TERMIDESK

ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ

СЛЕТ.10001-01 91 03

Версия 4.3.1. Выпуск от декабря 2023

Компонент «Виртуальный модуль Termidesk»

ОГЛАВЛЕНИЕ

1 . ОБЩИЕ СВЕДЕНИЯ

1.1 . О документе

Настоящий документ является инструкцией по использованию компонента «Виртуальный модуль Termidesk» программного комплекса«Диспетчер подключений виртуальных рабочих мест Termidesk» (далее - Termidesk). Документ предназначен для администраторов системы и сети.
В документе приведено назначение, настройка и использование компонента «Виртуальный модуль Termidesk». Для того чтобы получить информацию по доступным действиям в веб-интерфейсе Termidesk, необходимо обратиться к документам СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса» и СЛЕТ.10001-01 90 03 «Руководство администратора. Графический интерфейс управления программным комплексом».

1.2 . Назначение компонента «Виртуальный модуль Termidesk»

Компонент «Виртуальный модуль Termidesk» (далее - ВМТ) представляет собой образ виртуальной машины (ВМ) (или диска ВМ) с предварительно установленной и настроенной операционной системой (ОС) и набором программного обеспечения (ПО), необходимого для эксплуатации Termidesk.
ВМТ предоставляет фиксированный набор функций для быстрого развертывания и использования Termidesk с выполнением минимума действий по его настройке, что существенно упрощает ввод в эксплуатацию программного комплекса. Каждый экземпляр ВМТ может быть установлен с различным набором функций Termidesk:

- экземпляр, реализующий функции компонента «Универсальный диспетчер»;
- экземпляр, реализующий функции компонента «Шлюз»;
- экземпляр, реализующий функции компонента «Менеджер рабочих мест».

Состав ВМТ:

- ОС Astra Linux Special Edition 1.7.5;
- программные пакеты из состава подключенного в ВМТ репозитория Termidesk:
  - `termidesk-vdi`;
  - `termidesk-gateway`;
  - `termidesk-digsig-keys`;
- система управления базами данных Postgres-11;
- брокер сообщений RabbitMQ-server;
- веб-сервер Apache;
- служба ведения журналов syslog-ng;
- ПО обеспечения высокой доступности узлов и служб keepalived;
- инструмент организации списка сетей ipset.

При первичной настройке ВМТ выбирается один из двух режимов защищенности ОС Astra Linux Special Edition: «Базовый» («Орел») или «Усиленный» («Воронеж»). Режим защищенности определяет, какие механизмы безопасности ОС будут активированы. Для режима «Базовый» специальные механизмы безопасности ОС не активируются.

Для режима «Усиленный» активируются следующие специальные механизмы безопасности ОС Astra Linux Special Edition:

- режим замкнутой программной среды (`astra-digsig-control`);
- механизм контроля целостности в ядре (`astra-mic-control`);
- режим мандатного контроля целостности файловой системы (`set-fs-ilev`);
- режим безопасного удаления файлов (`astra-secdel-control`);
- блокировка загрузки неиспользуемых модулей ядра (`astra-modban-lock`);
- отключение отображения меню загрузчика GRUB (`astra-nobootmenu-control`).

1.3 . Комплект поставки

ВМТ распространяется в следующих форматах:

- для гипервизоров QEMU/KVM:
  - диск `image.qcow2`;
  - пакет открытого виртуального устройства (Open Virtual Appliance, OVA), представленный файлом `termidesk-virtual-appliance_<версия>_ovirt.ova`.
- для платформы виртуализации VMware:
  - формат открытой виртуализации (Open Virtualization Format, OVF), представленный файлами:
    - `termidesk.vmx`;
    - `image.vmdk`;
    - `termidesk.ovf`;
    - `termidesk.mf`;
  - пакет открытого виртуального устройства, представленный файлом `termidesk-virtual-appliance_<версия>_vmware.ova`.

В образе ВМТ используются разные наборы инструментов гостевой ОС для указанных платформ.

1.4 . Требования к уровню подготовки персонала

Требования к уровню подготовки и составу персонала совпадают с требованиями, предъявляемыми для эксплуатации Termidesk. Для штатной эксплуатации требуется:

- системный администратор;
- специалист по техническому обслуживанию.

Системный администратор должен иметь опыт работы с платформами виртуализации и администрирования серверов с ОС Astra Linux Special Edition 1.7.

Основными обязанностями системного администратора являются:

- установка, настройка и мониторинг работоспособности Termidesk;
- регламентные работы;
- восстановление работоспособности Termidesk после устранения неисправностей комплекса технических средств.

Специалист по техническому обслуживанию должен иметь опыт работы с ОС Astra Linux Special Edition 1.7, знать и понимать принципы работы сетей передачи данных, а также владеть базовыми знаниями по обслуживанию комплекса технических средств.

Основными обязанностями специалиста по техническому обслуживанию являются:

- настройка, модернизация и проверка состояния комплекса технических средств;
- диагностика типовых неисправностей комплекса технических средств;
- настройка сетевых подключений.

1.5 . Типографские соглашения

В настоящем документе приняты следующие типографские соглашения:

- моноширинный шрифт – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

2 . ПОДГОТОВКА К РАБОТЕ

2.1 . Получение образов ВМТ

ВМТ доступен из `iso`-образа Termidesk, получить который можно двумя способами:

- заполнив форму запроса на сайте Termidesk: `https://termidesk.ru/support/#request-support`;
- через личный кабинет: `https://lk-new.astralinux.ru/`.

2.2 . Порядок загрузки ВМТ

Для загрузки ВМТ на платформу виртуализации нужно:

- выполнить импорт образа ВМТ формата `.ovf` на платформу виртуализации. Для импорта может также использоваться образ формата `.ova`;

> ⚠ Если платформа виртуализации не поддерживает импорт из образов формата `.ovf` или `.ova`, необходимо создать ВМ на такой платформе вручную и подключить диск формата `.vmdk` (`qcow2` для ПК СВ Брест) из комплекта поставки.

- дождаться окончания импорта и создания ВМ;
- выполнить запуск ВМ;

> ⚠ Если ВМ не запускается, необходимо проверить, что в свойствах ВМ выбраны корректные параметры: тип ОС - «Linux», версия - «Other Linux (64-bit)», сеть - один из типов адаптера «Intel 1000».

- выбрать в меню GRUB (см. Рисунок 1) пункт «AstraLinux GNU/Linux» (по умолчанию) и нажать клавишу **<Enter>**;
- выполнить первоначальную настройку Termidesk в соответствии с подразделом **Первичная настройка ВМТ**.

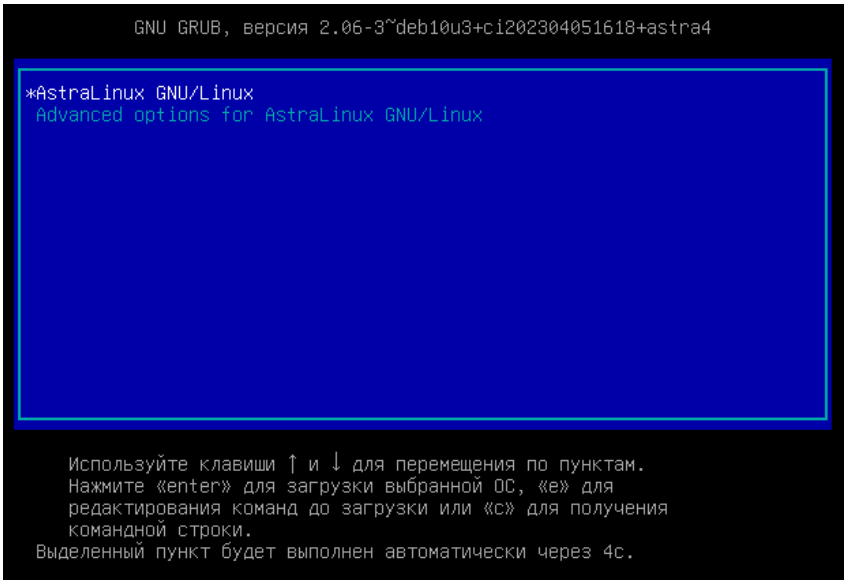

Рисунок 1 – Меню GRUB

3 . ПЕРВИЧНАЯ НАСТРОЙКА

3.1 . Порядок развертывания ВМТ

Общий порядок развертывания ВМТ должен выполняться по следующим правилам:

- ВМТ должен устанавливаться в распределенном варианте;
- первый экземпляр ВМТ устанавливается с ролью «Планировщик». При этом:
  - при необходимости можно установить второй узел ВМТ с этой же ролью для обеспечения высокой доступности (настройку высокой доступности нужно выполнить отдельно). В этом случае первый экземпляр с ролью «Планировщик» должен быть установлен с указанием типа ноды «Master». Для второго экземпляра «Планировщика» нужно выбирать тип ноды «Slave». Экземпляры должны быть синхронизированы (см. подразделы **Экспорт параметров Termidesk** и **Импорт параметров Termidesk**);
  - если первый ВМТ с ролью «Планировщик» устанавливался с инициализацией локальной базы данных (БД), то при первичной настройке второго «Планировщика» следует указать подключение к БД первого экземпляра;
- следующий экземпляр ВМТ устанавливается с ролью «Брокер». При этом:
  - нужно указать тип ноды «Slave» и выполнить синхронизацию параметров с «Планировщиком» (см. подразделы **Экспорт параметров Termidesk** и **Импорт параметров Termidesk**);
  - если ВМТ с ролью «Планировщик» устанавливался с инициализацией локальной БД, то при первичной настройке «Брокера» следует указать подключение к БД «Планировщика»;
- последним устанавливается экземпляр ВМТ с ролью «Шлюз». При этом:
  - нужно указать тип ноды «Slave» и выполнить синхронизацию параметров с «Планировщиком» (см. подразделы **Экспорт параметров Termidesk** и **Импорт параметров Termidesk**).

3.2 . Первичная настройка ВМТ с типом ноды «master»

Первичная настройка выполняется при первом включении ВМ с подключенным образом ВМТ.

В процессе первичной настройки нужно выполнить следующее:

- ознакомиться с лицензионным соглашением (см. Рисунок 2) и нажать экранную кнопку **[OK]**;

> Переключение между пунктами меню выполняется клавишей **<TAB>**. Подтверждение выбора выполняется клавишами **<ENTER>** или **< SPACE>**.

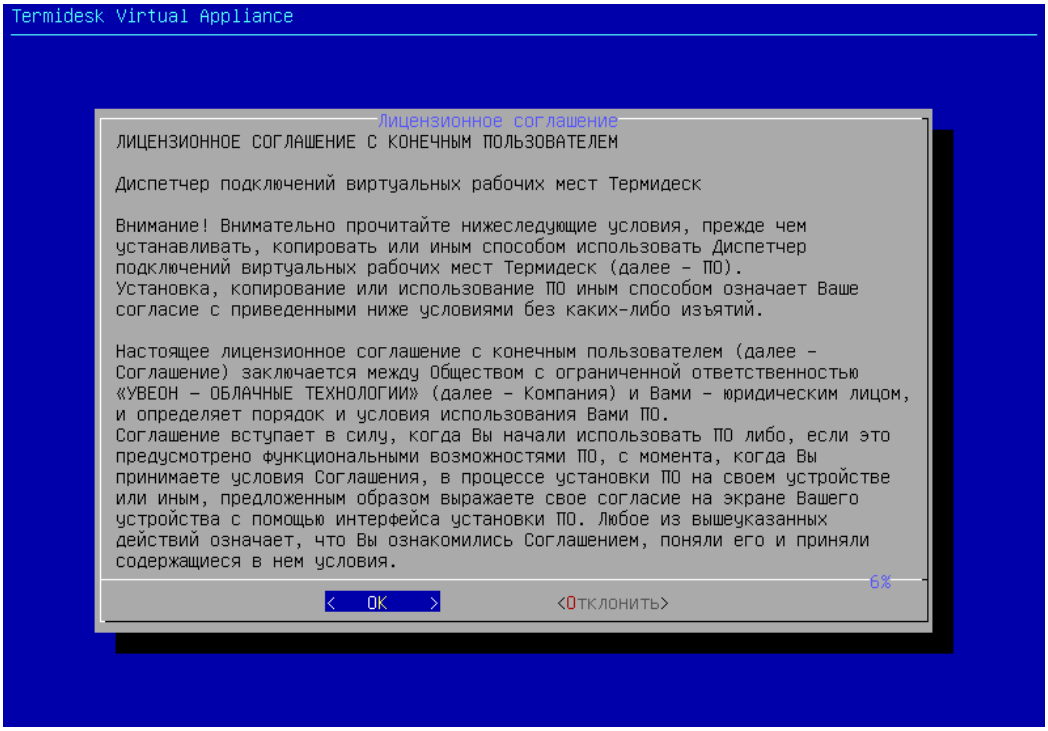

Рисунок 2 – Лицензионное соглашение

- выбрать режим защищенности ОС (см. Рисунок 3). Режим защищенности определяет, какие механизмы безопасности ОС будут активированы. Для режима «basic» («Базовый») специальные механизмы безопасности ОС не активируются;

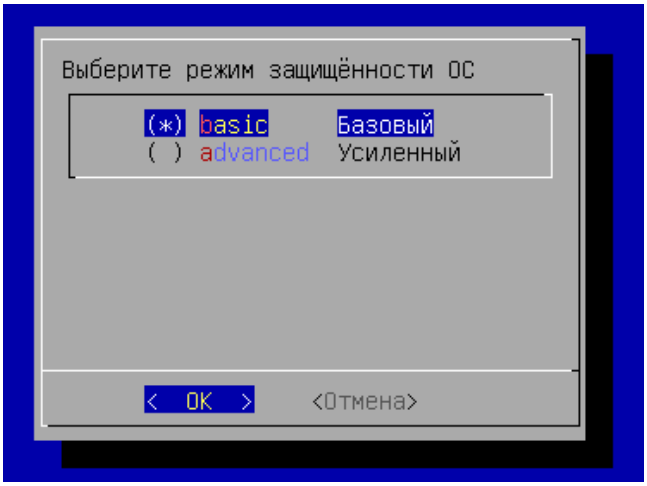

Рисунок 3 – Выбор режима защищенности ОС

- согласиться с перезапуском системы для применения режима защищенности ОС;
- после перезапуска системы будет показано информационное сообщение (см. Рисунок 4) о настроенном режиме защищенности ОС и активированных механизмах (см. Рисунок 5);

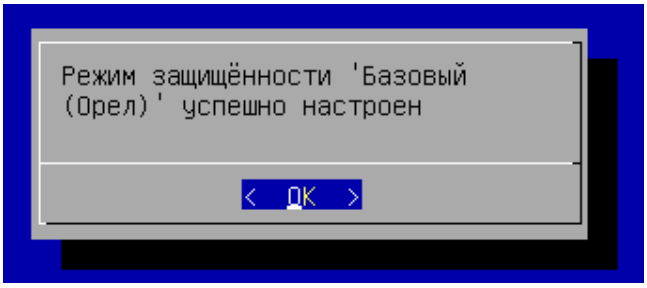

Рисунок 4 – Сообщение о настроенном режиме защищенности

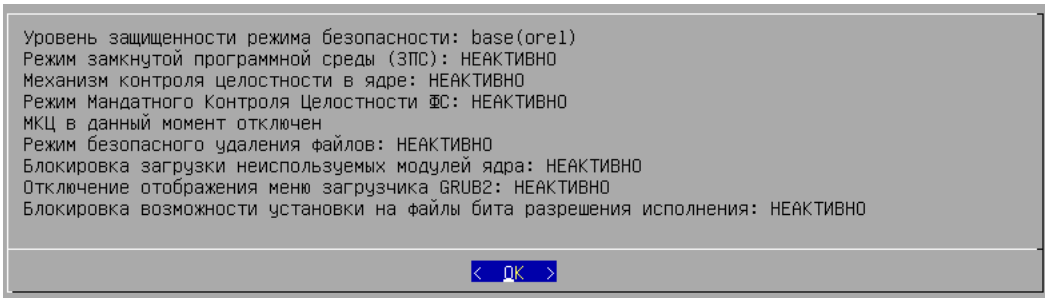

Рисунок 5 – Информационное сообщение об активированных механизмах безопасности на примере режима «Базовый»

- заполнить имя хоста (см. Рисунок 6) (hostname), которое будет использоваться для идентификации устройства в сети. Необходимо учесть, что указанный hostname, в свою очередь, должен являться полным доменным именем (FQDN), если BMT используется в домене. Указанный hostame будет использован для настройки веб-сервера apache;

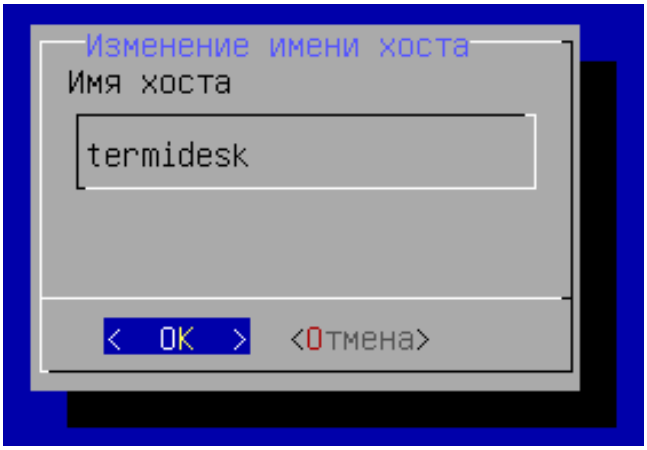

Рисунок 6 – Ввод имени хоста

- после применения настройки будет показано информационное сообщение (см. Рисунок 7);

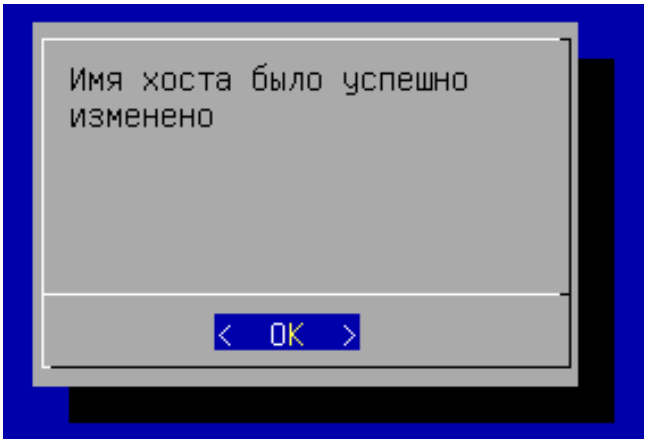

Рисунок 7 – Информационное сообщение об успешном изменении имени хоста

- выбрать сетевые интерфейсы (см. Рисунок 8) при помощи клавиши **<SPACE>**;

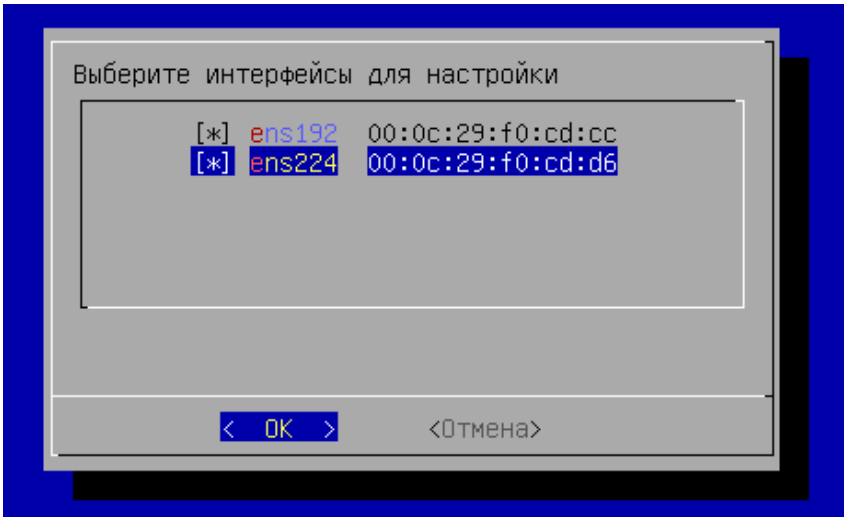

Рисунок 8 – Выбор сетевого интерфейса

- далее указать сетевые настройки: IP-адрес, маску сети, IP-адрес шлюза и IP-адреса DNS-серверов, выполняющих разрешение сетевых имен в IP-адреса. Настройки следует выполнить для каждого интерфейса. По умолчанию предложено задать статические настройки (см. Рисунок 9), однако при помощи клавиши **<TAB>** можно перейти к меню «DHCP», нажать клавишу **<ENTER>** и получить сетевые параметры от DHCP-сервера;

⚠ Все указанные IP-адреса должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре организации.

