

Программный  
«SimuStrike»

комплекс

Руководство администратора

## Аннотация

Данный документ представляет собой руководство администратора для работы с программным комплексом по защите системно-технической инфраструктуры «SimuStrike» (далее – ПК «SimuStrike», комплекс). Руководство содержит сведения, необходимые пользователям для установки и настройки работы комплекса. Администратор должен знать стандартные программные средства (операционные системы, утилиты, офисные пакеты, антивирусные пакеты), а также обладать общими знаниями по администрированию сетевых устройств.

ПК «SimuStrike» служит для специалистов следующих направлений:

- по информационной безопасности (ИБ). Позволяет использовать комплекс для регулярного тестирования устойчивости информационной инфраструктуры и проверки наличия уязвимостей;
- центра мониторинга и реагирования на киберугрозы, которые занимаются обеспечением кибербезопасности. Комплекс позволяет оценить, что центр отслеживает все атаки на инфраструктуру, а также для оценить реакцию установленных продуктов ИБ на угрозы;
- групп инженеров по тестированию на проникновение. Использование комплекса для автоматизации проверки инфраструктуры позволяет повысить эффективность тестирования.

## Содержание

1	Сведения о комплексе, технические и программные средства, обеспечивающие выполнение функций программы .....	4
1.1	Общие сведения о комплексе .....	4
1.2	Требования к составу и параметрам технических средств.....	5
1.3	Требования к сетевым портам ПК «Simustrike» .....	5
1.4	Системные требования.....	6
1.4.1	Платформа .....	6
1.4.2	Резидент .....	6
1.4.3	Агент .....	6
2	Общие указания по установке комплекса .....	8
3	Установка запуск программного комплекса SimuStrike.....	9
3.1	Установка РЕД ОС 7.3 на VMware Workstation Pro .....	9
3.2	Распаковка дистрибутива bas_core .....	21
3.3	Редактирование конфигурационного файла .....	24
3.4	Установка РЕД ОС 7.3 и Docker на ЭВМ с резидентом.....	33
3.5	Установка резидента.....	37
4	Рекомендуемая последовательность действий при работе с комплексом.....	58
5	Лицензирование .....	60
5.1	Основные положения лицензирования .....	60
5.2	Ограничения срока действия лицензии комплекса.....	60
5.2.1	Ограничение по сроку действия .....	60
5.2.2	Ограничения по функциональным модулям .....	61
5.2.3	Ограничение по количеству уникальных хостов.....	61
	Перечень терминов и определений.....	62
	Перечень сокращений .....	63

# 1 Сведения о комплексе, технические и программные средства, обеспечивающие выполнение функций программы

## 1.1 Общие сведения о комплексе

ПК «SimuStrike» является продуктом класса Breach and Attack Simulation (BAS) и предназначен для специалистов по ИБ для регулярного тестирования устойчивости информационной инфраструктуры и проверки наличия уязвимостей.

Более подробно класс решаемых задач рассмотрен в документе «Описание применения».

**Примечание.** В текущем релизе функциональные возможности комплекса работают в тестовом режиме, поэтому реализован доступ с ограниченной функциональностью.

ПК «SimuStrike» состоит из централизованного сервера и веб-интерфейса. Сервер отвечает за запуск автоматизированных сценариев кибератак, а интерфейс позволяет конфигурировать многоэтапные атаки, собирая их из готовых модулей, и отслеживать реакцию систем защиты в реальном времени.

Ниже представлена схема основных компонентов ПК «SimuStrike» (рис. 1).

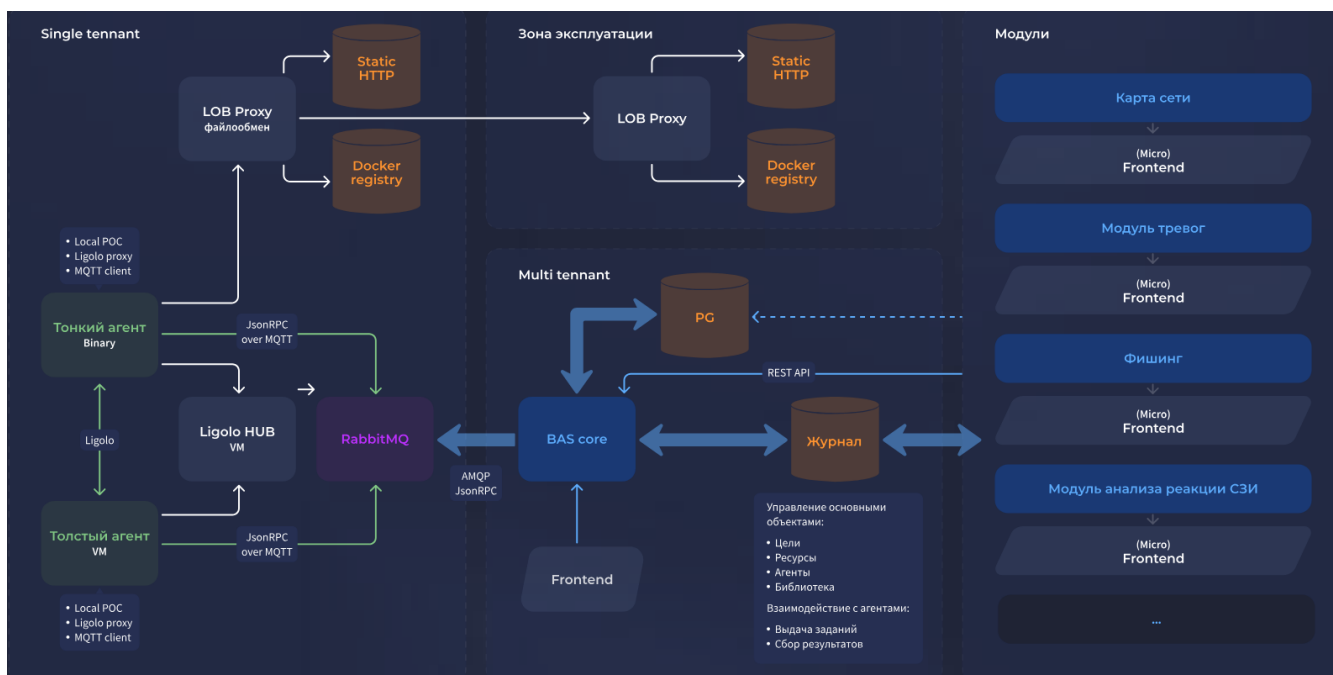


Рисунок 1 – Схема основных компонентов ПК «SimuStrike»

## 1.2 Требования к составу и параметрам технических средств

Технические характеристики электронных вычислительных машин (ЭВМ), на базе которых созданы автоматизированные рабочие места (АРМ) оператора и администратора ПК, должны иметь характеристики, приведенные ниже.

Для АРМ ПК не ниже:

- процессор с частотой не менее 1,8 ГГц;
- оперативное запоминающее устройство (ОЗУ) с объемом памяти не менее 8 Гбайт;
- жесткий диск объемом не менее 100 Гбайт;
- сетевой адаптер с пропускной способностью не менее 100Мбит/1Гбит/с.

Для сервера ПК не ниже:

- 8-и ядерный процессор с частотой не менее 1.8 ГГц;
- ОЗУ с объемом памяти не менее 16 Гбайт;
- жесткий диск объемом не менее 500 Гбайт;
- сетевой адаптер с пропускной способностью не менее 1Гбит/с.

Для корректной работы сервера управления ПК необходимы следующие программные средства:

- операционная система: ОС семейства Linux (версия ядра 5.19 и выше).
- СУБД:
  - PostgreSQL 13 и выше;
  - Jatoba, сертификат соответствия № 4327 (выдан ФСТЭК России 19.11.2020 г.);
- программное обеспечение Docker Engine актуальной версии.

## 1.3 Требования к сетевым портам ПК «Simustrike»

- 1) Платформа
  - Подключение к внешней СУБД PSGr – порт 5432/TCP;
  - Синхронизация времени (NTP) – порт 123/UDP;
  - Подключение к почтовым серверам SMTP – порт 25/TCP;
  - Удалённое управление комплексом SSH – порт 22/TCP;
  - Веб-интерфейс пользователя:
    - HTTP – порт 80/TCP;
    - HTTPS – порт 443/TCP.
  - Подключение к подсистеме LOB – порт 8444/TCP.
- 2) Резидент
  - Подключение платформы и агентов к резиденту – порт 1884/TCP;
  - Подключение агентов к системе LOB на резиденте – порт 8888/TCP.

## 1.4 Системные требования

### 1.4.1 Платформа

Программные требования:

- Операционная система: РедОС 7.3 или новее;
- Дополнительное ПО:
  - Docker (рекомендуемая версия: 28.x);
  - Docker Compose (версия 2.0 или новее).

Минимальные аппаратные требования:

- Процессор: 4 ядра (рекомендуется 8 ядер);
- Оперативная память: 8 ГБ (рекомендуется 16 ГБ);
- Дисковое пространство: 100 ГБ.

### 1.4.2 Резидент

Программные требования:

- Операционная система: Linux-дистрибутивы на архитектуре amd64, совместимые с:
  - Debian 11 или новее;
  - РЕД ОС 7.3 или новее;
- Дополнительное ПО:
  - Docker (рекомендуемая версия: 28.x);
  - Docker Compose (версия 2.0 или новее).

Минимальные аппаратные требования:

- Процессор: 2 ядра (рекомендуется 4 ядра);
- Оперативная память: 8 ГБ (рекомендуется 16 ГБ);
- Дисковое пространство: 40 ГБ.

### 1.4.3 Агент

Программные требования:

- Серверные ОС:
  - Windows Server 2012 R2 или новее;
- Клиентские ОС:
  - Windows 10 (версия 1809, сборка 17763 или новее);
  - Windows 11 (все поддерживаемые версии);
  - Linux:
    - Debian 11 или новее;
    - РЕД ОС 7.3 или новее.

---

**Примечание.** Для операционных систем Windows рекомендуется использование версий 1809 и новее в связи с наличием встроенной поддержки терминала, обеспечивающего расширенные возможности администрирования.

---

Минимальные аппаратные требования:

- Оперативная память: 512 МБ;
- Дисковое пространство: 100 МБ.

## 2 Общие указания по установке комплекса

Перед началом эксплуатации ПК «SimuStrike» необходимо ознакомиться с сопроводительными документами.

Установка изделия должна осуществляться под руководством специально подготовленного персонала. При установке комплекса на ЭВМ рекомендуется консультироваться с технической поддержкой ООО «Газинформсервис».

Телефон технической поддержки: 8 (800) 700-09-87. Официальный сайт: <https://www.gaz-is.ru/>. Email: [support@gaz-is.ru](mailto:support@gaz-is.ru). Электронный адрес для обращения в техническую поддержку: <https://www.gaz-is.ru/poddergka/zajavka.html>.

Пользователи комплекса могут обратиться в техническую поддержку по указанному телефону в рабочие дни с 09:00 до 18:00 (в пятницу до 17:00) по московскому времени (UTC+3), круглосуточно на сайте разработчика или по адресу электронной почты разработчика (производителя).

## 3 Установка запуск программного комплекса SimuStrike

Для развёртывания дистрибутива ПК «SimuStrike» необходимо: 2 электронно-вычислительные машины (ЭВМ) с установленной операционной системой РЕД ОС 7.3: - на первой ЭВМ установить и развернуть дистрибутив с ПК «SimuStrike»; - на второй ЭВМ развернуть резидента.

Допускается развёртывание ПК «SimuStrike» на виртуальных машинах (ВМ) при соблюдении следующих условий: - гипервизор поддерживает аппаратную виртуализацию; - ВМ имеют выделенные ресурсы (центральный процессор, оперативная память, диск), соответствующие требованиям; - настроен корректный сетевой мост или NAT для взаимодействия между ВМ.

Перед установкой проверить наличие всех необходимых драйверов.

---

**Примечание.** Рекомендуется использовать идентичные версии РЕД ОС 7.3 на обеих ЭВМ во избежание конфликтов. В инструкции по развёртыванию дистрибутива ПК приведён пример установки на VMware Workstation Pro.

---

### 3.1 Установка РЕД ОС 7.3 на VMware Workstation Pro

Для установки РЕД ОС 7.3 на ВМ необходимо выполнить следующие шаги:

- 1) Скачать файл-образ РЕД ОС 7.3 на ЭВМ для установки.
- 2) Установить программу виртуализации VMware Workstation Pro.
- 3) Установить ВМ на ЭВМ.
- 4) Запустить программу виртуализации и создать новую ВМ, для этого нажать кнопку «Создать новую виртуальную машину».
- 5) В окне конфигурации следует выбрать рекомендуемую конфигурацию и нажать кнопку «Далее» (рис. 2).

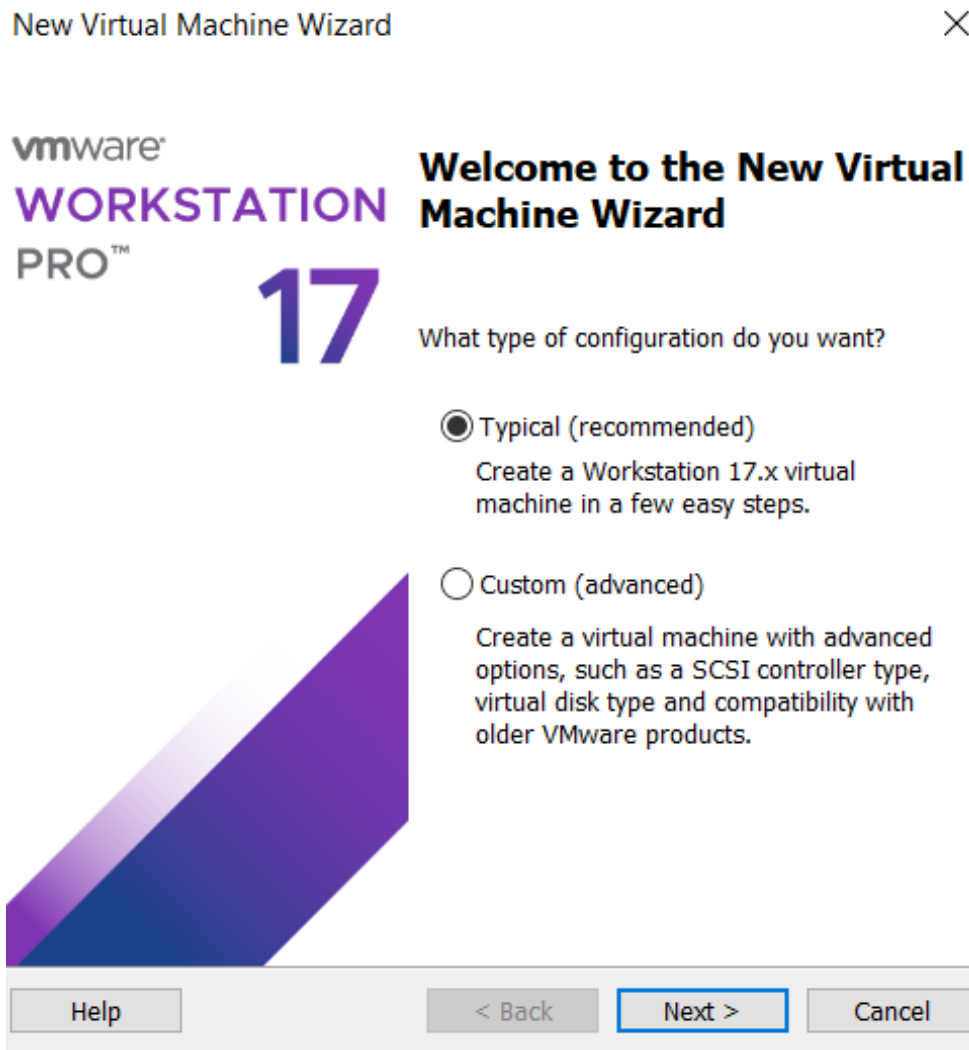


Рисунок 2 – Окно конфигурации

- 6) В окне «Установка гостевой операционной системы» выбрать скачанный на ЭВМ файл-образ РЕД ОС 7.3 с расширением .ISO и нажать кнопку «Далее» (рис. 3).

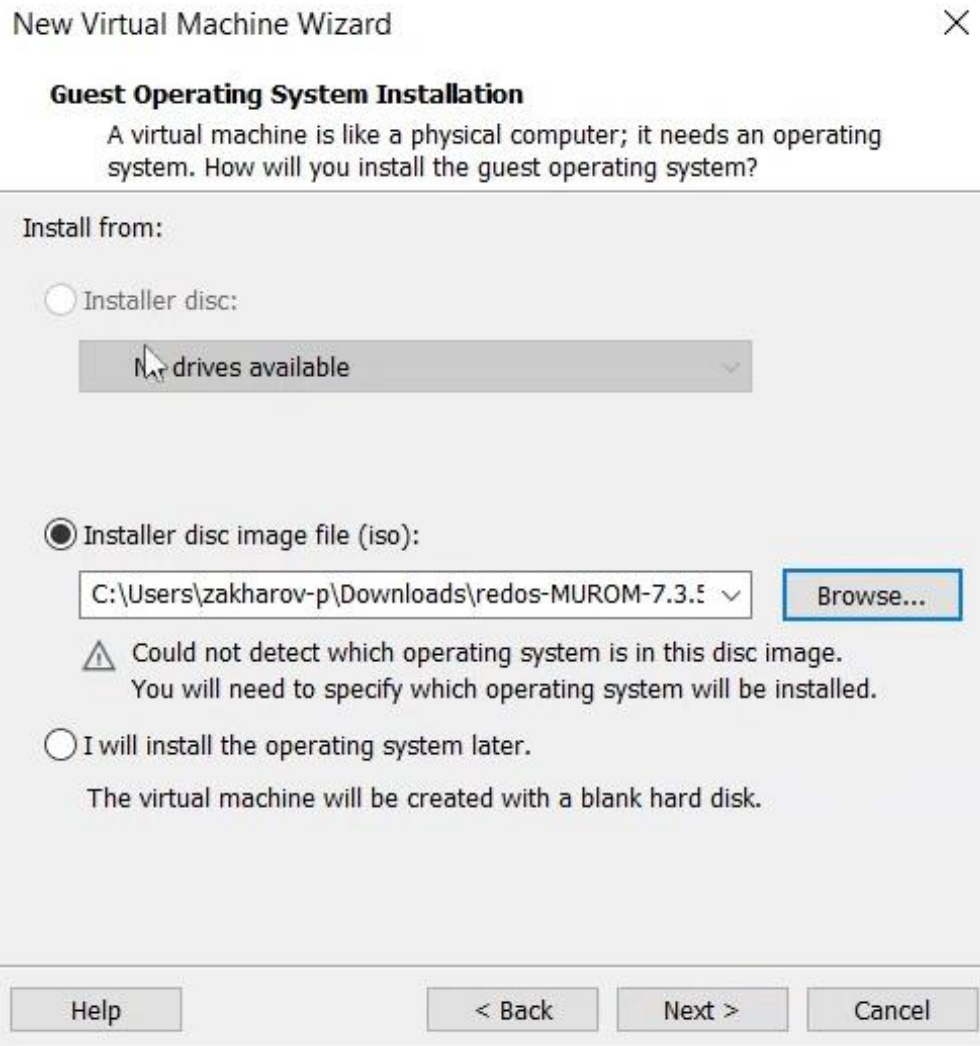


Рисунок 3 – Окно «Установка гостевой операционной системы»

- 7) В открывшемся окне «Выбор гостевой операционной системы» выбрать ОС Linux и версию «Linux 5.x kernel 64-bit» и нажать кнопку «Далее» (рис. 4).

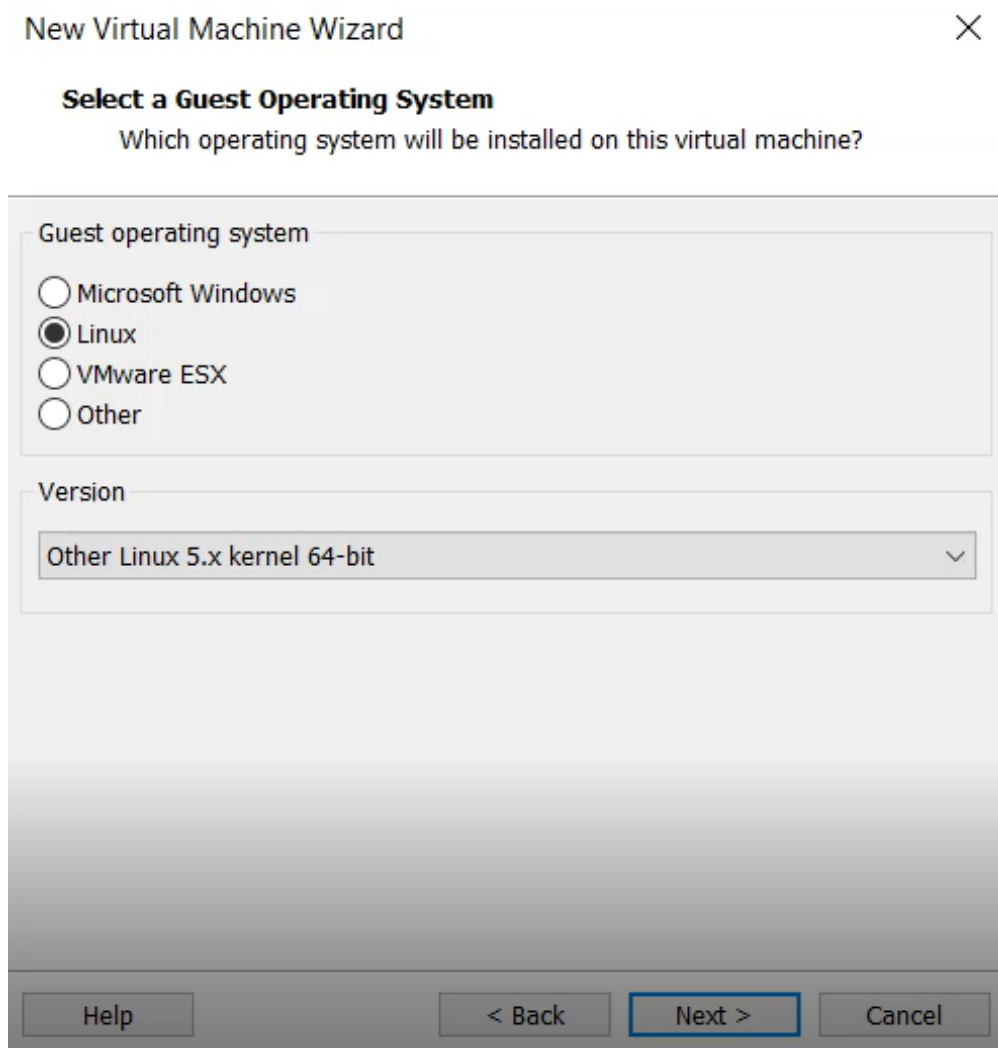


Рисунок 4 – Окно «Выбор гостевой операционной системы»

- 8) В открывшемся окне «Указание ёмкости диска» указать ёмкость диска 50 ГБ и нажать кнопку «Далее» (рис. 5).

