

# Международные системы сертификации специалистов

- Сертификационные программы
  - Cisco Systems
  - Microsoft
  - Oracle
  - Intel
  - IBM
  - ...
- Всемирные сети авторизованных центров тестирования
  - Sylvan Prometric (DRAKE TRAINING & TECHNOLOGIES в 90-х)
  - VUE (Virtual University Enterprises)

# Программы сертификации Linux Professional Institute (LPIC)

## I **LPIC Level 1**

- 101: General Linux I
- 102: General Linux II

## I **LPIC Level 2**

- 201: Advanced Administration.
- 202: Linux Optimization.

3-й уровень предполагается состоящим из набора специализированных экзаменов, по выбору будут сдаваться любые 2:

## I **LPIC Level 3.**

- 321: Windows Integration.
- 322: Internet Server.
- 323: Database Server.
- 324: Security, Firewalls, Encryption.
- 325: Kernel Internals & Device drivers; Creating distribution packages

# Программы сертификации SAIR

## Linux and GNU

- | **Linux Certified Professional (LCP) — 1 экзамен.**
  - 3X0-101: Installation & Configuration или 3X0-102: System Administration.
  
- | **Linux Certified Engineer (LCE) — 4 обязательных экзамена + экзамены по выбору.**
  - 3X0-101: Installation & Configuration.
  - 3X0-102: System Administration.
  - 3X0-103: Networking.
  - 3X0-104: Security, Ethics and Privacy.
  - ...
  
- | **Master Linux Certified Engineer (MLCE).**

На сегодня доступны экзамены 1-го уровня — 3X0-101 и 3X0-102.

# Администрирование

- | Установка ОС
- | Установка дополнительного ПО
- | Управление загрузкой ОС
- | Управление пользователями
- | Управление работающей системой
- | Сетевое администрирование

