

Отчёт по лабораторной работе №1

Основы информационной безопасности

Мурашов Иван Вячеславович

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Домашнее задание	12
5	Контрольные вопросы	14
6	Выводы	16

Список иллюстраций

3.1	Создание виртуальной машины	7
3.2	Создание виртуальной машины	7
3.3	Создание виртуальной машины	8
3.4	Создание виртуальной машины	8
3.5	Создание виртуальной машины	9
3.6	Создание виртуальной машины	9
3.7	Установка виртуальной машины	10
3.8	Установка виртуальной машины	10
3.9	Установка виртуальной машины	11
3.10	Установка виртуальной машины	11
4.1	Вывод информации о системе	12
4.2	Вывод информации о системе	13

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. Установка и настройка системы
2. Получить следующую информацию:
 1. Версия ядра Linux (Linux version).
 2. Частота процессора (Detected Mhz processor).
 3. Модель процессора (CPU0).
 4. Объем доступной оперативной памяти (Memory available).
 5. Тип обнаруженного гипервизора (Hypervisor detected).
 6. Тип файловой системы корневого раздела.
 7. Последовательность монтирования файловых систем.

3 Выполнение лабораторной работы

Создаю новую виртуальную машину в Oracle VMBox (рис. 3.1).

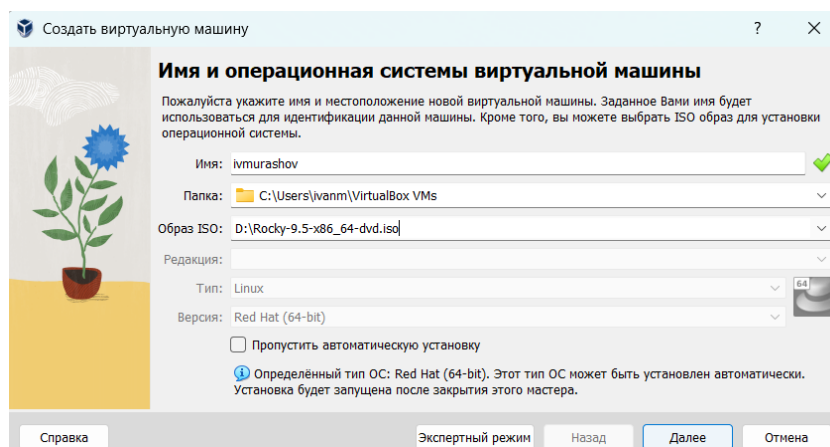


Рис. 3.1: Создание виртуальной машины

Выставляю размер основной памяти 5120 Мб и 5 ядер процессора (рис. 3.2).

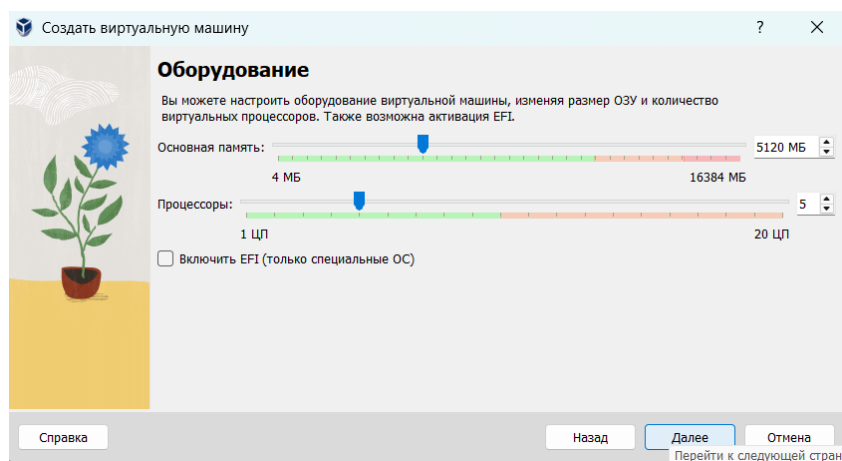


Рис. 3.2: Создание виртуальной машины

Устанавливаю пользователя и пароль (рис. 3.3).

