Операционные системы

Архитектура ОС семейства MS Windows 2000-2008

Архитектура MS Windows

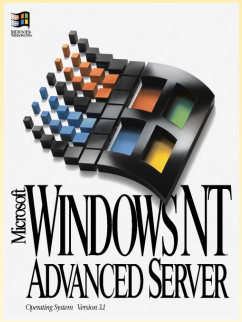
Краткая характеристика ОС семейства MS Windows 2000-2008

История развития Windows NT

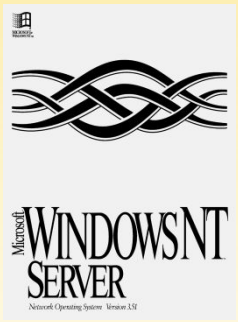
Product Name	Internal Version Number	Release Date
Windows NT 3.1	3.1	July 1993
Windows NT 3.5	3.5	September 1994
Windows NT 3.51	3.51	May 1995
Windows NT 4.0	4.0	July 1996
Windows 2000	5.0	December 1999
Windows XP	5.1	August 2001
Windows Server 2003	5.2	March 2003
Windows Vista	6 0 (Build 6000)	January 2007
Windows Server 2008	6.0 (Build 6001)	March 2008
Windows Server 2008 R2	6.1 (Build 61xx)	October 2009
Windows 7	6.1 (Build 61xx)	October 2009

Эволюция Windows Server

Сервер файлов и печати уровня департамента

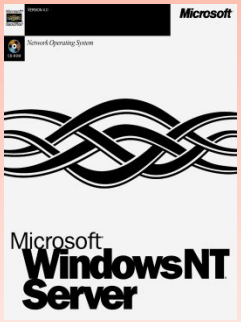


1993



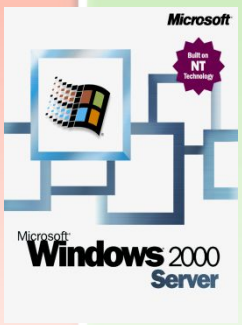
1994/5

Сервера интранет и центры обработки данных

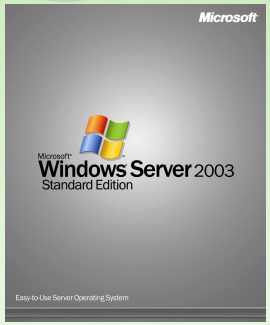


1996

Простота объединения с помощью веб-сервисов



2000



2003

Основная характеристика Windows 2000-2008

Система Windows 2000-2008 не является дальнейшим развитием ранее существовавших продуктов. Ее архитектура создавалась с нуля с учетом предъявляемых к современной ОС требований:

- *совместимость (compatible);*
- *переносимость (portability);*
- *масштабируемость (scalability);*
- *безопасность (security);*
- *распределенная обработка (distributed processing);*
- *надежность и отказоустойчивость (reliability and robustness);*
- *локализации (localization);*
- *расширяемость (extensibility).*

Совместимость

- *совместимость (compatible)* – поддержка существующих файловых систем, прикладных сред и сетевых интерфейсов. Специальные сервисы для интеграции с UNIX – Windows Services for UNIX;
- *переносимость (portability);*
- *масштабируемость (scalability);*
- *безопасность (security);*
- *распределенная обработка (distributed processing);*
- *надежность и отказоустойчивость (reliability and robustness);*
- *локализации (localization);*
- *расширяемость (extensibility).*

Windows Services for UNIX

- упрощают интеграцию Windows 2000-2008 с существующими UNIX-сетями;
- улучшают управляемость, упрощают администрирование сетей и учетных записей;
- позволяют продолжить использование существующих UNIX-ресурсов и опыта, накопленного в работе с UNIX-системами.

Переносимость

- *совместимость (compatible);*
- *переносимость (portability)* системы, которая работает как на CISC (x86), так и на RISC-процессорах (MIPS R4000 (только NT) и Digital Alpha AXP). ОС MS Windows 2003 поддерживает архитектуру x86 и IA64, AMD x86-64, EM64T.
- *масштабируемость (scalability);*
- *безопасность (security);*
- *распределенная обработка (distributed processing);*
- *надежность и отказоустойчивость (reliability and robustness);*
- *локализации (localization);*
- *расширяемость (extensibility).*

Переносимость

- MS Windows рассчитана на разные аппаратные платформы, включая как CISC-системы Intel, так и RISC-системы. Windows NT первого выпуска поддерживала архитектуры x86 и MIPS.
- Спустя некоторое время была добавлена поддержка Alpha AXP производства DEC. Хотя Alpha AXP был 64-разрядным процессором, Windows NT работала с ним в 32-разрядном режиме. В ходе разработки Windows 2000 была создана ее 64-разрядная версия специально под Alpha AXP, но в свет она так и не вышла. В Windows NT 3.51 ввели поддержку четвертой процессорной архитектуры — Motorola PowerPC. В связи с изменениями на рынке необходимость в поддержке MIPS и PowerPC практически отпала еще до начала разработки Windows 2000. Позднее производитель отозвал поддержку архитектуры Alpha AXP, и в Windows 2000 осталась поддержка лишь архитектуры x86.
- В самые последние выпуски — Windows XP и Windows Server 2003 — добавлена поддержка трех семейств 64-разрядных процессоров: Intel Itanium IA-64, AMD x86-64 и Intel 64-bit Extension Technology (EM64T) для x86 (эта архитектура совместима с архитектурой AMD x86-64, хотя есть небольшие различия в поддерживаемых командах). Последние два семейства процессоров называются *системами с 64-разрядными расширениями* и обычно обозначаются как x64.

Масштабируемость

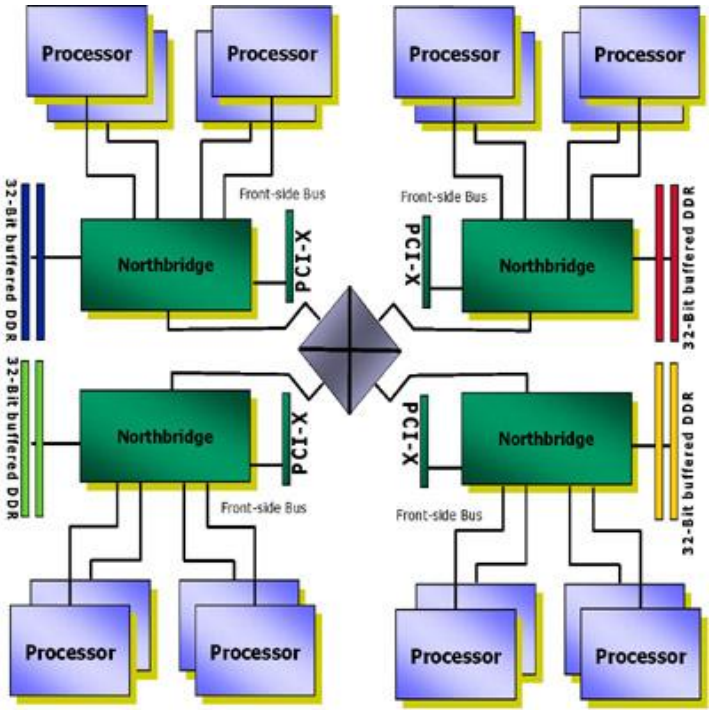
- *совместимость (compatible);*
- *переносимость (portability);*
- *масштабируемость (scalability)* означает, что Windows Server 2003 Datacenter Edition поддерживает многопроцессорные системы с числом процессоров от 1 до 64, Windows Server 2008 R2 до 256.
- *безопасность (security);*
- *распределенная обработка (distributed processing);*
- *надежность и отказоустойчивость (reliability and robustness);*
- *локализации (localization);*
- *расширяемость (extensibility).*

Масштабируемость MS Windows XP-2003

- SMP-системы (оперативная память физически представляет последовательное адресное пространство, доступ к которому имеют одновременно все процессоры системы по единой шине).
- Логические процессоры (hyperthreading)
- NUMA (Non-Uniform Memory Architecture)

NUMA

- Процессоры группируются в узлы (Nodes).
- В каждом узле несколько CPU и память (SMP-система, но за счет минимальной компоновки элементов достигается высокая пропускная способность между процессором и локальной памятью модуля).
- Узлы объединяются шиной.



Безопасность

- *совместимость (compatible);*
- *переносимость (portability);*
- *масштабируемость (scalability);*
- Windows 2000-2008 имеет однородную *систему безопасности (security)*, удовлетворяющую стандарту C-2 "Оранжевая книга". В корпоративной среде критическим приложениям обеспечивается полностью изолированное окружение.
- *распределенная обработка (distributed processing);*
- *надежность и отказоустойчивость (reliability and robustness);*
- *локализации (localization);*
- *расширяемость (extensibility).*

Распределенная обработка

- *совместимость (compatible);*
- *переносимость (portability);*
- *масштабируемость (scalability);*
- *безопасность (security);*
- *распределенная обработка (distributed processing)* означает, что Windows 2000-2008 имеет встроенные в систему сетевые возможности (TCP/IP, Netbios);
- *надежность и отказоустойчивость (reliability and robustness);*
- *локализации (localization);*
- *расширяемость (extensibility).*

Надежность и отказоустойчивость

- *совместимость (compatible);*
- *переносимость (portability);*
- *масштабируемость (scalability);*
- *безопасность (security);*
- *распределенная обработка (distributed processing);*
- *надежность и отказоустойчивость (reliability and robustness)* обеспечиваются архитектурными особенностями, которые защищают прикладные программы от повреждения друг другом и ОС. Windows 2000-2008 использует отказоустойчивую структурированную обработку особых ситуаций на всех архитектурных уровнях, которая включает восстанавливаемую файловую систему NTFS и обеспечивает защиту с помощью встроенной системы безопасности и усовершенствованных методов управления памятью;
- *локализации (localization);*
- *расширяемость (extensibility).*

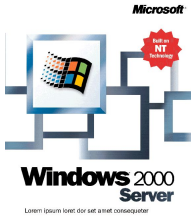
Локализация

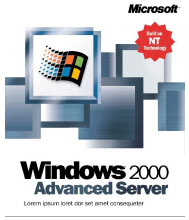
- *совместимость (compatible);*
- *переносимость (portability);*
- *масштабируемость (scalability);*
- *безопасность (security);*
- *распределенная обработка (distributed processing);*
- *надежность и отказоустойчивость (reliability and robustness);*
- возможности *локализации (localization)* предоставляют средства для работы на национальных языках, что достигается применением стандарта ISO Unicode (разработан Международной организацией по стандартизации);
- *расширяемость (extensibility).*

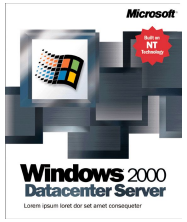
Расширяемость

- *совместимость (compatible);*
- *переносимость (portability);*
- *масштабируемость (scalability);*
- *безопасность (security);*
- *распределенная обработка (distributed processing);*
- *надежность и отказоустойчивость (reliability and robustness);*
- *локализации (localization);*
- благодаря модульному построению системы обеспечивается *расширяемость (extensibility)* Windows 2000-2008 – гибкое добавление новых модулей на различные уровни ОС.

