

ООО «ТИОНИКС»

**Программное обеспечение
«Защита виртуальных рабочих столов ТИОНИКС»
(TIONIX VDI Security)**

Версия 1.0

**Инструкция по установке
Руководство администратора**

RU.НРФЛ.00003-01 95 02

Листов 19

СОДЕРЖАНИЕ

1. Общие сведения	6
2. Системные требования	7
2.1. Сервер безопасности	7
2.2. Терминал.....	7
3. Процесс установки.....	8
3.1. Сервер безопасности	8
3.1.1. Установка дистрибутива	8
3.1.2. Настройка сервера безопасности	16
3.2. Терминал.....	16
3.2.1. Установка загрузчика	16
3.2.2. Настройка терминала.....	17

АННОТАЦИЯ

Программное обеспечение «Защита виртуальных рабочих столов ТИОНИКС» (английское наименование: TIONIX VDI Security, сокращенное наименование: ПО «TIONIX VDI Security») представляет собой операционную систему (ОС), предназначенную для организации безопасного терминального доступа к рабочим столам клиентских операционных систем, поддерживающих протокол RDP, в т.ч. к рабочим столам виртуальных машин инфраструктуры центра обработки данных (ЦОД).

Данный документ содержит:

- Системные требования для установки ПО «TIONIX VDI Security».
- Описание процесса установки ПО «TIONIX VDI Security».

Документ предназначен для администраторов ПО «TIONIX VDI Security».

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В документе использованы следующие термины:

Термин	Определение
Администратор системы	Лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.
Идентификация	Процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
Контейнер (контур безопасности)	Изолированные друг от друга виртуальные среды ПО «TIONIX VDI Security», в каждой из которой могут независимо выполняться системные процессы и процессы пользователей ОС.
Контроль целостности	Контроль за сохранением неизменности информации в условиях случайного и (или) преднамеренного искажения (разрушения).
Пароль	Секретный набор символов, используемый субъектом доступа для аутентификации в системе.
Персональный идентификатор	Аппаратно-программное средство персонального использования (электронный ключ), предназначенное для идентификации и аутентификации пользователя.
Объект доступа	Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.
Учетная запись пользователя	Запись, содержащая информацию о пользователе системы, необходимую для его работы в системе, в том числе сведения, используемые для идентификации и аутентификации пользователя при его подключении (регистрации) к системе.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В документе использованы следующие сокращения:

Сокращение	Определение
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ЦОД	Центр обработки данных

1. Общие сведения

ПО «TIONIX VDI Security» может функционировать в одном из следующих режимах работы (ролей), выбор которого определяется при установке ПО на компьютер:

1. Роль «Сервер безопасности» (выполняется на сервере ЦОД).
2. Роль «Терминал» (выполняется на терминале пользователя).

ПО «TIONIX VDI Security» имеет следующие функциональные возможности:

- идентификация и аутентификация пользователей на терминале, а терминала в системе;
- разграничение доступа к ресурсам системы (файлам, каталогам, приложениям, устройствам и проч.);
- контроль целостности программного обеспечения;
- регистрация событий безопасности;
- возможность работы в нескольких изолированных друг от друга контурах;
- балансировка нагрузки.

Установка ПО «TIONIX VDI Security» производится на виртуальную или аппаратную платформу, удовлетворяющую требованиям, перечисленным в разделе 2 «Системные требования».

Порядок установки ПО «TIONIX VDI Security» описан в разделе 3 «Процесс установки».

Настройка ПО «TIONIX VDI Security» после завершения установки производится в соответствии с документом «Программное обеспечение «Защита виртуальных рабочих столов ТИОНИКС». Руководство администратора».

2. Системные требования

2.1. Сервер безопасности

ПО «TIONIX VDI Security» в роли «Сервер безопасности» может быть установлено на виртуальную или аппаратную платформу сервера безопасности, удовлетворяющую минимальным требованиям, указанным в таблице ниже (Таблица 1).

Таблица 1 – Системные требования для сервера безопасности

Параметр	Значение
Частота процессора, ГГц	от 2
ОЗУ, Гб	от 8
Жесткий диск, Гб	от 50
Порты для подключения	11391, 11381, 11361, 11371
Платформа	x64

2.2. Терминал

ПО «TIONIX VDI Security» в роли «Терминал» может использовать специализированные устройства, а также персональные компьютеры, отвечающие минимальным требованиям, указанным в таблице ниже (Таблица 2).

Таблица 2 – Системные требования для терминала

Параметр	Значение
Частота процессора, ГГц	от 1
ОЗУ, Гб	от 4
Платформа	x86, Baikal-T1

3. Процесс установки

3.1. Сервер безопасности

3.1.1. Установка дистрибутива

Для установки ПО «TIONIX VDI Security» в роли «Сервер безопасности» необходимо подключить к виртуальному или физическому серверу носитель дистрибутива, на который записан образ диска *tionix.iso*, и настроить сервер на загрузку с указанного носителя.

После загрузки дистрибутива необходимо следовать указаниям мастера установки. Все значения, за исключением сетевых адресов и имен, рекомендуется оставлять теми, которые предложены по умолчанию.

Далее на рисунках показан процесс установки.



