

# Отчёт по лабораторной работе №1

## Основы информационной безопасности

Лисенков Е.Р.

### Содержание

1	Цель работы .....	1
2	Задачи .....	1
3	Выполнение лабораторной работы.....	1
4	Выводы.....	9
5	Ответы на контрольные вопросы.....	9
5.1	Какую информацию содержит учётная запись пользователя? .....	9
5.2	Укажите команды терминала и приведите примеры. ....	9
5.3	Что такое файловая система? .....	10
5.4	Как посмотреть, какие файловые системы подмонтированы в ОС? .....	10
5.5	Как удалить зависший процесс? .....	10

### 1 Цель работы

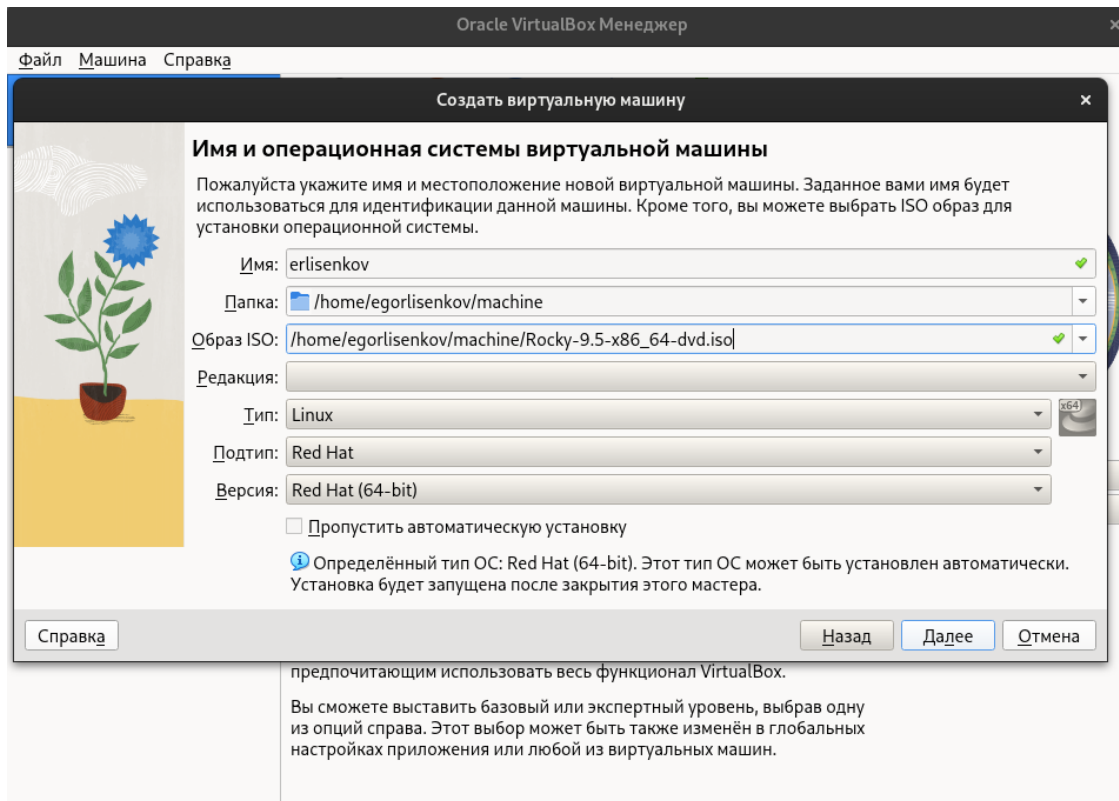
Целью данной работы является приобретение практических навыков установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов.

