Федеральное агентство по образованию

Нижегородский Государственный Технический Университет

Кафедра: «Вычислительные системы и технологии»

Операционные системы

**Лабораторная работа №1**

**Механизмы ОС Microsoft Windows**

Выполнил:

Студент группы 14-В-2

Носов А.В.

Проверил:

Кочешков А. А.

Нижний Новгород

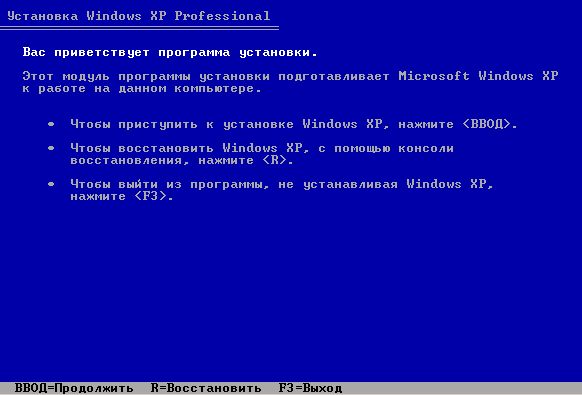
2017

1. **Установка ОС Windows**
2. Анализ совместимости с аппаратным и программным обеспечением



На рисунке выше представлены системные требования Windows XP. Так как мы будем ставить систему на платформу виртуализации VirtualBox, где её поддержка заявлена разработчиками платформы, то проблем с совместимостью быть не должно.

1. Процесс установки ОС

****

* Загрузка с загружаемого компактного диска ОС и программы инсталляции, загрузка минимального набора стандартных драйверов в частности дисковых (если дисковая система не стандартная имеется возможность загрузки драйвера с дискеты от производителя).
* Подготовка дискового пространства (удаление существующего и создание нового раздела, форматирование). Проверка жестких дисков на наличие ошибок.
* Копирование системных файлов.
* Ввод дополнительной информации и региональных параметров (язык, раскладка клавиатуры, форматы чисел и т.д.).
* Ввод параметров: имя, организация, пароль администратора, время, серийный код.
* Копирование системных файлов;
* Выбор режима установки сетевых компонентов (клиент для сетей Microsoft, протокол TCP/IP, планировщик пакетов QoS, служба доступа к файлам и принтерам сетей Microsoft);
* Выбор домена/рабочей группы
* Поиск физических устройств и установка драйверов

**2. Процесс загрузки Windows**

***Предварительная загрузка:***

Компьютер выполняет процедуру POST для определения объема физической памяти, проверки наличия аппаратных компонентов и т. д. Если на компьютере установлена базовая система ввода-вывода (BIOS) Plug and Play, то на этом этапе происходит просмотр и конфигурирование аппаратных устройств.

BIOS компьютера обнаруживает загрузочное устройство, загружает и выполняет главную загрузочную запись (MBR).

Главная загрузочная запись просматривает таблицу разделов в поисках активного раздела, загружает загрузочный сектор активного раздела в память и выполняет его.

Компьютер загружает и инициализирует файл Ntldr — загрузчик ОС.

***Загрузка:***

После загрузки в память файла Ntldr процедура загрузки собирает информацию об аппаратном обеспечении и драйверах. При этом используются файлы Ntldr, Boot.ini, Bootsect.dos (необязательно), Ntdetect.com и Ntoskrnl.exe.

При загрузке NTLDR выполняет следующие шаги:

1. Переводит процессор в [«плоский»](http://ru.wikipedia.org/w/index.php?title=Unreal_mode&action=edit&redlink=1) 32-битный режим работы (32-bit flat memory mode);
2. Организует доступ к текущей файловой системе ([FAT](http://ru.wikipedia.org/wiki/FAT) или [NTFS](http://ru.wikipedia.org/wiki/NTFS));
3. Если присутствует файл *hiberfil.sys* и загрузчик обнаруживает образ «спящего» режима, содержимое образа загружается в оперативную память и система восстанавливается в предыдущее состояние.
4. В противном случае, он читает файл [*boot.ini*](http://ru.wikipedia.org/wiki/Boot.ini) и выводит пользователю соответствующее меню для выбора запускаемой ОС:
   * если была выбрана не-NT система (например [Windows 98](http://ru.wikipedia.org/wiki/Windows_98)), тогда он загружает файл, указанный в [*boot.ini*](http://ru.wikipedia.org/wiki/Boot.ini) (*bootsect.dos*, если не указан иной файл, являющийся полноценной [загрузочной записью](http://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%BE%D1%87%D0%BD%D1%8B%D0%B9_%D1%81%D0%B5%D0%BA%D1%82%D0%BE%D1%80)), и управление передаётся этому файлу, либо он загружает операционную систему на базе DOS.
   * если же была выбрана система на базе Windows NT, то запускается программа *ntdetect.com*, которая собирает информацию о составе оборудования.
5. Запускает файл [*Ntoskrnl.exe*](http://ru.wikipedia.org/wiki/Ntoskrnl.exe) (ядро операционной системы), передавая ему собранную информацию о составе оборудования затем передаётся в , *ntoskrnl.exe*, и происходит запуск операционной системы.

В компьютерах с Процессором Intel поиск оборудования осуществляют файлы Ntdetect.com и Ntoskrnl.exe. Программа Ntdetect.com запускается, если на этапе выбора ОС выбрана система Windows XP (или по окончании времени ожидания). Если вы выбрали ОС, отличную от Windows XP, например, Windows 98, Ntldr загружает и выполняет файл Bootsect.dos, в котором содержится копия загрузочного сектора, находившегося в системном разделе до установки Windows 2000. Передача управления файлу Bootsect.dos означает начало загрузки выбранной ОС.

Ntdetect.com формирует список установленных аппаратных компонентов и передает его в Ntldr для включения в реестр в ключе HKEY\_LOCAL\_MACHINE\HARDWARE.

Ntdetect.com определяет:

тип шины/адаптера;

коммуникационные порты;

математический сопроцессор;

дисководы для гибких дисков;

клавиатуру;

мышь или другое указательное устройство;

параллельные порты;

адаптеры SCSI;

видеоадаптеры.

***Загрузка ядра:***

После выбора конфигурации загружается и инициализируется ядро Windows XP (Ntoskrnl.exe). Файл Ntoskrnl.exe также загружает и инициализирует драйверы устройств и загружает службы.

На этапе загрузки ядра Ntldr выполняет следующие действия:

- Загружает файл Ntoskrnl.exe (но не инициализирует его).  
    - Загружает файл слоя абстрагирования от оборудования(Hardware Abstraction Layer, HAL) Hal.dll.  
    - Загружает ключ реестра HKEY\_LOCAL\_MACHINE\SYSTEM из каталога systemroot\System32\Config\System.  
    - Выбирает управляющий набор(control set), который будет использоваться для инициализации компьютера. Управляющий набор содержит данные о конфигурации, необходимые для управления системой, например, список драйверов устройств и служб, которые необходимо загрузить и запустить.  
    - Загружает драйверы устройств, у которых значение параметра Start равно 0x0. Обычно это драйверы низкого уровня, например, необходимые для работы жесткого диска. Параметр List из подраздела реестра HKEY\_LOCAL\_MACHINE\ SYSTEM\ CurrentControlSet\ Control\ ServiceGroupOrder задает порядок их загрузки.

***Инициализация ядра.***

По завершении загрузки ядро инициализируется, затем ему передается управление. В этот момент система отображает графический экран, в строке состояния которого можно увидеть ход загрузки. На этапе инициализации ядра выполняются действия:

- Создается раздел Hardware.  
- Создается управляющий набор Clone.

- Загружаются и инициализируются драйверы устройств.

- Запускаются службы.

***Boot.ini***

NTLDR позволяет пользователю выбрать желаемую операционную систему для запуска из обычного меню; также, для операционных систем Windows NT и более поздних, могут быть указаны дополнительные опции загрузки ядра. Все эти настройки хранятся в файле [*boot.ini*](http://ru.wikipedia.org/wiki/Boot.ini), который должен находиться в корне того же логического диска, что и *NTLDR*.

[boot loader]

timeout=30

default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

[operating systems]

multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional RU" /noexecute=optin /fastdetect /bootlog

