SOLAR

SafeConnect

Версия 1.17.0

Руководство по установке SafeConnect

Москва, 2026

Содержание

1. Аннотация 3
2. Введение 4
3. Системные требования 5
    3.1. Системные требования к виртуальному устройству 5
        3.1.1. Виртуальное устройство на базе VMware Workstation, ESXi 5
    3.2. Поддерживаемые веб-браузеры 5
4. Проверка контрольных сумм дистрибутива 6
    4.1. Проверка контрольных сумм дистрибутива при использовании ОС Windows 6
        4.1.1. Проверка КС дистрибутива утилитой CertUtil 6
        4.1.2. Проверка КС дистрибутива утилитой cpverify 9
    4.2. Проверка контрольных сумм дистрибутива при использовании ОС Linux 12
        4.2.1. Проверка КС дистрибутива утилитами md5sum и sha256sum 12
        4.2.2. Проверка КС дистрибутива утилитами cpverify 15
        4.2.3. Проверка КС дистрибутива утилитами gostsum 17
5. Установка программы 18
    5.1. Установка и настройка ОС Astra Linux 18
        5.1.1. Установка ОС Astra Linux 1.7.7 18
        5.1.2. Инсталляция SafeConnect в виртуальной машине 35
    5.2. Создание и настройка VMware 36
        5.2.1. Создание ВМ на базе VMware Workstation 36
        5.2.2. Создание ВМ на базе VMware ESXi 43
        5.2.3. Инсталляция SafeConnect в ВМ 49
6. Запуск ПК SafeConnect 59

1. Аннотация

Настоящее руководство содержит инструкции по инсталляции программного комплекса SafeConnect, который предназначен для обеспечения эффективного удаленного доступа к IT ресурсам на уровне приложений, в современных информационных системах средних и крупных предприятий.

2. Введение

Данный документ предназначен для администратора или системного администратора, который планирует установку программного комплекса SafeConnect на виртуальную машину в среде VMware (Workstation, ESXi), ОС Astra Linux 1.7.7.9 с версией ядра 6.1.124-1-generic.

В этом руководстве содержится инструкция по инсталляции ПК SafeConnect (далее - SafeConnect, Портал) на виртуальную машину VMware (Workstation, ESXi), Astra Linux 1.7.7.9.

3. Системные требования

Программный комплекс SafeConnect может быть установлен как на аппаратное устройство (компьютер), так и на виртуальное устройство (виртуальную машину). В этом разделе приведены системные требования для установки на виртуальное устройство.

3.1. Системные требования к виртуальному устройству

Для установки SafeConnect в качестве виртуальной среды рекомендуется использовать:

- Proxmox Virtual Environment (версии 8.2.3, 8.2.7);
- VMware ESXi (версия 7.0);
- VMware Workstation (версия 17).

3.1.1. Виртуальное устройство на базе VMware Workstation, ESXi

Если вы инсталлируете SafeConnect на виртуальное устройство, необходимо создать виртуальную машину со спецификациями, которые приведены в таблице (Табл.3.1).

Табл. 3.1. Минимальные системные требования к ВМ VMware

Спецификация	Значение
Память	2 GB или более
Размер диска	20 GB или более
Тип гостевой операционной системы, установленной на виртуальную машину	Тип: Linux Версия: Astra Linux 1.7.7.9 с версией ядра 6.1.124-1-generic
Сетевое оборудование	Минимально 1 сетевой адаптер

3.2. Поддерживаемые веб-браузеры

Для использования веб-интерфейса администратора рекомендуем следующую спецификацию системы:

- Активированный JavaScript;
- Разрешение экрана 1024x768 или более;
- Предпочитаемый браузер Chrome (Chromium) или браузеры на его основе (некоторые специфичные функции, такие как copy-paste требовательны к используемому ПО).

4. Проверка контрольных сумм дистрибутива

4.1. Проверка контрольных сумм дистрибутива при использовании ОС Windows

4.1.1. Проверка КС дистрибутива утилитой CertUtil

Для определения целостности дистрибутива при использовании ОС Windows 7 и новее рекомендуется использовать утилиту CertUtil. Эта утилита входит в состав Windows 7 и новее.

Чтобы определить контрольные суммы дистрибутива необходимо:

1. Загрузить образ диска на локальное хранилище;
2. Запустить командную строку (открыть меню Пуск, найти приложение **Командная строка** или **Cmd**, нажать **Открыть**) (Рис.4.1);

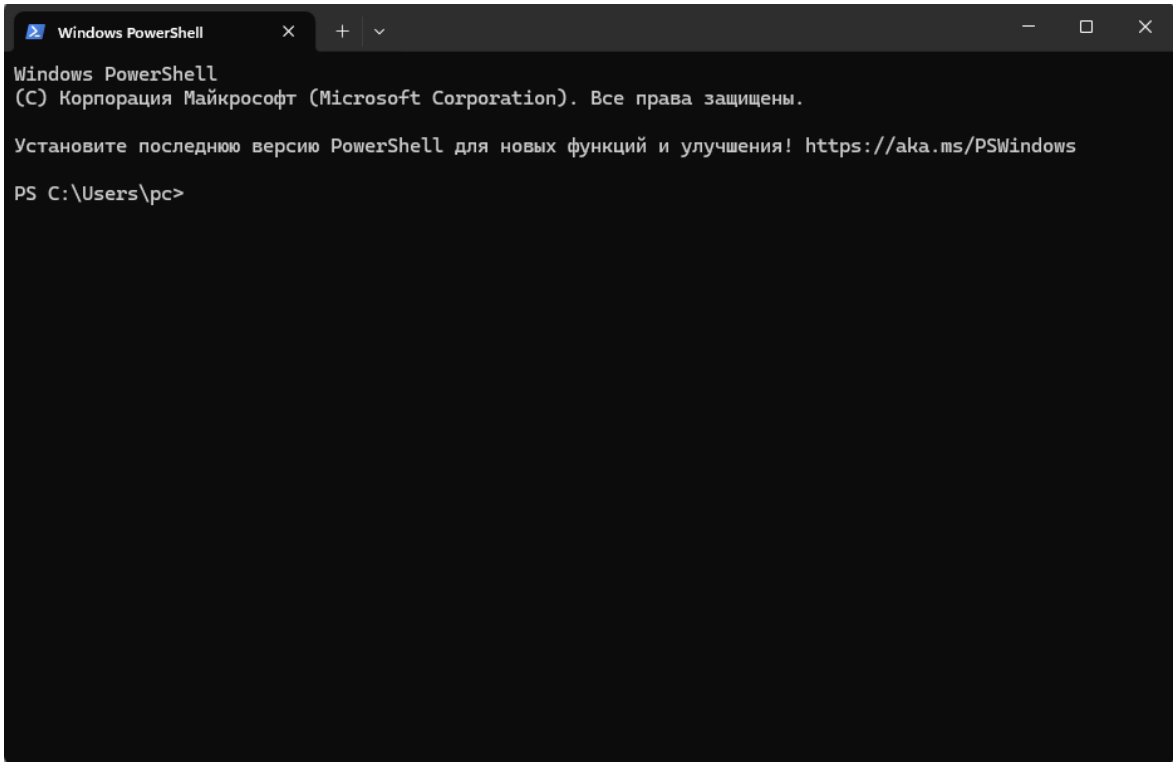


Рис. 4.1. Командная строка

3. В командной строке ввести команду:
   - для получения контрольной суммы MD5 (Рис.4.2):
     ```
     certutil -hashfile "<путь_к_файлу>\<имя_файла>.iso" MD5
     ```
     например (Рис.4.2):
     ```
     certutil -hashfile "C:\Users\pc\Downloads\solar_safeconnect.iso" MD5
     ```

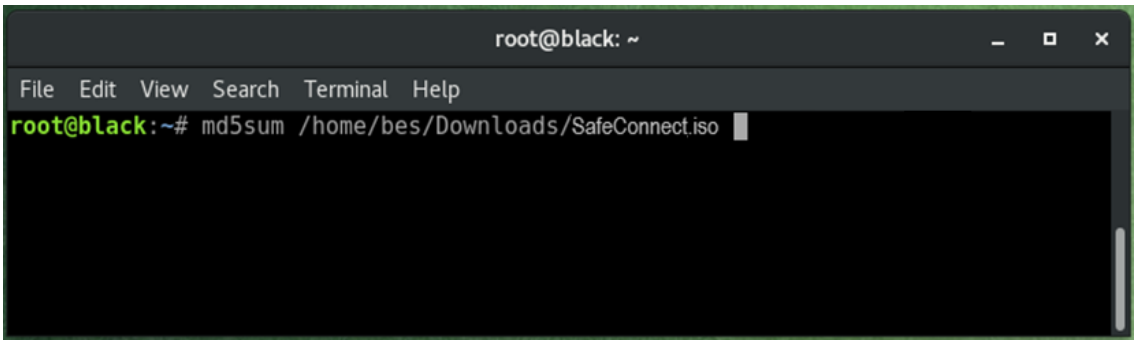


Рис. 4.2. Пример ввода команды

- для получения контрольной суммы SHA256:
  `certutil -hashfile "<путь_к_файлу>\<имя_файла>.iso" SHA256`

  например:
  `certutil -hashfile "C:\Users\pc\Downloads\solar_safeconnect.iso" SHA256`

4. Нажать **Enter**;
5. Дождаться окончания выполнения команды (Рис.4.3):

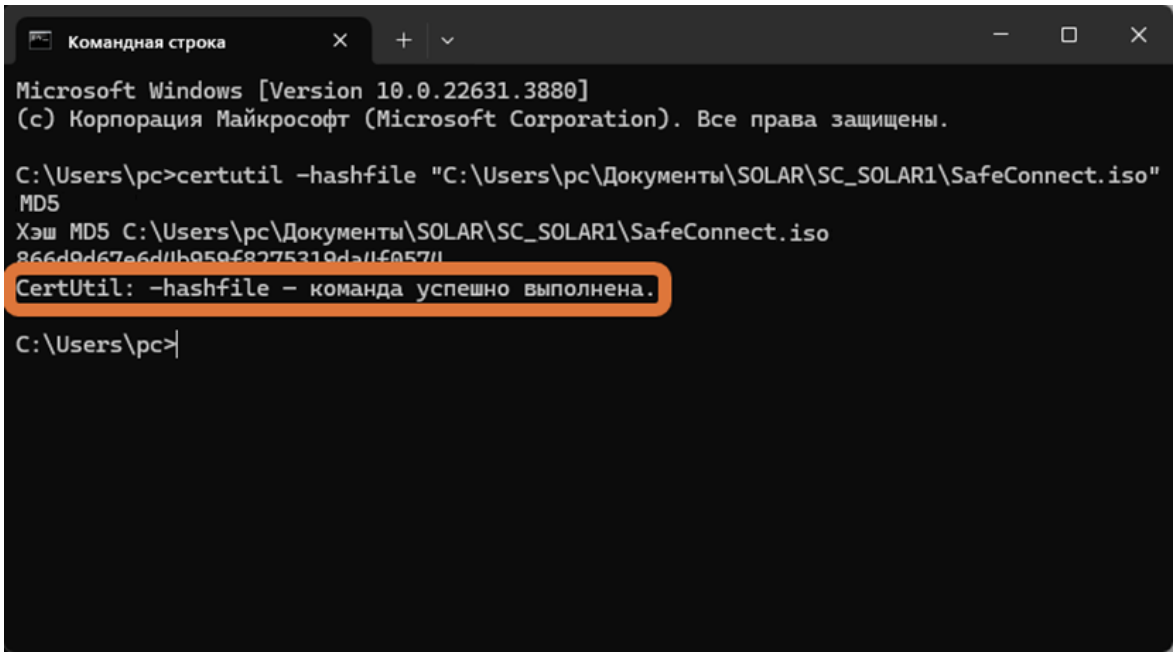


Рис. 4.3. Сообщение об успешном выполнении команды

6. Найти строку с полученным результатом (Рис.4.4):

   например:

   Хэш MD5 **C:\Users\pc\Downloads\SafeConnect.iso**:

   `866d9d67e6d4b959f8275319da4f0574`

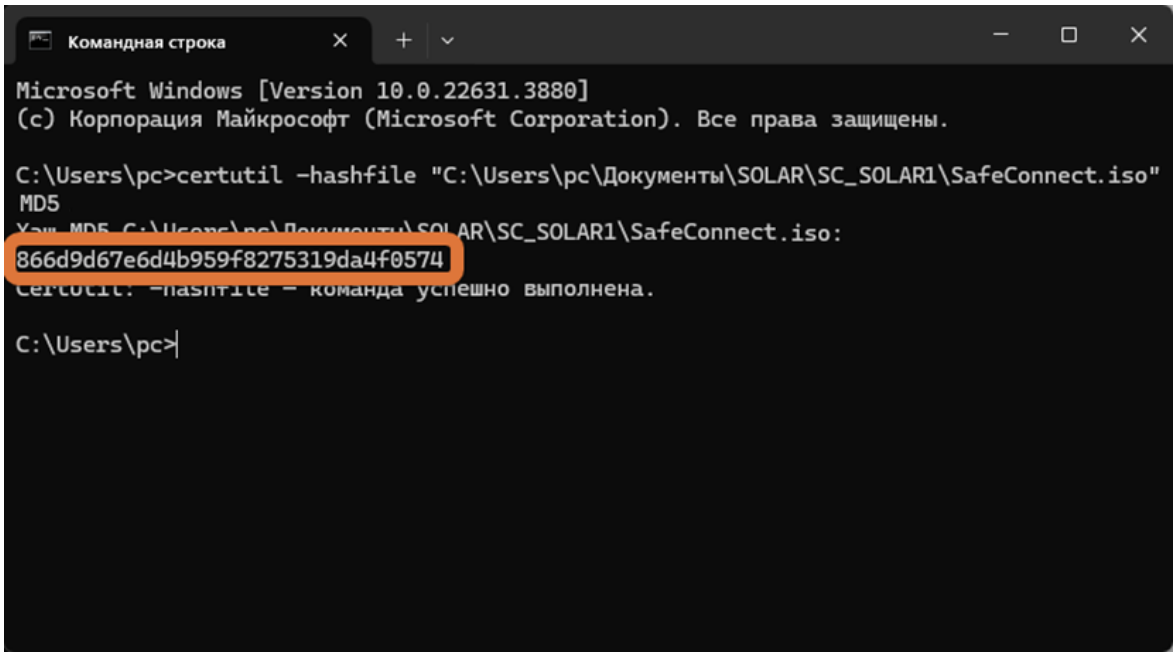


Рис. 4.4. Полученный результат

7. Сверить полученный результат с контрольными суммами дистрибутива, обозначенными в Release Notes (Рис.4.5).

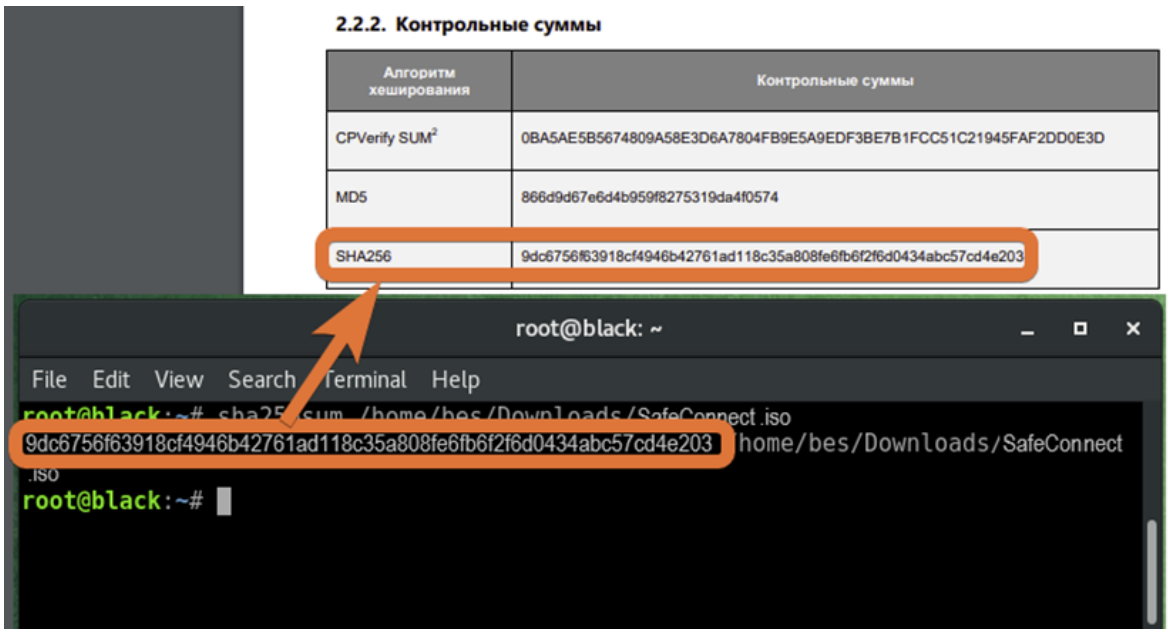


Рис. 4.5. Сверка полученного результата

В случае, если контрольные суммы файла совпадают с контрольными суммами дистрибутива, обозначенными в Release Notes, можно переходить к процессу инсталляции.

В противном случае, несовпадение означает, что целостность дистрибутива была нарушена, необходимо загрузить файл заново и проверить его контрольные суммы, или обратиться в службу сервиса для получения консультации.

4.1.2. Проверка КС дистрибутива утилитой cpverify

Проверка контрольных сумм CPVerify SUM может быть проведена при помощи утилиты cpverify.exe, входящей в состав СКЗИ КриптоПро CSP.

Ссылка для загрузки утилиты **cpverify.exe**:

http://www.cryptopro.ru/sites/default/files/public/cpverify.exe

Чтобы определить контрольные суммы дистрибутива, необходимо:

1. Загрузить образ диска на локальное хранилище;
2. При необходимости загрузить файл **cpverify.exe**;
3. Переместить файл **cpverify.exe** в ту же папку, что и образ диска;
4. Запустить командную строку (открыть меню Пуск, найти приложение **Командная строка** или **Cmd**, нажать **Открыть**) (**Рис.4.6**);

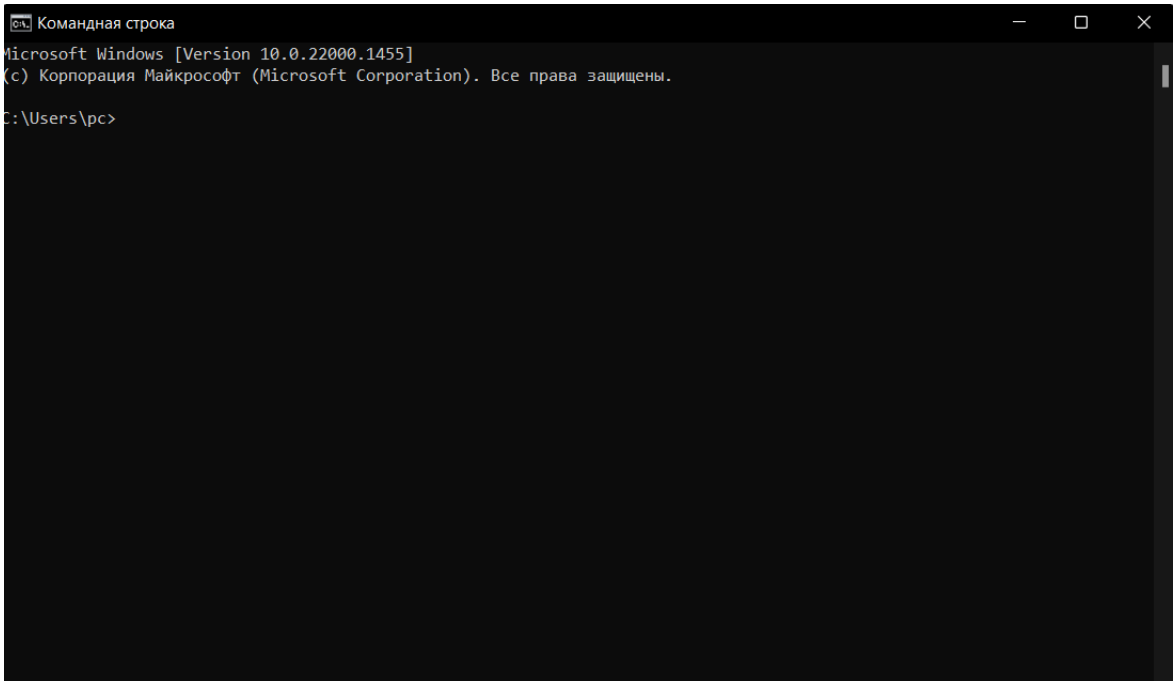


Рис. 4.6. Командная строка

5. В командной строке открыть папку с образом диска:
   `cd <путь_к_файлу>`

   например (**Рис.4.7**):
   `cd C:\Users\pc\SOLAR`

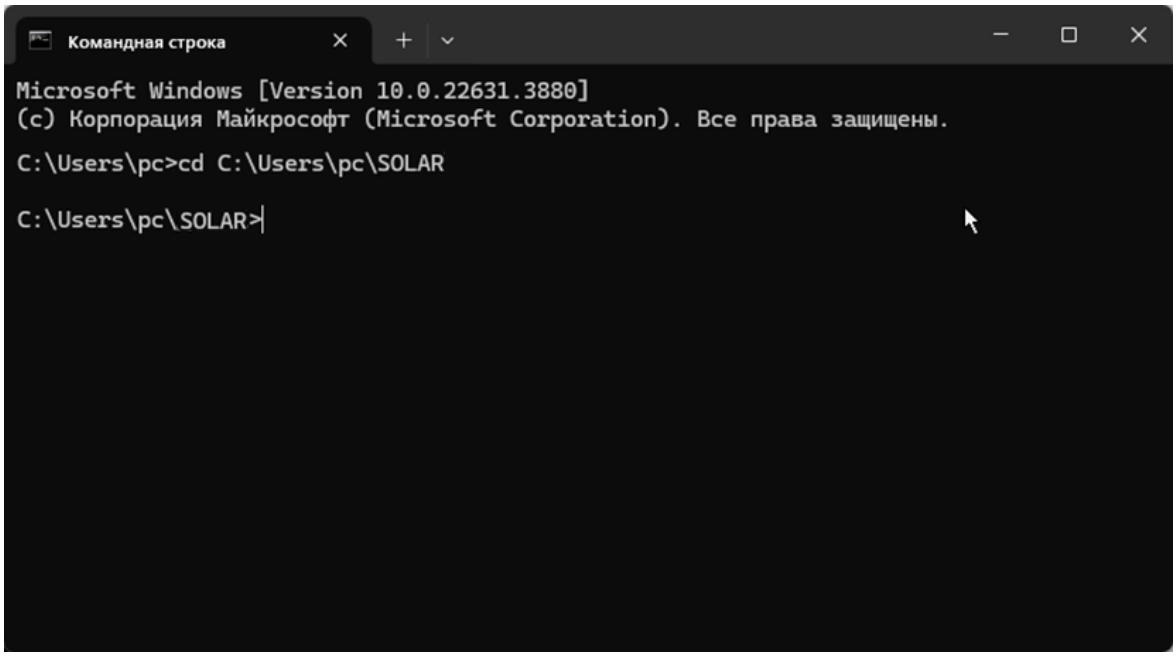


Рис. 4.7. Переход в папку с образом диска

6. В командной строке ввести:
   `cpverify -mk <имя_файла>.iso`

   например (Рис.4.8):
   `cpverify -mk SafeConnect.iso`

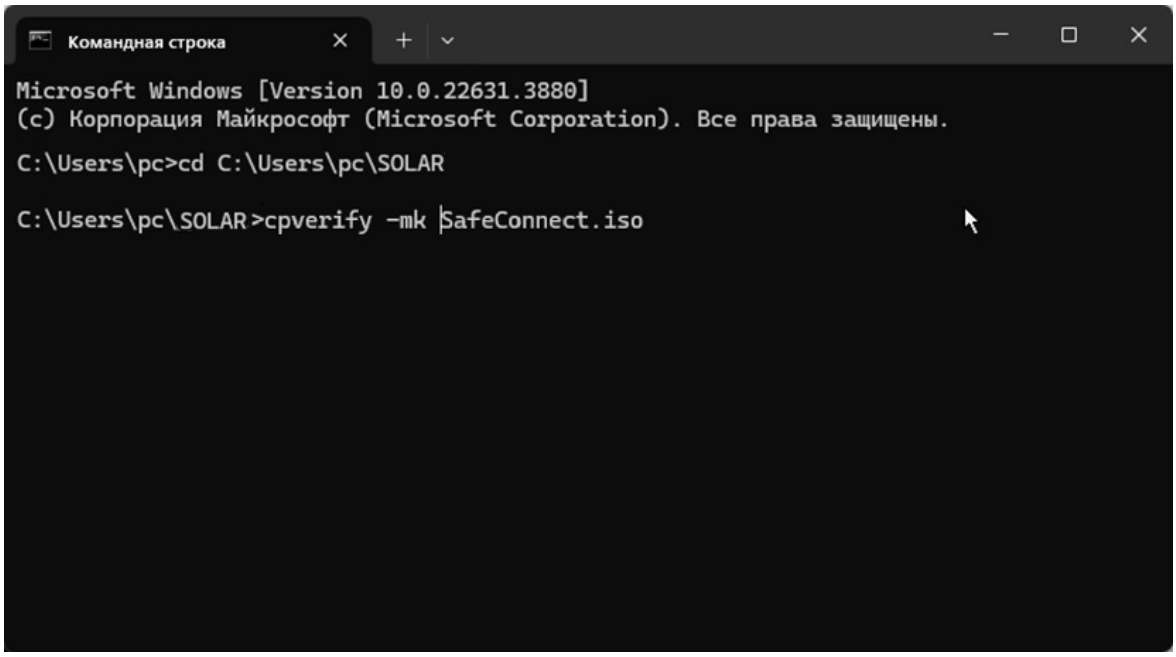


Рис. 4.8. Запуск cpverify

7. Нажать **Enter**;
8. Дождаться окончания выполнения команды (Рис.4.9).

