



ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ

СЛЕТ.10001-01 91 03

Версия 5.1. Выпуск от ноября 2024

**Компонент «Виртуальный модуль
Termidesk»**

ОГЛАВЛЕНИЕ

| | | |
|---------|---|----|
| 1 . | ОБЩИЕ СВЕДЕНИЯ..... | 4 |
| 1.1 . | О документе..... | 4 |
| 1.2 . | Назначение компонента «Виртуальный модуль Termidesk»..... | 4 |
| 1.3 . | Комплект поставки | 5 |
| 1.4 . | Типографские соглашения | 5 |
| 2 . | ПОДГОТОВКА К РАБОТЕ | 6 |
| 2.1 . | Получение образов ВМТ | 6 |
| 2.2 . | Порядок загрузки ВМТ..... | 6 |
| 3 . | УСТАНОВКА..... | 8 |
| 3.1 . | Порядок развертывания ВМТ | 8 |
| 3.2 . | Базовые настройки ВМТ | 9 |
| 3.3 . | Установка в режиме «Ферма» | 14 |
| 3.3.1 . | Комплексная установка | 14 |
| 3.3.2 . | Рекомендованная установка | 16 |
| 3.3.3 . | Произвольная установка | 23 |
| 3.4 . | Установка в режиме «База данных» | 27 |
| 3.5 . | Установка в режиме «Агрегатор» | 28 |
| 3.6 . | Проверка работоспособности | 29 |
| 4 . | ЛИЦЕНЗИРОВАНИЕ | 31 |
| 4.1 . | Получение лицензионного ключа..... | 31 |
| 4.2 . | Ввод лицензии | 33 |
| 4.3 . | Проверка сведений о лицензии..... | 33 |
| 5 . | РАСШИРЕННАЯ НАСТРОЙКА | 34 |
| 5.1 . | Действия, доступные в меню ВМТ | 34 |
| 5.1.1 . | Изменение настроек сети | 34 |
| 5.1.2 . | Диагностика сети | 35 |

| | | |
|----------|---|----|
| 5.1.3 . | Изменение имени узла ВМТ | 35 |
| 5.1.4 . | Смена пароля администратора | 36 |
| 5.1.5 . | Замена сертификата через меню ВМТ | 37 |
| 5.1.6 . | Сброс установленных сертификатов через меню ВМТ | 37 |
| 5.1.7 . | Экспорт параметров Termidesk | 37 |
| 5.1.8 . | Импорт параметров Termidesk | 38 |
| 5.1.9 . | Изменение настроек подключения к БД | 39 |
| 5.1.10 . | Изменение настроек подключения к RabbitMQ | 39 |
| 5.2 . | Действия, доступные в веб-интерфейсе ВМТ | 39 |
| 5.2.1 . | Обзор доступных функций веб-интерфейса | 39 |
| 5.2.2 . | Управление состоянием служб ВМТ | 41 |
| 5.2.3 . | Настройка режима высокой доступности | 42 |
| 5.2.4 . | Формирование и выгрузка журнала ВМТ | 43 |
| 5.2.5 . | Просмотр и замена сертификата через веб-интерфейс ВМТ | 44 |
| 5.2.6 . | Управление датой и временем на ВМТ | 47 |
| 5.3 . | Резервное копирование и восстановление БД | 49 |
| 5.4 . | Удаленное подключение к ВМТ | 49 |
| 5.4.1 . | Резервное копирование БД | 50 |
| 5.4.2 . | Восстановление БД из резервной копии | 50 |
| 6 . | ЗАВЕРШЕНИЕ РАБОТЫ | 52 |
| 6.1 . | Завершение работы ВМТ | 52 |
| 7 . | ПРИНЯТЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ | 53 |
| 8 . | ПЕРЕЧЕНЬ СОКРАЩЕНИЙ | 54 |

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.

Состав ВМТ:

- ОС Astra Linux Special Edition 1.8.1;
- программные пакеты из состава подключенного в ВМТ репозитория Termidesk:
 - termidesk-vdi;
 - termidesk-gateway;
 - termidesk-digsig-keys;
 - termidesk-assistant-server;
- система управления базами данных (СУБД) PostgreSQL версии 15;
- брокер сообщений RabbitMQ;
- 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 `termidesk-virtual-appliance_<версия>_kvm.qcow2`;
- для платформы виртуализации VMware:
 - 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 . Типографские соглашения

В настоящем документе приняты следующие типографские соглашения:

- моноширинный шрифт – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, 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 можно получить 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**.

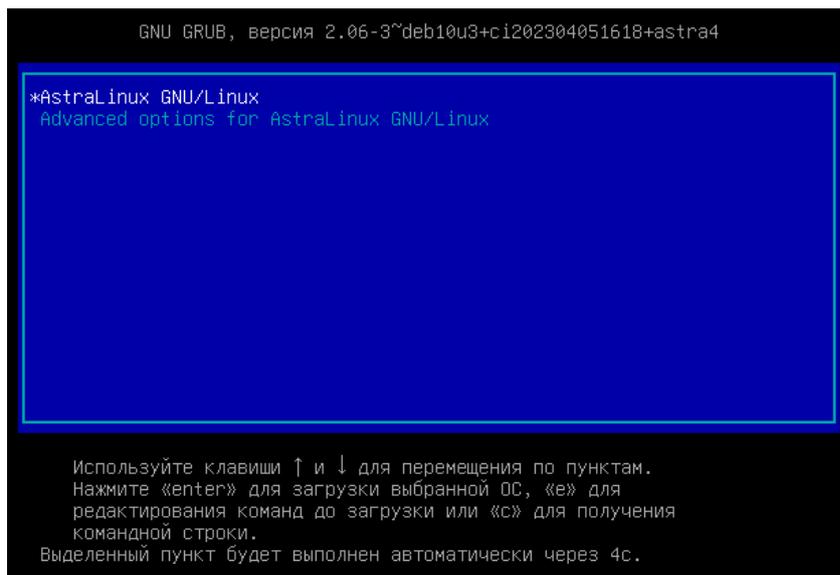


Рисунок 1 – Меню GRUB

3. УСТАНОВКА

3.1. Порядок развертывания ВМТ

ВМТ может быть установлен в следующих режимах:

- «Ферма» - используется для установки узлов фермы Termidesk;
- «Агрегатор» - используется для установки портала «Агрегатор»;
- «База данных» - используется для установки узла с СУБД. Узел может содержать несколько баз данных (БД).

 Ферма - логическое объединение узлов, взаимодействующих с одной БД.

Для режима «Ферма» используются три основных типа установки:

- «Комплексная» - используется для быстрой установки узла фермы с полным набором компонентов Termidesk. Этот тип применяется для ознакомления с функционалом Termidesk в тестовой среде;
- «Рекомендованная» - используется для установки узла фермы с минимальным набором компонентов («Менеджер рабочих мест» и «Универсальный диспетчер»), необходимых для функционирования Termidesk. Для установки требуется подключение к СУБД. Этот тип обычно применяется для установки фермы в распределенном варианте без обеспечения отказоустойчивости;
- «Произвольная» - используется для установки отдельных компонентов Termidesk («Менеджер рабочих мест», «Менеджер рабочих мест (очереди)», «Универсальный диспетчер», «Шлюз») или инфраструктурных компонентов (брокер сообщений RabbitMQ), исходя из потребности в них. Этот тип обычно применяется для установки фермы в распределенном отказоустойчивом варианте или для расширения узлов существующей фермы.

Общий порядок развертывания ВМТ определяется сценариями использования, приведенными в таблице (см. Таблица 1).

Таблица 1 – Сценарии использования ВМТ

| Сценарий | Установка |
|--|--|
| Комплексная установка узла фермы для ознакомления с функционалом Termidesk | Последовательность установки: 1) выбрать режим «Ферма»; 2) выбрать тип установки «Комплексная» |

| Сценарий | Установка |
|--|---|
| Установка фермы в распределенном варианте без обеспечения отказоустойчивости компонентов | Последовательность установки: 1) установить первый узел ВМТ с режимом «База данных»; 2) установить второй узел ВМТ с режимом «Ферма». Выбрать тип установки «Рекомендованная». Выбрать пункт «Менеджер рабочих мест». После установки выполнить экспорт ключей; 3) установить третий узел ВМТ с режимом «Ферма». Выбрать тип установки «Рекомендованная». Выбрать пункт «Диспетчер». Выполнить импорт ключей с узла, установленного на шаге 2); 4) (опционально) установить четвертый узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольная». Выбрать пункт «Шлюз». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне), выполнить импорт ключей с узла, установленного на шаге 2) |
| Установка фермы в распределенном варианте с обеспечением отказоустойчивости компонентов | Последовательность установки: 1) установить первый узел ВМТ с режимом «База данных»; 2) установить второй узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольная». Выбрать пункт «RabbitMQ». Не привязывать узел к существующей ферме (будет соответствующий запрос в диалоговом окне); 3) установить третий узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольная». Выбрать пункты «Taskman» и «Celeryman». Не привязывать узел к существующей ферме (будет соответствующий запрос в диалоговом окне). После установки выполнить экспорт ключей; 4) установить четвертый узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольная». Выбрать пункты «Taskman» и «Celeryman». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне), выполнить импорт ключей с узла, установленного на шаге 3); 5) установить пятый узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольный». Выбрать пункт «Диспетчер». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне), выполнить импорт ключей с узла, установленного на шаге 3); 6) установить шестой узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольный». Выбрать пункт «Диспетчер». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне), выполнить импорт ключей с узла, установленного на шаге 3); 7) (опционально, если планируется использование «Шлюза Termidesk») установить седьмой и восьмой узлы ВМТ с режимом «Ферма». Выбрать вариант установки «Произвольная». Выбрать пункт «Шлюз». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне), выполнить импорт ключей с узла, установленного на шаге 3) |
| Установка портала «Агрегатор» | Последовательность установки: 1) установить первый узел ВМТ с режимом «База данных»; 2) установить второй узел ВМТ с режимом «Агрегатор»; 3) (опционально, если планируется использование «Шлюза Termidesk») установить третий узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольная». Выбрать пункт «Шлюз». Не привязывать узел к существующей ферме (будет соответствующий запрос в диалоговом окне) |

3.2 . Базовые настройки ВМТ

Для первичной настройки ВМТ 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>.

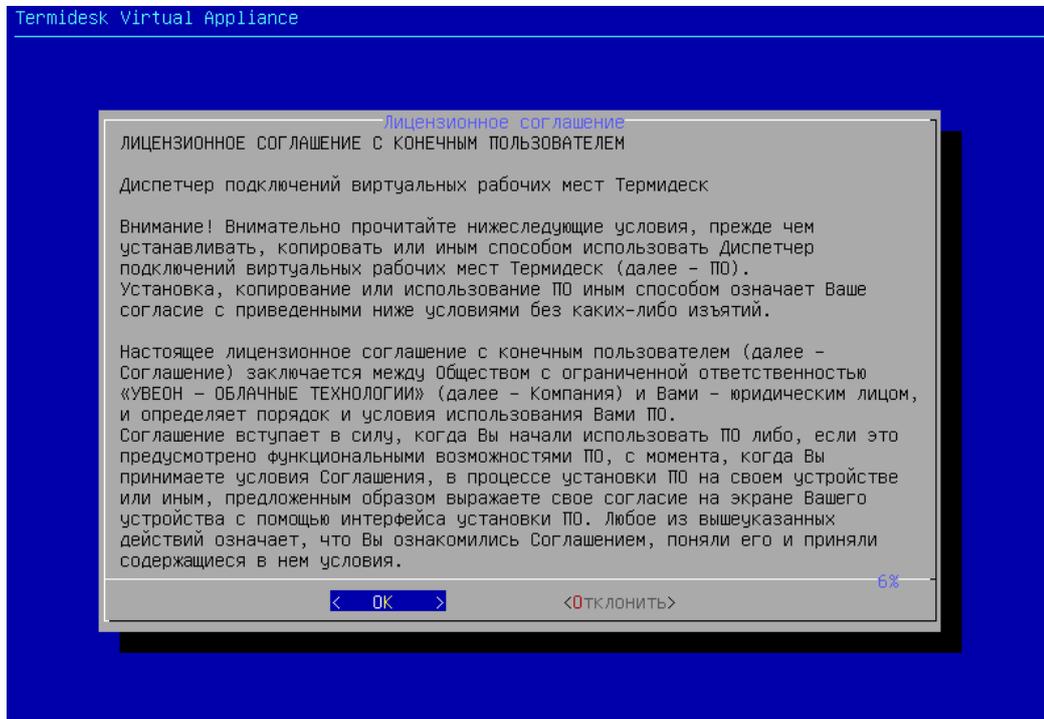


Рисунок 2 – Лицензионное соглашение

- 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;

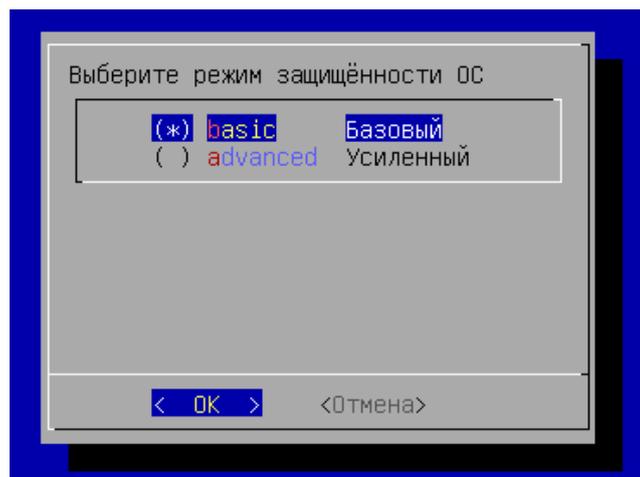


Рисунок 3 – Выбор режима защищенности ОС

- 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);

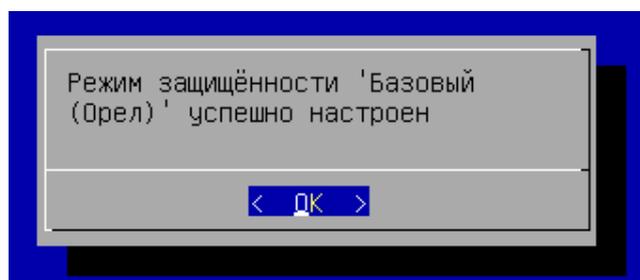


Рисунок 4 – Сообщение о настроенном режиме защищенности

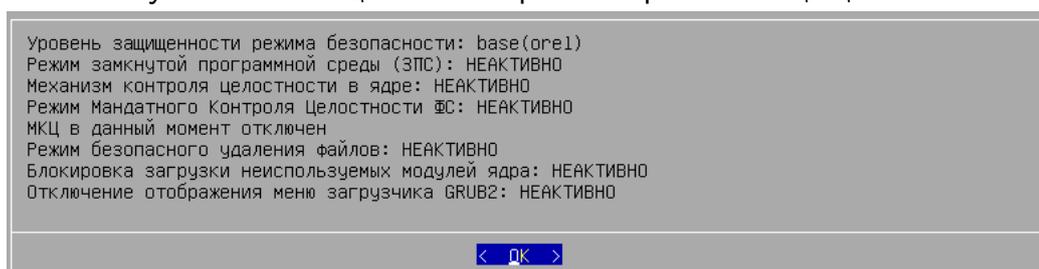


Рисунок 5 – Информационное сообщение об активированных механизмах безопасности на примере режима «Базовый»

- 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 ВМТ используется в домене. Указанный hostname 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).