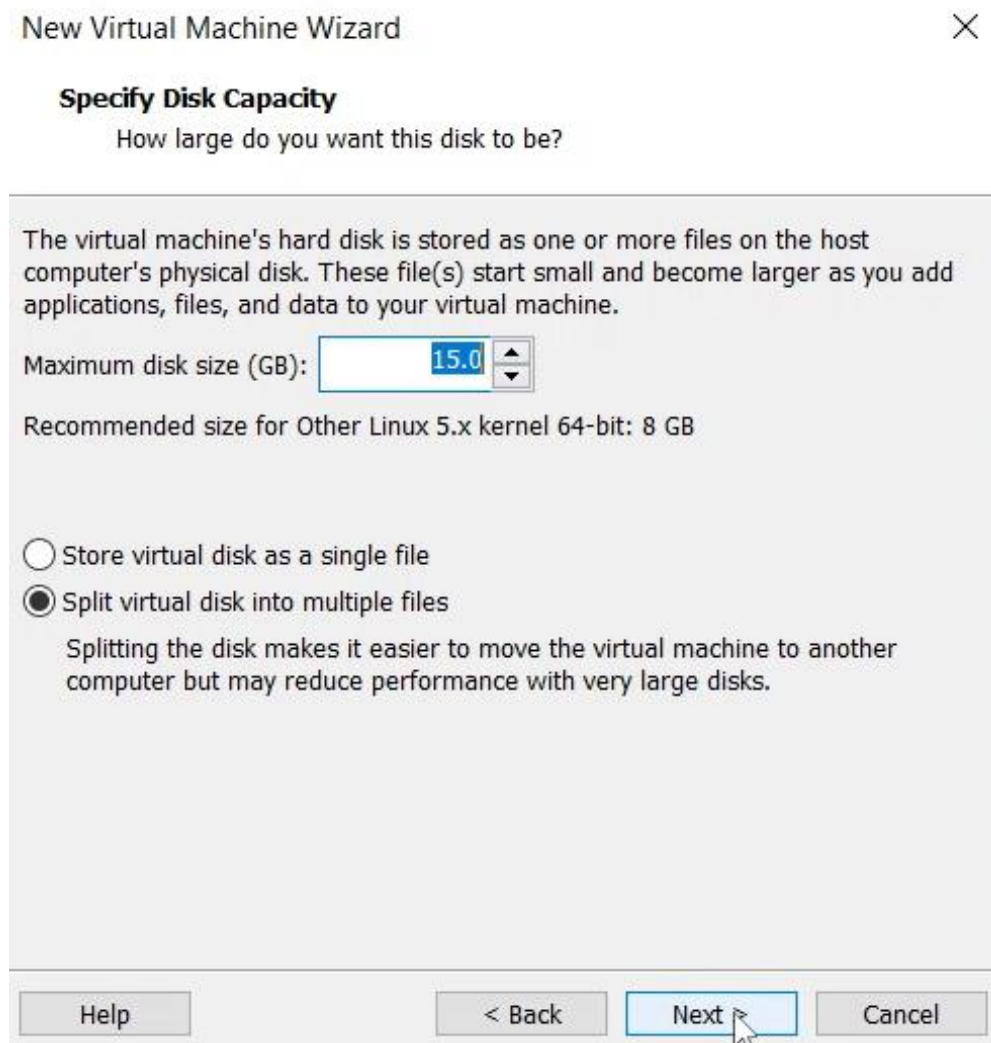


Рисунок 5 – Окно «Указание ёмкости диска»

- 9) В открывшемся окне «Готовая к созданию ВМ» нажать кнопку «Настройка аппаратного обеспечения» (рис. 6).

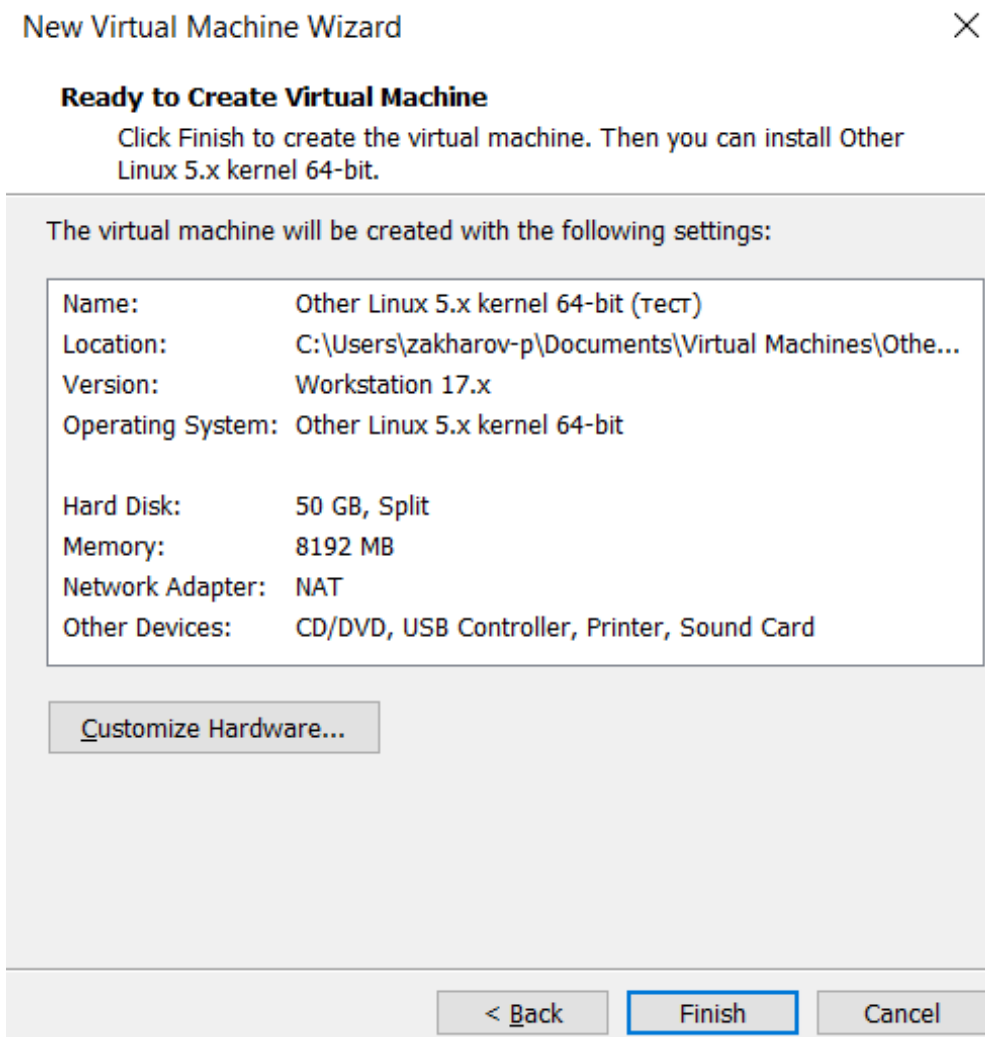


Рисунок 6 – Окно «Готовая к созданию ВМ»

- 10) В окне «Оборудование» изменить количество процессоров на 2 и установить объём оперативной памяти 8 ГБ. После этого нажать кнопку «Закреть» для применения изменений (рис. 7).

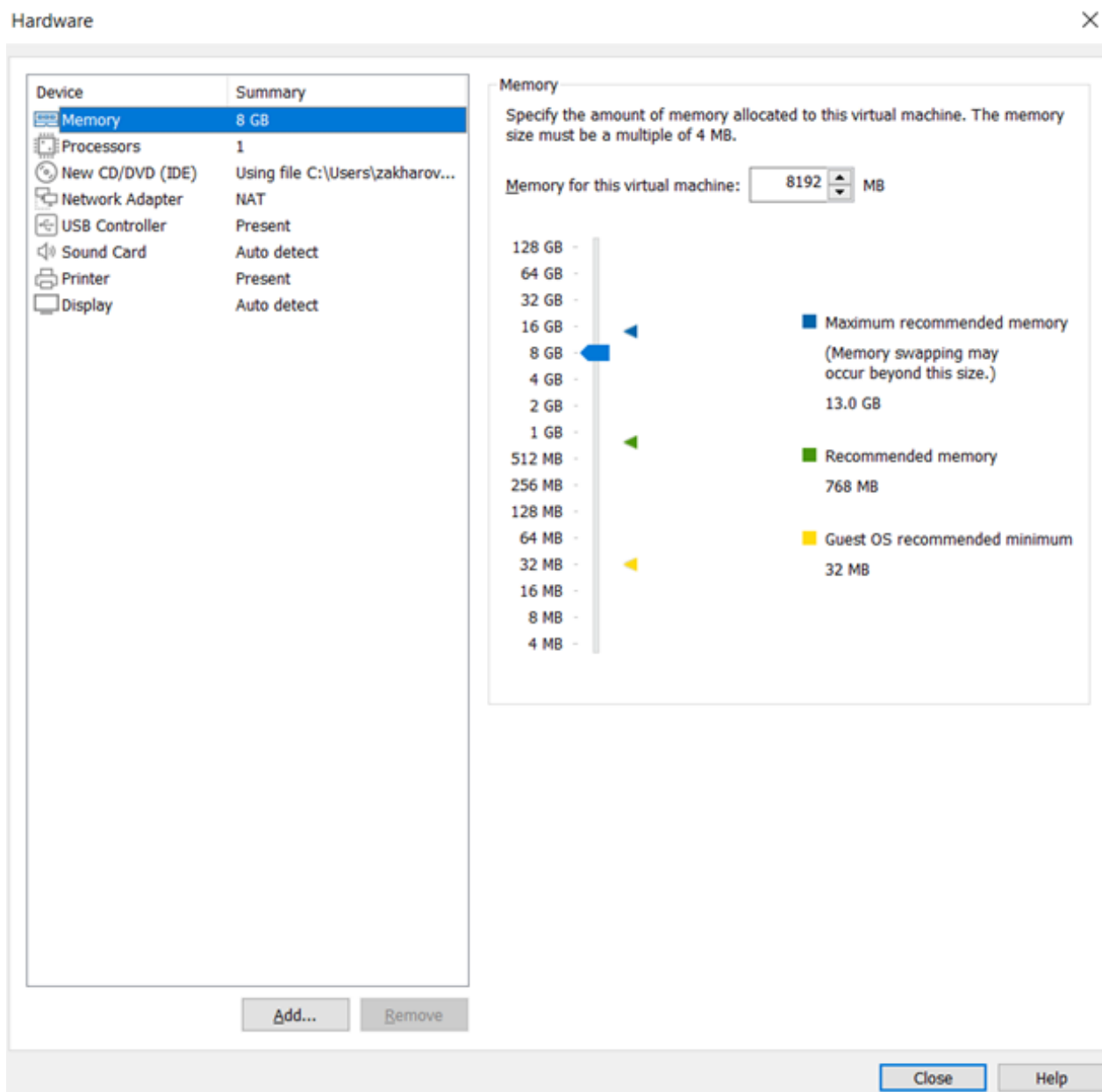


Рисунок 7 – Окно «Готовая к созданию ВМ»

- 11) В открывшемся окне «Готовая к созданию ВМ» проверить параметры оборудования и нажать кнопку «Готово» для завершения настройки ВМ.
- 12) Запустить установленную ВМ при помощи кнопки «Power» и дождаться запуска процесса установки ОС.
- 13) В появившемся окне «Установить RED OS 7.3» выбрать пункт меню «Установить RED OS».
- 14) В окне «Выбор языка» выбрать русский и нажать кнопку «Продолжить».
- 15) В окне «Обзор установки» перейти к настройке пароля для root. Для этого нажать кнопку «Пароль root» (рис. 8).

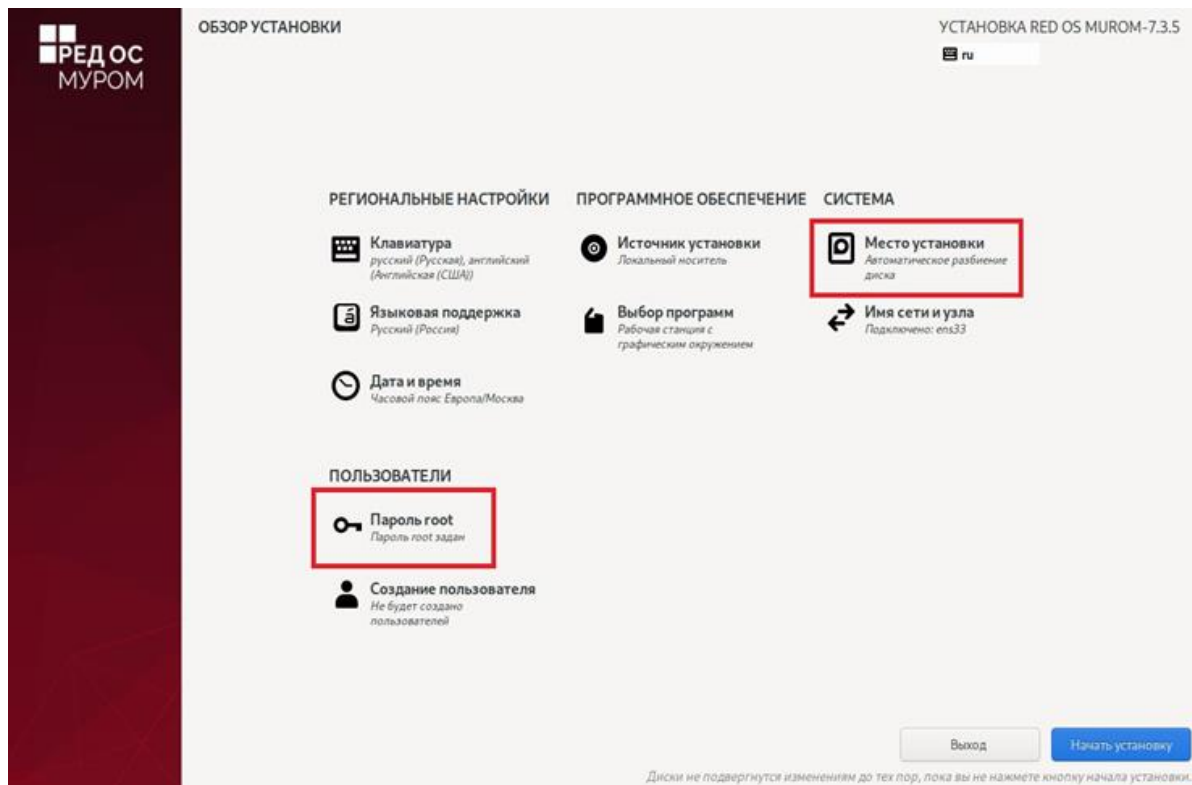


Рисунок 8 – Окно «Обзор установки»

- 16) В открывшемся окне «Пароль ROOT» (рис. 9) заполнить поля:
- создать и ввести пароль;
  - подтвердить пароль;
  - убрать галочку в чекбоксе «Заблокировать учётную запись root»;
  - поставить галочку в чекбоксе «Разрешить вход пользователем root с паролем через SSH».

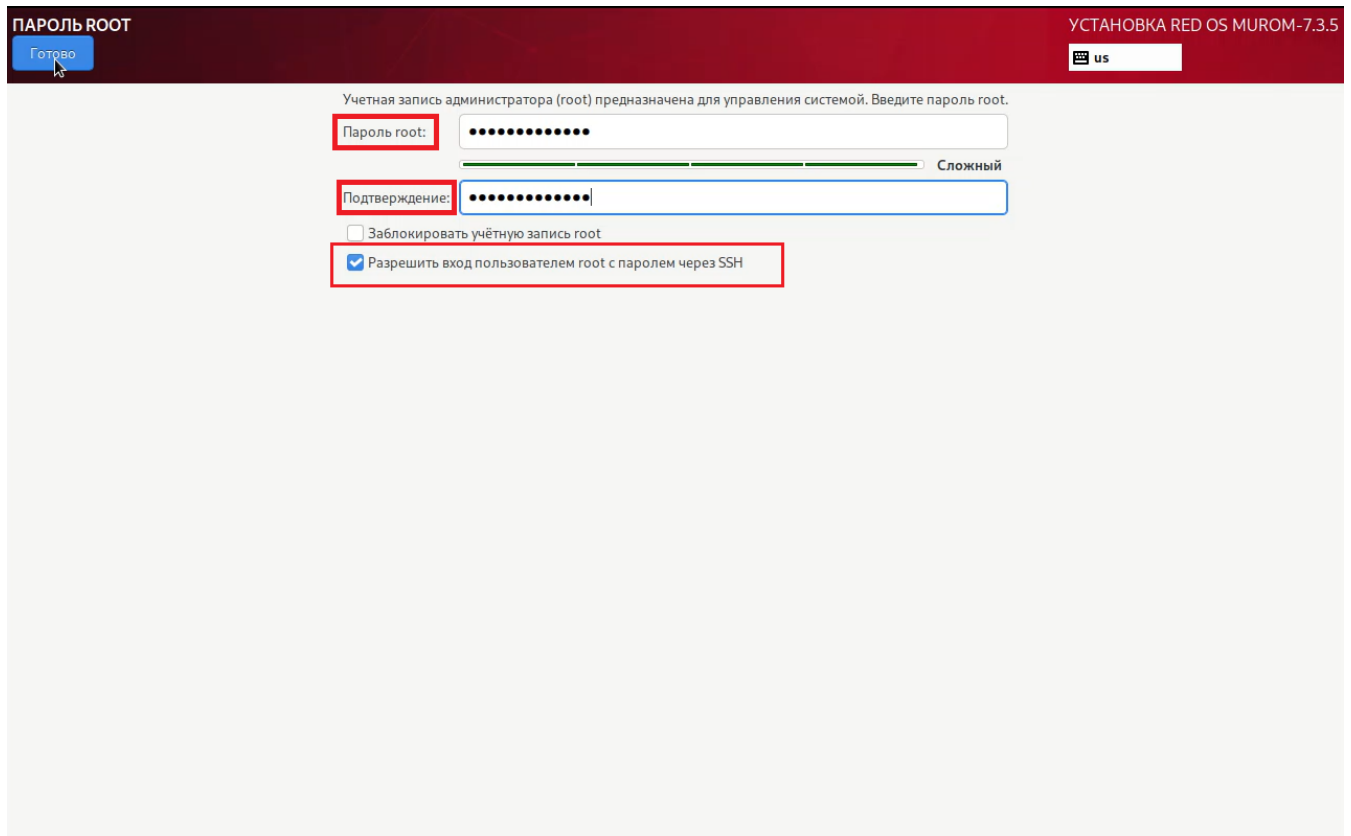


Рисунок 9 – Окно «Пароль ROOT»

- 17) После заполнения нужных параметров в окне «Пароль root» нажать кнопку «Готово».
- 18) В окне «Обзор установки» перейти к учетной записи пользователя, для этого нажать кнопку «Создание пользователя» (рис. 10).

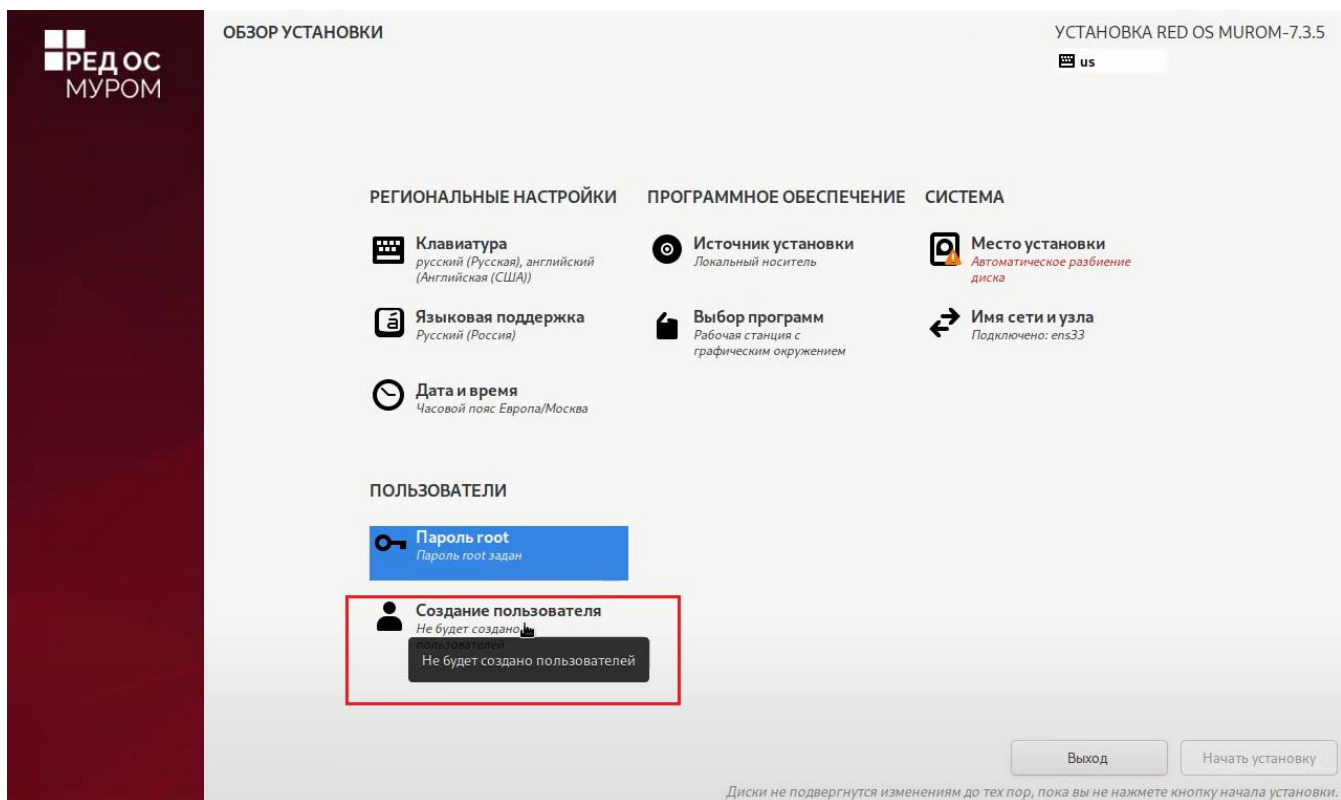


Рисунок 10 – Окно «Пароль ROOT»

- 19) В открывшемся окне «Создание пользователя» (рис. 11) заполнить поля:
- ввести полное имя создаваемой учетной записи пользователя;
  - установить галочку в чекбоксе с названием поля «Сделать этого пользователя администратором»;
  - установить галочку в чекбоксе с названием поля «Требовать пароль для этой учётной записи»;
  - создать и ввести пароль;
  - подтвердить пароль.

Рисунок 11 – Окно «Создание пользователя»

- 20) После заполнения нужных параметров в окне «Создание пользователя» нажать кнопку «Готово».
- 21) В окне «Обзор установки» перейти к настройке места установки (рис. 12). Для этого нажать кнопку «Место установки».

