

Лабораторная работа №1

Информационная безопасность

александрова Ульяна Вадимовна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
5	Домашнее задание	14
6	Контрольные вопросы	17
7	Выводы	18

Список иллюстраций

4.1	Оборудование	8
4.2	Виртуальный жесткий диск	9
4.3	Подключение образа	9
4.4	Настройки языка	10
4.5	Сводка установки	10
4.6	Скачивание	11
4.7	Подключение гостевой ОС	11
4.8	Процесс загрузки в терминале	12
4.9	dmesg	12
4.10	dmesg less	13
5.1	Версия ядра Linux	14
5.2	Частота процессора	14
5.3	Модель процессора	15
5.4	Тип обнаруженного гипервизора	15
5.5	Тип файловой системы	15
5.6	Последовательность монтирования файловых систем	16

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

1. Скачать необходимое ПО (Virtual Box, Rocky);
2. Настроить опции в соответствии с требованиями;
3. Выполнить домашнее задание.

3 Теоретическое введение

Лабораторная работа подразумевает установку на виртуальную машину VirtualBox (<https://www.virtualbox.org/>) операционной системы Linux (дистрибутив Rocky (<https://rockylinux.org/>)).

4 Выполнение лабораторной работы

Поскольку у меня уже имелся Virtual Box, я перехожу к скачиванию образа ISO и одновременно с этим начинаю создание виртуальной системы. Даю машине имя и при этом не загружаю сразу образ ISO (это лучше сделать после первоначальной настройки). В разделе “Оборудование” выставляю основной памяти 2048Мб (рис. 4.1).

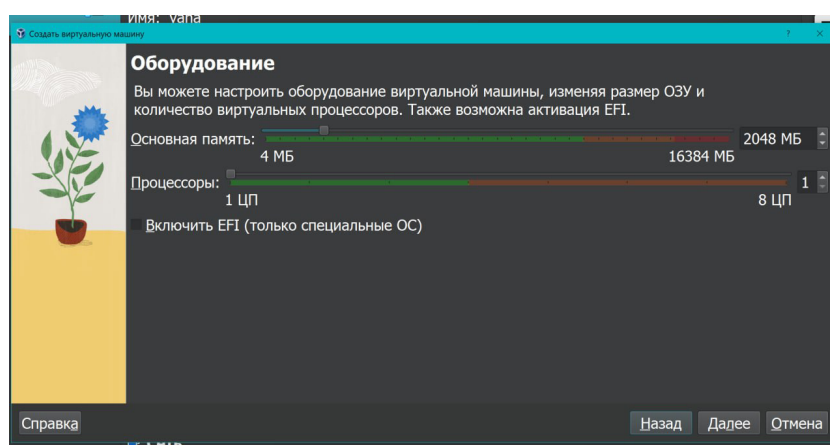


Рис. 4.1: Оборудование

В Разделе “Виртуальный жесткий диск” создаю новый виртуальный диск объемом в 40 ГБ. После этого захожу в настройки виртуальной машины, раздел “Носители” и подключаю скачанный ранее виртуальный образ Роки (рис. 4.2), (рис. 4.3).