Рисунок 1 – Выбор языка установки

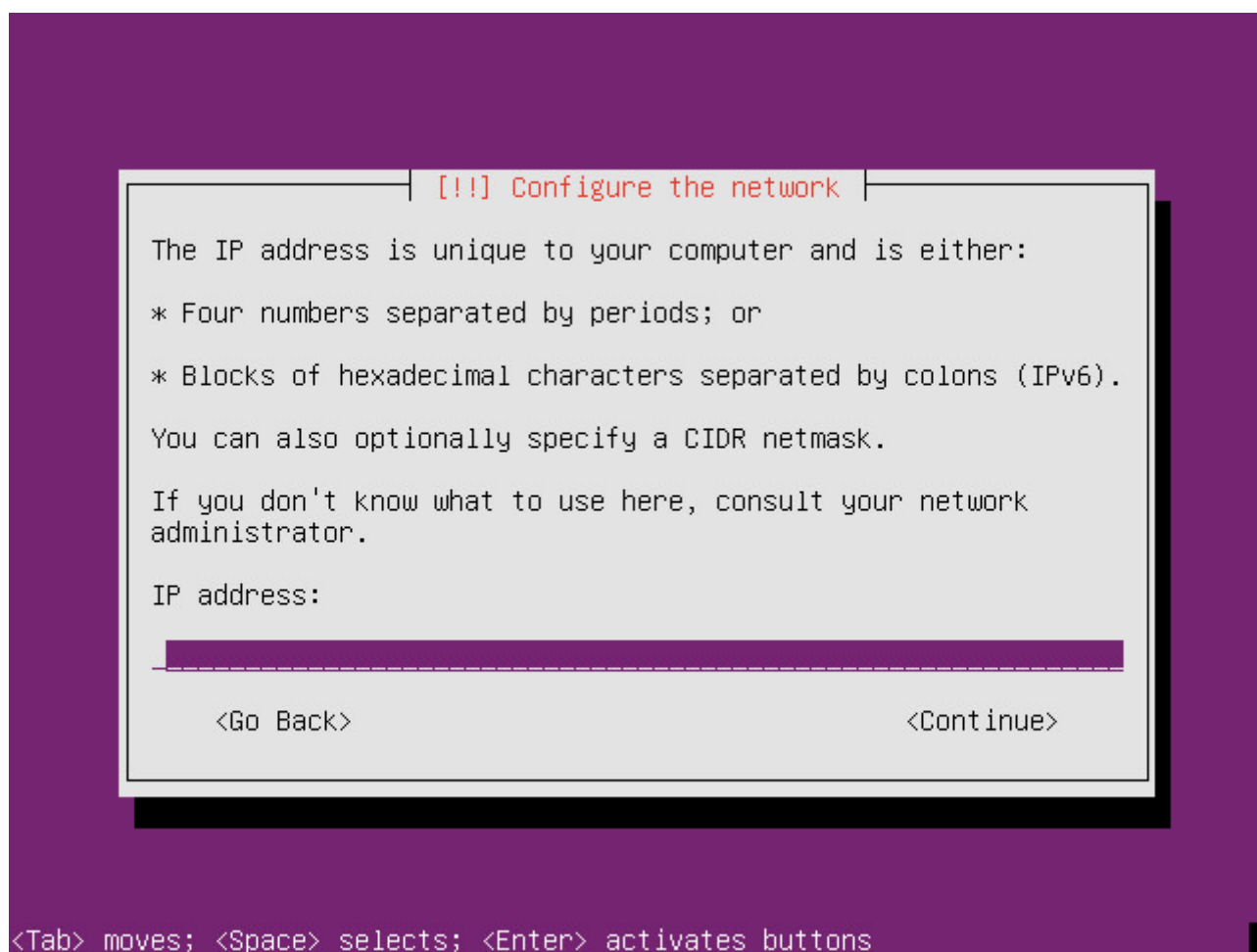


Рисунок 2 – Установка IP-адреса

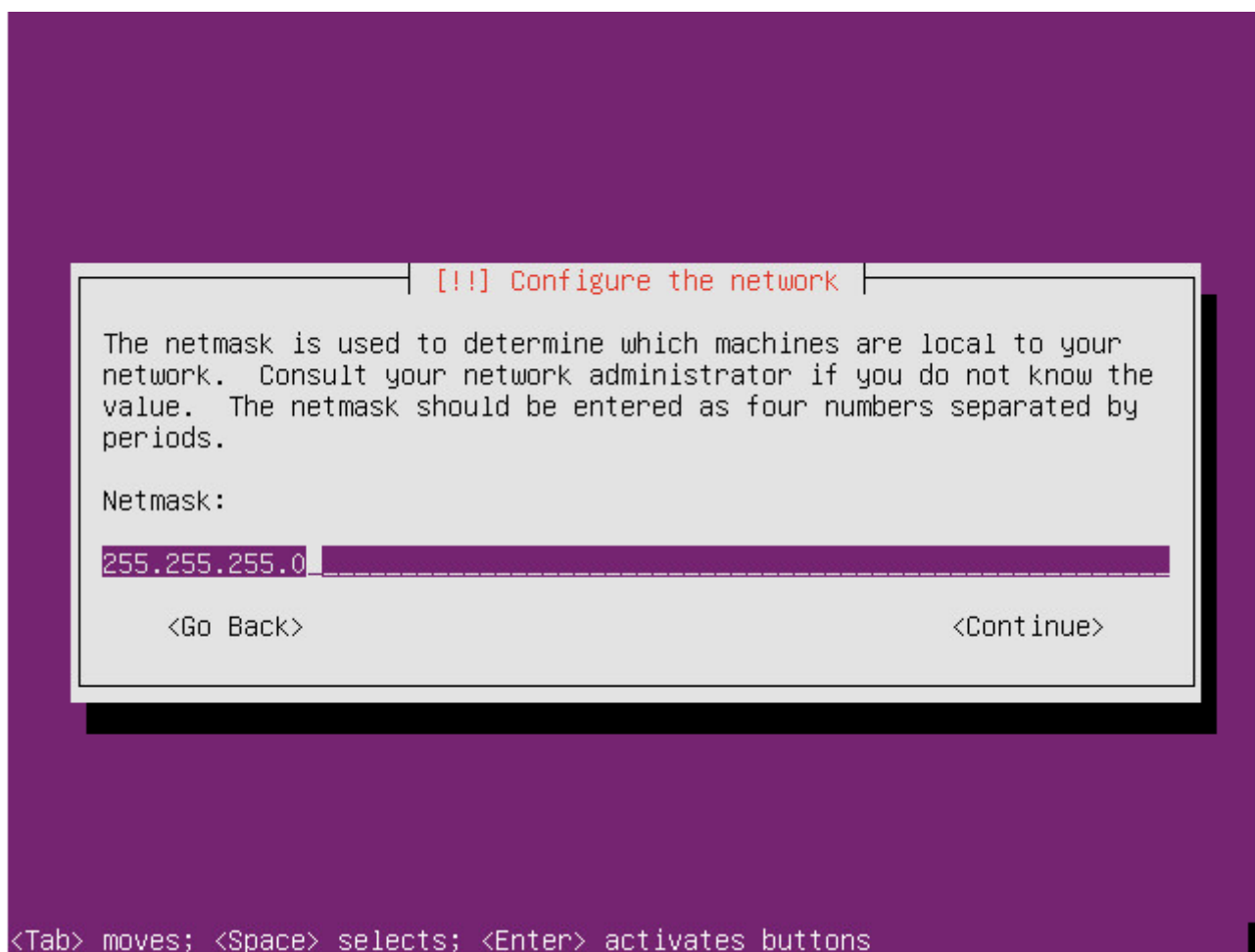


Рисунок 3 – Установка маски сети

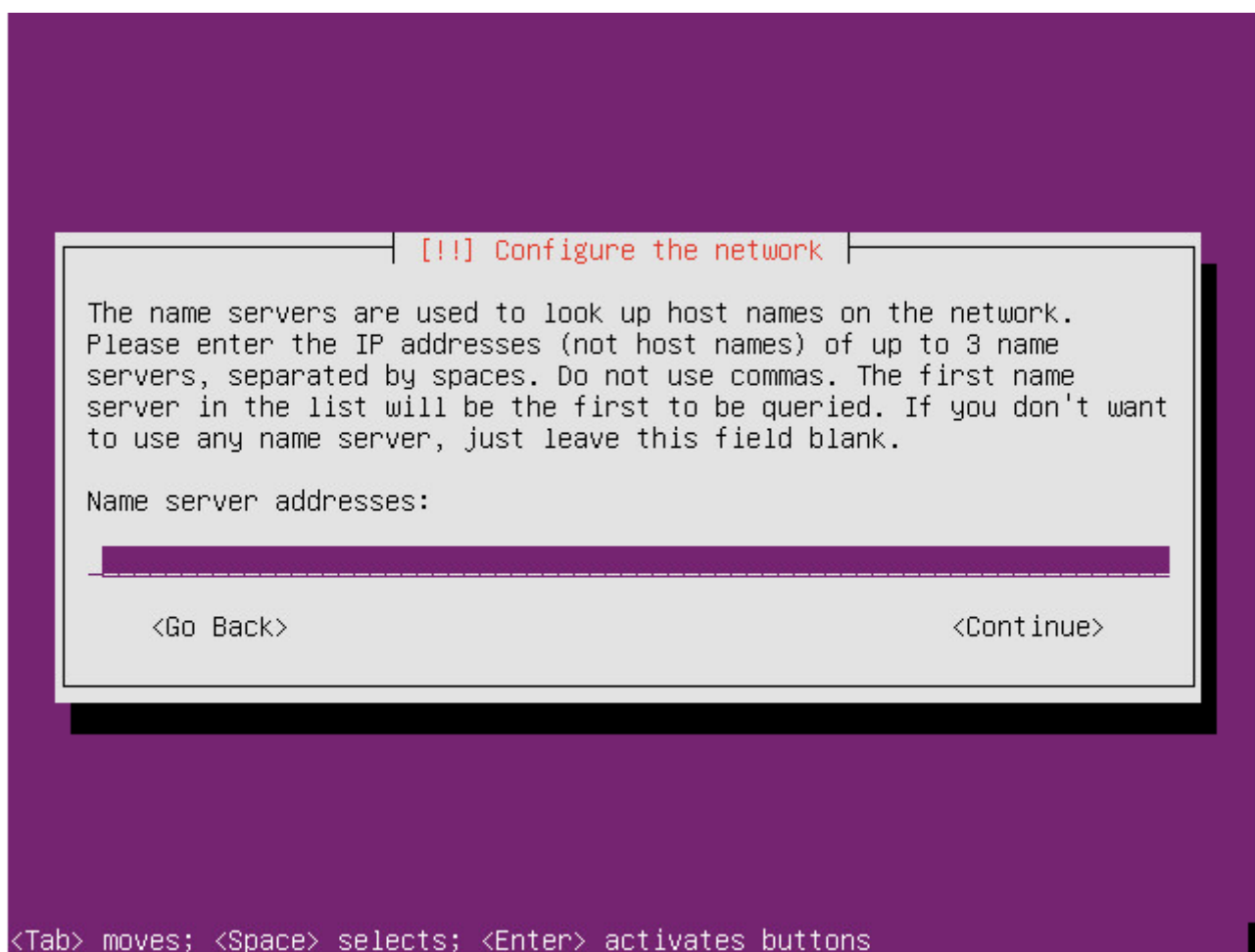


Рисунок 4 – Настройка адреса сервера DNS

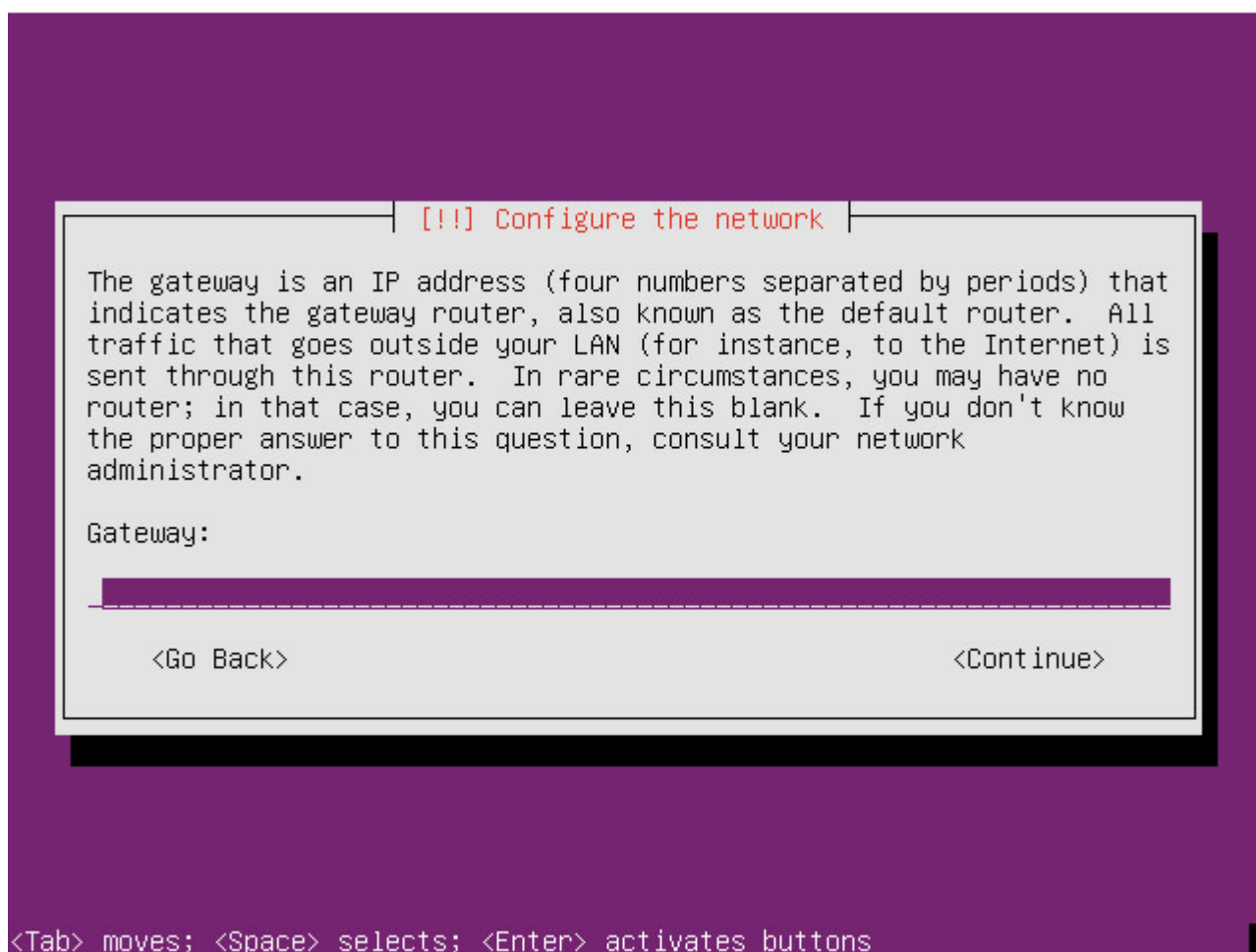


Рисунок 5 – Настройка шлюза по умолчанию

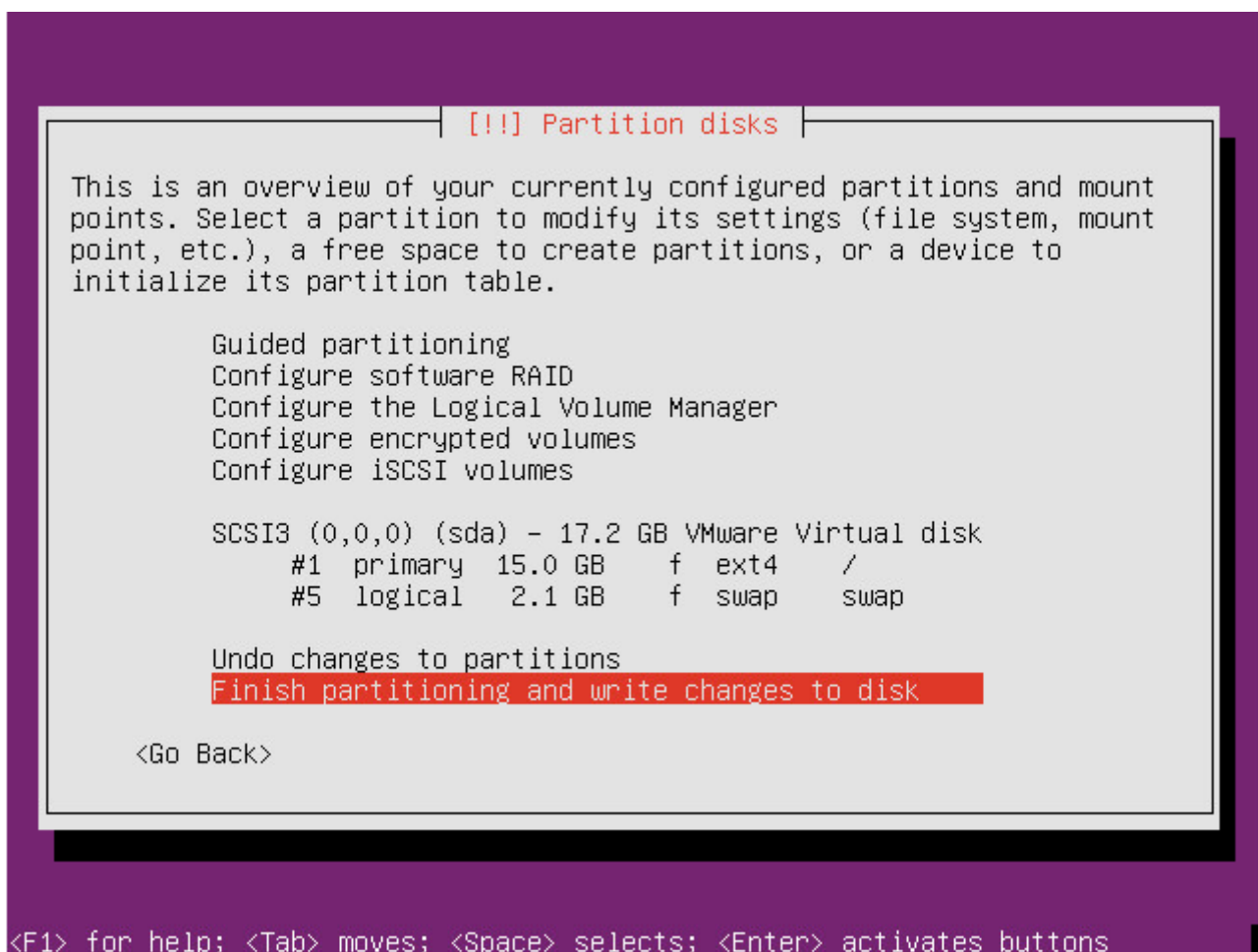


Рисунок 6 – Просмотр таблицы разделов жесткого диска

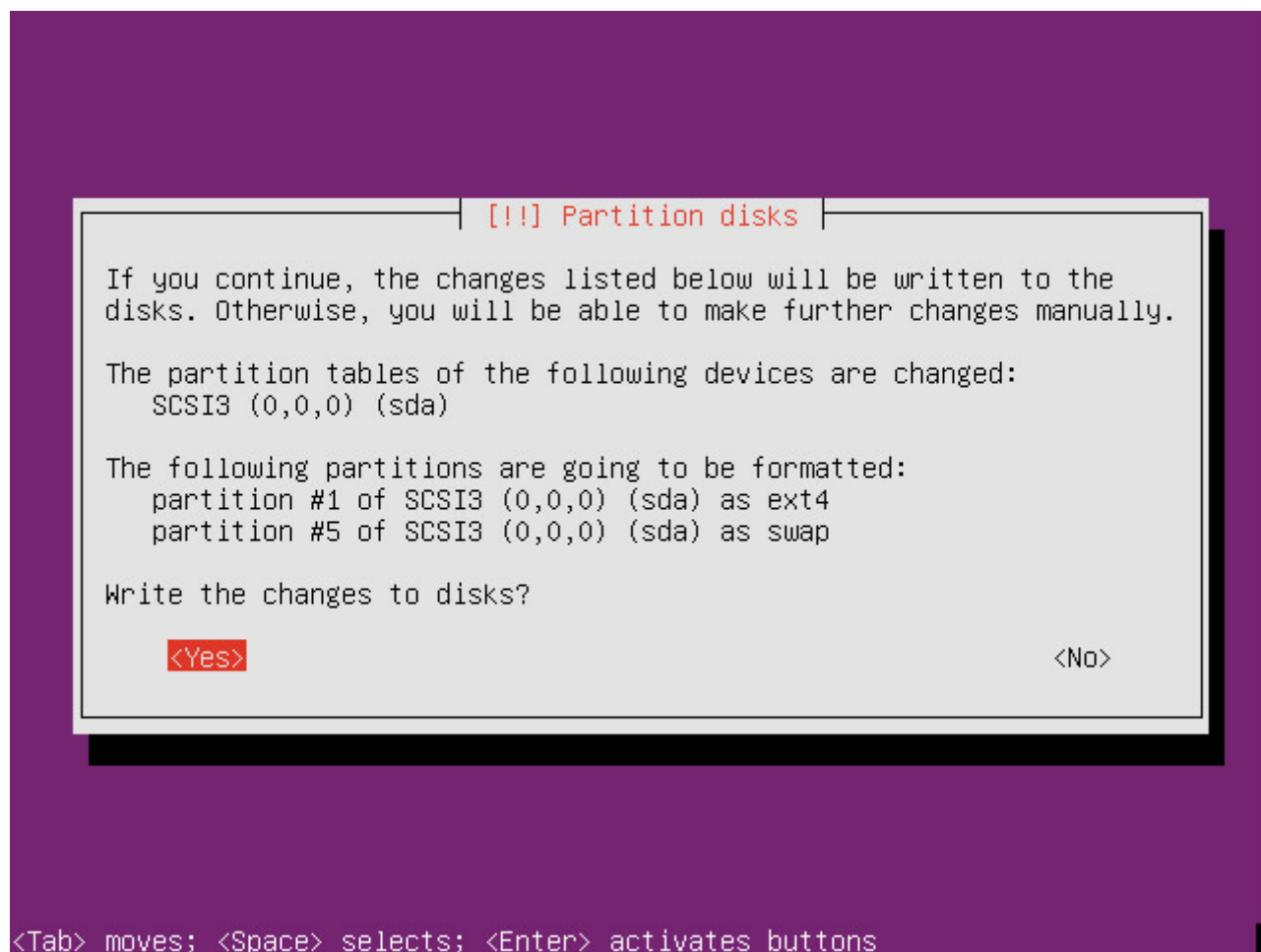


Рисунок 7 – Подтверждение выбора таблицы разделов жесткого диска

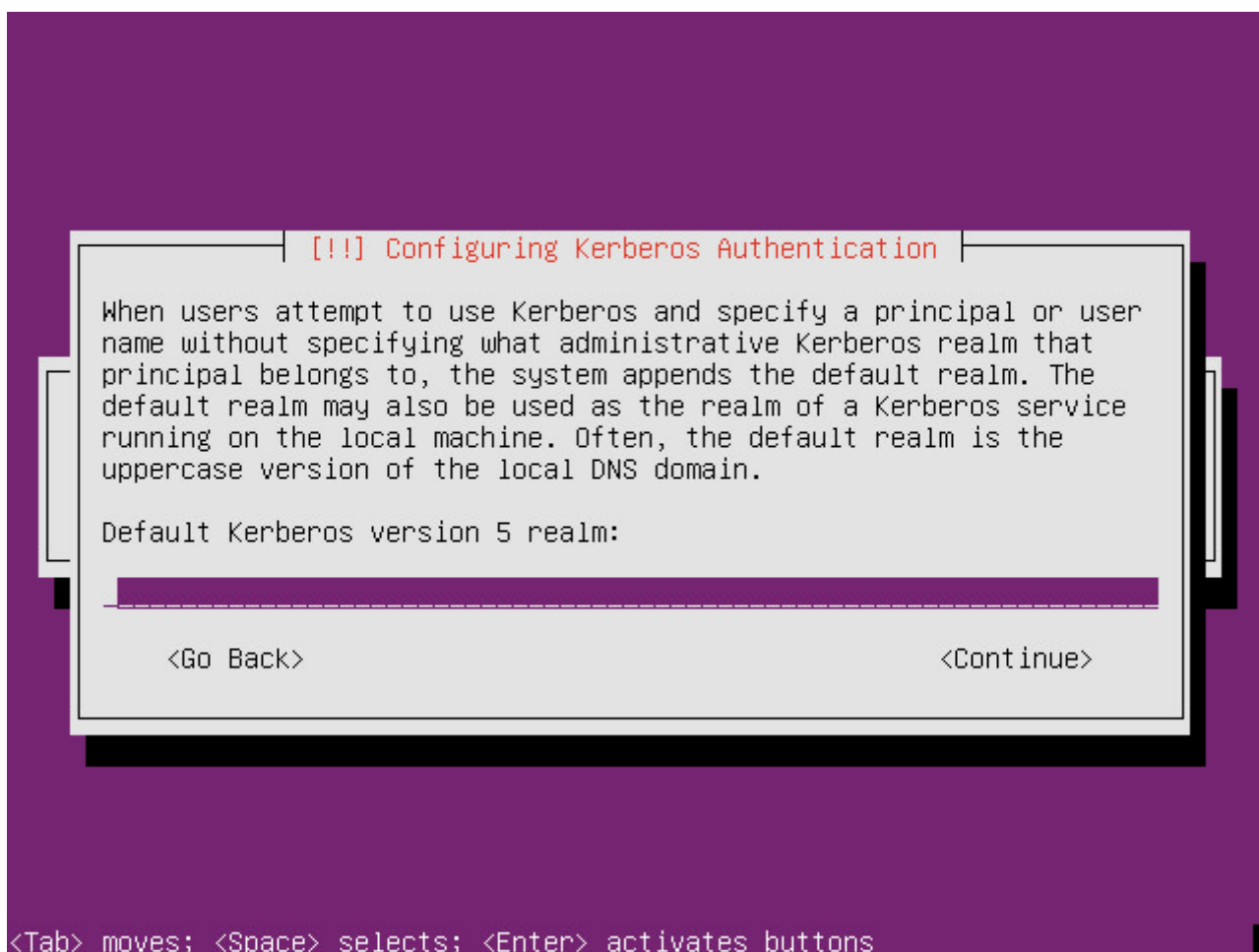


