

Лабораторная работа 1

Основы информационной безопасности

Наговицын А. В.

22.02.25

Российский университет дружбы народов, Москва, Россия

Информация

- Наговицын А. В.
- Студент, 2 курс, группа НКАбд-03-23
- Российский университет дружбы народов
- [1132239111@pfur.ru]
- <https://github.com/AVNagov>

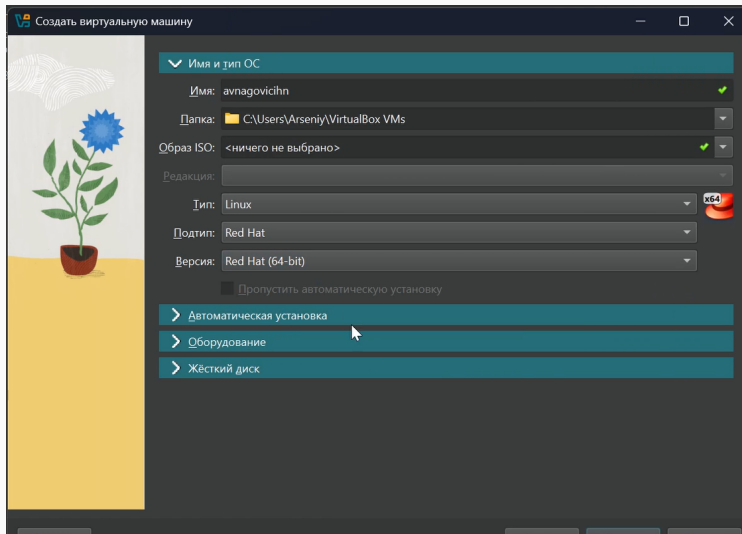
Вводная часть

Приобретение практических навыков установки операционной системы на виртуальную машину,настройки минимально необходимых для дальнейшей работы сервисов.

1. Настройка виртуальной машины
2. Установка Linux Rocky
3. Установка драйверов
4. Домашнее задание

