

Лабораторная работа №1

Основы информационной безопасности

Машков Илья Евгеньевич

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
3.1	Настройка виртуальной машины	7
3.2	Работа с установщиком Rocky	8
3.3	Работа с Rocky	11
3.4	Домашняя работа	12
4	Ответы на контрольные вопросы	15
5	Выводы	17
	Список литературы	18

Список иллюстраций

3.1	Создание виртуальной машины.	7
3.2	Выделение ОЗУ и ядер процессора.	8
3.3	Создание диска под систему.	8
3.4	Настройка языков системы.	9
3.5	Отключение KDUMPa.	9
3.6	Включение Etherneta.	10
3.7	Создание пользователя.	10
3.8	Добавления средств для разработки к системе.	11
3.9	Лицензионное соглашение.	11
3.10	Дополнения гостевой ОС.	12
3.11	Установка дополнения гостевой ОС.	12
3.12	Вывод команды dmesg.	13
3.13	Linux version.	13
3.14	Detected MHz processor.	13
3.15	CPU0.	14
3.16	Memory available.	14
3.17	Hypervisor detected.	14
3.18	Тип файловой системы.	14
3.19	Последовательность монтирования.	14

Список таблиц

1 Цель работы

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

2 Задание

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

3 Выполнение лабораторной работы

3.1 Настройка виртуальной машины

Создаю новую виртуальную машину, указывая на папку для хранения её данных и образ системы, который собираюсь установить (рис. 3.1).

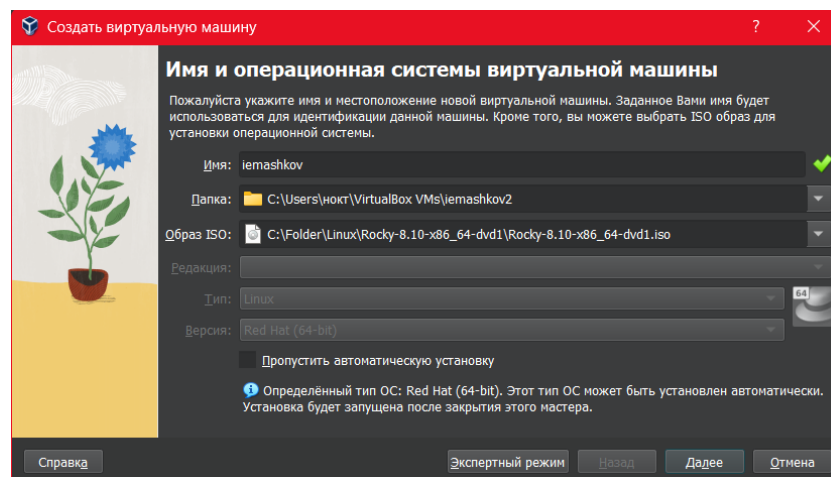


Рис. 3.1: Создание виртуальной машины.

Затем задаю количество ОЗУ и ядер процессора, которые будут использоваться (рис. 3.2).

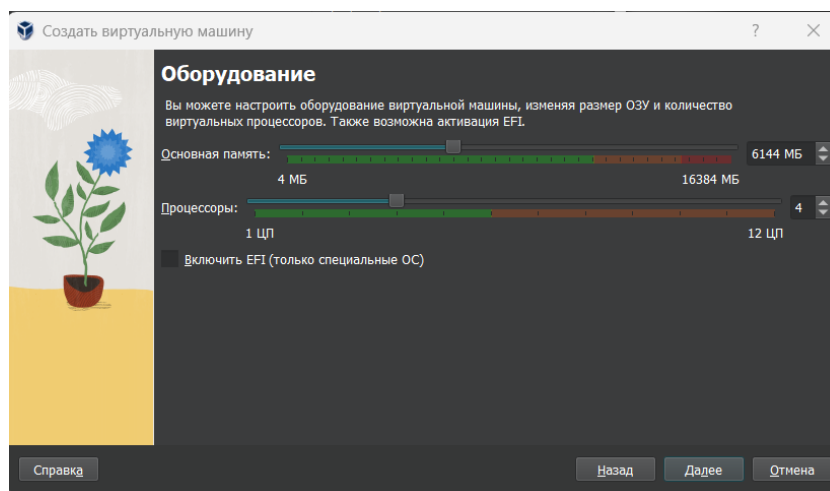


Рис. 3.2: Выделение ОЗУ и ядер процессора.

