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.

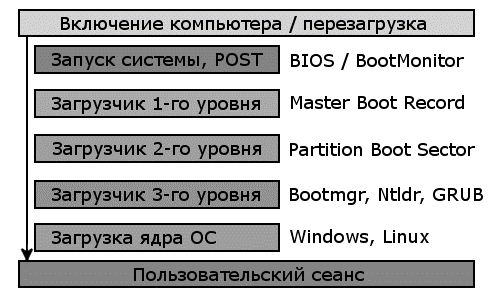
1. **Современные методы развертывания**:
   1. Windows автопилот — это новый набор возможностей, предназначенных для упрощения и модернизации развертывания и управления новыми компьютерами Windows 10 компьютеров. Windows автопилот позволяет ИТ-специалистам настраивать функцию out of Box Experience (OOBE) 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.

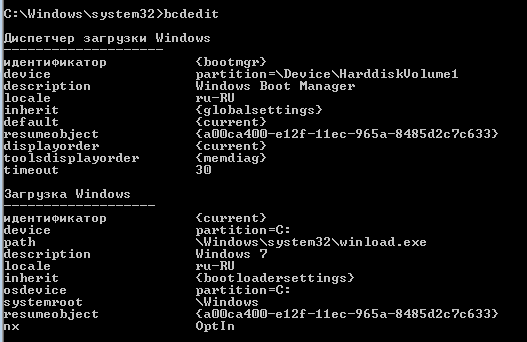
Этапы загрузки OC



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.

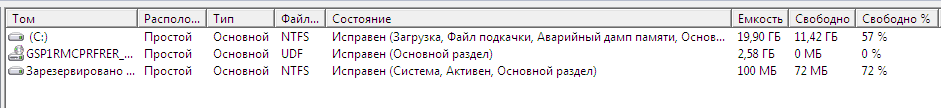
Boot manager и BCD

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.



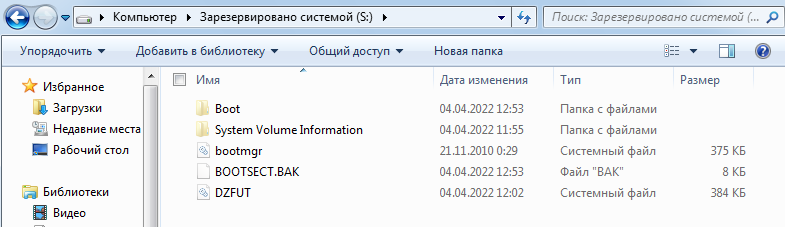
Процесс стандартной инсталляции операционной системы Windows Vista / 7 / 8 создает в начале диска дополнительный раздел «Зарезервировано системой». Ему не присваивается буква диска, благодаря чему, если не сделать дополнительных шагов, и сам раздел и его содержимое будут скрыты от пользователя. Этот 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.

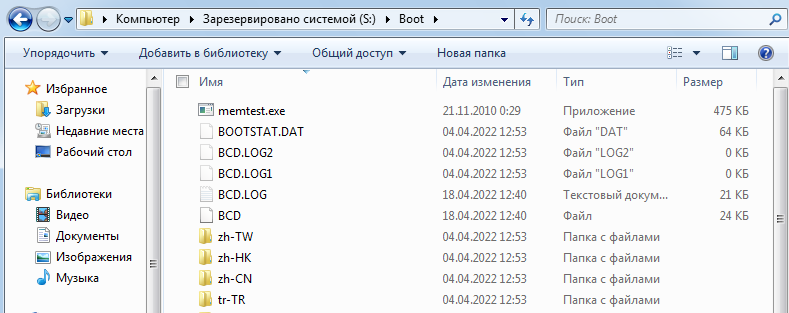


Посмотрим содержимое раздела «Зарезервировано системой». Для этого назначим ему букву диска в меню «Управление дисками». В панели управления компьютером включим отображение скрытых папок и файлов.

В корне раздела находится файл bootmgr, который является загрузчиком.



