



CTF – это соревнования в практической части информационной безопасности.

Основная цель – развитие личностных и профессиональных навыков в этой области









Хакер

User program

User interface

System Calls

Program
Control

I/O

File
System

Error
Management

Resource

Auditing

Security

Hardware

Операционная система

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



The top of the slide features a purple header with technical graphics, including a circular gauge with numbers 60, 170, 180, 190, 200, and 210, and various concentric circles and lines.

UNIX

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

Bell Labs

Кен Томпсон, Деннис Ритчи

The bottom of the slide features a blue footer with technical graphics, including a circular gauge with an arrow and various concentric circles and lines.

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 Not Unix

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

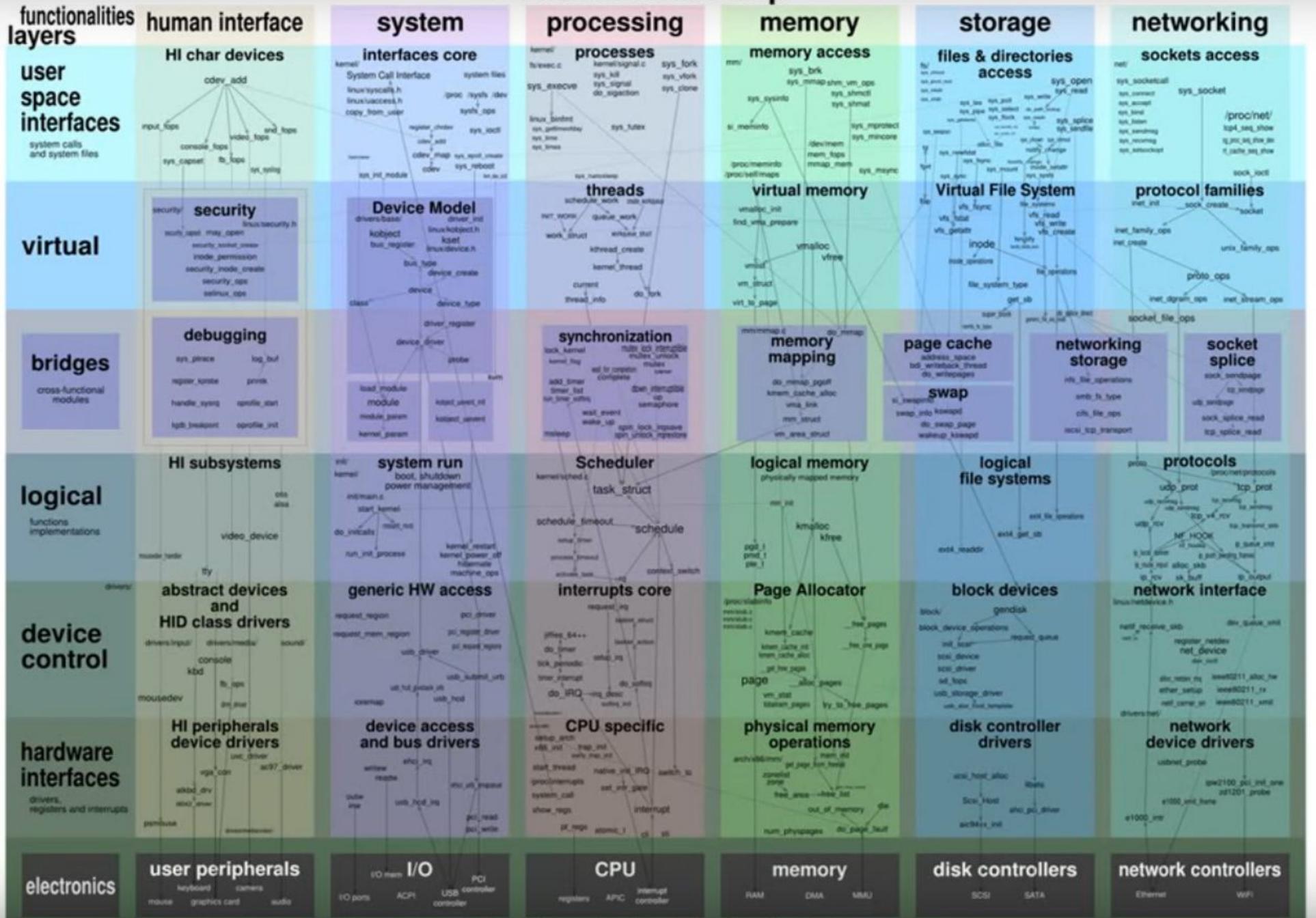
Linux сегодня

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

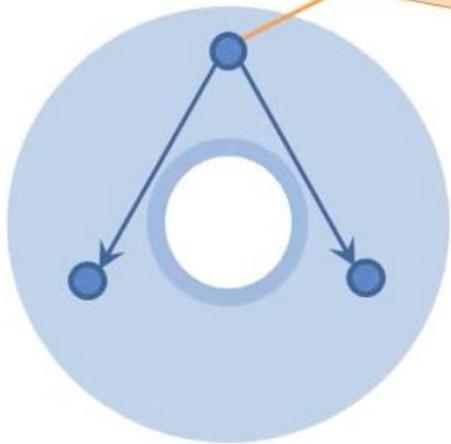
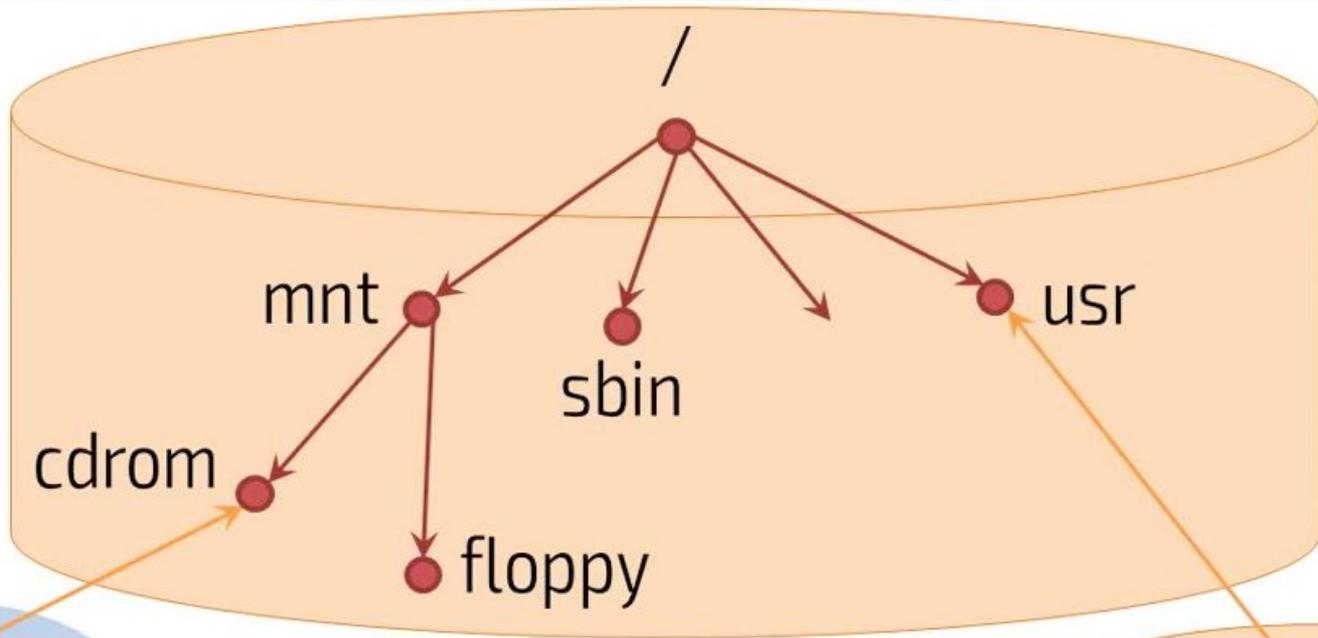
Ядро