Семейство Windows 2000

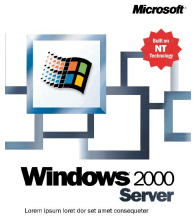


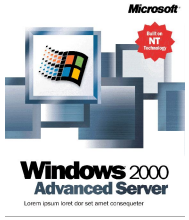


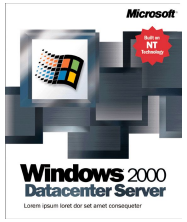


- **Windows 2000 Professional**
  - До 2 ЦПУ, 4 ГБ ОЗУ
- **Windows 2000 Server**
  - До 4 ЦПУ, 4 ГБ ОЗУ
- **Windows 2000 Advanced Server**
  - До 8 ЦПУ, 8 ГБ ОЗУ
  - 2-узловая кластеризация
- **Windows 2000 Datacenter Server**
  - До 32 ЦПУ, 64 ГБ ОЗУ
  - 4-узловая кластеризация

Семейство Windows 2003







- **Windows Server 2003 Web Edition**
  - До 2 ЦПУ, 2 ГБ ОЗУ
- **Windows Server 2003 Standard Edition**
  - До 4 ЦПУ, 4 ГБ ОЗУ
- **Windows Server 2003 Enterprise Edition**
  - До 8 ЦПУ, 32 ГБ ОЗУ
  - 2-узловая NUMA
- **Windows Compute Cluster Server 2003**
  Windows Server 2003 Datacenter Edition
  - До 64 (32) ЦПУ, 128 (64) ГБ ОЗУ
  - 8-узловая NUMA
- **Windows Storage Server**
  - Выделенный сервер печати и файловый сервер

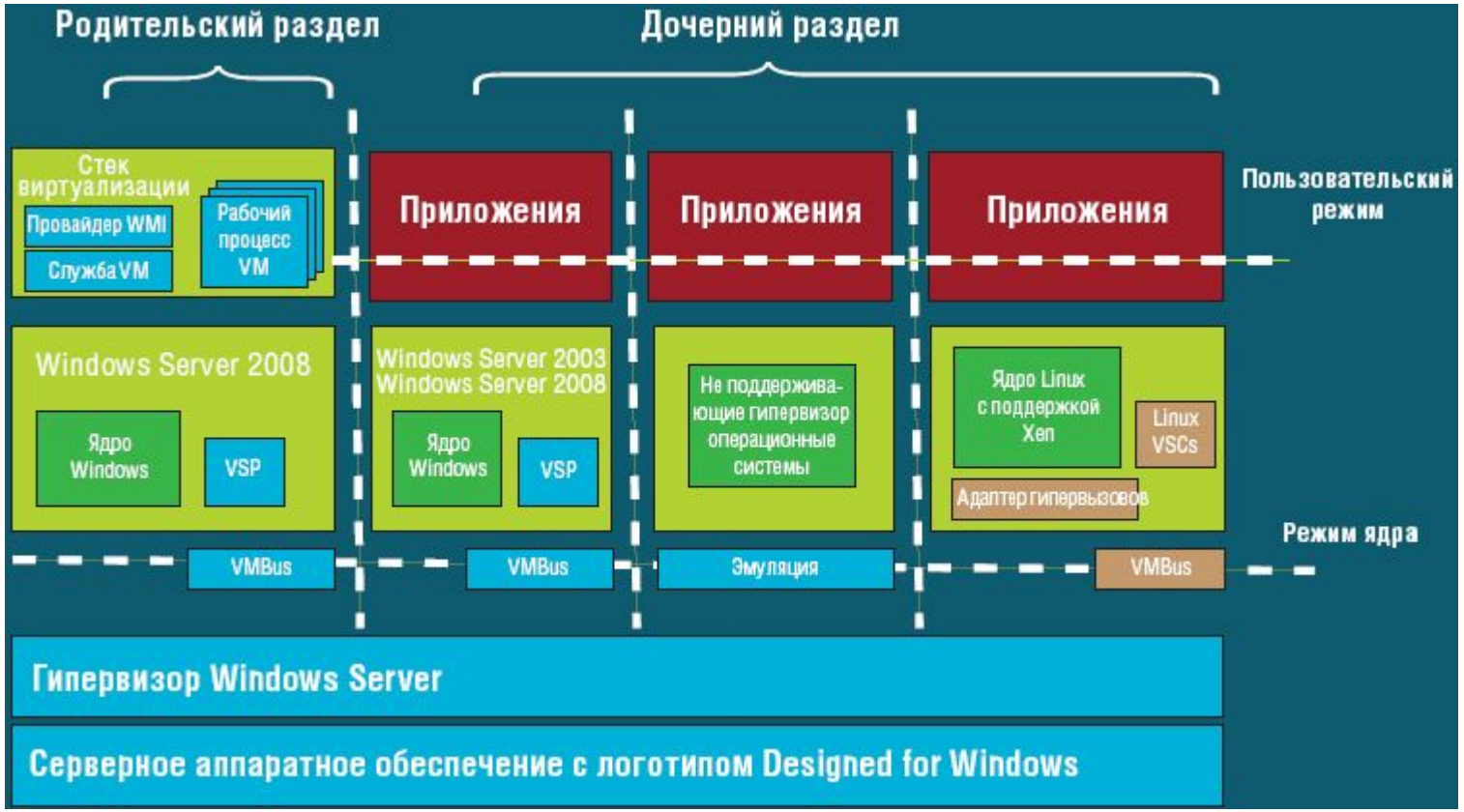
Windows Server 2008

- Windows Server 2008 включает вариант установки называемый **Server Core** (русск. *Установка ядра сервера*). *Server Core* — это существенно облегченная установка Windows Server 2008 в которую не включена оболочка Windows Explorer — это существенно облегченная установка Windows Server 2008 в которую не включена оболочка Windows Explorer. Вся настройка и обслуживание выполняется при помощи интерфейса командной строки — это существенно облегченная установка Windows Server 2008 в которую не включена оболочка Windows Explorer. Вся настройка и обслуживание выполняется при помощи интерфейса командной строки Windows, или подключением к серверу удалённо посредством Консоли управления.

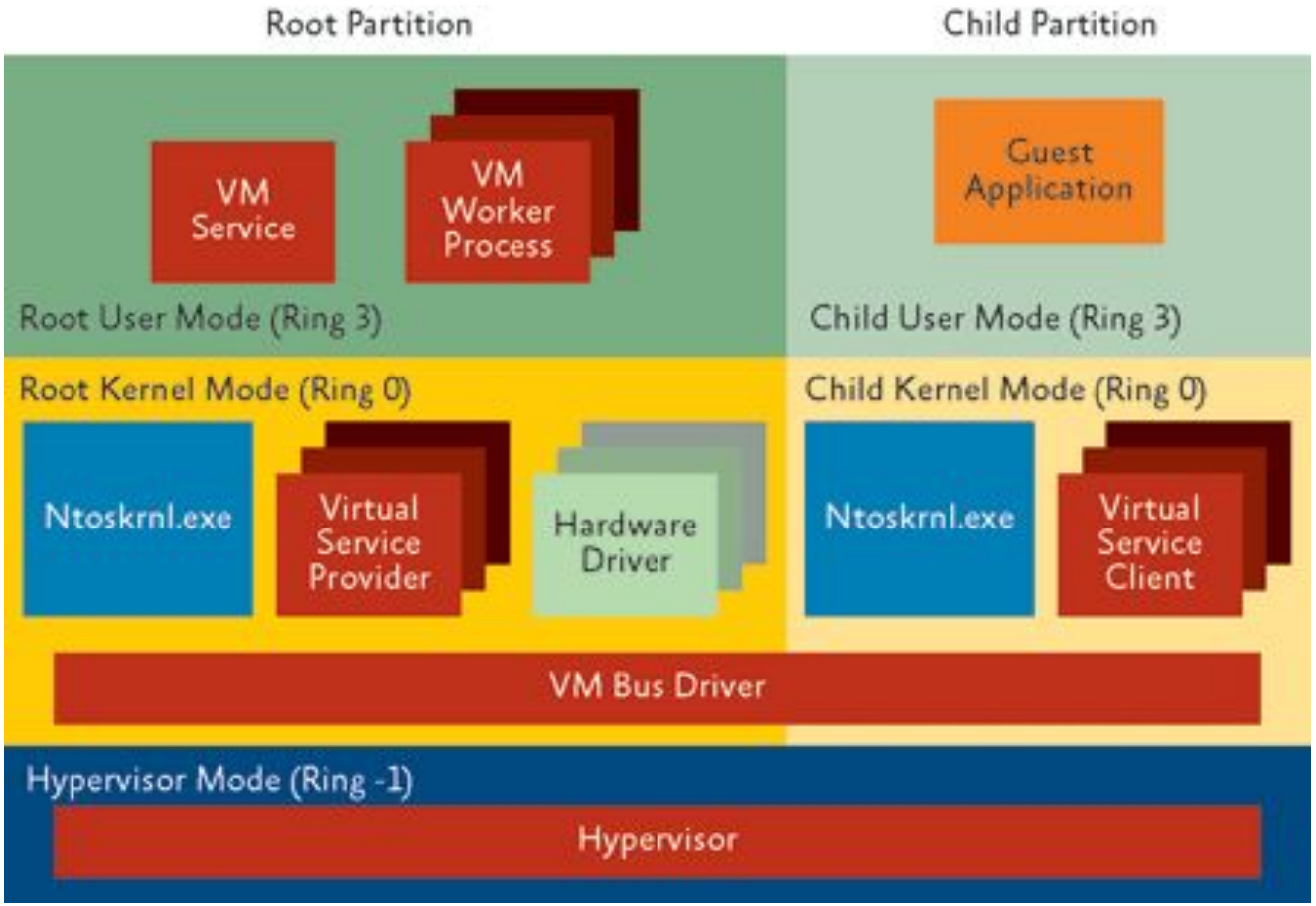
Windows Server 2008

- Службы Терминалов. произошло значительное обновление *Служб Терминалов* (Terminal Services). *Службы Терминалов* теперь поддерживают Remote Desktop Protocol 6.0.
- Windows PowerShell - расширяемая оболочкаWindows PowerShell - расширяемая оболочка с интерфейсом командной строкиWindows PowerShell - расширяемая оболочка с интерфейсом командной строки и сопутствующим языком сценариев.
- Самовосстанавливающаяся NTFS – нет необходимости перезагрузки сервера для исправления ошибок файловой системы.
- Microsoft Hyper-V – система виртуализацииMicrosoft Hyper-V – система виртуализации на основе

