

Лекция №4

Реестр

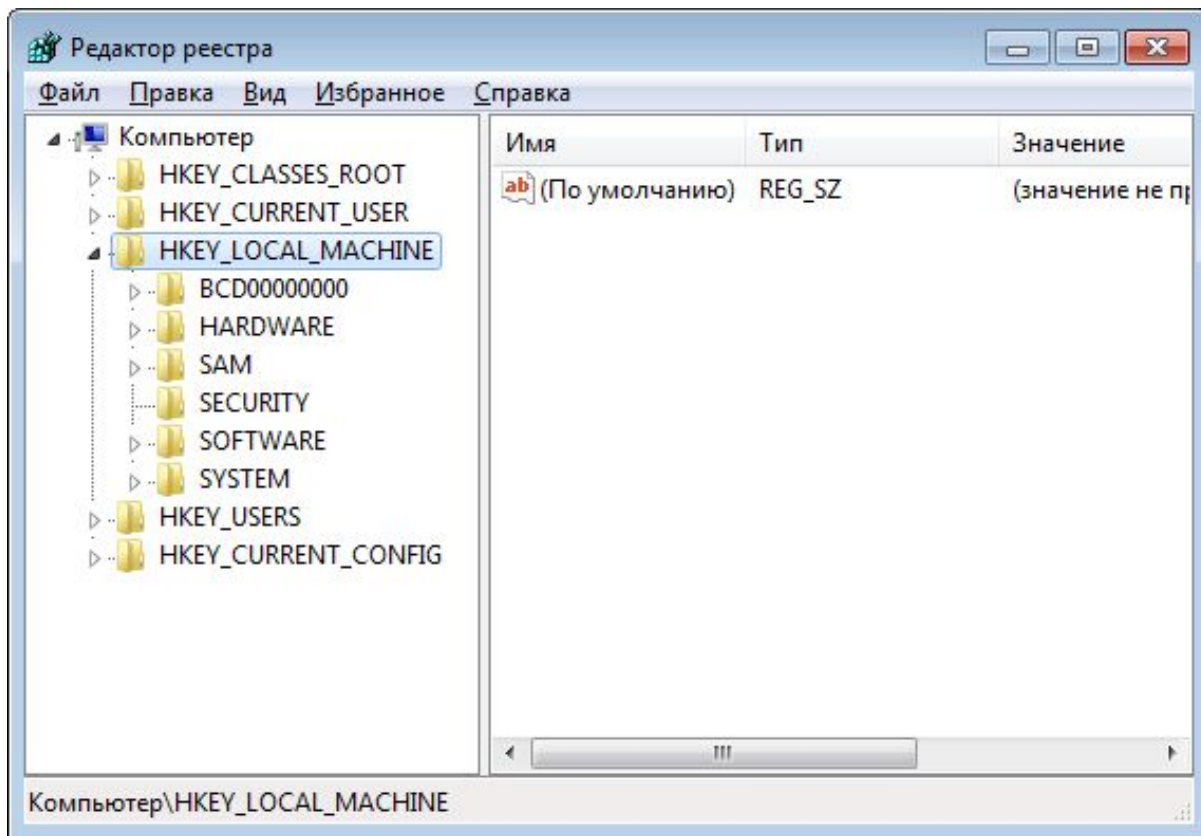
Реестр

- *Реестр* - это унифицированная база данных, в которой Windows NT хранит всю информацию о конфигурации оборудования и программного обеспечения локального компьютера. Реестр управляет ОС Windows NT, предоставляя информацию, используемую при запуске приложений и загрузке компонентов, например драйверов устройств и сетевых протоколов
- Альтернативой реестру являются конфигурационные файлы (изначально *win.ini*, *system.ini*)

Реестр содержит информацию о следующих элементах ОС:

- оборудовании, установленном на компьютере, включая центральный процессор, тип шины, указательное устройство или мышь и клавиатуру;
- установленных драйверах устройств; установленных приложениях;
- установленных сетевых протоколах;
- настройках платы сетевого адаптера (номер прерывания, базовый адрес памяти, базовый адрес портов ввода\вывода, тип трансивера);
- учетных записей пользователей (например, о принадлежности пользователей группам, их правах доступа и привилегиях).