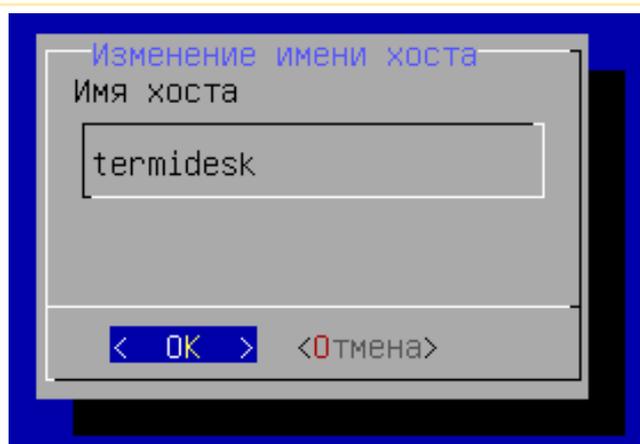


Рисунок 6 – Ввод имени хоста

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

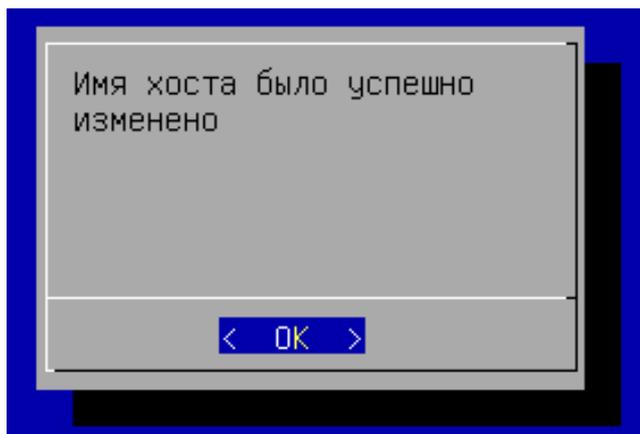


Рисунок 7 – Информационное сообщение об успешном изменении имени хоста

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

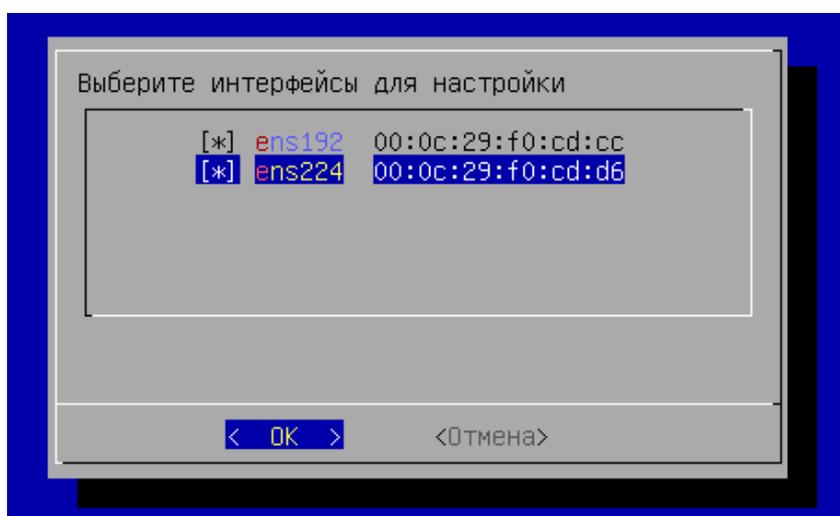


Рисунок 8 – Выбор сетевого интерфейса

- 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.

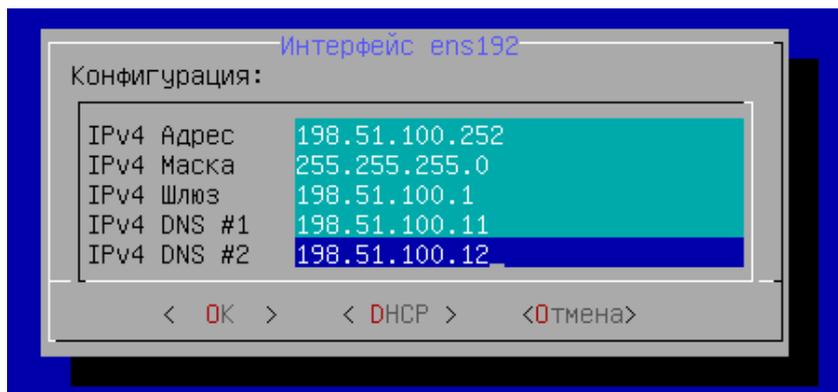


Рисунок 9 – Задание статических сетевых настроек

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

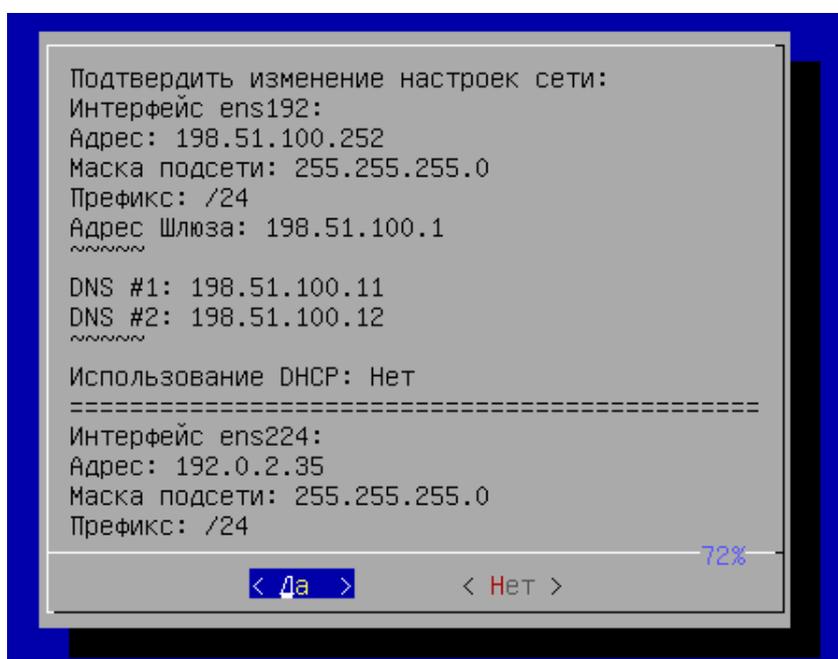


Рисунок 10 – Подтверждение сетевых настроек

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

```

Конфигурация сетевых интерфейсов завершена.
Итоговая (общая) конфигурация сетевых интерфейсов:

Интерфейс ens192:
Адрес: 198.51.100.252
Маска подсети: 255.255.255.0
Префикс: /24
Адрес Шлюза: 198.51.100.1
~~~~~
DNS #1: 192.51.100.11
DNS #2: 192.51.100.12
~~~~~
Использование DHCP: Нет

Интерфейс ens224:
Адрес: 192.0.2.35
Маска подсети: 255.255.255.0
Префикс: /24
Адрес Шлюза: 192.0.2.1
~~~~~
DNS #1: 192.0.2.2
DNS #2: 192.0.2.3
~~~~~
Использование DHCP: Нет
    
```

Рисунок 11 – Информационное сообщение об успешной конфигурации сетевых интерфейсов

3.3 . Установка в режиме «Ферма»

3.3.1 . Комплексная установка

Комплексная установка позволяет быстро установить и настроить на узле все необходимые компоненты Termidesk.

⚠ Комплексную установку рекомендуется использовать только для ознакомления в тестовой среде.

В процессе установки нужно:

- выполнить базовую настройку ВМТ (см. раздел **Базовые настройки ВМТ**);
- выбрать режим установки «Ферма» (см. Рисунок 12):

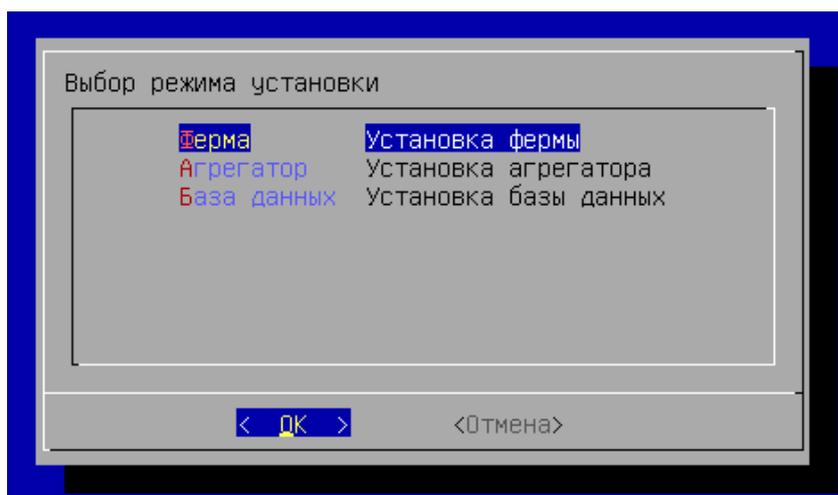


Рисунок 12 – Выбор режима установки

- далее выбрать тип установки в режиме фермы «Комплексная» (см. Рисунок 13);

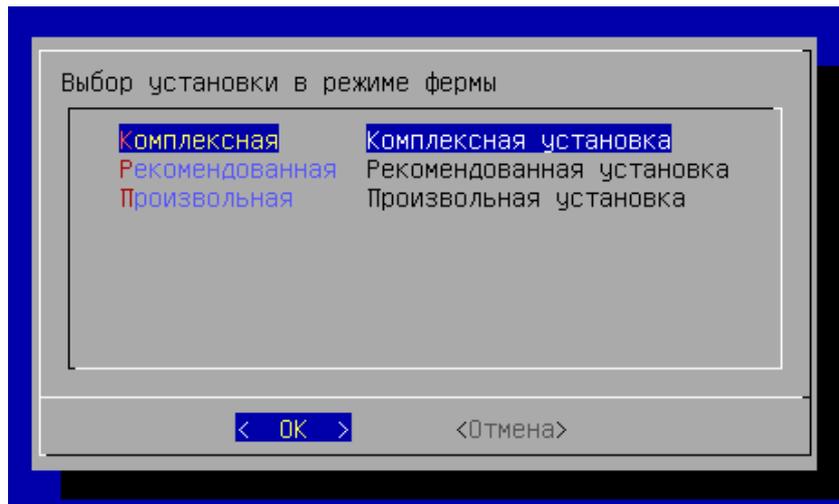


Рисунок 13 – Выбор комплексного типа установки в режиме фермы

После выполнения шагов по комплексной установке фермы произойдет переход в окно управления ВМТ (см. Рисунок 14). Службы Termidesk будут автоматически активированы, перезагрузка не требуется. IP-адрес, отображаемый в главном окне ВМТ, соответствует IP-адресу первого настроенного интерфейса.

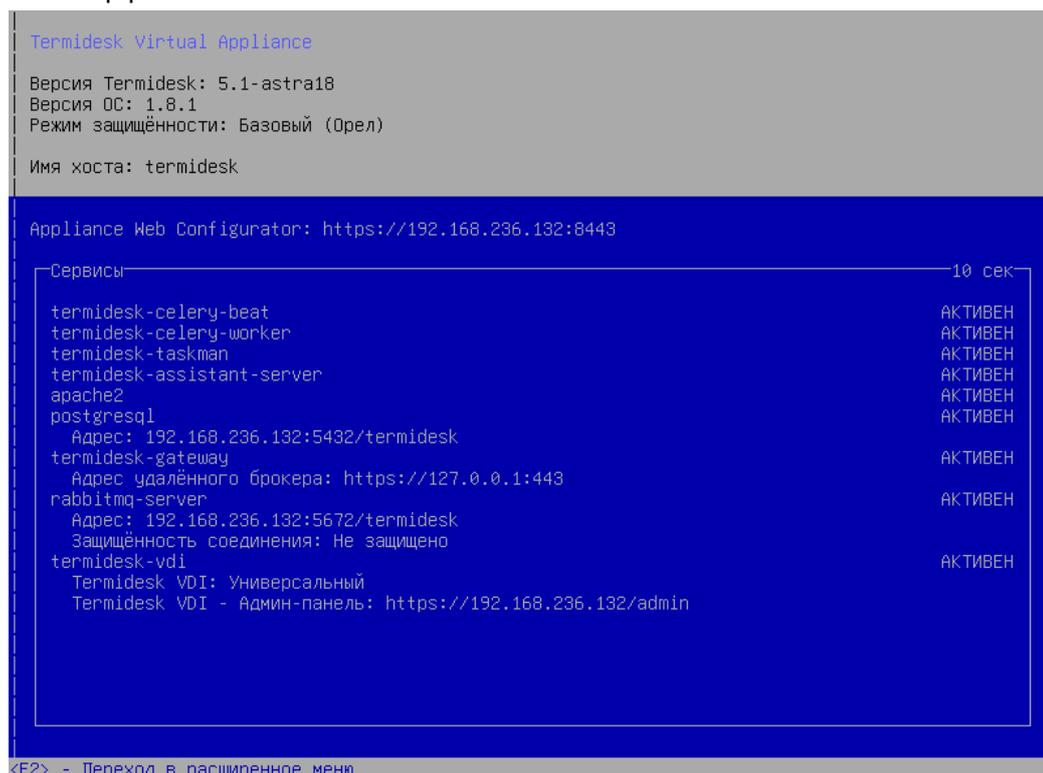


Рисунок 14 – Окно управления ВМТ

- ❗ После установки на узле будут установлены следующие компоненты:
 - «Универсальный диспетчер» с ролями «Портал администратора» и «Портал пользователя». После установки будет запущена служба termidesk-vdi;

- «Менеджер рабочих мест». После установки будут запущены службы `termidesk-taskman`, `termidesk-celery-beat`, `termidesk-celery-worker`;
- серверная часть компонента «Удаленный помощник». После установки будет запущена служба `termidesk-assistant-server`;
- веб-сервер Apache;
- СУБД PostgreSQL, настройка БД будет выполнена автоматически. Для подключения к БД используются стандартные параметры:
 - наименование БД - `termidesk`;
 - имя пользователя для подключения к БД - `termidesk`;
 - пароль для подключения к БД - `ksedimret`;
 - номер порта, используемого для соединения с сервером СУБД - `5432`;
- «Шлюз». После установки будет запущена служба `termidesk-gateway`;
- брокер сообщений RabbitMQ. После установки будет запущена служба `rabbitmq-server`. Для подключения к RabbitMQ используются стандартные параметры:
 - номер порта, используемого для соединения с RabbitMQ - `5672`;
 - виртуальный узел, к которому будет производиться подключение - `termidesk`;
 - имя пользователя для подключения - `termidesk`;
 - пароль для подключения - `ksedimret`.

3.3.2 . Рекомендованная установка

Рекомендованная установка позволяет создать узел фермы с минимальным набором компонентов для функционирования Termidesk.

