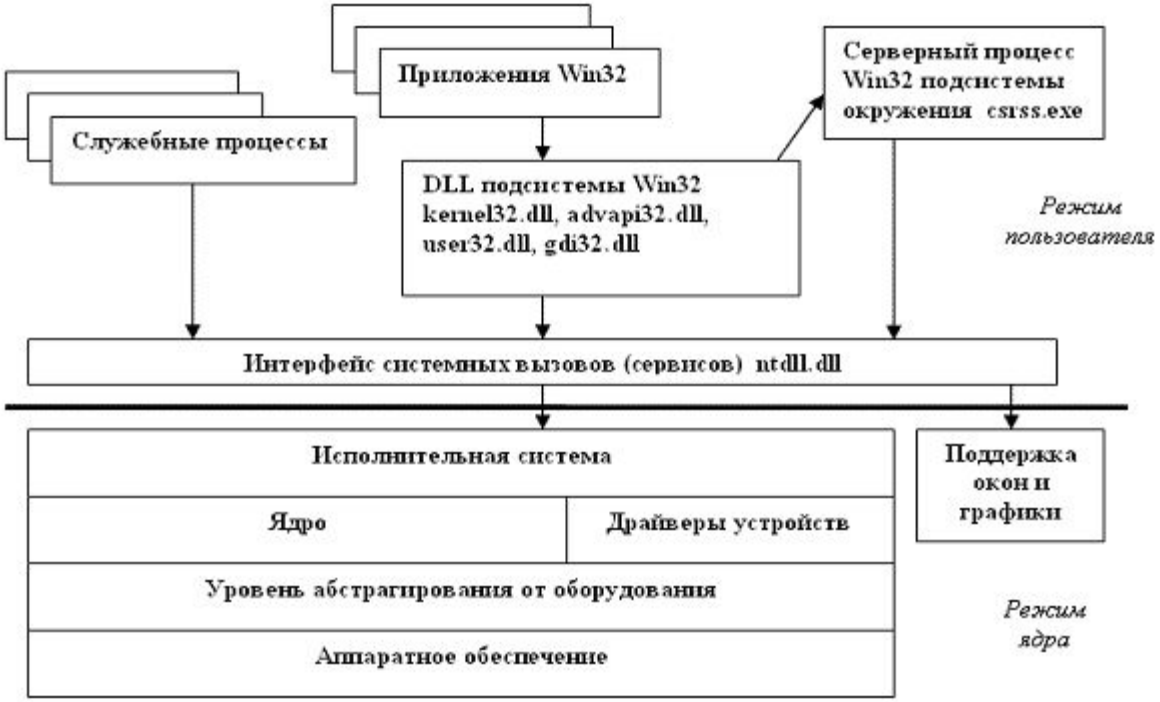
Архитектура ОС Windows

1. Принципы работы ОС:
   - режим ядра
   - режим пользователя
2. DLL
3. Реестр Windows

Упрощенная архитектурная схема ОС Windows NT (New Technology)



HAL(hardware abstraction layer)

Основные системные процессы:
- Winlogon.exe
- Smss.exe(Session Manager)
- Lsass.exe (Local Security Authentication Subsystem Server)
- Wininit.exe
- Userinit.exe
- Services.exe (SCM, Service Control Manager)

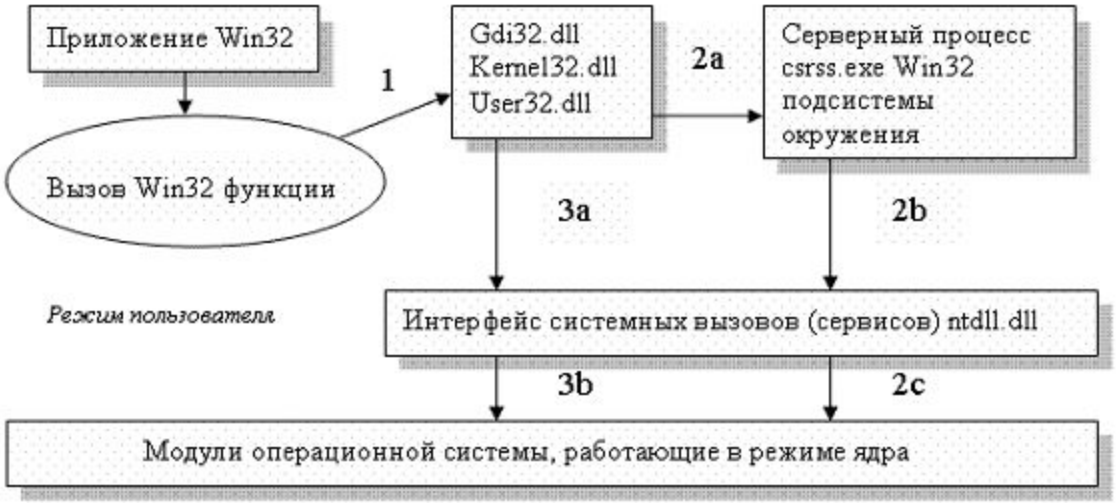
Службы (сервисы, services):например, Windows Audio, Print Spooler.
Пользовательские приложения (user applications)
Подсистемы окружения (environment subsystems)

Основные системные файлы(System32, SysWOW64):
- ntoskrnl.exe
- ntdll.dll
- hal.dll
- win32k.sys
- kernel32.dll, advapi32.dll, user32.dll, gdi32.dll

Win32 API (Application Programming Interface)

Win32 подсистема:
- csrss.exe
- Win32k.sys
- kernel32.dll, advapi32.dll, user32.dll, gdi32.dll

Различные маршруты выполнения вызовов Win32 API



DLL (динамически подключаемая библиотека)

Утилита depends, входящей в пакет Platform SDK

DLL- набор вызываемых подпрограмм, включенных в один двоичный файл, который приложения, использующие эти подпрограммы, могут динамически загружать в процессе своего выполнения.

Преимущество DLL перед статическими библиотеками состоит в том, что приложения могут разделять DLL-модули, при этом ОС Windows гарантирует, что в памяти будет находиться лишь по одному экземпляру используемых DLL

Реестр Windows

Операционная система управляет большим объемом информации, необходимой для ее загрузки и конфигурирования. Эта информация хранится в централизованной общесистемной базе данных, называемой *реестром (registry)*. Ранее в файлах с расширением ini.
Regedit – редактор реестра
Данные реестра хранятся в виде иерархической древовидной структуры. Каждый узел или каталог называется разделом или ключом. Каждый раздел может содержать подразделы (subkey). Записи нижней части структуры называются параметрами (values), данные которых строго типизированы.

Реестр содержит пять корневых разделов:

1. HKEY_CLASSES_ROOT
2. HKEY_USERS
3. HKEY_CURRENT_USER
4. HKEY_LOCAL_MACHINE
5. HKEY_CURRENT_CONFIG

API функции

- RegOpenKeyEx
- RegCreateKeyEx
- RegSetValue
- RegDeleteValue
- RegCloseKey
- RegQueryValueEx