

Глава 7



Реестр, загрузка системы и предотвращение сбоев

Сложность увеличивает вероятность поломки; двухмоторный самолет, по сравнению с одномоторным, имеет, по крайней мере, вдвое больше проблем с двигателями.

Правило самолета

Когда бы мы могли начать
С печальной мудрости огарка,
Как помогла бы нам свеча,
Когда она горела ярко.

П. Хэйн, "Груки"

Как уже говорилось в *главе 1*, реестр Windows Vista фактически управляет конфигурацией всей системы. Как и в ранних версиях Windows, информация реестра управляет и процессом загрузки. Понимание того, как информация реестра влияет на процесс загрузки системы, позволяет решать большинство проблем, связанных с невозможностью загрузки или некорректным запуском операционной системы.

ПРИМЕЧАНИЕ

В отличие от Windows XP, где процесс загрузки системы, несмотря на усовершенствования и нововведения, протекал аналогично процессу загрузки Windows NT/2000, в Windows Vista в последовательность загрузки были внесены существенные изменения. В этой главе процесс загрузки Windows Vista будет рассмотрен подробно, а загрузки предшествующих версий Windows¹ мы коснемся лишь вкратце, при рассмотрении мультизагрузочных конфигураций.

¹ На компакт-диске, прилагаемом к этой книге, в каталоге <CD_drive_letter>\Ch07\Supplementary вы найдете отрывок из моей книги по реестру Windows XP, подробно описывающий процесс загрузки Windows NT/2000/XP.

Каждый драйвер, установленный в системе, имеет собственный вложенный ключ в составе дерева `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services`. Каждый из этих ключей, в свою очередь, содержит в своем составе параметр `Start`. Значение этого параметра определяет стадию процесса загрузки системы, на которой осуществляется загрузка и инициализация этого драйвера. Более подробно параметр `Start` будет обсуждаться далее в этой главе.

Нововведения в процессе загрузки Windows Vista

Как уже говорилось ранее в этой главе, по сравнению с Windows XP последовательность загрузки Windows Vista претерпела серьезные изменения. Тем не менее, несмотря на эти модификации, в процессе загрузки все же присутствуют некоторые общие черты, свойственные не только всем операционным системам из семейства Windows, но всем операционным системам вообще. Упрощенная схема общего цикла работы системы (от загрузки до завершения работы) показана на рис. 7.2.

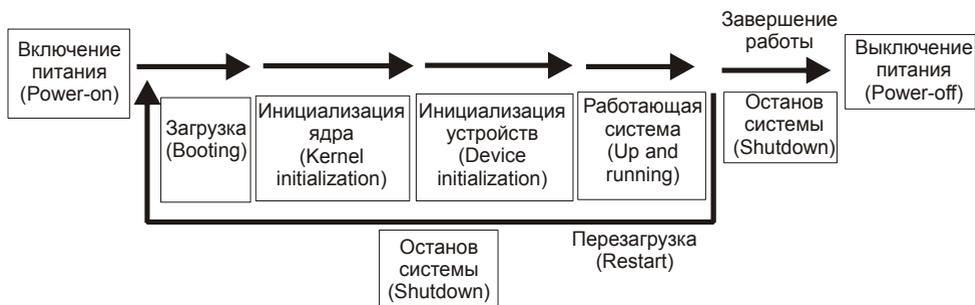


Рис. 7.2. Упрощенная схема рабочего цикла операционной системы от загрузки до перезагрузки или завершения работы

ПРИМЕЧАНИЕ

Схема процесса загрузки, показанная на рис. 7.2, справедлива для каждой операционной системы, и Windows Vista — не исключение из этого правила. Эта последовательность запуска применима к системам, загружаемым или перезагружаемым после нормального завершения работы системы (shutdown). Процедура запуска начинается после того, как пользователь выполняет одно из следующих действий: включает компьютер, который ранее был выключен, или перезагружает систему, выбрав опцию **Перезагрузка (Restart)** в окне **Завершение работы Windows** (Shut Down Windows), как показано на рис. 7.3.

Однако при возобновлении работы при выходе из спящих режимов эта последовательность будет иной.

