Как загружается твоя Windows XP

Источник: http://www.interface.ru/

Процесс загрузки компьютера казалось бы изучен нами до мелочей: кнопка - BIOS - операционная система - логин... А ты задумывался когда-нибудь о том что же на самом деле происходит в это время внутри твоего компьютера? Можешь по шагам рассказать как работает компьютер? Уверен, что нет. Поэтому сегодня проведем короткий ликбез - расскажем о том, как же на самом деле загружается компьютер.

Эта статья рассматривает работу Windows XP, в остальных системах процесс, естественно, несколько отличается.

Включается тумблер питания.

Блок питания проводит самодиагностику. Когда все электрические параметры в норме БП посылает сигнал Power Good процессору. Время между включением питания и уходом сигнала обычно 0.1-0.5 секунд.

Таймер микропроцессора получает сигнал Power Good.

С получением этого сигнала таймер перестает посылать сигнал Reset процессору, позволяя тому включиться.

CPU начинает выполнять код ROM BIOS.

Процессор загружает ROM BIOS начиная с адреса FFFF:0000. По этому адресу прописан только переход на адрес настоящего кода BIOS ROM.

Система выполняет начальный тест железа.

Каждая ошибка, встречающаяся на этом этапе сообщается определенными звуковыми кодами (в прошлом биканьем, сейчас уже вероятно более современно - голосом), так как видео система еще не инициализирована.

BIOS ищет адаптеры, которые могут потребовать загрузки своего BIOS-а.

Самым типичным случаем в этом случае является видео карта. Загрузочная процедура сканирует память с адреса C000:0000 по C780:0000 для поиска видео ROM. Таким образом загружаются системы всех адаптеров.

ROM BIOS проверяет выключение это или перезагрузка.

Процедура два байта по адресу 0000:0472. Любое значение отличное от 1234h является свидетельством "холодного" старта.

Если это включение ROM BIOS запускает полный POST (Power On Self Test). Если это перезагрузка, то из POST процедуры исключается проверка памяти.

Процедуру POST можно разделить на три компоненты:

- Видео тест инициализирует видео адаптер, тестирует карту и видео память, показывает конфигурацию или возникшие ошибки.
- Идентификация BIOS-а показывает версию прошивки, производителя и дату.
- Тест памяти проверяет чипы памяти и подсчитывает размер установленной памяти.

Ошибки, которые могут возникнуть в ходе POST проверки можно разделить на смертельные и не очень :). Во втором случае они показываются на экране, но позволяют продолжить процесс загрузки. Ясно, что в первом случае процесс загрузки останавливается, что обычно сопровождается серией бип-кодов.

BIOS читает конфигурационную информацию из CMOS.

Небольшая область памяти (64 байт) питается от батарейки на материнской платы. Самое главное для загрузки в ней - порядок, в котором должны опрашиваться приводы, какой из них должен быть первым - дисковод, CD-ROM или винчестер.

Если первым является жесткий диск, BIOS проверяет самый первый сектор диска на наличие Master Boot Record (MBR). Для дисковода проверяется Boot Record в первом секторе.

Master Boot Record - первый сектор на цилиндре 0, 0 головке, 512 байт размером. Если она находится, то загружается в память по адресу 0000:7C00, потом проверяется на правильную сигнатуру - два последних байта должны быть 55AAh. Отсутствие MBR или этих проверочных байт останавливает процесс загрузки и выдает предупреждение. Сама MBR состоит из двух частей - системного загрузчика (partition loader или Boot loader), программы, которая получает управление при загрузке с этого жесткого диска; таблицы разделов (партиций), которая содержит информацию о логических дисках, имеющихся на жестком диске.

Правильная MBR запись записывается в память и управление передается ее коду.
Процесс установки нескольких операционных систем на один компьютер обычно заменяет оригинальный лоадер на свою программу, которая позволяет выбрать с какого диска производить остальную загрузку.

Дальше Boot Loader проверяет таблицу партиций в поисках активной. Загрузчик дальше ищет загрузочную запись (Boot Record) на самом первом секторе раздела.
В данном случае Boot Record это еще 512 байт - таблица с описанием раздела (количество байт в секторе, количество секторов в кластере и т.п.) и переход на первый файл операционной системы (IO.SYS в DOS).

Операционная система.

Управление передается операционной системы. Как же она работает, как проходит процесс загрузки?

