Лекция №6

Архитектура операционной системы Windows 7

Соответствие клиентских и серверных версий Windows NT

Client OS	Server OS
Windows 10	Windows Server 2019, Windows Server 2016
Windows 8.1	Windows Server 2012 R2
Windows 8	Windows Server 2012
Windows 7	Windows Server 2008 R2 SP1
Windows XP	Windows Server 2003
Windows 2000 Workstation	Windows 2000 Server
Windows NT 4.0 Workstation	Windows 4.0 Server

Различия между Windows7 и Windows Server 2008R2

	Количество поддерживаемых сокетов (32-разр. версия)	Объем поддерживаемой физической памяти (32-разр. версия), Гбайт	Количество поддерживаемых сокетов (64-разр. версия)	Объем поддерживаемой физической памяти (Itanium-версии), Гбайт	Объем поддерживаемой физической памяти (x64-версии), Гбайт
Windows 7 Starter 1	1	2	Нет	Нет	2
Windows 7 Home Basic	1	4	1	Нет	8
Windows 7 Home Premium	1	4	1	Нет	16
Windows 7 Professional	2	4	2	Нет	192
Windows 7 Enterprise	2	4	2	Нет	192
Windows 7 Ultimate	2	4	2	Нет	192
Windows Server 2008 R2 Foundation	Нет	Нет	1	Нет	8
Windows Web Server 2008 R2	Нет	Нет	4	Нет	32
Windows Server 2008 R2 Standard	Нет	Нет	4	Нет	32
Windows HPC Server 2008 R2	Нет	Нет	4	Нет	128
Windows Server 2008 R2 Enterprise	Нет	Нет	8	Нет	2048
Windows Server 2008 R2 Datacenter	Нет	Нет	64	Нет	2048
Windows Server 2008 R2 for Itanium-Based Systems	Нет	Нет	64	2048	Нет

Различия между Windows7 и Windows Server 2008R2

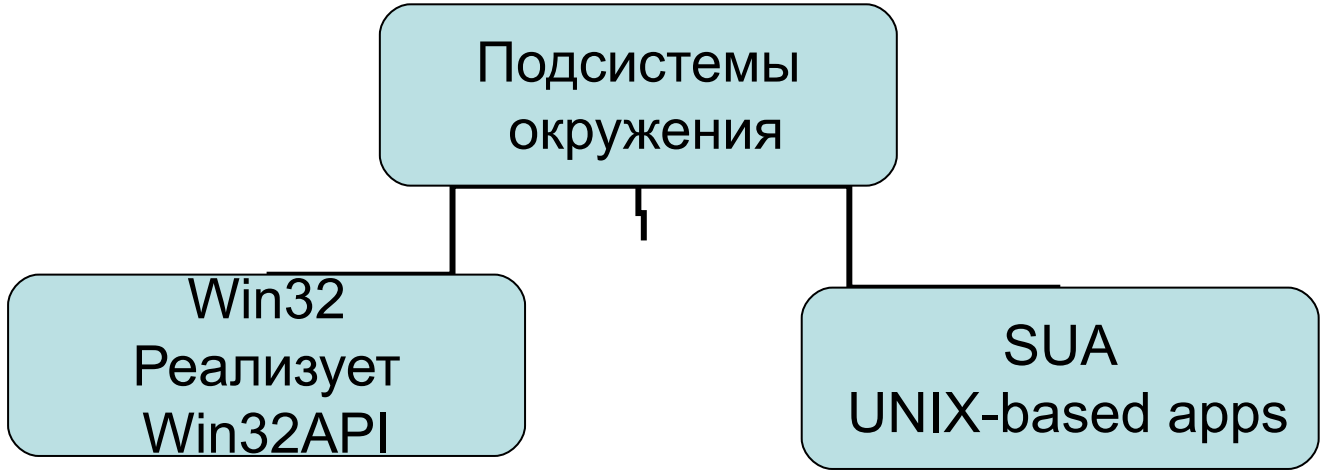
- Информация о типе системы хранится в ключах реестра ProductType и ProductSuite из раздела
- HKLM\SYSTEM\CurrentControlSet\Control\ProductOptions
- Значения ProductType