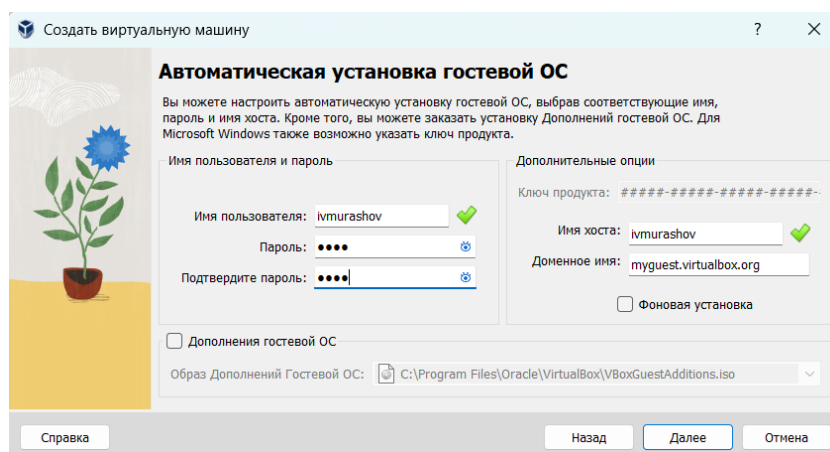


Рис. 3.3: Создание виртуальной машины

Выделяю 40 Гб на диск (рис. 3.4).

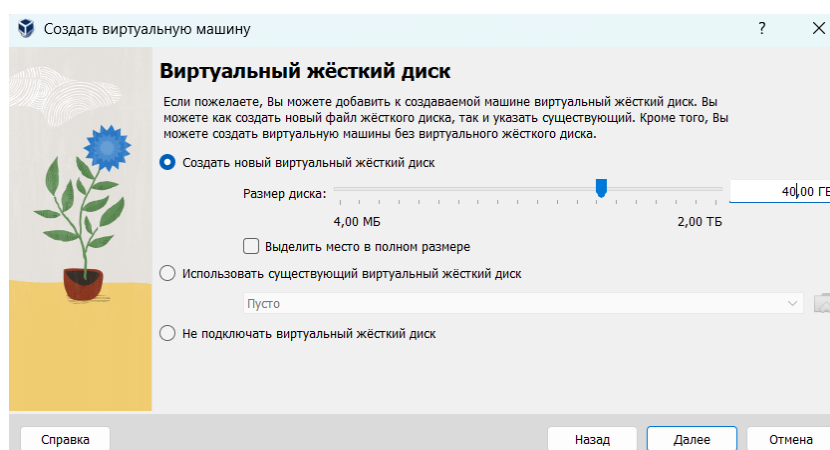


Рис. 3.4: Создание виртуальной машины

Просматриваю корректность данных (рис. 3.5).

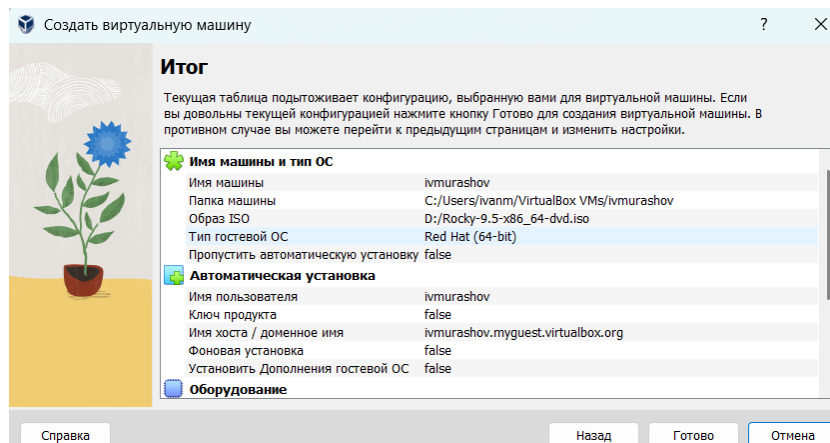


Рис. 3.5: Создание виртуальной машины

Выставляю 40 Мб на видеопамять (рис. 3.6).

