

Презентация по лабораторной работе №1

Основы информационной безопасности

Петрова А.А.

22 февраля 2025

Российский университет дружбы народов, Москва, Россия

Информация

::::::::::::: {.columns align=center} ::: {.column width="70%"}

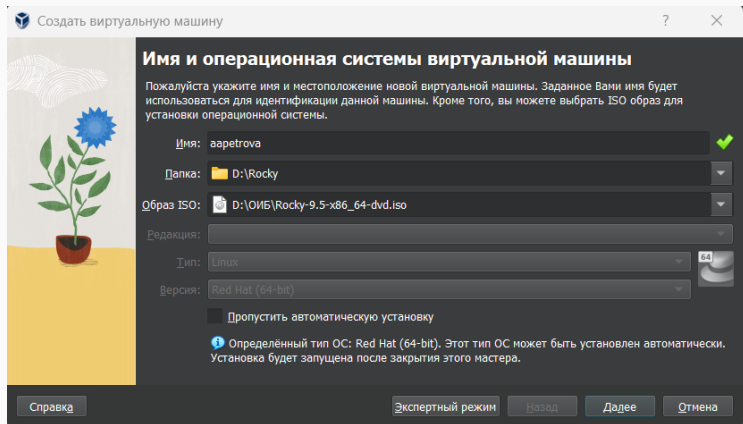
- Петрова Алевтина Александровна
- НКАбд-04-23
- Российский университет дружбы народов

Целью данной работы является приобретение практических навыков установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов.

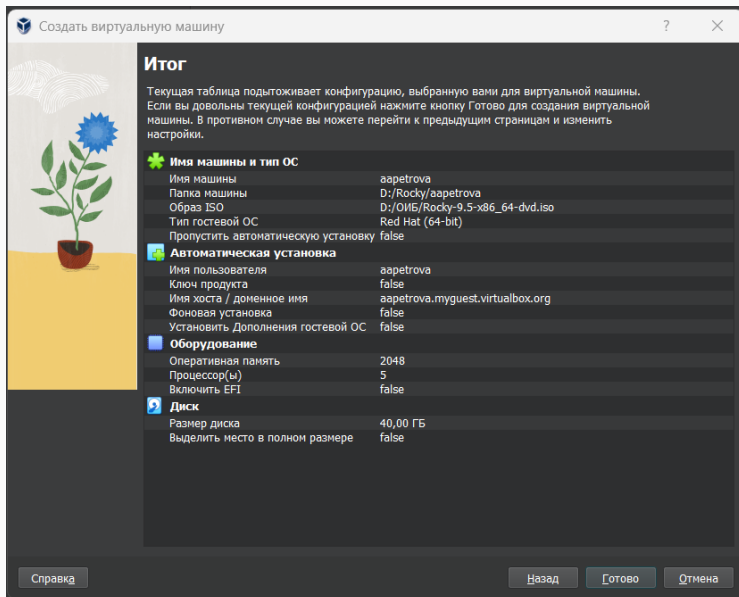
1. Установка и настройка операционной системы.
2. Найти следующую информацию:
 - 2.1 Версия ядра Linux (Linux version).
 - 2.2 Частота процессора (Detected Mhz processor).
 - 2.3 Модель процессора (CPU0).
 - 2.4 Объем доступной оперативной памяти (Memory available).
 - 2.5 Тип обнаруженного гипервизора (Hypervisor detected).
 - 2.6 Тип файловой системы корневого раздела.

Выполнение лабораторной работы

Для начала создаю новую виртуальную машину в VirtualBox, выбираю имя, местоположение и образ ISO, устанавливать будем операционную систему Rocky DVD



Соглашаюсь с предоставленными настройками



Начинается загрузка операционной системы

Rocky Linux 9.5

Install Rocky Linux 9.5

Test this media & install Rocky Linux 9.5

Troubleshooting

>

Press Tab for full configuration options on menu items.