И наконец, создаю диск под машину размером в 50ГБ (рис. 3.3).

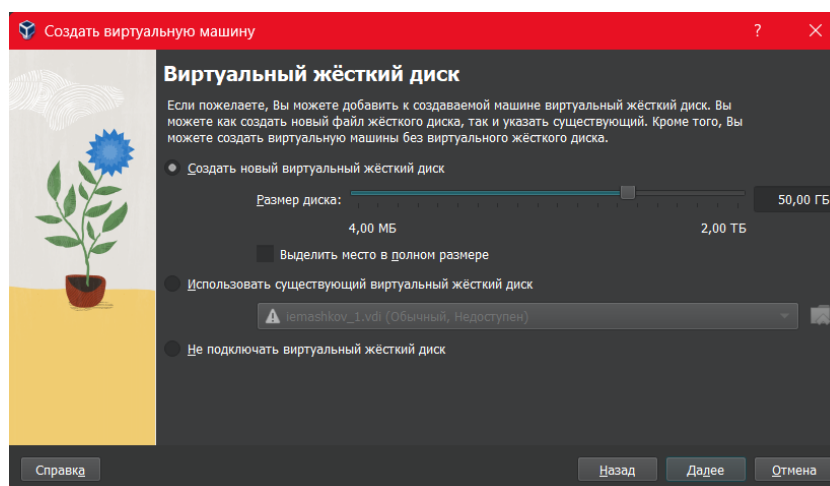


Рис. 3.3: Создание диска под систему.

3.2 Работа с установщиком Rocky

В установщике настраиваю языки, которые и будут использоваться в системе (рис. 3.4).

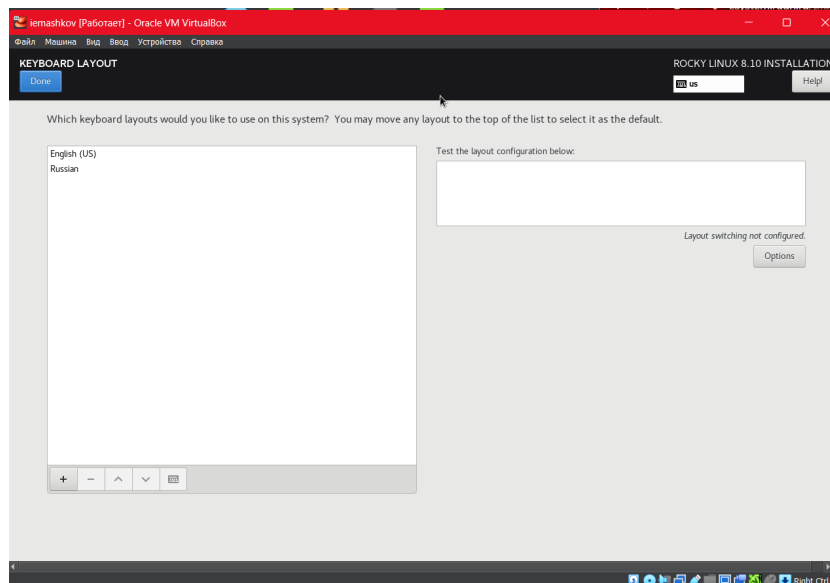


Рис. 3.4: Настройка языков системы.

Включаю параметр KDUMP (рис. 3.5).