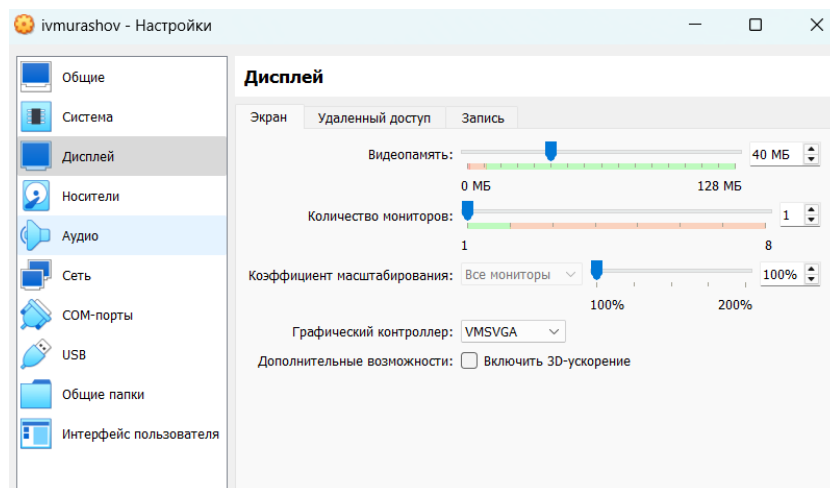


Рис. 3.6: Создание виртуальной машины

Выбираю язык установки (рис. 3.7).

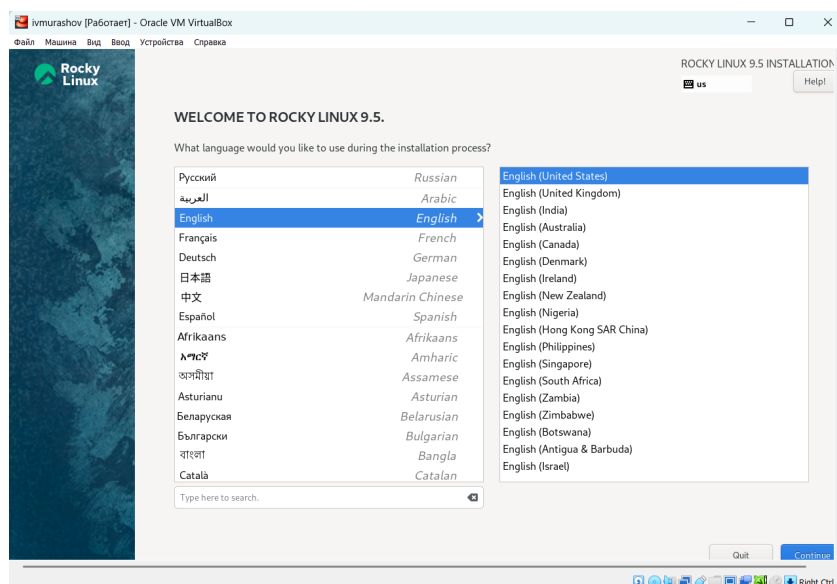


Рис. 3.7: Установка виртуальной машины

Выставляю правильные настройки: добавляю русскую раскладку, часовой пояс Москва, пароль для user и root, выбираю созданный ранее виртуальный диск, отключаю KDUMP, устанавливаю имя локальной сети (рис. 3.8).