В процессе установки нужно:

- выполнить базовую настройку ВМТ (см. раздел **Базовые настройки ВМТ**);
- выбрать режим установки «Ферма» (см. Рисунок 15):

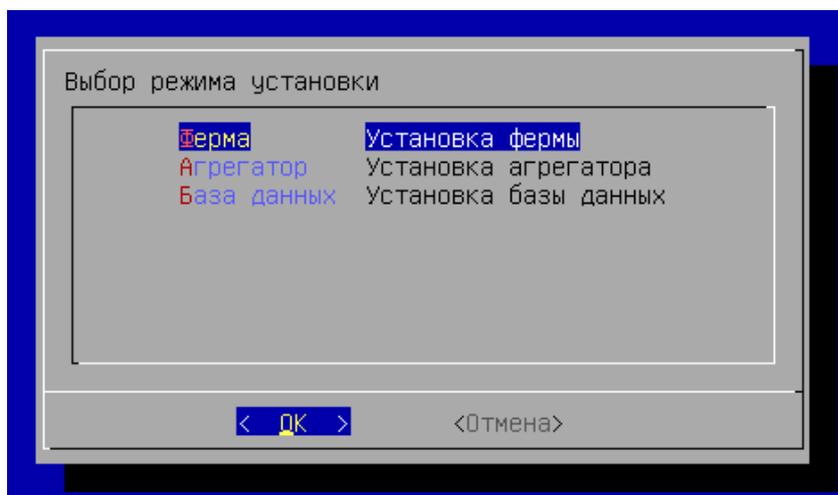


Рисунок 15 – Выбор режима установки

- далее выбрать тип установки «Рекомендованная» (см. Рисунок 16);

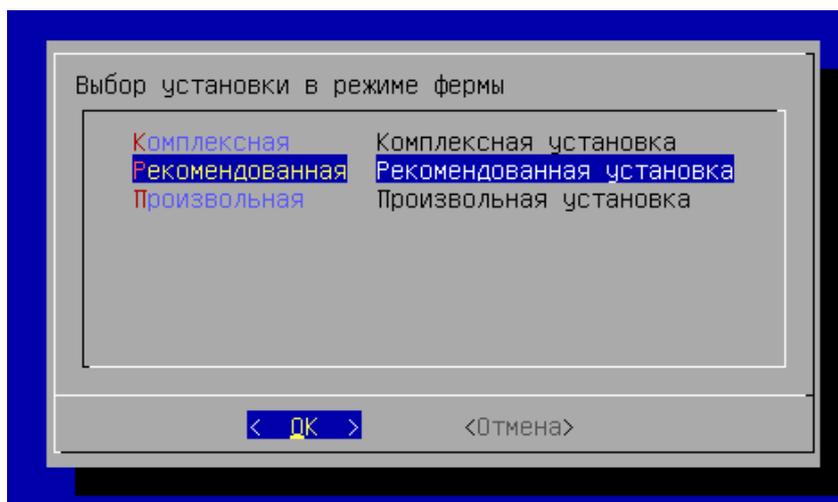


Рисунок 16 – Выбор рекомендованного типа установки в режиме фермы

- в окне «Выбор установки в режиме фермы (рекомендованная)» следует выбрать компонент, который будет установлен на узел (см. Рисунок 17).

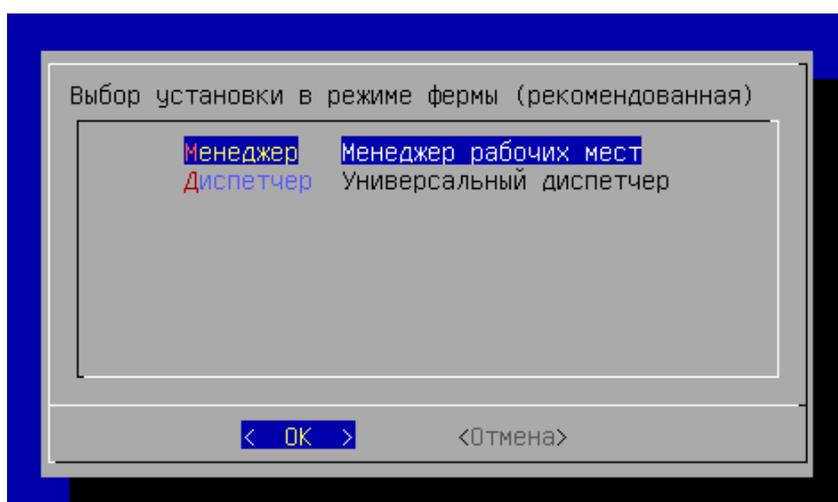


Рисунок 17 – Выбор компонента для установки

В зависимости от выбранного варианта дальнейшие действия по настройке будут отличаться.

Если был выбран пункт «Менеджер», далее нужно выполнить:

- настроить параметры подключения к СУБД (см. Рисунок 18):

⚠ Все указанные IP-адреса должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре организации. Следует учесть, что в БД должны отсутствовать записи (необходимо использовать чистую БД). Также узел не должен использовать экземпляры БД, предназначенные для других компонентов Termidesk (портала «Агрегатор»).

- «Имя пользователя»: имя пользователя для подключения к БД (termidesk, значение по умолчанию при установке БД из состава ВМТ);
- «Пароль»: пароль для подключения к БД (ksedimret, значение по умолчанию при установке БД из состава ВМТ);
- «Хост»: IP-адрес или FQDN узла с установленной СУБД;
- «Порт»: номер порта, используемого для соединения с сервером СУБД (стандартный порт 5432);
- «База данных»: наименование БД (termidesk, значение по умолчанию при установке БД из состава ВМТ);

❗ Если указанная БД не существует, но у пользователя есть права на ее создание, то будет отображен запрос «Подключение к базе данных прошло успешно, однако, база данных <имя> не существует. Желаете создать?». Следует ответить **<Да>**, если новая БД действительно нужна.

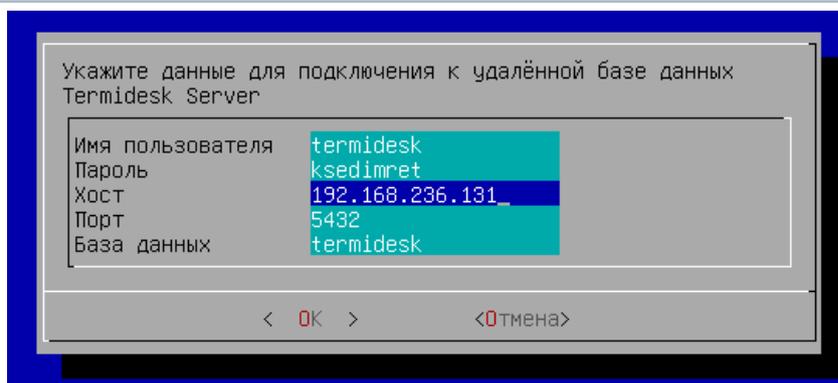


Рисунок 18 – Ввод параметров подключения к СУБД

- убедиться, что подключение успешно выполнено, результат отобразится в информационном окне (см. Рисунок 19):

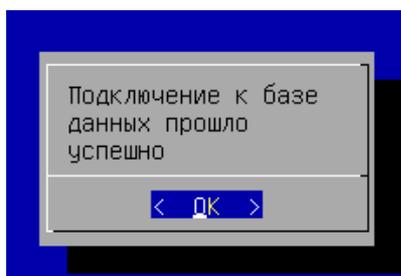


Рисунок 19 – Информационное сообщение о результате подключения к БД

- указать протокол (см. Рисунок 20), используемый для подключения к БД. При выборе значения «Disabled» защищенное соединение при подключении к БД использоваться не будет;

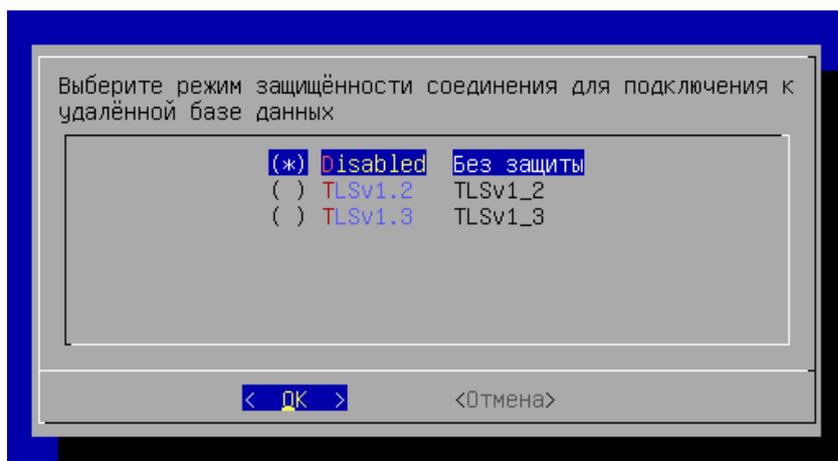


Рисунок 20 – Выбор протокола для подключения к БД

- задать параметры для подключения к RabbitMQ (см. Рисунок 21):
 - «Имя пользователя»: имя пользователя для подключения к RabbitMQ, по умолчанию termidesk;
 - «Пароль»: пароль для подключения к RabbitMQ, по умолчанию ksedimret;
 - «Хост»: в режиме рекомендованной установки RabbitMQ устанавливается на одном узле с компонентом «Менеджер рабочих мест»;
 - «Порт»: по умолчанию 5672;
 - «Очередь»: по умолчанию termidesk;

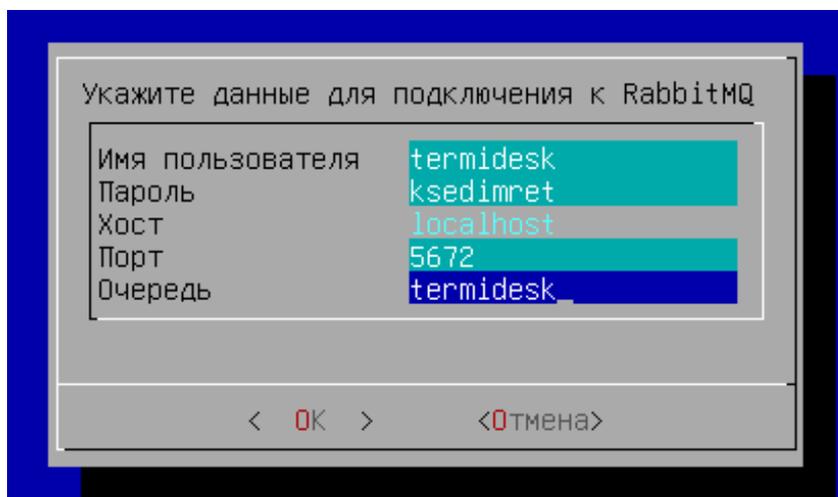


Рисунок 21 – Параметры для подключения к RabbitMQ

- выбрать протокол, используемый для подключения к RabbitMQ (см. Рисунок 22). При выборе значения «Disabled» защищенное соединение при подключении к RabbitMQ использоваться не будет;

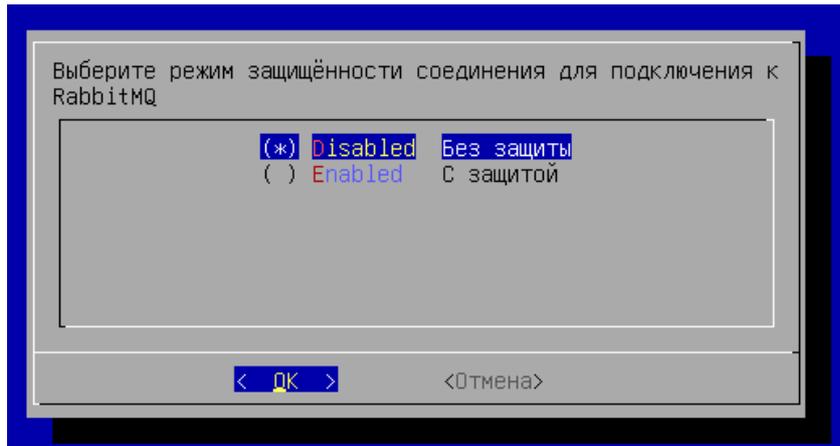


Рисунок 22 – Выбор протокола для подключения к RabbitMQ

- убедиться, что после установки произошел переход в окно управления ВМТ (см. Рисунок 23). Службы Termidesk будут автоматически активированы, перезагрузка не требуется. IP-адрес, отображаемый в главном окне ВМТ, соответствует IP-адресу первого настроенного интерфейса.

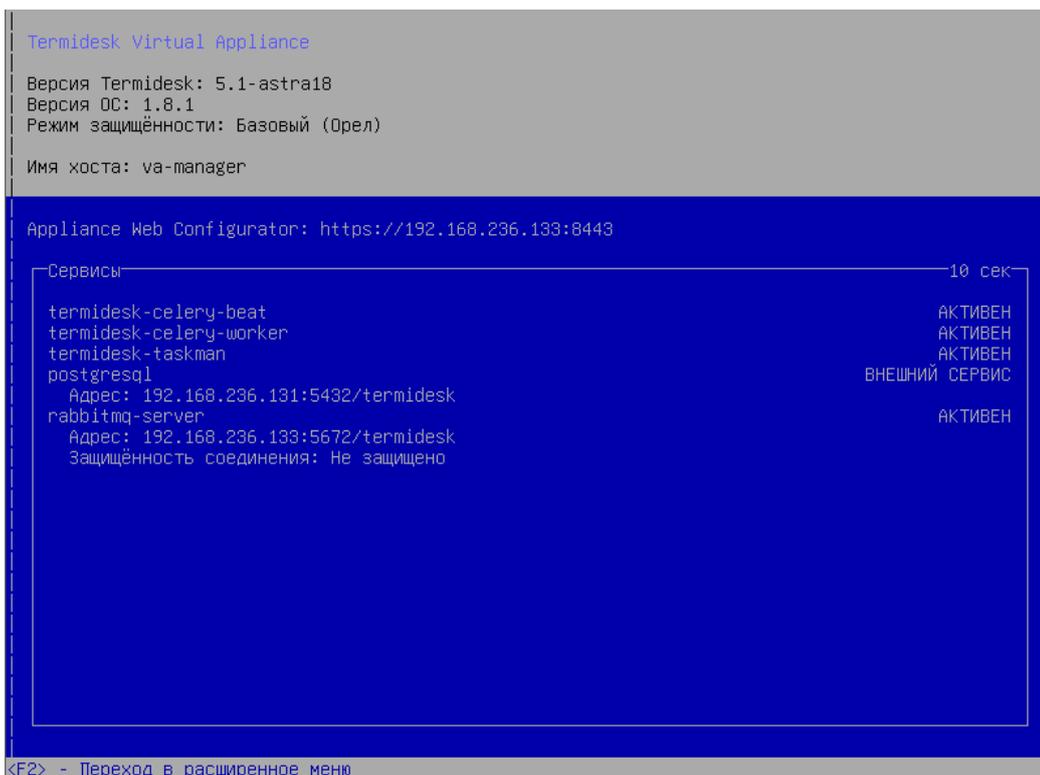


Рисунок 23 – Окно управления ВМТ с установленным компонентом «Менеджер рабочих мест»

❗ После установки на узле будут установлены:

- компонент «Менеджер рабочих мест», будут запущены службы termidesk-taskman, termidesk-celery-beat, termidesk-celery-worker;

- брокер сообщений RabbitMQ, будет запущена служба rabbitmq-server.

