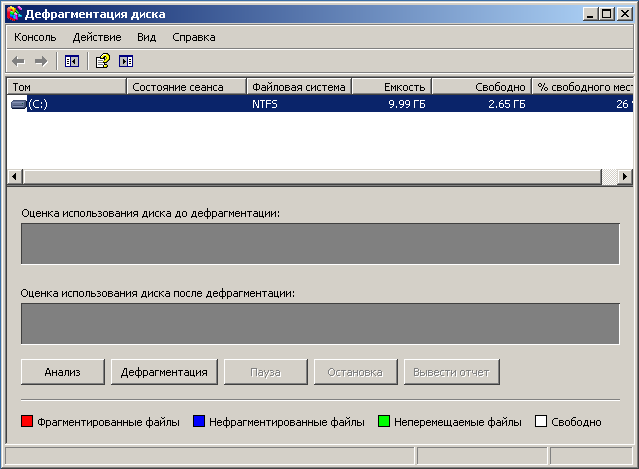
Монитор ресурсов (perfmon.exe) разработан корпорацией Microsoft, является частью операционной системы Microsoft Windows. Является монитором производительности, или системным монитором. PerfMon это утилита, предназначенная для отслеживания ряда процессов, дает возможность в режиме реального времени, получить графическое отображение загруженности различных процессов в различных версиях операционных систем Windows. Этот инструмент может быть использован, чтобы помочь вам в планировании апгрейда вашего сервера/ рабочей станции , слежении за процессами, которые должны быть оптимизированы. Использование системного монитора поможет выявить узкие места для их искоренения, что в результате даст бесперебойную работу ПК.

***5.2 Меры повышения производительности дисковой системы.***

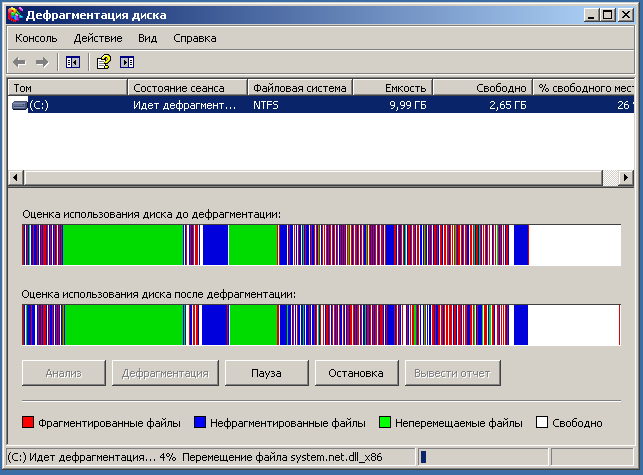
Для повышения производительности дисковой системы необходимо выполнять:

* Периодическая дефрагментация.
* Большой раздел, можно отформатировать под более быструю файловую систему.
* Размещение задач, активно использующих диск, на разных физических дисках или дисковых контроллерах.
* Обновление диска или установка дополнительных дисков.

В состав Windows входит утилита для дефрагментации диска, которую можно запустить из *Пуск-Все программы-Стандартные-Служебные-Дефрагментация диска*.



Утилита Дефрагментация диска - это системная служебная программа, выполняющая анализ локальных томов с последующим поиском и объединением фрагментированных файлов и папок.



Дефрагментацию дисков также можно запустить из командной строки с помощью команды *defrag***.**

