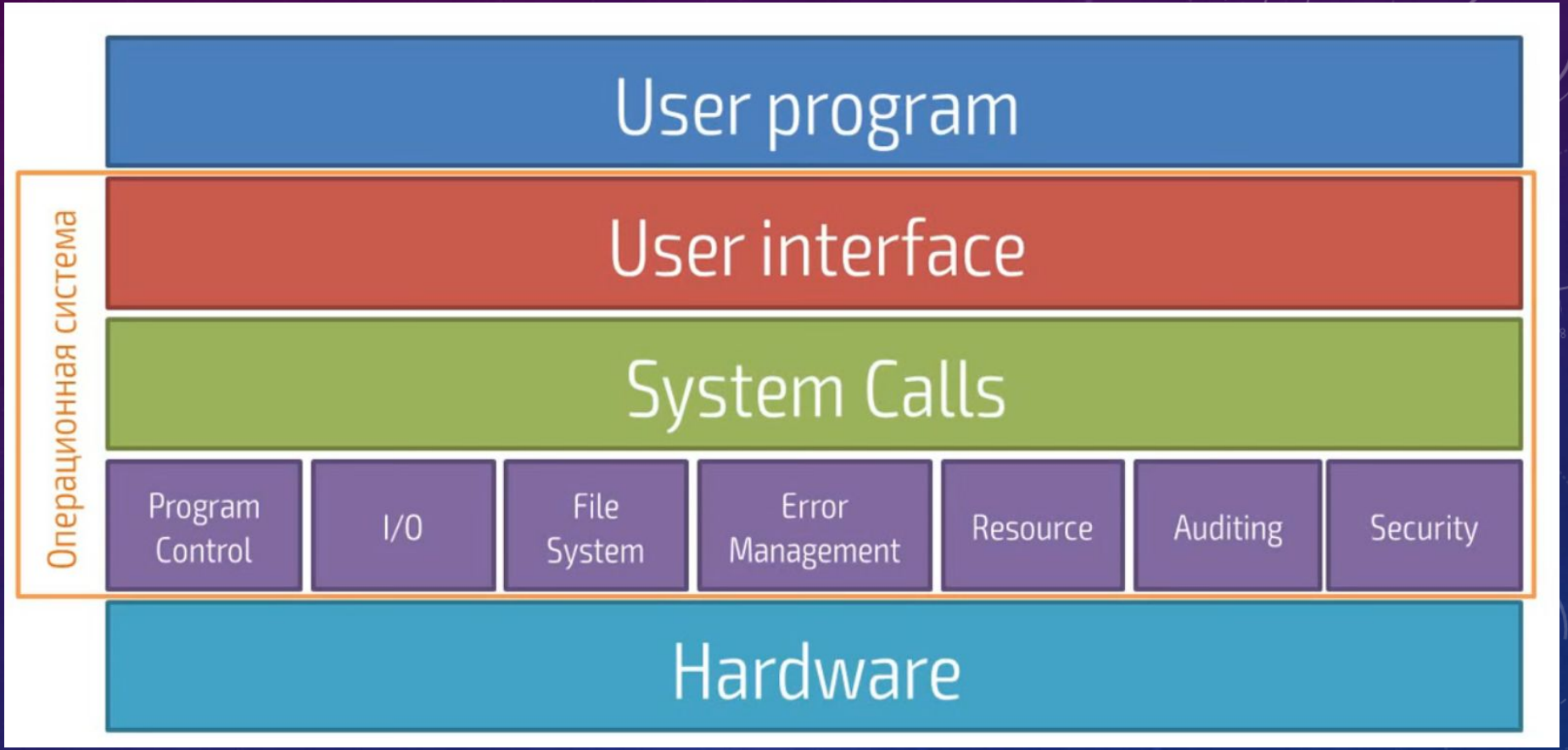
CTF – это соревнования в практической части информационной безопасности.

