МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

ОТЧЕТ

по лабораторной работе № 1

«Механизмы ОС Microsoft Windows»

по дисциплине

«Эксплуатация современных операционных систем»

РУКОВОДИТЕЛЬ:

Кочешков А. А.

СТУДЕНТЫ:

Игнаков К. М.

\_\_\_\_\_\_\_19-В-2\_\_\_\_\_\_\_\_

(шифр группы)

Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород 2021

1. Подготовка к установке ОС Windows.

Спецификация современных версий Windows для рабочих станций:

* Windows Home – данная версия домашней операционной системы создана специально для обычных пользователей, которые используют компьютер для развлечений, и простых задач. По этому меню и инструменты данной версии ОС четко оптимизирован именно для такого круга лиц.
* Windows 10 Pro – современная и многофункциональная операционная система от Micrososft. Ее редакция Pro обладает всеми функциями "домашней" ОС + функции для бизнеса, такие как шифрование, RDP, создание виртуальной машины Hyper-V. Т.е она обладает самым полным набором инструментов. Она включает возможность ускоренной обработки данных, и поддерживает оборудование, которая содержит в себе до 4 процессоров и 6ТБ ОЗУ на одной материнской плате. Данная Windows 10 Pro поддерживает процессоры серверного уровня Intel Xeon и AMD Opeteron.
* Windows 10 Enterprise (Корпоративная) – специальная редакция Windows 10, она поставляется для крупных предприятий, а так же для организаций среднего бизнеса. Но данный выпуск редакции вполне можно использовать для домашнего использования, т.к данная редакция устойчивая к различным сбоям операционной системы, содержит в себе усиленную безопасность и скачивает только проверенные пакеты обновления. Помимо всего дананя ОС может быть установлена на мобильные устройства с поддержкой x32 и ARM архитектуры.
* Windows 10 Enterprise LTSC 2019 - Windows 10 «Корпоративная с долгосрочным обслуживанием». Это новый релиз Windows 10 Enterprise 2019, самая актуальная версия, она пришла на смену Windows 10 Enterprise LTSB, является специальным вариантом "Корпоративной" версии, отличается от остальных редакций долгосрочной поддержкой одной "версии обновления", отсутствием Магазина и UWP приложений (кроме приложения «Параметры»).
* Windows 10 S – это операционная система, которая ориентирована на образовательный сегмент и позволяет устанавливать только проверенные приложения из Windows Store.

Дисковая конфигурация:

* MBR (Master Boot Record) – это загрузочная запись, которая встраивается в начало физического диска. В нём содержится информация о разделах диска и загрузчик ОС.
* GPT – таблица разделов жесткого диска. Является усовершенствованным аналогом MBR. Разработан, как один из компонетов EFI и нужен для размещения кода загрузки операционной системы.

Основные отличия от MBR:

|  |  |  |
| --- | --- | --- |
|  | **GPT** | **MBR** |
| Максимальный размер диска | 18 Экзабайт | 2 ТиБ |
| Максимальное количество разделов | 128 | 4 |
| Резервирование | Да | Нет |

Варианты установки Windows 10:

1. Установка Windows 10 из системы - Windows 10, в отличие от некоторых более старых версий Windows, можно установить из самой системы. Это можно сделать, запустив исполняемый файл setup.exe с того же накопителя.
2. Установка Windows 10 через BIOS – это процедура запуска загрузочного накопителя. Перед началом установки требуется попасть в BOOT Menu, которое позволит выбрать запуск флешки, на которой предустановлен установщик Windows 10, а не загрузку жёсткого диска.
3. Установка Windows 10 с помощью командной строки.
4. Установка Windows через Media Creation Tool – официальный инструмент Media Creation Tool от Microsoft позволяет обновить компьютер до последней версии ОС Windows 10, выполнить чистую установку системы, скачать образ Windows 10 ISO и создать установочный носитель.

Способы развертывания Windows 10.

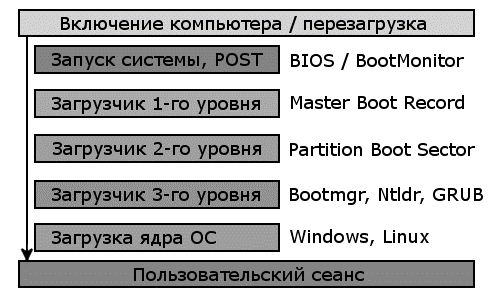
1. **Современные методы развертывания**:
   1. Windows автопилот — это новый набор возможностей, предназначенных для упрощения и модернизации развертывания и управления новыми компьютерами Windows 10 компьютеров. Windows автопилот позволяет ИТ-специалистам настраивать функцию out of Box Experience (OOBE) для пк Windows 10 и предоставлять конечным пользователям полностью настроенное новое устройство Windows 10 после нескольких щелчков мыши.
   2. Обновление на месте – для существующих компьютеров под управлением Windows 7, Windows 8 или Windows 8.1 для организаций, развертывающих Windows 10, рекомендуется использовать программу установки Windows (Setup.exe) для выполнения обновления на месте, которое автоматически сохранит все данные, параметры, приложения и драйвера из существующей версии операционной системы. При этом задействует наименьшее число ИТ-операций, так как нет необходимости создавать сложную инфраструктуру развертывания.
2. **Динамическая подготовка**
   1. Активация подписки на Windows 10 – это современный метод развертывания, позволяющий изменить SKU с версии Pro на версию Корпоративная без использования ключей и перезагрузки устройства.
   2. AAD/MDM – присоединение к Azure Active Directory (AAD) с автоматической регистрацией в решении по управлению мобильными устройствами (MDM) – в этом сценарии член организации должен просто предоставить свой рабочий или школьный идентификатор и пароль; затем устройство можно автоматически присоединить к Azure Active Directory и зарегистрировать в решении MDM без дополнительного взаимодействия с пользователем. После регистрации решение MDM может завершить конфигурацию устройства по мере необходимости.
   3. Конфигурация пакета подготовки – используя конструктор образов и конфигураций Windows, ИТ-администраторы могут создать автономный пакет, содержащий все настройки, параметры и приложения, которые необходимо применить на компьютере. Эти пакеты затем развертываются на новых компьютерах различными способами, выполнение осуществляется обычно ИТ-специалистами.
3. **Обычное развертывание**
   1. Новый компьютер – также называется развертыванием на чистой новой машине. Этот сценарий подходит при наличии у вас пустого компьютера, который следует развернуть, или существующего компьютера, который вы хотите очистить и развернуть заново без сохранения любых существующих данных. Программа установки запускается с загрузочного носителя, с компакт-диска, USB, ISO-файла или предзагрузочной среды выполнения (PXE). Также можно сформировать полный автономный носитель, включающий все файлы, необходимые для развертывания клиента, что дает возможность проводить развертывание без подключения к общей папке централизованного развертывания. Целью может быть физический компьютер, виртуальная машина или виртуальный жесткий диск (VHD), запущенный на физическом компьютере (загружающийся с VHD).
   2. Обновление компьютера – процесс обновления иногда также называется очисткой и загрузкой. Процесс обычно запускается в работающей операционной системе. В ходе выполнения процесса развертывания пользовательские данные и параметры архивируются и позже восстанавливаются. Цель может быть такая же, как в сценарии с новым компьютером.
   3. Замена компьютера сходна со сценарием обновления компьютера. Но так как компьютер все же заменяется, этот сценарий разбивается на две основные задачи: резервное копирование старого клиента и чистое развертывание нового. Как и в случае со сценарием обновления, пользовательские данные и параметры архивируются и восстанавливаются.

Способы активации

1. Активация с помощью цифровой лицензии - цифровые лицензии связаны с вашим оборудованием и учетной записью Майкрософт, поэтому вам не нужно ничего искать на своем компьютере. Все настраивается автоматически при подключении компьютера к Интернету и выполнении входа в свою учетную запись Майкрософт.
2. Активация с помощью ключа продукта – это 25-значный код, который выглядит следующим образом: КЛЮЧ ПРОДУКТА: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Процесс загрузки Windows.

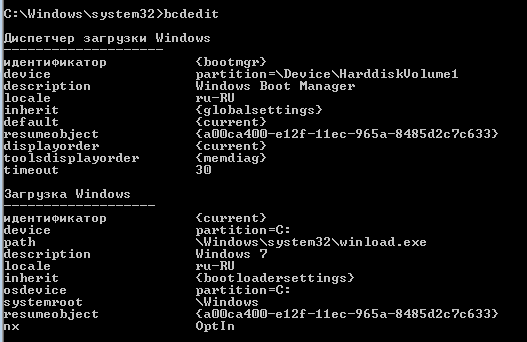
Этапы загрузки OC



1. Включение компьютера, POST, BootMonitor. Начальный этап загрузки операционной системы после включения компьютера начинается в BIOS (Basic Input/Output System — базовая система ввода-вывода). В настройках BIOS мы указываем загрузочное устройство, или ряд загрузочных устройств в порядке их приоритета. Возможны различные варианты загрузки и их комбинации: с жесткого диска, CD/DVD – диска, USB-flash и другие.  
   Сразу после прохождения POST (Power-On Self-Test — самотестирование после включения) BIOS компьютера начнет поочередно перебирать указанные загрузочные устройства до тех пор, пока на одном из них не найдет подходящую специальную запись, в которой содержится информация о дальнейших действиях.
2. Загрузчик 1-го уровня. Master Boot Record. Master Boot Record — главная загрузочная запись, расположена в первых физических секторах загрузочных устройств хранения. Она содержит таблицу разделов (Partition Table) и исполняемый код.  
   Главной задачей программы, записанной в MBR, является поиск активного системного раздела диска и передача управления его загрузочному сектору. Таким образом, эту стадию можно назвать подготовительной в силу того, что непосредственно загрузки самой ОС еще не происходит.  
   Системным принято называть раздел диска (устройства хранения), на котором расположены файлы операционной системы, отвечающие за процесс загрузки ОС (сама операционная система может размещаться в другом разделе). В принципе, системных разделов может быть несколько, поэтому один из них отмечается как активный. Именно его ищет программа, загруженная с MBR.
3. Загрузчик 2-го уровня. Partition Boot Sector. Следующим этапом загрузки компьютера является передача управления исполняемому коду, записанному в PBS (Partition Boot Sector — загрузочный сектор активного раздела). PBS расположен в первом секторе (секторах) соответствующего раздела диска. В коде PBS прописано имя файла за-грузчика операционной системы, которому и передается управление на этом этапе.
4. Начальный этап загрузки операционной системы. Менеджер загрузки ОС. В версиях Windows до Vista, например, Windows XP будет загружен Ntldr. Он, в свою очередь, считывает информацию из текстового файла Boot.ini, в котором записана информация об установленных операционных системах.
5. Загрузка ядра операционной системы. Завершающим этапом загрузки операционной системы является загрузка ядра ОС и передача ему управления.

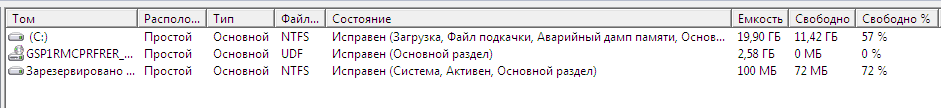
Boot manager и BCD

В Windows Vista или Windows 7 / 8 /10 диспетчер загрузки называется Bootmgr. Он читает список установленных операционных систем не из текстового файла, boot.ini, а из системного хранилища BCD (Boot Configuration Data), доступ к которому осуществляется посредством специальной утилиты bcdedit.exe.



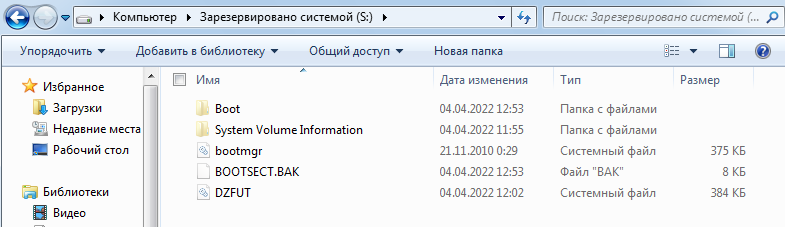
Процесс стандартной инсталляции операционной системы Windows Vista / 7 / 8 создает в начале диска дополнительный раздел «Зарезервировано системой». Ему не присваивается буква диска, благодаря чему, если не сделать дополнительных шагов, и сам раздел и его содержимое будут скрыты от пользователя. Этот основной раздел имеет статус «Системный» и «Активный» и, следовательно, удалить его тоже нельзя. В Windows 7 размер такого раздела составляет 100 МБ, из которых занято около 30 МБ.

