

# **Отчёт по лабораторной работе №1**

**дисциплина: Информационная безопасность**

Абрамян Артём Арменович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
<b>5</b>	<b>Домашнее задание</b>	<b>19</b>
<b>6</b>	<b>Контрольные вопросы</b>	<b>22</b>
<b>7</b>	<b>Выводы</b>	<b>25</b>
<b>8</b>	<b>Библиографический список</b>	<b>26</b>

## Список иллюстраций

4.1	Виртуальная машина . . . . .	8
4.2	Память виртуальной машины . . . . .	9
4.3	Конфигурация жёсткого диска . . . . .	9
4.4	Размер диска . . . . .	10
4.5	Образ операционной системы . . . . .	11
4.6	Окно настройки установки образа ОС . . . . .	12
4.7	Окно настройки установки: выбор программ . . . . .	13
4.8	Окно настройки установки: отключение KDUMP . . . . .	14
4.9	Окно настройки установки: место установки . . . . .	15
4.10	Окно настройки установки: сеть и имя узла . . . . .	16
4.11	Установка пароля . . . . .	17
4.12	Завершение установки ОС . . . . .	18
4.13	Пользователь существует . . . . .	18
5.1	Команда <code>sudo dmesg</code> . . . . .	19
5.2	Команда <code>dmesg   less</code> . . . . .	20
5.3	Поиск информации с помощью <code>grep</code> . . . . .	21

## Список таблиц

# 1 Цель работы

В данной лабораторной работе мне было необходимо приобрести практические навыки установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов.

## 2 Задание

Здесь приводится описание задания в соответствии с рекомендациями методического пособия и выданным вариантом.

### 3 Теоретическое введение

Лабораторная работа подразумевает установку на виртуальную машину VirtualBox (<https://www.virtualbox.org/>) операционной системы Linux (дистрибутив Rocky (<https://rockylinux.org/>) или CentOS (<https://www.centos.org/>)). Выполнение работы возможно как в дисплейном классе факультета физико-математических и естественных наук РУДН, так и дома. Описание выполнения работы приведено для дисплейного класса со следующими характеристиками: – Intel Core i3-550 3.2 GHz, 4 GB оперативной памяти, 20 GB свободного места на жёстком диске; – ОС Linux Gentoo (<http://www.gentoo.ru/>); – VirtualBox верс. 6.1 или старше; – каталог с образами ОС для работающих в дисплейном классе: [/afs/dk.sci.pfu.edu.ru/common/files/iso/](http://afs.dk.sci.pfu.edu.ru/common/files/iso/).

## 4 Выполнение лабораторной работы

1. Создайте новую виртуальную машину. Для этого в VirtualBox выберите “Машина” “Создать”. Укажите имя виртуальной машины (ваш логин в дисплейном классе), тип операционной системы — Linux, RedHat. (рис. 4.1)

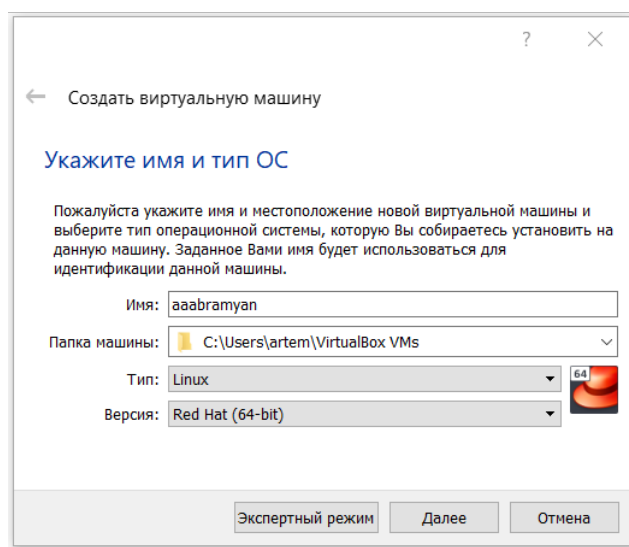


Рис. 4.1: Виртуальная машина

2. Укажите размер основной памяти виртуальной машины - 2048 МБ (или большее число, кратное 1024 МБ, если позволяют технические характеристики вашего компьютера). (рис. 4.2)