Microsoft Hyper-V



Microsoft Hyper-V



Семейство Windows 2008

- Windows Server 2008 Standard Edition (x86Windows Server 2008 Standard Edition (x86 и x64)
- Windows Server 2008 Enterprise Edition (x86 и x64)
- Windows Server 2008 Datacenter Edition (x86 и x64)
- Windows HPC Server 2008Windows HPC Server 2008 (заменяющий Windows Compute Cluster Server 2003)
- Windows Web Server 2008 (x86 и x64)
- Windows Storage Server 2008 (x86 and x64)
- Windows Server 2008 для систем основанных на Itanium

Windows 2008 R2

- Серверный вариант Windows 7 на основе нового ядра WinMin.
- Новые возможности включают улучшенную виртуализацию, новую версию Active Directory, Internet Information Services 7.5 и поддержку до 256 процессоров.
- Система доступна только в 64-разрядном варианте.

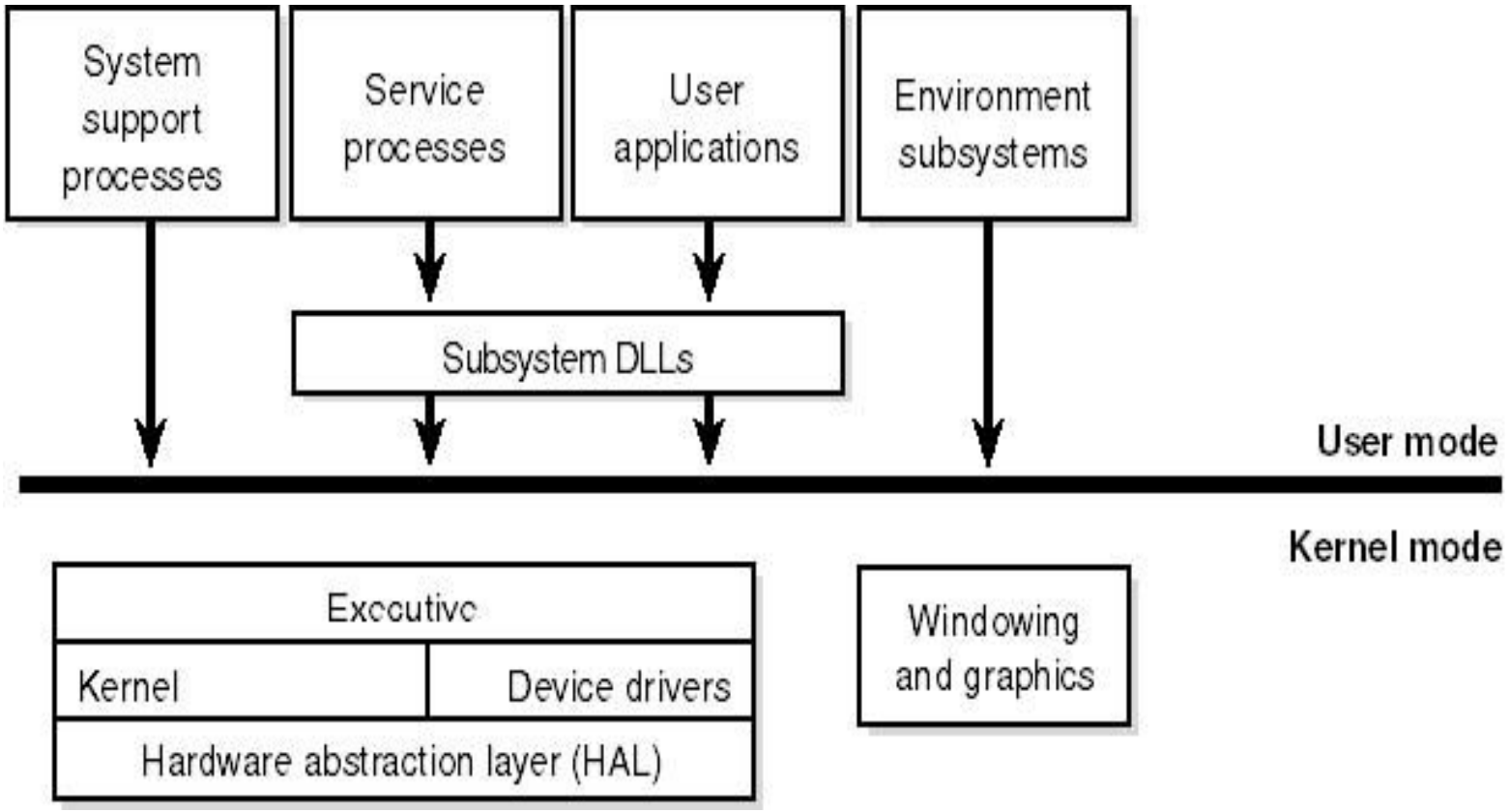
Архитектура MS Windows

Архитектура ОС Windows
2000-2003

Краткая характеристика

- Многоуровневая ОС.
- Ядро работает в защищенном режиме.
- Присутствует микроядро, но оно дополнительно не защищено от остальных фрагментов ядра (т.е. по сути присутствует гибридное ядро).
- В архитектуре можно выделить наноядро – уровень абстракции от оборудования HAL.
- Компоненты ядра спроектированы на основе принципов построения объектно-ориентированных систем, хотя Windows не является объектно-ориентированной системой в точном смысле этого понятия, поскольку основная часть кода системы написана на Си из соображений обеспечения высокой скорости выполнения и переносимости.