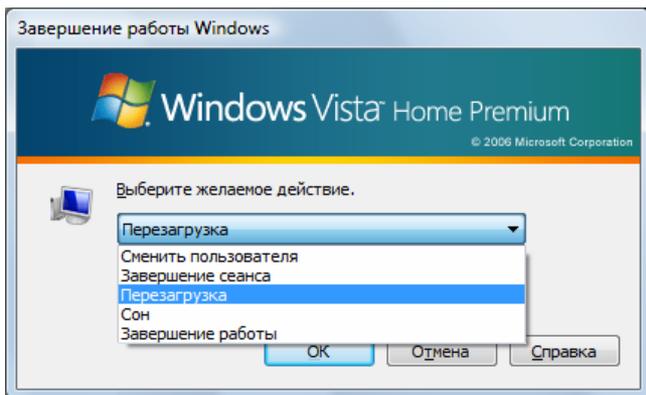


Рис. 7.3. Окно **Завершение работы Windows** (Shut Down Windows)

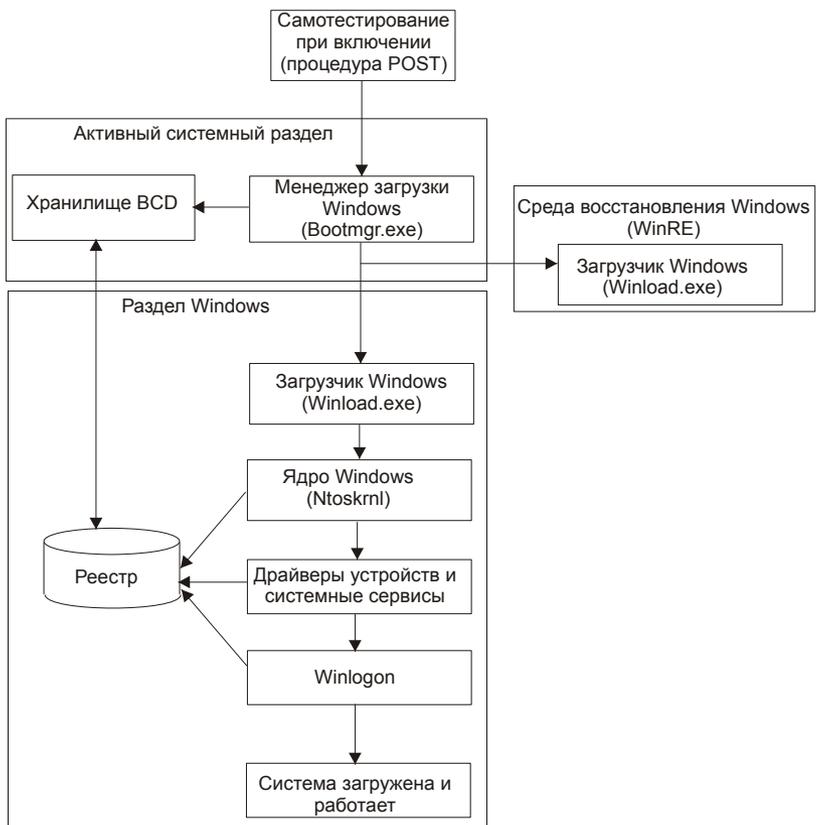


Рис. 7.4. Упрощенная диаграмма процесса загрузки Windows Vista

При успешном запуске Windows Vista процесс загрузки состоит из следующих этапов:

- самотестирование при включении питания (Power-on self test, POST);
- процесс начальной загрузки (bootstrap);
- работа менеджера загрузки (Boot manager phase);
- загрузка ядра (Kernel loading phase);
- загрузка и инициализация драйверов и сервисов;
- фаза регистрации пользователя в системе Windows Vista (logon phase).

Упрощенная диаграмма процесса загрузки Windows Vista показана на рис. 7.4.

До выпуска Windows Vista механизм загрузки операционных систем из семейства Windows зависел от аппаратной платформы (x86 или Itanium). Начиная с Windows Vista, этот процесс был унифицирован и больше не зависит от аппаратной платформы.

ПРИМЕЧАНИЕ

В действительности, процесс загрузки Windows Vista для платформ x86 и Itanium все же имеет незначительные отличия. Это касается только самых ранних стадий загрузки — самотестирования при включении питания и процесса начальной загрузки (bootstrap). Однако, как только управление передается менеджеру загрузки Windows Vista (Bootmgr), дальнейший процесс становится одинаковым для обеих платформ. Более подробная информация по данному вопросу будет приведена далее в этой главе.