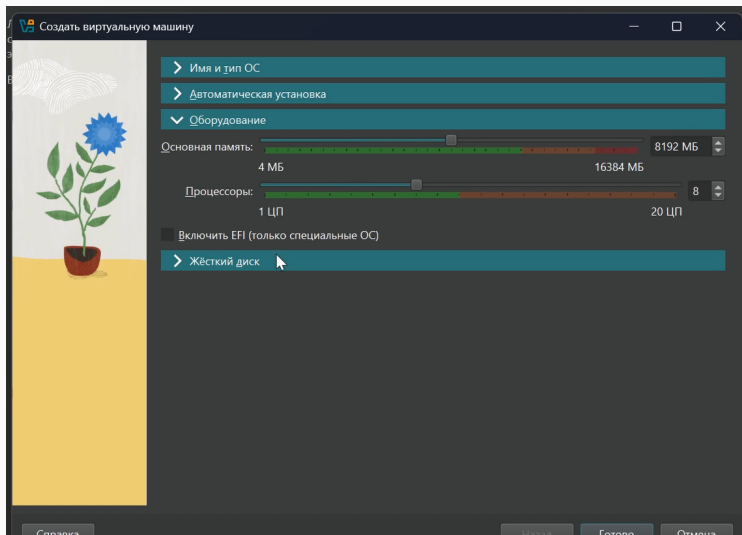
Выполнение лабораторной работы

Создаю виртуальную машину и выбираю систему RedHat



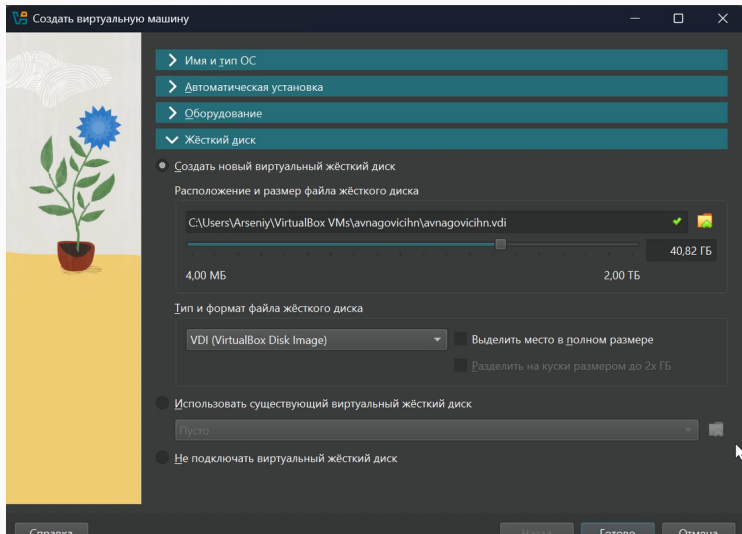
Настройка виртуальной машины

Настраиваю количество ОЗУ и количество ядер процессора



Настройка виртуальной машины

Создаю и настраиваю новый жесткий диск



Подключаю iso-образец системы Rocky

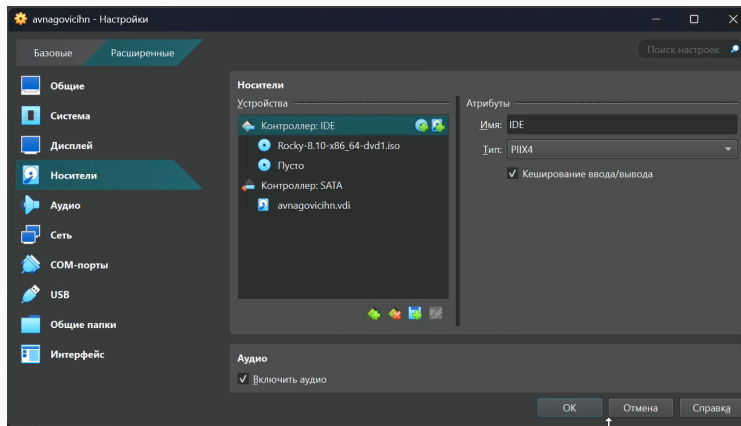
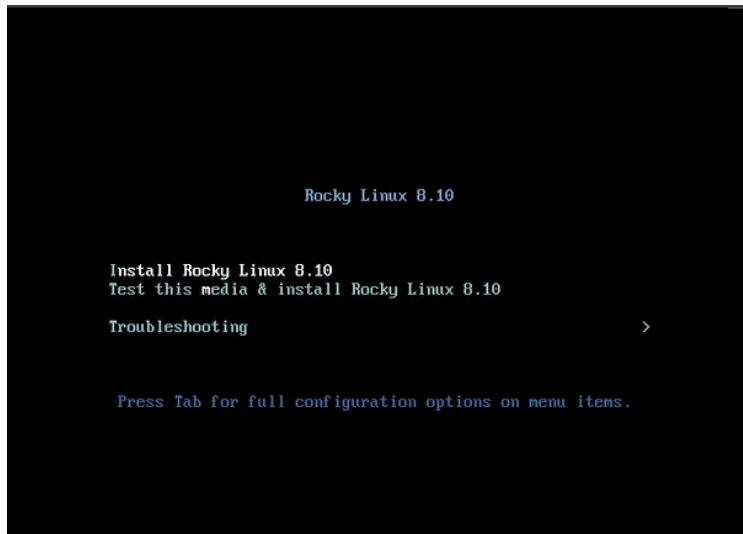