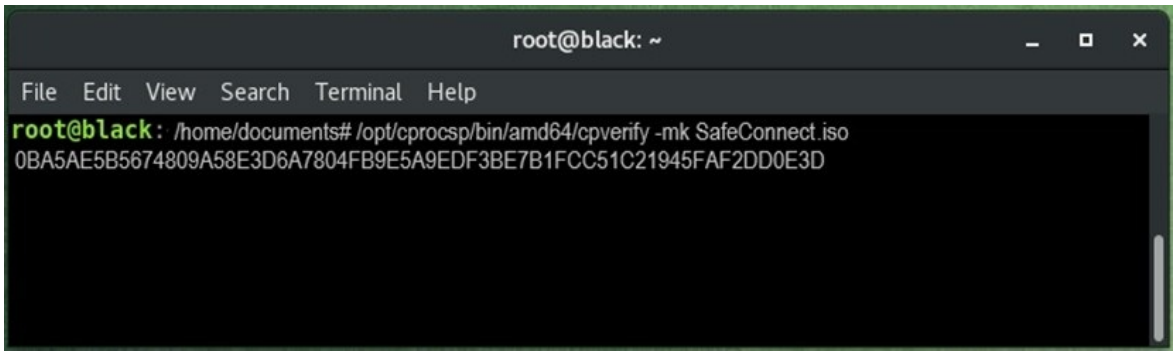


Рис. 4.9. Команда выполнена

9. Найти строку с полученным результатом (Рис.4.10):

   например:

   ```
   0BA5AE5B5674809A58E3D6A7804FB9E5A9EDF3BE7B1FCC51C21945FAF2DD0E3D
   ```

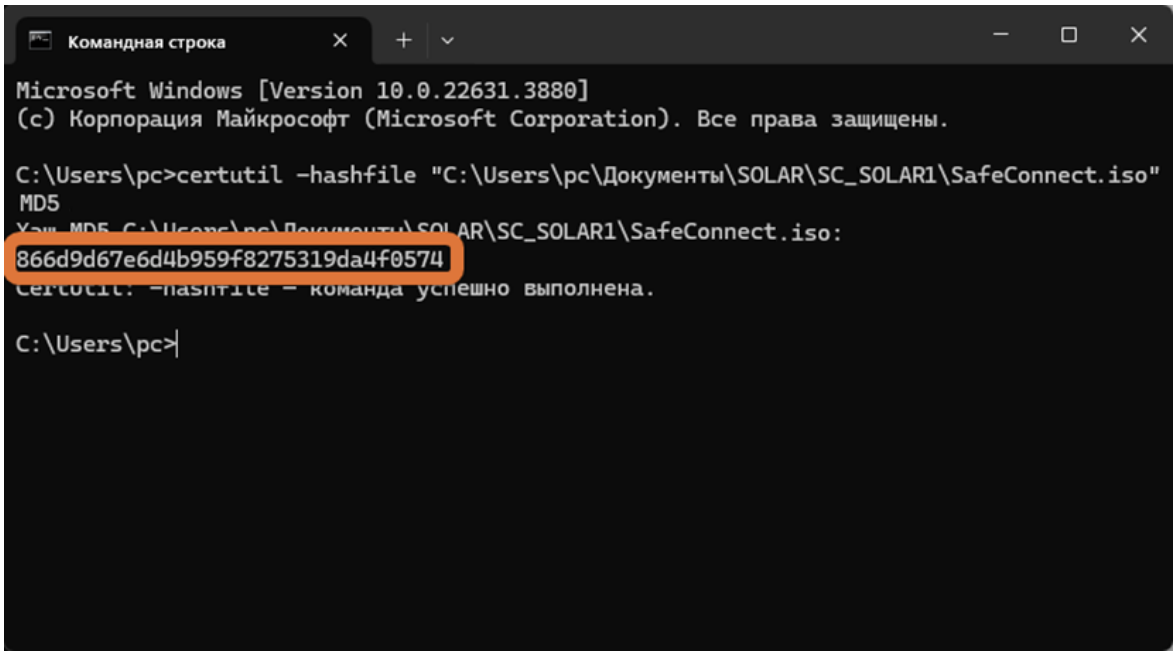


Рис. 4.10. Полученный результат

10. Сверить полученный результат с контрольными суммами дистрибутива, обозначенными в Release Notes (Рис.4.11).

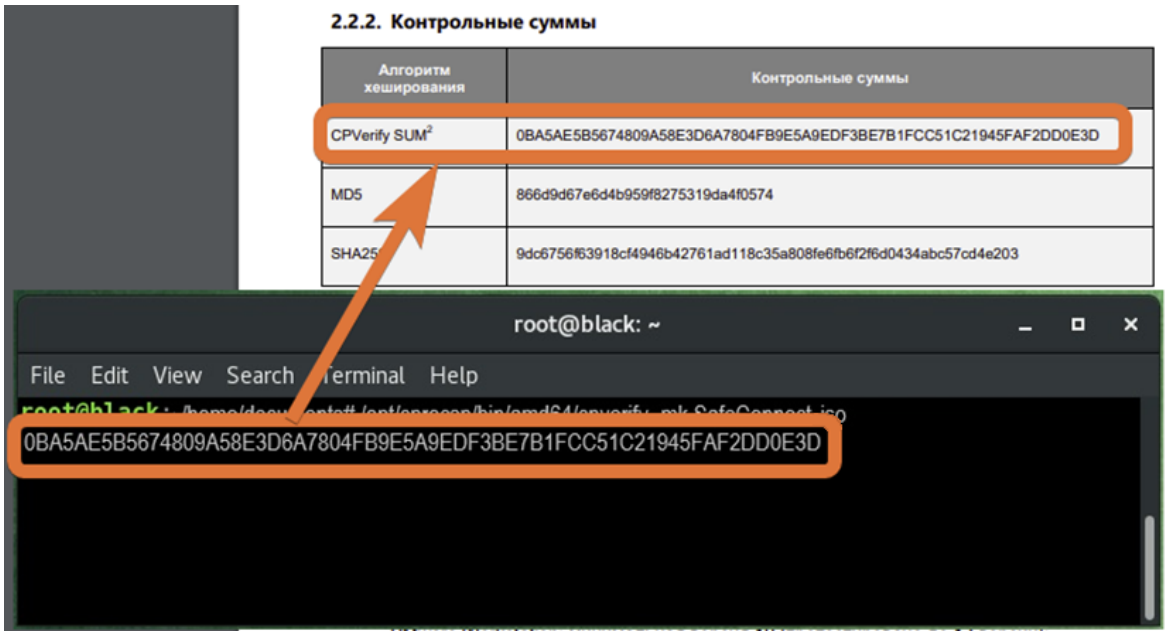


Рис. 4.11. Сверка полученного результата

В случае, если контрольные суммы файла совпадают с контрольными суммами дистрибутива, обозначенными в Release Notes, можно переходить к процессу инсталляции.

В противном случае, несовпадение означает, что целостность дистрибутива была нарушена, необходимо загрузить файл заново и проверить его контрольные суммы, или обратиться в службу сервиса для получения консультации.

4.2. Проверка контрольных сумм дистрибутива при использовании ОС Linux

4.2.1. Проверка КС дистрибутива утилитами md5sum и sha256sum

Для определения целостности дистрибутива при использовании ОС Linux рекомендуется использовать утилиты **md5sum** и **sha256sum**. Эта утилиты входит в состав разных ОС Linux.

Чтобы определить контрольные суммы дистрибутива необходимо:

1. Загрузить образ диска на локальное хранилище;
2. Запустить эмулятор терминала;
3. В эмуляторе терминала ввести следующие команды:
   - для получения контрольной суммы MD5:
     `md5sum <путь_к_файлу>\<имя_файла>.iso`

     например (Рис.4.12):
     `md5sum /home/bes/Downloads/SafeConnect.iso`

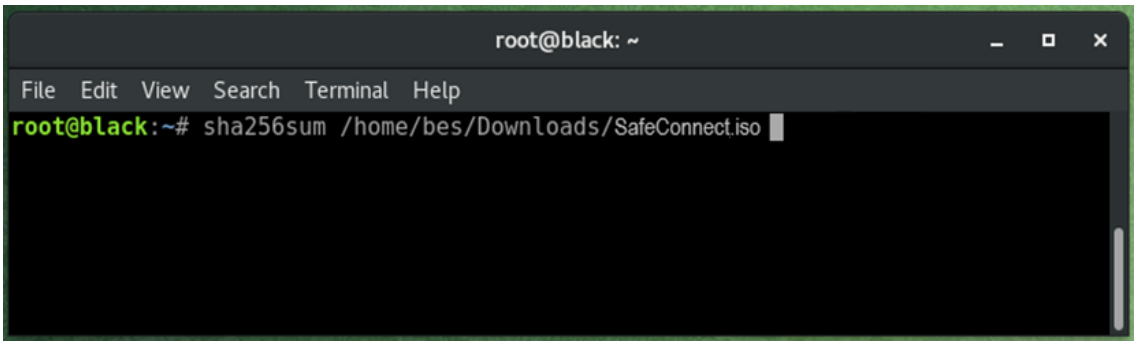


Рис. 4.12. Пример ввода команды

- для получения контрольной суммы SHA256:
  `sha256sum <путь_к_файлу>\<имя_файла>.iso`

  например (Рис.4.13):
  `sha256sum /home/bes/Downloads/SafeConnect.iso`

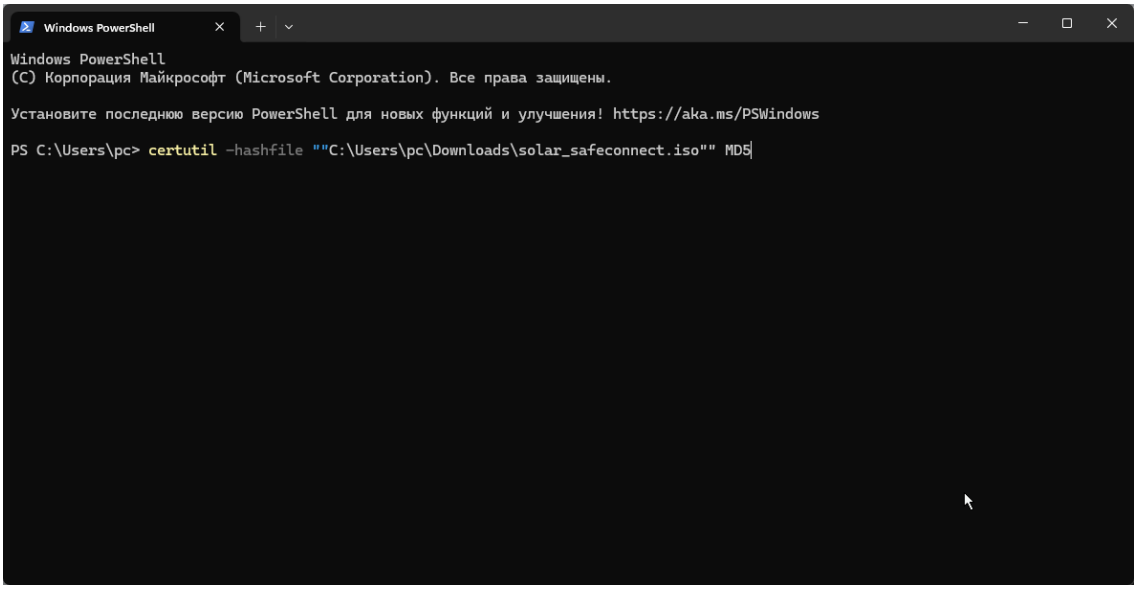


Рис. 4.13. Пример ввода команды

4. Нажать **Enter**;
5. Дождаться окончания выполнения команды;
6. Найти строку с полученным результатом:

   Например (Рис.4.14, Рис.4.14):
   `866d9d67e6d4b959f8275319da4f0574/home/bes/Downloads/SafeConnect.iso`
   `9dc6756f63918cf4946b42761ad118c35a808fe6fb6f2f6d0434abc57cd4e203/home/bes/Downloads/SafeConnect.iso`

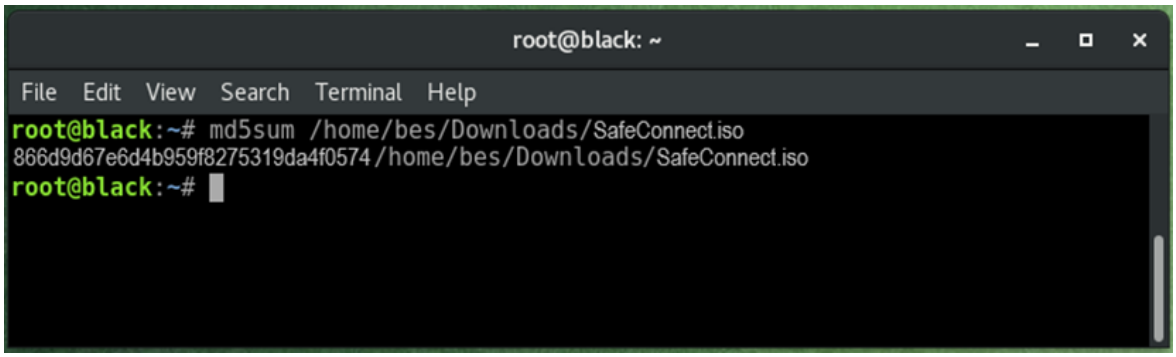


Рис. 4.14. Результат с MD5

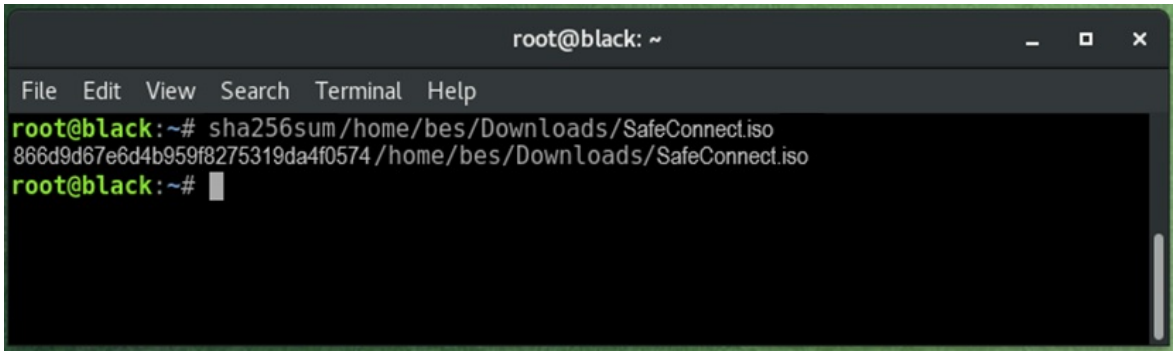


Рис. 4.15. Результат с SHA256

7. Сверить полученный результат с контрольными суммами дистрибутива, обозначенными в Release Notes (Рис.4.16).

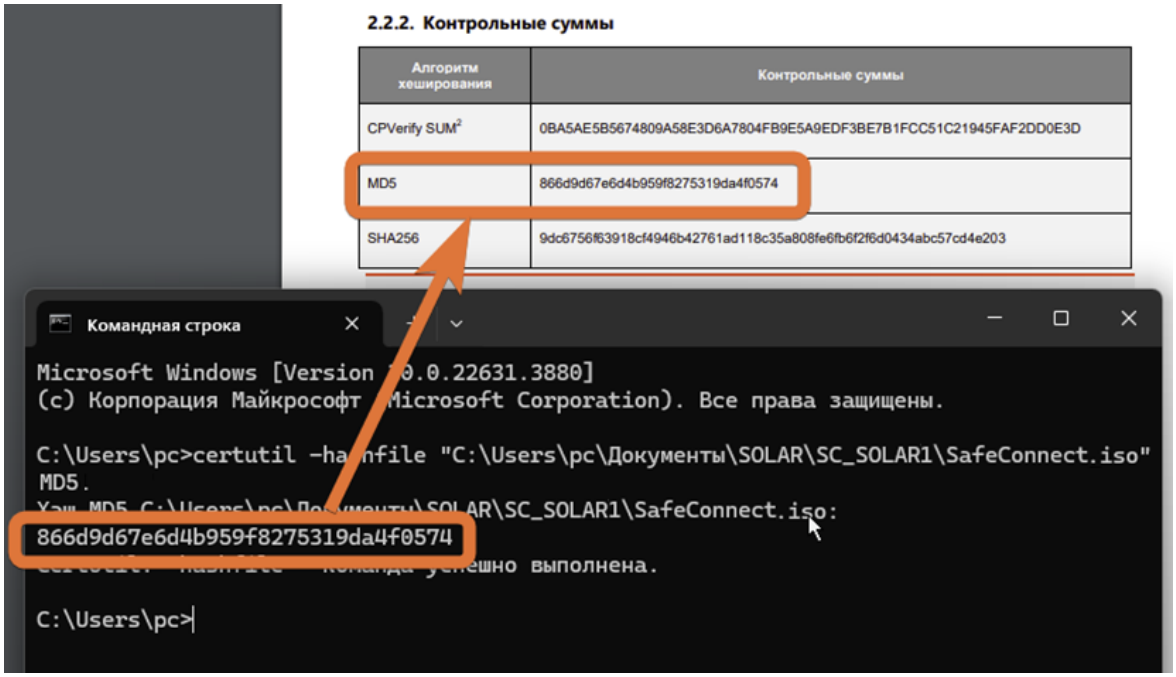


Рис. 4.16. Сверка полученного результата

В случае, если контрольные суммы файла совпадают с контрольными суммами дистрибутива, обозначенными в Release Notes, можно переходить к процессу инсталляции.

В противном случае, несовпадение означает, что целостность дистрибутива была нарушена, необходимо загрузить файл заново и проверить его контрольные суммы, или обратиться в службу сервиса для получения консультации.

4.2.2. Проверка КС дистрибутива утилитами cpverify

Проверка контрольных сумм CPVerify SUM может быть проведена при помощи утилиты **cpverify**, входящей в состав СКЗИ КриптоПро CSP.

Ссылка для загрузки утилиты **cpverify.exe**:

http://www.cryptopro.ru/sites/default/files/public/cpverify.exe

Чтобы определить контрольные суммы дистрибутива необходимо:

1. Установить **КриптоПро CSP**;
2. Загрузить образ диска на локальное хранилище;
3. Запустить терминал;
4. Перейти в папку с образом диска;
5. Ввести команду:
   `/opt/cprocsp/bin/amd64/cpverify -mk <путь к файлу>`

   например:
   `/opt/cprocsp/bin/amd64/cpverify -mk SafeConnect.iso`
6. Нажать **Enter**;
7. Дождаться окончания выполнения команды (**Рис.4.17**);

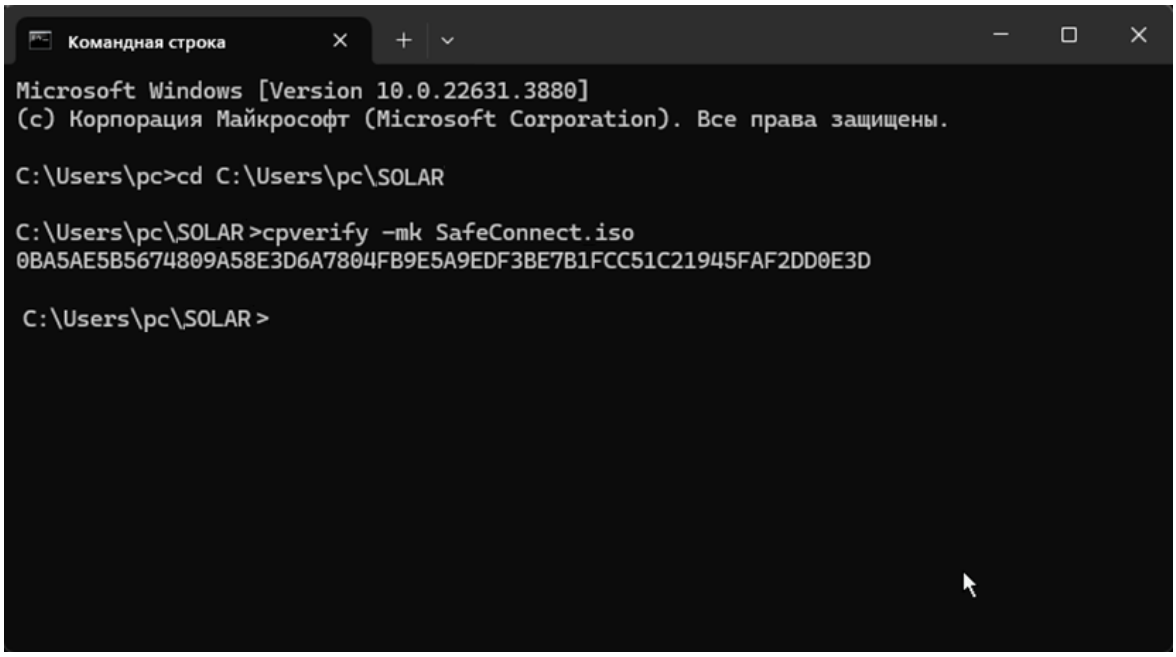


Рис. 4.17. Команда выполнена

8. Проверить полученный результат, например:

```
0BA5AE5B5674809A58E3D6A7804FB9E5A9EDF3BE7B1FCC51C21945FAF2DD0E3D
```

9. Сверить полученный результат с контрольными суммами дистрибутива, обозначенными в Release Notes (Рис.4.18).

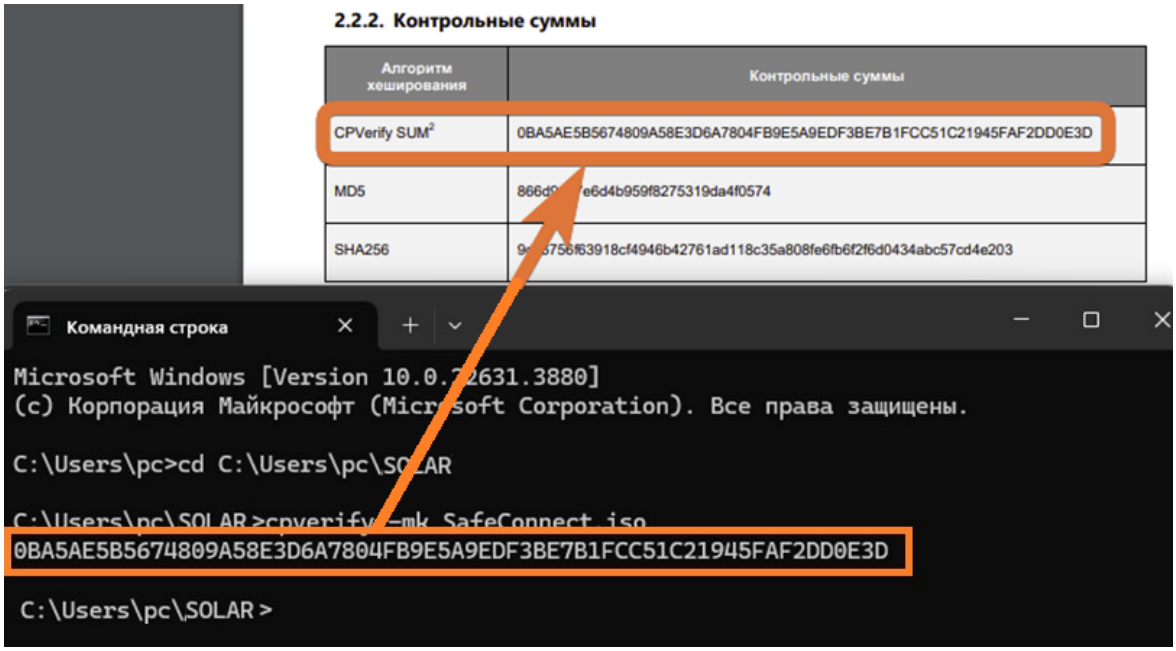


Рис. 4.18. Сверка полученного результата

В случае, если контрольные суммы файла совпадают с контрольными суммами дистрибутива, обозначенными в Release Notes, можно переходить к процессу инсталляции.

В противном случае, несовпадение означает, что целостность дистрибутива была нарушена, необходимо загрузить файл заново и проверить его контрольные суммы, или обратиться в службу сервиса для получения консультации.

4.2.3. Проверка КС дистрибутива утилитами gostsum

Для расчета контрольных сумм с помощью системной утилиты **gostsum** необходимо выполнить следующие действия:

1. Выполнить консольную команду:
   ```
   gostsum -H %file_name%
   ```

   где file_name - файл с именами файлов (каталогов) для расчета КС.

В результате выполнения на экран будет выведено значение КС, вычисленной по алгоритму ГОСТ Р 34.11-2012 для файла **file_name** (пример):

```
cffddad20f64bb9460691f981cf1de0d74d3573400ffb05de6beb89a2050cc10 file_name
```

Контрольные суммы, полученные в результате расчета с помощью системной утилиты **gostsum**, сверяются с контрольными суммами, указанными в Release Notes.

5. Установка программы

Дистрибутив SafeConnect поставляется в виде ISO-образа:

- для операционной системы Astra Linux 1.7.7.9 с версией ядра 6.1.124-1-generic.

Инсталляция представляет собой установку этого образа на пустой компьютер или на виртуальную машину. Для установки также требуется свободный IP-адрес в сети.

Процесс установки занимает некоторое время и требует от оператора стандартных ответов на вопросы инсталлятора.

5.1. Установка и настройка ОС Astra Linux

На виртуальную машину должна быть установлена ОС Astra Linux 1.7.7.9 с версией ядра 6.1.124-1-generic.

Внимание!

Для предотвращения конфликтов важно разворачивать виртуальные машины не посредством клонирования, а создавая каждую с уникальным секретом. Это гарантирует отсутствие дублирования критически важных идентификаторов!

5.1.1. Установка ОС Astra Linux 1.7.7

Для установки ОС Astra Linux 1.7.7 запустите сервер с использованием установочного диска или USB-носителя «Astra Linux 1.7.7» и выполните следующие действия:

1. В окне приветствия оставьте выбор параметров программы установки по умолчанию (Графическая установка, Русский) и нажмите **Enter**.