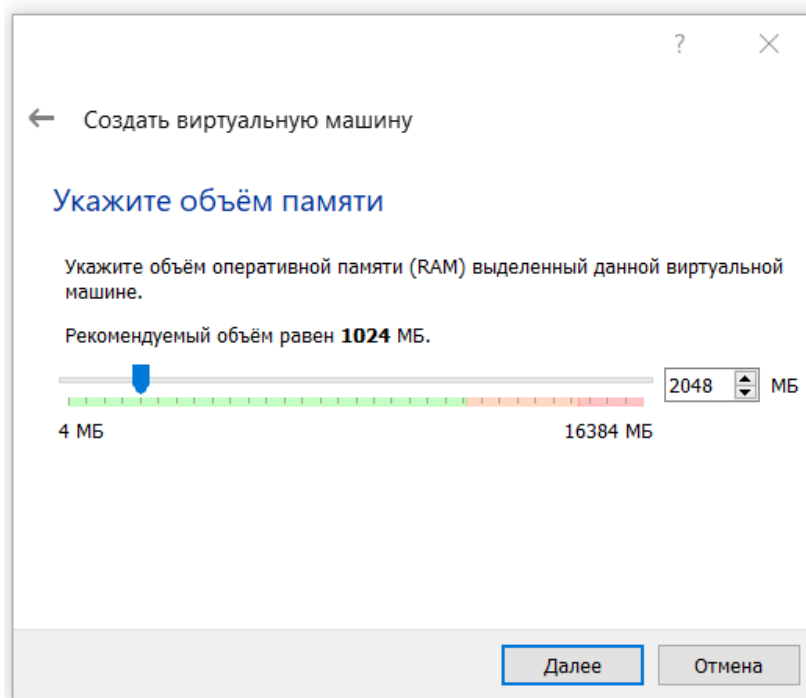


Рис. 4.2: Память виртуальной машины

3. Задайте конфигурацию жёсткого диска — загрузочный, VDI (VirtualBox Disk Image), динамический виртуальный диск. (рис. 4.3)

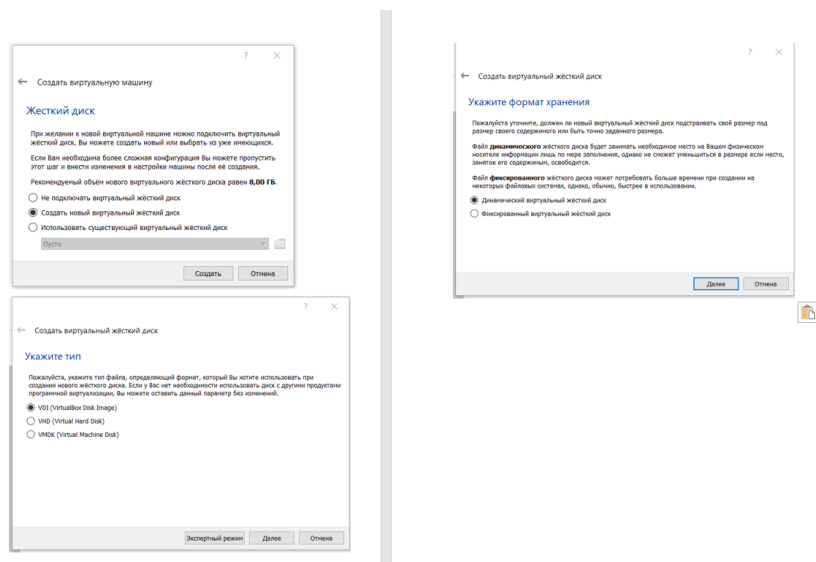


Рис. 4.3: Конфигурация жёсткого диска

4. Задайте размер диска — 40 ГБ (или больше), его расположение. (рис. 4.4)

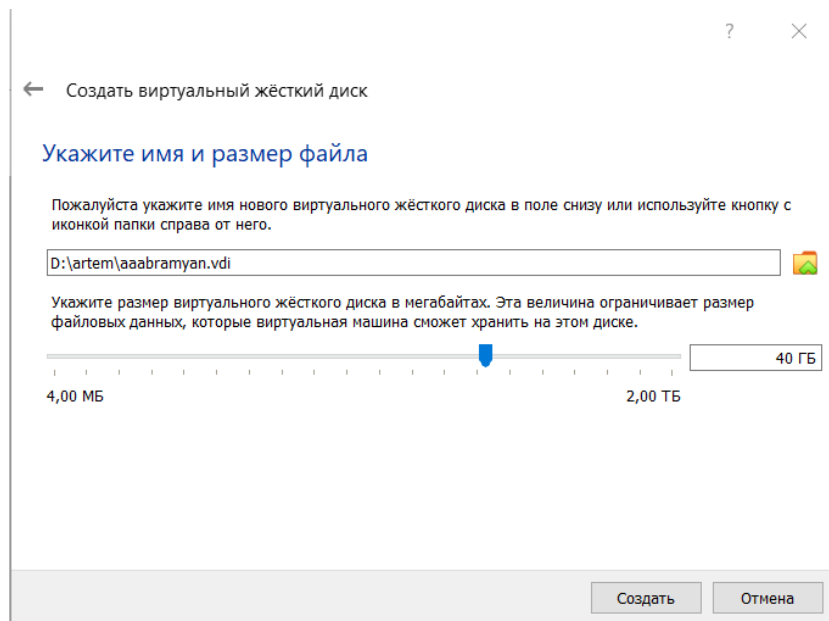


Рис. 4.4: Размер диска

5. Выберите в VirtualBox для Вашей виртуальной машины “Настройки” “Носители”. Добавьте новый привод оптических дисков и выберите образ операционной системы. (рис. 4.5)