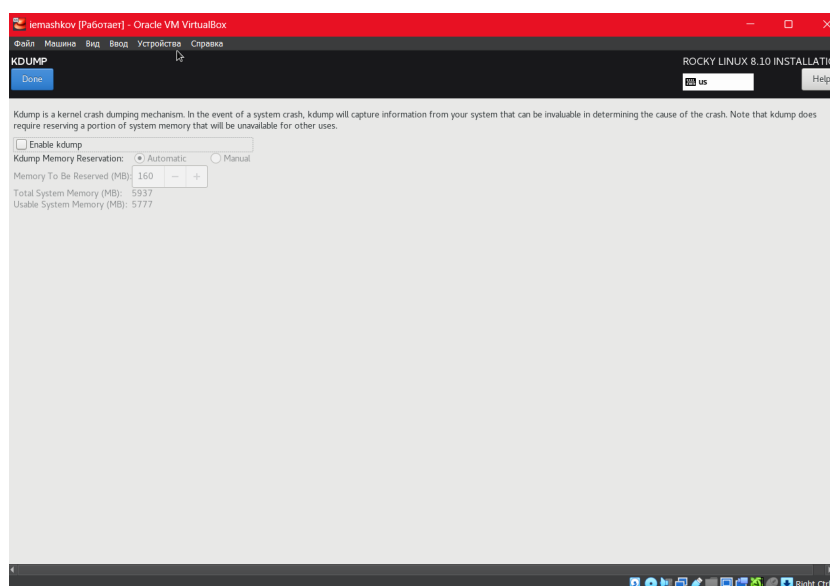


Рис. 3.5: Отключение KDUMPa.

Включаю Ethernet (рис. 3.6).

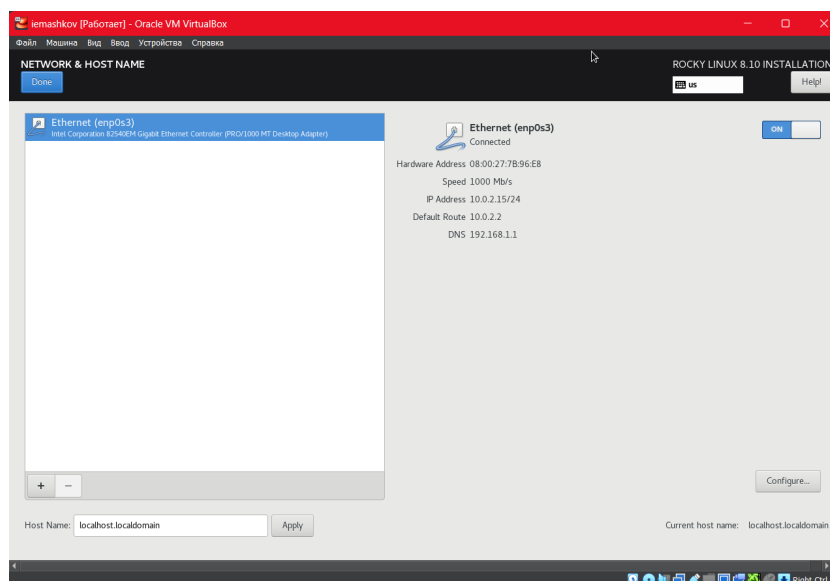


Рис. 3.6: Включение Ethernet.

Задаю имя пользователя и пароль для него, а также делаю его администратором по умолчанию (рис. 3.7).

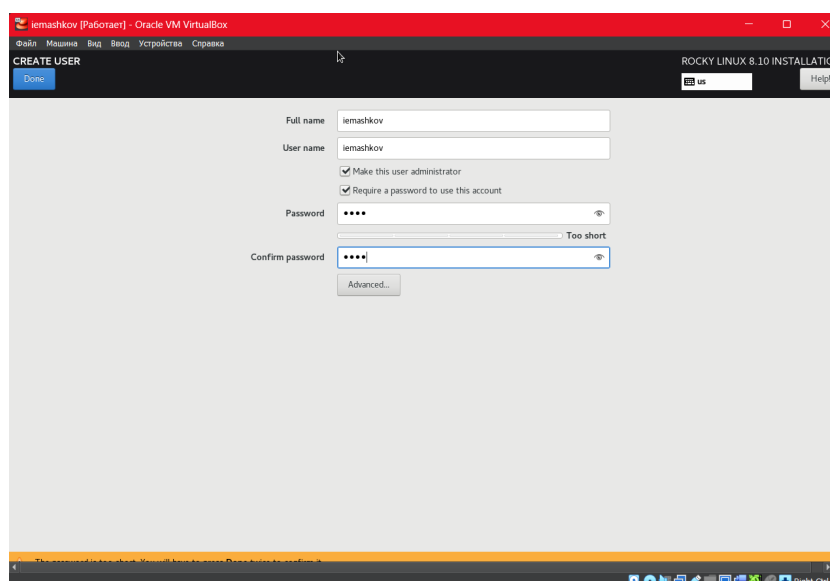


Рис. 3.7: Создание пользователя.