Основная цель – развитие личностных и профессиональных навыков в этой области

Хакер


User program
Операционная система
User interface
System Calls
Program Control
I/O
File System
Error Management
Resource
Auditing
Security
Hardware

Multics

Multiplexed **I**nformation and **C**omputing **S**ervice, 1964

Массачусетский Технологический Институт (MIT)

General Electric + Bell Labs

Ядро — 135 Кбайт

Multics

Иерархическая файловая система

Виртуальная память

Динамическое связывание (с библиотеками)

«Горячее» подключение и отключение процессоров, памяти, дисков

GE-645

UNIX

Uniplexed **I**nformation and **C**omputing **S**ervice

Bell Labs

Кен Томпсон, Деннис Ритчи

История UNIX

1969	Начало разработки
1971	Первый релиз
1972	Переписана на C
1973	Публичный релиз
1975-85	Рост популярности

PDP-7 1965

$ 72 000

18-битная архитектура

9–144 КБайт RAM

GNU Project 1983

Ричард Мэттью Столлман

Массачусетский Технологический Институт (MIT)

UNIX — $20 000 vs $150

GNU is **N**ot **U**nix

POSIX

Portable Operating System Interface

POSIX.1, Core Services — 1988

Процессы, сигналы, таймеры, пайпы

POSIX.1b, Real-time extensions — 1993

Расписание, семафоры, общая память

POSIX.1c, Threads — 1995

Потоки, управление потоками, синхронизация

POSIX.2, Shell and Utilities — 1992

POSIX-совместимые ОС

Полностью	Solaris, AIX, HP-UX, QNX
Частично	FreeBSD, GNU/Linux, MINIX
Windows	Cygwin, POSIX Subsystem

MINIX 1987

Эндрю Таненбаум, ОС для обучения

Амстердамский свободный университет

16-битная архитектура

Unix-подобная

Улучшения и патчи отвергались

История Linux

1991	GNU/Linux
1992	GNU/GPL
1993	>100 разработчиков, появились Slackware и Debian
1994	Linux 1.0

История Linux

1995	Поддержка платформ DEC Alpha, Sun SPARC
1996	Linux 2.0, Tux
1998	IBM, Compaq, Oracle заявили о поддержке Linux
1998	Начало разработки KDE
1999	GNOME