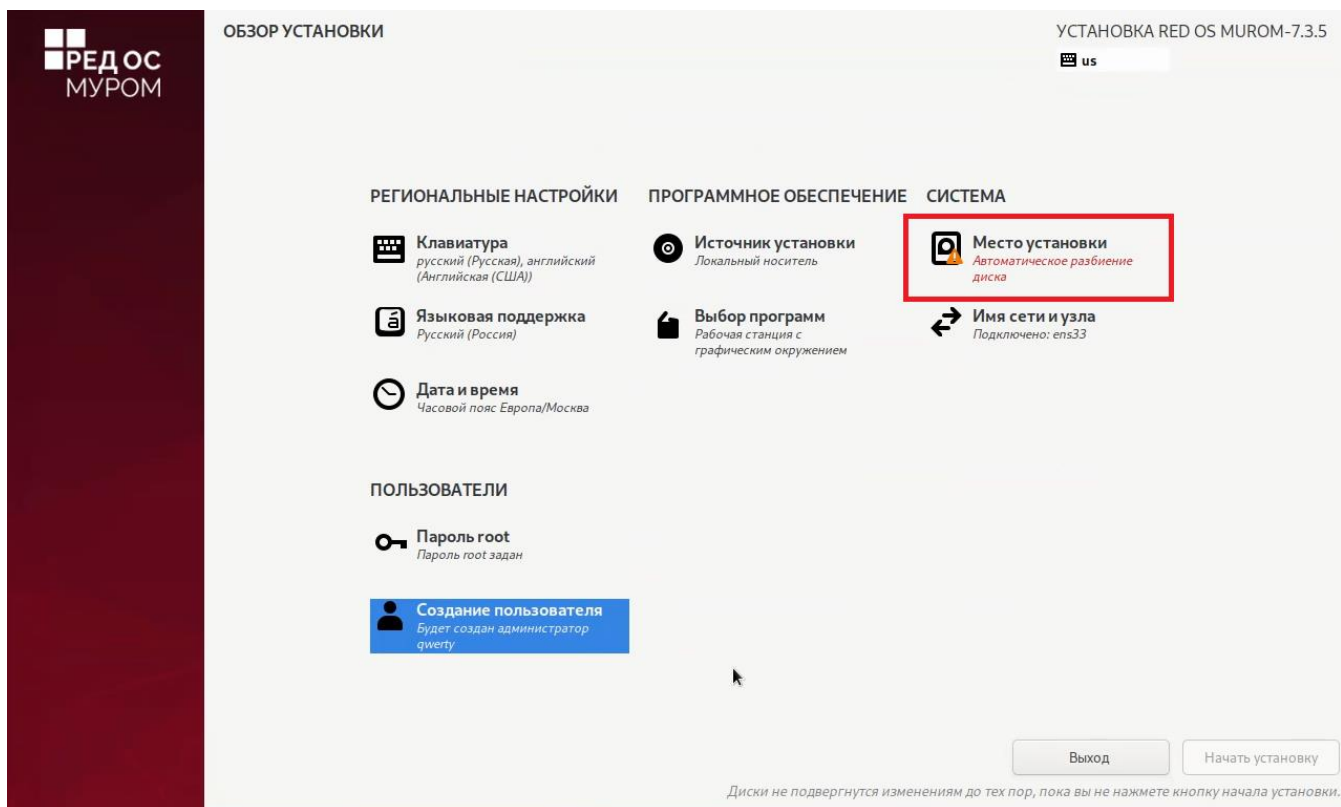


Рисунок 12 – Окно «Создание пользователя»

- 22) В открывшемся окне «Место установки» выбрать устройства для установки ОС и нажать кнопку «Готово».
- 23) В открывшемся окне «Обзор установки» нажать кнопку «Начать установку» для запуска установки ОС на VM.
- 24) После завершения установки нажать кнопку «Перезагрузка системы».
- 25) В окне «Первая настройка» нажать кнопку «Информация о лицензии».
- 26) В открывшемся окне «Информация о лицензии» ознакомиться с лицензией и установить галочку в чекбоксе напротив поля «Я принимаю лицензионное соглашение». После данных действий нажать кнопку «Готово».
- 27) В появившемся окне «Первая настройка» нажать кнопку «Завершить».
- 28) В окне аутентификации ввести данные учётной записи для созданного пользователя (рис. 13):

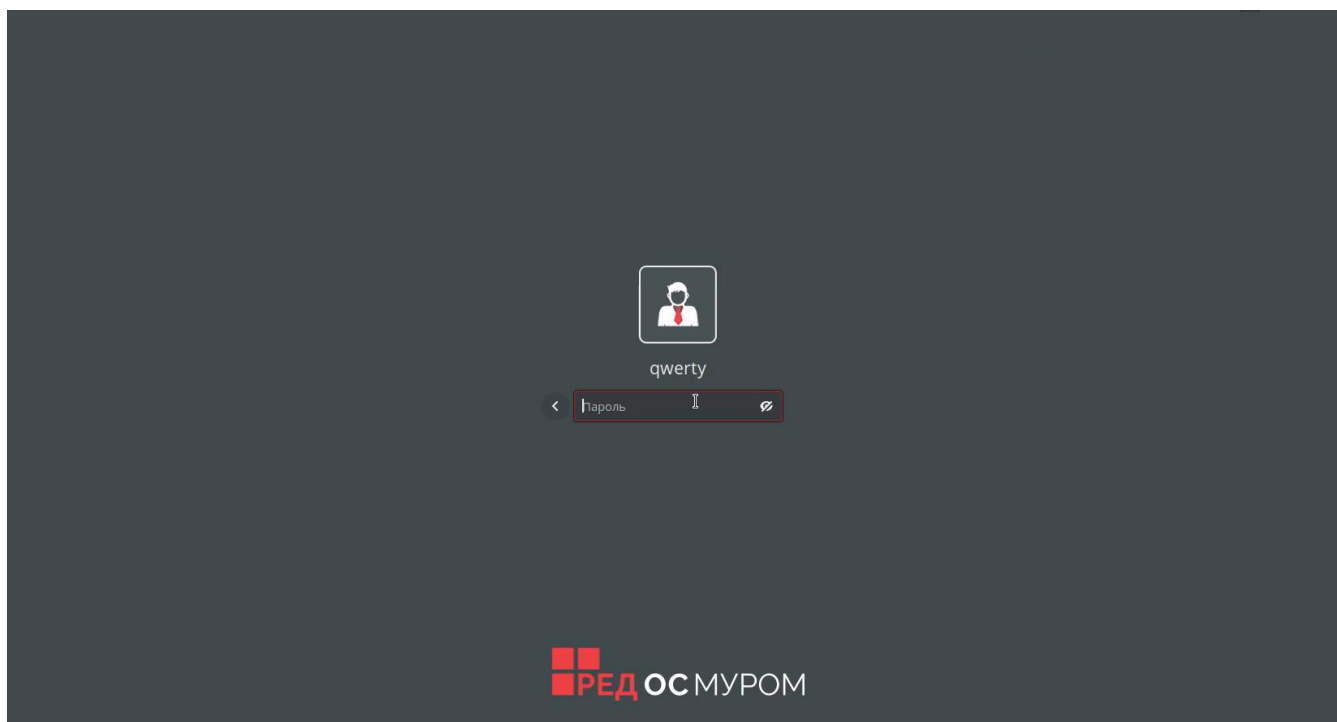


Рисунок 13 – Окно ввода учётных данных

- имя пользователя;
  - пароль.
- 29) После ввода учётных данных откроется рабочий стол РЕД ОС на ВМ (рис. 14).



Рисунок 14 – Окно Рабочий стол РЕД ОС»

**Примечание.** После установки ОС перейти к распаковки дистрибутива.

### 3.2 Распаковка дистрибутива `bas_core`

После установки РЕД ОС на ЭВМ необходимо распаковать дистрибутив «`bas_core`», в состав которого уже входит Docker. Для этого необходимо выполнить следующие шаги:

- 1) Скачать архивный файл «`bas_core.tgz`» на рабочий стол установленной ОС (рис. 15).

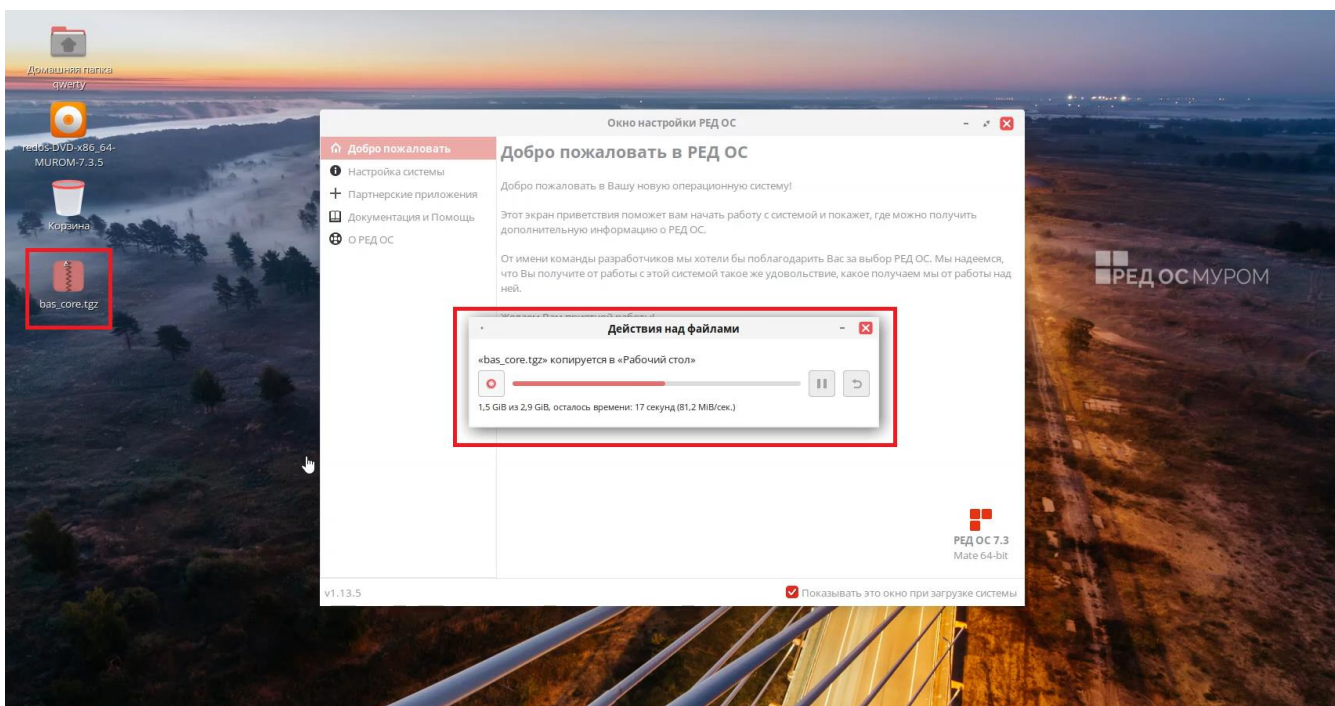


Рисунок 15 – Окно «Настройки РЕД ОС»

- Открыть терминал в установленной ОС и ввести команду `sudo su` (рис. 16). Эта команда запрашивает пароль текущего пользователя в группе sudo и переключает на root-пользователя. Нажать клавишу «Enter» и ввести пароль учётной записи созданного пользователя.

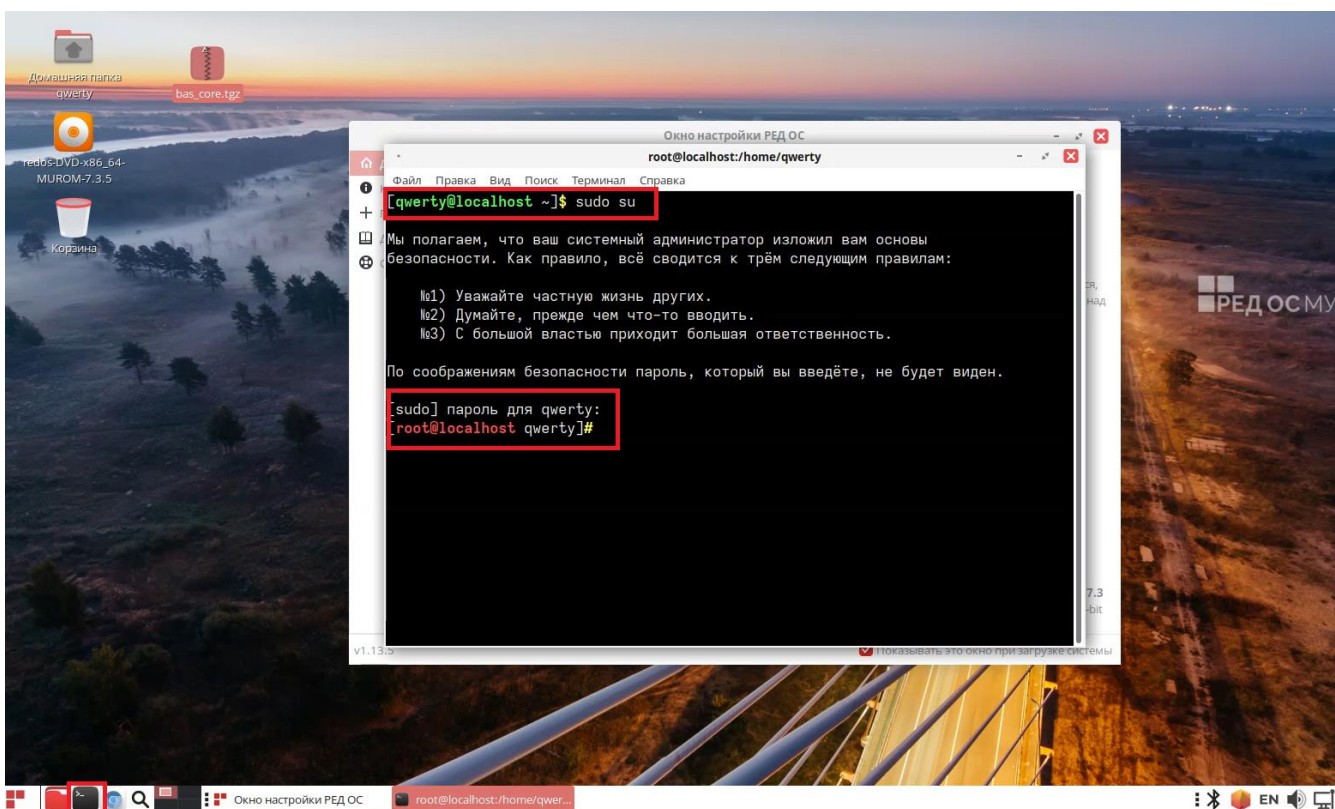
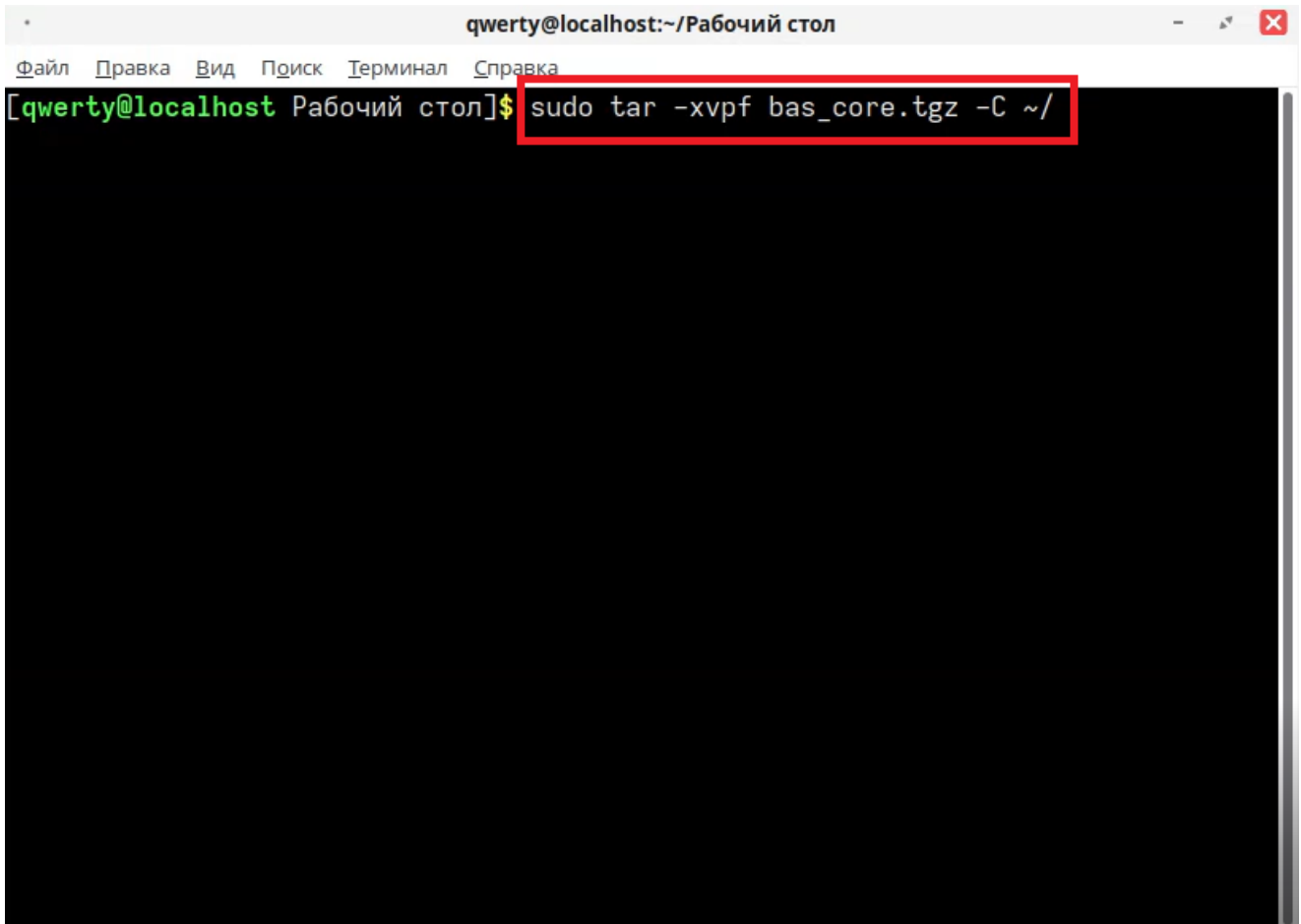


Рисунок 16 – Команда для переключения пользователя

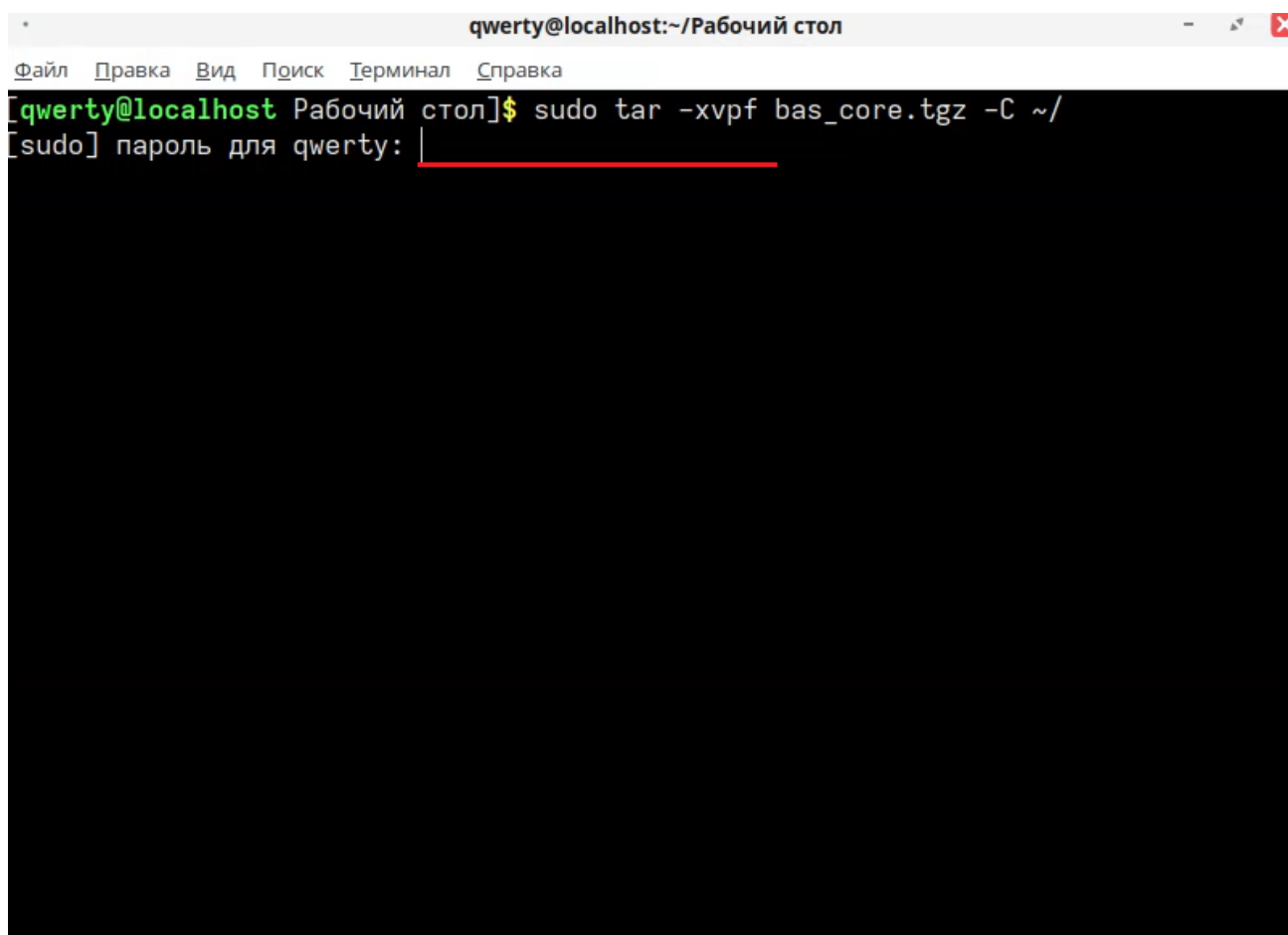
- 3) В терминале выполнить распаковку архива «bas\_core.tgz» в домашнюю директорию текущего пользователя (рис. 17), введя команду `sudo tar -xvpf bas_core.tgz -C ~/`. После ввода команды нажать на клавиатуре кнопку «Enter».



```
qwerty@localhost:~/Рабочий стол
Файл Правка Вид Поиск Терминал Справка
[qwerty@localhost Рабочий стол]$ sudo tar -xvpf bas_core.tgz -C ~/
```

Рисунок 17 – Команда для запуска распаковки архива

- 4) Ввести пароль пользователя и нажать на клавиатуре кнопку «Enter» (рис. 18).



```
qwerty@localhost:~/Рабочий стол
Файл Правка Вид Поиск Терминал Справка
[qwerty@localhost Рабочий стол]$ sudo tar -xvpf bas_core.tgz -C ~/
[sudo] пароль для qwerty: _____
```

Рисунок 18 – Ввод пароля пользователя

---

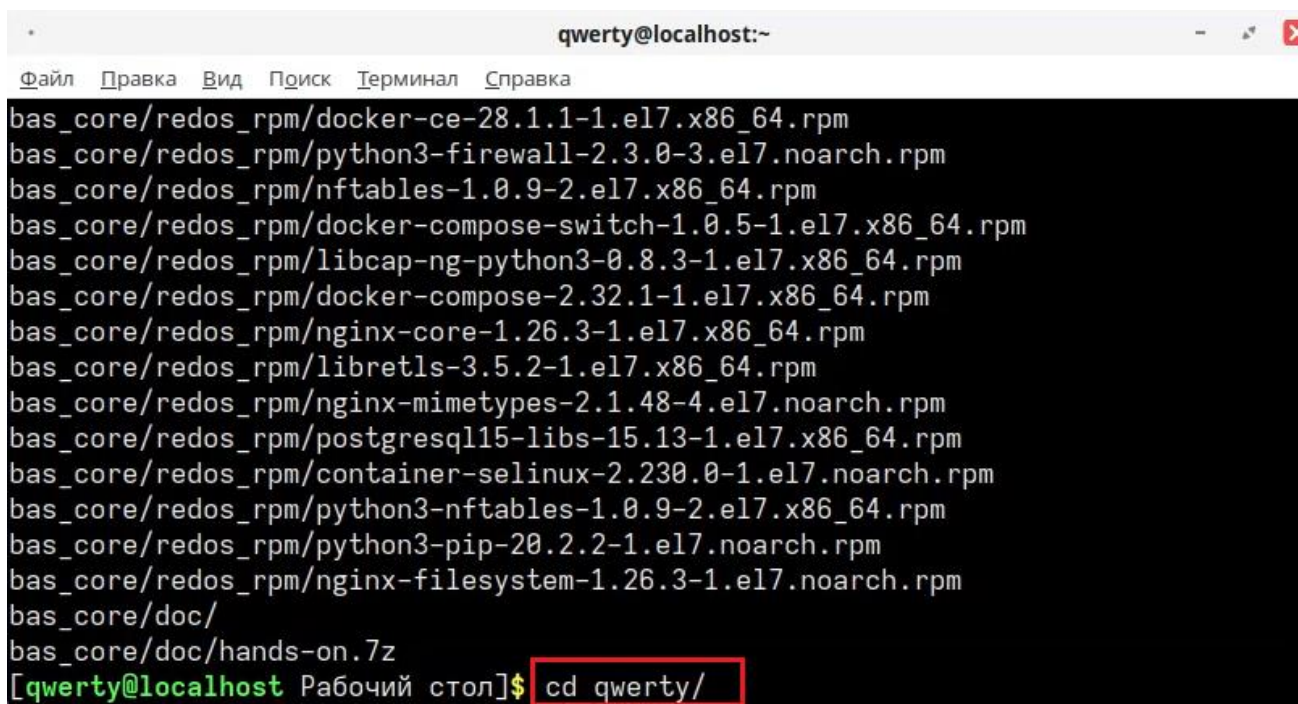
**Примечание.** После распаковки дистрибутива «bas\_core» перейти к редактированию конфигурационного файла.