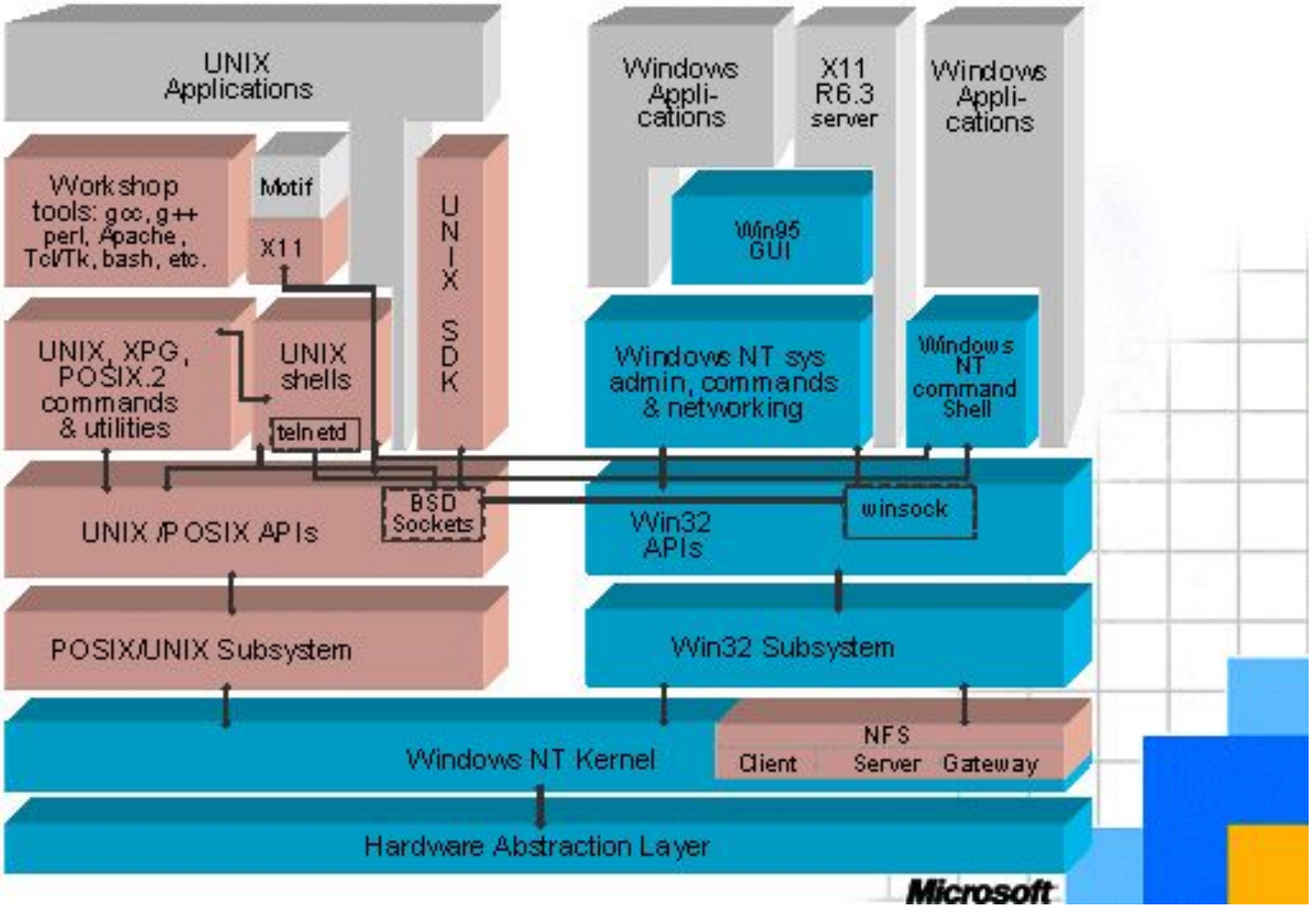
Упрощенная архитектура Windows 2000



Пользовательский режим

- **Специальные процессы поддержки системы**, например, процесс регистрации пользователя и менеджер сессий, которые не являются службами Windows.
- **Процессы сервера**, которые являются службами Windows (аналог демонов в ОС Unix). Примером может быть регистратор событий (Event Logger). Многие дополнительно устанавливаемые приложения, такие как MS SQL Server и Exchange Server, также включают компоненты, работающие как службы Windows.
- **Подсистемы среды** представляют собой защищенные серверы пользовательского режима (user-mode), которые обеспечивают выполнение и поддержку приложений, разработанных для различного операционного окружения (различных ОС). Примером подсистем среды могут служить подсистемы Win32, Posix и OS/2 (в Windows Server 2003 нет штатной поддержки Posix и OS/2, поддержка Posix выделена в отдельный продукт Interix – компонент SFU 3.0 и выше).
- **Пользовательские приложения**.

Interix и поддержка POSIX



Структура ядра

- **исполняющая система**, которая включает управление памятью, процессами, потоками, безопасностью, вводом/выводом, межпроцессорными обменами;
- **ядро (микроядро)** выполняет низкоуровневые функции ОС: диспетчеризация потоков, прерываний и исключений, синхронизация процессоров. Ядро также включает набор процедур и базовых объектов, используемый исполняемой частью для создания высокоуровневых конструкций;
- **уровень абстракции от оборудования** (HAL – Hardware Abstraction Layer), изолирует остальное ядро от специфики аппаратной платформы, на которой выполняется ОС. Подобный подход позволяет обеспечить переносимость Windows. HAL можно рассматривать в качестве наноядра.
- **драйверы устройств** включают как файловую систему, так и аппаратные драйверы, которые транслируют пользовательские вызовы функций ввода/вывода в запросы физических устройств ввода/вывода;
- **функции графического интерфейса** пользователя работают с окнами, элементами управления и изображениями.

Исполняющая система

- Важные для производительности ОС компоненты выполняются в режиме ядра, где они взаимодействуют с оборудованием и друг с другом без использования переключателей контекста и смены режимов.
- Например, исполняющая система включает в себя менеджер виртуальной памяти, менеджер кэш-памяти, менеджер объектов, менеджер системы безопасности.
- Все эти компоненты и полностью защищены от выполняемых приложений, которые не имеют прямого доступа к коду и данным из привилегированной части операционной системы.

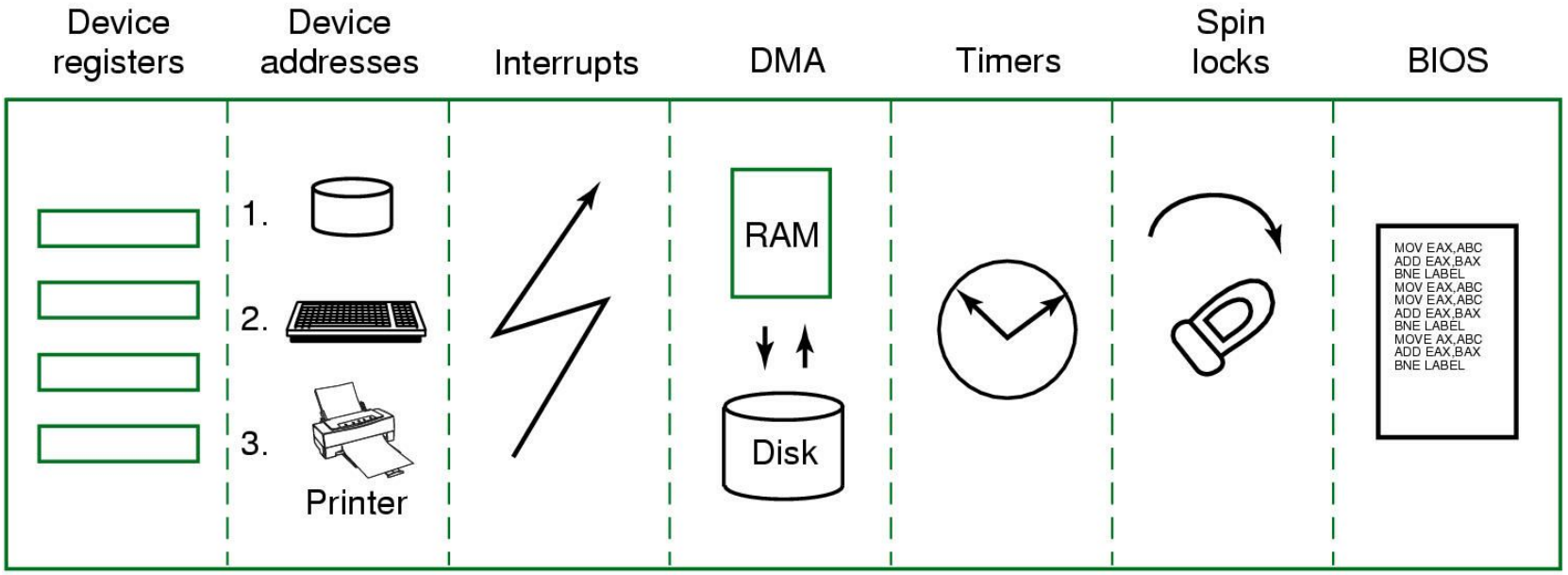
Ядро (микроядро) Windows 2000

- Микроядро (Microkernel) является основным компонентом операционной системы и координирует выполнение большинства базовых операций Windows.
- В отличие от остальной части ядра ОС, МЯ никогда не выгружается из оперативной памяти, его выполнение никогда не прерывается другими потоками.
- Код МЯ написан в основном на Си, а фрагменты, оказывающие наибольшую нагрузку на процессор, на языке Ассемблера.

Функции микроядра Windows 2000

- МЯ, в первую очередь, занимается планированием загрузки процессора на основании следующих принципов:
  - квантование времени;
  - абсолютные приоритеты;
  - динамические приоритеты.
- В случае если компьютер содержит несколько процессоров, МЯ может выполнятся на всех процессорах и синхронизирует их работу. МЯ осуществляет диспетчеризацию потоков, таким образом, чтобы максимально загрузить процессоры системы и обеспечить первоочередную обработку потоков с более высоким приоритетом.
- МЯ также обеспечивает работу других базовых объектов ядра, которые используются исполняющей системой (и в некоторых случаях экспортируются в режим пользователя).

Hardware Abstraction Layer

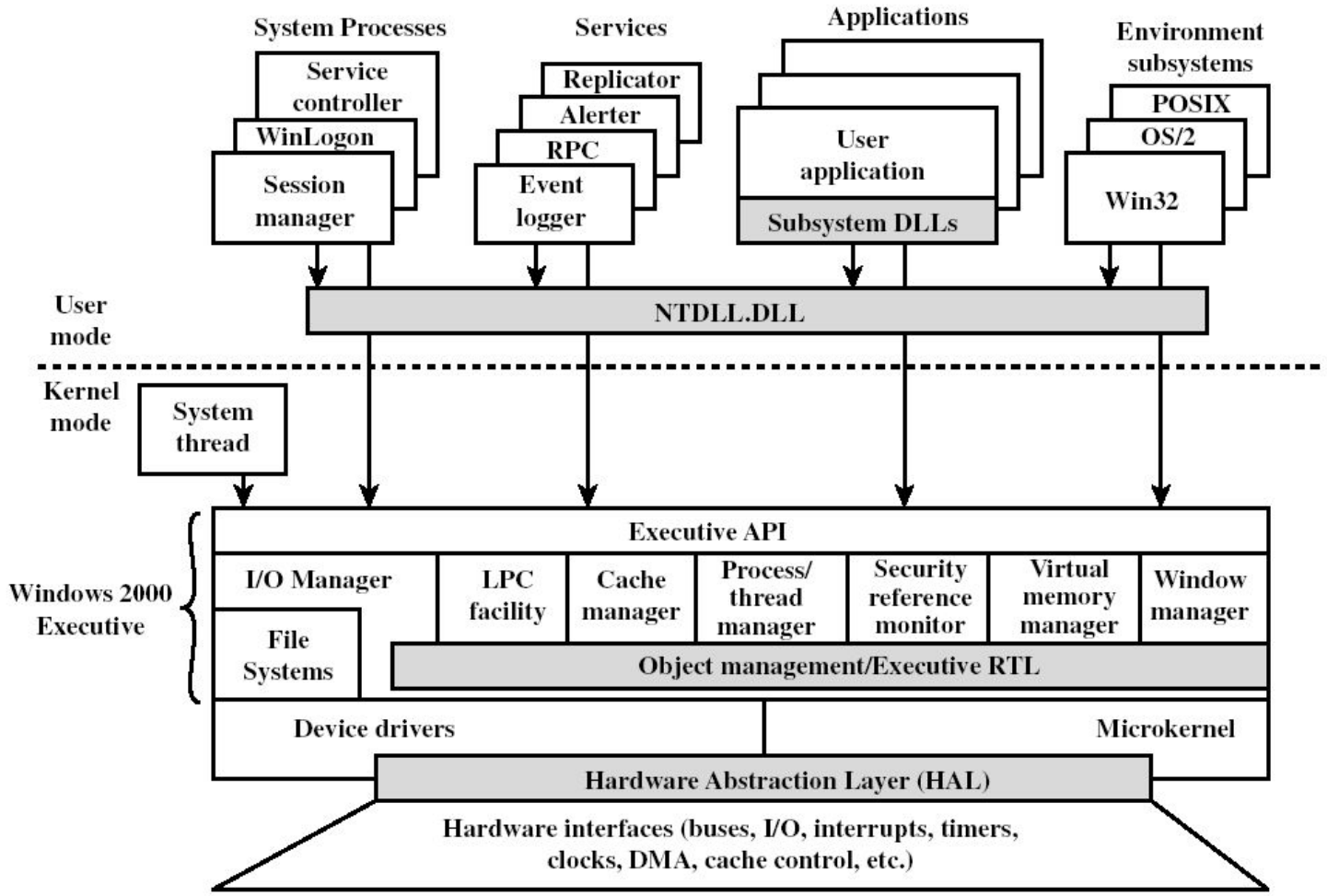


- На иллюстрации представлены элементы аппаратуры вычислительной системы, универсальный доступ к которым обеспечивает HAL.

