

# **Лабораторная работа №1**

**Основы информационной безопасности**

Астраханцева А. А.

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
3.1	Домашнее задание . . . . .	16
<b>4</b>	<b>Выводы</b>	<b>21</b>

# Список иллюстраций

3.1	Тип и имя ОС . . . . .	6
3.2	Объем памяти . . . . .	7
3.3	Жесткий диск . . . . .	7
3.4	Тип жесткого диска . . . . .	8
3.5	Формат хранения . . . . .	8
3.6	Имя и размер жесткого диска . . . . .	9
3.7	Установка контроллера IDE . . . . .	9
3.8	Выбор языка системы . . . . .	10
3.9	Настройка часового пояса . . . . .	10
3.10	Настройка клавиатуры . . . . .	11
3.11	Выбор программ . . . . .	11
3.12	Отключение KDUMP . . . . .	12
3.13	Место установки ОС . . . . .	12
3.14	Включение сетевого соединения . . . . .	13
3.15	Пароль для root-пользователя . . . . .	13
3.16	Пароль для обычного пользователя . . . . .	14
3.17	Установка ОС . . . . .	14
3.18	Установка ОС . . . . .	15
3.19	Подключение образа диска дополнений гостевой ОС . . . . .	15
3.20	Подключение образа диска дополнений гостевой ОС . . . . .	16
3.21	Проверка имени хоста . . . . .	16
3.22	Анализ последовательности загрузки системы . . . . .	17
3.23	Версия ядра Linux . . . . .	17
3.24	Частота процессора . . . . .	17
3.25	Модель процессора . . . . .	17
3.26	Объем доступной оперативной памяти . . . . .	18
3.27	Тип обнаруженного гипервизора . . . . .	18
3.28	Тип файловой системы и последовательность монтирования . . . . .	18

# 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

Установка операционной системы Linux, дистрибутив Rocky.

### 3 Выполнение лабораторной работы

Начинаем создание новой виртуальной машины, указываем тип и имя ОС. В моем случае имя ОС такое же как логин для работы в ДК. (рис. 3.1).

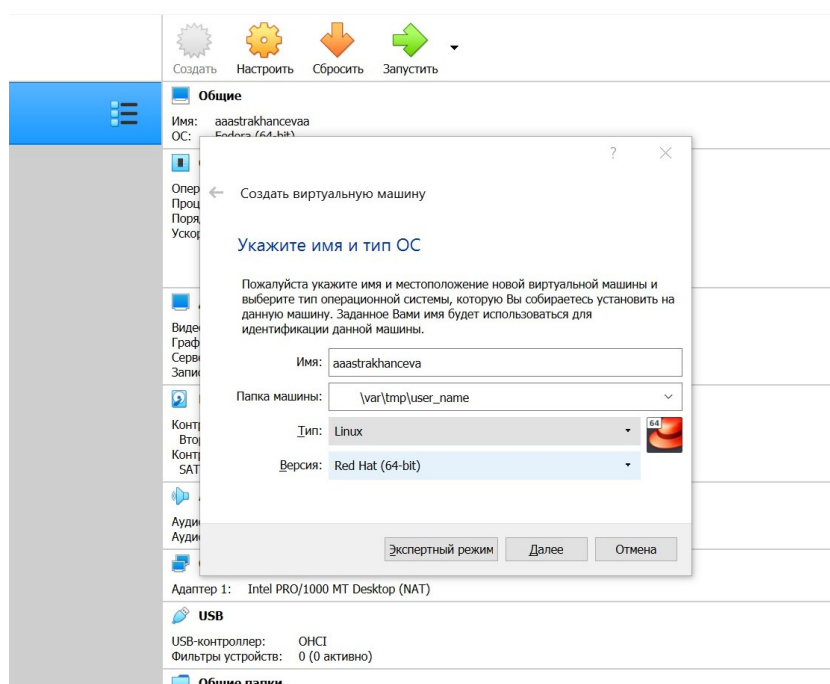


Рис. 3.1: Тип и имя ОС

Указываем объем памяти. Указываем 2048 МБ. (рис. 3.2).

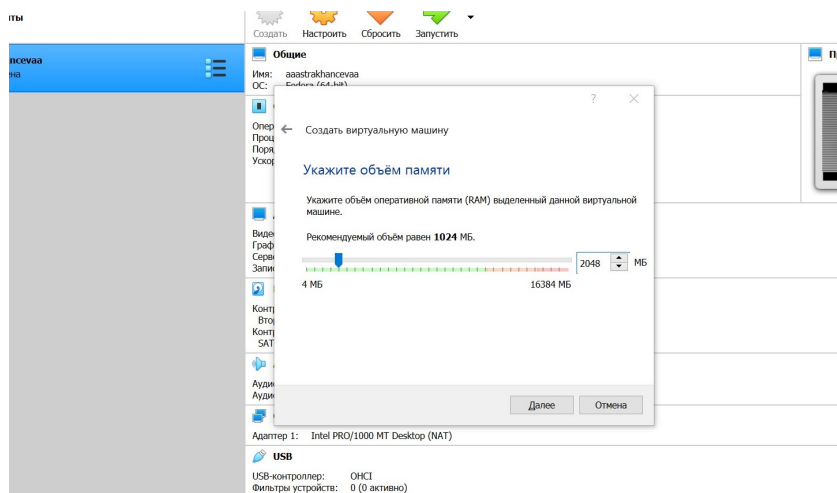


Рис. 3.2: Объем памяти

Создаем новый виртуальный жесткий диск (рис. 3.3).