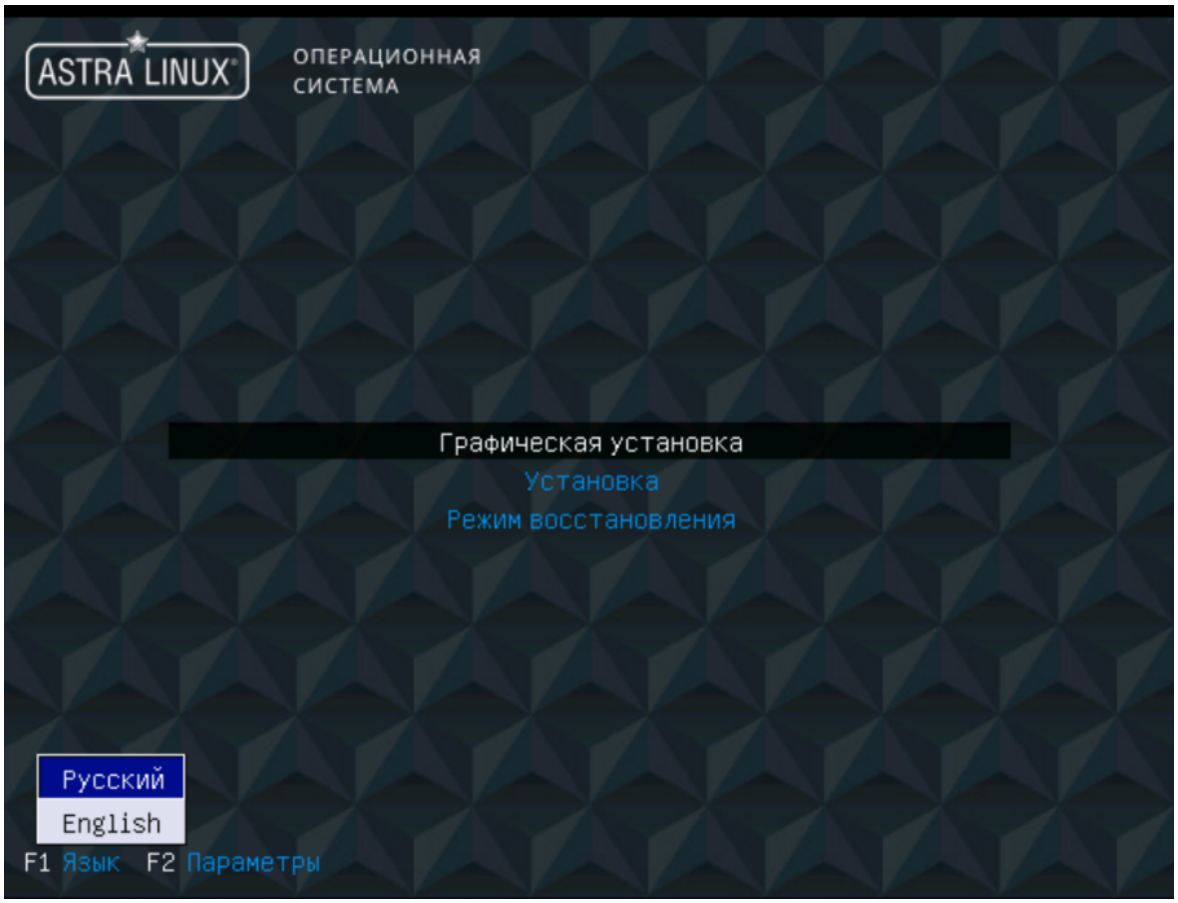


Рис. 5.1. Окно приветствия

2. В окне **Лицензия** нажмите **Продолжить**.

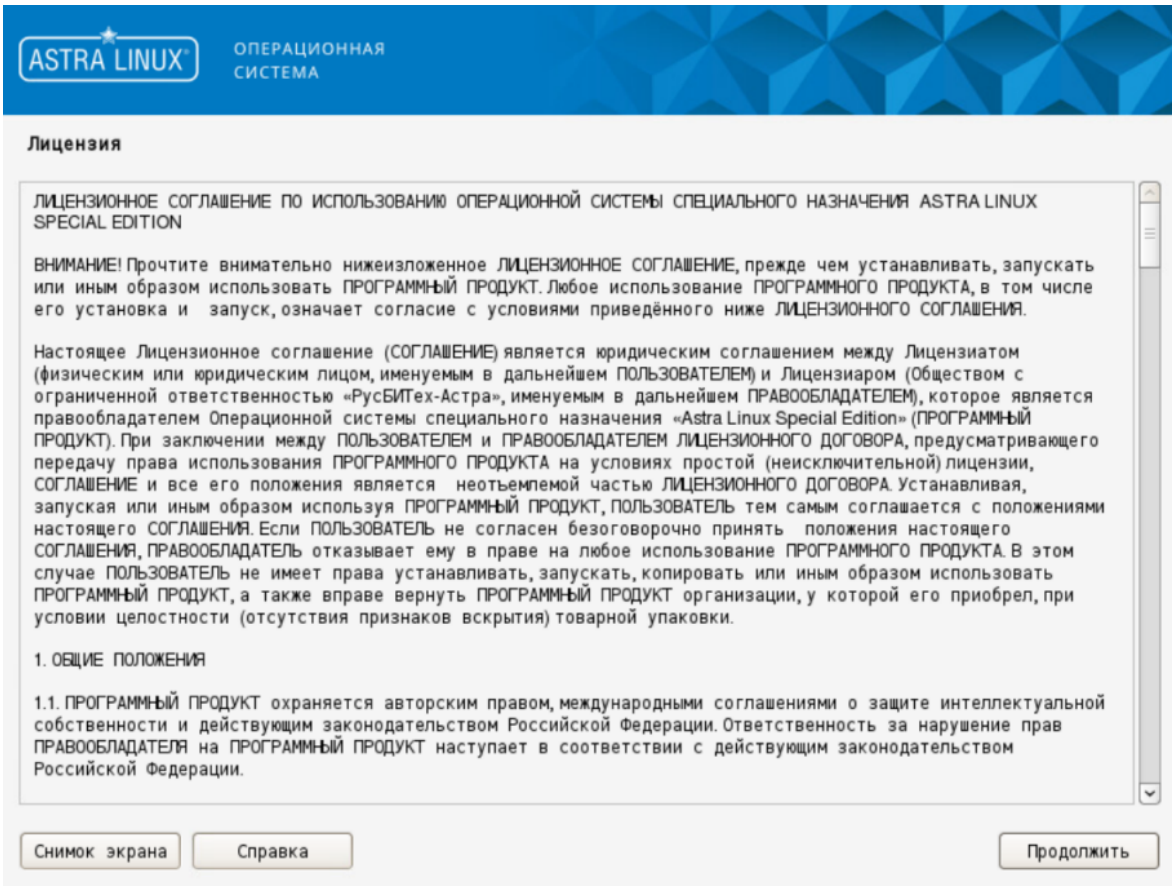


Рис. 5.2. Окно Лицензия

3. В окне **Настройка клавиатуры** выберите удобный способ переключения раскладки ввода с клавиатуры и нажмите **Продолжить**.

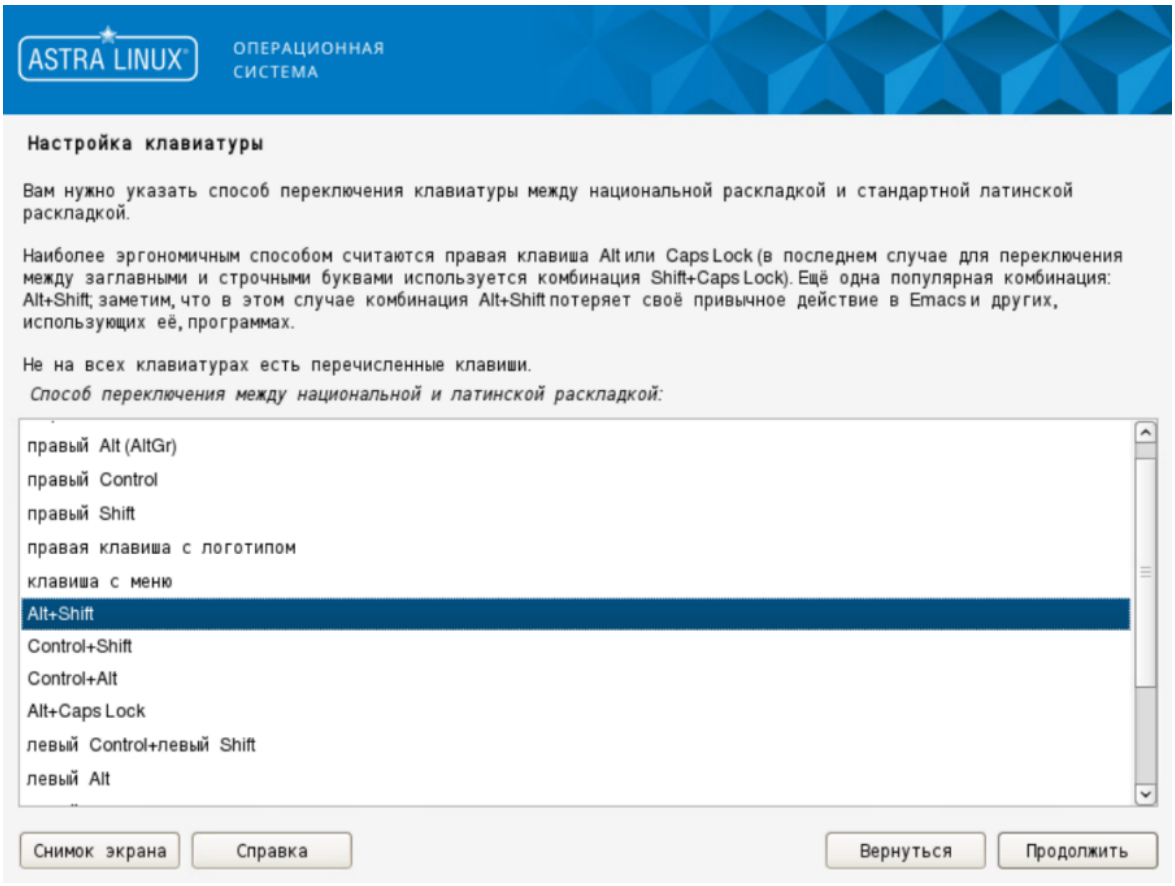


Рис. 5.3. Настройка клавиатуры

4. Дождитесь загрузки компонентов программы установки.

5. При необходимости используйте ручную настройку сети.

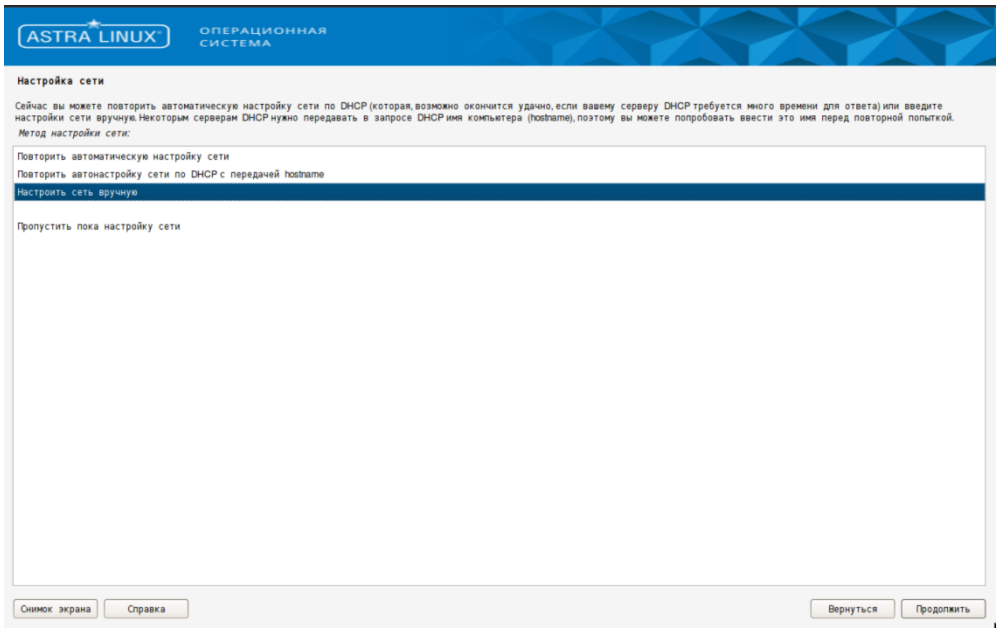


Рис. 5.4. Настройка сети

6. Введите IP–адрес (уточните сетевые настройки у вашего системного администратора).

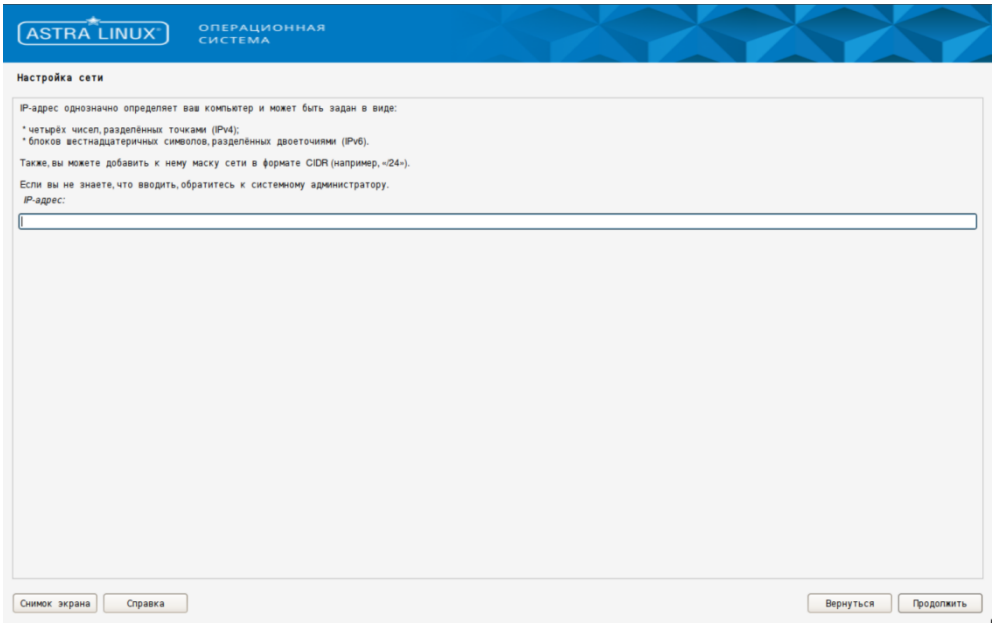


Рис. 5.5. Настройка сети

7. Укажите маску подсети.

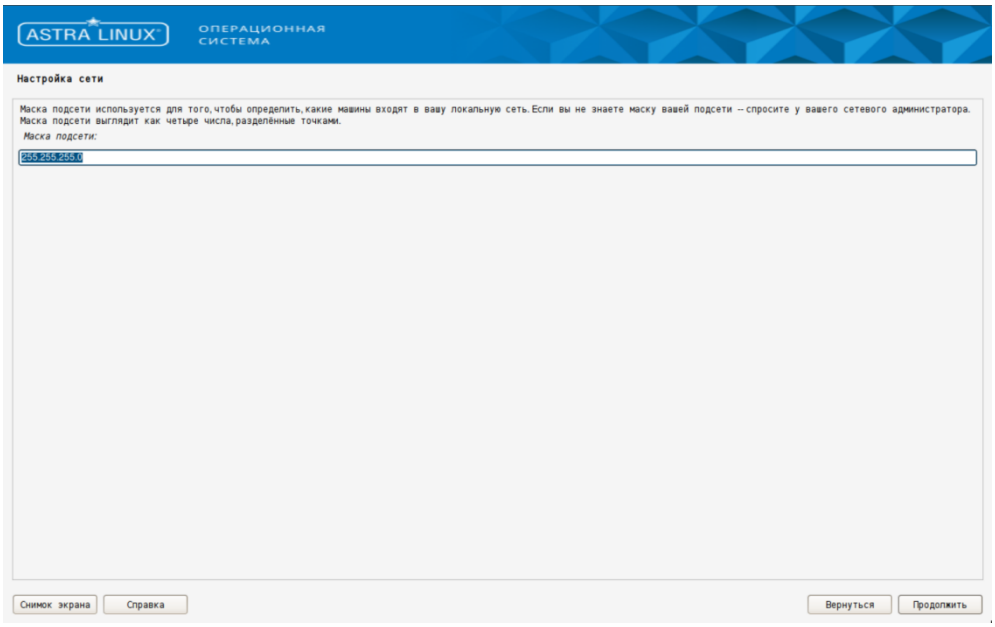


Рис. 5.6. Настройка сети

8. Введите шлюз.

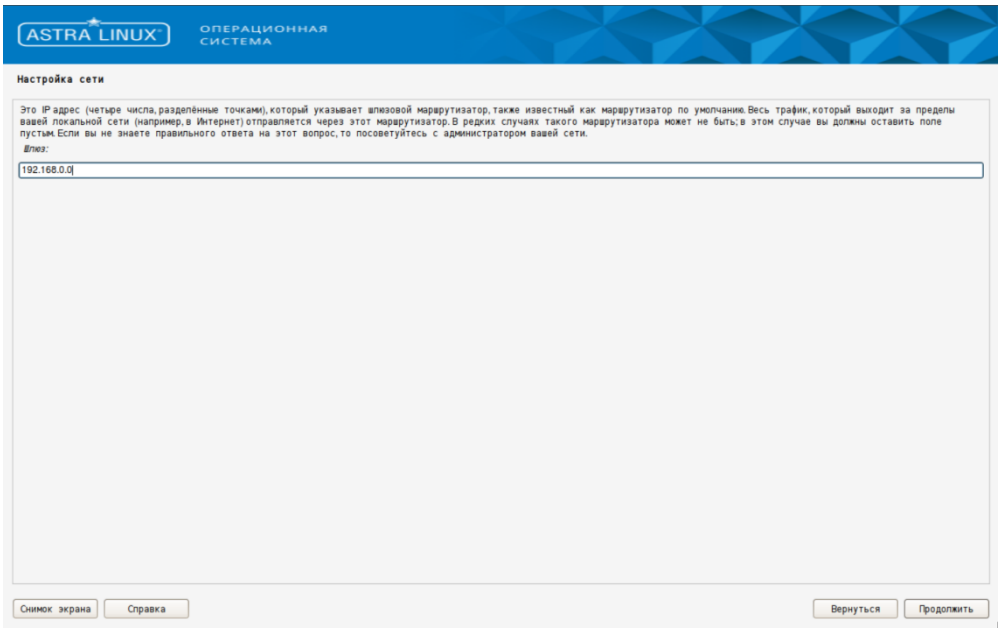


Рис. 5.7. Настройка сети

9. Укажите адреса DNS–серверов.

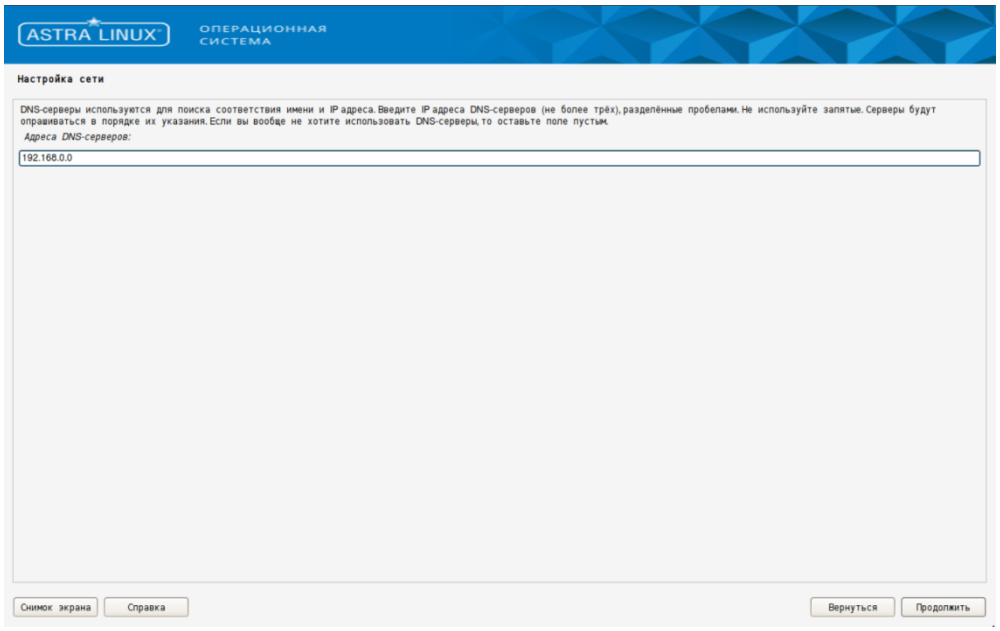


Рис. 5.8. Настройка сети

10. Укажите краткое сетевое имя сервера (после установки SafeConnect имя сервера поменяется).

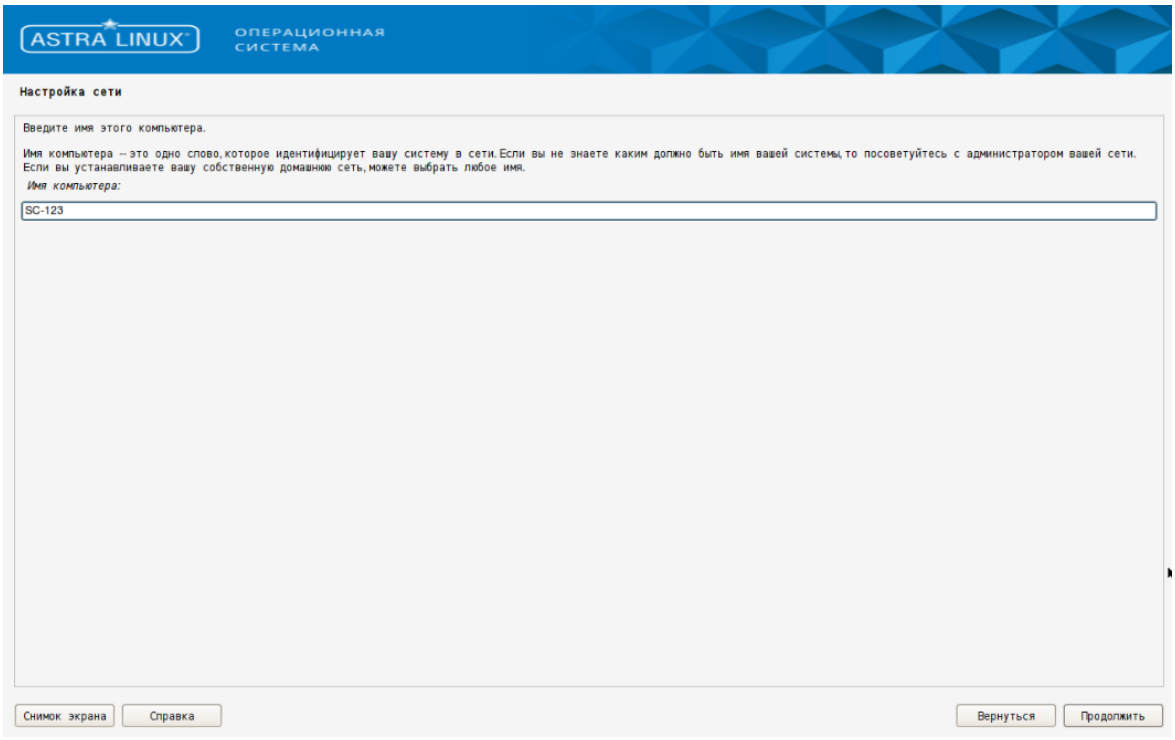


Рис. 5.9. Настройка сети

11. В окне **Настройка учётных записей пользователей и паролей** в поле **Имя учётной записи администратора** укажите произвольное имя и нажмите **Продолжить**.

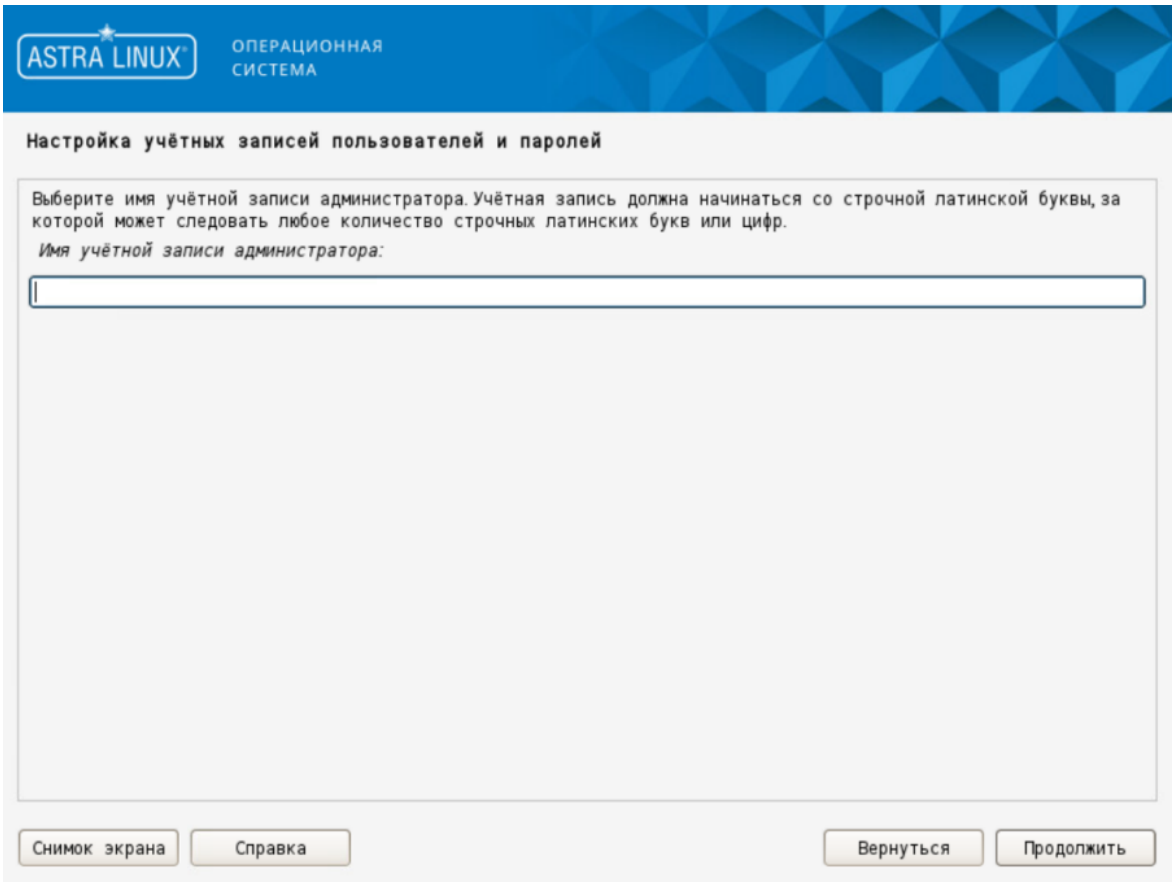


Рис. 5.10. Окно Настройка учётных записей

12. В появившемся окне задайте пароль для созданной учетной записи и подтвердите его. Нажмите **Продолжить**.

