

Отчёт по лабораторной работе №1

Дисциплина: Основы информационной безопасности

Ганина Таисия Сергеевна, НКАбд-01-22

Содержание

1 Цель работы	5
2 Задание	6
3 Теоретическое введение	7
3.1 Rocky Linux	7
3.2 VirtualBox	7
4 Выполнение лабораторной работы	9
5 Выводы	21
6 Контрольные вопросы	22
Список литературы	24

Список иллюстраций

4.1	VirtualBox	9
4.2	Загружаю образ Rocky DVD	9
4.3	Создание виртуальной машины, имя и операционная система . . .	10
4.4	Оборудование: 2048МБ памяти и 6 процессоров	10
4.5	Виртуальный жесткий диск	10
4.6	Загружаю образ	11
4.7	Итог	11
4.8	Установка языка	12
4.9	Место установки	12
4.10	Выбор программ	13
4.11	Отключение KDUMP	13
4.12	Сеть и имя узла	14
4.13	Пароль	14
4.14	Создание пользователя	15
4.15	Дата и время	15
4.16	Установка	16
4.17	Итог	16
4.18	dmesg less	17
4.19	Версия Линукс	17
4.20	Частота процессора	18
4.21	Модель процессора	18
4.22	Объем доступной оперативной памяти	19
4.23	Тип обнаруженного гипервизора	19
4.24	Тип файловой системы корневого раздела.	19
4.25	Последовательность монтирования файловых систем	20

Список таблиц

1 Цель работы

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

2 Задание

1. Создать новую виртуальную машину. Загрузить образ.
2. Установить операционную систему и произвести первичные настройки.
3. Домашнее задание.
4. Контрольные вопросы.

3 Теоретическое введение

3.1 Rocky Linux

Rocky Linux — дистрибутив Linux, разработанный Rocky Enterprise Software Foundation. Предполагается, что это будет полный бинарно-совместимый выпуск, использующий исходный код операционной системы Red Hat Enterprise Linux (RHEL). Цель проекта — предоставить корпоративную операционную систему производственного уровня, поддерживаемую сообществом. Rocky Linux, наряду с Red Hat Enterprise Linux и SUSE Linux Enterprise, стала популярной для использования в корпоративных операционных системах.

Первая версия-кандидат на выпуск Rocky Linux была выпущена 30 апреля 2021 г., а ее первая общедоступная версия была выпущена 21 июня 2021 г. Rocky Linux 8 будет поддерживаться до мая 2029 г.

3.2 VirtualBox

VirtualBox (Oracle VM VirtualBox) — программный продукт виртуализации для операционных систем Windows, Linux, FreeBSD, macOS, Solaris/OpenSolaris, ReactOS, DOS и других.

Программа была создана компанией Innotek с использованием исходного кода QEMU. Первая публично доступная версия VirtualBox появилась 15 января 2007 года. В феврале 2008 года Innotek был приобретён компанией Sun Microsystems, модель распространения VirtualBox при этом не изменилась. В январе 2010 года

Sun Microsystems была поглощена корпорацией Oracle, модель распространения осталась прежней.

4 Выполнение лабораторной работы

1. Я произвела настройку новой виртуальной машины (рис. 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7).



