

Лабораторная работа №1

Основы информационной безопасности

Намруев М. С.

22 февраля 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Намруев Максим Саналович
- студент, 2 курс, НКАбд-03-23
- Российский университет дружбы народов
- 1132236035@rudn.ru
- <https://msnamruev.io/ru/>

Цель работы

Целью данной работы является приобретение практических навыков установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов.

Задание

1. Настройка Виртуальной машины
2. Установка имени пользователя и названия хоста
3. Домашняя работа

Выполнение лабораторной работы

Создаю новую виртуальную машину, указывая её имя и тип операционной системы.

Создать виртуальную машину ? ×

Имя и операционная система виртуальной машины

Пожалуйста укажите имя и местоположение новой виртуальной машины. Заданное Вами имя будет использоваться для идентификации данной машины. Кроме того, вы можете выбрать ISO образ для установки операционной системы.

Имя:

Папка: C:\Users\maksi\VirtualBox VMs

Образ ISO: <ничего не выбрано>

Редакция:

Тип: Microsoft Windows

Версия: Windows 10 (64-bit)

Пропустить автоматическую установку

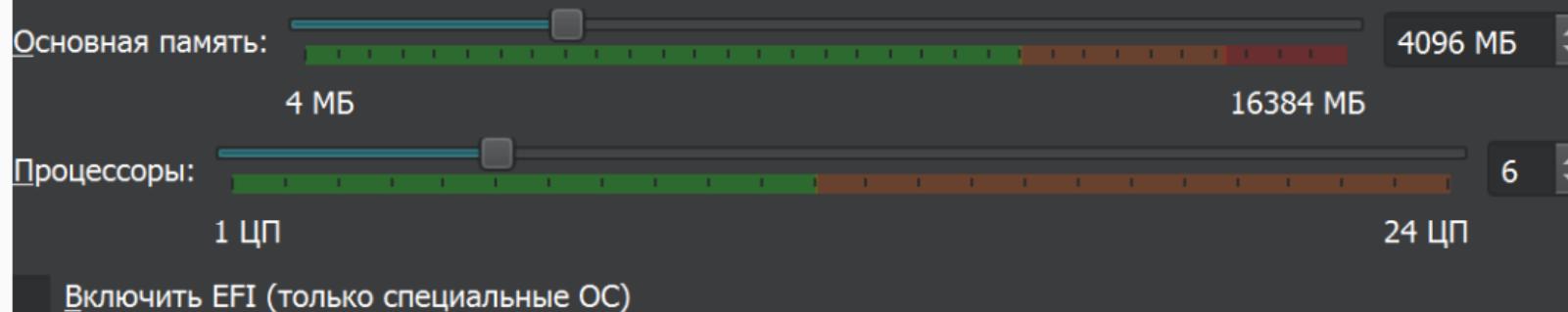
Образ ISO не выбран, гостевая ОС должна быть установлена вручную.

Выполнение лабораторной работы

Далле задаю размер основной виртуальной памяти ВМ

Оборудование

Вы можете настроить оборудование виртуальной машины, изменяя размер ОЗУ и количество виртуальных процессоров. Также возможна активация EFI.



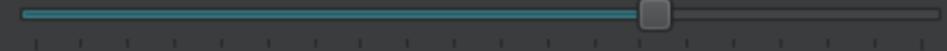
Выполнение лабораторной работы

Задаю конфигурацию жесткого диска и размер диска.

Виртуальный жёсткий диск

Если пожелаете, Вы можете добавить к создаваемой машине виртуальный жёсткий диск. Вы можете как создать новый файл жёсткого диска, так и указать существующий. Кроме того, Вы можете создать виртуальную машины без виртуального жёсткого диска.

- Создать новый виртуальный жёсткий диск

Размер диска:  40 ГБ

4,00 МБ

2,00 ТБ

Выделить место в полном размере

- Использовать существующий виртуальный жёсткий диск

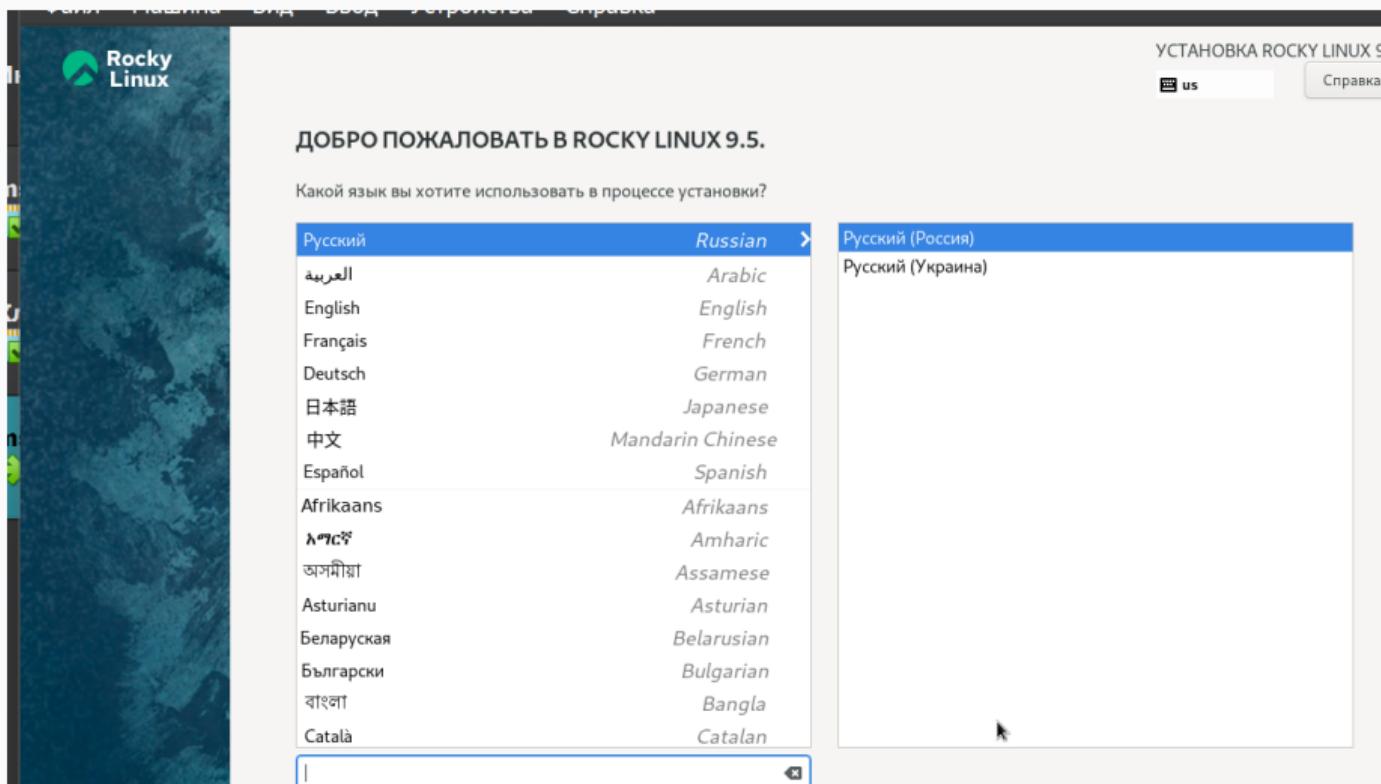
msnamtruev.vdi (Обычный, 90,00 ГБ)



- Не подключать виртуальный жёсткий диск

Выполнение лабораторной работы

Запускаю ВМ и выбираю язык настройки.



Выполнение лабораторной работы

В разделе выбора программ указываю в качестве базового окружения сервер и GUI, а в качестве дополнения Средства разработки.