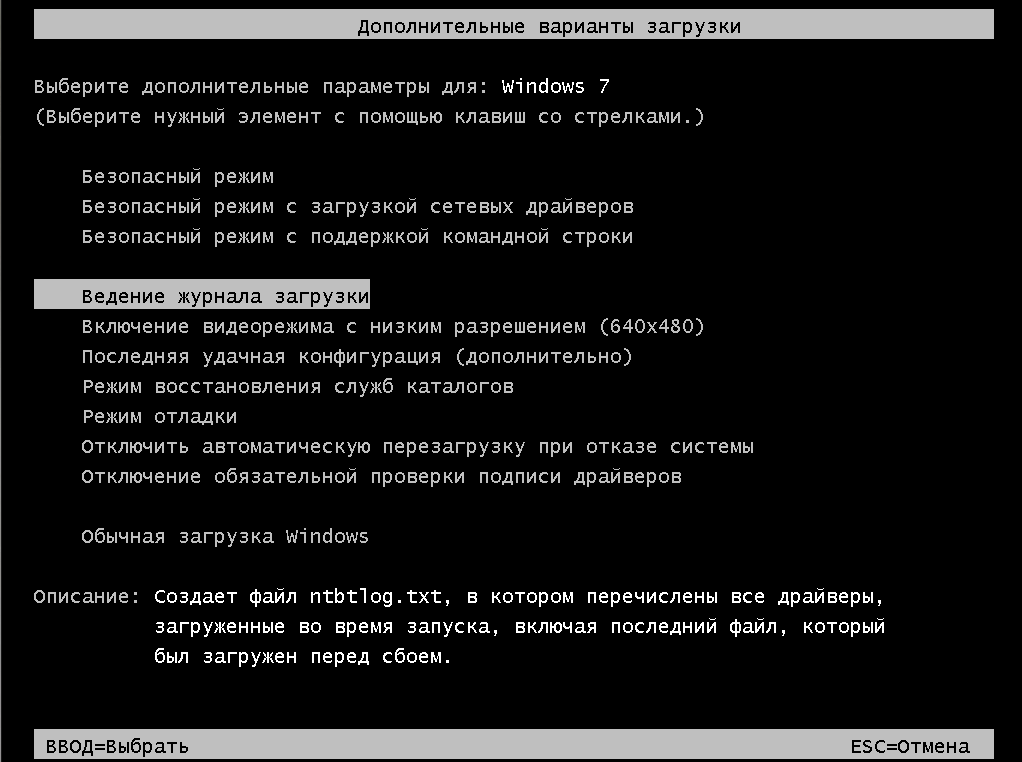
В каталоге Boot находится база хранилища конфигураций загрузки BCD, файлы для логов и папки с языковыми файлами.

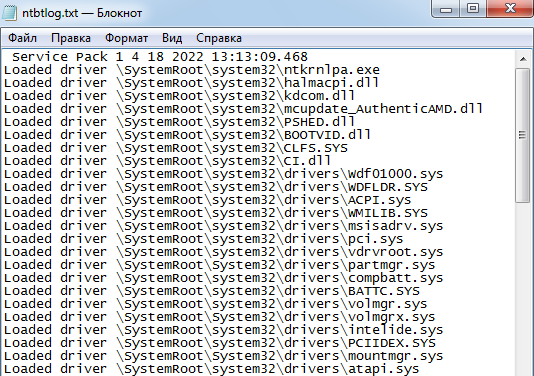


Раздел диска, который содержит загрузчик, называется системным диском, а раздел, содержащий основные файлы операционной системы – загрузочным. Системный и загрузочный диски могут находится на одном или разных физических дисках.

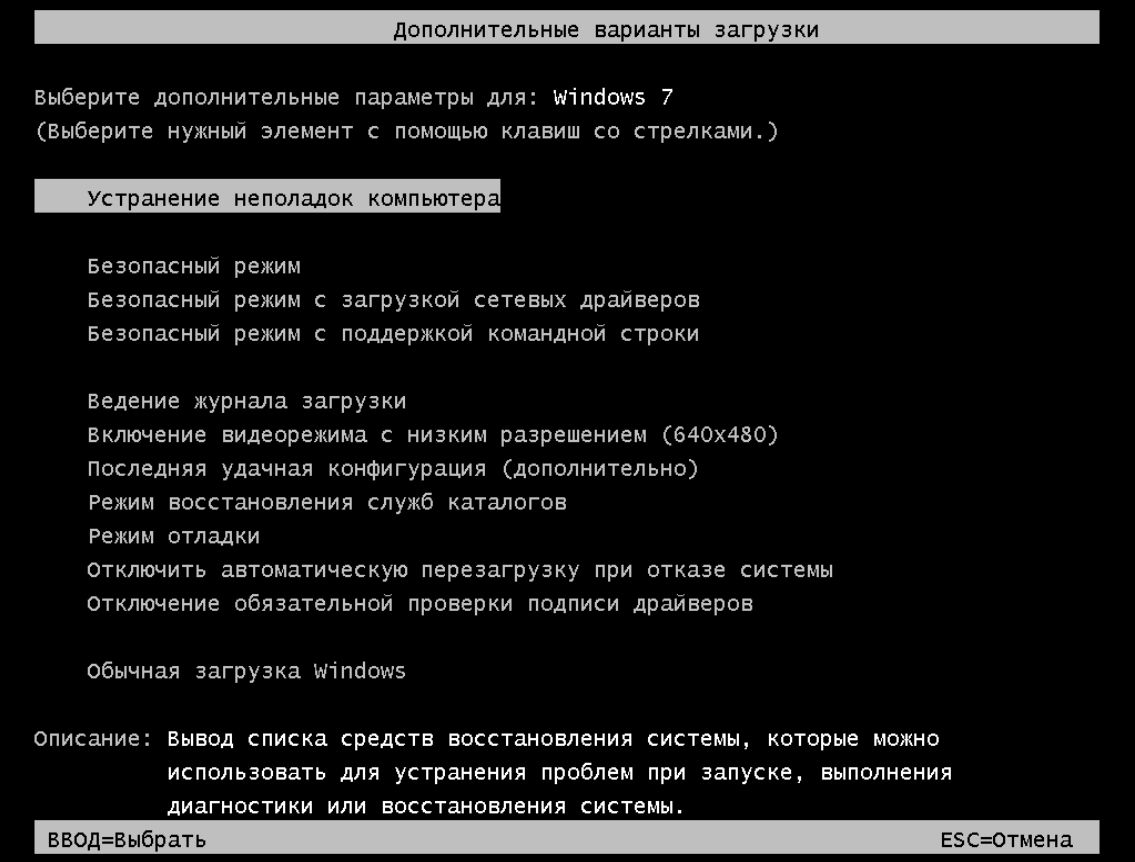
Загрузка с протоколированием журнала загрузки драйверов