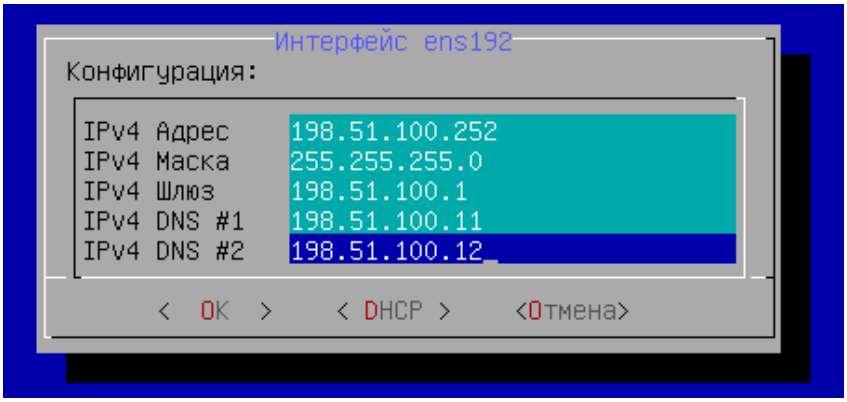

Рисунок 9 – Задание статических сетевых настроек

- изучить заданные параметры (см. Рисунок 10) и подтвердить изменение сетевых настроек, нажав экранную кнопку **[Да]**;

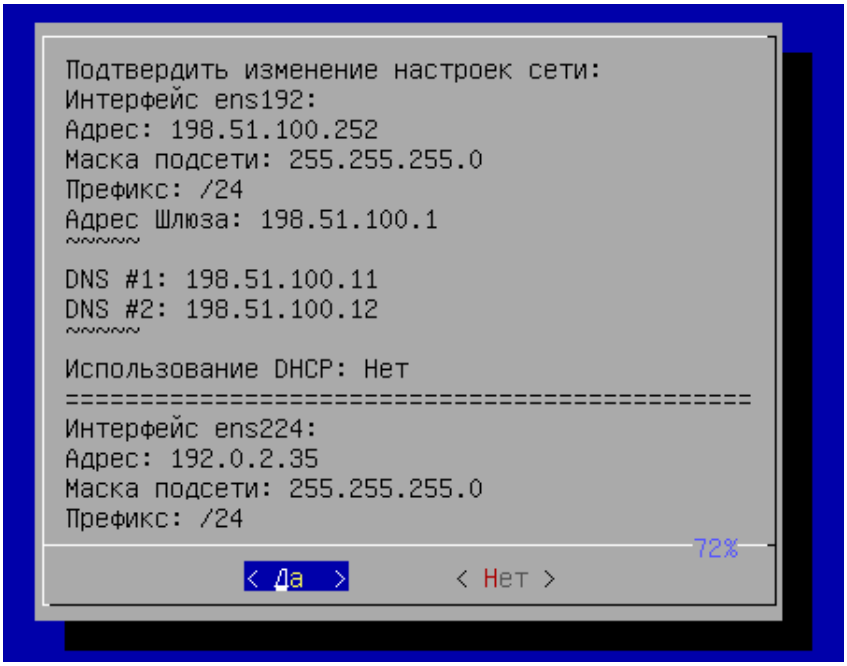

Рисунок 10 – Подтверждение сетевых настроек

- после применения настроек будет показано информационное сообщение (см. Рисунок 11);

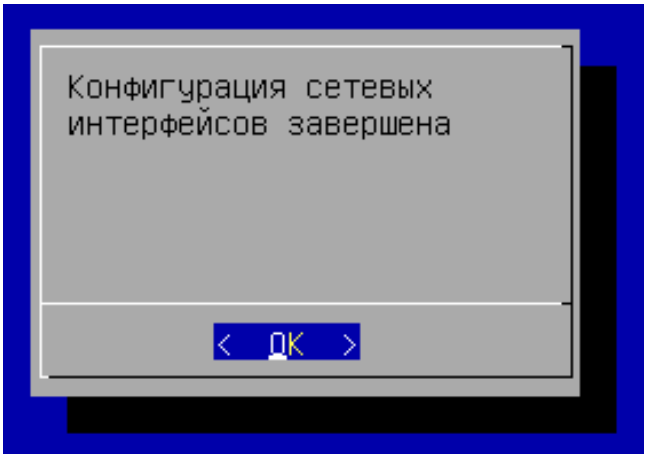

Рисунок 11 – Информационное сообщение об успешной конфигурации сетевых интерфейсов

- далее необходимо выбрать тип ноды BMT (см. Рисунок 12) «master» - нода обладает собственным набором ключей, используемыми в Termidesk для проверок пересылаемых между компонентами данных и состояния API. Этот тип ноды автоматически устанавливается с ролью «Планировщик»;

ⓘ Для роли «Планировщик» активируются службы `termidesk-taskman`, `termidesk-celery-beat`, `termidesk-celery-worker`. Также будет инициализирован брокер сообщений RabbitMQ-server и выполнен запуск службы `rabbitmq-server`.

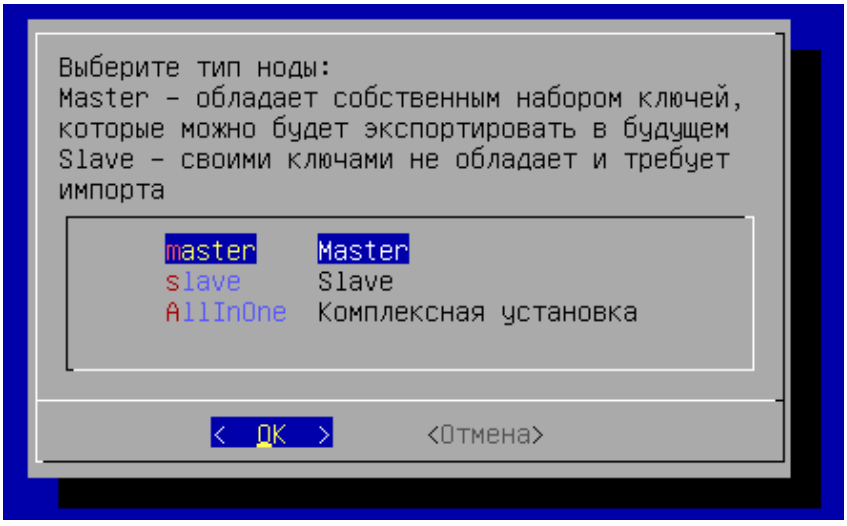

Рисунок 12 – Выбор типа устанавливаемой ноды BMT

- затем следует сконфигурировать использование SSL-сертификатов для веб-сервера apache. Эти параметры можно указать позже, тогда нужно выбрать экранную кнопку **[Отмена]**. Для конфигурирования указать (см. Рисунок 13):
  - IP-адрес хоста, на котором расположены сертификаты и ключ. У BMT должен быть сетевой доступ к хосту;

- порт подключения;
- полный путь к файлу закрытого ключа формата `.key`;
- полный путь к файлу сертификата формата `.pem`;
- полный путь к файлу проверки цепочки сертификатов формата `.crt`;

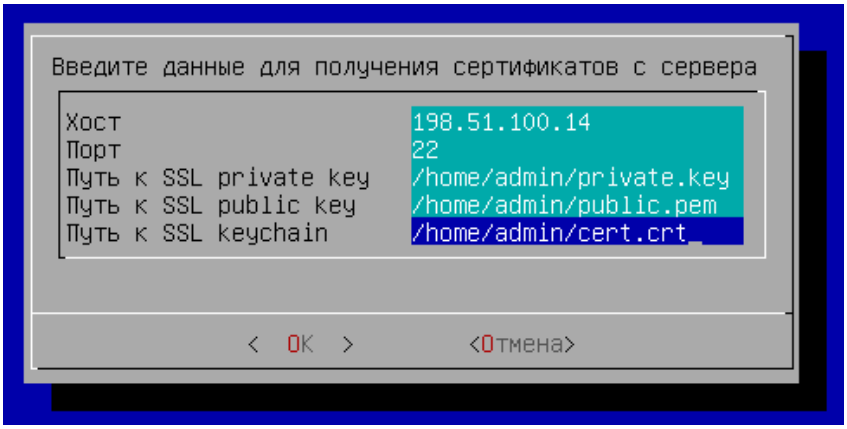

Рисунок 13 – Конфигурация сертификатов

- в следующем окне (см. Рисунок 14) заполнить имя пользователя и пароль для подключения к указанному на предыдущем шаге хосту. Для задания пароля переключиться на строку «Пароль» при помощи клавиши **<↓>** (**<СТРЕЛКА ВНИЗ>**) и ввести его, затем переключиться таким же способом на строку «Повтор пароля» и повторить ввод пароля. Поле «Имя пользователя» при этом изменится на другой цвет, как неактивное в данный момент, ввод пароля отображен не будет. Подтвердить данные, нажав экранную кнопку **[OK]**;

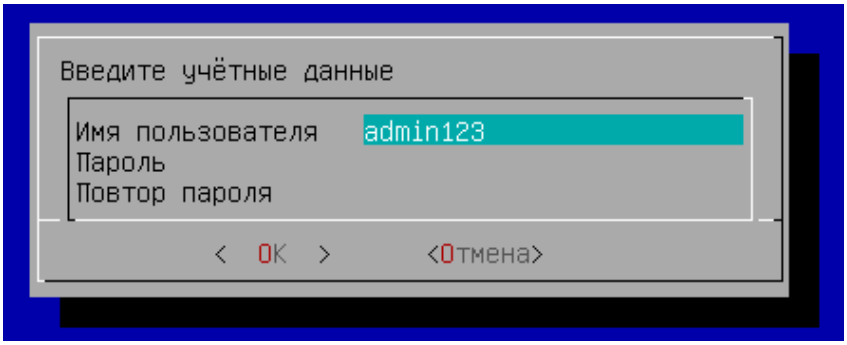

Рисунок 14 – Заполнение учетных данных для доступа

- выбрать тип используемой БД (см. Рисунок 15). При выборе удаленной БД локальная не активируется;

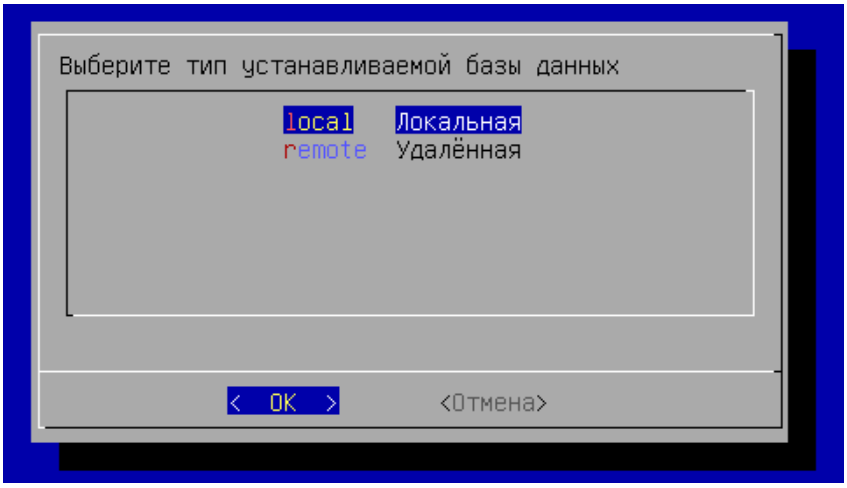

Рисунок 15 – Выбор типа используемой БД

- если была выбрана локальная БД, то нужно указать пароль (см. Рисунок 16) для нее. Пароль будет храниться в преобразованном виде;

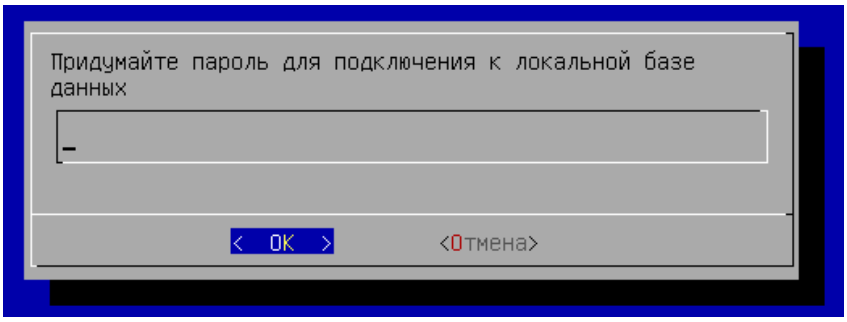

Рисунок 16 – Создание пароля для локальной БД

- если была выбрана удаленная БД, то нужно указать параметры подключения (см. Рисунок 17) к ней. В параметре «хост» должен указываться внешний IP-адрес или FQDN для подключения к БД. Затем выбрать экранную кнопку **[Тест]** для проверки доступа. В случае, если БД с указанными настройками не существует, переход к следующему окну будет невозможен. В случае, если БД с указанными настройками существует, будет повторно отображено окно с параметрами БД, в котором следует нажать экранную кнопку **[OK]**;

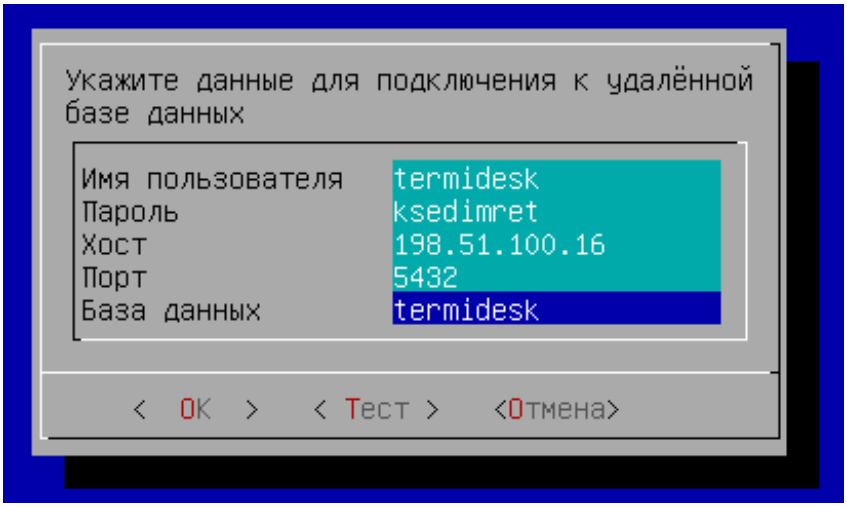

Рисунок 17 – Параметры подключения к удаленной БД

- в следующем окне необходимо указать пароль (см. Рисунок 18) для подключения к RabbitMQ;

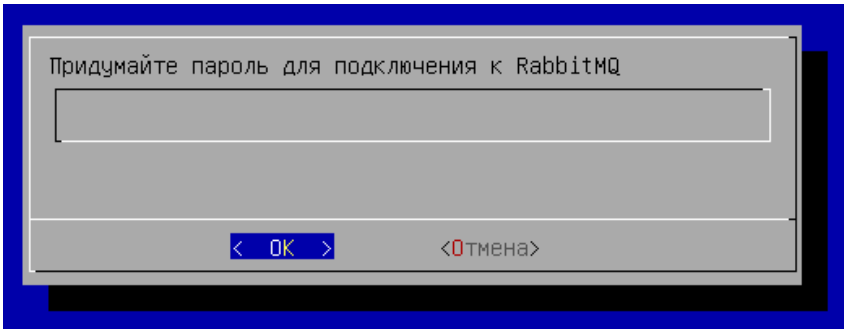

Рисунок 18 – Пароль для подключения к RabbitMQ

- после выполнения настроек изучить заданные параметры и подтвердить настройки выбранной роли, нажав экранную кнопку **[OK]**;
- дождаться успешного применения настроек и вывода сообщения (см. Рисунок 19).

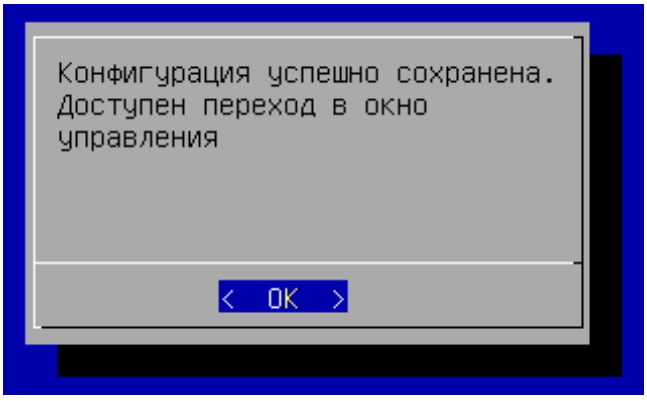

Рисунок 19 – Информационное сообщение об успешном применении конфигурации

После выполнения шагов по первичной настройке произойдет переход в окно управления ВМТ (см. Рисунок 20). Службы Termidesk будут автоматически активированы, перезагрузка не требуется.

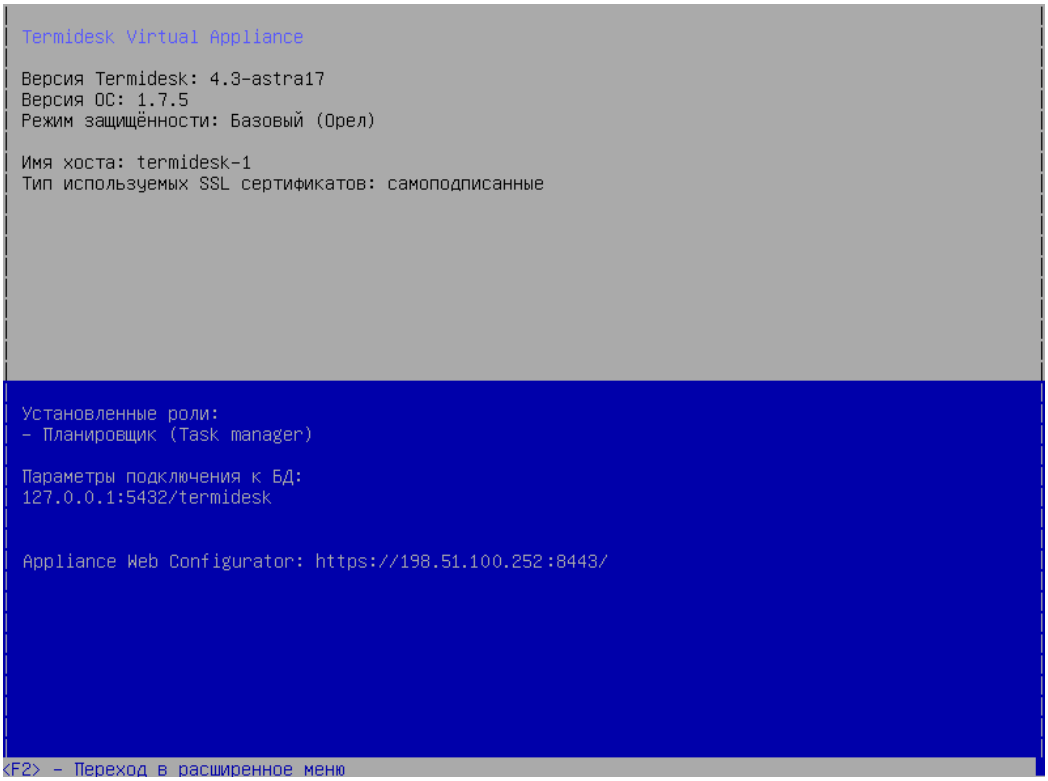

Рисунок 20 – Окно управления ВМТ

3.3 . Первичная настройка ВМТ с типом ноды «slave»

Первичная настройка выполняется при первом включении ВМ с подключенным образом ВМТ.

В процессе первичной настройки нужно выполнить следующее:

- ознакомиться с лицензионным соглашением (см. Рисунок 21) и нажать экранную кнопку **[OK]**;

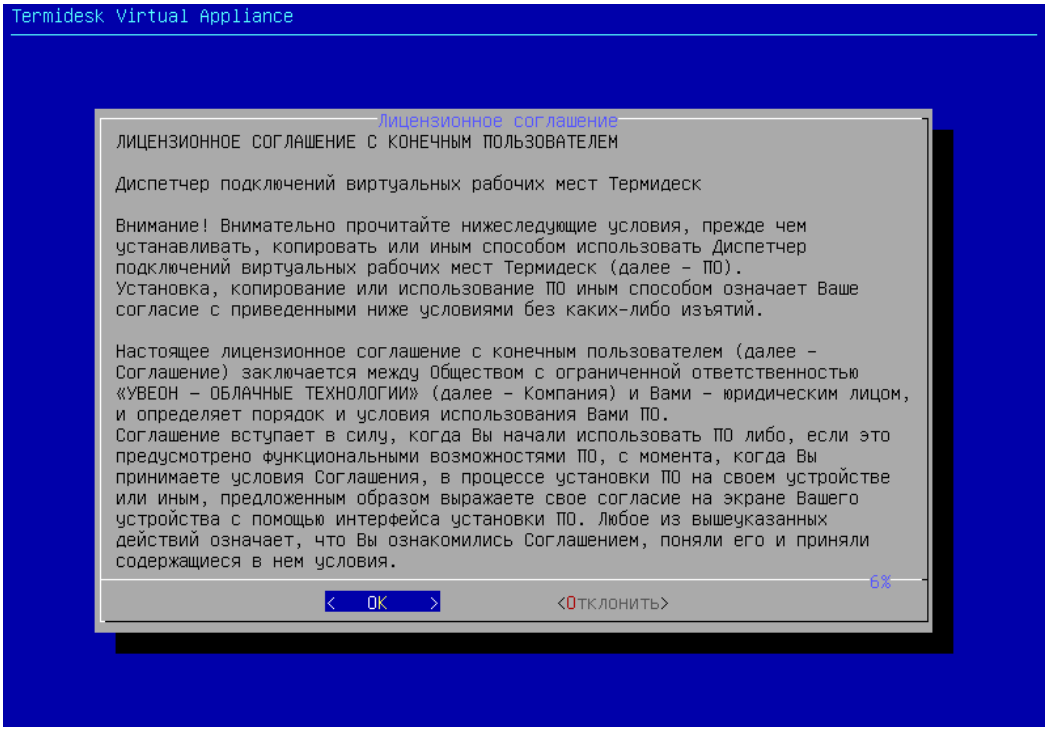

Рисунок 21 – Лицензионное соглашение

- выбрать режим защищенности ОС (см. Рисунок 22). Режим защищенности определяет, какие механизмы безопасности ОС будут активированы. Для режима «basic» («Базовый») специальные механизмы безопасности ОС не активируются;

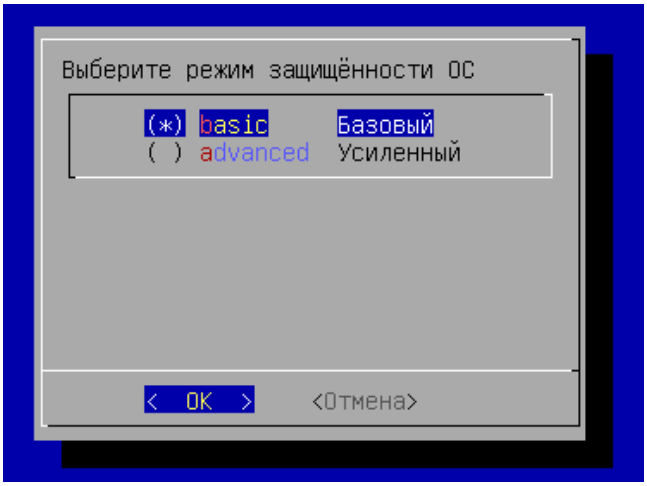

Рисунок 22 – Выбор режима защищенности ОС

- согласиться с перезапуском системы для применения режима защищенности ОС;
- после перезапуска системы будет показано информационное сообщение (см. Рисунок 23) о настроенном режиме защищенности ОС и активированных механизмах (см. Рисунок 24);

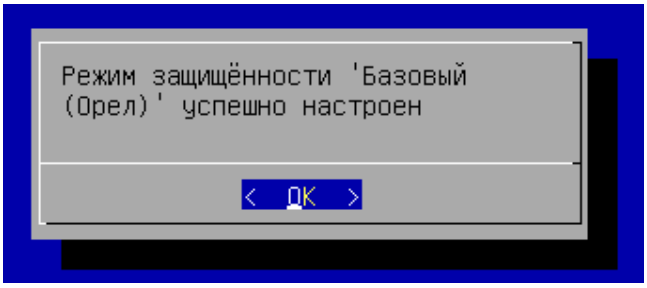

Рисунок 23 – Сообщение о настроенном режиме защищенности

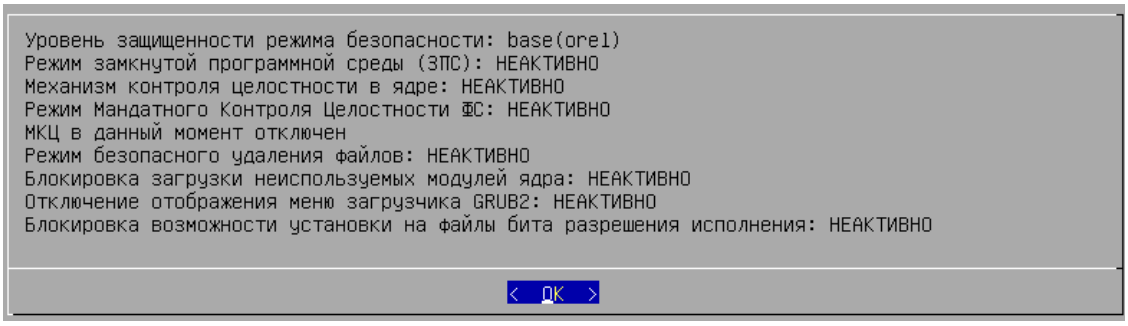

Рисунок 24 – Информационное сообщение об активированных механизмах безопасности на примере режима «Базовый»

- заполнить имя хоста (см. Рисунок 25) (hostname), которое будет использоваться для идентификации устройства в сети. Необходимо учесть, что указанный hostname, в свою очередь, должен являться полным доменным именем (FQDN), если ВМТ используется в домене. Указанный hostame будет использован для настройки веб-сервера apache;

> ⚠ Необходимо учесть, что при использовании указанного имени в других подключениях требуется, чтобы в сетевой инфраструктуре имена хостов могли разрешаться в IP-адреса (должен быть настроен DNS-сервер).