Рис. 4.1: VirtualBox

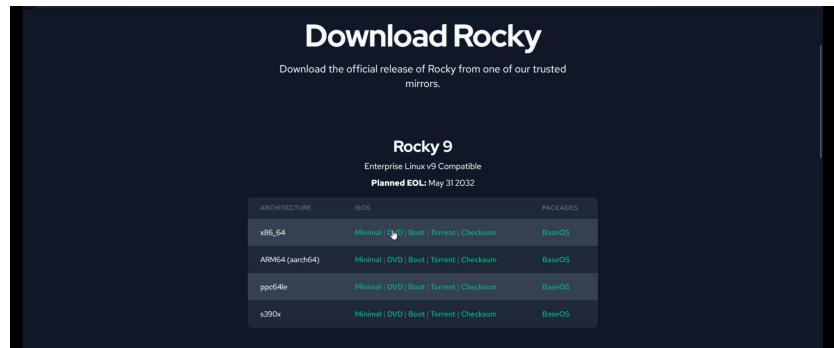


Рис. 4.2: Загружаю образ Rocky DVD

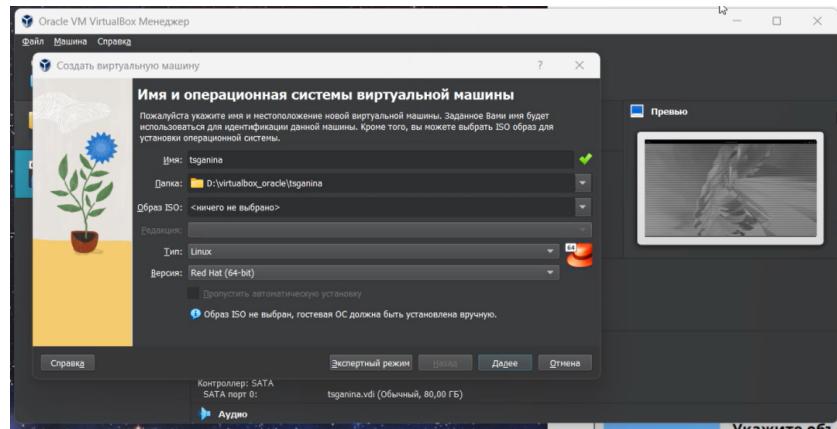


Рис. 4.3: Создание виртуальной машины, имя и операционная система

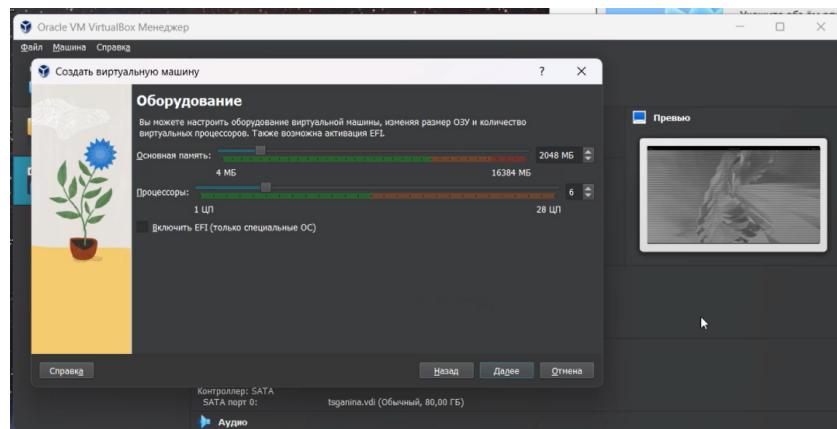


Рис. 4.4: Оборудование: 2048МБ памяти и 6 процессоров

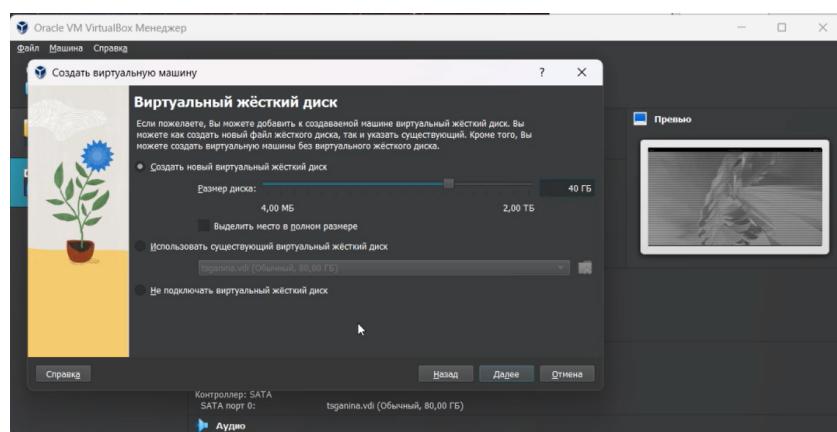


Рис. 4.5: Виртуальный жесткий диск

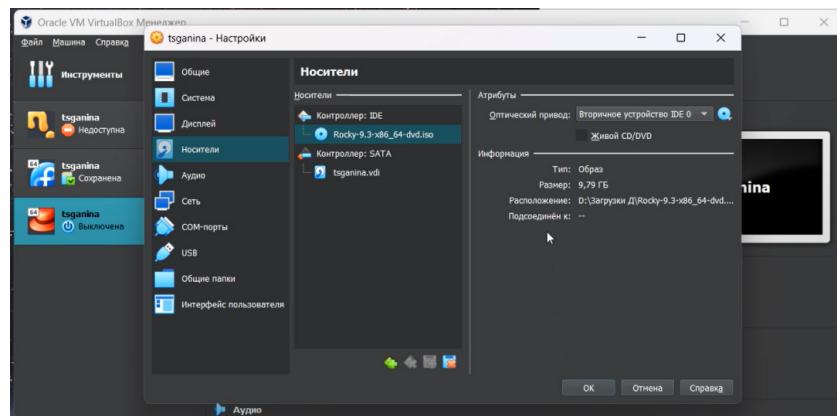


Рис. 4.6: Загружаю образ

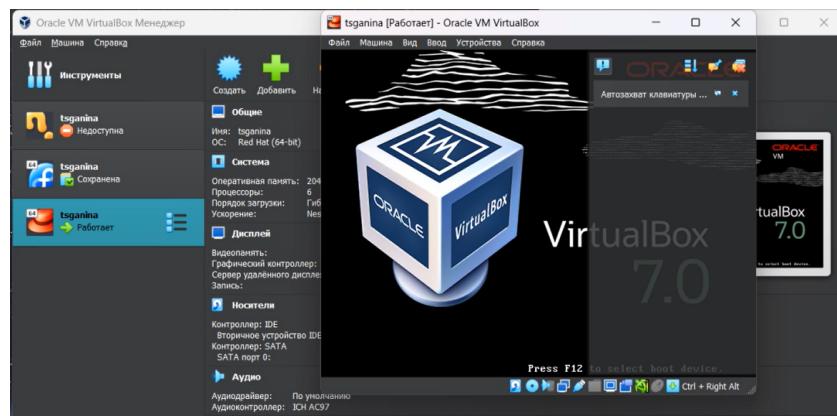


Рис. 4.7: Итог

2. Настройка системы (рис. 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 4.17).