Версия Windows	Значение ProductType
Windows client	WinNT
Windows server (контроллер домена)	LanmanNT
Windows server (только сервер)	ServerNT

- Значение ProductPolicy содержит кэшировнную копию данных, хранящихся в файле Tokens.dat
- Tokens.dat устанавливает различия между версиями Windows и допускаемыми в них функциями
- \Windows\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft\
- \SoftwareProtectionPlatform\Tokens.dat

Подсистемы окружения

- Каждый исполняемый файл (EXE) принадлежит одной подсистеме.
- Приложения не могут вызывать системные сервисы Windows NT напрямую. Вместо этого они обращаются к DLL подсистем. Эти DLL предоставляют документированный интерфейс между программами и вызываемой ими подсистемой.
- В Windows Ultimate и Enterprise и серверные версии включена подсистема SUA (Psxdll.dll)



Подсистема WIN32 состоит из:

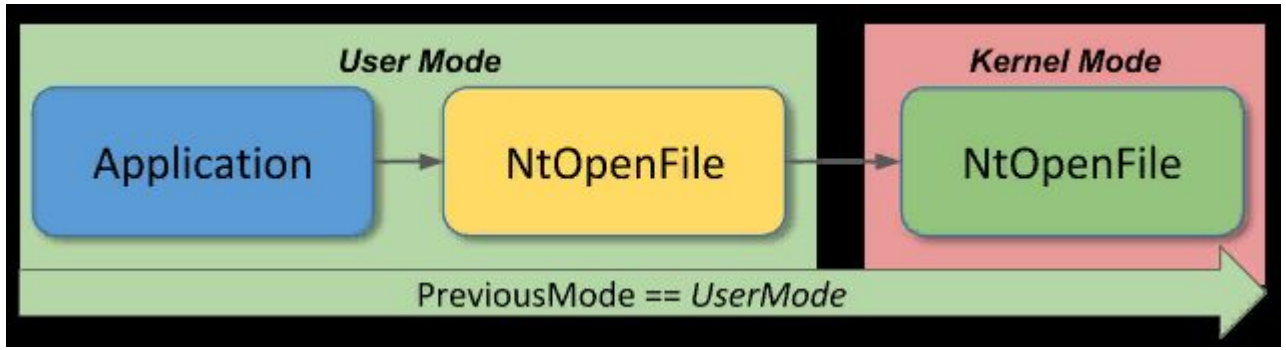
Процесса подсистемы окружения Csrss.exe (CSRSS.exe вызывает загрузку библиотек Basesrv.dll, Winsrv.dll, Csrsrv.dll), предоставляющего:

  - поддержку создания и удаления процессов и потоков;
  - частичную поддержку процессов 16-разрядной виртуальной DOS-машины (VDM);
  - множество других функций, например GetTmpFile, DefineDosDevice, ExitWindowsEx, а также несколько функций поддержки естественных языков.
- *Драйвера режима ядра (Win32k.sys),* включающего.-
  - диспетчер окон, который управляет отрисовкой и выводом окон на экран, принимает ввод с клавиатуры, мыши и других устройств, а также передает пользовательские сообщения приложениям;
  - Graphics Device Interface (GDI) - библиотеку функций для устройств графического вывода.
- *Хост процесса консоли conhost.exe* - предоставляющего поддержку символьных приложений
- *DLL-модулей подсистем* (Kernel32.dll, Advapi32.dll, User32.dll и Gdi32.dll)
- *Драйверов графических устройств*

Ntdll.dll — специальная библиотека системной поддержки

Она содержит функции двух типов:

- интерфейсы диспетчера системных сервисов (system service dispatch stubs):
  - *NtCreateFile, NtSetEvent*.
- внутренние функции поддержки, используемые подсистемами, DLL подсистем и другими компонентами ОС



Исполнительная система (executive) находится на верхнем уровне Ntoskrnl.exe (ядро располагается на более низком уровне). В ее состав входят функции следующего типа.

- Экспортируемые функции, доступные для вызова из пользовательского режима. Эти функции называются *системными сервисами* и экспортируются через Ntdll. Большинство сервисов доступно через Win32 API или API других подсистем окружения.