За счет чего же была достигнута унификация процесса загрузки Windows Vista? Рассмотрим вкратце нововведения, появившиеся в загрузочной архитектуре Windows Vista. Первое, что немедленно бросается в глаза — это замена старого загрузчика NTLDR на комбинацию файлов Bootmgr (Windows boot manager), Winload.exe (Windows operating system loader) и Winresume.exe (Windows resume loader). Нет больше и хорошо известного пользователям Windows NT/2000/XP файла Boot.ini, который был замещен базой данных загрузочной конфигурации (Boot Configuration Database, BCD).

К преимуществам, предоставляемым BCD, относятся:

- возможность абстрагирования от микропрограммного обеспечения, что и позволило унифицировать процесс загрузки Windows Vista для платформ x86 и Itanium;
- использование строк в формате Unicode, что обеспечивает широкие возможности по интернационализации программного обеспечения.

BCD хранится в двоичном формате. Соответствующий улей реестра хранится в каталоге \Boot\BCD на активном системном разделе. В реестре он отобра-

жается как ключ `HKLM\BCD00000000`, для защиты которого предприняты специальные меры безопасности (см. главу 9).

Более подробно все перечисленные нововведения будут рассмотрены в последующих разделах данной главы. Перед тем как приступить к их обсуждению, отметим, что, как и в Windows NT/2000/XP, к тому моменту, когда производится регистрация пользователя в системе, компьютер уже завершает загрузку Windows Vista и большую часть процесса инициализации. Однако полностью все процессы будут завершены только после успешной регистрации пользователя в системе.

Для начала успешной загрузки Windows Vista необходимо соблюдение следующих условий:

- корректная инициализация аппаратных средств компьютера;
- наличие всех файлов, необходимых для загрузки системы.

Последовательность загрузки Windows Vista

Как уже говорилось, последовательность загрузки Windows Vista отличается от последовательности загрузки Windows NT/2000/XP. Рассмотрим этот процесс более подробно.

Процесс самотестирования при включении

При включении питания или перезагрузке компьютер проходит стадию *самотестирования при включении* (Power On Self Test, POST), представляющую собой набор тестов, предназначенных для определения правильности функционирования аппаратных средств. В случае возникновения проблем с аппаратными средствами или настройкой компьютера уже на стадии самозагрузки, POST информирует пользователя серией звуковых сигналов. Для подобных случаев следует иметь под рукой сопроводительную документацию, полученную от поставщика в комплекте с компьютером.

Программа POST действует следующим образом:

- диагностическая подпрограмма, в зависимости от встроенного микропрограммного обеспечения, может выполнять некоторые элементарные проверки аппаратных средств, определять количество доступной памяти, физическое присутствие всех устройств, необходимых для запуска операционной системы (например, жесткого диска), и правильность их инициализации;

- ❑ после завершения диагностической подпрограммы POST извлекает конфигурационные параметры из CMOS-памяти (Complementary Metal Oxide Semiconductor; комплементарный металлооксидный полупроводник, КМОП), размещенной на материнской плате. После завершения процедуры POST материнской платы каждый дополнительный адаптер со встроенной микросхемой firmware (например, видеоконтроллеры или же контроллеры жестких дисков) выполняет собственную специализированную подпрограмму POST.

При обнаружении проблем, связанных с аппаратными средствами или настройками BIOS, процедура POST выдает серию звуковых сигналов. Программа POST управляется посредством BIOS компьютера и зависит от конкретного компьютера. Поэтому документацию на компьютер рекомендуется всегда иметь под рукой.

Тема отыскания и устранения неисправностей аппаратных средств компьютера выходит далеко за рамки этой книги. Интересующимся читателям можно рекомендовать замечательную книгу известного хакера Pinckzakko (Дармаван Салихан, "BIOS: дизассемблирование, модификация, программирование", СПб., БХВ-Петербург, 2007). Кроме того, можно обратиться к полезным ресурсам, которые помогут получить представление о кодах ошибок BIOS:

- ❑ BIOS Survival Guide —

http://burks.bton.ac.uk/burks/pcinfo/hardware/bios_sg/bios_sg.htm;

- ❑ "БИОС. Это так просто!" —

<http://www.istc.kiev.ua/~santana/bios/contents.html>.