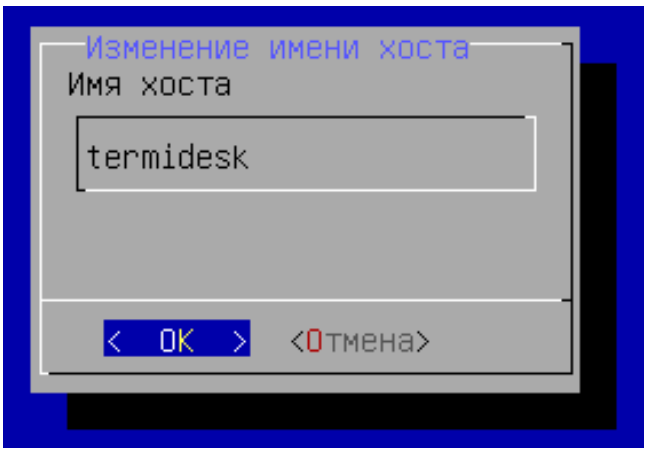

Рисунок 25 – Ввод имени хоста

- после применения настройки будет показано информационное сообщение (см. Рисунок 26);

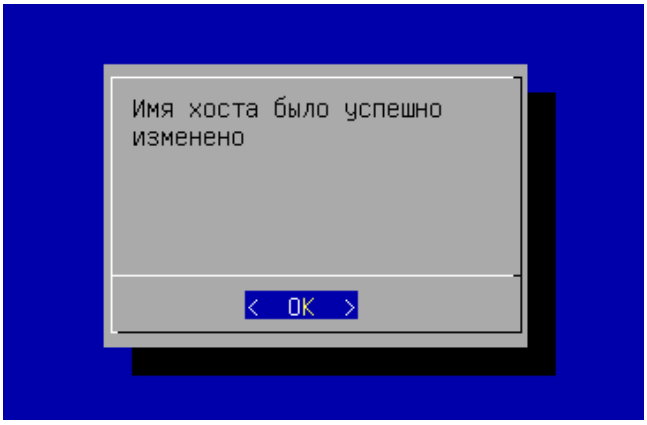

Рисунок 26 – Информационное сообщение об успешном изменении имени хоста

- выбрать сетевые интерфейсы (см. Рисунок 27) при помощи клавиши **<SPACE>**;

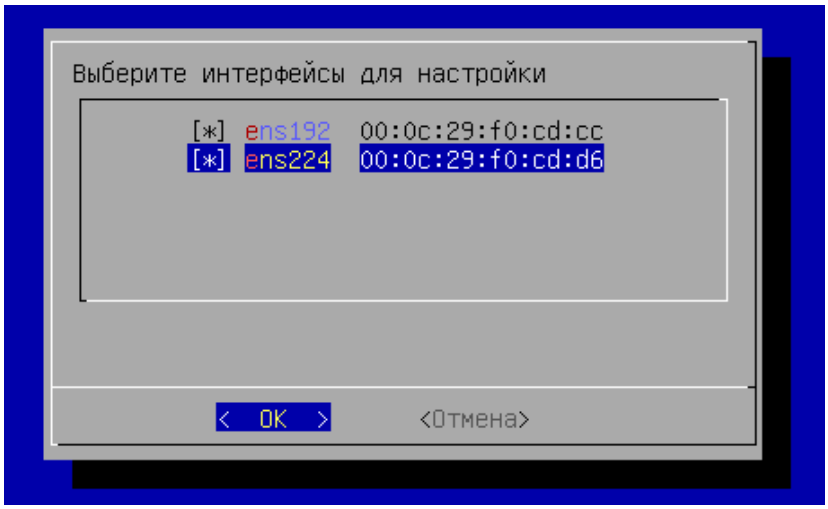

Рисунок 27 – Выбор сетевого интерфейса

- далее указать сетевые настройки: IP-адрес, маску сети, IP-адрес шлюза и IP-адреса DNS-серверов, выполняющих разрешение сетевых имен в IP-адреса. Настройки следует выполнить для каждого интерфейса. По умолчанию предложено задать статические настройки (см. Рисунок 28), однако при помощи клавиши **<TAB>** можно перейти к меню «DHCP», нажать клавишу **<ENTER>** и получить сетевые параметры от DHCP-сервера;

⚠ Все указанные IP-адреса должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре организации.

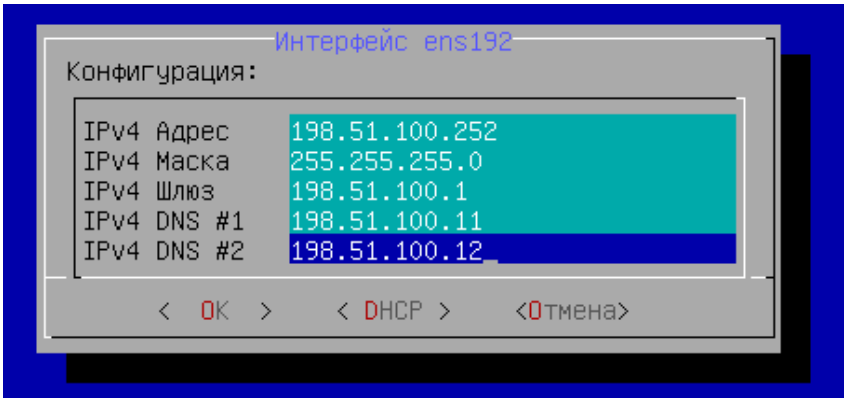

Рисунок 28 – Задание статических сетевых настроек

- изучить заданные параметры (см. Рисунок 29) и подтвердить изменение сетевых настроек, нажав экранную кнопку **[Да]**;

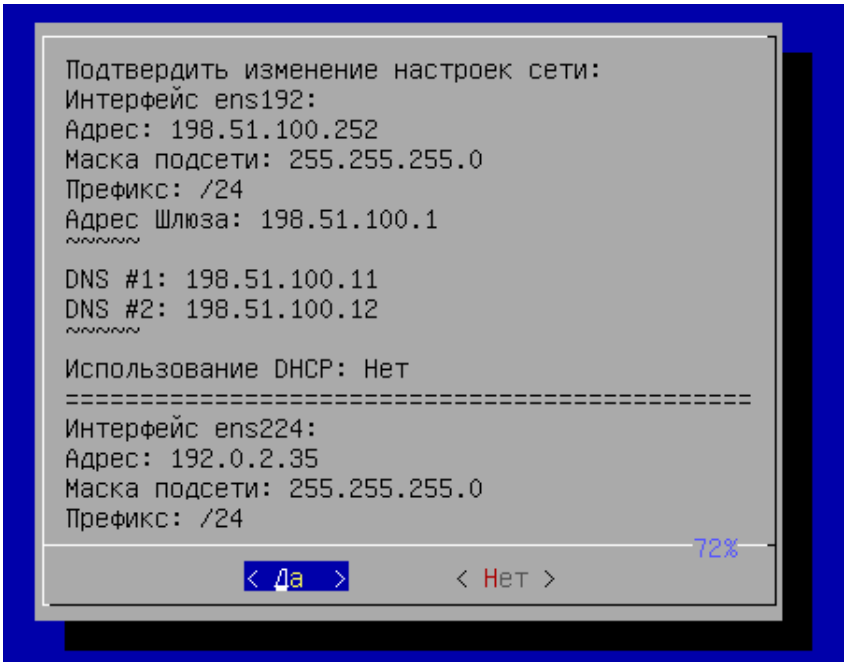

Рисунок 29 – Подтверждение сетевых настроек

- после применения настроек будет показано информационное сообщение (см. Рисунок 30);

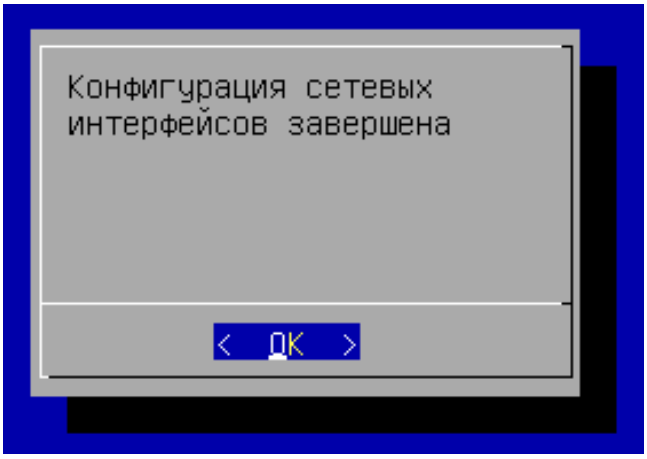

Рисунок 30 – Информационное сообщение об успешной конфигурации сетевых интерфейсов

- далее необходимо выбрать тип ноды BMT (см. Рисунок 31) «Slave» - нода не обладает собственным набором ключей. Ключи должны быть импортированы с ноды «Master». Для этого типа ноды доступен выбор устанавливаемой роли (см. ниже);

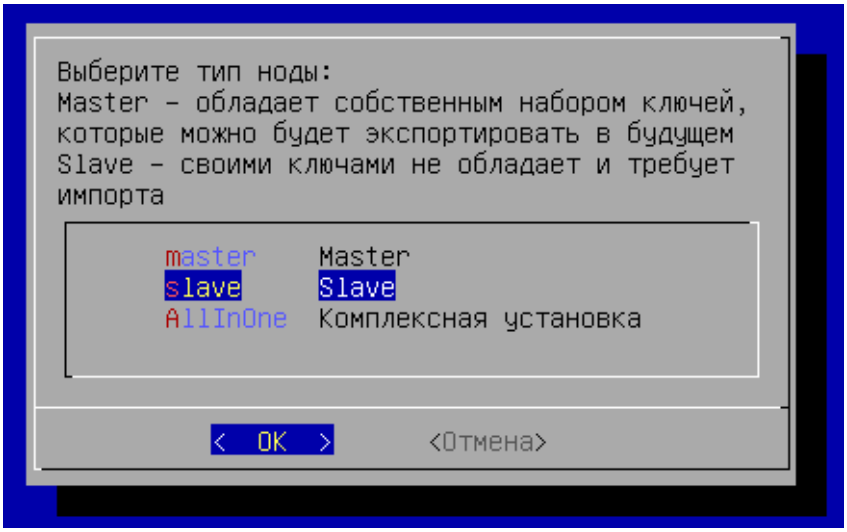

Рисунок 31 – Выбор типа устанавливаемой ноды BMT

- указать параметры сервера синхронизации, полученные с ноды «Master» (см. подраздел **Экспорт параметров Termidesk**) и ввести их;
- затем следует сконфигурировать использование SSL-сертификатов для веб-сервера apache. Эти параметры можно указать позже, тогда нужно выбрать экранную кнопку **[Отмена]**. Для конфигурирования указать (см. Рисунок 32):
  - IP-адрес хоста, на котором расположены сертификаты и ключ. У BMT должен быть сетевой доступ к хосту;
  - порт подключения;
  - полный путь к файлу закрытого ключа формата `.key`;

- полный путь к файлу сертификата формата `.pem`;
- полный путь к файлу проверки цепочки сертификатов формата `.crt`;

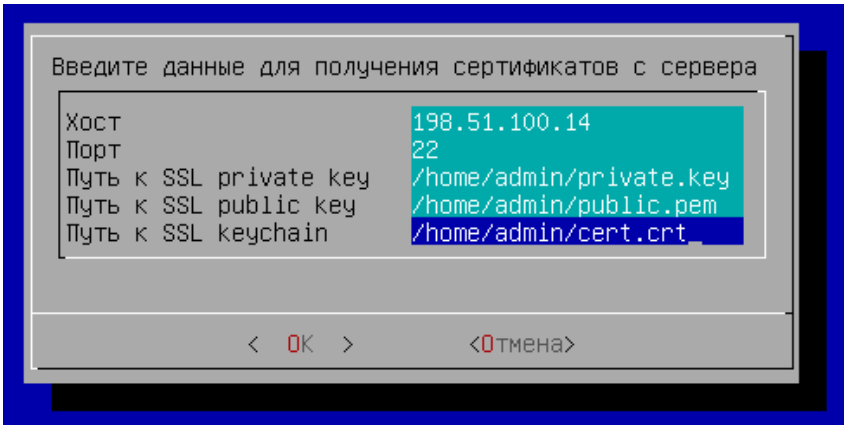

Рисунок 32 – Конфигурация сертификатов

- в следующем окне (см. Рисунок 33) заполнить имя пользователя и пароль для подключения к указанному на предыдущем шаге хосту. Для задания пароля переключиться на строку «Пароль» при помощи клавиши **<↓>** (**<СТРЕЛКА ВНИЗ>**) и ввести его, затем переключиться таким же способом на строку «Повтор пароля» и повторить ввод пароля. Поле «Имя пользователя» при этом изменится на другой цвет, как неактивное в данный момент, ввод пароля отображен не будет. Подтвердить данные, нажав экранную кнопку **[OK]**;

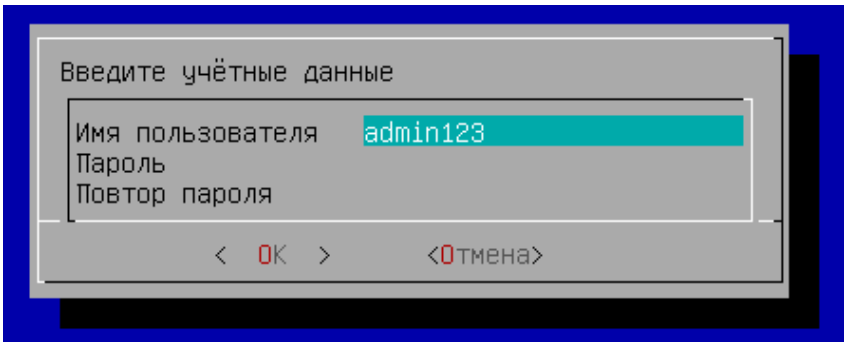

Рисунок 33 – Заполнение учетных данных для доступа

- затем выбрать устанавливаемую роль (см. Рисунок 34): «Шлюз», «Брокер» (компонент «Универсальный диспетчер» Termidesk), «Планировщик» (компонент «Менеджер рабочих мест» Termidesk);

При выборе той или иной роли будут автоматически активированы соответствующие службы Termidesk:

- при выборе роли «Шлюз»: служба `termidesk-gateway`;
- при выборе роли «Брокер»: служба `termidesk-vdi`. Также будет сконфигурирован и запущен веб-сервер apache;

- при выборе роли «Планировщик»: службы `termidesk-taskman`, `termidesk-celery-beat`, `termidesk-celery-worker`. Также будет инициализирован брокер сообщений RabbitMQ-server и выполнен запуск службы `rabbitmq-server`.

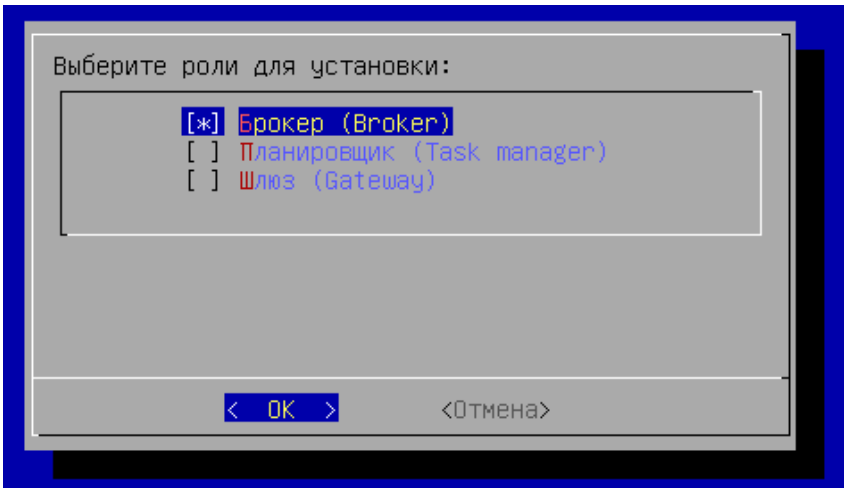

Рисунок 34 – Выбор устанавливаемой роли

- если была выбрана роль «Шлюз», то нужно ввести адрес узла с ролью «Брокер» или адрес балансировщика (если он используется) для подключения к нему (см. Рисунок 35). Указание порта для подключения является опциональным;

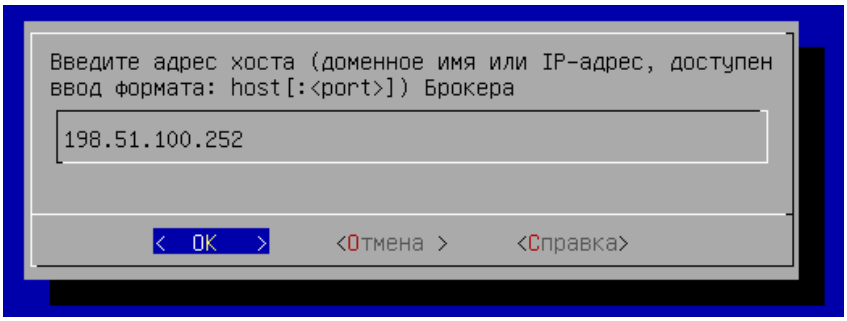

Рисунок 35 – Ввод адреса для подключения к «Брокеру»

- если была выбрана роль «Брокер» или «Планировщик», то нужно выбрать тип используемой БД (см. Рисунок 36). При выборе удаленной БД локальная не активируется;

⚠ В случае, если ранее тип ноды «master» был установлен с выбором локальной БД, то для функционирования комплекса в распределенном варианте необходимо выбрать пункт «remote» и указать параметры подключения к БД:

- «Имя пользователя»: `termidesk`;
- «Пароль»: пароль, заданный при настройке ноды «master»;
- «Хост»: **внешний** IP-адрес или FQDN узла «master»;
- «Порт»: `5432`;
- «База данных»: `termidesk`.