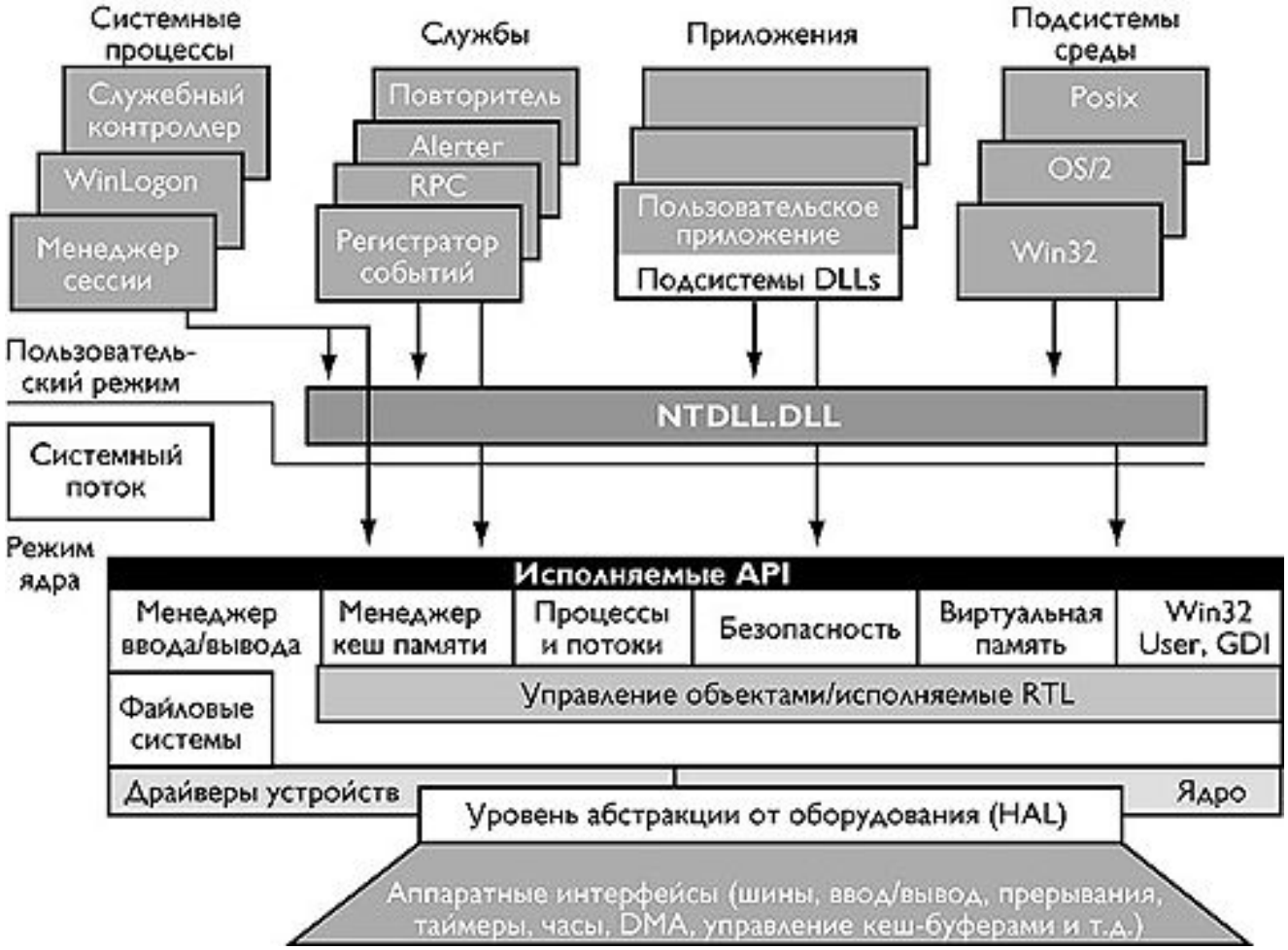
Подробная архитектура Windows 2000

- На слайде приведена общая архитектура Windows 2000-2003 и ее компонентов.
- Элементы над разделительной линией представляют собой процессы пользовательского режима, а под ней располагаются процессы ОС, выполняемые ядром.
- Потоки пользовательского режима выполняются в защищенном адресном пространстве. Однако, во время их выполнения в режиме ядра, они получают доступ к системному пространству. Таким образом, системные процессы, процессы сервера (службы), подсистема среды или пользовательское приложение имеют свое собственное адресное пространство.

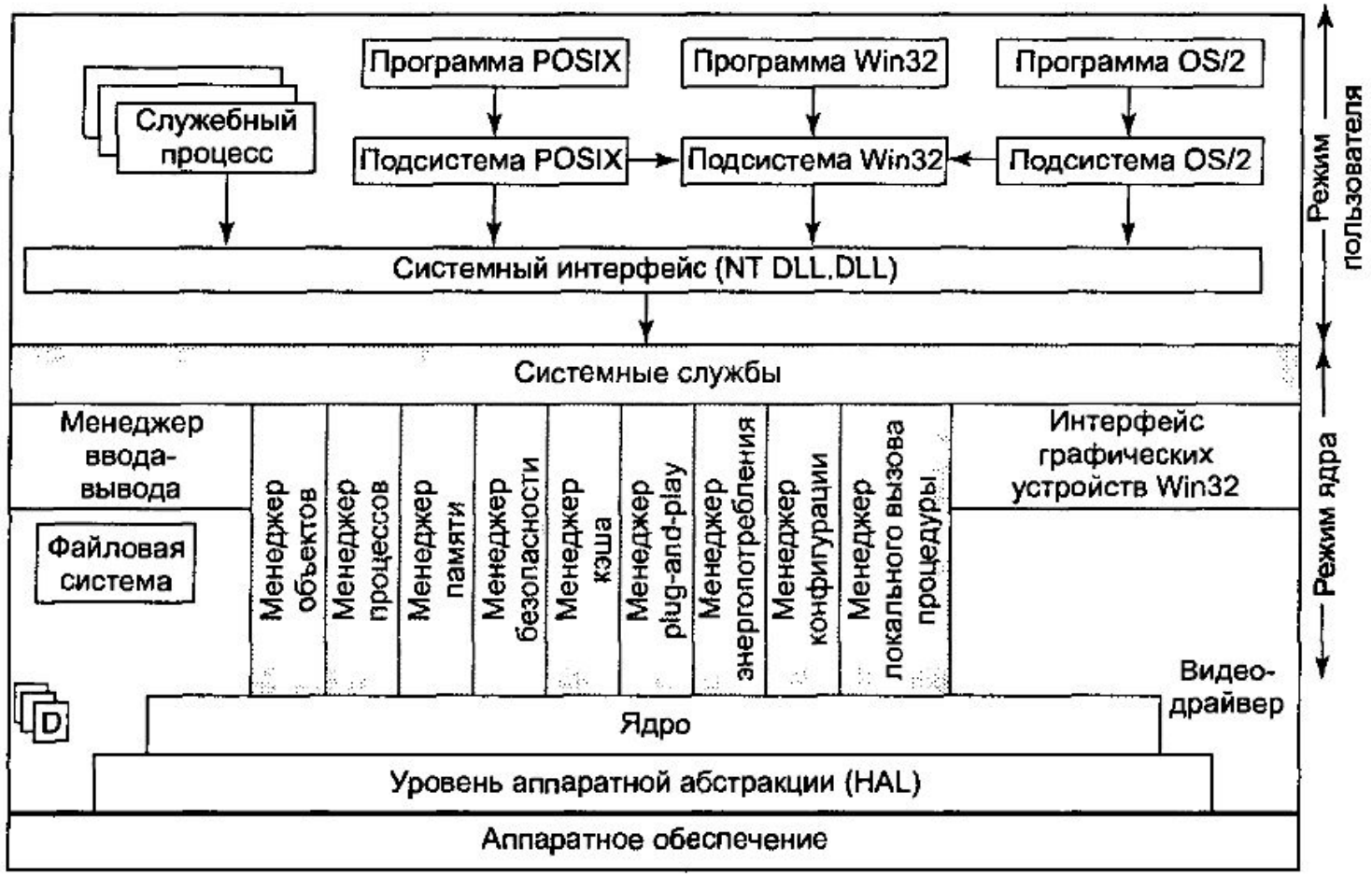
Подробная архитектура Windows 2000



Подробная архитектура Windows 2000



Подробная архитектура Windows 2000



Исполняющая система

- *Исполняющая система* включает в свой состав набор программных конструкций привилегированного режима (kernel-mode), предоставляющих базовый сервис ОС подсистемам среды.
- Исполняющая система состоит из нескольких компонентов, каждый из которых предназначен для поддержки определенного системного сервиса.

Компоненты Executive (1)

- **Менеджер процессов и потоков** управляет процессами и потоками. Фактически потоки и процессы поддерживаются в Microkernel, а менеджер добавляет новые возможности и пользовательский интерфейс.
- **Менеджер виртуальной памяти** обеспечивает для каждого процесса отдельное виртуальное адресное пространство, защищенное от воздействия других процессов. Менеджер памяти также обеспечивает низкоуровневую поддержку для менеджера кэш-памяти.
- **Менеджер кэш-памяти** улучшает производительность системы ввода/вывода файлов, размещая читаемые с диска данные в основной памяти для ускорения доступа к ним, а также откладывая на короткое время запись измененных данных на диск.