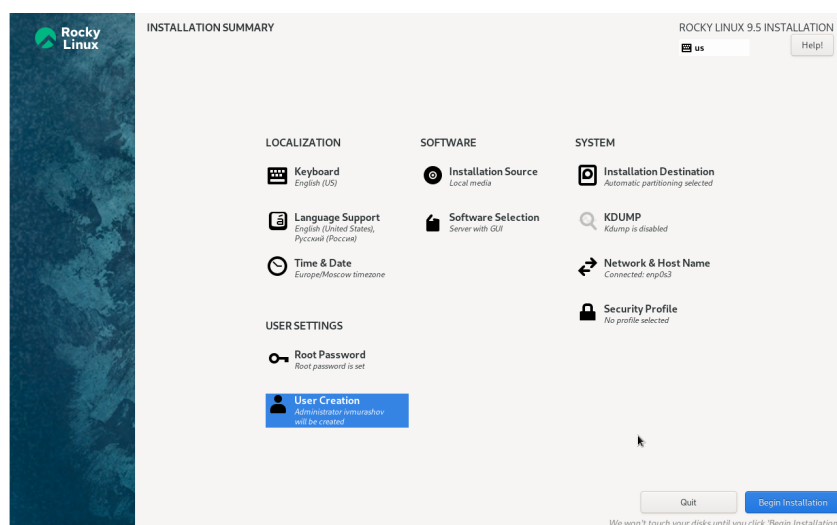


Рис. 3.8: Установка виртуальной машины

Подключаю образ гостевой ОС (рис. 3.9).

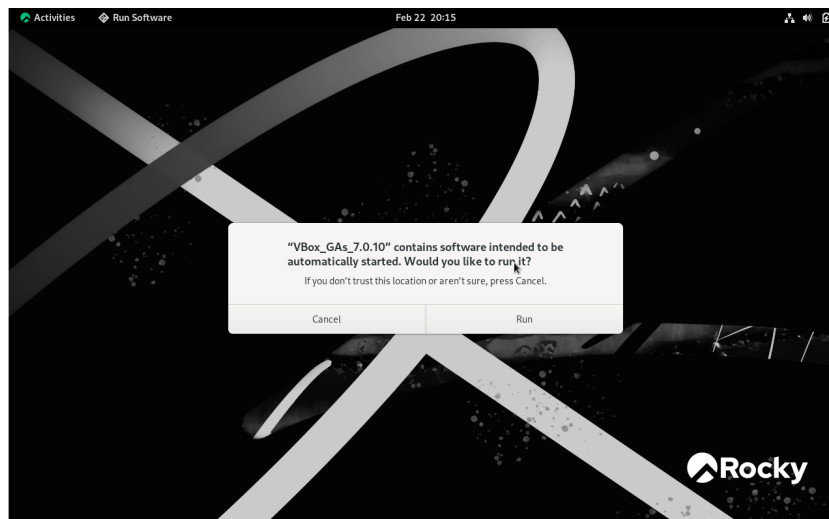


Рис. 3.9: Установка виртуальной машины

Проверяю, что имя хоста было установлено корректно (рис. 3.10).


```
ivmurashov@ivmurashov:~  
[ivmurashov@ivmurashov ~]$ hostnamectl  
Static hostname: ivmurashov.localdomain  
Icon name: computer-vm  
Chassis: vm   
Machine ID: 9525f148e6344c9bbc9718ad45526a3b  
Boot ID: ca98cb833bb84b36bd87868eb83acdf6  
Virtualization: oracle  
Operating System: Rocky Linux 9.5 (Blue Onyx)  
CPE OS Name: cpe:/o:rocky:rocky:9::baseos  
Kernel: Linux 5.14.0-503.14.1.el9_5.x86_64  
Architecture: x86-64  
Hardware Vendor: innotek GmbH  
Hardware Model: VirtualBox  
Firmware Version: VirtualBox  
[ivmurashov@ivmurashov ~]$
```

Рис. 3.10: Установка виртуальной машины

4 Домашнее задание

В окне терминала проверяем последовательность загрузки системы, выполнив команду `dmesg | less`.

Используем поиск с помощью `grep`: `dmesg | grep -i "то, что ищем"` Получаем следующую информацию (рис. 4.1), (рис. 4.2)