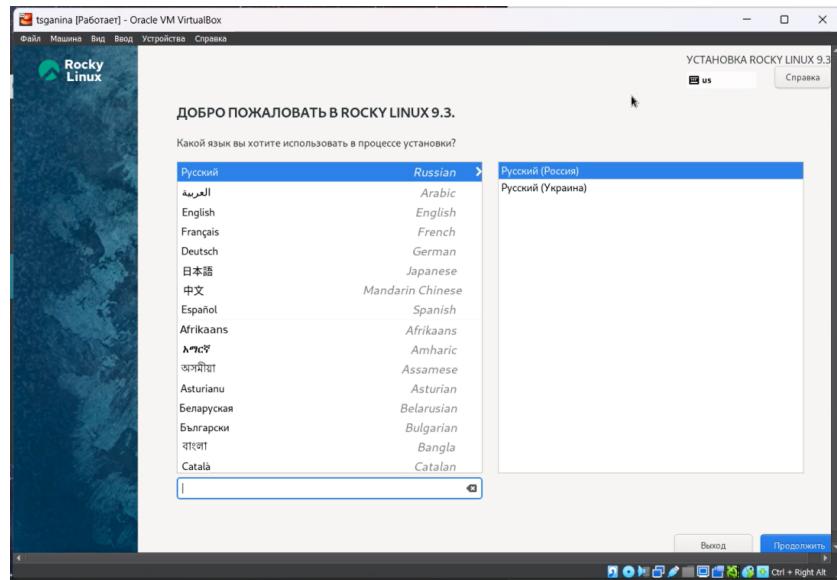


Рис. 4.8: Установка языка

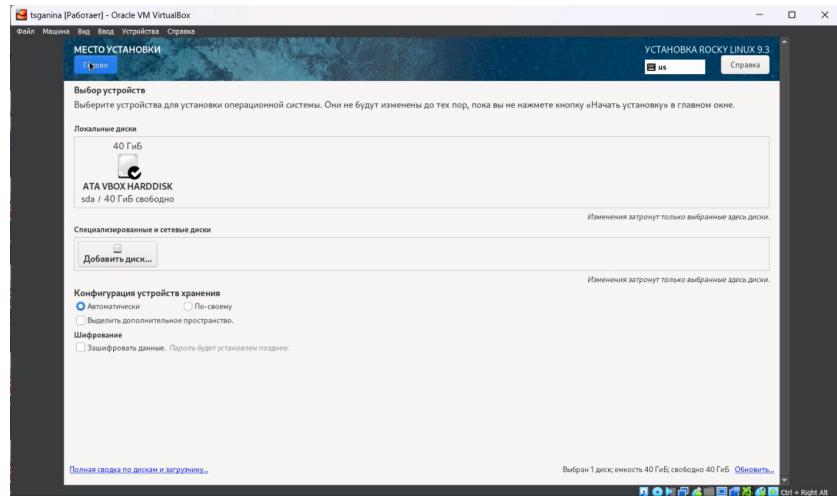


Рис. 4.9: Место установки

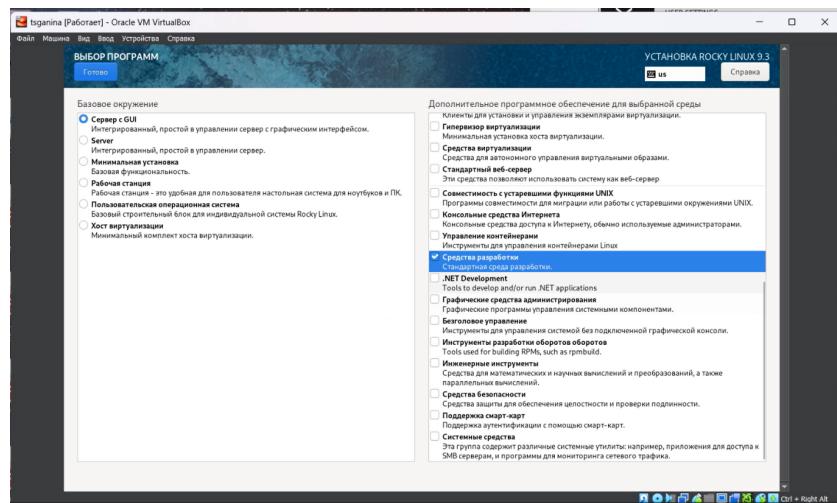


Рис. 4.10: Выбор программ

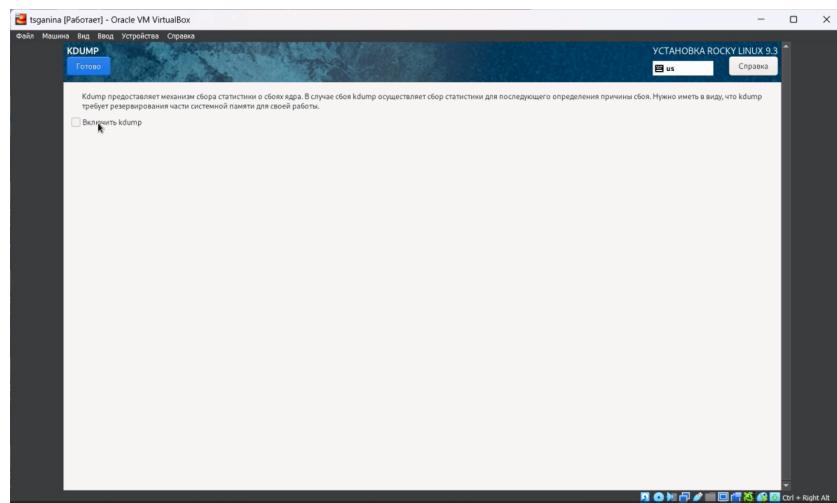


Рис. 4.11: Отключение KDUMP

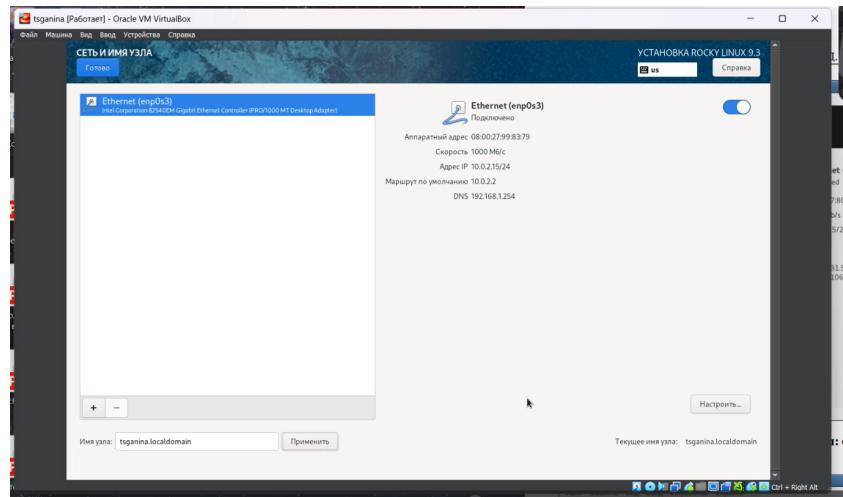


Рис. 4.12: Сеть и имя узла

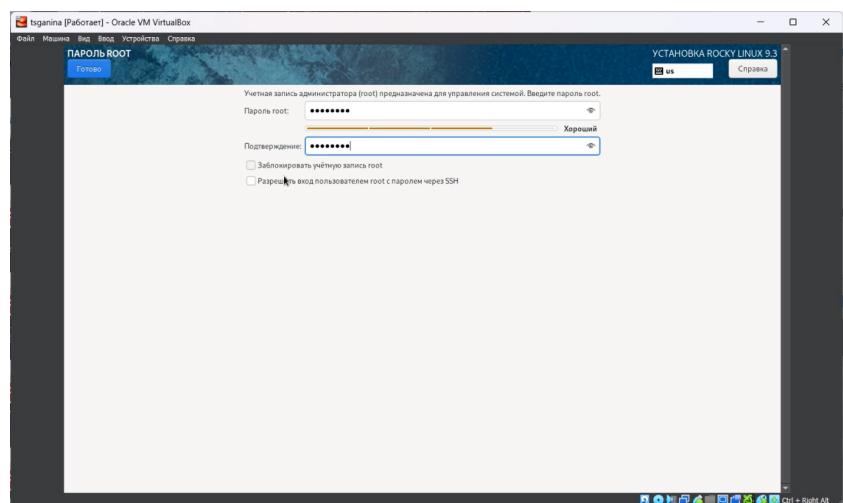


Рис. 4.13: Пароль

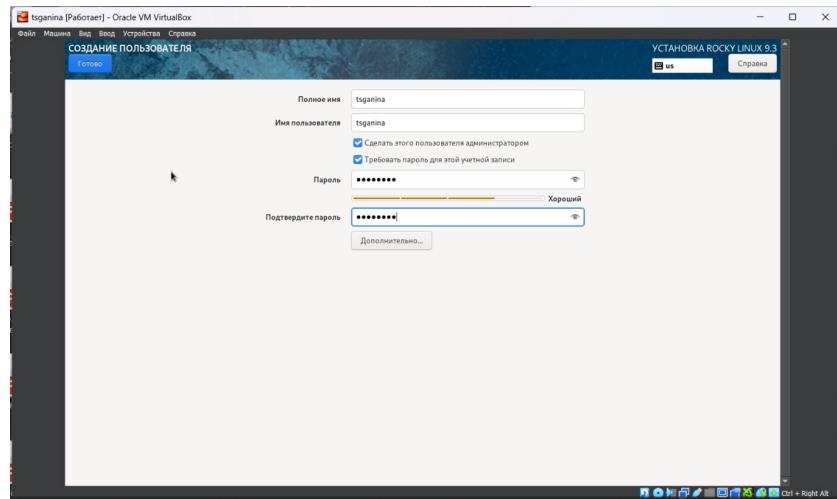


Рис. 4.14: Создание пользователя

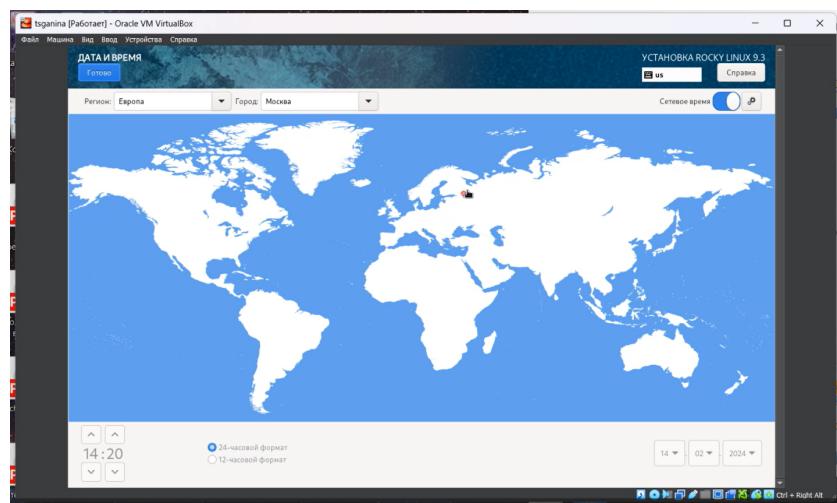


Рис. 4.15: Дата и время

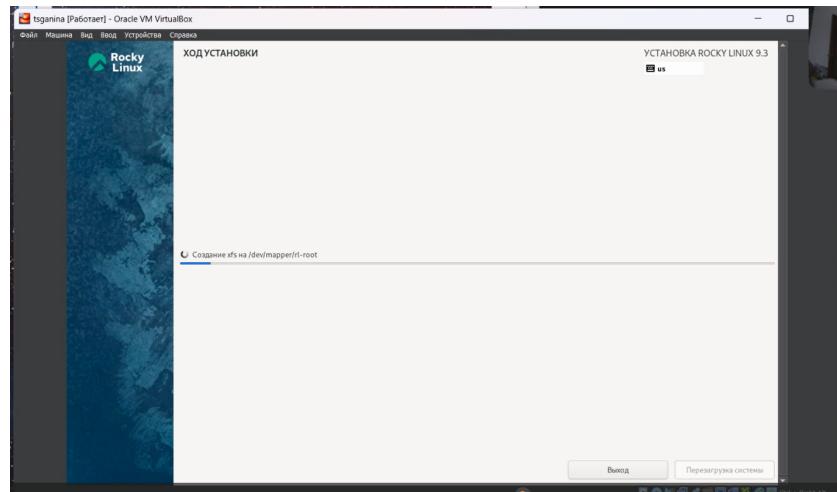


Рис. 4.16: Установка

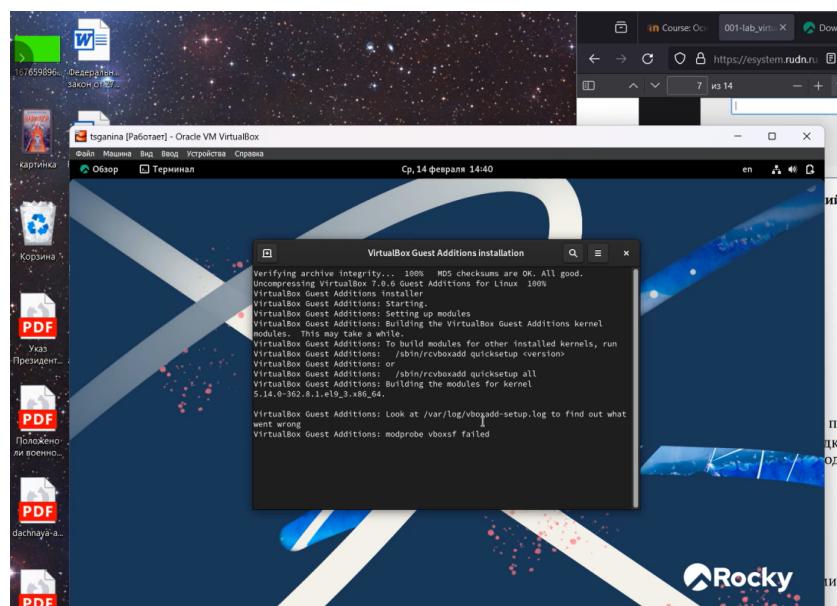


Рис. 4.17: Итог

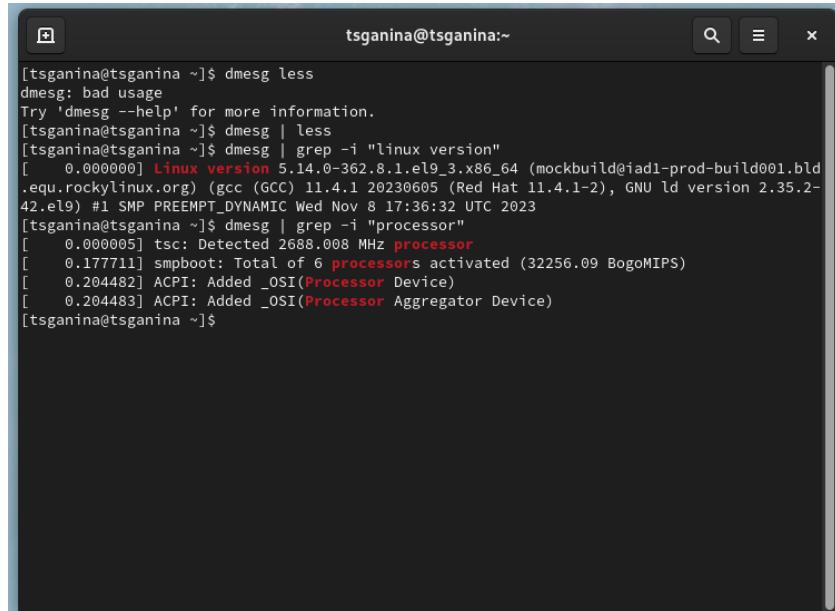
3. Задания (рис. 4.18, 4.19, 4.20, 4.21, 4.22, 4.23, 4.24, 4.25).