Компоненты Executive (2)

- **Менеджер объектов**, который создает, удаляет объекты и абстрактные типы данных, а также управляет ими. Объекты используются для представления таких ресурсов ОС, как процессы, потоки и объекты синхронизации.
- **Монитор безопасности** проводит политику обеспечения мер безопасности на локальном компьютере, охраняя системные ресурсы и выполняя процедуры аудита и защиты объектов.
- **Диспетчер ввода/вывода** использует независимый от устройств ввод/вывод и отвечает за пересылку данных соответствующим драйверам для дальнейшей обработки.
- **Диспетчер Plug&Play** – определяет какие драйвера нужны для конкретного устройства и загружает их.

Компоненты Executive (3)

- **Диспетчер конфигурации** отвечает за организацию и управление системным реестром.
- **Диспетчер электропитания** – координирует события, связанные с электропитанием, генерирует уведомления о событиях
- **LPC** (Local Procedure Call) передает сообщения между клиентским процессом и процессом сервера на том же самом компьютере. По сути, LPC – это оптимизированная версия процедуры удаленного вызова RPC (Remote Procedure Call).
- Широкий **набор библиотечных функций** общего типа: обработка строк, арифметические операции, преобразование типов данных, обработка структур.

Архитектура MS Windows

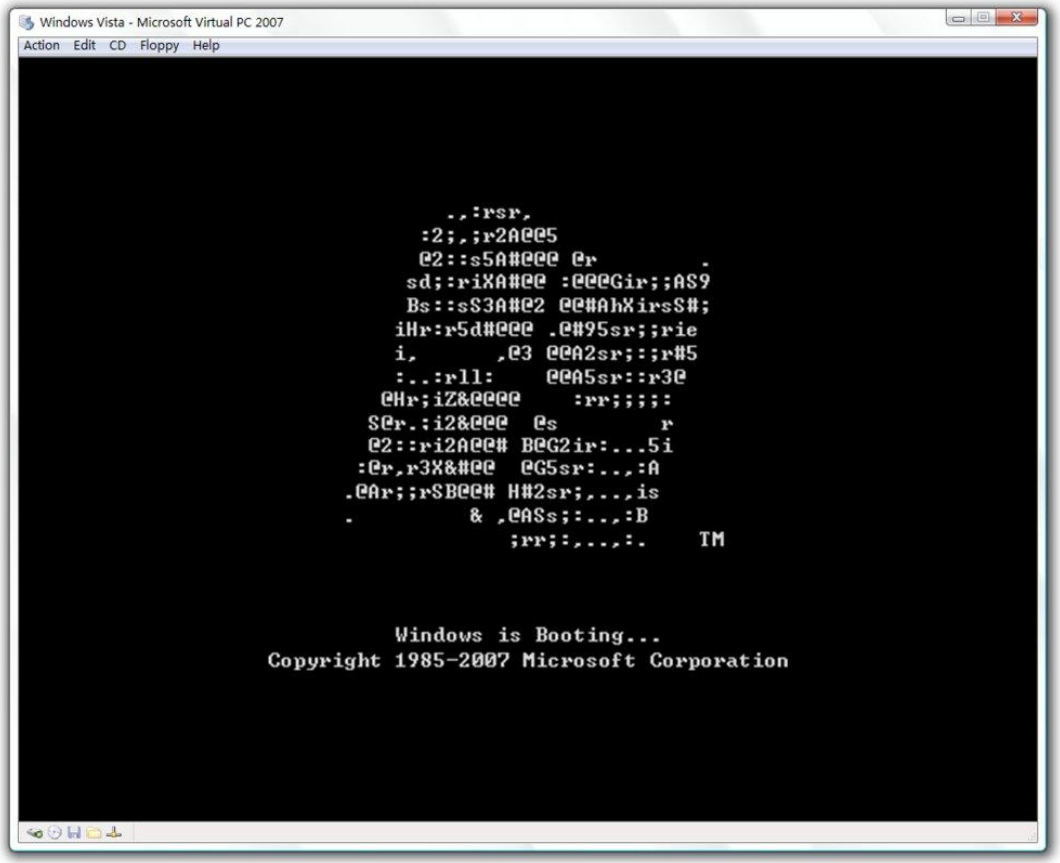
Архитектура ОС Windows
Vista и 2008 R2

Ядро MinWin

- MinWin – новое облегченное ядро Windows, реализованное в Windows 7 и Windows Server 2008 R2.
- Если некоторым образом очистить Windows, оставив лишь самые необходимые API, получится независимая ОС, которую можно загрузить и протестировать. Именно так выглядит MinWin. Это сердце Windows, организованное так, что ни один из компонентов MinWin не имеет зависимостей от компонентов, расположенных вне MinWin.
- Проводя чистку Windows путем освобождения различных слоев системы от многочисленных зависимостей, Microsoft намерена в будущем создать систему, в которой можно будет безболезненно отключать различные ее части.

Ядро MinWin в Windows 7 (1)

- В Windows 7 MinWin состоит из примерно 161 файла и занимает 28 Мб дискового пространства. При этом в нем есть свое микроядро, несколько базовых системных служб и TCP/IP-стек, в ядре нет даже интерфейса командной строки.



Ядро MinWin в Windows 7 (2)

- Кроме того, в Windows 7 применяется иная модель взаимодействия программных библиотек, отличная от "вертикальной" Win32, реализованной в Windows раньше. MinWin предполагает "горизонтальную" схему, состоящую из логических (виртуальных) и привязанных к ним физических DLL-файлов, взаимодействующих между собой на виртуальном слое с максимальной эффективностью.

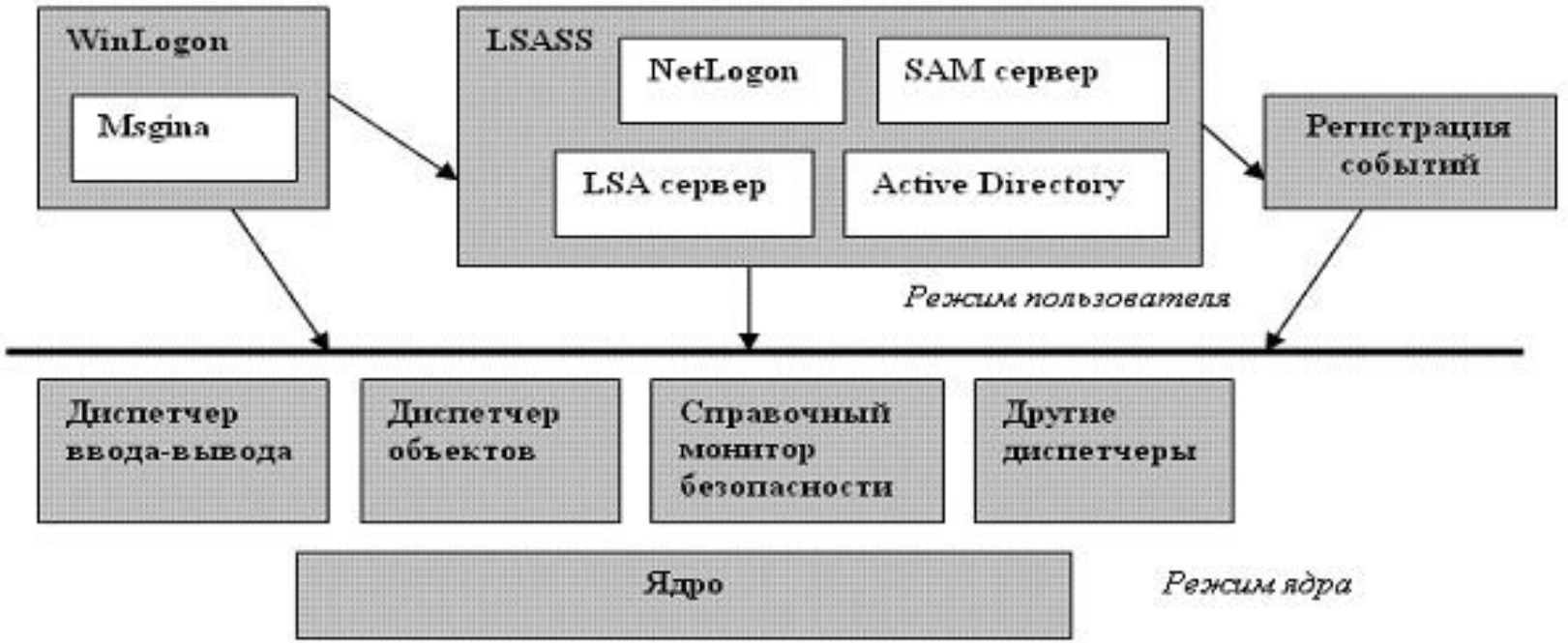
Архитектура Windows

Подсистема защиты
Windows 2000-2003

Базовые принципы уровня С2

- Выделяемая процессам память защищена таким образом, что прочитать информацию оттуда невозможно даже после того, как она уже освобождена процессом.
- Система должна быть защищена от вмешательства, например, от модификации системного кода в памяти или системных файлов на диске.
- Только системный администратор имеет физическую возможность управлять безопасностью системы и уровнем доступа отдельных лиц и групп лиц.
- Должно осуществляться управление доступом к ресурсам. Должно быть возможным разрешать или запрещать доступ к указанным ресурсам как отдельным пользователям, так и группам пользователей.
- Пользователи должны регистрировать себя в системе и иметь уникальные идентификаторы. Все действия пользователей, контролируемые системой, должны быть персонифицированы.

Основные компоненты подсистемы защиты



Процесс входа (Winlogon)

- Процесс пользовательского режима (\Windows\System32\Winlogon.exe), отвечающий за поддержку аутентификации и управление сеансами интерактивного входа в систему. Например, при регистрации пользователя Winlogon создает оболочку — пользовательский интерфейс. Стандартная библиотека аутентификации Gina (Graphical Identification and Authentication) реализована в файле Msgina.dll. Доступ к Winlogon осуществляется нажатием комбинации <Ctrl+Alt+Del>.