Процессы выполнения POST для систем, функционирующих на основе Itanium, подобны процессам, выполняемым в системах на базе процессоров x86. Расширяемый интерфейс встроенных программных средств (Extensible Firmware Interface, EFI) осуществляет элементарную проверку аппаратного обеспечения, подобную той, которую осуществляет BIOS, и проверяет наличие устройств, необходимых для запуска системы. Спецификация EFI определяет новую модель интерфейса между операционными системами и встроенным программным обеспечением платформы (для получения более подробной информации о спецификации EFI см: <http://www.microsoft.com/whdc/system/platform/firmware/efibrief.msp>).

Процесс инициализации при запуске

Как уже говорилось ранее, несмотря на унификацию, на ранних стадиях процесс загрузки Windows Vista для платформ x86 и Itanium все же имеет незначительные отличия. Рассмотрим эти процессы более подробно.

Процесс начальной загрузки на платформах x86

После успешного завершения процедуры POST начинается процесс инициализации при запуске, в ходе которого BIOS пытается обнаружить загрузочный диск. Порядок поиска загрузочного диска (флорпи-дисководы, жесткие IDE- и SCSI-диски, устройства CD-ROM) задается BIOS, и можно переконфигурировать этот порядок, называемый *последовательностью загрузки* (boot sequence). Подробную информацию о редактировании последовательности загрузки можно найти в сопроводительной документации к вашему компьютеру. Если при этом дисковод A: включен в последовательность загрузки первым, и в нем находится дискета, BIOS попытается использовать эту дискету в качестве загрузочной. Если дискеты в дисковом нет, BIOS проверяет первый жесткий диск, который к этому времени уже инициализировался. Для процесса запуска огромное значение играет первый сектор жесткого диска, который содержит *главную загрузочную запись* (Master Boot Record, MBR) и *таблицу разделов* (Partition Table).

BIOS считывает главную загрузочную запись и загружает ее в память, а затем передает ей управление. Код, содержащийся в главной загрузочной записи, сканирует таблицу разделов в поисках системного раздела. Найдя системный раздел, MBR загружает в память его нулевой сектор и исполняет код, содержащийся в этом секторе. Сектор 0 на системном разделе, так называемый *загрузочный сектор раздела* (partition boot sector), содержит загрузочный код операционной системы — загрузочную запись раздела (Partition boot record, PBR). Этот код и осуществляет запуск операционной системы определенным для нее способом.

Если на первом жестком диске нет системного раздела, главная загрузочная запись отобразит одно из следующих сообщений об ошибках:

- Invalid partition table (Неверная таблица разделов);
- Error loading operating system (Ошибка загрузки операционной системы);
- Missing operating system (Отсутствует операционная система).

Для предшествующих версий операционных систем из семейства Windows NT, главная загрузочная запись не зависела от конкретной операционной системы. Например, на компьютерах x86 одна и та же главная загруз-

зочная запись служила для запуска Windows NT/2000/XP, Windows 9x, а также комбинации "MS-DOS/Windows 3.1x".

ПРИМЕЧАНИЕ

В Windows Vista эта ситуация поменялась. В процессе загрузки операционная система Windows Vista несколько иначе, чем ее предшественницы, использует поле сигнатуры диска (`drive ID`) в главной загрузочной записи жесткого диска. Это поле, расположенное по смещению `0x01B8` от начала сектора, содержит уникальное число, идентифицирующее данный диск для операционной системы. Windows использует эту сигнатуру в качестве индекса для хранения информации о диске в подключе реестра `HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices`. В Windows NT/2000/XP эта сигнатура в MBR в большинстве случаев была не критичной, и загрузчик NTLDR мог инициировать процесс загрузки даже в случае нарушения ее целостности. В Windows Vista изменение или затирание этой сигнатуры приведет к остановке процесса загрузки с выдачей следующего сообщения об ошибке: `winload.exe..... is missing or corrupt`. Стоит отметить, что это сообщение является абсолютно неточным и никак не отражает фактической ситуации, потому что файл `winload.exe` как таковой вполне корректен и находится на своем месте. Действительная причина состоит в том, что если изменить хотя бы один бит в сигнатуре `drive ID`, менеджер загрузки просто не сможет найти файл `winload.exe`, чтобы передать ему управление. Если эту сигнатуру восстановить, то и возможность загрузки Windows Vista будет восстановлена.