- Экспортируемые функции, доступные для вызова только из режима ядра и документированные в *DDK (Device Driver Kit)* или *Windows Installable File System (IFS) Kit* (*www.microsoft.com/ddk/ifskit*).

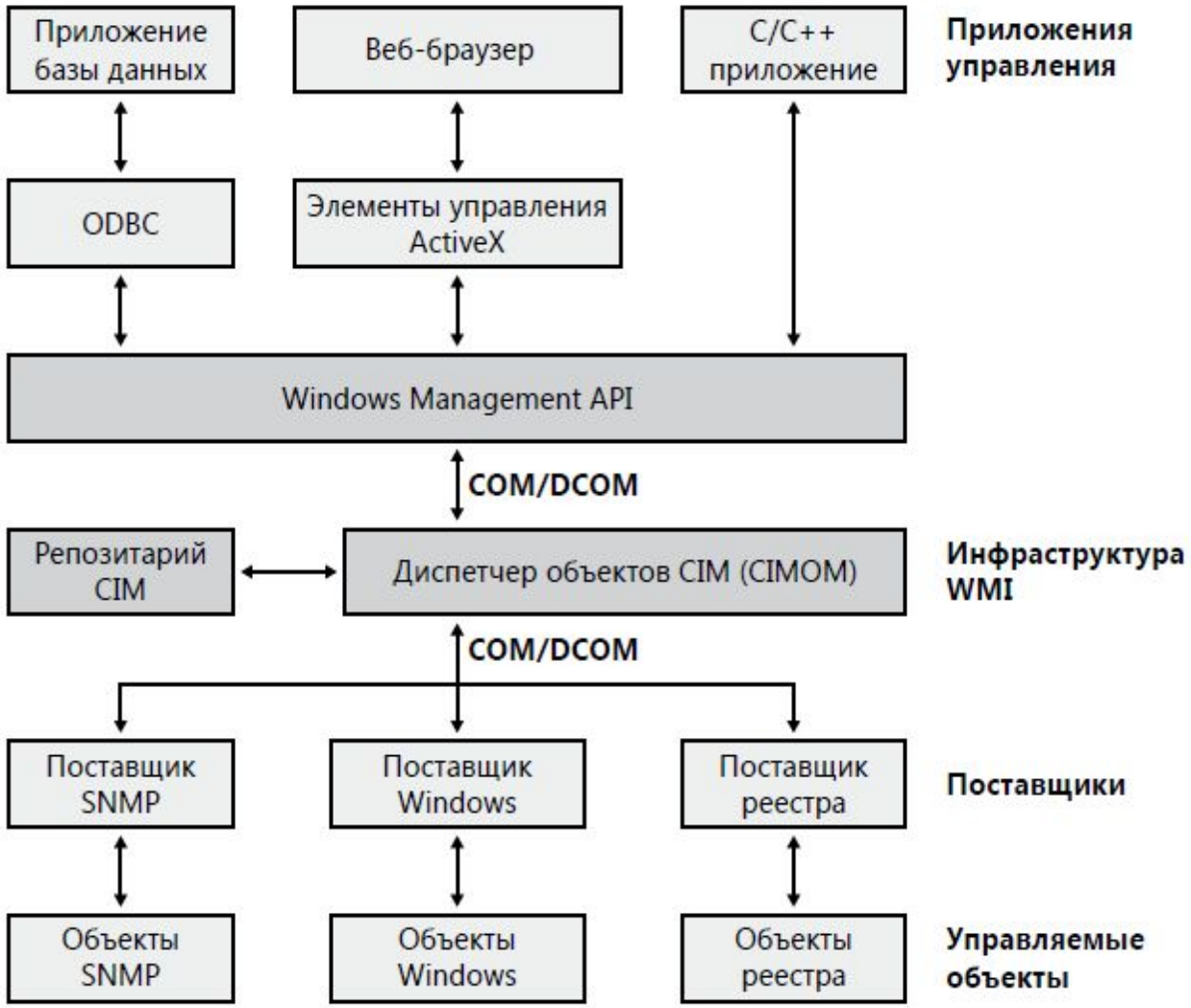
- Экспортируемые функции, доступные для вызова только из режима ядра, но не описанные в Windows DDK или IFS Kit (например, функции, которые используются видеодрайвером, работающим на этапе загрузки, и чьи имена начинаются с *Inbtf).*