Рисунок 8 – Настройка области безопасности

После завершения установки дистрибутива сервер безопасности должен быть перезагружен.

3.1.2. Настройка сервера безопасности

После успешной установки ПО «TIONIX VDI Security» в роли «Сервер безопасности» и перезагрузки сервера безопасности на консоли сервера появляется приглашение.

Необходимо авторизоваться на сервере под следующей учетной записью:

```
login: user
```

```
password: 2
```

После авторизации необходимо выполнить в консоли сервера команды:

```
cd /opt/tionix-dist
```

```
sudo ./install_simplified server_IP_address
```

Где *server_IP_address* это IP-адрес сервера безопасности.

Указанные команды запускают сценарий настройки сервера безопасности.

После запуска сценарий настройки сервера безопасности предложит задать пароль администратора сервера СУБД ElasticSearch, который

После установки пароля администратора сервера СУБД ElasticSearch необходимо следовать указаниям мастера установки. Все значения рекомендуется оставлять теми, которые предложены по умолчанию.

3.2. Терминал

Необходимость в установке ПО «TIONIX VDI Security» в роли «Терминал» может отсутствовать, если в качестве терминала используются специализированные устройства с заранее установленным ПО «TIONIX VDI Security» в роли «Терминал». В остальных случаях установка заключается в инсталляции и настройке специализированного загрузчика (специализированной операционной системы)

3.2.1. Установка загрузчика

Для установки загрузчика необходимо подключить к виртуальному или физическому персональному компьютеру (ПК) носитель дистрибутива, на который записан образ диска *firmware_terminal_installer.iso*, и настроить ПК на загрузку с указанного носителя.

После загрузки дистрибутива необходимо следовать указаниям мастера установки. Все значения, за исключением сетевых адресов и имен, рекомендуется оставлять теми, которые предложены по умолчанию.

3.2.2. Настройка терминала

После успешной загрузки терминальной ОС, на консоли появляется окно конфигурации с двумя вкладками, показанными на рисунках ниже (Рисунок 1 и Рисунок 2). В качестве сетевого адреса балансирующего необходимо указать IP-адрес сервера безопасности. Если в сети, в которой установлен терминал, не используется сервер DHCP, необходимо вручную настроить сетевую конфигурацию, заполнив поля, показанные на рисунке (Рисунок 2).