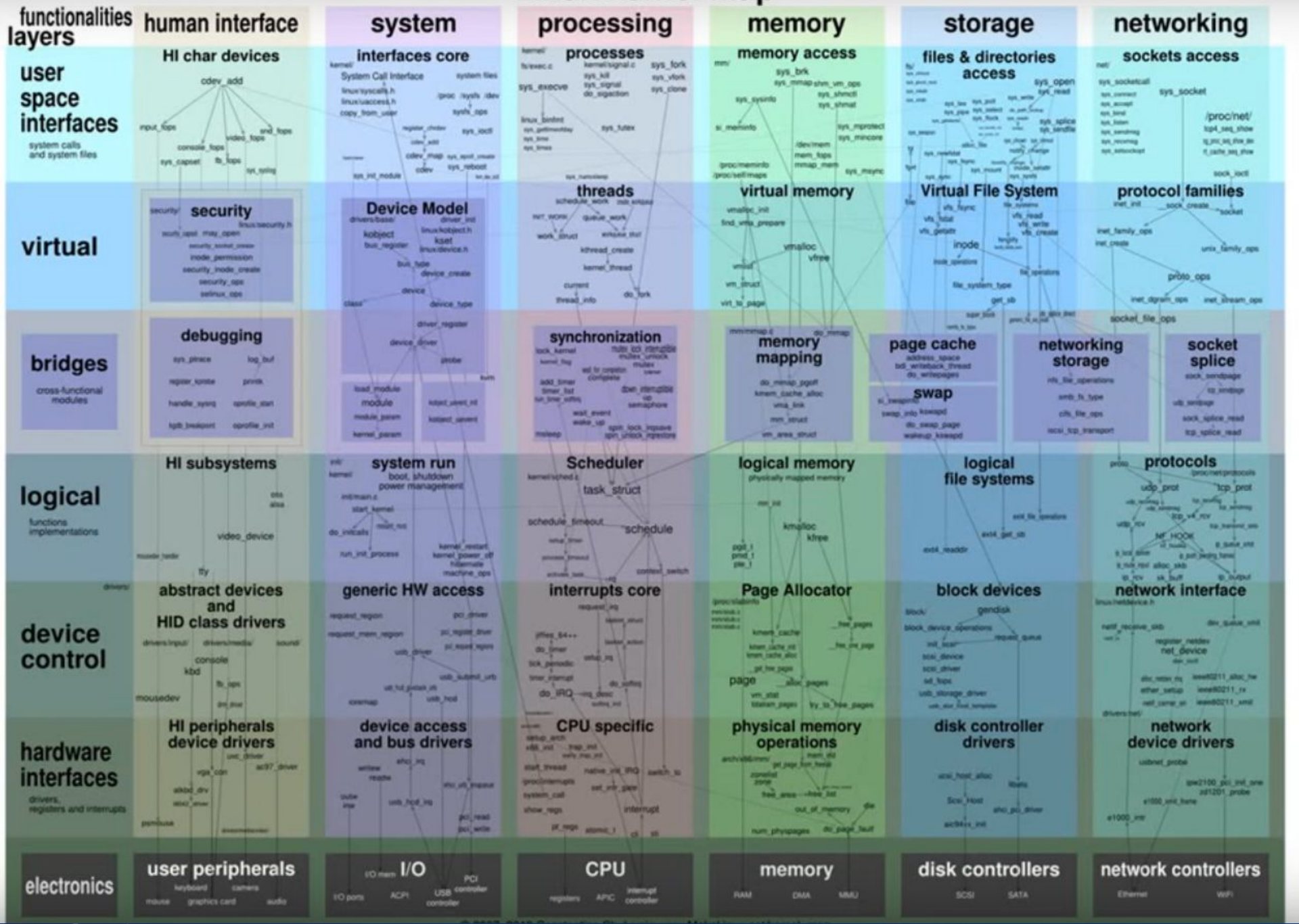
Linux сегодня

Android — 86% рынка смартфонов

98.8% из TOP500 суперкомпьютеров

Примерно 40 миллионов пользователей Ubuntu Desktop

Linux kernel map



Дистрибутивы GNU/Linux

ОС = ядро + софт + система пакетов

Коммерческие/community

Enterprise/Power user/Home user

LiveCD

GNU/Linux vs Windows

Open source/Closed source

Бесплатно/Платно

Лицензия: свободная/с ограничениями

Командная строка/Графический интерфейс

Репозиторий с ПО/—