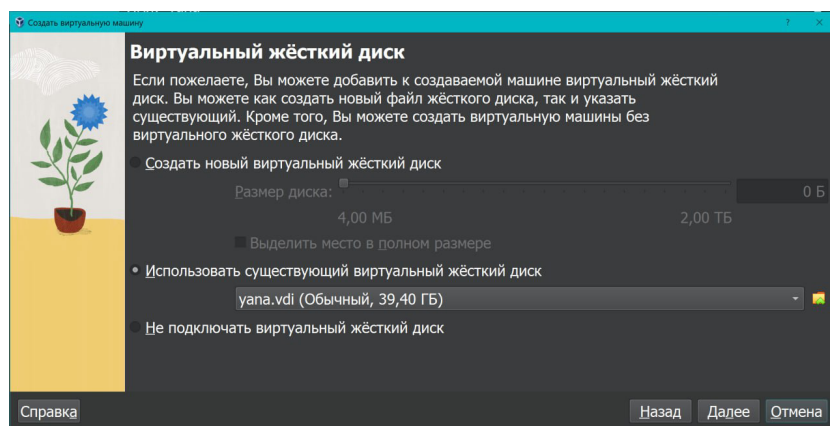


Рис. 4.2: Виртуальный жесткий диск

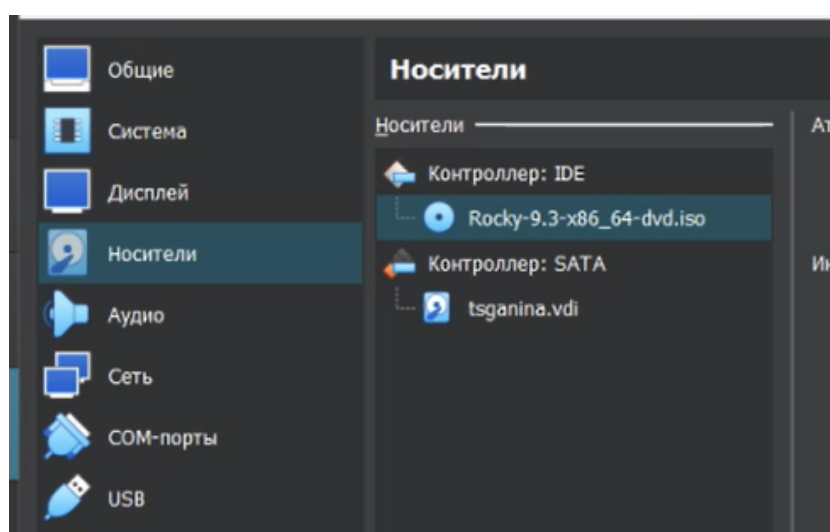


Рис. 4.3: Подключение образа

Выбираю Английский язык и перехожу в “Installation summary”. Здесь настраиваю обеспечение (“Software”): выбираю GUI и “Среда для разработки” (“Development tools”). Далее отключаю KDUMP, проверяю подключение к сети (“Network & Host name”), а также место скачивания (“Installation Destination”), где уже выбран диск, подключенный в самом начале, так что я просто нажимаю “Done”. В конце настраиваю пользователя (“User settings”): логин и пароль, а также корневой пароль (рис. 4.4), (рис. 4.5).