Логическая структура реестра



- **Ветвь:**

- HKCR
- HKCU
- HKLM
- HKU
- HKCC

- **Раздел и подраздел:**

- HKLM\Software=HKCC

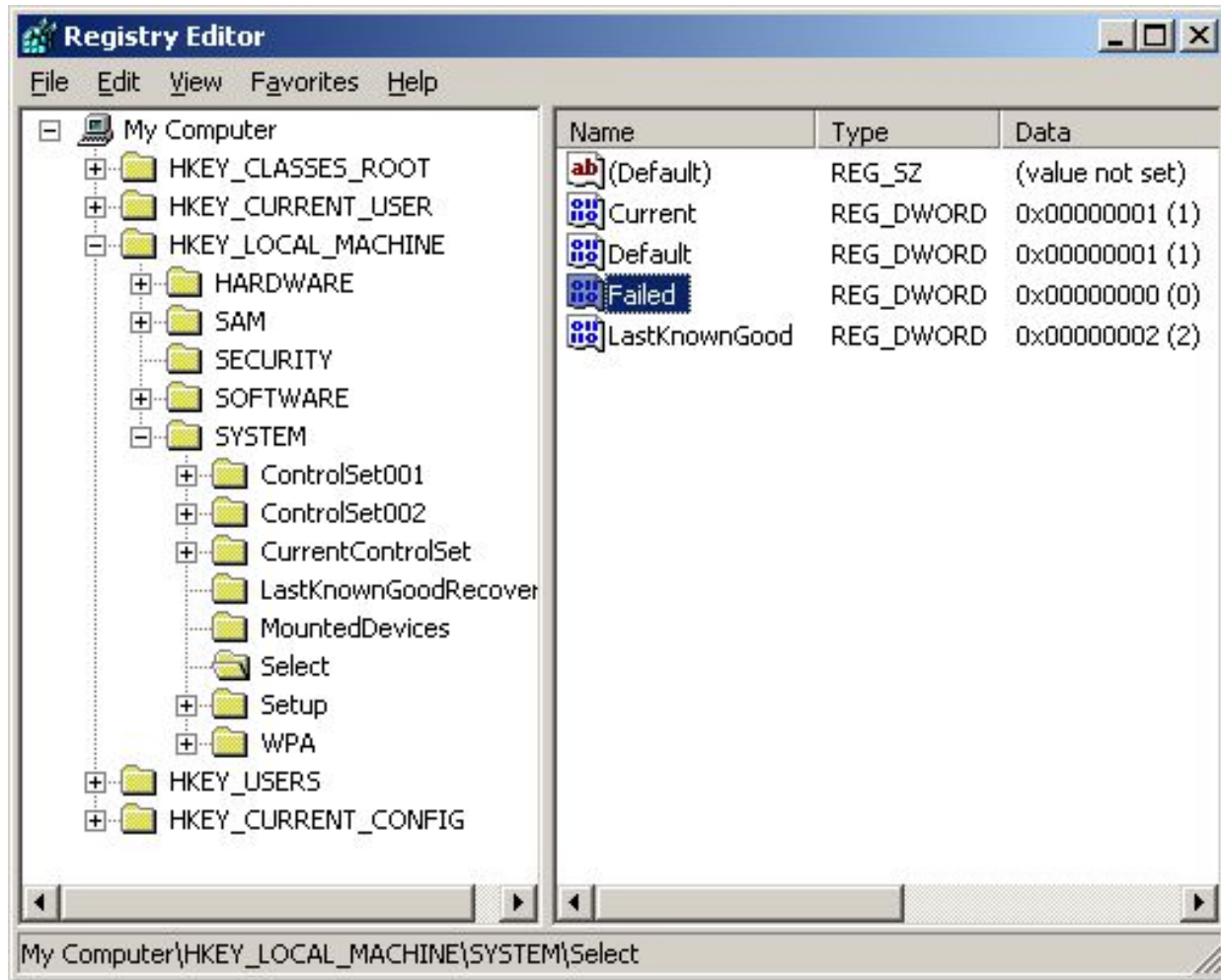
- **Параметр:**

- Имя
- Тип данных
- значение

Ветви реестра

Папка/стандартный раздел	Описание
HKEY_CURRENT_USER	Данный раздел является корневым для данных настройки пользователя, вошедшего в систему в настоящий момент. Здесь хранятся