Если был выбран пункт «Диспетчер», далее нужно выполнить:

- экспортировать конфигурацию с узла компонента «Менеджер рабочих мест» (см. Рисунок 24) (см. подраздел **Экспорт параметров Termidesk**);
- ввести данные (см. Рисунок 24) для импортирования ключей:
 - «IP Адрес Master`а»: IP-адрес или FQDN узла с установленным компонентом «Менеджер рабочих мест»;
 - «Временный пароль»: временный пароль, созданный на узле компонента «Менеджер рабочих мест» при экспорте ключей;
 - «Секретное слово»: секретная фраза, заданная администратором при экспорте ключей с узла компонента «Менеджер рабочих мест»;

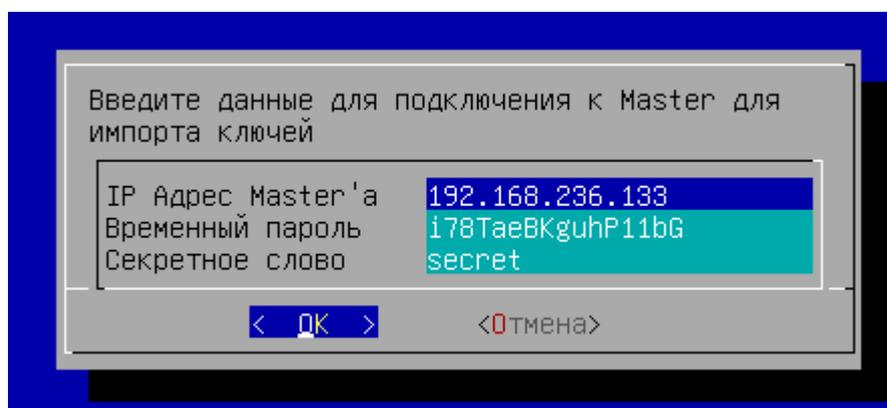


Рисунок 24 – Импортирование ключей с узла компонента «Менеджер рабочих мест»

- убедиться, что конфигурация была успешно применена, результат конфигурации узла отобразится в информационном окне (см. Рисунок 25):

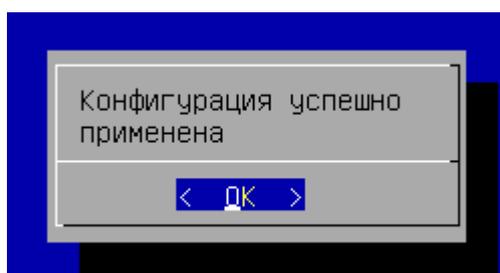


Рисунок 25 – Информационное сообщение о результате конфигурации узла

- задать параметры для подключения к СУБД и RabbitMQ (см. Рисунок 21) аналогично тому, как для узла компонента «Менеджер рабочих мест»;
- выбрать тип портала, который будет установлен для компонента «Универсальный диспетчер» (см. Рисунок 26):

- «Universal» - будет активирован «Портал универсальный», совмещающий в себе функции «Портала администратора» и «Портала пользователя»;
- «User» - будет активирован «Портал пользователя», предоставляющий пользовательский интерфейс Termidesk и интерфейс swagger для доступа к ограниченному списку модулей документации по командам REST API;
- «Admin» - будет активирован «Портал администратора», предоставляющий интерфейс управления Termidesk и интерфейс swagger для доступа к ограниченному списку модулей документации по командам REST API;

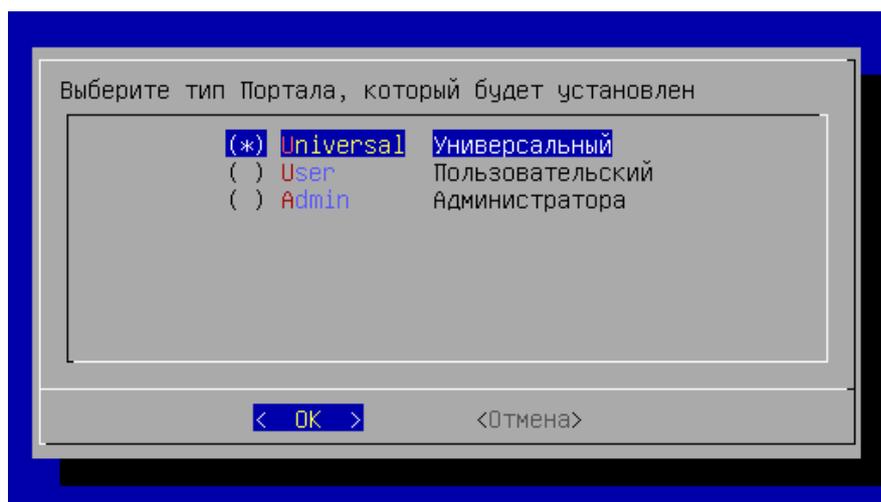


Рисунок 26 – Выбор типа портала, с которым будет установлен компонент «Универсальный диспетчер»

- убедиться, что после установки произошел переход в окно управления ВМТ (см. Рисунок 27). Службы Termidesk будут автоматически активированы, перезагрузка не требуется. IP-адрес, отображаемый в главном окне ВМТ, соответствует IP-адресу первого настроенного интерфейса.

```

Termidesk Virtual Appliance
Версия Termidesk: 5.1-astra18
Версия ОС: 1.8.1
Режим защищённости: Базовый (Орел)

Имя хоста: va-disp

Appliance Web Configurator: https://192.168.236.134:8443

Сервисы
-----
postgresql                               10 сек  ВНЕШНИЙ СЕРВИС
Адрес: 192.168.236.131:5432/termidesk
rabbitmq-server                           АКТИВЕН
Адрес: 192.168.236.133:5672/termidesk
Защищённость соединения: Не защищено
termidesk-vdi                             АКТИВЕН
Termidesk VDI: Универсальный
Termidesk VDI - Админ-панель: https://192.168.236.134/admin
termidesk-assistant-server                 АКТИВЕН
apache2                                   АКТИВЕН
    
```

<F2> - Переход в расширенное меню

Рисунок 27 – Окно управления ВМТ с установленным компонентом «Универсальный диспетчер»

i После установки «Универсального диспетчера» будут запущены службы `termidesk-vdi` и `apache2`. Если были выбраны «Портал универсальный» и «Портал администратора», то будет установлена серверная часть компонента «Удаленный помощник».

3.3.3 . Произвольная установка

Произвольная установка позволяет создать узел с отдельным компонентом Termidesk или инфраструктурным компонентом.

В процессе установки нужно:

- выполнить базовую настройку ВМТ (см. раздел **Базовые настройки ВМТ**);
- выбрать режим установки «Ферма»;
- далее выбрать тип установки «Произвольная»;
- в окне «Выбор установки в режиме фермы (произвольная)» следует выбрать компонент, который будет установлен на узел (см. Рисунок 28).

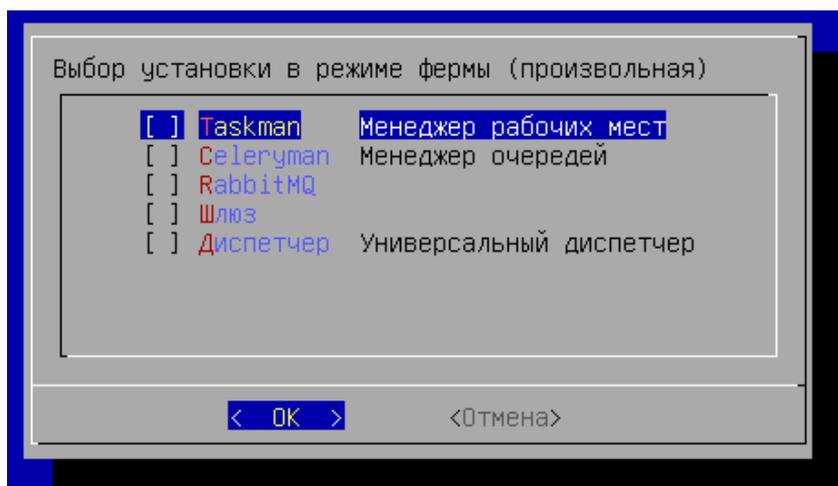


Рисунок 28 – Выбор компонента для установки

В зависимости от выбранного варианта дальнейшие действия по настройке будут отличаться.

Если был выбран пункт «Taskman» или «Celeryman», далее нужно выполнить:

- настроить параметры подключения к СУБД:
 - «Имя пользователя»: имя пользователя для подключения к БД (termidesk, значение по умолчанию при установке БД из состава ВМТ);
 - «Пароль»: пароль для подключения к БД (ksedimret, значение по умолчанию при установке БД из состава ВМТ);
 - «Хост»: IP-адрес или FQDN узла с установленной СУБД;
 - «Порт»: номер порта, используемого для соединения с сервером СУБД (стандартный порт 5432);
 - «База данных»: наименование БД (termidesk, значение по умолчанию при установке БД из состава ВМТ);

❗ Если указанная БД не существует, но у пользователя есть права на ее создание, то будет отображен запрос «Подключение к базе данных прошло успешно, однако, база данных <имя> не существует. Желаете создать?». Следует ответить **<Да>**, если новая БД действительно нужна.

- убедиться, что подключение успешно выполнено, результат отобразится в информационном окне;
- указать протокол, используемый для подключения к БД. При выборе значения «Disabled» защищенное соединение при подключении к БД использоваться не будет;
- задать параметры для подключения к RabbitMQ:
 - «Имя пользователя»: имя пользователя для подключения к RabbitMQ, по умолчанию termidesk;
 - «Пароль»: пароль для подключения к RabbitMQ, по умолчанию ksedimret;

- «Хост»: в режиме рекомендованной установки RabbitMQ устанавливается на одном узле с компонентом «Менеджер рабочих мест»;
- «Порт»: по умолчанию 5672;
- «Очередь»: по умолчанию termidesk;
- выбрать протокол, используемый для подключения к RabbitMQ. При выборе значения «Disabled» защищенное соединение при подключении к RabbitMQ использоваться не будет.

- ❗ После установки на узле будут установлены:
- если был выбран пункт «Taskman», то установится компонент «Менеджер рабочих мест», будет запущена служба termidesk-taskman;
 - если был выбран пункт «Celeryman», то установится компонент «Менеджер рабочих мест (очереди)», будут запущены службы termidesk-celery-beat, termidesk-celery-worker.

Если был выбран пункт «RabbitMQ», далее нужно выполнить:

- задать параметры RabbitMQ:
 - «Имя пользователя»: имя пользователя RabbitMQ;
 - «Пароль»: пароль подключения к RabbitMQ;
 - «Хост»: localhost (значение неизменяемое);
 - «Порт»: порт подключения к RabbitMQ;
 - «Очередь»: имя очереди;
- выбрать тип подключения, который будет настроен для RabbitMQ:
 - «Disabled» - защищенное соединение не будет настроено;
 - «Enabled» - будет автоматически настроено защищенное соединение по протоколу TLS 1.2.

- ❗ На узле будет установлен брокер сообщений RabbitMQ, будет запущена служба rabbitmq-server.

Если был выбран пункт «Шлюз», далее нужно выполнить:

- ввести адрес узла «Универсальный диспетчер» или адрес балансировщика (если он используется) для подключения к нему. Указание порта для подключения является опциональным;
- задать параметры для подключения к RabbitMQ:
 - «Имя пользователя»: имя пользователя для подключения к RabbitMQ, по умолчанию termidesk;
 - «Пароль»: пароль для подключения к RabbitMQ, по умолчанию ksedimret;

- «Хост»: в режиме рекомендованной установки RabbitMQ устанавливается на одном узле с компонентом «Менеджер рабочих мест»;
- «Порт»: по умолчанию 5672;
- «Очередь»: по умолчанию termidesk;
- выбрать протокол, используемый для подключения к RabbitMQ. При выборе значения «Disabled» защищенное соединение при подключении к RabbitMQ использоваться не будет.

i На узле будет установлен компонент «Шлюз», будет запущена служба termidesk-gateway.

Если был выбран пункт «Диспетчер», далее нужно выполнить:

- настроить параметры подключения к СУБД:
 - «Имя пользователя»: имя пользователя для подключения к БД (termidesk, значение по умолчанию при установке БД из состава ВМТ);
 - «Пароль»: пароль для подключения к БД (ksedimret, значение по умолчанию при установке БД из состава ВМТ);
 - «Хост»: IP-адрес или FQDN узла с установленной СУБД;
 - «Порт»: номер порта, используемого для соединения с сервером СУБД (стандартный порт 5432);
 - «База данных»: наименование БД (termidesk, значение по умолчанию при установке БД из состава ВМТ);

i Если указанная БД не существует, но у пользователя есть права на ее создание, то будет отображен запрос «Подключение к базе данных прошло успешно, однако, база данных <имя> не существует. Желаете создать?». Следует ответить **<Да>**, если новая БД действительно нужна.

- убедиться, что подключение успешно выполнено, результат отобразится в информационном окне;
- указать протокол, используемый для подключения к БД. При выборе значения «Disabled» защищенное соединение при подключении к БД использоваться не будет;
- задать параметры для подключения к RabbitMQ:
 - «Имя пользователя»: имя пользователя для подключения к RabbitMQ, по умолчанию termidesk;
 - «Пароль»: пароль для подключения к RabbitMQ, по умолчанию ksedimret;
 - «Хост»: в режиме рекомендованной установки RabbitMQ устанавливается на одном узле с компонентом «Менеджер рабочих мест»;
 - «Порт»: по умолчанию 5672;
 - «Очередь»: по умолчанию termidesk;

- выбрать протокол, используемый для подключения к RabbitMQ. При выборе значения «Disabled» защищенное соединение при подключении к RabbitMQ использоваться не будет.
- выбрать тип портала, который будет установлен для компонента «Универсальный диспетчер»:
 - «Universal» - будет активирован «Портал универсальный», совмещающий в себе функции «Портала администратора» и «Портала пользователя»;
 - «User» - будет активирован «Портал пользователя», предоставляющий пользовательский интерфейс Termidesk и интерфейс swagger для доступа к ограниченному списку модулей документации по командам REST API;
 - «Admin» - будет активирован «Портал администратора», предоставляющий интерфейс управления Termidesk и интерфейс swagger для доступа к ограниченному списку модулей документации по командам REST API.

i После установки «Универсального диспетчера» будут запущены службы `termidesk-vdi` и `apache2`. Если были выбраны «Портал универсальный» и «Портал администратора», то будет установлена серверная часть компонента «Удаленный помощник».

3.4 . Установка в режиме «База данных»

Установка в режиме «База данных» позволяет установить и настроить на узле СУБД PostgreSQL, которая будет использоваться компонентами Termidesk.

В процессе установки нужно:

- выполнить базовую настройку ВМТ (см. раздел **Базовые настройки ВМТ**);
- выбрать режим установки «База данных»;
- задать параметры для подключения к СУБД:
 - «Имя пользователя»: имя пользователя для подключения к БД, по умолчанию `termidesk`;
 - «Пароль»: пароль для подключения к БД, по умолчанию `ksedimret`;
 - «Хост»: установка СУБД в режиме «База данных» выполняется локально на текущем узле;
 - «Порт»: номер порта, используемого для соединения с сервером СУБД (стандартный порт 5432);
 - «База данных»: наименование БД, по умолчанию `termidesk`;
- настроить права на создание новых БД пользователем:
 - выбрать **<Да>**, для выдачи пользователю разрешения на создание новых БД;
 - выбрать **<Нет>**, для отказа в выдаче разрешения;

i Если пользователю выданы права на создание БД, при установке компонентов Termidesk из состава ВМТ можно указать несуществующую БД. В этом случае отобразится запрос: «Подключение к базе данных прошло успешно, однако база данных <имя> не существует. Желаете создать?». Для создания новой БД следует выбрать **<Да>**, после чего ее можно будет использовать при установке компонента.

- после установки СУБД PostgreSQL будет запущена служба postgresql.

3.5 . Установка в режиме «Агрегатор»

Установка в режиме «Агрегатор» позволяет установить на узле портал «Агрегатор» с набором компонентов, необходимых для его функционирования.

В процессе установки нужно:

- выполнить базовую настройку ВМТ (см. раздел **Базовые настройки ВМТ**);
- выбрать режим установки «Агрегатор»;
- настроить параметры подключения к СУБД:
 - «Имя пользователя»: имя пользователя для подключения к БД (termidesk, значение по умолчанию при установке БД из состава ВМТ);
 - «Пароль»: пароль для подключения к БД (ksedimret, значение по умолчанию при установке БД из состава ВМТ);
 - «Хост»: IP-адрес или FQDN узла с установленной СУБД;
 - «Порт»: номер порта, используемого для соединения с сервером СУБД (стандартный порт 5432);
 - «База данных»: наименование БД (termidesk, значение по умолчанию при установке БД из состава ВМТ);

i Если указанная БД не существует, но у пользователя есть права на ее создание, то будет отображен запрос «Подключение к базе данных прошло успешно, однако, база данных <имя> не существует. Желаете создать?». Следует ответить **<Да>**, если новая БД действительно нужна.