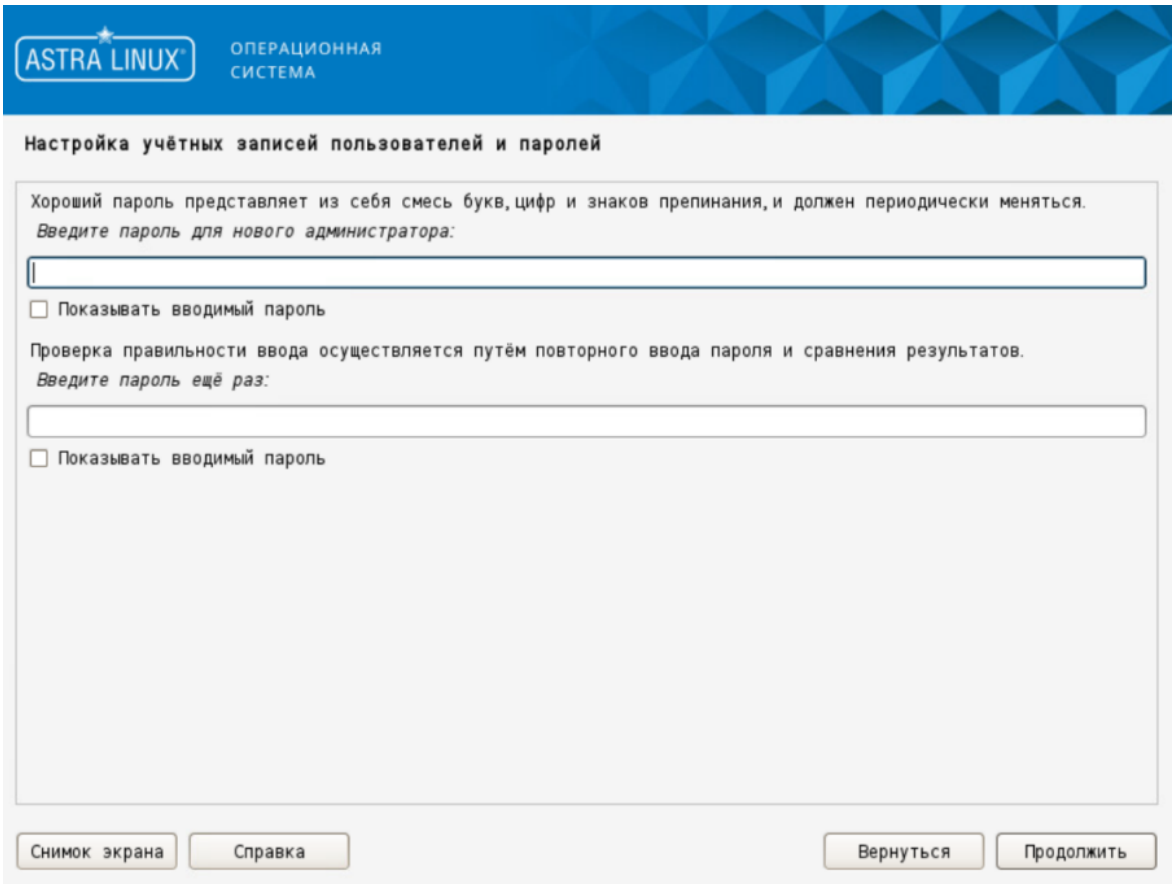


Рис. 5.11. Создание пароля для учетной записи администратора

13. В окне **Настройка времени** задайте требуемый часовой пояс и нажмите **Продолжить**.

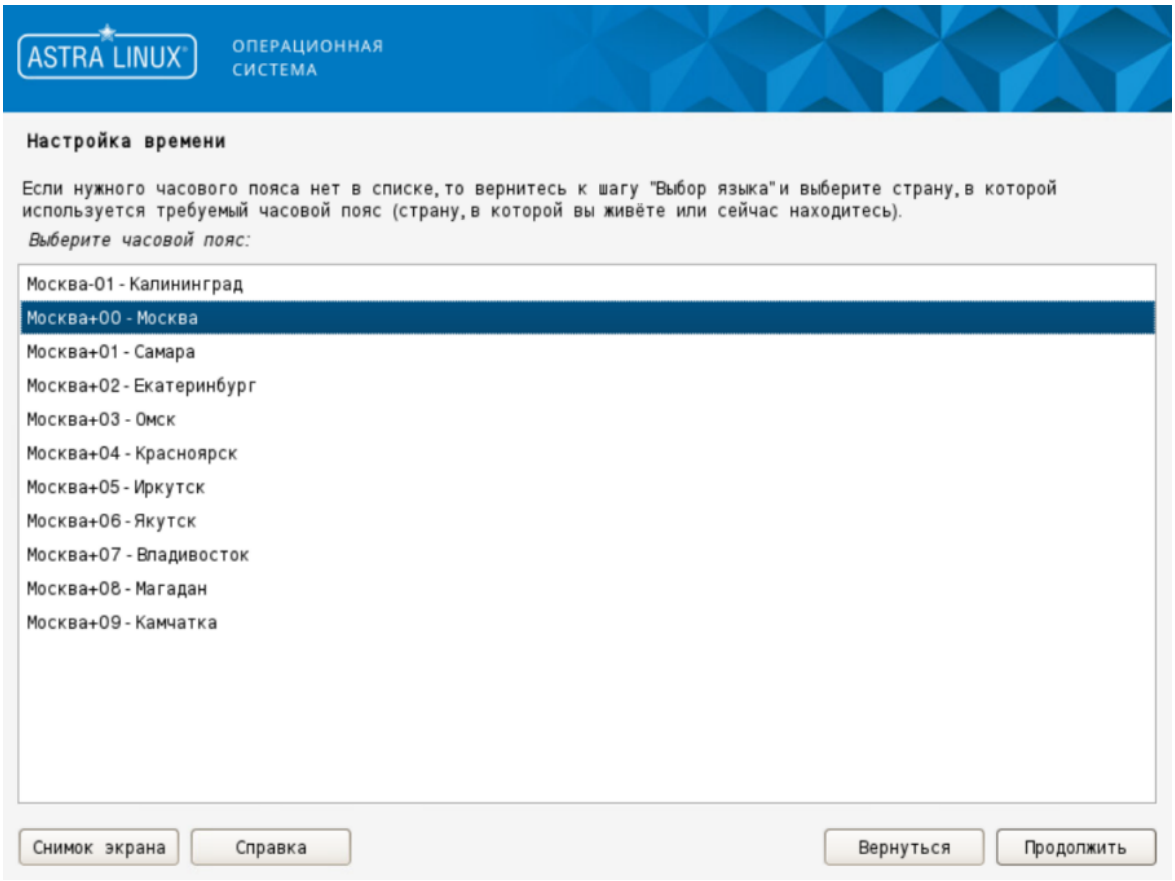


Рис. 5.12. Окно настройки времени

14. В появившемся окне **Разметка дисков** выберите метод разметки, установленный по умолчанию (Авто – использовать весь диск), и нажмите **Продолжить**.

Внимание!

При выборе методов разметки «Авто» все данные на диске будут потеряны.

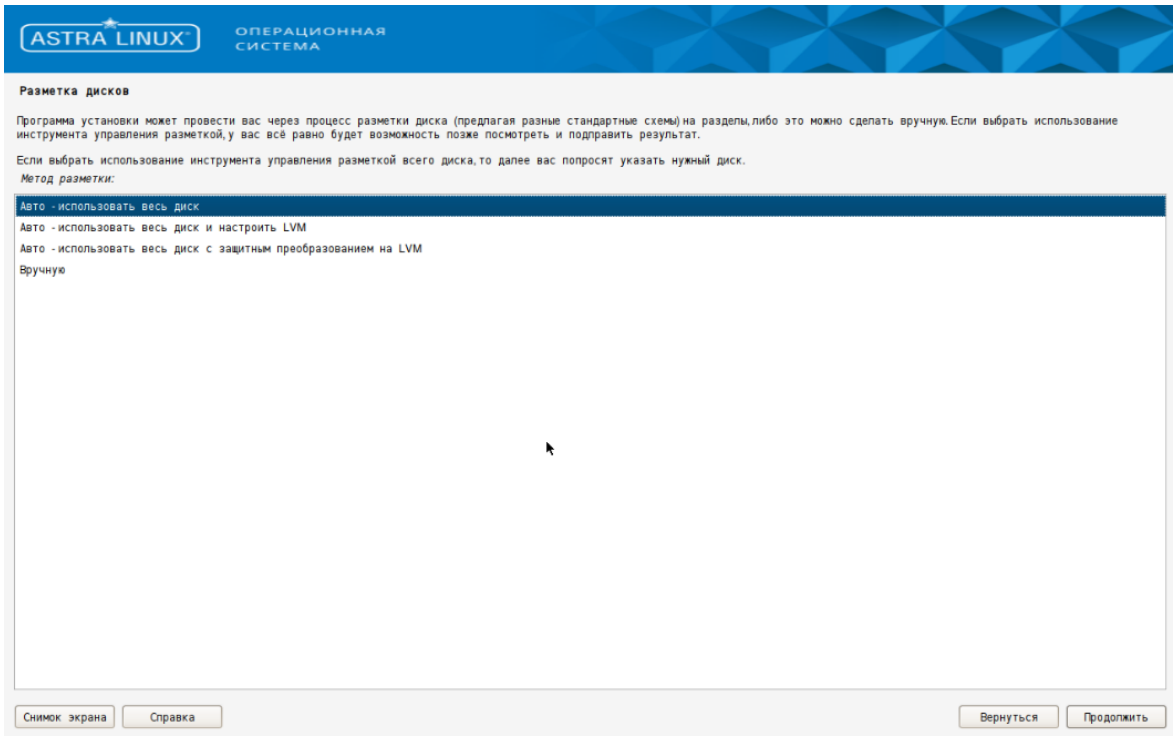


Рис. 5.13. Окно Разметка дисков

15. В появившемся окне выберите диск для установки, например, как показано ниже. Нажмите **Продолжить**.

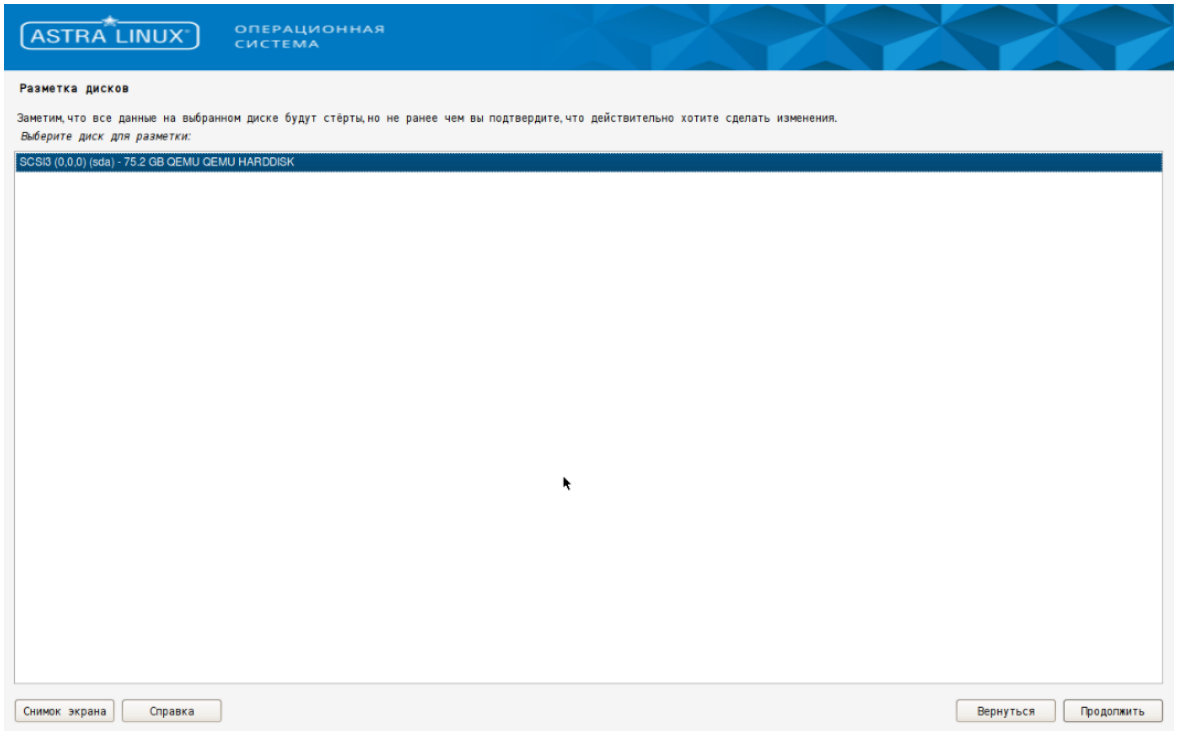


Рис. 5.14. Выбор диска для установки

16. В появившемся окне с выбором схемы разметки выберите вариант **Все файлы в одном разделе** и нажмите **Продолжить**.

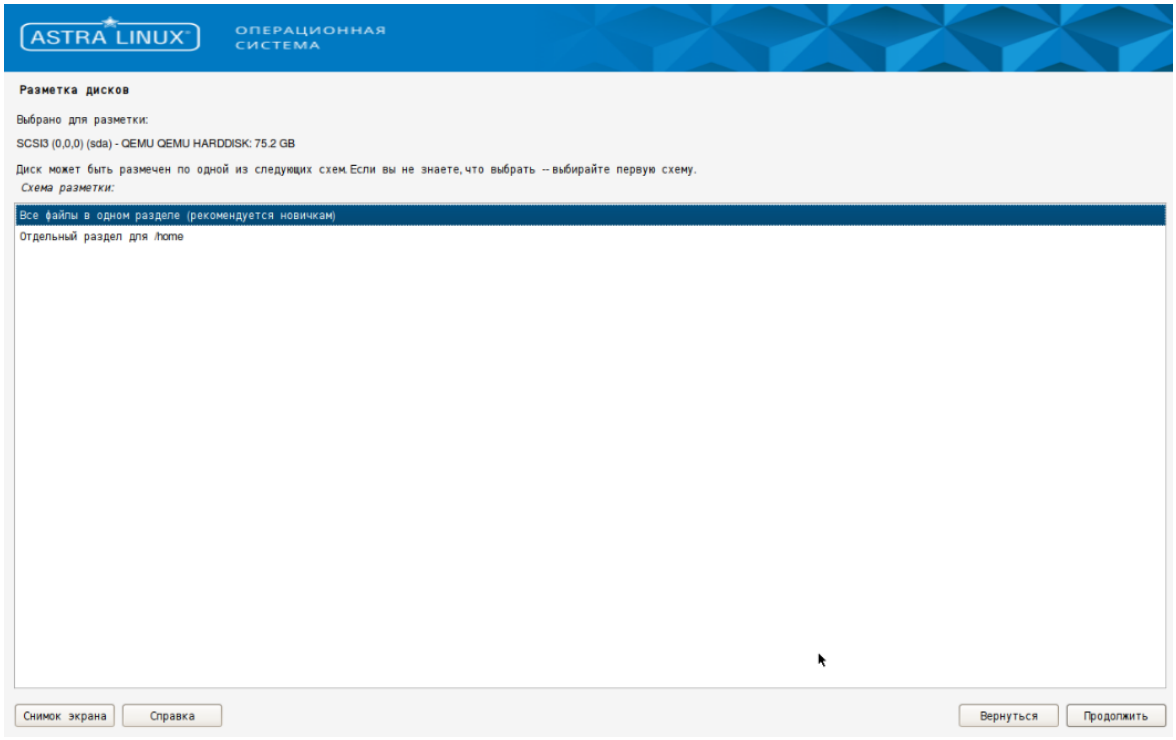


Рис. 5.15. Выбор схемы разметки

17. В следующем окне будет показан список настроенных разделов и точек монтирования. Выберите необходимый раздел, если требуется изменить его настройки. После настройки конфигурации выберите **Закончить разметку и записать изменения на диск** и нажмите **Продолжить**.

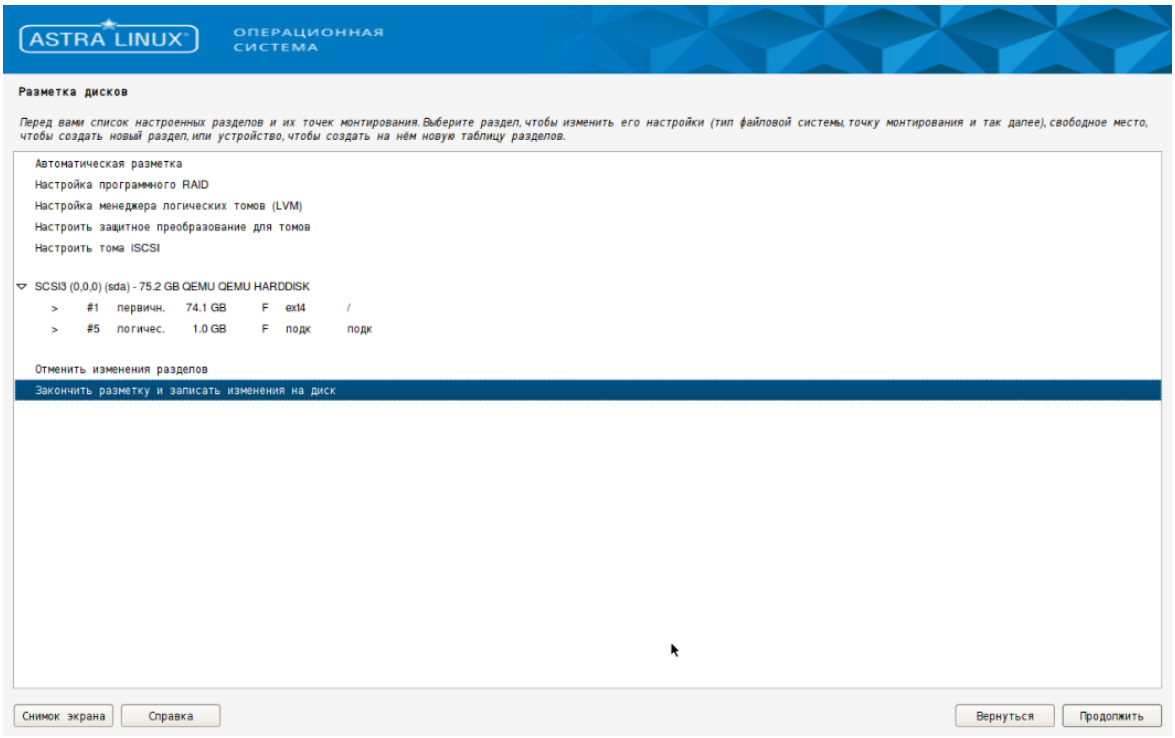


Рис. 5.16. Настройка разделов

18. В появившемся окне будет отображена информация о разметке дисков. Убедитесь, что эта информация верна, выберите **Да** и нажмите **Продолжить**.



Рис. 5.17. Информация о разметке дисков

19. Дождитесь установки базовой системы. В появившемся окне **Установка базовой системы** выберите последнюю версию ядра.

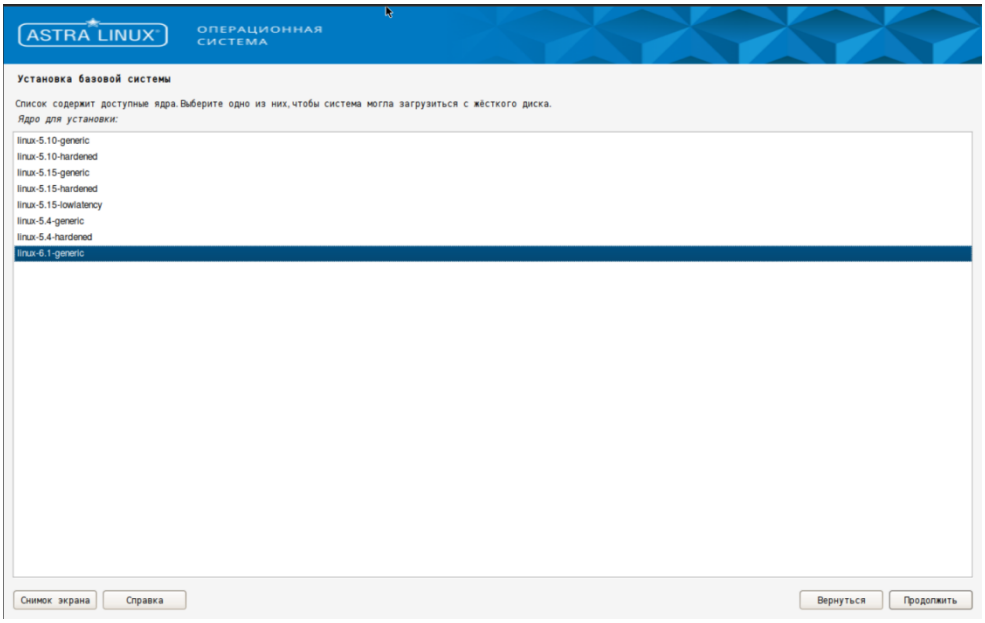


Рис. 5.18. Выбор ядра

20. После окончания установки в появившемся окне **Выбор программного обеспечения** выберите варианты **Консольные утилиты** и **Средства удаленного доступа SSH**. Нажмите **Продолжить**.

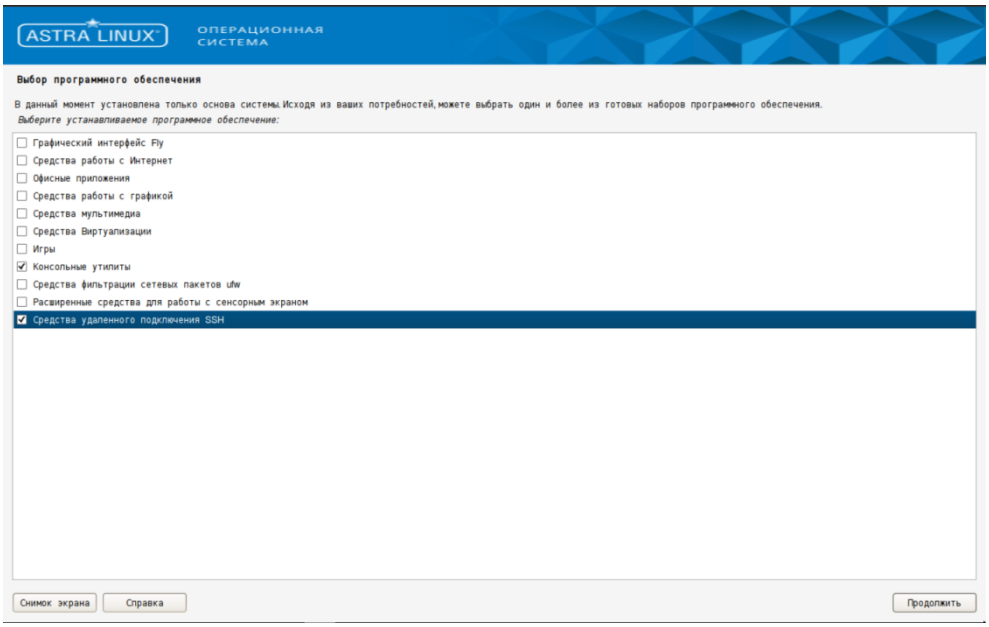


Рис. 5.19. Выбор программного обеспечения

21. В появившемся окне **Дополнительные настройки ОС** выберите **Усиленный уровень защищенности "Воронеж"**, если позволяет лицензия. Нажмите **Продолжить**.

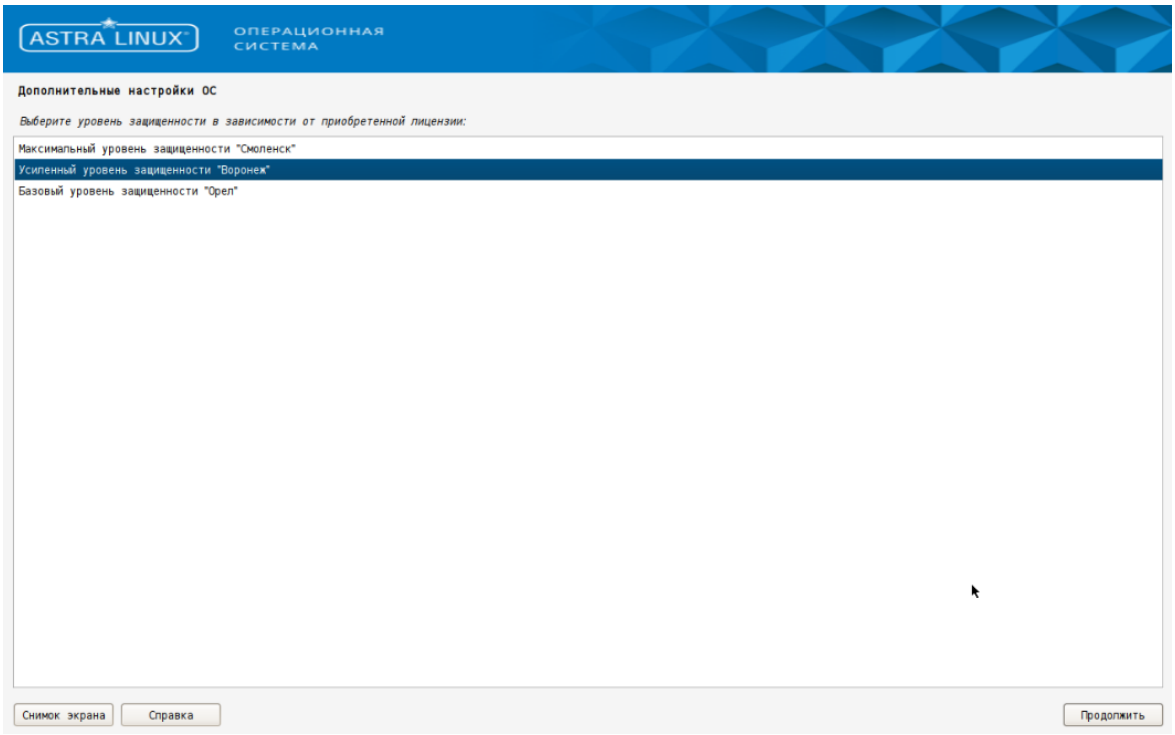


Рис. 5.20. Выбор уровня защищенности

22. В следующем окне оставьте все установленные по умолчанию флажки (при выборе уровня защищённости флажки выставляются автоматически в соответствии с уровнем) и нажмите **Продолжить**.