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

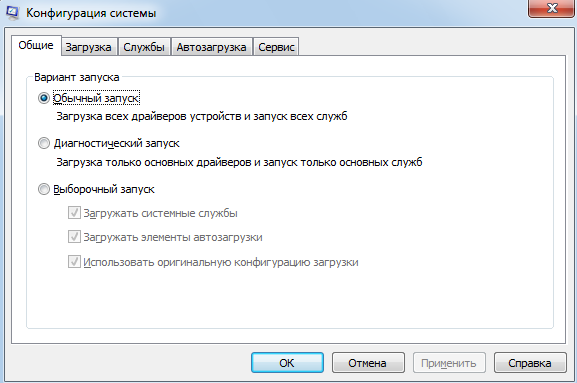
Безопасный режим запускает компьютер с минимально необходимым набором драйверов и служб. Все сторонние программы отключаются, и даже системные инструменты ограничены только необходимым набором функций.

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.



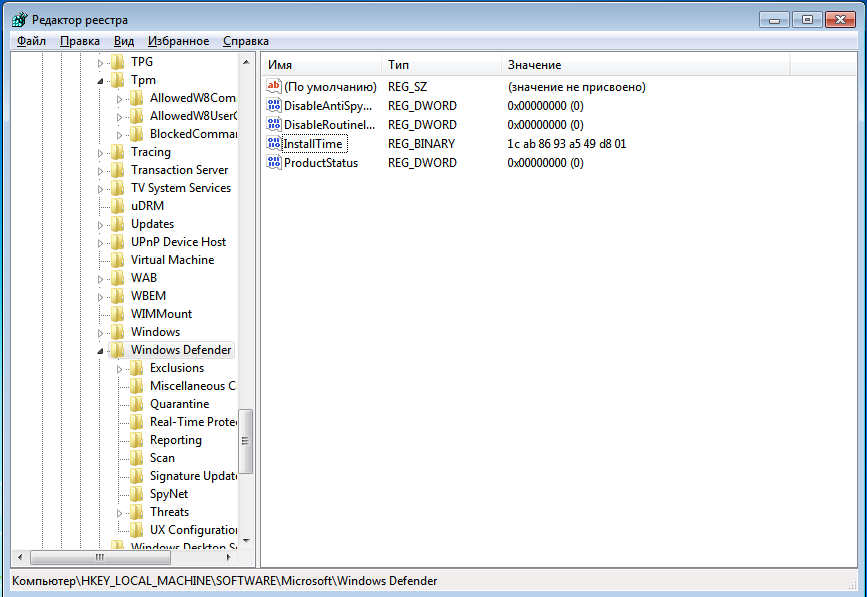
Описание возможностей программы

* 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

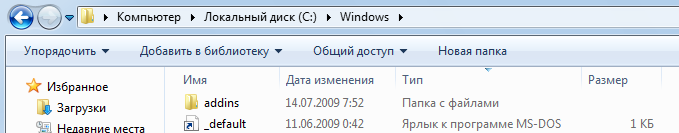
Установка DOS-программ сводится к размещению на диске, формированию переменных окружения (если для программы это необходимо). Для каждого приложения DOS ОС создает отдельную VDM. VDM работают в режиме вытесняющей многозадачности, деля процессорное время с системной виртуальной машиной. VDM не создают 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:

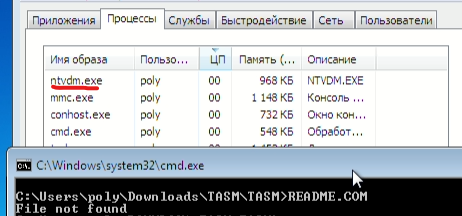
* режим выполнения (экранный или оконный)
* ресурсы памяти
* установки приоритетов для планирования процессов

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.

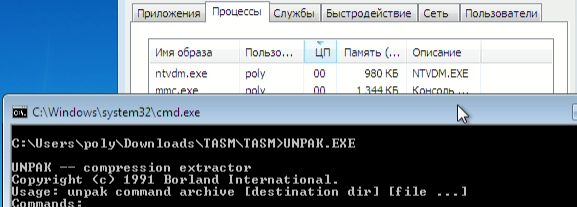
Процесс ntvdm.exe является процессом виртуальной машины.



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