```
tsganina@tsganina:~ — less
[    0.00000] Linux version 5.14.0-362.8.1.el9_3.x86_64 (mockbuild@iad1-prod-build001.bld
.equ.rockylinux.org) (gcc (GCC) 11.4.1 20230605 (Red Hat 11.4.1-2), GNU ld version 2.35.2-
42.el9) #1 SMP PREEMPT_DYNAMIC Wed Nov 8 17:36:32 UTC 2023
[    0.00000] The list of certified hardware and cloud instances for Enterprise Linux 9 c
an be viewed at the Red Hat Ecosystem Catalog, https://catalog.redhat.com.
[    0.00000] Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-362.8.1.el9_3.x86_64 r
oot=/dev/mapper/rl-root ro resume=/dev/mapper/rl-swap rd.lvm.lv=rl/root rd.lvm.lv=rl/swap
rhgb quiet
[    0.00000] x86/fpu: x87 FPU will use FXSAVE
[    0.00000] signal: max sigframe size: 1440
[    0.00000] BIOS-provided physical RAM map:
[    0.00000] BIOS-e820: [mem 0x0000000000000000-0x00000000009fbfff] usable
[    0.00000] BIOS-e820: [mem 0x0000000000009fc00-0x00000000009ffff] reserved
[    0.00000] BIOS-e820: [mem 0x0000000000f0000-0x0000000000ffff] reserved
[    0.00000] BIOS-e820: [mem 0x000000000100000-0x0000000007ffff] usable
[    0.00000] BIOS-e820: [mem 0x0000000007fff0000-0x0000000007ffff] ACPI data
[    0.00000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
[    0.00000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] reserved
[    0.00000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[    0.00000] NX (Execute Disable) protection: active
[    0.00000] SMBIOS 2.5 present.
[    0.00000] DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[    0.00000] Hypervisor detected: KVM
[    0.00000] kvm-clock: Using msrs 4b564d01 and 4b564d00