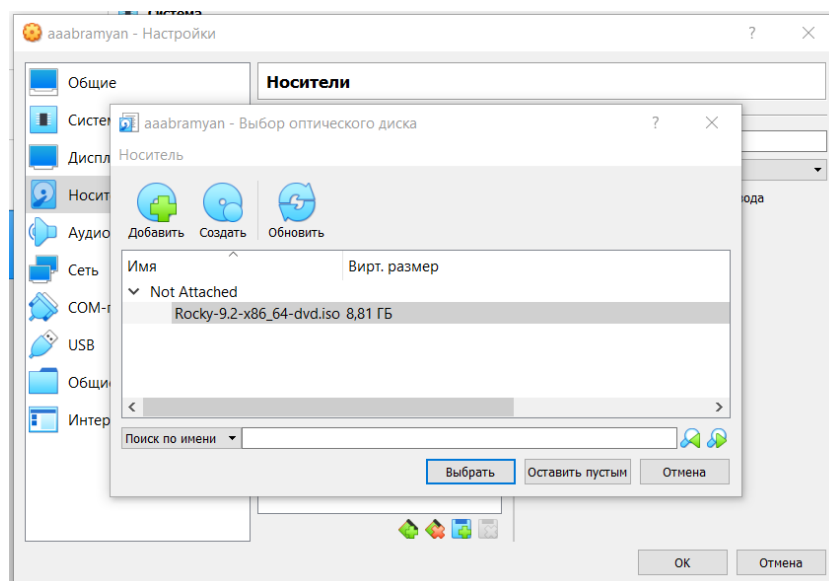


Рис. 4.5: Образ операционной системы

6. Запустите виртуальную машину, выберите English в качестве языка интерфейса и перейдите к настройкам установки операционной системы. (рис. 4.6)

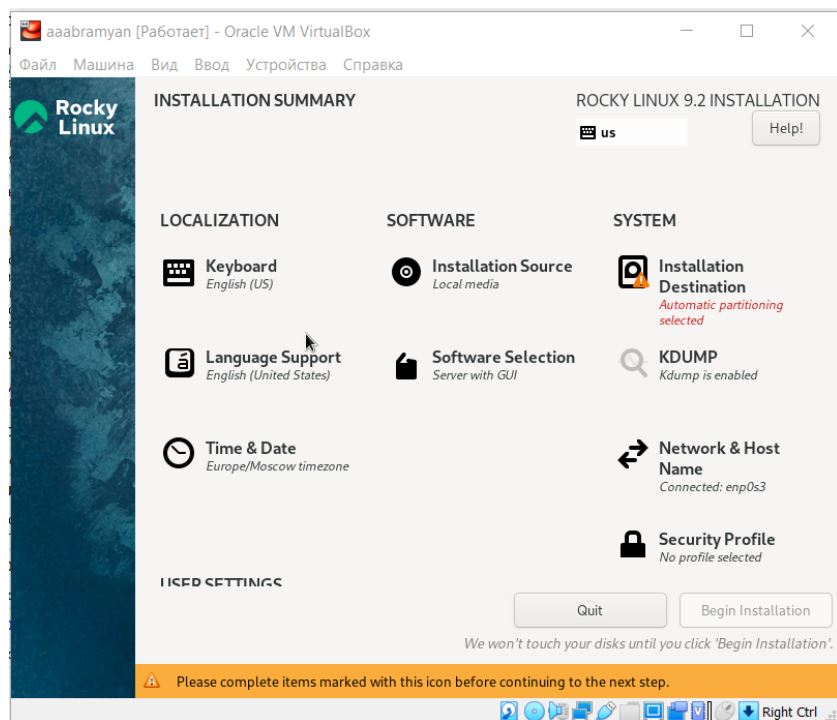


Рис. 4.6: Окно настройки установки образа ОС

7. В разделе выбора программ укажите в качестве базового окружения “Server with GUI”, а в качестве дополнения — “Development Tools”. (рис. 4.7)