***5.3 Настройка видеосистемы.***

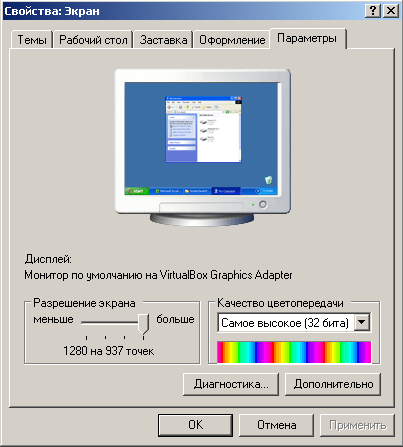
Настройка видеосистемы прямо зависит от оборудования. Так, например, процессор Pentium4 обеспечивает в дополнении к стандартному набору команд процессора еще около 30 команд для обработки битовых полей, которые могут использоваться для ускорения подготовки изображения перед выводом на экран; видеоадаптеры могут использовать для ускорения 32-, 64-, 128-разрядную шину данных или использовать графический процессор для обработки изображения. При настройке видеосистемы приходится исходить из возможностей видеоадаптера и монитора компьютера, количества имеющейся памяти, скорости процессора, типов обычно используемых приложений. Чтобы настроить монитор и видеоадаптер, проводим выбор "Пуск -> Настройка -> Панель управления -> Экран". В окне свойств экрана открываем закладку "Настройка". Бегунком "Область экрана" задается разрешение монитора. Второе важное поле на этой закладке - "Цветовая палитра". Тут устанавливается глубина цвета, (кол-во воспроизводимых цветов и оттенков). Для большинства мониторов и видеокарт могут быть установлены значения:

4 бита (16 цветов);

8 бит (256 цветов);

High color (16 бит);

True color (24 или 32 бита).



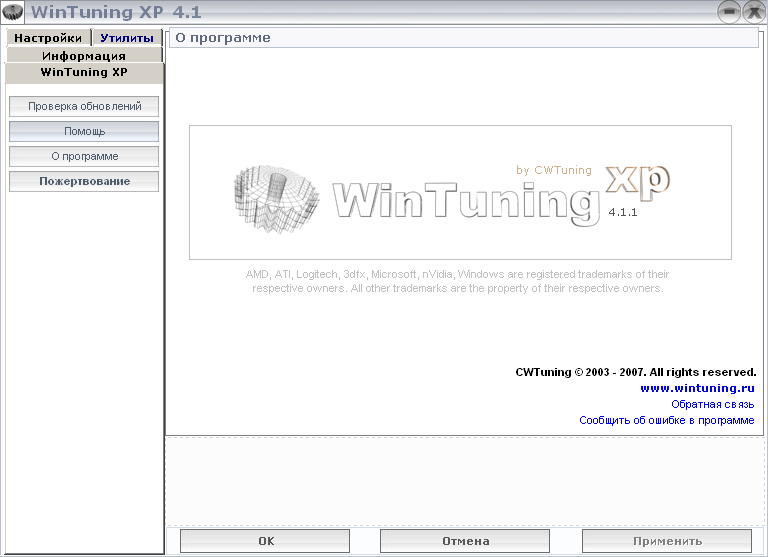
Для большинства приложений на сегодня оптимальны 16/32-битовые палитры. Если вы работаете в основном с текстами и качество отображения графики для вас не имеет значения, можете установить 8- или даже 4-битовую палитру. True color палитра нужна тем, кто профессионально работает со сложной графикой или хочет получить максимальное качество изображения. В закладке "Дополнительно -> Адаптер" имеется параметр "Частота обновления". Здесь можно задать частоту развертки, или частоту кадров. Чем частота кадров выше, тем меньше будут уставать ваши глаза. Рекомендуется установить максимально возможную частоту. Чем выше разрешение экрана и глубина цвета, тем меньшую частоту развертки сможет обеспечить ваша видеосистема.

Windows позволяет установить только те значения частоты развертки, которые поддерживают графическая плата и монитор. Если ОС не распознала монитор или видеокарту, то будет установлена частота 60 Гц, безопасная для работы компьютера.

***5.4 Стороннее ПО для оптимизации системы.***

*WinTuning XP* - это утилита для настройки и оптимизации систем Windows XP Home Edition/Professional. Программа включает в себя опции для изменения скрытых параметров Меню Пуск, Рабочего Стола, Проводника, программы Internet Explorer, ядра системы и др. Также в WinTuning XP содержатся опции, позволяющие улучшить безопасность системы и раскрыть недокументированные возможности Вашего оборудования. Кроме того, в программу включены утилиты для работы с системой: "Диски", "Автовыключение", "Изменение рабочего стола", "Чистка диска" и "Программы Windows". Все опции разбиты на группы - "Секции", что существенно облегчает навигацию по настройкам операционной системы. Плюс ко всему присутствует дружественный русский интерфейс и поддержка всех пользователей по любым вопросам, связанным с программой.