- убедиться, что подключение успешно выполнено, результат отобразится в информационном окне;
- указать протокол, используемый для подключения к БД. При выборе значения «Disabled» защищенное соединение при подключении к БД использоваться не будет;
- задать параметры для подключения к RabbitMQ:
 - «Имя пользователя»: имя пользователя для подключения к RabbitMQ, по умолчанию termidesk;
 - «Пароль»: пароль для подключения к RabbitMQ, по умолчанию ksedimret;

- «Хост»: в режиме рекомендованной установки RabbitMQ устанавливается на одном узле с порталом «Агрегатор»;
- «Порт»: по умолчанию 5672;
- «Очередь»: по умолчанию termidesk;
- выбрать протокол, используемый для подключения к RabbitMQ. При выборе значения «Disabled» защищенное соединение при подключении к RabbitMQ использоваться не будет.
- выбрать тип веб-интерфейса, который будет установлен для «Агрегатора»:
 - «Universal» - будет активирован «Портал универсальный», совмещающий в себе функции «Агрегатора администратора» и «Агрегатора пользователя»;
 - «User» - будет активирован «Агрегатор пользователя», веб-интерфейс для получения ресурсов, предоставляемых «Агрегатором»;
 - «Admin» - будет активирован «Агрегатор администратора», веб-интерфейс управления «Агрегатором».

 После установки будут запущены службы termidesk-vdi, apache2 и rabbitmq-server.

3.6 . Проверка работоспособности

ВМТ работоспособен, если после установки отобразилось главное меню ВМТ, а также при переходе по адресу https://<IP-адрес_ВМТ>:8443/ отобразилась страница авторизации (см. Рисунок 29) веб-интерфейса ВМТ.

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

- логин: admin;
- пароль: admin.

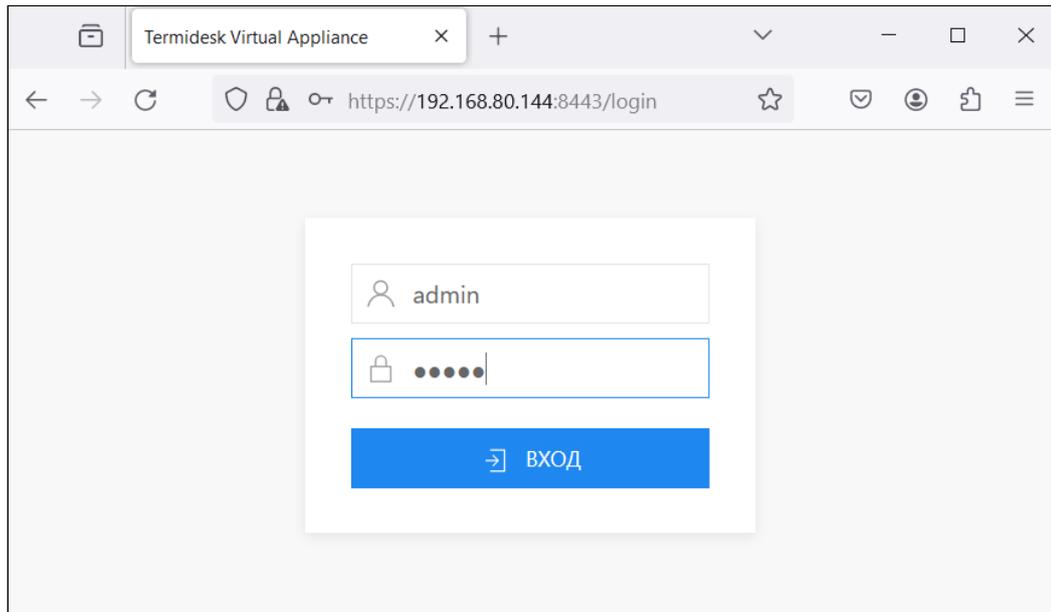


Рисунок 29 – Страница авторизации веб-интерфейса VA

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 терминальных серверов);
- Termidesk Terminal (поддержка только терминальных серверов для ОС Microsoft Windows и Astra Linux Special Edition).

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 соглашения с конечным пользователем можно ознакомиться на сайте компании: <https://termidesk.ru/eula.pdf>.

Для получения дополнительных лицензионных ключей с целью ознакомления 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 30).

⚠ Для получения лицензионного ключа при распределенном варианте установки Termidesk, необходимо предоставить в запросе системные UUID всех узлов с установленным компонентом «Универсальный диспетчер».

Для получения системных UUID следует:

- перейти на вкладку «Лицензия» и нажать экранную кнопку **[Сохранить в файл сведения для лицензии]**;
- выбрать каталог и сохранить файл. По умолчанию он сохранится в формате .tdsk, который можно открыть простым текстовым редактором. Файл будет содержать список идентификаторов узлов инфраструктуры, совпадающий с тем, что перечислен в поле «UID ноды» на странице «Инфраструктура - Диспетчеры подключений».

Информацию о системных UUID можно также получить из файла /sys/devices/virtual/dmi/id/product_uuid, выполнив на каждом узле с «Универсальным диспетчером»:

```
sudo cat /sys/devices/virtual/dmi/id/product_uuid
```

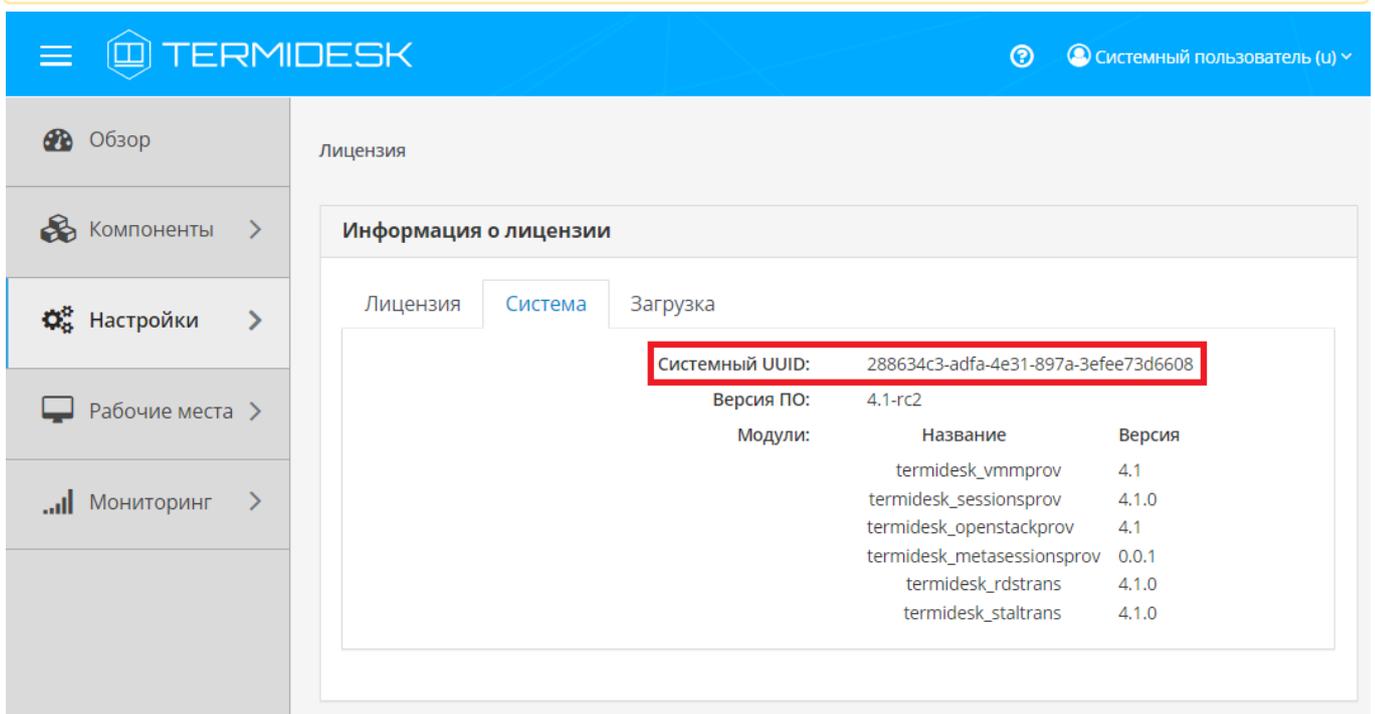


Рисунок 30 – Расположение информации о системном UUID

По завершении заполнения полей 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 31), а затем нажать экранную кнопку **[Загрузить]**.

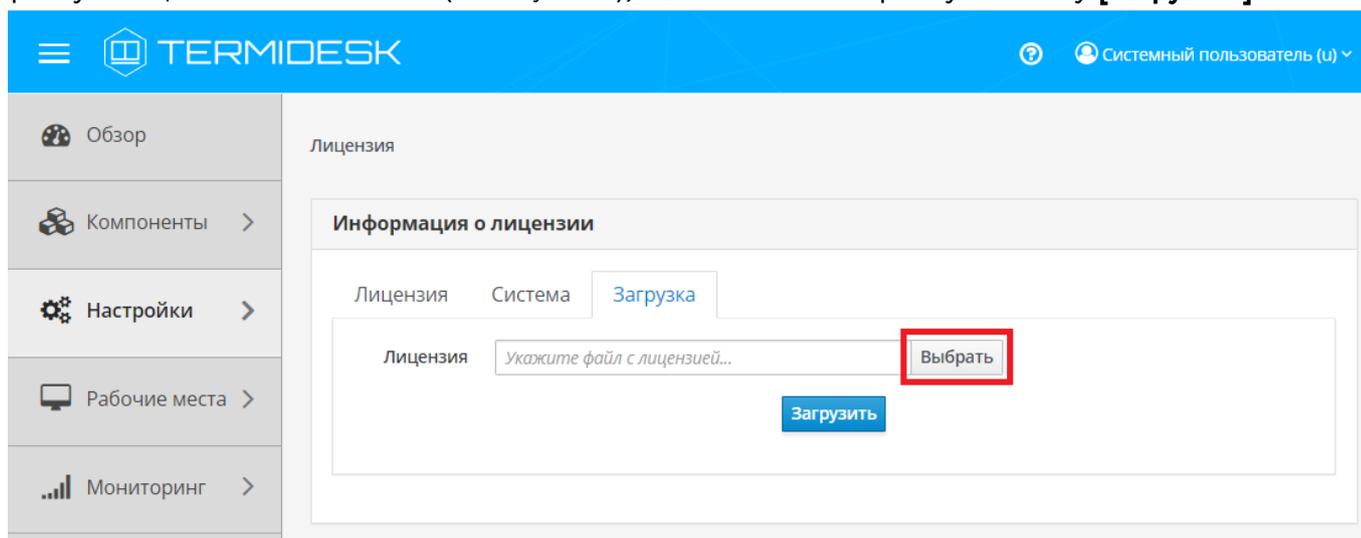


Рисунок 31 – Окно добавления файла с лицензией

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, на котором 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 РМ;
- «Доступные гостевые ОС» – варианты доступных для установленного вида лицензии гостевых ОС.

5. РАСШИРЕННАЯ НАСТРОЙКА

5.1 . Действия, доступные в меню ВМТ

5.1.1 . Изменение настроек сети

Для изменения настроек сети нужно в главном меню ВМТ нажать клавишу <F2>, ввести текущий пароль администратора (по умолчанию после установки - admin). Будет выполнен переход в меню расширенных настроек (см. Рисунок 32).

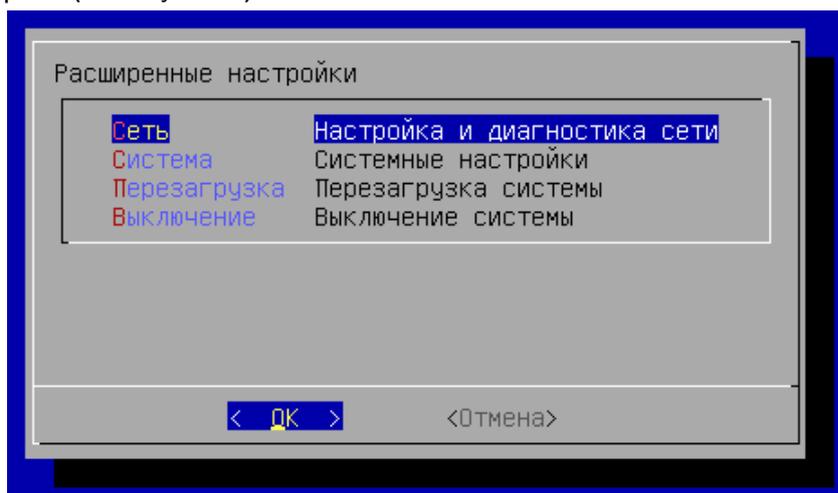


Рисунок 32 – Меню расширенных настроек VA

В меню настроек выбрать пункт «Сеть», затем «Настройка» (см. Рисунок 33). Далее действия не будут отличаться от процесса первичного конфигурирования сетевых параметров (см. подраздел **Базовые настройки ВМТ**).

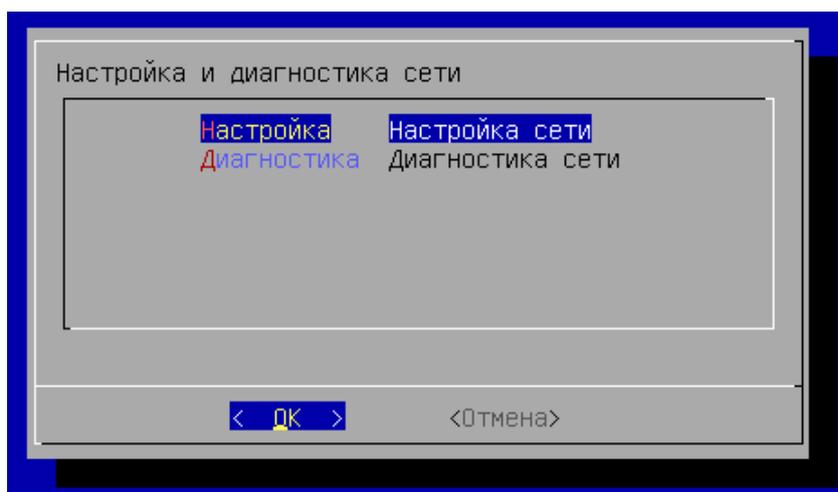


Рисунок 33 – Переход к конфигурации сети

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 34), подключение к которому нужно проверить. ВМТ выполнит команду ping до указанного узла.

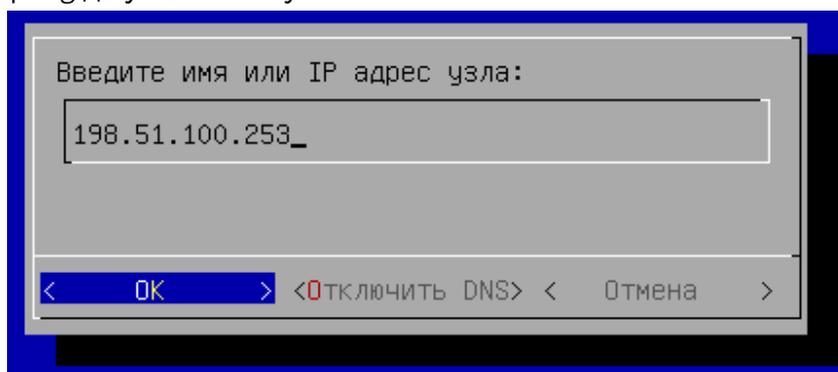


Рисунок 34 – Окно диагностики сети

Результат диагностики сети будет показан в окне (см. Рисунок 35).