The screenshot shows the 'Выбор программ' (Selection of programs) screen during the Rocky Linux 9.5 installation process. The top bar includes 'Готово' (Ready), the system name 'us', and 'Справка' (Help). The main area is divided into two sections: 'Базовое окружение' (Basic environment) and 'Дополнительное программное обеспечение для выбранной среды' (Additional software for selected environment).

Базовое окружение:

- Сервер с GUI
Интегрированный, простой в управлении сервер с графическим интерфейсом.
- Сервер
Интегрированный, простой в управлении сервер.
- Минимальная установка
Базовая функциональность.
- Рабочая станция
Рабочая станция - это удобная для пользователя настольная система для ноутбуков и ПК.
- Пользовательская операционная система
Базовый строительный блок для индивидуальной системы Rocky Linux.
- Хост виртуализации
Минимальный комплект хоста виртуализации.

Дополнительное программное обеспечение для выбранной среды:

- Средства контроля производительности
Средства диагностики системы и производительности на уровне приложений.
- Клиенты удалённого рабочего стола
- Удаленное управление Linux
Интерфейс удаленного управления для Rocky Linux.
- Файловый сервер Windows
Эта группа пакетов делает возможным доступ к файлам между системами Linux и MS Windows(tm).
- Клиент виртуализации
Клиенты для установки и управления экземплярами виртуализации.
- Гипервизор виртуализации
Минимальная установка хоста виртуализации.
- Средства виртуализации
Средства для автономного управления виртуальными образами.
- Стандартный веб-сервер
Эти средства позволяют использовать систему как веб-сервер.
- Совместимость с устаревшими функциями UNIX
Программы совместимости для миграции или работы с устаревшими окружениями UNIX.
- Консольные средства Интернета
Консольные средства доступа к Интернету, обычно используемые администраторами.
- Управление контейнерами
Инструменты для управления контейнерами Linux
- Средства разработки
Стандартная среда разработки.
- .NET Development
Tools to develop and/or run .NET applications

Выполнение лабораторной работы

Устанавливаю пароль для root и пользователя с правами администратора.

The screenshot shows the 'Обзор установки' (Installation Overview) screen of the Rocky Linux 9.5 installer. The interface is in Russian. On the left, there's a large background image of a forest. At the top right, it says 'УСТАНОВКА ROCKY LINUX 9.5' with a 'us' icon and a 'Справка' button. The main area has tabs for 'РЕГИОНАЛЬНЫЕ НАСТРОЙКИ' (Regional Settings), 'ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ' (Software), and 'СИСТЕМА' (System). Under 'РЕГИОНАЛЬНЫЕ НАСТРОЙКИ', there are three items: 'Клавиатура' (Keyboard), 'Языковая поддержка' (Language Support), and 'Дата и время' (Date and Time). Under 'ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ', there are two items: 'Источник установки' (Source) and 'Выбор программ' (Select Programs). Under 'СИСТЕМА', there are three items: 'Место установки' (Install Location), 'KDUMP' (Kdump enabled), and 'Имя сети и узла' (Network Name). In the 'ПОЛЬЗОВАТЕЛИ' (Users) section, there's an item for 'Пароль root' (root password) which states 'Пароль root задан' (root password set). A blue button at the bottom says 'Создание пользователя' (Create User) with the note 'Будет создан пользователь msnatmiev'. The bottom right corner shows the page number '10/22'.

УСТАНОВКА ROCKY LINUX 9.5

us Справка

ОБЗОР УСТАНОВКИ

РЕГИОНАЛЬНЫЕ НАСТРОЙКИ

Клавиатура
английский (Английская (США)), русский (Русская)

Языковая поддержка
Русский (Россия)

Дата и время
Часовой пояс Европа/Москва

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Источник установки
Локальный носитель