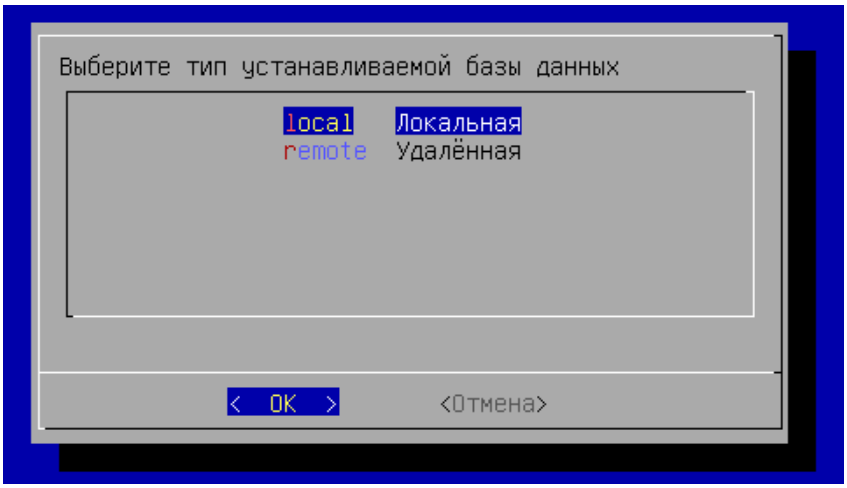

Рисунок 36 – Выбор типа используемой БД

- если была выбрана локальная БД, то нужно придумать пароль (см. Рисунок 37) для нее. Пароль будет храниться в преобразованном виде;

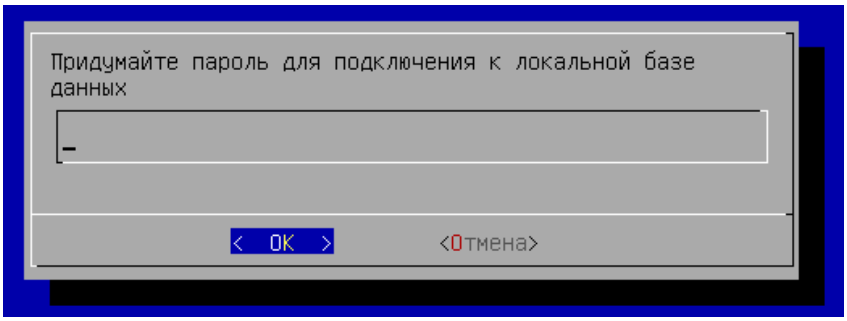

Рисунок 37 – Создание пароля для локальной БД

- если была выбрана удаленная БД, то нужно указать параметры подключения (см. Рисунок 38) к ней. В параметре «хост» должен указываться внешний IP-адрес или FQDN узла с БД. Затем выбрать экранную кнопку **[Тест]** для проверки доступа. В случае, если БД с указанными настройками не существует, переход к следующему окну будет невозможен. В случае, если БД с указанными настройками существует, будет повторно отображено окно с параметрами БД, в котором следует нажать экранную кнопку **[OK]**;

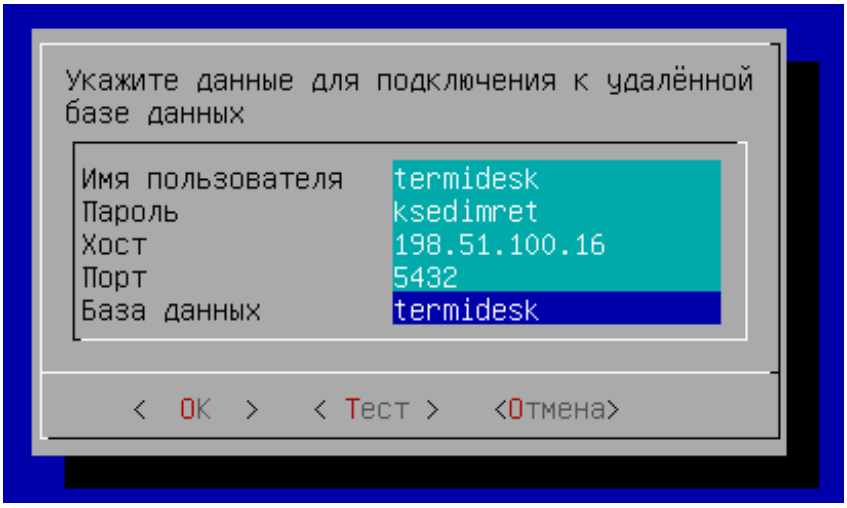

Рисунок 38 – Параметры подключения к удаленной БД

- если была выбрана удаленная БД, то нужно также указать протокол (см. Рисунок 39), который будет использоваться при подключении к БД. При выборе значения «Disable» защищенное соединение при подключении к БД использоваться не будет;

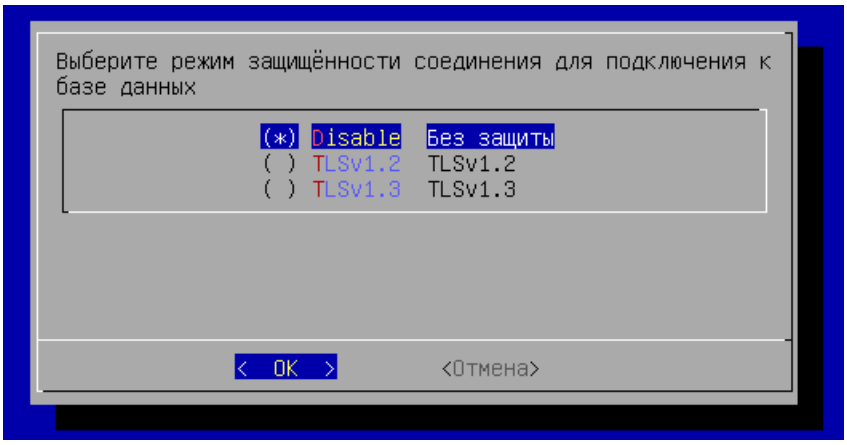

Рисунок 39 – Выбор протокола для подключения к БД

- если ранее была выбрана роль «Планировщик», то в следующем окне нужно указать пароль (см. Рисунок 40) для подключения к RabbitMQ;

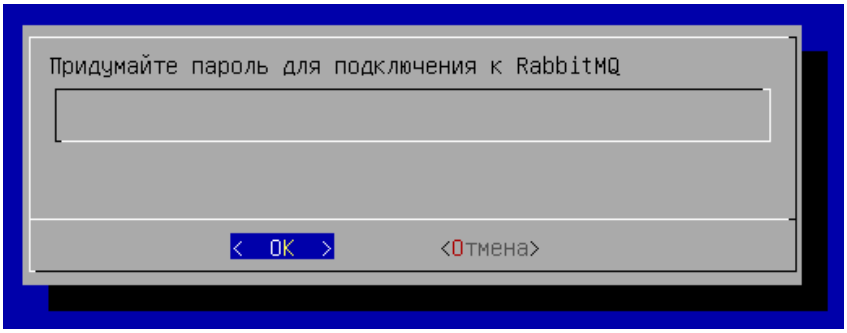

Рисунок 40 – Пароль для подключения к RabbitMQ

- если ранее для установки была выбрана роль «Брокер», то нужно указать тип (см. Рисунок 41) веб-интерфейса Termidesk:

- «Объединенный» - здесь будут доступны все функции веб-интерфейса и интерфейс swagger для доступа к документации по командам REST API;
- «Пользовательский» - здесь будет доступен только пользовательский веб-интерфейс. Интерфейс управления Termidesk и `swagger` будут недоступны;
- «Административный» - здесь будет доступен только веб-интерфейс для управления Termidesk и `swagger`, а пользовательский интерфейс нет;

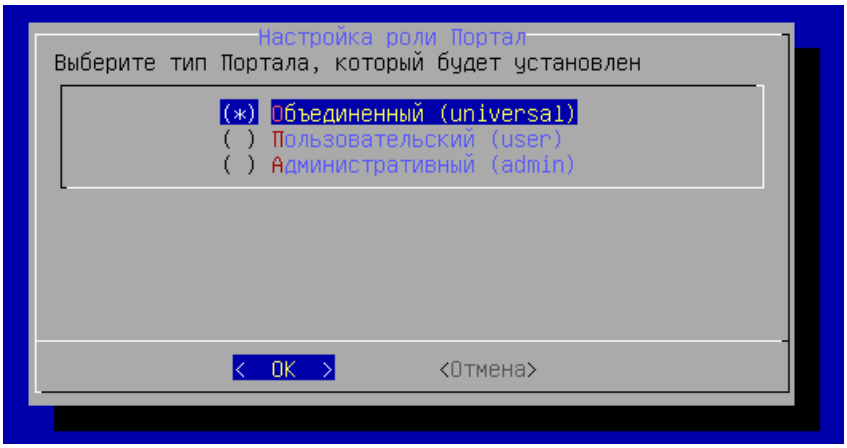

Рисунок 41 – Выбор типа веб-интерфейса

- после выполнения настроек изучить заданные параметры и подтвердить настройки выбранной роли, нажав экранную кнопку **[OK]**;
- дождаться успешного применения настроек и вывода сообщения (см. Рисунок 42).

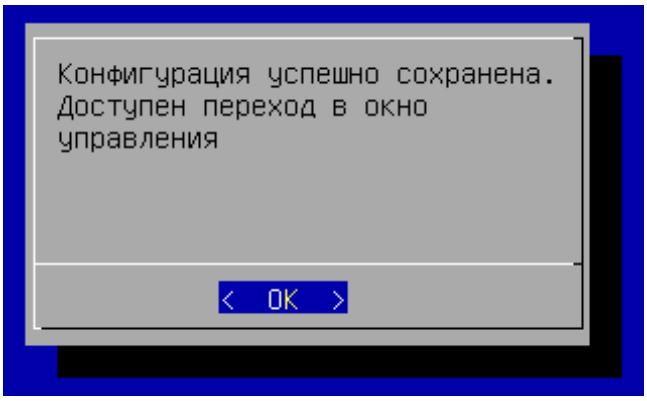

Рисунок 42 – Информационное сообщение об успешном применении конфигурации

После выполнения шагов по первичной настройке произойдет переход в окно управления ВМТ (см. Рисунок 43). Службы Termidesk будут автоматически активированы, перезагрузка не требуется.

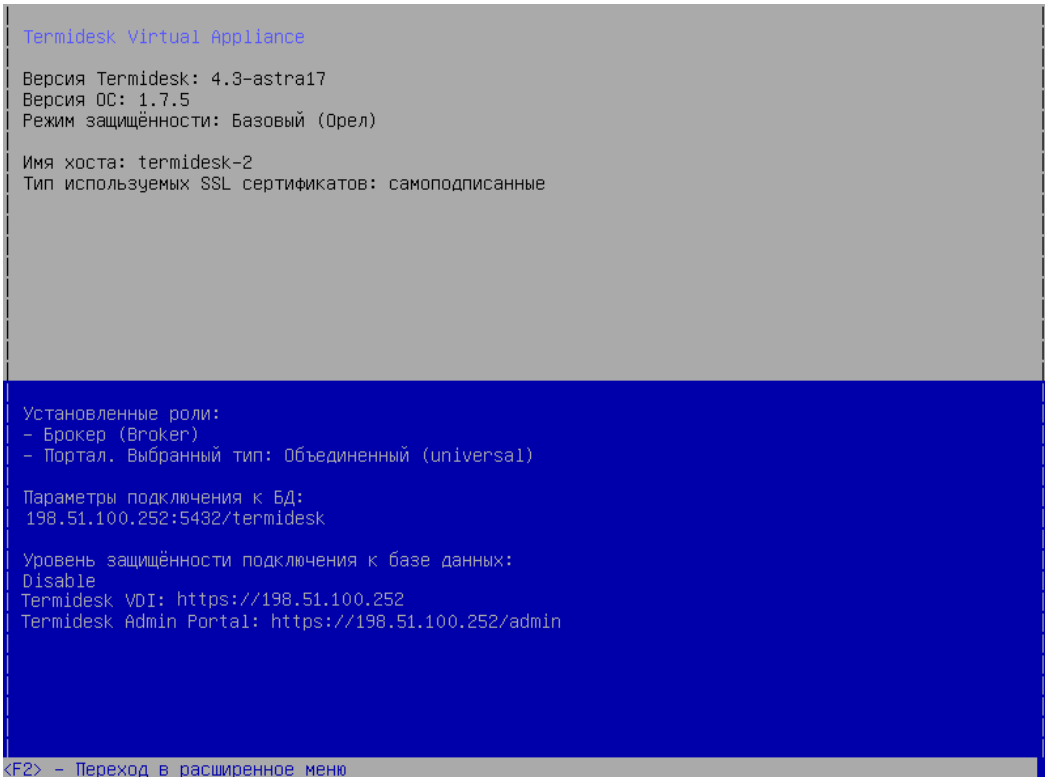

Рисунок 43 – Окно управления ВМТ

3.4 . Первичная настройка ВМТ в режиме комплексной установки

Первичная настройка выполняется при первом включении ВМ с подключенным образом ВМТ.

Комплексную установку рекомендуется использовать только для ознакомления в тестовой среде.

В процессе первичной настройки нужно выполнить следующее:

- ознакомиться с лицензионным соглашением (см. Рисунок 44) и нажать экранную кнопку **[OK]**;

Переключение между пунктами меню выполняется клавишей **<TAB>**. Подтверждение выбора выполняется клавишами **<ENTER>** или **< SPACE>**.

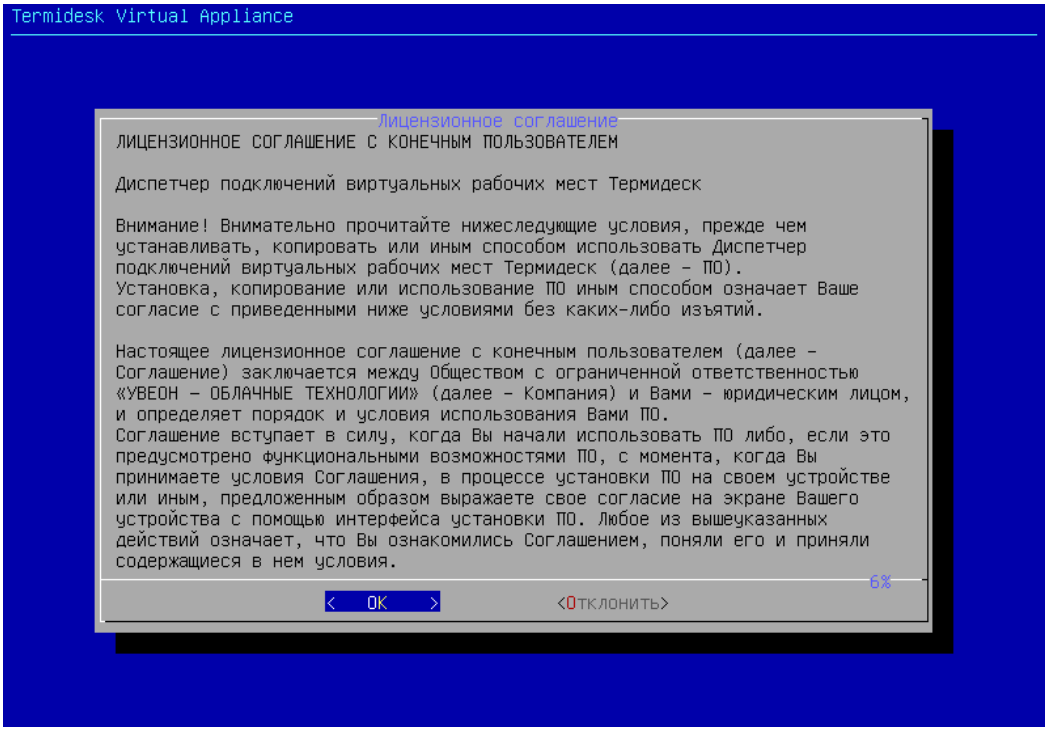

Рисунок 44 – Лицензионное соглашение

- выбрать режим защищенности ОС (см. Рисунок 45). Режим защищенности определяет, какие механизмы безопасности ОС будут активированы. Для режима «basic» («Базовый») специальные механизмы безопасности ОС не активируются;

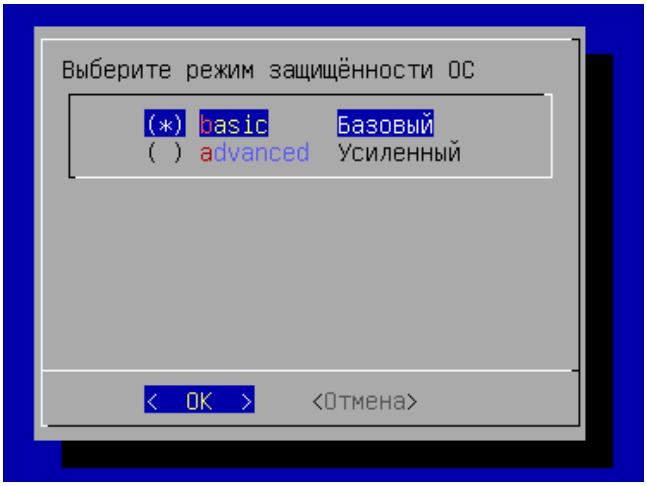

Рисунок 45 – Выбор режима защищенности ОС

- согласиться с перезапуском системы для применения режима защищенности ОС;
- после перезапуска системы будет показано информационное сообщение (см. Рисунок 46) о настроенном режиме защищенности ОС и активированных механизмах (см. Рисунок 47);

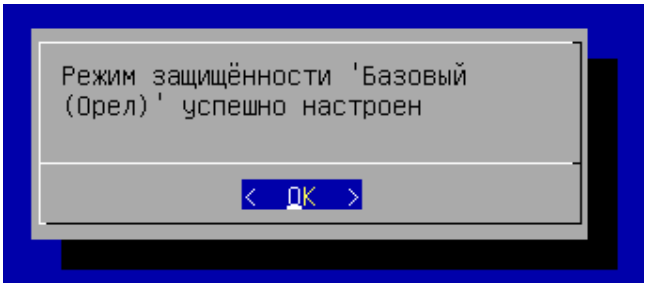

Рисунок 46 – Сообщение о настроенном режиме защищенности

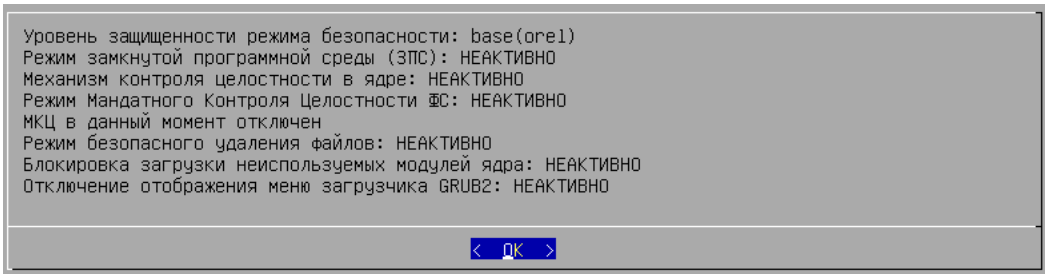

Рисунок 47 – Информационное сообщение об активированных механизмах безопасности на примере режима «Базовый»

- заполнить имя хоста (см. Рисунок 48) (`hostname`), которое будет использоваться для идентификации устройства в сети. Необходимо учесть, что указанный `hostname`, в свою очередь, должен являться полным доменным именем (FQDN), если BMT используется в домене. Указанный `hostame` будет использован для настройки веб-сервера `apache`;

> ⚠ Необходимо учесть, что при использовании указанного имени в других подключениях требуется, чтобы в сетевой инфраструктуре имена хостов могли разрешаться в IP-адреса (должен быть настроен DNS-сервер).

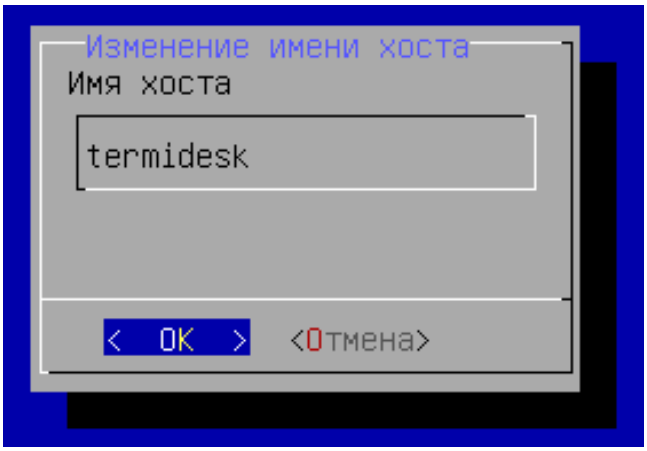

Рисунок 48 – Ввод имени хоста

- после применения настройки будет показано информационное сообщение (см. Рисунок 49);

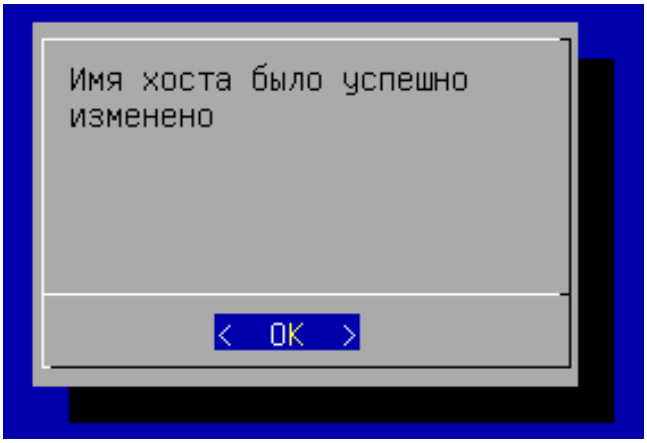

Рисунок 49 – Информационное сообщение об успешном изменении имени хоста

- выбрать сетевые интерфейсы (см. Рисунок 50) при помощи клавиши **<SPACE>**;

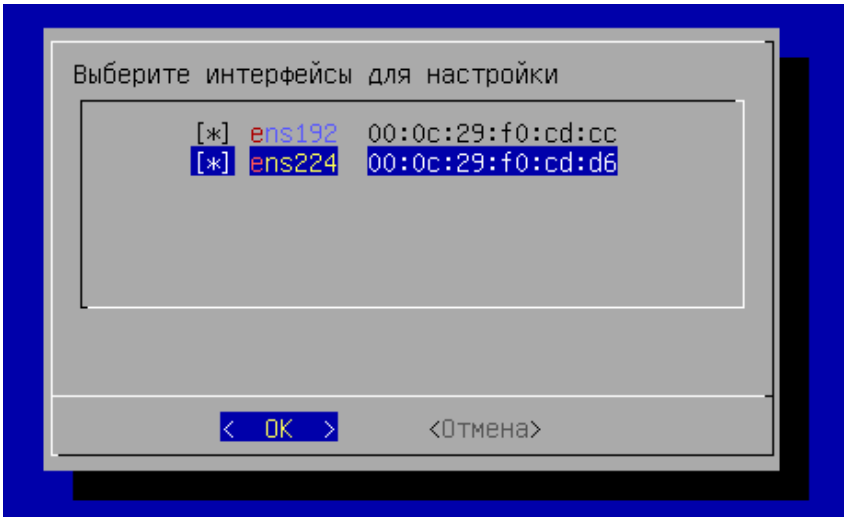

Рисунок 50 – Выбор сетевого интерфейса

- далее указать сетевые настройки: IP-адрес, маску сети, IP-адрес шлюза и IP-адреса DNS-серверов, выполняющих разрешение сетевых имен в IP-адреса. Настройки следует выполнить для каждого интерфейса. По умолчанию предложено задать статические настройки (см. Рисунок 51), однако при помощи клавиши **<TAB>** можно перейти к меню «DHCP», нажать клавишу **<ENTER>** и получить сетевые параметры от DHCP-сервера;

⚠ Все указанные IP-адреса должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре организации.