Automatic boot in 15 seconds...

При этом должен быть подключен в носителях образ диска!

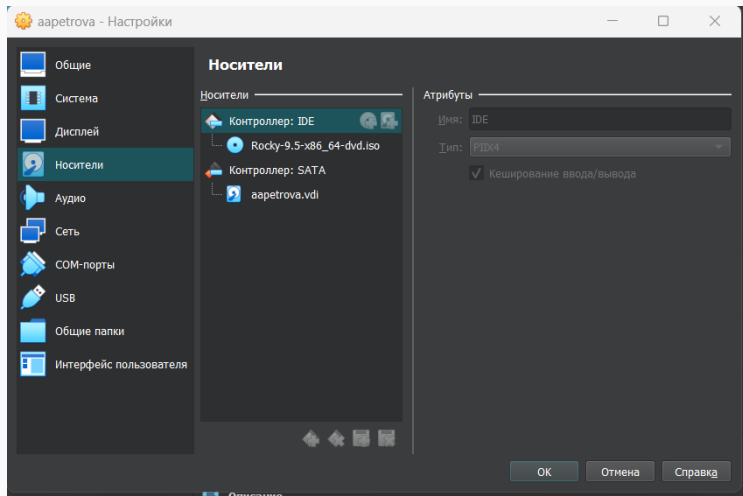


Рис. 4: Подключенные носители

Выбираю язык установки

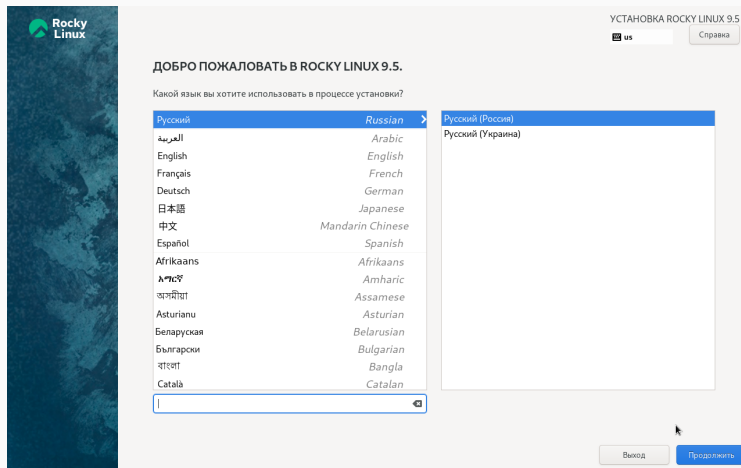


Рис. 5: Выбор языка установки

В обзоре установки будем проверять все настройки и менять на нужные

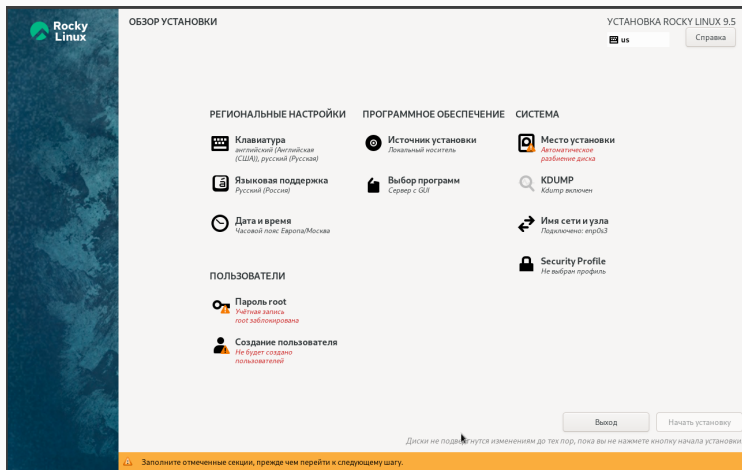


Рис. 6: Окно настроек

Начало установки

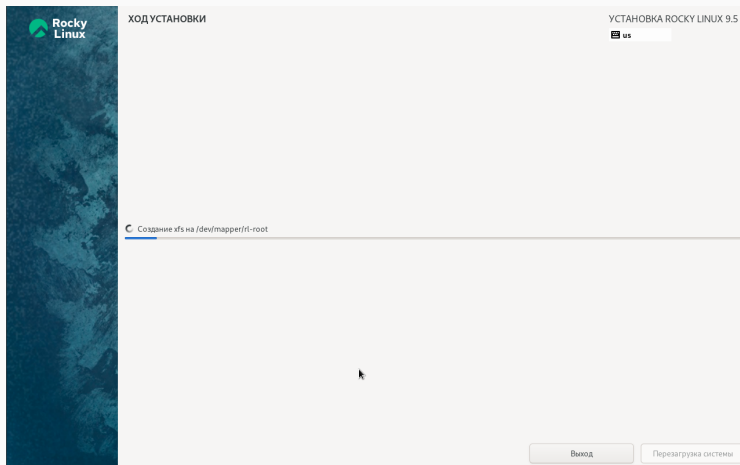