Выбор программ
Сервер с GUI

СИСТЕМА

Место установки
Автоматическое
разбиение диска

KDUMP
Kdump включен

Имя сети и узла
Подключено: ep0s3

ПОЛЬЗОВАТЕЛИ

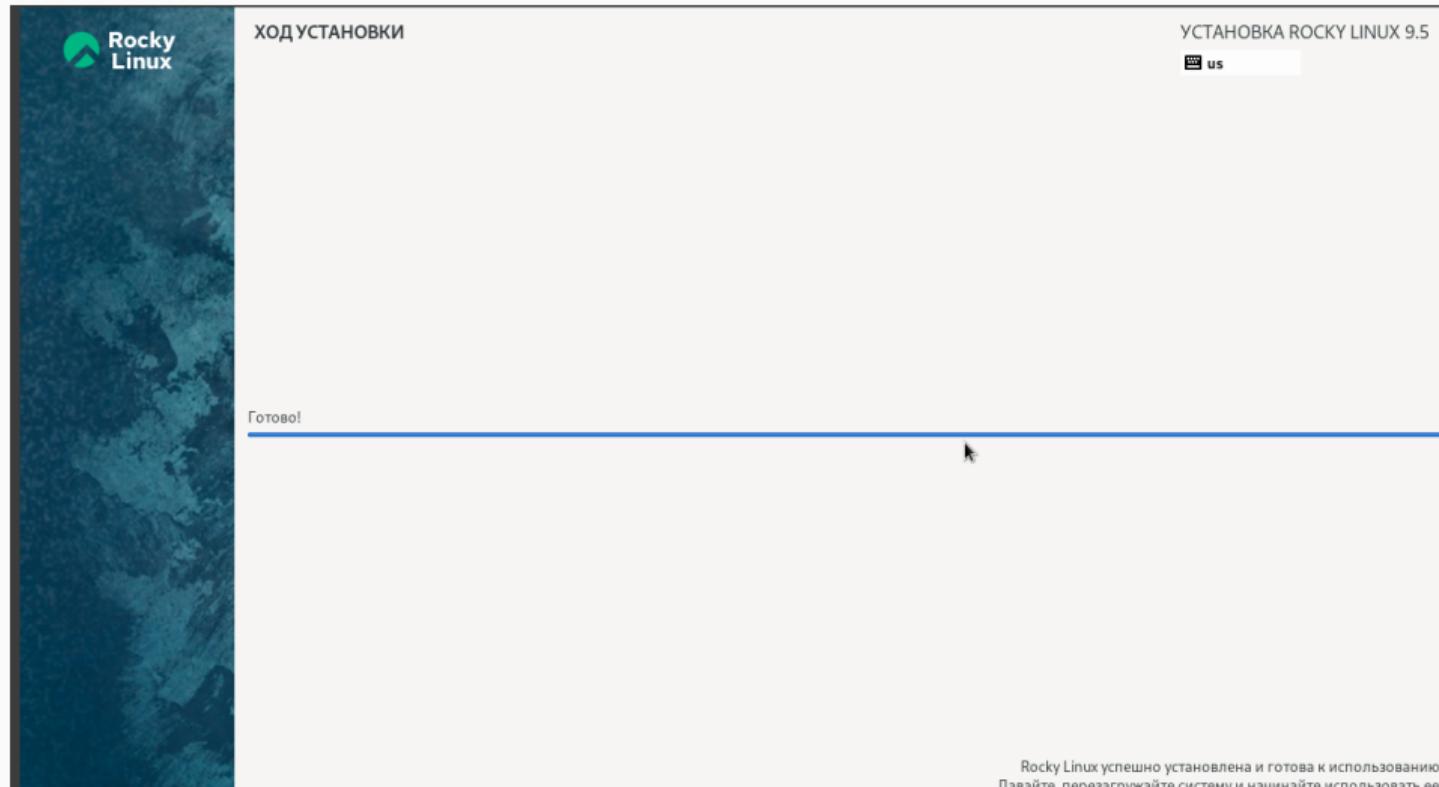
Пароль root
Пароль root задан

Создание пользователя
Будет создан пользователь
msnatmiev

10/22

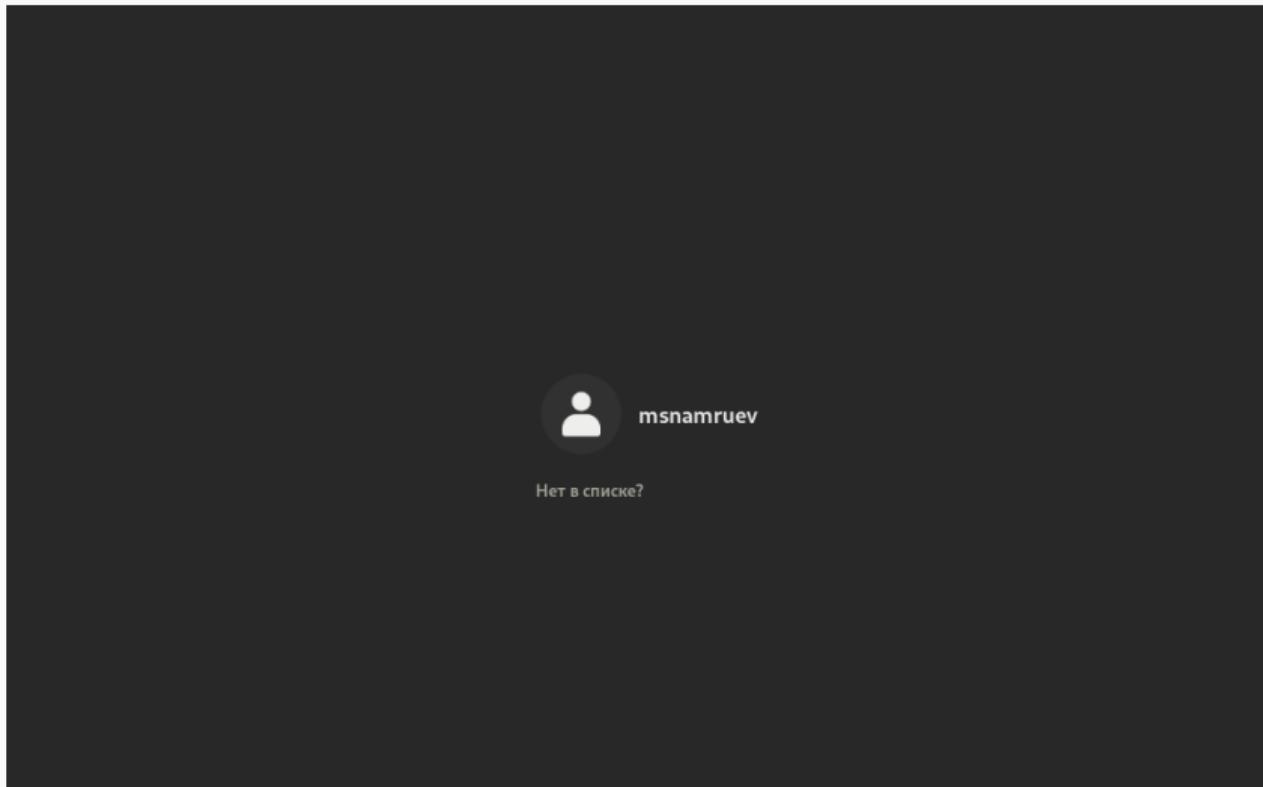
Выполнение лабораторной работы

Устанавливаю операционную систему и перезапускаю её.



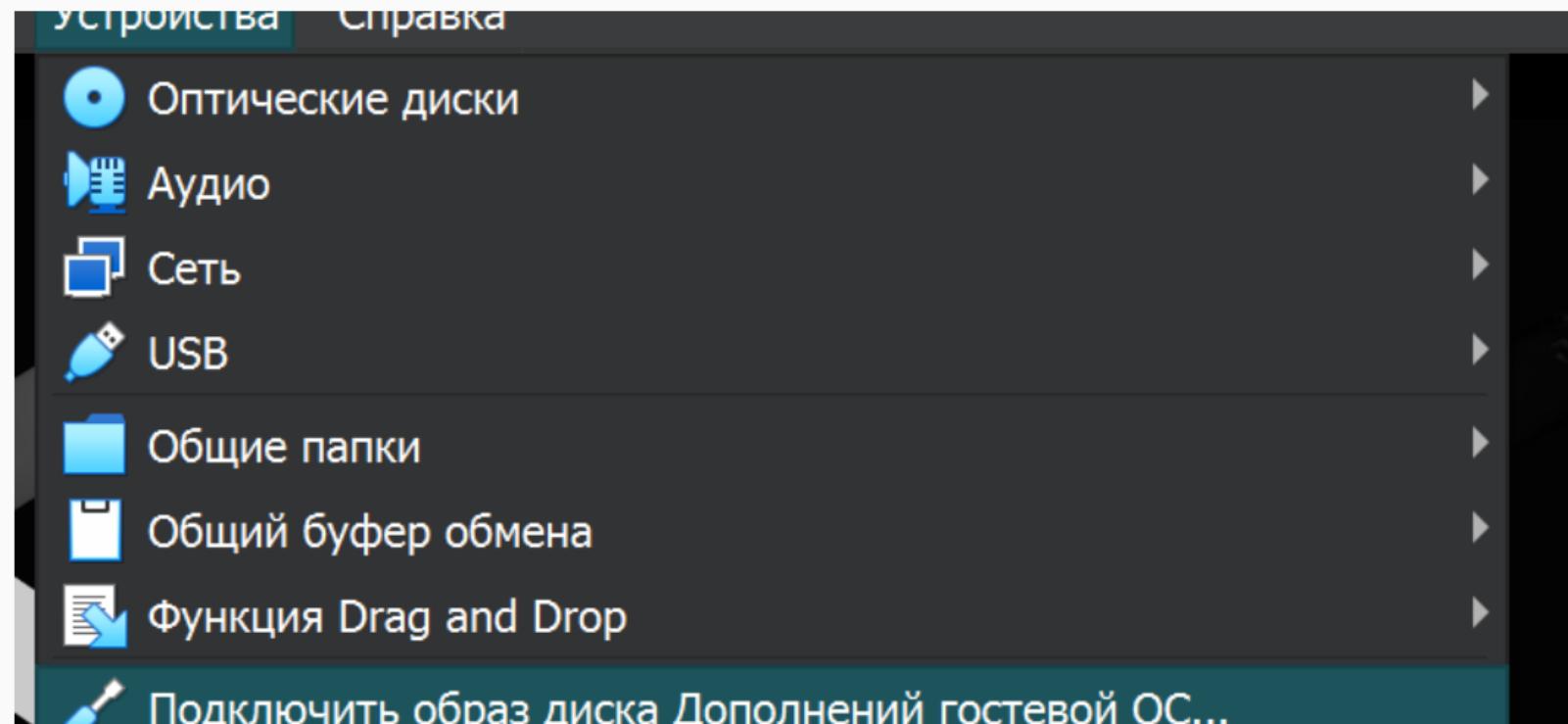
Выполнение лабораторной работы

после перезагрузки вхожу в ОС под созданной мной учетной записью.