***Протокол загрузки:***

Service Pack 3 3 31 2017 22:17:31.500

Loaded driver \WINDOWS\system32\ntoskrnl.exe

Loaded driver \WINDOWS\system32\hal.dll

Loaded driver \WINDOWS\system32\KDCOM.DLL

Loaded driver \WINDOWS\system32\BOOTVID.dll

Loaded driver ACPI.sys

Loaded driver \WINDOWS\system32\DRIVERS\WMILIB.SYS

Loaded driver pci.sys

Loaded driver isapnp.sys

Loaded driver compbatt.sys

Loaded driver \WINDOWS\system32\DRIVERS\BATTC.SYS

Loaded driver intelide.sys

Loaded driver \WINDOWS\system32\DRIVERS\PCIIDEX.SYS

Loaded driver MountMgr.sys

Loaded driver ftdisk.sys

Loaded driver dmload.sys

Loaded driver dmio.sys

Loaded driver PartMgr.sys

Loaded driver VolSnap.sys

Loaded driver atapi.sys

Loaded driver disk.sys

Loaded driver \WINDOWS\system32\DRIVERS\CLASSPNP.SYS

Loaded driver fltMgr.sys

Loaded driver sr.sys

Loaded driver KSecDD.sys

Loaded driver Ntfs.sys

Loaded driver NDIS.sys

Loaded driver Mup.sys

Loaded driver \SystemRoot\system32\DRIVERS\i8042prt.sys

Loaded driver \SystemRoot\system32\DRIVERS\kbdclass.sys

Loaded driver \SystemRoot\system32\DRIVERS\fdc.sys

Loaded driver \SystemRoot\system32\DRIVERS\mouclass.sys

Loaded driver \SystemRoot\system32\DRIVERS\parport.sys

Loaded driver \SystemRoot\system32\DRIVERS\cdrom.sys

Loaded driver \SystemRoot\system32\DRIVERS\pcntpci5.sys

Loaded driver \SystemRoot\system32\DRIVERS\CmBatt.sys

Loaded driver \SystemRoot\system32\DRIVERS\audstub.sys

Loaded driver \SystemRoot\system32\DRIVERS\rasl2tp.sys

Loaded driver \SystemRoot\system32\DRIVERS\ndistapi.sys

Loaded driver \SystemRoot\system32\DRIVERS\ndiswan.sys

Loaded driver \SystemRoot\system32\DRIVERS\raspppoe.sys

Loaded driver \SystemRoot\system32\DRIVERS\raspptp.sys

Loaded driver \SystemRoot\system32\DRIVERS\msgpc.sys

Loaded driver \SystemRoot\system32\DRIVERS\psched.sys

Loaded driver \SystemRoot\system32\DRIVERS\ptilink.sys

Loaded driver \SystemRoot\system32\DRIVERS\raspti.sys

Loaded driver \SystemRoot\system32\DRIVERS\rdpdr.sys

Loaded driver \SystemRoot\system32\DRIVERS\termdd.sys

Loaded driver \SystemRoot\system32\DRIVERS\swenum.sys

Loaded driver \SystemRoot\system32\DRIVERS\update.sys

Loaded driver \SystemRoot\system32\DRIVERS\mssmbios.sys

Loaded driver \SystemRoot\System32\Drivers\NDProxy.SYS

Did not load driver \SystemRoot\System32\Drivers\NDProxy.SYS

Loaded driver \SystemRoot\system32\DRIVERS\flpydisk.sys

Did not load driver \SystemRoot\System32\Drivers\lbrtfdc.SYS

Did not load driver \SystemRoot\System32\Drivers\Sfloppy.SYS

Did not load driver \SystemRoot\System32\Drivers\i2omgmt.SYS

Did not load driver \SystemRoot\System32\Drivers\Changer.SYS

Did not load driver \SystemRoot\System32\Drivers\Cdaudio.SYS

Loaded driver \SystemRoot\System32\Drivers\Fs\_Rec.SYS

Loaded driver \SystemRoot\System32\Drivers\Null.SYS

Loaded driver \SystemRoot\System32\Drivers\Beep.SYS

Loaded driver \SystemRoot\System32\drivers\vga.sys

Loaded driver \SystemRoot\System32\Drivers\mnmdd.SYS

Loaded driver \SystemRoot\System32\DRIVERS\RDPCDD.sys

Loaded driver \SystemRoot\System32\Drivers\Msfs.SYS

Loaded driver \SystemRoot\System32\Drivers\Npfs.SYS

Loaded driver \SystemRoot\system32\DRIVERS\rasacd.sys

Loaded driver \SystemRoot\system32\DRIVERS\ipsec.sys

Loaded driver \SystemRoot\system32\DRIVERS\tcpip.sys

Loaded driver \SystemRoot\system32\DRIVERS\netbt.sys

Loaded driver \SystemRoot\System32\drivers\afd.sys

Loaded driver \SystemRoot\system32\DRIVERS\netbios.sys

Did not load driver \SystemRoot\System32\Drivers\PCIDump.SYS

Did not load driver \SystemRoot\system32\DRIVERS\redbook.sys

Loaded driver \SystemRoot\system32\DRIVERS\rdbss.sys

Loaded driver \SystemRoot\system32\DRIVERS\mrxsmb.sys

Did not load driver \SystemRoot\system32\DRIVERS\imapi.sys

Loaded driver \SystemRoot\System32\Drivers\Fips.SYS

Loaded driver \SystemRoot\system32\DRIVERS\ipnat.sys

Loaded driver \SystemRoot\System32\Drivers\Cdfs.SYS

Loaded driver \SystemRoot\system32\DRIVERS\wanarp.sys

Loaded driver \SystemRoot\system32\DRIVERS\ndisuio.sys

Did not load driver \SystemRoot\system32\DRIVERS\rdbss.sys

Did not load driver \SystemRoot\system32\DRIVERS\mrxsmb.sys

Loaded driver \SystemRoot\System32\Drivers\Fastfat.SYS

Loaded driver \SystemRoot\system32\DRIVERS\mrxdav.sys

Loaded driver \SystemRoot\System32\Drivers\ParVdm.SYS

Did not load driver \SystemRoot\System32\Drivers\Serial.SYS

Loaded driver \SystemRoot\system32\DRIVERS\srv.sys

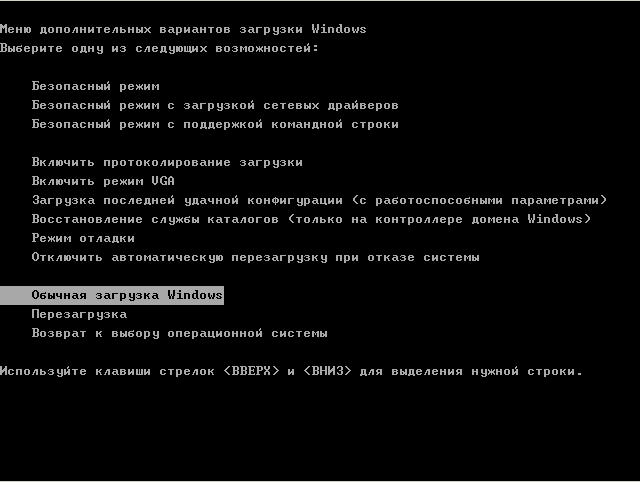
Did not load driver \SystemRoot\system32\DRIVERS\ipnat.sys

Loaded driver \SystemRoot\System32\Drivers\HTTP.sys

***Основные файловые компоненты необходимые для начальной загрузки:***

|  |  |  |
| --- | --- | --- |
| **Файл** | **Расположение** | **Описание** |
| Ntldr | \ | загрузчик для операционных систем Windows NT |
| Boot.ini | \ | файл конфигурации загружаемых ОС |
| Bootsect.dos | \ | необходим для загрузки MS-DOS или другой операционной системы (не NT) |
| Ntdetect.com | \ | выполняет выбор аппаратного профиля |
| Ntbootdd.sys | \ | Необходим для загрузки со SCSI-диска |
| Ntoskrnl.exe | *systemroot\Sysiem32* | файл ядра операционной системы |
| Hal.dll | *systemroot\Sysiem32* | слой аппаратных абстракций |

**3. Стартовое меню**



Для вызова стартового меню, необходимо на этапе загрузки нажать клавишу F8.

***Безопасный режим*** (SAFEBOOT\_OPTION=Minimal). Это особый режим запуска операционной системы Windows. Он предназначен для выявления и устранения ошибок и неполадок как запуска, так и основной работы операционной системы. В режиме Safe Mode можно воспользоваться ограниченным набором команд, служб и компонентов. При загрузки Windows в безопасном режиме загружаются только базовые компоненты файлы и драйвера, которые нужны для старта Windows.

***Безопасный режим с загрузкой сетевых драйверов*** (SAFEBOOT\_OPTION=Network). Для запуска Windows используется минимальный набор драйверов устройств и служб плюс драйверы для поддержки работы в сети.

***Безопасный режим с поддержкой командной строки*** (SAFEBOOT\_OPTION=Minimal(AlternateShell)). Аналогично безопасному режиму, только вместо проводника Windows запускается файл Cmd.exe.

***Включить протоколирование загрузки***. При выборе одного из вариантов безопасной загрузки (кроме «Загрузка последней удачной конфигурации») включается протоколирование загрузки. Для хранения результатов протоколирования используется файл Ntbtlog.txt из папки %SystemRoot%.

***Включить режим VGA***. Windows запускается с помощью текущего видео драйвера (а не Vga.sys) в режиме 640 x 480. Этот режим используется, когда выбрана конфигурация, которая не поддерживается монитором. В безопасном режиме и безопасном режиме с загрузкой сетевых драйверов загружается драйвер Vga.sys.

***Загрузка последней удачной конфигурации.*** Загружается последняя удачная конфигурация Windows.

Управляющий набор содержит конфигурационные данные, используемые для управления системой, например, список драйверов устройств и служб, которые необходимо загрузить и запустить. Управляющие наборы хранятся как подразделы раздела реестра HKEY\_LOCAL\_MACHINE\SYSТЕМ.

|  |  |
| --- | --- |
| *Default* | Содержит информацию, которую система сохраняет при выключении компьютера. |
| *LastKnownGood* | Содержит информацию, которую система сохраняет при успешной загрузке компьютера. Загружается только в случае восстановления системы после серьезной или критической ошибки загрузки драйвера устройства или если выбрана в процессе загрузки. |

***Восстановление службы каталогов***. Этот режим может быть использован только на контроллерах домена Windows. С его помощью производится восстановление службы каталогов. *Контроллер домена -* сервер в сети Active Directory, управляющий входом пользователей и доступом к сетевым и общим ресурсам.

***Режим отладки***. В Windows включается режим отладки. Отладочная информация может быть послана по последовательному кабелю на другой компьютер с запущенным отладчиком. В этом режиме используется порт СОМ2.

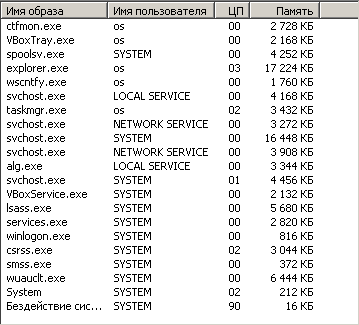
***Обычная загрузка Windows***. Windows запускается в обычном режиме.

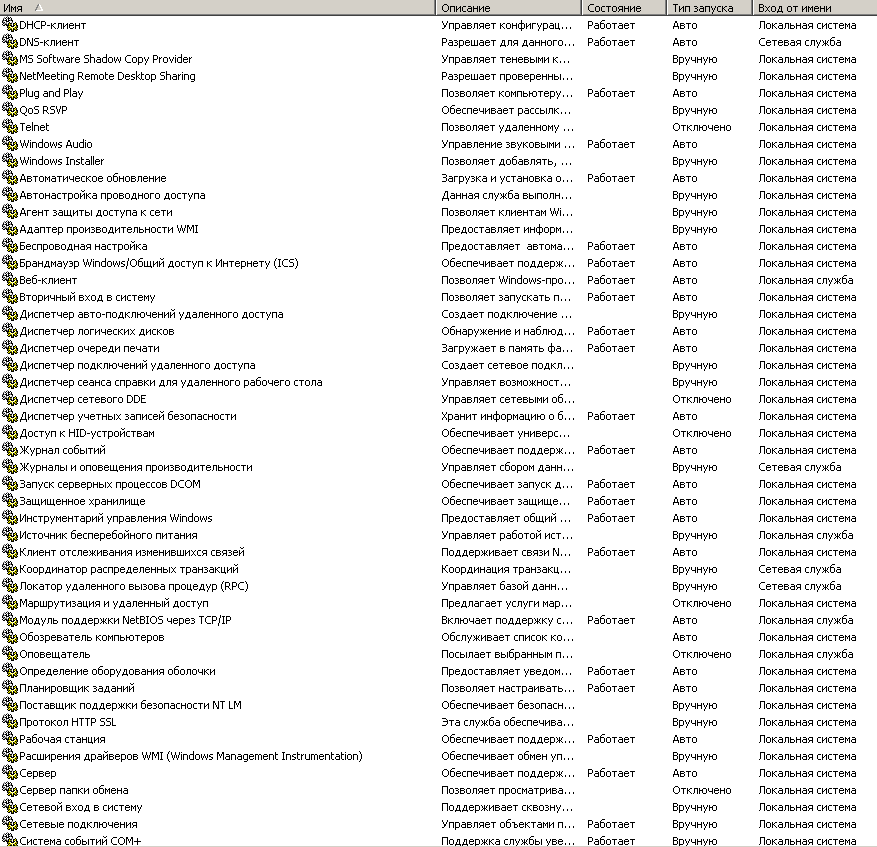
***Перезагрузка***. Выполняется перезагрузка компьютера.

***Возврат к выбору операционной системы***. На компьютере, настроенном для запуска нескольких операционных систем, происходит возврат к меню загрузки.

При выборе одного из вариантов безопасной загрузки устанавливается переменная окружения SAFEBOOT\_OPTION. Ей присваивается значение Network или Minimal.

***Обычная загрузка Windows:***





***Безопасный режим:***

1. Драйвера, запускаемые в безопасном режиме:

* драйвер дисководов гибких дисков при его наличии в системе;
* драйвер контролеров ATA, SATA или SCSI для подключения жестких дисков и дисководов компакт-дисков (CD, DVD);
* драйвер контроллеров USB, PS/2 и последовательного порта;
* видеодрайвер VGA (PCI, AGP).

Это минимальный набор драйверов, который необходим для запуска WIndows.

1. Локальные службы, запускаемые в безопасном режиме:

* Журнал событий Windows- позволяет просматривать и записывать события операционной системы. В безопасном режиме можно просмотреть события, которые привели к возникновению ошибок и сбоев Windows;
* Поддержка самонастраивающихся устройств – позволяет использовать устройства, подключенные к компьютеру, которые не требуют установки драйверов;
* Удаленный вызов процедур (RPC) – Обеспечивает правильную работу COM приложений;  
  Службы криптографии – служба проверки подписи файлов и приложений;
* Защитник Windows – служба защиты операционной системы;
* Инструментарий управления Windows (WMI) – позволяют использовать приложения и сервисы Windows для настройки операционной системы.

1. Сетевые сервисы и службы, которые доступны в безопасном режиме:

* Поддержка сетевых адаптеров и устройств, необходимых для проводного и беспроводного подключения к локальной сети;
* DHCP-клиент – служба, обеспечивающая получение и изменение IP-адреса, а также обновления DNS;
* DNS-клиент – служба, необходимая для регистрации имени компьютера в сети;
* Сетевые подключения – служба, необходимая для работы сервисов удаленный доступ и настройки локальной сети и сетевых подключений;
* Модуль поддержки NetBIOS через TCP/IP – Служба, позволяющая организовать общий доступ к папкам и принтерам компьютера, находящегося в локальной сети;
* Брандмауэр Windows – сетевой экран Windows, обеспечивающий безопасность и защиту от проникновения на компьютер с локальной сети.