---

### 3.3 Редактирование конфигурационного файла

После установки ПО для автоматизации развертывания Docker и распаковки дистрибутива bas\_core перейти к редактированию конфигурационного файла. Для этого необходимо выполнить следующие шаги:

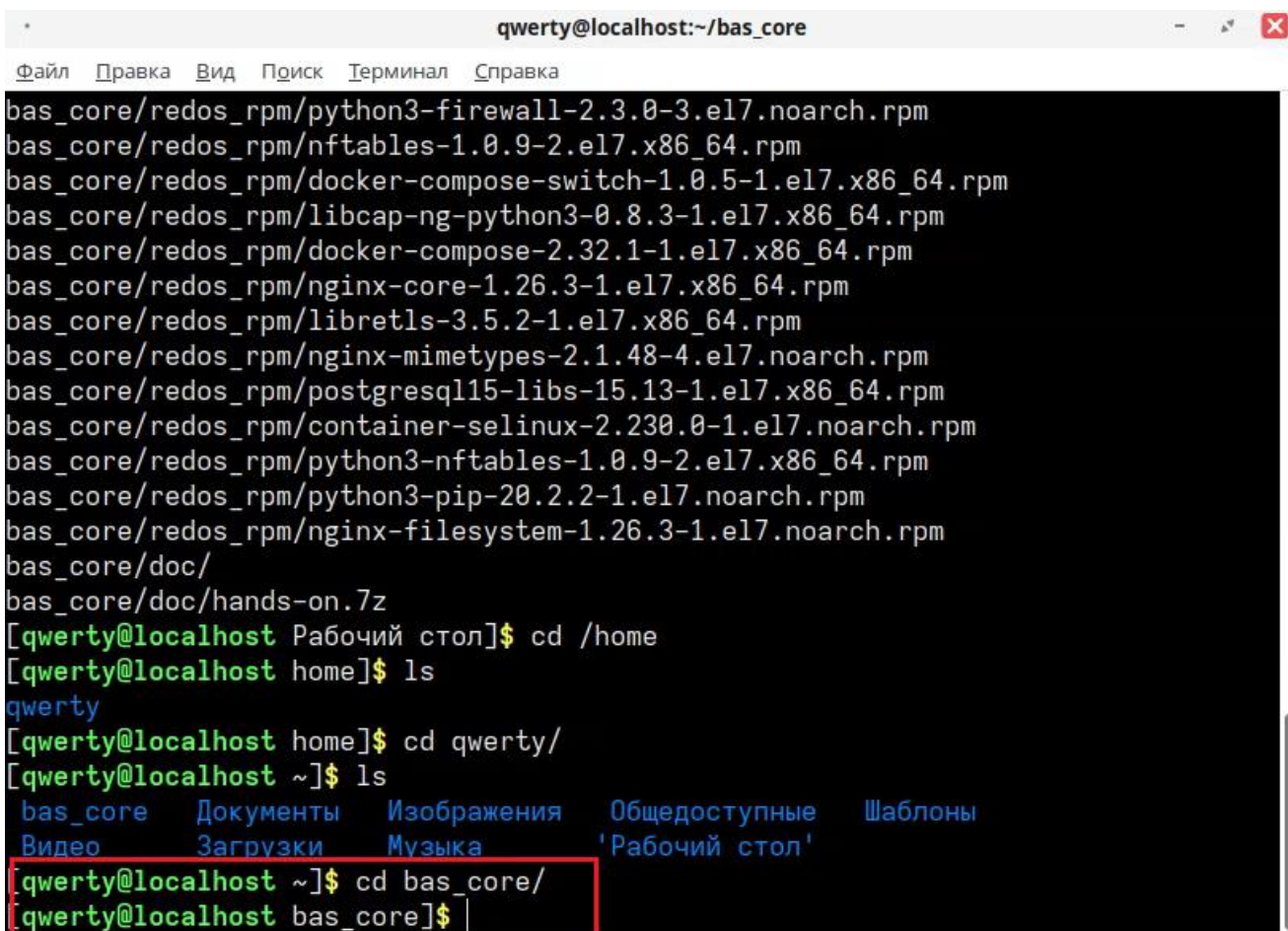
- 1) Перейти в директорию пользователя при помощи команды в терминале `cd qwerty/` (абсолютный путь к папке пользователя qwerty) и нажать на клавиатуре кнопку «Enter» (рис. 19).



```
qwerty@localhost:~
Файл  Правка  Вид  Поиск  Терминал  Справка
bas_core/redos_rpm/docker-ce-28.1.1-1.el7.x86_64.rpm
bas_core/redos_rpm/python3-firewall-2.3.0-3.el7.noarch.rpm
bas_core/redos_rpm/nftables-1.0.9-2.el7.x86_64.rpm
bas_core/redos_rpm/docker-compose-switch-1.0.5-1.el7.x86_64.rpm
bas_core/redos_rpm/libcap-ng-python3-0.8.3-1.el7.x86_64.rpm
bas_core/redos_rpm/docker-compose-2.32.1-1.el7.x86_64.rpm
bas_core/redos_rpm/nginx-core-1.26.3-1.el7.x86_64.rpm
bas_core/redos_rpm/libretls-3.5.2-1.el7.x86_64.rpm
bas_core/redos_rpm/nginx-mimetypes-2.1.48-4.el7.noarch.rpm
bas_core/redos_rpm/postgresql15-libs-15.13-1.el7.x86_64.rpm
bas_core/redos_rpm/container-selinux-2.230.0-1.el7.noarch.rpm
bas_core/redos_rpm/python3-nftables-1.0.9-2.el7.x86_64.rpm
bas_core/redos_rpm/python3-pip-20.2.2-1.el7.noarch.rpm
bas_core/redos_rpm/nginx-filesystem-1.26.3-1.el7.noarch.rpm
bas_core/doc/
bas_core/doc/hands-on.7z
[qwerty@localhost Рабочий стол]$ cd qwerty/
```

Рисунок 19 – Переход в директорию пользователя

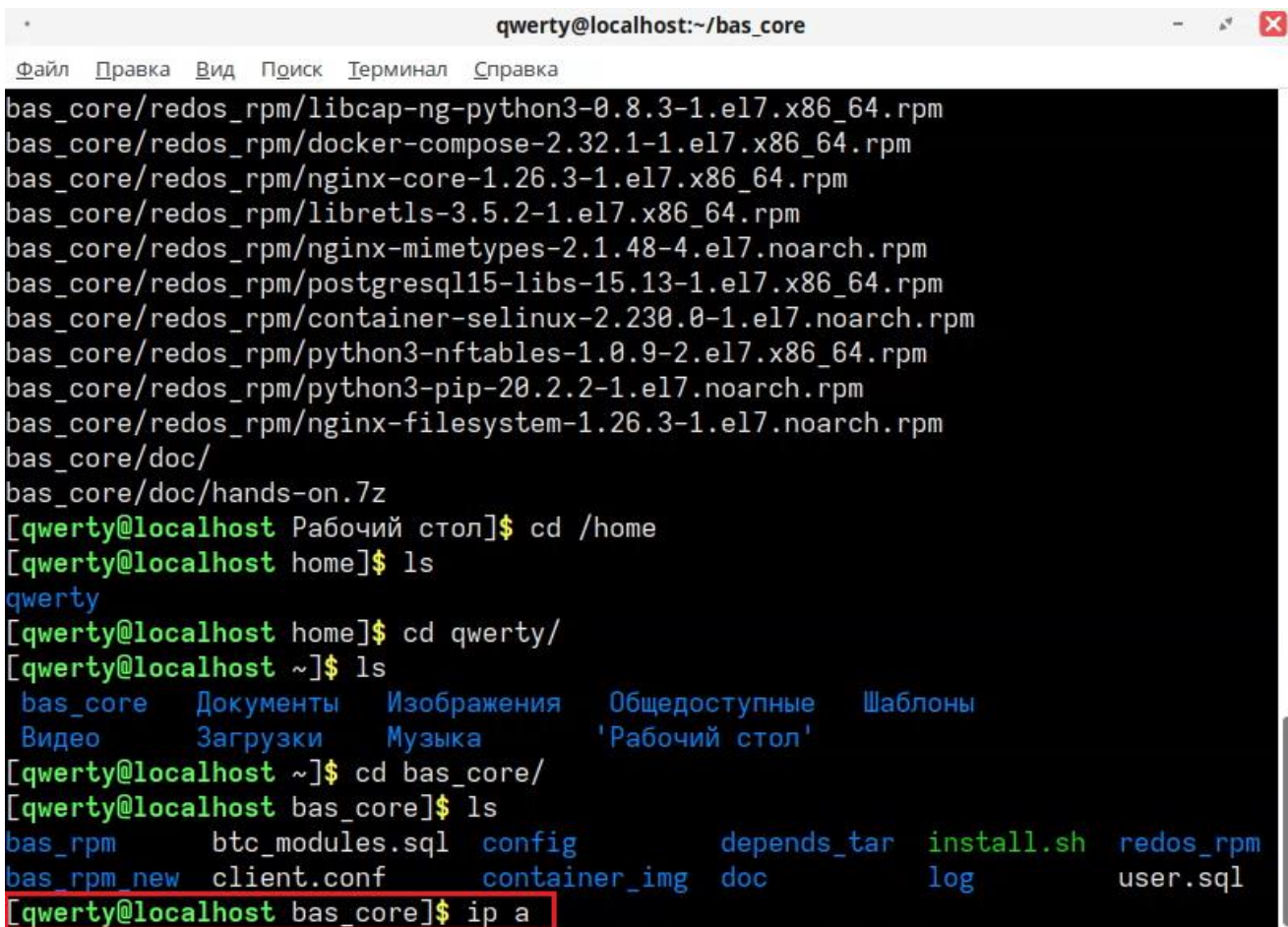
- 2) Перейти в директорию `bas_core` при помощи команды в терминале `cd bas_core/` (абсолютный путь к папке пользователя `qwerty`) и нажать на клавиатуре кнопку «Enter» (рис. 20).



```
qwerty@localhost:~/bas_core
Файл Правка Вид Поиск Терминал Справка
bas_core/redos_rpm/python3-firewall-2.3.0-3.el7.noarch.rpm
bas_core/redos_rpm/nftables-1.0.9-2.el7.x86_64.rpm
bas_core/redos_rpm/docker-compose-switch-1.0.5-1.el7.x86_64.rpm
bas_core/redos_rpm/libcap-ng-python3-0.8.3-1.el7.x86_64.rpm
bas_core/redos_rpm/docker-compose-2.32.1-1.el7.x86_64.rpm
bas_core/redos_rpm/nginx-core-1.26.3-1.el7.x86_64.rpm
bas_core/redos_rpm/libretls-3.5.2-1.el7.x86_64.rpm
bas_core/redos_rpm/nginx-mimetypes-2.1.48-4.el7.noarch.rpm
bas_core/redos_rpm/postgresql15-libs-15.13-1.el7.x86_64.rpm
bas_core/redos_rpm/container-selinux-2.230.0-1.el7.noarch.rpm
bas_core/redos_rpm/python3-nftables-1.0.9-2.el7.x86_64.rpm
bas_core/redos_rpm/python3-pip-20.2.2-1.el7.noarch.rpm
bas_core/redos_rpm/nginx-filestream-1.26.3-1.el7.noarch.rpm
bas_core/doc/
bas_core/doc/hands-on.7z
[qwerty@localhost Рабочий стол]$ cd /home
[qwerty@localhost home]$ ls
qwerty
[qwerty@localhost home]$ cd qwerty/
[qwerty@localhost ~]$ ls
bas_core  Документы  Изображения  Общедоступные  Шаблоны
Видео    Загрузки   Музыка        'Рабочий стол'
[qwerty@localhost ~]$ cd bas_core/
[qwerty@localhost bas_core]$
```

Рисунок 20 – Переход в директорию пользователя

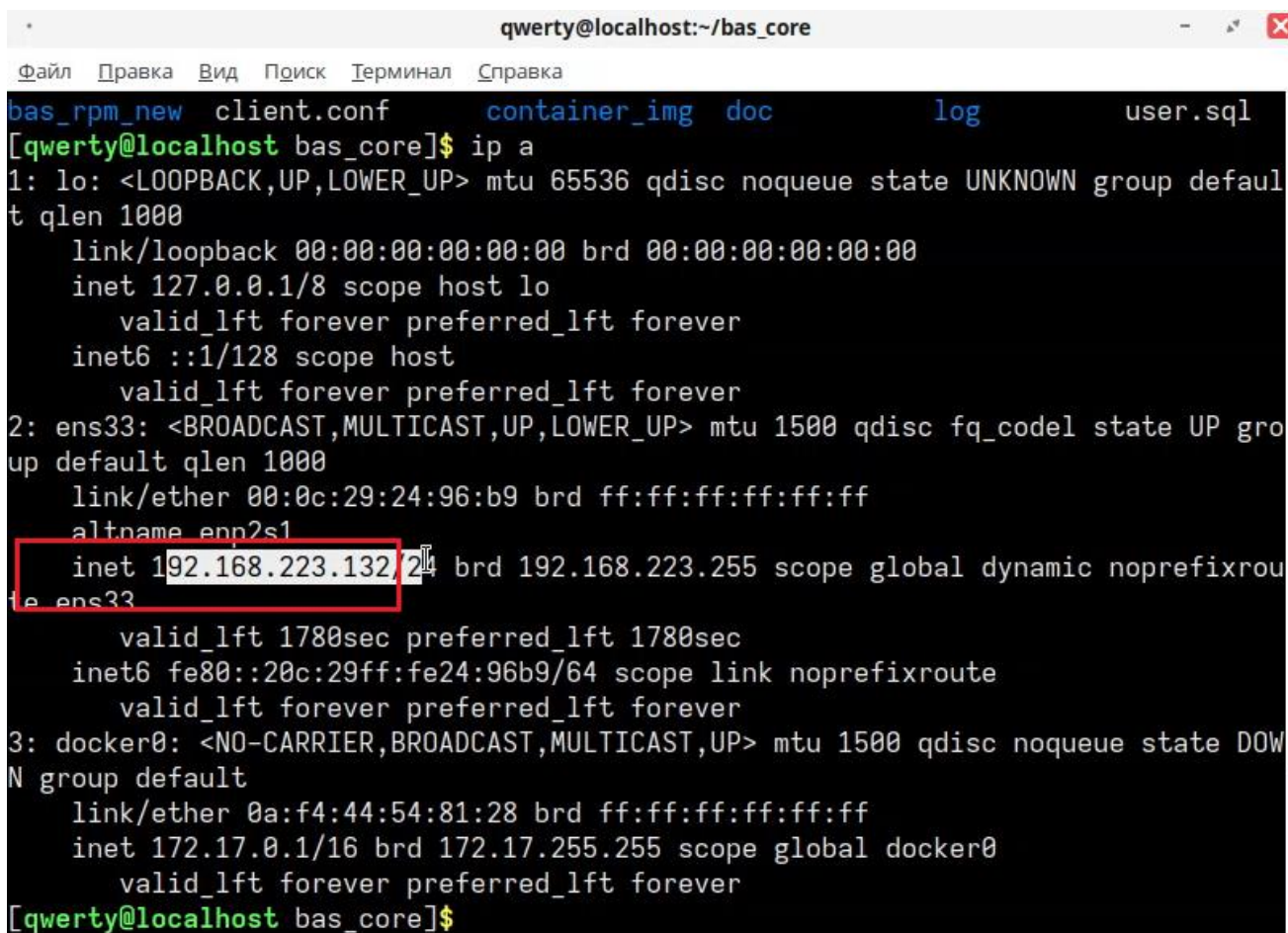
- 3) Ввести команду `ip a` и нажать кнопку «Enter». Это команда в Linux, которая отображает информацию о сетевых интерфейсах, их IP-адресах (IPv4 и IPv6), MAC-адресах и других параметрах (рис. 21).



```
qwerty@localhost:~/bas_core
Файл  Правка  Вид  Поиск  Терминал  Справка
bas_core/redos_rpm/libcap-ng-python3-0.8.3-1.el7.x86_64.rpm
bas_core/redos_rpm/docker-compose-2.32.1-1.el7.x86_64.rpm
bas_core/redos_rpm/nginx-core-1.26.3-1.el7.x86_64.rpm
bas_core/redos_rpm/libretls-3.5.2-1.el7.x86_64.rpm
bas_core/redos_rpm/nginx-mimetypes-2.1.48-4.el7.noarch.rpm
bas_core/redos_rpm/postgresql15-libs-15.13-1.el7.x86_64.rpm
bas_core/redos_rpm/container-selinux-2.230.0-1.el7.noarch.rpm
bas_core/redos_rpm/python3-nftables-1.0.9-2.el7.x86_64.rpm
bas_core/redos_rpm/python3-pip-20.2.2-1.el7.noarch.rpm
bas_core/redos_rpm/nginx-filesystem-1.26.3-1.el7.noarch.rpm
bas_core/doc/
bas_core/doc/hands-on.7z
[qwerty@localhost Рабочий стол]$ cd /home
[qwerty@localhost home]$ ls
qwerty
[qwerty@localhost home]$ cd qwerty/
[qwerty@localhost ~]$ ls
bas_core  Документы  Изображения  Общедоступные  Шаблоны
Видео    Загрузки   Музыка        'Рабочий стол'
[qwerty@localhost ~]$ cd bas_core/
[qwerty@localhost bas_core]$ ls
bas_rpm      btc_modules.sql  config          depends_tar  install.sh  redos_rpm
bas rpm new  client.conf      container_img  doc          log          user.sql
[qwerty@localhost bas_core]$ ip a
```

Рисунок 21 – Ввод команды «ip a» в терминал

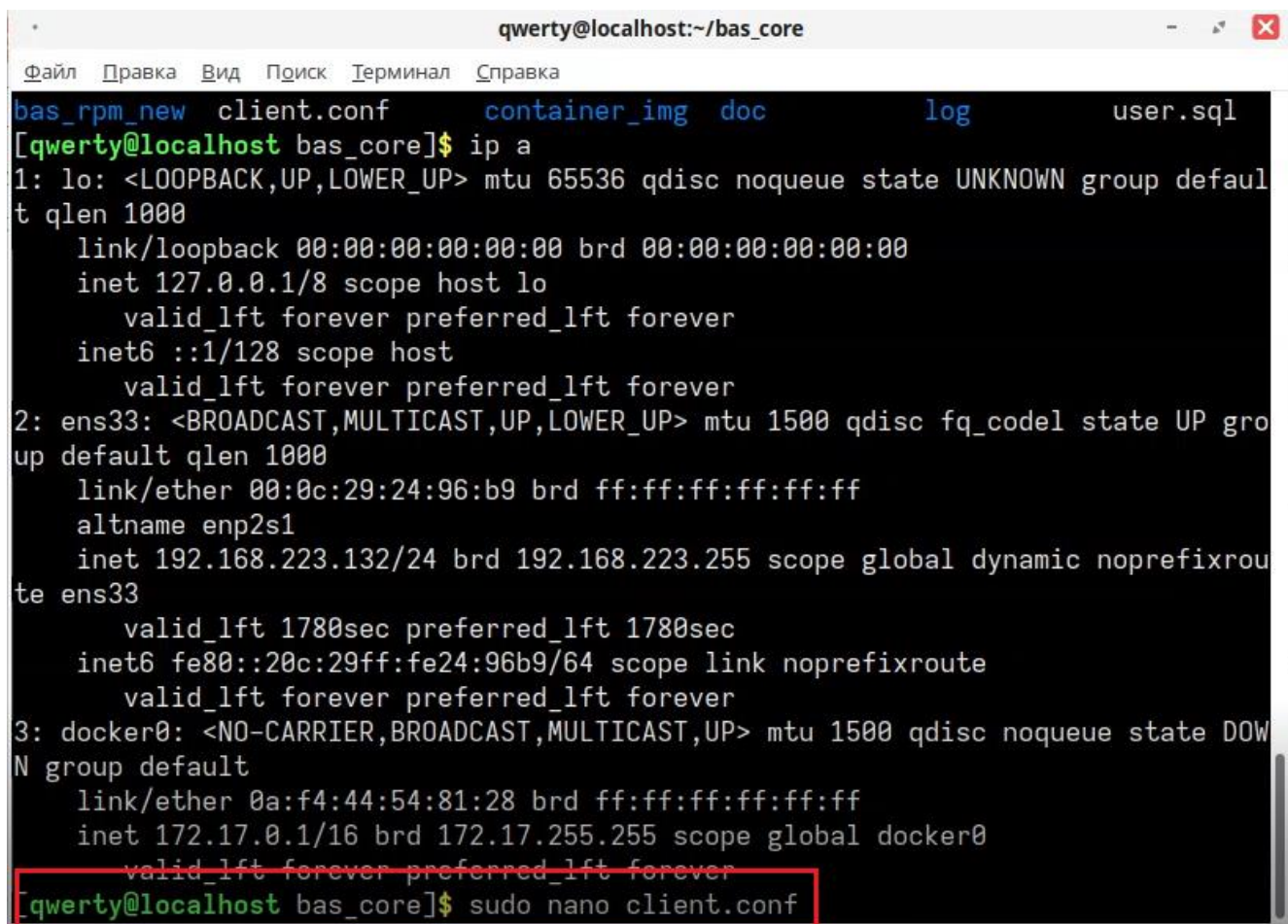
- 4) Зафиксировать поле IP-адреса, как показано на рисунке. Этот IP-адрес потребуется для дальнейшей настройки.(рис. 22).



```
qwerty@localhost:~/bas_core
Файл Правка Вид Поиск Терминал Справка
bas_rpm_new client.conf container_img doc log user.sql
[qwerty@localhost bas_core]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:24:96:b9 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.223.132/24 brd 192.168.223.255 scope global dynamic noprefixroute ens33
        valid_lft 1780sec preferred_lft 1780sec
    inet6 fe80::20c:29ff:fe24:96b9/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 0a:f4:44:54:81:28 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
[qwerty@localhost bas_core]$
```

Рисунок 22 – Окно терминала с полученным IP-адресом

- 5) Открыть для редактирования файл «client.conf» в текстовом редакторе Nano с правами суперпользователя. Для этого ввести команду `sudo nano client.conf` и нажать на клавиатуре кнопку «Enter» (рис. 23).



```
qwerty@localhost:~/bas_core
Файл  Правка  Вид  Поиск  Терминал  Справка
bas_rpm_new  client.conf  container_img  doc  log  user.sql
[qwerty@localhost bas_core]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:24:96:b9 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.223.132/24 brd 192.168.223.255 scope global dynamic noprefixroute ens33
        valid_lft 1780sec preferred_lft 1780sec
    inet6 fe80::20c:29ff:fe24:96b9/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 0a:f4:44:54:81:28 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
[qwerty@localhost bas_core]$ sudo nano client.conf
```

Рисунок 23 – Ввод команды «sudo nano client.conf» в терминал

- 6) В открытом в терминале файле «client.conf» с помощью клавиш-стрелок перейти к разделу «Хост для установки системы» (рис. 24). Заменить текущий IP-адрес на новый, полученный в результате команды (пункт 4).