Откроем консоль «Управление компьютером» и перейдём в меню «Управление дисками» и убедимся в наличии раздела.

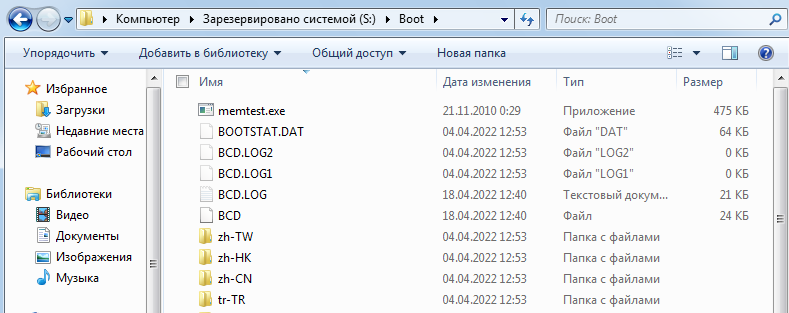


Посмотрим содержимое раздела «Зарезервировано системой». Для этого назначим ему букву диска в меню «Управление дисками». В панели управления компьютером включим отображение скрытых папок и файлов.

В корне раздела находится файл bootmgr, который является загрузчиком.



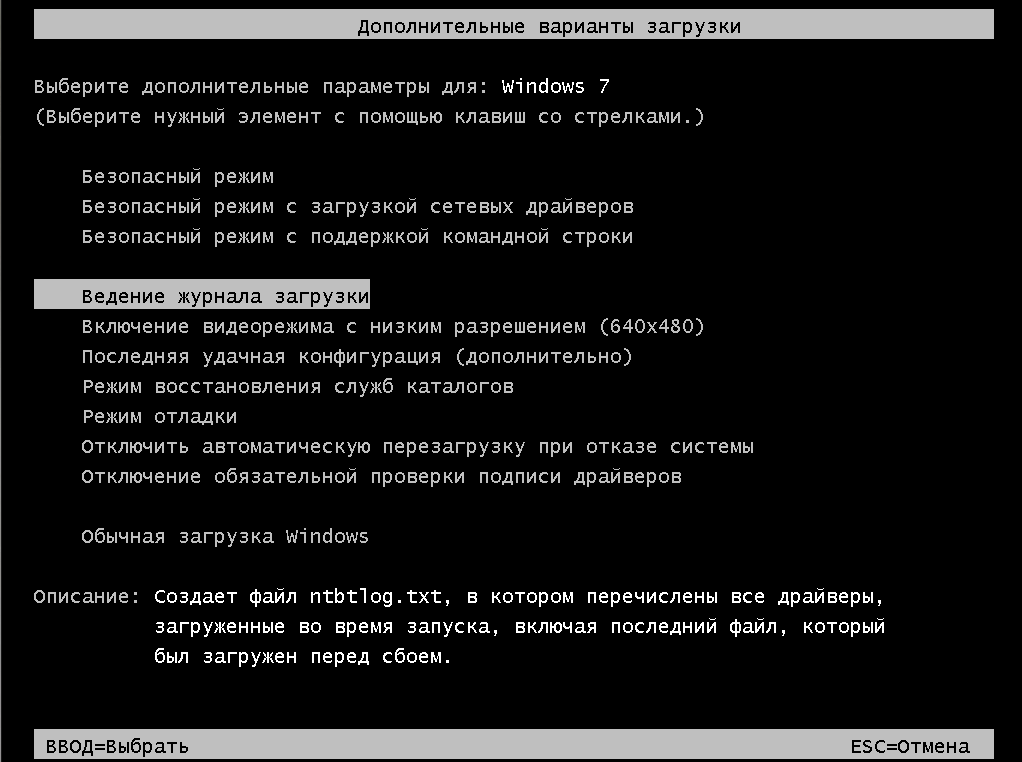
В каталоге Boot находится база хранилища конфигураций загрузки BCD, файлы для логов и папки с языковыми файлами.

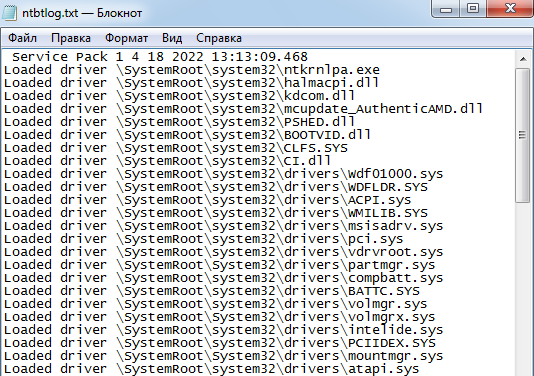


Раздел диска, который содержит загрузчик, называется системным диском, а раздел, содержащий основные файлы операционной системы – загрузочным. Системный и загрузочный диски могут находится на одном или разных физических дисках.

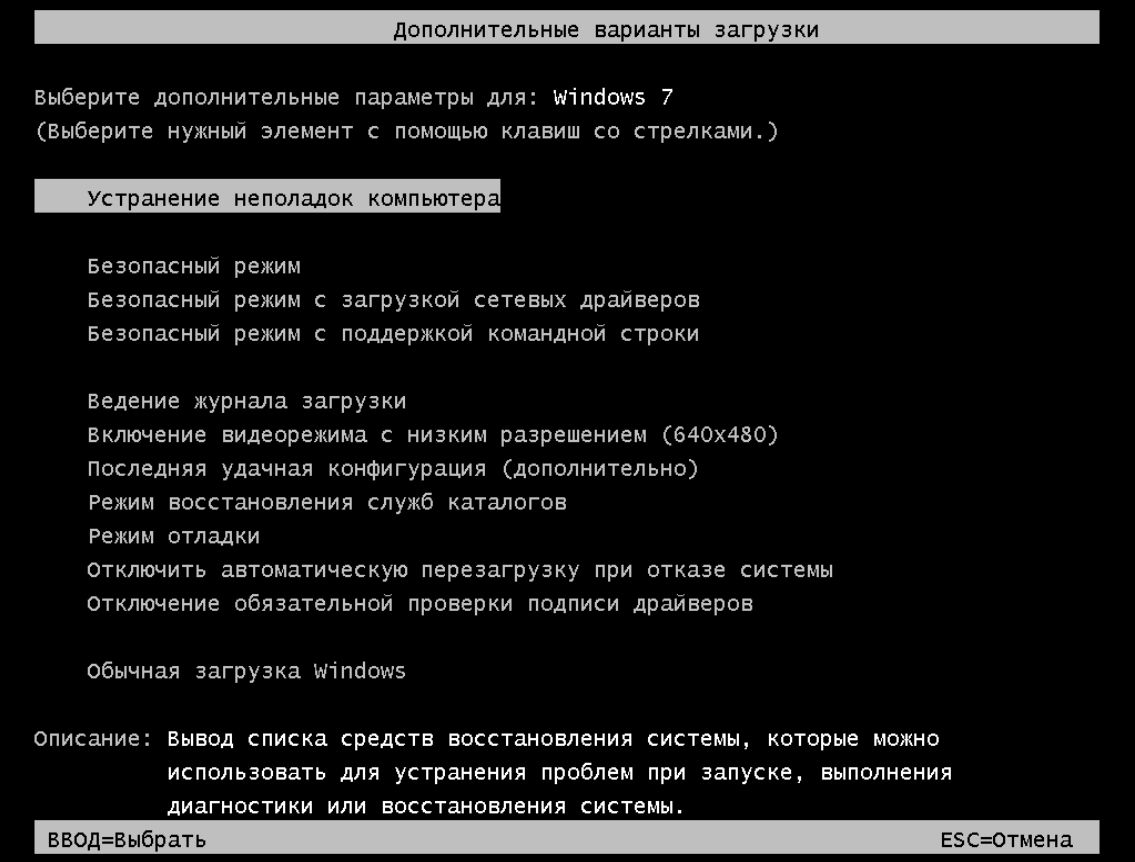
Загрузка с протоколированием журнала загрузки драйверов

Для перехода к вариантам загрузки необходимо нажать клавишу F8 до загрузки в операционную систему. Выберем пункт «Ведение журнала загрузки». При загрузке в данном режиме будет создан файл C:\Windows\ntbtlog.txt с описанием драйверов, загруженных во время запуска.





Стартовое меню.



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

Устранение неполадок компьютера

Вывод списка средств восстановления системы, которые можно использовать для устранения проблем при запуске, выполнения диагностики или восстановления системы.

Безопасный режим

Запуск Windows только с основными драйверами и службами. Применяется при невозможности загрузки после установки нового устройства.

Безопасный режим с поддержкой сетевых драйверов.

Запуск Windows только с драйверами и поддержкой сети.

Безопасный режим с поддержкой командной строки.

Запуск Windows только с драйверами, с последующим запуском командной строки.

Ведения журнала загрузки.

Создает файл ntbtlog.txt, в котором перечислены все драйверы, загруженные во время запуска, включая последний файл, который был загружен перед сбоем.

Включение видеорежима с низким разрешением (640х480)

Установка или сброс разрешения экрана. Запуск Windows в режиме низкого разрешения экрана (640 x 480).

Последняя удачная конфигурация (дополнительно)

Запуск системы Windows с использованием параметров последней успешной загрузки.

Система хранит как минимум два контрольных набора параметров. Один из них, загрузка в который выполнена в данный момент, помечается как текущий и стандартный. Еще один набор считается резервным и применяется для загрузки в последнюю удачную конфигурацию.

Настройки хранятся в разделе HKEY\_LOCAL\_MACHINE\System:

* CurrentControlSet – текущий набор параметров, с которыми загрузилась Windows. На самом деле этот раздел виртуальный. В зависимости от ситуации, в нем отображаются параметры одного из нумерованных наборов ControlSet00N.
* ControlSet001, ControlSet002 и т.д. – наборы параметров, работоспособность которых может варьироваться, как вы увидите ниже.

Режим восстановления служб каталогов

Запуск системы Windows в режиме восстановления служб каталогов (только для контроллеров домена Windows).

Режим отладки

Включение отладчика ядра Windows.

Отключить автоматическую перезагрузку при отказе системы

Запрет автоматической перезагрузки Windows после сбоя.

Отключение обязательной проверки подписи драйверов

Разрешает загрузку драйверов, содержащих неверную подпись.

Обычная загрузка Windows

Запуск Windows с обычными параметрами.

Сравнение возможностей ОС при нормальной загрузке, в безопасном режиме и режиме командной строки.

Для сравнения возможностей ОС, необходимо узнать какие драйверы будут загружены при запуске, какие службы и процессы будут активны. Состояние загрузки драйверов будем наблюдать в файле ntbtlog. Процессы и службы в графическом режиме можно отобразить с помощью диспетчера задач, в режиме командной строки активные процессы можно узнать с помощью команды tasklist, службы с помощью команды sc.

Загружаемые драйверы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Драйвер** | **Описание драйвера** | **Нормальный режим** | **Безопасный режим** | **Командная строка** |
| ntkrnlpa.exe | системный файл ядра Windows | + | + | + |
| halmacpi.dll | Hardware Abstraction Layer – уровень абстракции оборудования | + | + | + |
| kdcom.dll | Kernel-Mode driver –драйвер режима ядра | + | + | + |
| PSHED.dll | platform-specific hardware error driver -драйвер аппаратных ошибок | + | + | + |
| BOOTVID.dll | VGA Boot Driver - Загрузочный драйвер VGA | + | + | + |
| CI.dll | Code Integrity – целостность кода ОС | + | + | + |
| ACPI.sys | Поддержка управления питанием и перечисление устройств Plug and Play | + | + | + |
| pci.sys | Функциональный драйвер для шины PCI | + | + | + |
| vdrvroot.sys | Драйвер виртуальных дисков | + | + | + |
| partmgr.sys | Драйвер разделов диска | + | + | + |
| compbatt.sys | Composite Battery Driver – драйвер батареи | + | + | + |
| volmgr.sys | Volume Manager Driver - Драйвер диспетчера томов | + | + | + |
| intelide.sys | Intel PCI IDE Driver – драйвер IDE устройств | + | + | + |
| mountmgr.sys | Mount Point Manager (Менеджер монтирования) – упрвление именами томов | + | + | + |
| msahci.sys | Microsoft AHCI Driver – подключение накопителей информации стандарта SATA | + | + | + |
| fltmgr.sys | Microsoft Filesystem Filter Manager | + | + | + |
| Ntfs.sys | Драйвер файловой структуры NTFS | + | + | + |
| ksecdd.sys | Kernel Security Support Provider Interface - поддержка удаленного прямого доступа к памяти в режиме ядра в сетевом адаптере | + | + | + |
| NETIO.SYS | Network I/O Subsystem – подсистема сетевого ввода вывода | + | + | + |
| tcpip.sys | Драйвер стека протоколов TCP/IP | + | + | + |
| hwpolicy.sys | Hardware Policy Driver – политика загрузки драйверов | + | + | + |
| usbhub.sys | Драйвер usb устройств | + | + | + |
| vga.sys | Видеодрайвер VGA | + | + | + |
| cdrom.sys | Драйвер дисковода | + | + | + |
| tdx.SYS | TDI Translation Driver- общий интерфейс для драйверов, предназначенный для общения с различными сетевыми транспортными протоколами. | + | - | - |
| AFD.SYS | Ancillary Function Driver for WinSock - драйвер сокета ОС. | + | - | - |
| NetBIOS.SYS | NetBIOS interface driver – драйвер службы NetBIOS | + | - | - |
| TermDD.SYS | Terminal Desktop Server Driver –драйвер терминального сервера | + | - | - |
| rdbss.SYS | Redirected Drive Buffering SubSystem Driver – подсистема буферизации перенаправленного диска | + | - | - |
| nsiproxy.SYS | NSI Proxy Service Driver – драйвер прокси сервера | + | - | - |
| discache.SYS | Cache Driver | + | - | - |
| CSC.SYS | Windows Client Side Caching Driver | + | - | - |

При запуске ОС первыми запускаются файлы ядра системы и файл уровня абстракции оборудования. Драйвера, запускаемые в безопасном режиме и режиме командной строки:

* драйвер PCI шины;
* драйвер контролеров SATA для подключения жестких дисков
* драйвер дисководов компакт-дисков (CD, DVD);
* драйвер контроллеров USB;
* видеодрайвер VGA.