Loaded driver \WINDOWS\system32\ntoskrnl.exe

Loaded driver \WINDOWS\system32\hal.dll

Loaded driver \WINDOWS\system32\KDCOM.DLL

Loaded driver \WINDOWS\system32\BOOTVID.dll

Loaded driver ACPI.sys

Loaded driver \WINDOWS\system32\DRIVERS\WMILIB.SYS

Loaded driver pci.sys

Loaded driver isapnp.sys

Loaded driver compbatt.sys

Loaded driver \WINDOWS\system32\DRIVERS\BATTC.SYS

Loaded driver intelide.sys

Loaded driver \WINDOWS\system32\DRIVERS\PCIIDEX.SYS

Loaded driver MountMgr.sys

Loaded driver ftdisk.sys

Loaded driver dmload.sys

Loaded driver dmio.sys

Loaded driver PartMgr.sys

Loaded driver VolSnap.sys

Loaded driver atapi.sys

Loaded driver disk.sys

Loaded driver \WINDOWS\system32\DRIVERS\CLASSPNP.SYS

Loaded driver fltMgr.sys

Loaded driver sr.sys

Loaded driver KSecDD.sys

Loaded driver VBoxGuest.sys

Loaded driver Ntfs.sys

Loaded driver NDIS.sys

Loaded driver Mup.sys

Did not load driver Компьютер с ACPI

Did not load driver Аудио кодеки

Did not load driver Драйверы аудио (без PnP)

Did not load driver Устройство управления

Did not load driver Устройства записи видео (без PnP)

Did not load driver Видео кодеки

Did not load driver Минипорт WAN (L2TP)

Did not load driver Минипорт WAN (IP)

Did not load driver Минипорт WAN (PPPoE)

Did not load driver Минипорт WAN (PPTP)

Did not load driver Минипорт планировщика пакетов

Did not load driver Прямой параллельный порт

Did not load driver VirtualBox Graphics Adapter

Did not load driver AMD PCNET семейство PCI Ethernet адаптеров

Did not load driver Батарея с ACPI-совместимым управлением Microsoft

Did not load driver Адаптер блока питания (Майкрософт)

Did not load driver Порт принтера

Did not load driver Прямой параллельный порт

Loaded driver \SystemRoot\system32\DRIVERS\i8042prt.sys

Loaded driver \SystemRoot\system32\DRIVERS\kbdclass.sys

Loaded driver \SystemRoot\system32\DRIVERS\fdc.sys

Loaded driver \SystemRoot\system32\DRIVERS\VBoxMouse.sys

Loaded driver \SystemRoot\system32\DRIVERS\mouclass.sys

Loaded driver \SystemRoot\system32\DRIVERS\cdrom.sys

Did not load driver VirtualBox Graphics Adapter

Loaded driver \SystemRoot\system32\DRIVERS\usbohci.sys

Loaded driver \SystemRoot\system32\DRIVERS\usbehci.sys

Loaded driver \SystemRoot\system32\DRIVERS\rdpdr.sys

Loaded driver \SystemRoot\system32\DRIVERS\termdd.sys

Loaded driver \SystemRoot\system32\DRIVERS\swenum.sys

Loaded driver \SystemRoot\system32\DRIVERS\update.sys

Loaded driver \SystemRoot\system32\DRIVERS\mssmbios.sys

Loaded driver \SystemRoot\system32\DRIVERS\flpydisk.sys

Loaded driver \SystemRoot\system32\DRIVERS\usbhub.sys

Did not load driver \SystemRoot\System32\Drivers\lbrtfdc.SYS

Did not load driver \SystemRoot\System32\Drivers\Sfloppy.SYS

Did not load driver \SystemRoot\System32\Drivers\i2omgmt.SYS

Did not load driver \SystemRoot\System32\Drivers\Changer.SYS

Did not load driver \SystemRoot\System32\Drivers\Cdaudio.SYS

Loaded driver \SystemRoot\System32\Drivers\Fs\_Rec.SYS

Loaded driver \SystemRoot\System32\Drivers\Null.SYS

Loaded driver \SystemRoot\System32\Drivers\Beep.SYS

Loaded driver \SystemRoot\System32\drivers\vga.sys

Did not load driver mnmdd.SYS

Did not load driver RDPCDD.SYS

Loaded driver \SystemRoot\System32\Drivers\Msfs.SYS

Loaded driver \SystemRoot\System32\Drivers\Npfs.SYS

Did not load driver RasAcd.SYS

Did not load driver IPSec.SYS

Did not load driver Tcpip.SYS

Did not load driver NetBT.SYS

Did not load driver AFD.SYS

Did not load driver NetBIOS.SYS

Did not load driver VBoxSF.SYS

Did not load driver \SystemRoot\System32\Drivers\PCIDump.SYS

Did not load driver WS2IFSL.SYS

Did not load driver \SystemRoot\system32\DRIVERS\redbook.sys

Did not load driver Rdbss.SYS

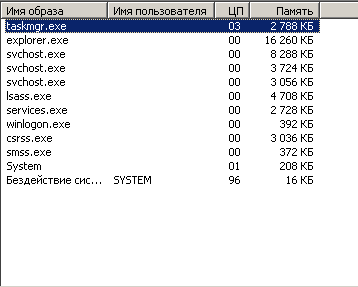
Did not load driver MRxSmb.SYS

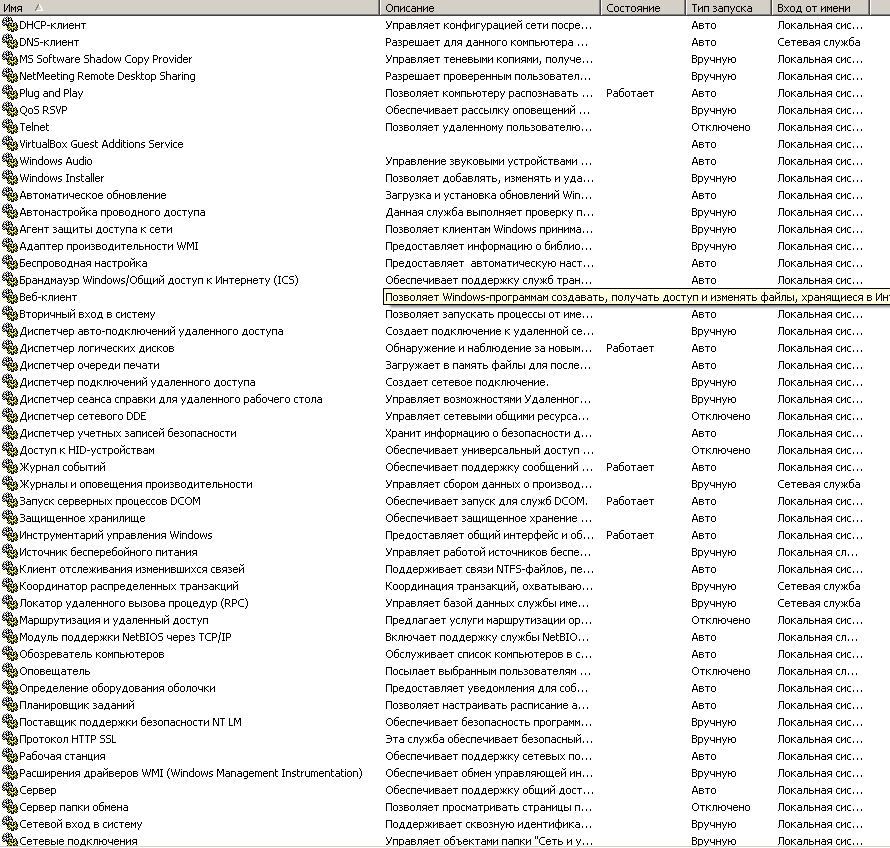
Did not load driver \SystemRoot\system32\DRIVERS\imapi.sys

Did not load driver Fips.SYS

Loaded driver \SystemRoot\System32\Drivers\Cdfs.SYS

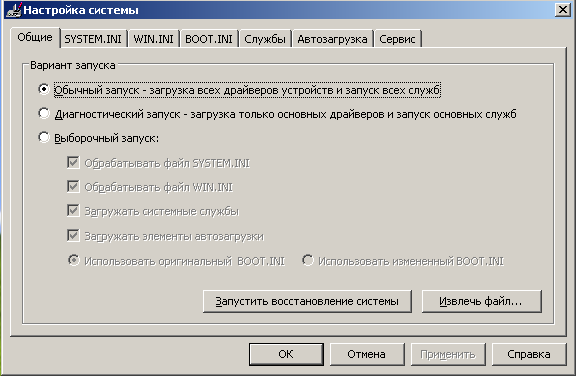
Loaded driver \SystemRoot\System32\Drivers\Fastfat.SYS





***MSConfig***

Это утилита для управления авто запускаемыми программами и загрузкой Windows. Начиная с Windows версии 98, Microsoft поставляет утилиту «MSConfig.exe», предоставляющую удобный интерфейс для управления файлами, запускающимися при загрузке Windows. Она находится в каталоге установки Windows. Её можно запустить из диалогового окна «Выполнить» или через командную строку. В ней нет возможности добавлять новый элемент с именем приложения или документа для автозапуска, но можно отключать, не удаляя, любой пункт из находящихся в списках.



***Описание возможностей программы***

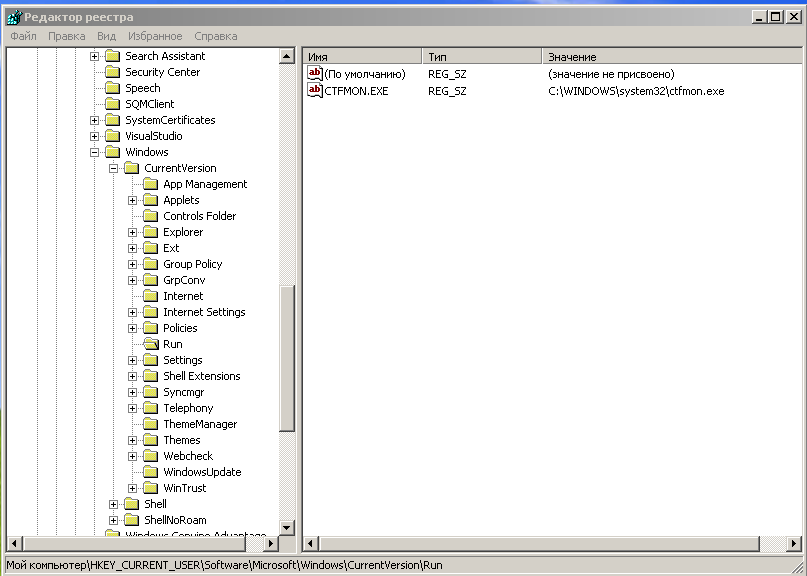
* На вкладке «Общие» возможно выбирать вариант загрузки: обычный, диагностический или выборочный.
* На вкладке SYSTEM.INI Вы можете отредактировать службы и драйверы, загружаемые из одноимённого файла.
* На следующей вкладке WIN.INI Вы можете отключить те или иные программы или службы, загружаемые через этот конфигурационный файл.
* На вкладке Службы можно отключить ненужные службы, запускаемые при загрузке системы. Многие программы, такие как антивирусы и программы безопасности компьютера, запускаются через службы операционной системы. В случае отключения служб такие программы могут перестать работать.
* Вкладка Автозагрузка отвечает за загрузку приложений (программ) а также определённых служебных утилит, загружаемых не через службы.

Для того, чтобы вы знали, какая программа откуда запускается, вкладка Автозагрузка разбита на три колонки. В левой колонке находится элемент (программа), рядом с которой стоит галочка (или квадратик пустой, что означает, что эта программа не загружается вместе с системой). В средней колонке находится путь, указывающий откуда (из какой папки) загружается та или иная программа. В правой колонке указывается каким образом (каким ключом реестра) запускается та или иная программа.

***Пути в реестре***

Все настройки программы хранятся в реестре по пути **HKLM\SOFTWARE\Microsoft\Shared Tools\MSConfig**.

Ключи, отвечающие за автозагрузку:



* **[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Run]** - программы, которые запускаются при входе в систему. Данный раздел отвечает за запуск программ для всех пользователей системы.
* **[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\RunOnce]** - программы, которые запускаются только один раз при входе пользователя в систему. После этого ключи программ автоматически удаляются из данного раздела реестра. Данный раздел отвечает за запуск программ для всех пользователей системы.
* **[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\RunOnceEx]** - программы, которые запускаются только один раз, когда загружается система. Этот раздел используется при инсталляции программ, например для запуска настроечных модулей. После этого ключи программ автоматически удаляются из данного раздела реестра. Данный раздел отвечает за запуск программ для всех пользователей системы.
* **[HKEY\_CURRENT\_USER\Software\Microsoft\ Windows\CurrentVersion\Run]**- программы, которые запускаются при входе текущего пользователя в систему
* **[HKEY\_CURRENT\_USER\Software\ Microsoft\Windows\CurrentVersion\RunOnce]** - программы, которые запускаются только один раз при входе текущего пользователя в систему. После этого ключи программ автоматически удаляются из данного раздела реестра.
* **[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\RunServices]** - программы, которые загружаются при старте системы до входа пользователя в Windows.
* **[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\RunServicesOnce]** - программы отсюда загружаются только один раз, когда загружается система.

**4. Архитектура Windows. Состав и функции основных компонентов**

менеджер объектов

NT Executive

Кольцо 0 (режим операционной системы)

(режим ядра)

Кольцо 3 (режим пользователя)

Защищ. подсист. среды

DOS-appl.

Win16-appl.

Win32-appl.

OS/2-appl.

POSIX-appl.

Win32

OS/2

POSIX

сист. службы

службы сервера

служба раб. станции

Безопасность

Active Directory

системный интерфейс (NTDLL.DLL)

Защищ.

интегрир.

подсис.

(серверы)

мен. IPC

мен. вирт. памяти

мен. процессов

мен. PnP

монит. безоп.

мен. упр. пит.

GDI + др. гр. устр.

п/с в/в

файл. сист.

мен. кэша

драйверы устр-в

микроядро (ntoskrnl.dll)

HAL (уровень абстракций оборудования)

Аппаратная часть

***Пользовательские процессы:***

Фиксированные процессы поддержки системы, например, диспетчер сеансов. Необходимы для нормальной работы системы. Имеют доступ напрямую к некоторым сервисам ОС, т.е. являются привилегированными процессами.

Процессы сервисов (сервисы Win32). Иначе называются службами. Пример — Планировщик задач. Работают в фоновом режиме, без интерактивного взаимодействия с пользователем.

Пользовательские приложения. Бывают пяти видов: Win32, Windows 3.1, MS-DOS, POSIX и OS/2.

Подсистемы окружения. Образуют окружение операционной среды, предоставляя сервисы ОС. Существует 3 подсистемы: Win32, POSIX и OS/2.