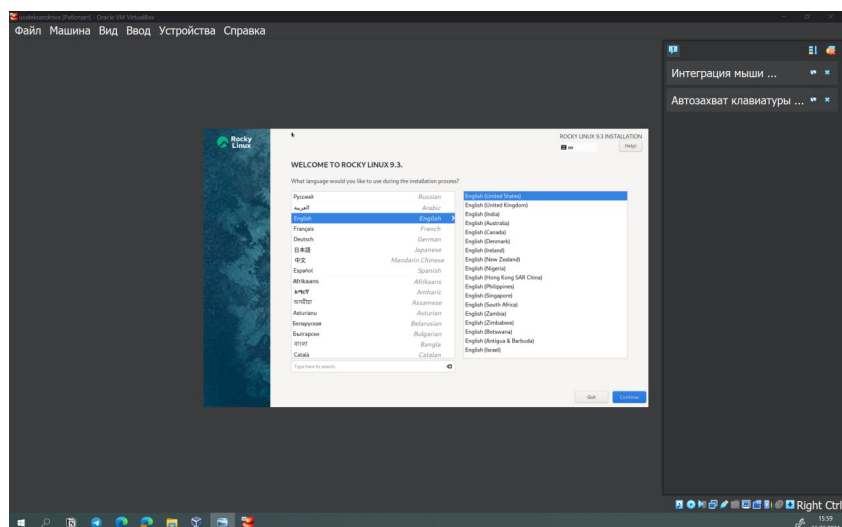


Рис. 4.4: Настройки языка

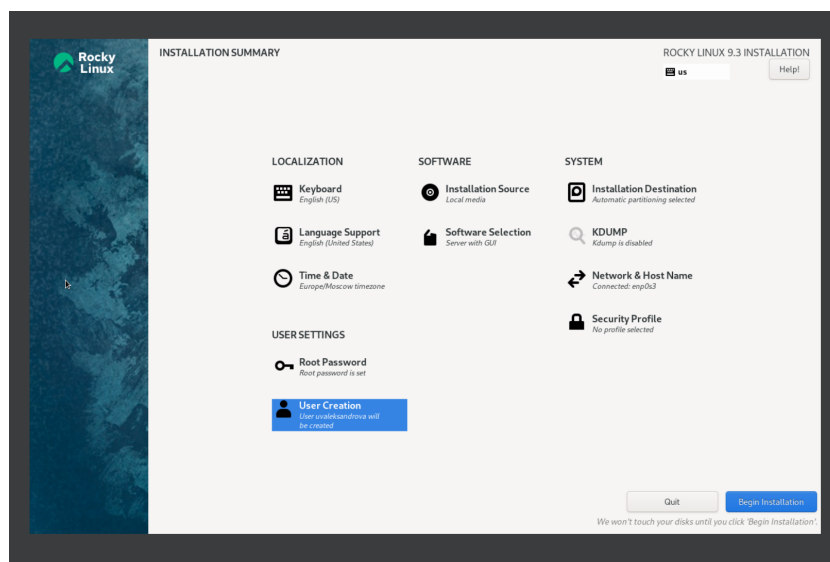


Рис. 4.5: Сводка установки

Начинаю скачивание и после перезапускаю машину (рис. 4.6).

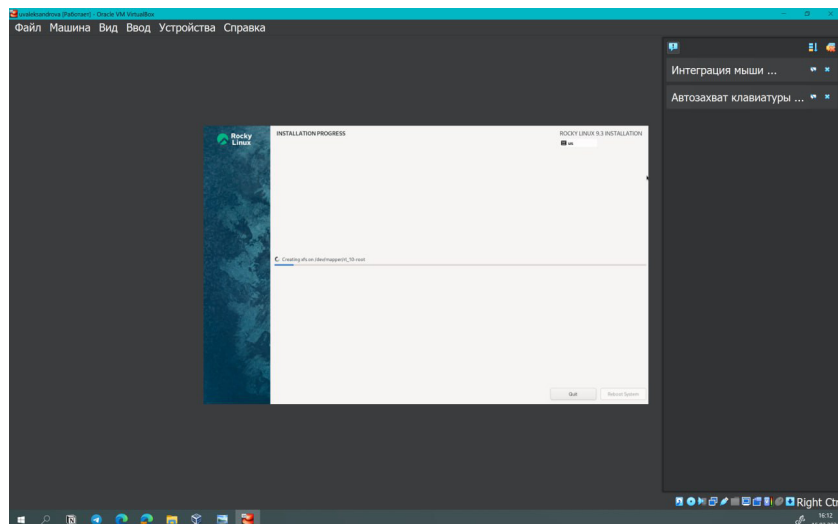


Рис. 4.6: Скачивание

Захожу в систему и, в меню “Устройства”, подключаю образ диска Дополнений гостевой ОС (рис. 4.7).