Это минимальный набор драйверов, который необходим для запуска Windows.

При запуске в нормальном режиме дополнительно запускаются драйвера, связанные с сетевыми функциями.

Загружаемые службы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Служба** | **Описание службы** | **Нормальный режим** | **Безопасный режим** | **Командная строка** |
| CryptSvc | Службы криптографии | + | + | + |
| DcomLaunch | Модуль запуска процессов DCOM-сервера | + | + | + |
| eventlog | Журнал событий Windows | + | + | + |
| PlugPlay | Plug-and-Play | + | + | + |
| Power | Питание | + | + | + |
| ProfSvc | Служба профилей пользователей | + | + | + |
| RpcSs | Удаленный вызов процедур (RPC) | + | + | + |
| RpcEptMapper | Сопоставитель конечных точек RPC | + | + | + |
| WinDefend | Защитник Windows | + | + | + |
| wscsvc | Центр обеспечения безопасности | + | + | - |
| wuauserv | Центр обновления Windows | + | + | - |
| AeLookupSvc | Информация о совместимости приложений | + | - | - |
| Appinfo | Сведения о приложении | + | - | - |
| AudioEndpointBuilder | Средство построения конечных точек Windows Audio | + | - | - |
| Audiosrv | Windows Audio | + | - | - |
| BFE | Служба базовой фильтрации | + | - | - |
| BITS | Фоновая интеллектуальная служба передачи | + | - | - |
| Browser | Браузер компьютеров | + | - | - |
| CscService | Автономные файлы | + | - | - |
| Dhcp | DHCP-клиент | + | - | - |
| DPS | Служба политики диагностики | + | - | - |
| EventSystem | Система событий COM+ | + | - | - |
| fdPHost | Хост поставщика функции обнаружения | + | - | - |
| FDResPub | Публикация ресурсов обнаружения функции | + | - | - |
| FontCache | Служба кэша шрифтов Windows | + | - | - |
| gpsvc | Клиент групповой политики | + | - | - |
| HomeGroupProvider | Поставщик домашней группы | + | - | - |
| iphlpsvc | Вспомогательная служба IP | + | - | - |
| lmhosts | Модуль поддержки NetBIOS через TCP/IP | + | - | - |
| MMCSS | Планировщик классов мультимедиа | + | - | - |
| MpsSvc | Брандмауэр Windows | + | - | - |
| Netman | Сетевые подключения | + | - | - |
| netprofm | Служба списка сетей | + | - | - |
| NlaSvc | Служба сведений о подключенных сетях | + | - | - |
| nsi | Служба интерфейса сохранения сети | + | - | - |
| p2pimsvc | Диспетчер удостоверения сетевых участников | + | - | - |
| PNRPsvc | Протокол PNRP | + | - | - |
| SamSs | Диспетчер учетных записей безопасности | + | - | - |
| Schedule | Планировщик заданий | + | - | - |
| SENS | Служба уведомления о системных событиях | + |  |  |
| SSDPSRV | Обнаружение SSDP | + | - | - |
| upnphost | Узел универсальных PNP-устройств | + | - | - |
| UxSms | Диспетчер сеансов диспетчера окон рабочего стола | + | - | - |
| WdiServiceHost | Узел службы диагностики | + | - | - |

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;
* Сервисы Windows для настройки операционной системы.

Сетевые сервисы и службы, которые остановлены в безопасном режиме и могут быть активированы:

* 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.

При запуске в нормальном режиме дополнительно активируются службы, позволяющие полноценно использовать ОС, например, включается служба, отвечающая за звук.

Загруженные процессы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Процесс** | **Описание процесса** | **Нормальный режим** | **Безопасный режим** | **Командная строка** |
| smss.exe | Диспетчер сеанса Windows | + | + | + |
| csrss.exe | Процесс исполнения клиент-сервер | + | + | + |
| winlogon.exe | Программа входа в систему Windows | + | + | + |
| service.exe | Приложение служб и контроллеров | + | + | + |
| lsass.exe | Local Security Authority Process | + | + | + |
| winint.exe | Автозагрузка приложений Windows | + | + | - |
| scvhost.exe | Хост-процесс для служб Windows | + | + | - |
| explorer.exe | Проводник | + | + | - |
| dwm.exe | Диспетчер окон рабочего стола | + | - | - |

Основные для ОС процессы запущены во всех трёх режимах. В режиме командной строки нет процессов, связанных с графической оболочкой и автозагрузкой приложений. В безопасном режиме не активен процесс диспетчера окон рабочего стола.

Вывод по возможностям режимов

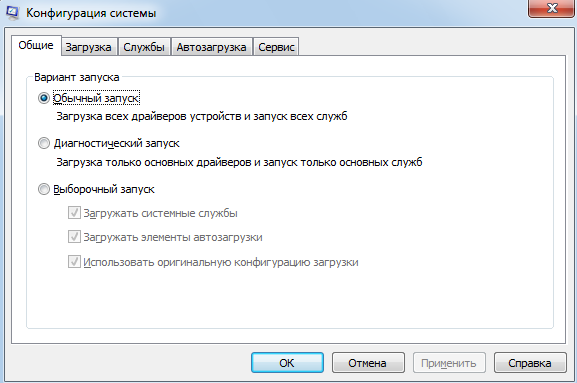
Безопасный режим запускает компьютер с минимально необходимым набором драйверов и служб. Все сторонние программы отключаются, и даже системные инструменты ограничены только необходимым набором функций.

Безопасный режим – хороший способ избавиться от вредоносных программ, блокирующих загрузку или работу компьютера. Он также обеспечивает среду, в которой можно «откатить» обновления системы или драйверов, очистить автозагрузку, удалить недавно установленные программы или провести диагностику и устранение неполадок Windows.

Безопасный режим с поддержкой командной строки обеспечивает большее быстродействие путём отключения графического интерфейса. Если пользователь умеет обращаться с командной строкой и знает её команды, то восстановление системы лучше проводить в этом режиме.

Утилита 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.



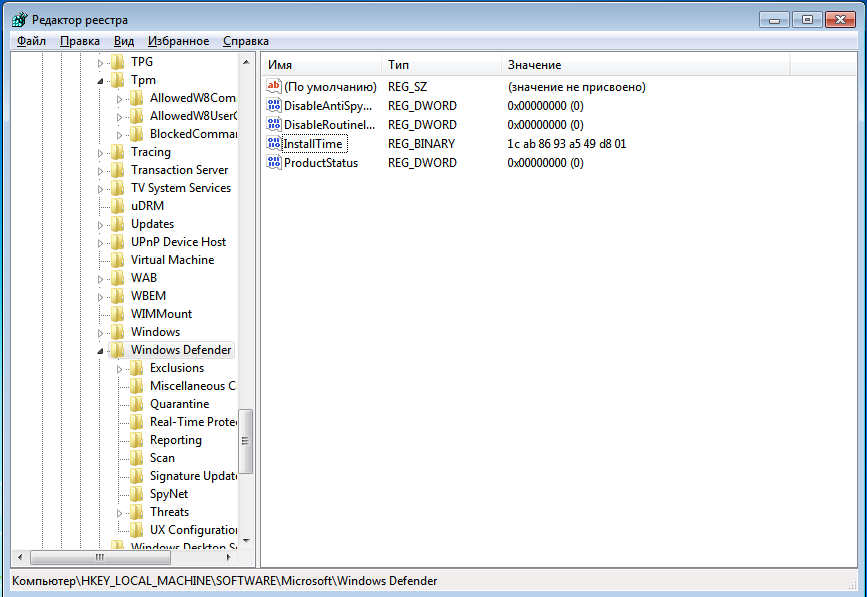
Описание возможностей программы

* На вкладке «Общие» есть возможно выбирать вариант загрузки: обычный, диагностический или выборочный.
* В разделе «Загрузка» можно настроить дополнительные параметры запуска ОС. Например, количество процессоров (ядер), количество памяти, включе-ние/отключение журнала загрузки, наличие графического интерфейса.
* На вкладке «Службы» можно отключить ненужные службы, запускаемые при загрузке системы. Многие программы, такие как антивирусы и программы безопас-ности компьютера, запускаются через службы операционной системы. В случае отключе-ния служб такие программы могут перестать работать.
* Вкладка «Автозагрузка» отвечает за загрузку приложений (программ) а также определённых служебных утилит, загружаемых не через службы.

Пути в реестре

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

Ключи для работы Windows Definder:



* [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] – программ, которые запускаются только один раз при входе пользователя в систему (раздел отвечает за запуск программ для всех пользователей системы). После этого ключи программ автоматически удаляются из данного раздела реестра.
* [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx] – программы, которые запускаются только один раз, когда загружается система (раздел отвечает за запуск программ для всех пользователей системы). Этот раздел используется при инсталляции программ, например, для запуска настроечных модулей. После этого ключи программ автоматически удаляются из данного раздела реестра.
* [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.

Архитектура Windows. Состав и функции основных компонентов.

Основные системные каталоги

* Каталог **Program Files** содержит папки с программами, установленными как в процессе инсталляции Windows, так и пользователями компьютера. Для каждой программы отведена отдельная папка. Если после удаления программы с компьютера, ее папка остается, то рекомендуется вручную удалить ее из каталога Program Files. Иначе при частой инсталляции и удалении программ в данной папке может накопиться изрядное количество мусора.
* Папка **ProgramData** является скрытой, служит хранилищем общих данных, например, настроек различных приложений. К информации, сохраненной в ней, могут обращаться все пользователи, независимо от наличия или отсутствия у них прав администратора. Данную папку удобно использовать, например, чтобы хранить в ней шаблоны для программ по редактированию фотографий, видео, общие документы и так далее.
* **Recovery** – хранится образ, необходимый для входа в среду восстановления.
* Папка **System Volume Information** по умолчанию является скрытой. Программа восстановления системы Windows создает в ней копии реестра. Т.е. здесь хранятся каталоги точек восстановления системы, отсортированные по дате создания. Windows не позволяет просматривать содержимое каталога System Volume Information обычным способом. Размер данной папки зависит от объема дискового пространства, резервируемого системой под точки восстановления.
* Каталог **Windows** – самая важная папка, размещающаяся на активном разделе жесткого диска. В ней хранятся все исполняемые файлы операционной системы, драйвера, модули и пр.
* **Windows.old** – папка со старой операционной системой. Возникает на жестком диске, если установка Windows была осуществлена без форматирования. Для подавляющего большинства пользователей она не нужна, а поэтому может быть удалена.
* **Users** – хранение профилей пользователей. По умолчанию размещается в корне диска с операционной системой. Содержит ряд стандартных папок, а также по одной папке на каждую учетную запись. В них находятся «пользовательские» подпапки, включая рабочий стол (Desktop), документы (Documents), картинки (Pictures), избранное (Favorites) и пр. Другие подпапки используются для хранения служебной информации различных приложений, браузеров и пр., они скрытые, и изменять их содержимое вручную не рекомендуется.
* **$Recycle.Bin** – папка является «Корзиной» Windows. Именно в нее перемещается вся удаляемая информация. Папка скрытая, однако, удалять можно как ее саму, так и ее содержимое. По сути, это будет равносильно очистке «Корзины» или ее части. На каждом разделе жесткого диска есть своя папка $Recycle.Bin, в которой хранятся файлы, удаленные именно с него.
* **C:\Windows\System32** – каталог содержит данные операционной системы, драйверов, данные реестра, утилиты для работы с системой.
* **C:\Windows\Temp** – каталог, содержащий временные файлы приложений.
* **C:\Users\ <Имя пользователя> \AppData** – папка содержит данные, относящиеся к учетной записи. Обычно включает в себя параметры конфигурации, которые относятся к вашему экземпляру установленной программы.