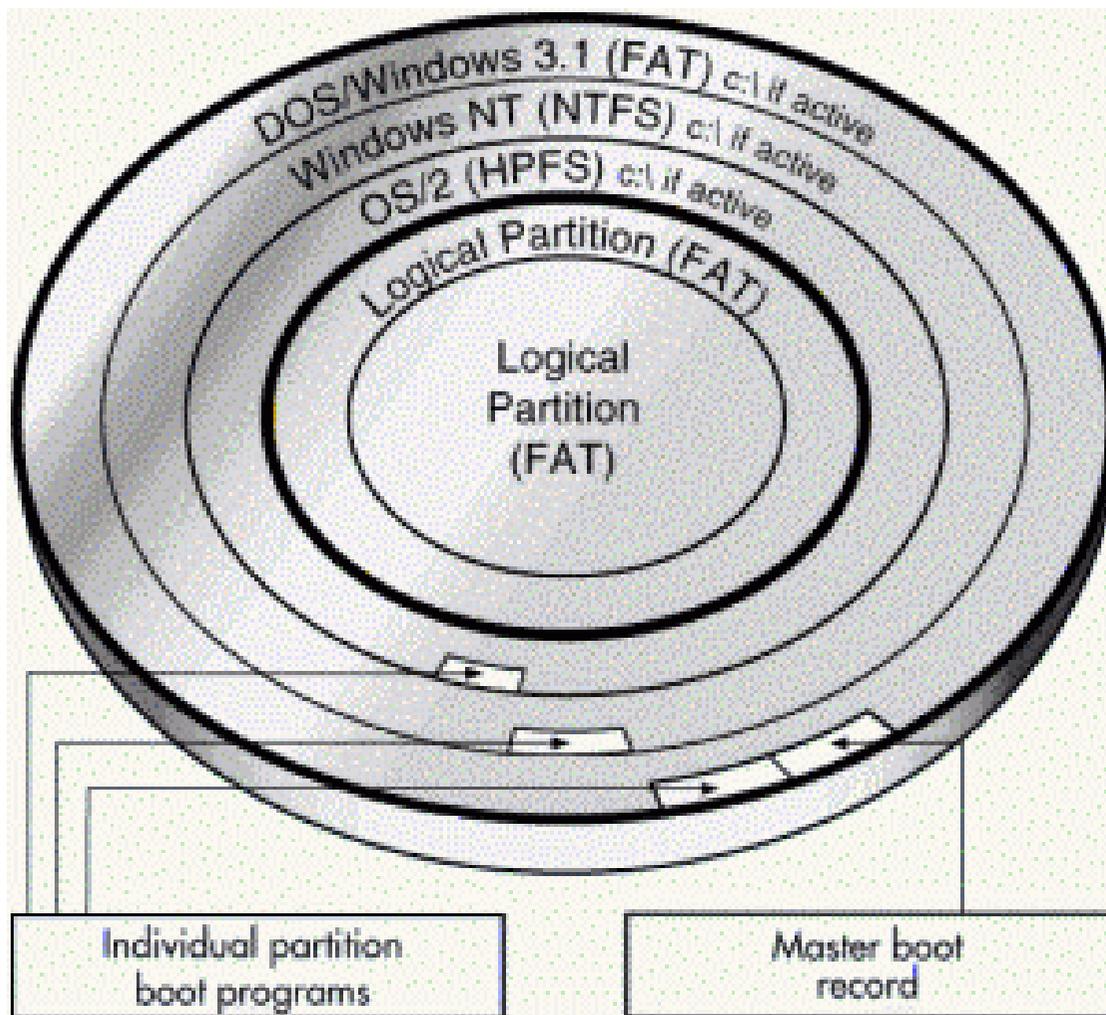
# Установка ОС и дополнительного ПО

- | В современных ОС осуществляется под управлением программ-менеджеров пакетов ПО (PM – package manager), например, RPM – Redhat Package Manager.
- | В задачи менеджера пакетов входит
  - | хранение в компактном виде ПО (обычно используются архиваторы tar, сrio и компрессоры gzip, bzip2)
  - | обеспечение гарантий подлинности ПО, например, с помощью цифровой подписи
  - | определение зависимостей устанавливаемого ПО от другого ПО, библиотек, ядра и т.п.
  - | ведение базы установленного ПО, например, для последующего удаления, модернизации, выдачи информации об установленном ПО и т.п.
  - | Хотя менеджер пакетов предназначен в основном для установки уже собранного (готового к использованию) ПО, исходные тексты программ также могут быть оформлены в виде пакетов и установлены с помощью менеджера.

# Загрузка ОС

- | загрузчик (bootstrap loader)
  - | реализуется по-разному на разном оборудовании, например, на ПК выполняется загрузка 1 сектора диска.
- | загрузка ядра
- | инициализация оборудования, конфигурирование драйверов, модули
- | монтирование корневой ФС в режиме read-only
  - | положение корневой ФС может быть определено ядром программой rdev или программами boot-manager
- | процесс init (/sbin/init) с PID=1, выполнение стартовых скриптов
- | запуск демонов, в т.ч. терминального getty
- | Для выключения системы необходимо завершить все процессы системы, синхронизировать разделы диска, содержащие ФС и соответствующие буферы, демонтировать ФС, например, с помощью программы shutdown. Для перезагрузки применяют shutdown -r now.