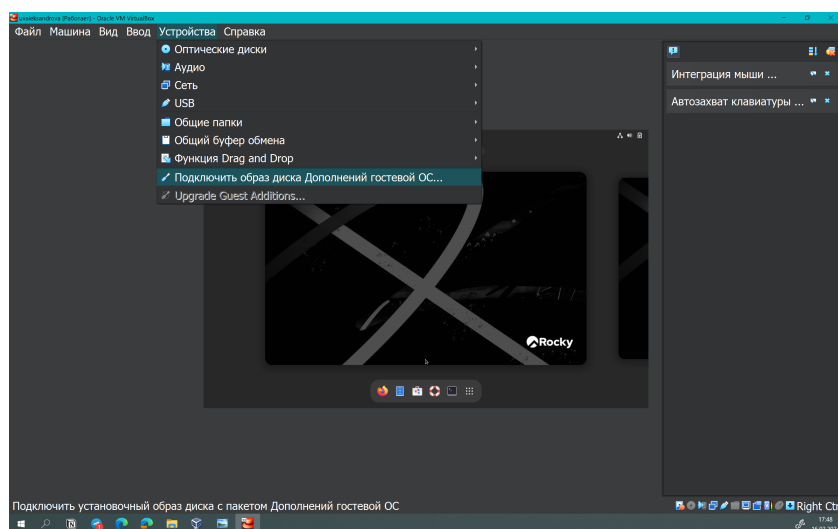


Рис. 4.7: Подключение гостевой ОС

Подтверждаю выполнение и жду окончания загрузки, а затем снова перезапускаю машину, следуя инструкциям от системы (рис. 4.8).

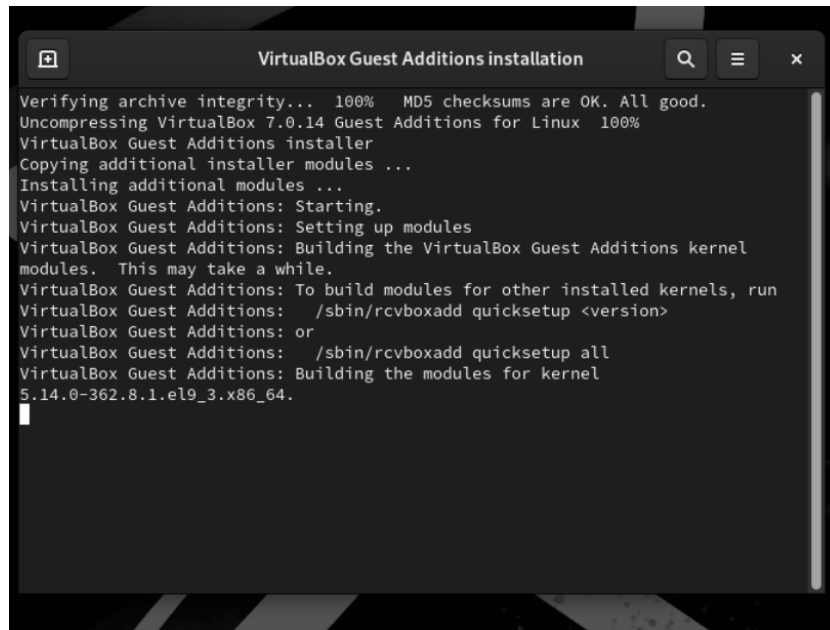


Рис. 4.8: Процесс загрузки в терминале

В окне терминала анализирую последовательность загрузки системы при помощи команды **dmesg** (рис. 4.9).