### 2 Задачи

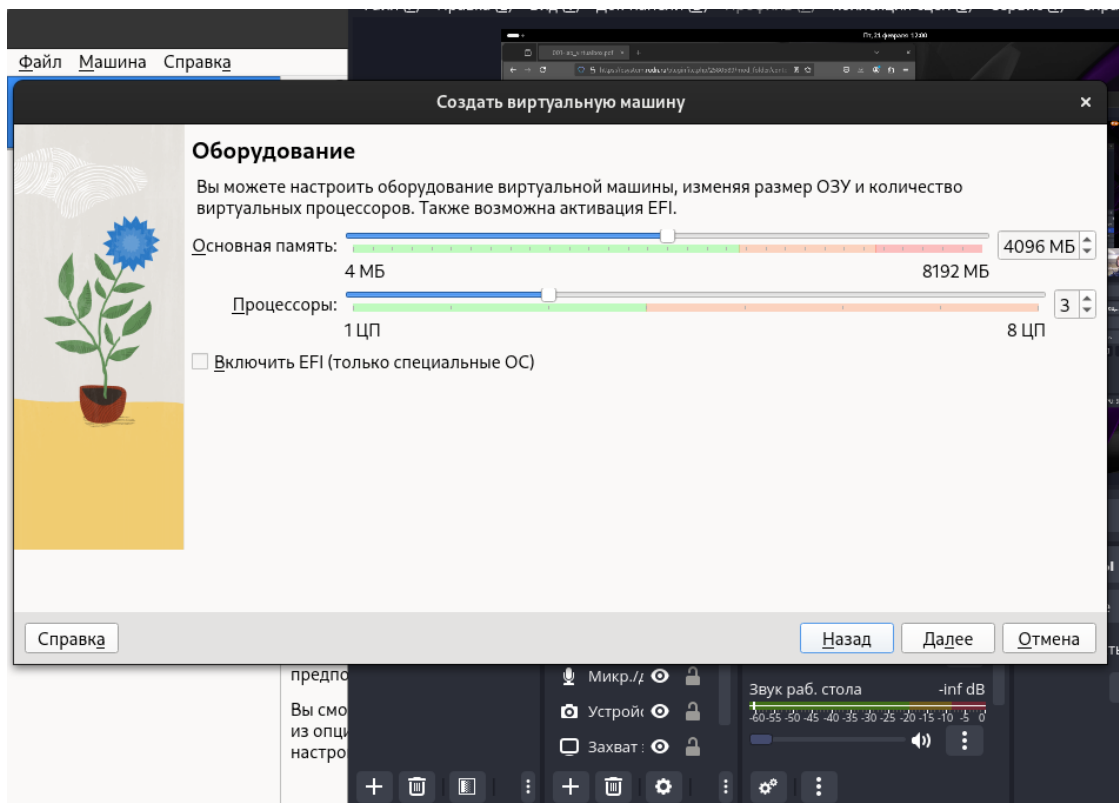
Установить Rocky Linux на виртуальную машину

### 3 Выполнение лабораторной работы

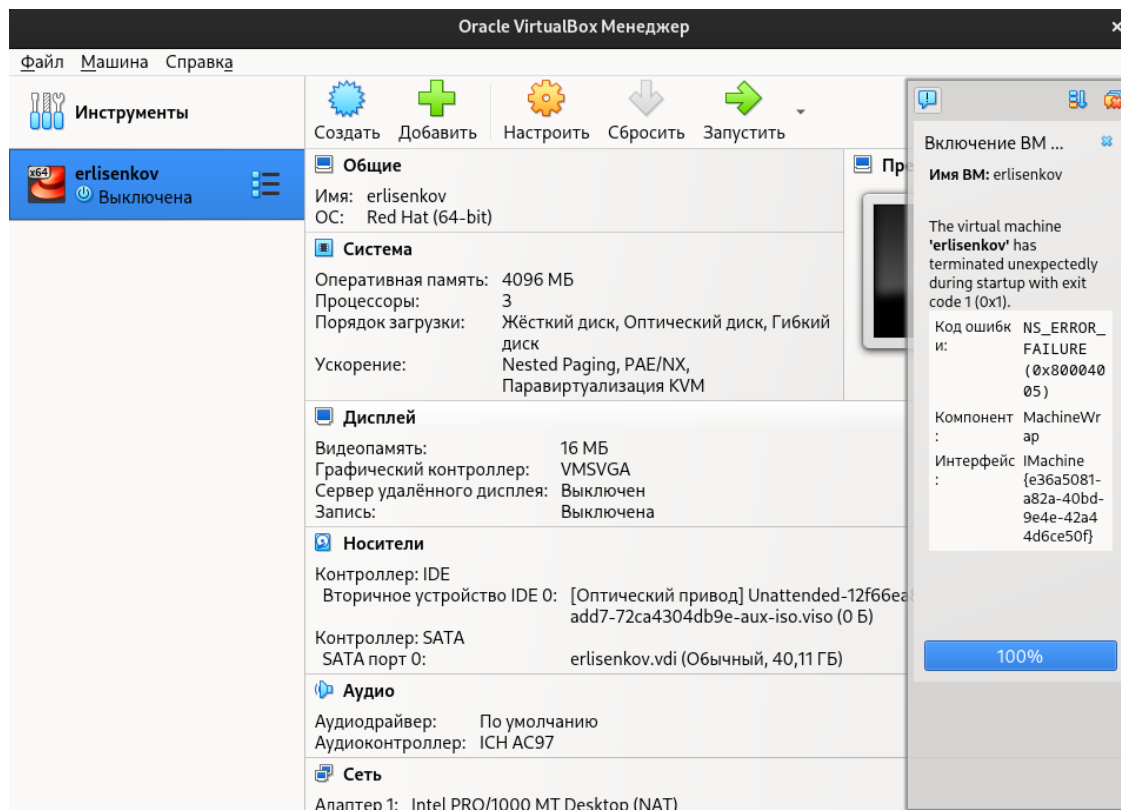
Начинаю настройку виртуальной машины, чтобы в последующем установить её (рис.1).