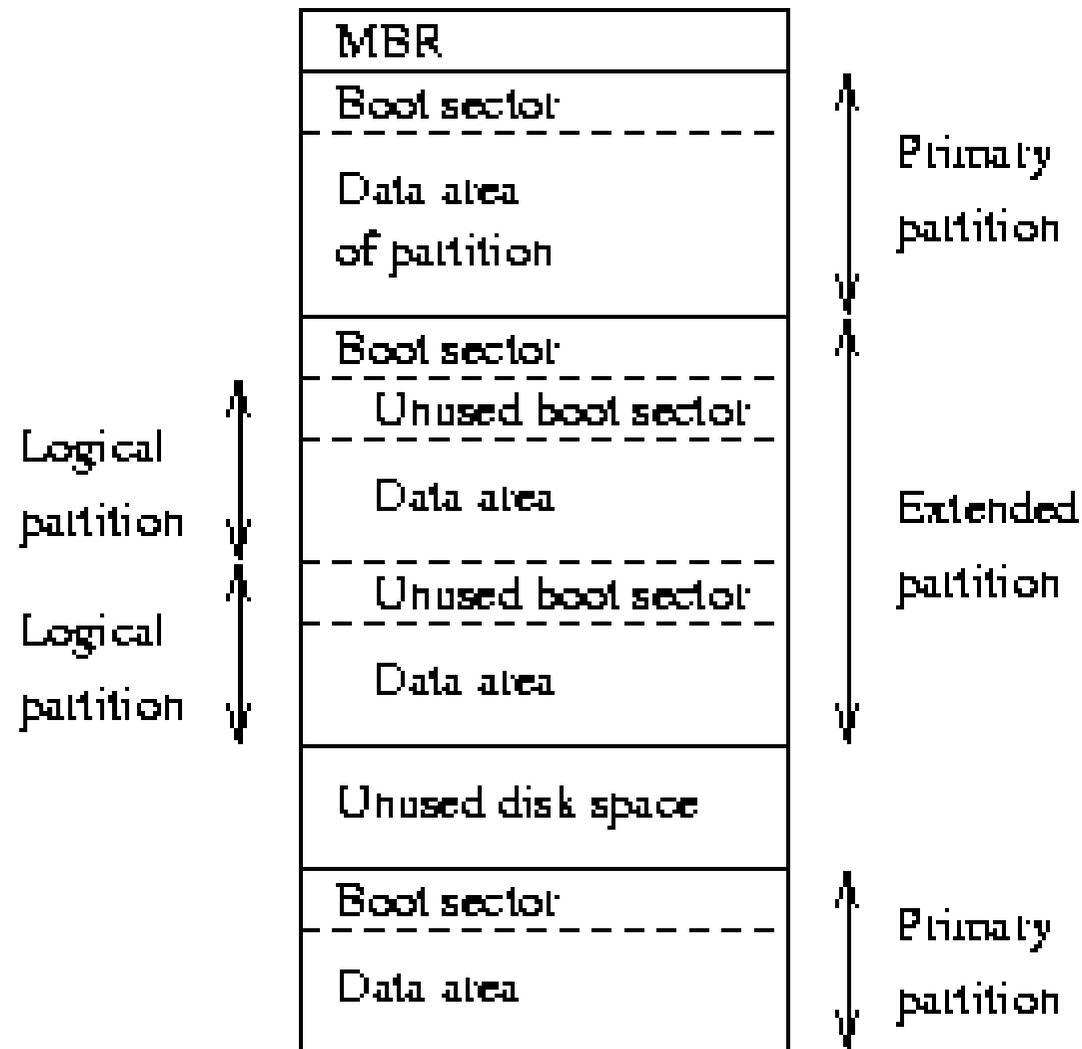
# Загрузка ОС на ПК



В MBR могут быть размещены:

- т.н. стандартный код, который, определяя флаг активности раздела, передает управление на загрузчик этого раздела
- специальная загрузочная программа «boot manager», например, LILO (Linux LOader), GRUB и т.п.

# Типы разделов, использование «расширенного» раздела



# Начало работы ядра

```
Loading linux.  
Console: colour EGA+ 80x25, 8 virtual consoles  
Serial driver version 3.94 with no serial options enabled  
tty00 at 0x03f8 (irq = 4) is a 16450  
tty01 at 0x02f8 (irq = 3) is a 16450  
lp_init: lp1 exists (0), using polling driver  
Memory: 7332k/8192k available (300k kernel code, 384k reserved, 176k  
data)  
Floppy drive(s): fd0 is 1.44M, fd1 is 1.2M  
Loopback device init  
Warning WD8013 board not found at i/o = 280.  
Math coprocessor using irq13 error reporting.  
Partition check:  
  hda: hda1 hda2 hda3  
VFS: Mounted root (ext filesystem).  
Linux version 0.99.pl9-1 (root@haven) 05/01/93 14:12:20
```