Рис. 7: Установка

После завершения установки образ диска сам пропадет из носителей

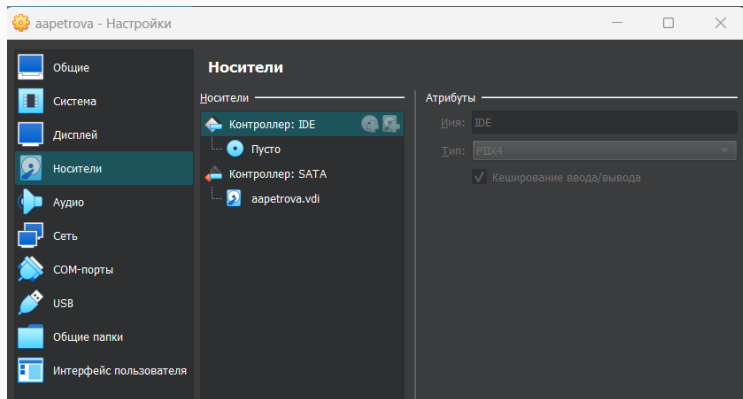


Рис. 8: Проверка носителей

##После установки при запуске операционной системы появляется окно выбора пользователя

Выполнение дополнительного задания

Открываю терминал, в нем прописываю `dmesg | less`

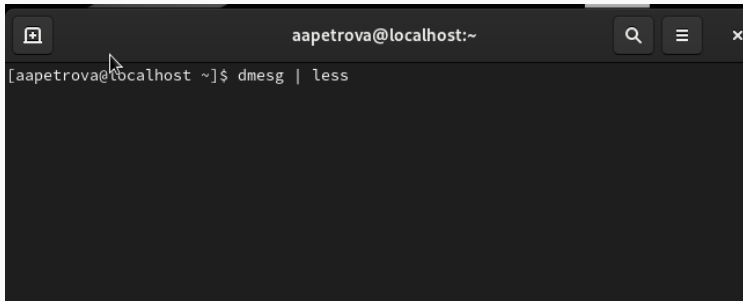
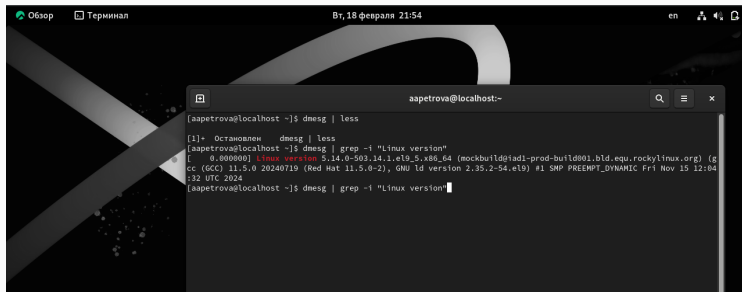