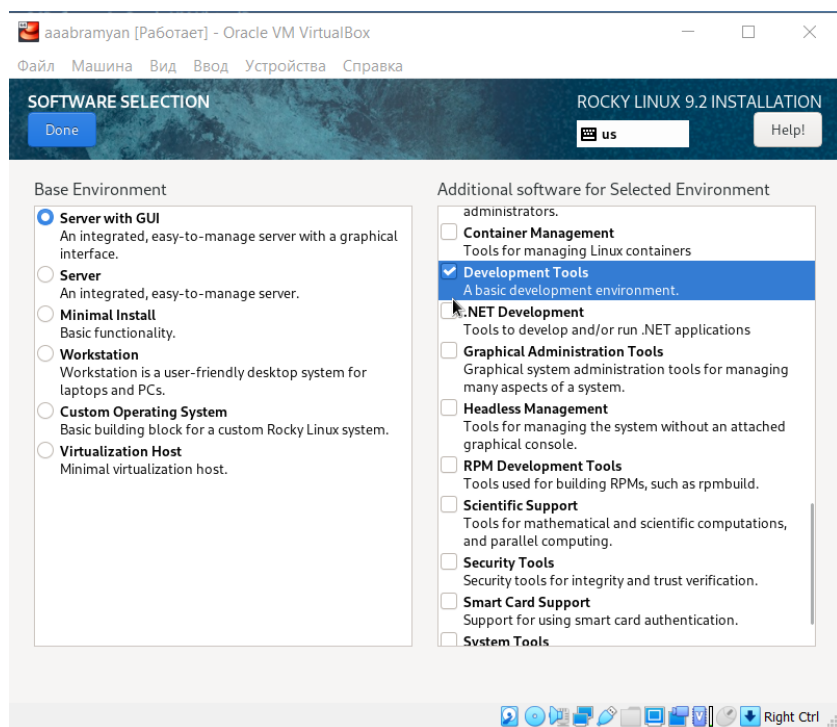


Рис. 4.7: Окно настройки установки: выбор программ

8. Отключите KDUMP.(рис. 4.8)

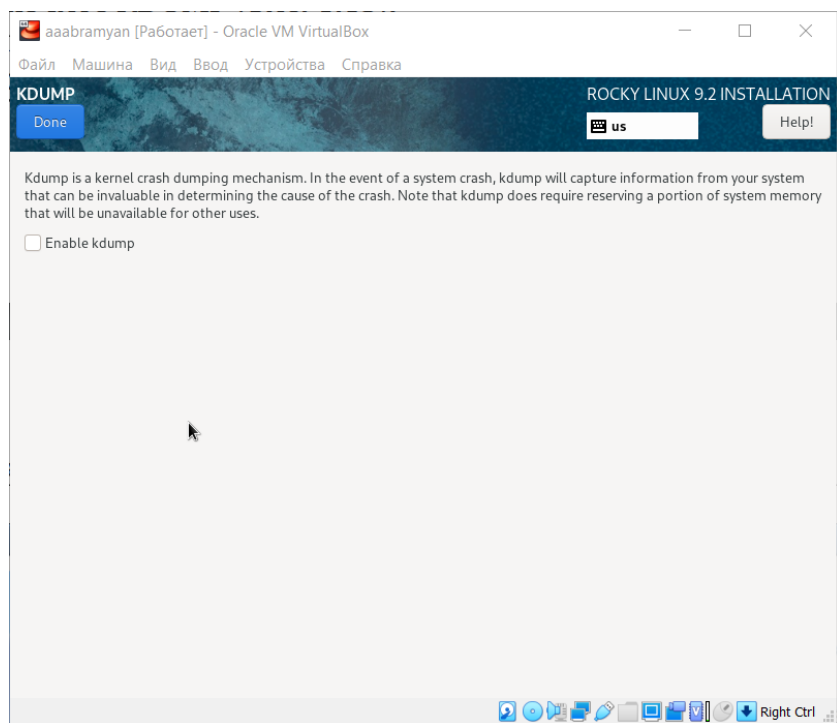


Рис. 4.8: Окно настройки установки: отключение KDUMP

9. Место установки ОС оставьте без изменения.(рис. 4.9)

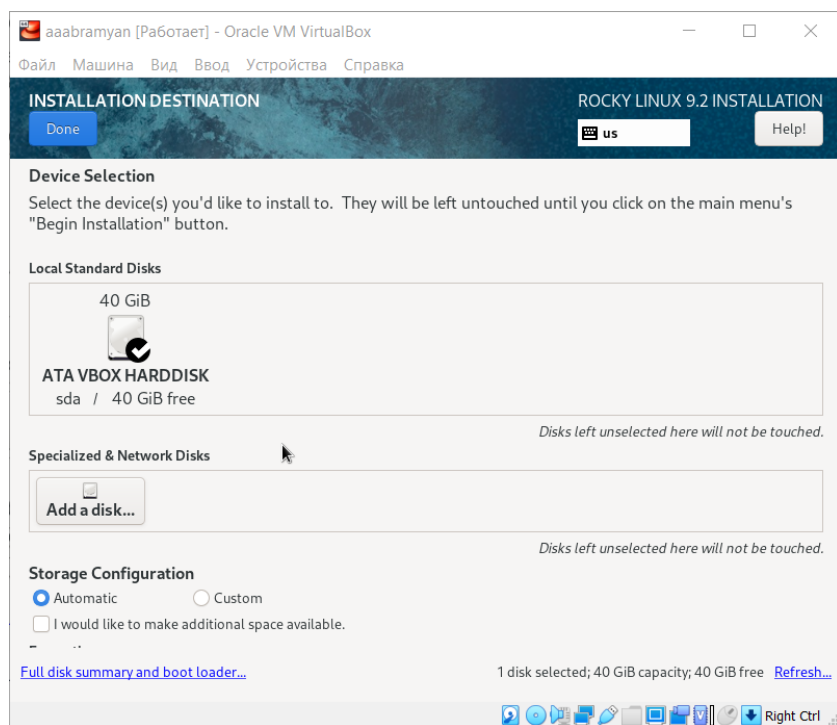


Рис. 4.9: Окно настройки установки: место установки

10. Включите сетевое соединение и в качестве имени узла укажите `user.localdomain`, где вместо `user` укажите имя своего пользователя в соответствии с соглашением об именовании.(рис. 4.10)