Процессы пользовательского режима не могут вызывать сервисы ядра ОС напрямую, вместо этого они используют DLL соответствующих подсистем окружения.

***Компоненты режима ядра:***

Исполнительная система. Содержит базовые сервисы ОС (управление памятью, процессами и потоками, защиту, ввод/вывод и взаимодействие между процессами).

Ядро — низкоуровневые функции ОС (планирование потоков, диспетчеризация прерываний и исключений и т.д.). Предоставляет набор процедур и базовых объектов исполнительной системе для реализации более сложных структур.

Драйверы устройств. Драйверы как аппаратных устройств, транслирующих стандартные запросы программ в специфичные запросы ввода/вывода к конкретному оборудованию, так и сетевые драйверы и драйверы файловых систем, службы операционных систем, обеспечивают выполнение различных запросов и приложений ОС, а также поддержку Plug and Play-технологии, DirectX.

Уровень абстрагирования от оборудования. Изолирует другие компоненты режима ядра от специфики оборудования данной платформы.

Подсистема поддержки окон и графики. Реализует функции графического интерфейса пользователя (GUI). Обеспечивает поддержку окон, элементов управления пользовательского интерфейса и отрисовку графики.

Диспетчер виртуальных машин (VMM). Управляет работой приложений. Его функции: подкачка страниц, роль планировщика (планирование процессов, управление памятью, динамическая загрузка VxD), DPMI-сервер (интерфейс защищенного режима для DOS-программ), диспетчер VDM.

***Основные компоненты ядра:***

Микроядро (Microkernel) - компактный код, можно сказать, сердце системы. В рамках микроядра работают ключевые службы: диспетчер памяти, диспетчер задач и другие.[1]Слой абстрагирования (Hardware Abstraction Layer, HAL). Полностью абстрагирует код системы от конкретного аппаратного оборудования. Использование HAL позволяет обеспечить переносимость 99% кода системы между различным оборудованием.

Диспетчер Ввода/Вывода (Input/Output Manager). Полностью контролирует потоки обмена между системой и устройствами. Драйверы устройств работают в контексте I/O Manager. Если драйвер написан с ошибками и может привести к сбою - это вызовет фатальный крах ядра и всей системы. 70% случаев фатальных сбоев ("синий экран") - есть результат некорректного поведения драйверов устройств.

Windows XP содержит встроенный механизм контроля драйверов: правильно написанный и тщательно протестированный драйвер поставляется с цифровой подписью (Driver Signing). Правильная настройка системы заключается в запрещении установки драйверов без корректной подписи.

Модуль управления объектами (Object Manager), управления виртуальной памятью (Virtual Memory Manager), управления процессами (Process Manager), управления безопасностью (Security Reference Monitor), управления локальными вызовами (Local Procedure Calls Facilities) - важные компоненты ядра системы подробно рассматриваться не будут.

Наконец, особое по значению и важности место в ядре системы занимает модуль графического интерфейса - Win32k.sys. Фактически - это часть подсистемы Win32, отвечающая за прорисовку и управление графическим интерфейсом.

***Динамически загружаемые модули*:**

Встроенные функции операционной системы Windows XP находятся в DLL – динамически загружаемых модулях. Модули DLL – это разделяемые библиотеки процедур, к которым по мере необходимости обращаются исполняемые программы.

Основой кода Windows XP, выполняемого в третьем кольце защиты процессора, служат модули Kernel, User и GDI. Каждый из них состоит из 2-х частей – 32-разрядной и 16-разрядной.

Имя файла 32-разрядного модуля Kernel – KERNEL32.DLL.16-разрядная часть Kernel, KRNL386.EXE, задействуется только на момент загрузки Windows и используется только для инициализации 32-разрядной части Kernel, а сам KERNEL32.DLL никогда не обращается к KRNL386.EXE. Модуль ядра операционной системы (krnl386.exe и kernel32.dll) обеспечивает базовые функциональные возможности операционной системы: поддержку файлового ввода/выводы, управление виртуальной памятью и планирование задач. Модуль krnl386.exe инициализирует в процессе загрузки 32-разрядную часть kernel.dll.Kernel отвечает за выделение виртуальной памяти, разрешение импорт-ссылок и выполняет поддержку подкачки страниц по запросу. При выполнении программы модуль отвечает за исполнение потоков каждого процесса и распределение между ними процессорного времени. Обработка исключений - еще одна функция ядра. Также kernel обеспечивает взаимодействие 16-разрядного и 32-разрядного кодов, применяя для преобразования 16-разрядного формата в 32-разрядный специальный процесс - трансформацию.

*GDI (Graphic Device Interface)* - интерфейс графического устройства. Это - графическая система, управляющая процессами отображения всех объектов Windows на экране и поддерживающая графический вывод на принтеры и другие устройства. Она отвечает за прорисовку графических примитивов, манипуляции растровыми изображениями и взаимодействие с аппаратно-независимыми графическими драйверами. Для реализации работы системы разработана 32-разрядная графическая машина - DIB-машина (Device Independent Bitmaps, аппаратно-независимая растровая графика). Она содержит набор оптимизированных универсальных графических функций для работы с графическими устройствами.

Модуль User управляет пользовательским вводом-выводом. Модуль user обслуживает события, генерируемые пользователем: управляет вводом с клавиатуры, от мыши и других координатных устройств, а также вводом через интерфейс пользователя (окнами, значками, меню и др.), также управляет взаимодействием со звуковыми драйверами, таймером и коммуникационными портами. Кроме того, выполняет операции асинхронного ввода для любого ввода в систему и приложения. Основные функции выполняет модуль user.exe. Модуль user32.dll выполняет переадресацию вызовов 16-разрядному модулю.

***Диспетчер конфигурации:***

Управляет конфигурированием системы, используется для поддержки функциональных возможностей технологии plug-and-play. В процессе конфигурирования могут участвовать множество шин различных архитектур и устройств. Диспетчер конфигурации вызывает драйверы, ответственные за создание дерева устройств. Дерево устройств - иерархическое представление всех шин и устройств в компьютере. Каждая шина и устройство рассматриваются как узел. В процессе перечисления устройств отыскивается и собирается информация от драйверов устройств или от BIOS. Для каждого устройства загружается драйвер. По окончании процессов конфигурирования системы Диспетчер конфигурации информирует драйверы устройств о конфигурации соответствующих устройств. Этот процесс повторяется, когда BIOS обнаруживает в системе новое устройство.

***Диспетчер виртуальной машины:***

Работу диспетчера обеспечивает файл vmm32.vxd. Выделяет ресурсы каждому приложению и системному процессу, выполняемому на компьютере. Создает и поддерживает виртуальную среду, в которой исполняются программы и системные процессы.

Виртуальная машина - среда в оперативной памяти ПК, которая кажется приложению отдельным компьютером - с теми же ресурсами, что и у физического компьютера.

В Windows создается одна виртуальная машина (ВМ) (системная) в которой используются все системные процессы, Win-16 и Win-32 приложения, и по отдельной виртуальной машине для каждой программы.

*Основные функции ДВМ:*

1) распределение процессорного времени;   
 2) подкачка страниц памяти;   
 3) поддержка режима MS-DOS для программ DOS.

За выделение системных ресурсов приложениям и другим выполняемым на компьютере процессам, а также за распределение процессорного времени отвечает планировщик.

***Основные системные файлы и каталоги:***

***Для нормальной загрузки ОС Windows XP требуются следующие файлы:***

*NTDLR* - находится в корневом каталоге загрузочного диска.

NTLDR (аббревиатура от NT Loader) является загрузчиком для операционных систем Windows NT и более поздних (2000/XP/Server 2003, за исключением Vista). NTLDR может быть запущен как с переносного устройства (такого как, например, CD-ROM или флэш-накопителя USB), так и с жесткого диска. NTLDR также способен загружать операционные системы, не основанные на технологии NT, путём задания соответствующего загрузочного сектора в отдельном файле. Для запуска NTLDR требуется, как минимум, наличие следующих двух файлов на активном разделе: NTLDR, который собственно и содержит код загрузчика, и boot.ini, в котором записаны команды для формирования меню выбора системы и параметры для её запуска. Чтобы загружать операционные системы на базе Windows NT, необходимо также наличие ntdetect.com.

При загрузке NTLDR выполняет следующие шаги:

Переводит процессор в 32-битный режим работы (32-bit flat memory mode);

Организует доступ к текущей файловой системе (FAT или NTFS);

Читает файл boot.ini и выводит пользователю соответствующее меню для выбора запускаемой ОС:

если была выбрана не-NT система (например Windows 98), тогда загружается файл bootsect.dos, являющийся полноценной загрузочной записью, и управление передаётся ему. Если же была выбрана система на базе Windows NT, то запускается программа ntdetect.com, которая собирает информацию о составе оборудования. Эта информация затем передаётся в ядро операционной системы, ntoskrnl.exe, и происходит запуск операционной системы.

*Boot.ini* - находится в корневом каталоге загрузочного диска. Скрытый загрузочный файл

имеющий множество настроек. Файл Ntldr использует информацию из файла Boot.ini для отображения меню запроса Please Select The Operating System To Start (Выберите операционную систему для запуска), из которого вы выбираете ОС для загрузки.

Bootsect.dos (Для систем с двойной загрузкой, в которой в качестве альтернативной ОС используются DOS, Windows 3.1x или Windows 9x) - находится в корневом каталоге загрузочного диска.

*Ntdetect.com* - находится в корневом каталоге загрузочного диска. Сборщик информации о составе

оборудования.

*Ntbootdd.sys* - является копией драйвера, используемого для загрузки SCSI-контроллера.

*Ntoskrnl.exe* - содержит программное ядро ОС Windows NT.

*Hal.dll* - содержит программный код уровня аппаратных абстракций занимается переключение

задач, вводом/выводом в порты и т.д., то есть тем, что может отличаться на разных аппаратных платформах.

*pagefile.sys* - cкрытый файл на жестком диске, используемый Windows для хранения частей

программ и файлов данных, не помещающихся в оперативной памяти.

*hiberfil.sys* - cкрытый файл на жестком диске используемый для функции "Спящий режим".

Спящий режим — это состояние, в котором компьютер завершает работу, предварительно сохранив все содержимое памяти на жестком диске. При перезапуске компьютера состояние рабочего стола полностью восстанавливается.

*Documents and Settings* - В папке находятся профили пользователей, работающих с системой

Windows XP

*Windows* – каталог предназначенный для хранения файлов ОС. В нем находятся прочие важные

подкаталоги:

Temp (Каталог предназначен для хранения временных файлов),

Prefetch (В каталоге находятся ссылки на запускаемые приложения и программы), SoftwareDistribution (В каталоге хранятся папки и файлы, полученные с помощью автоматического обновления.),

i386 (В каталоге находится кэш драйверов.),

*config* (В каталоге содержатся файлы, которые работают с реестром)

dllcache (В каталоге находится кэш защищенных системных файлов, которые используются для автоматического восстановления в случае повреждения системы).

*Program files* – каталог предназначенный для установки ПО по умолчанию.

**5. Установка, выполнение и удаление приложений**

Установка/удаление программ производится с помощью Мастера установки, который можно вызвать из Панели управления. Установка 16-битных приложения отличаются от 32-битных тем, что в процессе её выполнения 16-битные приложения создают свои ini файлы, в то время как большинство 32-битных хранят информацию в реестре.

***DOS – приложения:***

Установка DOS-программ сводится к размещению на диске, формированию переменных окружения. Для каждого приложения DOS ОС создает отдельную VDM. VDM работают в режиме вытесняющей многозадачности, деля процессорное время с системной виртуальной машиной. VDM не создают очередей сообщений. При выходе из программы завершается работа виртуальной машины и освобождаются ресурсы.

Загрузкой MS-DOS приложений можно управлять с помощью файлов autoexec.nt и config.nt из каталога Windows/system32.