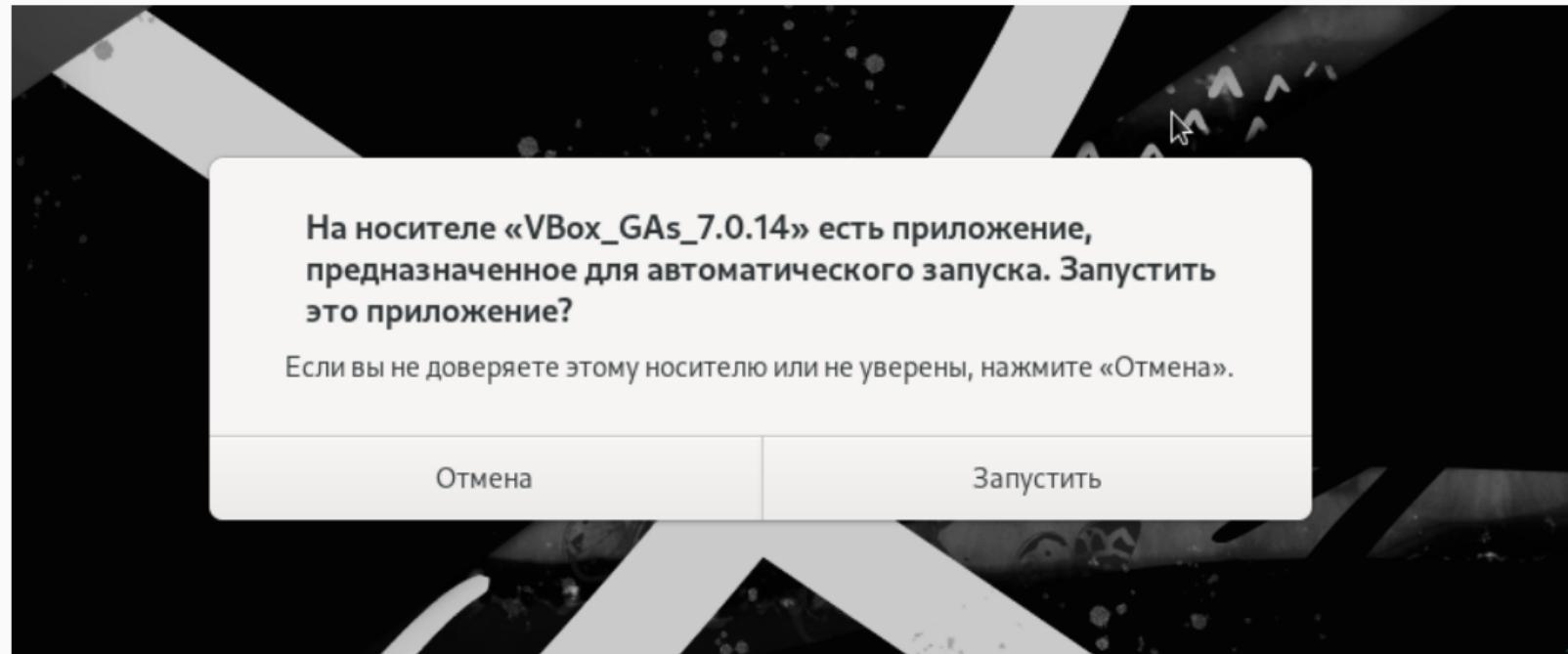
Выполнение лабораторной работы

в меню устройства подключаю образ дополнений гостевой ОС.



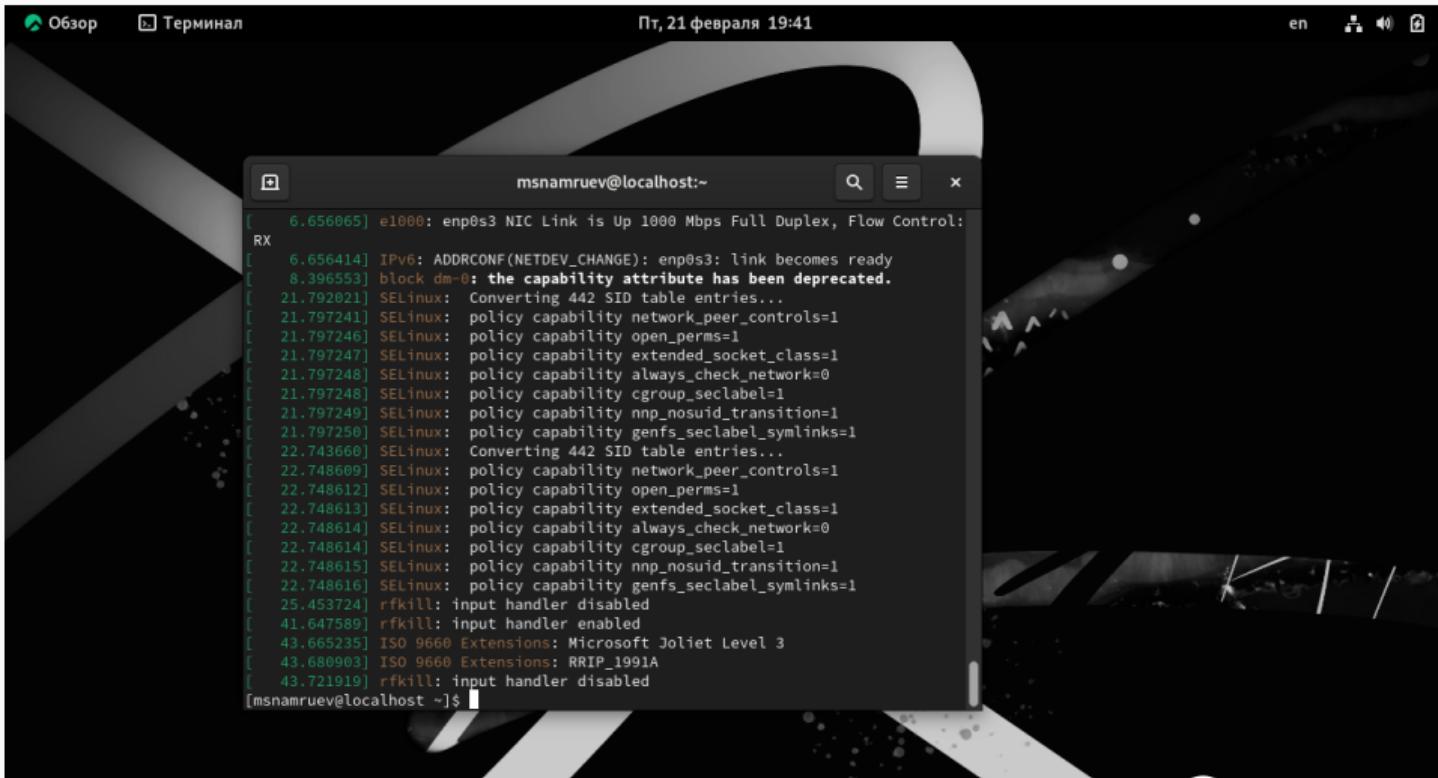
Выполнение лабораторной работы

Загуржаю его и потом перезагружаю ОС.



Домашнее задание

Использую команду dmesg.