- Функции, определенные как глобальные, но не экспортируемые символы. Включают внутренние функции поддержки, вызываемые в Ntoskrnl; их имена начинаются с *Iop* (функции поддержки диспетчера ввода-вывода) или с *Mi* (функции поддержки управления памятью).
- Внутренние функции в каком-либо модуле, не определенные как глобальные символы

Исполнительная система состоит из следующих основных компонентов

- *Диспетчер конфигурации* , отвечающий за реализацию и управление системным реестром
- *Диспетчер процессов и потоков*, создающий и завершающий процессы и потоки. Низкоуровневая поддержка процессов и потоков реализована в ядре Windows7, а исполнительная система дополняет эти низкоуровневые объекты своей семантикой и функциями.
- *Справочный монитор безопасности* , реализующий политики безопасности на локальном компьютере. Он охраняет ресурсы операционной системы, осуществляя аудит и контролируя доступ к объектам в период выполнения.
- *Диспетчер ввода-вывода*, реализующий ввод-вывод и отвечающий за пересылку ввода-вывода нужным драйверам устройств для дальнейшей обработки
- *Диспетчер Plug and Play*, определяющий, какие драйверы нужны для поддержки конкретного устройства, и загружающий их.
- *Диспетчер электропитания*, который координирует события, связанные с электропитанием, и генерирует уведомления системы управления электропитанием, посылаемые драйверам.
- *Подпрограммы WDM Windows Management Instrumentation*, позволяющие драйверам публиковать информацию о своих рабочих характеристиках и конфигурации, а также получать команды от службы WMI пользовательского режима. Потребители информации WMI могут находиться как на локальной машине, так и на любом компьютере в сети.
- *Диспетчер кэша*, повышающий производительность файлового ввода-вывода за счет сохранения в основной памяти дисковых данных
- *Диспетчер виртуальной памяти*, реализующий виртуальную память