В PIF-файле описываются параметры выполнения программы:

- режим выполнения (экранный или оконный)

- ресурсы памяти

- установки приоритетов для планирования процессов

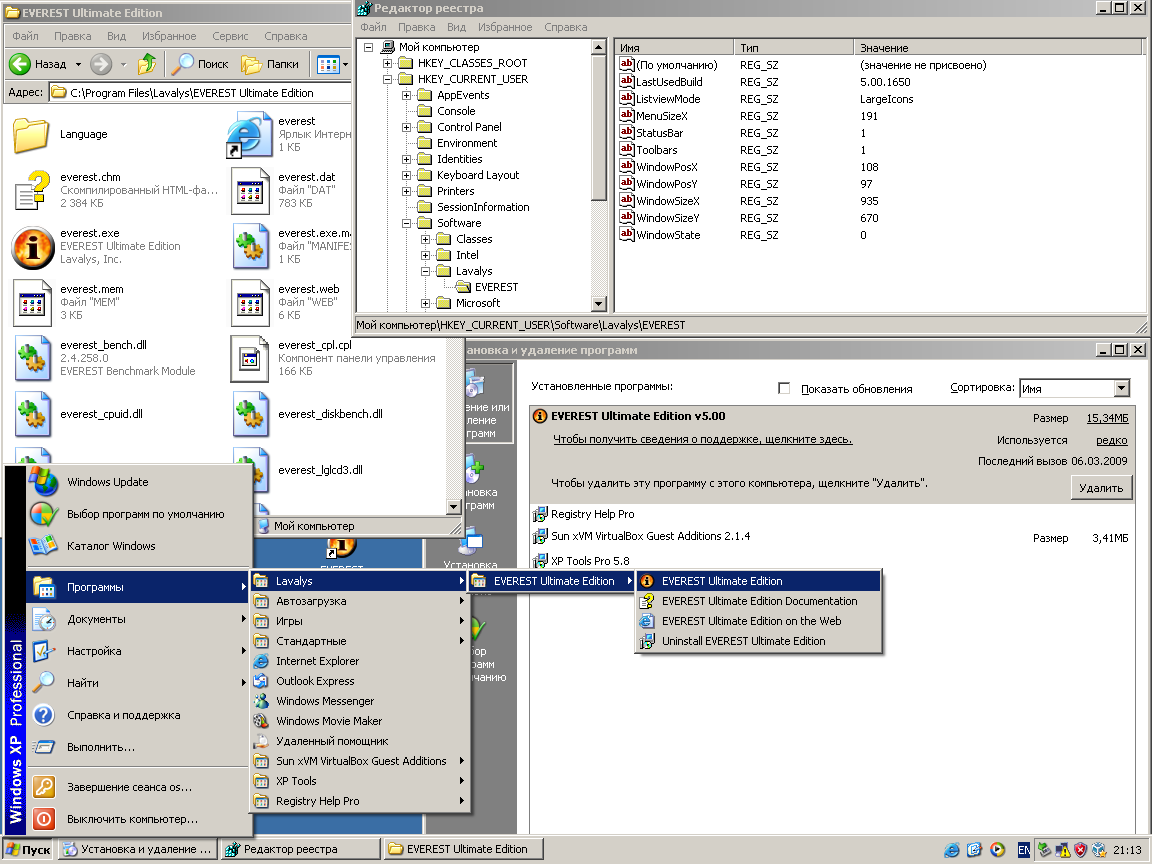
***Win16-приложения:***

Приложения Win16 выполняются в Windows XP в общем пространстве адресов в пределах системной виртуальной машины и имеют общую очередь сообщений. Ситуация с зависанием Win16 опасна, поскольку остальные программы Win16 перестанут получать сообщения и тоже зависнут. Кроме того, заблокированное приложение Win16 способно повлиять и на приложение Win32, несмотря на то, что они используют независимые очереди сообщений. В случае аварийного завершения Win16 все системные ресурсы, которые были заняты этим приложением, освободятся после того, как будут выгружены все текущие программы Win16.

***Win32 приложения:***

Для каждого приложения Win32 используется отдельная адресная область в пределах системной виртуальной машины. Приложения Win32 работают в режиме вытесняющей многозадачности, для каждого Win32-приложения и для каждого создаваемого ими потока используются отдельные очереди сообщений. Это делает ошибку в Win32-приложениях фактически безопасной для остальных приложений.

Установим Win32 приложение – Everest 5.00.1650



На рисунке видно все внесенные изменения в систему.

**6. Графический интерфейс Windows**

Реализуется с помощью функций модуля GDI; предоставляет пользователю возможность удобной работы в ОС. Графическая подсистема обеспечивает поддержку графики для устройств ввода/вывода.

Рабочий стол поддерживает механизм OLE, имеется возможность размещения на столе как самих объектов (программ, рисунков, текстовых файлов), так и ярлыков объектов. Windows позволяет просматривать рабочий стол, а также файлы и папки с применением различных стилей.

В меню “Свойства” ярлыка можно указать значок, режим совместимости, задать рабочий каталог, а также в каком режиме должно загружаться приложение (свернутым, развернутым на весь экран, в стандартном).

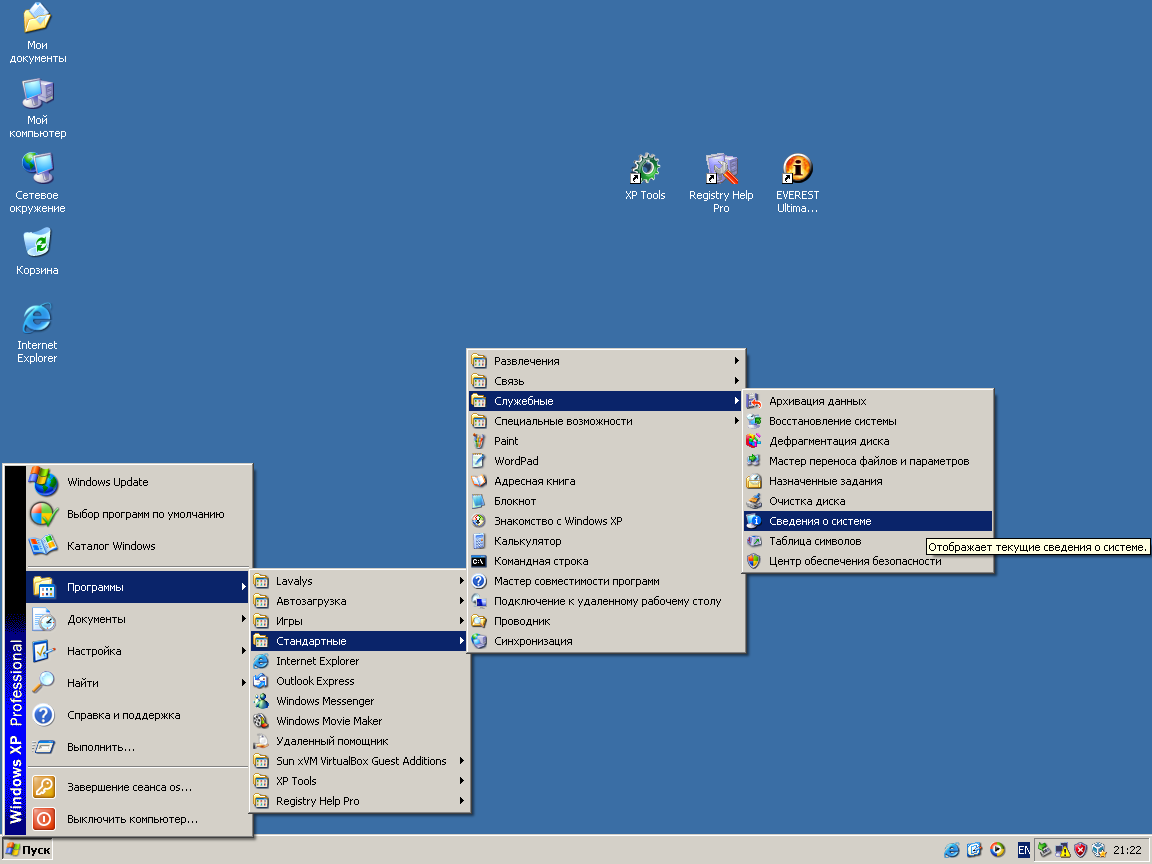
Главное меню Windows XP содержит подменю:

* программы, куда помещаются вложенные меню с пользовательскими приложениями, а

также программы, входящие в состав Windows;

* документы, куда помещаются ярлыки документов, к которым обращался пользователь;
* настройка, которая включает панель управления, принтеры, панель задач;
* поиск, через который можно найти файлы и папки
* справка, для запуска справочной системы Windows;
* выполнить, для выполнения программы по ее пути;
* завершение работы, для выключения PC и перезагрузки.

Панель задач Windows содержит кнопку “Пуск”, для вызова главного меню, а также может содержать некоторые опции быстрого доступа (настройка экрана, регулятор уровня, переключатель текущего языка, часы и пр.). При использовании GDI Windows для облегчения работы многие опции, доступные через всевозможные меню продублированы в контекстном меню.

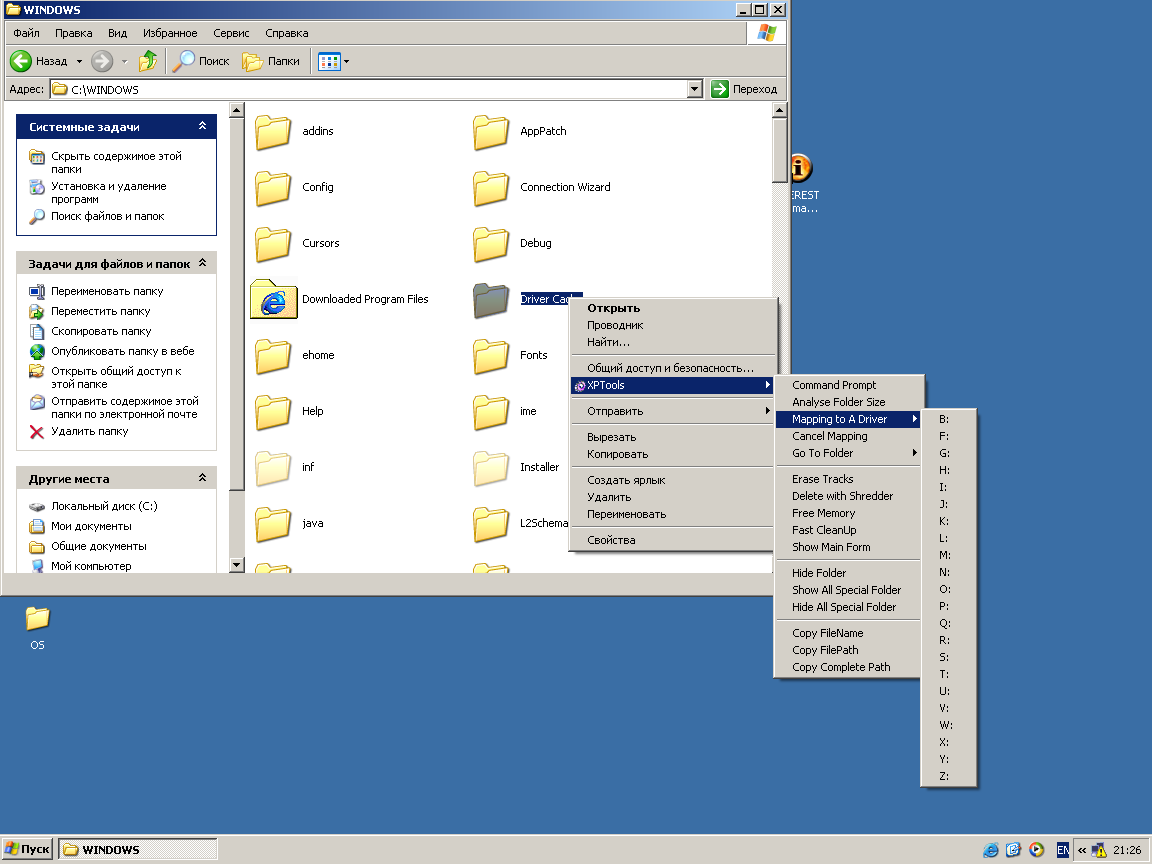


Настройка графического интерфейса рабочего стола может быть проведена через вызов свойств, где устанавливается разрешение, стиль, заставка, тема, цветовая схема и др. Через вкладку “Дополнительно” мы можем ознакомиться со свойствами видеоадаптера и установить некоторые параметры монитора, например частоту обновления экрана.

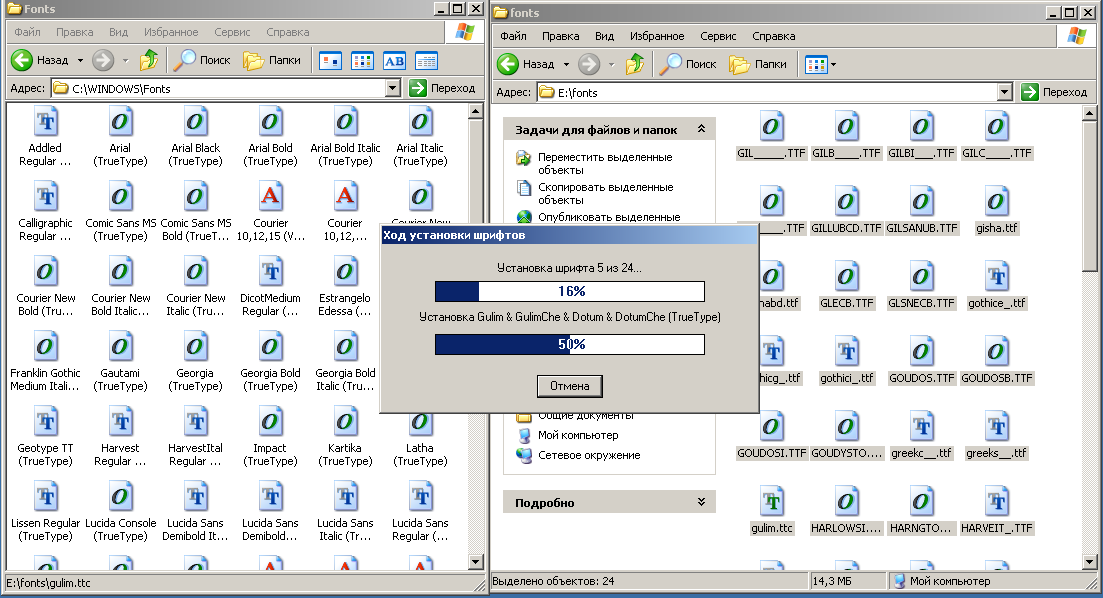
Мой компьютер позволяет просматривать диски и использовать системные средства. Чтобы просмотреть файлы, хранящиеся на компьютере, представленные в иерархическом виде, можно пользоваться Проводником.