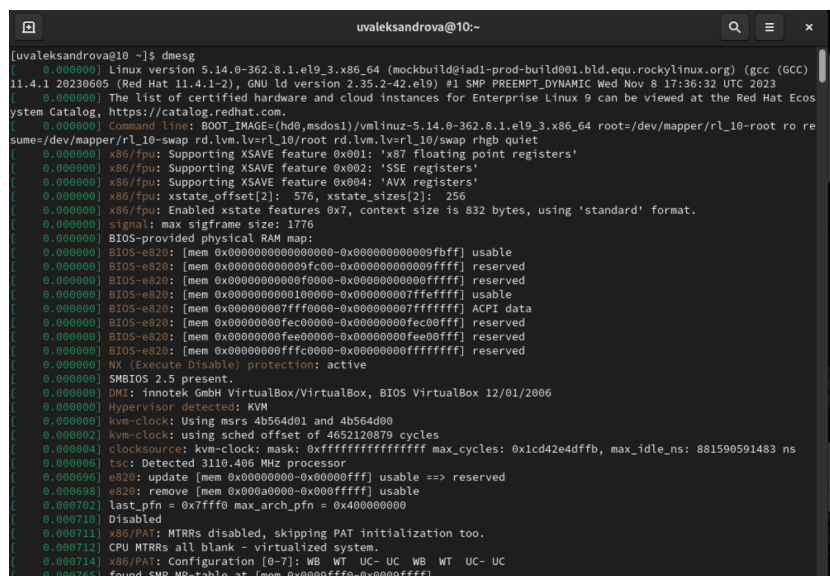


Рис. 4.9: dmesg

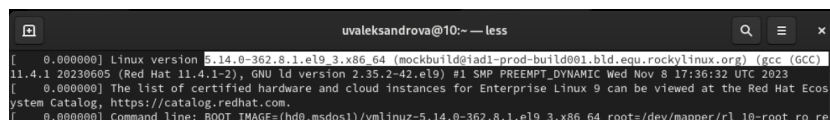
То же самое делаю через **dmesg | less** (рис. 4.10).

```
uvaleksandrova@10:~$ less
[ 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
[ 0.000000] The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red Hat Ecos
system Catalog, https://catalog.redhat.com.
[ 0.000000] Command line: BOOT_IMAGE=(hdd,msdos1)/vmlinuz-5.14.0-362.8.1.el9_3.x86_64 root=/dev/mapper/r1_l0-root ro re
sume=/dev/mapper/r1_l0-swap rd.lvm.lv=r1_l0/root rd.lvm.lv=r1_l0/swap rhgb quiet
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point 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 0x0000000000000000-0x000000000009fbff] usable
[ 0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x000000000009f000-0x000000000000ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000000007fffff] usable
[ 0.000000] BIOS-e820: [mem 0x00000000007ffff000-0x00000000007fffff] ACPI data
[ 0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffff] reserved
[ 0.000000] NX (Execute Disable) protection: active
[ 0.000000] SMBIOS 2.5 present.
[ 0.000000] DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[ 0.000000] Hypervisor detected: KVM
[ 0.000000] kvm-clock: Using msrs 4b564d01 and 4b564d00
[ 0.000002] kvm-clock: using sched offset of 4652120879 cycles
[ 0.000004] clocksource: kvm-clock: mask: 0xffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881590591483 ns
[ 0.000006] tsc: Detected 3110.406 MHz processor
[ 0.000696] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[ 0.000698] e820: remove [mem 0x000a0000-0x0000ffff] usable
[ 0.000702] last_pfn = 0x7ffff0 max_arch_pfn = 0x400000000
[ 0.000710] Disabled
[ 0.000711] x86/PAT: MTRRs disabled, skipping PAT initialization too.
[ 0.000712] CPU MTRRs all blank - virtualized system.
[ 0.000714] x86/PAT: Configuration [0-7]: WB WT UC- UC WB WT UC- UC
[ 0.000765] found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
[ 0.000889] RAMDISK: [mem 0x3101f000-0x34807fff]
[ 0.000893] ACPI: Early table checksum verification disabled
[ 0.000896] ACPI: RSDP 0x0000000000000000 000024 (v02 VBOX )
```

Рис. 4.10: dmesg | less

5 Домашнее задание

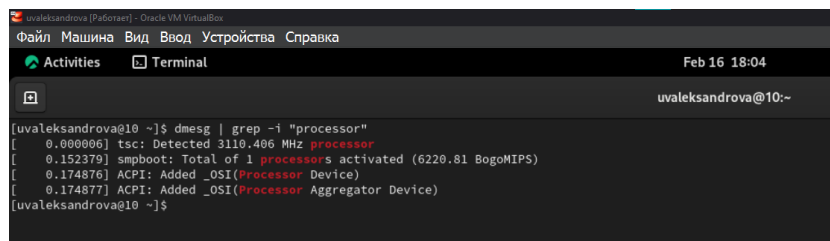
Получаю следующую информацию: 1. Версия ядра Linux (Linux version) с помощью **dmesg** (рис. 5.1).



```
uvaleksandrova@10:~ -- less
[ 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
[ 0.000000] The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red Hat Ecos
system Catalog, https://catalog.redhat.com.
[ 0.000000] Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-362.8.1.el9_3.x86_64 root=/dev/mapper/r1_l10-root ro re
```