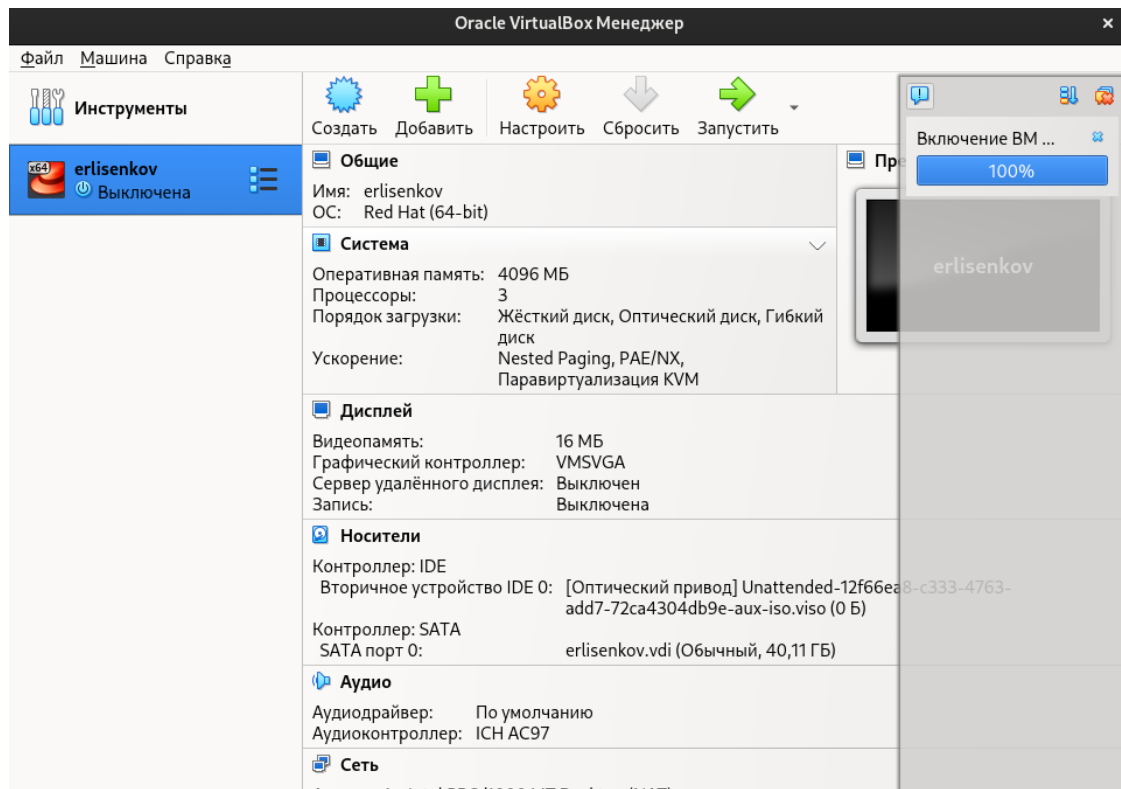
Расширяю память для виртуальной машины (рис.2)