Подсистема локальной аутентификации

- Процесс пользовательского режима, выполняющий образ \Windows\System32\l_sass.exe, который отвечает за политику безопасности в локальной системе (например, круг пользователей, имеющих право на вход в систему, правила, связанные с паролями, привилегии, выдаваемые пользователям и их группам, параметры аудита безопасности системы), а также за аутентификацию пользователей и передачу сообщений аудита безопасности в журнал событий.

Монитор безопасности

- **Монитор безопасности** – компонент исполнительной системы (\Windows\System32\Ntoskrnl.exe), отвечающий за определение структуры данных маркера доступа для представления контекста защиты, за проверку прав доступа к объектам, манипулирование привилегиями (правами пользователей) и генерацию сообщений аудита безопасности.

База данных политики LSASS

- База данных, содержащая параметры политики безопасности локальной системы. Она хранится в разделе реестра HKLM\SECURITY и включает следующую информацию: каким доменам доверена аутентификация попыток входа в систему, кто имеет права на доступ к системе и каким образом, кому предоставлены те или иные привилегии и какие виды аудита следует выполнять.

Диспетчер учетных записей безопасности

- **Диспетчер учетных записей безопасности** (Security Accounts Manager, SAM) Набор подпрограмм, отвечающих за поддержку базы данных, которая содержит имена пользователей и группы, определенные на локальной машине.

Active Directory

- **Active Directory –** служба каталогов, содержащая базу данных со сведениями об объектах домена, в том числе о пользователях, группах и компьютерах. Сведения о паролях и привилегиях пользователей домена и их групп содержатся в Active Directory.
- Домен – это совокупность компьютеров и сопоставленных с ними групп безопасности, которые управляются как единое целое.

Архитектура Windows

Объекты Windows 2000-2008

Объекты MS Windows

В ОС Windows 2000-2003 объект – это отдельный экземпляр периода выполнения (runtime instance) статически определенного типа объекта.

Тип объектов (object type), иногда называемый *классом объектов* (object class) состоит из общесистемного типа данных, функций, оперирующих экземплярами этого типа данных, и набора атрибутов.

Атрибут объекта *(object attribute)* – это поле данных внутри объекта частично определяющее его состояние.

Методы объекта (средства для манипулирования объектами) обычно считывают атрибуты объекта.

Объекты MS Windows

- Не все структуры данных в Windows 2000-2008 являются объектами. В объекты помещаются лишь те данные, которые нужно разделять, защищать, именовать или сделать доступными программам пользовательского режима (через системные сервисы).
- Структуры, используемые только одним из компонентов операционной системы для поддержки каких-то внутренних функций, к объектам не относятся.

Объекты MS Windows

MS Windows 2000 –
27 объектов

MS Windows XP-2003 –
29 объектов

Назначение объектов

Объекты очень удобны для поддержки четырех важных функций ОС:

- присвоения понятных имен системным ресурсам;
- разделения ресурсов и данных между процессами;
- защиты ресурсов от несанкционированного доступа;
- учета ссылок (благодаря этому система узнает, когда объект больше не используется, и автоматически уничтожает его).

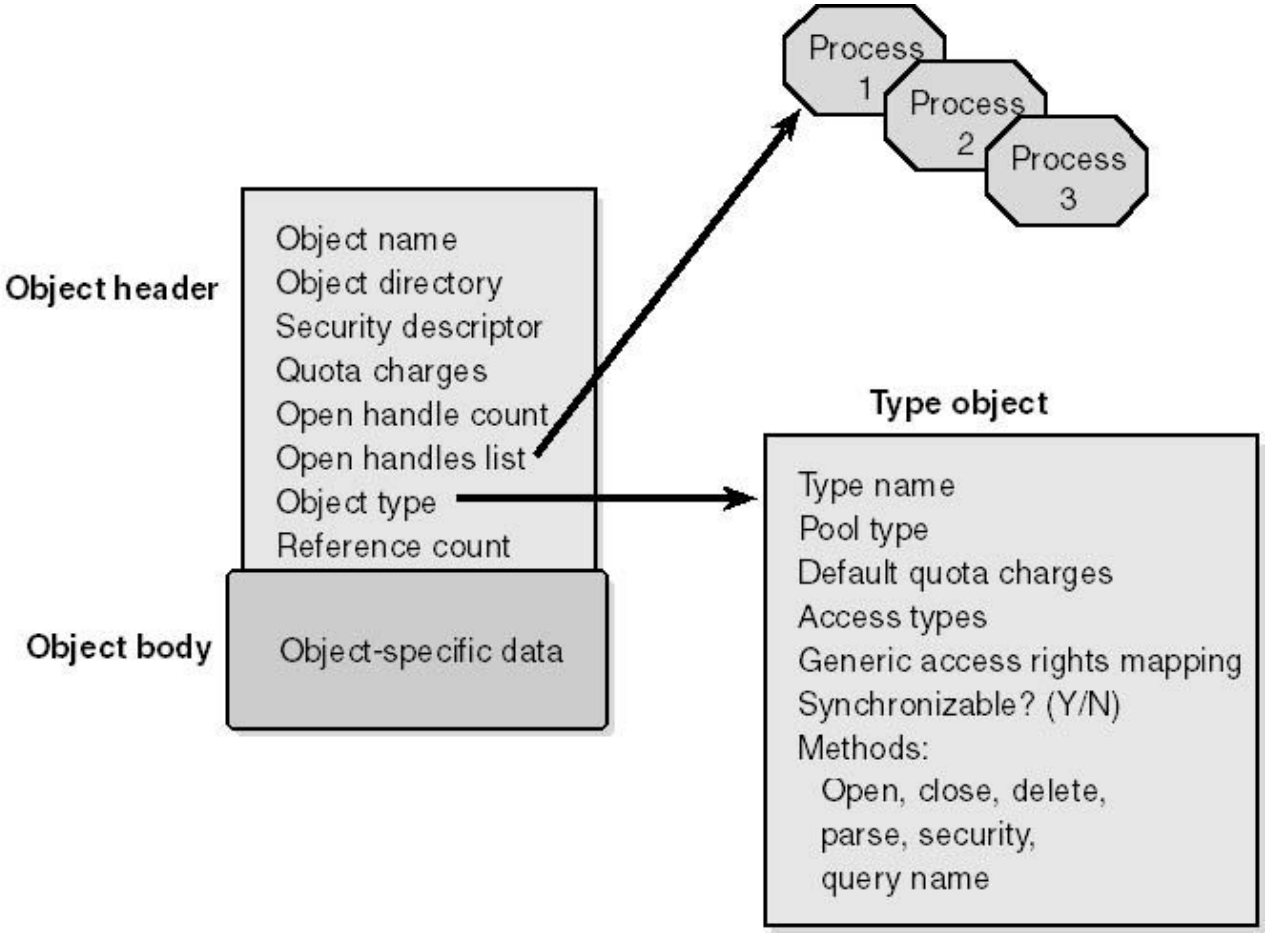
Типы объектов Windows 2000-2008

- **Объекты исполнительной системы** (executive object) представляются различными компонентами исполнительной системы. Они доступны программам пользовательского режима (защищенным подсистемам) посредством базовых сервисов и могут создаваться и использоваться как подсистемами, так и исполнительной системой.
- **Объекты ядра** (kernel object) – это более примитивный набор объектов, реализованный ядром. Большинство этих объектов создаются и используются только внутри исполнительной системы.
  - Управляющие объекты (объекты прерываний, …)
  - Объекты диспетчеризации (семафоры, события, мьютексы, таймеры,…)

Примеры объектов

- Файл
- Регион памяти
- Поток
- Процесс
- Семафор
- Таймер

Структура объектов Windows 2000-2003



Структура объектов Windows 2000-2003

Имя объекта	Делает объект видимым другим процессам для совместного использования
Каталог объектов	Обеспечивает иерархическую структуру, в которой хранятся имена объектов
Дескриптор безопасности	Определяет, кто и каким образом может использовать данный объект
Расход квоты	Задает квоту на использование ресурсов, которая списывается с процесса при открытии описателя данного объекта
Счетчик открытых дескрипторов	Подсчитывает количество открытых дескрипторов данного объекта
Список открытых дескрипторов	Содержит список процессов, открывших дескрипторы данного объекта
Временный/ постоянный статус	Указывает, можно ли уничтожить имя и освободить память объекта, если он более не используется
Режим: пользовательский/ ядра	Определяет доступность объекта в пользовательском режиме
Указатель на типовой объект	Ссылается на типовой объект, который содержит атрибуты, общие для набора однотипных объектов

Удержание объектов

- Удержание объектов включает две фазы. Первая фаза называется **удержанием имени** (name retention) и управляется количеством открытых дескрипторов данного объекта. Всякий раз, когда процесс открывает описатель объекта, диспетчер объектов увеличивает счетчик открытых дескрипторов в заголовке объекта.
- После того, как процесс закончил работу с объектом и закрыл имеющиеся у него дескрипторы данного объекта, диспетчер объектов уменьшает счетчик.
- Вторая фаза удержания объектов – это **прекращение удержания** (т.е. удаление объектов), когда они более не используются.

Учет использования ресурсов

- Каждому пользователю назначаются **предельные размеры квот**, ограничивающие суммарный объем системной памяти, который может быть использован его процессами. Соответственно, заголовок каждого объекта содержит атрибут, называемый "расход квоты" и содержащий значение, которое диспетчер объектов вычитает из выделенной процессу квоты, когда поток этого процесса открывает дескриптор данного объекта.