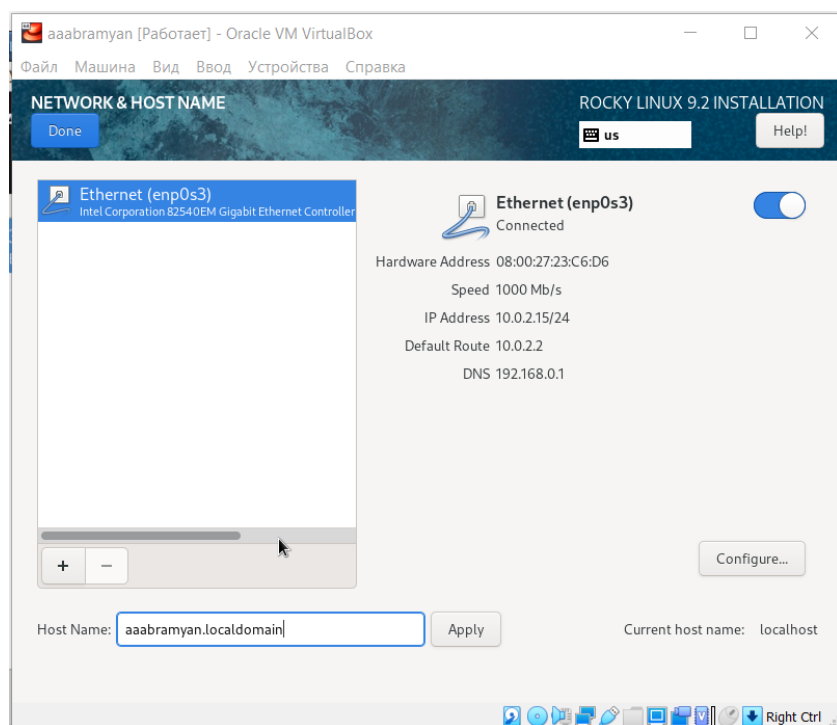


Рис. 4.10: Окно настройки установки: сеть и имя узла

11. Установите пароль для root и пользователя с правами администратора.(рис. 4.11)



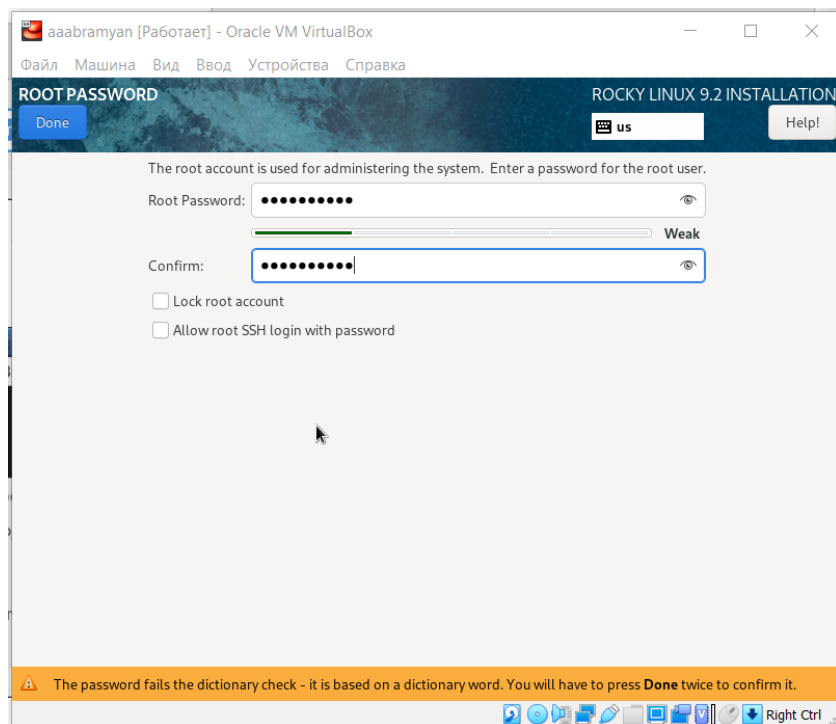


Рис. 4.11: Установка пароля

12. После завершения установки операционной системы корректно перезапустите виртуальную машину и примите условия лицензии.(рис. 4.12)