1. Версия ядра Linux (Linux version).
2. Частота процессора (Detected Mhz processor).
3. Модель процессора (CPU0).
4. Объем доступной оперативной памяти (Memory available).
5. Тип обнаруженного гипервизора (Hypervisor detected).
6. Тип файловой системы корневого раздела.

```
[root@ivmurashov ~]# dmesg | less
[0.000000] Linux version 5.14.0-503.14.1.el9_5.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.
3.0 20240719 (Red Hat 11.5.0-2)), GNU ld version 2.35.2-54.el9) #1 SMP PREEMPT_DYNAMIC Fri Nov 15 12:04:32 UTC 2024
[0.000005] tsc: Detected 2688.008 MHz processor
[2.822197] e1000 0000:00:03:0 eth0: (PCI:33MHz:32-bit) 08:00:27:60:c3:db
[0.394418] smpboot: CPU0: 12th Gen Intel(R) Core(TM) i7-12650H (family: 0x6, model: 0x9a, stepping: 0x3)
[0.001198] ACPI: Reserving FACP table memory at [mem 0xdfff00f0-0xdfff01e3]
[0.001191] ACPI: Reserving DSDT table memory at [mem 0xdfff0630-0xdfff2982]
[0.001192] ACPI: Reserving FACS table memory at [mem 0xdfff0200-0xdfff023f]
[0.001192] ACPI: Reserving FACS table memory at [mem 0xdfff0200-0xdfff023f]
[0.001192] ACPI: Reserving APIC table memory at [mem 0xdfff0240-0xdfff02b3]
[0.001193] ACPI: Reserving SSDT table memory at [mem 0xdfff02c0-0xdfff062b]
[0.002373] Early memory node ranges
[0.111668] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x00000fff]
[0.111670] PM: hibernation: Registered nosave memory: [mem 0x0009f000-0x0009ffff]
[0.111671] PM: hibernation: Registered nosave memory: [mem 0x000a0000-0x000effff]
[0.111671] PM: hibernation: Registered nosave memory: [mem 0x000f0000-0x000fffff]
[0.111672] PM: hibernation: Registered nosave memory: [mem 0xdfff0000-0xdfff0fff]
[0.111672] PM: hibernation: Registered nosave memory: [mem 0xe0000000-0xfebfffff]
[0.111672] PM: hibernation: Registered nosave memory: [mem 0xfec00000-0xfec0ffff]
[0.111672] PM: hibernation: Registered nosave memory: [mem 0xfec01000-0xfedfffff]
[0.111673] PM: hibernation: Registered nosave memory: [mem 0xfec00000-0xfec0ffff]
[0.111674] PM: hibernation: Registered nosave memory: [mem 0xfec01000-0xfec0ffff]
[0.111674] PM: hibernation: Registered nosave memory: [mem 0xfec00000-0xfec0ffff]
[0.222068] Memory: 3676416K/4193848K available (16384K kernel code, 5685K rwdata, 12904K rodata, 3976K init, 5672K bss, 25
1276K reserved, 0K cma-reserved)
[0.287863] Freeing SMP alternatives memory: 40K
[0.416483] x86/mem: Memory block size: 128MB
[0.969008] Non-volatile memory driver v1.3
[1.221863] Freeing initrd memory: 57788K
```