Основные системные файлы

Файлы реестра Windows:

* C:\Documents and Settings\Имя Пользователя\ntuser.dat – является кустом реестра Windows HKEY\_USERS/SID
* C:\Windows \system32\config\SAM – содержит раздел реестра HKLM\SAM
* C:\Windows\system32\config\SECURITY – содержит раздел реестра HKLM\SECURITY
* C:\Windows\system32\config\software – содержит раздел реестра HKLM\Software
* C:\Windows\system32\config\system – содержит раздел реестра HKLM\System

Другие системные файлы:

* C:\Windows\system32\config\AppEvent.Evt – является журналом событий приложений, используемым реестром операционной системой Windows.
* C:\Windows\system32\drivers\etc\hosts – предназначен для сопоставления IP-адресов и имен компьютеров.
* C:\Windows\system32\mydocs.dll – отвечает за пользовательский интерфейс папки "Мои документы"
* C:\Windows\system32\config\SecEvent.Evt – является журналом событий безопасности, используемым реестром Windows
* C:\Windows\WindowsUpdate.log – файл, содержащий историю автоматического обновления.
* C:\Windows\ ntbtlog.txt – Файл протоколирования загрузки ОС.

Установка, выполнение и удаление приложение

DOS – приложения

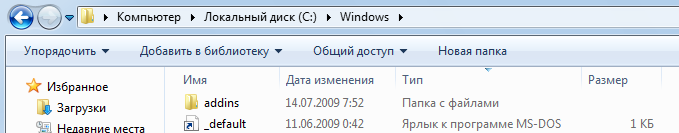
Установка DOS-программ сводится к размещению на диске, формированию переменных окружения (если для программы это необходимо). Для каждого приложения DOS ОС создает отдельную VDM. VDM работают в режиме вытесняющей многозадачности, деля процессорное время с системной виртуальной машиной. VDM не создают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

Загрузкой MS-DOS приложений можно управлять с помощью .pif файла, который является ярлыком на DOS программу.

В PIF-файле описываются параметры выполнения программы:

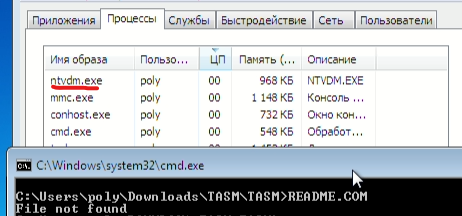
* режим выполнения (экранный или оконный)
* ресурсы памяти
* установки приоритетов для планирования процессов

В каталоге C:\Windows есть файл \_default.pif, который является стандартным ярлыком для DOS программ. Если для программы не создан отдельный ярлык, то она запускается с параметрами, указанными в этом файле.



Запустим DOS программу, написанную в рамках второй лабораторной курса ПиМОСПС 5 семестра. Чтобы убедиться в том, что запущена Виртуальная DOS Машина, запустим диспетчер. задач.

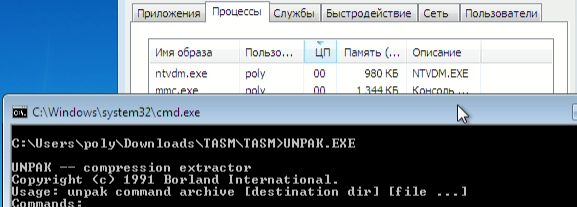
Процесс ntvdm.exe является процессом виртуальной машины.



Win16-приложения

Приложения Win16 выполняются в Windows 7 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.

Варианты установки

Установка вручную — установка выполняется без установщика или со значительным количеством операций, вручную выполняемых пользователем.

«Тихая» установка — установка, в процессе которой не отображаются сообщения или окна.

Автоматическая установка — установка, которая выполняется без вмешательства со стороны пользователя, исключая сам процесс её запуска. Процесс установки иногда требует взаимодействия с пользователем, который управляет процессом установки, делая выбор: принимая пользовательское соглашение, настраивая параметры, указывая пароли и так далее.

Этапы установки с помощью инсталлятора

1. Анализ возможностей установки
   1. Версия ОС – разрядность процессора
   2. Состав требуемого оборудования
   3. Наличие памяти на диске
2. Проверка лицензии
3. Проверка целостности с помощью цифровых подписей
4. Подготовка и копирование файлов
5. Регистрация в реестре
6. Установка в интерфейсе пользователя
7. Установка параметров автозапуска
8. Возможность отмены установки

Типы инсталляторов

Наиболее часто используются следующие типы инсталляторов:

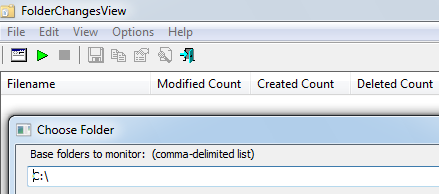
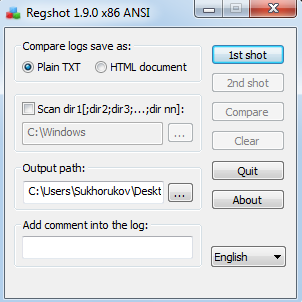
1. InstallShield
2. Windows Installer Service (\*.msi)
3. InstallShield с MSI
4. Inno Setup
5. Nullsoft SuperPiMP Install System (NSIS)
6. WISE Installer

Установка приложения

Установим приложение Notepad++ (приложение для удобного редактирования исходного кода программ) и определим, какие изменения вносятся в файловую систему и реестр. Для проверки состояния реестра используем программу Regshot, файловой системы – FolderChanhesView.

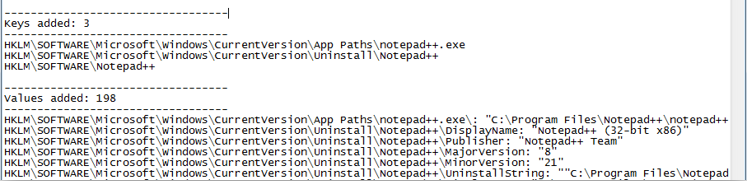
В программе Regshot сделаем снимок состояния реестра «1st shot», после установки приложения 7Zip сделаем второй снимок «2nd shot» и сравним состояния «Compare».

В программе FolderChanhesView в качестве каталога, состояние которого будет отслеживаться выберем корень диска С, после начала слежения в интерфейсе программы будут отображаться изменения.



Изменение в реестре

Результатом работы приложения Regshot является текстовый файл ~res-x86.txt, в котором описаны добавленные ключи и поля, измененные значения полей.



Добавлены ключи в разделы HKEY\_LOCAL\_MACHINE\SOFTWARE – раздел данных об установленных приложениях - и HKEY\_USERS\_S-1-5-21-4114… - раздел данных о пользователе.

Основными ключами являются:

HKLM \SOFTWARE \Microsoft \Windows \CurrentVersion \App Paths \notepad++.exe\: "C:\Program Files\Notepad++\notepad++.exe" – ключ, по котором храниться путь к исполняемому файлу.

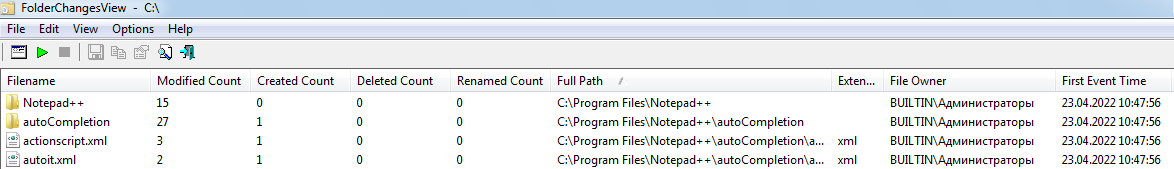
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Notepad++ – ключ, по которому хранится информация об удалении приложения.

HKLM\SOFTWARE\Notepad++\: "C:\Program Files\Notepad++" - указание пу-ти, по которому расположено приложение.

HKU \S-1-5-21-4114700349-3829428303-2104194-1001 \Software \Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\C: \Users\poly\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Notepad++.lnk: 0x00000001 – добавление приложения в интерфейс пользователя (Меню «Windows» -> «Все программы» -> «7Zip»).

Изменения в файловой системе

Результатом работы приложения FolderChanhesView является список каталогов и файлов, которые были изменены или добавлены.



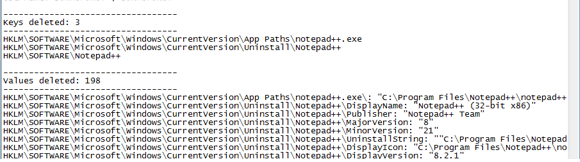
Изменения каталогов:

* C:\Program Files\Notepad++ – каталог, в котором установлено приложения, где находятся его исполняемый файл и необходимые для работы ресурсы.
* C:\ProgramData\Microsoft\Windows\Start Menu\Programs - добавление приложения в интерфейс пользователя (Меню «Windows» -> «Все программы» -> «7Zip»).
* C:\Users\poly\AppData\Roaming – добавление пользовательских настроек для приложения. При использовании данной учётной записи пользователя на другом компьютере, настройки приложения будут сохранены.
* C:\Users\poly\AppData\Local\ – добавление локальных пользовательских настроек приложения. Настройки сохраняются только на одном компьютере.
* C:\Users\poly\AppData\Local\Temp – добавление временных файлов настроек приложения.
* C:\Windows\Temp – добавление временных файлов приложения.
* C:\Users\poly\NTUSER.DAT – изменение файла реестра пользователя.
* C:\Windows\System32\config\SOFTWARE – изменение файла реестра.
* C:\Windows\System32\config\SYSTEM– изменение файла реестра.

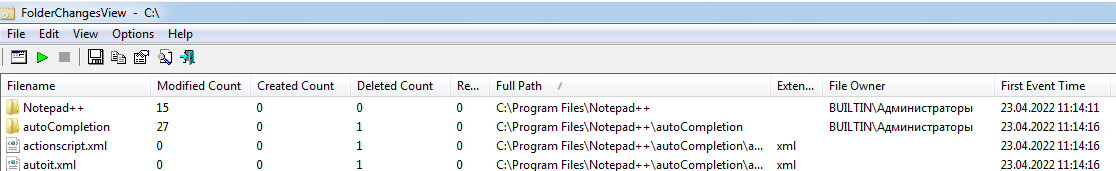
Удаление приложения

Изменения в реестре

Программа Regshot зафиксировала удаление всех, созданных при установке ключей.



Созданные каталоги, подкаталоги и временные файлы были удалены.



Программа удалилась полностью и не оставила после себя никаких файлов и «мусора».

Графический интерфейс

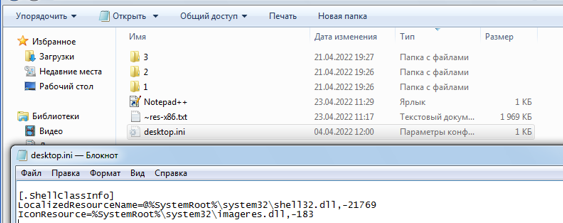
ОС Windows строится на методологии объектного подхода, в соответствии с которым весь мир и любая его часть рассматривается как совокупность объектов. Объекты обладают определенными свойствами и поведением. Причём разные объекты обладают разными свойствами и поведением.

Основными элементами графического интерфейса ОС Windows являются следующие объекты: Рабочий стол, окна, значки, ярлыки, кнопки, панели, меню, папки, приложения и документы.

Рабочий стол

Рабочим столом называется основной элемент графического интерфейса, который обеспечивает эффективный доступ пользователя ко всем ресурсам компьютера, к наиболее часто используемым программам, документам и аппаратным средствам.

Ярлыки, каталоги и файлы, отображаемые на рабочем столе, находятся в каталоге C:\Users\<username>\Desktop. Так же в этом каталоге находится файл конфигурации desktop.ini.

