Лекция 1. Введение

Архитектура ОС Windows

2 октября 2014 г.

Список литературы

Внутреннее устройство


Руссинович М., Соломон Д.
Внутреннее устройство Microsoft Windows: Пер. с англ., 6-е изд.
Питер, СПб., 2013.


Руссинович М., Соломон Д., Ионеску А.
Внутреннее устройство Microsoft Windows. Основные подсистемы ОС (Часть 2): Пер. с англ., 6-е изд.
Питер, СПб., 2014.

Список литературы

Программирование


Рихтер Дж.
Windows для профессионалов: создание эффективных Win32 приложений с учётом специфики 64-разрядной версии Windows: Пер. с англ., 4-е изд.
Питер, СПб., 2001.


Рихтер Дж., Назар К.
Windows via C/C++ Программирование на языке Visual C++. Мастер класс: Пер. с англ.
Русская редакция, Питер, М., СПб., 2009.

Применение знаний

Задачи, требующие знания устройство операционной системы

- Разработка приложений.
- Системное администрирование.

Разработка MS-DOS

Разработка

- Время: 1981–2000;
- Разработчик: Microsoft;
- Платформа: Intel 8086.

Основные особенности

- Однозадачная, однопользовательская система;
- Система команд терминала;
- Дисковая файловая система (FAT);
- Устанавливаемые драйверы устройств.

Разработка Windows

Разработка

- Время: 1985–настоящее время;
- Разработчик: Microsoft;
- Платформы: IA-32, MIPS, Alpha AXP, Motorola PowerPC, Itanium, x86-64, ARM, ...

Основные особенности

- Семейства: Windows 3.x, Windows 9x, Windows NT, Windows CE, Windows Phone.

Архитектуры Windows

Линейка	Настольные	Серверы	Устройства
3.x	Windows 1.0–3.1 Windows for Workgroups 3.11		
9x	Windows 95, 98, ME		
NT	Windows NT 3.1–4.0 Windows 2000, XP, Vista, 7, 8, 8.1	Windows NT 3.1–4.0 Windows 2000 Windows Server 2003, 2008, 2012	Windows NT 4.0 Embedded Windows XP Embedded Windows Vista for embedded systems Windows RT Windows Embedded 8

Таблица 1: архитектуры Windows

Архитектуры Windows (окончание)

Линейка	Настольные	Серверы	Устройства
CE			Windows CE 1.0–6.0 Pocket PC 2000, 2002 Windows Mobile 2003, 2003 CE, 5–6.5 Windows Embedded Automotive Windows Embedded Compact 7
Phone			Windows Phone 7–8

Таблица 2: архитектуры Windows (окончание)

Цели разработки Windows NT

Цели (1989 г.)

- Поддержка 32-разрядности, вытеснения, реентрабельности, виртуальной памяти.
- Работа на множестве аппаратных платформ.
- Масштабируемость на системах SMP.
- Работа в качестве клиента и сервера.
- Поддержка большинства существовавших 16-разрядных программ для MS-DOS и Windows 3.1.
- Поддержка правительственного стандарта POSIX 1003.1.
- Поддержка правительственных и индустриальных стандартов безопасности.
- Адаптируемость для мирового рынка при помощи поддержки Unicode.

Развитие линейки Windows NT

Продукт	№ версии	Дата выхода
Windows NT 3.1	3.1	Июль 1993
Windows NT 3.5	3.5	Сентябрь 1994
Windows NT 3.51	3.51	Май 1995
Windows NT 4.0	4.0	Июль 1996
Windows 2000	5.0 (Build 2195)	Декабрь 1999
Windows XP	5.1 (Build 2600)	Август 2001
Windows Server 2003	5.2 (Build 3790)	Март 2003
Windows Vista	6.0 (Build 6000)	Январь 2007
Windows Server 2008	6.0 (Build 6001)	Март 2008

Таблица 3: выпуски Windows линейки NT

Развитие линейки Windows NT (окончание)

Продукт	№ версии	Дата выхода
Windows 7	6.1 (Build 7600)	Октябрь 2009
Windows Server 2008 R2	6.1 (Build 7600)	Октябрь 2009
Windows 8	6.2 (Build 9200)	Август 2012
Windows Server 2012	6.2 (Build 9200)	Август 2012
Windows 8.1	6.3 (Build 9600)	Октябрь 2013
Windows Server 2012 R2	6.3 (Build 9600)	Октябрь 2013

Таблица 4: выпуски Windows линейки NT (окончание)