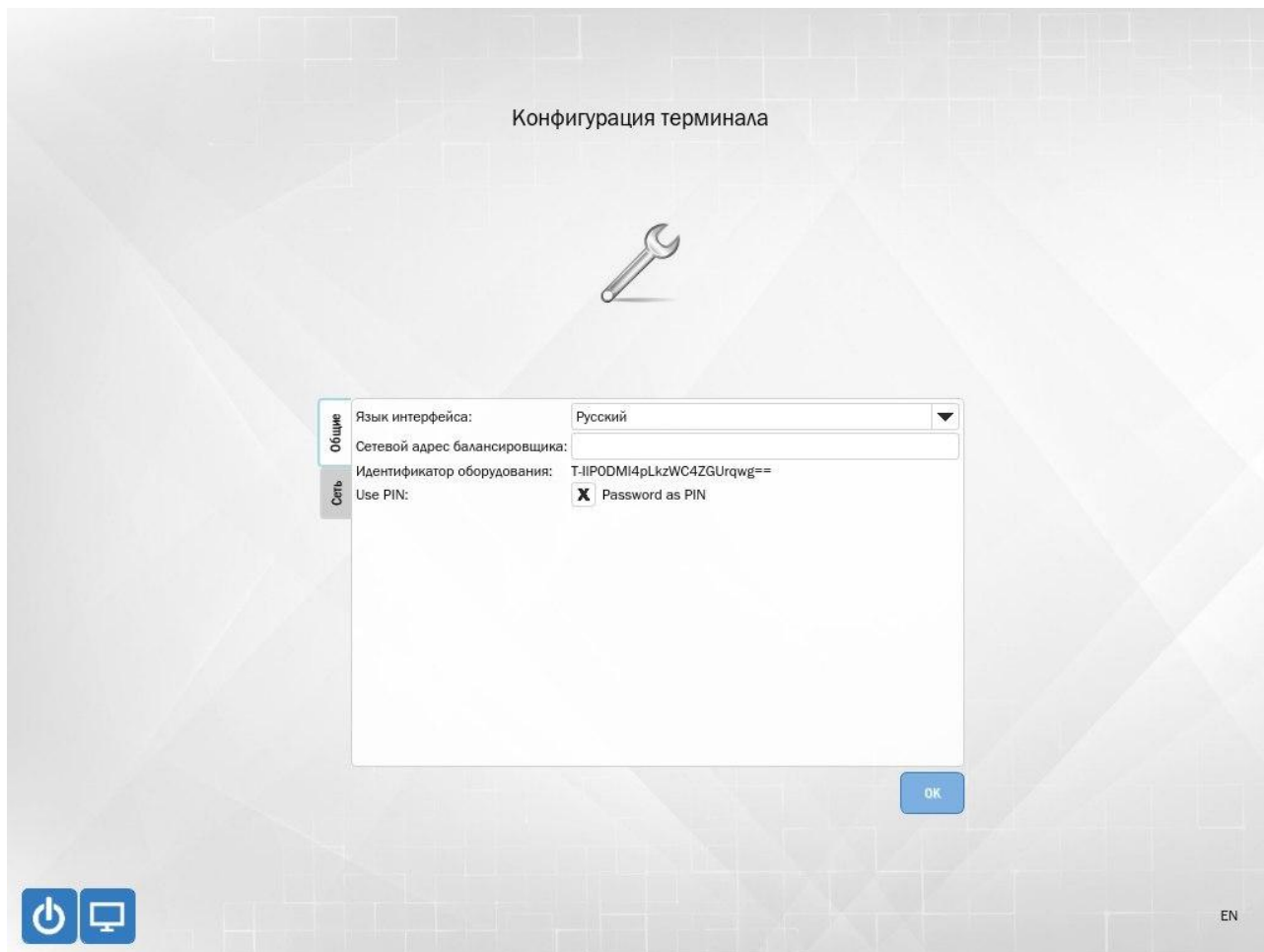


Рисунок 9 – Конфигурация терминала - вкладка общих настроек

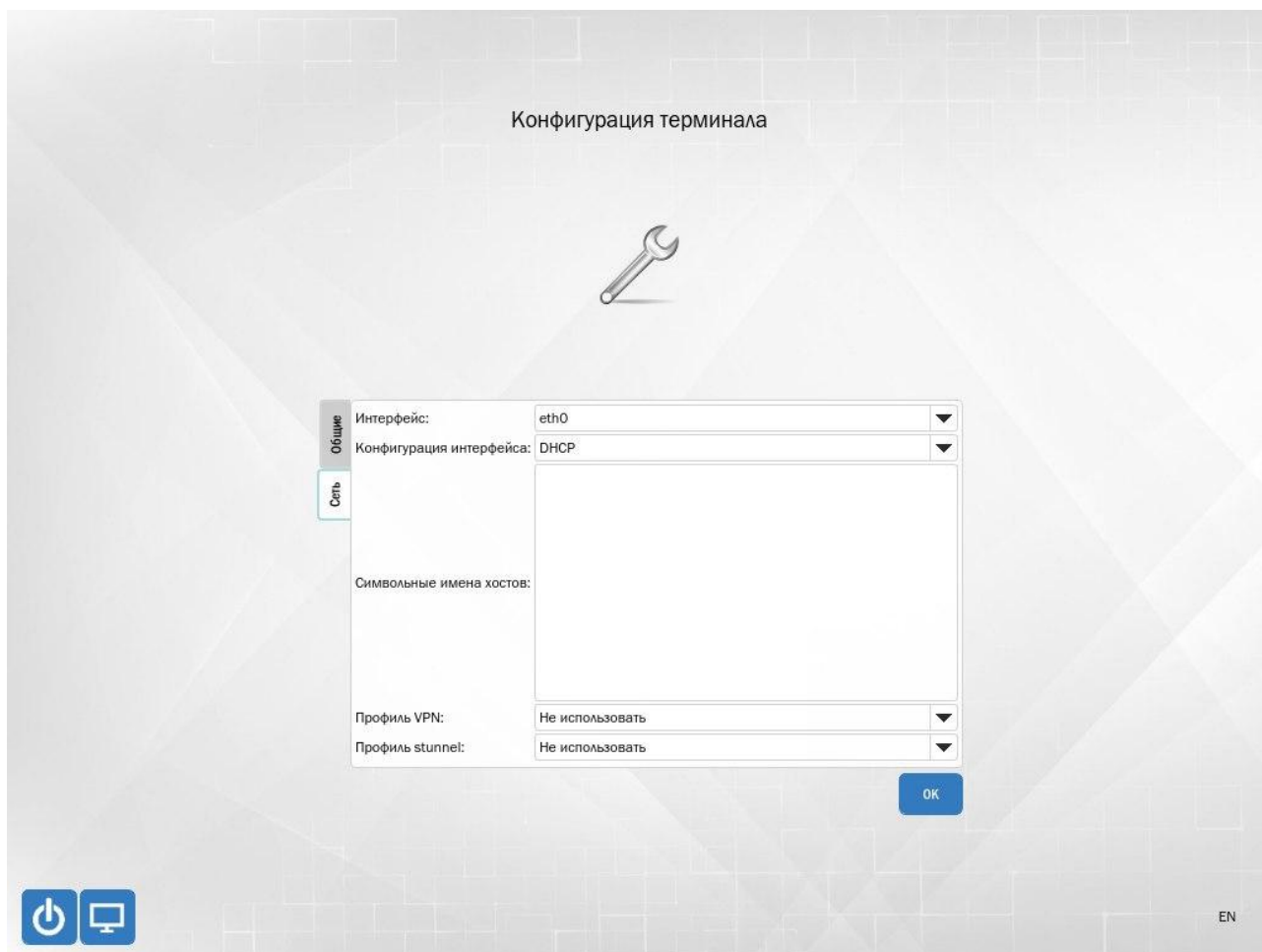


Рисунок 2 – Конфигурация терминала - вкладка сетевых настроек

После завершения конфигурации терминала необходимо нажать на кнопку «ОК». В