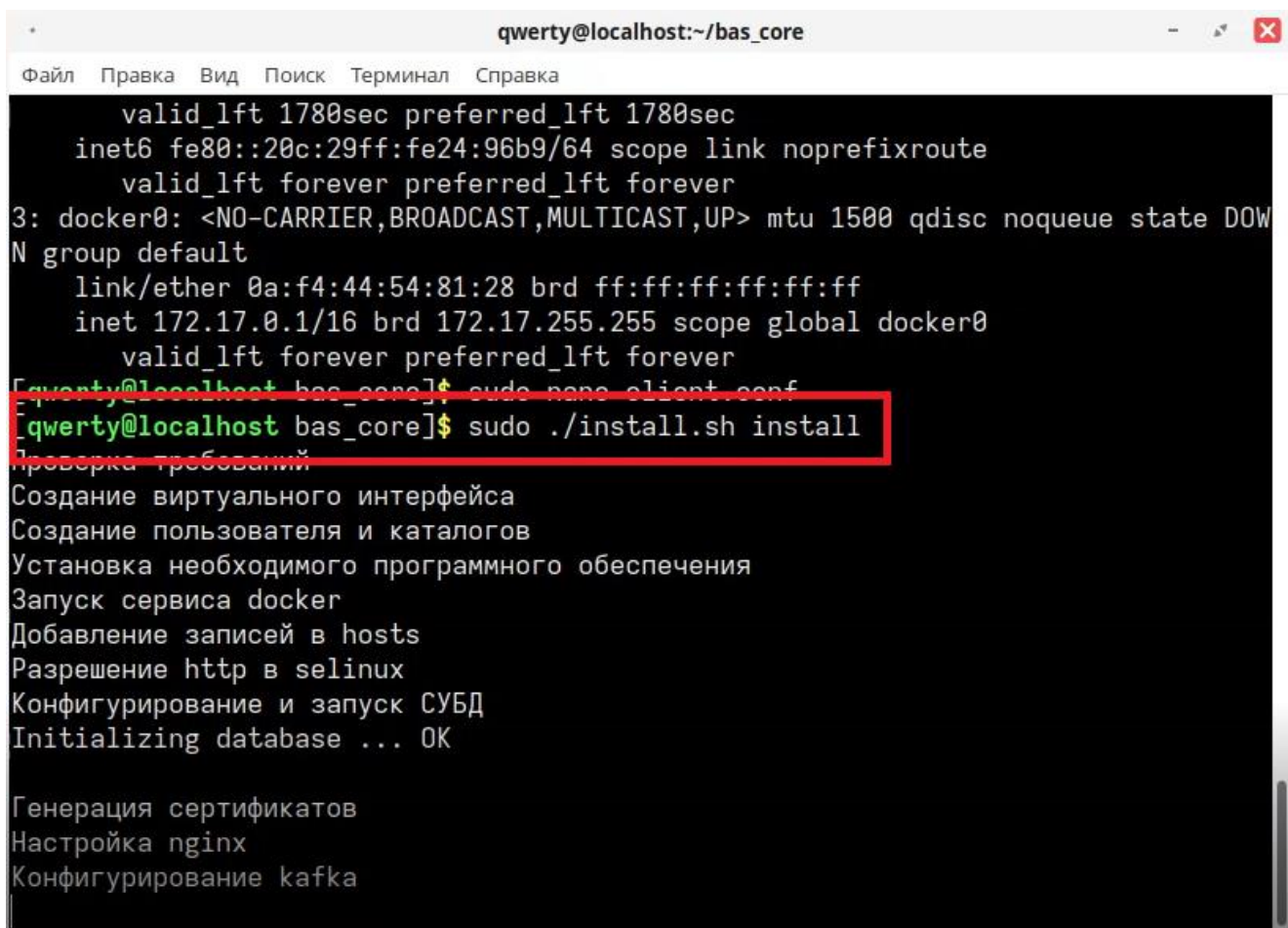
```
# ИМЯ ВИРТУАЛЬНОГО ИНТЕРФЕЙСА
VIRTUAL_IFNAME="bas-int"
VIRTUAL_IPADDR="169.254.0.1/24"
VIRTUAL_HOSTNAME="bascore"

# ХОСТ ДЛЯ УСТАНОВКИ СИСТЕМЫ
CORE_HOSTNAME="core-bas.local"
CORE_IPADDR="10.116.231.61"

# ВНОСИТЬ ХОСТЫ В ФАЙЛ /etc/hosts
USE_HOSTS="yes"
```

Рисунок 24 – Файл «client.conf»

- 7) Сохранить изменения и выйти из окна «client.conf» для этого нажать сочетание клавиш «Ctrl+O», а затем «Ctrl+X».
- 8) Ввести команду `sudo ./install.sh install` для установки программы из исходных текстов (рис. 25).



```
qwerty@localhost:~/bas_core
Файл Правка Вид Поиск Терминал Справка
valid_lft 1780sec preferred_lft 1780sec
inet6 fe80::20c:29ff:fe24:96b9/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
N group default
link/ether 0a:f4:44:54:81:28 brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
[qwerty@localhost bas_core]$ sudo nano client.conf
[qwerty@localhost bas_core]$ sudo ./install.sh install
Проверка требований
Создание виртуального интерфейса
Создание пользователя и каталогов
Установка необходимого программного обеспечения
Запуск сервиса docker
Добавление записей в hosts
Разрешение http в selinux
Конфигурирование и запуск СУБД
Initializing database ... OK

Генерация сертификатов
Настройка nginx
Конфигурирование kafka
```

Рисунок 25 – Установка программы

- 9) После установки программы на ЭВМ запустить браузер «Chromium», ввести в поисковую строку адрес <https://core-bas.local> и перейти по нему (рис. 26).

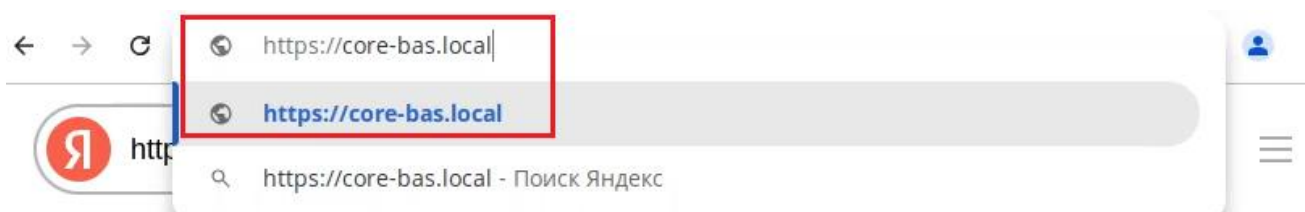


Рисунок 26 – Запуск браузера

- 10) В окне с предупреждением «Подключение не защищено» нажать кнопку «Дополнительно», после чего выбрать ссылку «Перейти на сайт core-bas.local» (рис. 27).



## Подключение не защищено

Возможно, злоумышленники пытаются похитить вашу информацию с сайта **core-bas.local**, например пароли, сообщения и данные кредитных карт. Подробнее [об этом предупреждении...](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

💡 Чтобы браузер Chrome стал максимально безопасным, [включите режим "Улучшенная защита"](#).

Дополнительные



Вернуться к безопасной странице

Рисунок 27 – Окно «Подключение не защищено»

- 11) В окне приветствия ПК «SimuStrike» ввести логин `user` и пароль `Super$ecret`. Нажать кнопку «Войти в систему» (рис. 28).



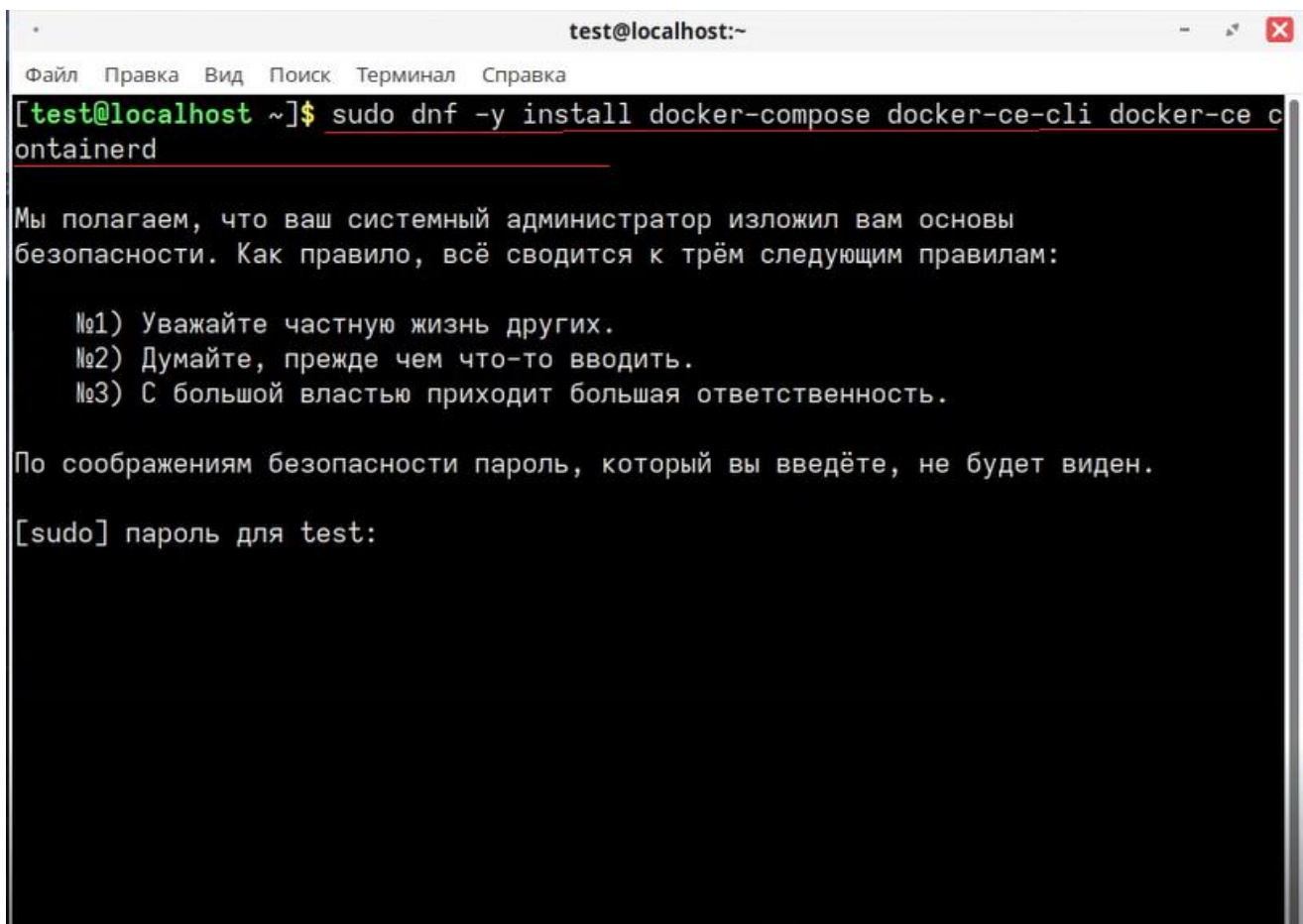
Рисунок 28 – Окно ввода учётных данных

**Примечание.** Перейти к установке РЕД ОС 7.3 на другую ЭВМ, где будет размещаться резидент.

### 3.4 Установка РЕД ОС 7.3 и Docker на ЭВМ с резидентом

Установить РЕД ОС 7.3 на вторую ВМ или ЭВМ, где будет размещаться резидент. Для этого необходимо выполнить шаги обозначенные в пункте 1.1 по установке РЕД ОС 7.3 на ЭВМ.

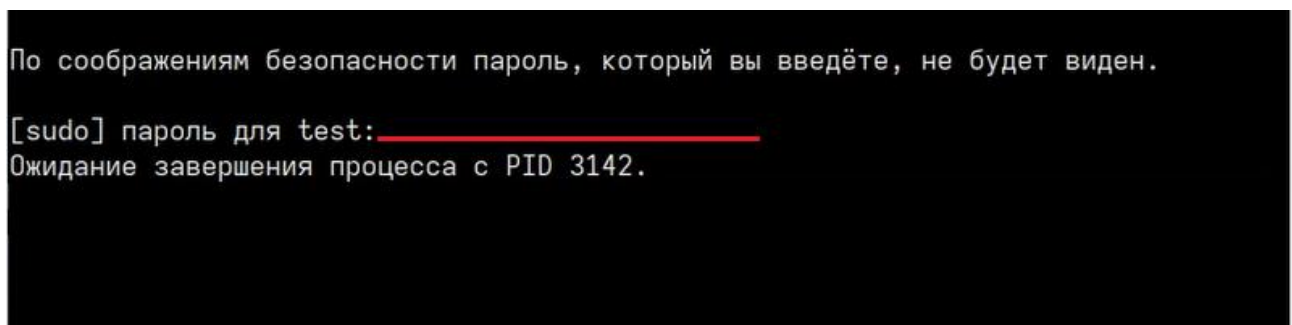
- 1) После установки РЕД ОС 7.3 на вторую ЭВМ установить Docker для этого открыть терминал и ввести команду `sudo su dnf -y install docker-compose docker-ce-cli docker-ce containerd` и нажать «Enter» на клавиатуре (рис. 29).



```
test@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[test@localhost ~]$ sudo dnf -y install docker-compose docker-ce-cli docker-ce containerd  
Мы полагаем, что ваш системный администратор изложил вам основы безопасности. Как правило, всё сводится к трём следующим правилам:  
  
№1) Уважайте частную жизнь других.  
№2) Думайте, прежде чем что-то вводить.  
№3) С большой властью приходит большая ответственность.  
  
По соображениям безопасности пароль, который вы введёте, не будет виден.  
[sudo] пароль для test:
```

Рисунок 29 – Команда для установки Docker

- 2) Ввести пароль для учетной записи созданной в ОС и нажать «Enter» на клавиатуре. Дождаться окончания установки (рис. 30).



```
По соображениям безопасности пароль, который вы введёте, не будет виден.  
[sudo] пароль для test: _____  
Ожидание завершения процесса с PID 3142.
```

Рисунок 30 – Ввод пароля пользователя

- 3) Ввести в терминал команду `systemctl start docker` (рис. 31). Используется в Linux-системах для запуска службы Docker. Нажать на клавиатуре кнопку «Enter», затем в появившемся окне введите пароль пользователя для подтверждения.

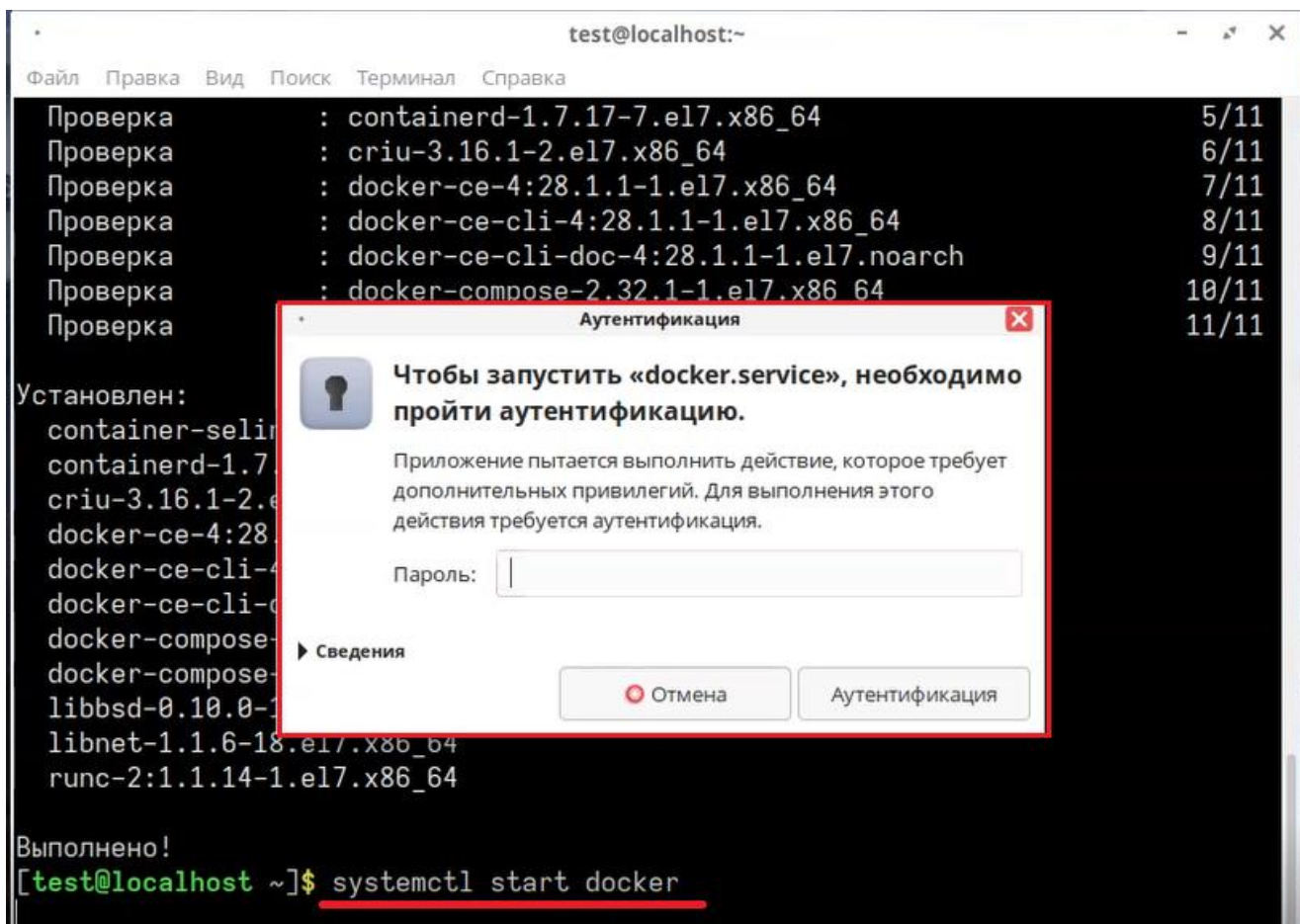
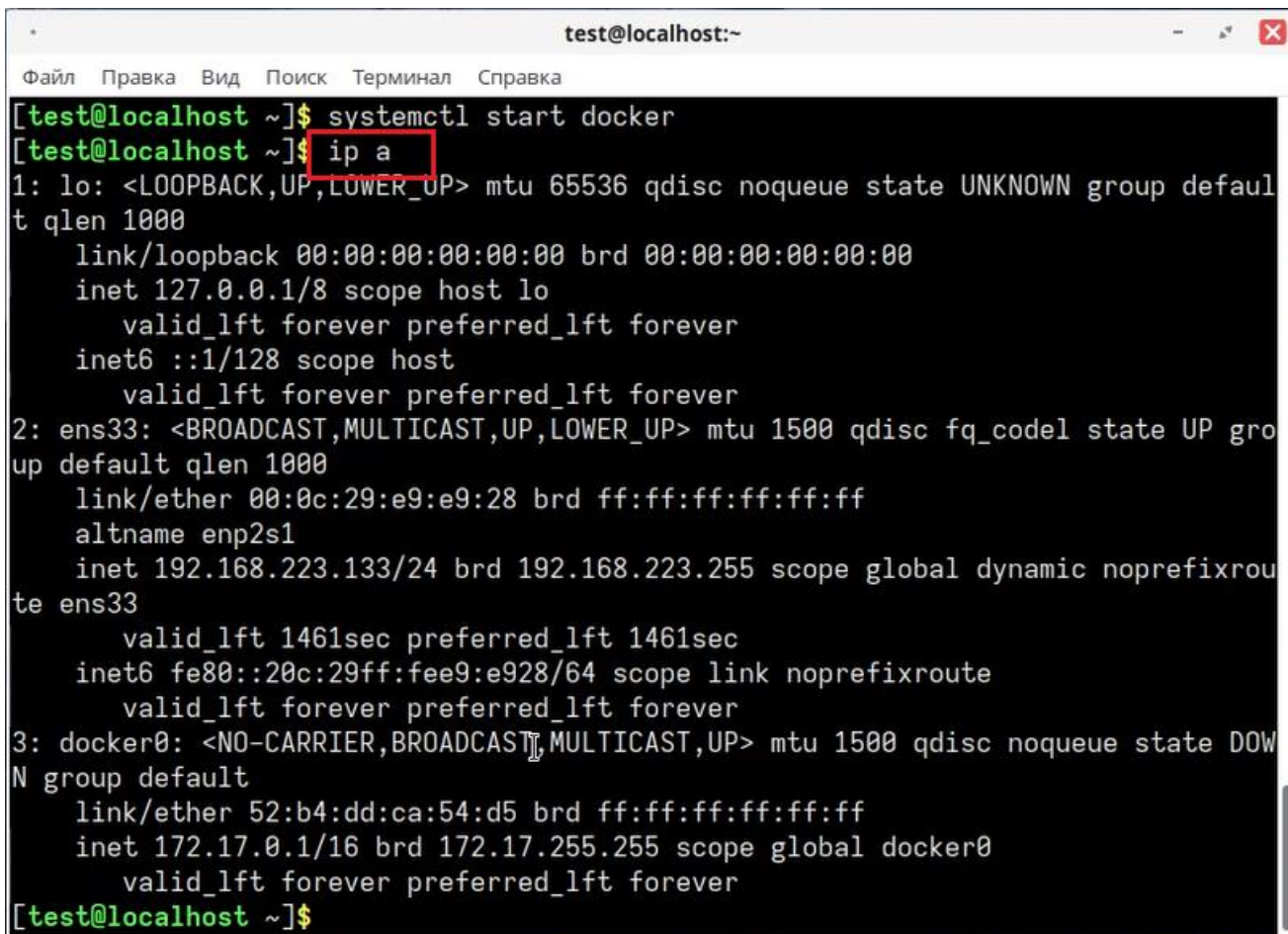


Рисунок 31 – Ввод пароля пользователя

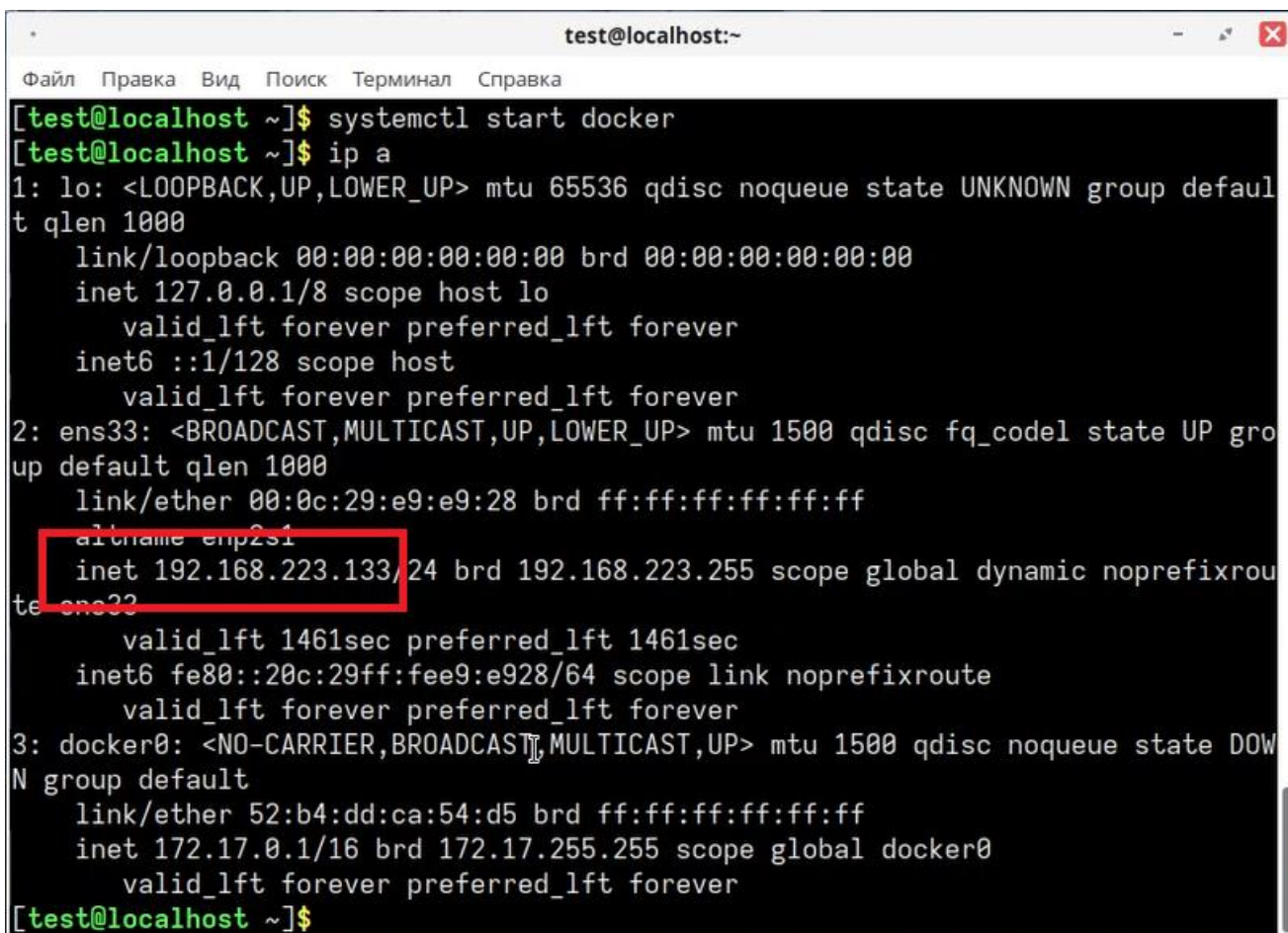
- 4) Ввести команду `ip` а в терминал. Нажать на клавиатуре кнопку «Enter» (рис. 32).



```
test@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[test@localhost ~]$ systemctl start docker  
[test@localhost ~]$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:e9:e9:28 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.223.133/24 brd 192.168.223.255 scope global dynamic noprefixroute ens33  
        valid_lft 1461sec preferred_lft 1461sec  
    inet6 fe80::20c:29ff:fee9:e928/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default  
    link/ether 52:b4:dd:ca:54:d5 brd ff:ff:ff:ff:ff:ff  
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0  
        valid_lft forever preferred_lft forever  
[test@localhost ~]$
```

Рисунок 32 – Окно терминала

- 5) Указать IP-адрес как приведено на рисунке (рис. 33). Данный IP-адрес потребуется для дальнейшей настройки.



```
test@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[test@localhost ~]$ systemctl start docker  
[test@localhost ~]$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:e9:e9:28 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.223.133/24 brd 192.168.223.255 scope global dynamic noprefixroute  
te ens33  
        valid_lft 1461sec preferred_lft 1461sec  
    inet6 fe80::20c:29ff:fee9:e928/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default  
    link/ether 52:b4:dd:ca:54:d5 brd ff:ff:ff:ff:ff:ff  
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0  
        valid_lft forever preferred_lft forever  
[test@localhost ~]$
```

Рисунок 33 – Окно терминала с полученным IP-адресом

**Примечание.** После установки РЕД ОС 7.3 и Docker на ЭВМ с резидентом на вторую ЭВМ, перейти к первой ЭВМ, на которой установлен дистрибутив с «bas\_core».