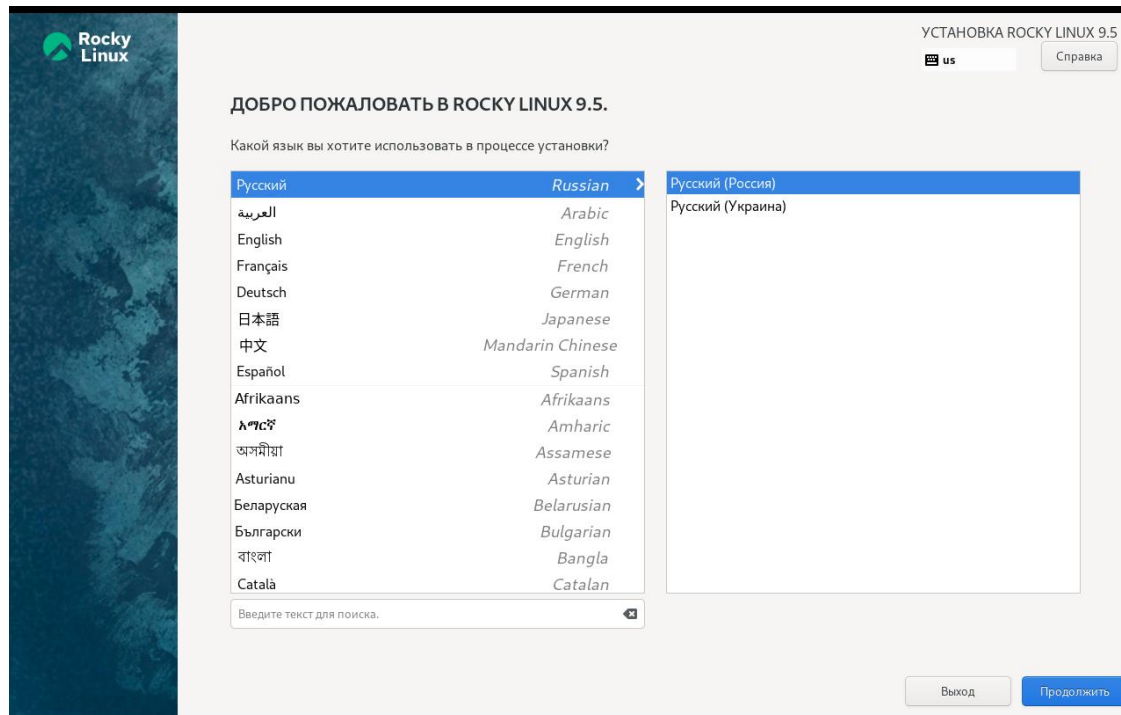
Проверяю окончательные настройки. (рис. 3)



(рис.4)



Запускаю виртуальную машину и приступаю к настройке внутренних компонентов. (рис.5).



Выбираю инструмент для разработчика чтобы в будущем пользоваться всеми функциями линукса (рис.6)

SOFTWARE SELECTION

ROCKY LINUX 9.5 INSTALLATION

Done

us

Help!

Base Environment

☒ **Server with GUI**  
An integrated, easy-to-manage server with a graphical interface.

☐ **Server**  
An integrated, easy-to-manage server.

☐ **Minimal Install**  
Basic functionality.

☐ **Workstation**  
Workstation is a user-friendly desktop system for laptops and PCs.

☐ **Custom Operating System**  
Basic building block for a custom Rocky Linux system.

☐ **Virtualization Host**  
Minimal virtualization host.

Additional software for Selected Environment

☐ **Virtualization Client**  
Clients for installing and managing virtualization instances.

☐ **Virtualization Hypervisor**  
Smallest possible virtualization host installation.

☐ **Virtualization Tools**  
Tools for offline virtual image management.

☐ **Basic Web Server**  
These tools allow you to run a Web server on the system.

☐ **Legacy UNIX Compatibility**  
Compatibility programs for migration from or working with legacy UNIX environments.

☐ **Console Internet Tools**  
Console internet access tools, often used by administrators.

☐ **Container Management**  
Tools for managing Linux containers

☒ **Development Tools**  
A basic development environment.

☐ **.NET Development**  
Tools to develop and/or run .NET applications

☐ **Graphical Administration Tools**  
Graphical system administration tools for managing many aspects of a system.

☐ **Headless Management**  
Tools for managing the system without an attached graphical console.

☐ **RPM Development Tools**  
Tools used for building RPMs, such as rpmbuild.

☐ **Scientific Support**  
Tools for mathematical and scientific computations, and parallel computing.

☐ **Security Tools**  
Security tools for integrity and trust verification.

☐ **Smart Card Support**  
Support for using smart card authentication.

☐ **System Tools**  
This group is a collection of various tools for the system, such as the client for connecting to SMB shares and tools to monitor network traffic.

