

Лабораторнаят работа №1

Основы информационной безопасности

Оширова Юлия Николаевна

Содержание

1 Цель работы	5
2 Задание	6
3 Теоретическое введение	7
4 Выполнение лабораторной работы	8
5 Выводы	19
6 Контрольные вопросы	20
7 Список литературы	22

Список иллюстраций

4.1	Подготовка виртуальной машины	8
4.2	Подготовка виртуальной машины	9
4.3	Подготовка виртуальной машины	9
4.4	Подготовка виртуальной машины	10
4.5	Выбор языка	10
4.6	Разметка диска	11
4.7	Выбираем базовое окружение и группу	11
4.8	Отключаем	12
4.9	Installation destination	12
4.10	Создаем пароль	13
4.11	Задаем	13
4.12	Создаем пользователя	14
4.13	Лицензия	14
4.14	Установка завершилась	15
4.15	Подготовка виртуальной машины	15
4.16	Подготовка виртуальной машины	16
4.17	Команда dmesg	16
4.18	Версия ядра	17
4.19	Частота процессора, модель процессора и объем памяти	17
4.20	Гипервизор	18
4.21	Тип FS	18

Список таблиц

1 Цель работы

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

2 Задание

Установить дистрибутив Rocky. Выполнить домашнее задание. Сделать отчет и презентацию по данной лабораторной работе.

3 Теоретическое введение

Rocky Linux – это дистрибутив Linux, разработанный Rocky Enterprise Software Foundation. Предполагается, что это будет полный бинарно-совместимый выпуск, использующий исходный код операционной системы Red Hat Enterprise Linux.

4 Выполнение лабораторной работы

Подготовка виртуальной машины

Создадим виртуальную машину:

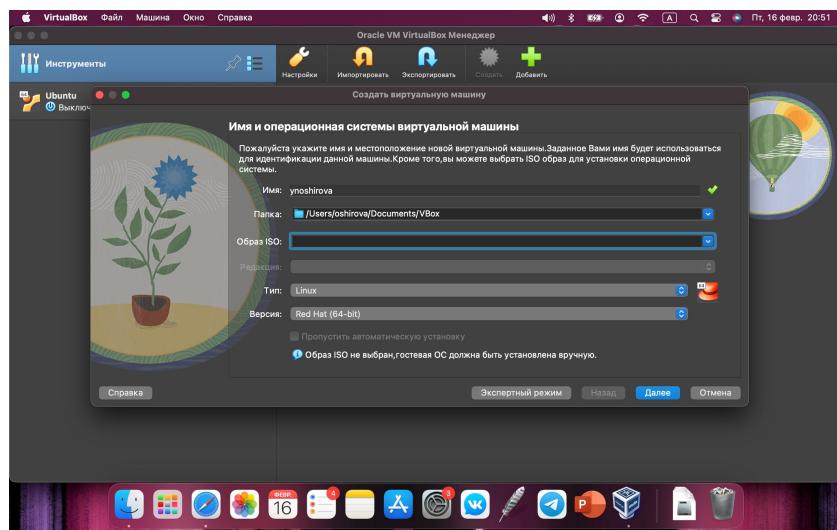


Рис. 4.1: Подготовка виртуальной машины

Добавим в нее раздел на 20 ГБ памяти, а также подключим iso образ инсталлятора Rocky Linux, а также установим виртуальный жесткий диск и т.д.:



Рис. 4.2: Подготовка виртуальный машины



Рис. 4.3: Подготовка виртуальный машины

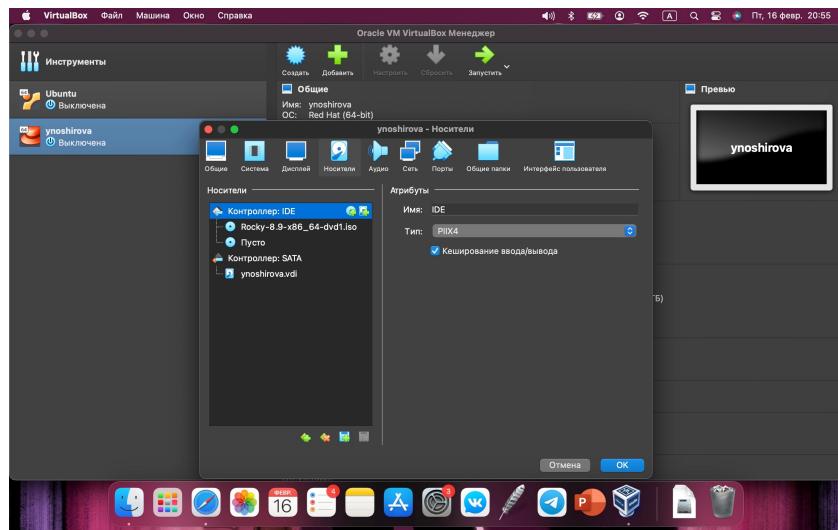


Рис. 4.4: Подготовка виртуальной машины

Запустим и перейдем к установке.

Установка Rocky Linux

Выбираем язык English и язык English (United States):

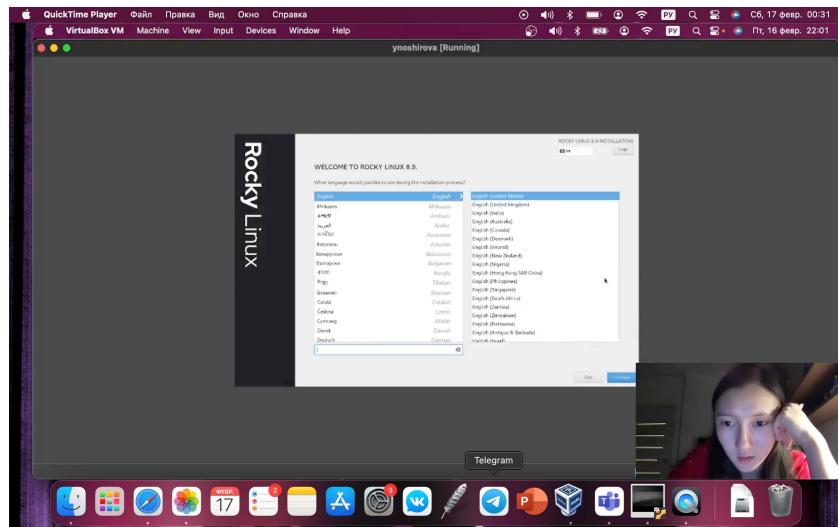


Рис. 4.5: Выбор языка

Выбираем автоматическую разметку диска:

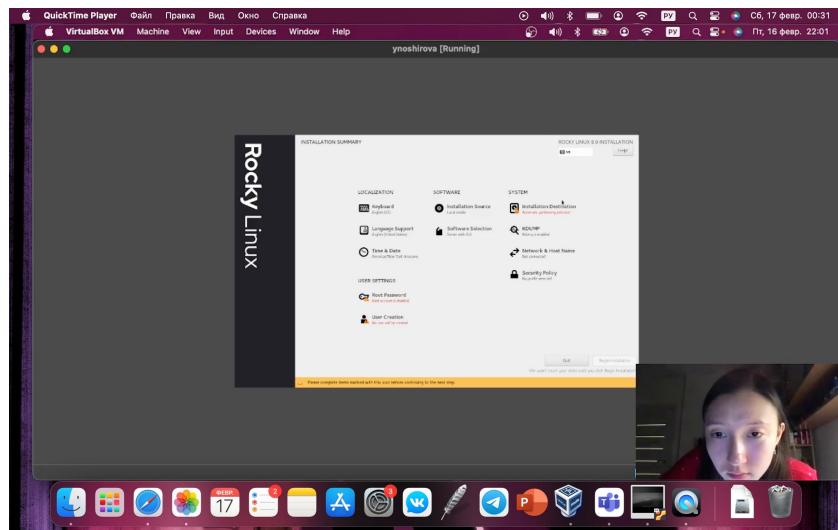


Рис. 4.6: Разметка диска

Добавляем нового пользователя, учитывая соглашение об именовании.
В предустановливаемом ПО выбираем базовое окружение “Сервер с GUI” и группу “Developments tool”:

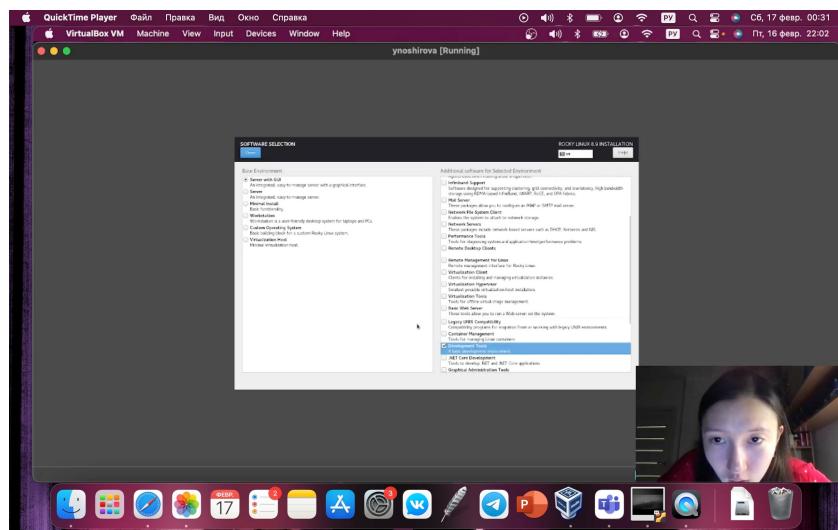


Рис. 4.7: Выбираем базовое окружение и группу

Отключаем kdump:

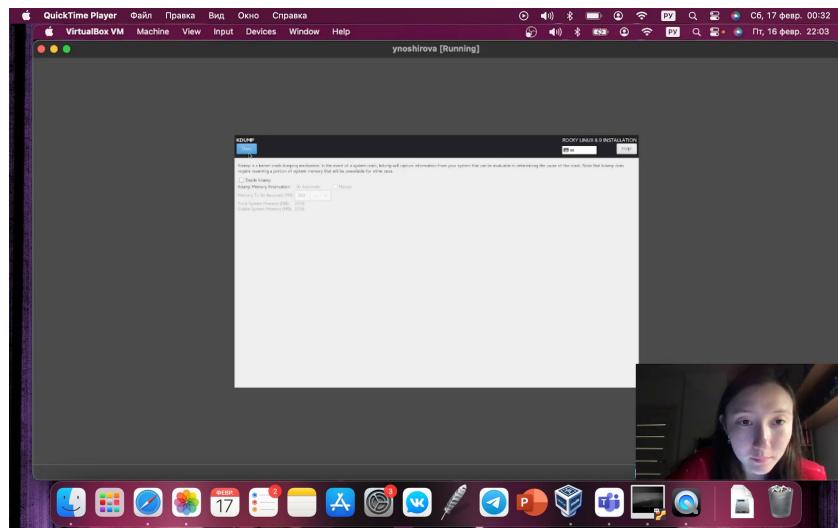


Рис. 4.8: Отключаем

Проверяем installation destination:

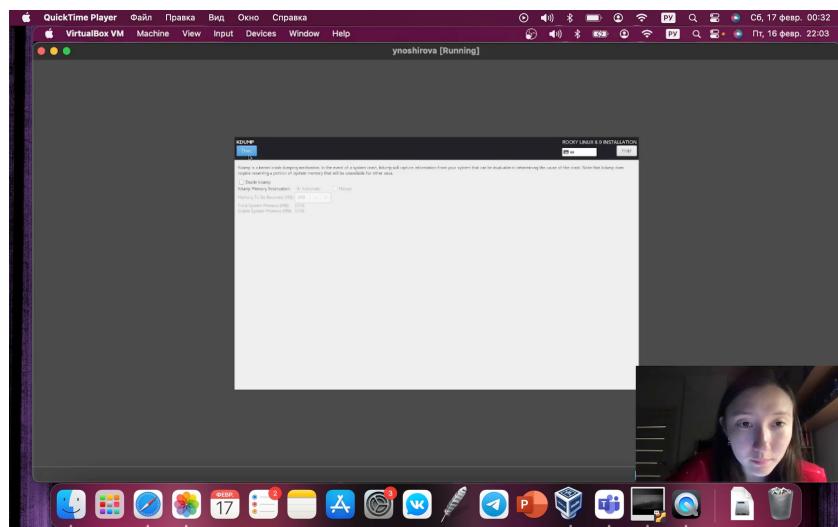


Рис. 4.9: Installation destination

Выставляем пароль для рута:

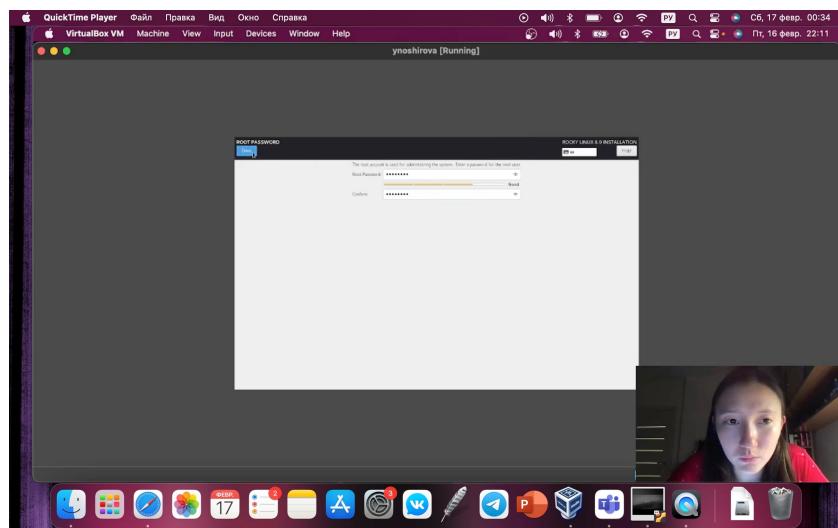


Рис. 4.10: Создаем пароль

Задаем hostname:

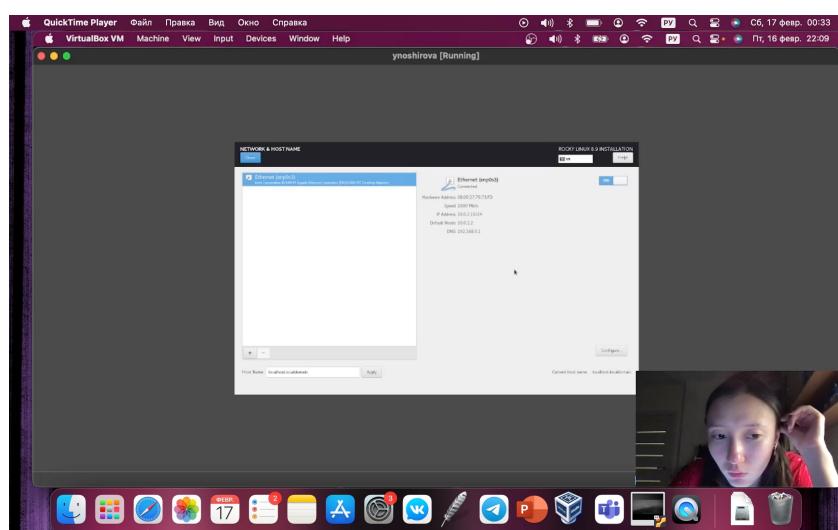


Рис. 4.11: Задаем

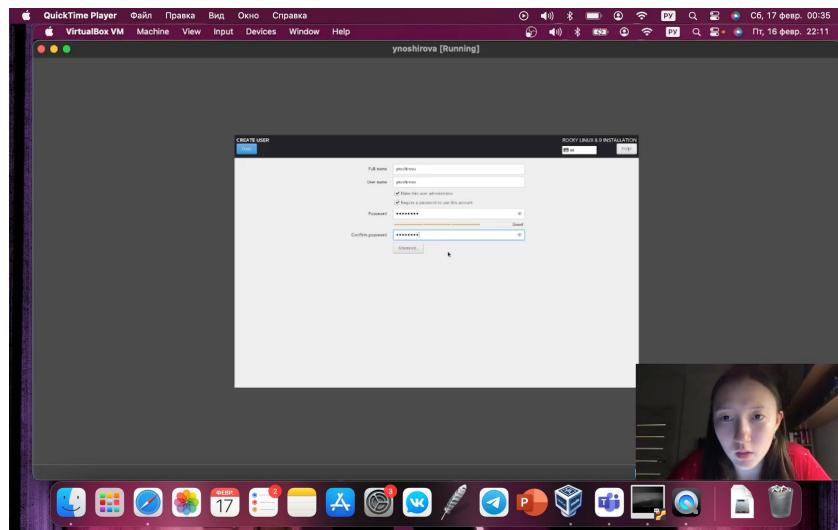


Рис. 4.12: Создаем пользователя

Принимаем лицензию:

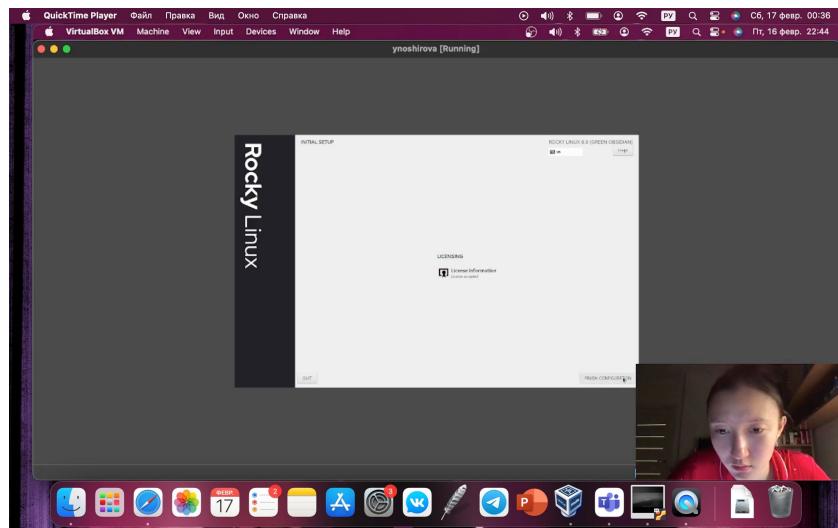


Рис. 4.13: Лицензия

Запускаем установку:

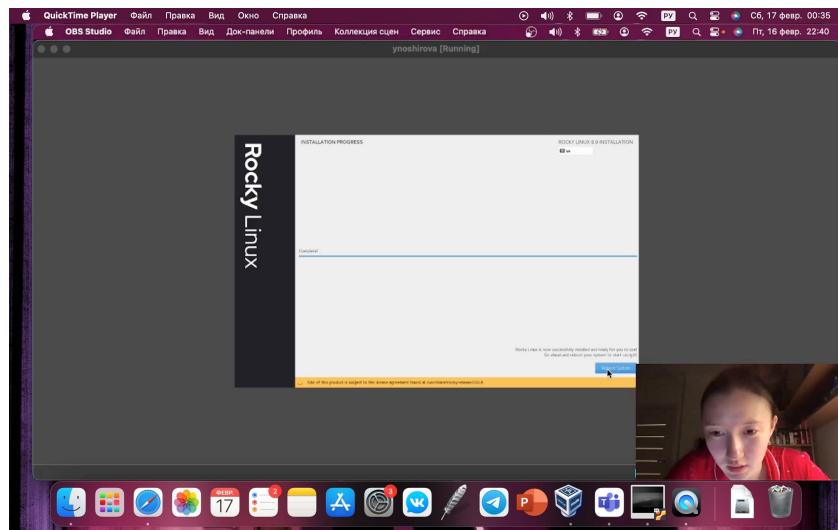


Рис. 4.14: Установка завершилась

Проверяем правильность установленного hostname и username (согласно соглашению об именовании).

Подключаем образ диска дополнений гостевой ОС:

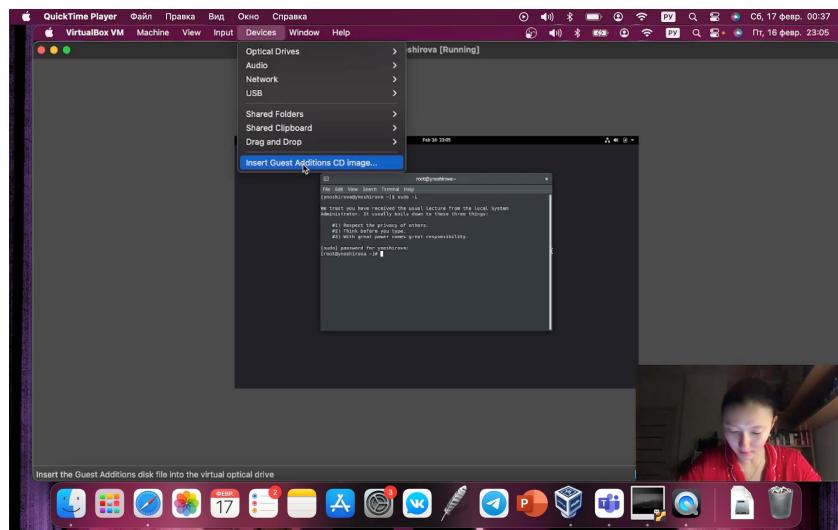


Рис. 4.15: Подготовка виртуальной машины

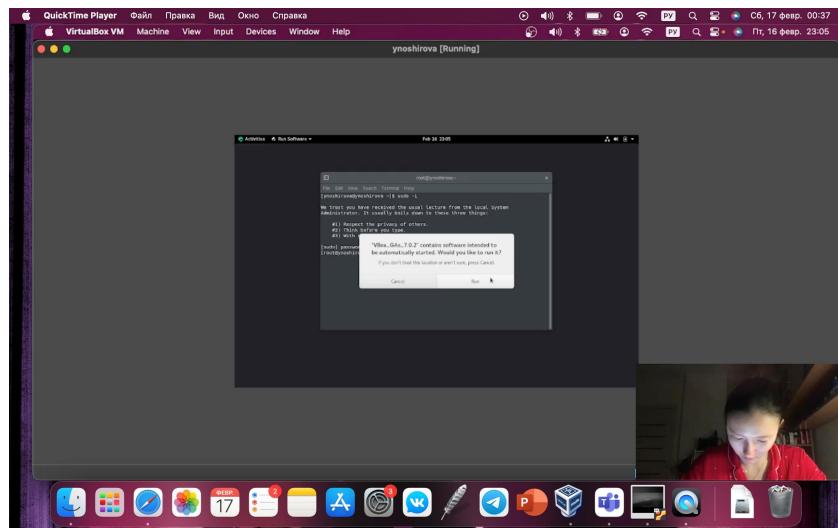


Рис. 4.16: Подготовка виртуальной машины

Домашнее задание

Команда dmesg:

```
[ynoshirova@ynoshirova ~]$ dmesg
[    0.000000] Linux version 4.18.0-513.5.1.el8_9.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc version 8.5.0 20210514 (Red Hat 8.5.0-20) (GCC)) #1 SMP Fri Nov 17 03:31:10 UTC 2023
[    0.000000] Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-4.18.0-513.5.1.el8_9.x86_64 root=/dev/mapper/rl-root ro resume=/dev/mapper/rl-swap rd.lvm.lv=rl/root rd.lvm.lv=rl/swap rhgb quiet
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[    0.000000] x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
[    0.000000] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
[    0.000000] signal: max sigframe size: 1776
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x80000000000000-0x800000000009fbff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000f8000-0x00000000000ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000010000-0x0000000007ffff] usable
[    0.000000] BIOS-e820: [mem 0x0000000007ffff000-0x0000000007fffffff] ACPI data
[    0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000ffffc0000-0x00000000ffffffff] reserved
```

Рис. 4.17: Команда dmesg

Версия ядра:

```

ynoshirova@ynoshirova:~ 
File Edit View Search Terminal Help
[ 18.757517] 20:33:54.289577 main      Executable: /opt/VBoxGuestAdditions-7.0.
2/sbin/VBoxService
[ 18.762960] 20:33:54.289579 main      Process ID: 1511
[ 18.762960] 20:33:54.289579 main      Package type: LINUX_64BITS_GENERIC
[ 18.777998] 20:33:54.310045 main      7.0.2 r154219 started. Verbose level = 0
[ 18.777998] 20:33:54.310045 main      vbglR3GuestCtrlDetectPeekGetCancelSuppor
t: Supported (#1)
[ 61.328714] ISO 9660 Extensions: Microsoft Joliet Level 3
[ 61.342789] ISO 9660 Extensions: Microsoft Joliet Level 3
[ 61.384316] ISO 9660 Extensions: RRIP_1991A
[ 61.386239] ISO 9660 Extensions: RRIP_1991A
[ynoshirova@ynoshirova ~]$ dmesg | grep -i "Linux version"
[ 0.000000] Linux version 4.18.0-513.5.1.el8_9.x86_64 (mockbuild@iad1-prod-bu
ild001.bld.equ.rockylinux.org) (gcc version 8.5.0 20210514 (Red Hat 8.5.0-20) (G
CC)) #1 SMP Fri Nov 17 03:31:10 UTC 2023
[ynoshirova@ynoshirova ~]$ dmesg | grep -i "processor"
[ 0.000000] tsc: Detected 1402.369 MHz processor
[ 0.107000] smpboot: Total of 1 processors activated (2804.73 BogoMIPS)
[ 0.108410] ACPI: Added _OSI(Processor Device)
[ 0.108411] ACPI: Added _OSI(Processor Aggregator Device)
[ynoshirova@ynoshirova ~]$ dmesg | grep -i "CPU0"
[ 0.106233] smpboot: CPU0: Intel(R) Core(TM) i5-8257U CPU @ 1.40GHz (family:
0x6, model: 0x8e, stepping: 0xa)
[ynoshirova@ynoshirova ~]$ dmesg | grep -i "memory"

```

Рис. 4.18: Версия ядра

Частота процессора модель процессора и объем памяти:

```

ynoshirova@ynoshirova:~ 
File Edit View Search Terminal Help
[ 0.000000] Linux version 4.18.0-513.5.1.el8_9.x86_64 (mockbuild@iad1-prod-bu
ild001.bld.equ.rockylinux.org) (gcc version 8.5.0 20210514 (Red Hat 8.5.0-20) (G
CC)) #1 SMP Fri Nov 17 03:31:10 UTC 2023
[ynoshirova@ynoshirova ~]$ dmesg | grep -i "processor"
[ 0.000000] tsc: Detected 1402.369 MHz processor
[ 0.107000] smpboot: Total of 1 processors activated (2804.73 BogoMIPS)
[ 0.108410] ACPI: Added _OSI(Processor Device)
[ 0.108411] ACPI: Added _OSI(Processor Aggregator Device)
[ynoshirova@ynoshirova ~]$ dmesg | grep -i "CPU0"
[ 0.106233] smpboot: CPU0: Intel(R) Core(TM) i5-8257U CPU @ 1.40GHz (family:
0x6, model: 0x8e, stepping: 0xa)
[ynoshirova@ynoshirova ~]$ dmesg | grep -i "memory"
[ 0.000000] ACPI: Reserving FACP table memory at [mem 0x7fff00f0-0x7fff01e3]
[ 0.000000] ACPI: Reserving DSDT table memory at [mem 0x7fff00f0-0x7fff2962]
[ 0.000000] ACPI: Reserving FACS table memory at [mem 0x7fff0200-0x7fff023f]
[ 0.000000] ACPI: Reserving FACS table memory at [mem 0x7fff0200-0x7fff023f]
[ 0.000000] ACPI: Reserving APIC table memory at [mem 0x7fff0240-0x7fff0293]
[ 0.000000] ACPI: Reserving SSDT table memory at [mem 0x7fff02a0-0x7fff060b]
[ 0.000000] Early memory node ranges
[ 0.000000] PM: Registered nosave memory: [mem 0x00000000-0x0000ffff]
[ 0.000000] PM: Registered nosave memory: [mem 0x0009f000-0x0009ffff]
[ 0.000000] PM: Registered nosave memory: [mem 0x000a0000-0x000effff]
[ 0.000000] PM: Registered nosave memory: [mem 0x000f0000-0x000fffff]
[ 0.000000] Memory: 232448K/2096696K available (14341 kernel code, 5952K rwd)