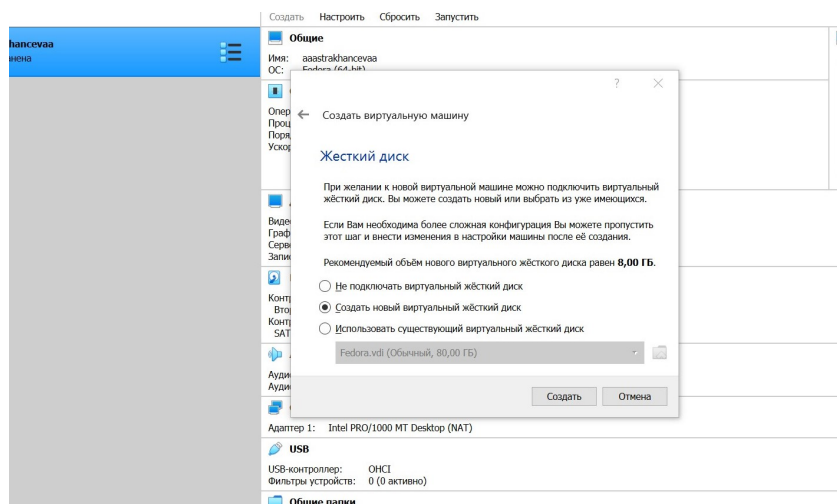


Рис. 3.3: Жесткий диск

Указываем тип виртуального жесткого диска (рис. 3.4).

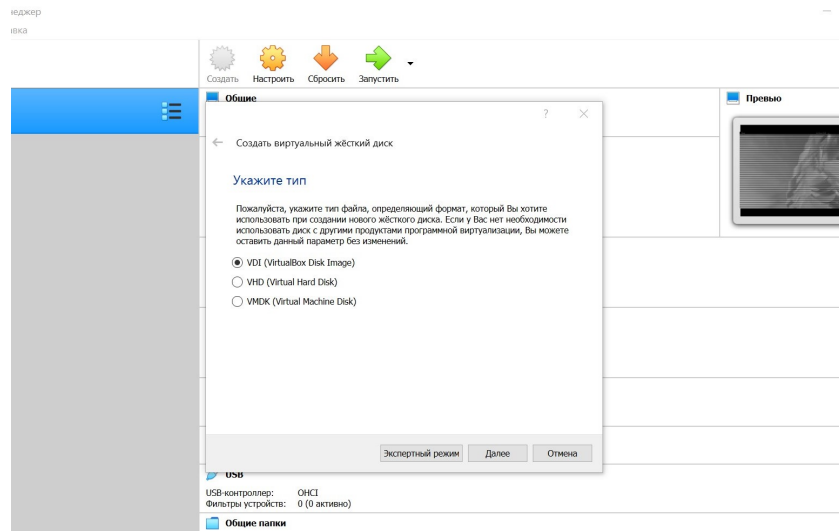


Рис. 3.4: Тип жесткого диска

Указываем формат хранения (рис. 3.5).

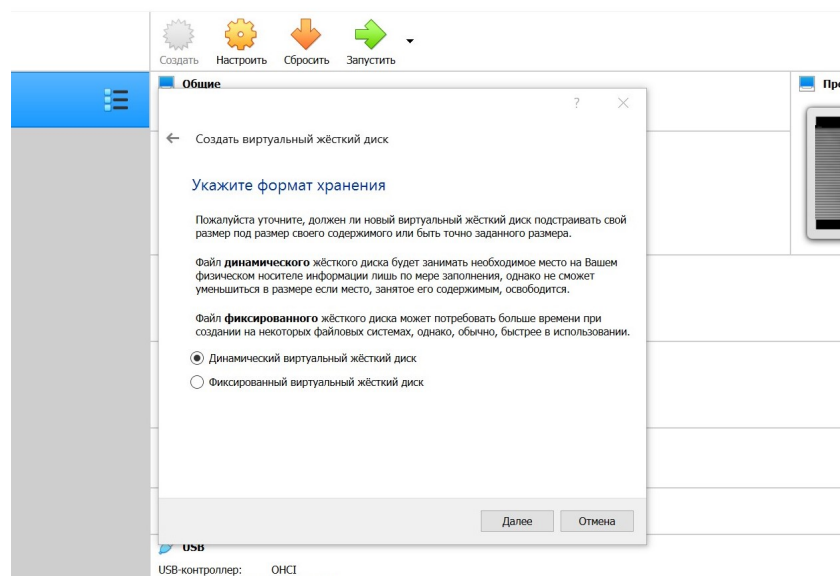


Рис. 3.5: Формат хранения

Указываем имя и размер нового виртуального жесткого диска. Выбираем 40 ГБ (рис. 3.6).



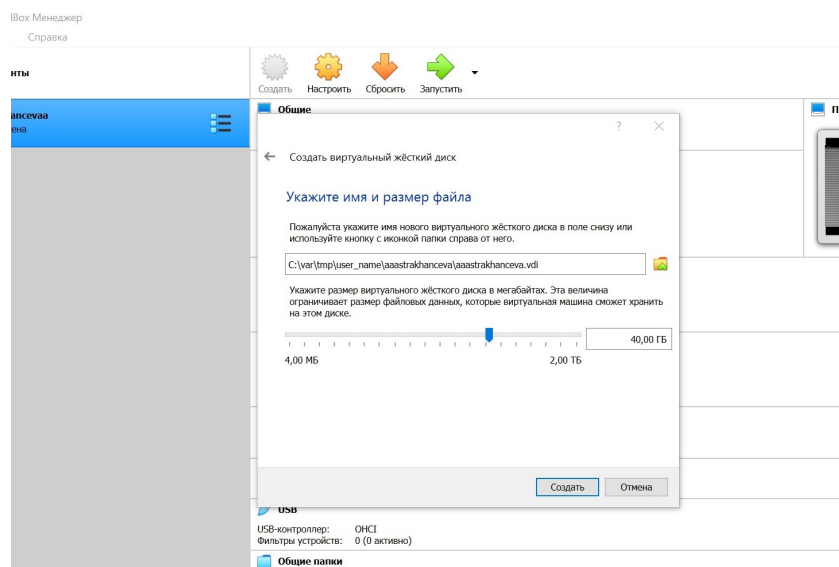


Рис. 3.6: Имя и размер жесткого диска

Далее необходимо было в настройках в разделе “Носители” выбрать контроллер IDE. Для этого нужно было предварительно установить Rocky в dvd формате. (рис. 3.7).