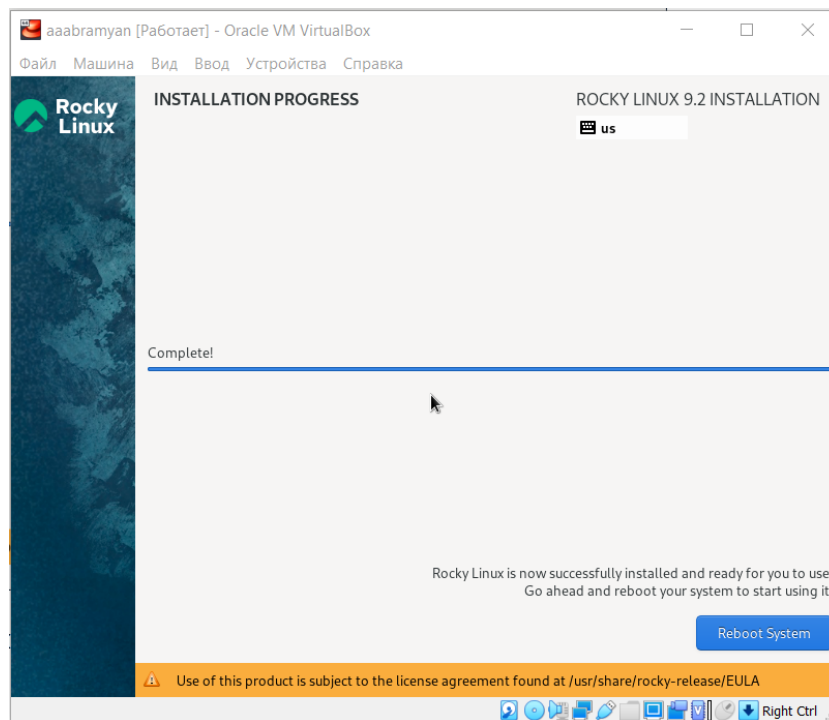


Рис. 4.12: Завершение установки ОС

13. Создадим пользователя.(рис. 4.13)

Пользователь существует

Рис. 4.13: Пользователь существует

## 5 Домашнее задание

1. Дождитесь загрузки графического окружения и откройте терминал. В окне терминала проанализируйте последовательность загрузки системы, выполнив команду `dmesg`. (рис. 5.1)

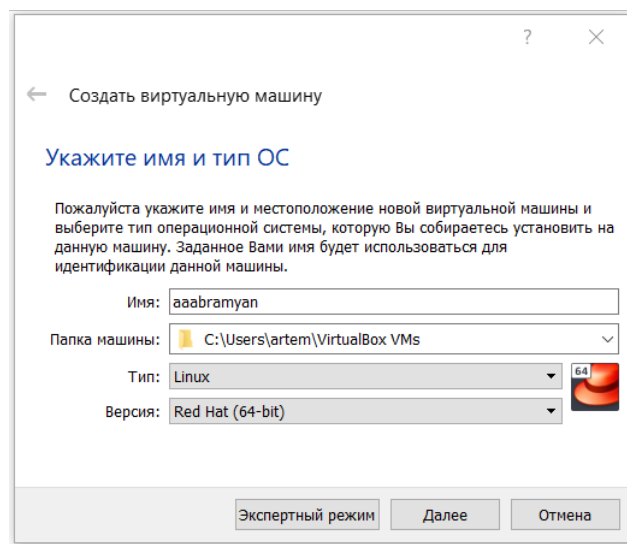
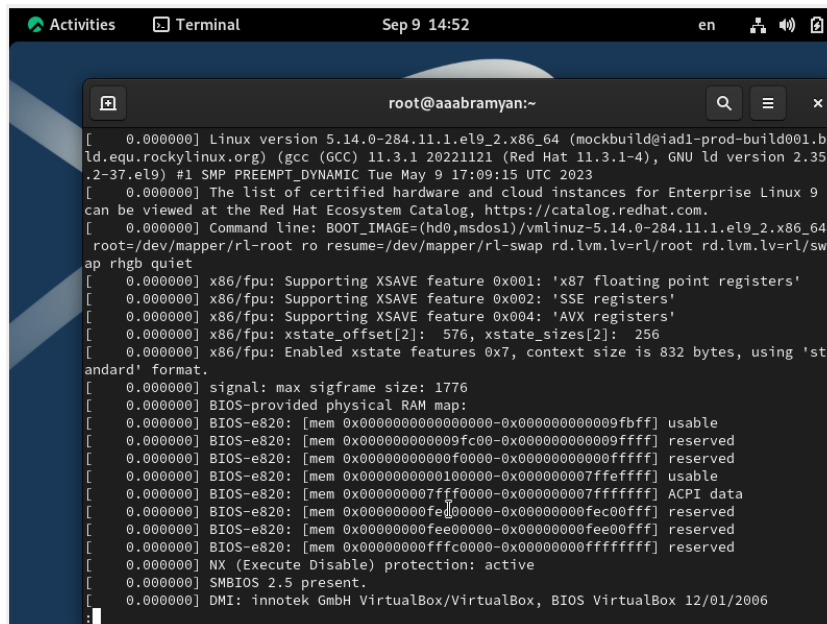