Важная особенность интерфейса – контекстное меню для различных типов объектов.

Графический интерфейс Windows XP стал гораздо более гибким, хотя нельзя не отметить, что часть задач стала более трудной для решения, в связи с множеством возможных установок, служб, мастеров.



Установка шрифтов, производится, перемещением файлов в каталог Windows\Fonts



**7. Базовые свойства файловой системы NTFS**

Файловая система NTFS - Улучшенная файловая система, обеспечивающая уровень быстродействия и безопасности, а также дополнительные возможности, недоступные ни в одной версии файловой системы FAT. В отличие от FAT, NTFS поддерживает разделы большего объема (до 16 TiB), б*о*льшие файлы и количество файлов, хранящихся в разделе. Кроме того, в NTFS используются также кластеры меньшего размера, чем в FAT 32, что позволяет более эффективно использовать дисковое пространство. Например, в разделе NTFS объемом 30 GiB используются кластеры размером 4 KiB, тогда как в разделе такого же объема, отформатированном в FAT 32, исполь­зуются кластеры размером 16 KiB. Использование кластеров меньшего размера позволяет снизить потери дискового пространства.

*Размеры кластеров NTFS*

|  |  |  |
| --- | --- | --- |
| Размер раздела | Количество секторов в каждом кластере | Размер кластера |
| От 16 до 512 MiB | 1 | 0,5 KiB |
| От 512 MiB до 1 GiB | 2 | 1 KiB |
| От 1 до 2 GiB | 4 | 2 KiB |
| От 2 GiB до 2 TiB\* | 8 | 4 KiB |

В NTFS используется специальная файловая структура, которая называется главной файло­вой таблицей (Master File Table — MFT), и файлы метаданных. В сущности, MFT представляет собой реляционную базу данных, состоящую из строк и столбцов, в которых содержатся записи и атрибуты файлов. Эта таблица содержит записи практически всех файлов, расположенных в разделе NTFS. Файловая система NTFS создает записи файлов и каталогов для каждого файла или каталога, созданного в разделе NTFS. Эти записи хранятся в MFT, причем каждая из них занимает 1 KiB. Записи файлов содержат данные о местоположении записи в MFT, а также ат­рибуты файлов и другую информацию, относящуюся к этим файлам.

Файловая система NTFS была предназначена для управления кластерами с помощью 64-раз­рядных чисел, представляющих собой астрономические величины, но в существующих версиях используются только 32-разрядные числа. Использование 32-разрядных чисел позволяет обес­печить адресацию до 4 294 967 295 кластеров, каждый из которых обычно занимает 4 KiB.

В общей сложности NTFS резервирует 32 сектора, 16 из которых занимает созданный по умолчанию загрузочный сектор раздела, а следующие 16 — его резервная копия. Загрузочный сектор раздела, созданный по умолчанию, размещается в начале раздела (в логическом секто­ре 0), тогда как его резервная копия записывается либо в логическом центре (если раздел был отформатирован с помощью NT 3.51 или более ранней версии), либо в конце тома раздела (если последний был отформатирован с помощью операционной системы NT 4.0 или более поздней версии, включая Windows 2000/XP).

Несмотря на то что NTFS теоретически может обрабатывать разде­лы объемом до 17,59 Тбайт, из-за ограничений, налагаемых форматом таблицы разделов MBR, эта величина уменьшается до 2,2 Тбайт, так как 32-разрядная нумерация секторов, используемая в таблицах разделов, размещенных в главной загрузочной записи (MBR), имеет ограничения по емкости диска. Операционные системы Windows 2000/XP позволяют обойти это ограничение, используя в незагрузочных накопителях новый формат хранения данных, который называется *динамическим диском* Все динамические диски, имеющиеся в компьютере, содержат точную копию базы данных, что позволяет ис­пользовать базу данных одного динамического диска для восстановления поврежденной базы данных другого диска. Применяя несколько составных или чередующихся накопителей с ди­намическим форматом, можно преодолеть ограничение в 2,2 Тбайт, свойственное разделам, содержащим только одну главную загрузочную запись (MBR).

Как уже отмечалось, 32-разрядная нумерация секторов в таблицах разделов на дисках MBR не позволяет создавать основные диски NTFS емкостью более 2 TiB. Тем не менее ис­пользование нескольких составных или чередующихся накопителей дает возможность созда­вать разделы NTFS более высокой емкости и, следовательно, динамические диски большего размера. Поскольку управление динамическими разделами осуществляется с помощью скры­той базы данных, то на них совершенно не влияет ограничение в 2,2 Тбайт, которое налагается таблицами разделов главной загрузочной записи. В сущности, динамические диски дают воз­можность операционным системам Windows 2000/XP Pro создавать разделы NTFS с емко­стью до 16 ТиБ.

*Характеристики NTFS*

* Размер файлов не превышает 16 ТиБ (без 64 КиБ) или ограничен размером раздела меньшей емкости. NTFS поддерживает до 4 294 967 295 (2 - 1) файлов в разделе.
* Обычно NTFS не используется на сменных носителях, так как не позволяет сразу же передать данные на жесткий диск. Кроме того, отключение носителей, отформатиро­ванных в NTFS, без использования приложения Safe Removal может привести к потере данных. Для сменных носителей, которые могут быть неожиданно отключены, лучше использовать файловые системы FAT 12, FAT 16 или FAT 32.
* NTFS поддерживает регистрацию транзакций и функции восстановления данных. В случае отказа в работе NTFS восстанавливает после перезагрузки целостность фай­ловой системы, используя для этого системный журнал и данные контрольных точек.
* NTFS динамически перераспределяет кластеры, содержащиеся в сбойных секторах, и отмечает дефектные кластеры как поврежденные, что препятствует их дальнейшему использованию.
* NTFS имеет встроенные средства защиты, которые дают возможность устанавли­вать разрешения для каждого файла или каталога.
* NTFS имеет встроенную файловую систему кодирования (EFS). Эта система проводит динамическое кодирование и декодирование в процессе работы с зашифрованными файлами или папками, не позволяя другим пользователям обращаться к этим файлам.
* NTFS предоставляет возможность указывать дисковые квоты. Существует возмож­ность отслеживать и контролировать использование различными пользователями дискового пространства в разделах NTFS.
* NTFS имеет функцию встроенного динамического сжатия, которая позволяет сжи­мать и разархивировать файлы по мере их использования.
* Домены, которые входят в состав [Active Directory](ms-its:C:\WINDOWS\Help\misc.chm::/ntfs.htmHELP=glossary.hlp%20TOPIC=gls_activedirectory) и позволяют настраивать средства безопасности, не усложняя задачи администрирования. Для работы [контроллеров домена](ms-its:C:\WINDOWS\Help\misc.chm::/ntfs.htmHELP=glossary.hlp%20TOPIC=gls_domain_controller) необходимо использовать файловую систему NTFS.
* Разреженные файлы. Это файлы очень больших размеров, создаваемые в приложениях таким образом, что для их хранения требуется немного места на диске. В связи с этим NTFS выделяет дисковое пространство только для тех частей файла, в которые производится запись данных
* Служба внешнего хранилища, позволяющая расширить дисковое пространство путем организации удобного доступа к съемным носителям, таким, как магнитные ленты.

*Архитектура NTFS*

Несмотря на существующие различия в структуре раздела файловых систем FAT и NTFS, они имеют подобные элементы, например загрузочную область. Раздел NTFS состоит из *главной таблицы файлов (master file table — MFT).* Однако MFT — это не то же самое, что FAT. Вместо использования таблицы со ссылками на кластеры, MFT содержит больше информации о файлах и каталогах в разделе. В некоторых случаях MFT может даже содержать файлы и каталоги.

При организации раздела NTFS система создает 10 системных файлов NTFS:

$mft (Master File Table (MFT)) – Содержит запись для каждого файла в разделе NTFS в его атрибуте Data.

*$mftmirr* (Master File Table2 (MFT2)) - Зеркальная копия MFT, используемая для восстановления.

$badclus (Файл поврежденных секторов) - Содержит все поврежденные секторы раздела.

*$bitmap* (Карта распределения кластеров) - Содержит карту всего раздела, указывающую на занятые кластеры

*$boot* (Загрузочный файл)- Содержит загрузочную информацию (если раздел загрузочный)

$attrdef (Таблица определения атрибутов) - Содержит определение всех системных и пользовательских атрибутов раздела.

$logfile (Файл журнала)- Представляет собой файл журнала транзакций, используемый для восстановления

$quota (Таблица квот) - Представляет собой таблицу квот пользователей на данном разделе (используется только в NTFS 5).

$upcase (Таблица символов) - Используется для преобразования символов верхнего и нижнего регистров в символы верхнего регистра Unicode.

$volume (Раздел) - Содержит информацию о разделе, например имя раздела и версию.

$extend (Файл расширения NTFS) - Используется для хранения дополнительных расширений, таких, как квоты, идентификаторы объектов и параметры точек монтирования

Первая запись в MFT называется *дескриптором* (*descriptor*) и содержит информацию о расположении самой MFT. Загрузочный сектор в разделе NTFS содержит ссылку на распо­ложение записи дескриптора.

Вторая запись в MFT — это копия дескриптора.

Третья запись — это запись файла журнала. Все операции (транзакции) в NTFS записы­ваются в специальный файл журнала, что позволяет восстановить данные после сбоя. Осталь­ная часть MFT состоит из записей для файлов и каталогов, которые хранятся в разделе. В файле NTFS хранятся атрибуты, определенные пользователем и системой. Атрибуты в раз­деле NTFS — это не простые флаги из раздела FAT. Вся информация о файле, т.е. атрибуты, в NTFS сохраняется вместе с файлом и является частью самого файла. Каталоги в NTFS со стоят в основном из индексов файлов в этом каталоге и не содержат такой информации о файле, как размер, дата, время и др.

Таким образом, MFT — это не просто список кластеров, это основная структура хранения данных в разделе. Если файл или каталог относительно небольшой (около 1 500 байт), его за­пись может храниться в MFT. Для больших массивов данных в MFT помещается указатель на файл или каталог, а сами данные располагаются в других кластерах в разделе. Эти кластеры называются *экстентами (extents).* Все записи в MFT, включая дескрипторы и файл журнала, могут использовать экстенты для хранения дополнительных атрибутов. Атрибуты файла, ко­торые являются частью записи MFT, называются *резидентными (resident),* а атрибуты, рас­положенные в экстентах, — *нерезидентными (nonresident).*

Особенность реализации NTFS в Windows XP — уменьшение объема данных MFT, считываемых из памяти. Если все диски отформатированы в NTFS, то во время загрузки Windows считывает из таблицы MFT всего несколько сотен килобайт данных. Таким образом, NTFS повышает эффективность использования системной памяти

***Монтирование тома к точке соединения NTFS, создание******Junction Point***

Монтирование можно произвести с помощью команды *moutntvol* или через утилиту Disk Management (Управление дисками), имеющую графический интерфейс.

C:\>mkdir mounttest

C:\>mountvol

Создание, удаление и просмотр точек подключения.

MOUNTVOL [<диск>:]<путь> <имя тома>

MOUNTVOL [<диск>:]<путь> /D

MOUNTVOL [<диск>:]<путь> /L

<путь> Существующая папка NTFS, в которой будет

располагаться точка подключения.

<имя тома> Имя подключаемого тома.

/D Удаление точки подключения тома из заданной папки.

/L Вывод списка имен подключенных томов для заданной папки.

Возможные значения имени тома вместе с текущими точками подключения:

\\?\Volume{f7e55ff2-0a98-11de-9357-806d6172696f}\

C:\

\\?\Volume{f7e55ff1-0a98-11de-9357-806d6172696f}\

D:\

\\?\Volume{f7e55ff0-0a98-11de-9357-806d6172696f}\

A:\

C:\>mountvol C:\mounttest \\?\Volume{f7e55ff2-0a98-11de-9357-806d6172696f}\

C:\>dir

Том в устройстве C не имеет метки.