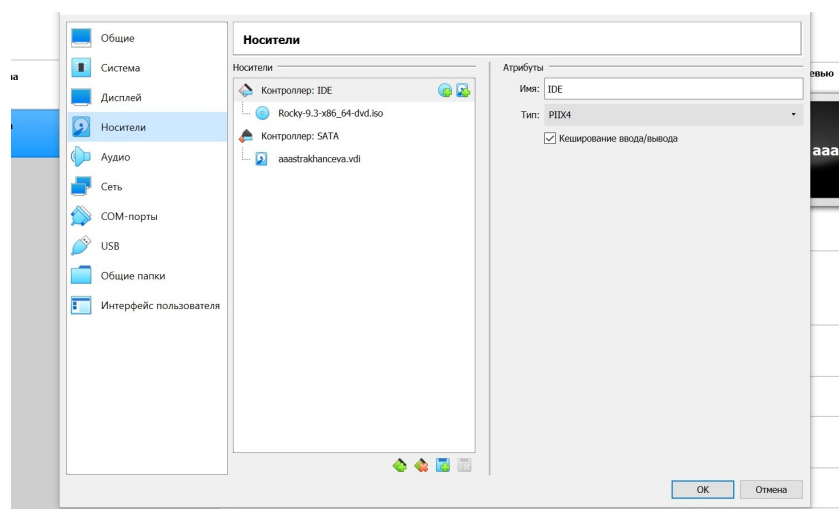


Рис. 3.7: Установка контроллера IDE

Запускаем виртуальную машину. Выбираем английский язык по умолчанию для всей системы (рис. 3.8).

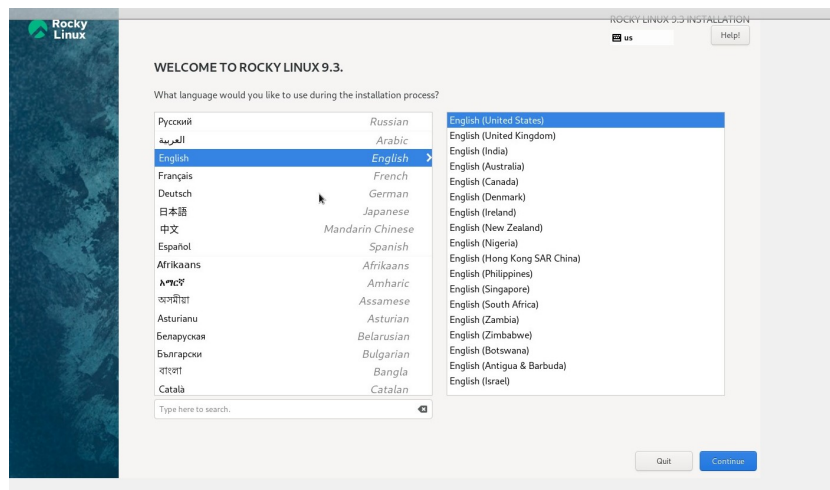


Рис. 3.8: Выбор языка системы

Настраиваем часовой пояс (рис. 3.9).

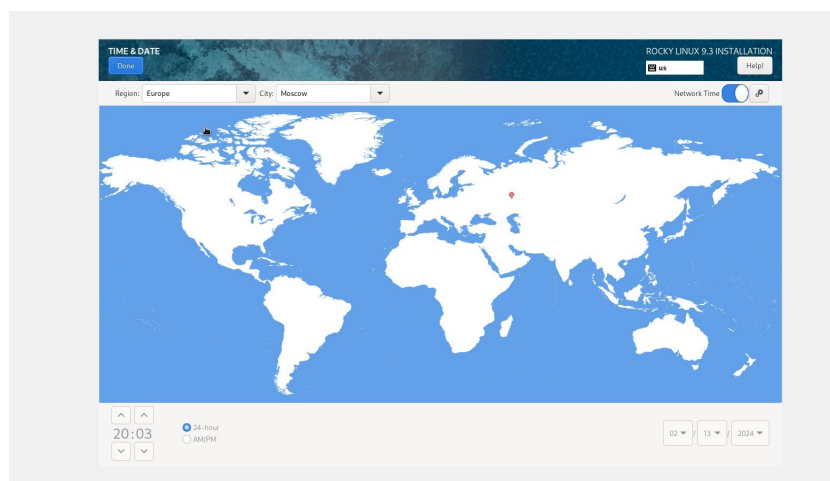


Рис. 3.9: Настройка часового пояса

Добавляем русскую раскладку клавиатуры. Настраиваем сочетание клавиш для переключения между клавиатурами (рис. 3.10).

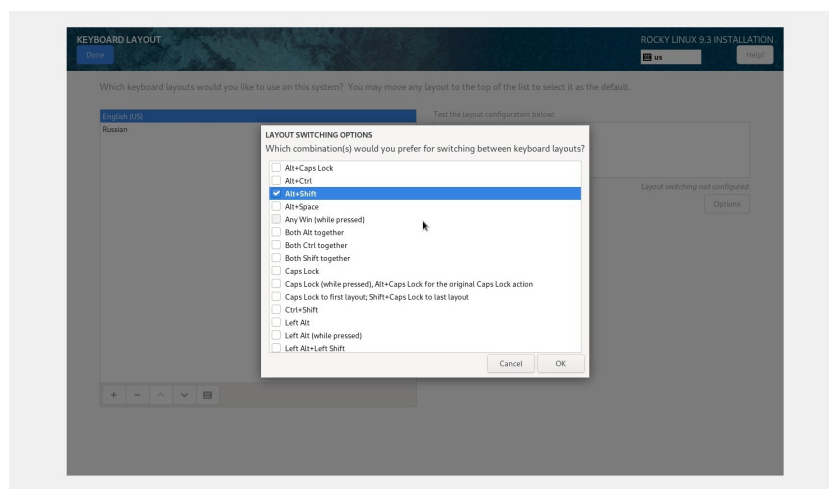


Рис. 3.10: Настройка клавиатуры

В разделе выбора программ указываем в качестве базового окружения Server with GUI, а в качестве дополнения — Development Tools (рис. 3.11).