[    0.00001] kvm-clock: using sched offset of 4963943879107 cycles
[    0.00003] clocksource: kvm-clock: mask: 0xfffffffffffffff max_cycles: 0x1cd42e4dfffb,
max_idle_ns: 881590591483 ns
[    0.00005] tsc: Detected 2688.008 MHz processor
:|
```

Рис. 4.18: dmesg | less

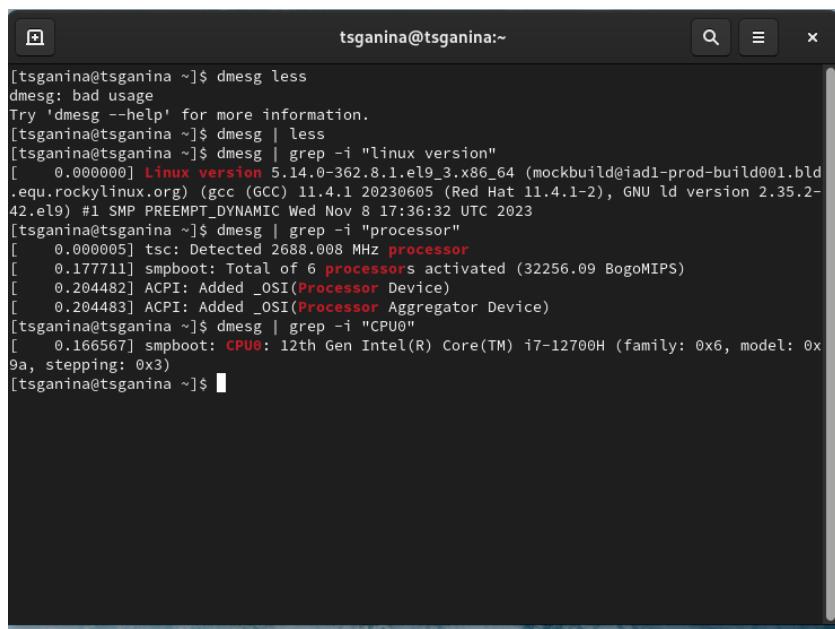
```
[tsganina@tsganina ~]$ dmesg less
dmesg: bad usage
Try 'dmesg --help' for more information.
[tsganina@tsganina ~]$ dmesg | less
[tsganina@tsganina ~]$ dmesg | grep -i "linux version"
[    0.00000] Linux version 5.14.0-362.8.1.el9_3.x86_64 (mockbuild@iad1-prod-build001.bld
.equ.rockylinux.org) (gcc (GCC) 11.4.1 20230605 (Red Hat 11.4.1-2), GNU ld version 2.35.2-
42.el9) #1 SMP PREEMPT_DYNAMIC Wed Nov 8 17:36:32 UTC 2023
[tsganina@tsganina ~]$
```