Рис. 5.1: Команда `sudo dmesg`

2. Можно просто посмотреть вывод этой команды: `dmesg less` (рис. 5.2)



```
root@aaabramyan:~  
[ 0.000000] Linux version 5.14.0-284.11.1.el9_2.x86_64 (mockbuild@iad1-prod-build001.b  
ld.equ.rockylinux.org) (gcc (GCC) 11.3.1 20221121 (Red Hat 11.3.1-4), GNU ld version 2.35  
.2-37.el9) #1 SMP PREEMPT_DYNAMIC Tue May 9 17:09:15 UTC 2023  
[ 0.000000] The list of certified hardware and cloud instances for Enterprise Linux 9  
can be viewed at the Red Hat Ecosystem Catalog, https://catalog.redhat.com.  
[ 0.000000] Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-284.11.1.el9_2.x86_64  
root=/dev/mapper/rl-root ro resume=/dev/mapper/rl-swap rd.lvm.lv=rl/root rd.lvm.lv=rl/sw  
ap 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 'st  
andard' 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 0x00000000000f0000-0x00000000000fffff] reserved  
[ 0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000000007fffff] usable  
[ 0.000000] BIOS-e820: [mem 0x00000000007fff0000-0x00000000007fffff] ACPI data  
[ 0.000000] BIOS-e820: [mem 0x0000000000fee00000-0x0000000000fec0ffff] reserved  
[ 0.000000] BIOS-e820: [mem 0x0000000000fee00000-0x0000000000fec0ffff] reserved  
[ 0.000000] BIOS-e820: [mem 0x0000000000fffc0000-0x0000000000ffffff] 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
```

Рис. 5.2: Команда dmesg | less

- Получим следующую информацию: Версия ядра Linux (Linux version). Частота процессора (Detected Mhz processor). Модель процессора (CPU0). Объем доступной оперативной памяти (Memory available). Тип обнаруженного гипервизора (Hypervisor detected). Тип файловой системы корневого раздела. (рис. 5.3)

```
#1 SMP PREEMPT_DYNAMIC Tue May 9 17:09:15 UTC 2023
[aaabramyan@aaabramyan ~]$ dmesg | grep -i "Mhz"
[ 0.000000] tsc: Detected 2208.000 MHz processor
[ 2.915950] e1000 0000:00:03:0 eth0: (PCI:33MHz:32-bit) 08:00:27:23:c6:d6
[aaabramyan@aaabramyan ~]$ dmesg | grep -i "CPU0"
[ 0.165625] smpboot: CPU0: Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz (family: 0x6, model: 0x9e, stepping: 0xa)
[aaabramyan@aaabramyan ~]$ dmesg | grep -i "Memory"
[ 0.001206] ACPI: Reserving FACP table memory at [mem 0x7fff00f0-0x7fff01e3]
[ 0.001207] ACPI: Reserving DSDT table memory at [mem 0x7fff0470-0x7fff2794]
[ 0.001208] ACPI: Reserving FACS table memory at [mem 0x7fff0200-0x7fff023f]
[ 0.001209] ACPI: Reserving FACS table memory at [mem 0x7fff0200-0x7fff023f]
[ 0.001210] ACPI: Reserving APIC table memory at [mem 0x7fff0240-0x7fff0293]
[ 0.001210] ACPI: Reserving SSDT table memory at [mem 0x7fff02a0-0x7fff046b]
[ 0.001783] Early memory node ranges
[ 0.002823] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x00000fff]
[ 0.002824] PM: hibernation: Registered nosave memory: [mem 0x00009f00-0x0000ffff]
[ 0.002825] PM: hibernation: Registered nosave memory: [mem 0x000a0000-0x000effff]
[ 0.002826] PM: hibernation: Registered nosave memory: [mem 0x000f0000-0x000fffff]
[ 0.011703] Memory: 260860K/2096696K available (14342K kernel code, 5536K rdata, 10180K ro data, 2792K init, 7524K bss, 143184K reserved, 0K cma-reserved)
[ 0.063452] Freeing SMP alternatives memory: 36K
[ 0.173831] x86/mm: Memory block size: 128MB
[ 0.372718] Non-volatile memory driver v1.3
[ 0.886625] Freeing initrd memory: 57032K
[ 1.016974] Freeing unused decrypted memory: 2036K
[ 1.017202] Freeing unused kernel image (initmem) memory: 2792K
[ 1.017202] Freeing unused kernel image (initmem) memory: 2792K
[ 1.019223] Freeing unused kernel image (text/rodata gap) memory: 2040K
[ 1.019260] Freeing unused kernel image (rodata/data gap) memory: 60K
[ 2.183281] vmwgfx 0000:00:02:0: [drm] Legacy memory limits: VRAM = 16384 kB, FIFO = 2048 kB, surface = 507904 kB
[ 2.183287] vmwgfx 0000:00:02:0: [drm] Maximum display memory size is 16384 kiB
[aaabramyan@aaabramyan ~]$ dmesg | grep -i "Hypervisor detected"
[ 0.000000] Hypervisor detected: KVM
[aaabramyan@aaabramyan ~]$ dmesg | grep -i "Mount"
[ 0.047872] Mount-cache hash table entries: 4096 (order: 3, 32768 bytes, linear)
[ 0.047876] Mountpoint-cache hash table entries: 4096 (order: 3, 32768 bytes, linear)
[ 3.728538] XFS (dm-0): Mounting V5 Filesystem
[ 4.064631] XFS (dm-0): Ending clean mount
[ 11.100454] systemd[1]: Set up automount Arbitrary Executable File Formats File System Automount Point.
[ 11.201896] systemd[1]: Mounting Huge Pages File System...
[ 11.203563] systemd[1]: Mounting POSIX Message Queue File System...
[ 11.206521] systemd[1]: Mounting Kernel Debug File System...
[ 11.208046] systemd[1]: Mounting Kernel Trace File System...
[ 11.500388] systemd[1]: Starting Remount Root and Kernel File Systems...
[ 11.510534] systemd[1]: Mounted Huge Pages File System.
[ 11.510837] systemd[1]: Mounted POSIX Message Queue File System.
[ 11.511082] systemd[1]: Mounted Kernel Debug File System.
[ 11.511301] systemd[1]: Mounted Kernel Trace File System.
[ 16.744617] XFS (sda1): Mounting V5 Filesystem
[ 18.053786] XFS (sda1): Ending clean mount
[aaabramyan@aaabramyan ~]$
```