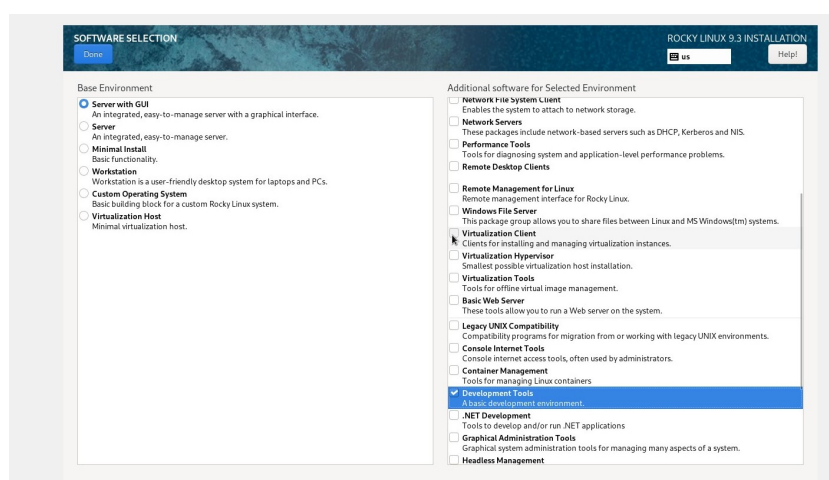


Рис. 3.11: Выбор программ

Отключаем KDUMP (рис. 3.12).

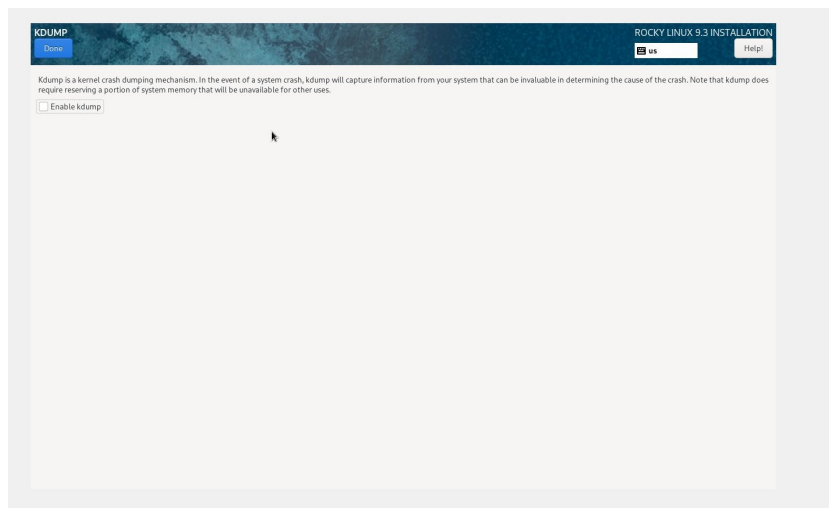


Рис. 3.12: Отключение KDUMP

Место установки ОС оставляем без изменения (рис. 3.13).

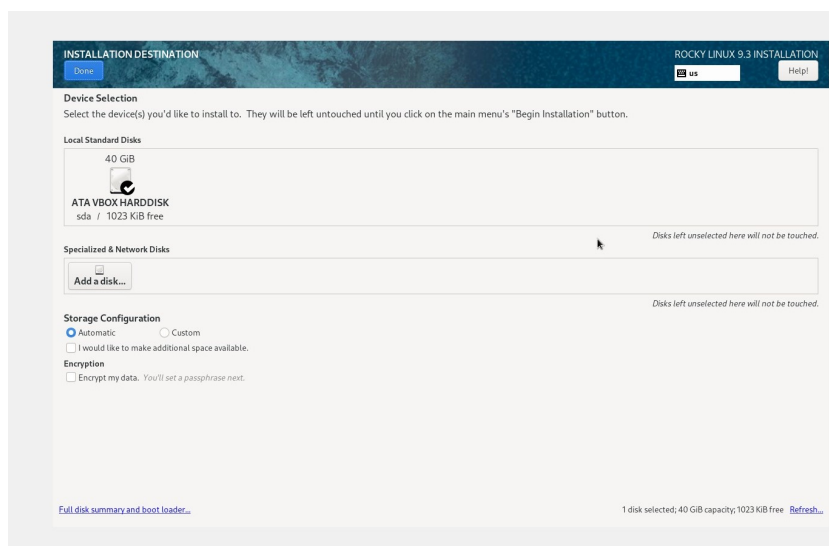


Рис. 3.13: Место установки ОС

Включаем сетевое соединение и в качестве имени узла указываем `user.localdomain`, где вместо `user` указываем имя пользователя в соответствии с соглашением об именовании. (рис. 3.14).