папки пользователя, цвета экрана и настройки панели управления. Эти данные называются профилем пользователя.
HKEY_USERS	Данный раздел содержит все профили пользователей компьютера. HKEY_CURRENT_USER является подразделом HKEY_USERS.
HKEY_LOCAL_MACHINE	Раздел содержит данные настройки, относящиеся к данному компьютеру (для всех пользователей).
HKEY_CLASSES_ROOT	Данный раздел является подразделом HKEY_LOCAL_MACHINE\Software. Хранящиеся здесь сведения обеспечивают открытие необходимой программы при открытии файла с помощью проводника.
HKEY_CURRENT_CONFIG	Данный раздел содержит сведения о профиле оборудования, используемом локальным компьютером при запуске системы.

Параметры

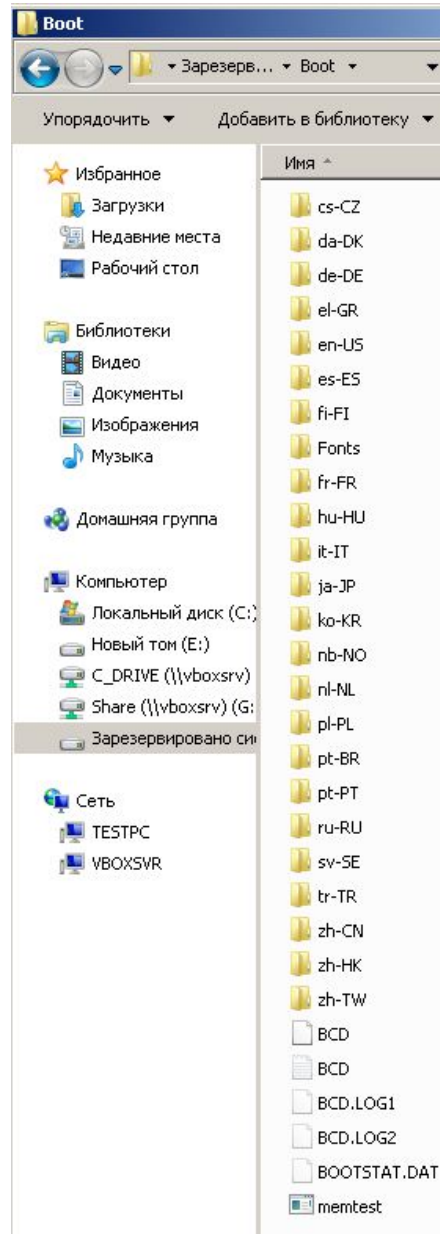
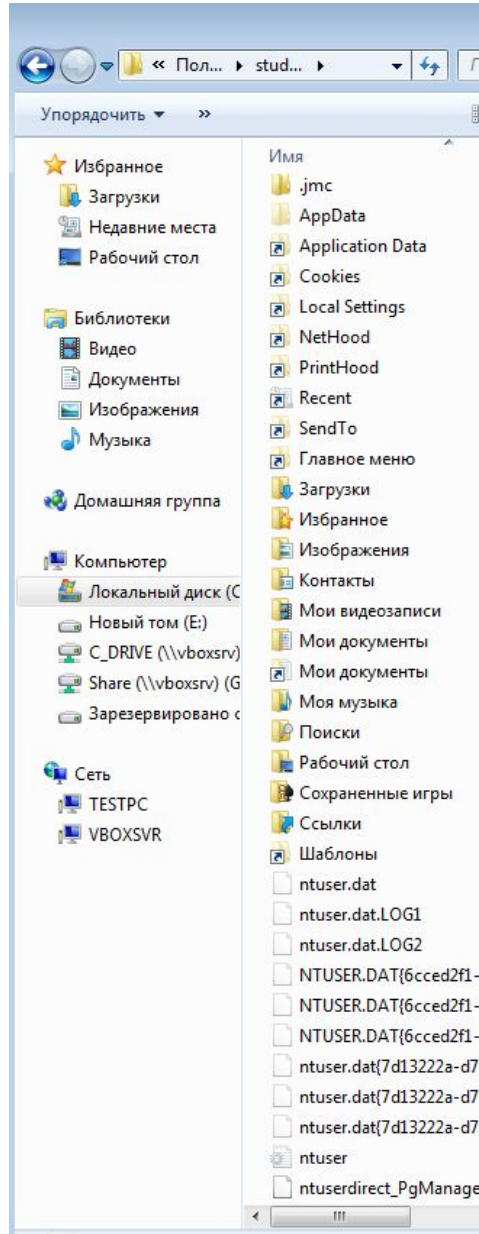
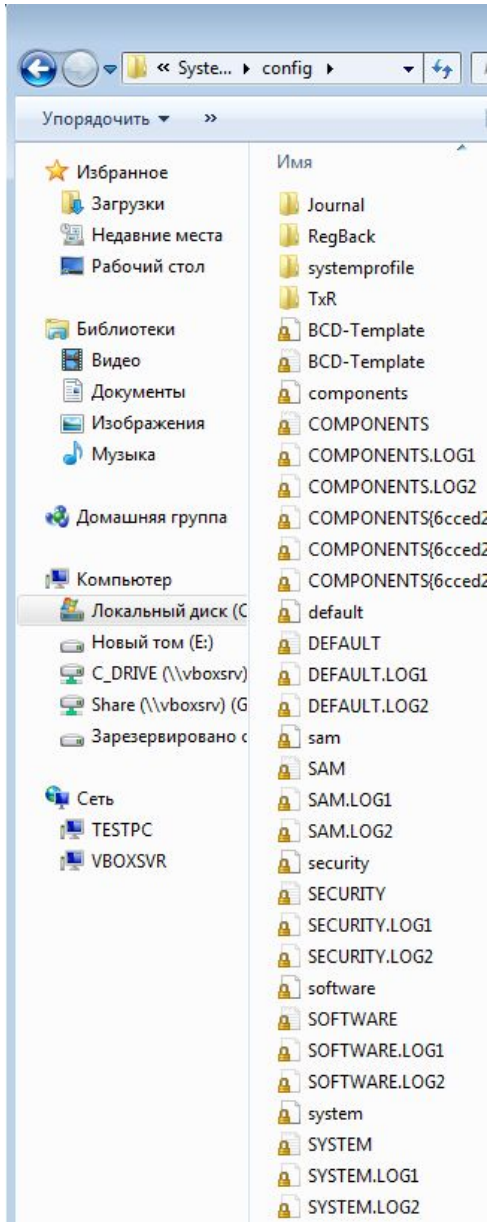