Более гибкий/менее гибкий

Unix Way

Простые, но мощные программы

Сила во взаимодействии программ

Текстовый интерфейс взаимодействия

(Почти) всё есть файл

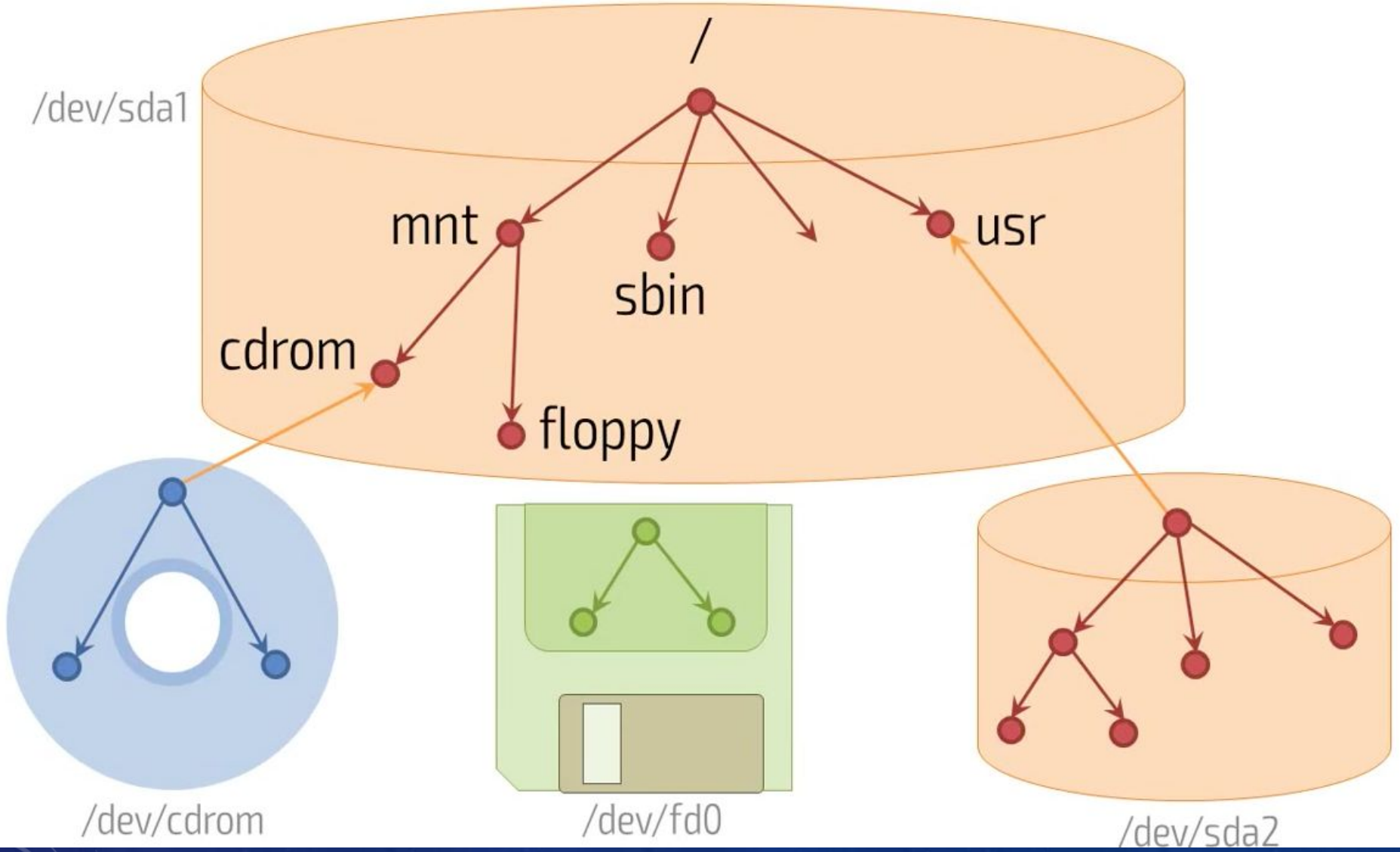
Консоль/командная строка

Примеры

```
grep var /etc/passwd | cut –d: -f1 | sort
dd if=/dev/hda | gzip –c > /mnt/backup/hda.gz
```

Загрузка системы

BIOS	Basic input-output system
MBR	Master Boot Record
GRUB	Загружает ядро
Ядро	Запускает процесс /init
Init	Запускает приложения