Серийный номер тома: 0CE4-7E12

Содержимое папки C:\

06.03.2017 23:04 0 AUTOEXEC.BAT

06.03.2017 23:04 0 CONFIG.SYS

15.04.2017 20:25 <DIR> distrib

06.03.2017 23:08 <DIR> Documents and Settings

15.04.2017 22:33 <JUNCTION> mounttest

15.04.2017 20:30 <DIR> Program Files

15.04.2017 20:29 <DIR> WINDOWS

2 файлов 0 байт

5 папок 8 651 059 200 байт свободно

C:\>cd mounttest

C:\mounttest>dir

Том в устройстве C не имеет метки.

Серийный номер тома: 0CE4-7E12

Содержимое папки C:\mounttest

06.03.2017 23:04 0 AUTOEXEC.BAT

06.03.2017 23:04 0 CONFIG.SYS

15.04.2017 20:25 <DIR> distrib

06.03.2017 23:08 <DIR> Documents and Settings

15.04.2017 22:33 <JUNCTION> mounttest

15.04.2017 20:30 <DIR> Program Files

15.04.2017 20:29 <DIR> WINDOWS

2 файлов 0 байт

5 папок 8 651 059 200 байт свободно

C:\mounttest>mountvol C:\mounttest /D

C:\mounttest>dir

Том в устройстве C не имеет метки.

Серийный номер тома: 0CE4-7E12

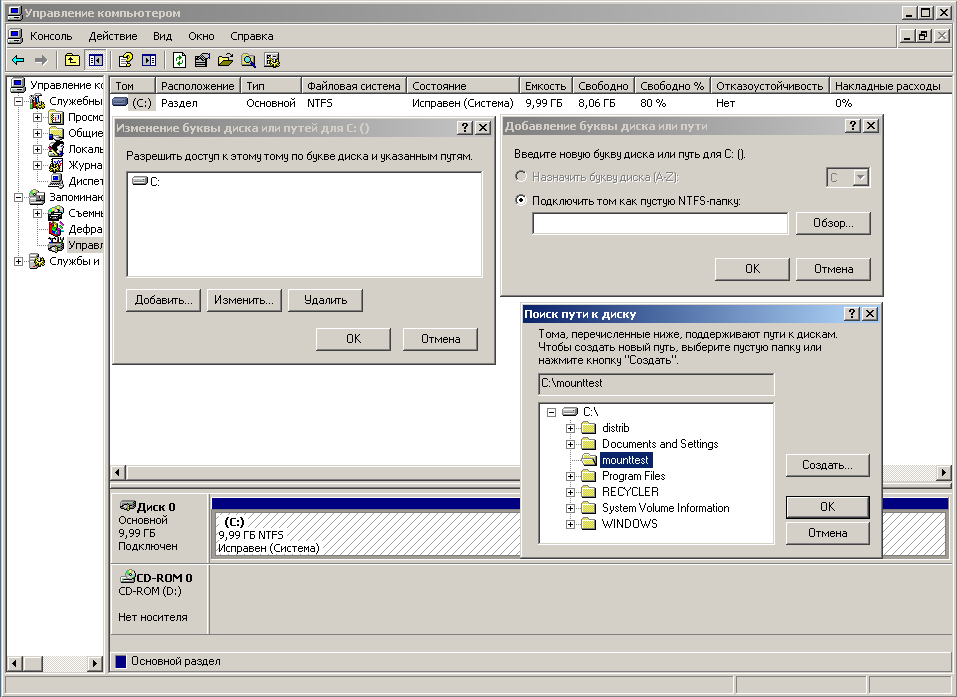
Содержимое папки C:\mounttest

15.04.2017 22:33 <DIR> .

15.04.2017 22:33 <DIR> ..

0 файлов 0 байт

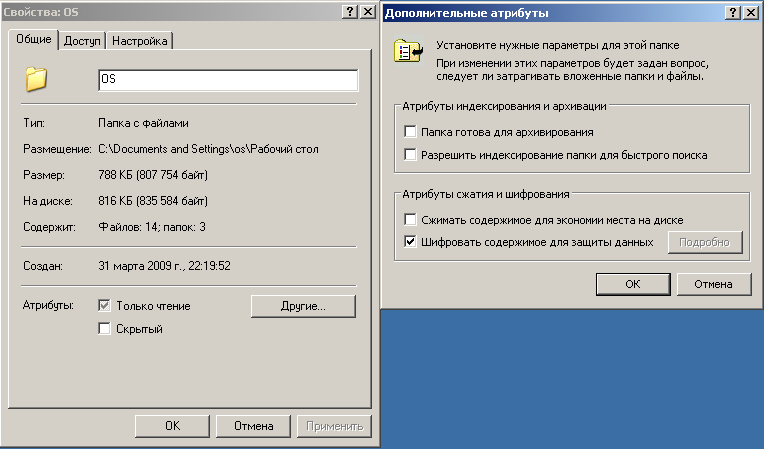
2 папок 8 651 059 200 байт свободно



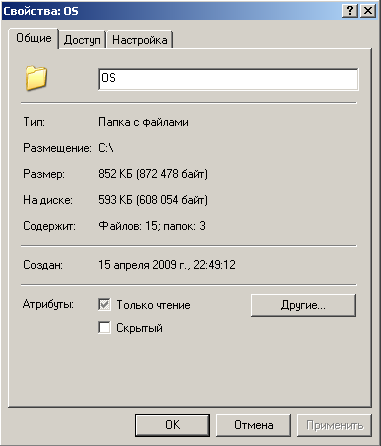
***Шифрация и сжатие каталога***

Шифрацию или сжатие каталога выполняем через контекстное меню: в меню “Свойства” во вкладке “Дополнительные настройки” устанавливаем флаг “Шифровать содержимое для защиты данных” или “Сжимать содержимое для экономии места на диске”.

После чего имеем возможность применить шифрацию ко всем входящим в каталог подкаталогам и файлам или только к вновь добавляемым. Цвет надписей относящихся к каталогу в проводнике изменяется (например для сжатой папки с синего на зеленый). Далее просматриваем свойства файла находящегося в каталоге (применили шифрацию ко всем входящим в каталог подкаталогам и файлам), и отмечаем, что имеем возможность добавить/удалить права доступа пользователей к данному файлу (мы обладаем правами администратора имеем доступ к файлу). Выполняем операцию расшифровки, по тому же алгоритму, что и шифрацию.

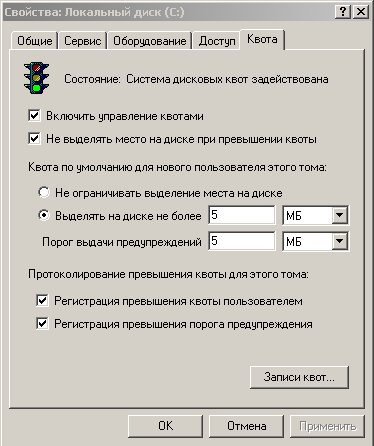


Результаты сжатия можно увидеть на рисунке:

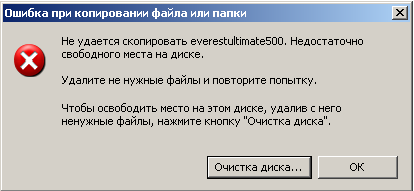


***Назначение дисковой квоты***

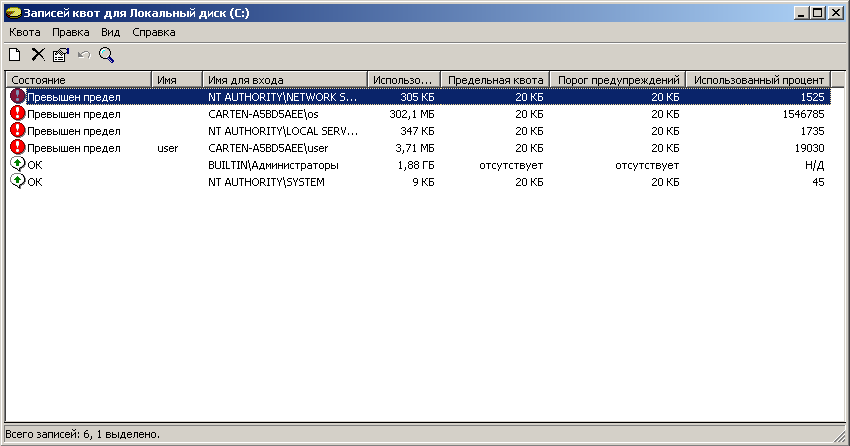
Через контекстное меню обращаемся к свойствам диска и переходим к вкладке “Квота”. Включаем управление квотами.



При попытке пользователя прквысить квоту, выводится сообщение:

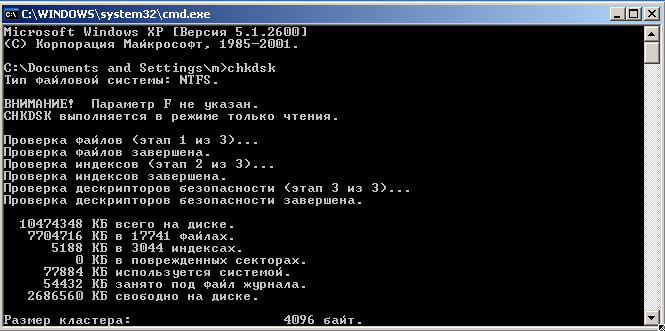


Информации о превышении квот можно посмотреть в журнале:



***CHKDSK***

Стандартное приложение в операционных системах DOS и Microsoft Windows, которое проверяет жёсткий диск или дискету на ошибки файловой системы

******

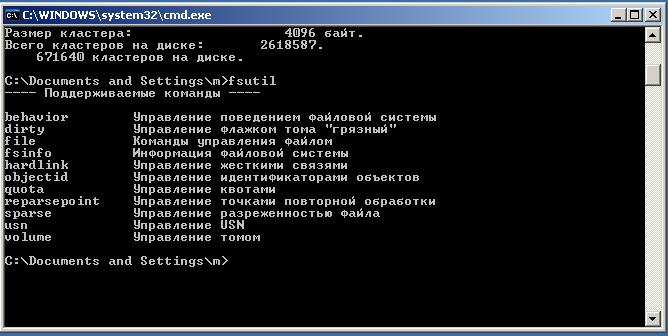
Команда: CHKDSK [том:[[путь]имя\_файла]] [/F] [/V] [/R] [/X] [/I] [/C] [/L[:размер] [/B]]

выполняет проверку указанного диска при помощи программы Check Disk, при вызове без аргументов осуществляется проверка текущего диска.

* том — определяет метку тома проверяемого диска, точку подключения либо имя диска с двоеточием (например, C:);
* путь, имя файла — имя файла или группы файлов для проверки на фрагментацию. Используется только в файловой системе FAT/FAT32;
* /F — выполнение проверки на наличие ошибок и их автоматическое исправление;
* /V — в процессе проверки диска выводить полные пути и имена хранящихся на диске файлов. Для дисков, содержащих разделы NTFS, также выводятся сообщения об очистке;
* /R — выполнить поиск поврежденных секторов и восстановить их содержимое. Включает в себя действие ключа /F;
* /X — в случае необходимости выполнить отключение тома перед его проверкой. После отключения все текущие дескрипторы для данного тома будут недействительны. Требует обязательного использования ключа /F;
* /I — не проводить строгую проверку индексных элементов. Используется только в файловой системе NTFS. Это ускоряет проверку, но делает её менее тщательной;
* /C — не проводить проверку циклов внутри структуры папок. Используется только в файловой системе NTFS. Это ускоряет проверку, но делает её менее тщательной;
* /L:размер — в ходе проверки изменить размер файла журнала до указанной величины (в килобайтах). Если значение не указано, выводится текущий размер файла. Используется только в файловой системе NTFS;
* /B — Только для NTFS: повторная оценка поврежденных кластеров на диске (требует обязательного использования ключа /R)

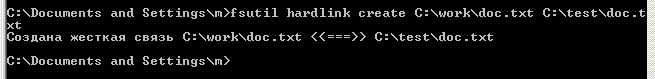
***FSUTIL***

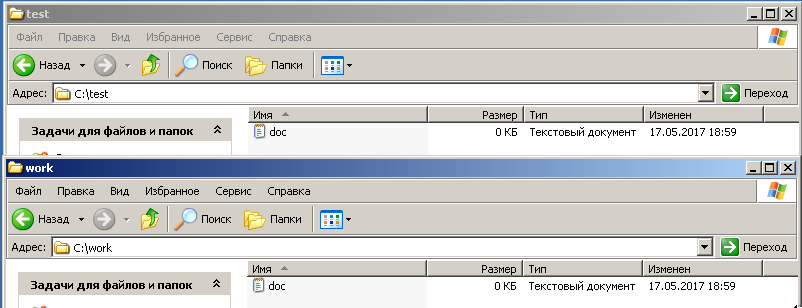
Fsutil является служебной программой командной строки, которая используется для выполнения связанных задач файловых систем FAT и NTFS, таких как управление точками повторной обработки, управление разреженными файлами, отключение тома или расширение тома.