Подключаю **средства для разработки** к своей системе (рис. 3.8).

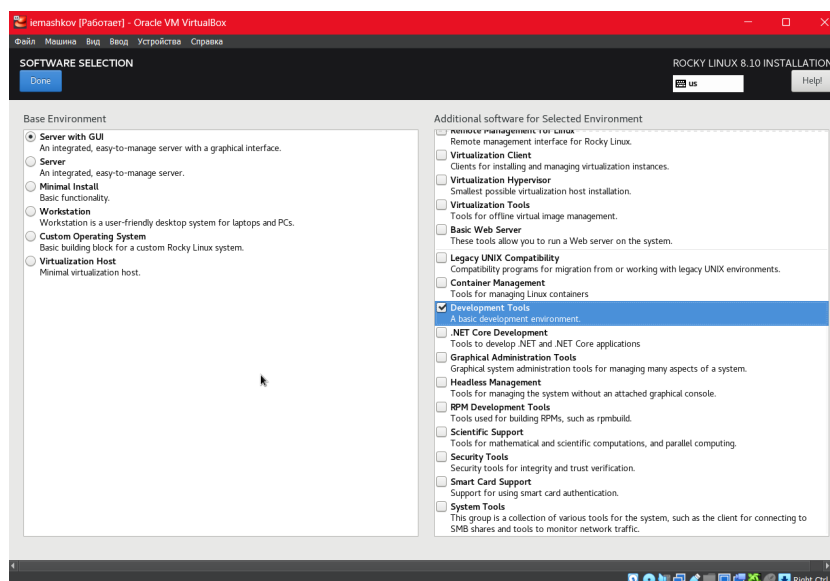


Рис. 3.8: Добавления средств для разработки к системе.

3.3 Работа с Rocky

Соглашаюсь с лицензионным соглашением (прошу прощения за тавтологию) (рис. 3.9).

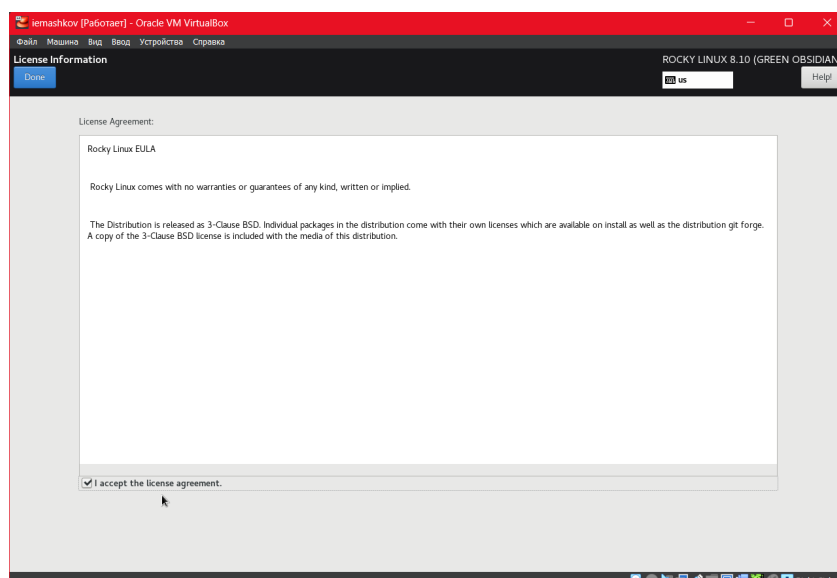


Рис. 3.9: Лицензионное соглашение.

Устанавливаю дополнение для гостевой ОС (рис. 3.10) (рис. 3.11).