Рис. 5.1: Версия ядра Linux

2. Частота процессора (Detected Mhz processor) при помощи **mesg | grep -i "processor"** (рис. 5.2).



```
uvaleksandrova@10 ~]$ dmesg | grep -i "processor"
[ 0.000000] tsc: Detected 3110.486 MHz processor
[ 0.152379] smpboot: Total of 1 processors activated (6220.81 BogoMIPS)
[ 0.174876] ACPI: Added _OSI(Processor Device)
[ 0.174877] ACPI: Added _OSI(Processor Aggregator Device)
uvaleksandrova@10 ~]$
```

Рис. 5.2: Частота процессора

3. Модель процессора (CPU0) и объем доступной оперативной памяти (Memory available) (рис. 5.3).

```

uvaleksandrova@10 ~$ dmesg | grep -i "CPU"
[ 0.151861] smpboot: CPU0: 11th Gen Intel(R) Core(TM) i5-11300H @ 3.10GHz (family: 0x6, model: 0x8c, stepping: 0x1)
uvaleksandrova@10 ~$ dmesg | grep -i "Memory"
[ 0.000019] ACPI: Reserving FACP table memory at [mem 0x7fff00f0-0x7fff0103]
[ 0.000020] ACPI: Reserving DSDT table memory at [mem 0x7fff0010-0x7fff0262]
[ 0.000022] ACPI: Reserving FACS table memory at [mem 0x7fff0200-0x7fff023f]
[ 0.000023] ACPI: Reserving FACS table memory at [mem 0x7fff0200-0x7fff023f]
[ 0.000023] ACPI: Reserving APIC table memory at [mem 0x7fff0240-0x7fff0293]
[ 0.000023] ACPI: Reserving SSDT table memory at [mem 0x7fff02a0-0x7fff0600]
[ 0.001831] Early memory node ranges
[ 0.001877] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x00000fff]
[ 0.001878] PM: hibernation: Registered nosave memory: [mem 0x0000f000-0x0000ffff]
[ 0.001879] PM: hibernation: Registered nosave memory: [mem 0x000a0000-0x000affff]
[ 0.001879] PM: hibernation: Registered nosave memory: [mem 0x000f0000-0x000fffff]
[ 0.008477] Memory: 240560K/209696K available (16384K kernel code, 5596K rodata, 11444K rodata, 3824K init, 18424K bss, 157768K reserved, 0K cma-reserved)
[ 0.049325] Freeing SMP alternatives memory: 36K
[ 0.156293] x86/mm: memory block size: 128MB
[ 0.331230] Non-volatile memory driver v1.3
[ 0.700130] Freeing initrd memory: 57252K
[ 0.975092] Freeing unused decrypted memory: 2036K
[ 0.975406] Freeing unused kernel image (initrd) memory: 3824K
[ 0.976319] Freeing unused kernel image (rodata/data gap) memory: 844K
[ 1.749028] vmwgfx 0000:00:02:0: [drm] Legacy memory limits: VRAM = 16384 kB, FIFO = 2048 kB, surface = 587904 kB
[ 1.749932] vmwgfx 0000:00:02:0: [drm] Maximum display memory size is 16384 kB

```

Рис. 5.3: Модель процессора

5. Тип обнаруженного гипервизора (Hypervisor detected) (рис. 5.4).

```

[ 1.749932] vmwgfx 0000:00:02:0: [drm] Maximum display memory size is 16384 kB
uvaleksandrova@10 ~$ dmesg | grep -i "Memory available"
uvaleksandrova@10 ~$ dmesg | grep -i "Hypervisor detected"
[ 0.000000] Hypervisor detected: KVM
uvaleksandrova@10 ~$