Рис. 4: Настройка оборудования виртуальной машины

Выбираю в меню установки, установку системы Linux Rocky



Выбираю в меню установки язык

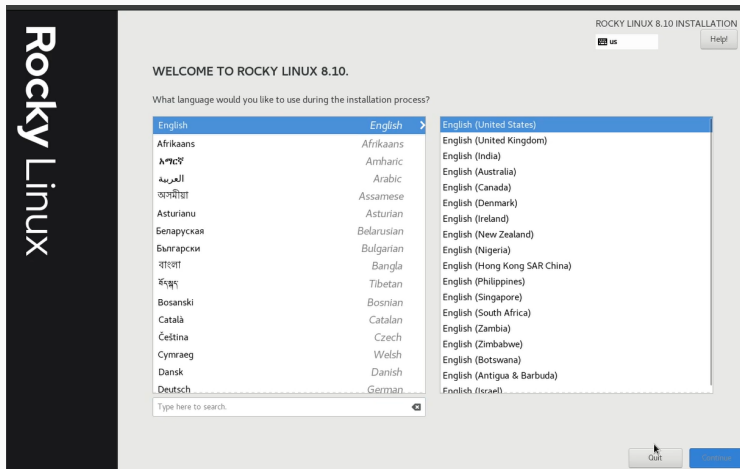


Рис. 6: Выбор языка установки

Перехожу к настройке жесткого диска

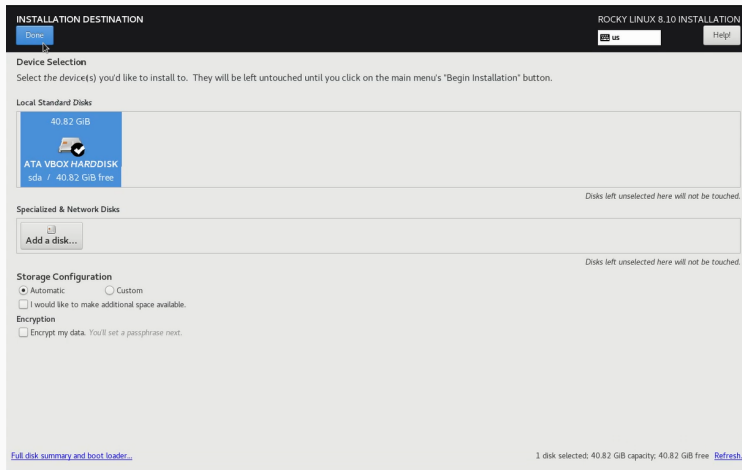
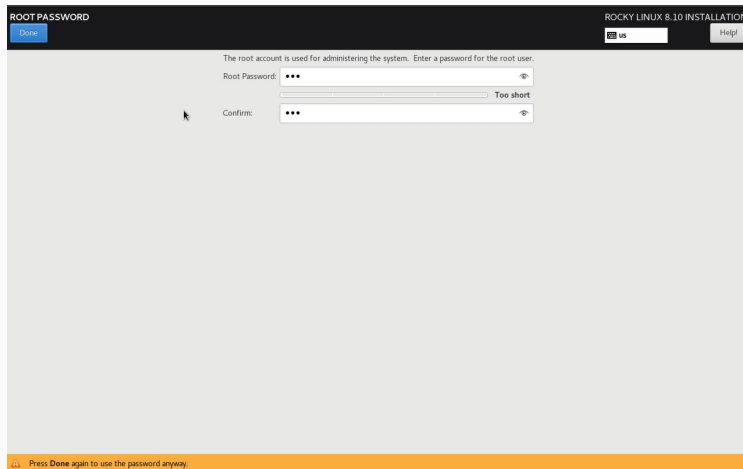


Рис. 7: Выбор жесткого диска для установки

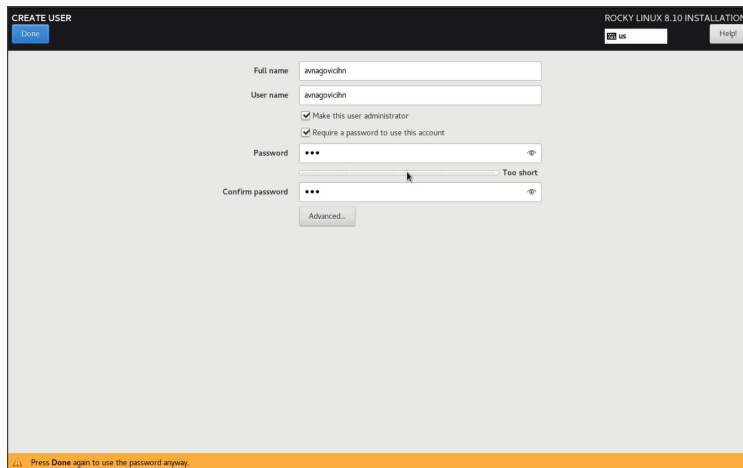
Устанавливаю пароль root



The screenshot shows the 'ROOT PASSWORD' screen in the Rocky Linux 8.10 installation process. The title bar at the top left says 'ROOT PASSWORD' with a 'Done' button. The top right says 'ROCKY LINUX 8.10 INSTALLATION' with a language selector set to 'en' and a 'Help!' button. The main text reads: 'The root account is used for administering the system. Enter a password for the root user.' Below this, there are two password input fields. The first is labeled 'Root Password:' and contains three dots. It has a visibility icon on the right and a feedback message 'Too short' below it. The second is labeled 'Confirm:' and also contains three dots with a visibility icon on the right. At the bottom, an orange banner contains a warning icon and the text: 'Press Done again to use the password anyway.'