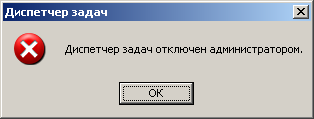
WinTuning XP работает только на платформах Windows XP (Professional и Home Edition). Работа только в этой системе даёт стопроцентную гарантию того, что все настройки работоспособны.



Проведем некоторые изменения в системе используя пакет WinTuning XP.

Выключим диспетчер задач:

Теперь после вызова Диспетчера задач мы получим сообщение:



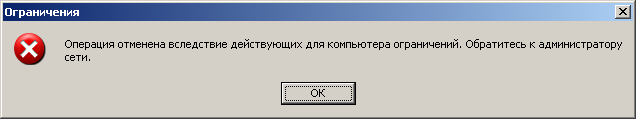
Отключим пункты “Выключение” и “Выход из системы”.

Изменим параметры меню ПУСК.

Оптимизируем скорость Com-портов (поднять до максимума).

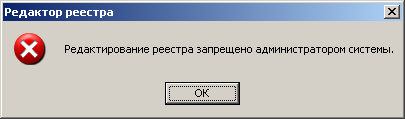
Запретим изменять параметры ActiveDesktop

При попытке изменений (вкладка Свойства ) получаем:

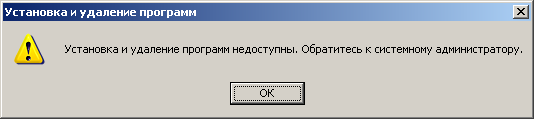


Запретим запуск редактора реестра

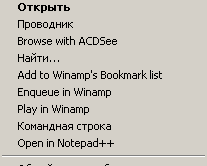
При попытке запуска regedit получаем:



В меню Безопасность поставим пароль на вкладку Установка и Удаление программ. При выборе ее с неверным паролем получим:

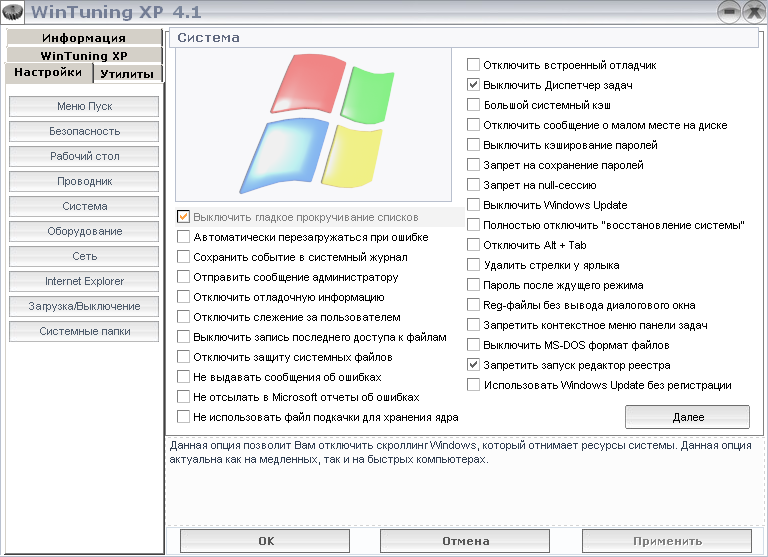


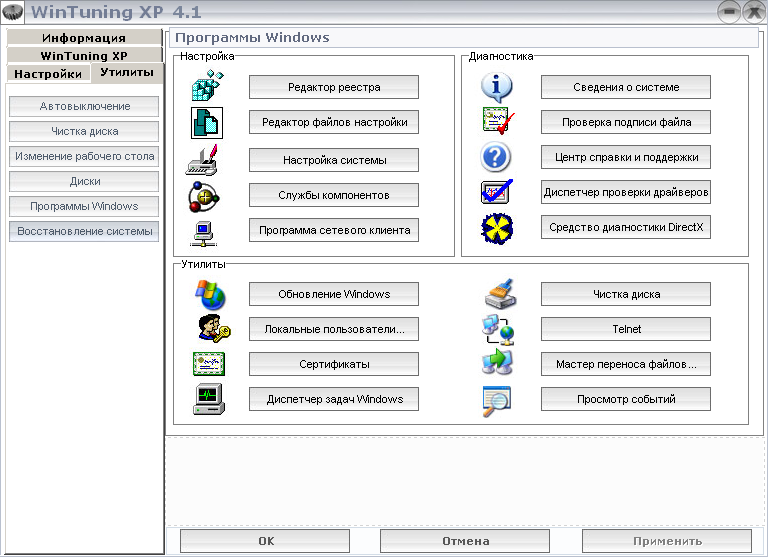
Установим возможность быстрого вызова командной строки. Теперь в контекстном меню для каталогов появилась соответствующая вкладка.



Можно провести еще множество экспериментов, но мы просто приведем два снимка меню программы WinTuning XP, чтобы дать возможность оценить ее возможности.

Меню Системных настроек и быстрого вызова программ Windows.





1. **Меры повышения устойчивости системы**

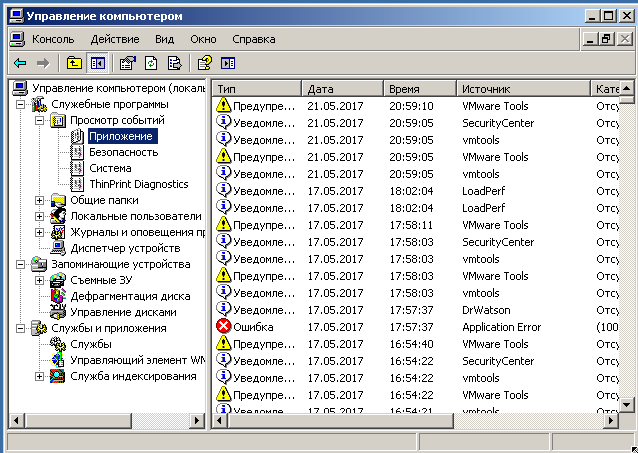
Число факторов, способных привести к нестабильной работе компьютерной системы и потере пользовательских данных, весьма велико - это и попытки заставить старые драйверы специфических устройств работать в Windows, и установка нового ПО, несовместимого с используемой ОС, и некорректное выключение компьютера, и множество других рискованных действий. Примерно в 80% случаев сбоев можно избежать печальных последствий, если заранее сделать резервную копию своих данных и грамотно воспользоваться имеющимися в ОС средствами восстановления.

Разработчики Windows XP постарались предусмотреть в этой новой ОС все возможные воздействия внешних факторов на стабильность ее работы, предложив пользователю широкий выбор средств для решения связанных с этим проблем. В частности, ОС семейства Windows XP содержат функции восстановления данных и средства преодоления проблем загрузки, унаследованные от предыдущих версий Windows и новые.

Специальные варианты загрузки:

В Windows XP пользователь может в полной мере оценить разнообразие вариантов загрузки, которые предусматривают практически все возможные случаи. Меню дополнительных вариантов загрузки вызывается нажатием клавиши F8 в процессе загрузки ОС (если используется несколько ОС - сразу после выбора Windows XP).

***Журнал отчётов***

******

На компьютере с Windows XP запись отчётов ведется в следующих трех журналах:

* Журнал приложений  
  В журнале приложений содержатся события, записанные программами. Например, программа работы с базами данных может записать в журнал приложений ошибку доступа к файлу. События для записи в журнал приложений определяются разработчиками программного обеспечения.
* Журнал безопасности  
  В журнал безопасности записываются такие события, как удачные и неудачные попытки входа в систему, а также события, связанные с использованием ресурсов (такие как создание, открытие или удаление файлов). Например, если включен аудит входа в систему, в журнал безопасности будет записываться событие при каждой попытке выполнить вход на этот компьютер. Чтобы включать и использовать запись событий в журнал безопасности, а также чтобы указывать события для записи, необходимо быть администратором компьютера или входить в группу администраторов.
* Журнал системы  
  В журнале системы содержатся события, записанные системными компонентами Windows XP. Например, если происходит сбой загрузки драйвера при запуске системы, соответствующее событие записывается в журнал системы. События, записываемые системными компонентами, предопределены в Windows XP.