Рис. 5.3: Поиск информации с помощью grep

## 6 Контрольные вопросы

1. Какую информацию содержит учётная запись пользователя? Учетная запись пользователя - это необходимая для системы информация о пользователе, которая хранится в специальных файлах. Вся информация о пользователе обычно хранится в файлах `/etc/passwd` и `/etc/group`. Учетная запись пользователя содержит: имя пользователя (user name), идентификационный номер группы (GID), идентификационный номер пользователя (UID), пароль (password), полное имя (full name), домашний каталог (home directory), начальную оболочку (login shell).
2. Укажите команды терминала и приведите примеры: – для получения справки по команде; – для перемещения по файловой системе; – для просмотра содержимого каталога; – для определения объёма каталога; – для создания / удаления каталогов / файлов; – для задания определённых прав на файл / каталог; – для просмотра истории команд.

Для получения справки по команде: `man` команда. Например, команда `man ls` выведет справку о команде `ls`.

Для перемещения по файловой системе: `cd` путь. Например, команда `cd newdir` осуществляет переход в каталог `newdir`.

Для просмотра содержимого каталога: `ls` опции путь. Например, команда `ls -a ~/newdir` отобразит имена скрытых файлов в каталоге `newdir`.

Для определения объёма каталога: `du` опция путь. Например, команда `du -k ~/newdir` выведет размер каталога `newdir` в килобайтах.

Для создания / удаления каталогов / файлов: `mkdir` опции путь / `rmdir` опции путь / `rm` опции путь. Например, команда `mkdir -p ~/newdir1/newdir2` создаст иерархическую цепочку подкаталогов, создав каталоги `newdir1` и `newdir2`; команда `rmdir -v ~/newdir` удалит каталог `newdir`; команда `rm -r ~/newdir` так же удалит каталог `newdir`.

Для задания определённых прав на файл / каталог: `chmod` опции путь. Например, команда `chmod g+r ~/text.txt` даст группе право на чтение файла `text.txt`.

Для просмотра истории команд: `history` опции. Например, команда `history 5` покажет список последних 5 команд.

3. Что такое файловая система? Приведите примеры с краткой характеристикой. Файловая система имеет два значения: с одной стороны - это архитектура хранения битов на жёстком диске, с другой - это организация каталогов в соответствии с идеологией Linux. Файловая система - это архитектура хранения данных в системе, хранение данных в оперативной памяти и доступа к конфигурации ядра. В физическом смысле файловая система Linux представляет собой пространство раздела диска, разбитое на блоки фиксированного размера. Их размер кратен размеру сектора: 1024, 2048, 4096 или 8120 байт. Примеры файловых систем:

XFS рассчитана на файлы большого размера, поддерживает диски до 2 терабайт. Преимущества: высокая скорость работы с большими файлами, отложенное выделение места, увеличение разделов на лету, незначительный размер служебной информации. Недостатки: невозможность уменьшения размера, сложность восстановления данных и риск потери файлов при аварийном отключении питания.

Ext2, Ext3, Ext4 или Extended Filesystem - стандартная файловая система, первоначально разработанная еще для Minix. Содержит максимальное количество функций и является наиболее стабильной в связи с редкими изменениями кодовой базы. Начиная с ext3 в системе используется функция журналирования. Сегодня версия ext4 присутствует во всех дистрибутивах Linux.

4. Как посмотреть, какие файловые системы подмонтированы в ОС? Команда “findmnt” или “findmnt –all” будет отображать все подмонтированные файловые системы или искать файловую систему
5. Как удалить зависший процесс? Команда “kill -сигнал pid\_процесса” позволяет удалить зависший процесс, где PID - уникальный идентификатор процесса.



## **7 Выводы**

В данной лабораторной работе мне успешно удалось приобрести практические навыки установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов.

## 8 Библиографический список

1. Документация Rocky (<https://docs.rockylinux.org/>)