Концепция ядра

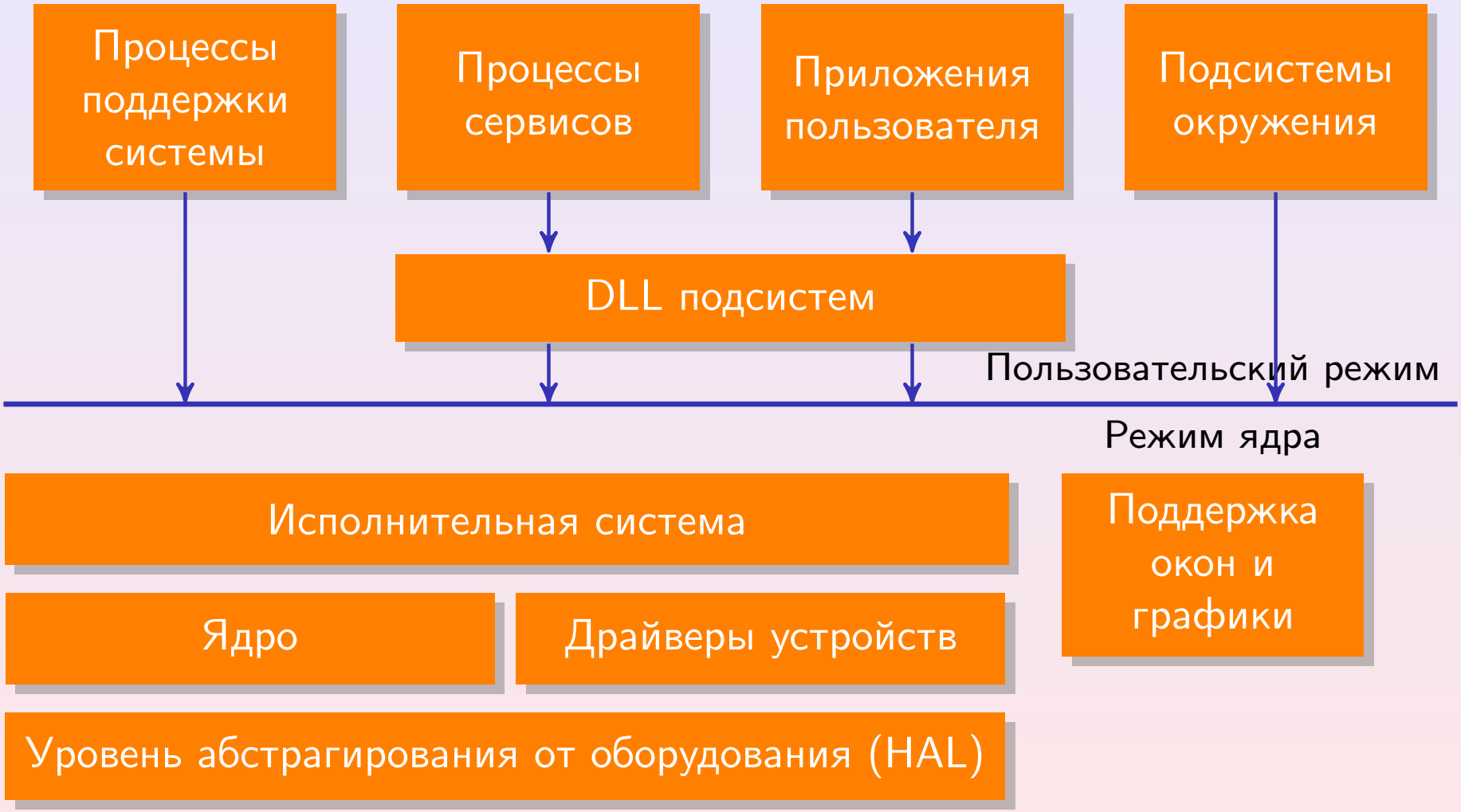

Рис. 1: архитектура Windows NT

Основные исполняемые файлы

Имя файла	Назначение
`Ntoskrnl.exe`	Ядро и исполнительная система.
`Ntkrnlpa.exe`	Ядро и исполнительная система с поддержкой PAE (Windows 32), NoExecute.
`Hal.dll`	HAL
`Win32k.sys`	часть подсистемы Windows, работающая в режиме ядра.

`Kernel32.dll`
`User32.dll`
`Gdi32.dll`
`Advapi32.dll`
	Основные библиотеки подсистемы Windows.

`Ntdll.dll`	Native API — недокументированные функции пользовательского уровня, вызываемые `Kernel32.dll`, . . . , а также при загрузке.

Таблица 5: основные исполняемые файлы Windows NT

Процессы поддержки системы

Системные процессы Windows NT

Процесс обработки входа в систему: (`WinLogon.exe`) — обработка SAS, загрузка профиля, блокировки на хранителе экрана.

Диспетчер сеансов: (`smss.exe`) — создаёт переменные окружения, подсистему Windows, устройства ДОС, файл подкачки, запускает WinLogon, ждёт, когда он или подсистема Windows завершится.

Диспетчер управления службами: (Service control manager, `services.exe`) — запускает службы.

Процессы поддержки системы (окончание)

Системные процессы Windows NT (окончание)

Сервер проверки подлинности локальной системы безопасности: (Local Security Authority Subsystem Service, `lsass.exe`) —

- отвечает за политику безопасности системы,
- проверяет заходящих пользователей,
- обрабатывает изменения паролей,
- создаёт маркеры доступа,
- ведёт журнал безопасности.

Процесс инициализации: (`WinInit.exe`) — инициализирует сеанс.