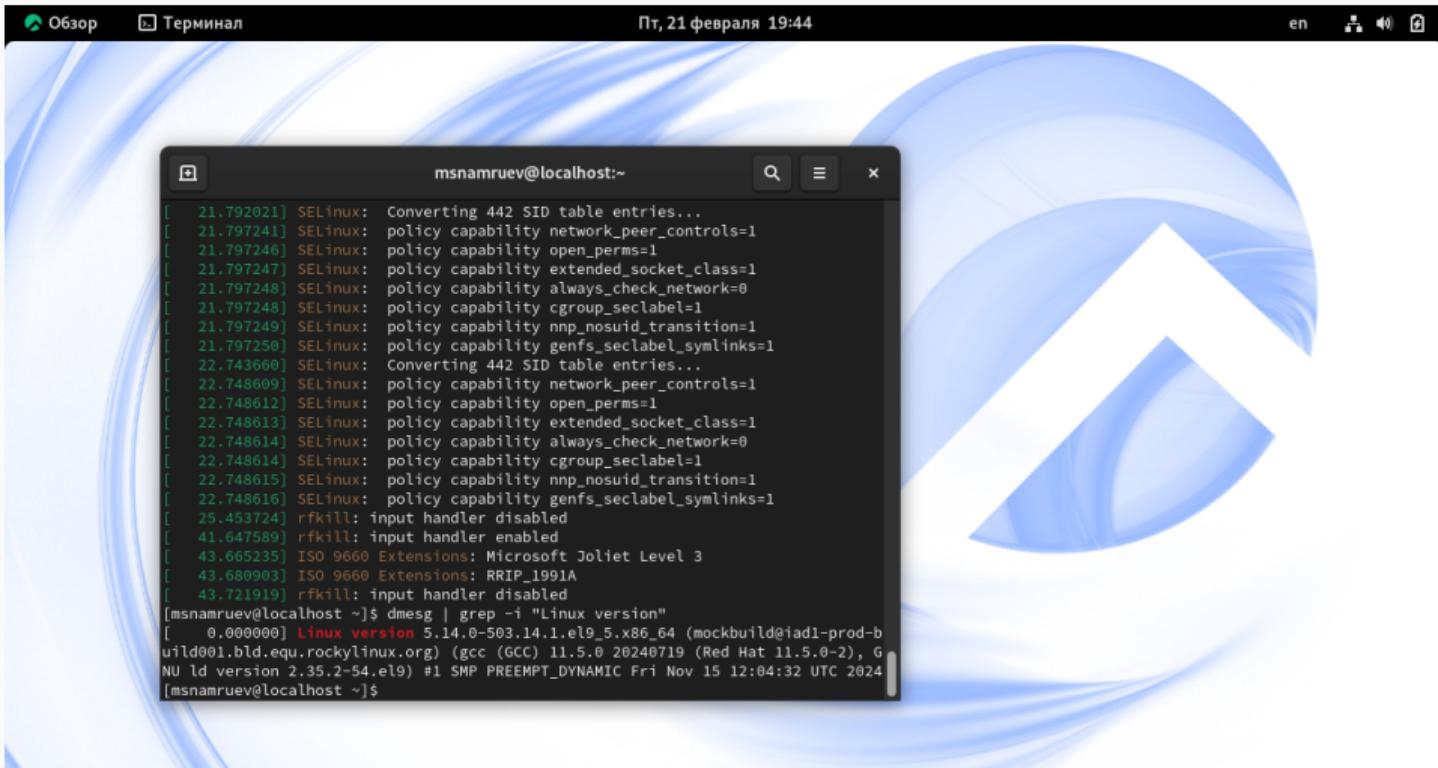
The screenshot shows a Linux desktop interface with a terminal window open. The terminal window title is "msnamruev@localhost:~". The window contains the output of the "dmesg" command, which displays kernel messages. Key messages include:

- [6.656065] e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
- [6.656414] IPv6: ADDRCONF(NETDEV_CHANGE): enp0s3: link becomes ready
- [8.396553] block dm-0: the capability attribute has been deprecated.
- [21.792021] SELinux: Converting 442 SID table entries...
- [21.797241] SELinux: policy capability network_peer_controls=1
- [21.797246] SELinux: policy capability open_perms=1
- [21.797247] SELinux: policy capability extended_socket_class=1
- [21.797248] SELinux: policy capability always_check_network=0
- [21.797248] SELinux: policy capability cgroup_seclabel=1
- [21.797249] SELinux: policy capability nnp_nosuid_transition=1
- [21.797250] SELinux: policy capability genfs_seclabel_symlinks=1
- [22.743660] SELinux: Converting 442 SID table entries...
- [22.748609] SELinux: policy capability network_peer_controls=1
- [22.748612] SELinux: policy capability open_perms=1
- [22.748613] SELinux: policy capability extended_socket_class=1
- [22.748614] SELinux: policy capability always_check_network=0
- [22.748614] SELinux: policy capability cgroup_seclabel=1
- [22.748615] SELinux: policy capability nnp_nosuid_transition=1
- [22.748616] SELinux: policy capability genfs_seclabel_symlinks=1
- [25.453724] rfkill: input handler disabled
- [41.647589] rfkill: input handler enabled
- [43.665235] ISO 9660 Extensions: Microsoft Joliet Level 3
- [43.680903] ISO 9660 Extensions: RRIP_1991A
- [43.721919] rfkill: input handler disabled

The terminal prompt at the bottom is "[msnamruev@localhost ~]\$".

Домашнее задание

С помощью поиска нахожу информацию о Версии ядра Linux.