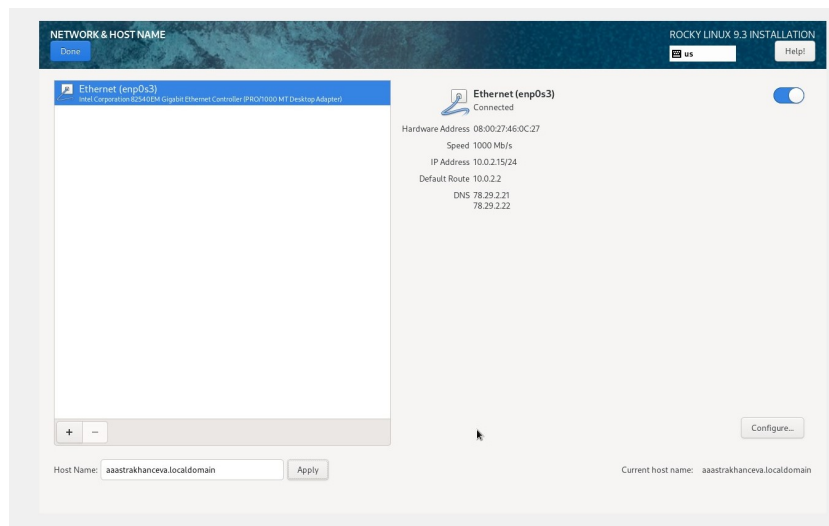


Рис. 3.14: Включение сетевого соединения

Указываем пароль для root-пользователя (рис. 3.15).

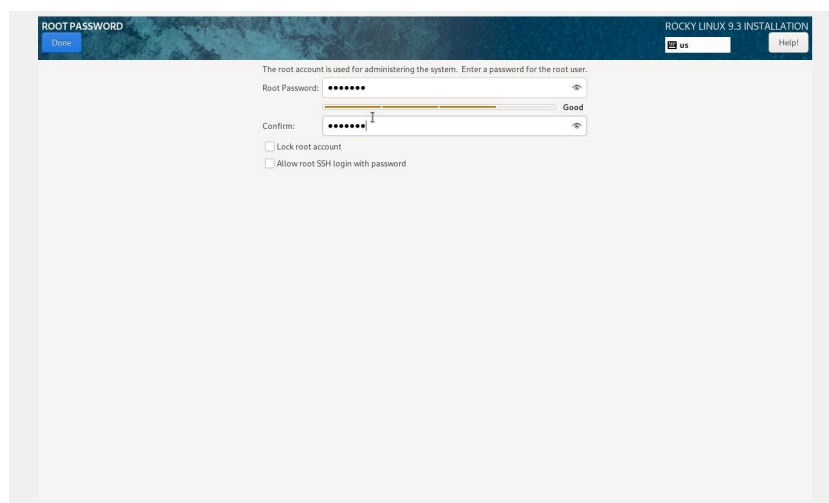


Рис. 3.15: Пароль для root-пользователя

Указываем пароль для обычного пользователя (рис.3.16).

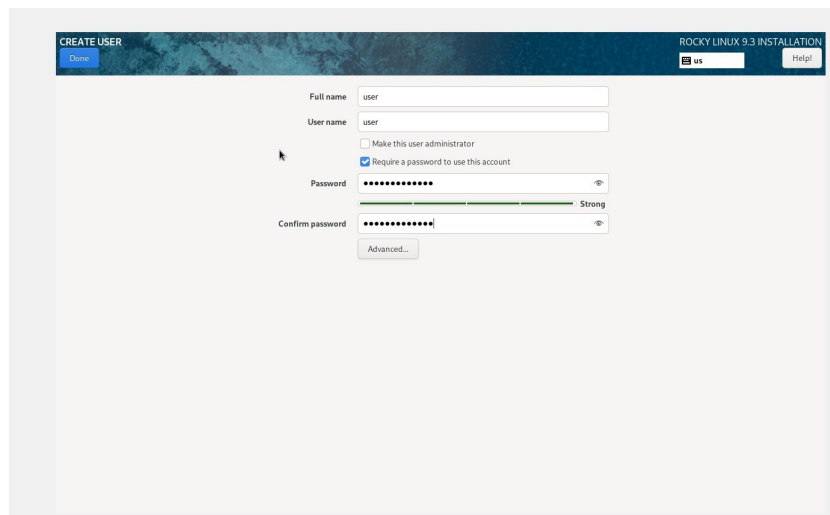
The image shows the 'CREATE USER' screen in the Rocky Linux 9.3 installation environment. The interface has a dark blue header with the 'Rocky Linux' logo on the left and 'ROCKY LINUX 9.3 INSTALLATION' on the right, including a language selector set to 'us' and a 'Help!' link. The main area is light gray and contains several input fields: 'Full name' with 'user' entered, 'User name' with 'user' entered, a checkbox for 'Make this user administrator' (unchecked), and a checked checkbox for 'Require a password to use this account'. Below these are 'Password' and 'Confirm password' fields, both filled with masked characters. A strength indicator for the password shows a green bar and the word 'Strong'. An 'Advanced...' button is located below the confirm password field.

Рис. 3.16: Пароль для обычного пользователя

Далее запускаем установку операционной системы и после этого перезагружаем виртуальную машину (рис.3.17).



Рис. 3.17: Установка ОС

Далее нужно проверить, что в настройках в разделе “Носители” в контроллере IDE пусто (рис. 3.18).

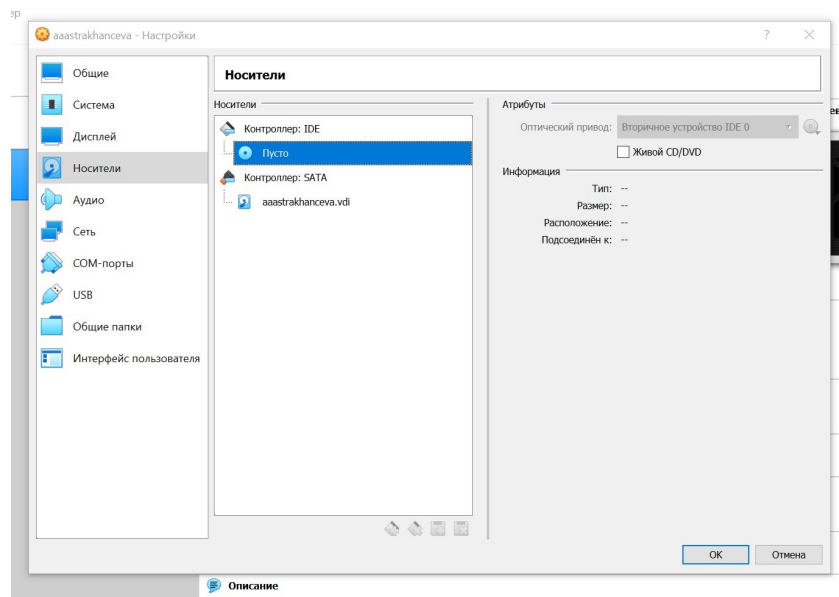


Рис. 3.18: Установка ОС

Далее после входа в ОС в меню Устройства виртуальной машины подключаем образ диска дополнений гостевой ОС (рис.3.19).