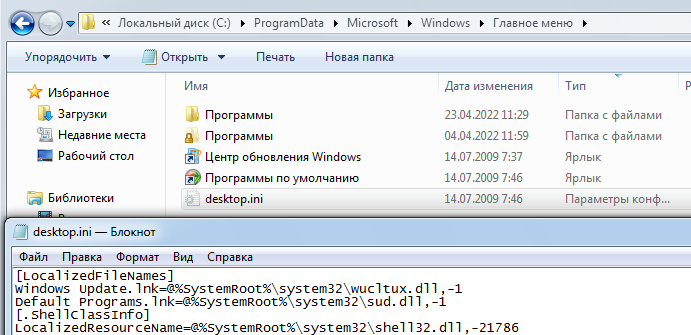
\

Главное меню

Меню называется элемент интерфейса пользователя, представляющий собой список альтернативных вариантов команд, действий режимов, установок и т.д., из которых пользователь может выбрать только один вариант. Отдельные варианты, из которых состоит список принято называть пунктами или строками меню.

Главное меню отображается при нажатии на значок Windows или нажатием соответствующей клавиши на клавиатуре.

Каталог главного меню - C:\ProgramData\Microsoft\Windows\Start Menu. В подкаталоге «Programs» отображается список установленных программ. В файле desktop.ini находятся пути, на которое ссылаются ярлыки.



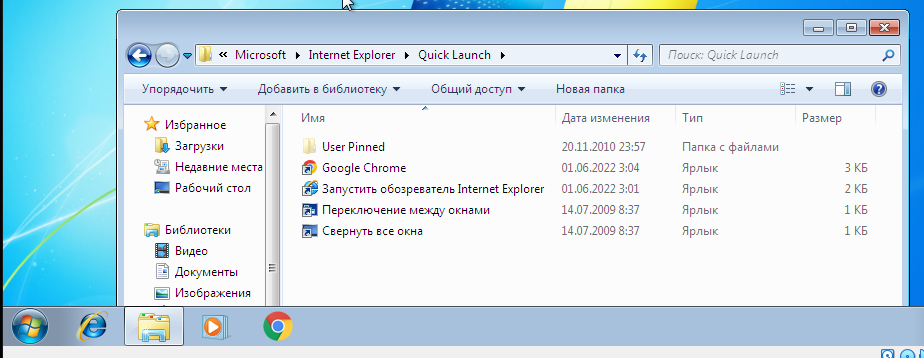
Через главное меню можно зайти в панель управления и папки текущего пользо-вателя. Утилиты, доступные в панели управления хранятся в каталогах C:\Windows\winsxs и C:\Windows\System32, каталоги текущего пользователя - C:\Users\<username>.

Панель задач

Панелью называется элемент графического интерфейса пользователя, который служит для объединения группы логически взаимосвязанных значков, элементов управления и индикаторов состояния операционной системы или выполняющей программы.

Панель задач располагается внизу рабочего стола. На ней отображаются запущенные приложения, ярлыки, по которым можно быстро открыть приложение, настройки времени, языка и сети.

Закрепленные ярлыки находятся в каталоге C:\Users\<username>\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar.



Программы, настройки времени, сети и языка находятся в каталоге C:\Windows и подкаталоге \System32.

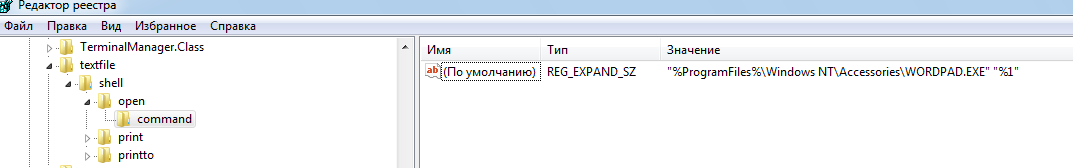
Контекстное меню

Контекстное меню — элемент графического интерфейса операционной системы, представляющий собой список команд, вызываемый пользователем для выбора необходимого действия над выбранным объектом. Команды контекстного меню относятся к тому объекту, над которым это меню было вызвано.

Контекстное меню папок и файлов Проводника, которое содержит такие команды, как "Открыть", "Изменить", "Открыть с помощью", "Создать" (с выбором типа файла) и т.д. Оно может быть изменено путём настройки некоторых разделов реестра.

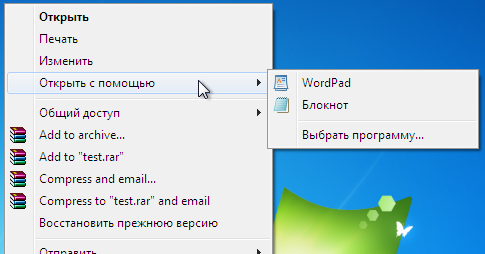
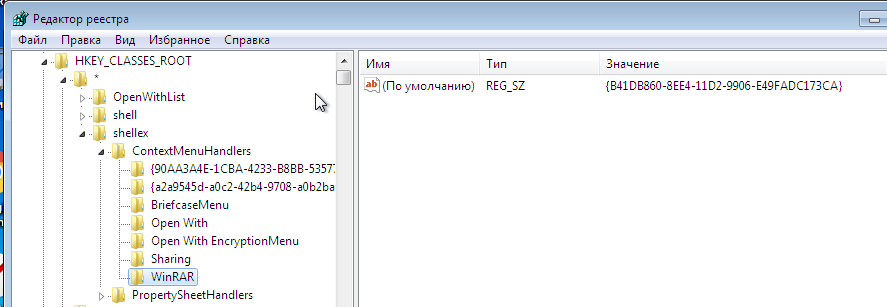
Информация о каждом зарегистрированном типе файлов и командах, применимых к нему, хранится в ветви реестра HKEY\_CLASSES\_ROOT. Каждому зарегистрированному типу файлов соответствуют два подраздела в разделе HKEY\_CLASSES\_ROOT. Первый подраздел имеет название, соответствующее расширению имени файла. В своём значении "по умолчанию" этот подраздел содержит идентификатор, который используется как название второго подраздела. Во втором подразделе хранятся описания команд, применяемых к данному типу файлов.

Например, текстовому типу файлов в реестре соответствуют два подраздела - ".txt" и "txtfile". Подраздел shell раздела "txtfile" содержит в себе подразделы, определяющие действия над данным типом файлов. Каждый подраздел-глагол может содержать подраздел command. Этот подраздел содержит командную строку в параметре "по умолчанию". Параметр "%1" в командной строке будет заменён путём и именем выбранного файла.



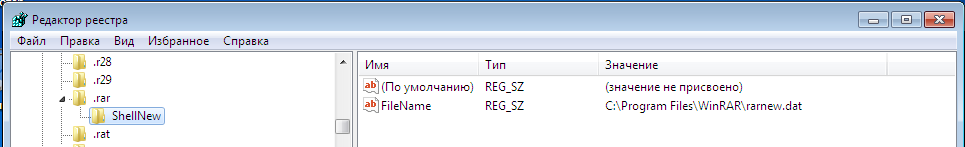
Информация, относящаяся одновременно ко всем типам файлов, хранится в подразделе "\*" ветви реестра HKEY\_CLASSES\_ROOT. Информация, относящаяся ко всем незарегистрированным типам файлов, хранится в подразделе "Unknown" ветви реестра. Информация, относящаяся к папкам, хранится в подразделах "Directory" и "Folder" ветви реестра.

На компьютере Sukhorukov-1 установлено 3 программы, которые добавили свои действия в контекстное меню: Winrar. Информацию об этих действиях можно увидеть в реестре



Ассоциация файлов

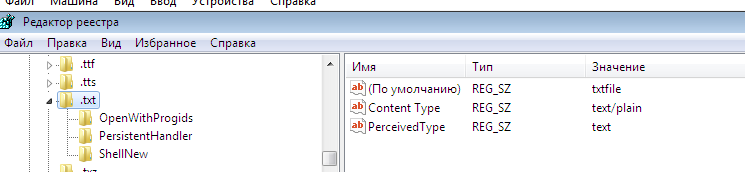
Файлы одного типа могут быть открыты разными программами. Информация о доступных программа записана в реестре. Подраздел с названием типа файла, например, .rar содержит информацию о программах, которыми можно открыть данный тип файла.



Как видим, есть 1 подключ:

ShellNew – возможность создать данный тип файла через меню «Создать».

Однако, если рассмотреть тип данных .txt, то увидим еще 2 новый ключа:



OpenWithProgIds – идентификаторы программы, которыми можно открыть данный тип файла.

PersistendHandler (Постоянный обработчик) – программа, которая выбрана приоритетной для данного типа файла.

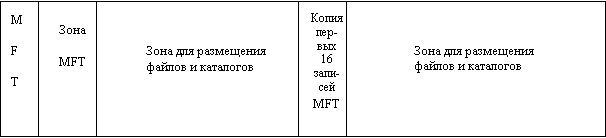
Базовые свойства файловой структуры NTFS

Структура тома с файловой системой NTFS.

Раздел NTFS называется томом (volume). Максимально возможные размеры тома (и размеры файла) составляют 16 Эбайт (264) (для MBR том ограничен 2ТБ, для GPT – 255 ТБ).

Как и многие другие системы, NTFS делит дисковое пространство тома на кластеры — блоки данных, адресуемые как единицы данных. NTFS поддерживает размеры кластеров от 512 байт до 64 Кбайт; стандартом же считается кластер размером 2 или 4 Кбайт.

Все дисковое пространство в NTFS делится на две неравные части.



Первые 12 % диска отводятся под так называемую MFT-зону — пространство, которое может занимать, увеличиваясь в размере, главный служебный метафайл MFT.

Запись каких-либо данных в эту область невозможна. MFT-зона всегда держится пустой — это делается для того, чтобы MFT-файл по возможности не фрагментировался при своем росте.

Остальные 88 % тома представляют собой обычное пространство для хранения файлов. в отличие от FAT, при заполнении всего выделенного пространства, MFT-зона начинает сжиматься, а на освободившееся место пишутся новые данные.

Каждый файл в файловой системе NTFS представляет собой файл, даже MFT. MFT является централизованным каталогом всех файлов на диске, в том числе и себя самого. MFT поделен на зоны фиксированного размера, каждая из которых соответствует файлу. Первые 16 файлов (в том числе и MFT)— метафайлы, они фиксированы. Также копия 16 первых метафайлов хранится посередине диска в отличие от FAT, где копия таблицы FAT хранится сразу после оригинальной. Метафайлы имеют в начале названия знак $ и для них указан реальный размер.

|  |  |
| --- | --- |
| **Метафайл** | **Назаначение** |
| $MFT | сам MFT |
| $MFTmirr | копия первых 16 записей MFT, размещенная посередине диска |
| $LogFile | файл поддержки журналирования (см. ниже) |
| $Volume | служебная информация - метка тома, версия файловой системы, т.д. |
| $AttrDef | список стандартных атрибутов файлов на томе |
| $. | корневой каталог |
| $Bitmap | карта свободного места тома |
| $Boot | загрузочный сектор (если раздел загрузочный) |
| $Quota | файл, в котором записаны права пользователей на использование дискового пространства (начал работать лишь в NT5) |
| $Upcase | файл - таблица соответствия заглавных и прописных букв в именах файлов на текущем томе. Нужен в основном потому, что в NTFS имена файлов записываются в Unicode, что составляет 65 тысяч различных символов, искать большие и малые эквиваленты которых очень нетривиально. |

В MFT хранится вся информация о файле, кроме самих данных: имя, размер, положение на диске фрагментов и т. д. Если не хватает одной записи, используется несколько. Имя файла может содержать максимум 255 символов и кодируется UTF-16. Также в таблице могут появляться и «опциональные элементы» - потоки данных файла. Если файл не имеет данных или настолько мал, что помещается в самой записи, то данные помещаются прямо в запись.