### 3.5 Установка резидента

Для установки резидента на VM необходимо выполнить следующие шаги:

- 1) в веб-интерфейсе ПК «SimuStrike» с адресом «<https://core-bas.local>» открыть раздел «Администрирование», затем перейти в подраздел «Пользователи» (рис. 34).

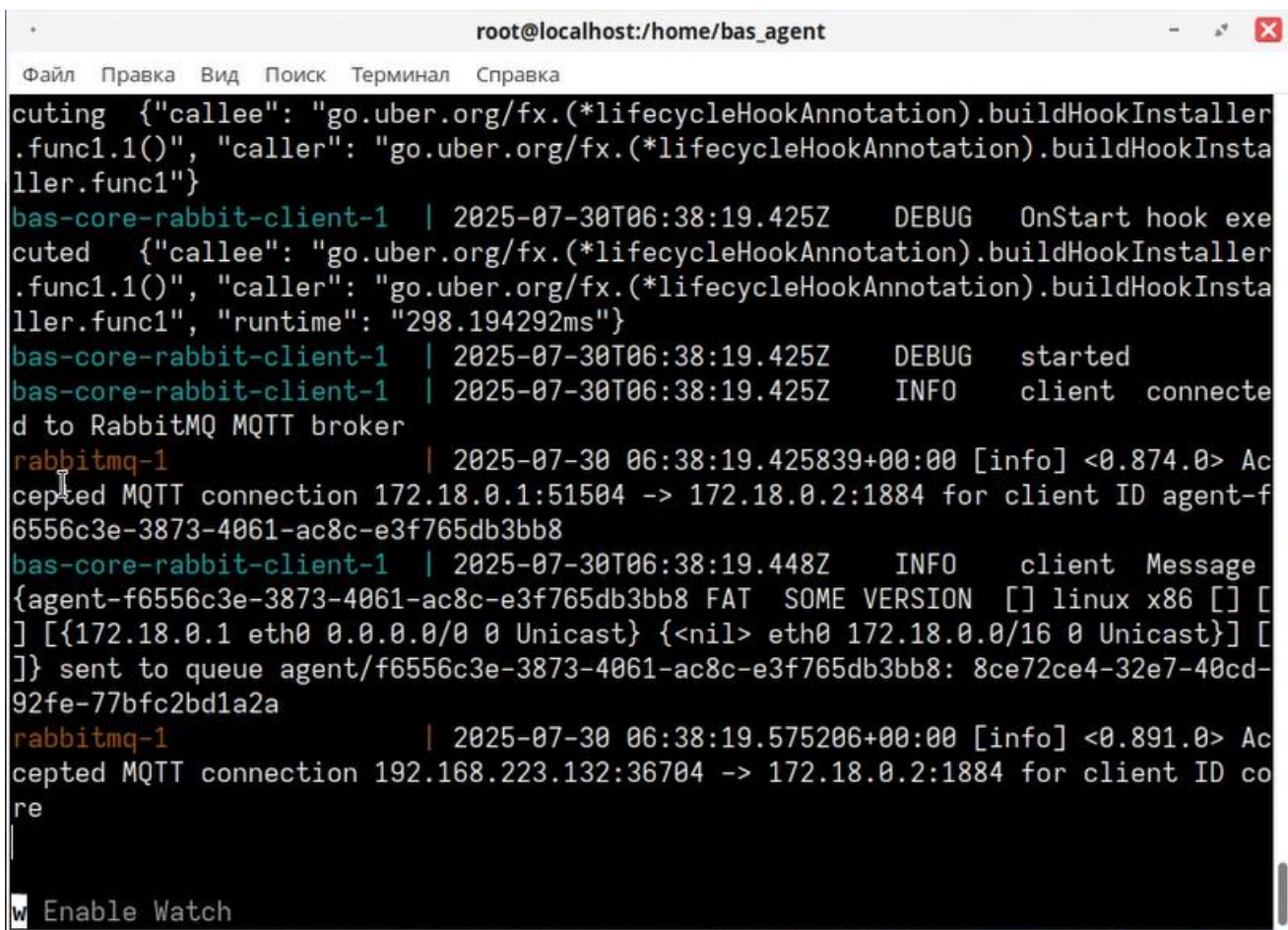


Рисунок 34 – Окно подраздела «Пользователи»

- 2) В подразделе «Пользователи» нажать кнопку «Добавить пользователя» (рис. 35).

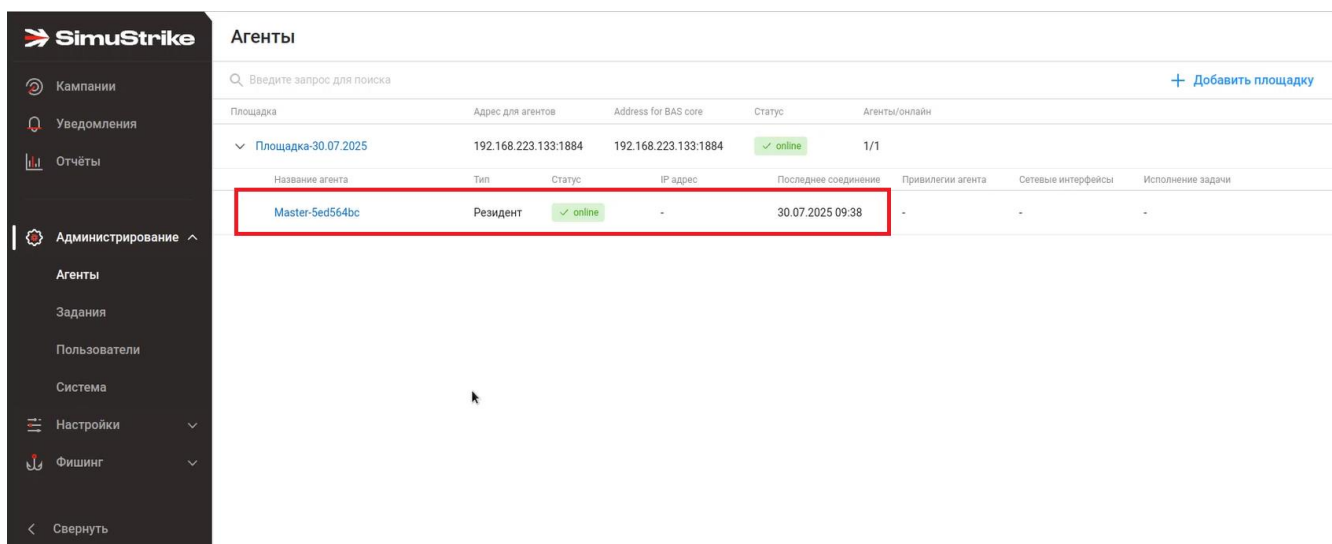


Рисунок 35 – Кнопка добавить пользователя «Добавить пользователя»

- 3) В открывшемся окне «Добавить пользователя» заполнить обязательные поля (рис. 36):

- роль. Раскрывающееся меню для выбора роли пользователя. Выбрать роль администратор;
- логин. Текстовое поле для ввода учетной записи пользователя;
- пароль. Текстовое поле для пароля пользователя со значком глаза для включения/выключения видимости пароля;
- подтверждение пароля. Текстовое поле для повторного ввода пароля для подтверждения;
- адрес электронной почты. Текстовое поле для адреса электронной почты пользователя;
- имя. Текстовое поле для имени пользователя;
- фамилия. Текстовое поле для фамилии пользователя;
- отчество. Текстовое поле для отчества пользователя. Необязательное поле.

× **Добавить пользователя**

---

Роль	<input type="text" value="Выбор роли"/>
Логин	<input type="text" value="Введите логин"/>
Пароль	<input type="password" value="Укажите пароль"/>
Подтвердите пароль	<input type="password" value="Введите подтверждение пароля"/>
E-mail адрес	<input type="text" value="email@domain.ru"/>

---

Имя	<input type="text" value="Введите имя"/>
Фамилия	<input type="text" value="Введите фамилию"/>
Отчество	<input type="text" value="Введите отчество"/>

---

Рисунок 36 – Окно «Добавить пользователя»

- 4) После заполнения обязательных полей нажать кнопку «Добавить».
- 5) Убедиться, что созданная учётная запись пользователя отображается в списке пользователей (рис. 37).

Пользователи [Пользователи](#) [Настройки](#)

🔍 Введите запрос для поиска + Добавить пользователя

Имя	Роль	Статус	Логин	Email	Создан	Дата последнего входа
Путин В.С.	Администратор	Активен	user1390	hello@123.ru	11.07.2025 09:00	-
Сутевич Д.В.	Администратор	Активен	dsutevich	sutevich-d@datagile...	14.07.2025 08:27	-
Овечкин Е.А.	-	Активен	amot1992	kazakovgrat@exam...	14.07.2025 10:28	-
Полков М.Г.	-	Активен	mg195	sevatjan_51@exam...	14.07.2025 10:32	-
Субботин А.Ф.	Пользователь	Активен	rafomkabanov	eduard1983@exampl...	09.07.2025 10:22	-
Алехин А.А.	Пользователь	Активен	login2345	-	10.07.2025 17:34	-
Никитин И.Г.	Пользователь	Активен	varlam_1999	moka_1917@exampl...	09.07.2025 10:20	-
Стрелков Р.А.	Администратор	Активен	ivanovagalina	krsamolov@example...	09.07.2025 10:57	-
Сутевич Д.В.	-	Заблокирован	jakovlejurj	sutevich-d@datagile...	09.07.2025 13:44	-
Суханов К.И.	-	Активен	ccatbev	emakarova@example...	14.07.2025 15:07	-
Левченко С.	Администратор	Активен	olevchenko	levchenko-d@datagi...	11.07.2025 12:20	-
admin	Администратор	Активен	user	-	09.07.2025 10:17	-
Семедкина Л.И.	-	Активен	samul70	genmed43@example...	15.07.2025 10:57	-
Купцов Б.М.	-	Активен	vsevolod1991	ju_b_58@example.net	16.07.2025 09:47	-
Путин А.И.	Администратор	Активен	user1234322	user@gmail.com	10.07.2025 17:36	-
Путин В.В.	Администратор	Заблокирован	user123456789101...	putin@gov.ru	10.07.2025 16:23	-

Рисунок 37 – Окно «Пользователи»

- 6) Нажать кнопку «admin» в главном меню, а затем на кнопку «Выйти» для смены пользователя (рис. 38).

Пользователи Пользователи 17 Настройки

Введите запрос для поиска

ФИО	Роль	Статус
Пупкин В.С.	Аудитор	Активен
Суткевич Д.В.	Администратор	Активен
Овчинников Е.А.	-	Активен
Поляков М.Г.	-	Активен
Субботин А.Ф.	Пользователь	Активен
Агентов А.А.	Пользователь	Активен
Никитин У.Г.	Пользователь	Активен
Стрелков Р.А.	Администратор	Активен
Суткевич Д.В.	-	Заблокирован
Суханов К.И.	-	Активен
Левченко О.	Администратор	Активен
admin	Администратор	Активен
Самойлов Л.И.	-	Активен
Куликов Б.М.	-	Активен
Пупкин А.И.	Администратор	Активен
	Аудитор	Заблокирован
	Пользователь	Заблокирован

admin  
Администратор

[-> Выйти]

Версия 0.1.1247

Всего: 17

Рисунок 38 – Кнопка «Выйти»

- 7) В открывшемся окне приветствия ПК «SimuStrike» ввести логин, пароль созданного пользователя и нажать кнопку «Войти в систему» (рис. 39).



Рисунок 39 – Окно ввода учётных данных

- 8) Открыть раздел «Администрирование», затем перейти в подраздел «Агенты» и нажать кнопку «Добавить площадку» (рис. 40).

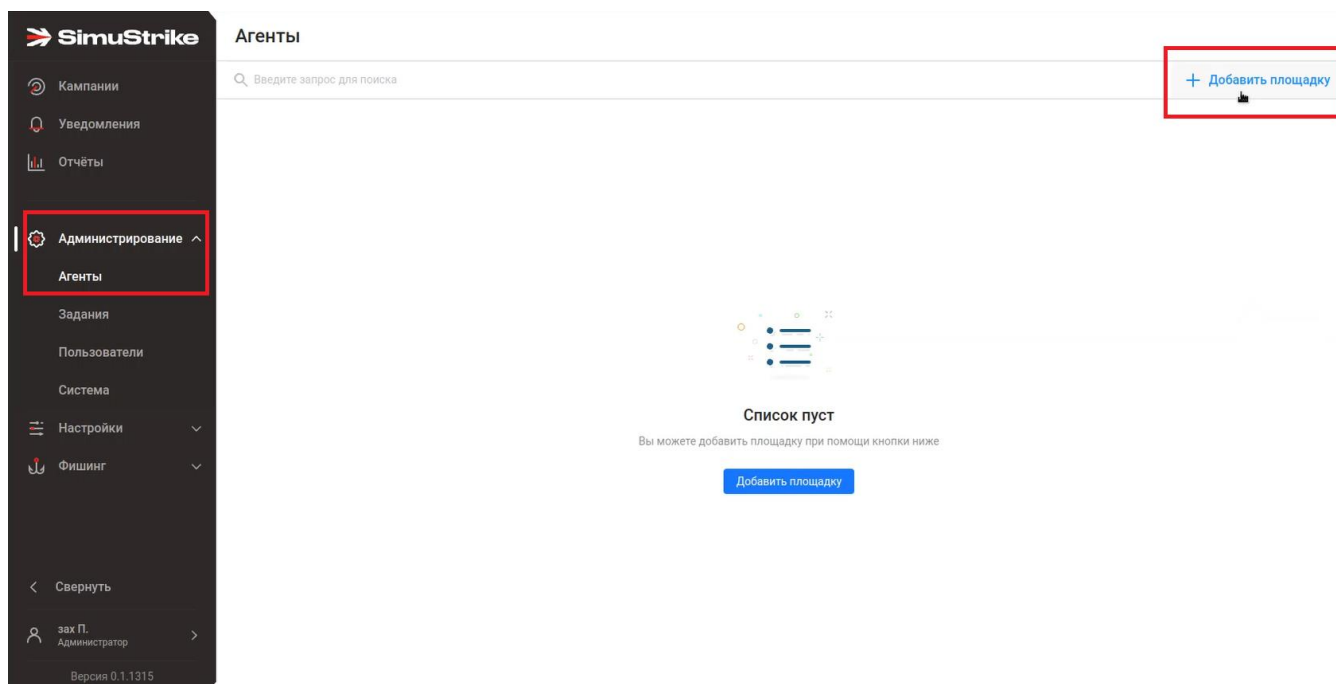


Рисунок 40 – Окно «Агенты»

- 9) В окне «Добавить площадку» заполнить поля формы (рис. 41):
- название площадки;
  - комментарий (необязательно);
  - переключатели оставить включёнными;
  - использовать порты по умолчанию;

- общий адрес агента и модуля обновления;
- адрес для площадки – IP-адрес ЭВМ, на которой установлен резидент;
- адрес для агента – IP-адрес ЭВМ, на которой установлен резидент;
- адрес обновления модулей оставить без изменения.

× **Добавить площадку**

**Подготовка:**

1. Выделите физическую или виртуальную машину на ОС RedOS 7.3+
2. Настройте сетевую доступность и маршрутизацию, в зависимости от целей площадки (внешний доступ, локальная сеть, контейнер)
- 2.a (Опционально) Присвойте FQDN и проверьте его доступность в целевой сети
3. Запишите или скопируйте сетевые параметры (IP-Адрес или FQDN)
4. Заполните необходимые настройки в форме и нажмите **Добавить**

Дополнительная информация приведена в подсказках к полям, а также в документации.

Название площадки	<input type="text" value="Площадка-30.07.2025"/>	
Комментарий	<input type="text" value="Добавьте комментарий"/>	
Использовать порты по умолчанию	<input checked="" type="checkbox"/>	
Общий адрес агента и модуля обновления	<input checked="" type="checkbox"/>	
Адрес для площадки ⓘ	<input type="text" value="192.168.223.133"/>	<input type="text" value="1884"/>
Адрес для Агента ⓘ	<input type="text" value="192.168.223.133"/>	<input type="text" value="1884"/>
Адрес обновления модулей ⓘ	<input type="text" value="192.168.223.133"/>	<input type="text" value="8888"/>

Рисунок 41 – Окно «Агенты»

- 10) Нажать кнопку «Добавить» для создания площадки.
- 11) Скачать пакет с резидентом. Для этого развернуть созданную площадку и нажать кнопку «Установить агента» (рис. 42).

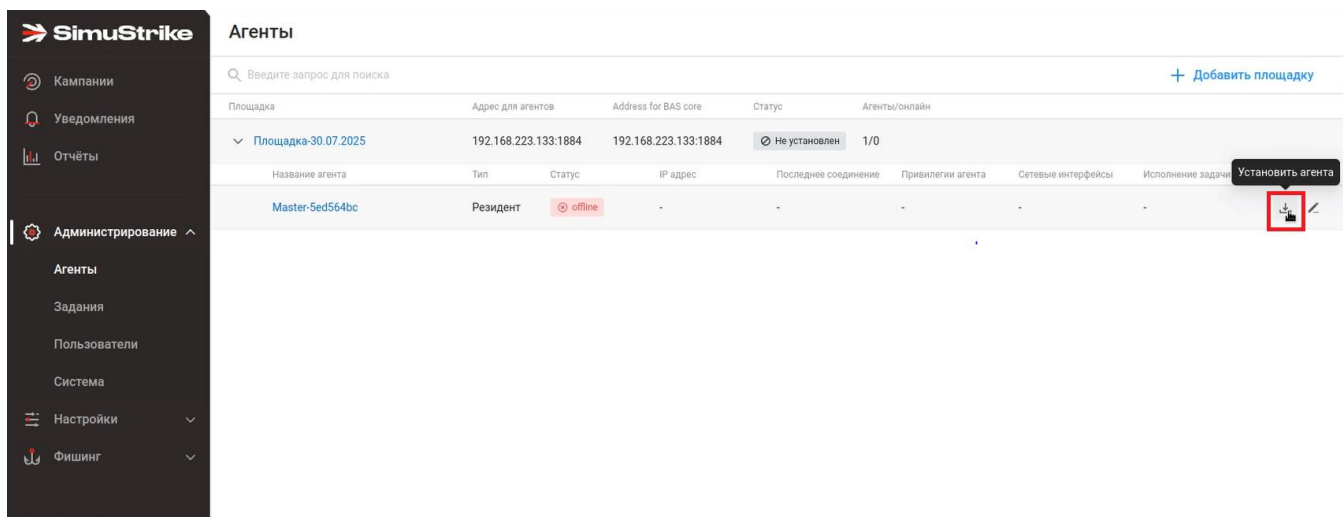


Рисунок 42 – Загрузка пакета с резидентом

12) В окне «Установка резидента» нажать кнопку «Создать токен агента» (рис. 43).

× Установка резидента

Название агента Mast  ed564bc

Тип агента Резидент

UUID агента f6556c3e-3873-4061-ac8c-e3f765db3bb8

Вид загрузки Bash скрипт

Токен агента

**1** Нажать кнопку "Создать токен агента"

**2** Выбрать необходимые параметры настройки скрипта

**3** Скопировать скрипт и запустить его в bash терминале

**Примечание**  
Скрипт работает только на Unix системах  
Для работы скрипта необходимо предварительно установить "docker"

Рисунок 43 – Окно «Установка резидента»

- 13) В окне «Установка резидента» включить переключатель «Отключить проверку SSL» и скопировать скрипт с помощью кнопки «Копировать в буфер». (рис. 44).

× **Установка резидента**

Тип агента

UUID агента

Вид загрузки

Токен агента

Отключить проверку SSL

Установить tar

Скрипт установки 

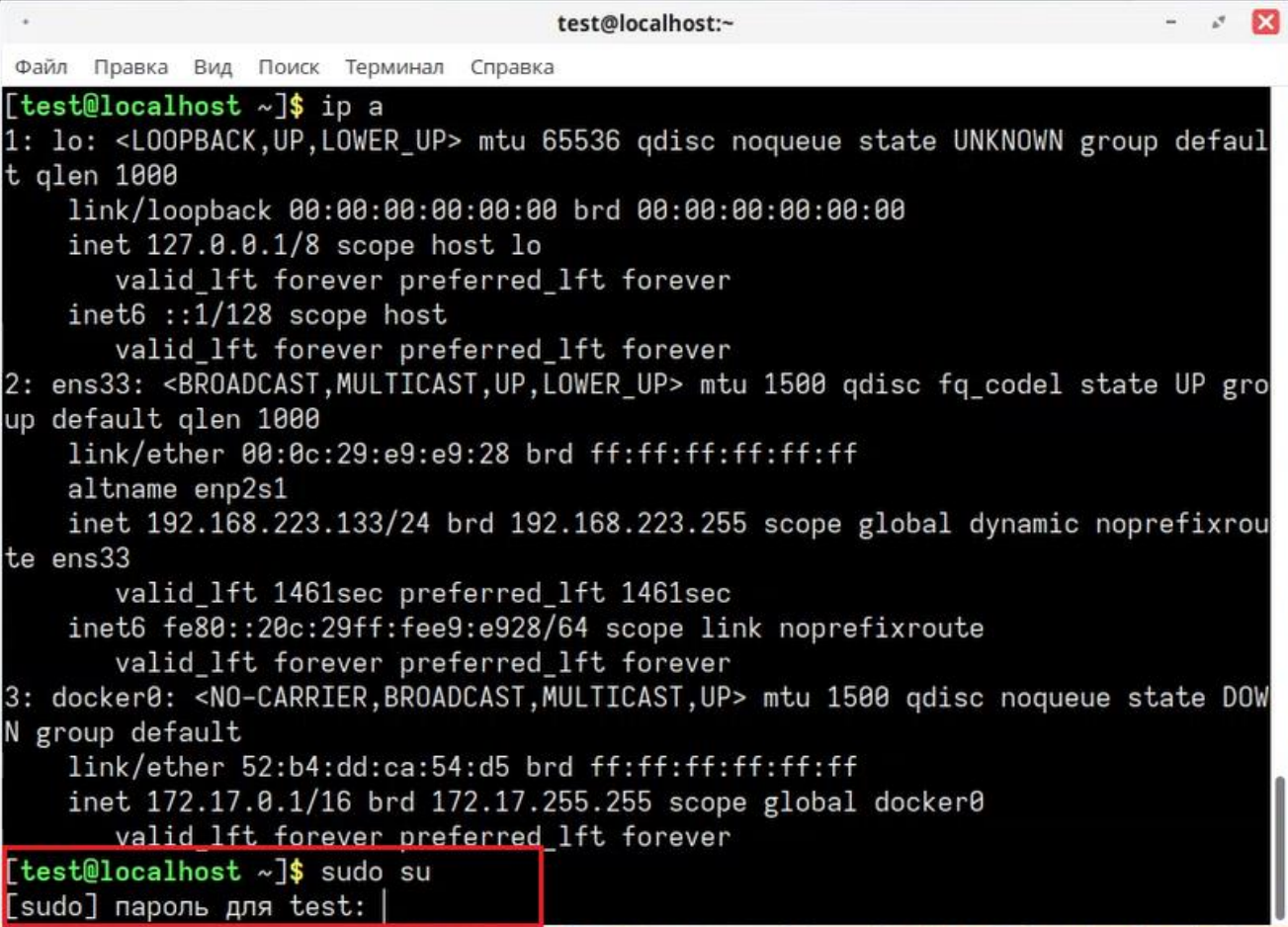
```
curl -location -X POST -H "Content-Type: application/json" -d '{"token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJJCQVMtY29yZSIsImV4cCI6MTc1Mzg2MDQ3NCwic3ViljoiZjY1NTZjM2UtMzg3My00MDYxLWFjO"}'
```

**1** Нажать кнопку "Создать токен агента"  
**2** Выбрать необходимые параметры настройки скрипта  
**3** Скопировать скрипт и запустить его в bash терминале

**Примечание**  
Скрипт работает только на Unix системах  
Для работы скрипта необходимо предварительно установить "docker"