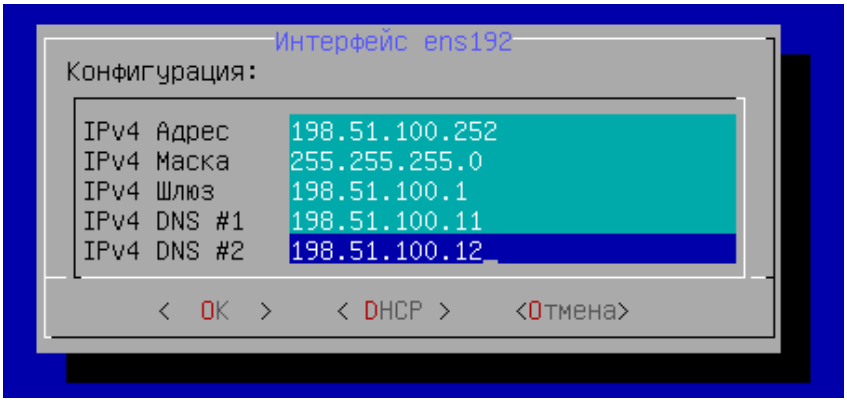

Рисунок 51 – Задание статических сетевых настроек

- изучить заданные параметры (см. Рисунок 52) и подтвердить изменение сетевых настроек, нажав экранную кнопку **[Да]**;

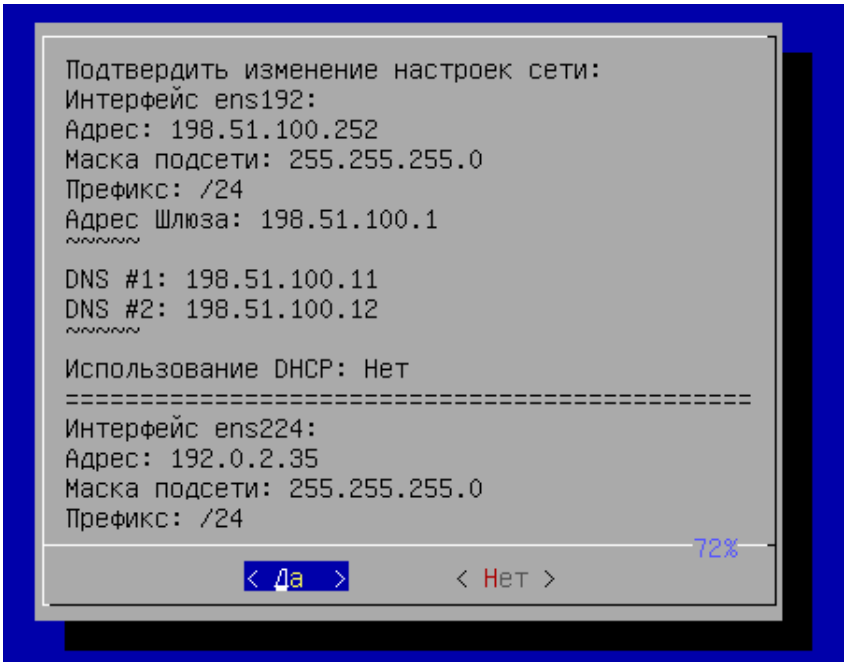

Рисунок 52 – Подтверждение сетевых настроек

- после применения настроек будет показано информационное сообщение (см. Рисунок 53);

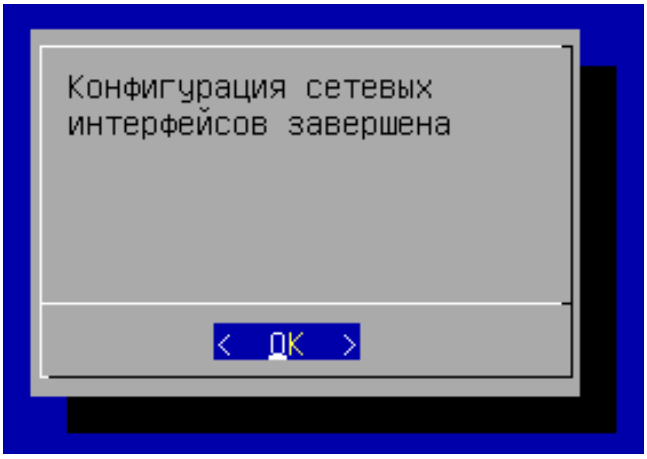

Рисунок 53 – Информационное сообщение об успешной конфигурации сетевых интерфейсов

- далее необходимо выбрать тип ноды BMT (см. Рисунок 54) «AllInOne»;

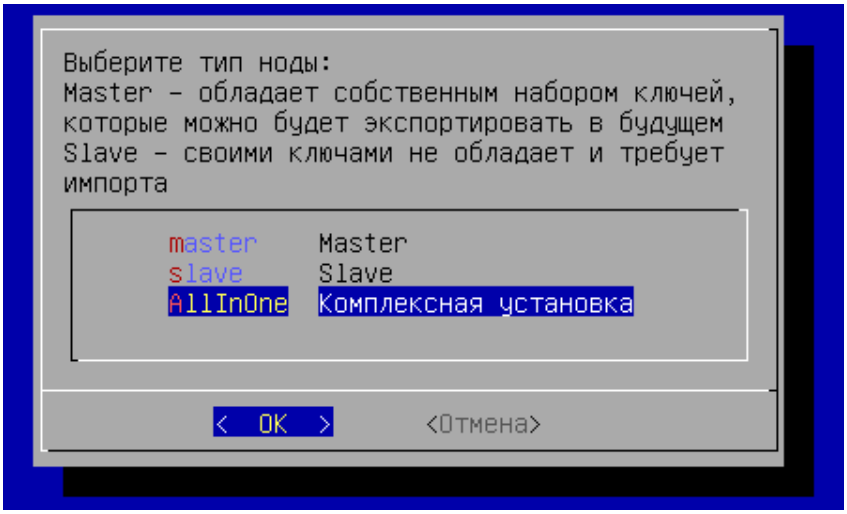

Рисунок 54 – Выбор типа устанавливаемой ноды BMT

- затем следует сконфигурировать использование SSL-сертификатов для веб-сервера apache. Эти параметры можно указать позже, тогда нужно выбрать экранную кнопку **[Отмена]**. Для конфигурирования указать (см. Рисунок 55):
  - IP-адрес хоста, на котором расположены сертификаты и ключ. У BMT должен быть сетевой доступ к хосту;
  - порт подключения;
  - полный путь к файлу закрытого ключа формата `.key`;
  - полный путь к файлу сертификата формата `.pem`;
  - полный путь к файлу проверки цепочки сертификатов формата `.crt`;

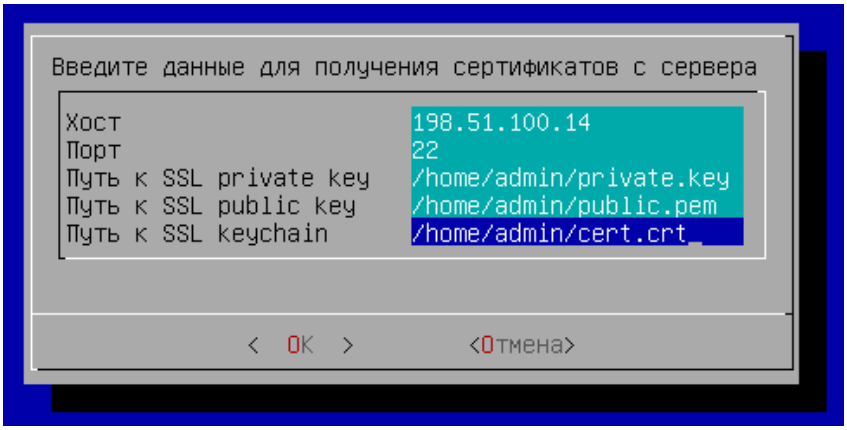

Рисунок 55 – Конфигурация сертификатов

- в следующем окне (см. Рисунок 56) заполнить имя пользователя и пароль для подключения к указанному на предыдущем шаге хосту. Для задания пароля переключиться на строку «Пароль» при помощи клавиши **<↓>** (**<СТРЕЛКА ВНИЗ>**) и ввести его, затем переключиться таким же способом на строку «Повтор пароля» и повторить ввод пароля. Поле «Имя пользователя» при этом изменится на другой цвет, как неактивное в данный момент, ввод пароля отображен не будет. Подтвердить данные, нажав экранную кнопку **[OK]**;

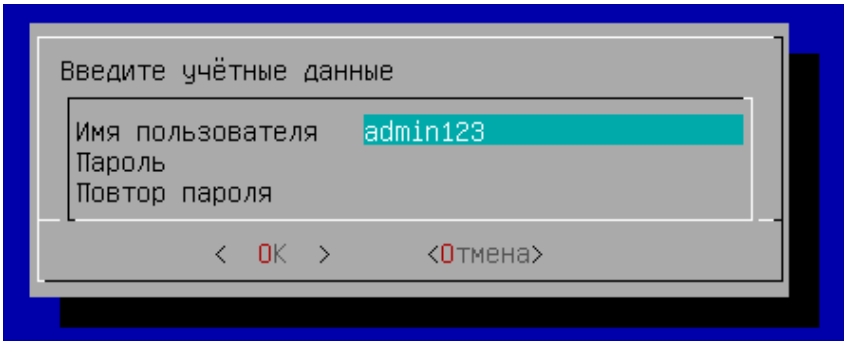

Рисунок 56 – Заполнение учетных данных для доступа

- затем отметить все пункты (см. Рисунок 57) для типа устанавливаемой роли: «Шлюз», «Брокер» (компонент «Универсальный диспетчер» Termidesk), «Планировщик» (компонент «Менеджер рабочих мест» Termidesk);

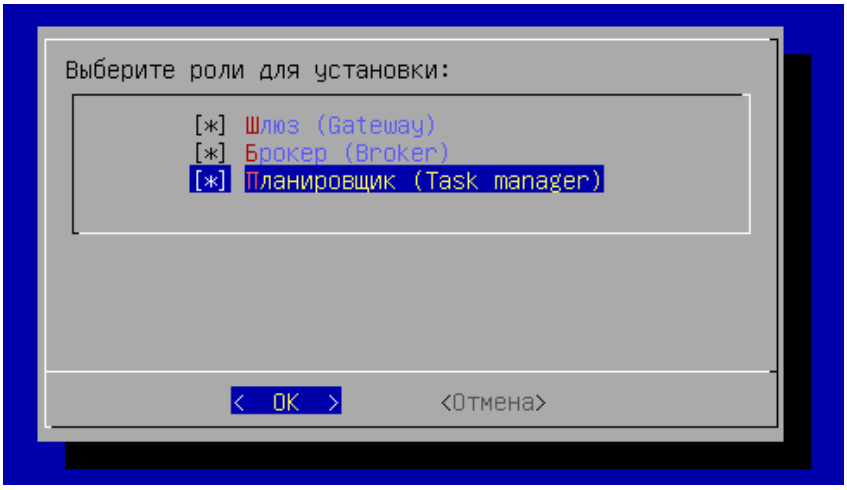

Рисунок 57 – Выбор устанавливаемой роли

При выборе ролей будут автоматически активированы соответствующие службы Termidesk:

- для роли «Шлюз»: служба `termidesk-gateway`;
- для роли «Брокер»: служба `termidesk-vdi`. Также будет сконфигурирован и запущен веб-сервер `apache`;
- для роли «Планировщик»: службы `termidesk-taskman`, `termidesk-celery-beat`, `termidesk-celery-worker`. Также будет инициализирован брокер сообщений RabbitMQ-server и выполнен запуск службы `rabbitmq-server`.

- выбрать тип используемой БД (см. Рисунок 58). При выборе удаленной БД локальная не активируется;

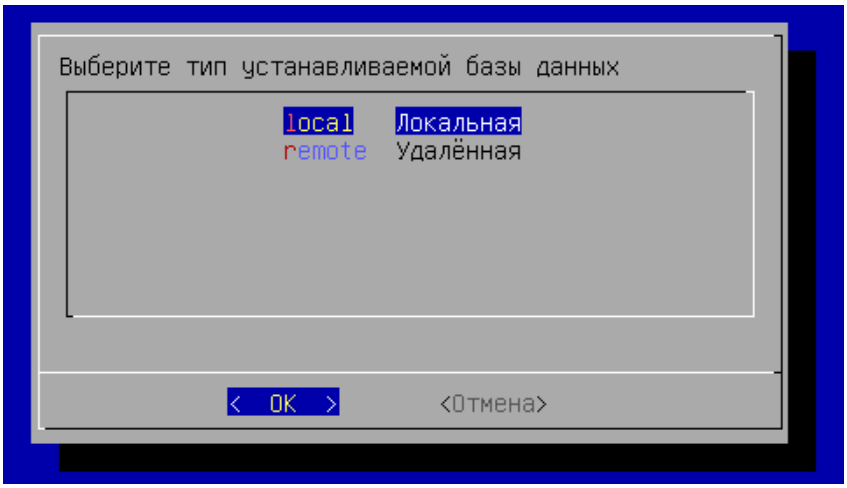

Рисунок 58 – Выбор типа используемой БД

- если была выбрана локальная БД, то нужно указать пароль (см. Рисунок 59) для нее. Пароль будет храниться в преобразованном виде;

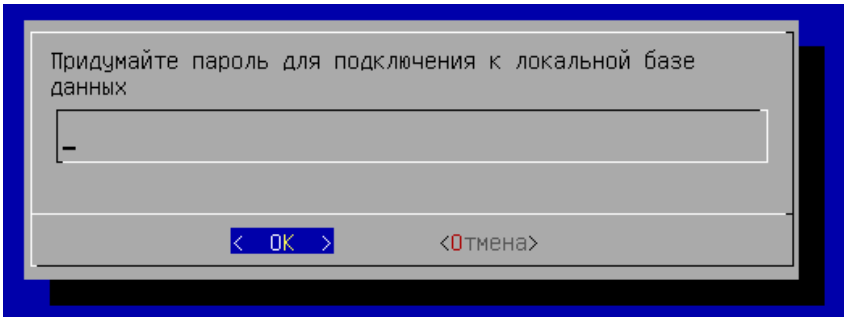

Рисунок 59 – Создание пароля для локальной БД

- если была выбрана удаленная БД, то нужно указать параметры подключения (см. Рисунок 60) к ней. В параметре «хост» должен указываться внешний IP-адрес или FQDN узла с БД. Затем выбрать экранную кнопку **[Тест]** для проверки доступа. В случае, если БД с указанными настройками не существует, переход к следующему окну будет невозможен. В случае, если БД с указанными настройками существует, будет повторно отображено окно с параметрами БД, в котором следует нажать экранную кнопку **[OK]**;

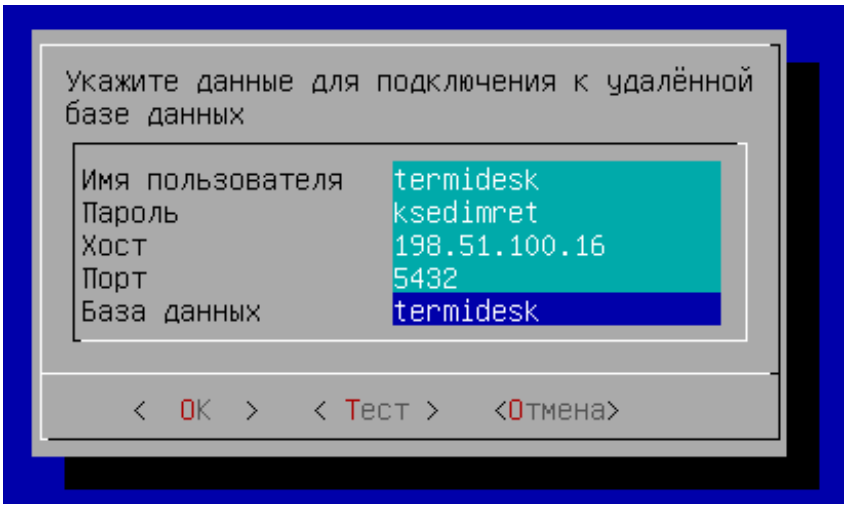

Рисунок 60 – Параметры подключения к удаленной БД

- если была выбрана удаленная БД, то нужно также указать протокол (см. Рисунок 61), который будет использоваться при подключении к БД. При выборе значения «Disable» защищенное соединение при подключении к БД использоваться не будет;

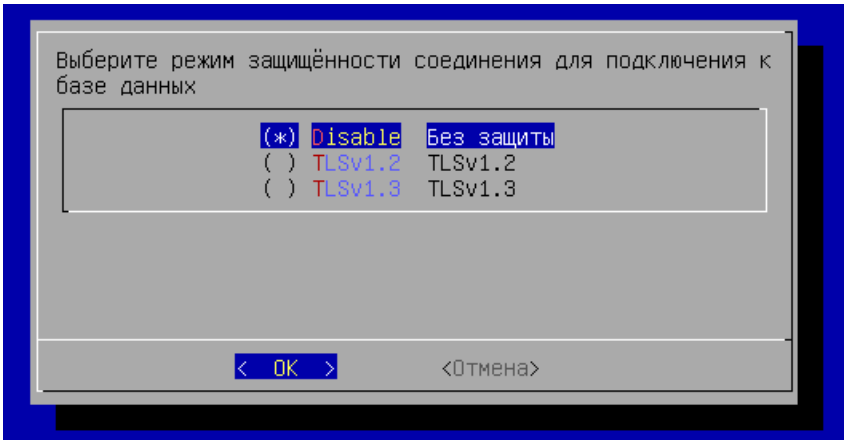

Рисунок 61 – Выбор протокола для подключения к БД

- в следующем окне необходимо указать пароль (см. Рисунок 62) для подключения к RabbitMQ;

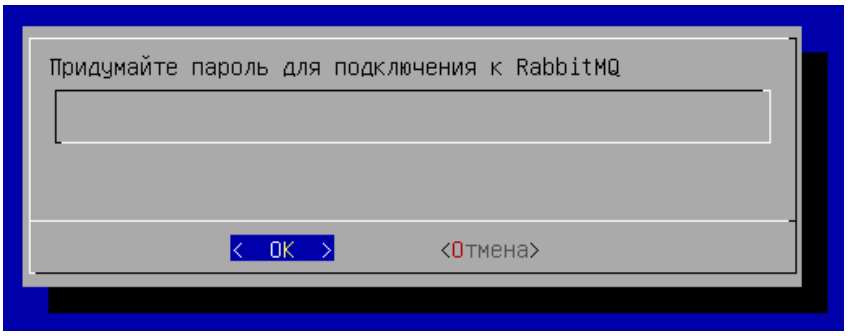

Рисунок 62 – Пароль для подключения к RabbitMQ

- затем указать тип (см. Рисунок 63) веб-интерфейса Termidesk:
  - «Объединенный» - здесь будут доступны все функции веб-интерфейса и интерфейс swagger для доступа к документации по командам REST API;
  - «Пользовательский» - здесь будет доступен только пользовательский веб-интерфейс. Интерфейс управления Termidesk и `swagger` будут недоступны;
  - «Административный» - здесь будет доступен только веб-интерфейс для управления Termidesk и `swagger`, а пользовательский интерфейс нет;

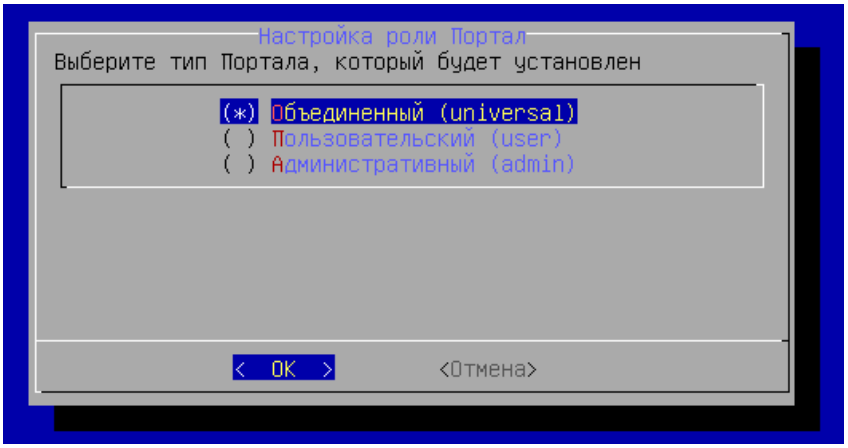

Рисунок 63 – Выбор типа веб-интерфейса

- ввести адрес узла с ролью «Брокер» или адрес балансировщика (если он используется) для подключения к нему (см. Рисунок 64). В режиме комплексной установки нужно ввести `127.0.0.1` или `localhost`. На запрос о недоступности узла ответить «Да»: поскольку в этот момент служба «Брокера» еще не запущена, ошибку можно пропустить;

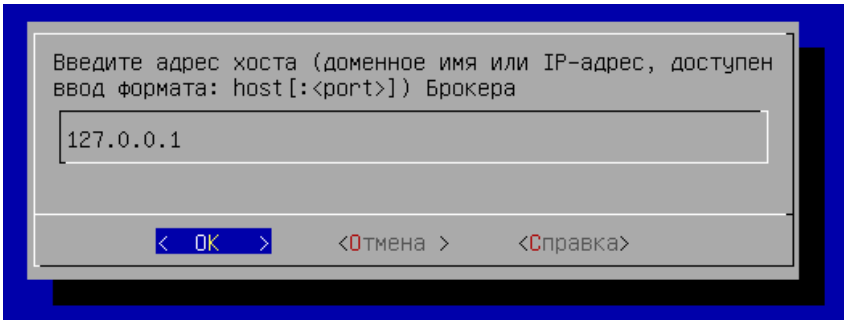

Рисунок 64 – Ввод адреса узла с ролью «Брокер»

- изучить заданные параметры и подтвердить настройки выбранной роли, нажав экранную кнопку **[OK]**;
- дождаться успешного применения настроек и вывода сообщения (см. Рисунок 65).