Рис. 10: Окно терминала

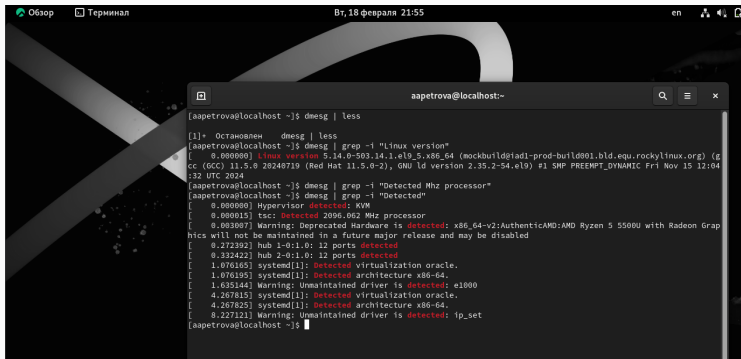
Версия ядра 5.14.0-362.8.1.el9_3.x86_64



```
[aapetrova@localhost ~]$ dmesg | less
[1]+  Остановлен  dmesg | less
[aapetrova@localhost ~]$ dmesg | grep -i "Linux version"
[    0.000000] Linux version 5.14.0-503.14.1.el9_5.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.5.0 20240719 (Red Hat 11.5.0-2), GNU ld version 2.35.2-54.el9) #1 SMP PREEMPT_DYNAMIC Fri Nov 15 12:04:32 UTC 2024
[aapetrova@localhost ~]$ dmesg | grep -i "Linux version"
```

Рис. 11: Версия ядра

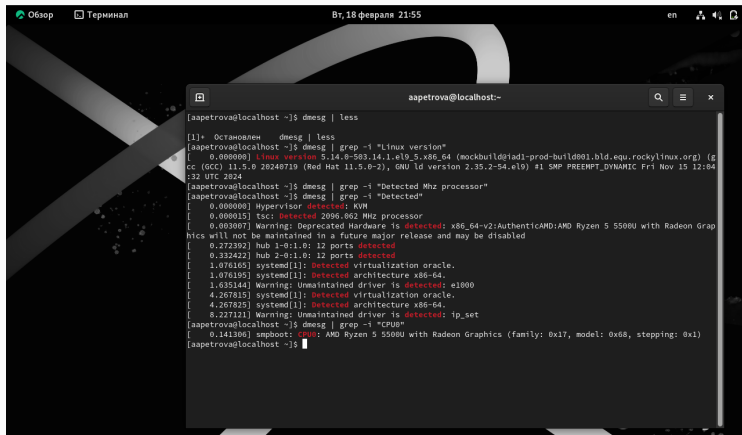
Частота процессора 1993 МГц



```
[aapetrova@localhost ~]$ dmesg | less
[1]+  Остановлен  dmesg | less
[aapetrova@localhost ~]$ dmesg | grep -i "Linux version"
[ 0.000000] Linux version 5.14.0-503.14.1.el9_5.x86_64 (mockbuild@ad1-prod-build001.bld.equ.rockylinux.org) (g
cc (GCC) 11.5.0 20240719 (Red Hat 11.5.0-2), GNU ld version 2.35.2-54.el9) #1 SMP PREEMPT_DYNAMIC Fri Nov 15 12:04
:32 UTC 2024
[aapetrova@localhost ~]$ dmesg | grep -i "Detected Mhz processor"
[aapetrova@localhost ~]$ dmesg | grep -i "Detected"
[ 0.000000] Hypervisor detected: KVM
[ 0.000015] tsc: Detected 2096.062 Mhz processor
[ 0.003007] Warning: Deprecated Hardware is detected: x86_64-v2:AuthenticAMD:AMD Ryzen 5 5500U with Radeon Grap
hics will not be maintained in a future major release and may be disabled
[ 0.272392] hub 1-0:1.0: 12 ports detected
[ 0.332422] hub 2-0:1.0: 12 ports detected
[ 1.076165] systemd[1]: Detected virtualization oracle.
[ 1.076195] systemd[1]: Detected architecture x86-64.
[ 1.635144] Warning: Unmaintained driver is detected: e1000
[ 4.267815] systemd[1]: Detected virtualization oracle.
[ 4.267825] systemd[1]: Detected architecture x86-64.
[ 8.227121] Warning: Unmaintained driver is detected: ip_set
[aapetrova@localhost ~]$
```