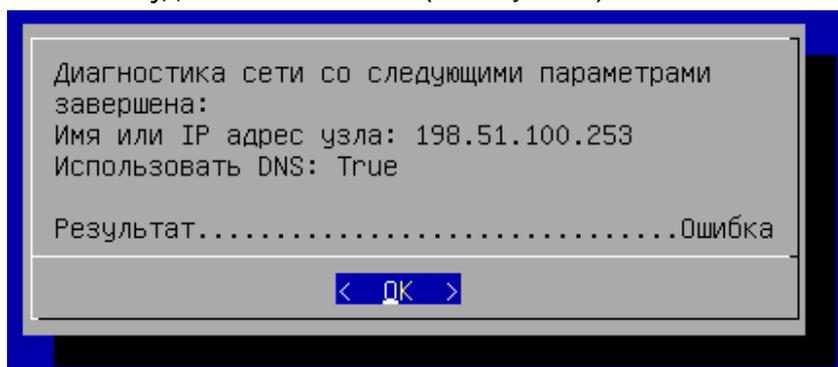


Рисунок 35 – Результат диагностики сети

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 36) задать новое имя узла ВМТ и нажать экранную кнопку **[OK]**, дождаться применения изменений. Новое имя узла будет отображено в главном меню ВМТ.

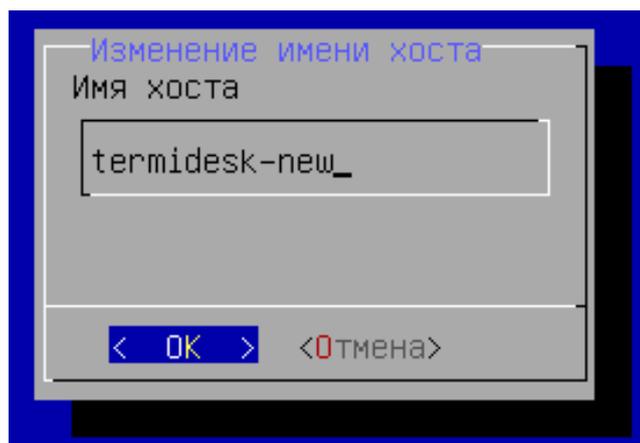


Рисунок 36 – Редактирование имени узла ВМТ

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 37) ввести текущий пароль (после установки пароль по умолчанию - `admin`) и нажать экранную кнопку **[ОК]**;
- затем (см. Рисунок 38) ввести новый пароль, переключиться на строку «Повтор пароля» при помощи клавиши **<↓>** (**<СТРЕЛКА ВНИЗ>**) и повторить ввод пароля. Подтвердить данные, нажав экранную кнопку **[ОК]**.

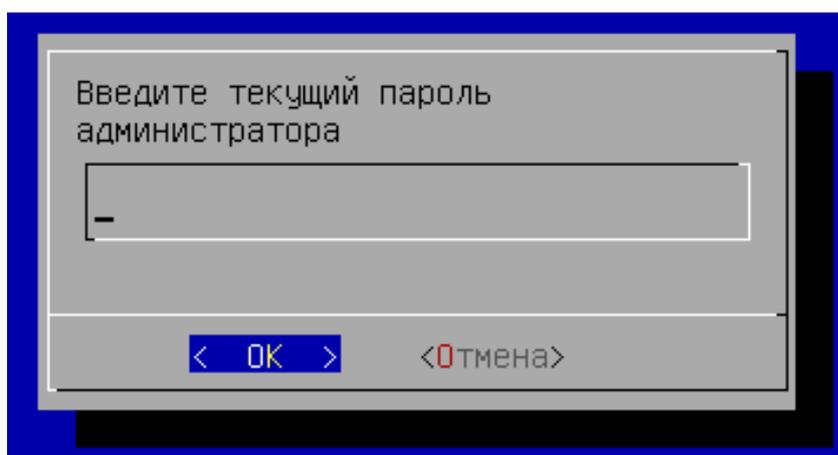


Рисунок 37 – Ввод текущего пароля администратора

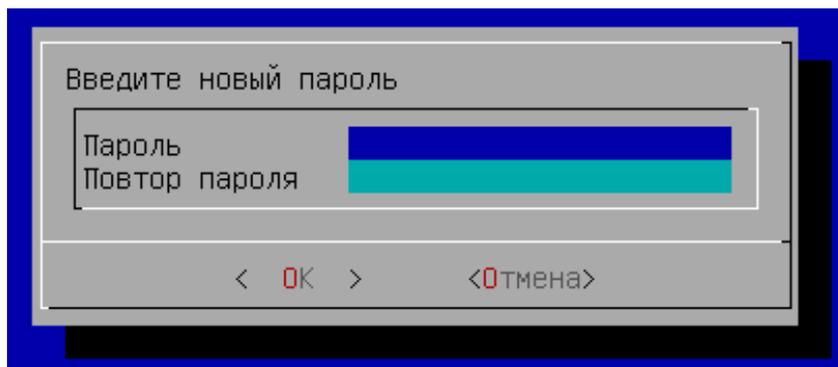


Рисунок 38 – Ввод нового пароля администратора

5.1.5 . Замена сертификата через меню ВМТ

Для доступа к веб-интерфейсу Termidesk по протоколу HTTPS на этапе первичной настройки генерируется самоподписанный сертификат.

Замена самоподписанных SSL-сертификатов доступна в веб-интерфейсе ВМТ (см. подраздел **Просмотр и замена сертификата через веб-интерфейс ВМТ**).

5.1.6 . Сброс установленных сертификатов через меню ВМТ

Сброс установленной конфигурации приведет к замене текущих сертификатов на самоподписанные.

Сброс установленных сертификатов доступен в веб-интерфейсе ВМТ (см. подраздел **Просмотр и замена сертификата через веб-интерфейс ВМТ**).

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 39) выбрать «Экспорт ключей»;

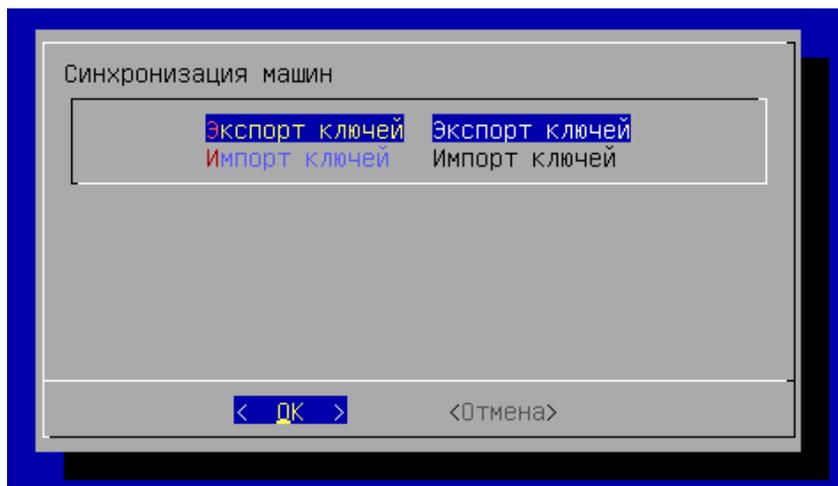


Рисунок 39 – Переход к экспорту ключей

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

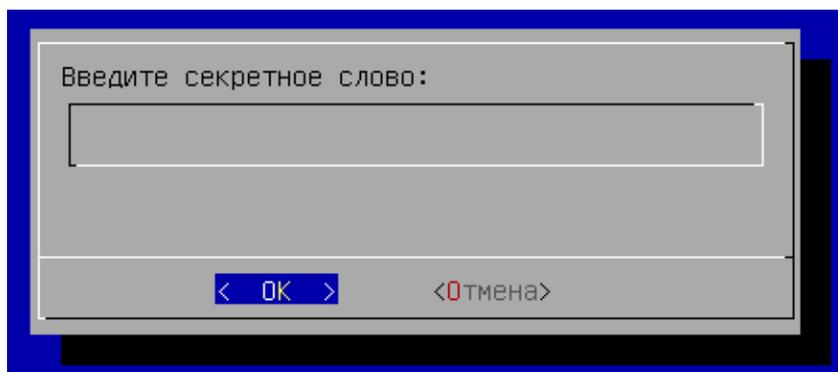


Рисунок 40 – Создание секретного слова

- запомнить сгенерированный временный пароль для синхронизации (см. Рисунок 41), который будет использоваться при импорте ключей на другую ноду ВМТ.

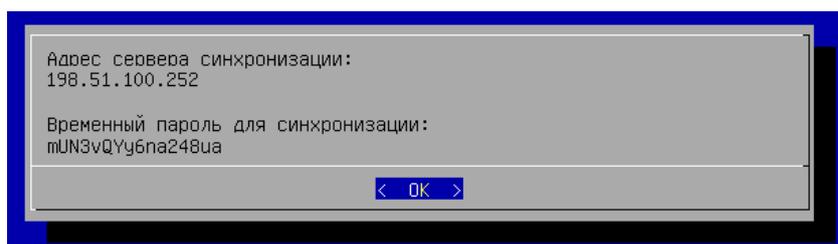


Рисунок 41 – Параметры для синхронизации между нодами

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 42) выбрать «Импорт ключей»;

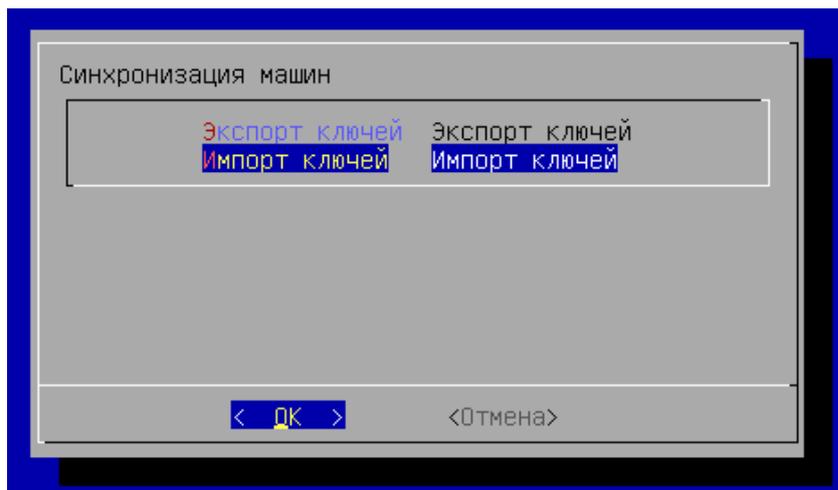


Рисунок 42 – Переход к импорту ключей

- 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.

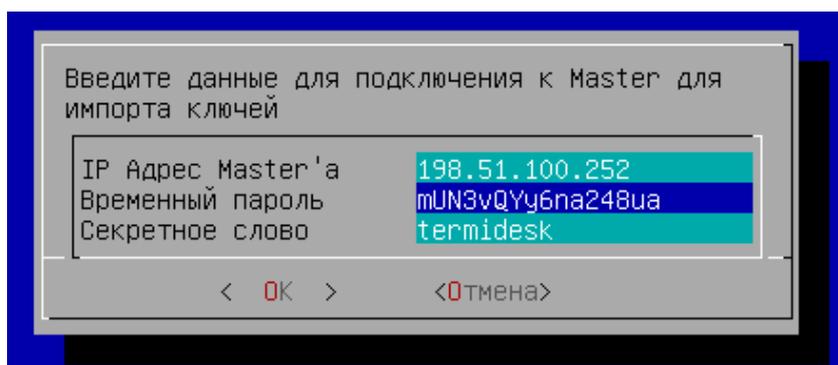


Рисунок 43 – Ввод параметров синхронизации

5.1.9 . Изменение настроек подключения к БД

 Функционал не поддерживается в версии Termidesk 5.1.

5.1.10 . Изменение настроек подключения к RabbitMQ

 Функционал не поддерживается в версии Termidesk 5.1.

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 ВМТ позволяет администратору выполнить ряд задач по настройке и управлению ВМТ, а именно:

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

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

- «Обзор» - предоставляет информацию об основных параметрах, характеризующих ВМТ (см. Рисунок 44), таких, как:
 - версия установленной ОС;
 - время доступности ВМТ, 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 ВМТ, позволяет управлять ими;
- «Сертификат» - предоставляет информацию об установленном сертификате, а также позволяет заменить его на другой;
- «VRRP» - позволяет выполнить настройку нод ВМТ в режиме высокой доступности. Пункт будет доступен, если ВМТ установлен с ролью «Планировщик»;
- «Дата и время» - позволяет выполнить настройку даты и времени, добавить информацию о NTP-серверах;
- «Журналы» - позволяет сформировать общий архив с файлами журналов ВМТ и выгрузить его.

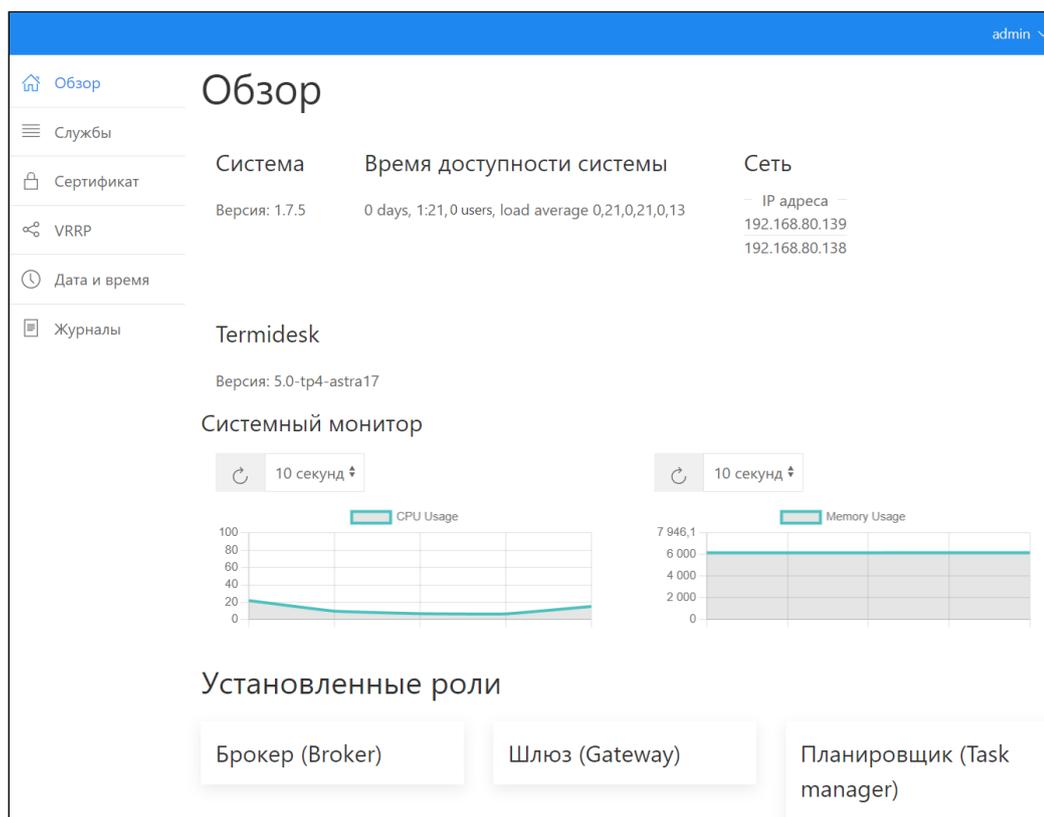


Рисунок 44 – Отображение функции «Обзор»

5.2.2 . Управление состоянием служб ВМТ

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

Список служб, отображаемый на странице, зависит от перечня ролей (или роли), выбранных при первичной настройке ВМТ. 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 45).