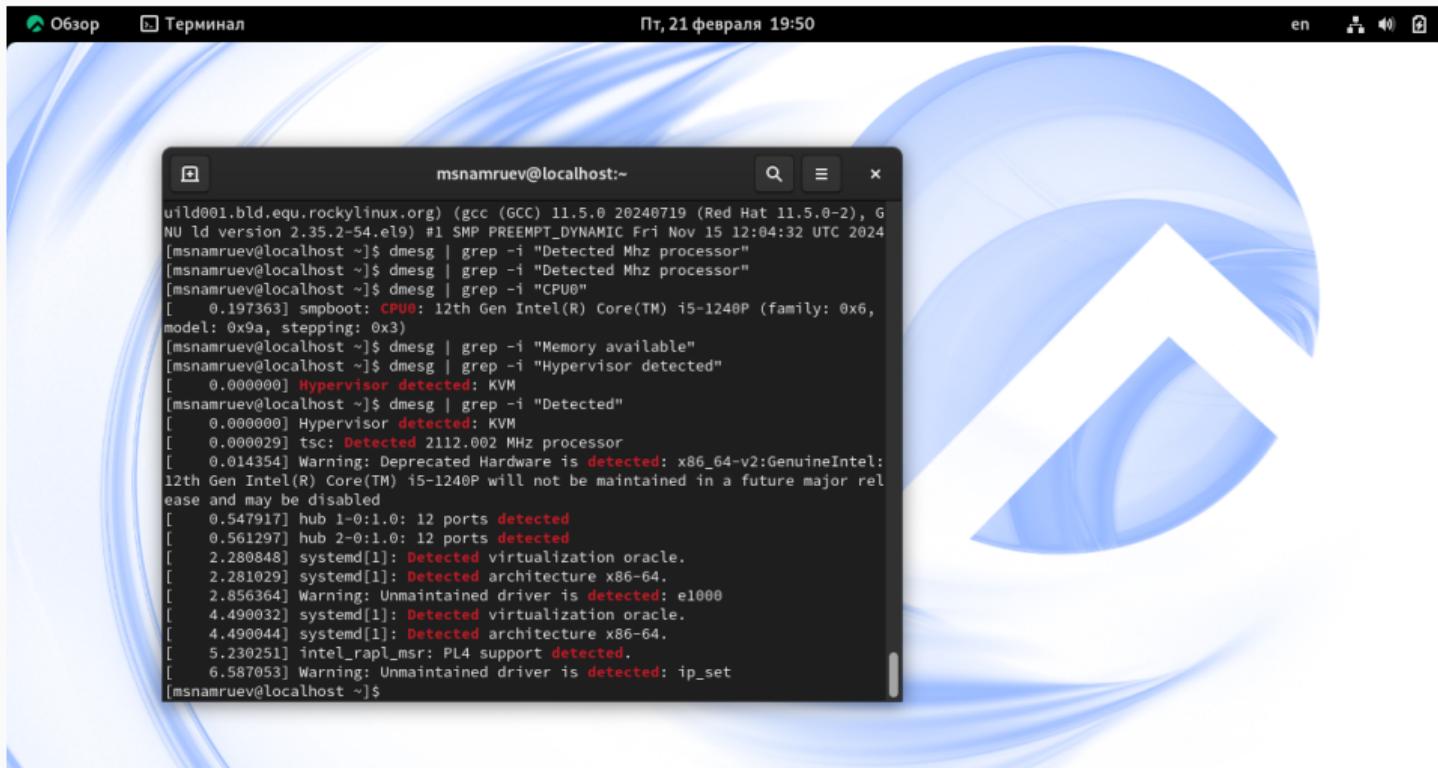


The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "msnamruev@localhost:~". The terminal displays a log of SELinux policy capability transitions and rfkill input handler status changes. At the bottom of the terminal, the command "dmesg | grep -i 'Linux version'" is run, followed by the output showing the kernel version 5.14.0-503.14.1.el9_5.x86_64. The desktop interface includes a top bar with icons for Overview, Terminal, date/time (Пт, 21 февраля 19:44), and system status (en, battery, volume, lock). A blurred background logo is visible behind the terminal window.

```
[ 21.792021] SELinux:  Converting 442 SID table entries...
[ 21.797241] SELinux:  policy capability network_peer_controls=1
[ 21.797246] SELinux:  policy capability open_perms=1
[ 21.797247] SELinux:  policy capability extended_socket_class=1
[ 21.797248] SELinux:  policy capability always_check_network=0
[ 21.797248] SELinux:  policy capability cgroup_seclabel=1
[ 21.797249] SELinux:  policy capability nnp_nosuid_transition=1
[ 21.797250] SELinux:  policy capability genfs_seclabel_symlinks=1
[ 22.743660] SELinux:  Converting 442 SID table entries...
[ 22.748609] SELinux:  policy capability network_peer_controls=1
[ 22.748612] SELinux:  policy capability open_perms=1
[ 22.748613] SELinux:  policy capability extended_socket_class=1
[ 22.748614] SELinux:  policy capability always_check_network=0
[ 22.748614] SELinux:  policy capability cgroup_seclabel=1
[ 22.748615] SELinux:  policy capability nnp_nosuid_transition=1
[ 22.748616] SELinux:  policy capability genfs_seclabel_symlinks=1
[ 25.453724] rfkill: input handler disabled
[ 41.647589] rfkill: input handler enabled
[ 43.665235] ISO 9660 Extensions: Microsoft Joliet Level 3
[ 43.689093] ISO 9660 Extensions: RRIP_1991A
[ 43.721919] rfkill: input handler disabled
[msnamruev@localhost ~]$ dmesg | grep -i "Linux version"
[    0.000000] Linux version 5.14.0-503.14.1.el9_5.x86_64 (mockbuild@jad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.5.0 20240719 (Red Hat 11.5.0-2), G
NU ld version 2.35.2-54.el9 #1 SMP PREEMPT_DYNAMIC Fri Nov 15 12:04:32 UTC 2024
[msnamruev@localhost ~]$
```

Домашнее задание

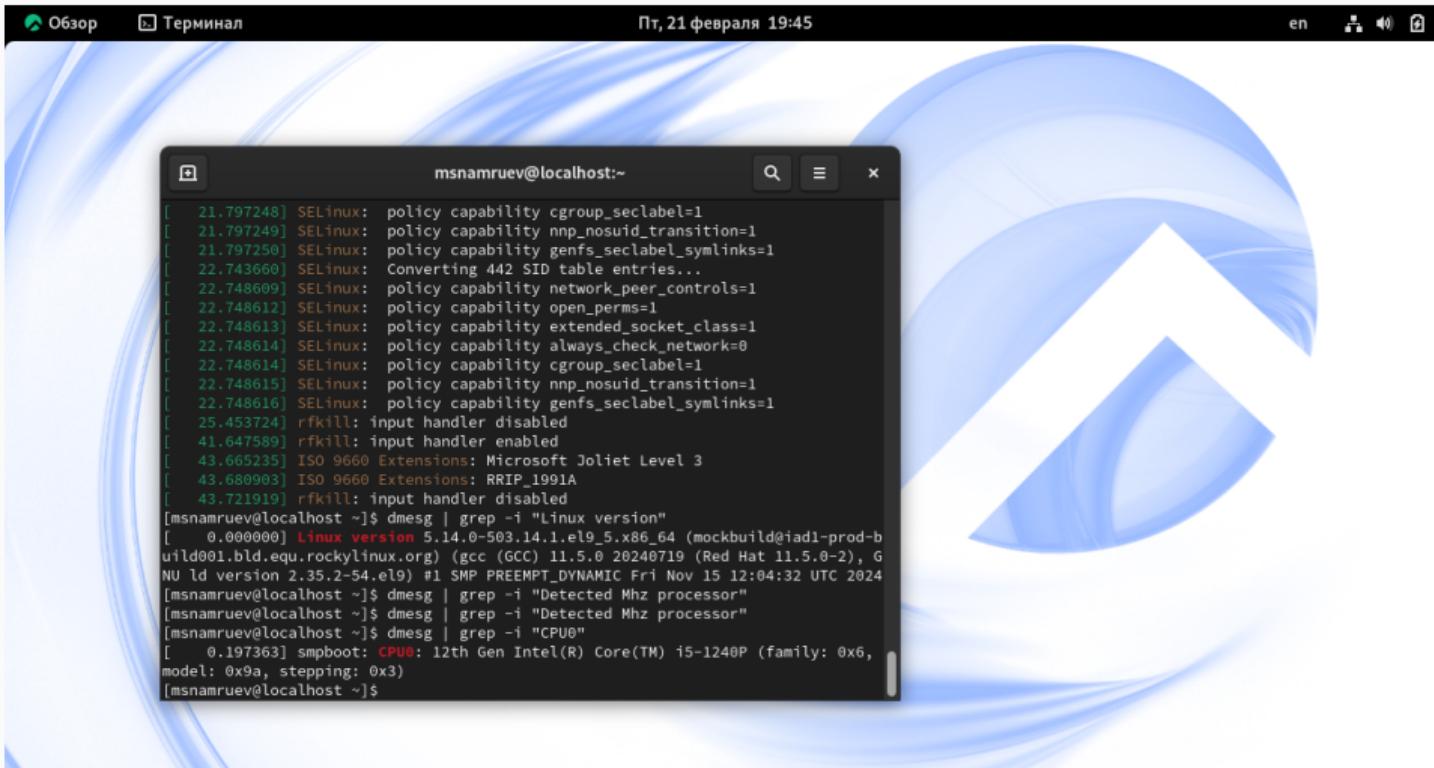
С помощью поиска нахожу информацию о Частоте процессора.



```
msnamruev@localhost:~$ dmesg | grep -i "Detected Mhz processor"
[msnamruev@localhost ~]$ dmesg | grep -i "Detected Mhz processor"
[msnamruev@localhost ~]$ dmesg | grep -i "CPU0"
[ 0.197363] smpboot: CPU0: 12th Gen Intel(R) Core(TM) i5-1240P (family: 0x6,
model: 0x9a, stepping: 0x3)
[msnamruev@localhost ~]$ dmesg | grep -i "Memory available"
[msnamruev@localhost ~]$ dmesg | grep -i "Hypervisor detected"
[ 0.000000] Hypervisor detected: KVM
[msnamruev@localhost ~]$ dmesg | grep -i "Detected"
[ 0.000000] Hypervisor detected: KVM
[ 0.000029] tsc: Detected 2112.002 MHz processor
[ 0.014354] Warning: Deprecated Hardware is detected: x86_64-v2:GenuineIntel:
12th Gen Intel(R) Core(TM) i5-1240P will not be maintained in a future major rel
ease and may be disabled
[ 0.547917] hub 1-0:1.0: 12 ports detected
[ 0.561297] hub 2-0:1.0: 12 ports detected
[ 2.280848] systemd[1]: Detected virtualization oracle.
[ 2.281029] systemd[1]: Detected architecture x86-64.
[ 2.856364] Warning: Unmaintained driver is detected: e1000
[ 4.490032] systemd[1]: Detected virtualization oracle.
[ 4.490044] systemd[1]: Detected architecture x86-64.
[ 5.230251] intel_rapl_msr: PL4 support detected.
[ 6.587053] Warning: Unmaintained driver is detected: ip_set
[msnamruev@localhost ~]$
```