```

Рис. 4.19: Частота процессора, модель процессора и объем памяти

Гипервизор:

```

ynoshirova@ynoshirova:~$ dmesg | grep -i "hypervisor"
[    0.000000] Hypervisor detected: KVM
[    0.003061] SRBDS: Unknown: Dependent on hypervisor status
[    0.003063] GDS: Unknown: Dependent on hypervisor status
[ynoshirova@ynoshirova ~]$ dmesg | grep -i "VFS: Mounted root"
[ynoshirova@ynoshirova ~]$ df -T
Filesystem      Type      1K-blocks      Used   Available  Use%  Mounted on
devtmpfs        devtmpfs     973400         0    973400   0% /dev
tmpfs           tmpfs       1002812        0   1002812   0% /dev/shm
tmpfs           tmpfs       1002812       9448   993364   1% /run
tmpfs           tmpfs       1002812        0   1002812   0% /sys/fs/cgroup
/dev/mapper/rl-root xfs       38749712 7009456  31740256 19% /
/dev/sd1         xfs       1038336 250088  788256 25% /boot
tmpfs           tmpfs       200560        24   200536   1% /run/user/1000
/dev/sr0         iso9660     51716       51716        0 100% /run/media/ynoshir
ova/VBox_GAs_7.0.21
/ova/VBox_GAs_7.0.2
[ynoshirova@ynoshirova ~]$ dmesg | grep -i "Mounted"
[ynoshirova@ynoshirova ~]$ dmesg |

```

Рис. 4.20: Гипервизор

Тип FS и последовательность монтирования:

```

ynoshirova@ynoshirova:~$ dmesg | grep -i "Mounted"
[ynoshirova@ynoshirova ~]$ dmesg | grep -i "mount"
[    0.003000] Mount-cache hash table entries: 4096 (order: 3, 32768 bytes, vmalloc)
[    0.003000] Mountpoint-cache hash table entries: 4096 (order: 3, 32768 bytes, vmalloc)
[    4.147668] XFS (dm-0): Mounting V5 Filesystem
[    7.813021] XFS (sd1): Mounting V5 Filesystem
[ynoshirova@ynoshirova ~]$ dmesg | grep -i "mounted"
[ynoshirova@ynoshirova ~]$ mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime,seclabel)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
devtmpfs on /dev type devtmpfs (rw,nosuid,seclabel,size=973400k,nr_inodes=243350,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,seclabel)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,seclabel,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,seclabel,mode=755)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,seclabel,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,xattr,release_agent=/usr/lib/systemd/systemd-cgroups-agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime,seclabel)

```

Рис. 4.21: Тип FS

5 Выводы

В ходе данной лабораторной работы мы ознакомились и установили новый дистрибутив Rocky. Выполнили домашнее задание с командой «dmesg».

6 Контрольные вопросы

1. Учётная запись, как правило, содержит сведения, необходимые для опознания пользователя при подключении к системе, сведения для авторизации и учёта. Это идентификатор пользователя (login) и его пароль. Пароль или его аналог, как правило, хранится в зашифрованном или хэшированном виде для обеспечения его безопасности.
2. manual (man) — для получения полной справочной информации по другой команде.

Для перемещения и переименования файлов и каталогов используется команда mv (move).

Для просмотра содержимого каталога используется команда ls.

Для просмотра размеров папок на диске используется команда du.

Touch — создать файл.

Для удаления директорий используется команда rmdir имя_директории.

Команда rm применяется для удаления ненужных файлов.

Команда chmod (change mode – сменить режим) предназначена для изменения прав доступа к файлам.

Достаточно выполнить команду history, для просмотра истории команд.

3. Файловая система — это структура, используемая операционной системой для организации и управления файлами на устройстве хранения, например на жестком диске, твердотельном накопителе (SSD) или USB-накопителе.

4. Команда `findmnt` – это простая утилита командной строки, используемая для отображения списка смонтированных файловых систем или поиска файловой системы в `/etc/fstab`, `/etc/mtab` и `/proc/self/mountinfo`.
5. Один из способов «убить», запущенное приложение или процесс в Linux, это использование таких команд, как `kill` или `killall`.

7 Список литературы

Что такое Роки?