23. В появившемся окне **Установка системного загрузчика GRUB на жесткий диск** нажмите **Продолжить**.

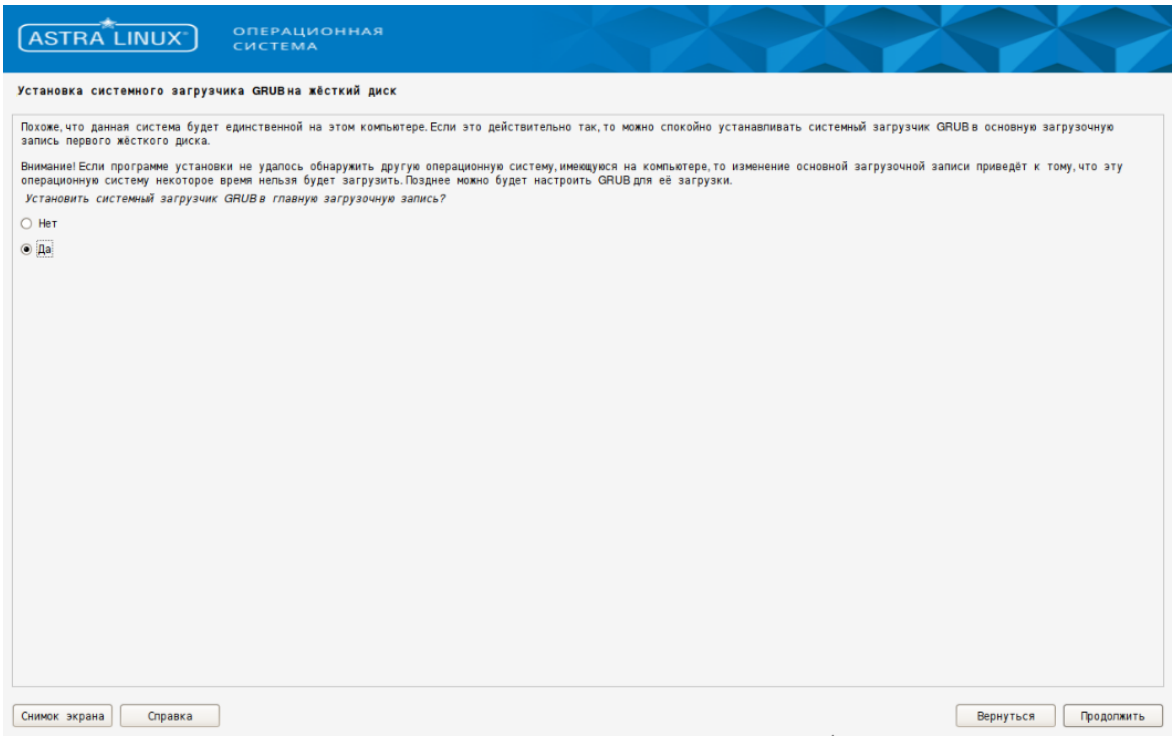


Рис. 5.21. Рис.5.23. Установка системного загрузчика GRUB на жесткий диск

24. В появившемся окне задайте пароль для системного загрузчика GRUB. Нажмите **Продолжить**, повторите ввод пароля и нажмите **Продолжить**.

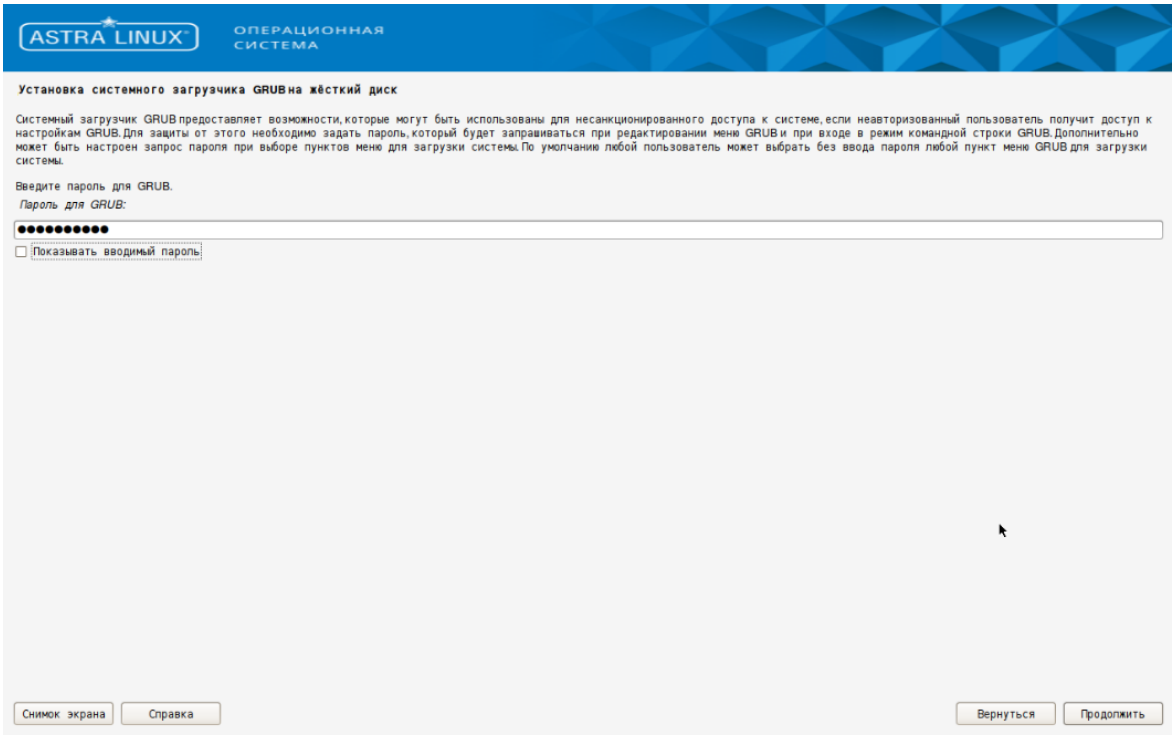


Рис. 5.22. Ввод пароля для GRUB

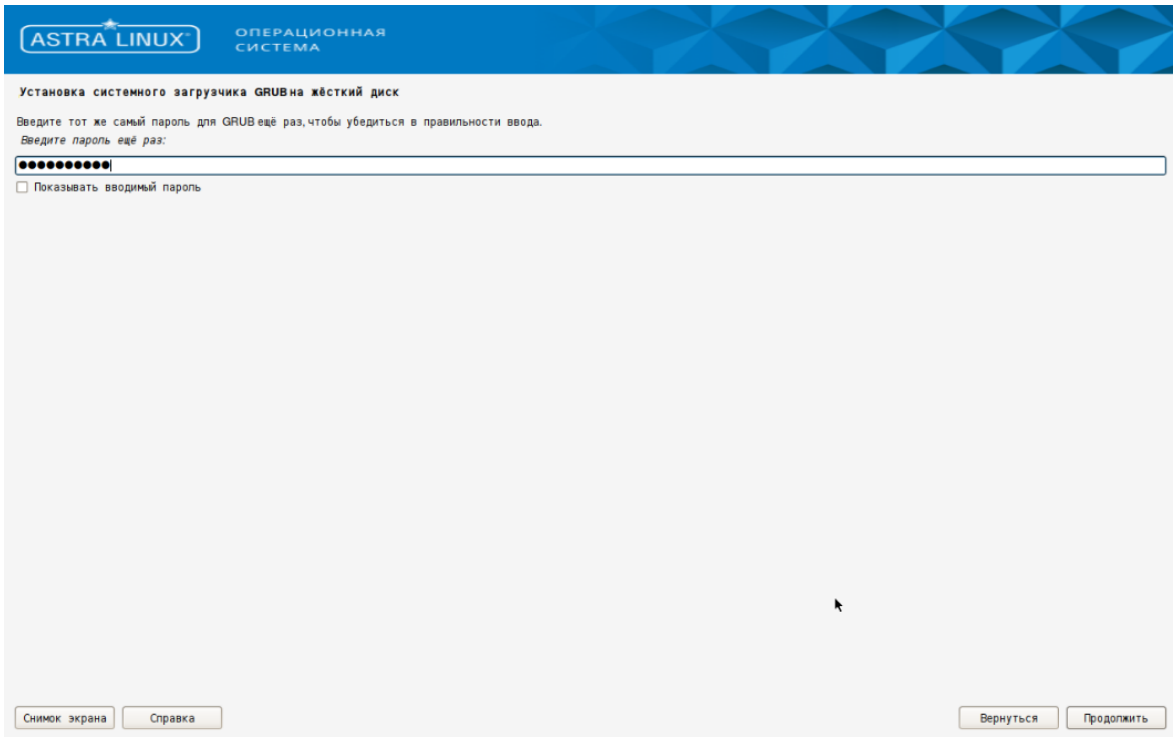


Рис. 5.23. Повторный ввод пароля для GRUB

25. После запроса системы отключите установочный носитель и нажмите **Продолжить**.

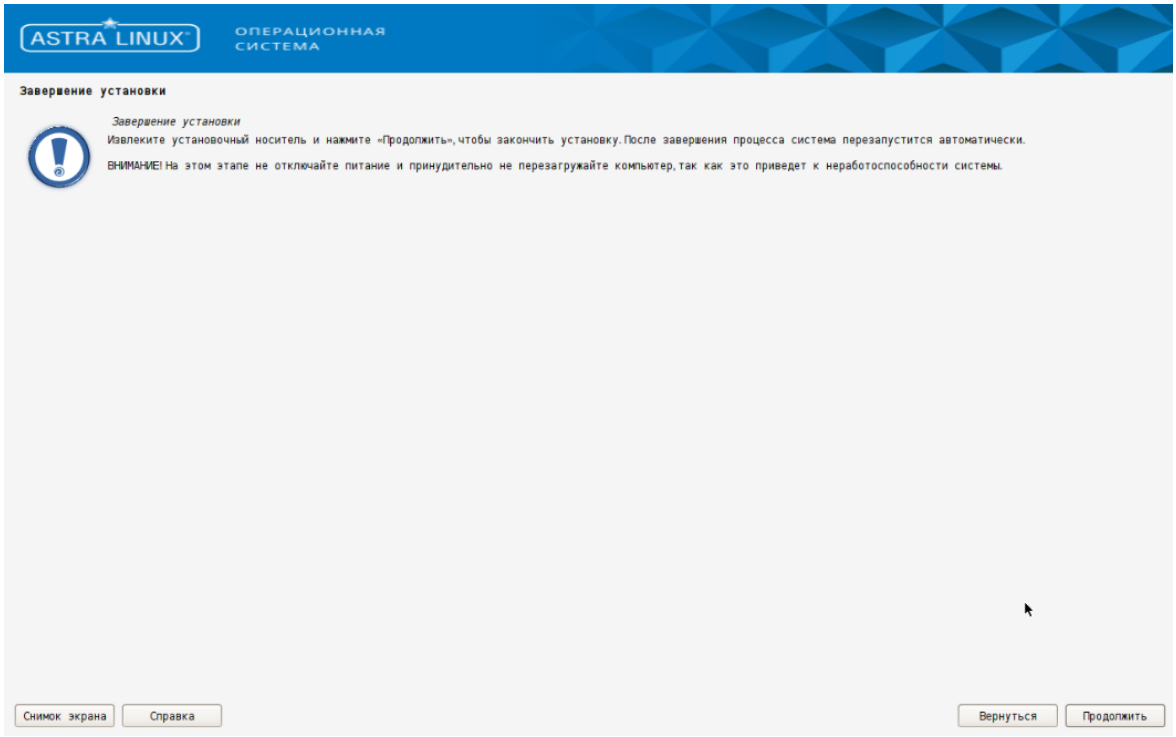


Рис. 5.24. Завершение установки

26. Смонтируйте установочный диск с ОС Astra и вручную установите пакеты **ieee-data**, **python3-netaddr**. Примеры команд:

```
mount -t iso9660 -o ro /dev/sr0 /media/cdrom
apt update
apt install ieee-data python3-netaddr
```

На данном этапе установка ОС Astra Linux завершена. Следующим шагом необходимо перейти к установке SafeConnect.

5.1.2. Инсталляция SafeConnect в виртуальной машине

5.1.2.1. Подготовка к установке SafeConnect

Перед началом установки необходимо создать учётную запись (например, **toor**).

Используйте следующие команды для создания:
```
useradd -m toor
```

Установите пароль:
```
passwd toor
```

Добавьте учетную запись в группу администраторов:
```
usermod -a -G astra-admin toor
```

Установите уровень целостности:
```
pdpl-user -i 63 toor
```

SafeConnect использует зависимости определённых версий. Для настройки зависимостей выполните следующие команды:
```
cat > /etc/apt/preferences.d/etcd-server << EOF
Package: etcd-server
Pin: version 3.5.16-7
Pin-priority: 1001"
EOF

cat > /etc/apt/preferences.d/etcd-client << EOF
Package: etcd-client
Pin: version 3.5.16-7
Pin-priority: 1001"
/etc/apt/preferences.d/etcd-client
EOF
```

Установите диск в CD-ROM или смонтируйте ISO–файл SafeConnect:
```
mount -t iso9660 -o ro /dev/sr0 /media/cdrom
```

Добавьте публичный ключ в список доверенных ключей системы:
```
apt-key add /media/cdrom/Packages/RT-Solar-deb-key.pub
```

Добавьте CD-ROM в список источников **/etc/apt/sources.list**:
```
apt-cdrom -m add
```

Отключите другие источники обновлений кроме CD-ROM в файле **/etc/apt/sources.list**

Обновите список доступных пакетов:
```
apt update
```

5.1.2.2. Установка SafeConnect

Установите SafeConnect командой:

```
apt install sc-common
```

Перейдите по адресу виртуальной машины в веб-портал для проведения первоначальной настройки.

5.2. Создание и настройка VMware

В этом разделе приведено 2 варианта создания виртуальной машины:

- Создание виртуальной машины на базе VMware Workstation (раздел 5.2.1);
- Создание виртуальной машины на базе VMware ESXi (раздел 5.2.2).

5.2.1. Создание ВМ на базе VMware Workstation

Установка SafeConnect в виртуальном устройстве начинается с установки и настройки виртуальной машины с параметрами, соответствующими программному комплексу. Для установки виртуальной машины запустите приложение VMware Workstation, и выполните следующие действия:

1. Войти в систему VMware Workstation, и нажать кнопку **Создать**;
2. Выбрать обычный (typical) тип инсталляции, нажать **Далее** (Next) (Рис.5.26);



Рис. 5.25. Создание новой виртуальной машины

3. В открывшемся окне **Guest Operating System Installation** (Рис.5.27) выбрать дистрибутив с ПО SafeConnect и нажать **Далее** (Next);

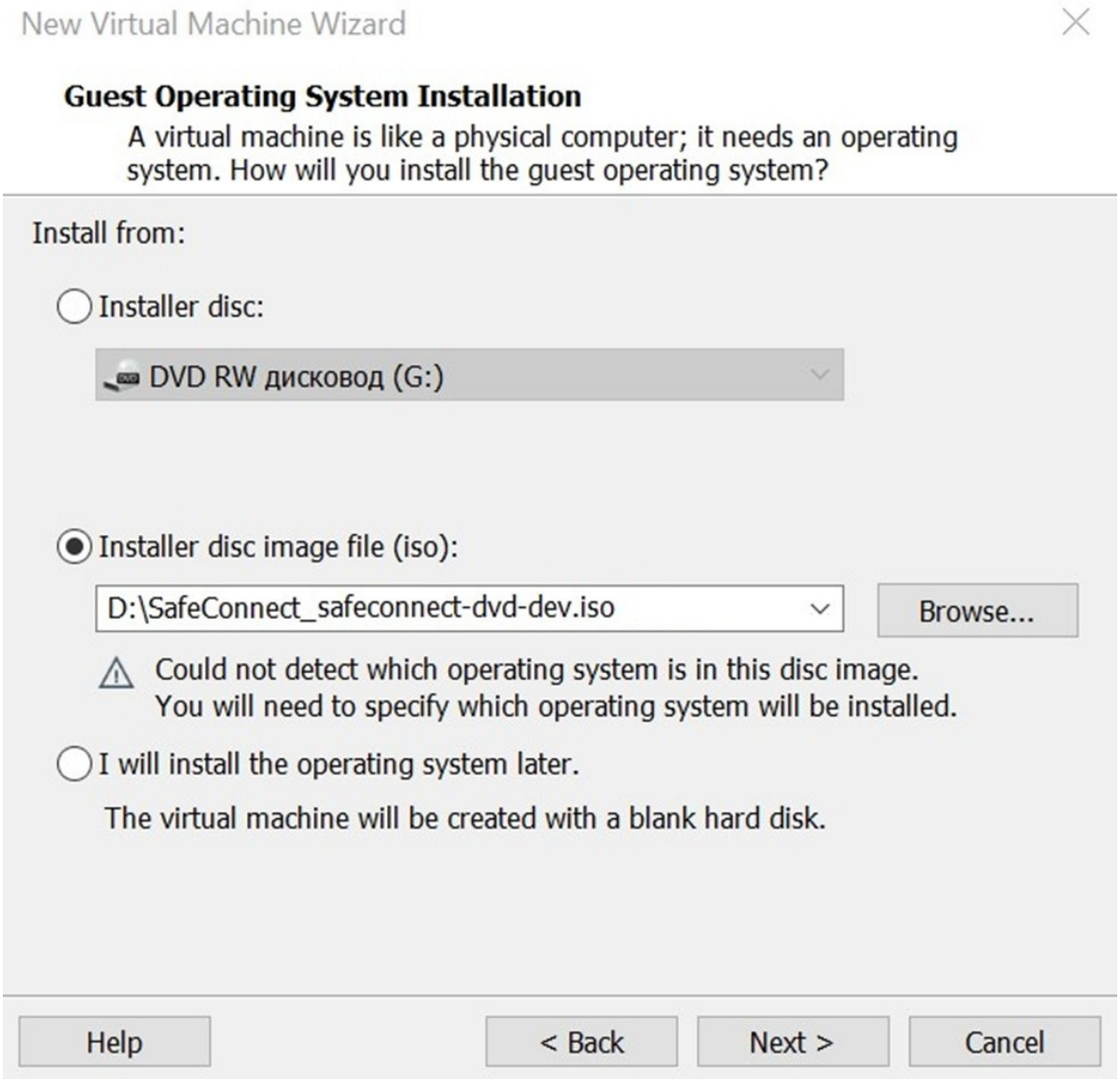


Рис. 5.26. Выбор дистрибутива

4. В случае, если в окне **Guest Operating System Installation** появилось сообщение о необходимости выбора ОС (Рис.5.28), то после нажатия кнопки **Далее** (Next) появится окно с выбором типа операционной системы (Рис.5.29). В окне **Select a Guest Operating System** установить значение Linux, выбрать из выпадающего списка **Debian 10.x 64-bit**, нажать кнопку **Далее** (Next).

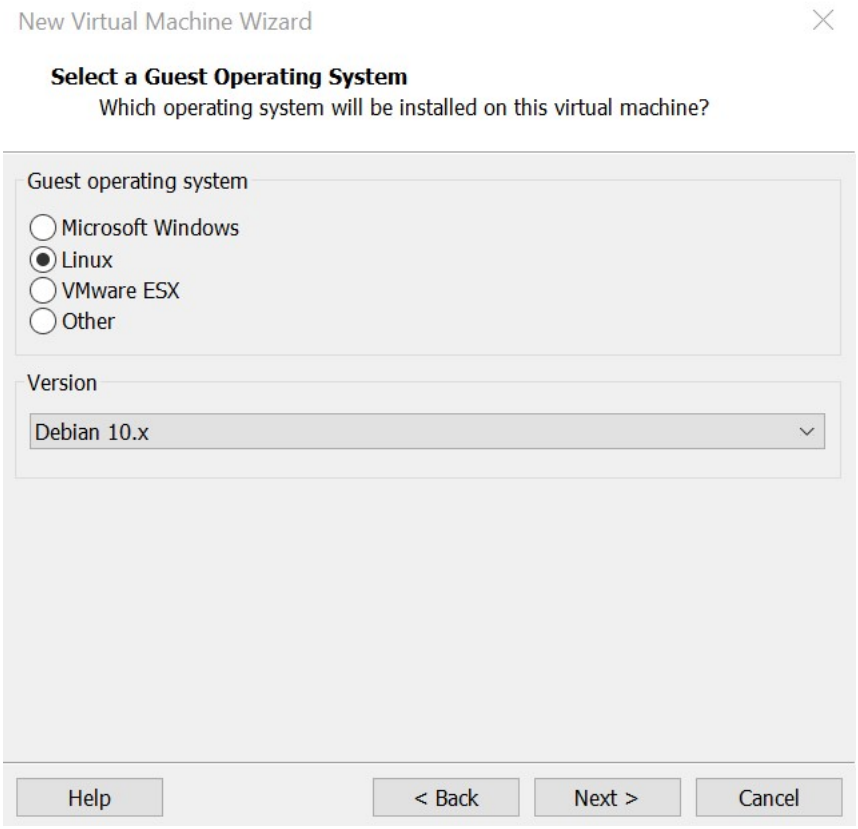


Рис. 5.27. Предупреждение о необходимости выбора ОС

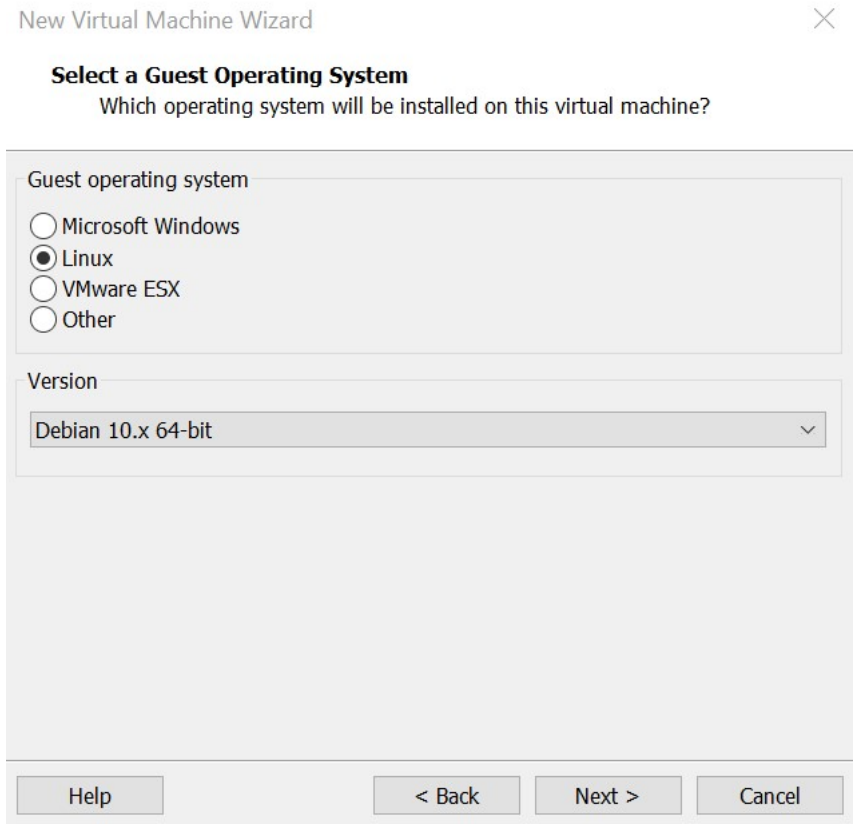


Рис. 5.28. Выбор ОС

5. В окне **Name the Virtual Machine** указать имя виртуальной машины и нажать кнопку **Далее** (Next) (Рис.5.30);

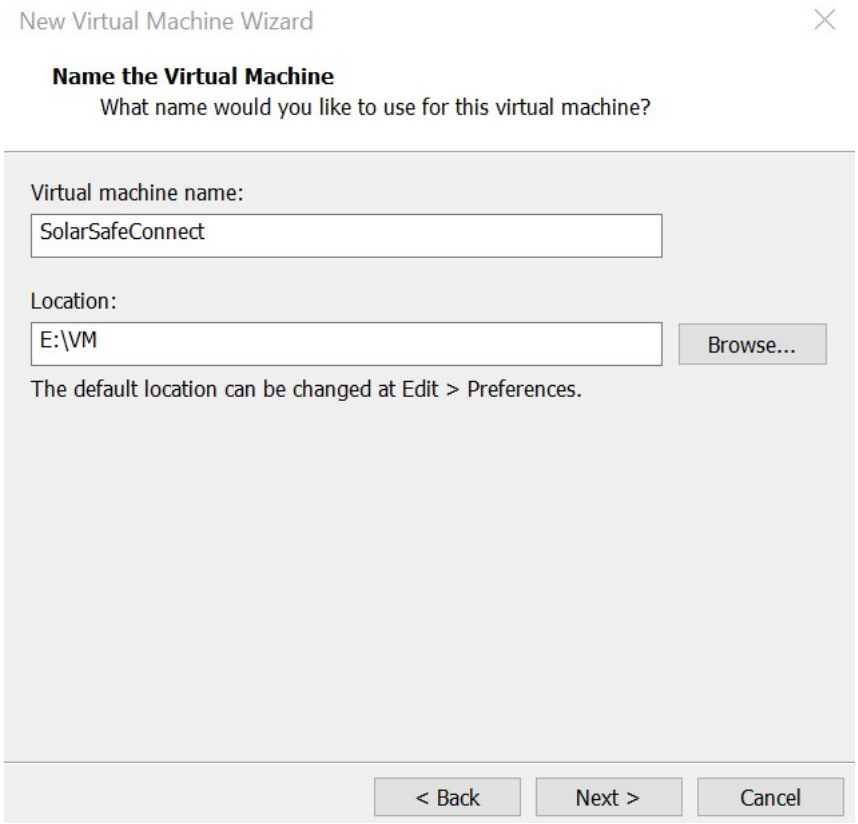


Рис. 5.29. Имя виртуальной машины

6. В окне **Specify Disk Capacity** указать необходимое дисковое пространство. Если виртуальная машина создается для тестов – 20 ГБ будет достаточно. Для бизнес-целей необходимо руководствоваться типом подсистем и количеством одновременных подключений по различным протоколам (Рис.5.32);