- Имя:
HKLM\SYSTEM\Select
- Тип данных:
REG_DWORD
- Значение:0

Типы данных параметров

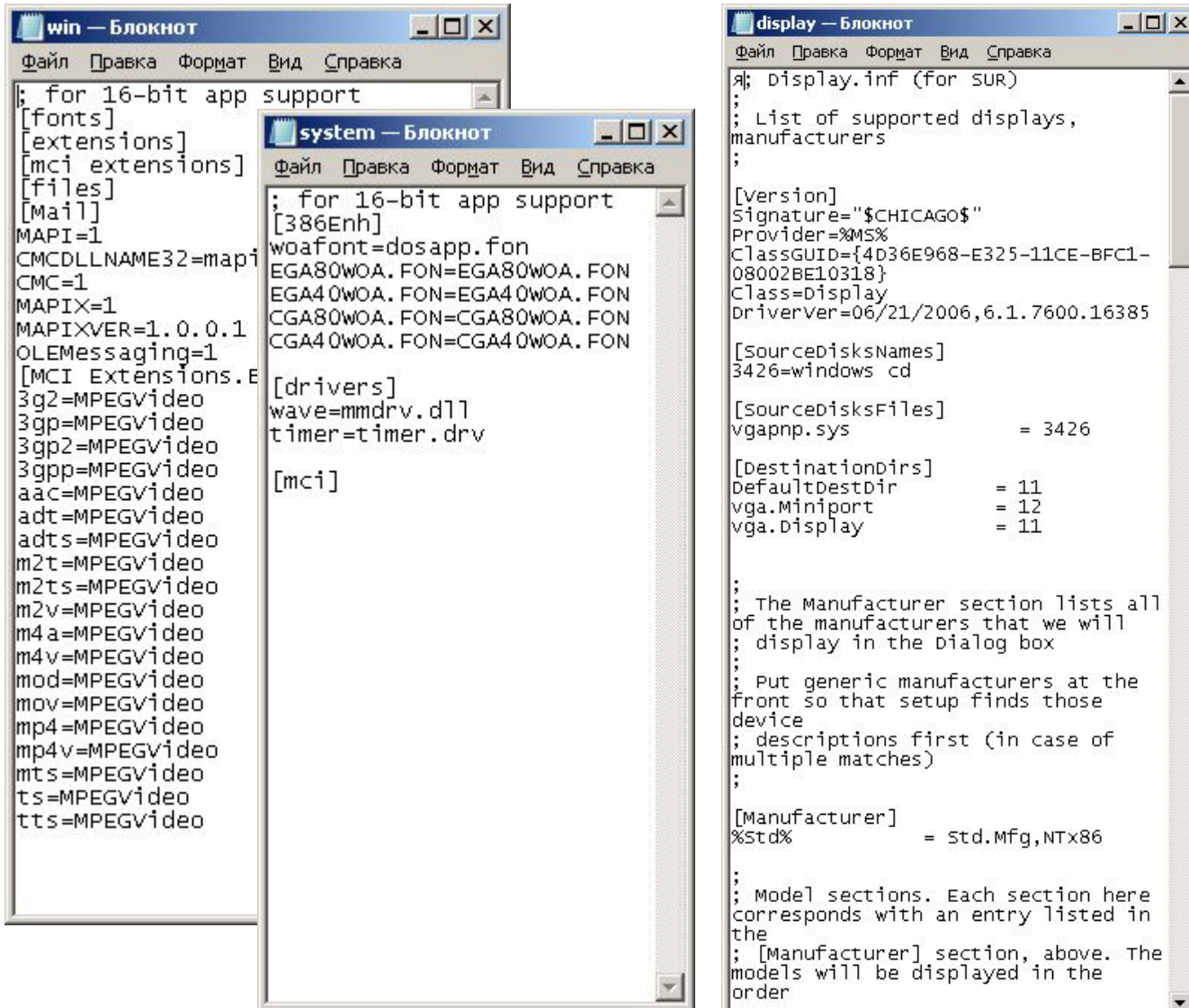
Тип данных	Описание
REG_BINARY	Необработанные двоичные данные. Большинство сведений об аппаратных компонентах хранится в виде двоичных данных и выводится в редакторе реестра в шестнадцатеричном формате.
REG_DWORD	Данные, представленные целым числом (4 байта). Многие параметры служб и драйверов устройств имеют этот тип и отображаются в двоичном, шестнадцатеричном или десятичном форматах.
REG_EXPAND_SZ	Строка данных переменной длины Этот тип данных включает переменные, обрабатываемые при использовании данных программой или службой.
REG_MULTI_SZ	Многострочный текст. Этот тип, как правило, имеют списки и другие записи в формате, удобном для чтения. Записи разделяются пробелами, запятыми или другими символами.
REG_SZ	Текстовая строка фиксированной длины.
REG_FULL_RESOURCE_DESCRIPTOR	Последовательность вложенных массивов, разработанная для хранения списка ресурсов аппаратного компонента или драйвера.

Физическая структура реестра



- **Куст (hive)** – это отдельный набор разделов, подразделов и параметров
- Каждый куст имеет соответствующий файл реестра, а также файл с расширением *.log*. По умолчанию большинство кустов (Default, SAM, Security, System) и соответствующие файлы кустов расположены в папке *системный_каталог\system32\config*
- Файлы с расширением *.log* используются для внесения изменений в реестр и для сохранения целостности реестра