Рис. 8: Установка пароля root

Создаю пользователя



The image shows the 'CREATE USER' screen during the Rocky Linux 8.10 installation. The interface is dark-themed. At the top left, it says 'CREATE USER' with a 'Done' button. At the top right, it says 'ROCKY LINUX 8.10 INSTALLATION' with a language selector set to 'en us' and a 'Help!' button. The main area contains the following fields and options:

- 'Full name' field with the value 'avagovicin'.
- 'User name' field with the value 'avagovicin'.
- Two checked checkboxes: 'Make this user administrator' and 'Require a password to use this account'.
- 'Password' field with masked characters '***'. Below it is a progress bar indicating password strength, with a tooltip that says 'Too short'.
- 'Confirm password' field with masked characters '***'.
- An 'Advanced...' button below the password fields.

At the bottom of the screen, there is an orange banner with a warning icon and the text: 'Press Done again to use the password anyway.'

Рис. 9: Создание пользователя

Выключаю KDUMP

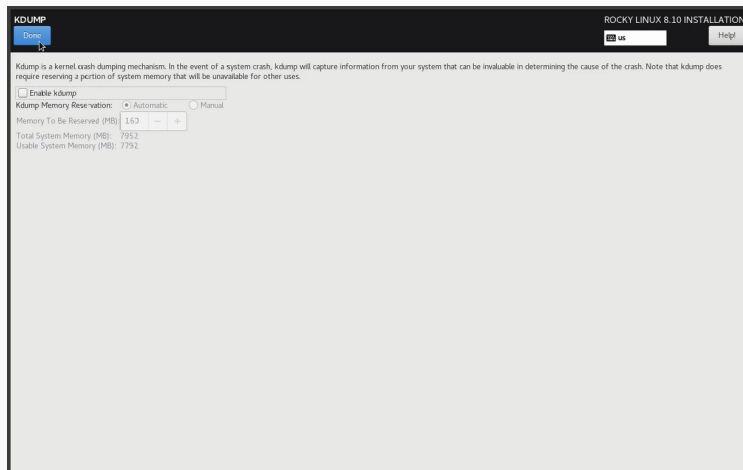


Рис. 10: Настройка KDUMP

Включаю инструменты разработки для установки Linux Rocky

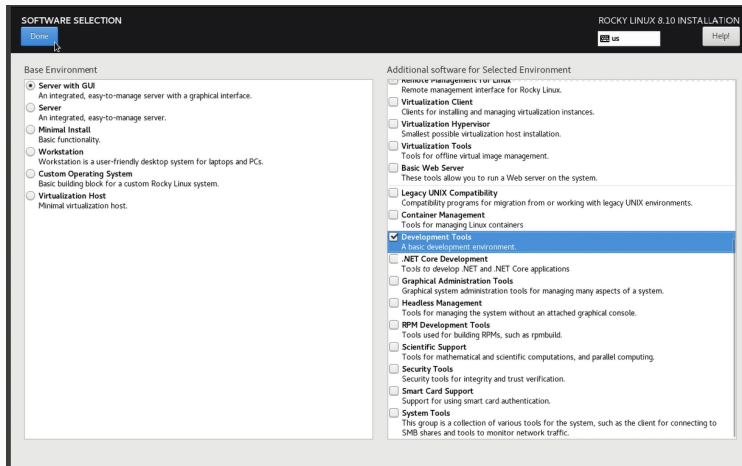


Рис. 11: Выбор программного обеспечения

Включаю свою сеть

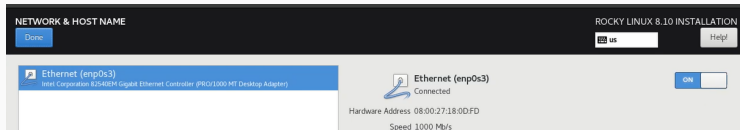


Рис. 12: Настройка сети

Установка завершена



Рис. 13: Завершение установки

Принимаю лицензионное соглашение

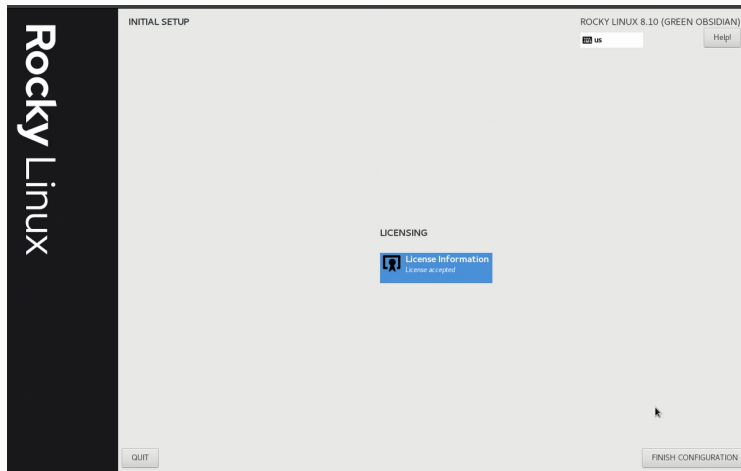
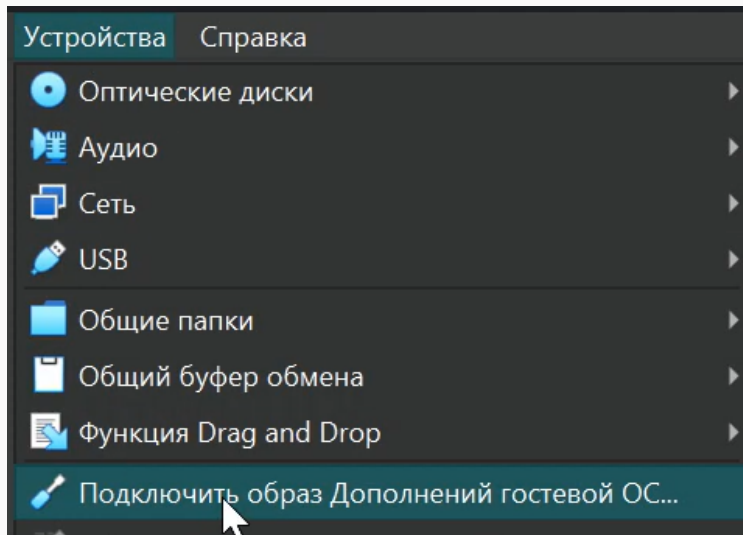