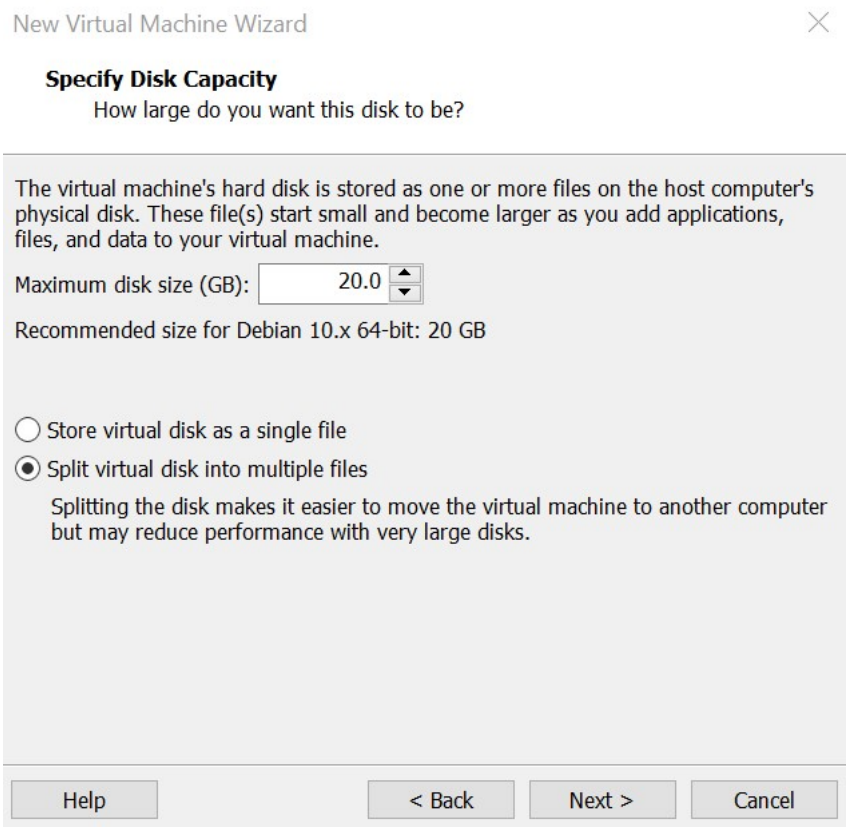


Рис. 5.30. Размер дискового пространства

7. В окне **Ready to Create Virtual Machine** нажать кнопку **Customize Hardware** (Рис.5.32);

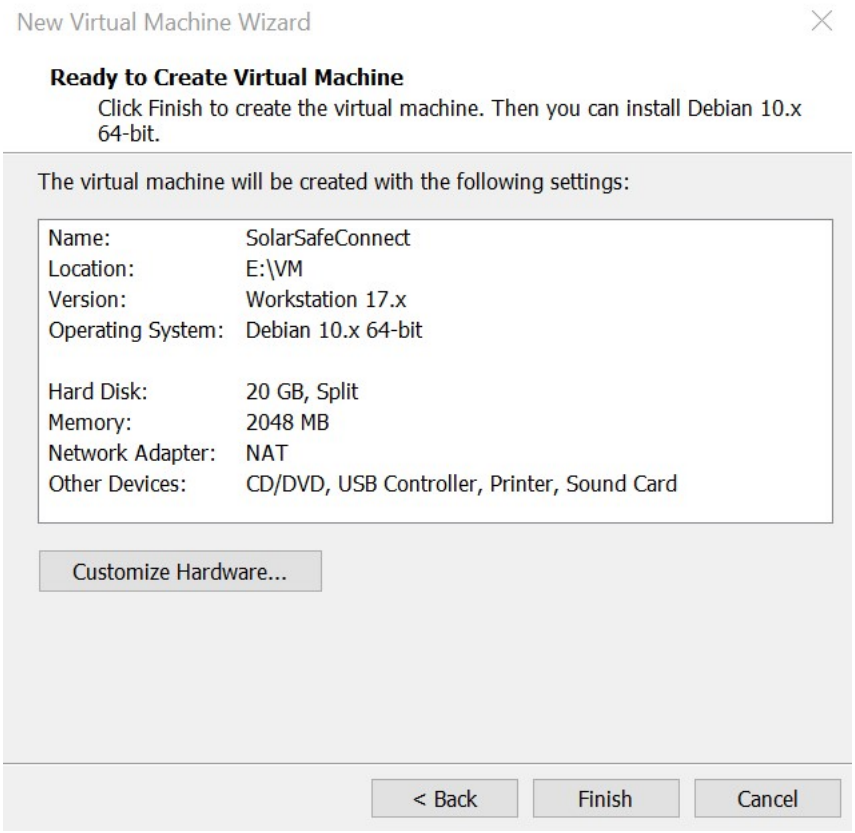


Рис. 5.31. Customize Hardware

8. Указать объем оперативной памяти (RAM), выделенный данной виртуальной машине: 2048 МБ (минимально) или больше, в соответствии с требованиями системы, количества и типа подключений. Нажать кнопку **Далее** (Next) (Рис.5.33);

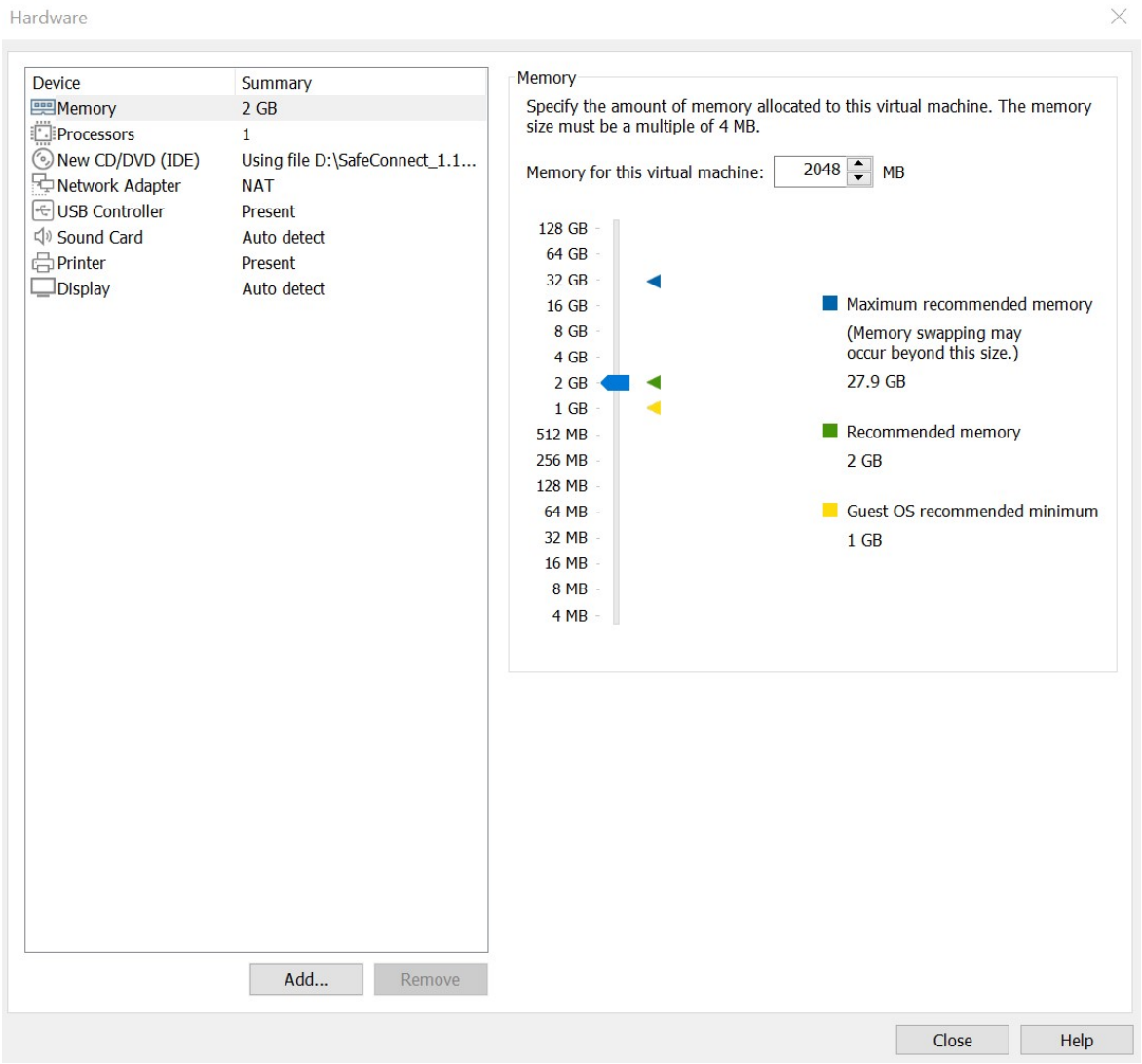


Рис. 5.32. Настройки оперативной памяти

9. Подключить сетевой адаптер к нужной виртуальной сети (Рис.5.34).

Внимание!

Для настройки Портала с фиксированными адресами необходимо предварительно выключить возможность получения адреса DHCP в данной виртуальной сети!

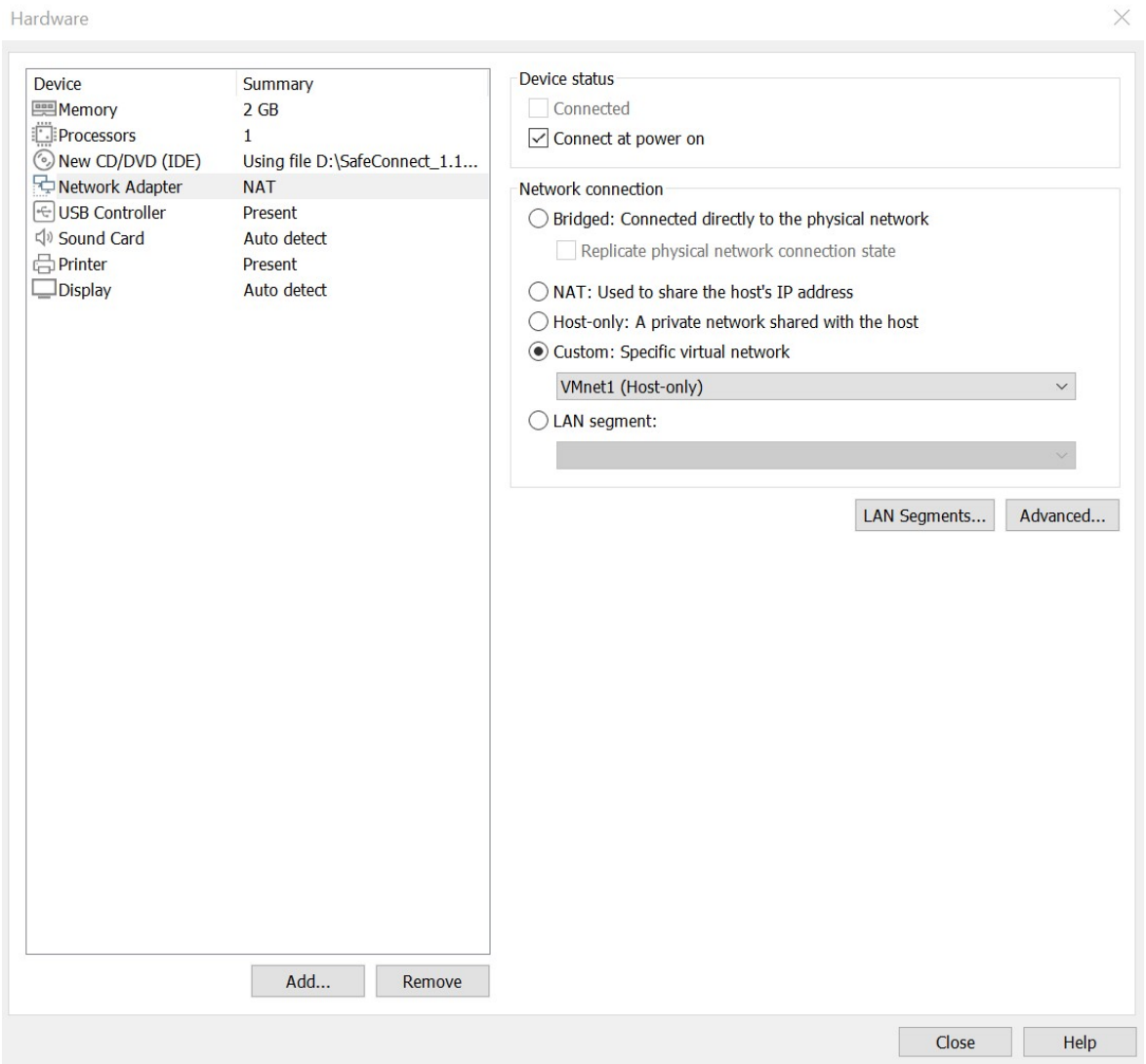


Рис. 5.33. Подключение сетевого адаптера

10. После выбора нужных параметров, необходимо нажать кнопку **Завершить** (Finish). После чего начнется инсталляция ПК SafeConnect (раздел 5.2.2).

5.2.2. Создание ВМ на базе VMware ESXi

Установка SafeConnect в виртуальном устройстве начинается с установки и настройки виртуальной машины с параметрами, соответствующими программному комплексу. Для установки виртуальной машины следует запустить приложение VMware ESXi и выполнить следующие действия:

1. Войти в систему VMware ESXi и нажать кнопку **Create/Register VM** (Рис.5.36);

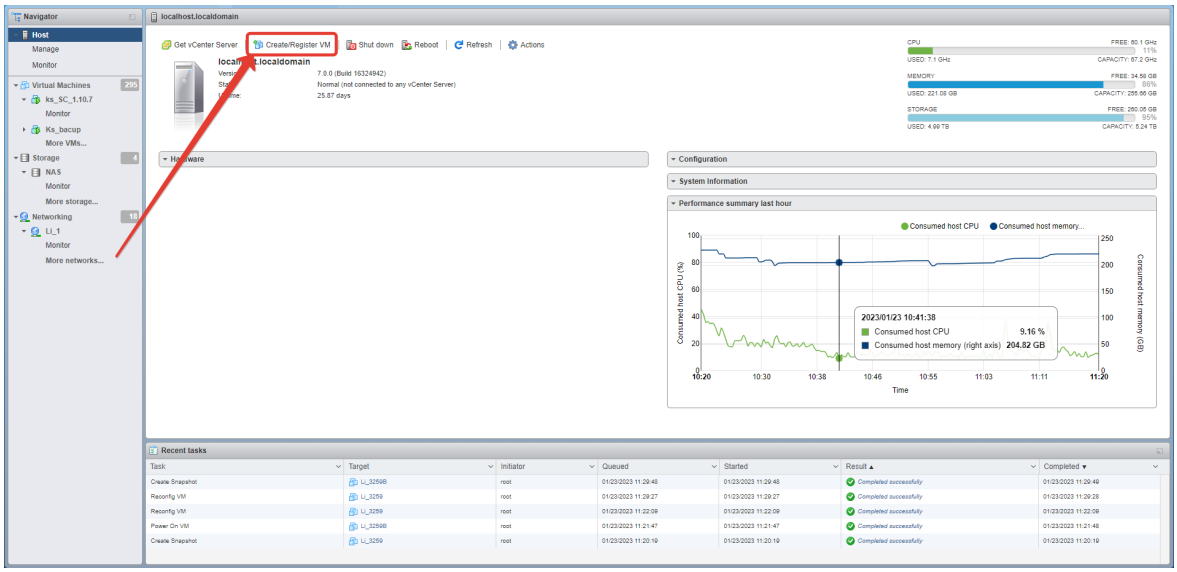


Рис. 5.34. Создание новой ВМ

2. В окне **Select creation type** выбрать **Create a new virtual machin** и нажать кнопку **Next** (Рис.5.37);

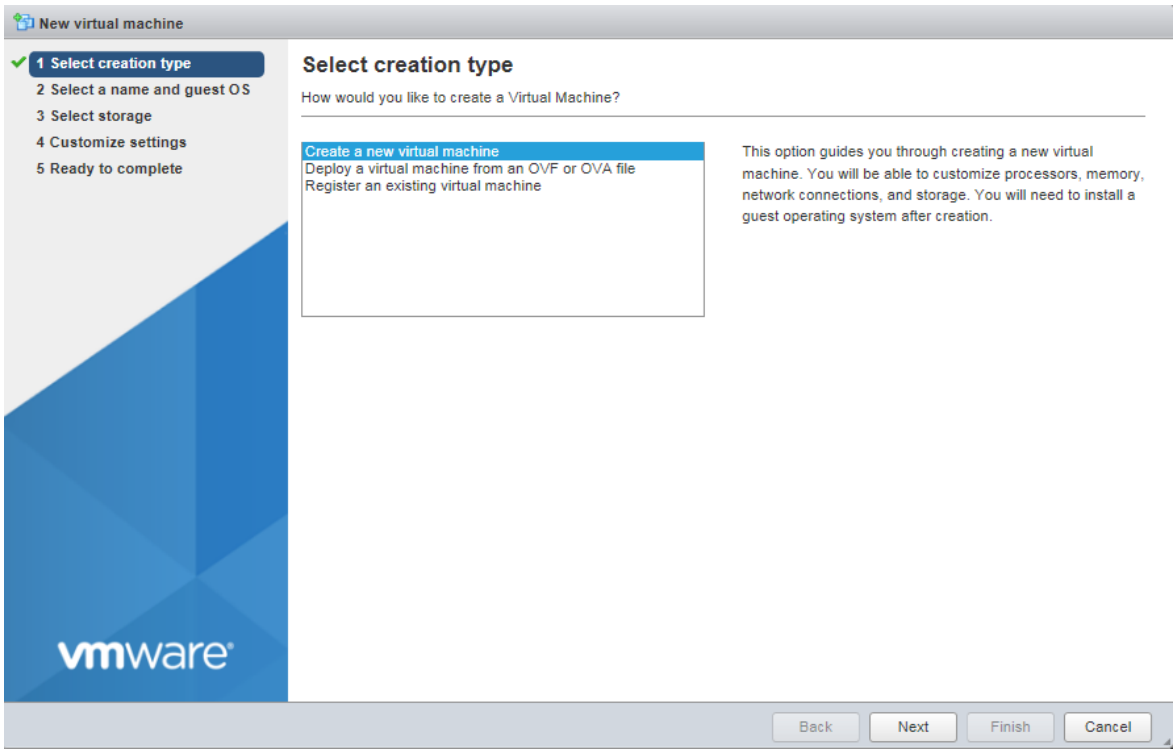


Рис. 5.35. Форма создания новой ВМ

3. В окне **Select a name and guest OS** задать уникальное имя виртуальной машины, гостевую операционную систему и ее версию. Нажать кнопку **Next** (Рис.5.38);

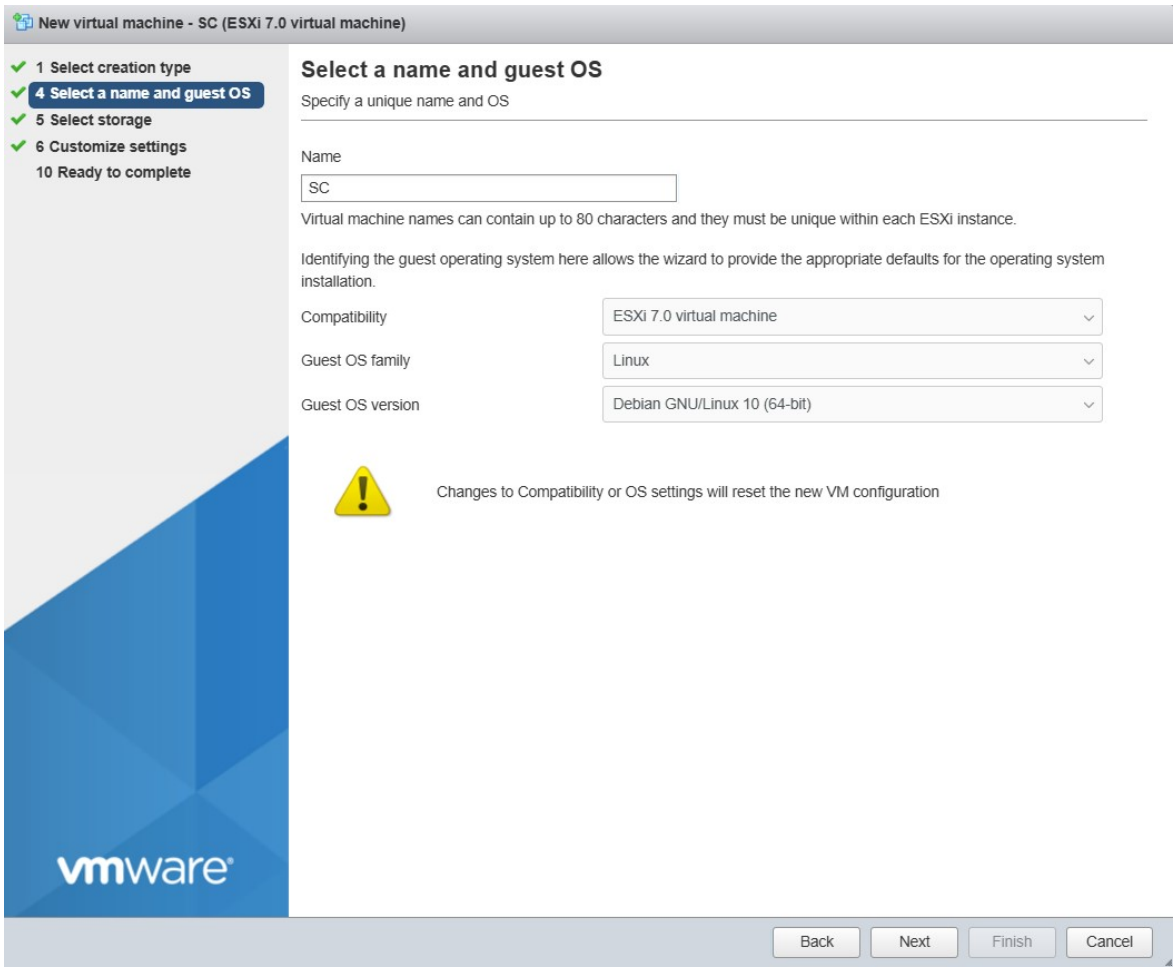


Рис. 5.36. Выбор имени и операционной системы

4. В окне **Select storage** выбрать хранилище, где хранится конфигурация виртуальной машины и виртуальные диски, и нажать кнопку **Next** (Рис.5.39);

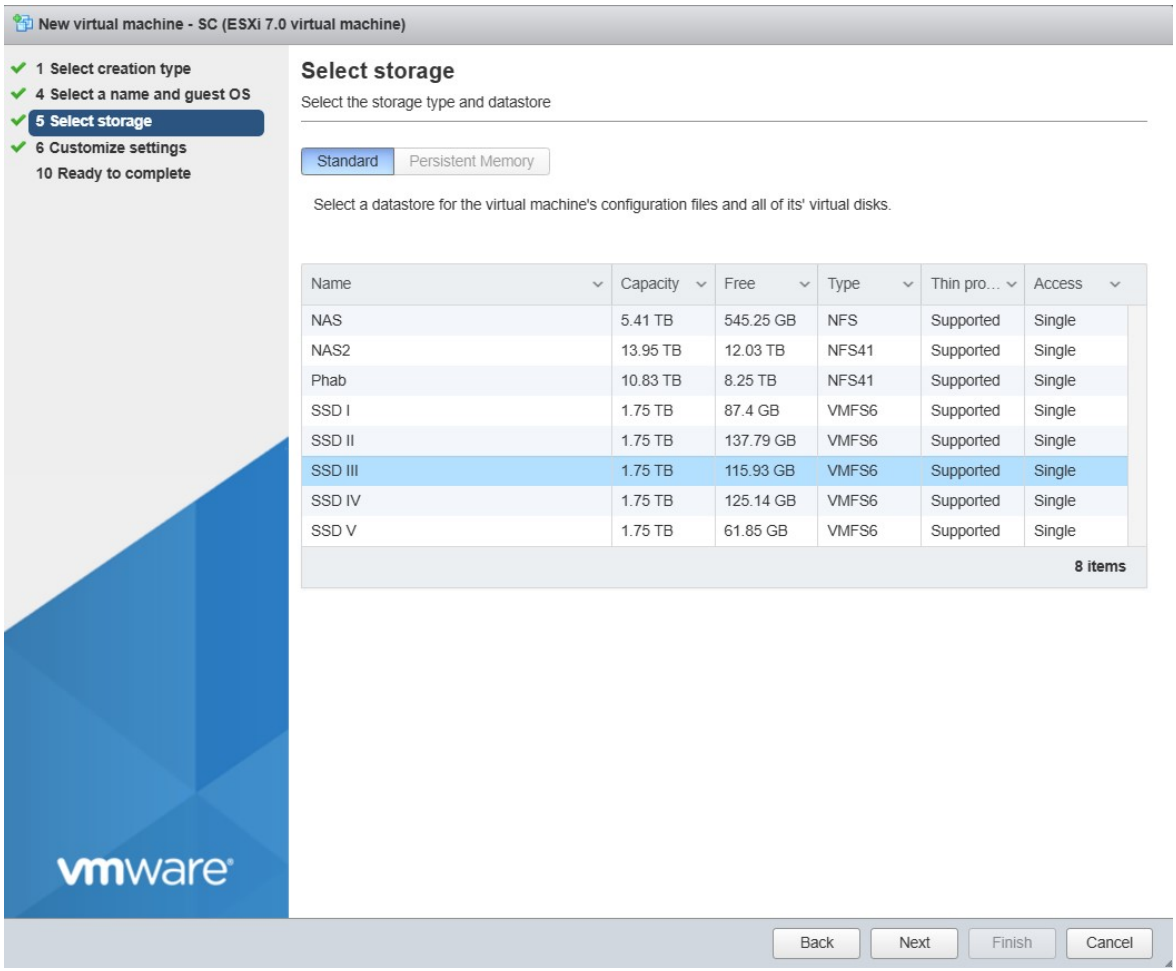


Рис. 5.37. Выбор хранилища

5. В окне **Customize settings** в поле CD/DVD Media нажать кнопку **Browse** и выбрать ISO-файл с образом SafeConnect. Нажать кнопку **Next** (Рис.5.40);