## Окно настройки установки: отключение KDUMP (рис. 7)

KDUMP

ROCKY LINUX 9.5 INSTALLATION

Done

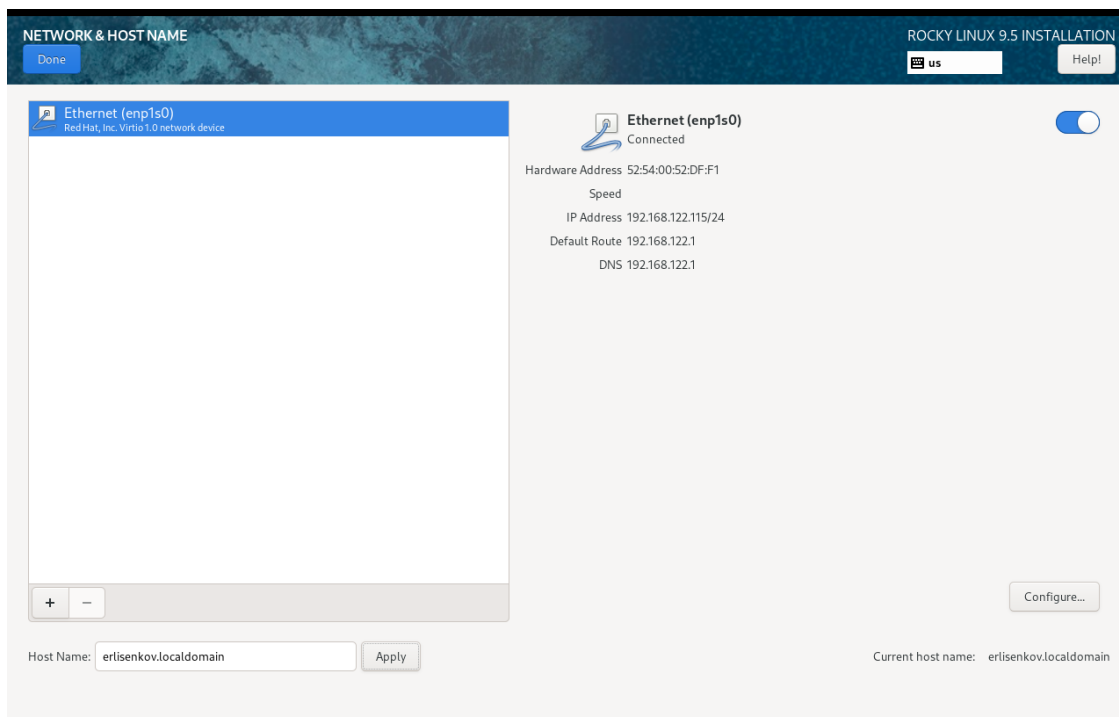
us

Help!

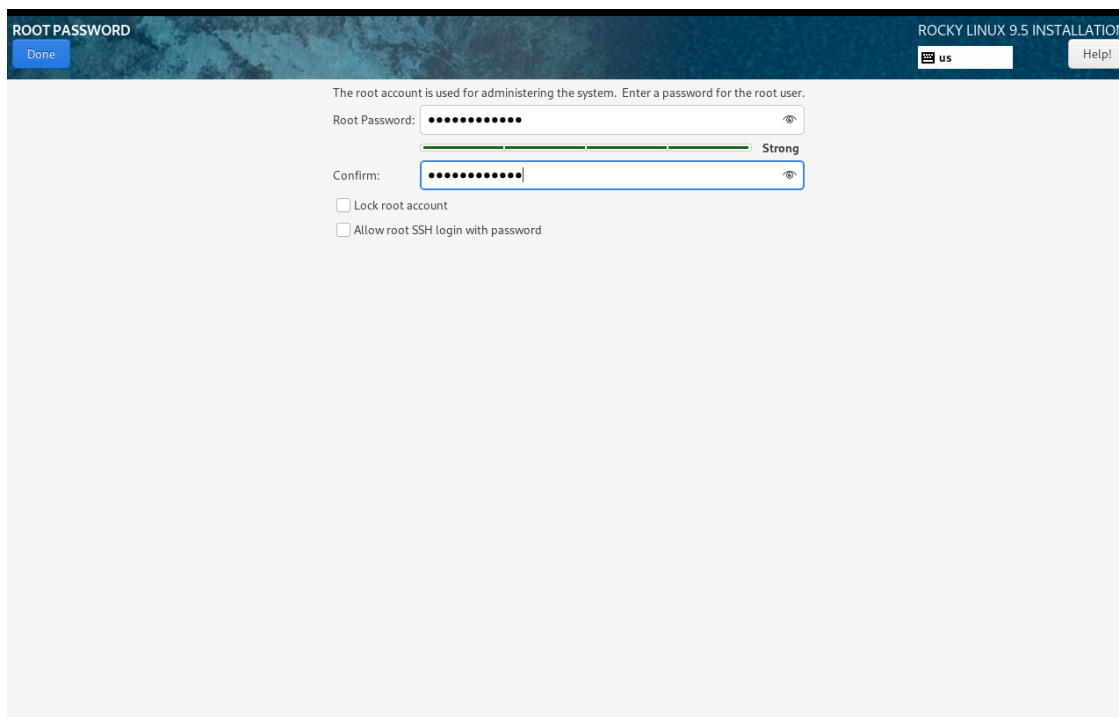
Kdump is a kernel crash dumping mechanism. In the event of a system crash, kdump will capture information from your system that can be invaluable in determining the cause of the crash. Note that kdump does require reserving a portion of system memory that will be unavailable for other uses.