Рис. 12: Частота процессора

Модель процессора Intel Core i7-8550U



```
[aapetrova@localhost ~]$ dmesg | less
[1]+  Остановлен  dmesg | less
[aapetrova@localhost ~]$ dmesg | grep -i "Linux version"
[ 0.000000] Linux version 5.14.0-503.14.1.el9_5.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (g
cc (GCC) 11.5.0 20240719 (Red Hat 11.5.0-2), GNU ld version 2.35.2-54.el9) #1 SMP PREEMPT_DYNAMIC Fri Nov 15 12:04
:32 UTC 2024
[aapetrova@localhost ~]$ dmesg | grep -i "Detected Mhz processor"
[aapetrova@localhost ~]$ dmesg | grep -i "Detected"
[ 0.000000] Hypervisor detected: KVM
[ 0.000015] tsc: Detected 2096.062 MHz processor
[ 0.003007] Warning: Deprecated Hardware is detected: x86_64-v2:AuthenticAMD:AMD Ryzen 5 5500U with Radeon Grap
hics will not be maintained in a future major release and may be disabled
[ 0.272392] hub 1-0:1.0: 12 ports detected
[ 0.332422] hub 2-0:1.0: 12 ports detected
[ 1.076165] systemd[1]: Detected virtualization oracle.
[ 1.076195] systemd[1]: Detected architecture x86_64.
[ 1.635144] Warning: Unmaintained driver is detected: e1000
[ 4.267815] systemd[1]: Detected virtualization oracle.
[ 4.267835] systemd[1]: Detected architecture x86_64.
[ 8.227121] Warning: Unmaintained driver is detected: ip_set
[aapetrova@localhost ~]$ dmesg | grep -i "CPU"
[ 0.141306] smpboot: CPU0: AMD Ryzen 5 5500U with Radeon Graphics (family: 0x17, model: 0x68, stepping: 0x1)
[aapetrova@localhost ~]$
```