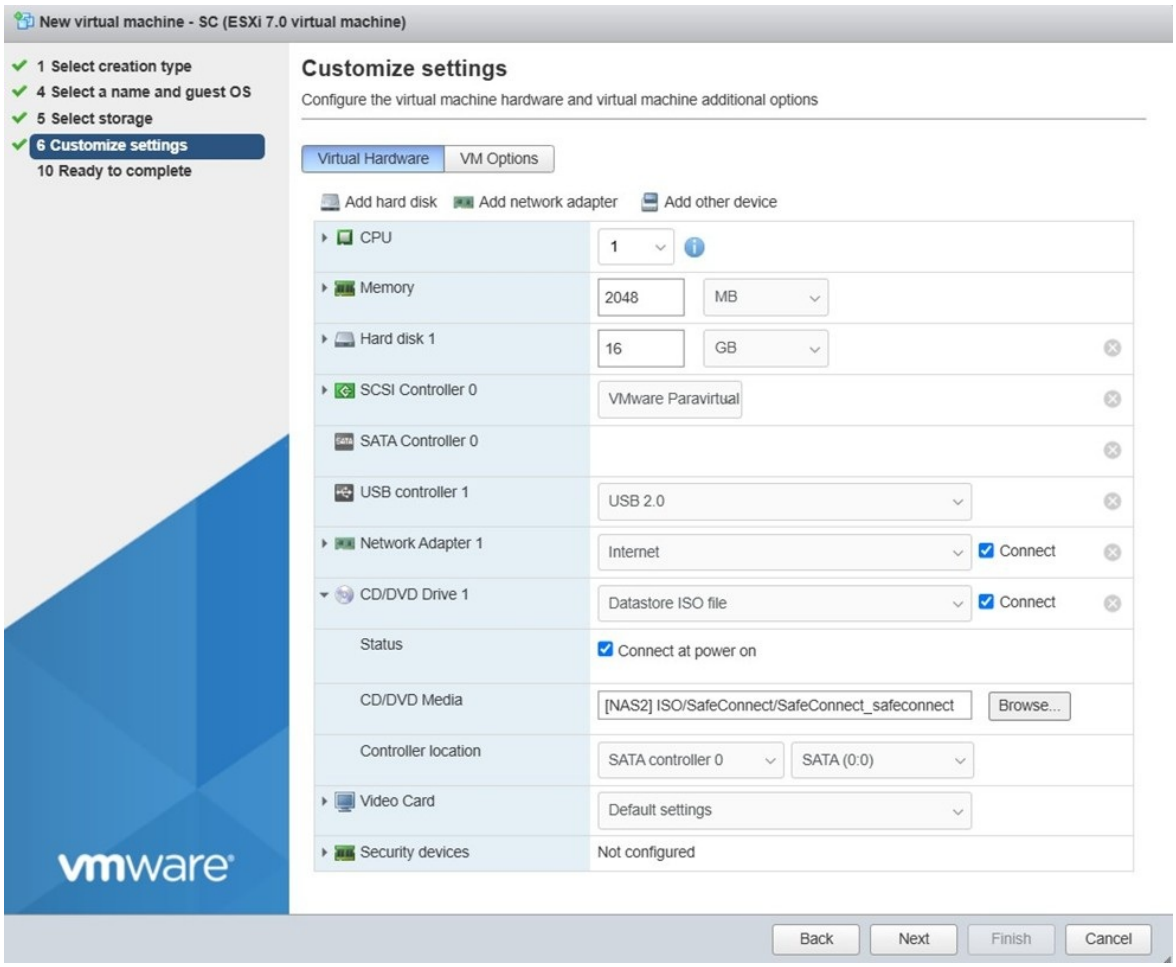


Рис. 5.38. Выбор настроек

6. В окне **Ready to complete** проверить заданные настройки и нажать кнопку **Finish** для завершения создания виртуальной машины (Рис.5.40);

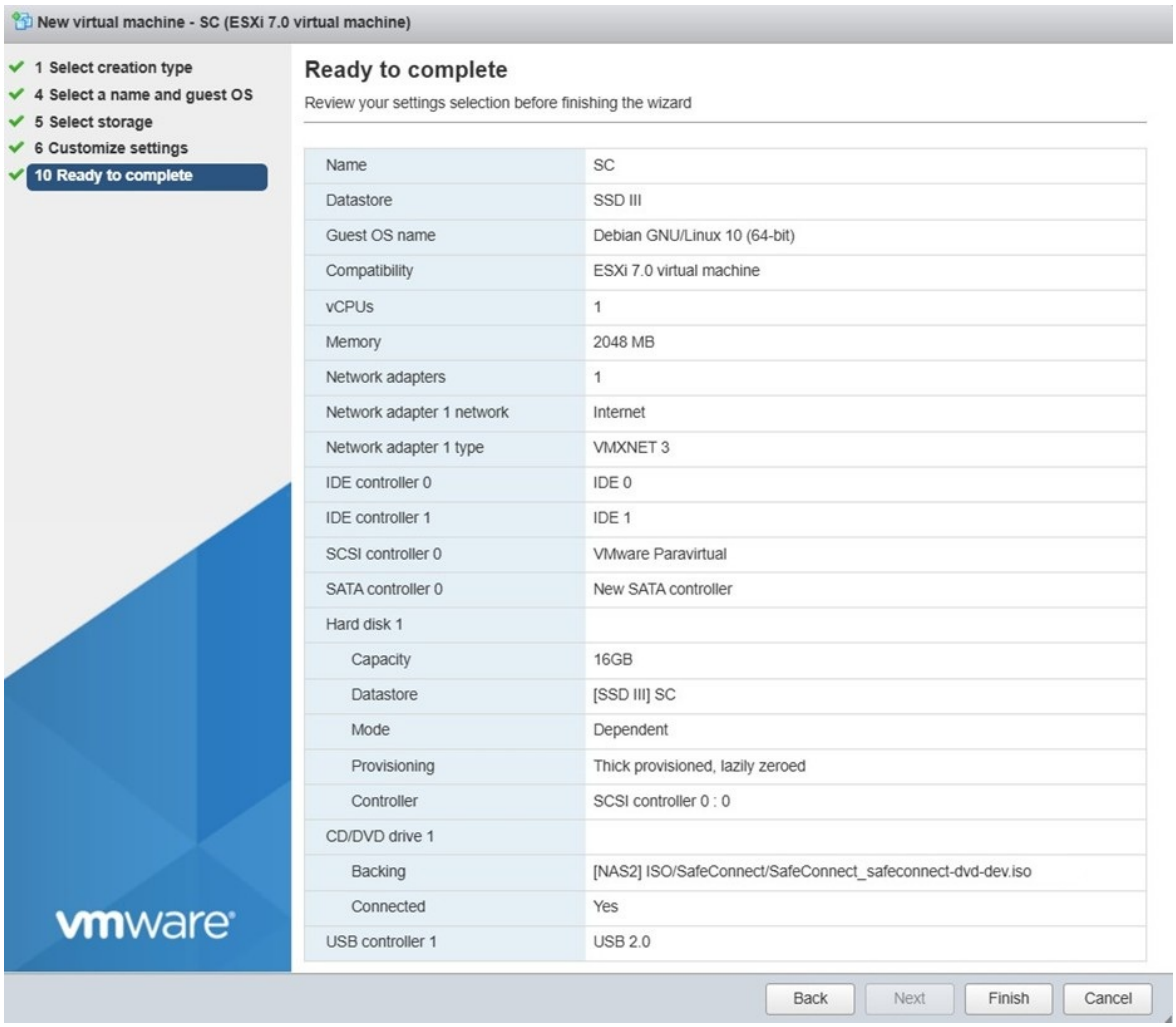


Рис. 5.39. Проверка настроек

7. Выбрать созданную виртуальную машину в списке виртуальных машин и запустить ее, нажав кнопку **Power on** (Рис.5.41). Начнется процесс установки SafeConnect на созданную виртуальную машину.

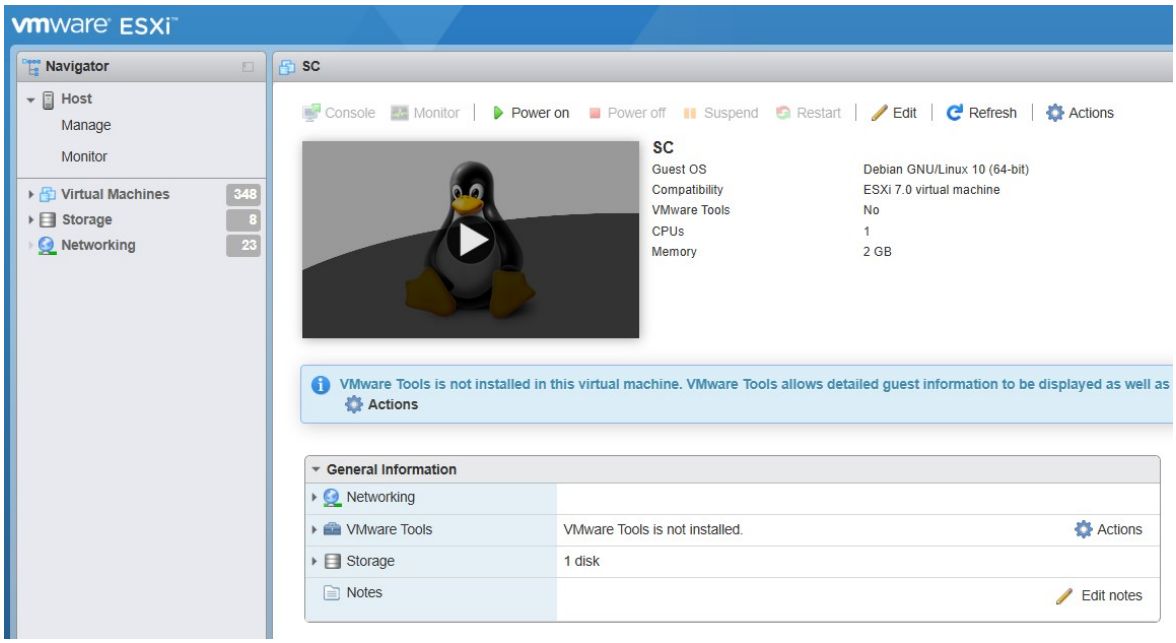


Рис. 5.40. Запуск ВМ

5.2.3. Инсталляция SafeConnect в ВМ

Для инсталляции SafeConnect выполните пошагово следующие действия:

1. Дождитесь начала загрузки ПО;
2. В течение 10 секунд в появившемся окне выбора типа инсталляции (Рис.5.42) выбрать между графическим (Graphical install) и текстовым (Install) типом инсталляции. Они полностью идентичны. В руководстве по инсталляции, описан текстовый вариант.

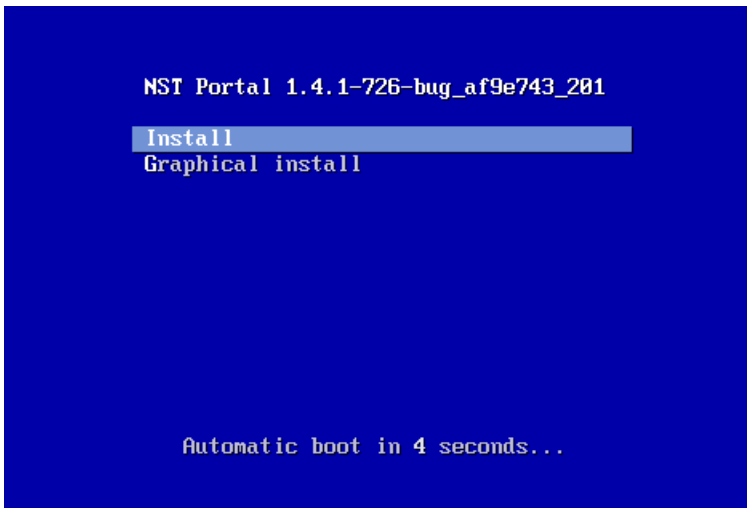


Рис. 5.41. Окно выбора типа инсталляции

Внимание!

Если в вашей виртуальной сети отсутствует DHCP-сервер, появится ошибка, показанная на рисунке (Рис.5.43).

*Необходимо нажать кнопку **Continue** для установки адреса сетевого адаптера. Если сервер DHCP в этой виртуальной сети был, то такой диалог не возникнет, и Портал получит адрес и другую информацию автоматически (в этом случае из интерфейса Портала, вы не сможете изменять IP адреса);*

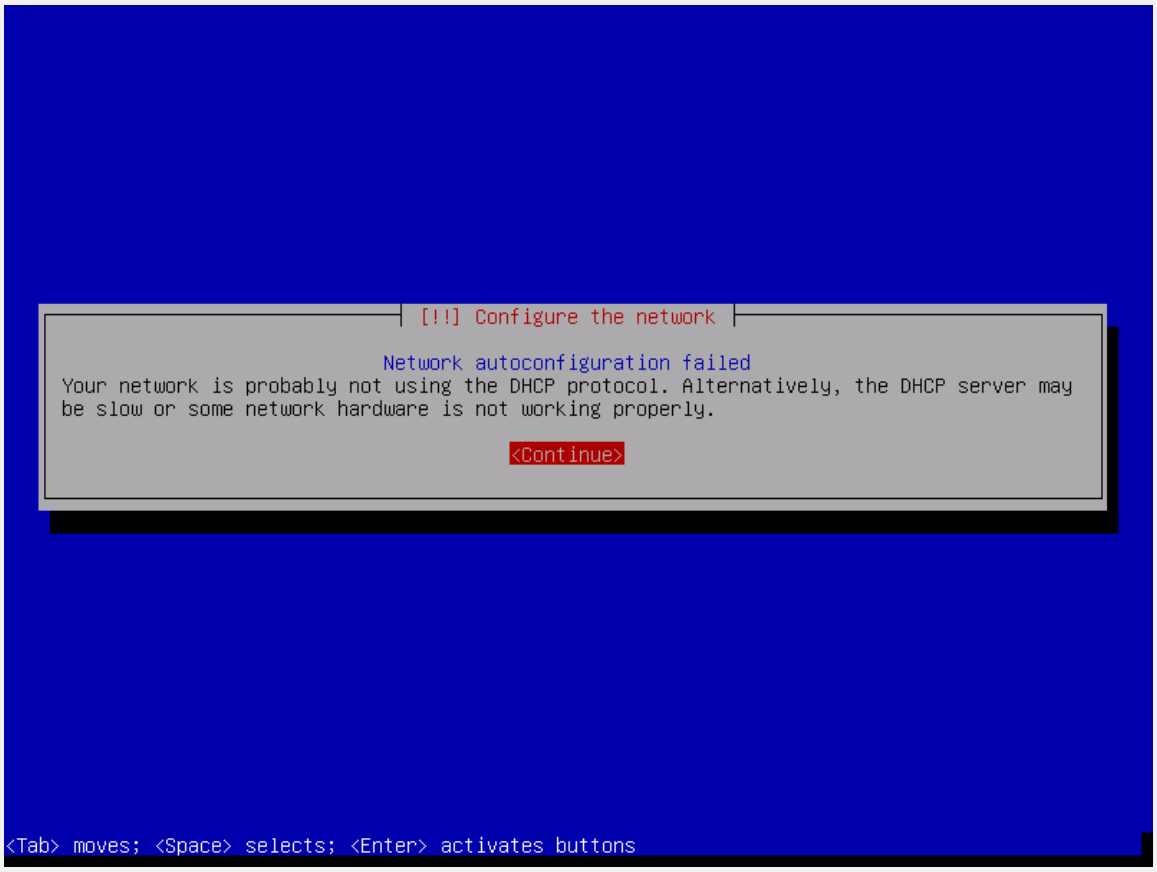


Рис. 5.42. Ошибка при отсутствии DHCP-сервера

3. В открывшемся окне (Рис.5.45) выбрать ввод адресов и другой информации вручную (Configure network manually);

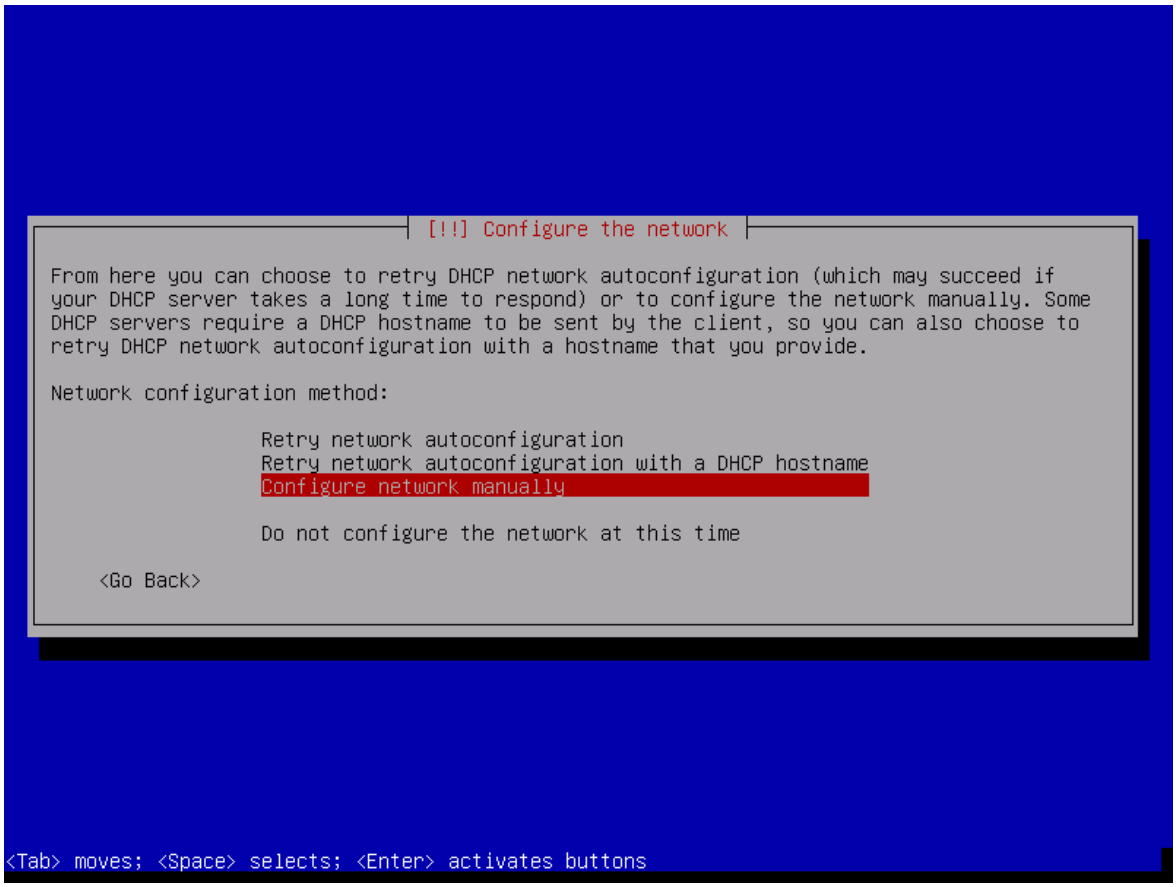


Рис. 5.43. Выбор ручного ввода информации

4. В следующих окнах **Configure the network**:
   - Ввести IP-адрес, нажать **Continue** (Рис.5.47);

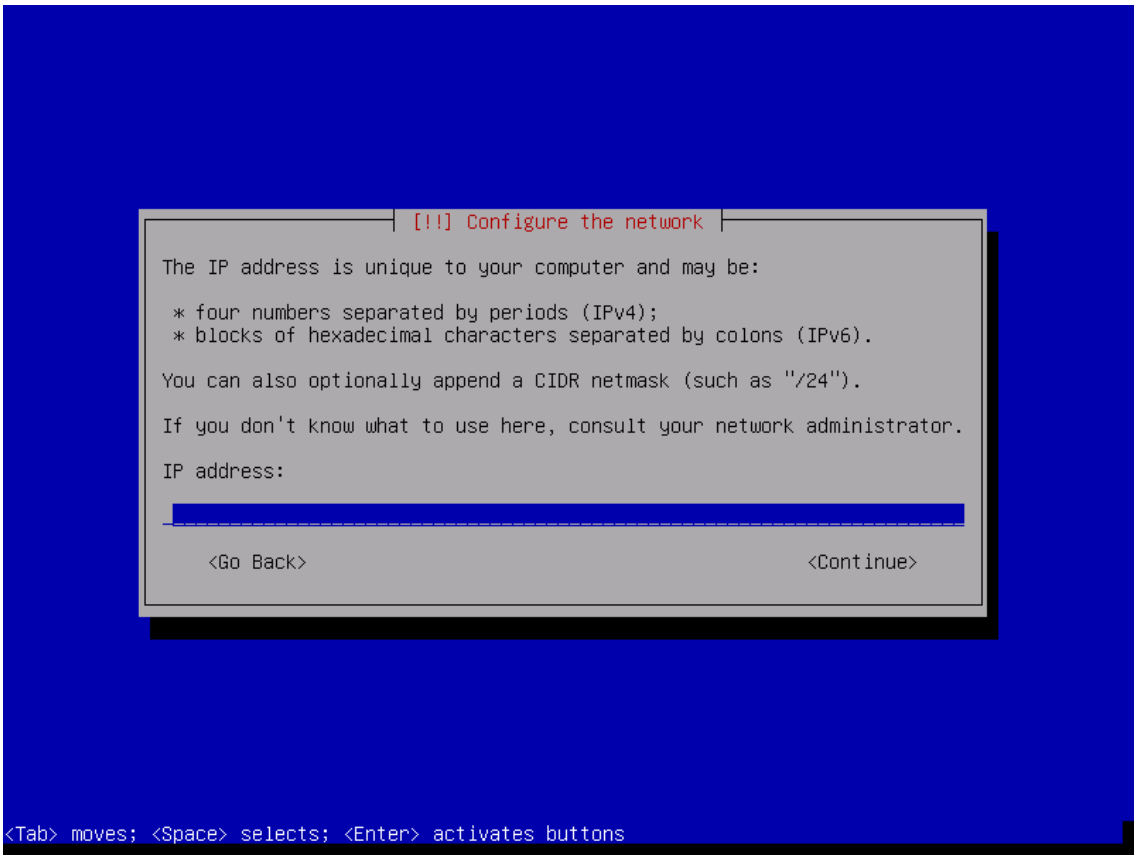


Рис. 5.44. Ввод IP-адреса

- Ввести маску сети, нажать **Continue** (Рис.5.47);

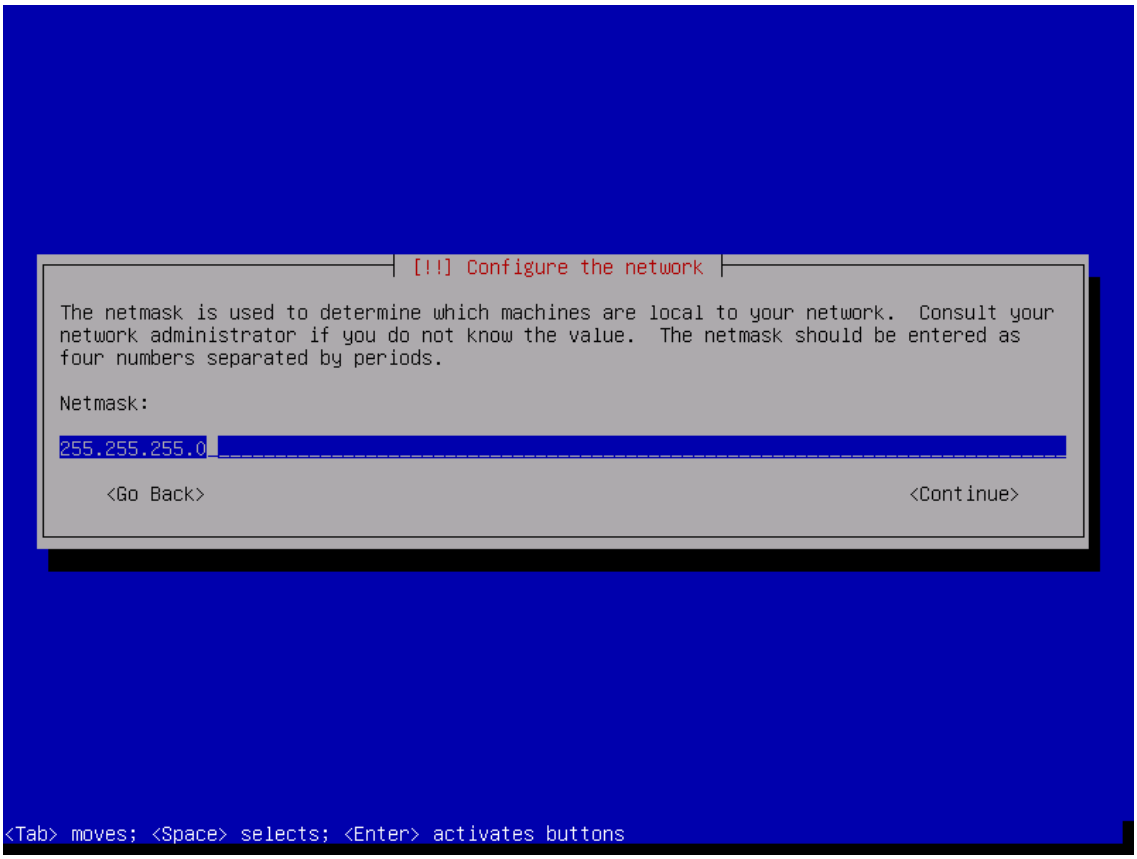


Рис. 5.45. Ввод маски подсети

- Ввести шлюз по умолчанию, нажать **Continue** (Рис.5.48);

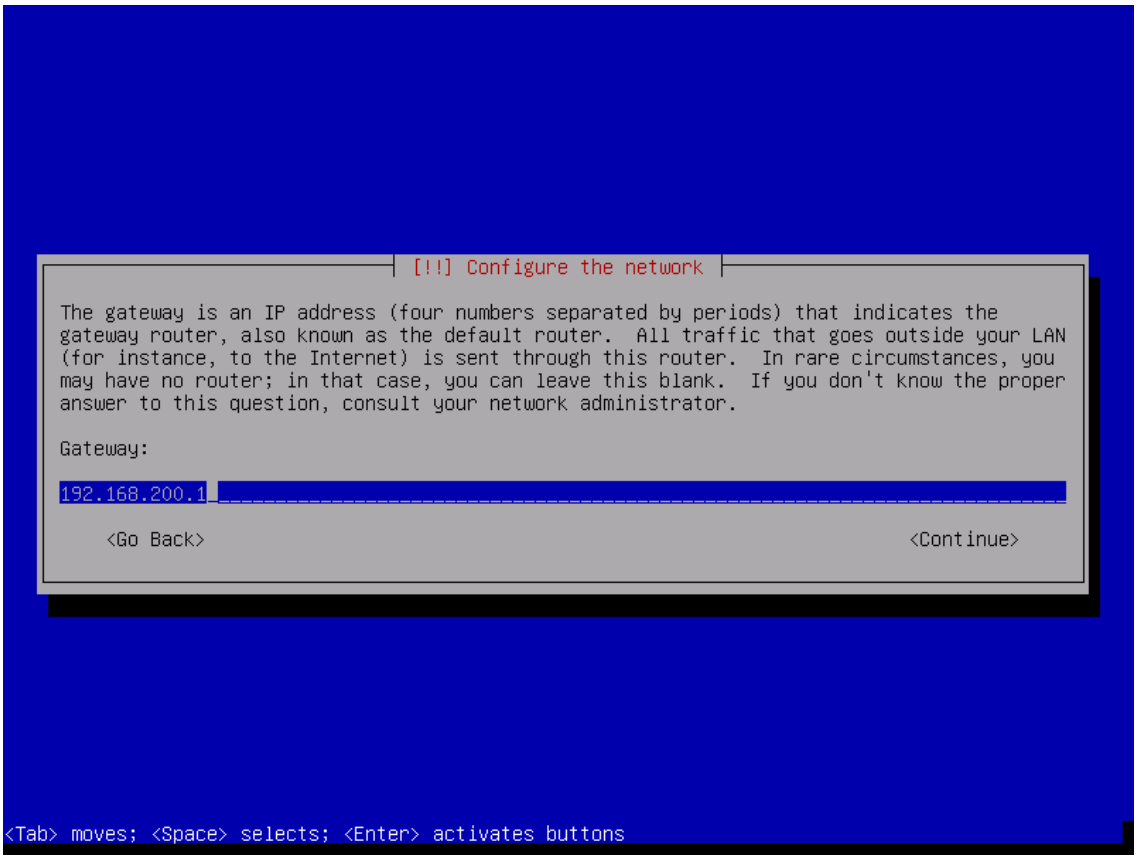


Рис. 5.46. Ввод шлюза по умолчанию

- Ввести адрес DNS сервера, нажать **Continue** (Рис.5.49).