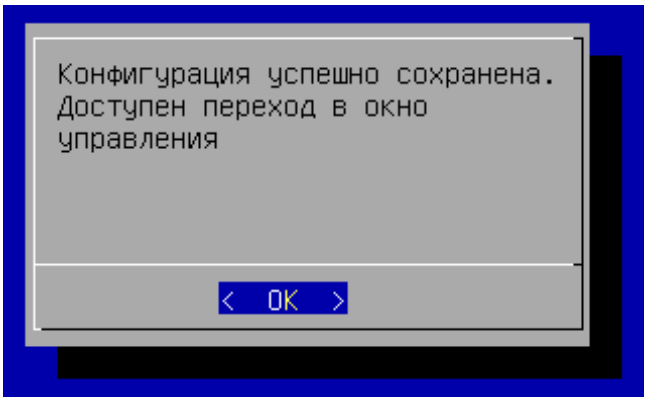

Рисунок 65 – Информационное сообщение об успешном применении конфигурации

После выполнения шагов по первичной настройке произойдет переход в окно управления ВМТ (см. Рисунок 66). Службы Termidesk будут автоматически активированы, перезагрузка не требуется. IP-адрес, отображаемый в главном окне ВМТ, соответствует IP-адресу первого настроенного интерфейса.

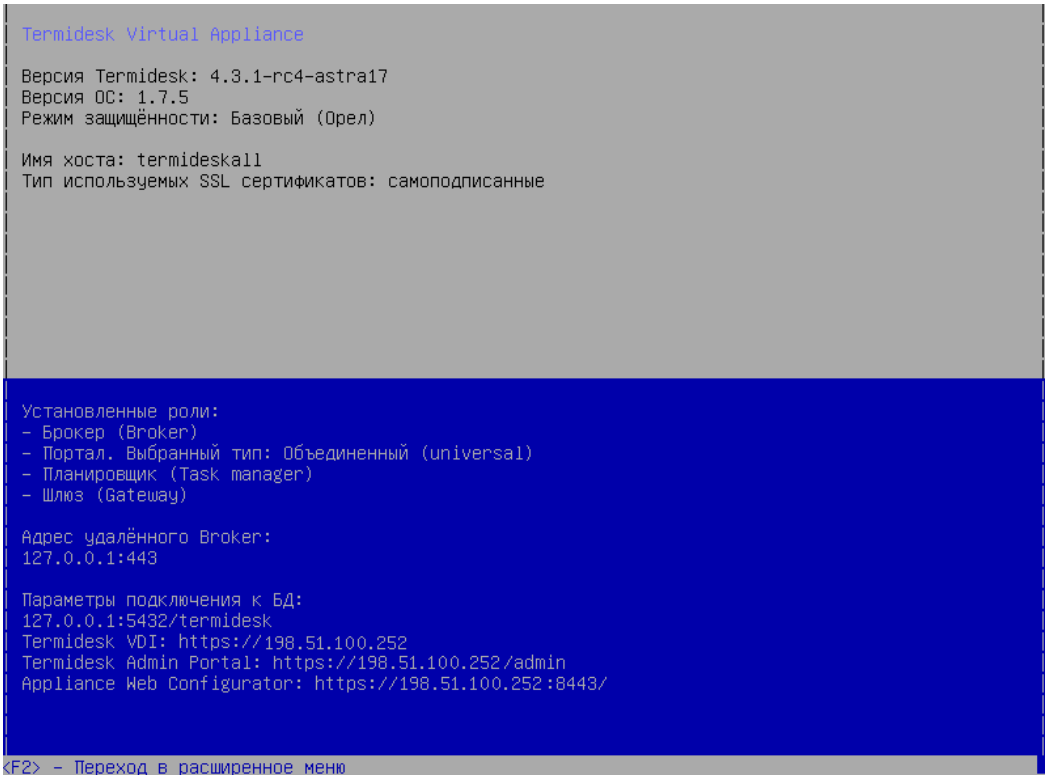

Рисунок 66 – Окно управления BMT

3.5 . Проверка работоспособности

BMT работоспособен, если после установки отобразилось главное меню BMT, а также при переходе по адресу `https://<IP-адрес_BMT>:8443/` отобразилась страница авторизации (см. Рисунок 67) веб-интерфейса BMT.

Для доступа к веб-интерфейсу BMT после установки необходимо использовать следующие данные:

- логин: `admin`;
- пароль: `admin`.

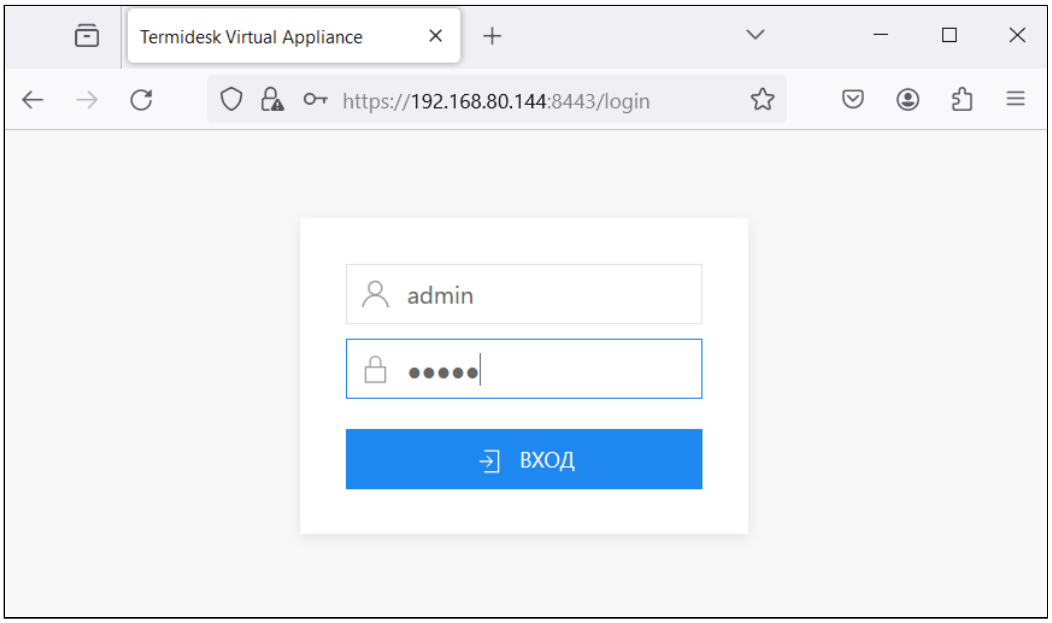

Рисунок 67 – Страница авторизации веб-интерфейса VA

4 . ЛИЦЕНЗИРОВАНИЕ

ВМТ не лицензируется отдельно от Termidesk. Ввод лицензии осуществляется в веб-интерфейсе Termidesk.

4.1 . Получение лицензионного ключа

Для Termidesk предусмотрены следующие варианты лицензирования:

- Termidesk VDI (поддержка совместимых платформ виртуализации и серверов терминалов);
- Termidesk Terminal (поддержка только серверов терминалов для ОС Windows (MS RDS/MS RDSH) и Astra Linux (STAL)).

В рамках доступных вариантов лицензирования существует поддержка двух типов лицензий:

- по пользователям - лицензия привязывается к пользователю системы;
- по конкурентным соединениям - лицензия привязывается к количеству одновременных подключений пользователей через систему.

⚠ Начиная с версии Termidesk 4.1 изменена политика лицензирования программного комплекса.
Все ранее выпущенные лицензии считаются неограниченными.
При активации лицензии с ограничениями, все объекты, связанные с нелицензированными поставщиками ресурсов или протоколами доставки, будут недоступны.

Дистрибутив Termidesk распространяется с предустановленным лицензионным ключом, имеющим ограничение на 4 (четыре) одновременных подключения для ознакомительных целей. Дистрибутив предназначен для проведения испытания, ознакомления или демонстрации его функциональных возможностей. Дистрибутив для ознакомительных целей может предоставляться без заключения соответствующего договора на срок 90 (девяносто) календарных дней. Подробнее с условиями лицензионного соглашение с конечным пользователем можно ознакомиться на сайте компании: `https://termidesk.ru/eula.pdf`.
Для получения дополнительных лицензионных ключей с целью ознакомления необходимо перейти по ссылке `https://termidesk.ru/products/#request-key` и сформировать запрос, заполнив корректными данными следующие экранные поля:

- «Корпоративный email»;
- «Имя лица, запрашивающего лицензию»;
- «Системный UUID»;
- «Согласие на обработку персональных данных».

Информация о системном UUID располагается в графическом интерфейсе управления «Настройка - Лицензия - Система», пример показан на рисунке (см. Рисунок 68).

⚠ Для получения лицензионного ключа при распределенном варианте установки Termidesk, необходимо предоставить в запросе системные UUID всех узлов с компонентом «Универсальный диспетчер» и всех узлов с компонентом «Менеджер рабочих мест». Информацию о системном UUID в этом случае необходимо получить для каждого узла из файла `/sys/devices/virtual/dmi/id/product_uuid`, выполнив команду на нужном узле:

```
:~$ sudo cat /sys/devices/virtual/dmi/id/product_uuid
```

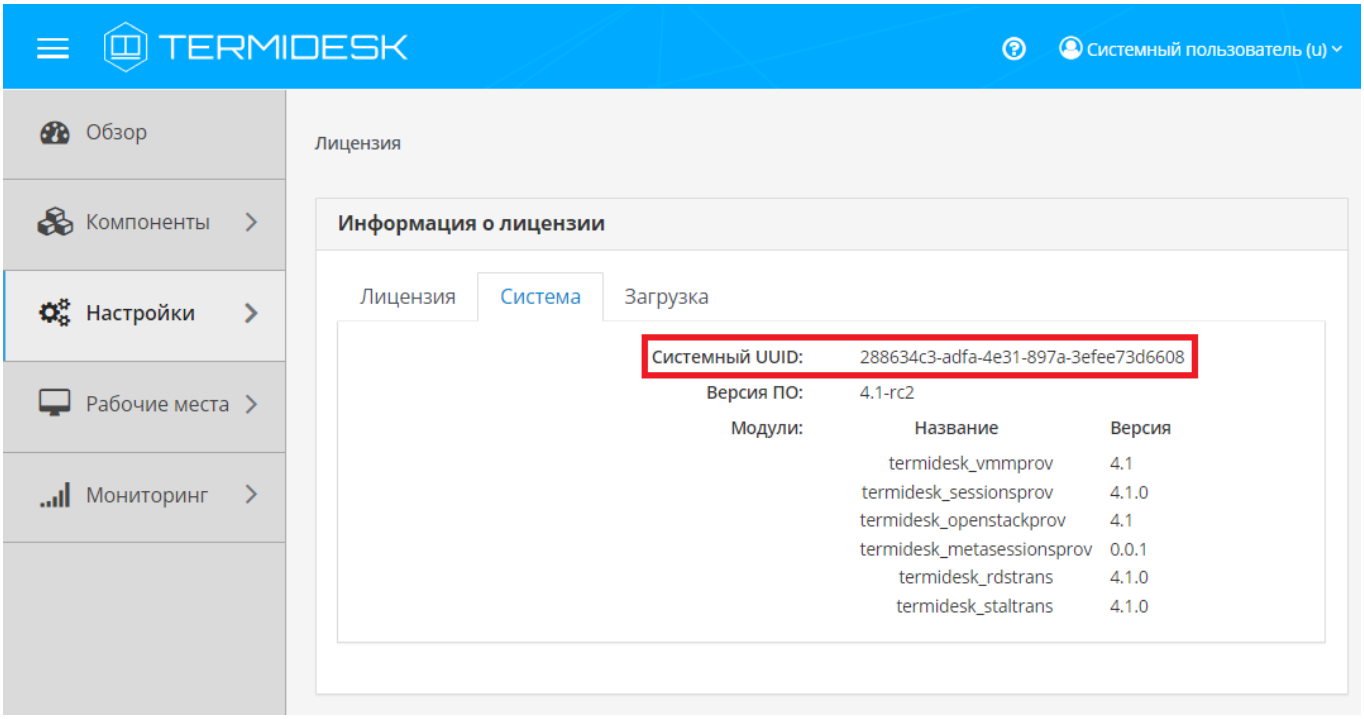

Рисунок 68 – Расположение информации о системном UUID

По завершении заполнения полей нужно нажать экранную кнопку **[Отправить запрос ключа активации]**.

Для получения лицензионного ключа на приобретенное количество лицензий следует перейти по ссылке `https://termidesk.ru/products/#request-key` и сформировать запрос, заполнив корректными данными следующие экранные поля:

- «Корпоративный email»;
- «Имя лица, запрашивающего лицензию»;
- «Системный UUID»;
- «Согласие на обработку персональных данных».

4.2 . Ввод лицензии

Для добавления лицензионного ключа в Termidesk в графическом интерфейсе управления следует перейти «Настройки - Лицензия - Загрузка». Нажав экранную кнопку **[Выбрать]**, указать путь к файлу с лицензионным ключом (см. Рисунок 69), а затем нажать экранную кнопку **[Загрузить]**.

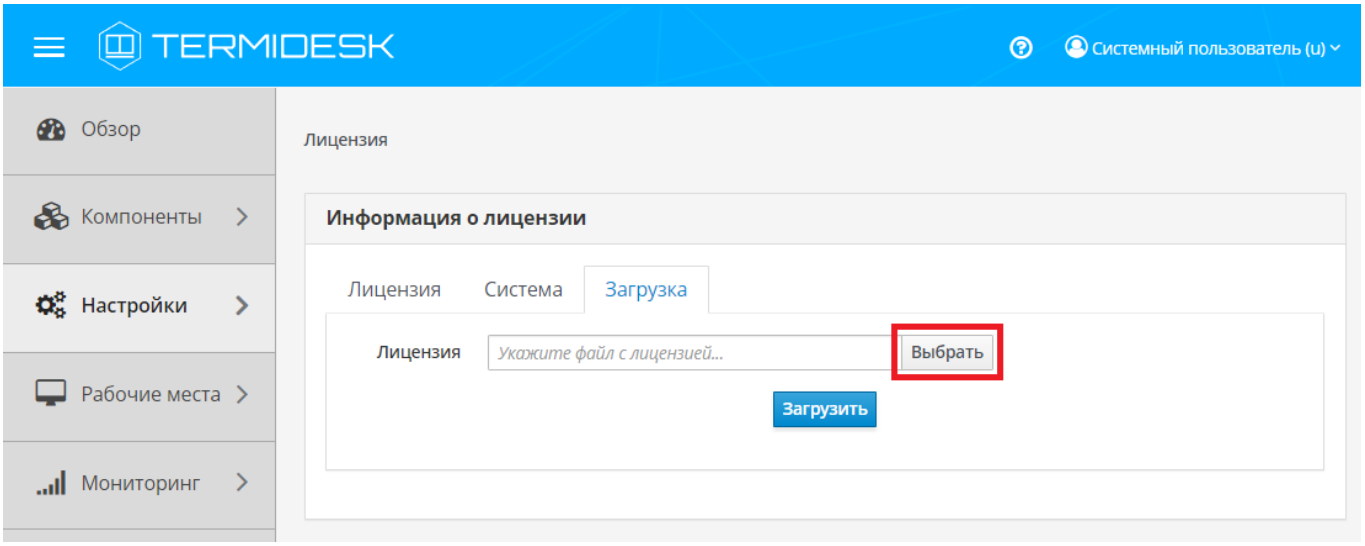

Рисунок 69 – Окно добавления файла с лицензией

4.3 . Проверка сведений о лицензии

Для просмотра информации об используемом лицензионном ключе следует перейти в графический интерфейс управления, выбрать «Настройки - Лицензия - Лицензия» и просмотреть сведения в следующих экранных полях:

- «Имя» – системное имя устройства, где функционирует Termidesk;
- «Организация» – наименование организации, для которой сформирован лицензионный ключ;
- «Email» – адрес электронной почты, указанный при запросе лицензионного ключа;
- «Конкурентные соединения» – максимально возможное количество одновременных соединений с BPM;
- «Доступные гостевые ОС» – варианты доступных для установленного вида лицензии гостевых ОС.

5 . РАСШИРЕННАЯ НАСТРОЙКА

5.1 . Действия, доступные в меню BMT

5.1.1 . Изменение настроек сети

Для изменения настроек сети нужно в главном меню BMT нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`). Будет выполнен переход в меню расширенных настроек (см. Рисунок 70).

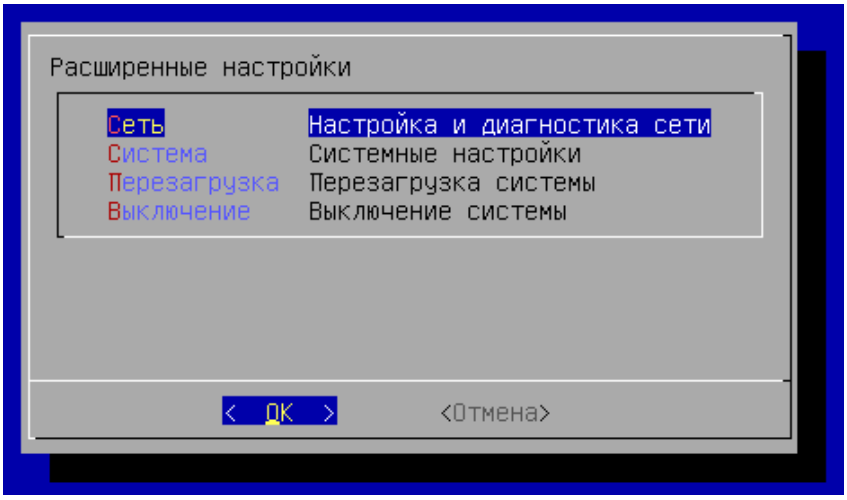

Рисунок 70 – Меню расширенных настроек VA

В меню настроек выбрать пункт «Сеть», затем «Настройка» (см. Рисунок 71). Далее действия не будут отличаться от процесса первичного конфигурирования сетевых параметров (см. подраздел **Первичная настройка BMT**).

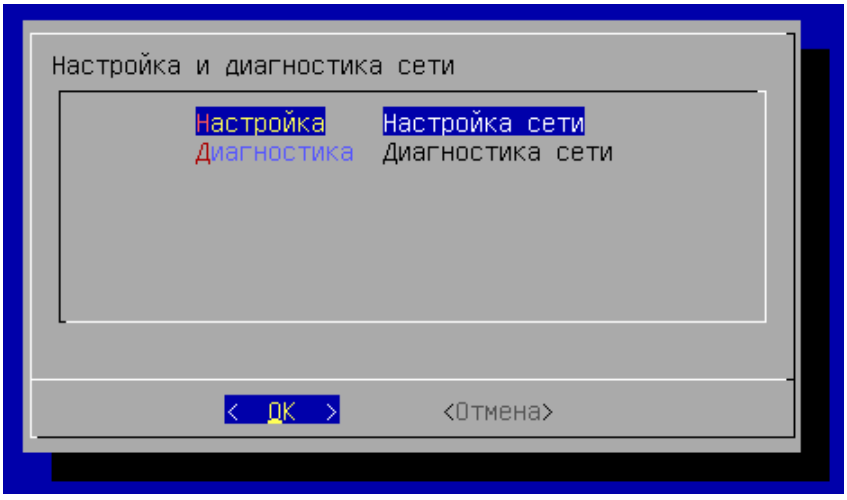

Рисунок 71 – Переход к конфигурации сети

5.1.2 . Диагностика сети

Для диагностики сети нужно перейти в меню расширенных настроек, нажав клавишу **<F2>** в главном меню ВМТ, ввести текущий пароль администратора (по умолчанию после установки - `admin`). Далее выбрать пункт «Сеть», затем «Диагностика».

Ввести имя или IP-адрес узла (см. Рисунок 72), подключение к которому нужно проверить. ВМТ выполнит команду `ping` до указанного узла.

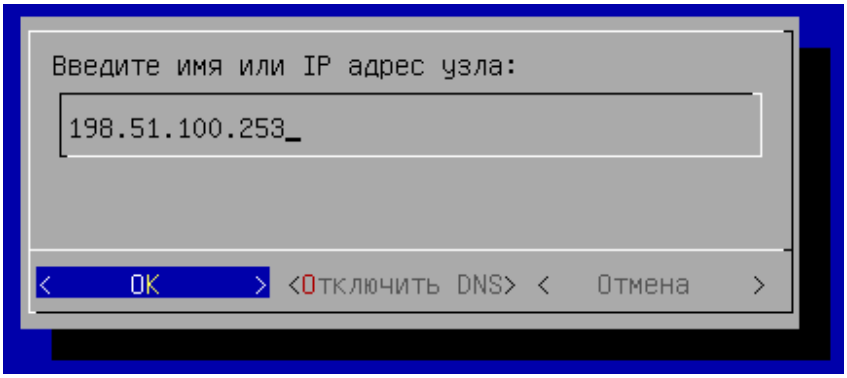

Рисунок 72 – Окно диагностики сети

Результат диагностики сети будет показан в окне (см. Рисунок 73).