Конфигурационные файлы Windows



The image shows three Notepad windows. The first window, titled 'win', contains a list of file extensions for 16-bit applications, including [files], [mail], [MCI Extensions], and various video file types like 3g2, 3gp, 3gp2, 3gpp, aac, adt, adts, m2t, m2ts, m2v, m4a, m4v, mod, mov, mp4, mp4v, mts, and tts. The second window, titled 'system', shows font configuration for 16-bit applications, listing fonts like woafont, EGA80WOA, EGA40WOA, CGA80WOA, and CGA40WOA, along with drivers like wave and timer. The third window, titled 'display', shows the structure of a display configuration file (display.inf), including sections for [Version], [SourceDisksNames], [SourceDisksFiles], [DestinationDirs], [Manufacturer], and [Model].

```
win — Блокнот
; for 16-bit app support
[files]
[mail]
MAPI=1
CMCDLLNAME32=mapi
CMC=1
MAPIX=1
MAPIXVER=1.0.0.1
OLEMessaging=1
[MCI Extensions.E
3g2=MPEGvideo
3gp=MPEGvideo
3gp2=MPEGvideo
3gpp=MPEGvideo
aac=MPEGvideo
adt=MPEGvideo
adts=MPEGvideo
m2t=MPEGvideo
m2ts=MPEGvideo
m2v=MPEGvideo
m4a=MPEGvideo
m4v=MPEGvideo
mod=MPEGvideo
mov=MPEGvideo
mp4=MPEGvideo
mp4v=MPEGvideo
mts=MPEGvideo
tts=MPEGvideo

system — Блокнот
; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON

[drivers]
wave=mmdrv.dll
timer=timer.driv

[mci]

display — Блокнот
; Display.inf (for SUR)
; List of supported displays,
; manufacturers
;
[Version]
Signature="$CHICAGO$"
Provider=%MS%
ClassGUID={4D36E968-E325-11CE-BFC1-
08002BE10318}
Class=Display
DriverVer=06/21/2006,6.1.7600.16385

[SourceDisksNames]
3426=windows cd

[SourceDisksFiles]
vgapnp.sys = 3426

[DestinationDirs]
DefaultDestDir = 11
vga.Miniport = 12
vga.Display = 11

; The Manufacturer section lists all
; of the manufacturers that we will
; display in the Dialog box
;
; Put generic manufacturers at the
; front so that setup finds those
; device
; descriptions first (in case of
; multiple matches)
;
[Manufacturer]
%Std% = std.Mfg,NTx86

;
; Model sections. Each section here
; corresponds with an entry listed in
; the
; [Manufacturer] section, above. The
; models will be displayed in the
; order
```

- Конфигурационные файлы Windows имеют структуру: название раздела в квадратных скобках, затем параметры, используются для устаревших 16-разрядных приложений
- Файл с расширением inf входит в состав драйвера и содержит параметры конфигурации устройства

Конфигурационные файлы Linux

```
system.conf [Только для чтения] (/etc/systemd)
Файл  Правка  Вид  Поиск  Сервис  Документы  Справка
[Иконки: вырезать, копировать, вставить, отменить, повторить, поиск, лупа]
# This file is part of systemd.
#
# systemd is free software; you can redistribute it and/or modify it
# under the terms of the GNU Lesser General Public License as published by
# the Free Software Foundation; either version 2.1 of the License, or
# (at your option) any later version.
#
# Entries in this file show the compile time defaults.
# You can change settings by editing this file.
# Defaults can be restored by simply deleting this file.
#
# See systemd-system.conf(5) for details.

[Manager]
#LogLevel=info
#LogTarget=journal-or-kmsg
#LogColor=yes
#LogLocation=no
#DumpCore=yes
#ShowStatus=yes
#CrashChangeVT=no
#CrashShell=no
#CrashReboot=no
#CtrlAltDelBurstAction=reboot-force
#CPUAffinity=1 2
#JoinControllers=cpu,cpuacct net_cls,net_prio
#RuntimeWatchdogSec=0
#ShutdownWatchdogSec=10min
#CapabilityBoundingSet=
#SystemCallArchitectures=
#TimerSlackNSec=
#DefaultTimerAccuracySec=1min

[Иконки: панель задач, панель быстрого запуска, панель уведомлений]
Текст ▾  Ширина табуля
```

//boot/System.map - путь до ядра linux

(перенаправляет адреса ядра в имена функций и переменных);

/boot/vmlinuz - !!!ядро linux.

/etc/fstab - информация о доступных для монтирования файловых системах и где каждая файловая система будет монтирована.

/etc/group - информация о группах.

/etc/init.d - директория со скриптами, которые запускают сервера

/etc/issue - с приветствием до входа в текстовом режиме.

/etc/mtab - информация об уже смонтированных файловых системах.

/etc/shadow - все зашифрованные пароли хранятся тут!!! можно прочитать только с правами root

/etc/passwd - информация обо всех пользовательских аккаунтах

/var/log/messages --- Системный журнал!!!

/etc/X11/xorg.conf - конфигурационный файл X Window System