***Консоль восстановления:***

Средство Recovery Console (Консоль восстановления) впервые было реализовано в Windows 2000. Его следует использовать только тогда, когда ни один из дополнительных вариантов загрузки не помогает решить возникшую проблему. Для применения Консоли восстановления нужно знать пароль учетной записи "Администратор" для регистрации в системе; подразумевается также наличие определенного опыта работы с командами ОС для устранения неполадок.

С помощью Консоли восстановления обычно решаются следующие задачи:

* + - запуск или остановка службы;
    - перенастройка служб, препятствующих нормальному запуску ОС;
    - форматирование жестких дисков;
    - чтение и запись данных с локальных дисков, использующих файловые системы FAT или NTFS;
    - восстановление системы путем копирования файлов с гибких дисков или установочного компакт-диска Windows XP;
    - другие административные задачи.

Для установки Консоли восстановления запустите файл winnt32.exe из папки I386 на установочном компакт-диске, задав ключ /cmdcons, и следуйте инструкциям системы. После установки Консоли восстановления вы сможете выбирать режим восстановления в окне выбора ОС. Данный метод восстановления системы подходит только для опытных пользователей и системных администраторов. Варианты использование команд Консоли восстановления для решения проблем загрузки приведены в таблице.

Использование команд Консоли восстановления (Recovery Console)

|  |  |
| --- | --- |
| Проблема | Решение |
| Служба или драйвер устройства загружены, но препятствуют нормальному запуску ОС | Используйте команду disable для отключения службы или драйвера устройства, перезагрузите ОС без использования службы и установите источник проблемы |
| Отсутствует файл, требующийся для запуска ОС | Используйте команду copy для распаковки восстановления данного файла с гибкого диска или установочного компакт-диска Windows XP |
| Поврежден загрузочный сектор | Используйте команду fixboot для восстановления |
| Повреждена главная загрузочная запись | Используйте команду fixmbr для восстановления главной загрузочной записи |

Полный список команд можно получить, вызвав команду Help в Консоли восстановления.

Другие возможности восстановления данных:

Windows XP, в отличие от предыдущих версий, использует принципиально новый механизм восстановления самой системы и данных после программных и аппаратных сбоев, аварийных ситуаций, вызванных некорректными действиями пользователя и прочими "объективными" обстоятельствами.

Средство восстановления системы System Restore позволяет возвращать систему в рабочее состояние, основываясь на точках восстановления (Restore Points), без потери пользовательских данных - документов Microsoft Office, почтовых сообщений, ссылок Internet Explorer и т. д. С помощью этого средства можно восстановить исправную версию системы, поврежденную неграмотными действиями пользователя, установкой некорректного драйвера устройства или ПО сторонних производителей. Механизм System Restore отслеживает изменения, происходящие с основными системными файлами, и сохраняет предыдущие версии перед тем, как перезаписать их. Определенный набор системных файлов сохраняется автоматически перед установкой ПО или драйвера устройства; кроме того, один раз в день в заданное время создается точка восстановления.

*Утилита восстановления системы служит для создания копии вашей системы – хранилища всех программ, которые вы установили. System Restore восстанавливает реестр, локальные профили, базу данных COM+, кэш (wfp.dll) системы защиты Windows File Protection (WFP), базу данных Windows Management Instrumentation (WMI), метабазу Microsoft IIS, а также файлы, которые она копирует по умолчанию в архив Restore. При этом выделить тот или иной компонент нельзя — восстановлению подлежит либо все, либо ничего.*

Назначение System Restore — вернуть систему в работоспособное состояние без необходимости полностью переустанавливать ОС и файлы данных. Утилита работает в фоновом режиме и автоматически создает точку восстановления (restore point) или копию, снимок вашей системы, когда происходит некое инициирующее событие. К числу таких событий относятся установка приложений, установки AutoUpdate, запуск процедуры восстановления с помощью Microsoft Backup Utility, установка неподписанных драйверов, а также создание точек восстановления вручную. Дополнительно утилита System Restore по умолчанию создает точки восстановления каждый день.