Рисунок 44 – Создание токена

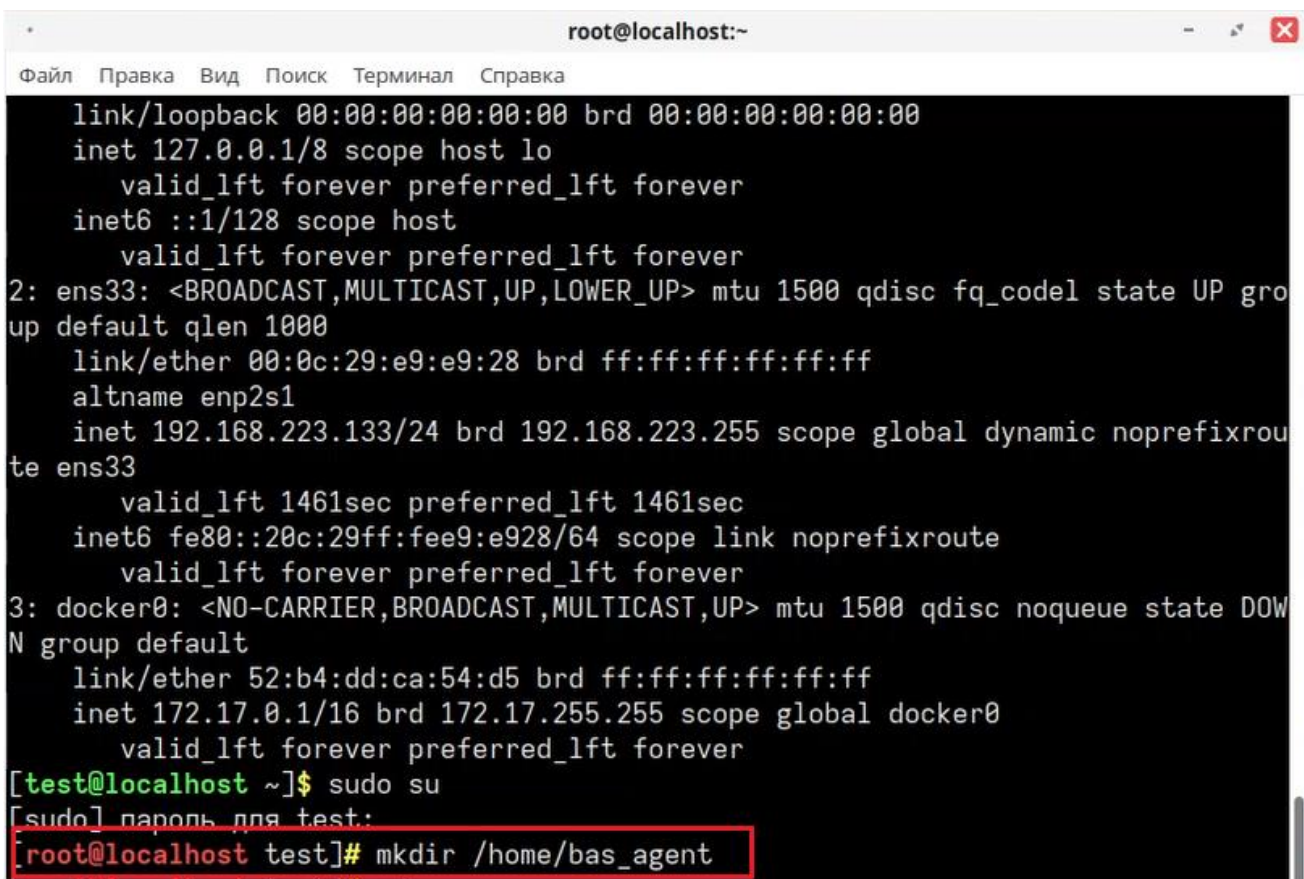
- 14) Перейти на ЭВМ с резидентом и запустить терминал с правами администратора.
- 15) Выполнить команду `sudo su` и ввести пароль от пользователя (рис. 45).



```
test@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[test@localhost ~]$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:e9:e9:28 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.223.133/24 brd 192.168.223.255 scope global dynamic noprefixroute ens33  
        valid_lft 1461sec preferred_lft 1461sec  
    inet6 fe80::20c:29ff:fee9:e928/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default  
    link/ether 52:b4:dd:ca:54:d5 brd ff:ff:ff:ff:ff:ff  
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0  
        valid_lft forever preferred_lft forever  
[test@localhost ~]$ sudo su  
[sudo] пароль для test: |
```

Рисунок 45 – Запуск скрипта от имени администратора

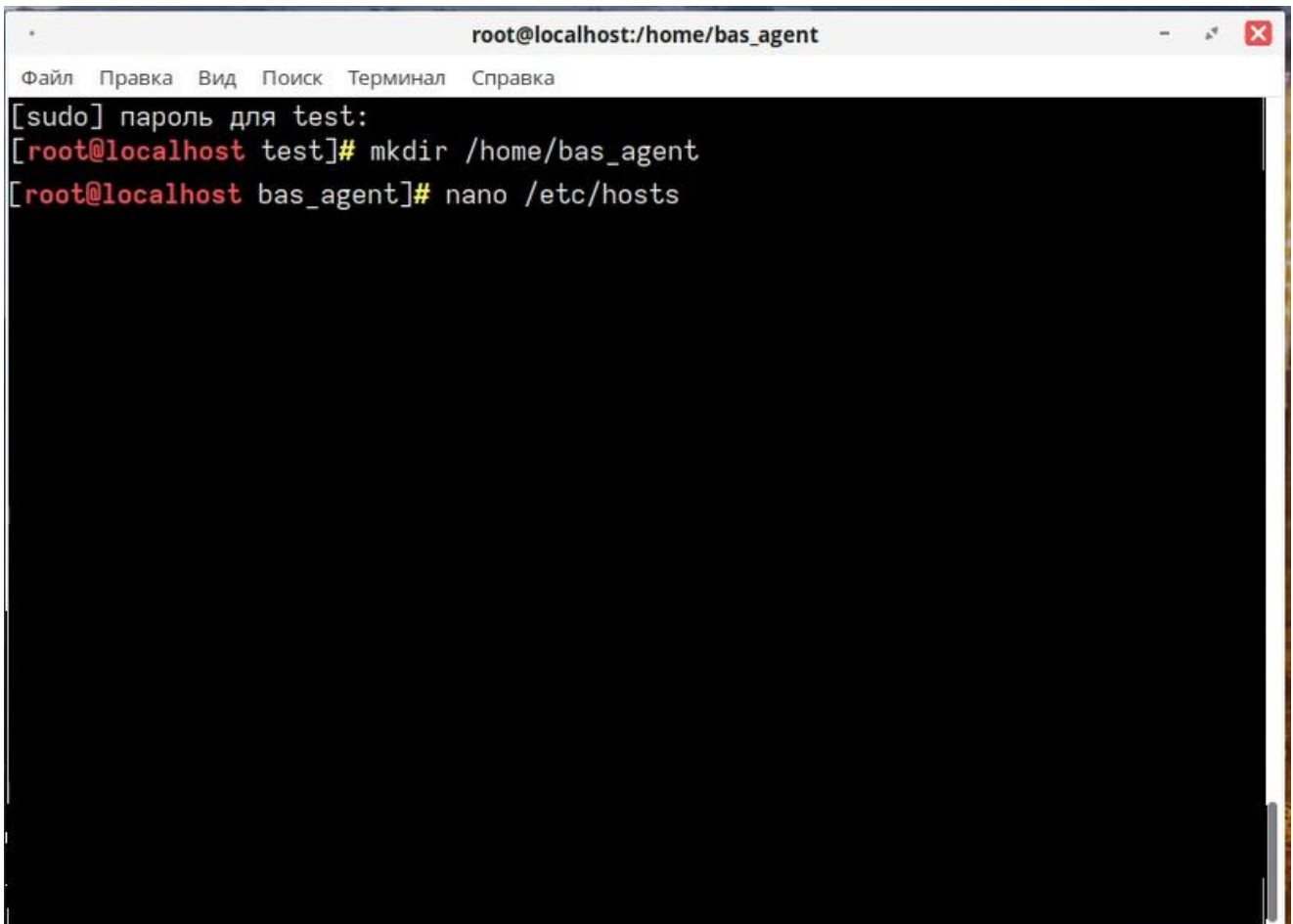
- 16) Создать отдельный каталог «bas\_agent» при помощи команды `mkdir /home/bas_agent` (рис. 46).



```
root@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
inet 127.0.0.1/8 scope host lo  
    valid_lft forever preferred_lft forever  
inet6 ::1/128 scope host  
    valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro  
up default qlen 1000  
    link/ether 00:0c:29:e9:e9:28 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.223.133/24 brd 192.168.223.255 scope global dynamic noprefixrou  
te ens33  
    valid_lft 1461sec preferred_lft 1461sec  
    inet6 fe80::20c:29ff:fee9:e928/64 scope link noprefixroute  
    valid_lft forever preferred_lft forever  
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOW  
N group default  
    link/ether 52:b4:dd:ca:54:d5 brd ff:ff:ff:ff:ff:ff  
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0  
    valid_lft forever preferred_lft forever  
[test@localhost ~]$ sudo su  
[sudo] пароль для test:  
[root@localhost test]# mkdir /home/bas_agent
```

Рисунок 46 – Создание каталога «bas\_agent»

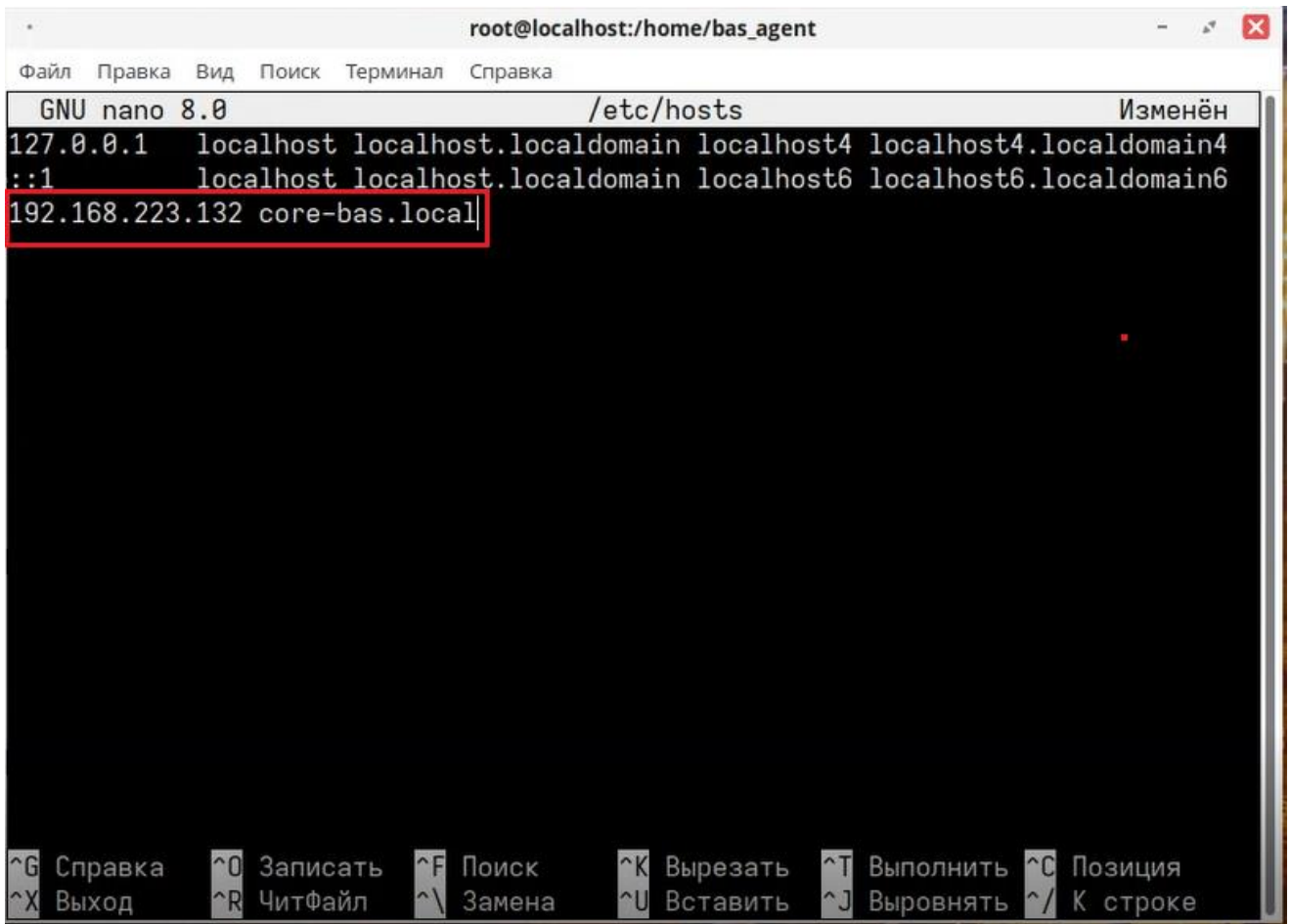
- 17) В терминале ввести команду `nano /etc/hosts`. Системный файл, который сопоставляет доменные имена с IP-адресами и используется для локального разрешения имён до обращения к DNS (рис. 47).



```
root@localhost:/home/bas_agent
Файл Правка Вид Поиск Терминал Справка
[sudo] пароль для test:
[root@localhost test]# mkdir /home/bas_agent
[root@localhost bas_agent]# nano /etc/hosts
```

Рисунок 47 – Открытие системного файла

- 18) В открывшемся редакторе снизу добавить новую строку с IP-адресом сервера, на котором установлен дистрибутив «SimuStrike» (рис. 48).

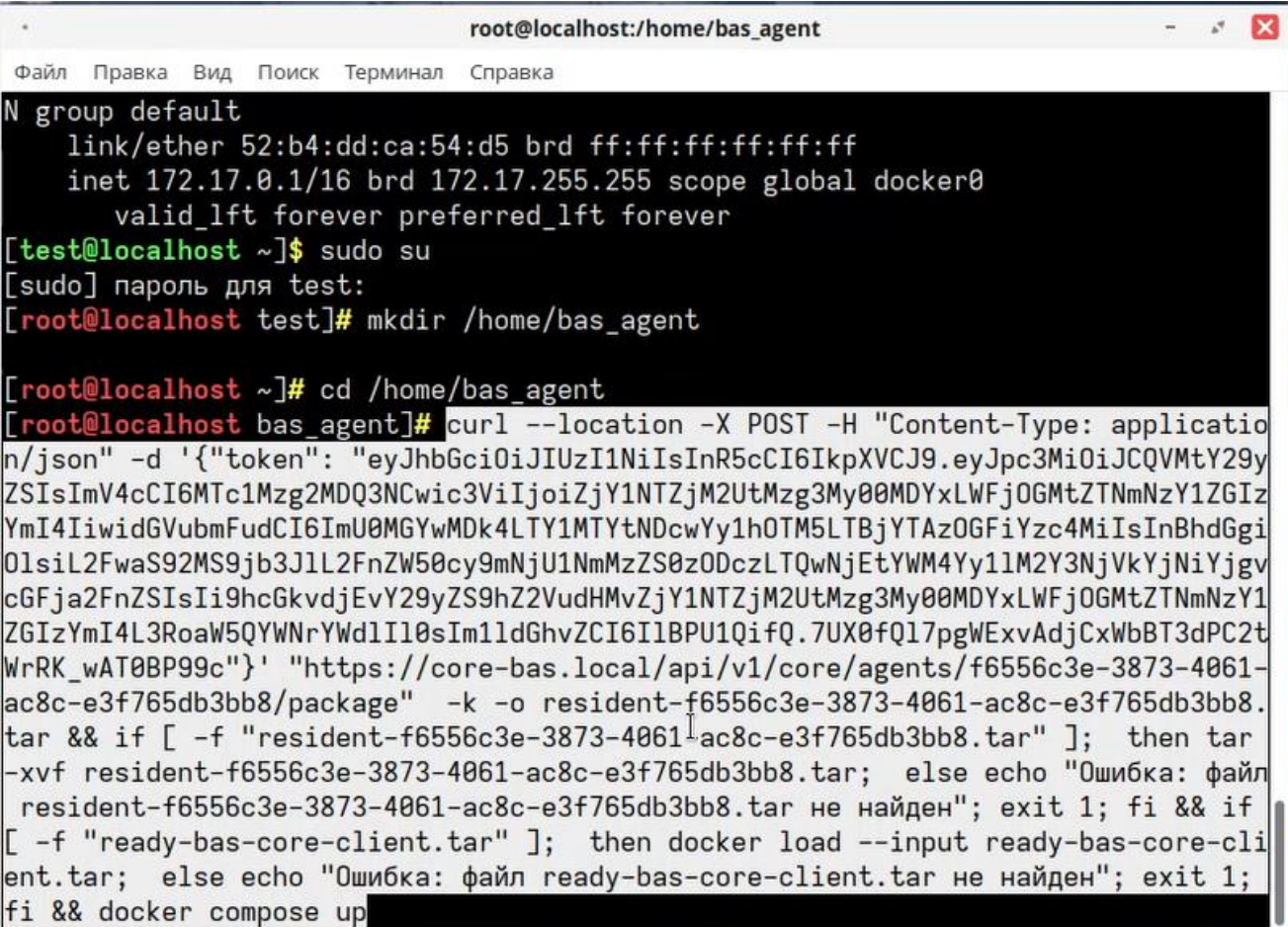


```
root@localhost:/home/bas_agent
GNU nano 8.0 /etc/hosts                               Изменён
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.223.132 core-bas.local
```

^G Справка    ^O Записать    ^F Поиск    ^K Вырезать    ^T Выполнить    ^C Позиция  
^X Выход    ^R ЧитФайл    ^\ Замена    ^U Вставить    ^J Выровнять    ^/ К строке

Рисунок 48 – IP-адрес сервера

- 19) В редакторе нажать сочетание клавиш «Ctrl+O» для сохранения изменений, затем «Enter» (подтверждение записи), после чего «Ctrl+X» для выхода из редактора.
- 20) Перейти в каталог «bas\_agent» при помощи команды `cd /home/bas_agent`. Далее ввести и выполнить скрипт установки, полученный в окне «Установка резидента» на шаге 13 (рис. 49).

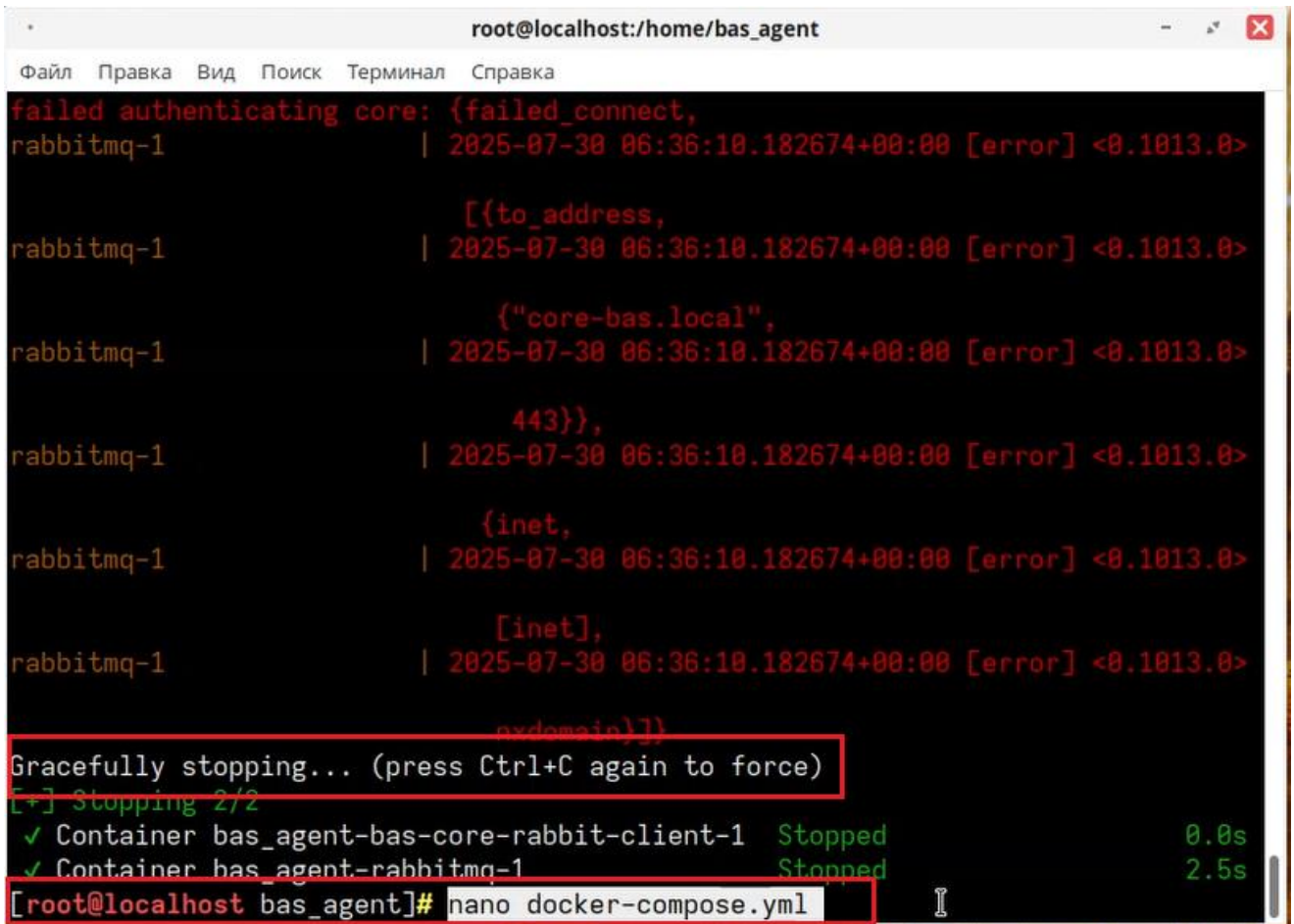


```
root@localhost:/home/bas_agent
Файл Правка Вид Поиск Терминал Справка
N group default
  link/ether 52:b4:dd:ca:54:d5 brd ff:ff:ff:ff:ff:ff
  inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
    valid_lft forever preferred_lft forever
[test@localhost ~]$ sudo su
[sudo] пароль для test:
[root@localhost test]# mkdir /home/bas_agent

[root@localhost ~]# cd /home/bas_agent
[root@localhost bas_agent]# curl --location -X POST -H "Content-Type: applicatio
n/json" -d '{"token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJJCQVMtY29y
ZSIsImV4cCI6MTc1Mzg2MDQ3NCwic3ViOiJoiZjY1NTZjM2UtMzg3My00MDYxLWFjOGMtZTNmNzY1ZGIz
YmI4IiwidGVubmFudCI6ImU0MGYwMDk4LTUyMTYtNDcwYy1hOTM5LTBjYTAzOGFiYzcyMjY3NjVjYjNiYjgv
cGFja2FnZSI6Ii9hcGkvZjEvY29yZS9hZ2VudHMvZjY1NTZjM2UtMzg3My00MDYxLWFjOGMtZTNmNzY1
ZGIzYmI4L3RoYW50YWNrYWdlIi0sIm1ldGhvZCI6IiBPU1QifQ.7UX0fQ17pgWExvAdjCxWbBT3dPC2t
WrRK_wAT0BP99c"}' "https://core-bas.local/api/v1/core/agents/f6556c3e-3873-4061-
ac8c-e3f765db3bb8/package" -k -o resident-f6556c3e-3873-4061-ac8c-e3f765db3bb8.
tar && if [ -f "resident-f6556c3e-3873-4061-ac8c-e3f765db3bb8.tar" ]; then tar
-xvf resident-f6556c3e-3873-4061-ac8c-e3f765db3bb8.tar; else echo "Ошибка: файл
resident-f6556c3e-3873-4061-ac8c-e3f765db3bb8.tar не найден"; exit 1; fi && if
[ -f "ready-bas-core-client.tar" ]; then docker load --input ready-bas-core-cli
ent.tar; else echo "Ошибка: файл ready-bas-core-client.tar не найден"; exit 1;
fi && docker compose up
```

Рисунок 49 – Токен «Установка резидента»

- 21) При возникновении ошибки остановить терминал нажатием сочетания клавиш «Ctrl+C» и ввести команду `nano docker-compose.yml` для открытия файла `docker-compose.yml` в текстовом редакторе для редактирования (рис. 50).