Домашнее задание

С помощью поиска нахожу информацию о Модели процессора.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "msnamruev@localhost:~". The window displays a log of system events and command-line outputs. Key visible text includes:

```
[ 21.797248] SELinux: policy capability cgroup_seclabel=1
[ 21.797249] SELinux: policy capability nnp_nosuid_transition=1
[ 21.797250] SELinux: policy capability genfs_seclabel_symlinks=1
[ 22.743660] SELinux: Converting 442 SELinux table entries...
[ 22.748609] SELinux: policy capability network_peer_controls=1
[ 22.748612] SELinux: policy capability open_perms=1
[ 22.748613] SELinux: policy capability extended_socket_class=1
[ 22.748614] SELinux: policy capability always_check_network=0
[ 22.748614] SELinux: policy capability cgroup_seclabel=1
[ 22.748615] SELinux: policy capability nnp_nosuid_transition=1
[ 22.748616] SELinux: policy capability genfs_seclabel_symlinks=1
[ 25.453724] rfkill: input handler disabled
[ 41.647589] rfkill: input handler enabled
[ 43.665235] ISO 9660 Extensions: Microsoft Joliet Level 3
[ 43.689993] ISO 9660 Extensions: RRIP_1991A
[ 43.721919] rfkill: input handler disabled
[msnamruev@localhost ~]$ dmesg | grep -i "Linux version"
[ 0.000000] Linux version 5.14.0-503.14.1.el9_5.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.5.0 20240719 (Red Hat 11.5.0-2), G
NU ld version 2.35.2-54.el9) #1 SMP PREEMPT_DYNAMIC Fri Nov 15 12:04:32 UTC 2024
[msnamruev@localhost ~]$ dmesg | grep -i "Detected Mhz processor"
[msnamruev@localhost ~]$ dmesg | grep -i "Detected Mhz processor"
[msnamruev@localhost ~]$ dmesg | grep -i "CPU0"
[ 0.197363] smpboot: CPU0: 12th Gen Intel(R) Core(TM) i5-1240P (family: 0x6,
model: 0x9a, stepping: 0x3)
[msnamruev@localhost ~]$
```

Домашнее задание

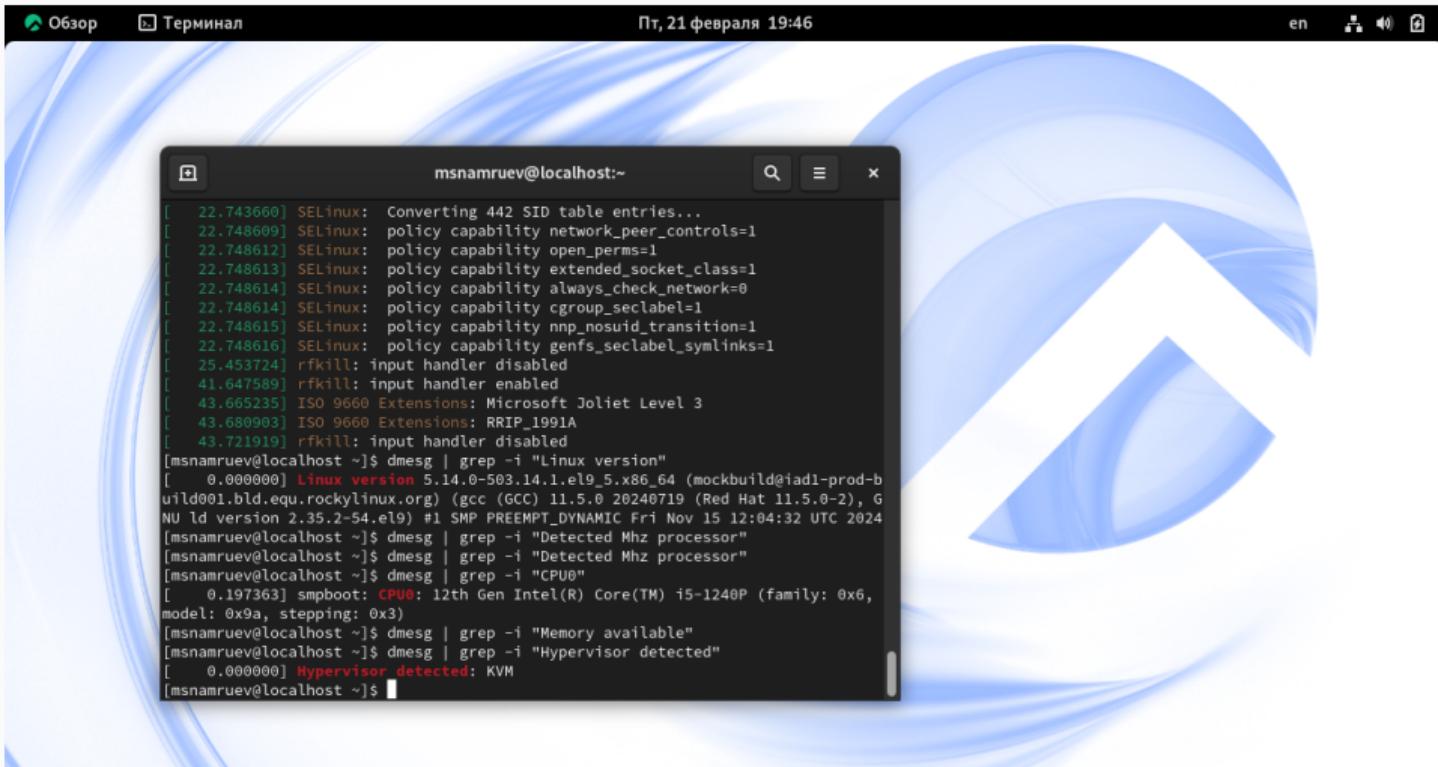
С помощью поиска нахожу информацию о Объеме доступной оперативной памяти.

The screenshot shows a terminal window titled "msnamruev@localhost:~" displaying the output of the "dmesg" command. The output lists various kernel messages related to memory freeing, file system mounting, and system initialization. A large blue and white circular logo is visible in the background.

```
[ 2.164102] Freeing unused kernel image (rodata/data gap) memory: 1432K
[msnamruev@localhost ~]$ dmesg | grep -i "Mount"
[ 0.092769] Mount-cache hash table entries: 8192 (order: 4, 65536 bytes, line
ar)
[ 0.092769] Mountpoint-cache hash table entries: 8192 (order: 4, 65536 bytes,
linear)
[ 4.005027] XFS (dm-0): Mounting V5 Filesystem 340cc6e2-4d43-4dce-b17a-ec5511
f132ad
[ 4.016848] XFS (dm-0): Ending clean mount
[ 4.869532] systemd[1]: Set up automount Arbitrary Executable File Formats Fi
le System Automount Point.
[ 4.889024] systemd[1]: Mounting Huge Pages File System...
[ 4.890248] systemd[1]: Mounting POSIX Message Queue File System...
[ 4.891517] systemd[1]: Mounting Kernel Debug File System...
[ 4.892716] systemd[1]: Mounting Kernel Trace File System...
[ 4.912047] systemd[1]: Starting Remount Root and Kernel File Systems...
[ 4.917730] systemd[1]: Mounted Huge Pages File System.
[ 4.917939] systemd[1]: Mounted POSIX Message Queue File System.
[ 4.918056] systemd[1]: Mounted Kernel Debug File System.
[ 4.918217] systemd[1]: Mounted Kernel Trace File System.
[ 4.922960] systemd[1]: Mounting FUSE Control File System...
[ 4.924404] systemd[1]: Mounting Kernel Configuration File System...
[ 5.593448] XFS (sdal): Mounting V5 Filesystem 5095287a-3266-49ba-b931-99a904
6ffffa9
[ 5.623897] XFS (sdal): Ending clean mount
[msnamruev@localhost ~]$
```

Домашнее задание

С помощью поиска нахожу информацию о типе обнаруженного гипервизора.