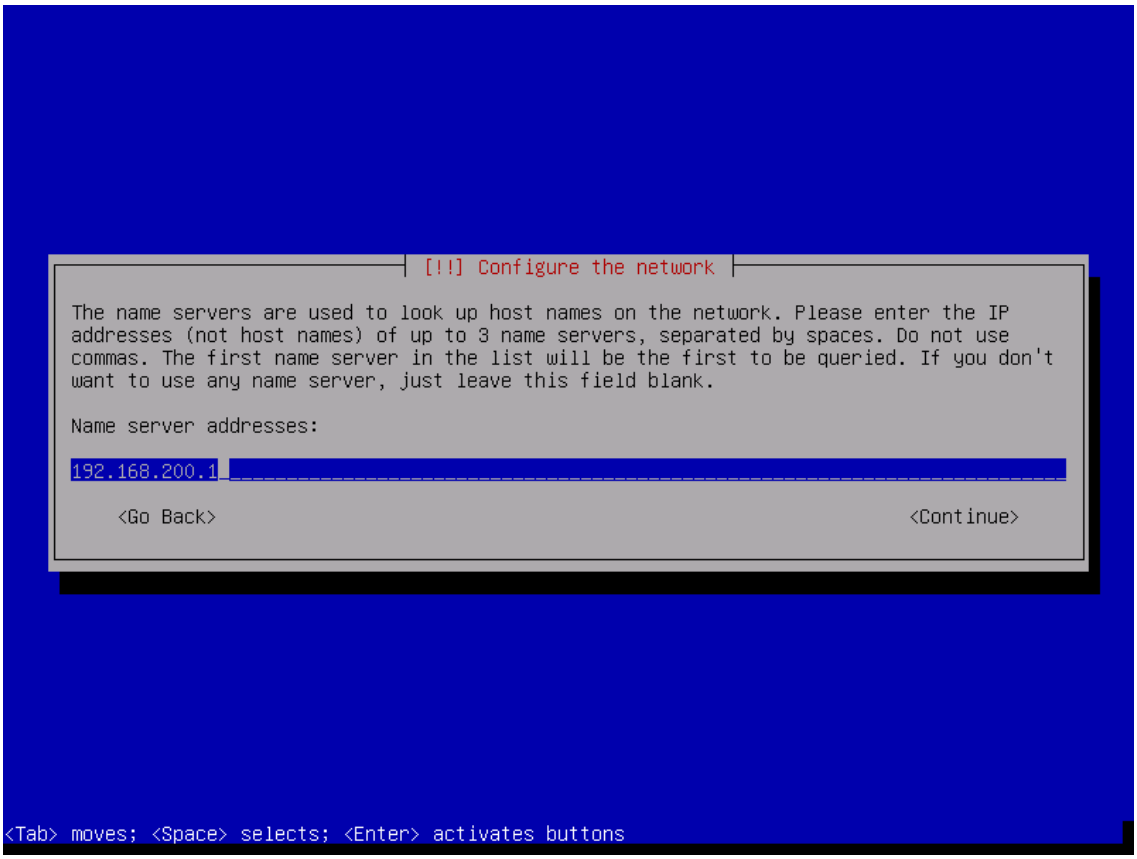


Рис. 5.47. Ввод DNS-сервера

5. В открывшемся окне в ответ на предложение ввести пароль для доступа к Порталу по протоколу SSH, нажать кнопку **Continue** (Рис.5.50);

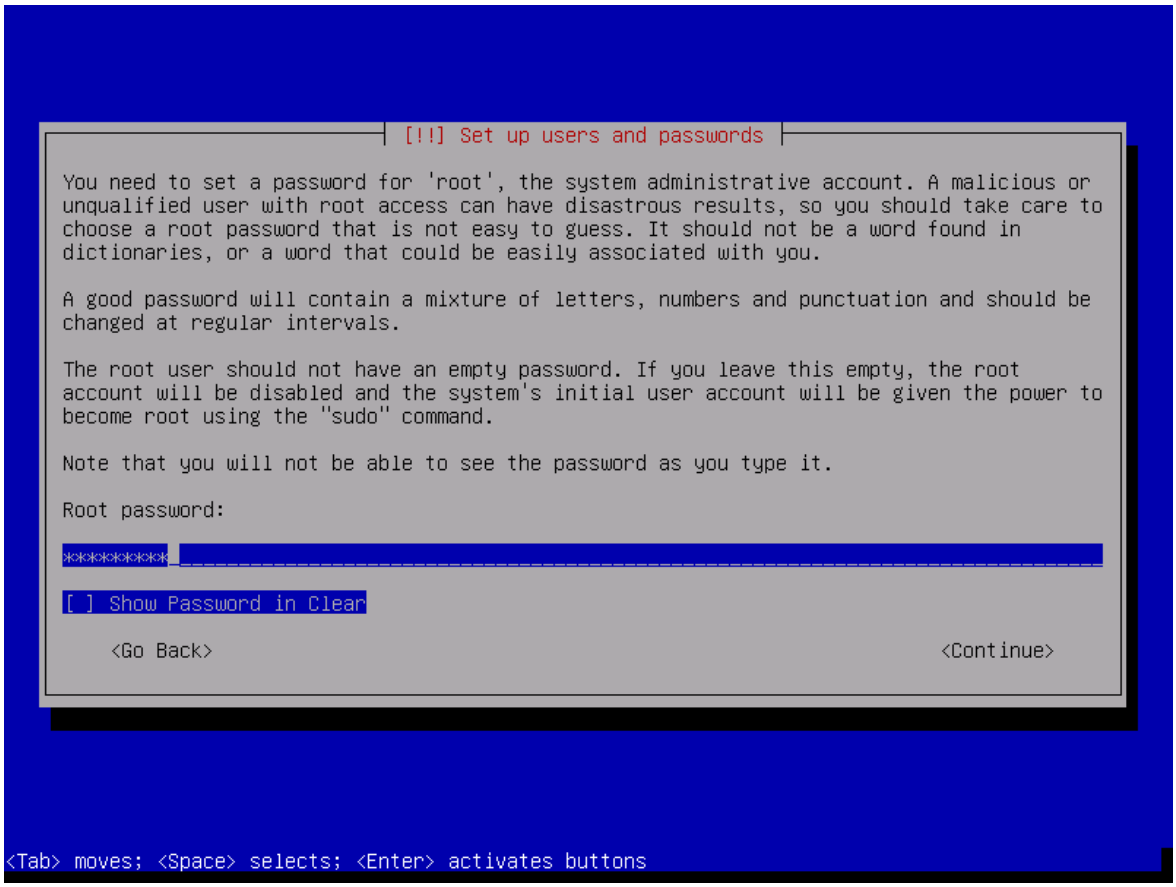


Рис. 5.48. Ввод пароля доступа к Порталу

6. В следующем окне подтвердить пароль, введенный на предыдущем этапе, и нажать **Continue**;

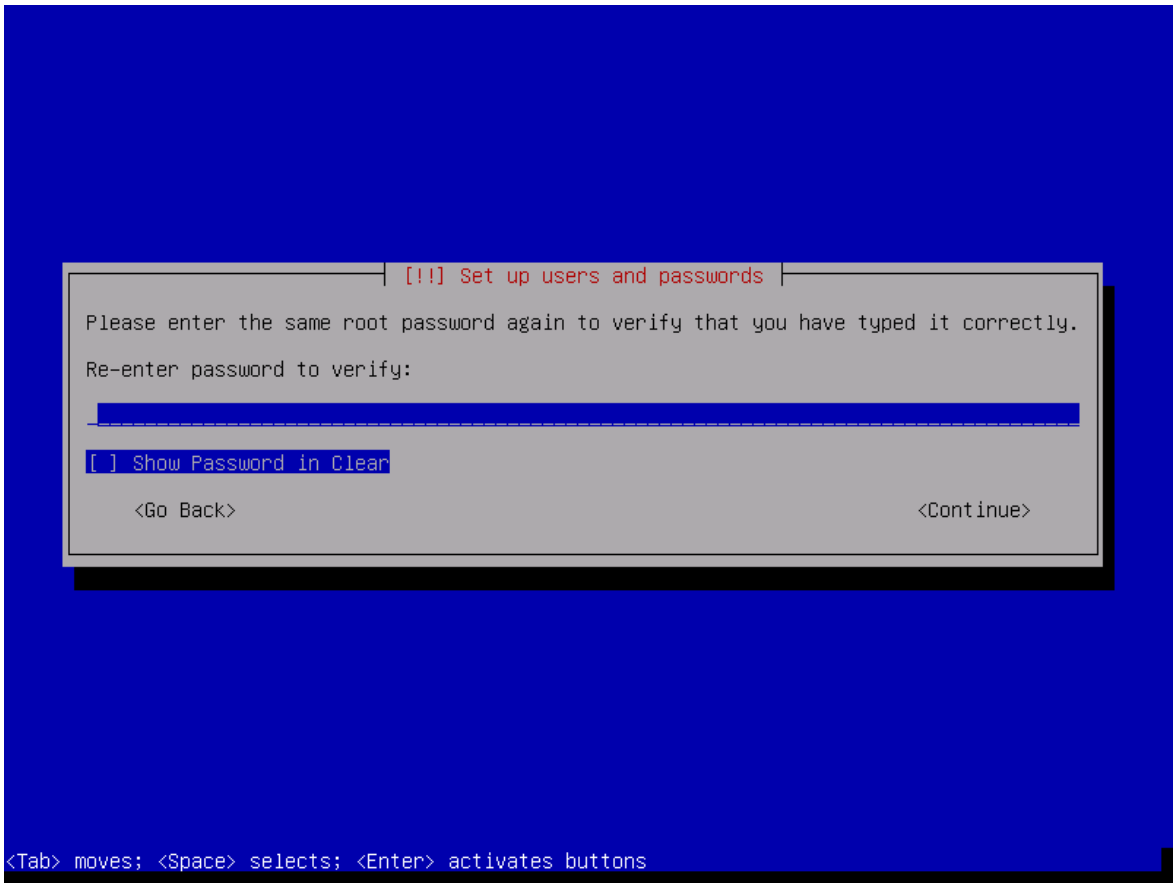


Рис. 5.49. Подтверждение пароля

7. В открывшемся окне нужно сделать разметку файловой системы. Необходимо выбрать ответ **Yes**;
8. На вопрос о записи изменений на диск ответить утвердительно **Yes**;
9. Нажать кнопку **Continue** (Рис.6.1);

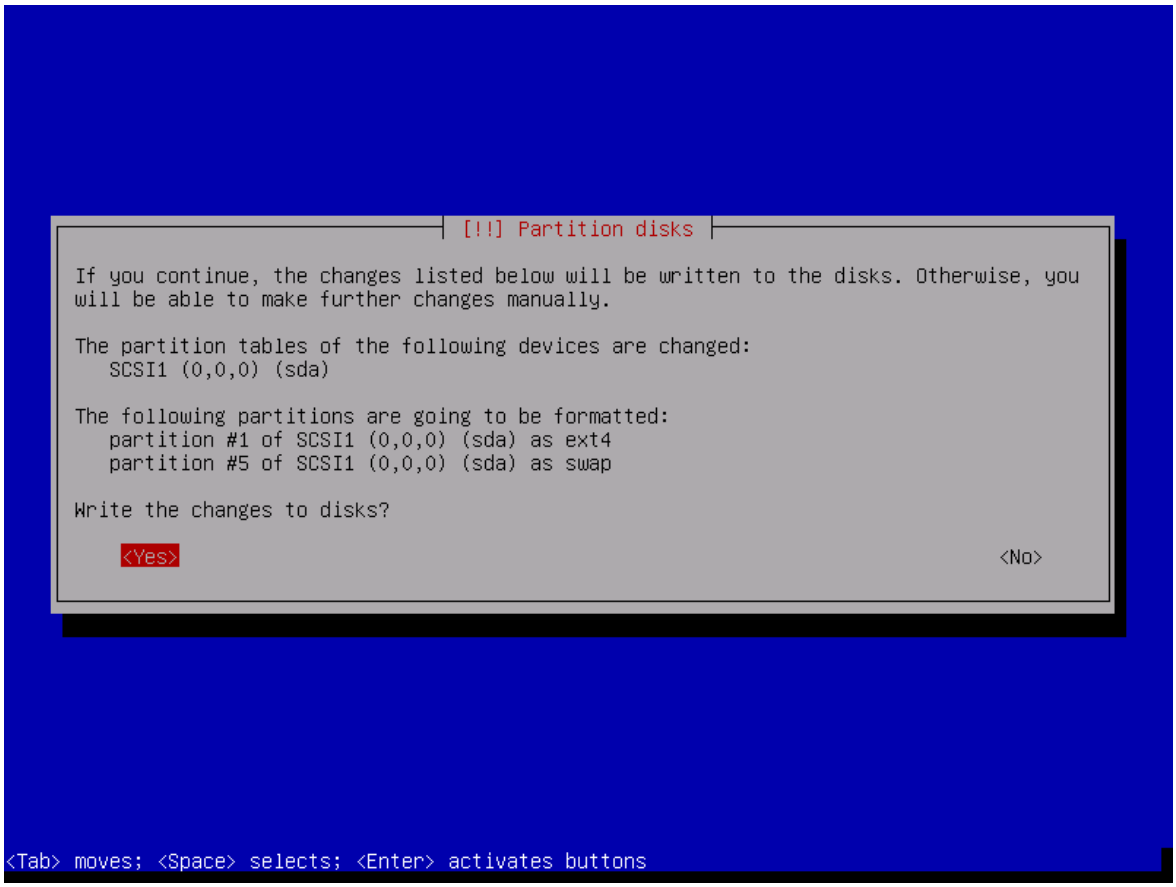


Рис. 5.50. Разметка файловой системы

10. Далее проводится распаковка программы и запись ее на диск. Происходит установка программы. После того, как установка будет завершена, нажать кнопку **Continue**. После чего произойдет перезагрузка. Загрузка происходит в полностью автоматическом режиме.

6. Запуск ПК SafeConnect

Для запуска программного комплекса SafeConnect в веб-браузере необходимо ввести IP-адрес, который был введен во время инсталляции. После этого появится диалоговое окно Создание суперадминистратора с приглашением ввести логин и пароль суперадминистратора (Рис.6.2).

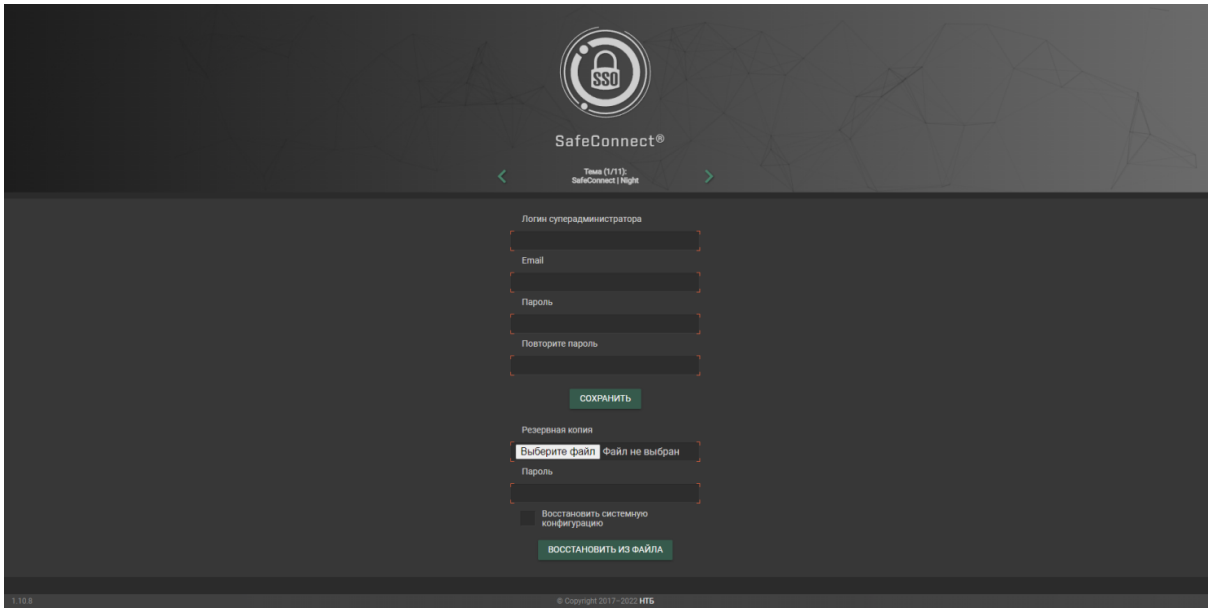


Рис. 6.1. Создание суперадминистратора

Откроется главное окно программного комплекса SafeConnect.

Для первоначального входа в систему нужно ввести:

- логин суперадминистратора,
- e-mail,
- пароль,
- повторить пароль.

Дополнительно есть возможность выбора темы (с помощью переключателя в верхнем меню) (Рис.6.3).

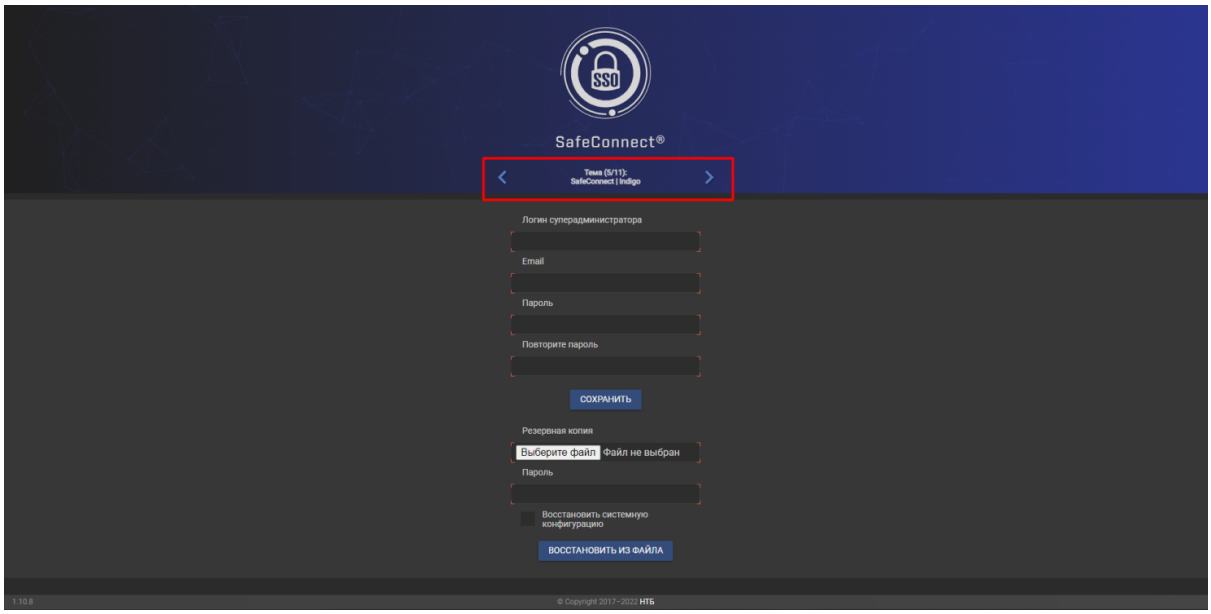


Рис. 6.2. Выбор темы

Для ввода данных нажать кнопку **Сохранить**.

Также реализована возможность восстановления системы из резервной копии сразу после установки. Для этого:

1. выбрать файл резервной копии по кнопке выбрать файл;
2. ввести пароль, назначенный при создании резервной копии;
3. при необходимости установить флажок Восстановить системную конфигурацию (настройки сети не восстанавливаются, если резервная копия была сделана на другой машине);
4. нажать кнопку Восстановить из файла.

После сохранения первоначальных настроек (после восстановления системы из резервной копии) откроется главное окно программного комплекса SafeConnect (Рис.6.3).

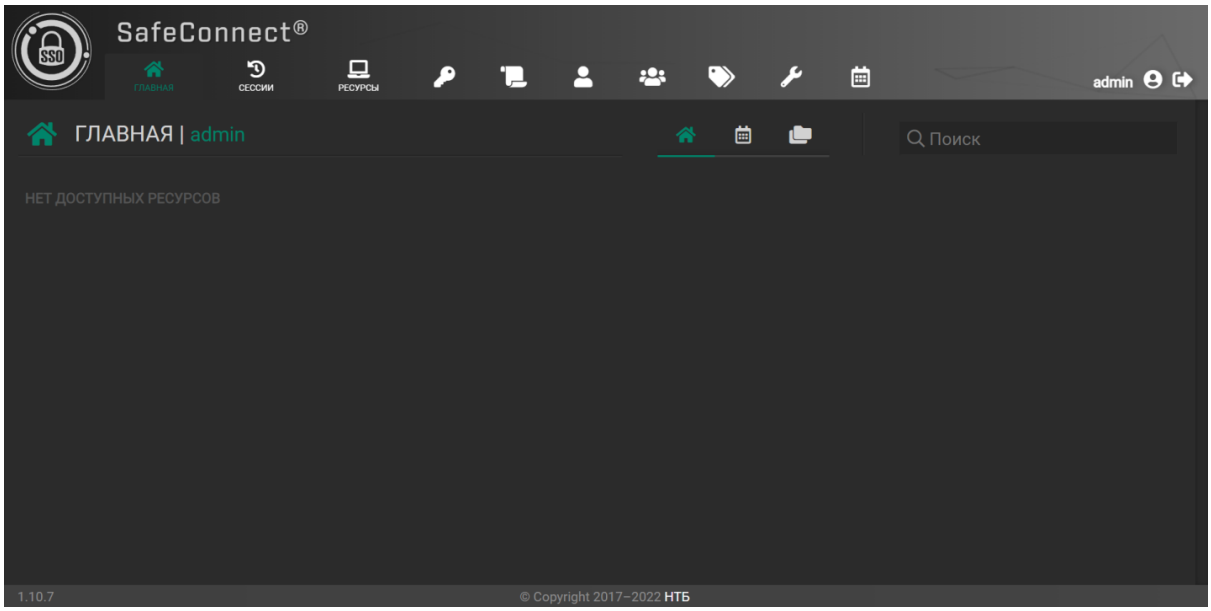


Рис. 6.3. Главное окно SafeConnect

После появления главного окна инсталляция считается завершенной. Дальнейшие действия по настройке и работе описаны в Руководстве администратора SafeConnect.