☐ Enable kdump

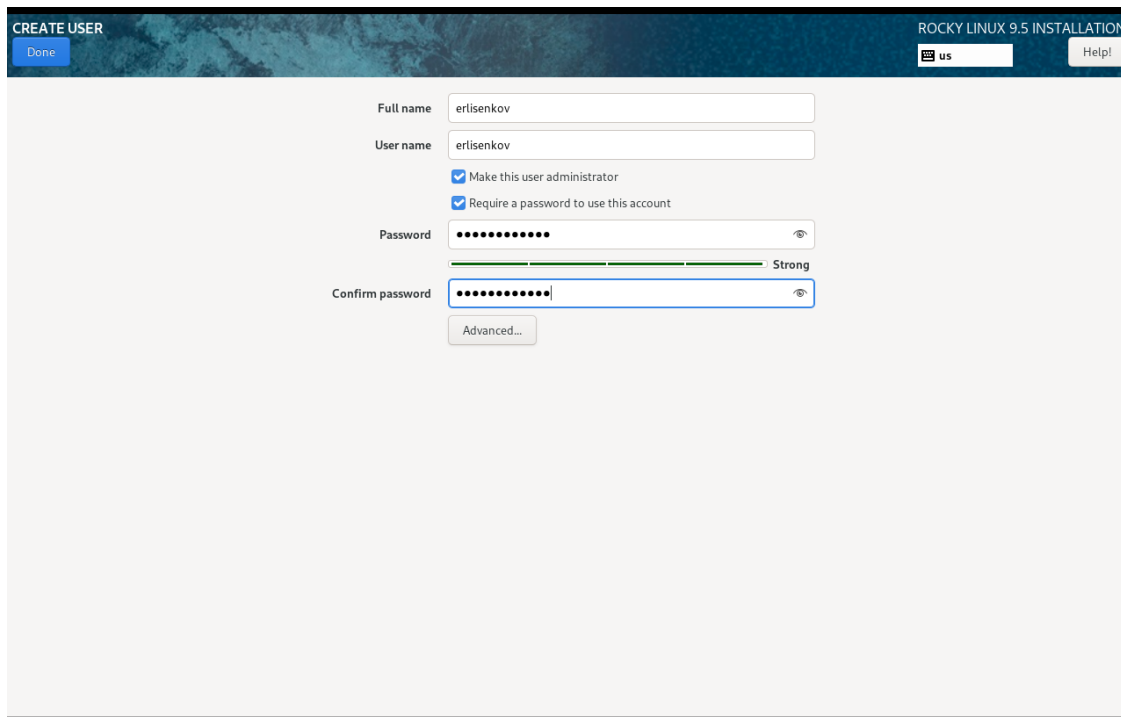
## Окно настройки установки: сеть и имя узла(рис.8).