Для работы System Restore необходимо иметь на диске свободные 200 Мбайт, предназначенные для создания хранилища данных. Если нужного объема нет, System Restore остается отключенной до тех пор, пока не освободится дисковое пространство, после чего утилита активизирует себя сама. Утилита System Restore использует схему хранения FIFO: удаляет старые архивы, освобождая место для новых данных при достижении некоторого лимита объема данных в хранилище.

Утилита System Restore проводит мониторинг различных типов файлов, среди них большинство расширений, которые входят в состав устанавливаемого программного обеспечения (.cat, .com, .dll, .exe, .inf, .ini, .msi, .ole, .sys).

Далеко не всегда System Restore оказывается лучшим средством восстановления. Данная утилита изменяет много различных файлов и записей в реестре, и иногда она выполняет столько изменений, что вызывает еще большие проблемы. System Restore может отбросить компьютер назад на значительный период времени, и после решения проблем многое придется инсталлировать заново.

Разделы и параметры System Restore хранятся в реестре в трех местах.

Сведения о System Restore в реестре можно найти в следующих разделах:

\* HKEY\_LOCAL\_MACHINE\ SYSTEM\ CurrentControlSet\ Services\ Sr;

\* HKEY\_LOCAL\_MACHINE\ SYSTEM\ CurrentControlSet\ Services\ SrService;

\* HKEY\_LOCAL\_MACHINE\ SOFTWARE\ Microsoft\ Windows. NT\ CurrentVersion\ SystemRestore

Первый раздел отвечает за фильтр System Restore, его параметр менять не следует. Второй раздел управляет службой System Restore, и его тоже лучше не трогать. Если любой из первых двух разделов будет изменен, нормальное функционирование системы, скорее всего, будет нарушено.

В третьем разделе есть параметры, подлежащие изменению. Например, значение параметра DiskPercent можно увеличить, тогда для хранения точек восстановления будет отведено больше места на диске. По умолчанию для них отводится 12% дискового пространства, хотя реально используемый объем может быть иным. Для настройки System Restore через графический интерфейс пользователя необходимо открыть Control Panel, щелкнуть на вкладке System Restore, выбрать жесткий диск из списка доступных, Settings и с помощью ползунка подобрать нужное значение параметра Disk space to use.

Можно также изменить параметр RPGlobalInterval, чтобы указать интервал между моментами автоматического создания точек восстановления. Например, чтобы изменить частоту создания точек восстановления с одного раза в сутки на один раз в неделю, следует значение параметра по умолчанию (86 400 с) поменять на 604 800.

Если из соображений безопасности не хочется долгое время хранить точки восстановления, нужно изменить значение параметра RPLifeInterval. По умолчанию время жизни точки восстановления составляет 7 776 000 с (90 дней).

Пользователю также рекомендуется, не довольствуясь только этим, создавать точки восстановления вручную перед внесением существенных программно-аппаратных модификаций. В случае серьезных сбоев вы затем сможете привести систему в рабочее состояние без потери данных, вернув ее к ранее созданной точке восстановления.

Чтобы не давать пользователям возможности изменять установки System Restore, можно воспользоваться Group Policy Editor (GPE) или редактором реестра для отключения пользовательского интерфейса System Restore.

Если для отключения интерфейса пользователя System Restore применяется редактор реестра, следует открыть раздел HKEY\_LOCAL\_MACHINE\ SOFTWARE\ Policies\ Microsoft\ Windows NT. Необходимо создать новый подраздел с именем SystemRestore и в нем — новый параметр DisableConfig (тип DWORD), которому следует присвоить 1.