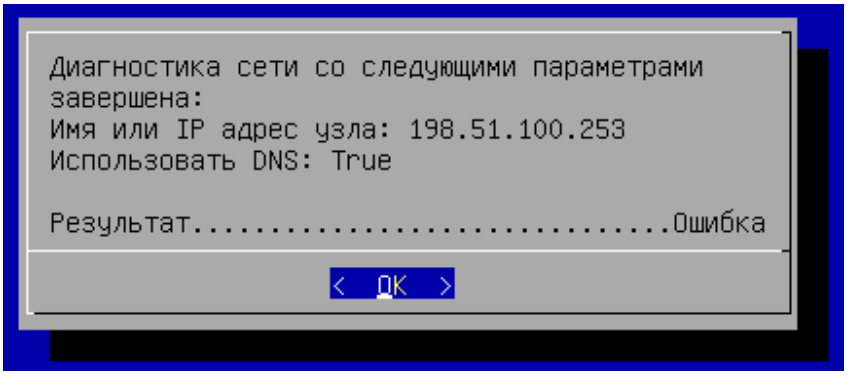

Рисунок 73 – Результат диагностики сети

5.1.3 . Изменение имени узла ВМТ

Для изменения имени узла нужно в главном меню ВМТ нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`). Далее выбрать пункт «Система», затем «Имя хоста».

В появившемся окне (см. Рисунок 74) задать новое имя узла ВМТ и нажать экранную кнопку **[OK]**, дождаться применения изменений. Новое имя узла будет отображено в главном меню ВМТ.

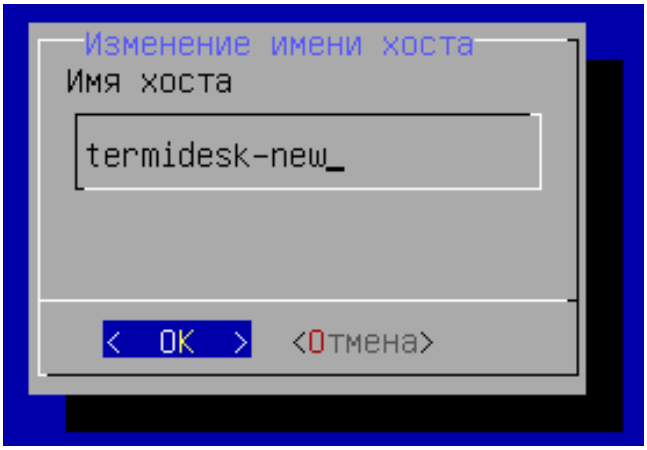

Рисунок 74 – Редактирование имени узла ВМТ

5.1.4 . Смена пароля администратора

После установки ВМТ по умолчанию используется логин `admin` с паролем `admin` для доступа к веб-интерфейсу Termidesk и ряду функций управления.

Для смены пароля нужно:

- в главном меню ВМТ нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`);
- далее выбрать пункт «Система», затем «Пароль»;
- в появившемся окне (см. Рисунок 75) ввести текущий пароль (после установки пароль по умолчанию - `admin`) и нажать экранную кнопку **[OK]**;
- затем (см. Рисунок 76) ввести новый пароль, переключиться на строку «Повтор пароля» при помощи клавиши **<↓>** (**<СТРЕЛКА ВНИЗ>**) и повторить ввод пароля. Подтвердить данные, нажав экранную кнопку **[OK]**.

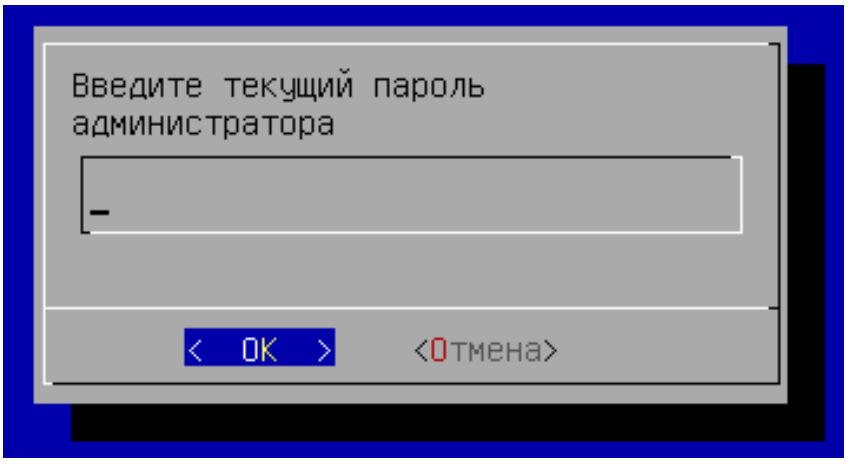

Рисунок 75 – Ввод текущего пароля администратора

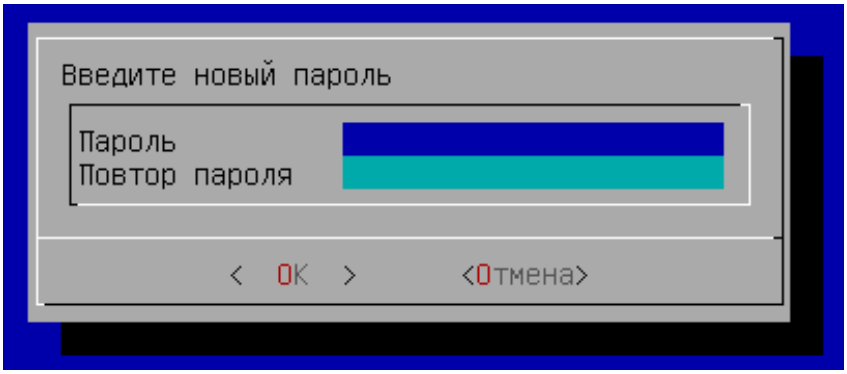

Рисунок 76 – Ввод нового пароля администратора

5.1.5 . Замена SSL-сертификата веб-сервера через меню BMT

Для доступа к веб-интерфейсу Termidesk по протоколу HTTPS на этапе первичной настройки нужно было указать расположение сертификата и закрытый ключ к нему. Если этот пункт был пропущен, сгенерировался самоподписанный сертификат.

Для замены самоподписанных SSL-сертификатов необходимо:

- в главном меню BMT нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`);
- далее выбрать пункт «Система», затем «Сертификаты»;
- в появившемся окне (см. Рисунок 77) выбрать «Настройка»;

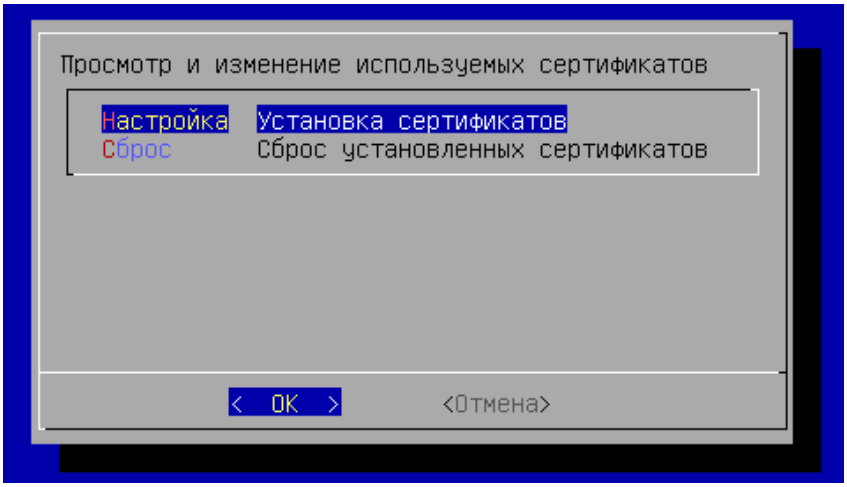

Рисунок 77 – Переход к установке сертификатов

- далее действия не будут отличаться от процесса настройки сертификатов при первичном конфигурировании - нужно указать (см. Рисунок 78):
  - IP-адрес хоста, на котором расположены сертификаты и ключ. У BMT должен быть сетевой доступ к хосту;
  - порт подключения;
  - полный путь к файлу закрытого ключа формата `.key`;
  - полный путь к файлу сертификата формата `.pem`;

- полный путь к файлу проверки цепочки сертификатов формата `.crt`;

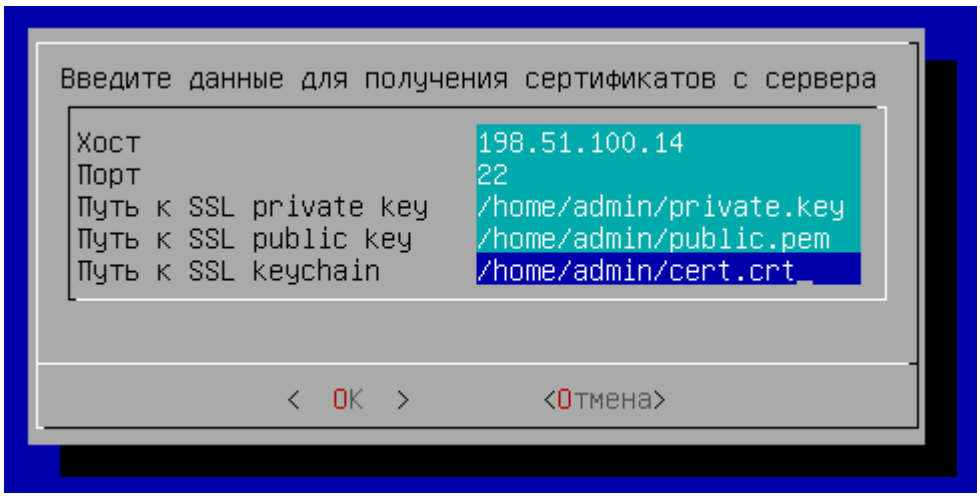

Рисунок 78 – Данные для получения сертификатов

- в следующем окне (см. Рисунок 79) заполнить имя пользователя и пароль для подключения к указанному на предыдущем шаге хосту. Для задания пароля переключиться на строку «Пароль» при помощи клавиши **<↓>** (**<СТРЕЛКА ВНИЗ>**) и ввести его, затем переключиться таким же способом на строку «Повтор пароля» и повторить ввод пароля. Поле «Имя пользователя» при этом изменится на другой цвет, как неактивное в данный момент, ввод пароля отображен не будет. Подтвердить данные, нажав экранную кнопку **[OK]**.

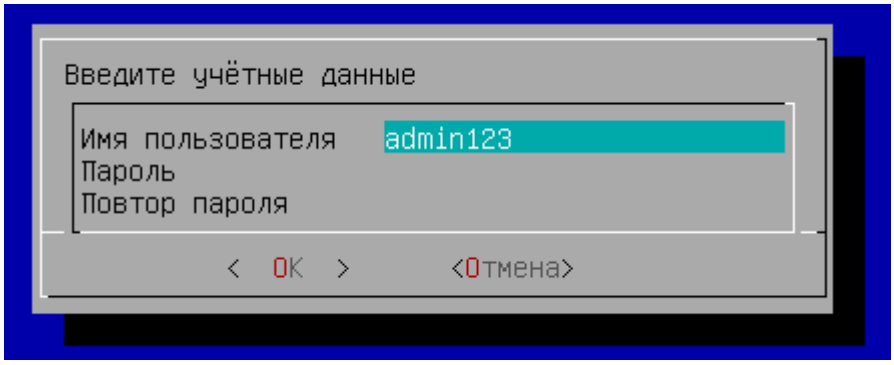

Рисунок 79 – Заполнение учетных данных

5.1.6 . Сброс установленных сертификатов веб-сервера через меню BMT

Сброс установленной конфигурации приведет к замене текущих сертификатов на самоподписанные.

Для сброса установленных сертификатов веб-сервера следует:

- в главном меню BMT нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`);
- далее выбрать пункт «Система», затем «Сертификаты»;

- в появившемся окне (см. Рисунок 80) выбрать «Сброс» и согласиться со сбросом конфигурации сертификатов;

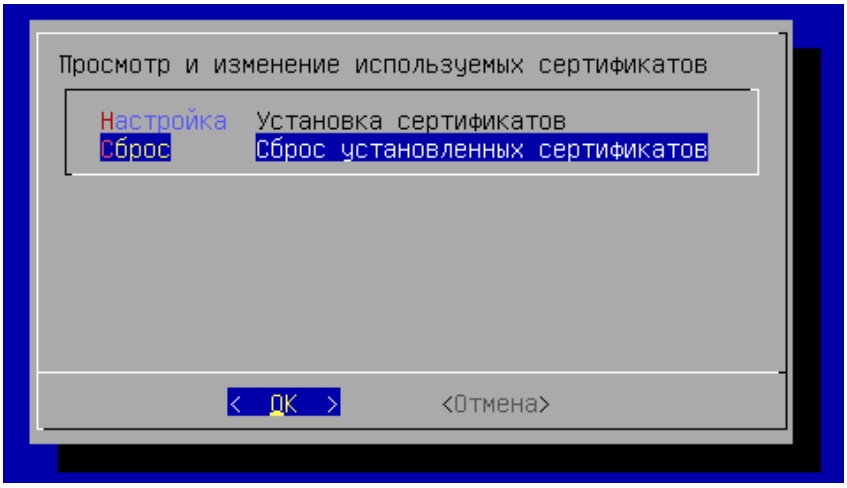

Рисунок 80 – Переход к сбросу конфигурации сертификатов

- дождаться выполнения операции;
- убедиться, что в главном меню BMT (см. Рисунок 81) отображено использование самоподписанных SSL-сертификатов.

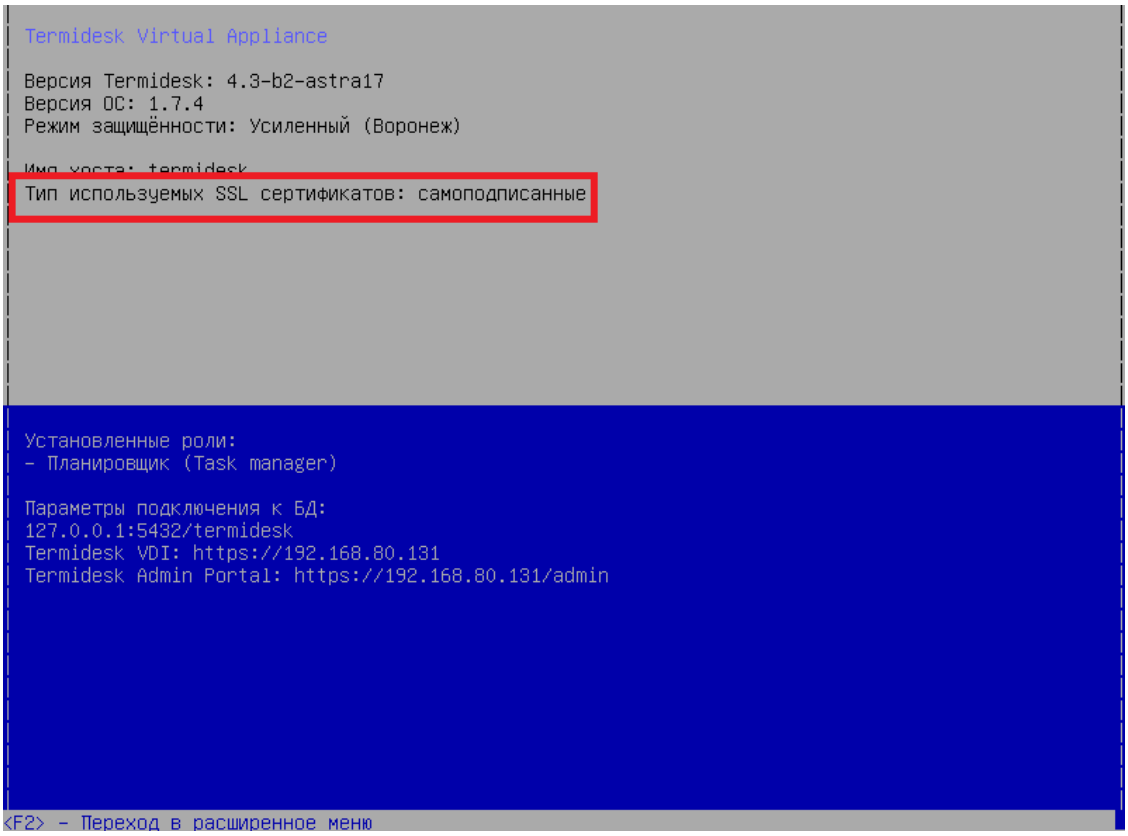

Рисунок 81 – Главное меню BMT

5.1.7 . Экспорт параметров Termidesk

Параметры DJANGO_SECRET_KEY и HEALTH_CHECK_ACCESS_KEY используются в Termidesk для проверок пересылаемых между компонентами данных и состояния API. При распределенной установке эти параметры должны быть одинаковыми на всех узлах ВМТ.

Для передачи конфигураций и параметров ВМТ использует механизм `ETCD` и сетевые порты 2379, 2380 (протоколы TCP/UDP).

> ⚠ Синхронизация указанных параметров не подразумевает синхронизацию учетных данных для подключения RabbitMQ.

Для экспорта параметров с ноды ВМТ нужно:

- в главном меню ВМТ нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`);
- далее выбрать пункт «Система», затем «Синхронизация»;
- в появившемся окне (см. Рисунок 82) выбрать «Экспорт ключей»;

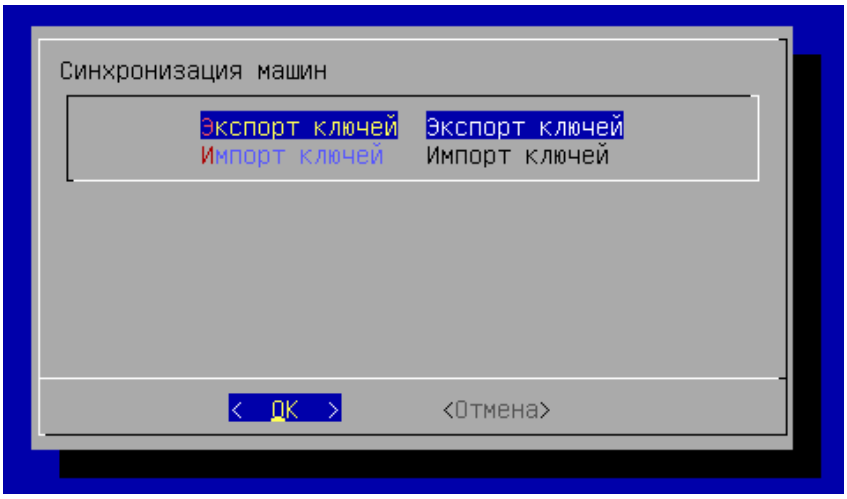

Рисунок 82 – Переход к экспорту ключей

- задать секретное слово, которое будет использоваться при импорте ключей на другую ноду ВМТ;

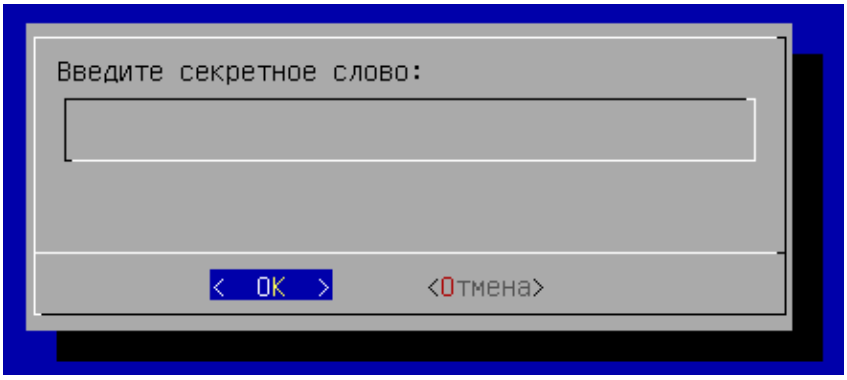

Рисунок 83 – Создание секретного слова

- запомнить сгенерированный временный пароль для синхронизации (см. Рисунок 84), который будет использоваться при импорте ключей на другую ноду ВМТ.

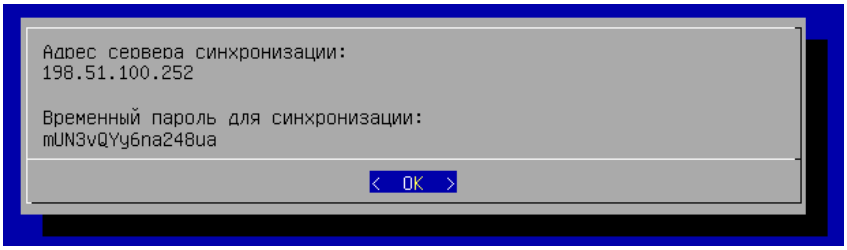

Рисунок 84 – Параметры для синхронизации между нодами

5.1.8 . Импорт параметров Termidesk

Для импорта параметров на ноду ВМТ нужно:

- в главном меню ВМТ нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`);
- далее выбрать пункт «Система», затем «Синхронизация»;
- в появившемся окне (см. Рисунок 85) выбрать «Импорт ключей»;

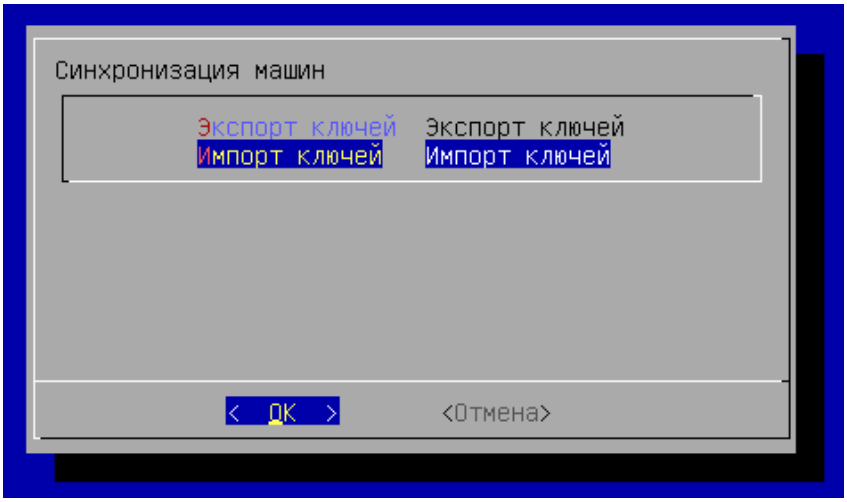

Рисунок 85 – Переход к импорту ключей

- ввести параметры синхронизации, полученные при экспорте ключей с другой ноды (см. подраздел **Экспорт параметров Termidesk**). Нажать экранную кнопку **[OK]** и дождаться сообщения об успешном применении конфигурации.