Рис. 13: Модель процессора

Доступно 260860 Кб из 2096696 Кб

```

[ 1.635144] Warning: Unmaintained driver is detected: e1000
[ 4.267815] systemd[1]: Detected virtualization oracle.
[ 4.267825] systemd[1]: Detected architecture x86-64.
[ 8.227121] Warning: Unmaintained driver is detected: ip_set
[aapetrova@localhost ~]$ dmesg | grep -i "CPU0"
[ 0.141286] apbboot: CPU0: AMD Ryzen 5 5600U with Radeon Graphics (family: 0x17, model: 0x68, stepping: 0x1)
[aapetrova@localhost ~]$ dmesg | grep -i "Memory available"
[aapetrova@localhost ~]$ dmesg | grep -i "Memory"
[ 0.001703] ACPI: Reserving FACP table memory at [mem 0x7ffff0f0-0x7ffff01e3]
[ 0.001704] ACPI: Reserving DSDT table memory at [mem 0x7ffff0620-0x7ffff2972]
[ 0.001704] ACPI: Reserving FACS table memory at [mem 0x7ffff0200-0x7ffff023f]
[ 0.001705] ACPI: Reserving FACS table memory at [mem 0x7ffff0200-0x7ffff023f]
[ 0.001706] ACPI: Reserving APIC table memory at [mem 0x7ffff0240-0x7ffff02ab]
[ 0.001706] ACPI: Reserving SSDT table memory at [mem 0x7ffff02b0-0x7ffff061b]
[ 0.002055] Early memory node ranges
[ 0.002996] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x00000fff]
[ 0.002997] PM: hibernation: Registered nosave memory: [mem 0x0009f000-0x0009ffff]
[ 0.002998] PM: hibernation: Registered nosave memory: [mem 0x000a0000-0x000effff]
[ 0.002998] PM: hibernation: Registered nosave memory: [mem 0x000f0000-0x000fffff]
[ 0.010677] Memory: 242428K/2096696K available (16384K kernel code, 5685K rodata, 12904K rodata, 3976K init, 5672K bss, 148664K reserved, 0K cma-reserved)
[ 0.032225] Freeing SMP alternatives memory: 48K
[ 0.155309] x86/mm: Memory block size: 128MB
[ 0.263418] Non-volatile memory driver v1.3
[ 0.805748] Freeing initrd memory: 57584K
[ 1.006018] Freeing unused decrypted memory: 2028K
[ 1.006827] Freeing unused kernel image (initmem) memory: 3976K
[ 1.007524] Freeing unused kernel image (rodata/data gap) memory: 1432K
[ 2.106932] vmwgfx 0000:00:02.0: [drm] Legacy memory limits: VRAM = 51200 kB, FIFO = 2048 kB, surface = 473088 kB
[ 2.106941] vmwgfx 0000:00:02.0: [drm] Maximum display memory size is 51200 kiB
[aapetrova@localhost ~]$
  
```

Рис. 14: Объем доступной оперативной памяти

Обнаруженный гипервизор типа KVM

```

[ 8.227121] Warning: Unmaintained driver is detected: ip_set
[aapetrova@localhost ~]$ dmesg | grep -i "CPU0"
[ 0.141306] smpboot: CPU0: AMD Ryzen 5 5500U with Radeon Graphics (family: 0x17, model: 0x68, stepping: 0x1)
[aapetrova@localhost ~]$ dmesg | grep -i "Memory available"
[aapetrova@localhost ~]$ dmesg | grep -i "Memory"
[ 0.001703] ACPI: Reserving FACP table memory at [mem 0x7ffff000-0x7ffff01c]
[ 0.001704] ACPI: Reserving DSDT table memory at [mem 0x7ffff020-0x7ffff072]
[ 0.001704] ACPI: Reserving FACS table memory at [mem 0x7ffff200-0x7ffff23f]
[ 0.001705] ACPI: Reserving FACS table memory at [mem 0x7ffff200-0x7ffff23f]
[ 0.001706] ACPI: Reserving APIC table memory at [mem 0x7ffff240-0x7ffff2ab]
[ 0.001706] ACPI: Reserving SSDT table memory at [mem 0x7ffff2b0-0x7ffff61b]
[ 0.002055] Early memory node ranges
[ 0.002996] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x00000fff]
[ 0.002997] PM: hibernation: Registered nosave memory: [mem 0x0009f000-0x0009ffff]
[ 0.002998] PM: hibernation: Registered nosave memory: [mem 0x000a0000-0x000aefff]
[ 0.002998] PM: hibernation: Registered nosave memory: [mem 0x000f0000-0x000fffff]
[ 0.010677] Memory: 242428K/2096696K available (16384K kernel code, 5685K rdata, 12904K rodata, 3976K init, 5672K bss, 148664K reserved, 0K cma-reserved)
[ 0.032225] Freeing SMP alternatives memory: 40K
[ 0.155309] x86/mm: Memory block size: 128MB
[ 0.263418] Non-volatile memory driver v1.3
[ 0.805748] Freeing initrd memory: 57584K
[ 1.006018] Freeing unused decrypted memory: 2028K
[ 1.006827] Freeing unused kernel image (initmem) memory: 3976K
[ 1.007524] Freeing unused kernel image (rodata/data gap) memory: 1432K
[ 2.106932] vmwgfx 0000:00:02.0: [drm] Legacy memory limits: VRAM = 51200 kB, FIFO = 2048 kB, surface = 473088 kB
[ 2.106941] vmwgfx 0000:00:02.0: [drm] Maximum display memory size is 51200 kB
[aapetrova@localhost ~]$ dmesg | grep -i "Hypervisor"
[ 0.000000] Hypervisor detected: KVM
[ 2.106883] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported hypervisor.
[aapetrova@localhost ~]$
  