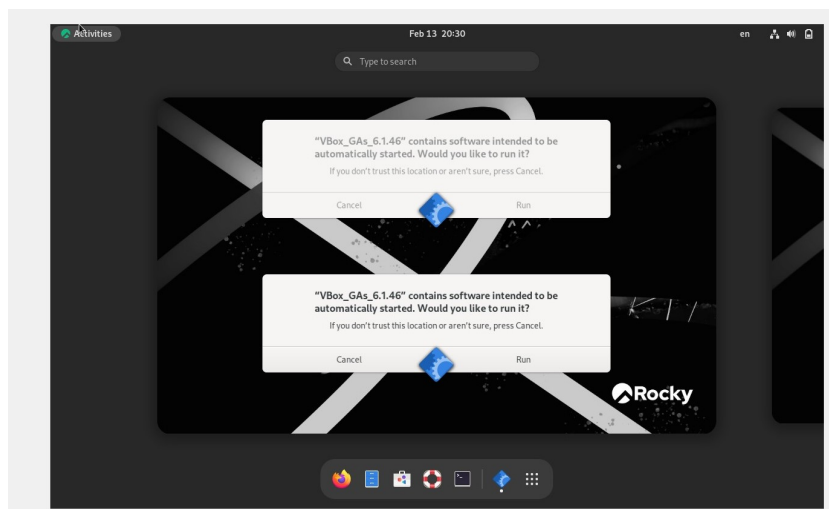


Рис. 3.19: Подключение образа диска дополнений гостевой ОС

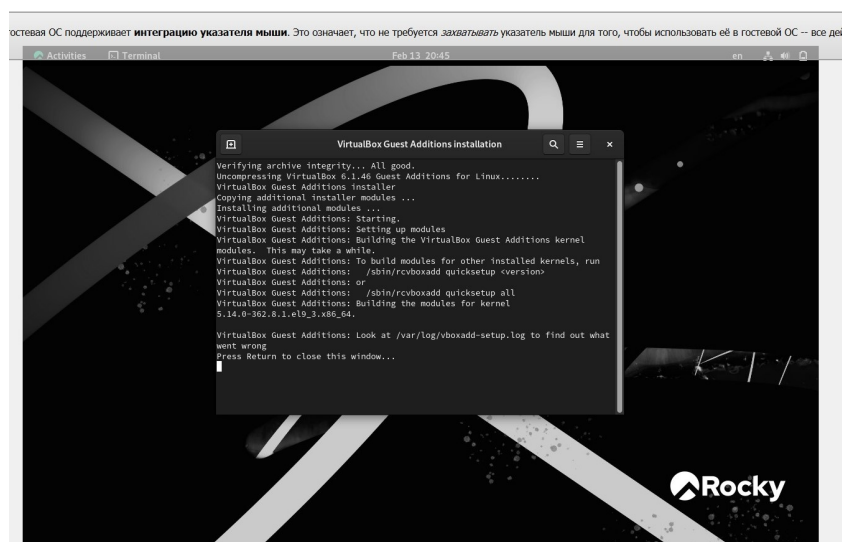


Рис. 3.20: Подключение образа диска дополнений гостевой ОС

Далее проверяем, что имя хоста установлено верно (рис.3.21).