## Установка пароля для root (рис.9)



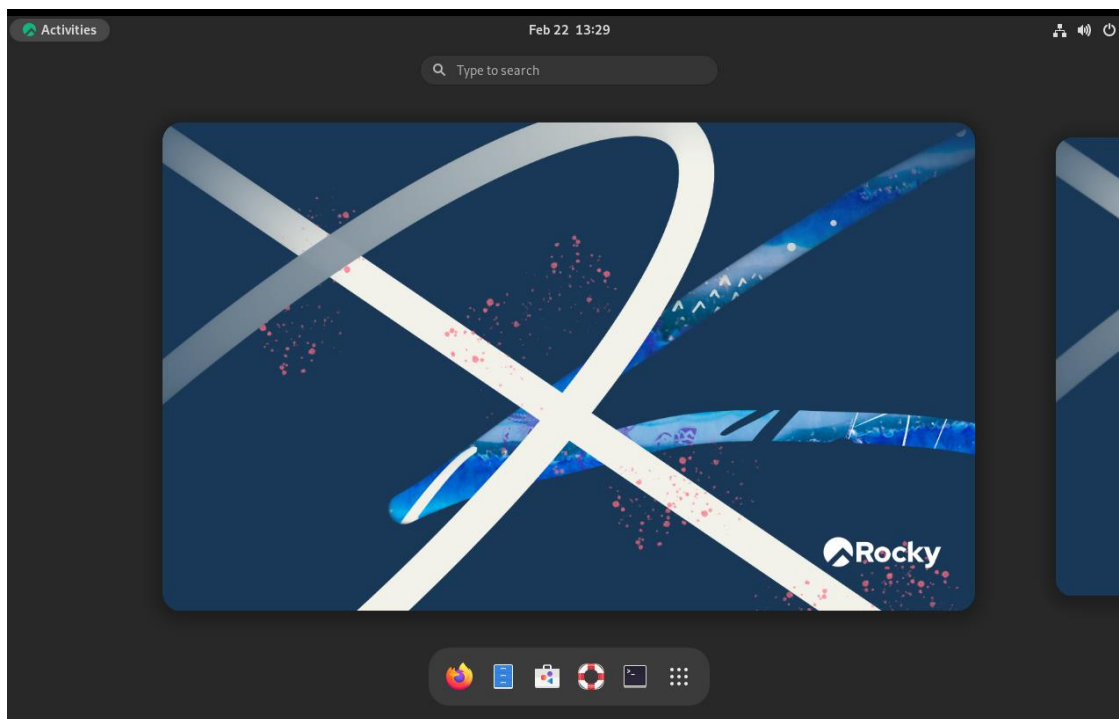
## Установка пароля для пользователя с правами администратора (рис. 10)



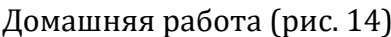
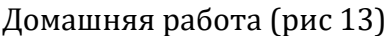
The image shows the 'CREATE USER' screen in the Rocky Linux 9.5 installation environment. The header bar is dark blue with 'CREATE USER' on the left, 'ROCKY LINUX 9.5 INSTALLATION' on the right, and a 'Done' button. Below the header, the form contains the following fields and options:

- Full name:** A text input field containing 'erlisenkov'.
- User name:** A text input field containing 'erlisenkov'.
- Options:** Two checked checkboxes: 'Make this user administrator' and 'Require a password to use this account'.
- Password:** A password input field with a strength indicator below it showing 'Strong'.
- Confirm password:** A second password input field.
- Advanced...:** A button to expand additional options.

Да здравствует 52 и линукс который успешно скачался (рис. 11)



Небольшая информация о системе, чтобы понять что мы сделали всё правильно (рис. 12)





```
Activities Terminal Feb 22 13:48
erlisenkov@erlisenkov:~
[erlisenkov@erlisenkov ~]$ 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
[erlisenkov@erlisenkov ~]$ dmesg | grep -i "Mhz"
[ 0.000005] tsc: Detected 1799.986 MHz processor
[erlisenkov@erlisenkov ~]$ dmesg | grep -i "CPU"
[erlisenkov@erlisenkov ~]$ dmesg | grep -i "CPU0"
[ 0.067444] smpboot: CPU0: Intel(R) Core(TM) i5-9265U CPU @ 1.60GHz (family: 0x6, model: 0x8e, stepping: 0xc)
[erlisenkov@erlisenkov ~]$ dmesg | grep -i "Memory:"
[ 0.017003] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x00000fff]
[ 0.017004] PM: hibernation: Registered nosave memory: [mem 0x0009f000-0x0009ffff]
[ 0.017005] PM: hibernation: Registered nosave memory: [mem 0x000a0000-0x000aefff]
[ 0.017006] PM: hibernation: Registered nosave memory: [mem 0x000f0000-0x000fffff]
[ 0.017007] PM: hibernation: Registered nosave memory: [mem 0x7ffdb000-0x7fffffff]
[ 0.017007] PM: hibernation: Registered nosave memory: [mem 0x80000000-0xffffffff]
[ 0.017008] PM: hibernation: Registered nosave memory: [mem 0xb0000000-0xbfffffff]
[ 0.017008] PM: hibernation: Registered nosave memory: [mem 0xc0000000-0xfed1bfff]
[ 0.017009] PM: hibernation: Registered nosave memory: [mem 0xfed1c000-0xfed1ffff]
[ 0.017009] PM: hibernation: Registered nosave memory: [mem 0xfed20000-0xfefbffff]
[ 0.017010] PM: hibernation: Registered nosave memory: [mem 0xfefc0000-0xfefcffff]
[ 0.017010] PM: hibernation: Registered nosave memory: [mem 0xffff0000-0xffffffff]
[ 0.017011] PM: hibernation: Registered nosave memory: [mem 0xffffc000-0xffffffff]
[ 0.040894] Memory: 2103600K/3096036K available (16384K kernel code, 5685K rdata, 12904K rodata, 3976K init, 5672K bss, 234496K reserve
d, 0K cma-reserved)
[ 0.067444] Freeing SMP alternatives memory: 40K
[ 1.124665] Freeing initrd memory: 57656K
[ 1.358900] Freeing unused decrypted memory: 2028K
[ 1.359695] Freeing unused kernel image (initmem) memory: 3976K
[ 1.360702] Freeing unused kernel image (rodata/data gap) memory: 1432K
[erlisenkov@erlisenkov ~]$ dmesg | grep "Memory:"
[ 0.040894] Memory: 2103600K/3096036K available (16384K kernel code, 5685K rdata, 12904K rodata, 3976K init, 5672K bss, 234496K reserve
d, 0K cma-reserved)
[erlisenkov@erlisenkov ~]$ dmesg | grep "Hypervisor"
[ 0.000000] Hypervisor detected: KVM
[erlisenkov@erlisenkov ~]$ dmesg | grep "filesystem"
[erlisenkov@erlisenkov ~]$ dmesg | grep "File system"
[erlisenkov@erlisenkov ~]$ dmesg | grep -i "File system"
[ 1.48216] systemd[1]: Reached target Initrd /usr File System.
[ 4.082101] systemd[1]: Set up automount Arbitrary Executable File Formats File System Automount Point.
[ 4.082282] systemd[1]: Stopped target Initrd File Systems.
[ 4.082308] systemd[1]: Stopped target Initrd Root File System.
[ 4.082395] systemd[1]: Reached target Remote File Systems.
```