Что касается загрузочного сектора раздела, то он зависит как от операционной системы, так и от используемой файловой системы. На компьютерах x86 загрузочный сектор раздела Windows Vista отвечает за выполнение следующих действий:

- ❑ распознавание используемой файловой системы и ее применение для поиска менеджера загрузки `bootmgr` и базы данных конфигурационной информации (BCD) в корневом каталоге системного раздела. На томах FAT структура данных, называемая загрузочным сектором раздела, действительно имеет длину в 1 сектор физической разметки диска. На томах FAT32 эта структура занимает уже 2 сектора физической разметки диска, поскольку загрузочный код занимает более 512 байт. На томах NTFS структура данных, называемая загрузочным сектором раздела, может занимать до 16 секторов, причем дополнительные секторы могут содержать код файловой системы, необходимый для поиска требуемых файлов;
- ❑ нахождение менеджера загрузки `bootmgr`, его загрузку в память и передачу ему управления.

На компьютерах x86 системный раздел должен находиться на первом физическом жестком диске. Загрузочный раздел (тот, что содержит системные файлы операционной системы) может совпадать с системным разделом, но

допустимо также его размещение и в другом разделе того же жесткого диска или даже на другом жестком диске.

ПРИМЕЧАНИЕ

В Windows NT/2000/XP и Windows Server 2003 функции менеджера загрузки и диспетчера загрузки выполнялись файлами NTLDR, Ntdetect.com и boot.ini, причем все три файла должны были находиться в корневом каталоге активного главного раздела первого жесткого диска (раздела System). В Windows Vista эти три файла были заменены на bootmgr (менеджер загрузки), BCD (база данных конфигурационной информации) и winload.exe (загрузчик операционной системы), но только bootmgr и BCD остались на системном разделе. Файл загрузчика winload.exe переместился в каталог %SystemRoot%\system32 загрузочного раздела (раздел Boot).

Если первый жесткий диск не содержит системного раздела, который должен использоваться для запуска компьютера, необходимо отключить этот диск, чтобы системная BIOS могла получить доступ к нужному жесткому диску, с которого будет запускаться операционная система.

Если в дисковомоду A: имеется дискета, BIOS загрузит в память первый сектор этой дискеты. Если дискета является системной, то ее первый сектор представляет собой *загрузочный сектор раздела* (Partition Boot Sector). Если дискета не является загрузочной, то вы увидите на экране примерно следующие сообщения об ошибках:

- Если дискета отформатирована в формате DOS или Windows 9x/ME —
Non-System disk or disk error
Replace and press any key when ready.
- Если дискета отформатирована в Windows NT/2000/XP —
Ntldr is missing
Replace and press any key when ready.
- Если дискета отформатирована в Windows Vista —
Bootmgr is missing
Replace and press any key when ready.

Для успешной загрузки операционных систем из семейства Windows NT с дискеты требуется, чтобы ее первым сектором был загрузочный сектор раздела. Кроме того, на этой дискете должны присутствовать все файлы, необходимые для того, чтобы начать процесс загрузки. Как и в случае с Windows NT/2000/XP, Windows Vista тоже может быть загружена с дискеты. Чтобы изготовить загрузочную дискету Windows Vista, необходимо проделать следующее:

1. Возьмите чистую дискету и отформатируйте ее под управлением Windows Vista.
2. Скопируйте на эту дискету файл bootmgr из корневого каталога системного раздела.
3. Создайте на этой дискете папку \Boot и скопируйте в нее улей реестра BCD. Для локализованных версий Windows Vista в эту папку следует скопировать и папку, содержащую локализованную версию менеджера загрузки (например, для русской версии это будет папка \Boot\ru-RU).