/
/dev/sda1
mnt
sbin
usr
cdrom
floppy
/dev/cdrom
/dev/fd0
/dev/sda2

Файловая система

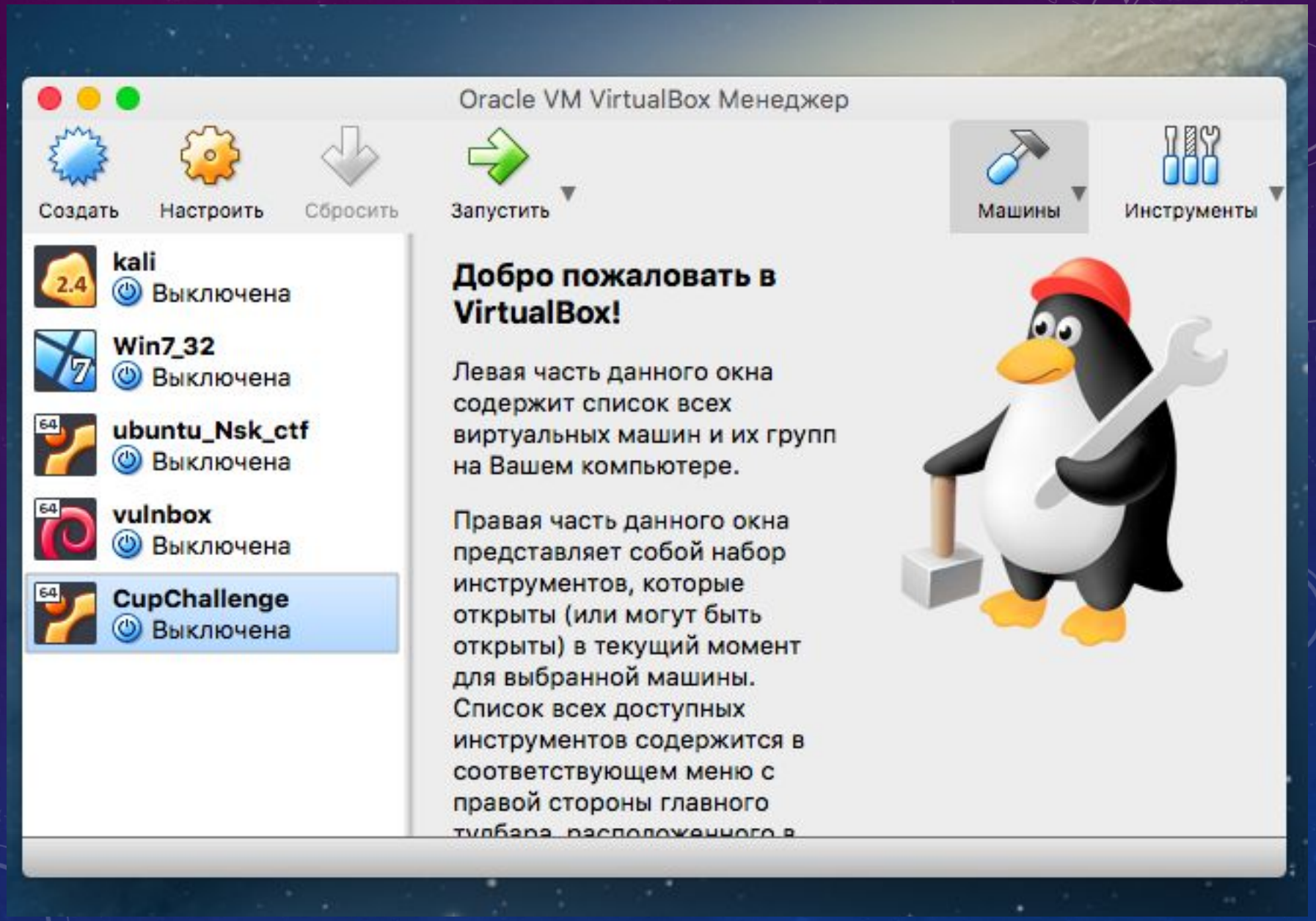
/bin	исполняемые файлы
/boot	ядро, загрузчик, начальный образ ФС
/dev	устройства
/etc	настройки
/home	домашние каталоги пользователей
/lib	библиотеки и модули ядра