```

Рис. 5.4: Тип обнаруженного гипервизора

6. Тип файловой системы корневого раздела (рис. 5.5).

```

uvaleksandrova@10 ~$ dmesg | grep -i "Hypervisor detected"
[ 0.000000] Hypervisor detected: KVM
uvaleksandrova@10 ~$ df -T
Filesystem      Type      1K-blocks    Used Available Use% Mounted on
devtmpfs        devtmpfs   4096          0    4096      0% /dev
tmpfs           tmpfs     1001460        0   1001460    0% /dev/shm
tmpfs           tmpfs     400584    8360   392224    3% /run
/dev/mapper/r1_10-root xfs     38916096 5695980 33220116   15% /
/dev/sda1       xfs     983040  273032   710008   28% /boot
tmpfs           tmpfs     200292    128   200164    1% /run/user/1000
/dev/sr0        iso9660    52272    52272      0 100% /run/media/uvaleksandrova/VBox_GAs_7.0.14
uvaleksandrova@10 ~$

```

Рис. 5.5: Тип файловой системы

7. Последовательность монтирования файловых систем (рис. 5.6).

```

[ 1.749932] vmgfx 0000:00:02.0: [drm] Maximum display memory size is 16384 KiB
[uvaleksandrova@10 ~]$ dmesg | grep -i "Memory available"
[uvaleksandrova@10 ~]$ dmesg | grep -i "Hypervisor detected"
[ 0.000000] Hypervisor detected: KVM
[uvaleksandrova@10 ~]$ df -T
Filesystem      Type      1K-blocks    Used Available Use% Mounted on
devtmpfs        devtmpfs   4096          0    4096   0% /dev
tmpfs           tmpfs     1681460        0   1681460   0% /dev/shm
tmpfs           tmpfs     486084         8360    477724   2% /run
/dev/mapper/r1_10-root xfs     38916986 5695980 33226116 15% /
/dev/sdal       xfs     983840 273032   710808 28% /boot
tmpfs           tmpfs     280292       128    280164   1% /run/user/1000
/dev/sr0        iso9660    52272    52272      0 100% /run/media/uvaleksandrova/VBox_GAs_7.0.14
[uvaleksandrova@10 ~]$ 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=8096K,nr_inodes=242370,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=480584K,nr_inodes=619200,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_10-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,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=18494)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime,seclabel)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,seclabel,pagesize=2M)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime,seclabel)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime,seclabel)
configfs on /sys/kernel/config type configfs (rw,nosuid,nodev,noexec,relatime)
fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatime)
none on /run/credentials/systemd-sysusers.service type ramfs (ro,nosuid,nodev,noexec,relatime,seclabel,mode=700)
none on /run/credentials/systemd-tmpfiles-setup-dev.service type ramfs (ro,nosuid,nodev,noexec,relatime,seclabel,mode=700)
none on /boot type xfs (rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
none on /run/credentials/systemd-tmpfiles-setup.service type ramfs (ro,nosuid,nodev,noexec,relatime,seclabel,mode=700)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,seclabel,size=280292K,nr_inodes=50873,mode=700,uid=1000,gid=1000,inode64)
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1000,group_id=1000)
/dev/sr0 on /run/media/uvaleksandrova/VBox_GAs_7.0.14 type iso9660 (ro,nosuid,nodev,relatime,nojoliet,check=s,map=n,blocksize=2048,uid=1000,gid=1000)

```

Рис. 5.6: Последовательность монтирования файловых систем

6 Контрольные вопросы

1. Какую информацию содержит учётная запись пользователя?

Учетная запись содержит данные пользователя (логин, пароль и тд), необходимые для входа в систему. 2. Укажите команды терминала и приведите примеры:

- для получения справки по команде: `help (dmesg help)`;
- для перемещения по файловой системе: `cd (cd ~/work/study)`;
- для просмотра содержимого каталога: `ls (ls work)`;
- для определения объёма каталога: `du (du work)`;
- для создания / удаления каталогов / файлов: `mkdir/rm/mv`;
- для задания определённых прав на файл/каталог: `chmod -r`;
- для просмотра истории команд: клавиши вверх и вниз.

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

Файловая система - способ организации и комплектации данных в системе (~/work/study/2023-2024/infosec)

4. Как посмотреть, какие файловые системы подмонтированы в ОС? При помощи команды `mount` или с помощью команды `df`. 5. Как удалить зависший процесс? При помощи утилиты `killall` (останавливает все работающие процессы) или `kill <>`.

7 Выводы

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