Реестр

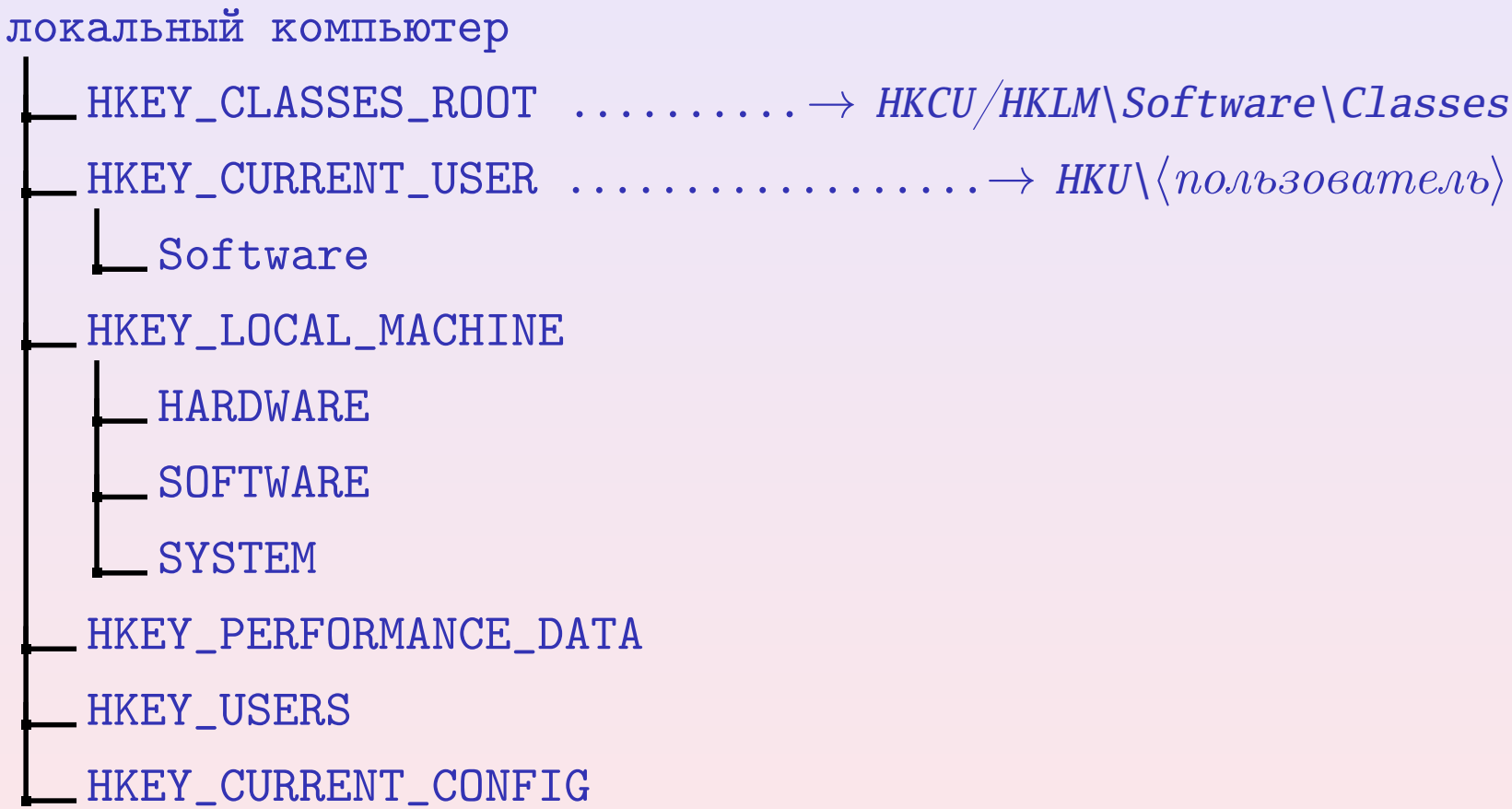

Рис. 2: структура реестра в Windows NT

Уровни безопасности

Классификация систем безопасности

- D (Minimal Protection, минимальная защита)
- C
  - C1 (Discretionary Access Protection, защита с разграниченным доступом)
  - C2 (Controlled Access Protection — защита с управляемым доступом)
- B
  - B1
  - B2
  - B3
- A
  - A1
  - Выше A1

Стандарт безопасности

Требования класса C1 (избирательная защита безопасности)

- Механизм безопасной регистрации;
- Разделение пользователей и данных;
- Управление избирательным доступом;
- Обязательная системная документация и руководства пользователя.

Дополнительные требования класса C2

- Аудит безопасности;
- Защита при повторном использовании объектов;
- Функциональность пути доверительных отношений;
- Управление доверительными отношениями.

Стандарт безопасности

Требования класса C1 (избирательная защита безопасности)

- Механизм безопасной регистрации;
- Разделение пользователей и данных;
- Управление избирательным доступом;
- Обязательная системная документация и руководства пользователя.

Дополнительные требования класса C2

- Аудит безопасности;
- Защита при повторном использовании объектов;
- Функциональность пути доверительных отношений;
- Управление доверительными отношениями.