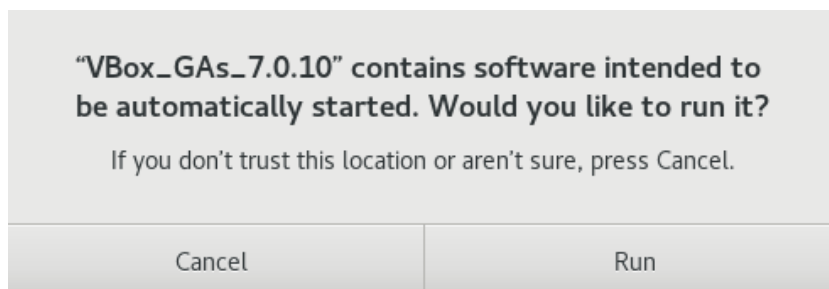


Рис. 3.10: Дополнения гостевой ОС.

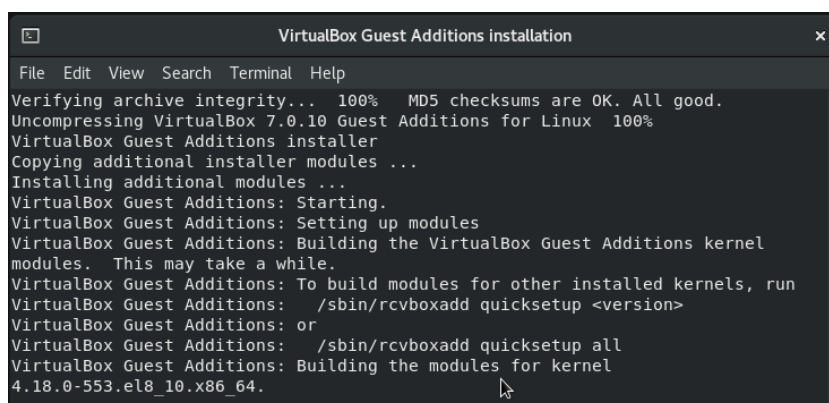


Рис. 3.11: Установка дополнения гостевой ОС.

3.4 Домашняя работа

1. Используя команду **"dmesg | less"** читаю информацию о своей системе (рис. 3.12).

```
iemashkov@localhost:~  
File Edit View Search Terminal Help  
[ 0.000000] Linux version 4.18.0-553.el8_10.x86_64 (mockbuild@iad1-prod-build  
001.bld.equ.rockylinux.org) (gcc version 8.5.0 20210514 (Red Hat 8.5.0-22) (GCC)  
) #1 SMP Fri May 24 13:05:10 UTC 2024  
[ 0.000000] Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-4.18.0-553.el8_10.x  
86_64 root=/dev/mapper/rl-root ro resume=/dev/mapper/rl-swap rd.lvm.lv=rl/root r  
d.lvm.lv=rl/swap 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 0x0000000000000000-0x000000000009fbff] usable  
[ 0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved  
[ 0.000000] BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved  
[ 0.000000] BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable  
[ 0.000000] BIOS-e820: [mem 0x000000000dff0000-0x000000000dffffff] 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 0x0000000010000000-0x0000000019ffffff] usable  
[ 0.000000] NX (Execute Disable) protection: active  
[ 0.000000] SMBIOS 2.5 present.  
[ 0.000000] DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/20  
06  
[ 0.000000] Hypervisor detected: KVM
```

Рис. 3.12: Вывод команды dmesg.

2. Затем благодаря параметру **“grep -i”название”**“ и той же команды **dmesg** ищу различные вещи.

- Версия ядра Linux (Linux version) рис. 3.13).

```
iemashkov@localhost ~]$ dmesg | grep -i "Linux version"  
[ 0.000000] Linux version 4.18.0-553.el8_10.x86_64 (mockbuild@iad1-prod-build  
001.bld.equ.rockylinux.org) (gcc version 8.5.0 20210514 (Red Hat 8.5.0-22) (GCC)  
) #1 SMP Fri May 24 13:05:10 UTC 2024
```

Рис. 3.13: Linux version.