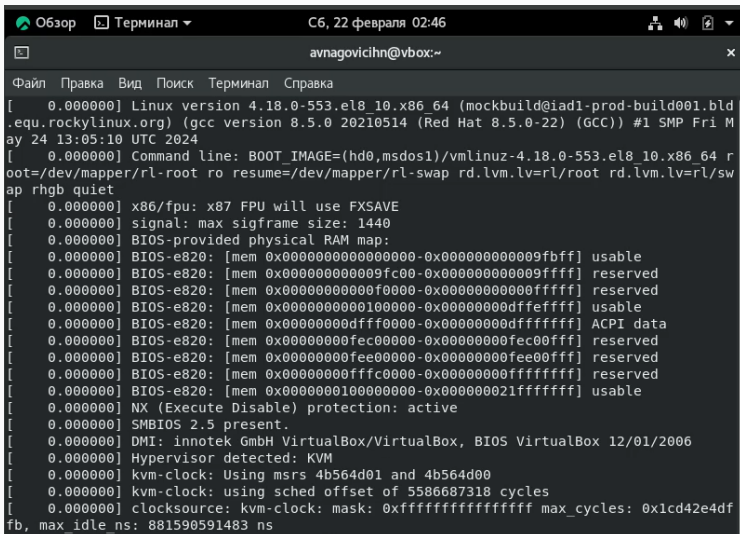
Рис. 14: Прием лицензии

Нажимаю устройства->Подключить образ Дополнений гостевой ОС



Домашнее задание

Ввожу команду dmesg | less



```
Обзор Терминал C6, 22 февраля 02:46
avnagovicnh@vbox:~

Файл Правка Вид Поиск Терминал Справка
[ 0.000000] Linux version 4.18.0-553.el8_10.x86_64 (mockbuild@iad1-prod-build001.bld
.equ.rockylinux.org) (gcc version 8.5.0 20210514 (Red Hat 8.5.0-22) (GCC)) #1 SMP Fri M
ay 24 13:05:10 UTC 2024
[ 0.000000] Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-4.18.0-553.el8_10.x86_64 r
oot=/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: x87 FPU will use FXSAVE
[ 0.000000] signal: max sigframe size: 1440
[ 0.000000] BIOS-provided physical RAM map:
[ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] usable
[ 0.000000] BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000000100000-0x000000000000dffff] usable
[ 0.000000] BIOS-e820: [mem 0x00000000000dfff0000-0x00000000000dfffffff] ACPI data
[ 0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000100000000-0x0000000021fffffff] usable
[ 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
[ 0.000000] kvm-clock: using sched offset of 5586687318 cycles
[ 0.000000] clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4df
fb, max_idle_ns: 881590591483 ns
```

Ввожу команду dmesg

```
[avnagovicihn@vbox ~]$ dmesg
[ 0.000000] Linux version 4.18.0-553.el8_10.x86_64 (mockbuild@iad1-prod-build001.bld
.equ.rockylinux.org) (gcc version 8.5.0 20210514 (Red Hat 8.5.0-22) (GCC)) #1 SMP Fri M
ay 24 13:05:10 UTC 2024
[ 0.000000] Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-4.18.0-553.el8_10.x86_64 r
oot=/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: x87 FPU will use FXSAVE
[ 0.000000] signal: max sigframe size: 1440
[ 0.000000] BIOS-provided physical RAM map:
[ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] usable
[ 0.000000] BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
[ 0.000000] BIOS-e820: [mem 0x0000000000100000-0x000000000dffff] usable
[ 0.000000] BIOS-e820: [mem 0x000000000dffff0000-0x00000000dfffffff] ACPI data
[ 0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000100000000-0x0000000021fffffff] usable
[ 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
[ 0.000000] kvm-clock: using sched offset of 5586687318 cycles
[ 0.000000] clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4df
```

Рис. 17: Окно терминала

Ответы на контрольные вопросы

1. Учетная запись содержит необходимые для идентификации пользователя при подключении к системе данные, а так же информацию для авторизации и учета: системного имени (user name) (оно может содержать только латинские буквы и знак нижнее подчеркивание, еще оно должно быть уникальным), идентификатор пользователя (UID) (уникальный идентификатор пользователя в системе, целое положительное число), идентификатор группы (GID) (группа, к к-рой относится пользователь. Она, как минимум, одна, по умолчанию - одна), полное имя (full name) (Могут быть ФИО), домашний каталог (home directory) (каталог, в к-рый попадает пользователь после входа в систему и в к-ром хранятся его данные), начальная оболочка (login shell) (командная оболочка, к-рая запускается при входе в систему).

Ответы на контрольные вопросы

2. Для получения справки по команде: `—help`; для перемещения по файловой системе - `cd`; для просмотра содержимого каталога - `ls`; для определения объёма каталога - `du` ; 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`

Ответы на контрольные вопросы

3. Файловая система - это порядок, определяющий способ организации и хранения и именования данных на различных носителях информации. Примеры: FAT32 представляет собой пространство, разделенное на три части: одна область для служебных структур, форма указателей в виде таблиц и зона для хранения самих файлов. ext3/ext4 - журналируемая файловая система, используемая в основном в ОС с ядром Linux.

Ответы на контрольные вопросы

4. С помощью команды `df`, введя ее в терминале. Это утилита, которая показывает список всех файловых систем по именам устройств, сообщает их размер и данные о памяти. Также посмотреть подмонтированные файловые системы можно с помощью утилиты `mount`.

Ответы на контрольные вопросы

5. Чтобы удалить зависший процесс, вначале мы должны узнать, какой у него id: используем команду `ps`. Далее в терминале вводим команду `kill < id процесса >`. Или можно использовать утилиту `killall`, что “убьет” все процессы, которые есть в данный момент, для этого не нужно знать id процесса.

Выводы

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