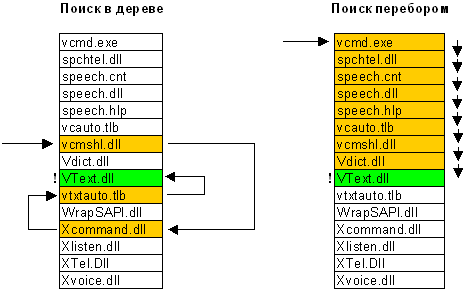
Атрибуты файлов

Стандартные атрибуты для файлов и каталогов в томе NTFS имеют фиксированные имена и коды типа.

|  |  |
| --- | --- |
| Атрибут | Описание |
| Standart Information | Содержит такую стандартную информацию, как дата создания и число ссылок |
| Attribute List | Список местонахождения всех атрибутов, размещенных вне записи MTF |
| File Name | Повторяющийся атрибут для длинных и коротких имен файлов. Длинное имя файла состоит из 13 – 255 символов Unicode, короткое представлено в формате 8.3. Возможно использование дополнительных имен, например, в формате Posix |
| Security Descriptor | Информация о том, кто является владельцем файла, и кто имеет доступ к файлу |
| Data | Данные, содержащиеся в файле. NTFS позволяет использовать более одного атрибута этого типа для каждого файла. Каждый файл обычно имеет наименованный атрибут типа Data. Помимо этого, файл может иметь дополнительные именованный атрибуты данного типа, каждый из которых использует собственный синтаксис. |
| Object ID | Уникальный в рамках тома идентификатор файла. Используется сервисом слежения за ссылками |
| Logged Tool Stream | Схож с потоковыми операциями, но в данном случае изменения заносятся в протокол. Используется Encrypting File System (EFS) – файловой системой с шифрованием, поддерживаемой в Windows 2000. |
| Reparse Point | Использование при монтировании томов, драйверами – фильтрами и в ряде других случаев |
| Index Root | Используется для реализации каталогов и других индексов |
| Index Allocation | Используется для реализации каталогов и других индексов |
| Bitman | Используется для реализации каталогов и других индексов |
| Volume Information | Используется только в системном файле $Volume. Содержит версию тома |
| Volume Name | Используется только в системном файле $Volume. Содержит метку тома. |

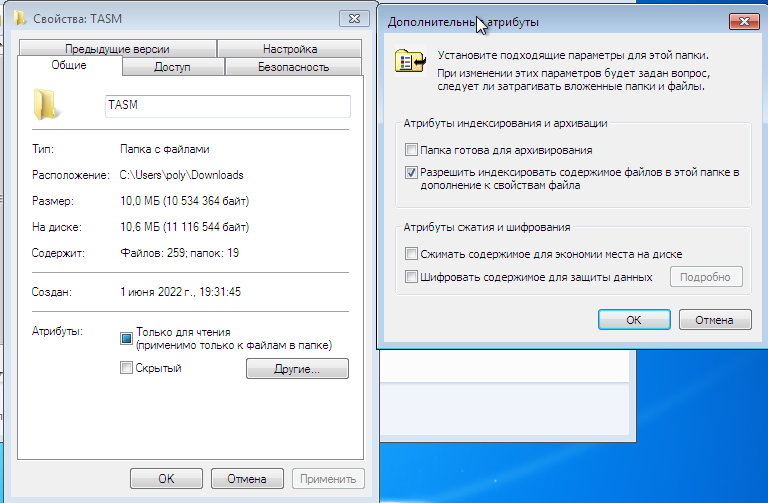
Атрибуты файла в записях MFT расположены в порядке возрастания числовых значений кодов типа, причем некоторые типы атрибутов могут встречаться в записи более одного раза: например, если у файла есть несколько атрибутов данных или несколько имен. Обязательными для каждого файла в томе NTFS являются атрибут стандартной информации, атрибут имени файла, атрибут дескриптора защиты и атрибут данных. Остальные атрибуты могут встречаться при необходимости.

Каталог на NTFS представляет собой специфический файл, хранящий ссылки на другие файлы и каталоги, создавая иерархическое строение данных на диске. Файл каталога поделен на блоки, каждый из которых содержит имя файла, базовые атрибуты и ссылку на элемент MFT, который уже предоставляет полную информацию об элементе каталога. Внутренняя структура каталога представляет собой бинарное дерево. Вот что это означает: для поиска файла с данным именем в линейном каталоге, таком, например, как у FAT-а, операционной системе приходится просматривать все элементы каталога, пока она не найдет нужный. Бинарное же дерево располагает имена файлов таким образом, чтобы поиск файла осуществлялся более быстрым способом - с помощью получения двухзначных ответов на вопросы о положении файла. Вопрос, на который бинарное дерево способно дать ответ, таков: в какой группе, относительно данного элемента, находится искомое имя - выше или ниже? Мы начинаем с такого вопроса к среднему элементу, и каждый ответ сужает зону поиска в среднем в два раза. Файлы, скажем, просто отсортированы по алфавиту, и ответ на вопрос осуществляется очевидным способом - сравнением начальных букв. Область поиска, суженная в два раза, начинает исследоваться аналогичным образом, начиная опять же со среднего элемента.

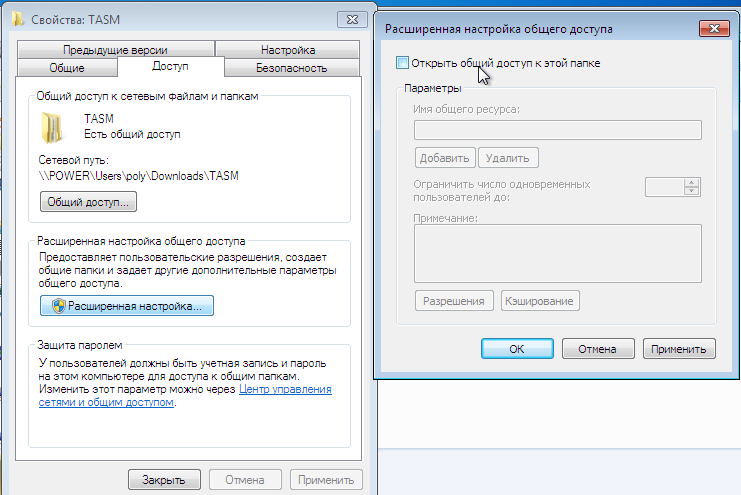


С помощью контекстного меню определить настраиваемые свойства файла и каталога.

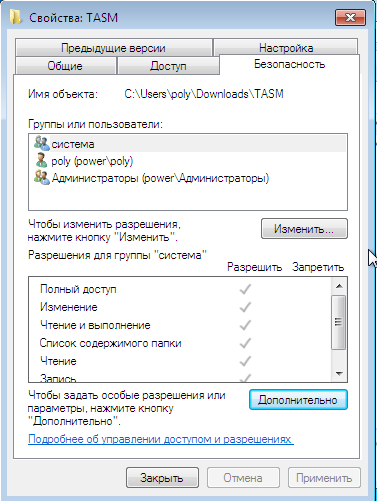
Во вкладке «Общие» отображены сведения о каталоге (тип, расположение, размер, содержимое, дата). Также доступна настройка атрибутов (скрытый, атрибуты сжатия, шифрования и т.д.).



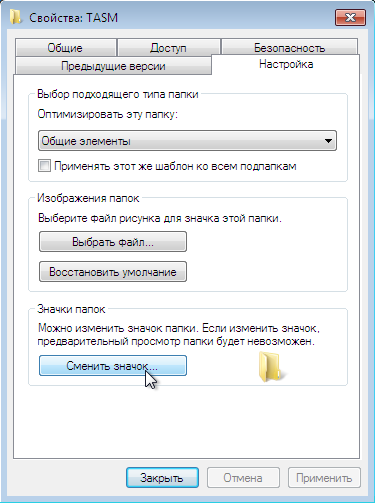
Во вкладке «Доступ» можно настроить параметры общего доступа к данному каталогу.



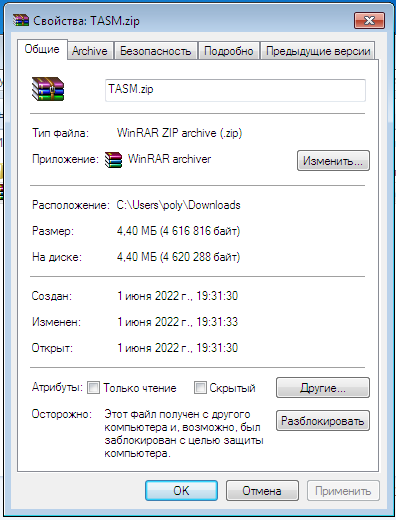
Во вкладке «Безопасность» можно настроить параметры доступа к папке для групп или отдельных пользователей, отдельные разрешения для них.



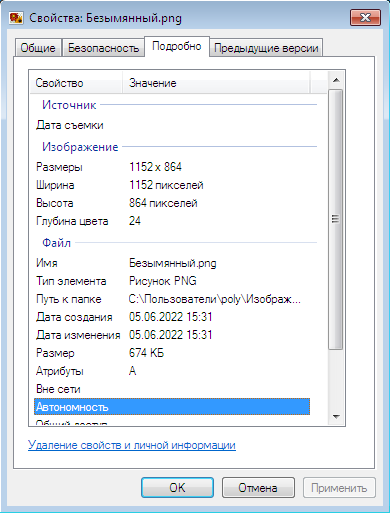
Во вкладке «Настройка» можно оптимизировать папку под тип содержимого, сменить значок папки.



Аналогично каталогу, у файла на вкладке «Общие» есть возможность настройки атрибутов, отображена общая информация.

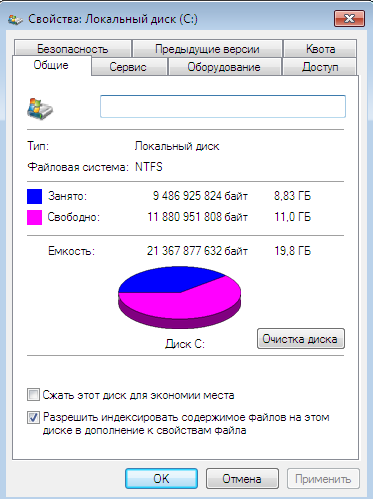
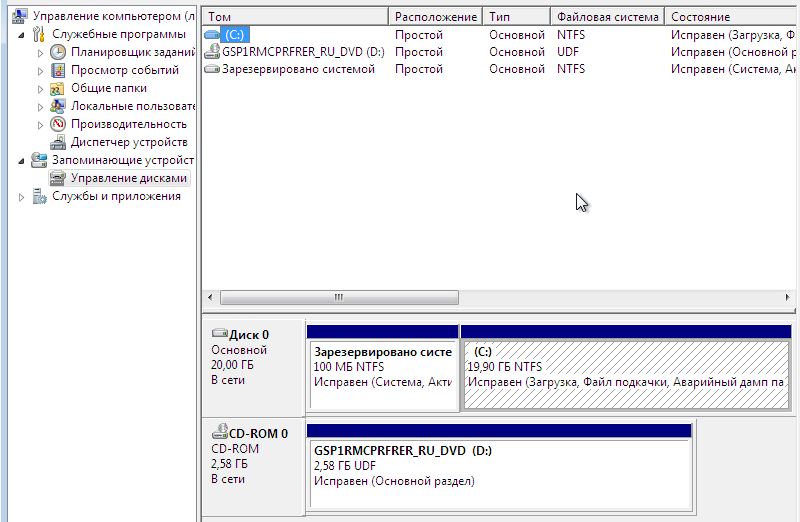
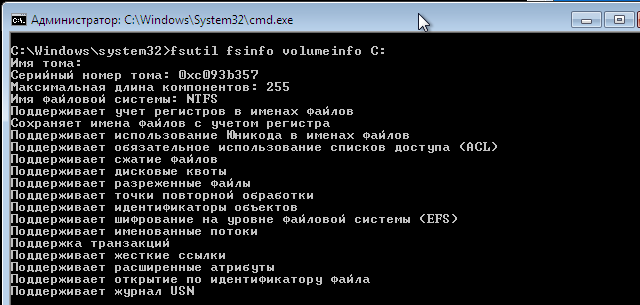


На вкладке «Подробно» можно увидеть дополнительную информацию о данном файле, соответствующую типу файла.



Выполнение операций

Получить информацию о томе можно несколькими способами:

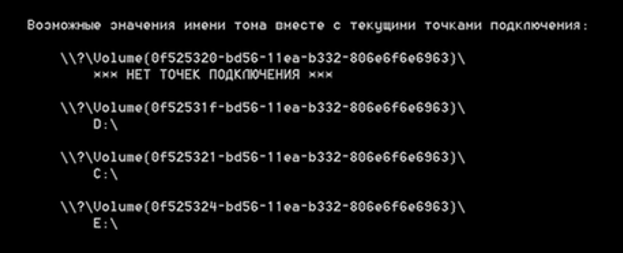
1. Через контекстное меню  
   Здесь можно найти основную информацию: тип файловой системы, количество занятого и свободного места, диаграмму.  
   
2. «Управление дисками» оснастки «Управление компьютером». В списке находим нужный том (в данном случае С:). Здесь указан тип тома, файловая система, его состояние.  
   
3. С помощью утилиты fsutil. Используя команду fsutil fsinfo (сведения о файловой системе) volumeinfo (запрос информации о томе) C: (нужный нам том), получим сведения о томе: его серийный номер, файловую систему, поддержка диском функций  
     
   Используя команду fsutil fsinfo (сведения о файловой системе) ntfsinfo (запрос информации о NTFS) C: (нужный нам том), получим сведения: информация о секторах и кластерах, допустимую длину MFT, информацию о зоне MFT.  
   

Монтирование тома к точке соединения NTFS

Точка соединения NTFS – нововведение в файловой системе NTFS 3.0 (файловая система по умолчанию в Windows 2000). Суть нововведения заключается в том, что указанный логический диск либо папка будет отображаться как папка на другом логическом диске, либо в другой папке.

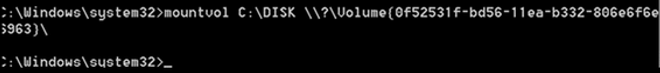
Команда MOUNTVOL позволяет создавать, удалять и просматривать точки подключения томов (точки монтирования) в командной строке Windows.

При вводе без параметров будут отображены тома с точками подключения.

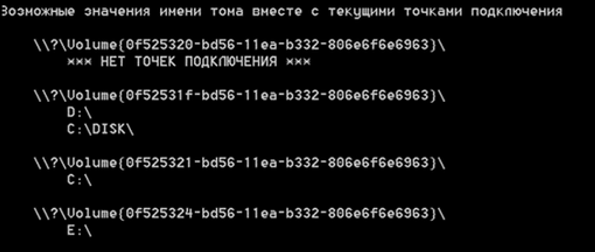


Подключим диск D: в папку C:\DISK:

Укажем в параметрах команды путь до папки на диске C: и идентификатор дискового раздела



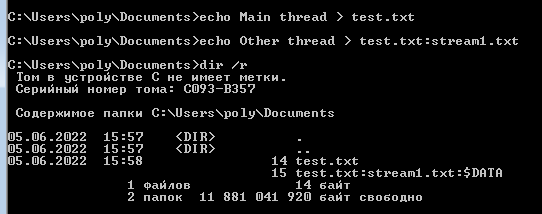
Проверим, используя команду mountvol без параметров:



Аналогичные действия можно выполнить с помощью: «Управление компьютером» - «Управление дисками» - «Изменить букву диска или путей».

Создание многопотокового файла

Создать многопотоковый файл можно с помощью команды echo. Для этого создадим текстовый файл test.txt и запишем «Главный поток». И ещё раз напишем в него «Это альтернативный поток», но дописав к названию файла ":stream1.txt".



Создание hardlink, symlink, junction point

Hard links представляют собой псевдонимы пути файла. Они позволяют разместить файл в нескольких местах сразу. Создавать их можно только на файлы, но не на каталоги, и только для файлов, которые расположены на одном разделе диска.

Symlink – это объекты файловой системы, ссылающиеся на другие объекты ФС. Они могут указывать на файлы, каталоги или сетевые каталоги. Символическая ссылка хранит текстовую запись, обрабатываемую ОС как путь к другому файлу или папке. Объект, на который ссылается ссылка, называется целью. при удалении оригинального файла больше не сможет ссылаться на данные.

Junction Point – работает практически аналогично символическим ссылкам на папки, но исключительно в пределах одного тома. Единственным преимуществом соединений в данном случае является совместимость с предыдущими версиями Windows, которой нет у symlink.

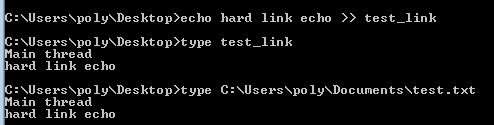
Все ссылки можно создать с помощью команды mklink, указав типа, имя и назначение ссылки.

Создадим в документах пользователя текстовый файл test.txt, который создали ранее в Документах.

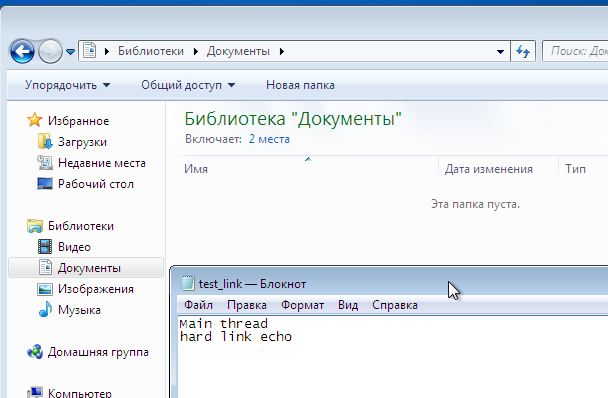




При открытии файла, видно содержимое файла, находящегося в Документах. При записи, запись также происходит в оба файла.



При удалении файла содержимое ссылки сохранилось:

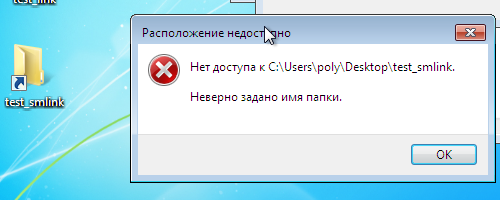


Можно сделать вывод о том, что содержимое файла удаляется после удаления всех ссылок на него.

Создадим symlink на восстановленный файл на рабочем столе:



При попытке открыть символическую ссылку, появляется данная ошибка:



Аналогично показывается пример работы junction point. Для удобства сравнения ссылок создадим таблицу:

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр сравнения | **Hard Link** | **Junction points** | **Symbolic Link** |
| Поддерживающие ОС | Windows NT4 и старше | Windows 2000 и XP и старше | Windows Vista и старше |
| Расположение ссылки и цели | Файлы и ссылки должны быть на том же томе | Каталоги должны быть на локальном компьютере | Любой путь (локальный/ удаленный/SMB) |
| При удалении | оригинал и остальные ссылки остаются | в версиях 2000, XP и 2003 оригинал удаляется, начиная с Vista не изменяется | цель не изменилась, ссылается на несуществующий объект |
| Перемещение цели (оригинала) | остается в силе | становится недействительным | становится недействительным |
| Работа с | Файлы | Папки | Файлы/Папки |

Сжатие

NTFS поддерживает сжатие файловых данных, выполняется оно прозрачно драйвером ФС. NTFS-сжатие может применяться к файлам, папкам и дискам. Для этого каждому сжатому объекту присваивается атрибут сжатия (compression state), который указывает, сжат файл или нет. У такого типа сжатия есть свои особенности: выполняется только на разделах с файловой системы NTFS; пользователь не видит различий между сжатым и обычным файлом; скорость доступа сжатого файла ниже; эффективность хуже других архиваторов, но скорость сжатия выше.

Для расчёта коэффициента сжатия была создана папка, в неё помещены файлы разных типов. К каждому файлу и папке в целом был применён атрибут сжатия. Рассчитанные коэффициенты:

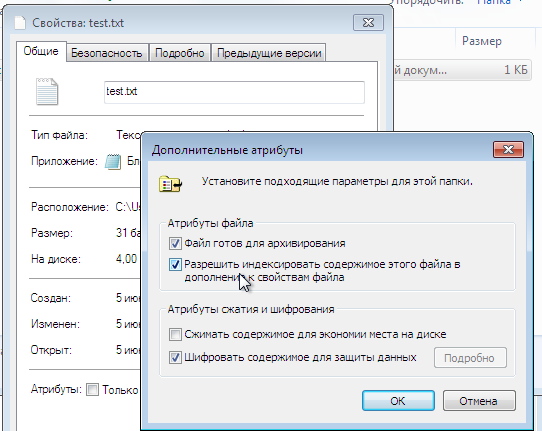
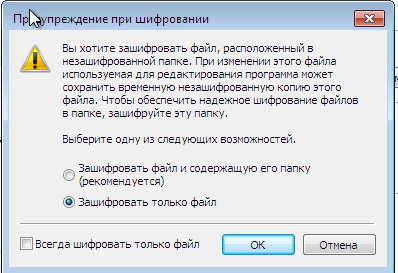
|  |  |
| --- | --- |
| Тип файла | Коэффициент сжатия NTFS |
| exe | 1,275 |
| pdf | 1 |
| jpg | 1,0035 |
| xls | 2,0783 |
| txt | 3,323 |
| папка | 1,031 |

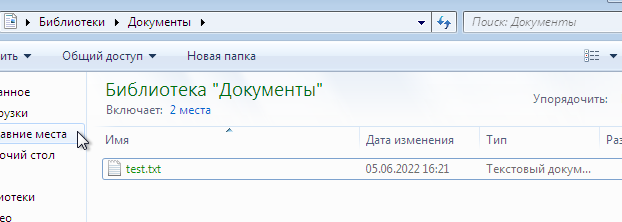
Относительно некоторых типов данных (например, pdf) сжатие не работает. Сжатие NTFS особо заметно при сжатии файлов типа xls и txt. Во всех остальных случаях отношение входного и выходного потока близко к единице.

Шифрование

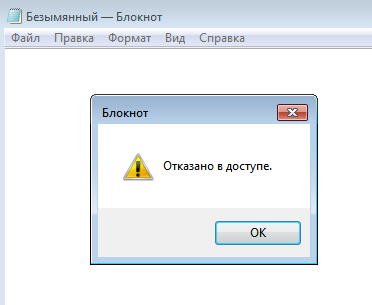
В NTFS входит средство шифрования файлов EFS, с помощью которого пользователи могут шифровать конфиденциальные данные. В процессе шифрования EFS генерирует для файла случайное число, называемое ключом шифрования файла (File Encryption Key, FEK). В этом случае EFS применяет симметричное шифрование. Затем EFS шифрует сам ключ шифрования файла, используя ассиметричный открытый ключ, и сохраняет результат для файла в дополнительном потоке данных $EFS. При этом ключи защищены паролем учетной записи.

Для шифрования, аналогично сжатию, необходимо добавить атрибут в свойствах файла. После шифрования цветовая схема изменится на зелёный.



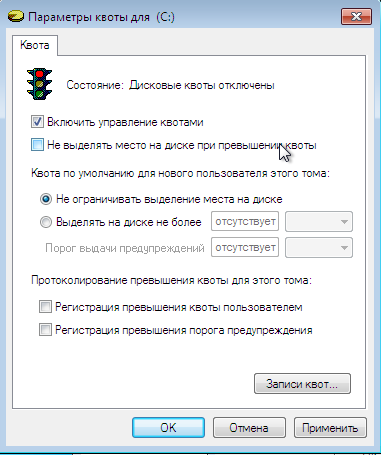
Для выполнившего шифрование пользователя папка доступна. Другие пользователи смогут посмотреть содержимое папки (так как шифровали только файл), но при этом не смогут открыть:



Квотирование

Квоты в NTFS позволяют ограничивать дисковое пространство, занимаемое пользователями на томах общего доступа. Каждому пользователю может быть выделена квота, а NTFS отслеживает превышение порогового значения.

Для назначения квоты необходимо в свойствах тома перейти во вкладку «Квота» и включить управлением квотами.

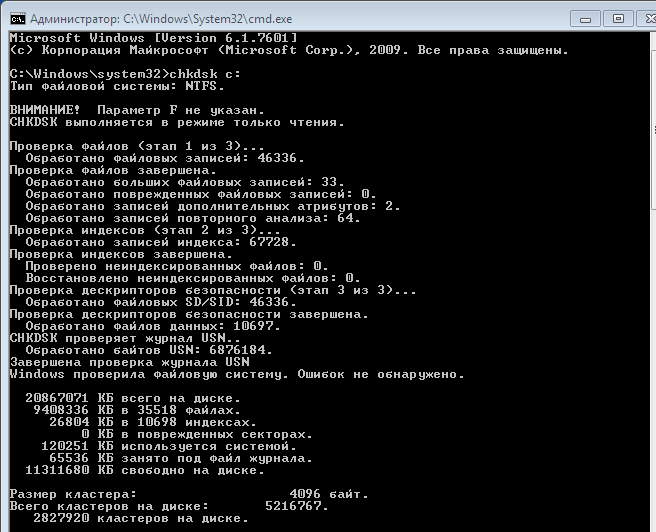


Можно создать запись квоты отдельно для каждого пользователя, настроить выделяемый объём и порог выдачи предупреждений. В случае исчерпания квоты будет выведен красный восклицательный знак, сигнализирующий о превышении квоты.

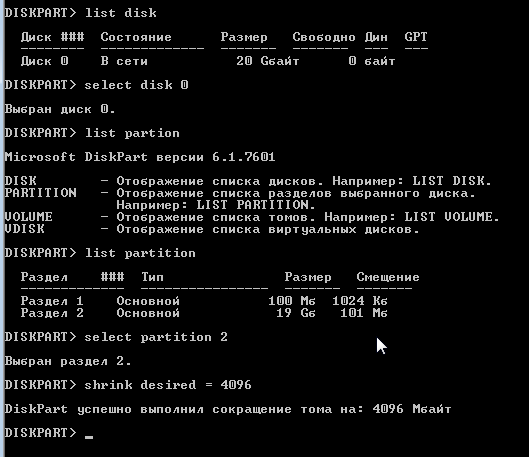
Команды управления томами

Chkdsk проверяет диск на наличие ошибок и выводит информацию о диске и ошибках. При указании параметра: /f – утилита выполнит исправление найденных ошибок; /r – выполнить обнаружение повреждённых секторов и восстановить информацию.

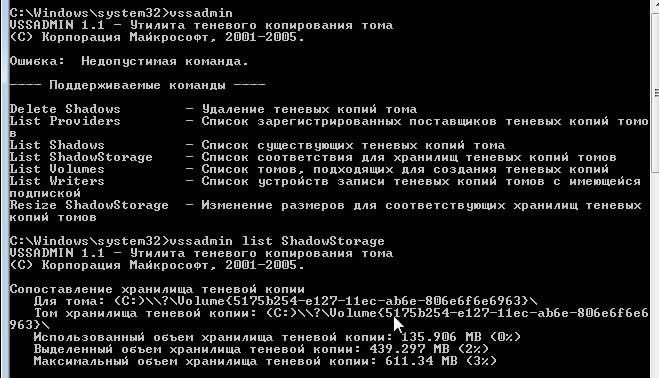
Chkdsk проверяет файловые записи, записи индекса, файлы данных и журнал USN.



Утилита diskpart даёт возможность работать с дисками, разделами, томами, виртуальными дисками. В качестве примера сократим размер тома.



VssAdmin работает с теневым копированием томов. Она позволяет просмотреть выделенные размеры теневых копий, а также диски, к которым они относятся, а также список устройств записи теневых копий. Также утилита позволяет изменять размер теневых копий и удалять их. Выведем список сопоставления теневых копий и томов:



Теневые копии, в отличии от резервных копий, можно считать временными файлами. При создании новых теневых копий старые стираются при превышении лимита по размеру. Они незаметны для пользователя, пока ему не понадобиться восстановить файл.

Командный язык и работа с командной строкой

Администраторы часто используют в своей работе командную строку, в котором можно вводить встроенные системные команды и запускать утилиты командной строки. Для получения информации по командам в окне консоли CMD необходимо ввести команду HELP. Группировка основных команд по функциям:

|  |  |
| --- | --- |
| 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 |
| 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. |
| 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 |
| 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 |

Переменные окружения

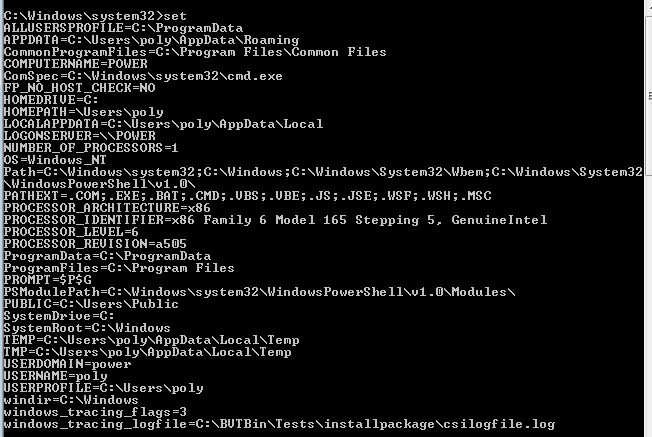
Переменная окружения/среды - текстовая короткая ссылка на элемент ОС, предназначенная для получения быстрого доступа к объекту системы, или к данным о каталогах и конфигурации компьютера, может содержать информацию о настройках системы или данные о текущем пользователе компьютера. С помощью переменной среды можно быстро перейти к нужному ресурсу на компьютере без указания полного пути к файлу.

Их можно использовать в командной строке, адресной строке Проводника, диалоговом окне «Выполнить.»

Переменные среды Windows делятся на два вида:

* Пользовательские переменные среды — содержат указания пути к пользовательским каталогам.
* Системные переменные среды — содержат информацию о каталогах ОС и конфигурации ПК.

Выведем переменные окружения, используя команду set без параметров.



PATH — переменная окружения Microsoft Windows, представляющая собой набор каталогов, в которых расположены исполняемые файлы. Например, если укажем в командной строке name.cmd, то выполнится последовательный поиск данного файла по указанным в PATH путям. Если исполняемый файл будет в нескольких каталогах, то выполнится запуск из того, что определен в переменной ранее. Если файл не будет найден ни в одном из указанных в Path каталогов, то система сообщит об этом.



При использовании компьютера и установке программ, изменяется переменная PATH. Некоторые установленные программы записывают свои пути для исполняемых файлов, иногда для собственного удобства пользователь добавляет новые пути.

Механизмы обмена данными между приложениями

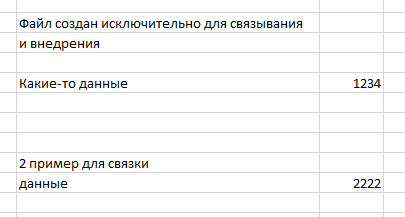
Clipboard - универсальный буфер обмена, так как пользователь может записать в него самую различную информацию. Это общая область для хранения дескрипторов данных, через которую прикладные программы могут обмениваться форматированными данными. Методика работы с Clipboard одинакова для всех приложений и обычно заключается в том, что пользователь выделяет нужную часть документа или изображения, а затем выбирает из меню "Edit" строки "Copy" или "Cut". Clipboard может содержать данные одновременно в нескольких форматах. 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 – 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). Большая часть DDE-функций реализована в последних версиях OLE.

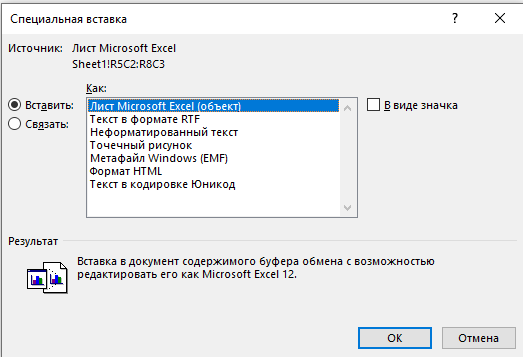
OLE (Object Linking and Embedding). Механизм OLE (Связывание и Встраивание Объектов) позволяет обеспечить интеграцию различных по своей сути объектов. При связывании объекта с документом создается ссылка на его файл (технология OLE1 – жесткая ссылка, технология OLE2 – относительная ссылка). OLE является набором средств, позволяющим легко подготавливать документы, включающие в себя данные, подготовленные в различных приложениях. Для реализации этих возможностей соответствующие приложения должны иметь опцию Object (Объект) в меню Insert (Включение). 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).

Внедрение и связывание

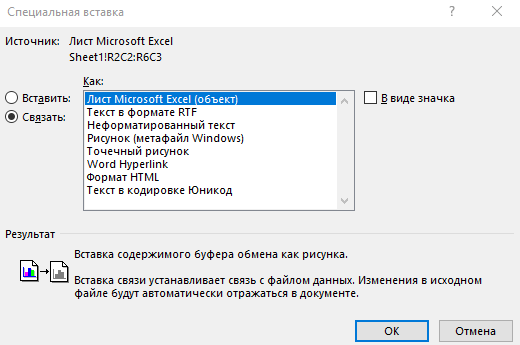
Внедрим и свяжем файл test.xslx с test.docx.



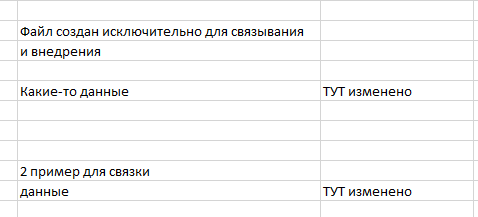
Один экземпляр таблицы вставим как лист Microsoft Excel.



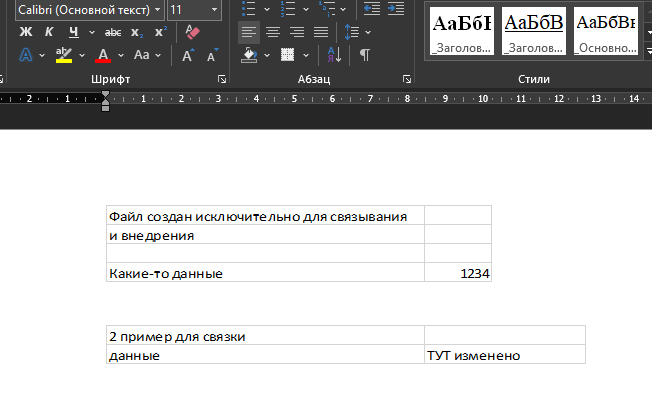
Другой экземпляр таблицы свяжем как лист Microsoft Excel.



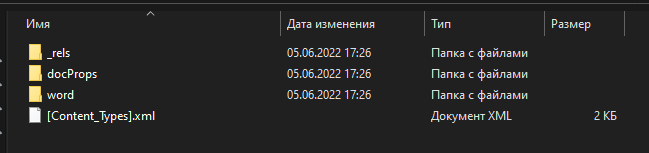
Получилось следующее содержимое файла, попробуем изменить файл Excel.

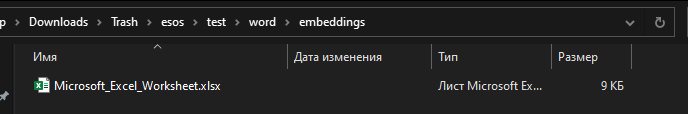


Сохраним изменения и посмотрим содержимое файла Docx.

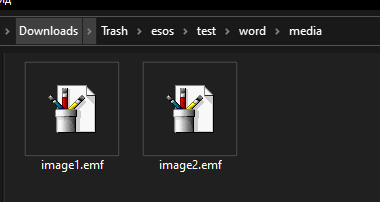


Чтобы найти связь таблицы, необходимо поменять расширение файла docx на zip, разархивировать файл и перейти в путь word/embeddings/ где хранятся связанные файлы.

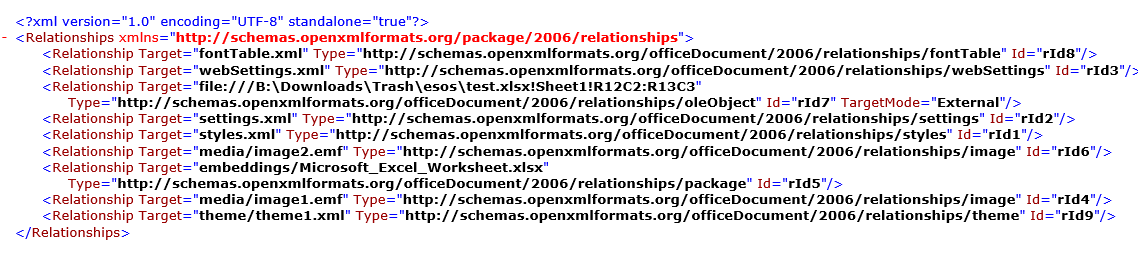




По пути word/media/ хранятся мультимедиа, в нашем случае изображения встроенной и связанной таблицы.



Документ document.xml.rels, расположенный по пути word/\_rels/. Здесь содержится список связей части word/document.xml. В данном файле можно найти ссылку на файл test.xlsx, с которым связывал Docx:



Выбор внедрения или связывания

Внедрение позволяет хранить и изменять копию объекта прямо в документе. При этом изменения в оригинальном файле и в копии никак не связаны. Этот способ подходит в случае необходимости свободного переноса документа на другие диски, при этом не беспокоясь об оригинале. Также если нужно зафиксировать состояние оригинала в копии. Но в данном случае стоит учесть, что данная копия будет хранится в самом документе. Связывание позволяет не хранит саам объект в документе и динамически изменять все его копии. При это необходимо гарантировать существование оригинала на данном диске. Этот способ подходит при наличии большого количества копий объекта, которые надо динамически изменять.

Вывод

В ходе выполнения лабораторной работы была изучена ОС Windows 7, различные редакции, дисковые конфигурации и варианты загрузки. Был приобретён опыт по установке Dos, Win16 и Win32 приложений и отслеживанию изменений в системе, значимость реестра в системе. Были изучены архитектура Windows 7, интерфейс. Также были приобретены знания о файловой системе NTFS, опробованы различные команды и утилиты, позволяющие управлять дисками, разделами и томами. Были изучены механизмы обмена информации между приложениями. Были рассмотрены внедрение и связывание, изучены их достоинства и недостатки.