```

Рис. 15: Тип обнаруженного гипервизора

`sudo fdisk -l` показывает тип файловой системы, типа Linux, Linux LVM

```

aapetrova@localhost:~$ sudo fdisk -l

Мы полагаем, что ваш системный администратор изложил вам основы
безопасности. Как правило, все сводится к трём следующим правилам:

#1) Уважайте частную жизнь других.
#2) Думайте, прежде что-то вводить.
#3) С большой властью приходит большая ответственность.

[sudo] пароль для aapetrova:

Диск /dev/sda: 40 GiB, 42949672960 байт, 83886080 секторов
Disk model: VBOX HARDDISK
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Тип метки диска: dos
Идентификатор диска: 0xb9009355

Устр-во  Загрузочный  начало  Конец  Секторы  Размер  Идентификатор  Тип
/dev/sda1 *          2048  2099199  2097152    1G      83 Linux
/dev/sda2             2099200 83886079 81786880   39G      8e Linux LVM

Диск /dev/mapper/rl-root: 36,95 GiB, 39673921536 байт, 77488128 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт

Диск /dev/mapper/rl-swap: 2,05 GiB, 2197815296 байт, 4292608 секторов
  
```

Рис. 16: Тип файловой системы

Далее показана последовательно монтирования файловых систем

```

aapetrova@localhost:~$ df -h /dev/mapper/rl-root
Диск /dev/mapper/rl-root: 36,95 GiB, 39673921536 байт, 77488128 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт

aapetrova@localhost:~$ df -h /dev/mapper/rl-swap
Диск /dev/mapper/rl-swap: 2,05 GiB, 2197815296 байт, 4292608 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт

aapetrova@localhost:~$ grep -i "mount"
^Z
[2]+  Остановлен      grep --color=auto -i "Mount"
aapetrova@localhost:~$ dmesg | grep -i "Mount"
[ 0.032225] Mount-cache hash table entries: 4096 (order: 3, 32768 bytes, linear)
[ 0.032225] Mountpoint-cache hash table entries: 4096 (order: 3, 32768 bytes, linear)
[ 3.767680] XFS (dm-0): Mounting V5 Filesystem 3ec9dd80-fb21-46d8-8544-934984c04f0f
[ 3.782693] XFS (dm-0): Ending clean mount
[ 4.677280] systemd[1]: Set up automount Arbitrary Executable File Formats File System Automount Point.
[ 4.705107] systemd[1]: Mounting Huge Pages File System...
[ 4.707523] systemd[1]: Mounting POSIX Message Queue File System...
[ 4.709647] systemd[1]: Mounting Kernel Debug File System...
[ 4.712255] systemd[1]: Mounting Kernel Trace File System...
[ 4.744699] systemd[1]: Starting Remount Root and Kernel File Systems...
[ 4.759529] systemd[1]: Mounted Huge Pages File System.
[ 4.760183] systemd[1]: Mounted POSIX Message Queue File System.
[ 4.760508] systemd[1]: Mounted Kernel Debug File System.
[ 4.760905] systemd[1]: Mounted Kernel Trace File System.
[ 6.444176] XFS (sdal): Mounting V5 Filesystem 20aebd12-4f92-4722-83ef-bcdd03f043dd
[ 6.612798] XFS (sdal): Ending clean mount
aapetrova@localhost:~$
  
```

Рис. 17: Последовательность монтирования файловых систем

Я приобрела практические навыки установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов.

...