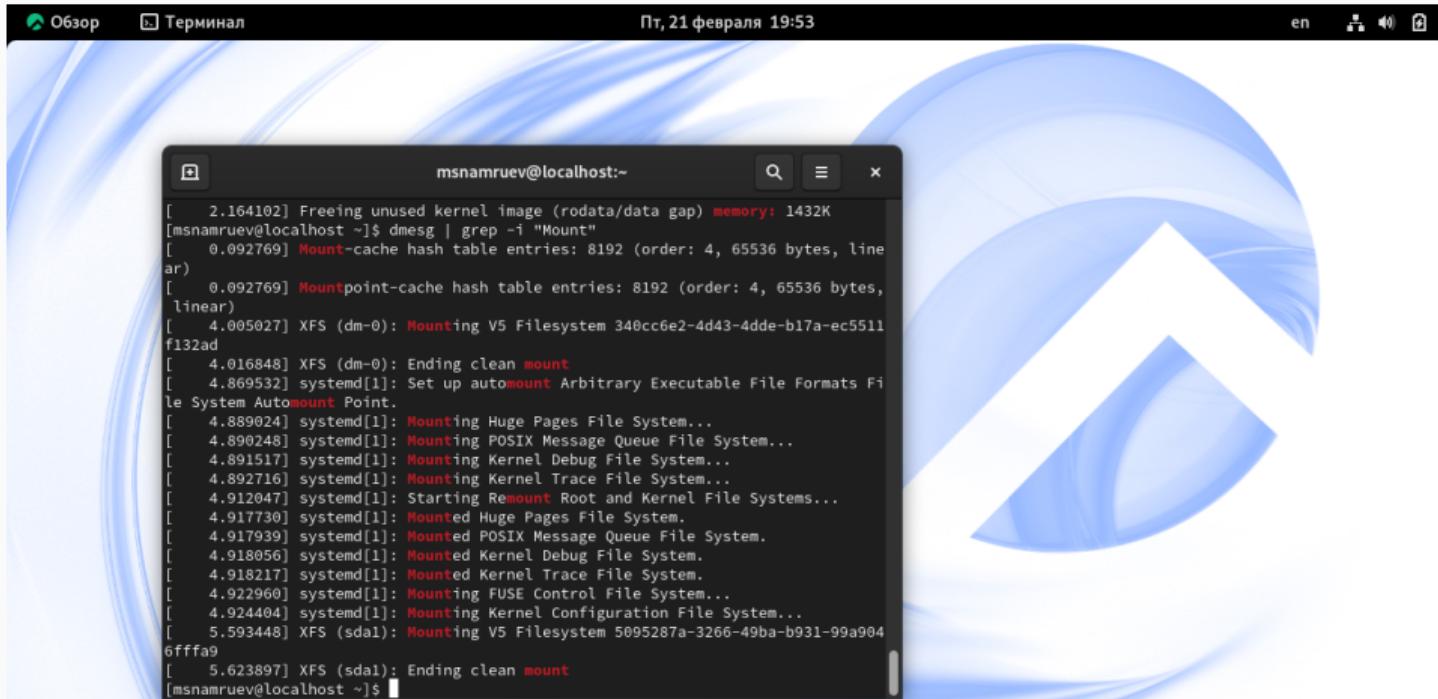


The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "msnamruev@localhost:~". The window contains the following log output:

```
[ 22.743660] SELinux:  Converting 442 SID table entries...
[ 22.748609] SELinux: policy capability network_peer_controls=1
[ 22.748612] SELinux: policy capability open_perms=1
[ 22.748613] SELinux: policy capability extended_socket_class=1
[ 22.748614] SELinux: policy capability always_check_network=0
[ 22.748614] SELinux: policy capability cgroup_seclabel=1
[ 22.748615] SELinux: policy capability nnp_nosuid_transition=1
[ 22.748616] SELinux: policy capability gens_seclabel_symlinks=1
[ 25.453724] rfkill: input handler disabled
[ 41.647589] rfkill: input handler enabled
[ 43.665235] ISO 9660 Extensions: Microsoft Joliet Level 3
[ 43.680903] ISO 9660 Extensions: RRIP_1991A
[ 43.721919] rfkill: input handler disabled
[msnamruev@localhost ~]$ dmesg | grep -i "Linux version"
[ 0.000000] Linux version 5.14.0-503.14.1.el9_5.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.5.0 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
[msnamruev@localhost ~]$ dmesg | grep -i "Detected Mhz processor"
[msnamruev@localhost ~]$ dmesg | grep -i "Detected Mhz processor"
[msnamruev@localhost ~]$ dmesg | grep -i "CPU0"
[ 0.197363] smpboot: CPU0: 12th Gen Intel(R) Core(TM) i5-1240P (family: 0x6,
model: 0x9a, stepping: 0x3)
[msnamruev@localhost ~]$ dmesg | grep -i "Memory available"
[msnamruev@localhost ~]$ dmesg | grep -i "Hypervisor detected"
[ 0.000000] Hypervisor detected: KVM
[msnamruev@localhost ~]$
```

Домашнее задание

С помощью поиска нахожу информацию о Типе файловой системы корневого раздела.

A large, semi-transparent watermark of the Ubuntu logo (a blue and white triangle) is positioned in the background of the terminal window.

```
msnamruev@localhost:~$ lsblk
lsblk: no such command
msnamruev@localhost:~$ df -h
Filesystem      Size  Used  Avail   Type   Mounted on
/dev/sda1        10G   10G     0K  ext4   /
tmpfs           1.9G  1.9G     0K  tmpfs  /tmp
msnamruev@localhost:~$ mount | grep -i 'xfs|ext4'
/dev/sda1 on / type ext4 (rw)
msnamruev@localhost:~$
```

msnamruev@localhost:~\$ cat /proc/mounts

```
[ 2.164102] Freeing unused kernel image (rodata/data gap) memory: 1432K
[msnamruev@localhost ~]$ dmesg | grep -i "Mount"
[ 0.092769] Mount-cache hash table entries: 8192 (order: 4, 65536 bytes, linear)
[ 0.092769] Mountpoint-cache hash table entries: 8192 (order: 4, 65536 bytes, linear)
[ 4.005027] XFS (dm-0): Mounting V5 Filesystem 340cc6e2-4d43-4dde-b17a-ec5511f132ad
[ 4.016848] XFS (dm-0): Ending clean mount
[ 4.869532] systemd[1]: Set up automount Arbitrary Executable File Formats File System Automount Point.
[ 4.889024] systemd[1]: Mounting Huge Pages File System...
[ 4.890248] systemd[1]: Mounting POSIX Message Queue File System...
[ 4.891517] systemd[1]: Mounting Kernel Debug File System...
[ 4.892716] systemd[1]: Mounting Kernel Trace File System...
[ 4.912047] systemd[1]: Starting Remount Root and Kernel File Systems...
[ 4.917730] systemd[1]: Mounted Huge Pages File System.
[ 4.917939] systemd[1]: Mounted POSIX Message Queue File System.
[ 4.918056] systemd[1]: Mounted Kernel Debug File System.
[ 4.918217] systemd[1]: Mounted Kernel Trace File System.
[ 4.922960] systemd[1]: Mounting FUSE Control File System...
[ 4.924404] systemd[1]: Mounting Kernel Configuration File System...
[ 5.593448] XFS (sda1): Mounting V5 Filesystem 5095287a-3266-49ba-b931-99a9046ffffa9
[ 5.623897] XFS (sda1): Ending clean mount
[msnamruev@localhost ~]$
```

Выводы

после выполнения данной лабораторной работы я установил rocky linux на ВМ