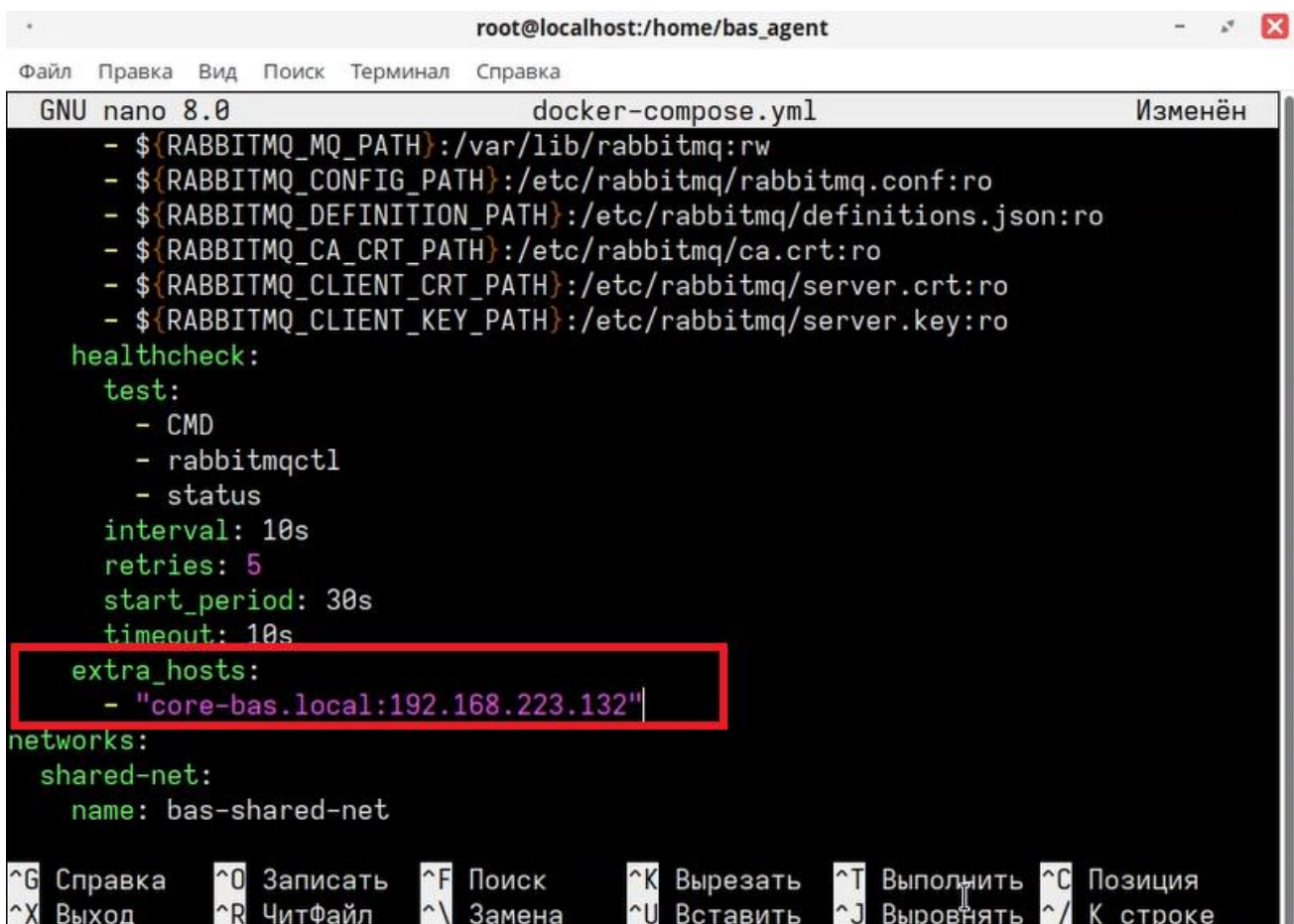


```
root@localhost:/home/bas_agent
Файл  Правка  Вид  Поиск  Терминал  Справка
failed authenticating core: {failed_connect,
rabbitmq-1      | 2025-07-30 06:36:10.182674+00:00 [error] <0.1013.0>
                | [{to_address,
rabbitmq-1      | 2025-07-30 06:36:10.182674+00:00 [error] <0.1013.0>
                | {"core-bas.local",
rabbitmq-1      | 2025-07-30 06:36:10.182674+00:00 [error] <0.1013.0>
                | 443}},
rabbitmq-1      | 2025-07-30 06:36:10.182674+00:00 [error] <0.1013.0>
                | {inet,
rabbitmq-1      | 2025-07-30 06:36:10.182674+00:00 [error] <0.1013.0>
                | [inet],
rabbitmq-1      | 2025-07-30 06:36:10.182674+00:00 [error] <0.1013.0>
                | rxdomain)}}
Gracefully stopping... (press Ctrl+C again to force)
[+] Stopping 2/2
✓ Container bas_agent-bas-core-rabbit-client-1  Stopped      0.0s
✓ Container bas_agent-rabbitmq-1              Stopped      2.5s
[root@localhost bas_agent]# nano docker-compose.yml
```

Рисунок 50 – Команда открытия файла «docker-compose.yml»

- 22) В открытом файле «docker-compose.yml» добавить две строки с IP-адресом сервера, на котором установлен дистрибутив «SimuStrike», перед секцией «networks» (рис. 51):

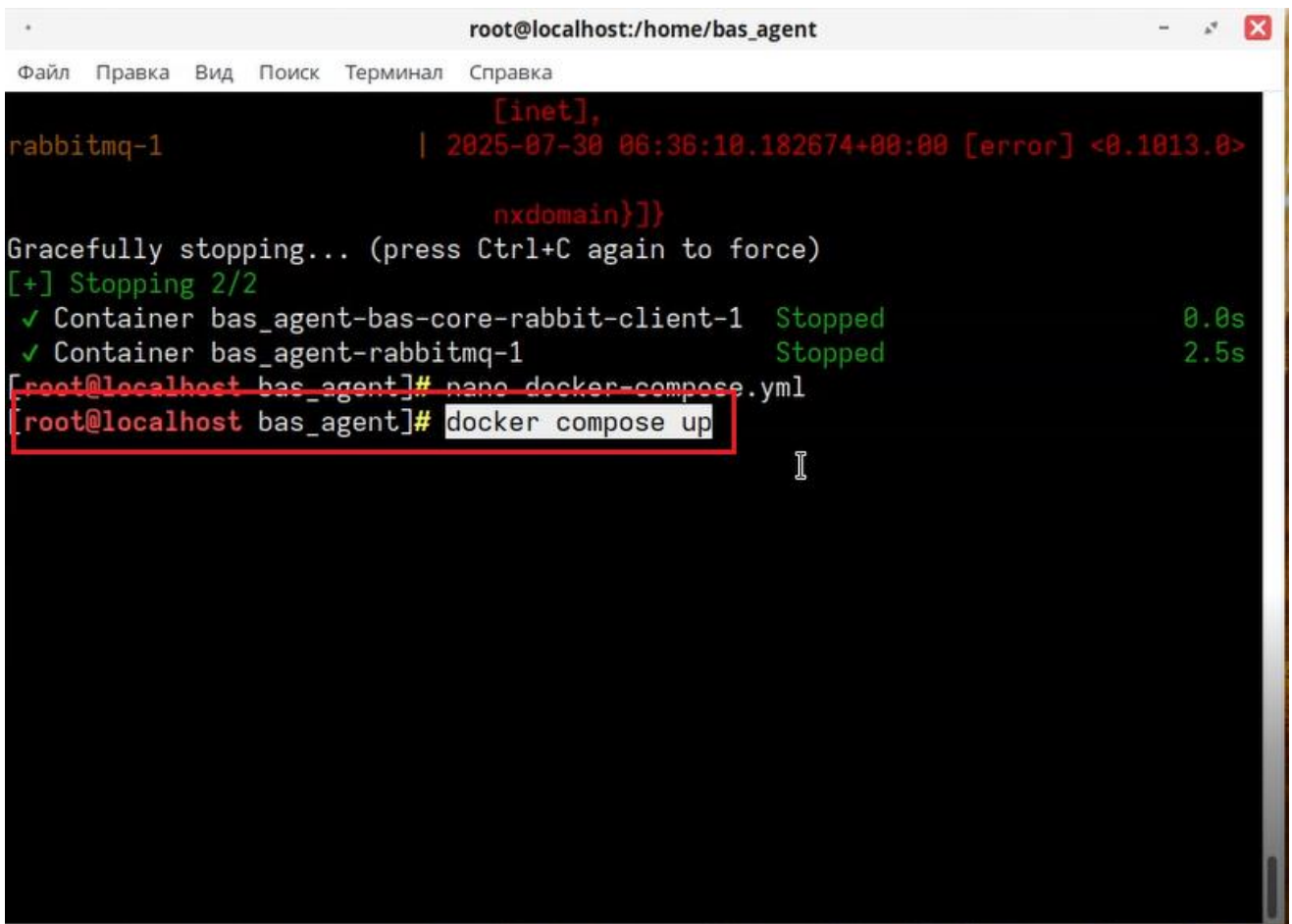
```
extra hosts:  
- "core-bas.local:192.168.223.132"
```



```
root@localhost:/home/bas_agent  
Файл Правка Вид Поиск Терминал Справка  
GNU nano 8.0 docker-compose.yml Изменён  
- ${RABBITMQ_MQ_PATH}:/var/lib/rabbitmq:rw  
- ${RABBITMQ_CONFIG_PATH}:/etc/rabbitmq/rabbitmq.conf:ro  
- ${RABBITMQ_DEFINITION_PATH}:/etc/rabbitmq/definitions.json:ro  
- ${RABBITMQ_CA_CERT_PATH}:/etc/rabbitmq/ca.crt:ro  
- ${RABBITMQ_CLIENT_CERT_PATH}:/etc/rabbitmq/server.crt:ro  
- ${RABBITMQ_CLIENT_KEY_PATH}:/etc/rabbitmq/server.key:ro  
healthcheck:  
  test:  
    - CMD  
    - rabbitmqctl  
    - status  
  interval: 10s  
  retries: 5  
  start_period: 30s  
  timeout: 10s  
extra_hosts:  
  - "core-bas.local:192.168.223.132"  
networks:  
  shared-net:  
    name: bas-shared-net  
^G Справка ^O Записать ^F Поиск ^K Вырезать ^T Выполнить ^C Позиция  
^X Выход ^R ЧитФайл ^\ Замена ^U Вставить ^J Выровнять ^/_ К строке
```

Рисунок 51 – Редактирование файла «docker-compose.yml»

- 23) В редакторе нажать сочетание клавиш «Ctrl+O» (для сохранения изменений), затем «Enter» (подтверждение записи), после чего «Ctrl+X» для выхода из редактора.
- 24) В терминале ввести и запустить команду `docker compose up`. Запуск контейнера, описанного в файле «docker-compose.yml» (рис. 52).



```
root@localhost:/home/bas_agent
Файл Правка Вид Поиск Терминал Справка
[inet],
rabbitmq-1 | 2025-07-30 06:36:10.182674+00:00 [error] <0.1013.0>
nxdomain}}
Gracefully stopping... (press Ctrl+C again to force)
[+] Stopping 2/2
✓ Container bas_agent-bas-core-rabbit-client-1 Stopped 0.0s
✓ Container bas_agent-rabbitmq-1 Stopped 2.5s
[root@localhost bas_agent]# nano docker-compose.yml
[root@localhost bas_agent]# docker compose up
```

Рисунок 52 – Запуск контейнера «docker-compose.yml»

- 25) После успешной установки в терминале перейти в браузер установленный на ОС с дистрибутивом «SimuStrike» (рис. 53).

```

root@localhost:/home/bas_agent
Файл  Правка  Вид  Поиск  Терминал  Справка
cuting {"callee": "go.uber.org/fx.(*lifecycleHookAnnotation).buildHookInstaller.func1()", "caller": "go.uber.org/fx.(*lifecycleHookAnnotation).buildHookInstaller.func1"}
bas-core-rabbit-client-1 | 2025-07-30T06:38:19.425Z    DEBUG    OnStart hook executed {"callee": "go.uber.org/fx.(*lifecycleHookAnnotation).buildHookInstaller.func1()", "caller": "go.uber.org/fx.(*lifecycleHookAnnotation).buildHookInstaller.func1", "runtime": "298.194292ms"}
bas-core-rabbit-client-1 | 2025-07-30T06:38:19.425Z    DEBUG    started
bas-core-rabbit-client-1 | 2025-07-30T06:38:19.425Z    INFO     client connected to RabbitMQ MQTT broker
rabbitmq-1 | 2025-07-30 06:38:19.425839+00:00 [info] <0.874.0> Accepted MQTT connection 172.18.0.1:51504 -> 172.18.0.2:1884 for client ID agent-f6556c3e-3873-4061-ac8c-e3f765db3bb8
bas-core-rabbit-client-1 | 2025-07-30T06:38:19.448Z    INFO     client Message {agent-f6556c3e-3873-4061-ac8c-e3f765db3bb8 FAT SOME VERSION [] linux x86 [] [] [{172.18.0.1 eth0 0.0.0.0/0 0 Unicast} {<nil> eth0 172.18.0.0/16 0 Unicast}] []} sent to queue agent/f6556c3e-3873-4061-ac8c-e3f765db3bb8: 8ce72ce4-32e7-40cd-92fe-77bfc2bd1a2a
rabbitmq-1 | 2025-07-30 06:38:19.575206+00:00 [info] <0.891.0> Accepted MQTT connection 192.168.223.132:36704 -> 172.18.0.2:1884 for client ID core
W Enable Watch
    
```

Рисунок 53 – Установка связи резидента с дистрибутивом «SimuStrike»

26) После успешной установки резидента на хосте в интерфейсе отобразится резидент со статусом «Онлайн» (рис. 54).

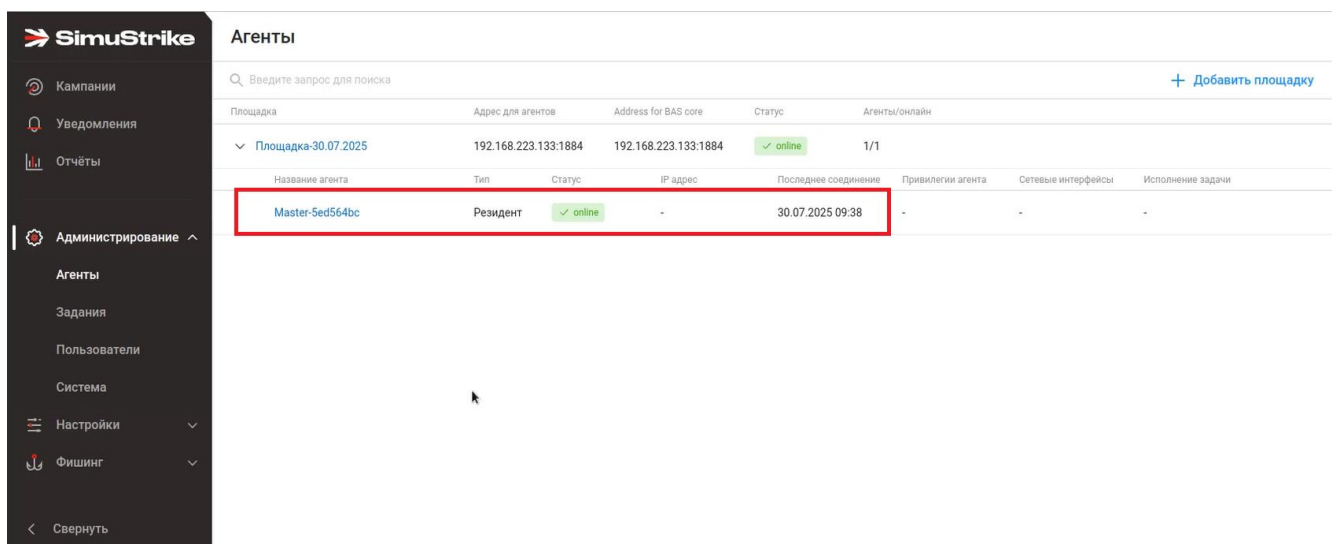


Рисунок 54 – Резидент со статусом онлайн

---

**Примечание.** После выполнения всех обязательных шагов можно приступить к созданию и настройке кампании. Дальнейшая работа с ПК «SimuStrike» описана в документе «Руководство пользователя».

---

## 4 Рекомендуемая последовательность действий при работе с комплексом

- 1) Аутентифицироваться в ПК «SimuStrike» под своим логином и паролем, выданным администратором. Для этого необходимо в веб-браузере перейти по сетевому адресу приложения и войти в комплекс, используя выданные уникальные логин и пароль, чтобы получить авторизованный доступ к личному рабочему пространству.
- 2) Создать площадку. Для этого необходимо в главном меню последовательно выбрать в разделе «Администрирование» подраздел «Агенты», нажать кнопку «Добавить площадку», заполнить форму требуемыми параметрами и нажать кнопку «Добавить».
- 3) Установить резидента в соответствии с выбранным сценарием в инфраструктуру:
  - Моделирование атаки внешнего нарушителя. Находясь во внешней сети, BAS подключается к резиденту по внешнему адресу, передавая ему задачи по атаке внутренних ресурсов организации; резидент, в свою очередь, выполняет эти задачи (сканирование, распространение, сбор данных) изнутри сети, а развёрнутые в ней агенты подключаются к резиденту по указанному адресу для получения исполняемых модулей.
  - Моделирование атаки внутреннего нарушителя. Находясь внутри сети, BAS подключается к резиденту по внутреннему адресу, ставит ему задачи на атаку других внутренних ресурсов (например, перемещение по сети и поиск ценных данных), после чего резидент выполняет эти задачи, а агенты, как и сам BAS, подключаются к нему для дальнейшей работы.
- 4) Создать кампанию и заполнить «Основные настройки». Для создания кампании необходимо в разделе «Кампании» главного меню нажать кнопку «Добавить кампанию», перейти в блок «Основные настройки» и заполнить обязательные поля.
- 5) В созданной кампании выбрать, настроить и активировать необходимые целевые модули. Выбрать из предложенного списка и детально настроить конкретные методы атаки (модули), которые резидент будет выполнять в рамках сценария.
- 6) Сохранить и запустить созданную кампанию. После активации всех нужных модулей нажать кнопку «Завершить создание кампании», после чего резидент начнет выполнять все активированные и настроенные модули атаки.
- 7) Осуществить мониторинг на странице карточки кампании. Для осуществления мониторинга необходимо открыть соответствующую кампанию в разделе «Кампании» и выбрать нужную вкладку.
- 8) Завершить кампанию в случае необходимости. Для завершения кампании с целью сбора финальных логов и освобождения ресурсов комплекса при достижении целей или возникновении такой необходимости следует в

разделе «Кампании» открыть нужную кампанию, нажать кнопку «Управление» и выбрать опцию «Завершить кампанию».

## 5 Лицензирование

Для проведения активации комплекса необходимо перейти в раздел «Администрирование», подраздел «Лицензия» (рис. 47).

Возможны два варианта проведения активации комплекса:

- online активация – при наличии подключения к серверу лицензирования;
- offline активация – при отсутствии подключения к серверу лицензирования.

### 5.1 Основные положения лицензирования

- 1) Возможности определенного функционального модуля в ПК «SimuStrike» доступны только при наличии лицензии на его использование.
- 2) В ПК «SimuStrike» доступна базовая (гарантийная) и расширенная лицензия. Их различие заключается в уровне сервисной поддержки и составе предоставляемых модулей:
  - Базовая лицензия включает в себя: модуль сетевого сканирования, модуль сканирования Web, модуль сканирования AD, модуль проверки утечек данных, модуль первоначального доступа, модуль горизонтального перемещения, модуль эксфильтрации данных, модуль удаления и шифрования данных, модуль локальной разведки, модуль перебора УЗ, модуль закрепления, модуль повышения привилегий.
  - Лицензии модулей расширения включают в себя: модуль фишинга, модуль TI-фидов, модуль перебора хешей. Лицензия поддерживает мультитенантность и сопровождается приоритетной технической поддержкой по более высокому сервисному соглашению.
- 3) Лицензия активируется для всего комплекса в целом, в ней определены:
  - перечень функциональных модулей;
  - лимит количества доступных тенантов;
  - дата начала и окончания действия лицензии комплекса;
  - номер лицензии для технической поддержки.

### 5.2 Ограничения срока действия лицензии комплекса

#### 5.2.1 Ограничение по сроку действия

- 1) Все лицензии являются срочными. Бессрочные лицензии не предоставляются.
- 2) Поведение комплекса зависит от статуса активации лицензии:
  - За месяц до окончания срока действия лицензии комплекс выводит предупреждение: «Срок действия лицензии закончится <ДАТА>». Необходимо перейти во вкладку «Лицензия» для продления периода использования.
  - При истечении срока действия лицензии комплекс блокирует функциональность и выводит сообщение: «Срок действия лицензии закончился». Необходимо перейти во вкладку «Лицензия» для возобновления использования. Доступ

сохраняется только для локального администратора с возможностью управления вкладками «Лицензия» и «Пользователи».

---

**Примечание.** До момента пока лицензия не активирована функциональные возможности комплекса недоступны.

---

### **5.2.2 Ограничения по функциональным модулям**

Перечень доступных модулей (например, «Фишинг» и другие) определяется свойствами лицензии.

### **5.2.3 Ограничение по количеству уникальных хостов**

- 1) Каждая лицензия имеет ограничение на максимальное количество хостов. Комплекс контролирует использование этого лимита, учитывая все хосты в кампаниях со статусом «В работе». При этом один и тот же хост, встречающийся в разных кампаниях, учитывается каждый раз как новый в связи с разными контекстами настройки кампании.
  - 2) При превышении лимита хостов более чем на 10% комплекс блокирует создание новых кампаний и отображает соответствующее предупреждение.
- 

**Примечание.** Для разблокировки необходимо завершить часть активных кампаний или расширить лицензию.

---

## Перечень терминов и определений

- Кампании – Представляют собой имитацию многоступенчатых хакерских атак. Их можно настраивать различными способами, включая сценарии, которые моделируют действия только внутренних нарушителей. В таких случаях достаточно активировать модули эксплуатации, перемещения в сети и закрепления, в то время как разведка может не потребоваться.
- Площадка – Часть поверхности атаки, доступная основному агенту (резиденту). Например, если резидент установлен удалённо от инфраструктуры, он может начать атаку с внешнего веб-сервера. В случае, когда резидент установлен внутри инфраструктуры, он имитирует внутреннего нарушителя. Резидент обладает всеми необходимыми инструментами для проведения атак.
- Резидент – Ключевой компонент, необходимый для пользования ПК. Для корректного функционирования системы требуется наличие как минимум одного резидента.
- Агентская система – Предназначена для распространения функциональных возможностей программы по всей сети, включая подсети, DMZ и изолированные VLAN, при наличии как минимум одной сетевой связи с сегментом сети, в котором уже присутствует агент.
- Тонкий агент – Используются для закрепления и распространения в инфраструктуре: «не содержат большого количества инструментов, но способны выполнять скрипты и при необходимости загружать дополнительные инструменты». Это позволяет им быть гибкими и адаптивными в процессе атаки, обеспечивая возможность быстрого реагирования на изменяющиеся условия.
- Толстый агент – Необходим для выполнения ряда ключевых задач в системе BAS. Он содержит все необходимые инструменты и функции для проведения проверок, сканирования и анализа, что позволяет эффективно выявлять уязвимости и угрозы. Кроме того, толстый агент способен запускать скрипты и инструменты для анализа защищенности, что позволяет тестировать новые идеи и решения в реальных условиях. Толстый агент также может обрабатывать и анализировать большие объемы данных, что способствует более глубокому пониманию состояния безопасности системы. Он способен функционировать независимо, что позволяет ему выполнять задачи даже в условиях ограниченной сетевой связи. Наконец, толстый агент может взаимодействовать с другими компонентами BAS и системами безопасности, обеспечивая комплексный подход к защите информации. Таким образом, толстый агент играет ключевую роль в обеспечении безопасности и эффективности работы системы.

## Перечень сокращений

AD	–	Active Directory
API	–	Application Programming Interface
BAS	–	Breach and Attack Simulation
HTTP	–	HyperText Transfer Protocol
HTTPS	–	HyperText Transfer Protocol Secure
IP	–	Internet Protocol
SSH	–	Secure Shell
БД	–	База данных
ВМ	–	Виртуальная машина
ИБ	–	Информационная безопасность
ОС	–	Операционная система
ПК	–	Программный комплекс
ПО	–	Программное обеспечение
СрЗИ	–	Средства защиты информации
СЗИ	–	Система защиты информации
ИБ	–	Информационная безопасность