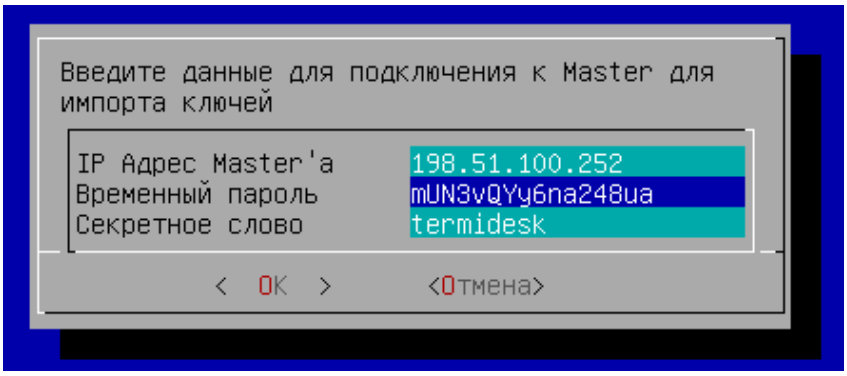

Рисунок 86 – Ввод параметров синхронизации

5.2 . Действия, доступные в веб-интерфейсе BMT

5.2.1 . Обзор доступных функций веб-интерфейса

Доступ к веб-интерфейсу управления BMT осуществляется из веб-браузера по протоколу HTTPS с указанием URL-адреса подключения: `https://<IP-адрес_BMT>:8443/`.

Веб-интерфейс BMT позволяет администратору выполнить ряд задач по настройке и управлению BMT, а именно:

- настроить ноды BMT в режиме высокой доступности по протоколу VRRP через `keepalived`;
- проверить состояние служб BMT и выполнить их останов, запуск и перезапуск;
- сформировать и выгрузить журналы работы BMT.

Сразу после аутентификации администратору доступна панель, содержащая список основных функций:

- «Обзор» - предоставляет информацию об основных параметрах, характеризующих BMT (см. Рисунок 87), таких, как:
  - версия установленной ОС;
  - время доступности BMT, информация об активных пользователях системы (доступна при нажатии ссылки «<количество> users» в блоке «Время доступности системы»), полученная утилитой `w`;
  - назначенные IP-адреса;
  - версия Termidesk;
  - список установленных ролей;
  - графики использования процессора («CPU Usage») и памяти («Memory Usage»).
- «Службы» - предоставляет информацию о состоянии служб BMT, позволяет управлять ими;
- «VRRP» - позволяет выполнить настройку нод BMT в режиме высокой доступности;

- «Журналы» - позволяет сформировать общий архив с файлами журналов BMT и выгрузить его.

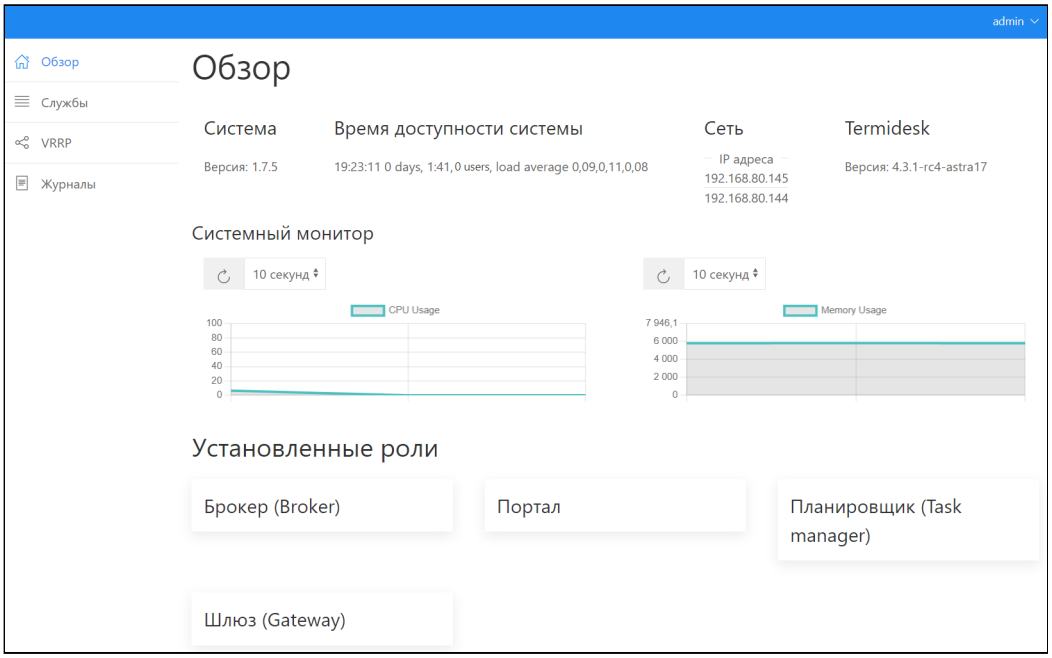

Рисунок 87 – Отображение функции «Обзор»

5.2.2 . Управление состоянием служб BMT

Для просмотра состояния служб, критичных для BMT, необходимо перейти в функцию «Службы» веб-интерфейса BMT.

Список служб, отображаемый на странице, зависит от перечня ролей (или роли), выбранных при первичной настройке BMT. Список может быть отсортирован по столбцам «Служба», «Загружено», «Состояние», «Подробности».

Для управления состоянием службы нужно выбрать строку с наименованием службы (за раз можно выбрать только одну) и воспользоваться экранными кнопками **[Запустить]**, **[Остановить]** или **[Перезапустить]**, в зависимости от действия, которое нужно произвести над службой.

Список обновится после того, как выбранная ранее служба изменила свое состояние после выполненного действия, не ожидая обновления по таймеру (по умолчанию 10 секунд). Для принудительного обновления статусов можно воспользоваться экранной кнопкой, приведенной на рисунке (см. Рисунок 88).

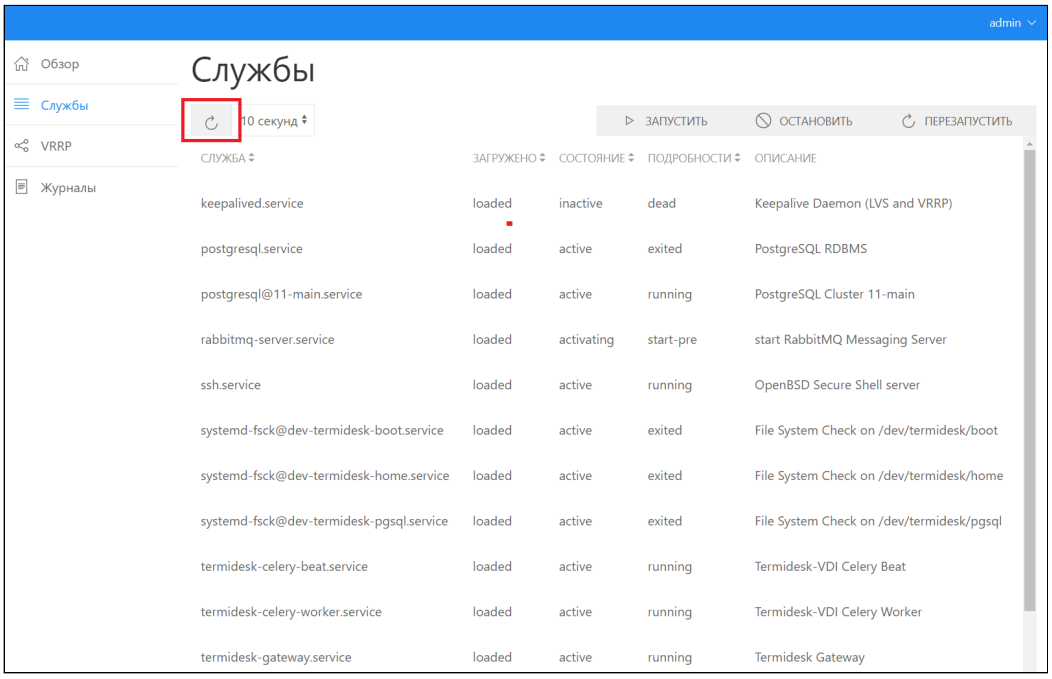

Рисунок 88 – Отображение функции «Службы»

5.2.3 . Настройка режима высокой доступности

Для настройки режима высокой доступности ВМТ нужно перейти в функцию «VRRP» веб-интерфейса ВМТ и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 1).

Таблица 1 – Данные для настройки режима высокой доступности

Параметр	Описание
«router id»	Идентификатор узла. По умолчанию - значение сетевого имени ВМТ (`hostname`), недоступно для изменения
«script_user»	Пользователь, от имени которого будет выполнен запуск службы `keepalived`. Значение по умолчанию - «root», недоступно для изменения
«interface»	Выбор интерфейса, для которого будет применена конфигурация
«virtual_router_id»	Уникальный идентификатор виртуального роутера. Значение по умолчанию - «105»
«priority»	Приоритет ноды относительно других. Нода с наибольшим приоритетом переходит в состояние «MASTER». Значение по умолчанию - «128»
«auth_pass»	Парольная фраза, которая будет использована для синхронизации VRRP между нодами. Значение по умолчанию - «ksedimret»
«virtual_ip_address/mask»	Виртуальный адрес, который будет присвоен службой `keepalived` для данной ноды в формате `<IP-адрес>/<маска>`, например 192.0.2.1/255.255.255.0

Изменения, внесенные в параметры, применяются в файле `/etc/keepalived/keepalived.conf`, содержимое которого динамически отображается в правой части страницы.

Для применения изменений нужно последовательно воспользоваться экранными кнопками **[ПРИМЕНИТЬ КОНФИГУРАЦИЮ]** и **[ВКЛЮЧИТЬ VRRP]**. Для сброса конфигурации к значениям по умолчанию нужно воспользоваться экранной кнопкой, приведенной на рисунке (см. Рисунок 89).

> Если конфигурация VRRP была выполнена ранее и применена, значения параметров будут отображать текущие настройки. При действующей конфигурации VRRP экранная кнопка **[ВКЛЮЧИТЬ VRRP]** будет заменена кнопкой **[ОТКЛЮЧИТЬ VRRP]**.

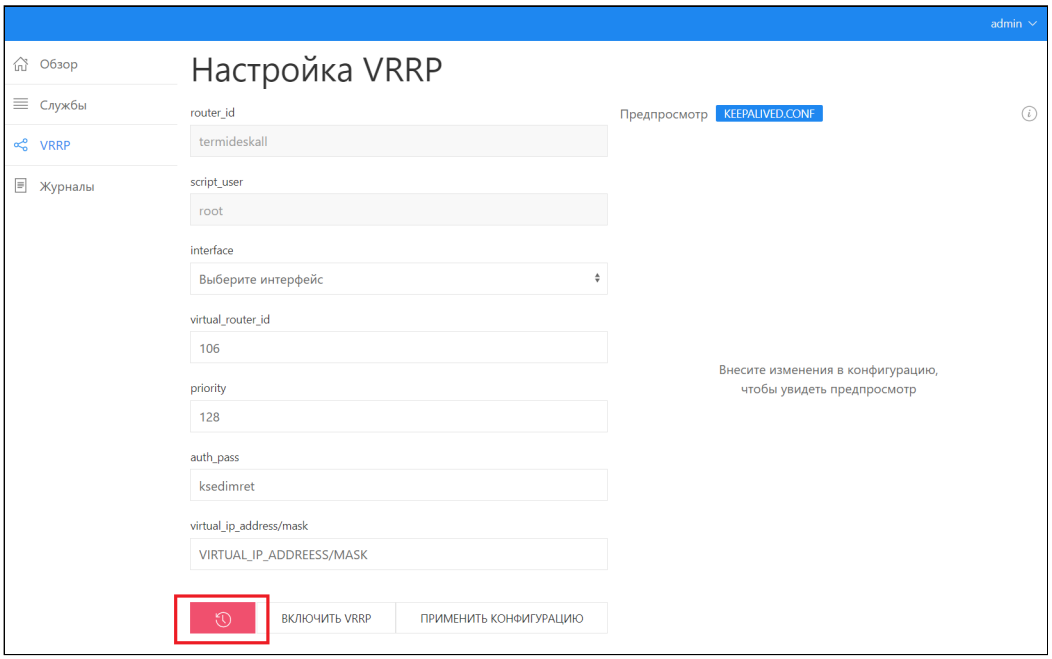

Рисунок 89 – Отображение функции «VRRP»

5.2.4 . Формирование и выгрузка журнала ВМТ

Для формирования архива с файлами журналов и конфигурации нужно перейти в функцию «Журналы» веб-интерфейса ВМТ и нажать экранную кнопку, отмеченную на рисунке (см. Рисунок 90). Будет сформирован архив формата `.tar.gz` с именем `TDVAlogs_<временная_метка>.tar.gz`, в который будут помещены файлы из каталогов `/var/log/` и `/etc/opt/termidesk-vdi/`.

По завершении формирования архива станут доступны следующие действия (см. Рисунок 91):

- скачать сформированный архив;
- обновить архив. Новый архив перезапишет предыдущий без подтверждения. До окончания формирования нового архива предыдущий не удалится;
- удалить архив. После применения этого действия архив будет удален, строка с его наименованием и размером исчезнет.

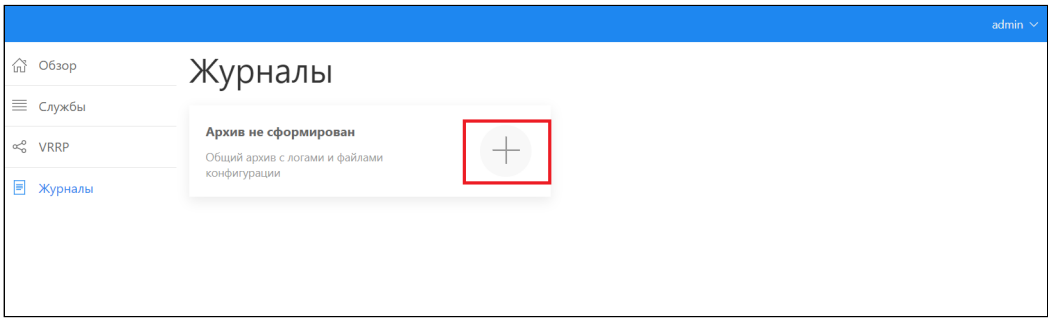

Рисунок 90 – Отображение функции «Журналы»

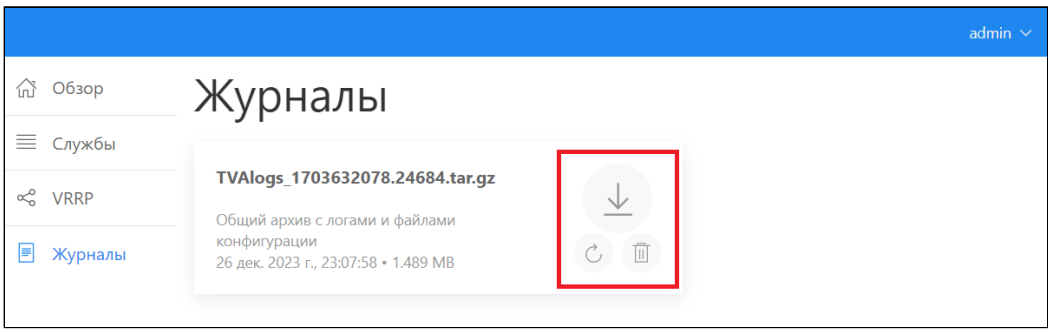

Рисунок 91 – Доступные действия с архивом

5.3 . Удаленное подключение к ВМТ

Для расширенной настройки ВМТ может использоваться удаленное подключение по протоколу SSH к ВМ, на которой он предварительно установлен.

По умолчанию удаленное подключение по протоколу SSH включено. Для управления режимом включения и отключения SSH нужно:

- в главном меню ВМТ нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`);
- далее выбрать пункт «Сеть», затем «SSH»;
- выбрать нужный вариант: «on» (включение) или «off» (выключение) и нажать экранную кнопку **[OK]**. После выбора режима настройки применятся автоматически и сразу.

Данные по умолчанию для подключения:

- логин: `admin`;
- пароль: `admin`. В случае, если пароль был изменен через меню ВМТ (см. подраздел **Смена пароля администратора**), при подключении нужно использовать измененный пароль.

Сертификат, используемый для удаленного подключения, генерируется при первом запуске ВМТ. Таким образом для каждого экземпляра ВМТ будет использоваться индивидуальный сертификат.

5.4 . Резервное копирование БД

Резервное копирование БД, созданной СУБД Postgres-11 можно выполнить утилитой `pg_dump`:

```
:$ pg_dump -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W
--format=t > <имя_файла_для_сохранения_БД.tar>
```

где:

`-d <наименование БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`-h <IP-адрес_хоста>` - IP-адрес узла, где расположена БД. Если БД устанавливалась локально, нужно указать `localhost`;

`-p <порт>` - порт для подключения к БД. При стандартных настройках используется `5432`;

`-U <пользователь>` - имя пользователя для подключения. При стандартных настройках используется имя `termidesk`;

`-W` - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать `ksedimret`;

`--format=t` - ключ для экспорта БД в формате `tar`;

`<имя_файла_для_сохранения_БД.tar>` - имя и формат файла (`tar`) для сохранения БД.

5.5 . Восстановление БД из резервной копии

Восстановление БД из резервной копии выполняется командой:

```
:$ pg_restore -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь>
-W -f <файл_копии_БД.tar>
```

где:

`-d <наименование БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`-h <IP-адрес_хоста>` - IP-адрес узла, где расположена БД. Если используется локальная БД, нужно указать `localhost`;

`-p <порт>` - порт для подключения к БД. При стандартных настройках используется `5432`;

`-U <пользователь>` - имя пользователя для подключения. При стандартных настройках используется имя `termidesk`;

`-W` - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать `ksedimret`;

`-f <файл_копии_БД.tar>` - путь к файлу резервной копии БД.

6 . ЗАВЕРШЕНИЕ РАБОТЫ

6.1 . Завершение работы ВМТ

Для завершения работы ВМТ и выключения ВМ следует:

- перейти в меню расширенных настроек, нажав клавишу **<F2>** в главном меню ВМТ;
- выбрать пункт «Выключение»;
- подтвердить действие (см. Рисунок 92), нажав экранную кнопку **[Да]**.

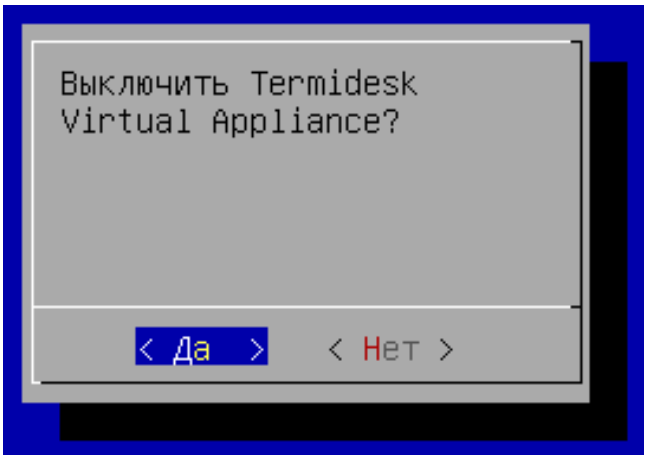

Рисунок 92 – Подтверждение выключения ВМТ

7 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
ВМ	Виртуальная машина
ВМТ	Виртуальный модуль Termidesk
ОС	Операционная система
ПО	Программное обеспечение
API	Application Programming Interface (интерфейс прикладного программирования)
DHCP	Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста)
DNS	Domain Name System (система доменных имен)
GRUB	GRand Unified Bootloader (загрузчик ОС)
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
IP	Internet Protocol (межсетевой протокол)
KVM	Kernel-based Virtual Machine (программное решение, обеспечивающее виртуализацию в среде Linux на платформе, которая поддерживает аппаратную виртуализацию на базе Intel VT (Virtualization Technology) либо AMD SVM (SecureVirtual Machine))
OVA	Open Virtual Appliance (открытое виртуальное устройство)
OVF	Open Virtualization Format (формат открытой виртуализации)
QEMU	Quick Emulator (средства эмуляции аппаратного обеспечения)
REST	Representational State Transfer (программная архитектура, определяющая условия работы API)
SSH	Secure Shell Protocol (протокол защищенной передачи информации)
SSL	Secure Sockets Layer (криптографический протокол)
Termidesk	Программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk»
UUID	Unique User Identifier (уникальный идентификатор пользователя)
VRRP	Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности)

Адрес: 119571, г. Москва, Ленинский проспект, д. 119А, помещ. 9Н
Сайт: https://termidesk.ru
Телефон: +7 (495) 975-1-975

Общий e-mail: info@uveon.ru
Отдел продаж: sales@uveon.ru
Техническая поддержка: support@uveon.ru