- Частота процессора (Detected MHz processor) рис. 3.14).

```
iemashkov@localhost ~]$ dmesg | grep -i "Detected"  
[ 0.000000] Hypervisor detected: KVM  
[ 0.000000] tsc: Detected 2688.010 MHz processor  
[ 1.224087] hub 1-0:1.0: 12 ports detected  
[ 1.237153] hub 2-0:1.0: 12 ports detected  
[ 1.531008] systemd[1]: Detected virtualization oracle.  
[ 1.531011] systemd[1]: Detected architecture x86-64.  
[ 7.494469] systemd[1]: Detected virtualization oracle.  
[ 7.494476] systemd[1]: Detected architecture x86-64.
```

Рис. 3.14: Detected MHz processor.

- Модель процессора (CPU0) рис. 3.15).

```
[iemashkov@localhost ~]$ dmesg | grep -i "CPU0"
[ 0.102547] smpboot: CPU0: 11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz (family: 0x6, model: 0x8d, stepping: 0x1)
```

Рис. 3.15: CPU0.

- Объём ОЗУ (Memory available) рис. 3.16).

```
[iemashkov@localhost ~]$ dmesg | grep -i "memory"
[ 0.000000] ACPI: Reserving FACP table memory at [mem 0xdfff00f0-0xdfff01e3]
[ 0.000000] ACPI: Reserving DSDT table memory at [mem 0xdfff0620-0xdfff2972]
[ 0.000000] ACPI: Reserving FACS table memory at [mem 0xdfff0200-0xdfff023f]
[ 0.000000] ACPI: Reserving FACS table memory at [mem 0xdfff0200-0xdfff023f]
[ 0.000000] ACPI: Reserving APIC table memory at [mem 0xdfff0240-0xdfff02ab]
[ 0.000000] ACPI: Reserving SSDT table memory at [mem 0xdfff02b0-0xdfff061b]
[ 0.000000] Early memory node ranges
[ 0.000000] PM: Registered nosave memory: [mem 0x00000000-0x00000fff]
[ 0.000000] PM: Registered nosave memory: [mem 0x0009f000-0x0009ffff]
[ 0.000000] PM: Registered nosave memory: [mem 0x000a0000-0x000effff]
[ 0.000000] PM: Registered nosave memory: [mem 0x000f0000-0x000fffff]
[ 0.000000] PM: Registered nosave memory: [mem 0xdfff0000-0xdfff0fff]
[ 0.000000] PM: Registered nosave memory: [mem 0xe0000000-0xfefbffff]
[ 0.000000] PM: Registered nosave memory: [mem 0xfec00000-0xfec0ffff]
[ 0.000000] PM: Registered nosave memory: [mem 0xfec01000-0xfedfffff]
[ 0.000000] PM: Registered nosave memory: [mem 0xfef00000-0xfef0ffff]
[ 0.000000] PM: Registered nosave memory: [mem 0xfef01000-0xfefbffff]
```

Рис. 3.16: Memory available.

- Тип гипервизора (Hypervisor detected) рис. 3.17).

```
[iemashkov@localhost ~]$ dmesg | grep -i "Hypervisor detected"
[ 0.000000] Hypervisor detected: KVM
```

Рис. 3.17: Hypervisor detected.

- Тип файловой системы корневого раздела рис. 3.18).

```
[iemashkov@localhost ~]$ df -T /
Filesystem      Type 1K-blocks    Used Available Use% Mounted on
/dev/mapper/rl-root xfs   46110724 7809080  38301644  17% /
```

Рис. 3.18: Тип файловой системы.

- Последовательность монтирования файловых систем рис. 3.19).

```
[iemashkov@localhost ~]$ dmesg | grep -i "Mount"
[ 0.001000] Mount-cache hash table entries: 16384 (order: 5, 131072 bytes, vm
alloc)
[ 0.001000] Mountpoint-cache hash table entries: 16384 (order: 5, 131072 byte
s, vmalloc)
[ 6.573668] XFS (dm-0): Mounting V5 Filesystem
[ 6.615687] XFS (dm-0): Ending clean mount
[ 9.777877] XFS (sda1): Mounting V5 Filesystem
[ 10.952427] XFS (sda1): Ending clean mount
```

Рис. 3.19: Последовательность монтирования.

4 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).
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`.
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.

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`.
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.

5 Выводы

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

Список литературы

Основы информационной безопасности