Рис. 4.19: Версия Линукс



```
[tsganina@tsganina ~]$ dmesg less
dmesg: bad usage
Try 'dmesg --help' for more information.
[tsganina@tsganina ~]$ dmesg | less
[tsganina@tsganina ~]$ dmesg | grep -i "linux version"
[ 0.000000] Linux version 5.14.0-362.8.1.el9_3.x86_64 (mockbuild@iad1-prod-build001.bld
.equ.rockylinux.org) (gcc (GCC) 11.4.1 20230605 (Red Hat 11.4.1-2), GNU ld version 2.35.2-
42.el9) #1 SMP PREEMPT_DYNAMIC Wed Nov 8 17:36:32 UTC 2023
[tsganina@tsganina ~]$ dmesg | grep -i "processor"
[ 0.000005] tsc: Detected 2688.008 MHz processor
[ 0.177711] smpboot: Total of 6 processors activated (32256.09 BogoMIPS)
[ 0.204482] ACPI: Added _OSI(Processor Device)
[ 0.204483] ACPI: Added _OSI(Processor Aggregator Device)
[tsganina@tsganina ~]$
```

Рис. 4.20: Частота процессора



```
[tsganina@tsganina ~]$ dmesg less
dmesg: bad usage
Try 'dmesg --help' for more information.
[tsganina@tsganina ~]$ dmesg | less
[tsganina@tsganina ~]$ dmesg | grep -i "linux version"
[ 0.000000] Linux version 5.14.0-362.8.1.el9_3.x86_64 (mockbuild@iad1-prod-build001.bld
.equ.rockylinux.org) (gcc (GCC) 11.4.1 20230605 (Red Hat 11.4.1-2), GNU ld version 2.35.2-
42.el9) #1 SMP PREEMPT_DYNAMIC Wed Nov 8 17:36:32 UTC 2023
[tsganina@tsganina ~]$ dmesg | grep -i "processor"
[ 0.000005] tsc: Detected 2688.008 MHz processor
[ 0.177711] smpboot: Total of 6 processors activated (32256.09 BogoMIPS)
[ 0.204482] ACPI: Added _OSI(Processor Device)
[ 0.204483] ACPI: Added _OSI(Processor Aggregator Device)
[tsganina@tsganina ~]$ dmesg | grep -i "CPU0"
[ 0.166567] smpboot: CPU0: 12th Gen Intel(R) Core(TM) i7-12700H (family: 0x6, model: 0x
9a, stepping: 0x3)
[tsganina@tsganina ~]$
```

Рис. 4.21: Модель процессора

```
[tsganina@tsganina ~]$ dmesg | grep -i "Memory:"\n[    0.003210] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x0000ffff]\n[    0.003211] PM: hibernation: Registered nosave memory: [mem 0x0009f000-0x0009ffff]\n[    0.003212] PM: hibernation: Registered nosave memory: [mem 0x000a0000-0x000effff]\n[    0.003212] PM: hibernation: Registered nosave memory: [mem 0x000f0000-0x000fffff]\n[    0.008978] Memory: 260860K/2096696K available (16384K kernel code, 5596K rwdata, 11444\nK rodata, 3824K init, 18424K bss, 159156K reserved, 0K cma-reserved)\n[    0.066836] Freeing SMP alternatives memory: 36K\n[    0.837878] Freeing initrd memory: 57356K\n[   1.506188] Freeing unused decrypted memory: 2036K\n[   1.507112] Freeing unused kernel image (initmem) memory: 3824K\n[   1.525581] Freeing unused kernel image (rodata/data gap) memory: 844K\n[tsganina@tsganina ~]$
```