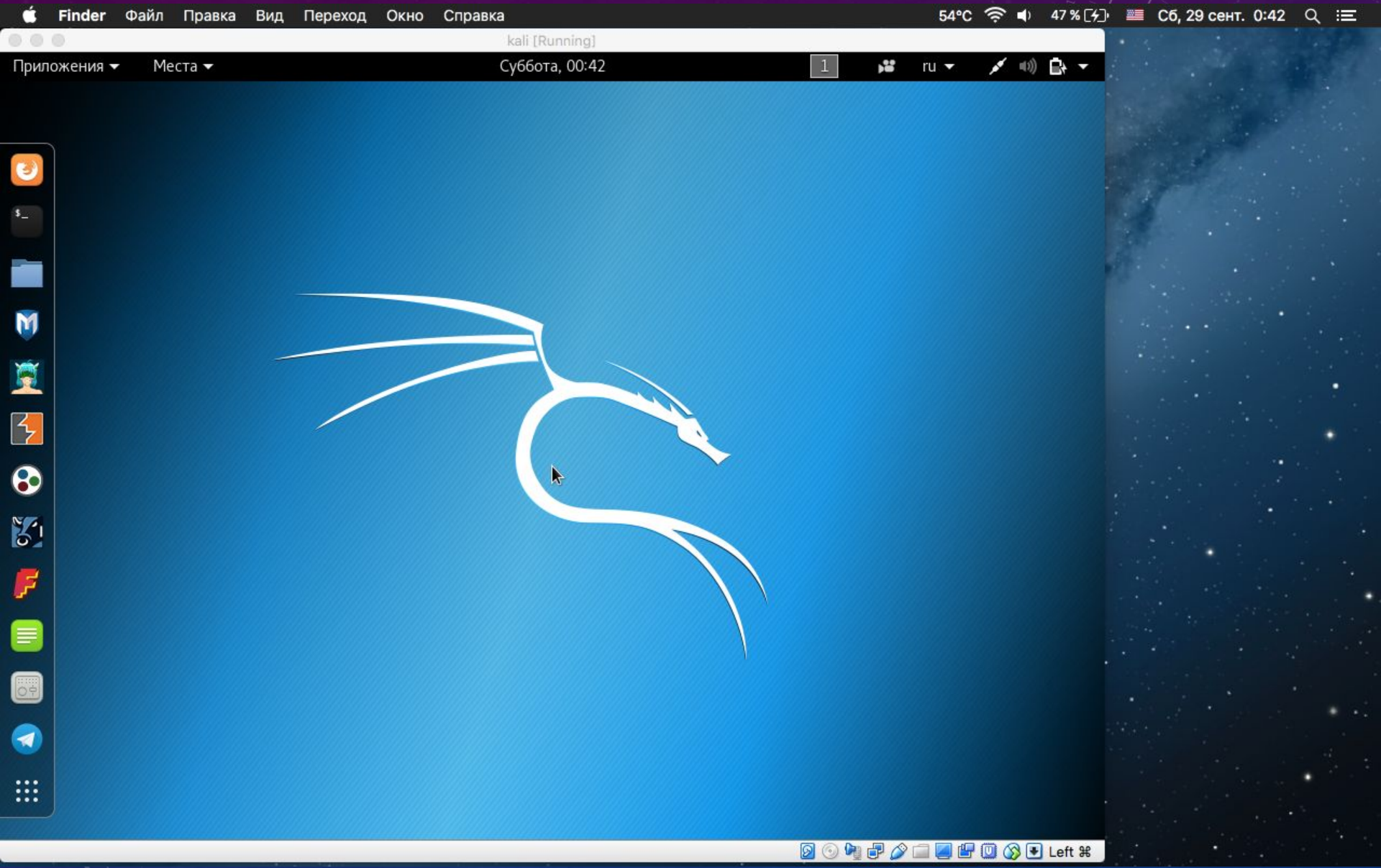
Файловая система

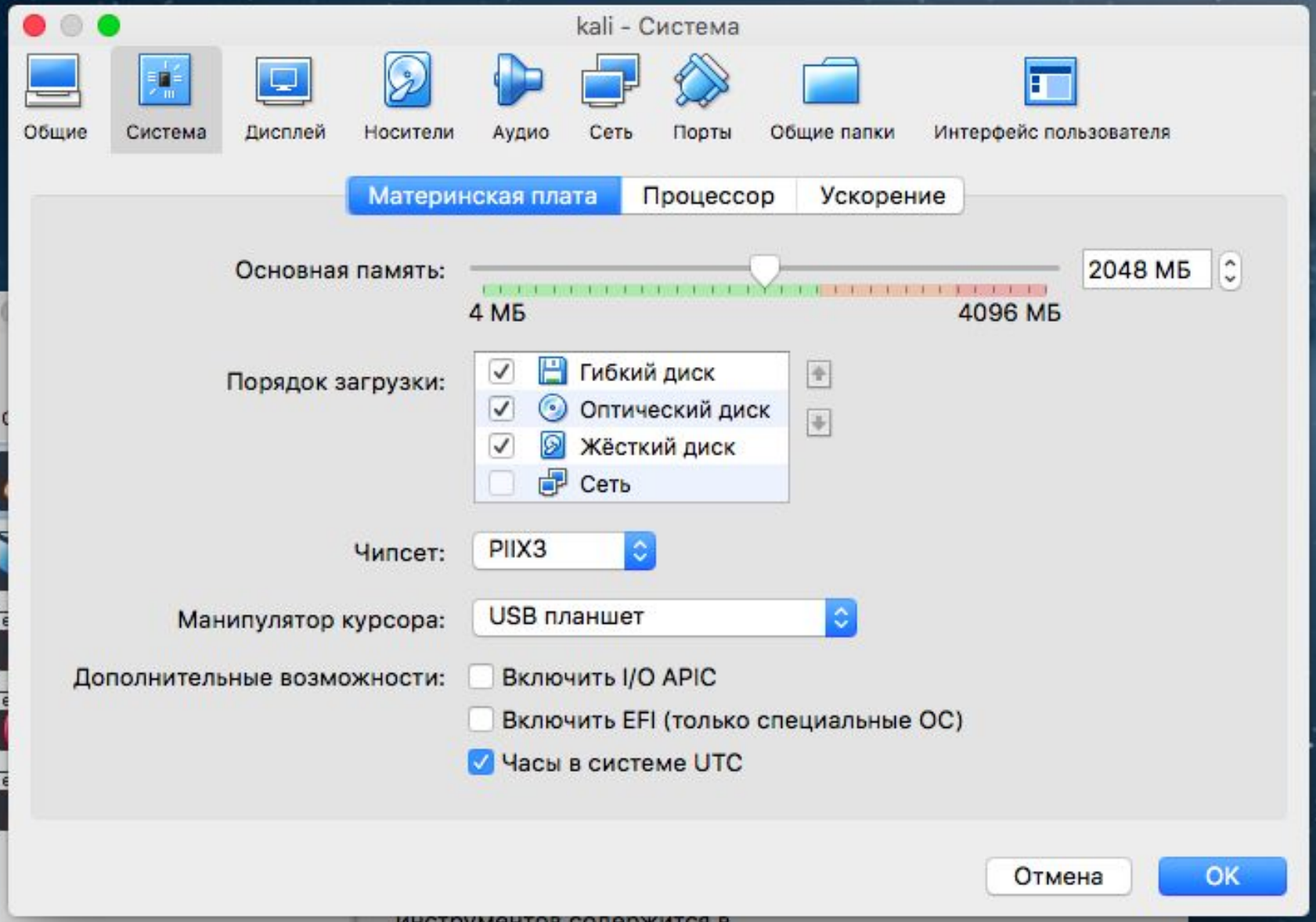
/lost+found	найденные файлы
/mnt	точки монтирования
/proc	информация ядра
/root	домашний каталог root'а
/tmp	временные файлы
/var	часто изменяемые файлы

Важные файлы в /etc

/etc/passwd	пользователи
/etc/group	группы
/etc/shadow	хеши паролей
/etc/fstab	точки монтирования
/etc/inittab	настройка старта системы
/etc/sysctl.conf	настройка ядра


Oracle VM VirtualBox Менеджер
Создать
Настроить
Сбросить
Запустить
Машины
Инструменты
kali
Выключена
Win7_32
Выключена
ubuntu_Nsk_ctf
Выключена
vulnbox
Выключена
CupChallenge
Выключена
Добро пожаловать в VirtualBox!
Левая часть данного окна содержит список всех виртуальных машин и их групп на Вашем компьютере.
Правая часть данного окна представляет собой набор инструментов, которые открыты (или могут быть открыты) в текущий момент для выбранной машины. Список всех доступных инструментов содержится в соответствующем меню с правой стороны главного


Finder Файл Правка Вид Переход Окно Справка
54°C
47 %
Сб, 29 сент. 0:42
kali [Running]
Приложения
Места
Суббота, 00:42
1
ru
Left ⌘



инструментов содержится в
соответствующем меню с
правой стороны главного
тулбара, расположенного в