Boot Record проверяется на правильность и если код признается правильным то код загрузочного сектора исполняется как программа.
Загрузка Windows XP контролируется файлом NTLDR, находящемся в корневой директории системного раздела. NTLDR работает в четыре приема:

1. Начальная фаза загрузки
2. Выбор системы
3. Определение железа
4. Выбор конфигурации

В начальной фазе NTLDR переключает процессор в защищенный режим. Затем загружает соответствующий драйвер файловой системы для работы с файлами любой файловой системы, поддерживаемой XP.
Если кто забыл, то наша любимая ОСь может работать с FAT-16, FAT-32 и NTFS.

Если в корневой директории есть BOOT.INI, то его содержание загружается в память. Если в нем есть записи более чем об одной операционной системе, NTLDR останавливает работу - показывает меню с выбором и ожидает ввода от пользователя определенный период времени.
Если такого файла нет, то NTLDR продолжает загрузку с первой партиции первого диска, обычно это C:\.

Если в процессе выбора пользователь выбрал Windows NT, 2000 или XP, то проверяется нажатие F8 и показ соответствующего меню с опциями загрузки.
После каждой удачной загрузки XP создает копию текущей комбинации драйверов и системных настроек известную как Last Known Good Configuration. Этот коллекцию можно использовать для загрузки в случае если некое новое устройство внесло разлад в работу операционной системы.

Если выбранная операционная система XP, то NTLDR находит и загружает DOS-овскую программу NTDETECT.COM для определения железа, установленного в компьютере.
NTDETECT.COM строит список компонентов, который потом используется в ключе HARDWARE ветки HKEY_LOCAL_MACHINE реестра.

Если компьютер имеет более одного профиля оборудования программа останавливается с меню выбора конфигурации.

После выбора конфигурации NTLDR начинает загрузку ядра XP (NTOSKRNK.EXE).
В процессе загрузки ядра (но перед инициализацией) NTLDR остается главным в управлении компьютером. Экран очищается и внизу показывается анимация из белых прямоугольников. Кроме ядра загружается и Hardware Abstraction Layer (HAL.DLL), дабы ядро могло абстрагироваться от железа. Оба файла находятся в директории System32.

NTLDR загружает драйвера устройств, помеченные как загрузочные. Загрузив их NTLDR передает управление компьютером дальше.
Каждый драйвер имеет ключ в HKEY_LOCAL_MACHINE\SYSTEM\Services. Если значение Start равно SERVICE_BOOT_START, то устройство считается загрузочным. Для кажого такого устройства на экране печатается точка.

NTOSKRNL в процессе загрузки проходит через две фазы - так называемую фазу 0 и фазу 1. Первая фаза инициализирует лишь ту часть микроядра и исполнительные подсистемы, которая требуется для работы основных служб и продолжения загрузки. На этом этапе на экране показывается графический экран со статус баром.

XP дизейблит прерывания в процессе фазы 0 и включает их только перед фазой 1. Вызывается HAL для подготовки контроллера прерываний. Инициализируются Memory Manager, Object Manager, Security Reference Monitor и Process Manager. Фаза 1 начинается когда HAL подготавливает систему для обработки прерываний устройств. Если на компьютере установлено более одного процессор они инициализируются. Все исполнительные подсистемы реинициализируются в следующем порядке:

1. Object Manager
2. Executive
3. Microkernel
4. Security Reference Monitor
5. Memory Manager
6. Cache Manager
7. LPCS
8. I/O Manager
9. Process Manager

Инициализация Менеджера ввода/Вывода начинает процесс загрузки всех системных драйверов. С того момента где остановился NTLDR загружаются драйвера по приоритету. Сбой в загрузке драйвера может заставить XP перезагрузиться и попытаться восстановить Last Known Good Configuration.

Последняя задача фазы 1 инициализации ядра - запуск Session Manager Subsystem (SMSS). Подсистема ответственна за создание пользовательского окружения, обеспечивающего интерфейс NT.

SMSS работает в пользовательском режиме, но в отличии от других приложений SMSS считается доверенной частью операционной системы и "родным" приложением (использует только исполнительные функции), что позволяет ей запустить графическую подсистему и login.

SMSS загружает win32k.sys - графическую подсистему.

Драйвер переключает компьютер в графический режим, SMSS стартует все сервисы, которые должны автоматически запускаться при старте. Если все устройства и сервисы стартовали удачно процесс загрузки считается удачным и создается Last Known Good Configuration.

Процесс загрузки не считается завершенным до тех пор, пока пользователь не залогинился в систему. Процесс инициализируется файлом WINLOGON.EXE, запускаемым как сервис и поддерживается Local Security Authority (LSASS.EXE), который и показывает диалог входа в систему.

Это диалоговое окно показывается примерно тогда, когда Services Subsystem стартует сетевую службу.