Если необходимо загрузить систему с загружаемого компакт-диска (например, для инсталляции Windows с дистрибутивного диска или для восстановления системы), то вам следует установить привод CD-ROM в качестве основного загрузочного устройства — первым пунктом в списке порядка загрузки. При загрузке системы с загрузочного компакт-диска с системой Windows Vista, программа Setup проверяет жесткий диск на наличие установленной копии Windows Vista. Если программа Setup обнаружит, что на диске имеется установленная система, то она предложит опцию обхода запуска с CD-ROM (для этого достаточно не отреагировать на предложение системы **Press any key to boot from CD-ROM**). Если в течение трех секунд вы не нажмете какую-либо клавишу, то программа Setup выполняться не будет, и компьютер передаст управление от CD-ROM к жесткому диску.

ПРИМЕЧАНИЕ

Если вы не хотите запускать программу Setup для инсталляции или же восстановления поврежденной системы, извлеките компакт-диск из дисковода, поскольку это позволит минимизировать время, необходимое для запуска Windows.

Процесс начальной загрузки на платформах Itanium

На платформах Itanium этот процесс протекает иначе. После стандартной инициализации микропрограммного обеспечения EFI производится загрузка драйверов и приложений EFI. Код микропрограммного обеспечения EFI должен содержать *собственный менеджер загрузки*, который загрузит первую исполняемую программу EFI (это может быть специализированная утилита или загрузчик операционной системы). Программа Windows Vista Setup добавляет в меню менеджера загрузки EFI всего одну строку — **Windows Boot Manager**. Эта строка указывает на \EFI\Microsoft\Boot\bootmgfw.efi как на исполняемую программу EFI, которая должна запускаться, когда пользователь выбирает эту опцию из загрузочного меню. Об-

ратите внимание, что таким образом в системах EFI фактически появляется два менеджера загрузки — собственный менеджер загрузки и менеджер загрузки Windows Vista. Таким образом, различия в процессе загрузки Windows Vista на платформах x86 и Itanium наблюдаются только на самых ранних этапах загрузки (рис. 7.5).

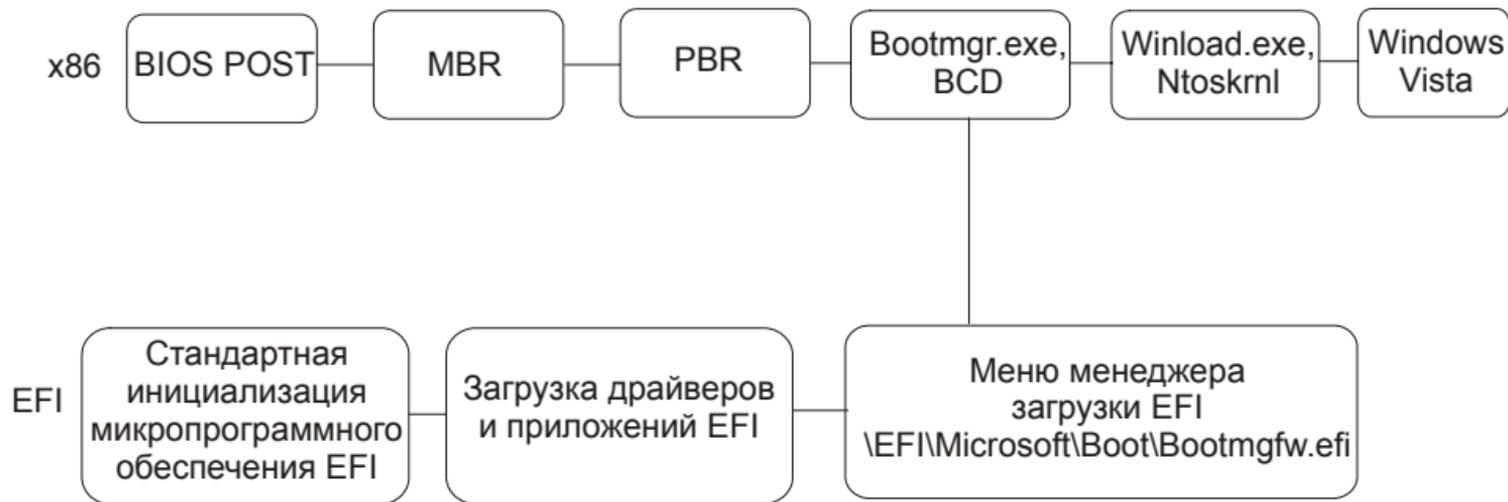


Рис. 7.5. Различия в последовательности загрузки Windows Vista на платформах x86 и EFI