# Уровни работы ОС

- Большинство дистрибутивов Linux используют вариант init sysvinit, основанный на System V init. BSD варианта традиционно не поддерживают «уровни».
- Уровни (run levels) – состояния ОС (можно менять командой telinit):

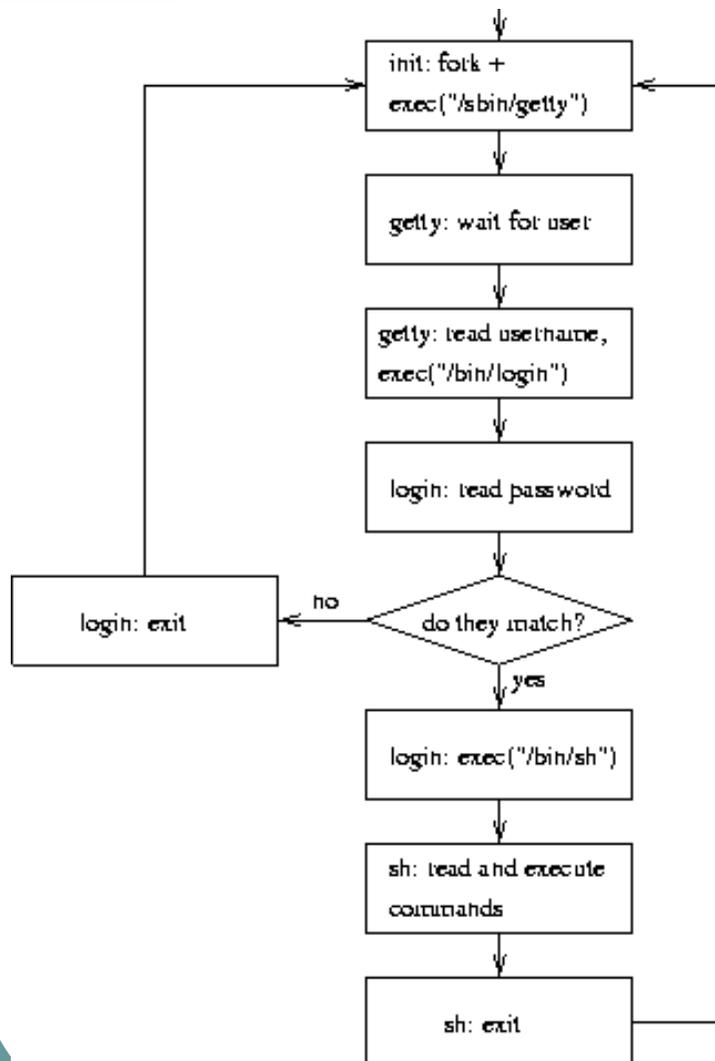
0	Halt the system. Остановка ОС
1	Single-user mode. Однопользовательский режим
2-5	Normal operation (user defined). Часто 3 – а/ц терминал, 5 – X Window
6	Reboot. Перезагрузка

Уровни конфигурируются в /etc/inittab (формат id:runlevels:action:process) :

```
id:3:initdefault:          1:2345:respawn:/sbin/mingetty tty1
l0:0:wait:/etc/rc.d/rc.halt 2:2345:respawn:/sbin/mingetty tty2
l1:1:wait:/etc/rc.d/rc.single 3:2345:respawn:/sbin/mingetty tty3
l2:2345:wait:/etc/rc.d/rc.multi
l6:6:wait:/etc/rc.d/rc.reboot x:5:respawn:/etc/X11/prefdm -nodaemon

m1:23:respawn:/usr/local/sbin/mgetty -n 5 tty00
```

# Регистрация пользователей в системе, «ВХОД В СИСТЕМУ» (login)



Программа login выполняет:

- аутентификацию пользователя
- устанавливает атрибуты на линию
- стартует шелл

Важные файлы для программы login, кроме баз passwd, shadow, group:

- /etc/motd
- /etc/nologin
- /var/run/utmp (w, who)
- /var/log/wtmp (last)

Система X использует xdm (менеджер дисплея) вместо login

# Начало выполнения шелла

- При запуске любой шелл выполняет predetermined стартовые скрипты. Положение и названия этих скриптов зависит от шелла, но обычно для sh это:
  - /etc/profile (редактируется системным администратором)
  - /etc/profile.d/ (в некоторых дистрибутивах, редактируется системным администратором)
  - .profile (редактируется пользователем)
- Для шелла bash иногда используются
  - .bash\_login, .bash\_profile, .bash\_logout

# Управление пользователями

- | редактирование файла `/etc/passwd` (и, возможно, `/etc/shadow`) с помощью редактора `vi`
- | редактирование файла `/etc/group` с помощью `vi`, если нужна новая группа
- | Создание домашнего каталога `mkdir`
- | Копирование "скелета" `/etc/skel` в домашний каталог
- | Установка атрибутов для домашнего каталога и его содержимого с помощью `chown` и `chmod` с ключом `-R`:
  - | `cd /home/ivanov`
  - | `chown -R ivanov.users .`
  - | `chmod -R u+rwX, go= .`
  - | `chmod go=x .`
- | Установка пароля с помощью `passwd`
- | Задание персональной информации и шелла: **chfn, chsh**
- | Удаление – обратная задача. Найти файлы: `find / -user ivanov`
- | Временное блокирование: `chsh -s /usr/local/lib/no-login/security ivanov`



# Службы наблюдения, протоколирования. Система регистрации событий SYSLOG (XPG4-UNIX, CISCO)

- | В ОС UNIX нет встроенной системы аудита, однако есть регистратор событий SYSLOG (XPG4-UNIX, CISCO)
  - | facility – система, источник сообщения
    - | kern, user, mail, daemon, auth, local0 .. local7
    - | соответствующие константы LOG\_KERN, ...
  - | priority/level – важность сообщения
    - | emerg, alert, crit, err, warning, notice, info, debug
    - | соответствующие константы: LOG\_EMERG, ...
  - | Использует дейтаграммный транспорт – UDP/IP, порт 514

# Библиотечные функции системы SYSLOG

```
openlog(const char *id, int log_option, int facility);
```

Типичное использование:

```
openlog(p->myname, POP_LOGOPTS, POP_FACILITY);  
syslog (stat, "%s", msgbuf);  
closelog();
```

Функции:

`openlog()`, `closelog()` открытие/инициализация лога и закрытие  
`syslog()` - запись в `syslog`  
`setlogmask()` - установка битов, разрешающих протоколирование  
для заданных приоритетов. Установленный бит - протоколирование  
сообщение с данным приоритетом разрешено.

# Конфигурация SYSLOG

```
#
# Конфигурационный файл демона syslogd
#
kern.debug          /var/adm/syslog/kern.log
kern.debug          /dev/console
daemon.debug        /var/adm/syslog/daemon.log
auth.debug          /var/adm/syslog/auth.log
syslog.debug        /var/adm/syslog/syslog.log
*.notice;mail.info /var/adm/syslog/mail
*.crit              /var/adm/syslog/critical
kern.err            @nix.cs.vsu.ru
*.emerg            *
*.alert            andrey, sergey
*.alert;auth.warning ivan
```

# Недостатки и достоинства SYSLOG

## I Некоторые недостатки:

- I события поступают от приложений и проверить правильность их нельзя;
- I нельзя проверить источник сообщения;
- I тип сообщения определяет приложение;
- I нет защиты от привилегированного приложения/пользователя.

## I Некоторые достоинства:

- I поддерживает прием сообщений по сети;
- I возможно создание изолированного сервера-регистратора;
- I поддерживается сетевым оборудованием: маршрутизаторы, управляемые коммутаторы, точки доступа и т.п.