Рис. 4.1: Вывод информации о системе

```

[ 0.001192] ACPI: Reserving FACS table memory at [mem 0xdfff0200-0xdfff023f]
[ 0.001192] ACPI: Reserving FACS table memory at [mem 0xdfff0200-0xdfff023f]
[ 0.001192] ACPI: Reserving APIC table memory at [mem 0xdfff0240-0xdfff02b3]
[ 0.001193] ACPI: Reserving SSDT table memory at [mem 0xdfff02c0-0xdfff062b]
[ 0.002373] Early memory node ranges
[ 0.111668] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x00000fff]
[ 0.111670] PM: hibernation: Registered nosave memory: [mem 0x0009f000-0x0009ffff]
[ 0.111671] PM: hibernation: Registered nosave memory: [mem 0x000a0000-0x000effff]
[ 0.111671] PM: hibernation: Registered nosave memory: [mem 0x000f0000-0x000fffff]
[ 0.111672] PM: hibernation: Registered nosave memory: [mem 0xdfff0000-0xdfff0fff]
[ 0.111672] PM: hibernation: Registered nosave memory: [mem 0xe0000000-0xf0000fff]
[ 0.111673] PM: hibernation: Registered nosave memory: [mem 0xfec00000-0xfec00fff]
[ 0.111673] PM: hibernation: Registered nosave memory: [mem 0xfec01000-0xfec0ffff]
[ 0.111673] PM: hibernation: Registered nosave memory: [mem 0xfec00000-0xfec00fff]
[ 0.111674] PM: hibernation: Registered nosave memory: [mem 0xfec01000-0xfec0ffff]
[ 0.111674] PM: hibernation: Registered nosave memory: [mem 0xfec00000-0xfec00fff]
[ 0.222068] Memory: 3676416K/4193848K available (16384K kernel code, 5685K rwdata, 12904K rodata, 3976K init, 5672K bss, 25
1276K reserved, 0K cma-reserved)
[ 0.287863] Freeing SMP alternatives memory: 49K
[ 0.416483] x86/mm: Memory block size: 128MB
[ 0.969008] Non-volatile memory driver v1.3
[ 1.221863] Freeing initrd memory: 57788K
[ 1.432829] Freeing unused decrypted memory: 2028K
[ 1.433512] Freeing unused kernel image (initmem) memory: 3976K
[ 1.434373] Freeing unused kernel image (rodata/data gap) memory: 1432K
[ 2.957598] vmwgfx 0000:00:02.0: [drm] Legacy memory limits: VRAM = 32768 kB, FIFO = 2048 kB, surface = 491520 kB
[ 2.957603] vmwgfx 0000:00:02.0: [drm] Maximum display memory size is 32768 kiB
root@ivmurashov ~# dmesg | grep -i "Hypervisor"
[ 0.000000] Hypervisor detected: KVM
[ 2.957249] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported hypervisor.
root@ivmurashov ~# dmesg | grep -i "filesystem"
[ 4.188005] XFS (dm-0): Mounting V5 filesystem e0b5f3e1-8f30-4a3c-81e5-24c7e8d4f9f6
[ 6.367020] XFS (sda1): Mounting V5 filesystem 5fd258cb-ecc6-4d6b-a38c-72a0a6ebfb7a

```

Рис. 4.2: Вывод информации о системе

5 Контрольные вопросы

1. Какую информацию содержит учётная запись пользователя?

Совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам. Учётная запись, как правило, содержит сведения, необходимые для опознавания пользователя при подключении к системе, сведения для авторизации и учёта. Это идентификатор пользователя (login) и его пароль. Пароль или его аналог, как правило, хранится в зашифрованном или хэшированном виде для обеспечения его безопасности.

2. Укажите команды терминала и приведите примеры:

- для получения справки по команде: команда `man`;
- для перемещения по файловой системе: команда `cd` ;
- для просмотра содержимого каталога: команда `ls`;
- для определения объёма каталога: команда `du`;
- для создания / удаления каталогов / файлов: команда `mkdir`/ команда `rm -r`/ команда `rm`;
- для задания определённых прав на файл / каталог: команда `chmod`;
- для просмотра истории команд: команда `history`.

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

Файловая система — это метод управления файлами и папками на пользовательских устройствах хранения, таких как жёсткие диски, флеш-накопители и другие носители данных.

- FAT – одна из самых старых файловых систем, разработанная для использования в операционных системах MS-DOS и Windows.
- NTFS – файловая система, разработанная компанией Microsoft и используемая в операционных системах Windows NT и последующих версиях Windows.
- ext4 – файловая система, используемая в операционных системах Linux.

4. Как посмотреть, какие файловые системы подмонтированы в ОС?

df (аббревиатура от disk free) — утилита в UNIX и UNIX-подобных системах.

Она показывает список всех файловых систем по именам устройств, сообщает их размер, занятое и свободное пространство и точки монтирования.

Утилиту df можно использовать для получения информации о том, к какой файловой системе относится какой-либо каталог.

5. Как удалить зависший процесс?

Чтобы удалить зависший процесс в Linux, можно использовать следующие команды:

Команда kill принимает в качестве параметра PID процесса и отправляет сигнал процессу. По умолчанию посылается сигнал SIGTERM.

Команда killall предназначена для «убийства» всех процессов, имеющих одно и то же имя.

6 Выводы

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