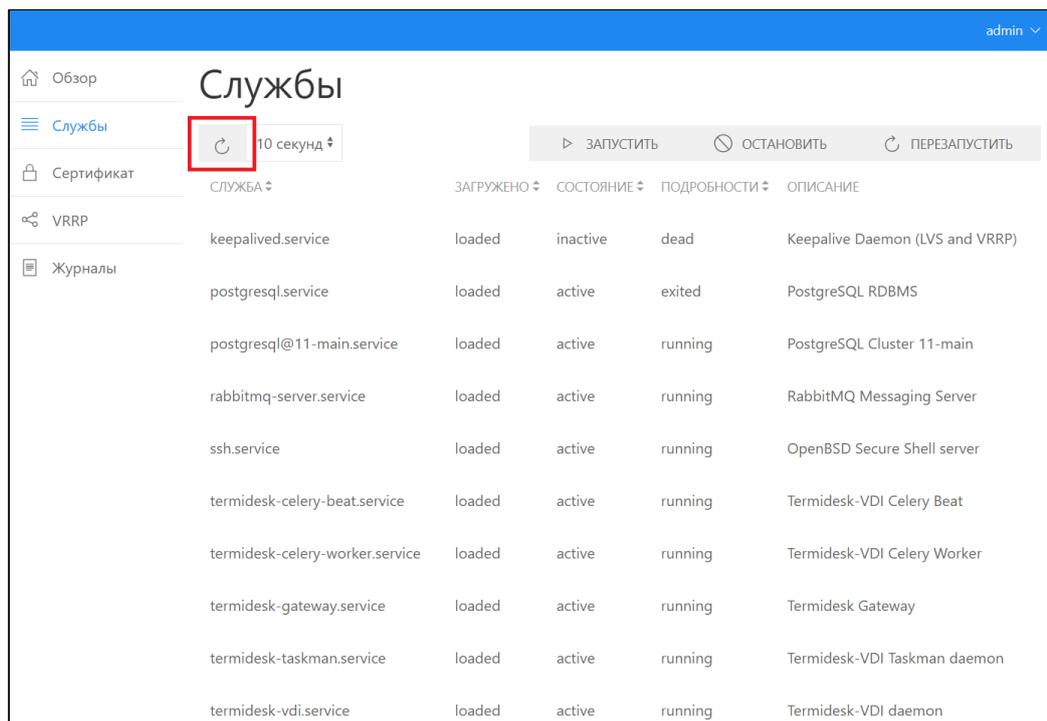


Рисунок 45 – Отображение функции «Службы»

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 2). Пункт «VRRP» будет доступен, если ВМТ установлен с ролью «Менеджер рабочих мест».

Таблица 2 – 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» |

| Параметр | Описание |
|---------------------------|---|
| «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 46).

i 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]**.

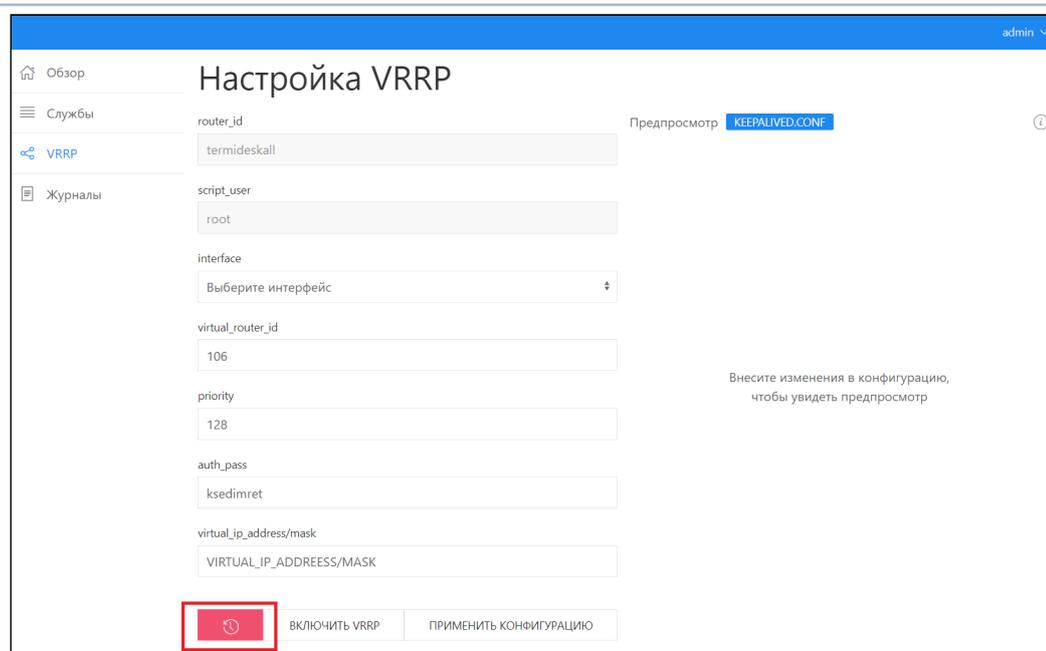


Рисунок 46 – Отображение функции «VRRP»

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 47). Будет сформирован архив формата .tar.gz с именем TDVAlogs_<временная_метка>.tar.gz, в который будут помещены файлы из каталогов /var/log/ и конфигурационные файлы /etc/opt/termidesk-vdi/termidesk.conf, /etc/rabbitmq/definitions.json, /etc/keepalived/keepalived.conf.

По завершении формирования архива станут доступны следующие действия (см. Рисунок 48):

- 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.

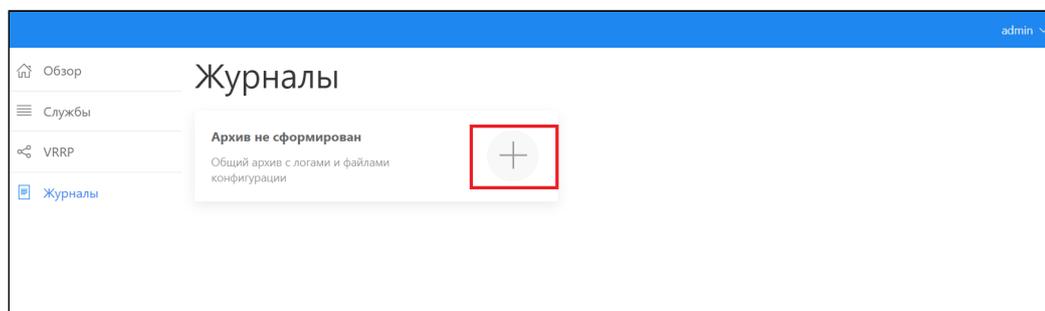


Рисунок 47 – Отображение функции «Журналы»

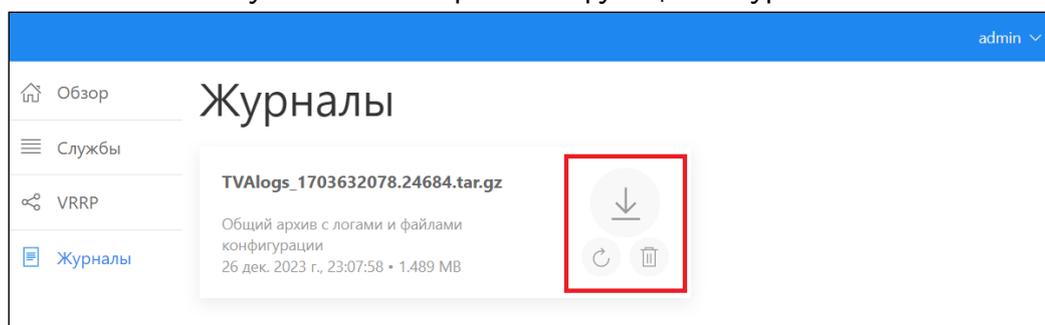


Рисунок 48 – Доступные действия с архивом

5.2.5 . Просмотр и замена сертификата через веб-интерфейс ВМТ

Для доступа к веб-интерфейсу Termidesk по протоколу HTTPS, а также для других подключений, требующих защищенного соединения, на этапе первичной настройки сгенерировался самоподписанный сертификат.

Для просмотра текущего сертификата, установленного в ВМТ, нужно перейти в функцию «Сертификат» веб-интерфейса ВМТ, затем нажать экранную кнопку **[Подробнее]**. В отдельном окне будет отображено подробное описание (см. Рисунок 49) созданного или загруженного на ВМТ сертификата.

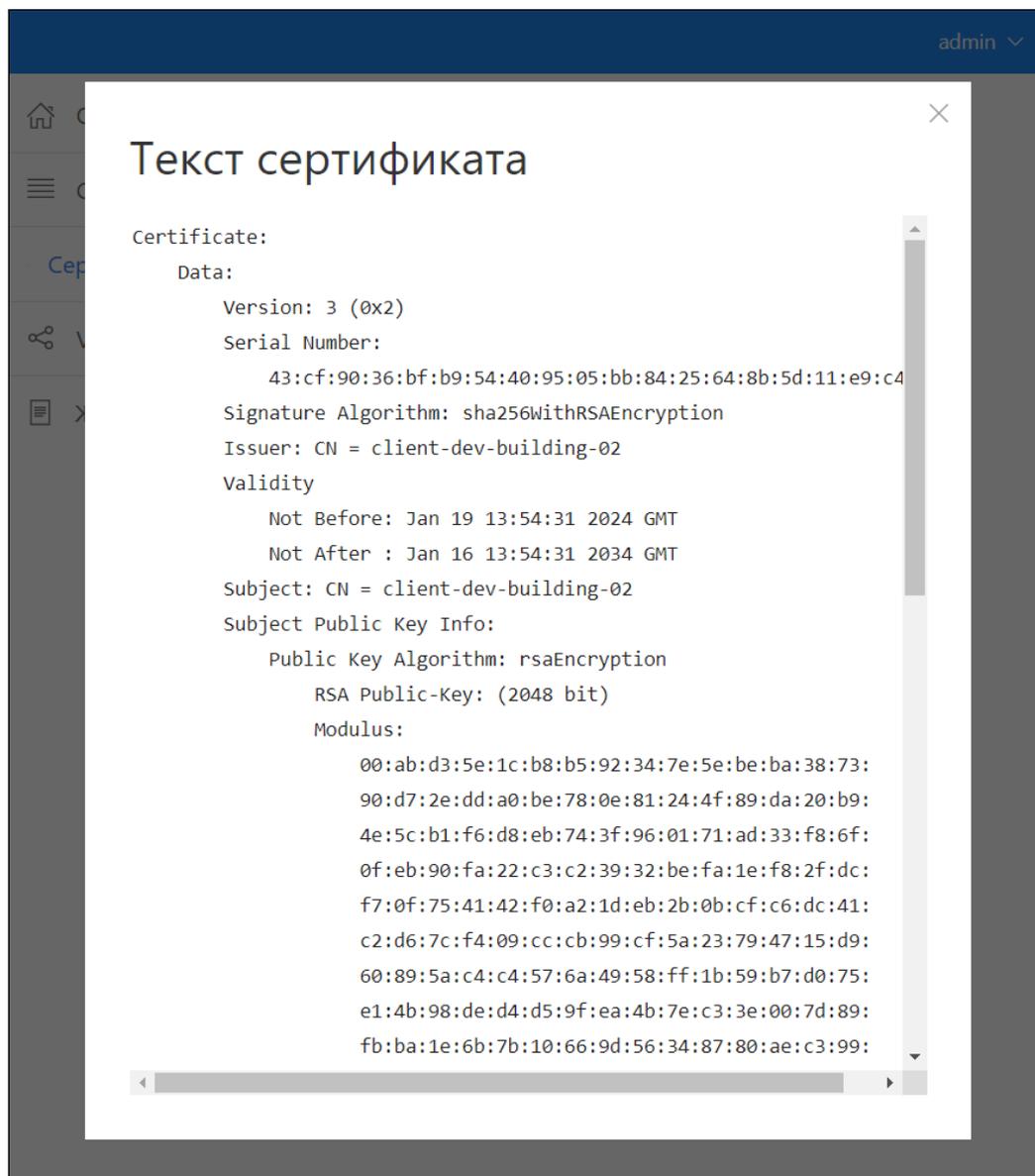


Рисунок 49 – Отображение подробного описания сертификата

Для замены текущего сертификата на новый нужно:

- в функции «Сертификат» нажать экранную кнопку **[Изменить]**;
- в открывшейся форме (см. Рисунок 50) выбрать:
 - файл нового сертификата. Поддерживаются форматы: .pfx, .pem, .crt, .cer;
 - файл закрытого ключа. Поддерживаются форматы: .pem, .key;
 - файл проверки цепочки сертификатов (необязательно). Поддерживаются форматы: .pfx, .pem, .crt, .cer.

i В случае, если выбранный файл защищен паролем, то при попытке его загрузить в веб-браузере появится всплывающее окно ввода пароля. Необходимо ввести пароль и нажать экранную кнопку **[OK]**.

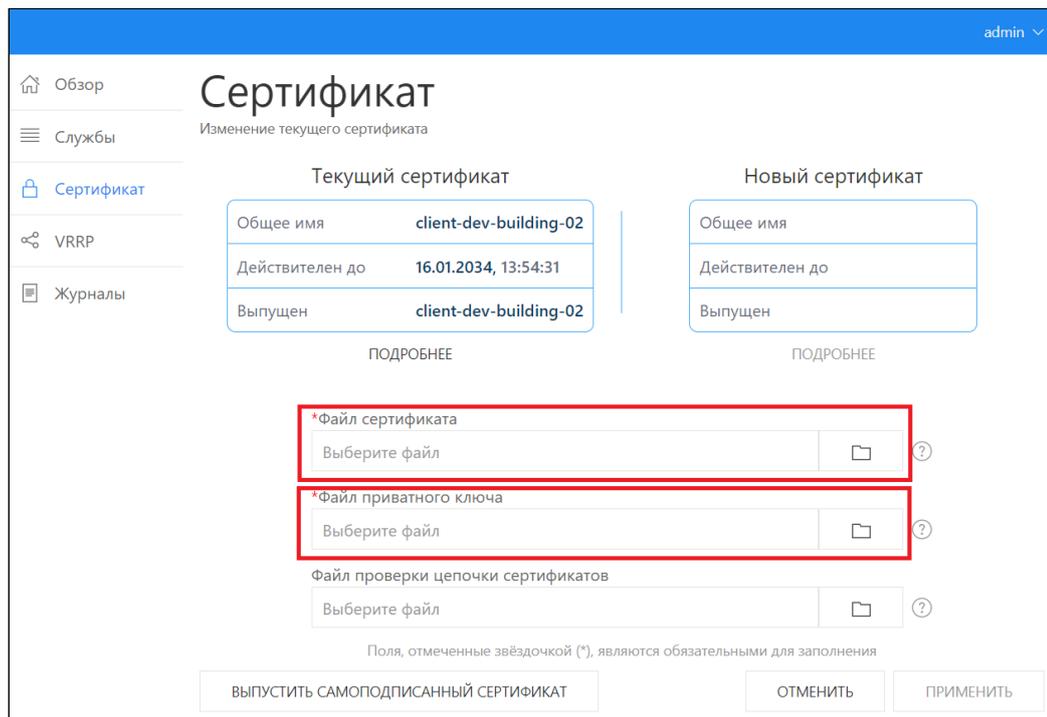


Рисунок 50 – Замена сертификата через веб-интерфейс ВМТ

- после загрузки файлов параметры нового сертификата отобразятся рядом с параметрами текущего сертификата. Для отображения полного описания сертификата нужно нажать экранную кнопку **[Подробнее]**. Для применения изменений нужно нажать экранную кнопку **[Применить]**.