случае, если настройки сделаны правильно, терминал подключится к серверу.

Далее на консоли терминала появляется приглашение, показанное на рисунке ниже (Рисунок 3).

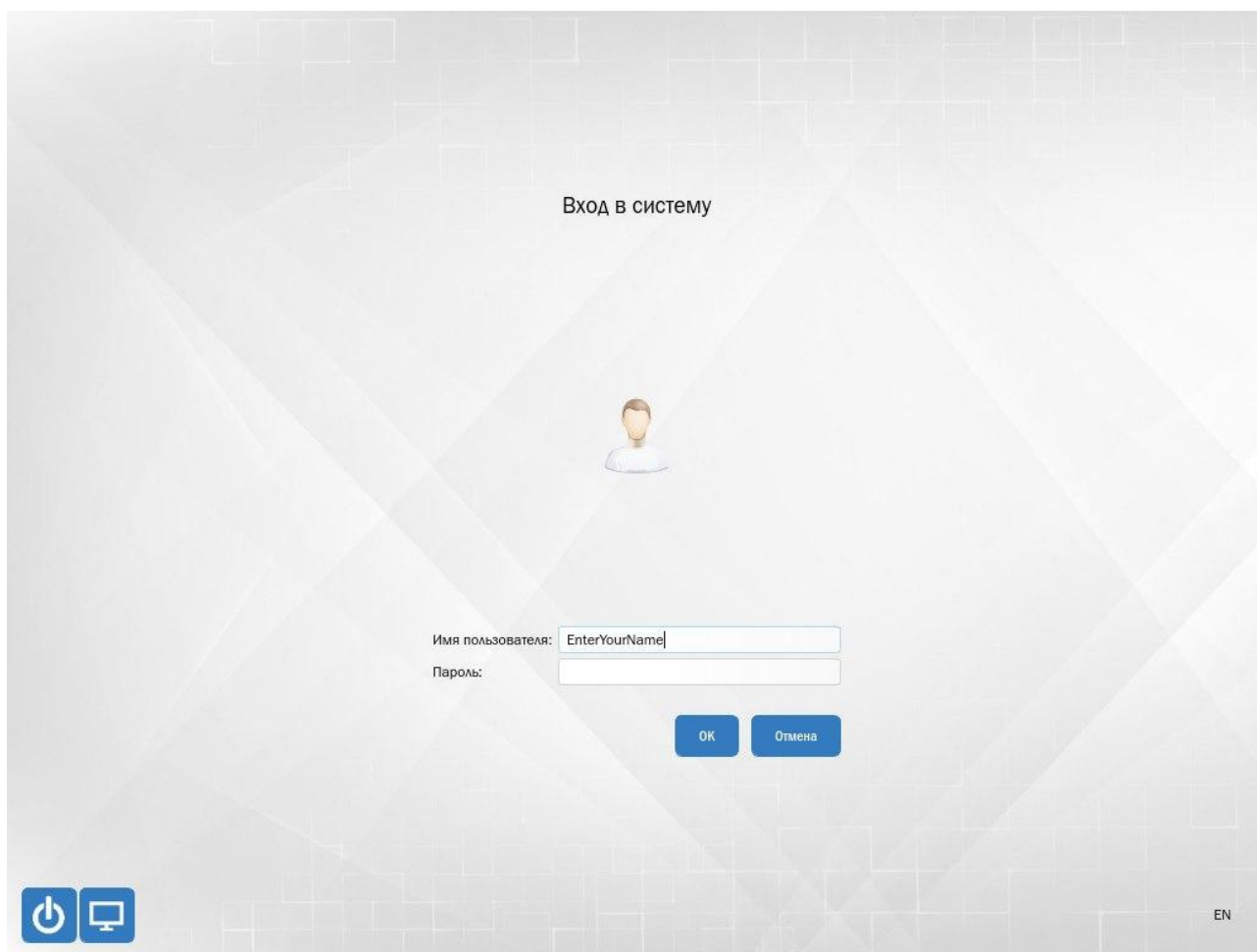


Рисунок 3 – Консоль терминала после подключения к серверу безопасности