Защита объектов

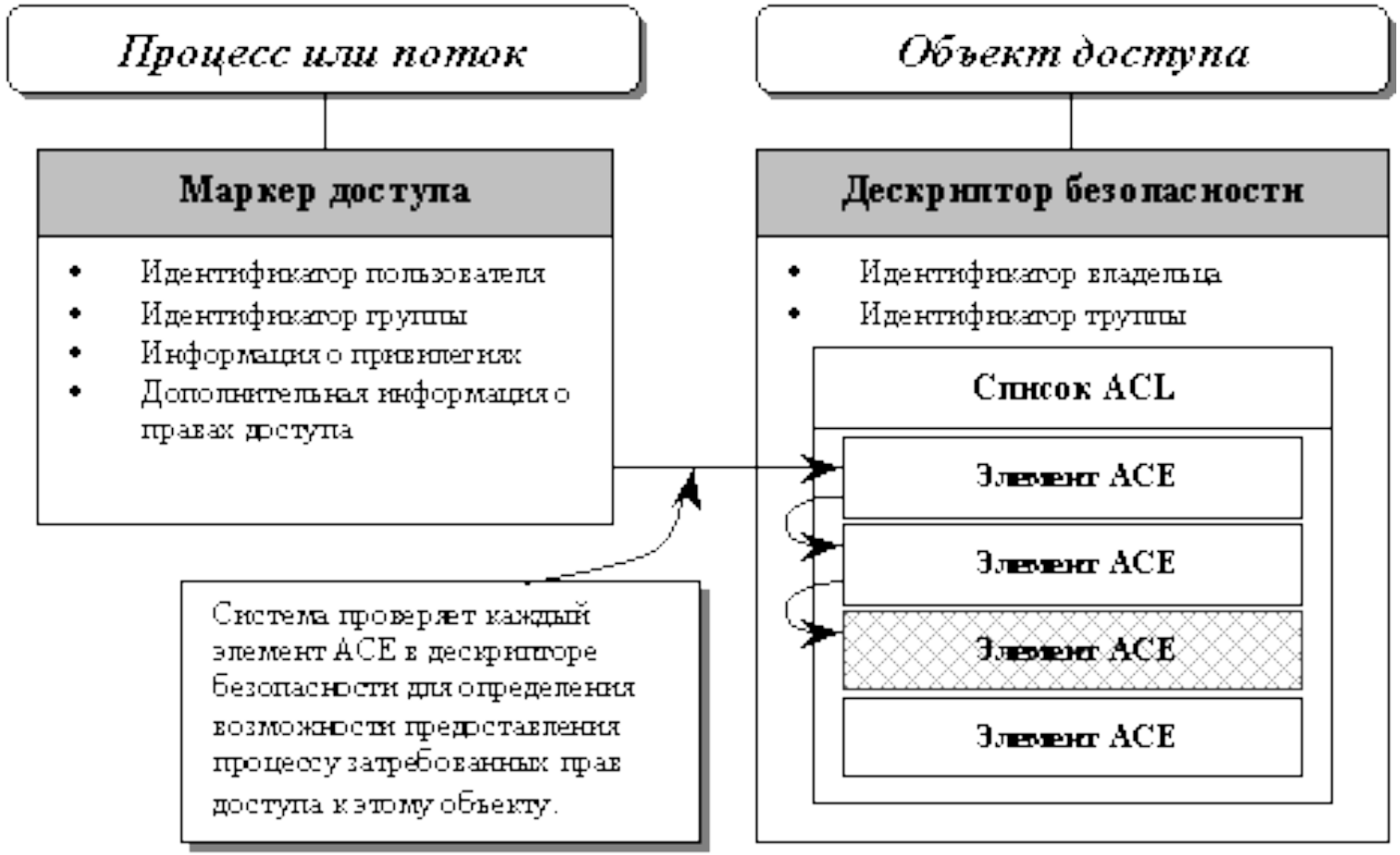
ОС Windows 2000 поддерживает два вида контроля доступа к объектам:

- **управление избирательным доступом** (discretionary access control) – основной механизм контроля доступа, при котором владельцы объектов разрешают или запрещают доступ к ним для других пользователей (процессов). При первой попытке доступа процесса (приложения) к общему (разделяемому) объекту подсистема Windows проверяет, имеет ли это приложение соответствующие права. Если проверка завершается успешно, подсистема Windows разрешает приложению доступ.
- **управление привилегированным доступом** (privileged access control) – необходим в тех случаях, когда управления избирательным доступом недостаточно. Данный метод гарантирует, что пользователь сможет обратиться к защищенным объектам, даже если их владелец недоступен.

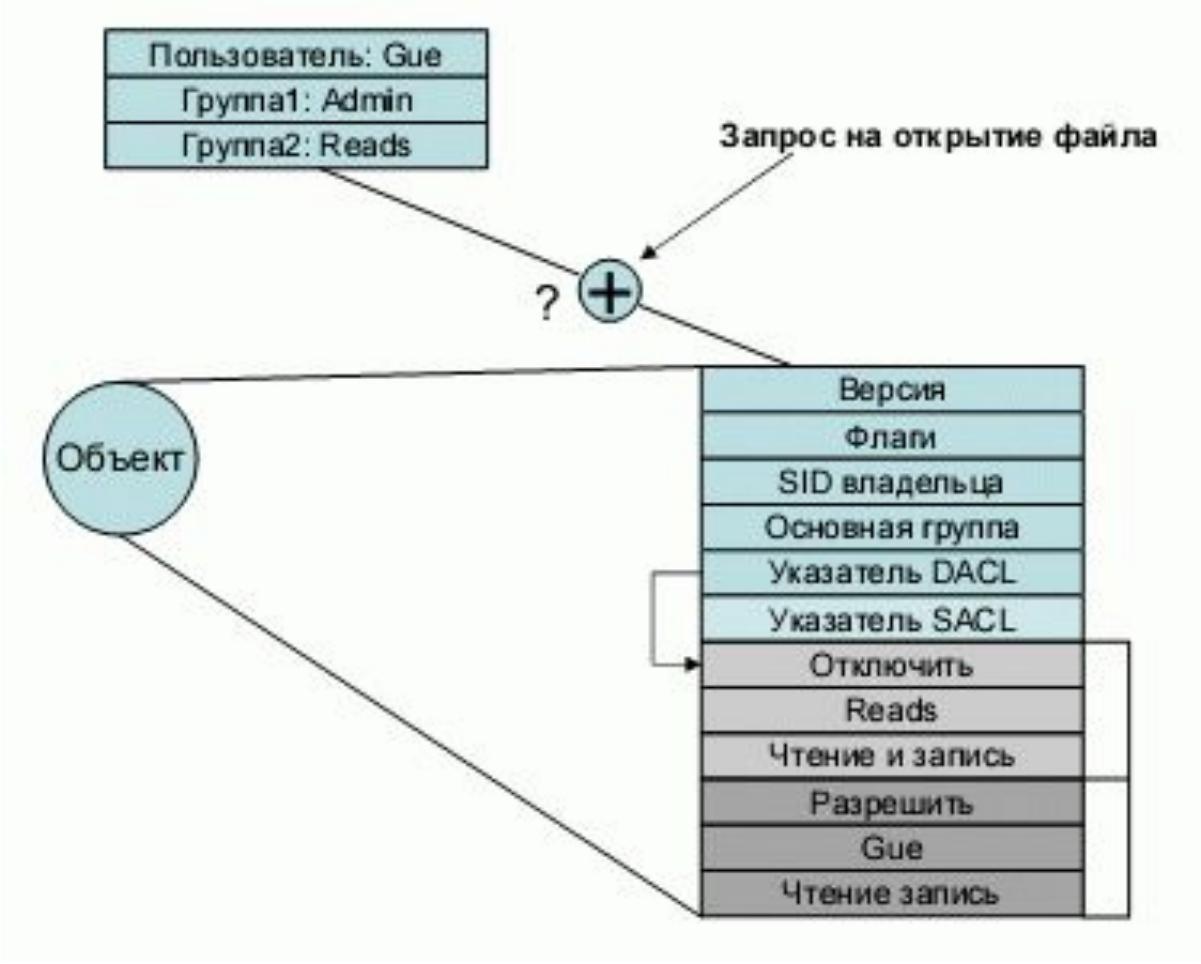
Избирательный доступ

- Основан на списках контроля доступа (access control list, ACL), которые описывают каким пользователям можно выполнять какие операции.
- При отсутствии ACL объект является незащищенным, и система защиты предоставляет к нему запрошенный тип доступа.
- ACL представляет собой список элементов контроля доступа (access control element, ACE) . Когда процесс пытается использовать какой-либо объект, система проводит просмотр всех ACE в ACL — от первого до последнего.
- В списке ACL есть записи ACE двух типов - разрешающие и запрещающие доступ. В ходе просмотра выполняется сравнение маски доступа с проверяемыми правами. Для запрещающих ACE даже при частичном совпадении прав доступ немедленно отклоняется. Для успешной проверки разрешающих элементов необходимо совпадение всех прав. Для ускорения рекомендуется размещать запрещающие элементы перед разрешающими.

Отношения между маркером доступа и атрибутами безопасности объекта



Пример проверки ACE



Архитектура Windows

Реестр

Реестр

- Операционная система управляет большим объемом информации, необходимой для ее загрузки и конфигурирования. В ранних версиях Windows эта информация содержалась в различных текстовых файлах с расширением .ini (Win.ini, System.ini и т.д.).
- Начиная с Windows 95, эта информация хранится в централизованной общесистемной базе данных, называемой реестром (registry). Для просмотра и модификации данных реестра имеется штатный утилиты редактор реестра regedit.

Структура реестра

- Данные реестра хранятся в виде иерархической древовидной структуры. Каждый узел или каталог называется разделом или ключом (keys), а названия каталогов верхнего уровня начинаются со строки HKEY. Каждый раздел может содержать подраздел (subkey).
- Реестр содержит шесть корневых разделов: HKEY_CURRENT_USER, HKEY_USERS, HKEY_CLASSES_ROOT, HKEY_LOCAL_MACHINE, HKEY_PERFORMANCE_DATA (виртуальный) и HKEY_CURRENT_CONFIG.
- Наиболее важным, вероятно, является раздел HKEY_LOCAL_MACHINE. В нем содержится вся информация о локальной системе.

Хранение реестра

- Реестр хранится на диске в виде набора файлов, называемых "кустами" или "ульями" (hives). Большинство из них находится в каталоге \Systemroot\System32\Config. Большое значение уделяется повышению надежности хранения.
- В частности, система ведет протоколы модификации кустов (при помощи так называемых регистрационных кустов, log hives), которые обеспечивают гарантированную возможность восстановления постоянных кустов реестра. Для еще большей защиты целостности на диске поддерживаются зеркальные копии критически важных кустов.

Подробнее

- Структура кустов подробно описана в (Руссинович М., Соломон Д. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000).