Архитектура WMI



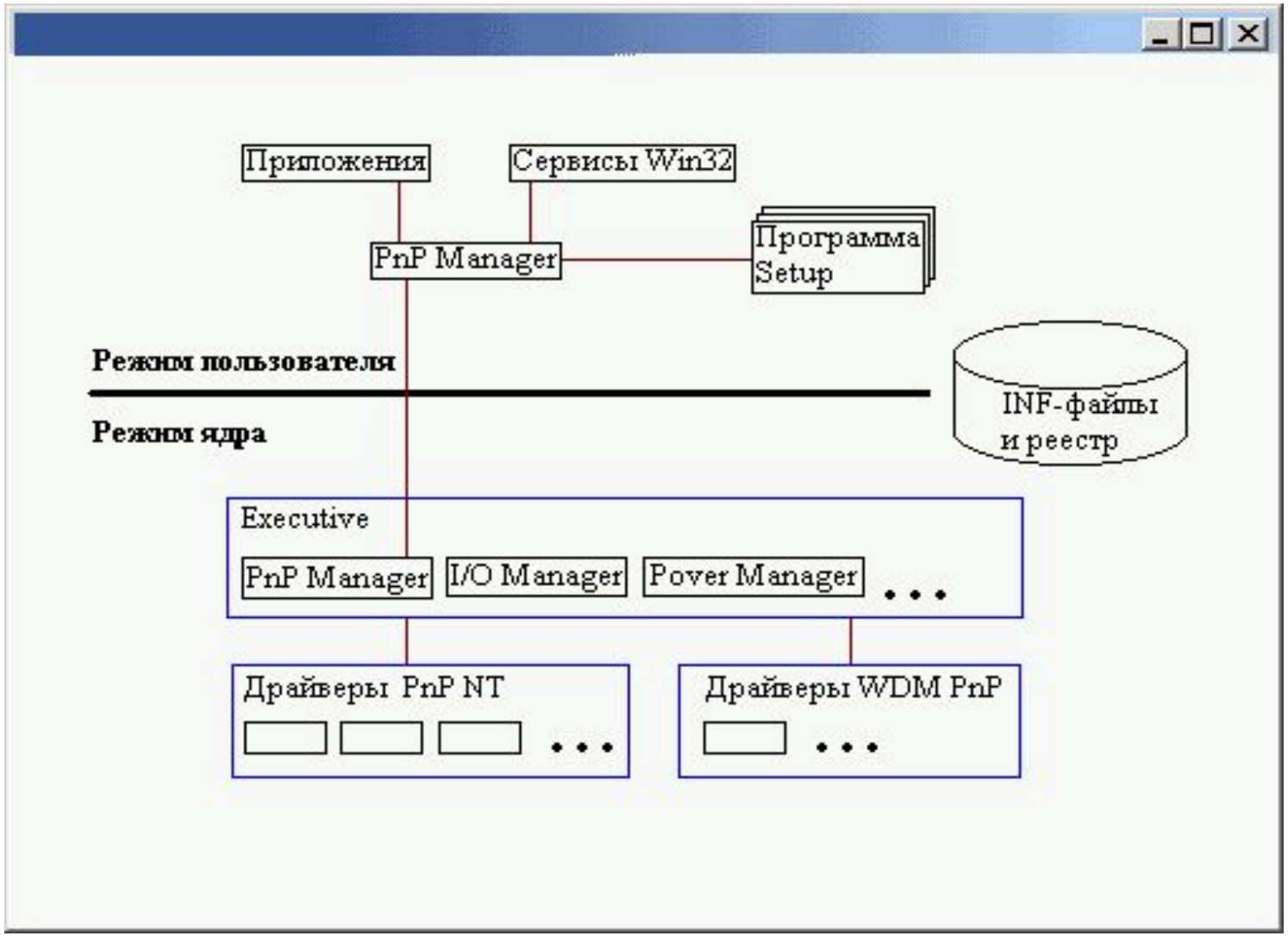
Common Information Model (CIM) — стандарт, определяющий согласованную модель, с помощью которой сетевые устройства, системы и приложения могут отображать информацию о самих себе и предоставлять ее инструментам управления

CIM — это часть Web Based Enterprise Management (WBEM), инициативы группы по стандартам Desktop Management Task Force, которая приняла язык расширяемой разметки Extensible Markup Language (XML) в качестве стандартизованного средства структурирования данных CIM, а протокол HyperText Transfer Protocol (HTTP) — для передачи подготовленной таким образом данных от системы к системе

Состав WMI (Windows Management Instrumentation):

- управляющие программы (management applications, например, Windows Script Host, MMC)
- ядро WMI (WMI infrastructure)
- провайдеры или поставщики(providers)
- управляемые объекты (managed objects)
- WMI Code Creator v1.0

Архитектура Plug and Play



Технология Plug-and-play (PnP) поддерживается комбинацией аппаратного и программного обеспечения, позволяющей распознавать и настраивать аппаратные изменения в конфигурации почти без вмешательства пользователя

Ядро и HAL

- Ядро состоит из набора функций в Ntoskrnl.exe, предоставляющих фундаментальные механизмы (в том числе планирования потоков и синхронизации), которые используются компонентами исполнительной системы и низкоуровневыми аппаратно-зависимыми средствами поддержки (диспетчеризации прерываний и исключений), различными в каждой процессорной архитектуре
- HAL — это загружаемый модуль режима ядра (Hal.dll), предоставляющий низкоуровневый интерфейс с аппаратной платформой, на которой выполняется Windows

x86:

- *«Компьютер с ACPI», ACPI PIC HAL (Halacpi.dll)*

Стандартный компьютер•Компьютер с ACPI

- *«Многопроцессорный компьютер с ACPI», ACPI APIC MP HAL (Halmacpi.dll)*

Стандартный компьютер•Компьютер с ACPI•Многопроцессорный компьютер с ACPI•Многопроцессорный компьютер с MPS

x64 и ARM процессоры:

Hal.dll, так как эти процессоры нуждаются в поддержке APIC и ACPI