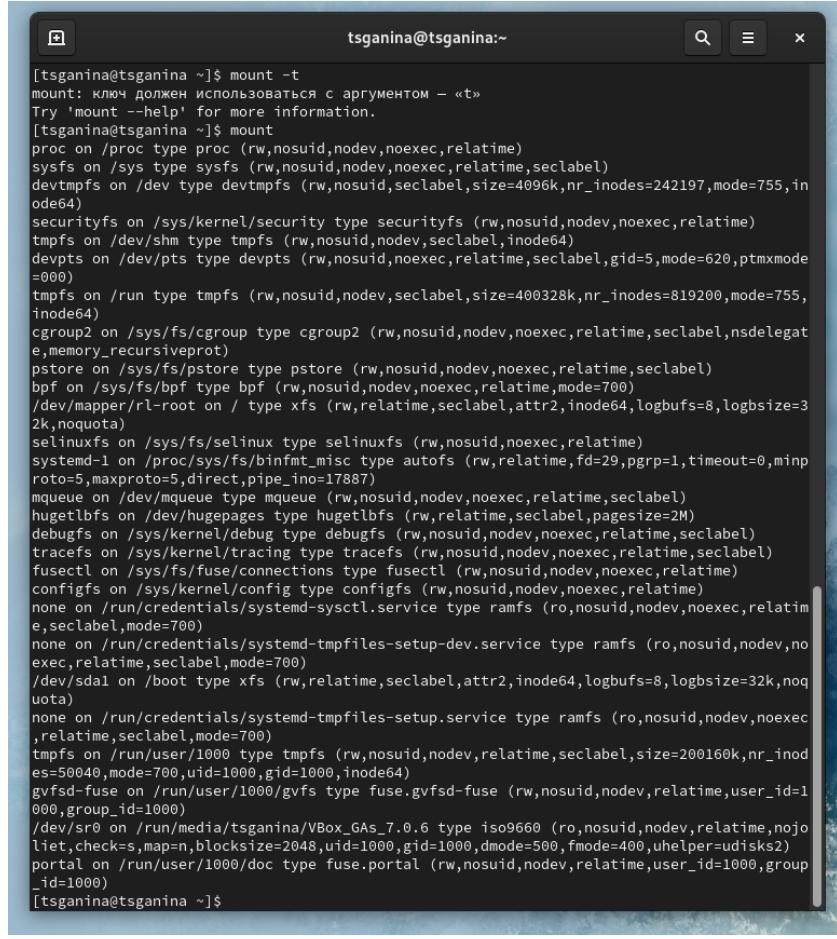
Рис. 4.22: Объем доступной оперативной памяти

```
[tsganina@tsganina ~]$ dmesg | grep -i "Hypervisor detected"\n[    0.000000] Hypervisor detected: KVM\n[tsganina@tsganina ~]$
```

Рис. 4.23: Тип обнаруженного гипервизора

```
[tsganina@tsganina ~]$ df -T\nФайловая система    Тип      1К-блоков Использовано Доступно Использовано% Смонтировано в\n/devtmpfs        devtmpfs     4096       0    4096       0% /dev\ntmpfs           tmpfs      1000816    0  1000816       0% /dev/shm\ntmpfs           tmpfs      400328    6244  394084       2% /run\n/dev/mapper/rl-root xfs  38690816  15269964  23420852      40% /\n/dev/sda1         xfs      983040  274924  708116      28% /boot\ntmpfs           tmpfs      200160     108  200052       1% /run/user/1000\n/dev/sr0          iso9660   51806      51806       0    100% /run/media/tsga\nnina/VBox_GAs_7.0.6\n[tsganina@tsganina ~]$
```

Рис. 4.24: Тип файловой системы корневого раздела.



```
[tsganina@tsganina ~]$ mount -t
mount: ключ должен использоваться с аргументом - «t»
Try 'mount --help' for more information.
[tsganina@tsganina ~]$ mount
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime,seclabel)
devtmpfs on /dev type devtmpfs (rw,nosuid,seclabel,size=4096k,nr_inodes=242197,mode=755,inode64)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,seclabel,inode64)
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,size=400328k,nr_inodes=819200,mode=755,inode64)
cgroup2 on /sys/fs/cgroup type cgroup2 (rw,nosuid,nodev,noexec,relatime,seclabel,nsdelegate,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime,seclabel)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
/dev/mapper/r1-root on / type xfs (rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
selinuxfs on /sys/fs/selinux type selinuxfs (rw,nosuid,noexec,relatime)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=29,pgroup=1,timeo
```

Рис. 4.25: Последовательность монтирования файловых систем

5 Выводы

Был установлен дистрибутив Rocky.

6 Контрольные вопросы

1. Какую информацию содержит учётная запись пользователя?

Учетная запись пользователя содержит информацию по авторизации - учётные данные. Это идентификатор для подключения к системе. То есть, это:

- Системное имя - должно быть уникальным, содержит только латинские знаки.
- Уникальных идентификатор пользователя в системе, содержит число.
- Полное имя - ФИО пользователя.

2. Укажите команды терминала и приведите примеры:

- для получения справки по команде = `-help`;
- для перемещения по файловой системе = `cd`;
- для просмотра содержимого каталога = `ls`;
- для определения объёма каталога = `du + имя каталога`;
- для создания / удаления каталогов = `mkdir/rmdir`;
- для создания / удаления файлов = `touch/rm`;
- для задания определённых прав на файл / каталог = `chmod`;
- для просмотра истории команд = `history`;

3. Что такое файловая система? Приведите примеры с краткой характеристикой.

Это способ хранения, организации и именования данных на различных носителях.

Примеры: - FAT32 - файловая система, в которой пространство разделено на три части: область служебных структур, указатели в виде таблиц и область хранения файлов; - ext4 - система, которая используется в основном в ОС на Linux. Журналируемая файловая система, в последней версии максимальный размер файла - 16Гб.

4. Как посмотреть, какие файловые системы подмонтированы в ОС?

Для этого нужно ввести в терминал команду df - это покажет список всех файловых систем по номерам устройств, размеры и данные о памяти. Но при этом можно посмотреть в свойствах папок все эти данные вручную.

5. Как удалить зависший процесс?

- killall - остановит все процессы, которые есть в данный момент.
- kill + id-процесса. Это поможет удалить один конкретный процесс. (Чтобы узнать id нужно написать в терминале команду ps).

Список литературы

1. Руководство к лабораторной работе