Для замены текущего сертификата на новый самоподписанный нужно:

- в функции «Сертификат» нажать экранную кнопку **[Изменить]**;
- в открывшейся форме нажать экранную кнопку **[Выпустить самоподписанный сертификат]**;
- задать (см. Рисунок 51) общее имя (Common Name, CN) и дату, до которой будет действителен сертификат;

⚠ Новое общее имя (CN) должно отличаться от предыдущего.

- нажать экранную кнопку **[Сгенерировать]**;
- закрыть окно выпуска и нажать экранную кнопку **[Применить]**.

✕

Выпуск самоподписанного сертификата

Общее имя (CN)

Действителен до

📅

Без указания даты, сертификат будет создан с датой по-умолчанию (+1 год от текущей)

СГЕНЕРИРОВАТЬ

Рисунок 51 – Выпуск самоподписанного сертификата

i Новый сертификат отобразится в функции «Сертификат» после обновления страницы.

5.2.6 . Управление датой и временем на ВМТ

Для просмотра текущего времени и даты следует перейти в функцию «Дата и время» веб-интерфейса ВМТ.

Для более подробного просмотра установленных значений даты и времени нужно воспользоваться экранной кнопкой **[Подробный просмотр]**, которая отобразит вывод команды `timedatectl`.

Для изменения даты и времени:

- нажать экранную кнопку **[Изменить]** в функции «Дата и время» веб-интерфейса ВМТ;
- на открывшейся странице вновь нажать экранную кнопку **[Изменить]** (см. Рисунок 52) для поля «Текущее время»;
- задать нужные значения и нажать экранную кнопку **[Выбрать]** (см. Рисунок 53);
- нажать экранную кнопку **[Применить]**.

i Для сброса значений используется экранная кнопка **[Очистить]**, восстанавливающая значения, которые были актуальны в момент перехода на страницу, если не была активирована экранная кнопка **[Применить]**. После активации экранной кнопки **[Применить]** сброс значений не действует.

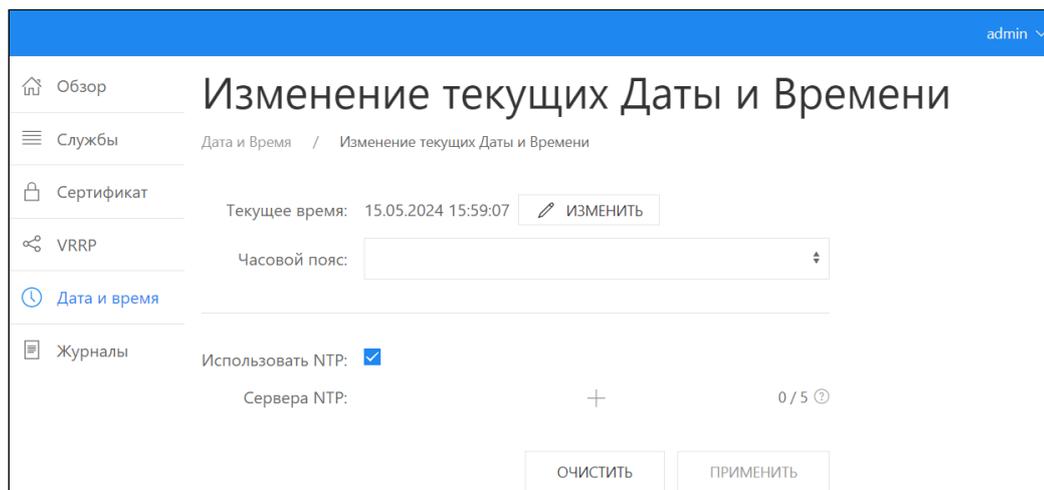


Рисунок 52 – Изменение даты и времени узла BMT

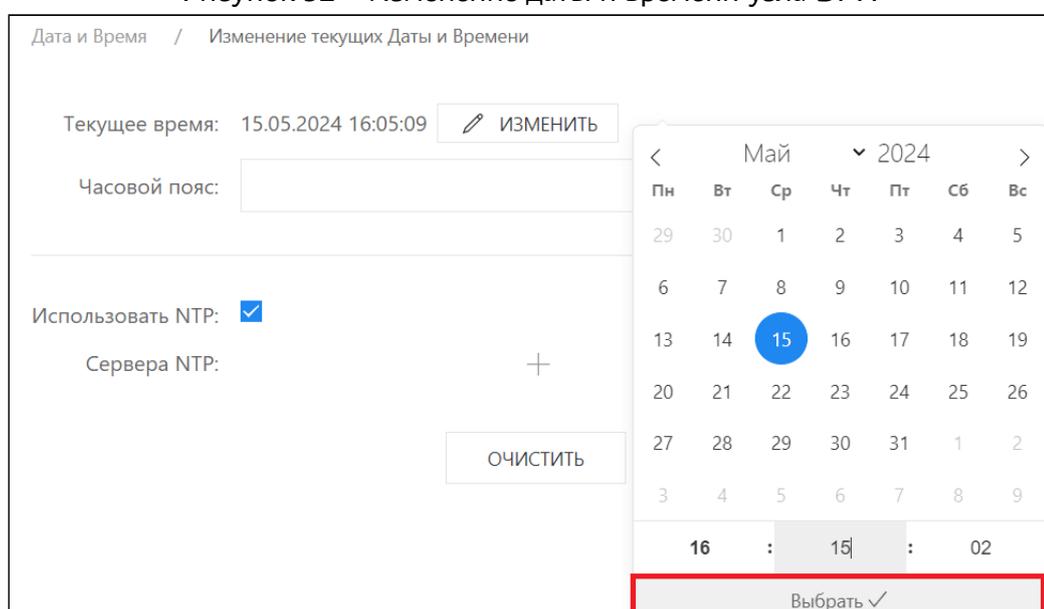
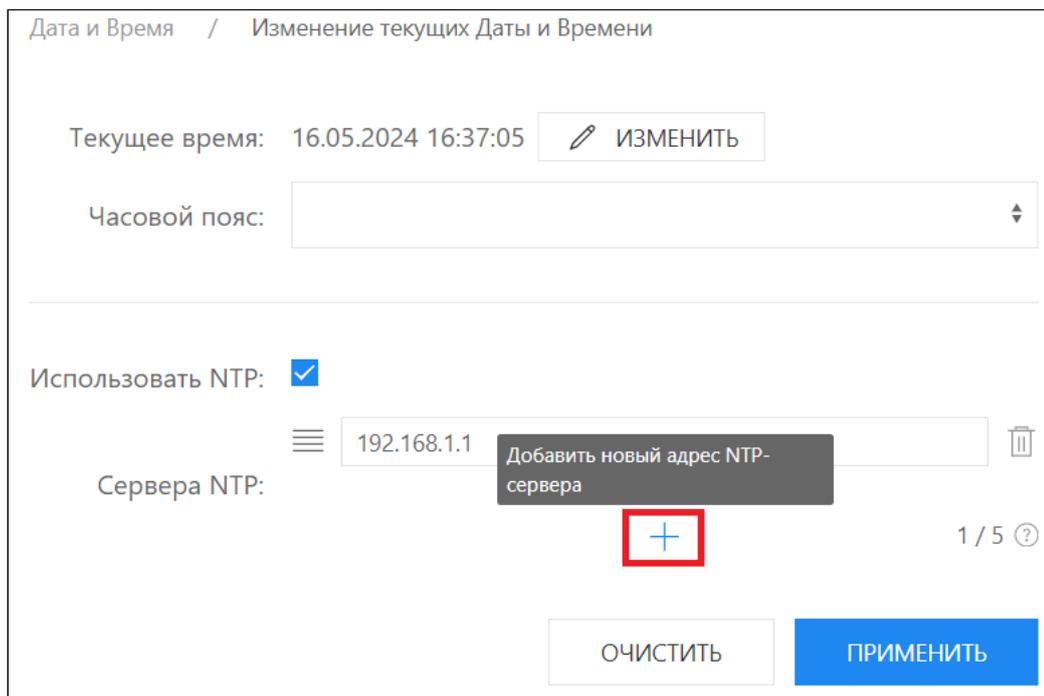


Рисунок 53 – Выбор новых значений даты и времени

BMT поддерживает задание NTP-сервера для автоматического получения даты и времени, для этого нужно:

- нажать экранную кнопку **[Изменить]** в функции «Дата и время» веб-интерфейса BMT;
- воспользоваться экранной кнопкой **[+]** (см. Рисунок 54) и ввести IP-адрес или FQDN сервера. Поддерживается добавление до пяти (включительно) NTP-серверов. Если сервер недоступен, будет выведено соответствующее сообщение (см. Рисунок 55);
- нажать экранную кнопку **[Применить]**.



Дата и Время / Изменение текущих Даты и Времени

Текущее время: 16.05.2024 16:37:05

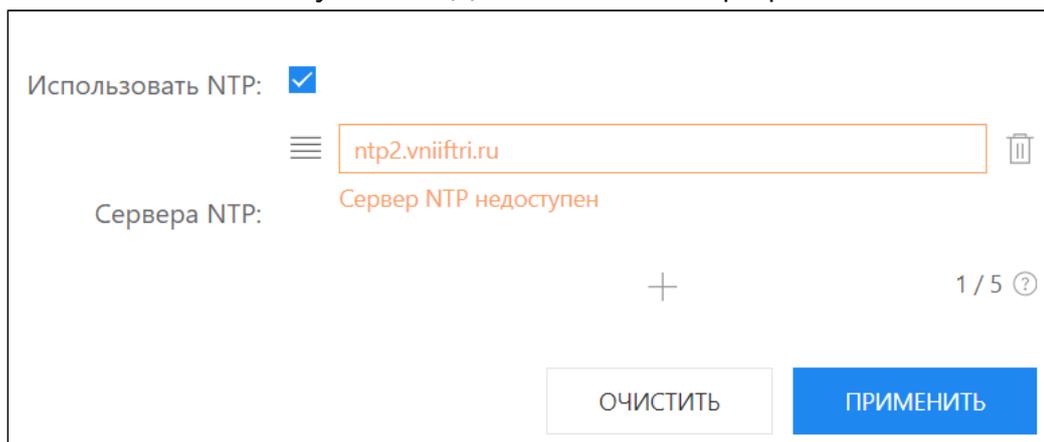
Часовой пояс:

Использовать NTP:

Сервера NTP:

1 / 5 ?

Рисунок 54 – Добавление NTP-сервера



Использовать NTP:

Сервера NTP:

1 / 5 ?

Рисунок 55 – Сообщение о недоступности NTP-сервера

5.3 . Резервное копирование и восстановление БД

5.4 . 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 [ОК]. 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.

5.4.1 . Резервное копирование БД

Резервное копирование БД, созданной СУБД PostgreSQL можно выполнить утилитой pg_dump:

```
1 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.

5.4.2 . Восстановление БД из резервной копии

Восстановление БД из резервной копии выполняется командой:

```
1 pg_restore -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь>
  -W --format=t <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;

--format=t <файл_копии_БД.tar> - ключ для восстановления БД из резервной копии в формате tar.

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 56), нажав экранную кнопку **[Да]**.

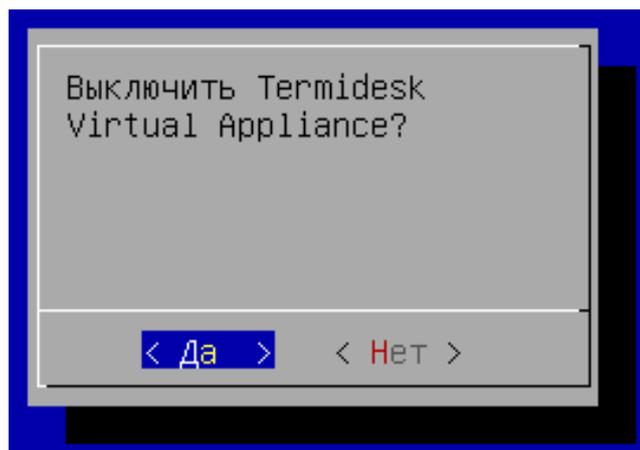


Рисунок 56 – Подтверждение выключения ВМТ

7. ПРИНЯТЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

| Термин | Определение |
|-------------------------------------|--|
| Агрегатор администратора | Веб-интерфейс управления порталом «Агрегатор» |
| Агрегатор пользователя | Веб-интерфейс пользователя для получения ресурсов, предоставляемых порталом «Агрегатор» |
| Виртуальное рабочее место (ВРМ) | Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО. Подключение к ВРМ происходит при помощи протоколов удаленного доступа |
| Рабочее место (РМ) | Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под РМ подразумеваются как ВРМ, так и терминальный доступ или доступ к опубликованным на сервере терминалов приложениям |
| Гостевая ОС | ОС, функционирующая на ВМ |
| Компонент «Менеджер рабочих мест» | Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом РМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета termidesk-vdi. Наименование службы после установки: termidesk-taskman.service |
| Поставщик ресурсов | ОС, платформа виртуализации или терминальный сервер, предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ |
| Протокол доставки | Поддерживаемый в Termidesk протокол удаленного доступа к РМ |
| Компонент «Универсальный диспетчер» | Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ. Устанавливается из пакета termidesk-vdi. Наименование службы после установки: termidesk-vdi.service |
| Компонент «Шлюз» | Компонент Termidesk. Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP. Устанавливается из пакета termidesk-gateway. Наименование службы после установки: termidesk-gateway.service. |
| Портал «Агрегатор» | Роль компонента «Универсальный диспетчер», доступная при установке Termidesk. Является единой точкой входа для получения ресурсов пользователями, предоставляет им объединенный список приложений и ВРМ с ферм Termidesk |
| Портал администратора | Предоставляет веб-интерфейс для управления Termidesk и интерфейс swagger для доступа к ограниченному списку модулей документации по командам REST API |
| Портал пользователя | Предоставляет пользовательский веб-интерфейс Termidesk (без доступа к функциям управления) и интерфейс swagger для доступа к ограниченному списку модулей документации по командам REST API |
| Портал универсальный | Предоставляет функции обоих вариантов порталов, как пользовательского, так и административного |
| Ключ | Последовательность псевдослучайных чисел, сгенерированная особым образом |
| Сертификат | Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу |
| Ферма | Логическое объединение узлов, взаимодействующих с одной БД |

8. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

| Сокращение | Пояснение |
|------------|--|
| БД | База данных |
| ВМ | Виртуальная машина |
| ВМТ | Виртуальный модуль Termidesk |
| ВРМ | Виртуальное рабочее место |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| РМ | Рабочее место |
| СУБД | Система управления базами данных |
| API | Application Programming Interface (интерфейс прикладного программирования) |
| CN | Common Name (общее имя) |
| CPU | Central Processing Unit (центральный процессор) |
| DHCP | Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста) |
| DNS | Domain Name System (система доменных имен) |
| FQDN | Fully Qualified Domain Name (полностью определенное имя домена) |
| 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)) |
| NTP | Network Time Protocol (протокол сетевого времени) |
| 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) |
| TCP | Transmission Control Protocol (протокол управления передачей) |
| UUID | Unique User Identifier (уникальный идентификатор пользователя) |

| Сокращение | Пояснение |
|------------|--|
| VDI | Virtual Desktop Infrastructure (инфраструктура виртуальных рабочих столов) |
| VRRP | Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности) |



© ООО «УВЕОН»

119571, г. Москва, Ленинский проспект,
д. 119А, помещ. 9Н
<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