## 4 Выводы

Я усвоил материал и готов к дальнейшему изучению линукс!

## 5 Ответы на контрольные вопросы

### 5.1 Какую информацию содержит учётная запись пользователя?

Учётная запись пользователя в Linux содержит следующую информацию: имя пользователя (Username) — уникальное имя для идентификации пользователя; UID (User ID) — уникальный числовой идентификатор пользователя; группа (Group) — основная группа, к которой принадлежит пользователь, а также дополнительные группы; GID (Group ID) — числовой идентификатор основной группы; домашний каталог (Home Directory) — каталог, назначенный пользователю для хранения его файлов; оболочка (Shell) — команда оболочки, которая запускается при входе пользователя в систему.

### 5.2 Укажите команды терминала и приведите примеры.

Для получения справки по команде используйте `man` или `-help`. Например, `man ls` или `ls -help`. Для перемещения по файловой системе используется `cd`, например, `cd /home/user`. Для просмотра содержимого каталога применяйте `ls`, например, `ls -l /home/user`. Чтобы определить объём каталога, используйте `du -sh`, например, `du -sh /home/user`. Для создания каталогов применяйте `mkdir`, например, `mkdir myfolder`. Для создания файла используйте `touch`, например, `touch myfile.txt`. Для удаления

файла применяйте `rm` , например, `rm myfile.txt`. Для удаления каталога используйте `rmdir` (если пустой) или `rm -rf` (рекурсивно), например, `rmdir myfolder` или `rm -rf myfolder`. Для задания прав на файл/каталог используйте `chmod` , например, `chmod 755 myfile.txt`. Также можно изменить владельца и группу с помощью `chown` : , например, `chown user:group myfile.txt`. Для просмотра истории команд используйте `history`.

### 5.3 Что такое файловая система?

Приведите примеры с краткой характеристикой. Файловая система — это способ организации данных на диске или другом накопителе. Она определяет, как данные будут храниться, индексироваться и извлекаться. Примеры файловых систем: `ext4` — современная файловая система Linux, поддерживающая большие тома и файлы, имеет журнал операций для надёжности; `NTFS` — используется в Windows, поддерживает большие файлы и шифрование; `FAT32` — старая файловая система, совместимая со многими операционными системами, но с ограничением размера файла (4 ГБ).

### 5.4 Как посмотреть, какие файловые системы подмонтированы в ОС?

Используйте команду `df -hT` для просмотра подключённых файловых систем. Эта команда покажет все подмонтированные файловые системы, их типы и использование дискового пространства.

### 5.5 Как удалить зависший процесс?

Чтобы удалить зависший процесс, выполните следующие шаги: найдите PID (идентификатор процесса) с помощью команды `ps aux` или `top`, например, `ps aux | grep` . Затем убейте процесс с помощью команды `kill` или `kill -9` для принудительного завершения, например, `kill 1234` или `kill -9 1234`.