Automated System Recovery

Действие функции автоматического восстановления системы (Automated System Recovery, ASR) основано на использовании ASR-дисков. Обычно набор таких дисков создается после установки или обновления ОС. ASR-диски содержат файлы, необходимые для загрузки ОС, - в случае сбоя они позволят вернуть Windows XP Professional к состоянию на момент создания этих дисков. Стандартный мастер ASR Preparation позволяет создать резервную копию системы на носителях высокой емкости -- таких, как диски CD-R/RW, магнитные ленты или жесткие диски; одновременно создаются и ASR-диски. Файлы, размещаемые на них, в числе прочего служат для доступа к созданной резервной копии и возврата системы в предыдущее рабочее состояние. Чтобы восстановить систему с помощью данного механизма, загрузите компьютер, используя заранее созданные диски, и следуйте указаниям системы. Необходимо учесть, что при восстановлении Windows XP Professional с ASR-дисков все изменения в данных и конфигурации, сделанные после создания этих дисков, теряются.

Поскольку механизм ASR - это единственный способ загрузки ОС в случае серьезного сбоя, рекомендуется использовать планировщик задач для автоматического создания дисков восстановления. Это особенно актуально для систем, содержащих критически важные или часто обновляемые данные. Функция Automated System Recovery заменила механизм Emergency Repair Disk (ERD), используемый в предыдущих версиях Windows. ERD сохраняет только системные настройки,ASR создает резервную копию всей системы.

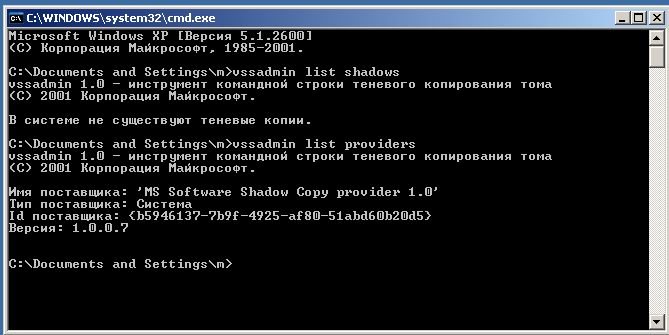
Перечисленные методы необходимо сочетать с другими средствами восстановления данных, такими, как Driver Rollback и загрузочная конфигурация LastKnownGood, - в зависимости от характера и причины сбоя. В таблице ниже перечислены основные причины сбоев и оптимальные методы их устранения.

***Арсенал средств восстановления в Windows XP Professional***

|  |  |
| --- | --- |
| Проблема | Решение |
| После установки или обновления драйвера устройства ОС перестала отвечать на запросы | Используйте конфигурацию LastKnownGood для запуска компьютера. Запретите использование измененного драйвера, перезагрузите компьютер и воспользуйтесь механизмом Driver Rollback |
| После внесения изменений в конфигурацию ОС система перестала отвечать на запросы или возникли серьезные сбои в ее работе | Используйте загрузочную конфигурацию LastKnownGood для отмены сделанных изменений |
| Устройство работает некорректно после установки или обновления его драйвера | Воспользуйтесь механизмом Driver Rollback для восстановления предыдущей версии драйвера |
| Вам необходимо вернуть ОС к предыдущему состоянию без потери информации | Используйте механизм System Restore |
| ОС не загружается даже при использовании конфигурации LastKnownGood | Используйте механизм Automated System Recovery |

***VSSADMIN***

Теневое копирование тома (Volume Shadow Copy) – технология, используемая в операционных системах Windows и позволяющая копировать системные и заблокированные файлы, с которыми в данный момент времени ведется работа. Теневое копирование реализовано с использованием специальной службы VSS (Теневое копирование ) и системных драйверов для получения снимков томов (Volume Snapshot). Основным назначением теневого копирования является создание системных точек восстановления, архивных образов системы, и архивирования пользовательских данных.



Утилита VSSADMIN.EXE предназначена для администрирования в командной строке службы теневого копирования томов.