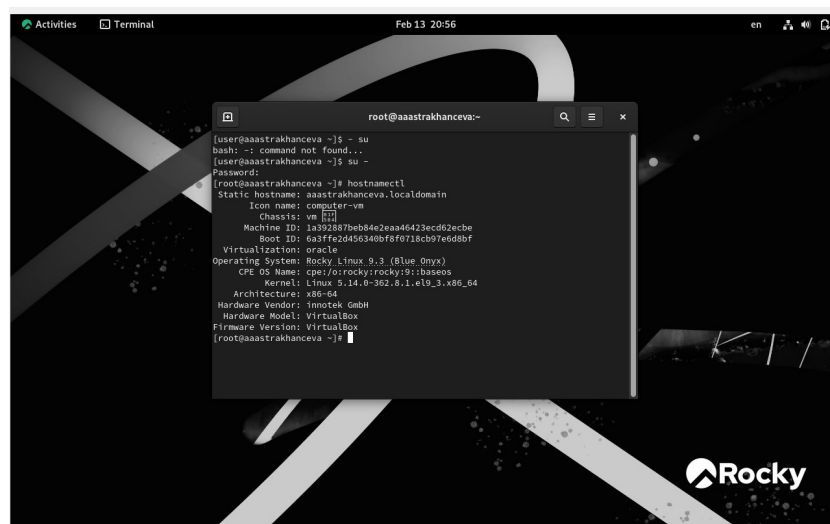


Рис. 3.21: Проверка имени хоста

### 3.1 Домашнее задание

После загрузки графического окружения открываем терминал. В окне терминала с помощью команды `dmesg` анализируем последовательность загрузки системы. (рис. 3.22).



```
root@aaastrakhanceva:~# dmesg
[ 0.000000] Linux version 5.14.0-362.8.1.el9_3.x86_64 (mockbuild@ad1-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 Ecosystem 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/rl-root resume=/dev/mapper/rl-swap rd.lvm.lv=rl/r
oot 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 0x0000000000000000-0x0000000000000bfff] usable
[ 0.000000] BIOS-e820: [mem 0x0000000000000c00-0x0000000000000ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x000000000000f000-0x0000000000000ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x0000000000100000-0x0000000000000ffff] usable
[ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x0000000000000ffff] ACPI data
[ 0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] 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 msrc 4b564d01 and 4b564d00
[ 0.000000] kvm-clock: using sched offset of 384338479 cycles
[ 0.000000] clocksource: kvm-clock: mask: 0xffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881590591483 ns
[ 0.000000] tsc: Detected 2112.000 Mhz processor
[ 0.01483] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[ 0.01483] e820: remove [mem 0x00000000-0x00000fff] usable
[ 0.01494] last_pfn = 0x7ffff0 max_arch_pfn = 0x400000000
[ 0.01500] Disabled
[ 0.01510] x86/PAT: MTRRs disabled, skipping PAT initialization too.
[ 0.01513] CPU MTRRs all blank - virtualized system.
[ 0.01515] x86/PAT: Configuration [0-7]: WB WT UC- UC WB WT UC- UC
[ 0.01589] found SMP MP-table at [mem 0x00000fff-0x00009fff]
[ 0.01612] RAMDISK: [mem 0x31021000-0x34808fff]
[ 0.01618] ACPI: Early table checksum verification disabled
[ 0.01621] ACPI: RSDP 0x0000000000000000 000024 (v02 VBOX )
```

Рис. 3.22: Анализ последовательности загрузки системы

Получите следующую информацию:

1. Версия ядра Linux (Linux version) (рис.3.23).

```
root@aaastrakhanceva:~# dmesg | less
root@aaastrakhanceva:~# dmesg | grep -i "Linux version"
[ 0.000000] Linux version 5.14.0-362.8.1.el9_3.x86_64 (mockbuild@ad1-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
root@aaastrakhanceva:~#
```

Рис. 3.23: Версия ядра Linux

2. Частота процессора (Detected Mhz processor) (рис. 3.24).

```
root@aaastrakhanceva:~# dmesg | grep -i "Mhz processor"
[ 0.000000] tsc: Detected 2112.000 Mhz processor
root@aaastrakhanceva:~# dmesg | grep -i "processor"
[ 0.000000] tsc: Detected 2112.000 Mhz processor
[ 0.184964] smpboot: Total of 1 processors activated (4224.00 BogoMIPS)
[ 0.230167] ACPI: Added _OSI(Processor Device)
[ 0.230168] ACPI: Added _OSI(Processor Aggregator Device)
root@aaastrakhanceva:~#
```

Рис. 3.24: Частота процессора

3. Модель процессора (CPU0) (рис.3.25).

```
[ 0.555801] intel_pstate: CPU model not supported
root@aaastrakhanceva:~# dmesg | grep -i "CPU0"
[ 0.184605] smpboot: CPU0: Intel(R) Core(TM) i7-8665U CPU @ 1.90GHz (family: 0x6, model: 0x8e, stepping: 0xc)
root@aaastrakhanceva:~#
```

Рис. 3.25: Модель процессора

4. Объем доступной оперативной памяти (Memory available) (рис. 3.26).

```
root@baastrahkaneva:~# dmesg | grep -i "Memory available"
root@baastrahkaneva:~# dmesg | grep -i "Memory"
0.001855 ACPI: Reserving FACP table memory at [mem 0x7fff00f0-0x7fff00e3]
0.001857 ACPI: Reserving DSDT table memory at [mem 0x7fff0470-0x7fff0274]
0.001861 ACPI: Reserving FACS table memory at [mem 0x7fff0200-0x7fff023f]
0.001859 ACPI: Reserving FACS table memory at [mem 0x7fff0200-0x7fff023f]
0.001860 ACPI: Reserving APIC table memory at [mem 0x7fff0420-0x7fff0253]
0.001861 ACPI: Reserving SSDT table memory at [mem 0x7fff0240-0x7fff040b]
0.002358 Early memory node ranges
0.003737 PM: hibernation: Registered nosave memory: [mem 0x00000000-0x000000ff]
0.003740 PM: hibernation: Registered nosave memory: [mem 0x0000f000-0x0000ffff]
0.003741 PM: hibernation: Registered nosave memory: [mem 0x00000000-0x0000ffff]
0.003741 PM: hibernation: Registered nosave memory: [mem 0x00000000-0x0000ffff]
0.014151 Memory: 2686860/2966968 available (16384k kernel code, 5596k rwdata, 11444k rodata, 3824k init, 18424k bss, 157764k reserved, 0K cma-reserved)
0.025125 Freeing SWP alternate memory: 36k
0.193513 x86/mem: 16384k size: 128MB
0.494218 Non-volatile memory driver v1.3
1.728544 Freeing initrd memory: 57248k
1.932577 Freeing unused decrypted memory: 2036k
1.951860 Freeing unused kernel image (initmem): 3824k
1.958430 Freeing unused kernel image (rodata/data gap): memory: 844k
3.036740 vmwgfx 0000:02:00.0: [drm] Legacy memory limits: VMW = 16384 kB, P10 = 2048 kB, surface = 507904 kB
3.118840 vmwgfx 0000:02:00.0: [drm] Maximum display memory size is 16384 KiB
root@baastrahkaneva:~#
```

Рис. 3.26: Объем доступной оперативной памяти

5. Тип обнаруженного гипервизора (Hypervisor detected) (рис. 3.27).

```
[ 3.118840] vmwgfx 0000:00:02.0: [drm] Maximum display memory size is 16384 KiB
[root@aaastrakhanceva ~]# dmesg | grep -i "Hypervisor detected"
[ 0.000000] Hypervisor detected: KVM
[root@aaastrakhanceva ~]#
```