**Создание hardlink**

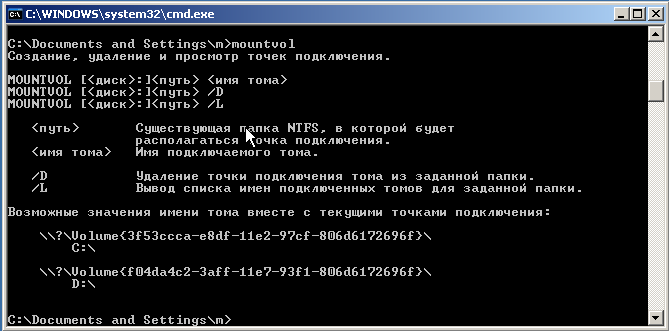
Использование команды *fsutil hardlink create* позволяет создать несколько логических файлов в различных местах. При этом все они будут ссылаться на один и тот же физический файл. Использование постоянных ссылок позволяет прозрачно для пользователей перенаправить обращение к файлу в одном месте к данным, фактически хранящимся в другом месте.





**Создание symlink**

Встроенными средствами Windows XP создать символическую ссылку нельзя. Поддержка символьных ссылок появилась только в следующем поколении Windows – Vista.

***MOUNTVOL***

Служит для создания, удаления и получения списка точек подключения тома. Команда *mountvol* обеспечивает подключение томов, не требуя для этого букву диска.

Пример работы с mountvol был представлен выше.

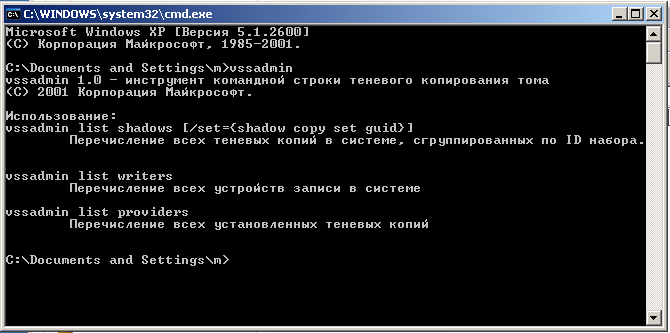
***DISKPART***

****

Программа DiskPart.exe это работающий в текстовом режиме командный интерпретатор, который позволяет управлять объектами (дисками, разделами или томами) с помощью сценариев или команд, вводимых с командной строки. Перед использованием команд DiskPart.exe для диска, раздела или тома, необходимо сначала составить список объектов, а затем выбрать объект для работы. После этого все введенные команды DiskPart.exe выполняются для данного объекта.

Составить список всех доступных объектов и определить номер объекта или букву диска можно с помощью команд list disk, list volume и list partition. Команды list disk и list volume позволяют вывести все диски и тома компьютера. Команда list partition, однако, выводит разделы только выбранного диска. При использовании команды list рядом с выбранным объектом отображается звездочка (\*). Объект выбирается по номеру или букве диска, например диск 0, раздел 1, том 3 или том C.

***VSSADMIN***



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

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.

**8. Командный язык и работа в режиме командной строки**

По своим функциям команды можно разделить на несколько групп: управление файлами и каталогами, управление устройствами, управление процессами, информационные команды ввода-вывода, команды программирования командных файлов, другие.

*Команды работы с каталогами и файлами:*

ATTRIB Отображение и изменение атрибутов файлов.

DEL Удаление одного или нескольких файлов.

COPY Копирование одного или нескольких файлов в другое место.

MKDIR Создание папки.

CHDIR Вывод имени либо смена текущей папки.

RMDIR Удаление папки.

DIR Вывод списка файлов и подпапок из указанной папки.

TYPE Вывод на экран содержимого текстовых файлов.

COMPACT Отображение/изменение сжатия файлов в разделах NTFS.

FINDSTR Поиск строк в файлах.

FIND Поиск текстовой строки в одном или нескольких файлах.

FC Сравнение двух файлов или двух наборов файлов и вывод различий между ними.

ERASE Удаление одного или нескольких файлов.

REPLACE Замещение файлов.

RENAME Переименование файлов и папок.

XCOPY Копирование файлов и дерева папок.

PRINT Вывод на печать содержимого текстовых файлов.

C:\>dir

Том в устройстве C не имеет метки.

Серийный номер тома: 0CE4-7E12

Содержимое папки C:\

06.03.2009 23:04 0 AUTOEXEC.BAT

06.03.2009 23:04 0 CONFIG.SYS

15.04.2009 20:25 <DIR> distrib

06.03.2009 23:08 <DIR> Documents and Settings

15.04.2009 22:33 <JUNCTION> mounttest

15.04.2009 20:30 <DIR> Program Files

15.04.2009 20:29 <DIR> WINDOWS

2 файлов 0 байт

5 папок 8 651 059 200 байт свободно

*Команды управления работой с устройствами и процессами:*

BREAK Включение/выключение режима обработки комбинации клавиш CTRL+C.

CHKDSK Проверка диска и вывод статистики.

CHKNTFS Отображение или изменение выполнения проверки диска во время загрузки.

CONVERT Преобразование дисковых томов FAT в NTFS. Нельзя выполнить преобразование текущего активного диска.

DISKCOMP Сравнение содержимого двух гибких дисков.

FORMAT Форматирование диска для работы с Windows.

VERIFY Установка режима проверки правильности записи файлов на диск.

VOL Вывод метки и серийного номера тома для диска.

FOR Запуск указанной команды для каждого из файлов в наборе.

MORE Последовательный вывод данных по частям размером в один экран.

COPY CON Перенаправление потока ввода информации с консоли в файл.

C:\>vol

Том в устройстве C не имеет метки.

Серийный номер тома: 0CE4-7E12

*Информационные команды и команды реконфигурация:*

MEM Вывод сведений о полной и свободной системной памяти.

KEYB Настройка клавиатуры на национальный алфавит.

MODE Отображение статуса и режима работы посимвольных устройств. Команда выполняет множество функций, для примера рассмотрим ее применение для поддержки кодовых страниц. Конфигурирование системных устройств.

SET Установка значения глобальной переменной в окружении DOS и отображение окружения.

ECHO Вывод сообщений и переключение режима отображения команд на экране.

PROMPT Задает формат приглашения DOS.

PATH Установка и отображение маршрутов поиска исполняемых файлов

MORE Последовательный вывод данных по частям размером в один экран.

VER Отображение номера версии.

DATE Установка и отображение соответственно даты.

TIME Установка и отображение соответственно времени.

C:\>echo 'Hello world!'

'Hello world!'

*Команды используемые для программирования пакетных файлов:*

PAUSE Приостановка выполнения пакетного файла и вывод сообщения.

CALL Вызов одного пакетного файла из другого.

ENDLOCAL Конец локальных изменений среды для пакетного файла.

GOTO Передача управления в отмеченную строку пакетного файла.

IF Оператор условного выполнения команд в пакетном файле.

REM Помещение комментариев в пакетные файлы и файл CONFIG.SYS.

SETLOCAL Начало локальных изменений среды для пакетного файла.

SHIFT Изменение содержимого (сдвиг) подставляемых параметров для пакетного файла.

***Пример командного файла***

@ECHO OFF

REM write here name of you file.

SET NAME=main

ECHO .

ECHO BUILD PROJECT %NAME%

ECHO .

ECHO TRANSLATION:

ECHO .

C:\PR\TOOLS\BORLANDC\BIN\TASM -la -zi %NAME%

IF NOT EXIST %NAME%.obj GOTO error\_translation

ECHO LINKING:

ECHO .

C:\PR\TOOLS\BORLANDC\BIN\TLINK -t %NAME%

IF NOT EXIST %NAME%.com GOTO error\_linking

ECHO .

ECHO FINISH

ECHO BUILDED: %NAME%.obj, %NAME%.lst, %NAME%.com, %NAME%.map

GOTO exit

:error\_translation

ECHO TRANSLATION FAULT

GOTO exit

:error\_linking

ECHO .

ECHO LINKING FAULT

:exit

ECHO .

PAUSE

**9. Механизм обмена данными между приложениями**

***Clipboard***

Clipboard называют универсальным буфером обмена, так как пользователь может записать в него самую различную информацию. Это общая область для хранения дескрипторов данных, через  которую прикладные программы могут обмениваться форматированными данными.

Методика работы с Clipboard одинакова для всех приложений и обычно заключается в том, что пользователь выделяет нужную часть документа или изображения, а затем выбирает из меню "Edit" строки "Copy" или "Cut". В первом случае выделенный фрагмент копируется в Clipboard, во втором - также копируется, но после копирования фрагмент удаляется из документа. Clipboard может содержать данные одновременно в нескольких форматах.

Во-первых, приложение может записать в Clipboard данные в одном из форматов, предопределенных для Windows. Можно записать данные в текстовом формате, битовое изображение в формате, зависящем от устройства отображения (DDB), цветовую палитру, битовое изображение в формате, независящем от устройства отображения (DIB), в виде метафайла, а также в нескольких других форматах, созданных на базе текстового формата данных.

Во-вторых, приложение может использовать свой собственный, уникальный формат данных, зарегистрировав его в Windows при помощи специальной функции. Память, в которой хранятся данные, должна быть доступна для всех приложений. Кроме того, содержимое памяти не должно исчезать при завершении работы отдельных приложений.

***DDE – технология (Dynamic Data Exchange)***

DDE – технология позволяет создать постоянно действующие каналы между несколькими одновременно работающими приложениями Windows. Эти каналы могут создаваться автоматически при запуске приложения или при необходимости, а также по явному запросу пользователя. После того как каналы созданы, они будут работать без вмешательства пользователя. Приложения, использующие технологию динамического обмена данных DDE, выступают как клиенты или серверы (или одновременно как клиенты и серверы). Начиная с версии 3.1 в составе Windows появилось расширение - управляющая библиотека динамического обмена данными DDEML, выполненная как обычная DLL-библиотека. Механизм Network DDE позволяет организовать каналы обмена данными между приложениями, которые запущены на разных рабочих станциях сети. Большая часть DDE-функций реализована в последних версиях OLE.

***OLE(Object Linking and Embedding)***

Работа с Windows носит документно-ориентированный характер. Однако документы этой системы могут иметь сложную структуру, объединяющую тексты с графиками и различными объектами мультимедиа. Для создания и применения таких документов служит специальная технология, реализуемая системой Windows.

Механизм OLE (Object Linking and Embedding - Связывание и Встраивание Объектов) позволяет обеспечить интеграцию различных по своей сути объектов. При связывании объекта с документом создается ссылка на его файл (технология OLE1 – жесткая ссылка, технология OLE2 – относительная ссылка)

OLE является набором средств, позволяющим легко подготавливать документы, включающие в себя данные, подготовленные в различных приложениях. В Windows 95 используется новая реализация этого метода, известная как OLE-2.

Для реализации этих возможностей соответствующие приложения должны иметь опцию Object (Объект) в меню Insert (Включение).

Стандартные приложения Windows поддерживают OLE. Кроме стандартных приложений Windows, многие другие приложения, разработанные фирмой Microsoft и другими независимыми фирмами, включают в себя поддержку OLE-технологии.

В отличие от операции встраивания, при выполнении операции связывания внутрь документа помещается не сам объект, а только ссылка на него (путь исходного файла, подготовленного приложением-сервером).

Использование операции связывания вместо операции вставки имеет два важных преимущества.

\* Если объект, подготовленный приложением-сервером, используется в нескольких документах (приложениях-клиентах), то когда вы изменяете объект, автоматически происходит обновление всех документов, которые содержат ссылку на этот объект.

\* Так как в документе помещается только ссылка на связываемый объект, то размер документа получается меньше, чем при включении объекта в документ.

Однако, операция связывания имеет и свои недостатки. Вы должны сами выбрать что вы будете использовать - операцию вставки или операцию связывания.

\* Так как связываемые объекты хранятся отдельно от документа, к которому они привязаны, то вместо одного файла документ будет состоять из множества файлов, расположенных в различных каталогах.

\* Если вы перемещаете файл, содержащий связываемый объект в другой каталог, то вам необходимо изменить в документе ссылку на перемещенный объект.

\* Активизация объекта по месту. Позволяет получить доступ к включенному объекту по месту, без переключения на другое окно или приложение. Вы можете записывать, отображать, проигрывать и редактировать включенные объекты оставаясь в основном приложении (документе).

\* Поддержка вложенных объектов. Позволяет взаимодействовать с объектами, вложенными в другие объекты

\* Поддержка механизма Drag and Drop. Теперь можно перетаскивать объект из одного приложения в другое с помощью мыши. При этом происходит автоматическое встраивание объекта в документ другого приложения

\* Независимые связи. Допускаются связи между включенными объектами, не записанными на диске в виде файлов. Это позволяет встраивать объекты внутри одного и того же или различных приложений вне зависимости от наличия файла

\* Адаптируемые связи. Сохраняется связь между объектами и главным документом в случае выполнения операций копирования и перемещения

\* Логическая разбивка на страницы. Позволяет включать в документ объекты, перекрывающие границу страницы.

В итоге видим, что Windows предоставляет разнообразные средства для обмена данными между приложениями, как с сохранением связи с источником, так и без, что является плюсом в плане гибкости системы.