Запускает процесс /init

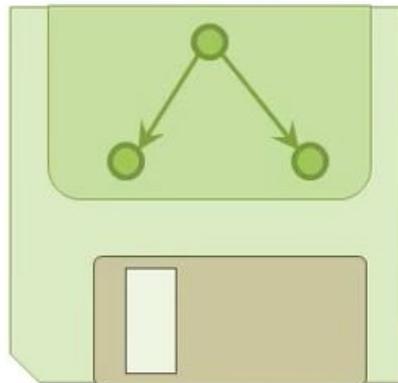
Init

Запускает приложения

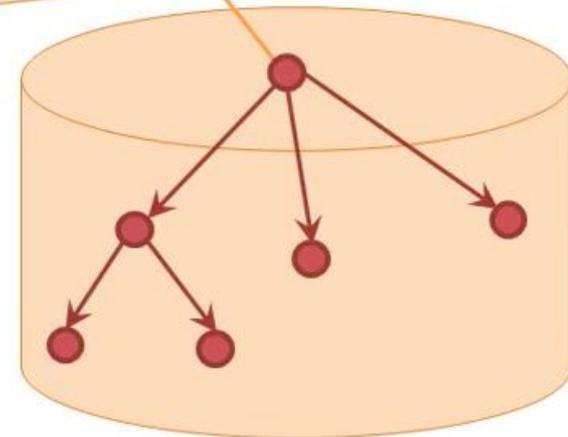
/dev/sda1



/dev/cdrom



/dev/fd0



/dev/sda2

Файловая система

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

Файловая система

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

Важные файлы в /etc

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



Oracle VM VirtualBox Менеджер



Создать



Настроить



Сбросить



Запустить



Машины



Инструменты



kali

Выключена



Win7_32

Выключена



ubuntu_Nsk_ctf

Выключена



vulnbox

Выключена



CupChallenge

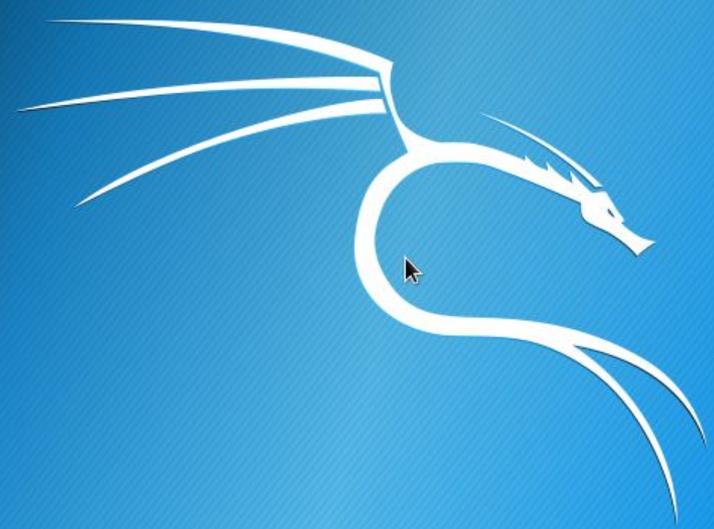
Выключена

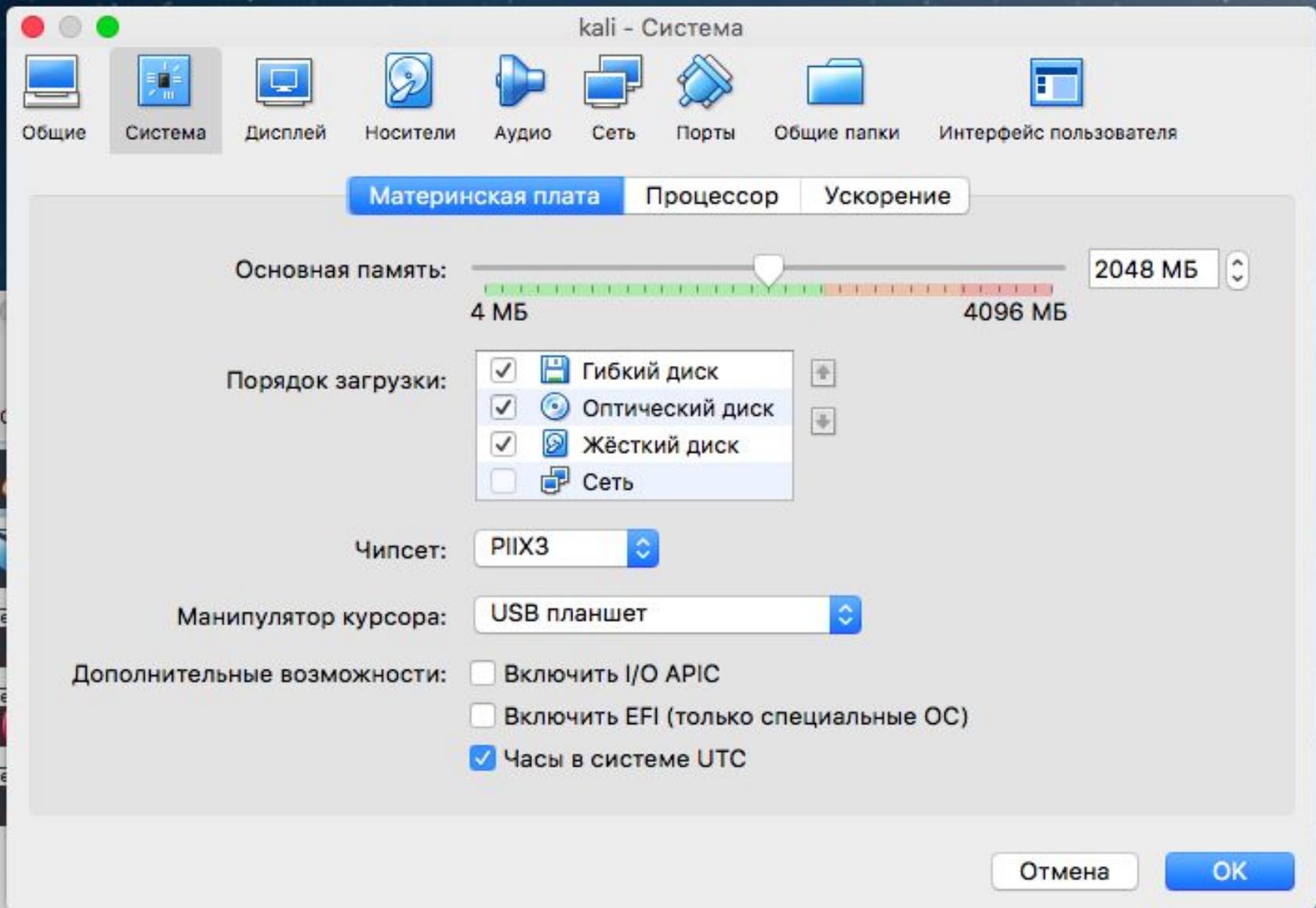
Добро пожаловать в VirtualBox!

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 тулбара, расположенного в







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