Рис. 3.27: Тип обнаруженного гипервизора

## 6. Тип файловой системы корневого раздела

7. Последовательность монтирования файловых систем (рис. 3.28).

```

Activities Terminal Feb 23 11:11 en
root@basastrakhanceva:~
root@basastrakhanceva:~# lsblk -f
NAME        FSTYPE      FSVER      LABEL      UUID                                  FSAVAIL  FSSUEN  MOUNTPOINTS
nvd         xfs
sda1        xfs                                     bbd3d757-4d56-4071-abb6-047a97826ac1  693.4M   28% /boot
sda2        xfs_member LVM2 001    a5HC3-b1ja-w1ko-Uduw-cH3R-wkK-1B80f1 1726f3cd-7ba3-46db-b1bb-fbbe4735e1d2  31.7G   14% /
l-rwmap swp 1                                     8292c6db-244e-4a84-9c47-4cb569704b04 [SWAP]
sro         iso9660      Joliet Extension VBox_GS_6.1.46 2023-07-12-17-05-32-49 0 100% /run/media/user/VBox_GS_6.1.46

root@basastrakhanceva:~# dmesg | grep -i "file system"
1.740850s systemd[1]: Reached target Initrd Jusr File System.
1.452165s systemd[1]: Set up automount Arbitrary Executable File Formats File System Automount Point.
5.452493s systemd[1]: Stopped target Initrd File System.
5.453536s systemd[1]: Stopped target Initrd Root File System.
5.468066s systemd[1]: Mounting Huge Pages File System...
5.474243s systemd[1]: Mounting POSIX Message Queue File System...
5.484823s systemd[1]: Mounting Kernel Debug File System...
5.490150s systemd[1]: Mounting Kernel Trace File System...
5.564864s systemd[1]: Starting File System Check on Root Device.
5.628851s systemd[1]: Starting Remount Root and Kernel File System...
5.703342s systemd[1]: Mounted Huge Pages File System.
5.707157s systemd[1]: Mounted POSIX Message Queue File System.
5.709328s systemd[1]: Mounted Kernel Debug File System.
5.709662s systemd[1]: Mounted Kernel Trace File System.

root@basastrakhanceva:~# dmesg | grep -i "fstype"
root@basastrakhanceva:~# dmesg | grep -i "mount"
0.061076s Mount-cache hash table entries: 4096 (order: 3, 32768 bytes, linear)
0.061883s Mountpoint-cache hash table entries: 4096 (order: 3, 32768 bytes, linear)
4.388210s XFS (dm-0): Mounting VS Filesystem
4.406377s XFS (dm-0): Ending clean mount
4.454523s systemd[1]: Set up automount Arbitrary Executable File Formats File System Automount Point.
5.468066s systemd[1]: Mounting Huge Pages File System...
5.474243s systemd[1]: Mounting POSIX Message Queue File System...
5.484823s systemd[1]: Mounting Kernel Debug File System...
5.490150s systemd[1]: Mounting Kernel Trace File System...
5.628851s systemd[1]: Starting Remount Root and Kernel File System...
5.703342s systemd[1]: Mounted Huge Pages File System.
5.707157s systemd[1]: Mounted POSIX Message Queue File System.
5.709328s systemd[1]: Mounted Kernel Debug File System.
5.709662s systemd[1]: Mounted Kernel Trace File System.
8.495027s XFS (sda1): Mounting VS Filesystem
9.495010s XFS (sda1): Ending clean mount

root@basastrakhanceva:~#

```

Рис. 3.28: Тип файловой системы и последовательность монтирования

## Контрольные вопросы

1. Какую информацию содержит учётная запись пользователя?

Ответ: имя пользователя, пароль (зашифрован), идентификационный номер пользователя и идентификационный номер группы пользователя, домашний каталог пользователя, командный интерпретатор пользователя.

2. Укажите команды терминала и приведите примеры:

Ответ:

для получения справки по команде - man

для перемещения по файловой системе - cd - переход в домашний каталог, cd - переход к определенному каталогу

для просмотра содержимого каталога - ls

для создания каталогов - mkdir

для создания файлов - touch

для удаления каталогов - rm

для удаления файлов - rm -r

для задания определённых прав на файл / каталог - chmod

для просмотра истории команд - history

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

Файловая система (ФС) - часть операционной системы, представляющая собой совокупность организованных наборов данных, хранящихся на внешних запоминающих устройствах и программных средств, гарантирующих именованный доступ к этим данным и их защиту. Данные называются файлами, их имена - именами файлов.

Ext2, Ext3, Ext4 - является стандартом для Linux. Как следствие, это самые распространенные системы. Они редко обновляются, но зато стабильны. Ext2 создавалась специально под Linux

JFS - Журналируемая ФС — первая альтернатива для ФС группы Ext. Ее разработали в IBM специально для операционной системы AIX UNIX. Главные плюсы этой системы: стабильность и минимальные требования для работы.

ReiserFS - Подходит исключительно под Linux, чаще всего ее используют в качестве возможной замены Ext3. Главные особенности: увеличенная производительность и более широкие возможности.

XFS - Еще одна журналируемая ФС. Однако, в отличие от аналогов, в логи записывает исключительно те изменения, которые претерпевают метаданные. Разработана для ОС в Silicon Graphics. Важные особенности: быстро работает с файлами сравнительно большого размера, умеет выделять место в отложенном режиме, а также менять размеры разделов в процессе работы.

Btrfs - Современная ФС, главной особенностью которой является высокая отказоустойчивость. Из дополнительных «бонусов»: удобна для сисадминов и поддерживает сравнительно простой процесс восстановления данных.

4. Как посмотреть, какие файловые системы подмонтированы в ОС? Ввести команду `mount`
5. Как удалить зависший процесс? Ввести команду `kill`

## 4 Выводы

В ходе выполнения лабораторной работы я приобрела практические навыки установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов.