TERMIDESK

РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-01 90 01

Версия 6.0. Выпуск от июня 2025

Установка программного комплекса

ОГЛАВЛЕНИЕ

1 . ОБЩИЕ СВЕДЕНИЯ 5
1.1 . О документе 5
1.2 . Назначение 5
1.3 . Область применения 5
1.4 . Основные характеристики 5
1.5 . Требования к уровню подготовки персонала 8
1.6 . Типографские соглашения 13
2 . ТРЕБОВАНИЯ К СРЕДЕ ФУНКЦИОНИРОВАНИЯ 14
2.1 . Требования к аппаратному обеспечению 14
2.2 . Требования к программному обеспечению 14
2.3 . Требования к синхронизации времени 14
2.4 . Требования к DNS и DHCP 14
2.5 . Требования к серверам каталогов 14
2.6 . Требования к терминальным серверам 15
2.7 . Требования к платформе виртуализации 15
3 . ИСПОЛЬЗОВАНИЕ КОНТЕКСТУАЛИЗАЦИИ ПК СВ БРЕСТ 18
3.1 . Контекстуализация в ПК СВ Брест 18
4 . ПОДГОТОВКА СРЕДЫ ФУНКЦИОНИРОВАНИЯ 19
4.1 . Установка СУБД PostgreSQL 19
4.2 . Настройка СУБД PostgreSQL 19
4.3 . Установка брокера сообщений RabbitMQ 22
4.4 . Настройка брокера сообщений RabbitMQ 22
4.5 . Подготовка ОС Astra Linux Special Edition 26
4.6 . Настройка СУБД Tantor 26
5 . УСТАНОВКА ПРОГРАММНОГО КОМПЛЕКСА 29
5.1 . Получение пакетов установки в ОС Astra Linux Special Edition 29

5.2 . Комплексная установка Termidesk ... 31
5.2.1 . Автоматизированная установка ... 31
5.2.1.1 . Автоматизированная установка через исполняемый файл ... 31
5.2.1.2 . Автоматизированная установка через конфигурационный файл ... 31
5.2.2 . Неавтоматизированная установка Termidesk ... 32
5.3 . Распределенная установка программного комплекса ... 44
5.3.1 . Основные принципы распределенной установки ... 44
5.3.2 . Установка и настройка СУБД PostgreSQL ... 47
5.3.3 . Установка первого узла с «Универсальным диспетчером» ... 47
5.3.4 . Установка «Шлюзов» ... 48
5.3.5 . Установка «Менеджеров рабочих мест» ... 49
5.3.6 . Установка балансировщиков ... 49
5.3.7 . Действия после распределенной установки ... 50
5.4 . Отказоустойчивая установка Termidesk ... 50
5.4.1 . Основные принципы отказоустойчивой установки ... 50
5.4.2 . Установка и настройка СУБД PostgreSQL ... 47
5.4.3 . Установка основного узла Termidesk ... 53
5.4.4 . Перенос каталога с конфигурационными файлами и ключами ... 54
5.4.5 . Установка резервных узлов Termidesk ... 55
5.4.6 . Проверка работоспособности узлов Termidesk ... 55
5.4.7 . Настройка узлов в режиме высокой доступности ... 55
5.5 . Установка в режиме замкнутой программной среды ... 59
5.6 . Постановка Termidesk на контроль целостности ... 60
5.7 . Проверка работоспособности после установки ... 61
6 . ОБНОВЛЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА ... 63
6.1 . Комплексное обновление Termidesk ... 63
6.2 . Обновление для распределенной конфигурации установки ... 66
6.2.1 . Общая концепция обновления ... 66

6.2.2 . Шаг 1. Редактирование конфигурации балансировщика нагрузки 69
6.2.3 . Шаг 2. Перевод фондов РМ в режим техобслуживания 70
6.2.4 . Шаг 3. Установка и настройка RabbitMQ 71
6.2.5 . Шаг 4. Резервное копирование RSA-ключей 71
6.2.6 . Шаг 5. Останов служб на «Менеджере рабочих мест» 71
6.2.7 . Шаг 6. Обновление «Менеджеров рабочих мест» 71
6.2.8 . Шаг 7. Восстановление RSA-ключей на «Менеджере рабочих мест» 72
6.2.9 . Шаг 8. Отключение службы keepalived 72
6.2.10 . Шаги 9. Обновление резервного «Менеджера рабочих мест» 72
6.2.11 . Шаг 10. Обновление «Универсальных диспетчеров» 72
6.2.12 . Шаги 11. Обновление «Шлюзов» 73
6.2.13 . Шаг 12. Восстановление конфигурации балансировщика нагрузки 74
6.2.14 . Шаг 13. Обновление компонентов в ОС РМ и новая публикация 75
7 . УДАЛЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА 76
8 . ЛИЦЕНЗИРОВАНИЕ 78
8.1 . Получение лицензионного ключа 78
8.2 . Ввод лицензии 80
8.3 . Проверка сведений о лицензии 80
9 . ПЕРЕЧЕНЬ ТЕРМИНОВ 81
10 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ 83

1 . ОБЩИЕ СВЕДЕНИЯ

1.1 . О документе

Настоящий документ является первой частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Термидеск» (далее - Termidesk). Документ предназначен для администраторов системы и сети.

В первой части руководства приведено назначение и установка Termidesk. Для того, чтобы получить информацию о настройке Termidesk, необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

1.2 . Назначение

Termidesk предназначен для доставки рабочих мест (РМ), таких, как: виртуальных рабочих мест (ВРМ), приложений, организации терминального доступа пользователей к ресурсам посредством различных протоколов удаленного доступа.

1.3 . Область применения

Termidesk:

- может применяться для создания или модернизации инфокоммуникационной инфраструктуры масштаба организации, а также поставщиками услуг, реализующих облачную услугу РМ;
- ориентирован на образовательные и иные организации, в которых предусмотрено использование одного РМ множеством пользователей, с возможностью очистки РМ по завершению сеанса работы;
- удобен для использования в организациях с обширной сетью филиалов;
- позволяет реализовать политики повышенных требований к безопасности данных, препятствующих несанкционированному распространению информации. Помимо этого, Termidesk обеспечивает работу с виртуализированными графическими адаптерами (vGPU) и адаптацией к низкоскоростным каналам связи.

1.4 . Основные характеристики

Termidesk состоит из ряда компонентов, которые могут быть либо отделяемыми (подразумевает выбор роли при установке из общего пакета), либо самостоятельными (компонент устанавливается из отдельного пакета, но используется в составе общего комплекса). Такое разделение обеспечивает гибкое масштабирование системы для различных сценариев применения.

В состав Termidesk входят следующие компоненты:

- «Универсальный диспетчер» - компонент, отвечающий за идентификацию пользователей, назначение и контроля доставки им РМ (ВРМ, приложений, терминального доступа);
- «Шлюз» - компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP;
- «Менеджер рабочих мест» - компонент, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом ВРМ, включая создание, настройку, запуск, отключение и удаление;
- «Агент» - компонент, отвечающий за контролируемую доставку РМ, взаимодействие с «Универсальным диспетчером» и «Менеджером рабочих мест»;
- «Клиент» - компонент, отвечающий за доставку РМ на пользовательскую рабочую станцию с возможностью перенаправления периферии, каталогов, и оптимизацию их использования в протоколе доставки;
- «Оркестратор» - компонент, отвечающий за автоматизацию развертывания Termidesk в облачных структурах;
- «Сервер терминалов Astra Linux» - компонент, отвечающий за организацию терминального доступа в ОС Astra Linux Special Edition;
- «Удаленный помощник» - компонент, предоставляющий администратору или специалисту технической поддержки экран пользователя через сеанс удаленного подключения и обеспечивающий передачу голосовой информации для взаимодействия с пользователем;
- «Виртуальный модуль Termidesk» - компонент, представляющий 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. Компонент позволяет быстро развернуть и использовать компоненты «Универсальный диспетчер», «Шлюз», «Менеджер рабочих мест»;
- «Termidesk Live» - компонент, представляющий собой загрузочный образ ОС с предустановленным компонентом «Клиент»;
- TERA (англ. Termidesk Remote Access protocol) - протокол удаленного доступа собственной разработки.

Компоненты «Универсальный диспетчер», «Менеджер рабочих мест» являются отделяемыми, устанавливаемыми из единого пакета. Они могут разворачиваться как в комплексном варианте (на одном узле), так и в распределенной конфигурации (на разных узлах).

Параметры конфигурирования отделяемых компонентов приведены в СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Остальные компоненты являются самостоятельными, но работающими в составе программного комплекса.

> Компоненты могут быть объединены в фермы.
> Ферма - логическое объединение узлов, взаимодействующих с одной базой данных (БД).
> Для объединения ресурсов с ферм Termidesk используется специальная роль, доступная при установке Termidesk - «Агрегатор», являющаяся единой точкой входа для получения ресурсов пользователями.
> Установка «Агрегатора» должна быть отделена от установки фермы Termidesk и должна использовать отдельную БД.

К компоненту «Агент» относятся следующие подкомпоненты, каждый из которых устанавливается отдельно:

- «Агент виртуального рабочего места», устанавливается в гостевую ОС ВМ или в ОС автономной ВМ;
- «Агент узла виртуализации», устанавливается на узел виртуализации;
- «Сессионный агент», устанавливается на узел терминального сервера;
- «Видеоагент», устанавливается в гостевую ОС ВМ;
- «Агент виртуальных смарт-карт», устанавливается в гостевую ОС ВМ.

Параметры установки и конфигурирования компонентов приведены:

- для «Шлюза» - в документе СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз»;
- для «Агента» - в документе СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»;
- для «Клиента» - в документе СЛЕТ.10001-01 92 01 «Руководство пользователя. Настройка и эксплуатация компонента «Клиент»;
- для «Оркестратора» - документе СЛЕТ.10001-01 90 06 «Руководство администратора. Настройка компонента «Оркестратор»;
- для «Сервера терминалов Astra Linux» - в документе СЛЕТ.10001-01 90 07 «Руководство администратора. Настройка компонента «Сервер терминалов»;
- для «Агрегатора» - в документе СЛЕТ.10001-01 90 08 «Руководство администратора. Установка и настройка «Агрегатора»;
- для TERA - в документе СЛЕТ.10001-01 90 08 «Руководство администратора. Настройка компонента TERA;
- для «Удаленного помощника» - в документе СЛЕТ.10001-01 91 02 «Инструкция по использованию. Компонент «Удаленный помощник»;
- для «Виртуального модуля Termidesk» - в документе СЛЕТ.10001-01 91 03 «Инструкция по использованию. Компонент «Виртуальный модуль Termidesk»;

- для «Termidesk Live» - в документе СЛЕТ.10001-01 91 04 «Инструкция по использованию. Компонент «Termidesk Live».

Termidesk обеспечивает доставку РМ на пользовательскую рабочую станцию посредством следующих протоколов:

- SPICE (оптимизированный, только для варианта лицензирования Termidesk VDI);
- TERA (только для варианта лицензирования Termidesk VDI);
- RDP. Для варианта лицензирования Termidesk Terminal доступны только протоколы доступа к ресурсам терминального сервера;
- VNC (только для варианта лицензирования Termidesk VDI);
- Loudplay (только для варианта лицензирования Termidesk VDI).

Termidesk реализует режим прямого и туннельного соединения. Прямое соединение позволяет подключиться к протоколу, запущенному внутри гостевой ОС или на гипервизоре. Туннельное соединение применяется при подключении к РМ из недоверенных сетей. Комбинация протоколов доставки и способы подключения предопределены в Termidesk.

Termidesk поддерживает работу с платформами виртуализации:

- программный комплекс «Средства виртуализации «Брест» (далее - ПК СВ Брест, только для варианта лицензирования Termidesk VDI);
- VMmanager (только для варианта лицензирования Termidesk VDI);
- zVirt (только для варианта лицензирования Termidesk VDI);
- oVirt (только для варианта лицензирования Termidesk VDI);
- «РЕД Виртуализация» (только для варианта лицензирования Termidesk VDI);
- Openstack (версия Xena, только для варианта лицензирования Termidesk VDI);
- VMware vSphere (только для варианта лицензирования Termidesk VDI).

Termidesk поддерживает работу с терминальными серверами (терминальными сессиями и приложениями):

- Microsoft Windows Server с ролью «Remote Desktop Session Host» из состава «Remote Desktop Services» (далее - MS RDS, MS RDSH);
- Terminal Server Astra Linux, реализуется компонентом «Сервер терминалов Astra Linux» (далее - STAL).

1.5 . Требования к уровню подготовки персонала

Уровень подготовки персонала для штатной эксплуатации Termidesk приведен в таблице (см. Таблица 1).

Таблица 1 – Рекомендации по уровню подготовки персонала

Уровень персонала	Описание	Обязанности	Навыки
Уровень 1. Специалист(ы) службы поддержки	Оказывает первую линию технической поддержки по поступившим запросам: принимает, фиксирует запрос через доступные каналы связи. Выполняет первоначальный анализ и определение проблемы, классифицирует поступившие заявки, обслуживает типовые и повторяющиеся запросы по заранее подготовленным инструкциям	Определение проблемы, первоначальный анализ и базовое решение проблемы. Начальное устранение неполадок для определения характера проблемы. Создание заявки, сбор информации о пользователе и фиксация всех выполненных действий по устранению неполадок. Решение основных и повторяющихся проблем, связанных с Termidesk, используя существующие статьи базы знаний и справочного центра. Предварительное соотнесение проблемы к определенной области: ▪ операционная система; ▪ платформа виртуализации; ▪ сетевая связность или наличие необходимых сервисов; ▪ корректность конфигурации Termidesk; ▪ особенности настройки программного обеспечения в РМ. При недостаточности навыков или знаний для определения или разрешения проблемы - эскалирование проблемы на Уровень 2. Если проблема влияет на производственную среду или потенциально может привести к сбою на уровне системы, то эскалирование проблемы на Уровень 3. При необходимости создание запросов на дополнительные инструкции по решению проблем. Сбор обратной связи от конечного пользователя после закрытия заявки в службу поддержки для подтверждения решения проблемы	Необходимые навыки: ▪ пользовательский опыт работы с настольными ОС Windows и ОС Linux; ▪ знание персонального компьютера и офисных программ; ▪ базовое понимание организации локальной сети и работы сетевого оборудования; ▪ умение работать с ПО для приема, обработки и регистрации заявок и обращений пользователей; ▪ понимание принципов работы с запросами пользователей (систематизация, определение уровня важности и приоритета запроса); ▪ доброжелательное общение и способность ясно излагать свои мысли

Уровень персонала	Описание	Обязанности	Навыки
Уровень 2. Инженер(ы)	В первую очередь поддерживает ежедневные операции инфраструктуры Termidesk, включающие проактивный мониторинг и управление. Выполняет устранение неполадок промежуточного уровня и использует доступные инструменты мониторинга или устранения неполадок. Помогает в решении проблем, эскалированных поддержкой Уровня 1.	Выполнение промежуточного анализа, определение и разрешения проблем, эскалированных с Уровня 1. Систематизация и связывание отдельных проблем для выявления возможной первопричины их появления. Оперативное реагирование на уведомления и сбои системы. Создание еженедельного отчета о количестве проблем, скорости их закрытия и контроль решения открытых проблем. Создание статей внутренней базы знаний и сценарий решения проблем, а также поддержание рабочих процессов устранения неполадок для Уровня 1. Выполнение основных процедур обслуживания и эксплуатации Termidesk. При недостаточности навыков или знаний для определения или разрешения проблемы - эскалирование проблемы на Уровень 3 или обращение в службу технической поддержки производителя. Изучение и анализ встроенных журналов событий Termidesk, ОС Windows и ОС Linux для выполнения базовых задач по устранению неполадок на основе общедоступной информации	Необходимые навыки: ▪ успешное прохождение обучения по курсу «Установка и администрирование Termidesk»; ▪ навыки администрирования ОС Windows и ОС Astra Linux, включая опыт работы в командной строке; ▪ навыки администрирования систем серверной виртуализации; ▪ понимание принципов работы сетей передачи и хранения данных

Уровень персонала	Описание	Обязанности	Навыки
Уровень 3. Администратор(ы)	Является центральной точкой внедрения, администрирования и обслуживания инфраструктуры VDI. Специализируется на развертывании и запуске новых вариантов использования Termidesk и управлению жизненным циклом новых фондов РМ. Эскалирует проблему в техническую поддержку производителя стороннего ПО и уведомляет о проблеме Уровень 4	Выполнение расширенного анализа, моделирования и решения проблем. Выполнение технического обслуживания и модернизации среды функционирования Termidesk. Устранение серьезных неполадок и сбоев в обслуживании. Управление Termidesk и средой функционирования. Контроль и управление административными задачами, выполняемыми Уровнем 2. Управление сетевой инфраструктурой и инфраструктурой хранения данных, связанных с функционированием Termidesk. Просмотр периодических отчетов о состоянии сервера, использовании ресурсов, пользовательском опыте и общей производительности среды. Ознакомление со статьями базы знаний производителей ПО и недавно выпущенными обновлениями, включая обновления безопасности ОС. Выполнение расширенного обслуживания серверов и инфраструктуры Termidesk. При необходимости передача запроса в службу технической поддержки производителя и уведомление о проблеме Уровня 4	Необходимые навыки: ▪ успешное прохождение обучения по курсу «Установка и администрирование Termidesk»; ▪ практический опыт администрирования серверных ОС на базе ОС Windows и ОС Linux; ▪ опыт администрирования систем серверной виртуализации; ▪ опыт в проектировании, обслуживании и поиске неисправностей в сетях передачи и хранения данных; ▪ опыт настройки и поиска неисправностей для сетевых сервисов и служб: DNS, DHCP, MS AD, LDAP, SSL, FIREWALL, LOAD BALANCING; ▪ знание кластеризации СУБД; ▪ знакомство с автоматизацией использования командной строки при помощи скриптовых языков

Уровень персонала	Описание	Обязанности	Навыки
Уровень 4. Архитектор(ы)	Оказывает минимальное воздействие на административные задачи, но концентрируется на планировании и валидации системно значимых изменений сервисов доставки BPM и приложений, включая погружение в связанные изменения в работе корпоративной сети передачи и хранения данных и сопутствующих сервисов, оказывающих непосредственное влияние на работу Termidesk	Техническое руководство предстоящими изменениями в программных компонентах, дизайне, сетевых сервисах предприятия. Устранение серьезных проблем и сбоев в обслуживании. Проведение нагрузочного тестирования для подтверждения соответствия технических характеристик потребностям бизнеса. Обновление проектной документации	Подтвержденные навыки разработки архитектуры, включая практический опыт в: ▪ управлении жизненным циклом информационных систем масштаба предприятия; ▪ понимании принципов управления жизненными циклами архитектурных ландшафтов и проектирования облачных приложений; ▪ проектировании высоконагруженных систем, в том числе платформ виртуализации. Знание принципов построения облачных платформ

Рекомендации по численности персонала приведены в таблице (см. Таблица 2) для различных окружений, включая количественные характеристики ферм и образов ОС.

Под фермой понимается отдельный набор сервисов Termidesk, реализуемый для задач масштабируемости, отказо- и катастрофоустойчивости, включая следующие компоненты:

- компонент Termidesk «Универсальный диспетчер»;
- компонент Termidesk «Шлюз»;
- компонент Termidesk «Менеджер рабочих мест»;
- серверы БД;
- балансировщики БД;
- балансировщики подключений.

Под образом понимается пользовательское окружение, состав которого может кардинальным образом отличаться между образами:

- тип ОС;
- версия ОС;
- используемое ядро ОС;
- установленные драйверы;
- установленные обновления и исправления, в том числе исправления безопасности в ОС;
- набор используемых приложений;
- версионность установленных приложений.

ⓘ Небольшое окружение: 1 ферма, менее 500 пользователей, до 2 образов.

Среднее окружение: до 2 ферм, от 1000 до 5000 пользователей, до 5 образов.
Большое окружение: от 2 ферм, от 5000 пользователей, от 5 образов.
Корпоративное окружение: от 2 ферм, от 10000 пользователей, от 10 образов.

Таблица 2 – Рекомендации по численности персонала

Уровень персонала	Небольшое окружение	Среднее окружение	Большое окружение	Корпоративное окружение
Уровень 1. Служба поддержки	2	4	8	от 16
Уровень 2. Инженеры	1	2	4	от 12
Уровень 3. Администраторы	1	2	3	от 5
Уровень 4. Архитекторы	1	1	2	от 2

1.6 . Типографские соглашения

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 . ТРЕБОВАНИЯ К СРЕДЕ ФУНКЦИОНИРОВАНИЯ

2.1 . Требования к аппаратному обеспечению

Минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры x86-64 (AMD, Intel), не менее 4 шт.;
- оперативная память, не менее 4 ГБ. Следует учесть, что для работы службы `termidesk-celery-worker` требуется, чтобы на каждое ядро процессора было выделено по 500 Мб оперативной памяти;
- свободное дисковое пространство, не менее 1 ГБ;
- сетевое соединение, не менее 100 Мбит/с.

2.2 . Требования к программному обеспечению

В среде функционирования должны быть предварительно установлены:

- ОС Astra Linux Special Edition версии 1.8 (минимальная версия - 1.8.1);
- СУБД PostgreSQL версии 15 из состава репозитория ОС Astra Linux Special Edition версии 1.8. Из внешних по отношению к ОС Astra Linux Special Edition версии 1.8 СУБД поддерживается СУБД PostgreSQL версии 12 и выше;
- брокер сообщений RabbitMQ из состава репозитория ОС Astra Linux Special Edition.

ОС Astra Linux Special Edition версии должна быть установлена из `iso`-образа, доступного в личном кабинете на портале Astra Linux: https://lk-new.astralinux.ru/. Работа Termidesk на преднастроенных образах ОС не гарантируется.

2.3 . Требования к синхронизации времени

В сетевой инфраструктуре должен быть настроен NTP-сервер, обеспечивающий синхронизацию времени для компонентов Termidesk.

2.4 . Требования к DNS и DHCP

В сетевой инфраструктуре должны быть развернуты и исправно функционировать службы доменных имен (DNS) и автоматического назначения сетевых параметров (DHCP) в необходимых сегментах сети.

Службы DNS и DHCP могут быть реализованы как отдельно, так и средствами платформы виртуализации (например, контекстуализацией ПК СВ Брест).

2.5 . Требования к серверам каталогов

Серверы каталогов должны удовлетворять следующим требованиям:

- сервер каталогов должен размещаться в том же сегменте локальной сети, где будут развернуты РМ. Если выполнение требования невозможно и сервер каталогов находится в другом сегменте, то необходимо обеспечить маршрутизацию между этими сегментами;
- при использовании в качестве сервера каталогов MS AD необходимо создать сервисную учетную запись для взаимодействия Termidesk с контроллером домена (КД). Допускается использование учетной записи администратора домена;
- при использовании MS AD рекомендуется создавать отдельные организационные подразделения (OU) для пользователей РМ и для учетных записей типа «Компьютер» для самих РМ. Права на OU для компьютеров должны быть либо у созданной сервисной учетной записи, либо у отдельной созданной учетной записи, допускается также использовать учетную запись администратора домена;
- при использовании серверов каталогов FreeIPA и ALDPro в качестве сервисной учетной записи для взаимодействия Termidesk с КД по умолчанию используется учетная запись администратора домена, либо отдельная учетная запись с аналогичными полномочиями.

⚠ Механизм подключения к LDAP-серверу `simple bind` передает данные для подключения в открытом виде.

2.6 . Требования к терминальным серверам

При использовании терминального сервера Microsoft необходимо наличие внутри домена MS AD серверов с соответствующими ролями (MS RDSH - роль терминального сервера, MS RDS - роль сервера публикации приложений).

2.7 . Требования к платформе виртуализации

Узлы платформы виртуализации должны удовлетворять следующим требованиям:

- должна быть поддержка виртуального чипсета (ich9-intel-hda);
- пул в настройках DHCP или параметрах контекстуализации должен поддерживать достаточное количество IP-адресов;
- виртуальный коммутатор платформы должен поддерживать достаточное количество MAC-адресов;
- в платформе виртуализации на базе QEMU/KVM должны быть реализованы необходимые для работы Termidesk именованные каналы:
  - для перенаправления каталогов - `org.spice-space.webdav.0`(`/dev/virtio-ports/org.spice-space.webdav.0`;
  - для взаимодействия с `libvirt` (необходим компоненту «Агент узла виртуализации») - `ru.termidesk.tvm.0` (`/dev/virtio-ports/ru.termidesk.tvm.0`);

- для включения перенаправления видеокамеры - `ru.termidesk.RealtimeStreaming.0` (`/dev/virtio-ports/ru.termidesk.RealtimeStreaming.0`);
- канал для включения перенаправления смарт-карт - `ru.termidesk.PCSC.0` (`/dev/virtio-ports/ru.termidesk.PCSC.0`);
- канал для включения перенаправления принтера - `ru.termidesk.Printer.0` (`/dev/virtio-ports/ru.termidesk.Printer.0`).

Для ПК СВ Брест включение именованных каналов определяется конфигурационным файлом `/etc/one/vmm_exec/vmm_exec_kvm.conf`, находящимся на фронтальных машинах ПК СВ Брест.

Для включения каналов на узле системы виртуализации ПК СВ Брест необходимо:

- установить компонент «Агент узла виртуализации» (подробно о назначении и установке компонента см. документ СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»):

```
sudo apt install termidesk-vmsd
```

- убедиться, что состояние службы компонента «Агент узла виртуализации» находится в состоянии «`active (running)`»:

```
systemctl status termidesk-vmsd
```

Затем на фронтальной машине ПК СВ Брест выполнить активацию именованных каналов:

- открыть на редактирование файл `/etc/one/vmm_exec/vmm_exec_kvm.conf`;
- присвоить параметрам `WEBDAV_USE_DEFAULT`, `VIDEOCAM_OPTIMIZATION_USE_DEFAULT`, `PRINTER_OPTIMIZATION_USE_DEFAULT`, `USBTOKEN_OPTIMIZATION_USE_DEFAULT`, `SPICE_DETECT_USE_DEFAULT` значение «yes». Пример фрагмента файла с нужными значениями:

```
1  #rbt: webdav use
2  WEBDAV_USE_DEFAULT="yes"
3  WEBDAV_OPTIONS="
4      <channel type='spiceport'>
5          <source channel='org.spice-space.webdav.0'/>
6          <target type='virtio' name='org.spice-space.webdav.0'/>
7      </channel>"
8
9  #rbt: camera optimization
10 VIDEOCAM_OPTIMIZATION_USE_DEFAULT="yes"
11 VIDEOCAM_OPTIMIZATION_OPTIONS="
12     <channel type='spiceport'>
13         <source channel='TDSK_STREAM'/>
14         <target type='virtio' name='ru.termidesk.RealtimeStreaming.0'/>
15     </channel>"
16
17 #rbt: printer optimization
18 PRINTER_OPTIMIZATION_USE_DEFAULT="yes"
19 PRINTER_OPTIMIZATION_OPTIONS="
```

```
20      <channel type='spiceport'>
21          <source channel='TDSK_PRINTER'/>
22          <target type='virtio' name='ru.termidesk.Printer.0'/>
23      </channel>"
24
25  #rbt: USB token optimization
26  USBTOKEN_OPTIMIZATION_USE_DEFAULT="yes"
27  USBTOKEN_OPTIMIZATION_OPTIONS="
28      <channel type='spiceport'>
29          <source channel='TDSK_PCSC'/>
30          <target type='virtio' name='ru.termidesk.PCSC.0'/>
31      </channel>"
32
33  #rbt: SPICE detect
34  SPICE_DETECT_USE_DEFAULT="yes"
35  SPICE_DETECT_OPTIONS="
36      <channel type='unix'>
37          <source mode='connect' path='/var/run/tvmd.sock' >
38              <reconnect enabled='yes' timeout='1'/>
39          </source>
40          <target type='virtio' name='ru.termidesk.tvm.0'/>
41      </channel>"
```

⚠ Присвоение параметру `SPICE_DETECT_USE_DEFAULT` значения «yes» должно выполняться только после установки на узлы системы виртуализации компонента «Агент узла виртуализации» и успешного запуска его службы.

- сохранить изменения в файле `/etc/one/vmm_exec/vmm_exec_kvm.conf`;
- перезапустить службу `opennebula`:

```
sudo systemctl restart opennebula
```

3 . ИСПОЛЬЗОВАНИЕ КОНТЕКСТУАЛИЗАЦИИ ПК СВ БРЕСТ

3.1 . Контекстуализация в ПК СВ Брест

В ПК СВ Брест применяется метод контекстуализации для отправки информации на ВМ во время загрузки. Основная задача метода - передача настроек сети и учетных данных для настройки ВМ. Дополнительная задача - передача индивидуальных сценариев для загрузки ВМ.

> ⓘ Использование метода контекстуализации ПК СВ Брест не является обязательным, однако значительно упрощает и автоматизирует процесс подготовки узлов с компонентами Termidesk.

Для включения контекстуализации в гостевой ОС Astra Linux нужно в базовый образ установить пакет `one-context`:

```
sudo apt install one-context
```

Если после выполнения команды появляются сообщения об ошибке «Невозможно найти пакет one-context», «Пакеты имеют неудовлетворенные зависимости» необходимо убедиться, что в файле `/etc/apt/sources.list` заданы и не закомментированы источники получения пакетов (репозитории), затем обновить списки пакетов:

```
sudo apt update
```

После этого нужно вновь выполнить команду установки пакета `one-context`.

Для включения контекстуализации в гостевой ОС Microsoft Windows нужно включить службу, обрабатывающую скрипты контекстуализации. Для этого следует установить пакет `one-context-6.2.0` или более новый.

Параметры непосредственно контекста задаются в шаблоне ВМ, для этого в панели управления ПК СВ Брест надо открыть шаблон ВМ и перейти во вкладку «Контекст».

4 . ПОДГОТОВКА СРЕДЫ ФУНКЦИОНИРОВАНИЯ

Если Termidesk планируется устанавливать автоматизированно согласно подразделу **Автоматизированная установка**, то подготовку среды функционирования выполнять не нужно.

4.1 . Установка СУБД PostgreSQL

Для установки СУБД PostgreSQL необходимо:

- отредактировать файл `/etc/apt/sources.list`, оставив в качестве источников получения пакетов сетевые репозитории. Пример файла `/etc/apt/sources.list` для ОС Astra Linux Special Edition 1.8:

Приведен только пример файла! Он должен быть скорректирован, исходя из используемой и поддерживаемой версии ОС. Подробную информацию о сетевых репозиториях ОС Astra Linux Special Edition можно получить в справочном центре Astra Linux для ОС Astra Linux Special Edition 1.8: https://wiki.astralinux.ru/pages/viewpage.action?pageId=302043111.
Если в файле `/etc/apt/sources.list` присутствует репозиторий `astra-ce`, то необходимо закомментировать его, чтобы избежать установки несовместимых версий пакетов.

```
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-main/ 1.8_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-extended/ 1.8_x86-64 main contrib non-free
```

- перейти в интерфейс командной строки и обновить списков пакетов:

```
sudo apt update
```

- установить СУБД PostgreSQL:

При установке на ОС Astra Linux Specail Edition 1.8 следует выбирать СУБД PostgreSQL версии 15 (входит в состав ОС).

```
sudo apt install -y postgresql
```

где:

`-y` - ключ для пропуска подтверждения установки.

4.2 . Настройка СУБД PostgreSQL

Перед установкой Termidesk нужно выполнить настройку базы данных (БД).

При работе с СУБД следует учитывать ее ограничения: суммарное количество подключений к СУБД должно быть не более 75% от максимально разрешенного количества подключений. Для СУБД PostgreSQL по умолчанию максимальное количество подключений - 100.
Для оценки количества подключений к СУБД можно воспользоваться формулой: (количество порталов «Универсального диспетчера» × количество ядер процессоров × 3) + (количество узлов с запущенными службами `termidesk-celery-beat` и `termidesk-celery-worker` × количество ядер на этих узлах).

Для настройки БД следует перейти в интерфейс командной строки и выполнить:

- переключиться на пользователя `postgres`:

```
sudo su postgres
```

- запустить терминальный клиент СУБД PostgreSQL:

```
psql
```

Если после выполнения команды отображается ошибка «could not change directory to "/home/": Отказано в доступе» и не появляется приглашение командной строки `postgres=#`, необходимо вместо `su postgres` использовать конструкцию `su - postgres`. Если приглашение `postgres=#` появилось, то сообщение об ошибке можно проингорировать.
Если приглашение `postgres=#` не появляется, то вероятнее всего ОС Astra Linux Special Edition используется в более защищенном режиме, например, «Смоленск». В таком случае нужно для пользователя `postgres` назначить высокий уровень целостности:

```
sudo pdpl-user -i 63 postgres
```

- используя интерактивный интерфейс терминального клиента СУБД PostgreSQL, создать БД `termidesk` (символ ; в конце строки при работе с интерактивным интерфейсом обязателен):

```
postgres=# CREATE DATABASE termidesk LC_COLLATE 'ru_RU.utf8' LC_CTYPE 'ru_RU.utf8'
TEMPLATE template0;
```

где:

`LC_COLLATE` - порядок сортировки для использования в БД, влияет на порядок сортировки, применяемый к строкам. Значение `ru_RU.utf8` указывает на использование русской локализации;

`LC_CTYPE` - классификация символов для использования в БД, влияет на категоризацию символов;

`TEMPLATE` - имя шаблона, из которого создается БД. Шаблон `template0` используется для системной БД самой СУБД PostgreSQL.

- создать пользователя `termidesk` с паролем `ksedimret` для дальнейшего подключения к БД:

```
postgres=# CREATE USER termidesk WITH PASSWORD 'ksedimret';
```

В приведенной команде имя пользователя и пароль используются в качестве примера. Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты. Для задания пароля разрешено использовать только латинские буквы A-Z, a-z, цифры 0-9 и символы $!@%^&#_-=+~`;:.,?()*{}[]\/.

- назначить права по использованию БД `termidesk` созданному пользователю `termidesk`:

```
postgres=# GRANT ALL PRIVILEGES ON DATABASE termidesk TO termidesk;
```

- в случае, если используется СУБД PostgreSQL из состава ОС Astra Linux Special Edition 1.8, то сделать пользователя `termidesk` владельцем БД `termidesk`, тем самым предоставив ему все возможные права:

```
postgres=# ALTER DATABASE termidesk OWNER TO termidesk;
```

- выйти из интерактивного интерфейса терминального клиента СУБД PostgreSQL:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

- отредактировать файл `/etc/parsec/mswitch.conf`, установив параметр `zero_if_notfound` в значение `yes`, точно соблюдая отступы и пробелы:

```
1  # Return zero data instead of ENOENT/ENODATA in the absence of record
2  zero_if_notfound: yes
```

В случае последующего обновления СУБД PostgreSQL может понадобиться пересоздать БД. В этом случае следует предусмотреть экспорт БД перед обновлением СУБД PostgreSQL.

4.3 . Установка брокера сообщений RabbitMQ

> Если узел с уже установленным RabbitMQ будет переименован, то брокер сообщений перестанет принимать подключения. Для исправления ситуации необходимо удалить RabbitMQ, затем выполнить его переустановку.

Для установки RabbitMQ нужно перейти в интерфейс командной строки через программу «Терминал Fly» и выполнить:

```
sudo apt install -y rabbitmq-server
```

где:

`-y` - ключ для пропуска подтверждения установки.

4.4 . Настройка брокера сообщений RabbitMQ

Для настройки RabbitMQ следует:

- перейти в интерфейс командной строки через программу «Терминал Fly» и убедиться в наличии каталога `/etc/rabbitmq`:

```
ls /etc/ | grep rabbitmq
```

- если каталог отсутствует, необходимо создать его:

```
sudo mkdir -p /etc/rabbitmq
```

  где:

  - `p` - ключ для автоматического создания директорий, указанных внутри пути;

- перейти в каталог `/etc/rabbitmq`:

```
cd /etc/rabbitmq
```

- создать пустые файлы `rabbitmq.conf` (основной файл конфигурации RabbitMQ) и `definitions.json` (файл определения данных для подключения):

```
1 sudo touch rabbitmq.conf
2 sudo touch definitions.json
```

> Файл `definitions.json` можно скопировать из `iso`-образа Termidesk.

- поменять владельца (`rabbitmq`) и идентификатор группы (`rabbitmq`) для созданных файлов:

```
sudo chown rabbitmq:rabbitmq definitions.json rabbitmq.conf
```

- отредактировать файл `rabbitmq.conf`, приведя его к виду:

```
# ========================================== Management section ==========================================
## Preload schema definitions from the following JSON file.
## Related doc guide: https://rabbitmq.com/management.html#load-definitions.
##
# management.load_definitions = /path/to/exported/definitions.json
management.load_definitions = /etc/rabbitmq/definitions.json
```

Если необходимо, чтобы RabbitMQ работал через TLS-соединение, то файл `rabbitmq.conf` нужно привести к виду:

```
# ========================================== Management section ==========================================
## Preload schema definitions from the following JSON file.
## Related doc guide: https://rabbitmq.com/management.html#load-definitions.
##
# management.load_definitions = /path/to/exported/definitions.json
management.load_definitions = /etc/rabbitmq/definitions.json
listeners.tcp.default = 5672

# TLS Порт
listeners.ssl.default = 5671
# Пути к сертификатам
ssl_options.cacertfile = /var/ssl/root-ca.crt
ssl_options.certfile   = /var/ssl/cert.crt
ssl_options.keyfile    = /var/ssl/private/private-key.key
# Пароль для ключа
#ssl_options.password =  # Should peer verification be enabled?
ssl_options.verify     = verify_peer

# When set to true, TLS connection will be rejected if client fails to provide a certificate
ssl_options.fail_if_no_peer_cert = false

ssl_options.versions.default = tlsv1.2
```

Предполагается, что файлы корневого сертификата (`/var/ssl/root-ca.crt`), сертификата узла (`/var/ssl/cert.crt`) и закрытого ключа (`/var/ssl/private/private-key.key`) к нему уже существуют и доступны по указанному пути.

- отредактировать файл `definitions.json`, задав пользователей `termidesk` и `admin`, приведя его к виду:

В файле `/etc/rabbitmq/definitions.json` пароли указываются в виде преобразованного значения, которое можно получить через исполняемый файл `rabbitmq_password2hash.sh`. Процесс преобразования пароля будет приведен далее.

```
{
    "rabbit_version": "3.7.8",
    "users": [
        {
            "name": "termidesk",
            "password_hash": "pnXiDJtUdk7ZceL9iOqx44PeDgRa+X1+eIq+7wf/PTONLb1h",
            "hashing_algorithm": "rabbit_password_hashing_sha256",
            "tags": ""
        },
        {
            "name": "admin",
            "password_hash": "FXQ9WFNSrsGwRki9BT2dCITnsDwYu2lsy7BEN7+UncsPzCDZ",
            "hashing_algorithm": "rabbit_password_hashing_sha256",
            "tags": "administrator"
        }
    ],
    "vhosts": [
        {
            "name": "/"
        },
        {
            "name": "termidesk"
        }
    ],
    "permissions": [
        {
            "user": "termidesk",
            "vhost": "termidesk",
            "configure": ".*",
            "write": ".*",
            "read": ".*"
        },
        {
            "user": "admin",
            "vhost": "termidesk",
            "configure": ".*",
            "write": ".*",
            "read": ".*"
        }
    ],
    "topic_permissions": [
        {
            "user": "termidesk",
            "vhost": "termidesk",
            "exchange": "",
            "write": ".*",
            "read": ".*"
        }
    ],
    "parameters": [],
    "global_parameters": [
        {
            "name": "cluster_name",
            "value": "rabbit@rabbitmq"
```

```
55          }
56      ],
57      "policies": [],
58      "queues": [],
59      "exchanges": [],
60      "bindings": []
61  }
```

⚠ В примере используются следующие пары логин-пароль: `admin:admin`, `termidesk:ksedimret`.
Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты. Для задания пароля разрешено использовать только латинские буквы A-Z, a-z, цифры 0-9 и символы !$%^&_-=+~`.,()*{}[]\|.

- выполнить команду инициализации RabbitMQ:

```
sudo rabbitmq-plugins enable rabbitmq_management
```

- перезапустить службу `rabbitmq-server`:

```
sudo systemctl restart rabbitmq-server
```

Чтобы получить преобразованное значение пароля, нужно воспользоваться исполняемым файлом `rabbitmq_password2hash.sh`, расположенным в подключенном репозитории Termidesk (см. **Получение пакетов установки в ОС Astra Linux Special Edition**) по пути `/var/repos/Addons/Scripts/`. Для этого:

- перейти в каталог `/var/repos/Addons/Scripts/`:

```
cd /var/repos/Addons/Scripts/
```

- задать файлу `rabbitmq_password2hash.sh` флаг для запуска:

```
sudo chmod +x rabbitmq_password2hash.sh
```

где:

`+x` - ключ установки разрешения на запуск файла для всех пользователей;

- выполнить исполняемый файл:

```
sudo ./rabbitmq_password2hash.sh
```

При выполнении исполняемого файла будет предложено ввести пароль и повторить его. Преобразованное значение введенного пароля отображается в интерфейсе командной строки.

Необходимо внести полученное значение при формировании файла /etc/rabbitmq/definitions.json (секция password_hash).

Если конфигурационный файл /etc/rabbitmq/definitions.json уже существует, но требуется изменить в нем значение преобразованного пароля, нужно:

- выполнить преобразование и добавление пароля в файл /etc/rabbitmq/definitions.json:

```
sudo ./rabbitmq_password2hash.sh -w -u <user> -p <пароль>
```

где:

-w - ключ для сохранения изменений в файл /etc/rabbitmq/definitions.json;

-u - пользователь RabbitMQ. В стандартной установке можно указывать admin;

-p - пароль;

- перезапустить службу rabbitmq-server:

```
sudo systemctl restart rabbitmq-server
```

4.5 . Подготовка ОС Astra Linux Special Edition

Для корректной установки Termidesk версии 6.X на ОС Astra Linux Special Edition версии 1.8 дополнительной подготовки не требуется.

4.6 . Настройка СУБД Tantor

Помимо поддержки PostgreSQL Termidesk может работать с другими СУБД, такими как Tantor, основанным на PostgreSQL. Установка СУБД должна быть выполнена согласно документации на нее.

После установки нужно последовательно выполнить шаги для настройки БД:

- переключиться на пользователя postgres:

```
sudo su postgres
```

- выполнить инициализацию БД:

```
/opt/tantor/db/<версия_Tantor>/bin/initdb -D /var/lib/postgresql/<каталог_Tantor>/data/
```

- запустить терминальный клиент СУБД:

```
./psql
```

- используя интерактивный интерфейс терминального клиента СУБД, создать БД termidesk (символ «;» в конце строки при работе с интерактивным интерфейсом обязателен):

```
postgres=# CREATE DATABASE termidesk LC_COLLATE 'ru_RU.utf8' LC_CTYPE 'ru_RU.utf8'
TEMPLATE template0;
```

- создать пользователя `termidesk` с паролем `ksedimret` для дальнейшего подключения к БД:

```
postgres=# CREATE USER termidesk WITH PASSWORD 'ksedimret';
```

> В приведенной команде имя пользователя и пароль используются в качестве примера. Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты. Для задания пароля разрешено использовать только латинские буквы A-Z, a-z, цифры 0-9 и символы $!@%^&#_-=+~`;:.,?()*{}[]\/.

- назначить все права по использованию БД `termidesk` созданному пользователю `termidesk`:

```
postgres=# GRANT ALL PRIVILEGES ON DATABASE termidesk TO termidesk;
```

- назначить права на создание объектов для схемы `public`:

```
postgres=# GRANT CREATE ON SCHEMA public TO termidesk;
```

- в случае, если используется СУБД PostgreSQL из состава ОС Astra Linux Special Edition 1.8, то сделать пользователя `termidesk` владельцем БД `termidesk`, тем самым предоставив ему все возможные права:

```
postgres=# ALTER DATABASE termidesk OWNER TO termidesk;
```

- выйти из интерактивного интерфейса терминального клиента СУБД:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
1  exit
```

- отредактировать файл `/etc/parsec/mswitch.conf`, установив параметр `zero_if_notfound` в значение `yes`, точно соблюдая отступы и пробелы:

```
1  # Return zero data instead of ENOENT/ENODATA in the absence of record
2  zero_if_notfound: yes
```

При работе с СУБД следует учитывать ее ограничения: суммарное количество подключений к СУБД должно быть не более 75% от максимально разрешенного количества подключений. Для PostgreSQL по умолчанию максимальное количество подключений - 100.

Для оценки количества подключений к СУБД можно воспользоваться формулой: (количество порталов «Универсального диспетчера» × количество ядер процессоров × 3) + (количество узлов с запущенными службами `termidesk-celery-beat` и `termidesk-celery-worker` × количество ядер на этих узлах).

5 . УСТАНОВКА ПРОГРАММНОГО КОМПЛЕКСА

5.1 . Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в deb-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате iso-образа.

Получить iso-образ можно двумя способами:

- заполнив запрос через сайт Termidesk: https://termidesk.ru/support/#request-support;
- через личный кабинет: https://lk-new.astralinux.ru/.

Для подключения локального репозитория Termidesk на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска termidesk-<версия>.iso;
- подключить образ диска к файловой системе в каталог /mnt:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

-o loop - параметры для привязки петлевого устройства (/dev/loop) к файлу termidesk-<версия>.iso, устройство затем монтируется в указанный каталог /mnt;

- скопировать содержимое каталога repos подключенного образа диска в каталог /var локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

-Rp - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет lsb-release:

```
sudo apt install -y lsb-release
```

где:

-y - ключ для пропуска подтверждения установки;

- добавить локальный репозиторий Termidesk (`/var/repos/astra`) в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:

```
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs) non-free" > /etc/apt/sources.list.d/termidesk_local.list'
```

где:

`-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

`echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки `deb file:/var/repos/astra $(lsb_release -cs) non-free` в файл `/etc/apt/sources.list.d/termidesk_local.list`;

`deb file:/var/repos/astra $(lsb_release -cs) non-free` - добавляемый репозиторий, вложенная команда `$(lsb_release -cs)` подставляет версию - `1.8_x86-64`;

- выполнить поиск ключа репозитория Termidesk `GPG-KEY-PUBLIC` и добавить его:

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o /etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ `GPG-KEY-PUBLIC` существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, необходимо проверить правильность выполнения шагов по добавлению репозитория Termidesk в файл `/etc/apt/sources.list.d/termidesk_local.list`.
При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.
В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- обновить данные пакетного менеджера:

```
sudo apt update
```

Данную команду (`sudo apt update`) необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

5.2 . Комплексная установка Termidesk

5.2.1 . Автоматизированная установка

5.2.1.1 . Автоматизированная установка через исполняемый файл

Начиная с Termidesk версии 5.1 установка через исполняемый файл (скрипт) не поддерживается. Автоматизированная установка выполняется через конфигурационный файл.

5.2.1.2 . Автоматизированная установка через конфигурационный файл

Установка через файл ответов не поддерживается, начиная с Termidesk версии 5.0.

Для автоматизированной установки рекомендуется предварительно подготовить файл `/etc/opt/termidesk-vdi/termidesk.conf`, описание параметров которого приведено в подразделе **Параметры конфигурирования компонентов «Универсальный диспетчер», «Менеджер рабочих мест»** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса».

Перед установкой Termidesk следует убедиться, что в БД отсутствуют записи (необходимо использовать чистую БД).
Для установки портала «Агрегатор» в режиме автоматизированной установки следует обратиться к документу СЛЕТ.10001-01 90 08 «Руководство администратора. Установка и настройка портала «Агрегатор».

Пример файла `/etc/opt/termidesk-vdi/termidesk.conf` с установленными значениями имени пользователи и пароля по умолчанию и их хранением в конфигурационном файле (без использования хранилища, а также без использования защищенного подключения к БД и RabbitMQ (см. раздел **Подготовка среды функционирования**):

```
SECRETS_STORAGE_METHOD='config'
DB_CLUSTER_MODE='single'
DBHOST='localhost'
DBPORT='5432'
DBSSL='Disable'
DBNAME='termidesk'
DBUSER='termidesk'
```

```
8  DBPASS='ksedimret'
9  DBCERT=
10 DBKEY=
11 DBCHAIN=
12 DJANGO_SECRET_KEY='XejStbL6jtZ7DGTH02vJpw4vf1zTWM07RqWhwWGYKgs='
13 RABBITMQ_URL1='amqp://termidesk:ksedimret@localhost:5672/termidesk'
14 RABBITMQ_URL2=
15 RABBITMQ_URL3=
16 RABBITMQ_SSL='Disable'
17 LOG_LEVEL='INFO'
18 LOG_ADDRESS='/dev/log'
19 LOG_FACILITY='local3'
20 HEALTH_CHECK_ACCESS_KEY='270c1e6a4cd013a3824982458a26ec4dcac17f60f80a74098a62994
   f775351e2'
21 METRICS_ACCESS_KEY='2559773a3b1104064bbcb0b5315749a3783cb4f2fae6ee1925dc84ac0eef
   0f09'
22 NODE_ROLES='ADMIN,USER,CELERYMAN'
23 EULA_ACCEPTED='YES'
24 AGGREGATOR_ACCESS_TOKEN_TITLE='Termidesk JWT Title'
25 AGGREGATOR_JWT_SSL_CERT=
```

После установки указанные в открытом виде пароли можно привести к преобразованным значениям (см. подраздел **Параметры конфигурирования компонентов «Универсальный диспетчер», «Менеджер рабочих мест»** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса»).

5.2.2 . Неавтоматизированная установка Termidesk

Для установки фермы Termidesk с использованием псевдографического интерфейса нужно:

- подготовить среду функционирования (см. раздел **Подготовка среды функционирования**);
- подключить репозиторий Termidesk (см. подраздел **Получение пакетов установки**);
- установить Termidesk:

```
sudo apt -y install termidesk-vdi
```

где:

`-y` - ключ для пропуска подтверждения установки.

> При установке пакета `termidesk-vdi` возможно активировать режим отладки через переменную окружения `TDSK_PKG_DEBUG=1`.

> В зависимостях пакета установки `termidesk-vdi` есть:
> - служба ведения журналов `syslog-ng`. Работа с другими службами ведения журналов не гарантируется;

- пакет `libpython3.11` для ОС Astra Linux Special Edition 1.8, предоставляющий возможность установить Termidesk в ОС с минимальной конфигурацией (без графического интерфейса ОС).

Перед обновлением ОС или службы `syslog-ng` рекомендуется создать резервную копию файла `syslog-ng.conf`. В случае обновления ОС или службы `syslog-ng` без предварительного создания резервной копии файла, может потребоваться переустановка Termidesk для восстановления его корректной работы.
Компонент «Шлюз» устанавливается из пакета `termidesk-gateway`. Для установки или обновления «Шлюза» следует обратиться к подразделам **Установка Шлюза** и **Обновление Шлюза** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз».

В процессе установки нужно:

Для переключения между экранными кнопками **[Ок]** и **[Отмена]** в псевдографическом интерфейсе используется клавиша **<Tab>**.

- ознакомиться с лицензионным соглашением и нажать экранную кнопку [Далее] (см. Рисунок 1);

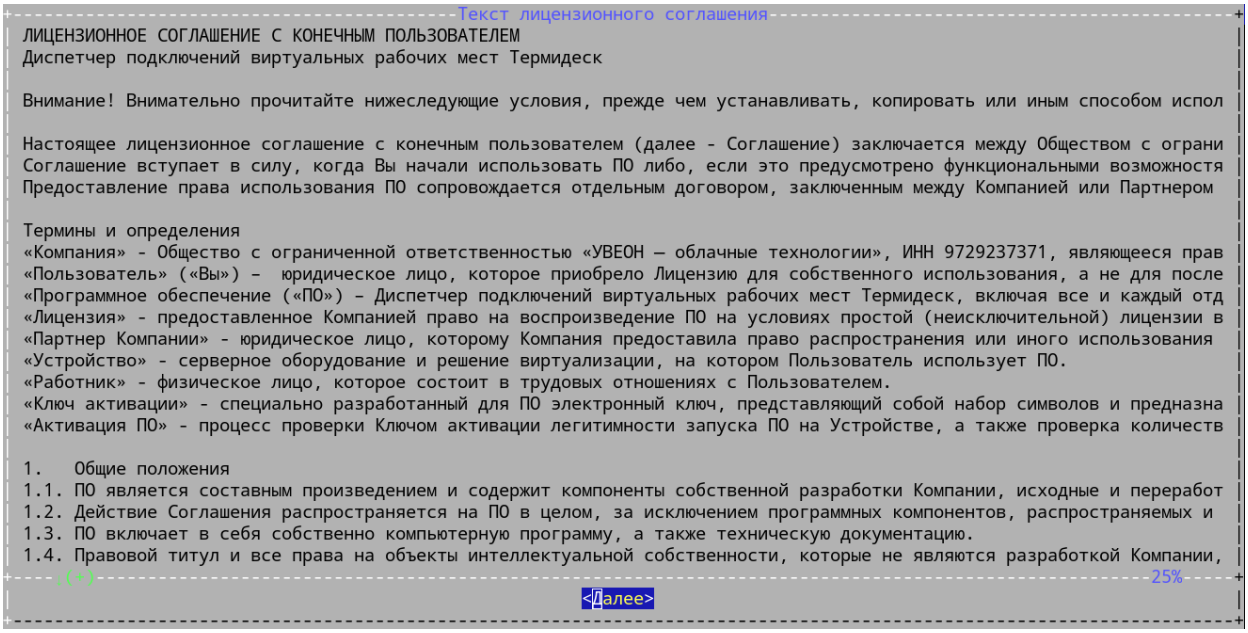

Рисунок 1 – Лицензионное соглашение

- нажать экранную кнопку [Да] (см. Рисунок 2) для принятия условий лицензионного соглашения и продолжения установки или экранную кнопку **[Нет]** в случае отказа, при этом установка прервется;

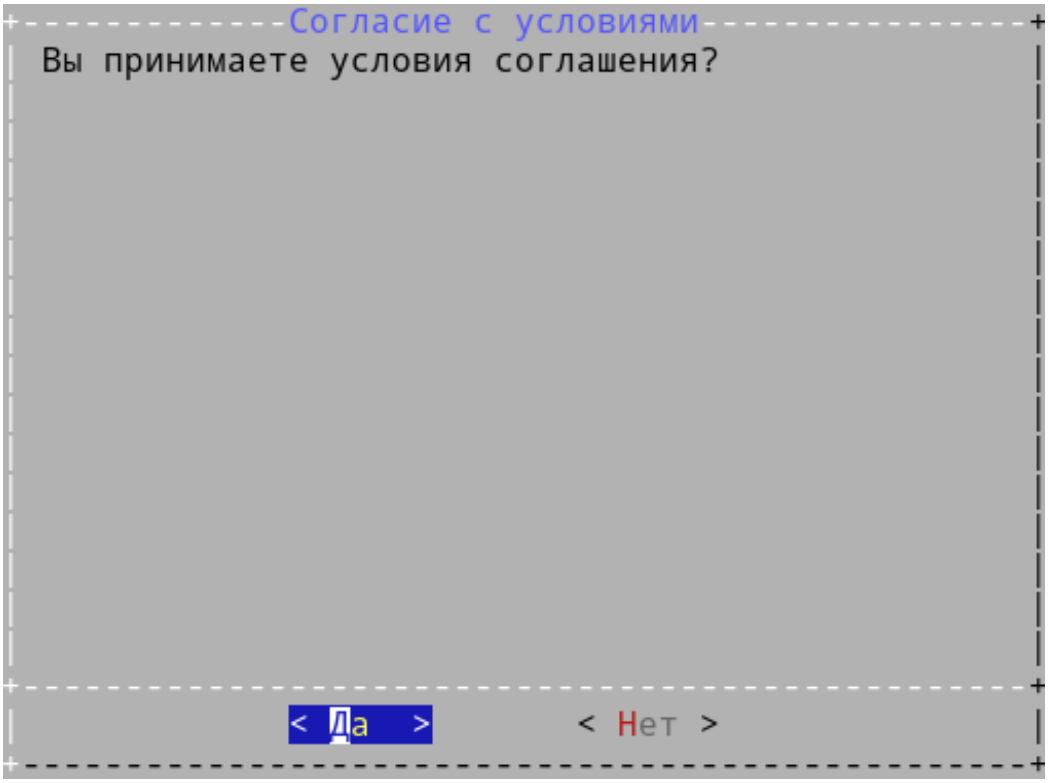

Рисунок 2 – Принятие условий лицензионного соглашения

- после принятия условий лицензионного соглашения выбрать способ хранения паролей (см. Рисунок 3) подключения к СУБД и RabbitMQ:

> Для всех узлов фермы Termidesk должен выбираться единый способ хранения и единое хранилище (в случае выбора способа «hvac»).

- «config» (по умолчанию) - пароли будут храниться в преобразованном виде в файле `/etc/opt/termidesk-vdi/termidesk.conf`;
- «hvac» (рекомендуемый способ для безопасного хранения) - для хранения паролей будет использоваться хранилище паролей OpenBao или Hashicorp Vault (хранилище должно быть заранее создано и настроено). Подробная информация по этому способу хранения паролей приведена в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»;
- «openbao» (экспериментальный) - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено). При этом пароли располагаются внутри хранилища, имена контейнеров хранения генерируются автоматически;

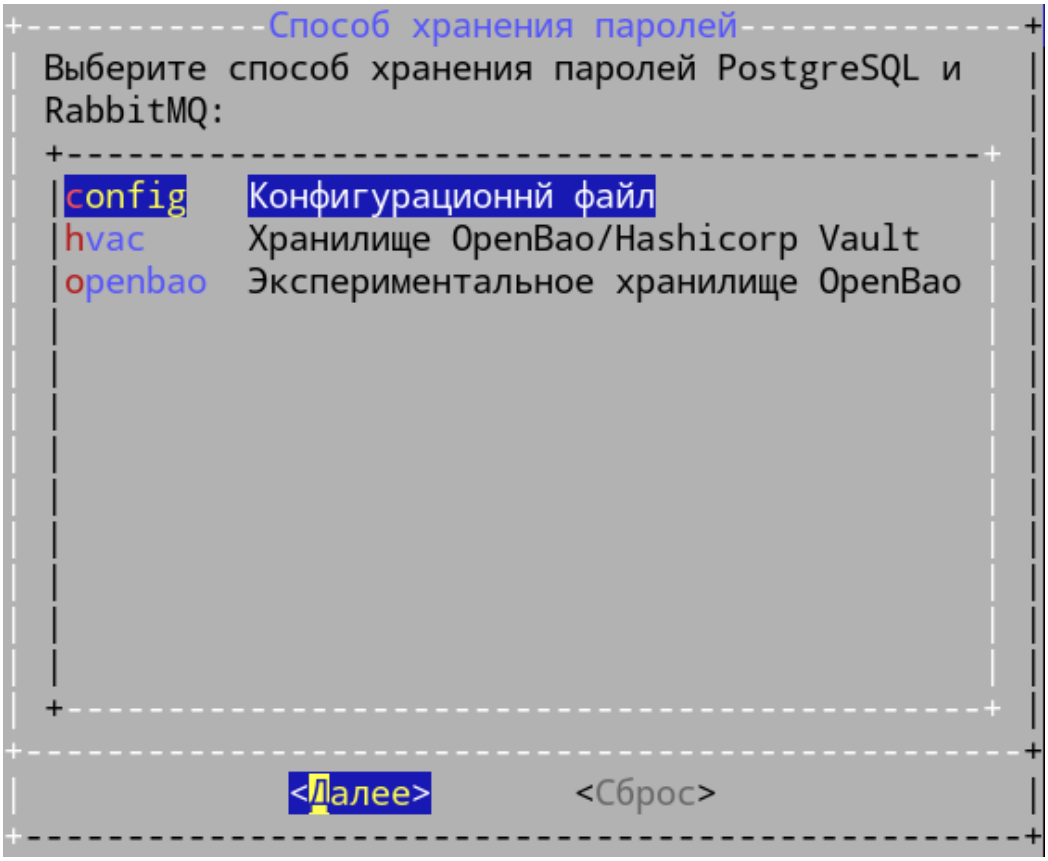

Рисунок 3 – Выбор способа хранения паролей

- при выборе хранения паролей «openbao» или «hvac» нужно задать параметры подключения к хранилищу и параметры, настроенные непосредственно на хранилище (см. Рисунок 4):
  - «URL хранилища» - IP-адрес или FQDN узла и порт с установленным хранилищем OpenBao. Формат: `http://<IP-адрес>:8200` или `http://<FQDN>:8200`. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом. В этом случае на следующем шаге будет открыт диалог настройки путей к сертификатам;

> ⚠ Хранилище паролей OpenBao должно быть реализовано в отказоустойчивом варианте, иначеTermidesk не будет работать в период простоя узлов OpenBao.

  - «Версия API OpenBao» - установленная версия API на OpenBao (`1` или `2`);
  - «Токен доступа к хранилищу» - токен (Initial Root Token), сформированный при инициализации хранилища;
  - «Путь к паролю СУБД» - путь, настроенный на OpenBao для хранения пароля СУБД;
  - «Роль доступа к паролю СУБД» - роль, настроенная на OpenBao, имеющая доступ к паролю СУБД;
  - «Путь к паролям RabbitMQ» - путь, настроенный на OpenBao для хранения пароля RabbitMQ;

- «Роль доступа к паролям RabbitMQ» - роль, настроенная на OpenBao, имеющая доступ к паролю RabbitMQ;
- «Путь к паролям Termidesk» - путь, настроенный на OpenBao для хранения пароля Termidesk;
- «Роль доступа к паролям Termidesk» - роль, настроенная на OpenBao, имеющая доступ к паролю Termidesk;
- «Время кеширования паролей, сек» - время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти;

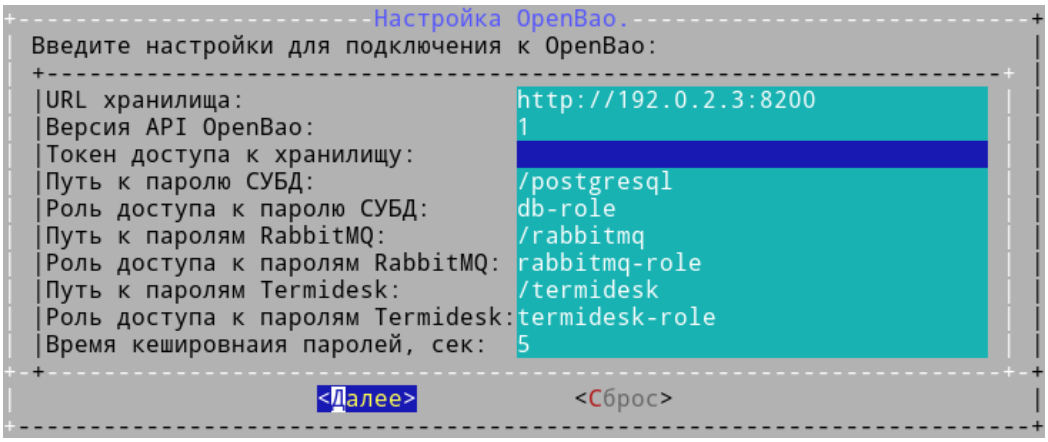

Рисунок 4 – Настройка подключения к OpenBao

- после настройки способа хранения паролей нужно выбрать протокол, который будет использоваться при подключении к БД (см. Рисунок 5). При выборе значения «Disable» защищенное соединение при подключении к БД использоваться не будет;

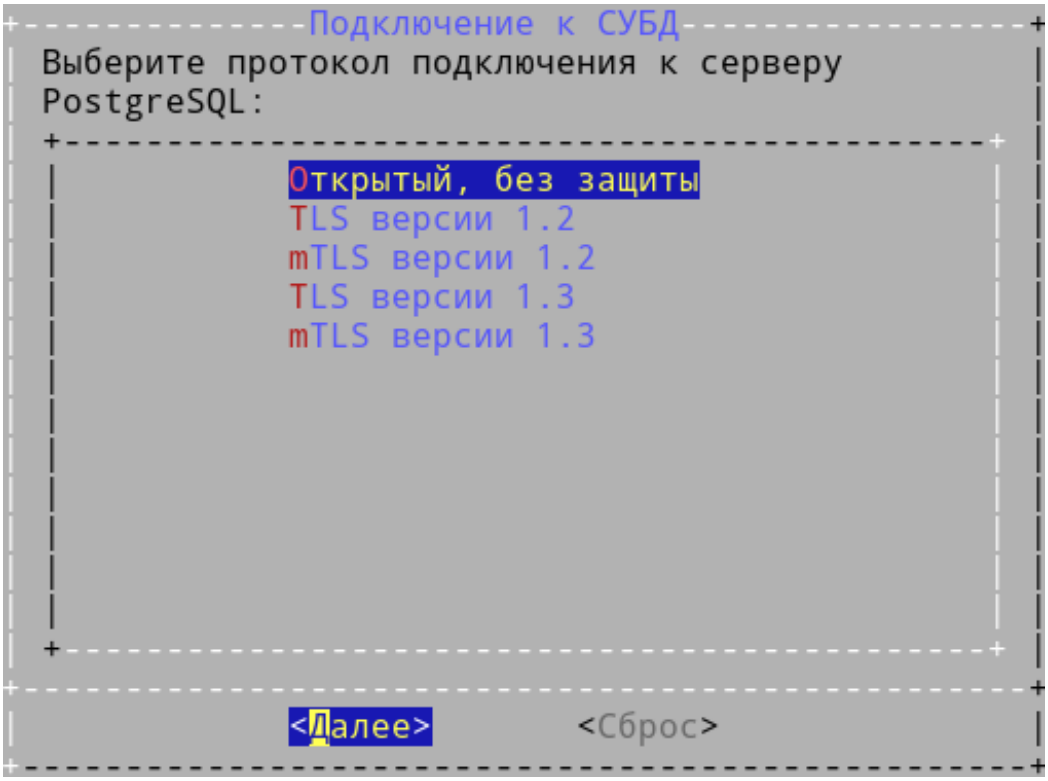

Рисунок 5 – Выбор протокола для подключения к БД

- при выборе защищенного подключения к БД или к OpenBao станет доступен раздел «Настройка сертификатов», в котором можно определить пути (см. Рисунок 6) к сертификатам и ключам:
  - «Сертификат Health Check»: путь к сертификату SSL/TLS для защищенного подключения к API проверки состояния;
  - «Секр. ключ Health Check»: путь к ключу SSL/TLS для защищенного подключения к API проверки состояния;
  - «Сертификат Postgres mTLS»: путь к сертификату SSL/TLS для защищенного подключения к СУБД;
  - «Секр. ключ Postgres mTLS»: путь к ключу SSL/TLS для защищенного подключения к СУБД;
  - «Серт. промеж. ЦС Postgres mTLS»: путь к промежуточному сертификату ЦС SSL/TLS для защищенного подключения к СУБД;
  - «Сертификат OpenBao mTLS»: путь к сертификату SSL/TLS для защищенного подключения к OpenBao. Задается, в случае, если выбран способ хранения паролей через OpenBao и нужно настроить защищенное подключение к нему;
  - «Секр. ключ OpenBao mTLS»: путь к ключу SSL/TLS для защищенного подключения к OpenBao. Задается, в случае, если выбран способ хранения паролей через OpenBao и нужно настроить защищенное подключение к нему;

- «Серт. промеж. ЦС OpenBao mTLS»: путь к промежуточному сертификату ЦС SSL/TLS для защищенного подключения к OpenBao. Задается, в случае, если выбран способ хранения паролей через OpenBao и нужно настроить защищенное подключение к нему;
- «Осн. серт. для расшифровки JWT-токена»: путь к сертификату для получения значения JWT-токена портала «Агрегатор». Задается в случае, если устанавливается «Портал администратора» и (или) «Портал пользователя», который затем будет подключен как узел в портале «Агрегатор»;
- «Рез. серт. для расшифровки JWT-токена»: путь к резервному сертификату для получения значения JWT-токена портала «Агрегатор». Задается в случае, если устанавливается «Портал администратора» и (или) «Портал пользователя», который затем будет подключен как узел в портале «Агрегатор»;
- «Секр. ключ для подписи JWT-токена»: путь к закрытому ключу для подписи JWT-токена портала «Агрегатор». Задается **только** в случае, если устанавливаются роли «Агрегатор администратора» и (или) «Агрегатор пользователя»;
- «Сертификат для подключения к серверу RA»: путь к серверному сертификату SSL/TLS для проверки подключения к «Удаленному помощнику»;
- «Сертификат RabbitMQ mTLS»: путь к клиентскому сертификату mTLS для защищенного подключения к RabbitMQ;
- «Секр. ключ RabbitMQ mTLS»: путь к клиентскому ключу mTLS для защищенного подключения к RabbitMQ;
- «Серт. ЦС RabbitMQ mTLS»: путь к корневому сертификату ЦС mTLS для защищенного подключения к RabbitMQ;
- «Публичный ключ ws-proxy»: путь к открытому ключу `id_rsa.pub`. Явно задавать путь следует только при использовани внешнего хранилища;
- «Секретный ключ ws-proxy»: путь к озакрытому ключу `id_rsa`. Явно задавать путь следует только при использовани внешнего хранилища;

- для продолжения установки нажать экранную кнопку **[Далее]**;

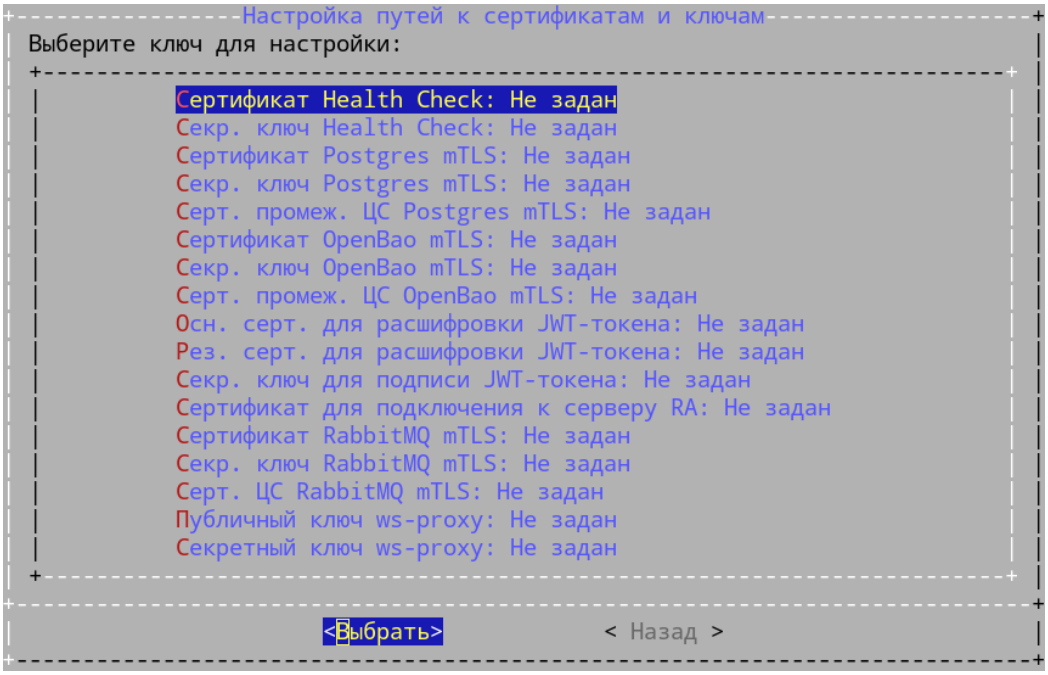

Рисунок 6 – Конфигурация сертификатов и ключей

- выбрать тип установки (см. Рисунок 7) СУБД:
  - «Отдельно стоящий сервер»: подключение производится к отдельному серверу СУБД;
  - «Кластер СУБД»: подключение производится к кластеру СУБД;

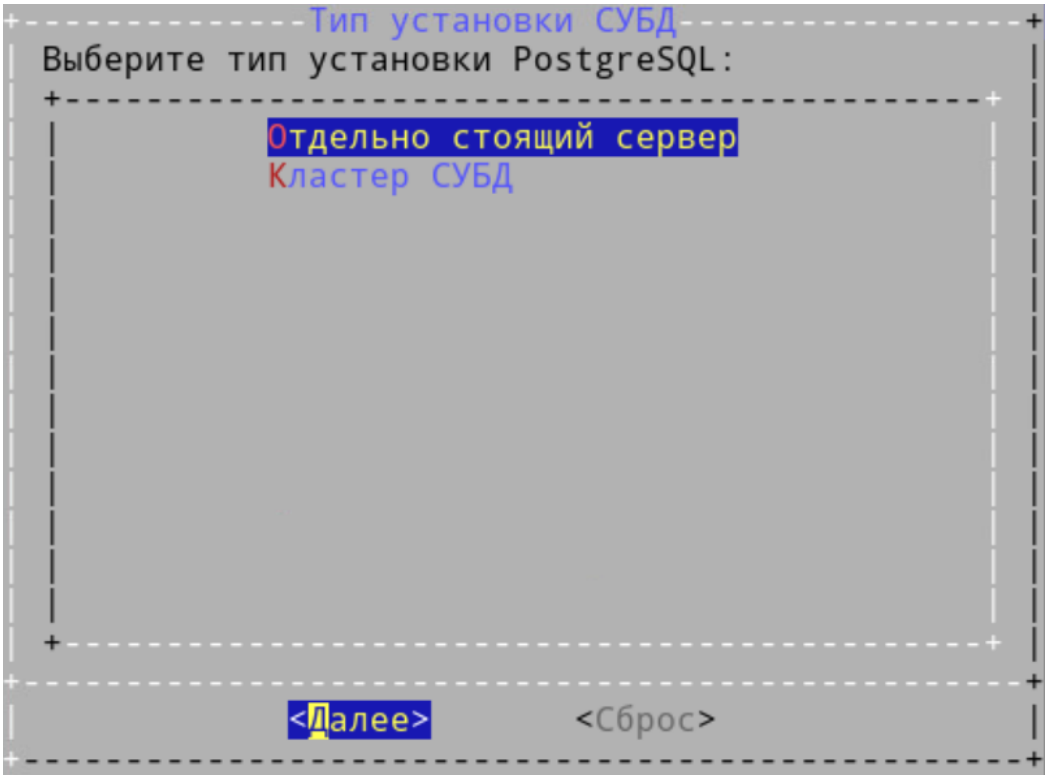

Рисунок 7 – Выбор типа установки СУБД

- заполнить параметры подключения к СУБД (см. Рисунок 8):

- «Адрес СУБД»: IP-адрес или FQDN узла с установленной СУБД (в случае локальной установки `127.0.0.1`);
- «Адрес СУБД (узел 2)»: IP-адрес или FQDN дополнительного узла СУБД (необязательный параметр, при необходимости может быть задан только для кластера СУБД);
- «Адрес СУБД (узел 3)»: IP-адрес или FQDN дополнительного узла СУБД (необязательный параметр, при необходимости может быть задан только для кластера СУБД);
- «Порт СУБД»: номер порта, используемого для соединения с сервером СУБД (стандартный порт `5432`);
- «Имя базы данных»: наименование БД (`termidesk`, параметр задавался при создании БД);
- «Имя пользователя»: имя пользователя БД для подключения к ней (`termidesk`, параметр задавался при создании БД);
- «Пароль»: пароль для подключения к БД (`ksedimret`, параметр задавался при создании БД);

▪ нажать экранную кнопку **[Тест]** для проверки подключения, ознакомиться с результатом тестирования подключения и для продолжения установки нажать экранную кнопку **[Далее]**;

> ⓘ Для корректной работы кнопки **[Тест]** требуется наличие установленных утилит `psql` и `expect`.
> При выборе типа установки СУБД «Кластер СУБД» можно задать до трех узлов СУБД, к которым будет подключаться Termidesk. При этом предполагается, что порт, имя БД, имя пользователя и его пароль идентичны для всех узлов.

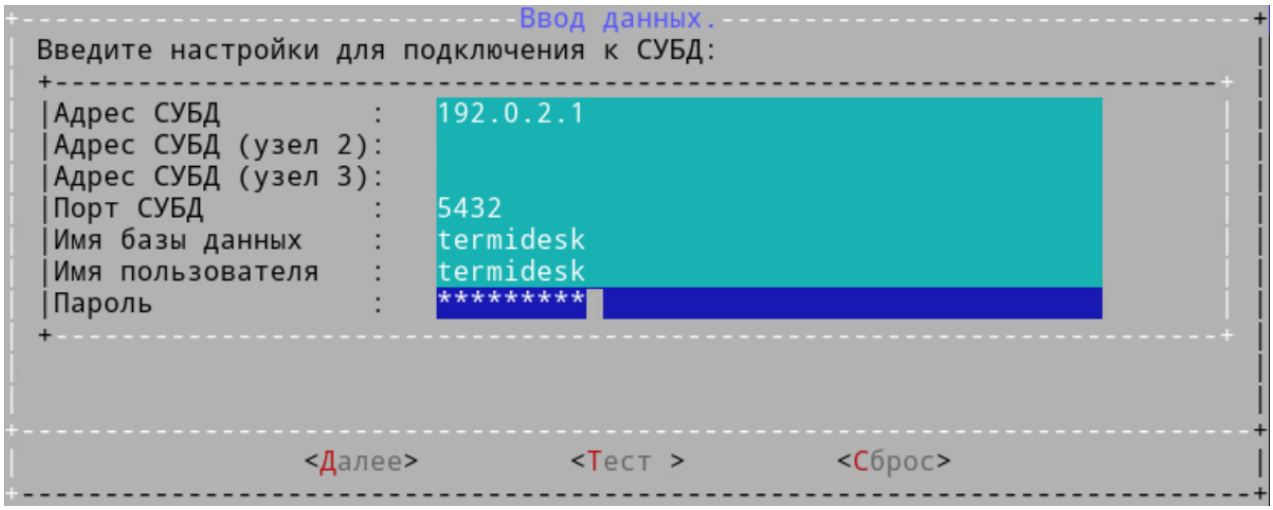

Рисунок 8 – Ввод параметров подключения к СУБД

- выбрать протокол, который будет использоваться при подключении к RabbitMQ (см. Рисунок 9). При выборе значения «Disable» защищенное соединение при подключении к RabbitMQ использоваться не будет;

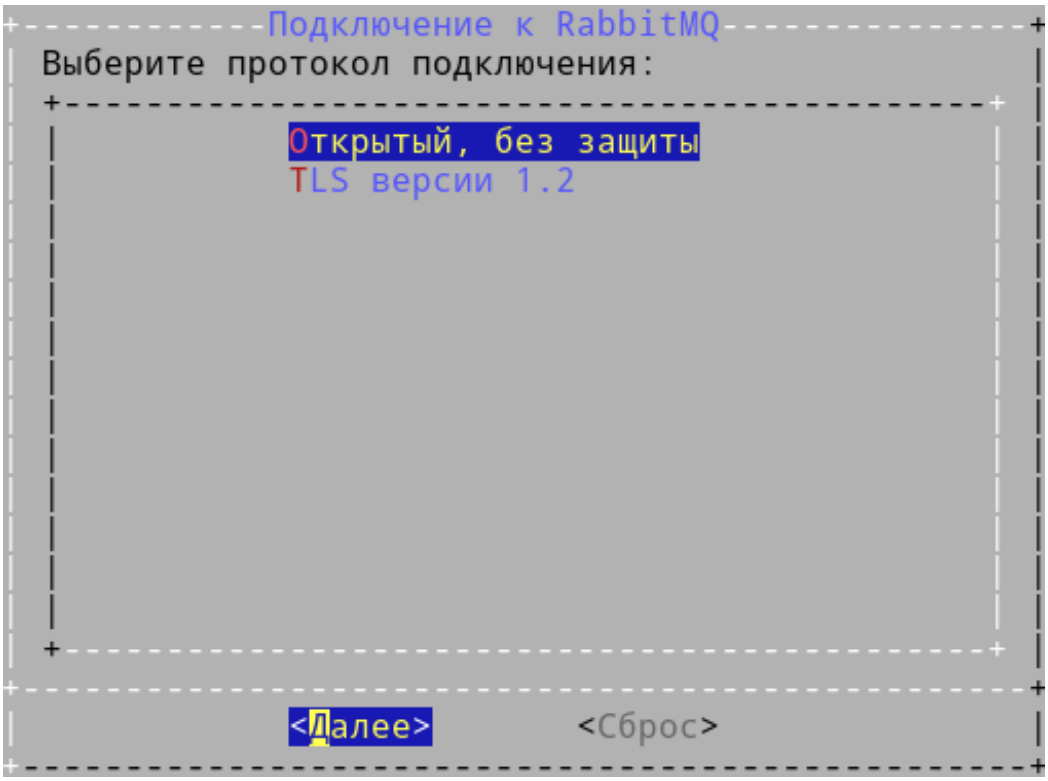

Рисунок 9 – Выбор протокола для подключения к RabbitMQ

- настроить подключение к RabbitMQ. Для этого выбрать в следующем окне пункт «Empty» и нажать экранную кнопку **[Выбрать]** (см. Рисунок 10). Необходимо задать хотя бы одно подключение к RabbitMQ, если не будет задано ни одно подключение, то при нажатии на кнопку **[Далее]** произойдет возврат в диалог настройки подключений;

Рисунок 10 – Экранная форма начала настройки подключения RabbitMQ

- выполнить настройку подключения к RabbitMQ, заполнив параметры (см. Рисунок 11):
  - «Адрес сервера»: IP-адрес или FQDN узла с установленным RabbitMQ (в случае локальной установки `127.0.0.1`);
  - «Порт сервера»: номер порта, используемого для соединения с RabbitMQ (по умолчанию 5672);
  - «Виртуальный хост»: виртуальный узел, к которому будет производиться подключение (`termidesk`);
  - «Имя пользователя»: имя пользователя для подключения (`termidesk`);
  - «Пароль»: пароль для подключения (`ksedimret`);
- нажать экранную кнопку **[OK]** для продолжения установки;

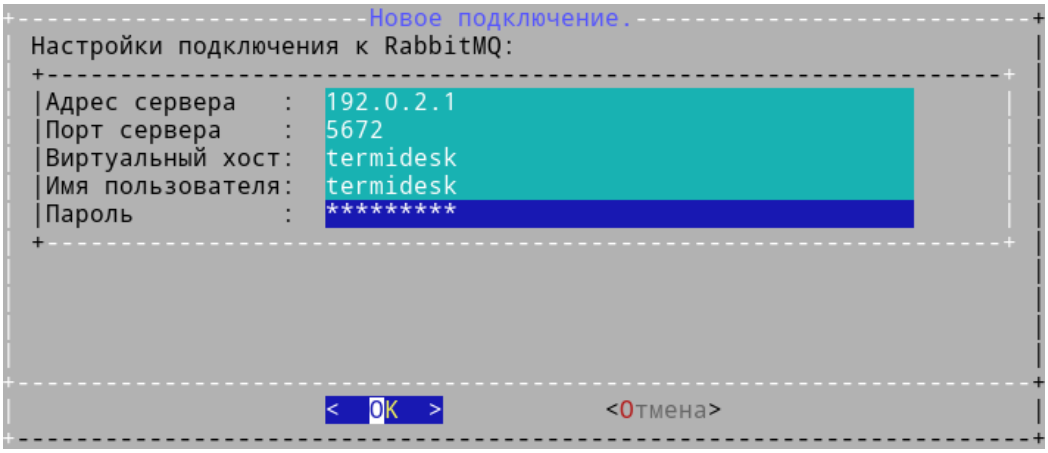

Рисунок 11 – Настройка подключения к RabbitMQ

- в следующем окне отобразится информация (см. Рисунок 12) о настроенном подключении. При необходимости можно добавить до трех экземпляров RabbitMQ для подключения, выбрав пустые строки «Empty» и повторив ввод параметров подключения. Для продолжения установки следует нажать экранную кнопку **[Далее]**;

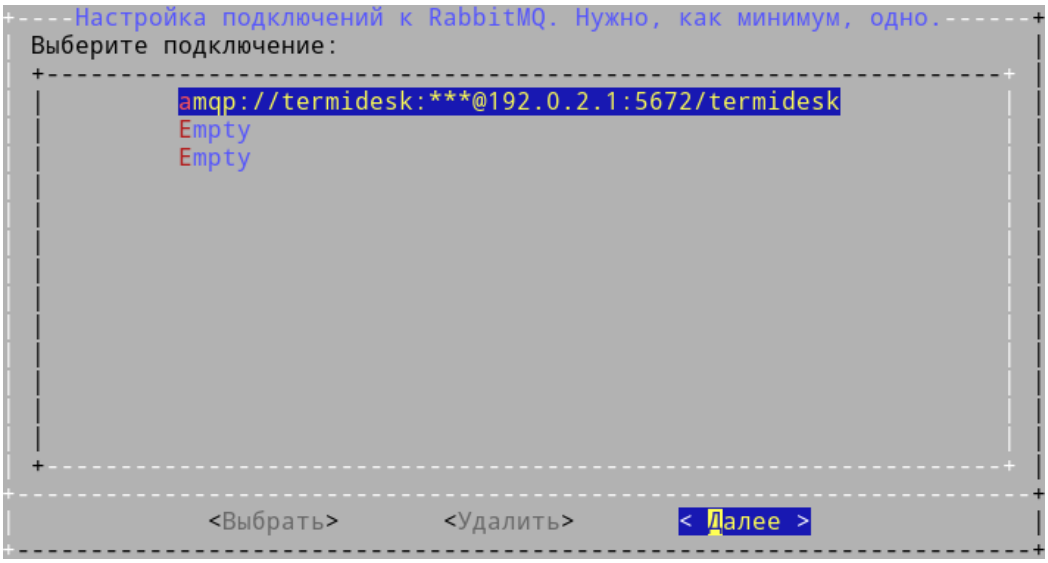

Рисунок 12 – Отображение параметров подключения к RabbitMQ

- затем выбрать устанавливаемую роль:

> Установка «Агрегатора» должна производиться на отдельном узле, отличном от «Портала администратора» и/или «Портала пользователя». Информация по выбору ролей при установке приведена в документе СЛЕТ.10001-01 90 08 «Руководство администратора. Установка и настройка портала «Агрегатор».
> Установка «Агрегатора» не предусмотрена в рамках лицензии Termidesk Terminal.

> При комплексной установке Termidesk необходимо выбрать роли: «Портал администратора», «Портал пользователя» (опционально, если нужно активировать все доступные функции), «Менеджер рабочих мест».
> Если не выбрать ни одного компонента, то ни одна служба Termidesk запущена не будет.

- «Портал администратора (ADMIN)»: установится компонент «Универсальный диспетчер» с «Порталом администратора». «Портал администратора» предоставляет интерфейс для управления Termidesk и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API («auth», «discover», «health», «agent», «webui»). После установки будет запущена служба `termidesk-vdi`;
- «Портал пользователя (USER)»: установится компонент «Универсальный диспетчер» с «Порталом пользователя». «Портал пользователя» предоставляет пользовательский интерфейс Termidesk и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API («auth», «discover», «health», «client», «wsproxy», «agent»). Интерфейс управления Termidesk будет недоступен. После установки будет запущена служба `termidesk-vdi`. При выборе и роли «Портал администратора», и роли «Портал пользователя» будут доступны функции обоих вариантов, при этом активируется доступ ко всем модулям документации по командам REST API, предоставляемым интерфейсом `swagger`;
- «Агрегатор администратора (AGGR_ADM)»: установится компонент «Универсальный диспетчер» с порталом «Агрегатор администратора». Портал «Агрегатор администратора» предоставляет интерфейс для управления объединенными ресурсами (фермами) Termidesk и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API. После установки будет запущена служба `termidesk-vdi`;
- «Агрегатор пользователя (AGGR_USR)»: установится компонент «Универсальный диспетчер» с порталом «Агрегатор пользователя». Портал «Агрегатор пользователя» предоставляет пользовательский интерфейс для подключения к фермам Termidesk и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API. После установки будет запущена служба `termidesk-vdi`. При

выборе и роли «Агрегатор администратора», и роли «Агрегатор пользователя» будут доступны функции обоих вариантов, при этом активируется доступ ко всем модулям документации по командам REST API, предоставляемым интерфейсом `swagger`;

- «Менеджер рабочих мест (CELERYMAN)»: установится компонент «Менеджер рабочих мест», после установки будут запущены службы `termidesk-celery-beat`, `termidesk-celery-worker`.

После установки Termidesk необходимо скорректировать файл конфигурации веб-сервера `/etc/apache2/apache2.conf`. Для этого нужно найти и раскомментировать строку с параметром `AstraMode`, далее присвоить данному параметру значение `off`, точно соблюдая отступы и пробелы в файле:

```
# Astra security mode
#
AstraMode off
```

Затем перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

> После установки параметры могут быть изменены через файл `/etc/opt/termidesk-vdi/termidesk.conf` (см. подраздел **Параметры конфигурирования компонентов «Универсальный диспетчер», «Менеджер рабочих мест»** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса») или через утилиту `termidesk-config` (см. подраздел **Утилита termidesk-config** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»).
> После успешного завершения установки на узел может быть установлен компонент «Шлюз» (`termidesk-gateway`). В распределенном варианте этот компонент устанавливается на отдельный узел.

5.3 . Распределенная установка программного комплекса

5.3.1 . Основные принципы распределенной установки

В Termidesk предусмотрена распределенная установка компонентов на отдельные серверы или ВМ.

> Описание применимо к ферме Termidesk.

Установка компонентов Termidesk выполняется в среде функционирования ОС Astra Linux Special Edition.

В распределенном варианте устанавливаются компоненты:

- «Универсальный диспетчер» (служба `termidesk-vdi`);
- «Шлюз» (служба `termidesk-gateway`);

- «Менеджер рабочих мест» (службы `termidesk-celery-beat`, `termidesk-celery-worker`).

Перечень условий для распределенной установки:

- брокер сообщений RabbitMQ устанавливается на одном узле с СУБД (в общем случае этот компонент может устанавливаться на отдельный узел, но в рамках настоящей процедуры данный вариант не рассматривается);

> ⚠ При использовании внешней по отношению к Termidesk СУБД, следует установить брокер сообщений RabbitMQ на узел «Менеджера рабочих мест» или на отдельный узел.

- на всех узлах, предназначенных для установки компонентов, настроены статические IP-адреса;
- на всех узлах настроена синхронизация времени от единого источника.

Упрощенная общая схема при распределенной установке Termidesk приведена на рисунке (см. Рисунок 13).

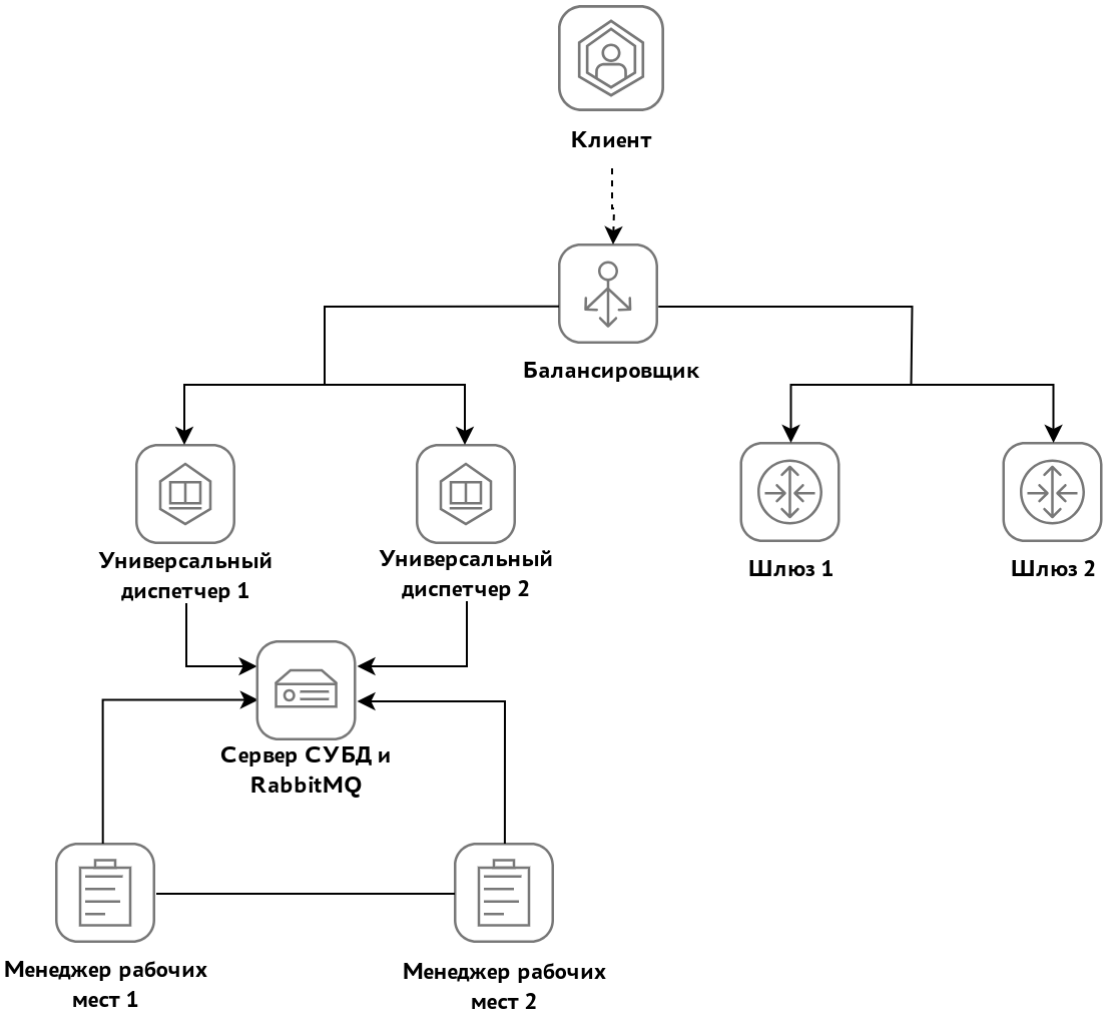

Рисунок 13 – Схема распределенной установки

Перечень обозначенных на схеме компонентов приведен в таблице (см. Таблица 3).

Таблица 3 – Перечень компонентов

Компонент	FQDN	Подпись на схеме
«Универсальный диспетчер» №1 с ролью «Портал универсальный»	`disp1.termidesk.local`	«Универсальный диспетчер 1»
«Универсальный диспетчер» №2 с ролью «Портал универсальный»	`disp2.termidesk.local`	«Универсальный диспетчер 2»
«Шлюз» №1	`gw1.termidesk.local`	«Шлюз 1»
«Шлюз» №2	`gw2.termidesk.local`	«Шлюз 2»
«Менеджер рабочих мест» №1	`tsk1.termidesk.local`	«Менеджер рабочих мест 1»
«Менеджер рабочих мест» №2	`tsk2.termidesk.local`	«Менеджер рабочих мест 2»
Балансировщик нагрузки (nginx)	`nginx.termidesk.local`	«Балансировщик»
База данных с брокером сообщений RabbitMQ	`db.termidesk.local`	«Сервер СУБД и RabbitMQ»

Распределенная установка проводится в следующей последовательности:

1) на одном узле устанавливаются СУБД и RabbitMQ. При установке следует учесть, что в БД должны отсутствовать записи (необходимо использовать чистую БД);

2) устанавливается первый (эталонный) узел с «Универсальным диспетчером». При установке необходимо выбрать роль «Портал универсальный». Роль активируется при одновременном выборе ролей «Портал администратора» и «Портал пользователя» в диалоговом окне псевдографического интерфейса инсталлятора;

> ⚠ Настройки первого узла с «Универсальным диспетчером» Termidesk будут использоваться как эталонные для узлов других «Универсальных диспетчеров» и «Менеджеров рабочих мест».
> Параметры конфигурации Termidesk находятся в файле `/etc/opt/termidesk-vdi/termidesk.conf`.
> Нужно скопировать каталог `/etc/opt/termidesk-vdi` вместе с его содержимым на узлы других «Универсальных диспетчеров» и «Менеджеров рабочих мест».

3) устанавливаются остальные «Универсальные диспетчеры» с копированием файлов, указанных в п.2, с эталонного узла;

4) устанавливаются «Шлюзы», настраивается защищенное подключение к «Шлюзу», каталог `/etc/termidesk/` копируется с первого узла «Шлюза» на другие узлы с этим компонентом;

5) устанавливаются «Менеджеры рабочих мест» с копированием файлов, указанных в п.2, с эталонного узла.

Заключительным этапом устанавливаются и настраиваются балансировщики нагрузки на базе ОС Astra Linux Special Edition и nginx.

5.3.2 . Установка и настройка СУБД PostgreSQL

Процесс установки брокера сообщений RabbitMQ не отличается от процесса, описанного в разделе **Подготовка среды функционирования**. Установка и настройка СУБД PostgreSQL осуществляется согласно выбранной версии.

Для завершения настройки нужно:

- отредактировать файл `/etc/rabbitmq/rabbitmq-env.conf`, приведя его к виду:

```
# Defaults to rabbit. This can be useful if you want to run more than one node
# per machine - RABBITMQ_NODENAME should be unique per erlang-node-and-machine
# combination. See the clustering on a single machine guide for details:
# http://www.rabbitmq.com/clustering.html#single-machine
#NODENAME=rabbit

# By default RabbitMQ will bind to all interfaces, on IPv4 and IPv6 if
# available. Set this if you only want to bind to one network interface or#
# address family.
NODE_IP_ADDRESS=0.0.0.0
# Defaults to 5672.
NODE_PORT=5672
```

- сохранить файл и перезапустить службу `rabbitmq-server`:

```
sudo systemctl restart rabbitmq-server
```

5.3.3 . Установка первого узла с «Универсальным диспетчером»

Процесс установки первого узла с «Универсальным диспетчером» аналогичен комплексной установке Termidesk, за исключением выбора только ролей «Портал администратора» и «Портал пользователя».

После установки передать каталог `/etc/opt/termidesk-vdi` на остальные узлы «Универсальных диспетчеров» и «Менеджеров рабочих мест»:

```
sudo scp -r /etc/opt/termidesk-vdi localuser@ipaddr_or_fqdn_host:/home/user/
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Перед началом установки остальных узлов «Универсальных диспетчеров» необходимо переместить скопированный ранее каталог `termidesk-vdi` в каталог `/etc/opt/`:

```
sudo mv /home/user/termidesk-vdi /etc/opt/
```

Установить второй узел с «Универсальным диспетчером» по аналогии с первым, не меняя параметры в диалогах подключения к СУБД и заполнения информации о подключении к RabbitMQ.

5.3.4 . Установка «Шлюзов»

Установка «Шлюзов» выполняется из пакета `termidesk-gateway`.

> ⚠ Для установки «Шлюза» следует обратиться к подразделу **Установка Шлюза** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз».

После завершения установки нужно:

- настроить защищенное подключение к «Шлюзу» согласно подразделу **Настройка защищенного подключения к Шлюзу** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз»;
- привести файл `/etc/termidesk/gateway.yaml` к виду согласно подразделу **Параметры конфигурирования компонента** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз». Задать актуальные значения IP-адресов (или FQDN) параметрам:
  - `url: ${urlCheckToken}` - для обслуживания API-запросов по валидации подключений, запрашиваемых «Универсальным диспетчером» через «Шлюз»;
  - `url: ${coordinatorUrl}` - для подключения к RabbitMQ;
- сохранить файл, а затем перезапустить службу:

```
sudo systemctl restart termidesk-gateway
```

После настройки нужно передать каталог `/etc/termidesk/` с первого узла «Шлюза» на другие узлы с этим компонентом:

```
sudo scp -r /etc/termidesk localuser@ipaddr_or_fqdn_host:/home/user/
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Перед началом установки остальных узлов «Шлюзов» необходимо:

- переместить скопированный ранее каталог `termidesk` в каталог `/etc/`:

```
sudo mv /home/user/termidesk /etc/
```

- назначить права по использованию ключа и сертификата пользователю `termidesk-gateway`:

```
sudo chown termidesk-gateway:termidesk-gateway /etc/termidesk/ssl-cert-snakeoil.*
```

- предоставить права на чтение ключа и сертификата:

```
1 sudo chmod 640 /etc/termidesk/ssl-cert-snakeoil.key
2 sudo chmod 644 /etc/termidesk/ssl-cert-snakeoil.pem
```

- перезапустить службу:

```
sudo systemctl restart termidesk-gateway
```

Установка второго узла «Шлюза» выполняется по аналогии с первым.

5.3.5 . Установка «Менеджеров рабочих мест»

Установка «Менеджеров рабочих мест» производится на два узла, работающих в режиме `network failover`.

Установка компонента на первый узел проводится в следующей последовательности:

- перемещается скопированный ранее каталог `termidesk-vdi` в каталог `/etc/opt/`:

```
sudo mv /home/user/termidesk-vdi /etc/opt/
```

- редактируется файл `/etc/opt/termidesk-vdi/termidesk.conf`, параметру `NODE_ROLES` присваивается значение «CELERYMAN»;
- устанавливается пакет `termidesk-vdi`:

```
sudo apt -y install termidesk-vdi
```

где:

`-y` - ключ для пропуска подтверждения установки.

В результате установки пакета `termidesk-vdi` на узле будут запущены службы `termidesk-celery-beat`, `termidesk-celery-worker`.

Установка второго узла с «Менеджером рабочих мест» выполняется по аналогии с первым.

5.3.6 . Установка балансировщиков

Балансировщики нагрузки необходимы для балансировки клиентских подключений к «Универсальным диспетчерам» и «Шлюзам», равномерного распределения нагрузки на них. Средой функционирования для балансировщиков нагрузки является ОС Astra Linux Special Edition.

Балансировщик nginx устанавливается командой:

```
sudo apt install -y nginx
```

где:

`-y` - ключ для пропуска подтверждения установки.

5.3.7 . Действия после распределенной установки

Настройка балансировщика нагрузки приведена в подразделе **Настройка балансировщика для работы с самоподписанными сертификатами** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

5.4 . Отказоустойчивая установка Termidesk

5.4.1 . Основные принципы отказоустойчивой установки

В Termidesk предусмотрена отказоустойчивая установка для сохранения работоспособности при возникновении нештатных ситуаций.

> ⓘ Описание применимо к ферме Termidesk.

Перечень условий для отказоустойчивой установки:

- брокер сообщений RabbitMQ устанавливается на одном узле с СУБД (в общем случае этот компонент может устанавливаться на отдельный узел, но в рамках настоящей процедуры данный вариант не рассматривается);

> ⚠ При использовании внешней по отношению к Termidesk СУБД, следует установить брокер сообщений RabbitMQ на отдельный узел.

- на всех узлах настроены статические IP-адреса;
- на всех узлах настроена синхронизация времени от единого источника;
- в инфраструктуре организации должна работать служба DNS, которая должна правильно разрешать имена всех узлов фермы Termidesk в IP-адреса.

Упрощенная схема отказоустойчивой установки фермы Termidesk приведена на рисунке (см. Рисунок 14).

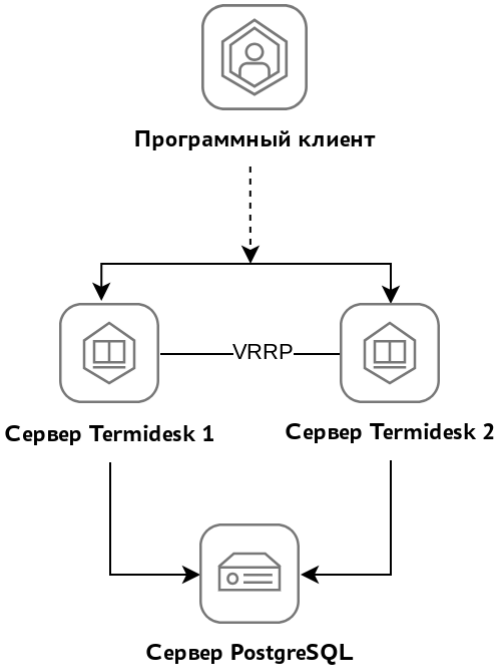

Рисунок 14 – Отказоустойчивая схема установки Termidesk

Перечень обозначенных компонентов приведен в таблице (см. Таблица 4).

> ⚠ Все примеры IP-адресов и FQDN должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре организации. Следует учесть, что в примерах конфигурационных файлов и запросах также используются IP-адреса и FQDN из таблицы, в рабочей конфигурации их следует изменить на актуальные.

Таблица 4 – Перечень компонентов для отказоустойчивой установки

Обозначение на схеме	Установленные на узел компоненты	FQDN узла
Ферма Termidesk		
«Сервер Termidesk 1»	Основной узел (master). Установлен с компонентами: ▪ «Универсальный диспетчер» (служба `termidesk-vdi`) с ролью «Портал универсальный»; ▪ «Менеджер рабочих мест» (службы `termidesk-celery-beat` и `termidesk-celery-worker`); ▪ «Шлюз» (служба `termidesk-gateway`)	`disp1.termidesk.local`
«Сервер Termidesk 2»	Резервный узел (slave). Установлен с компонентами: ▪ «Универсальный диспетчер» (служба `termidesk-vdi`) с ролью «Портал универсальный»; ▪ «Менеджер рабочих мест» (службы `termidesk-celery-beat` и `termidesk-celery-worker`); ▪ «Шлюз» (служба `termidesk-gateway`)	`disp2.termidesk.local`

Обозначение на схеме	Установленные на узел компоненты	FQDN узла
«Сервер СУБД и RabbitMQ 1»	Установлены СУБД PostgreSQL и RabbitMQ (обе службы на одном узле)	`db1.termidesk.local`

Отказоустойчивая установка фермы Termidesk проводится в следующей последовательности:

1) на одном узле устанавливаются СУБД и RabbitMQ. При установке следует учесть, что в БД должны отсутствовать записи (необходимо использовать чистую БД);

> ⚠ При использовании внешней по отношению к Termidesk СУБД, следует установить брокер сообщений RabbitMQ на узел «Менеджера рабочих мест» или на отдельный узел.

2) устанавливается основной узел Termidesk с компонентом «Универсальный диспетчер». При установке необходимо выбрать роль «Портал универсальный». Роль активируется при одновременном выборе ролей «Портал администратора» и «Портал пользователя» в диалоговом окне псевдографического интерфейса инсталлятора. На этот же узел устанавливается «Шлюз» из пакета `termidesk-gateway`;

3) с основного узла Termidesk на резервные копируется каталог `/etc/opt/termidesk-vdi` вместе с его содержимым;

4) устанавливаются резервные узлы Termidesk;

5) проверяется работоспособность узлов Termidesk;

6) выполняется настройка узлов в режиме высокой доступности.

5.4.2 . Установка и настройка СУБД PostgreSQL

Процесс установки СУБД PostgreSQL и брокера сообщений RabbitMQ не отличается от процесса, описанного в разделе **Подготовка среды функционирования**.

Для завершения настройки RabbitMQ нужно:

- отредактировать файл `rabbitmq-env.conf`, приведя его к виду:

```
# Defaults to rabbit. This can be useful if you want to run more than one node
# per machine - RABBITMQ_NODENAME should be unique per erlang-node-and-machine
# combination. See the clustering on a single machine guide for details:
# http://www.rabbitmq.com/clustering.html#single-machine
#NODENAME=rabbit

# By default RabbitMQ will bind to all interfaces, on IPv4 and IPv6 if
# available. Set this if you only want to bind to one network interface or#
# address family.
NODE_IP_ADDRESS=0.0.0.0
# Defaults to 5672.
NODE_PORT=5672
```

- сохранить файл и перезапустить службу `rabbitmq-server`:

```
sudo systemctl restart rabbitmq-server
```

СУБД должна быть настроен так, чтобы она могла принимать подключения с узлов Termidesk, для этого нужно:

- отредактировать файл `/etc/postgresql/15/main/postgresql.conf`: в разделе `CONNECTIONS AND AUTHENTICATION` изменить строку `listen_addresses`, заменив `localhost` на «*». Пример:

```
#------------------------------------------------------------------------------
# CONNECTIONS AND AUTHENTICATION
#------------------------------------------------------------------------------
# - Connection Settings -
listen_addresses = '*' # what IP address(es) to listen on;
 # comma-separated list of addresses;
 # defaults to 'localhost'; use '*' for all
 # (change requires restart)
port = 5432 # (change requires restart)
```

- отредактировать файл `/etc/postgresql/<версия СУБД PostgreSQL>/main/pg_hba.conf`: в разделе `#IPv4 local connections` в столбце `ADDRESS` текущее значение нужно изменить на `all`. Пример:

```
# TYPE DATABASE USER ADDRESS METHOD
# "local" is for Unix domain socket connections only
local all all peer
# IPv4 local connections:
host all all all md5
# IPv6 local connections:
host all all ::1/128 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local replication all peer
host replication all 127.0.0.1/32 md5
host replication all ::1/128 md5
```

- сохранить файлы и перезапустить службу `postgresql`:

```
sudo systemctl restart postgresql
```

5.4.3 . Установка основного узла Termidesk

Процесс установки основного узла Termidesk аналогичен комплексной установке Termidesk: при установке выбираются роли «Портал администратора», «Портал пользователя», «Менеджер рабочих мест». Компонент «Шлюз» устанавливается на этот же узел из пакета `termidesk-gateway`. После установки необходимо скорректировать файл конфигурации веб-сервера `/etc/apache2/apache2.conf`. Для этого нужно найти и раскомментировать строку с параметром `AstraMode`, далее присвоить данному параметру значение `off`, точно соблюдая отступы и пробелы в файле:

```
# Astra security mode
#
```

```
3 AstraMode off
```

После установки компонента «Шлюз» выполнить:

- настроить защищенное подключение к «Шлюзу» согласно подразделу **Настройка защищенного подключения к Шлюзу** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз»;
- привести файл `/etc/termidesk/gateway.yaml` к виду согласно подразделу **Параметры конфигурирования компонента** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз». Задать актуальные значения IP-адресов (или FQDN) параметрам:
  - `url: ${urlCheckToken}` - для обслуживания API-запросов по валидации подключений, запрашиваемых «Универсальным диспетчером» через «Шлюз»;
  - `url: ${coordinatorUrl}` - для подключения к RabbitMQ;
- сохранить файл, а затем перезапустить службу:

```
sudo systemctl restart termidesk-gateway
```

5.4.4 . Перенос каталога с конфигурационными файлами и ключами

⚠ Настройки основного узла Termidesk используются как эталонные для остальных узлов Ternidesk.

После установки основного узла Termidesk нужно передать каталоги `/etc/opt/termidesk-vdi` и `/etc/termidesk/` на остальные узлы Termidesk:

```
sudo scp -r /etc/opt/termidesk-vdi localuser@ipaddr_or_fqdn_host:/home/user/
sudo scp -r /etc/termidesk localuser@ipaddr_or_fqdn_host:/home/user/
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Перед началом установки остальных узлов необходимо выполнить на них:

- переместить скопированные ранее каталоги:

```
sudo mv /home/user/termidesk-vdi /etc/opt/
sudo mv /home/user/termidesk /etc/
```

- назначить права по использованию ключа и сертификата пользователю `termidesk-gateway`:

```
sudo chown termidesk-gateway:termidesk-gateway /etc/termidesk/ssl-cert-snakeoil.*
```

- предоставить права на чтение ключа и сертификата:

```
sudo chmod 640 /etc/termidesk/ssl-cert-snakeoil.key
sudo chmod 644 /etc/termidesk/ssl-cert-snakeoil.pem
```

5.4.5 . Установка резервных узлов Termidesk

Процесс установки резервных узлов Termidesk аналогичен установке основного узла, но в диалоге подключения к СУБД и RabbitMQ информация о подключении не заполняется. Действия после установки также аналогичны действиям, выполняемым на основном узле.

5.4.6 . Проверка работоспособности узлов Termidesk

После установки нужно убедиться, что на основном и резервных узлах Termidesk правильно запущены службы, для этого выполнить на каждом узле:

```
sudo systemctl -a | grep termidesk
```

На основном узле вывод команды должен отображать, что активны и загружены все службы Termidesk, пример вывода:

```
admin@disp1.termidesk.localsudo systemctl -a | grep termidesk
termidesk-celery-beat.service loaded active running Termidesk-VDI Celery Beat
termidesk-celery-worker.service loaded active running Termidesk-VDI Celery Beat
termidesk-vdi.service loaded active running Termidesk-VDI daemon
termidesk-gateway.service loaded active running Termidesk-Gateway daemon
```

На резервных узлах вывод команды должен отображать, что активны и загружены все службы, пример вывода:

```
admin@disp1.termidesk.localsudo systemctl -a | grep termidesk
termidesk-celery-beat.service loaded active running Termidesk-VDI Celery Beat
termidesk-celery-worker.service loaded active running Termidesk-VDI Celery Beat
termidesk-vdi.service loaded active running Termidesk-VDI daemon
termidesk-gateway.service loaded active running Termidesk-Gateway daemon
```

Затем необходимо проверить доступность резервных узлов по протоколу HTTPS, выполнив в веб-браузере переход по адресу: https://disp2.termidesk.local. Убедиться, что отобразилась страница входа в Termidesk.

5.4.7 . Настройка узлов в режиме высокой доступности

⚠ Начиная с Termidesk версии 6.0 служба `termidesk-taskman` исключена из компонента «Менеджер рабочих мест». Конфигурационный файл изменен по сравнению с предыдущими версиями.

Последовательность настройки узлов:

- на узлах `master` и `slave` установить пакеты программ для организации высокой доступности:

```
sudo apt install -y keepalived ipset
```

- на узлах `master` и `slave` создать каталог `/etc/keepalived/` (если каталог ранее не был создан):

```
sudo mkdir -p /etc/keepalived
```

- на узлах `master` и `slave` в каталоге `/etc/keepalived/` создать пустой файл `keepalived.conf` (файл настроек режима высокой доступности):

```
sudo touch /etc/keepalived/keepalived.conf
```

- отредактировать созданный файл `/etc/keepalived/keepalived.conf`, приведя его к следующему виду (по очереди на каждом из узлов):

Значения параметров в файле `keepalived.conf` приведены в качестве примера. Значения должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре организации.
Параметры, явно подлежащие изменению, отмечены комментарием «# НУЖНО УКАЗАТЬ».

```
1  global_defs {
2
3      router_id disp1.termidesk.local # НУЖНО УКАЗАТЬ: hostname хоста
4      script_user user # НУЖНО УКАЗАТЬ: вместо user -> пользователь, от имени
   которого запускается keepalived
5      enable_script_security
6  }
7
8  vrrp_script check_httpd {
9      script "/usr/bin/pgrep apache"
10     interval 1
11     timeout 3
12     rise 1
13     fall 2
14     init_fail
15 }
16
17 # Для каждого виртуального IPv4-адреса создается свой экземпляр vrrp_instance
18 vrrp_instance termidesk-celery {
19
20     state BACKUP
21
22     # НУЖНО УКАЗАТЬ: eth0 -> интерфейс, смотрящий в Интернет
23     interface eth0
24
```

```
25      # НУЖНО УКАЗАТЬ: вместо 2 -> номер экземпляра vrrp_instance
26      virtual_router_id 2
27
28      # НУЖНО УКАЗАТЬ: вместо 128 -> приоритет  экземпляра vrrp_instance
29      priority 128
30
31      preempt_delay 5 # значение в секундах
32      advert_int 1
33
34      # НУЖНО УКАЗАТЬ: вместо 192.0.2.1 -> IPv4-адрес интерфейса, смотрящего в
    Интернет
35      unicast_src_ip 192.0.2.1
36
37      authentication {
38          auth_type PASS
39          # НУЖНО УКАЗАТЬ: ksedimret -> заменить на безопасный пароль
40          auth_pass ksedimret
41      }
42
43      virtual_ipaddress {
44          # В этой секции происходит назначение IP-алиаса
45          # НУЖНО УКАЗАТЬ: вместо 192.0.2.1/24 -> виртуальный IPv4-адрес и сетевой
    префикс с интерфейса, смотрящего в Интернет
46          # НУЖНО УКАЗАТЬ: вместо eth0 -> интерфейс, смотрящий в Интернет
47          # НУЖНО УКАЗАТЬ: вместо eth0:106 -> интерфейс, смотрящий в Интернет:4-й
    октет виртуального IPv4-адреса
48          192.0.2.1/24 dev eth0 label eth0:106
49      }
50
51      track_script {
52          check_httpd
53      }
54  }
55
56  vrrp_instance termidesk-vdi {
57
58      state BACKUP
59
60      # НУЖНО УКАЗАТЬ: eth0 -> интерфейс, смотрящий в Интернет
61      interface eth0
62
63      # НУЖНО УКАЗАТЬ: вместо 107 -> номер экземпляра vrrp_instance
64      virtual_router_id 107
65
66      # НУЖНО УКАЗАТЬ: вместо 128 -> приоритет  экземпляра vrrp_instance
67      priority 128
68
69      preempt_delay 5
70      advert_int 1
71
72      # НУЖНО УКАЗАТЬ: вместо 192.0.2.3 -> IPv4-адрес интерфейса, смотрящего в
    Интернет
73      unicast_src_ip 192.0.2.3
74
75      authentication {
```

```
76          auth_type PASS
77          # НУЖНО УКАЗАТЬ: ksedimret -> заменить на безопасный пароль
78          auth_pass ksedimret
79      }
80
81      virtual_ipaddress {
82          # В этой секции происходит назначение IP-алиаса
83          # НУЖНО УКАЗАТЬ: вместо 192.0.2.1/24 -> виртуальный IPv4-адрес и сетевой
    префикс с интерфейса, смотрящего в Интернет
84          # НУЖНО УКАЗАТЬ: вместо eth0 -> интерфейс, смотрящий в Интернет
85          # НУЖНО УКАЗАТЬ: вместо eth0:107 -> интерфейс, смотрящий в Интернет:4-й
    октет виртуального IPv4-адреса
86          192.0.2.1/24 dev eth0 label eth0:107
87      }
88
89      track_script {
90          check_httpd
91      }
92  }
93
94  vrrp_instance termidesk-gateway {
95
96      state BACKUP
97
98      # НУЖНО УКАЗАТЬ: eth0 -> интерфейс, смотрящий в Интернет
99      interface eth0
100
101     # НУЖНО УКАЗАТЬ: вместо 108 -> номер экземпляра vrrp_instance
102     virtual_router_id 108
103
104     # НУЖНО УКАЗАТЬ: вместо 64 -> приоритет  экземпляра vrrp_instance
105     priority 64
106
107     preempt_delay 5
108     advert_int 1
109
110     # НУЖНО УКАЗАТЬ: вместо 192.0.2.2 -> IPv4-адрес интерфейса, смотрящего в
    Интернет
111     unicast_src_ip 192.0.2.2
112
113     authentication {
114         auth_type PASS
115         # НУЖНО УКАЗАТЬ: ksedimret -> заменить на безопасный пароль
116         auth_pass ksedimret
117     }
118
119     virtual_ipaddress {
120         # В этой секции происходит назначение IP-алиаса
121         # НУЖНО УКАЗАТЬ: вместо 192.0.2.1/24 -> виртуальный IPv4-адрес и сетевой
    префикс с интерфейса, смотрящего в Интернет
122         # НУЖНО УКАЗАТЬ: вместо eth0 -> интерфейс, смотрящий в Интернет
123         # НУЖНО УКАЗАТЬ: вместо eth0:108 -> интерфейс, смотрящий в Интернет:4-й
    октет виртуального IPv4-адреса
124         192.0.2.1/24 dev eth0 label eth0:108
125     }
```

```
    track_script {
        check_httpd
    }
}
```

- на узлах `master` и `slave` добавить в автоматическую загрузку и запустить сервис `keeaplived`

```
sudo systemctl enable keepalived
sudo systemctl start keepalived
```

5.5 . Установка в режиме замкнутой программной среды

Замкнутая программная среда (ЗПС) является средством повышения безопасности ОС путем контроля целостности (неизменности) файлов. Механизм контроля реализован в виде невыгружаемого модуля ядра ОС Astra Linux Special Edition (модуль `digsig_verif`), выполняющего проверку электронной цифровой подписи файлов (ЭЦП).

Перед установкой компонента Termidesk необходимо установить пакет `termidesk-digsig-keys`, выполнив следующее:

- подключить репозиторий Termidesk или получить отдельный пакет `termidesk-digsig-keys` из репозитория;
- выполнить установку с использованием репозитория:

```
sudo apt -y install termidesk-digsig-keys
```

- либо выполнить установку из deb-пакета:

```
sudo apt install -y /home/user/termidesk-digsig-keys-XXXXXX_amd64.deb
```

  где:

  `-y` - ключ для пропуска подтверждения установки;

  `/home/user/termidesk-digsig-keys-XXXXXX_amd64.deb` - расположение пакета `termidesk-digsig-keys-XXXXXX_amd64.deb`.

- перезагрузить ОС:

```
sudo reboot
```

- выполнить установку компонента Termidesk.

Для ЗПС может быть активирован режим проверки встроенной ЭЦП в расширенных атрибутах (`DIGSIG_XATTR_MODE`). В этом случае потребуется подписать файлы, которые будут проходить проверку, имеющимися в организации ключами. Информация о процессе подписи и активации

механизма проверки встроенной ЭЦП в расширенных атрибутах приведена в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634.

5.6 . Постановка Termidesk на контроль целостности

После установки и настройки Termidesk необходимо поставить его на контроль целостности. В подразделе приведена процедура для компонентов «Универсальный диспетчер» и «Менеджер рабочих мест». Постановка на контроль целостности других компонентов приведена в соответствующих им документах.

Для контроля целостности используются встроенные в ОС Astra Linux Special Edition программные средства на основе `Another File Integrity Checker`, представленного пакетом `afick`.

Настройка регламентного контроля целостности выполняется в конфигурационном файле `/etc/afick.conf`.

> Настройку следует производить только после окончательного внедрения Termidesk, поскольку с файлов конфигурации и исполняемых файлов будут сняты эталонные контрольные суммы.

Для постановки на контроль целостности компонента «Универсальный диспетчер» необходимо добавить в конфигурационный файл `/etc/afick.conf` строки:

```
/etc/default/termidesk-vdi PARSEC
/etc/logrotate.d/termidesk.local PARSEC
/etc/opt/termidesk-vdi PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-vdi.service PARSEC
/opt/termidesk PARSEC
/usr/lib/systemd/system/termidesk-celery-beat.service PARSEC
/usr/lib/systemd/system/termidesk-celery-worker.service PARSEC
/usr/lib/systemd/system/termidesk-vdi.service PARSEC
/usr/lib/udev/rules.d/99-termidesk-vdi.rules PARSEC
/usr/share/doc/termidesk-vdi PARSEC
/var/opt/termidesk-vdi PARSEC

#Репозиторий Termidesk
/var/repos/ PARSEC
```

Для постановки на контроль целостности компонента «Менеджер рабочих мест» необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

```
/etc/default/termidesk-vdi PARSEC
/etc/logrotate.d/termidesk.local PARSEC
/etc/opt/termidesk-vdi PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-celery-beat.service PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-celery-worker.service
PARSEC
/opt/termidesk PARSEC
```

```
7  /usr/lib/systemd/system/termidesk-celery-beat.service PARSEC
8  /usr/lib/systemd/system/termidesk-celery-worker.service PARSEC
9  /usr/lib/systemd/system/termidesk-vdi.service PARSEC
10 /usr/lib/udev/rules.d/99-termidesk-vdi.rules PARSEC
11 /usr/share/doc/termidesk-vdi PARSEC
12 /var/opt/termidesk-vdi PARSEC
13
14 #Репозиторий Termidesk
15 /var/repos/ PARSEC
```

Для снятия эталонных значений контрольных сумм используется команда:

```
afick -i
```

Для проверки соответствия контрольных сумм эталонным значениям автоматически создаются задания в системном планировщике заданий `cron`.

Для ручной проверки соответствия контрольных сумм используется команда:

```
afick -k
```

> ⚠ В случае отсутствия по какой-либо причине исполняемых фалов `*.pyc`, они будут повторно сгенерированы при перезапуске сервера Python. В этом случае нужно повторно проинициализировать средство регламентного контроля целостности `afick`.

5.7 . Проверка работоспособности после установки

Termidesk является работоспособным, если в результате перехода в веб-браузере по адресу https://localhost/ или https://127.0.0.1/ отобразилась страница входа (см. Рисунок 15) в Termidesk. Если страница сразу не отобразилась, следует подождать 10-15 секунд и обновить ее.

Указанные адреса используются в случае локальной установки. Если Termidesk установлен на сервере, отличном от узла, на котором происходит проверка, необходимо вместо localhost или 127.0.0.1 использовать IP-адрес сервера Termidesk.

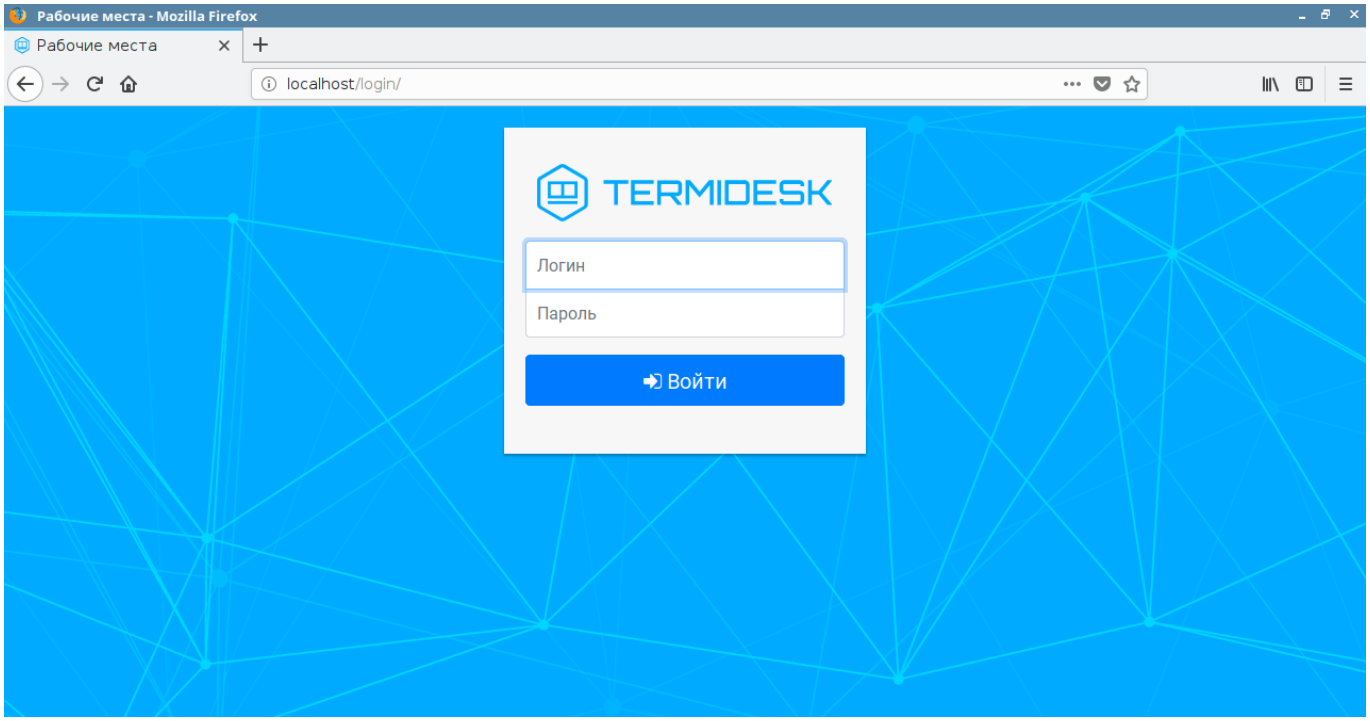

Рисунок 15 – Начальная веб-страница Termidesk

По умолчанию после установки вход в интерфейс управления Termidesk доступен только авторизованному пользователю ОС с ролью «Администратор». Пользователь ОС должен быть членом группы `astra-admin (1001)`. Для входа в интерфейс управления в полях «Логин» и «Пароль» необходимо указать идентификатор пользователя ОС и его пароль соответственно, а затем нажать экранную кнопку **[Войти]**.

Проверка добавления ключа от репозитория производителя в ОС выполняется командой:

```
apt-key list
```

Проверка состояния компонентов выполняется командой:

```
systemctl status termidesk-vdi.service
```

Строка «`Active`» отображает состояние сервиса, где статус «`active (running)`» свидетельствует об успешном запуске Termidesk.

6 . ОБНОВЛЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА

6.1 . Комплексное обновление Termidesk

Описание применимо к ферме Termidesk.

Комплексное обновление подразумевает, что компоненты «Универсальный диспетчер», «Шлюз», «Менеджер рабочих мест» были установлены на одном узле, и ранее при установке были выбраны роли:

- «Портал администратора»;
- «Портал пользователя» (опционально);
- «Менеджер рабочих мест».

Перед обновлением **требуется** удалить:

- фонды и шаблоны, созданные ранее для поставщика ресурсов «Static IP Machines»;
- шаблоны РМ «Статичная ВМ» (для всех поставщиков ресурсов, ранее имевших эти шаблоны) и ассоциированные с ними фонды;
- шаблоны, созданные ранее для поставщика ресурсов VMmanager. Если шаблоны не были удалены перед обновлением, то после него необходимо отредактировать существующие шаблоны и корректно задать значения новых параметров.

Обновление Termidesk должно осуществляться с соблюдением условий:

- обновление выполняется последовательно, с установкой промежуточных версий релизов. Например, если сейчас установлена версия 4.3, то порядок обновления до 6.0 будет следующим: 4.3 - 4.3.1 - 4.3.2 - 5.0 - 5.1 - 5.1.1 - 6.0;
- обновление выполняется операцией установки поверх предыдущей версии. В противном случае, если ранее Termidesk был удален без удаления БД, при повторной установке может возникнуть ряд ошибок;
- после начала процедуры обновления запрещается производить операции удаления объектов на «Порталах» с предыдущими версиями Termidesk.

Если после удаления Termidesk (удаление БД при этом не производилось) возникла необходимость повторной установки программного комплекса, то после инсталляции может понадобиться снова ввести данные для доступа (пароль, токен доступа) в поставщике ресурсов.
Если в файлы запуска Termidesk вручную были внесены какие-либо изменения, то эти изменения при обновлении не сохраняются.

Перед любым обновлением Termidesk рекомендуется выполнить резервное копирование БД:

- остановить службы Termidesk:

```
sudo systemctl stop termidesk-vdi termidesk-gateway termidesk-taskman termidesk-celery-beat termidesk-celery-worker
```

- выполнить резервное копирование БД:

```
pg_dump -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W > <имя_файла_для_сохранения_БД.sql>
```

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`;

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

Для комплексного обновления Termidesk нужно:

- убедиться, что службы Termidesk были ранее остановлены;
- удалить кеш файла ответов `debconf` командами:

```
sudo rm -f /var/cache/debconf/config.dat
sudo rm -f /var/cache/debconf/config.dat-old
```

где:

`-f` - ключ игнорирования несуществующих файлов;

- подключить репозиторий Termidesk (см. подраздел **Получение пакетов установки**);
- выполнить обновление:

```
sudo apt install -y termidesk-vdi
```

где:

`-y` - ключ для пропуска подтверждения установки.

- в диалогах ввода параметров подключения к СУБД и RabbitMQ нажать экранную кнопку **[OK]**;
- в диалоге выбора ролей Termidesk нажать экранную кнопку **[OK]**;

⚠ Диалоги настройки параметров отображаются в том случае, если ранее они не были заданы.
Служба `termidesk-taskman` исключена из Termidesk. При обновлении она будет автоматически отключена, если была ранее активирована. «Менеджер рабочих мест» теперь состоит только из служб `termidesk-celery-beat` и `termidesk-celery-worker`.

- выполнить обновление компонента «Шлюз»:

```
sudo apt install -y termidesk-gateway
```

Если нужно выполнить обновление без подключения репозитория (при наличии `deb`-пакета) следует выполнить:

```
sudo apt install -y <путь к deb-пакету>
```

В случае, если при обновлении появляется сообщение о неразрешенных зависимостях, следует выполнить:

```
sudo apt install -f
```

где:

`-f` - ключ, указывающий, что нужно исправить зависимости пакетов.

После завершения обновления нужно:

- проверить состояние служб Termidesk:

```
sudo systemctl -a | grep termidesk
```

где:

`-a` - ключ для вывода списка служб;

`grep` - утилита для поиска текста в выводе предыдущей команды.

- проверить доступность веб-интерфейса Termidesk (см. подраздел **Проверка работоспособности после установки**).

6.2 . Обновление для распределенной конфигурации установки

6.2.1 . Общая концепция обновления

Описание применимо к ферме Termidesk, установленной в распределенной конфигурации. Общая последовательность действий приведена на рисунке (см. Рисунок 16). Если в инфраструктуре Termidesk используется портал «Агрегатор», то процесс обновления нужно начинать с него (см документ СЛЕТ.10001-01 90 08 «Руководство администратора. Установка и настройка портала «Агрегатор»).

Перед обновлением **требуется** удалить:

- фонды и шаблоны, созданные ранее для поставщика ресурсов «Static IP Machines»;
- шаблоны РМ «Статичная ВМ» (для всех поставщиков ресурсов, ранее имевших эти шаблоны) и ассоциированные с ними фонды;
- шаблоны, созданные ранее для поставщика ресурсов VMmanager. Если шаблоны не были удалены перед обновлением, то после него необходимо отредактировать существующие шаблоны и корректно задать значения новых параметров.

Во время обновления распределенной или отказоустойчивой конфигурации установки:

- изменение политик нужно проводить после обновления всех узлов Termidesk;
- изменение системных параметров нужно проводить после обновления всех узлов Termidesk.

Обновление Termidesk должно осуществляться с соблюдением условий:

- обновление выполняется последовательно, с установкой промежуточных версий релизов. Например, если сейчас установлена версия 5.0, то порядок обновления до 6.0 будет следующим: 5.0 - 5.1 - 5.1.1 - 6.0;
- обновление выполняется операцией установки поверх предыдущей версии. В противном случае, если ранее Termidesk был удален без удаления БД, при повторной установке может возникнуть ряд ошибок;
- после начала процедуры обновления запрещается производить любые операции с объектами на «Порталах» с предыдущими версиями Termidesk.

Во время обновления возможна временная неработоспособность функции автоматического входа пользователя в гостевую ОС ВМ, пока не будет обновлен последний узел с «Универсальным диспетчером».

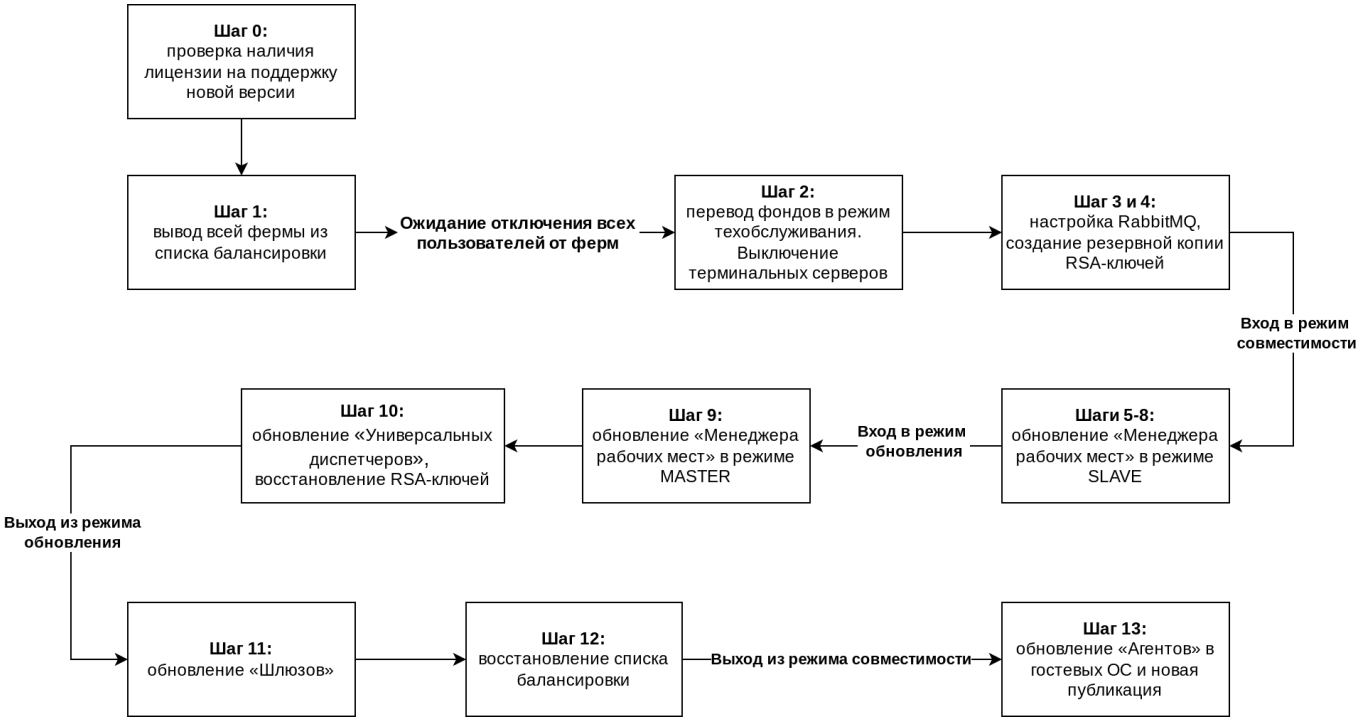

Рисунок 16 – Последовательность обновления распределенной конфигурации фермы Termidesk

На схеме:

- режим совместимости - режим, характеризующийся отличием в версиях между любыми компонентами фермы Termidesk;
- режим обновления - режим, характеризующийся наличием не обновленных «Универсальных диспетчеров» при уже обновленных записях БД. Становится ограничен в действиях «Портал администратора». Ферма Termidesk при этом должна работать с теми записями БД, которые есть на момент входа в этот режим.

Если планируется добавить новый узел с «Универсальным диспетчером», то любой новый узел будет иметь свой IP-адрес (или FQDN). В этом случае все компоненты «Агента» должны получить новый адрес для регистрации в Termidesk.

⚠ Если в файлы конфигурации и запуска Termidesk (`/lib/systemd/system/termidesk-*`) вручную были внесены какие-либо изменения, то необходимо выполнить резервное копирование данных файлов, поскольку эти изменения при обновлении сбрасываются до значений по умолчанию.
В случае с переходом на ОС Astra Linux Special Edition 1.8 потребуется переустановка ОС и Termidesk.
Тогда для сохранения существующей БД нужно:

- выполнить экспорт БД из Termidesk предыдущей версии;
- выполнить резервное копирование файлов конфигурации и запуска Termidesk (`/lib/systemd/system/termidesk-*`, `/etc/opt/termidesk-vdi/*`);

- выполнить установку ОС Astra Linux Special Edition 1.8;
- выполнить установку и настройку RabbitMQ согласно подразделам **Установка брокера сообщений RabbitMQ** и **Настройка брокера сообщений RabbitMQ**;
- выполнить установку и настройку СУБД согласно подразделам **Установка СУБД PosrgreSQL** и **Настройка СУБД PosrgreSQL**;
- выполнить импорт ранее сохраненной БД;
- выполнить установку Termidesk согласно подразделу **Распределенная установка программного комплекса**.

Последовательность обновления фермы Termidesk, установленной в распределенной отказоустойчивой конфигурации:

Обновление выполняется с приостановкой обслуживания пользователей!

Шаг 0. Проверить наличие лицензии на поддержку новой версии Termidesk.

Шаг 1. На всех балансировщиках нагрузки, отвечающих за распределение подключений к «Шлюзам» и «Универсальным диспетчерам», из списка балансировки выводятся все компоненты: «Шлюзы» и «Универсальные диспетчеры».

Шаг 2. Все пользователи должны отключиться от фондов РМ. Нужно дождаться завершения работы пользователей. Затем:

- через веб-интерфейс «Портал администратора» перевести все фонды РМ в режим техобслуживания;
- выключить все терминальные серверы, которые были подключены в Termidesk как поставщики ресурсов.

Шаг 3. На сервер с СУБД, либо на отдельно выделенный сервер, устанавливается и настраивается компонент RabbitMQ в случае, если ранее RabbitMQ не был установлен.

Шаг 4. Создается резервная копия RSA-ключей, расположенных в каталоге `/etc/opt/termidesk-vdi/wsproxy/`.

Шаг 5. На узлах с установленным «Менеджером рабочих мест», который работает в отказоустойчивой конфигурации в режиме «SLAVE», должен быть выполнен останов служб `keepalived`.

Служба `termidesk-taskman` исключена из Termidesk. При обновлении она будет автоматически отключена, если была ранее активирована. «Менеджер рабочих мест» теперь состоит только из служб `termidesk-celery-beat` и `termidesk-celery-worker`.

Шаг 6. Обновляется выбранный «Менеджер рабочих мест». Запуск служб выполняется автоматически.

Шаг 7. На обновленном «Менеджере рабочих мест» восстанавливаются RSA-ключи из резервной копии, созданной на **Шаге 4**. В этом процессе автоматически будут обновлены записи в БД.

Шаг 8. Выполняется отключение служб `keepalived`. Узел перезагружается.

Шаг 9. На узлах с установленным «Менеджером рабочих мест», который работает в отказоустойчивой конфигурации в режиме «MASTER», должен быть выполнен останов служб `keepalived`. Выполняются **Шаги 5-8** для «Менеджера рабочих мест» режима «SLAVE».

Шаг 10. Последовательно (по одному за раз) обновляются все «Универсальные диспетчеры» («Портал администратора», «Портал пользователя», «Портал универсальный»). Запуск служб выполняется автоматически. На обновленных «Универсальных диспетчерах» восстанавливаются RSA-ключи из резервных копий, созданных на **Шаге 4**. Узлы перезагружается.

Шаг 11. Обновляются все «Шлюзы». Запуск службы `termidesk-gateway` выполняется автоматически.

Шаг 12. По завершении обновления **ВСЕХ** узлов список балансировки восстанавливается до исходного. Проверяется доступность графического интерфейса Termidesk сначала обращением на IP-адрес каждого из «Универсальных диспетчеров», затем обращением на IP-адрес балансировщика нагрузки.

Шаг 13. После выполнения обновления узлов:

- обновить компоненты в гостевых ОС РМ (в базовом ВРМ - «золотом образе» или в ОС терминального сервера) в соответствии с документацией на них:
  - «Агент виртуального рабочего места»;
  - «Агент виртуальных смарт-карт»;
  - «Видеоагент»;
  - «Сессионный агент»;
  - STAL (если используется);
  - TERA (если используется);
- выполнить новую публикацию в фондах РМ, если публикация применима к ним (для фондов с терминальными серверами публикация не выполняется).

6.2.2 . Шаг 1. Редактирование конфигурации балансировщика нагрузки

На балансировщике нагрузки открыть и отредактировать файл `/etc/nginx/sites-available/sampledomain.ru.conf`.

В данном конфигурационном файле следует найти директиву `daas-upstream-ws` и `daas-upstream-nodes` с перечислением списка «Шлюзов» и «Универсальных диспетчеров», закомментировать все узлы и сохранить файл.

Пример для списка балансировки:

⚠ Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре организации.

```
upstream daas-upstream-ws {
 least_conn;
     server 192.0.2.30;
     server 192.0.2.31;
     server 192.0.2.32;
 }

upstream daas-upstream-nodes {
 least_conn;
     server 192.0.2.33;
     server 192.0.2.34;
     server 192.0.2.35;
 }
```

Для исключения всех узлов файл приводится к виду:

```
upstream daas-upstream-ws {
 least_conn;
     # server 192.0.2.30;
     # server 192.0.2.31;
     # server 192.0.2.32;
 }

upstream daas-upstream-nodes {
 least_conn;
     # server 192.0.2.33;
     # server 192.0.2.34;
     # server 192.0.2.35;
 }
```

После изменения файла перезапустить веб-сервер:

```
sudo systemctl restart nginx
```

6.2.3 . Шаг 2. Перевод фондов РМ в режим техобслуживания

Для продолжения обновления нужно дождаться отключения пользователей от фондов РМ.

Затем:

- через веб-интерфейс «Портал администратора» перевести **все** фонды РМ в режим техобслуживания. Для этого перейти «Компоненты - Фонды» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить». Подтвердить включение режима;

- выключить каждый узел терминального сервера, который подключен к Termidesk как поставщик ресурсов.

6.2.4 . Шаг 3. Установка и настройка RabbitMQ

При отсутствии ранее установленного RabbitMQ выполняется его установка в соответствии с подразделами **Установка брокера сообщений RabbitMQ** и **Настройка брокера сообщений RabbitMQ**.

6.2.5 . Шаг 4. Резервное копирование RSA-ключей

Выполнить резервное копирование RSA-ключей с одного из узлов «Универсального диспетчера». Резервные копии ключей можно скопировать, например, на другой сетевой узел командой:

```
sudo scp -r /etc/opt/termidesk-vdi/wsproxy localuser@ipaddr_or_fqdn_host:/home/localuser/
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

6.2.6 . Шаг 5. Останов служб на «Менеджере рабочих мест»

На узлах с установленным «Менеджером рабочих мест», работающем в отказоустойчивой конфигурации в режиме «SLAVE», выполняется останов службы `keepalived` командой:

```
sudo systemctl stop keepalived
```

6.2.7 . Шаг 6. Обновление «Менеджеров рабочих мест»

Перед запуском процедуры обновления нужно:

- отредактировать файл `/etc/opt/termidesk-vdi/termidesk.conf` и задать значение для параметра `METRICS_ACCESS_KEY`, если оно не задано;

> ⚠ При редактировании файла `/etc/opt/termidesk-vdi/termidesk.conf` рекомендуется использовать одинаковое значение параметра `METRICS_ACCESS_KEY` для всех «Менеджеров рабочих мест».

- остановить службы Termidesk:

```
sudo systemctl stop termidesk-taskman termidesk-celery-beat termidesk-celery-worker
```

- удалить кеш файла ответов `debconf` командами:

```
sudo rm -f /var/cache/debconf/config.dat
sudo rm -f /var/cache/debconf/config.dat-old
```

Для обновления «Менеджера рабочих мест»:

- обновить список пакетов и выполнить запуск файла установщика:

```
sudo apt update
sudo apt install termidesk-vdi
```

- в диалоговом окне псевдографического интерфейса инсталлятора выбирается роль «Менеджер рабочих мест».

6.2.8 . Шаг 7. Восстановление RSA-ключей на «Менеджере рабочих мест»

Выполнить копирование сохраненных на Шаге 4 (see page 71) RSA-ключей на узел с обновленным «Менеджером рабочих мест».

6.2.9 . Шаг 8. Отключение службы keepalived

Выполнить отключение службы `keepalived`:

```
sudo systemctl disable keepalived
```

Затем перезагрузить узел:

```
sudo reboot
```

6.2.10 . Шаги 9. Обновление резервного «Менеджера рабочих мест»

Обновление осуществляется аналогично **Шагам 5-8**.

6.2.11 . Шаг 10. Обновление «Универсальных диспетчеров»

Перед запуском процедуры обновления нужно:

- отредактировать файл `/etc/opt/termidesk-vdi/termidesk.conf` и задать значение для параметра `METRICS_ACCESS_KEY`, если оно не задано;

> ⚠ Корректировка файла `/etc/apache2/apache2.conf` при обновлении не производится.
> При редактировании файла `/etc/opt/termidesk-vdi/termidesk.conf` рекомендуется задать одинаковое значение параметра `METRICS_ACCESS_KEY` для всех узлов «Универсального диспетчера».

- остановить службу Termidesk:

```
sudo systemctl stop termidesk-vdi
```

- удалить кеш файла ответов `debconf` командами:

```
sudo rm -f /var/cache/debconf/config.dat
sudo rm -f /var/cache/debconf/config.dat-old
```

где:

`-f` - ключ игнорирования несуществующих файлов.

Для обновления «Универсального диспетчера»:

- обновить список пакетов и выполнить запуск файла установщика:

```
sudo apt update
sudo apt install termidesk-vdi
```

- в диалоговом окне псевдографического интерфейса инсталлятора выбирается роль «Портал администратора» и/или «Портал пользователя» в зависимости от ранее установленной роли.

Выполнить копирование сохраненных на Шаге 4 (see page 71) RSA-ключей на узлы с обновленными «Универсальными диспетчерами».

Затем перезагрузить узлы:

```
sudo reboot
```

После загрузки узла проверить состояние служб:

```
sudo systemctl -a | grep termidesk
```

где:

`-a` - ключ для вывода списка служб;

`grep` - утилита для поиска текста в выводе предыдущей команды.

Проверить доступность веб-порталов Termidesk через веб-браузер.

6.2.12 . Шаги 11. Обновление «Шлюзов»

Процедура обновления проводится с помощью установки новой версии «Шлюза» Termidesk поверх уже имеющейся. Установка «Шлюзов» выполняется из пакета `termidesk-gateway`.

> ⚠ Для установки «Шлюза» следует обратиться к подразделу **Установка Шлюза** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз».

После завершения установки первого «Шлюза» нужно изменить настройки запуска `termidesk-gateway`:

- привести файл `/etc/termidesk/gateway.yaml` к виду согласно подразделу **Параметры конфигурирования компонента** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз». Задать актуальные значения IP-адресов (или FQDN) параметрам:

- `url: ${urlCheckToken}` - для обслуживания API-запросов по состоянию «Шлюза»;
- `url: ${coordinatorUrl}` - для подключения к RabbitMQ;

- сохранить файл, а затем перезапустить службу:

```
sudo systemctl restart termidesk-gateway
```

После настройки нужно передать каталог `/etc/termidesk/` с первого узла «Шлюза» на другие узлы с этим компонентом:

```
sudo scp -r /etc/termidesk localuser@ipaddr_or_fqdn_host:/home/user/
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Перед началом установки остальных узлов «Шлюзов» необходимо:

- переместить скопированный ранее каталог `termidesk` в каталог `/etc/`:

```
sudo mv /home/user/termidesk /etc/
```

- назначить права по использованию ключа и сертификата пользователю `termidesk-gateway`:

```
sudo chown termidesk-gateway:termidesk-gateway /etc/termidesk/ssl-cert-snakeoil.*
```

- предоставить права на чтение ключа и сертификата:

```
1 sudo chmod 640 /etc/termidesk/ssl-cert-snakeoil.key
2 sudo chmod 644 /etc/termidesk/ssl-cert-snakeoil.pem
```

- перезапустить службу:

```
sudo systemctl restart termidesk-gateway
```

Настройка после установки остальных узлов «Шлюза» выполняется по аналогии с первым.

6.2.13 . Шаг 12. Восстановление конфигурации балансировщика нагрузки

По завершении обновления **ВСЕХ** узлов фермы Termidesk список балансировки на **ВСЕХ** балансировщиках восстанавливается до исходного.

Ранее закомментированные строки нужно раскомментировать, затем выполнить перезагрузку службы `nginx` на каждом балансировщике:

```
sudo systemctl restart nginx
```

Выполнить проверку доступности веб-портала Termidesk через веб-браузер сначала обращением на IP-адрес каждого из «Универсальных диспетчеров» (или «Шлюзов»), затем обращением на IP-адрес балансировщика нагрузки.

6.2.14 . Шаг 13. Обновление компонентов в ОС РМ и новая публикация

После выполнения обновления **ВСЕХ** узлов:

- обновляются компоненты в ОС РМ (в базовом ВРМ - «золотом образе» или в ОС терминального сервера) в соответствии с документацией на них:
  - «Агент виртуального рабочего места»;
  - «Агент виртуальных смарт-карт»;
  - «Видеоагент»;
  - «Сессионный агент»;
  - STAL (если используется);
  - TERA (если используется);
- выполняется новая публикация в фондах РМ, если публикация применима к ним.

> ⚠ Для фондов с терминальными серверами публикация не выполняется: достаточно того, чтобы узел с терминальным сервером был включен.

7 . УДАЛЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА

Для удаления нужно:

- выполнить:

```
sudo aptitude purge -y termidesk-vdi
```

где:

`-y` - ключ для пропуска подтверждения удаления;

- очистить оставшиеся зависимости и конфигурации:

```
sudo aptitude purge ~c -y
```

Команда полностью удалит оставшиеся настройки и зависимости уже удаленных пакетов.

Для удаления БД и роли пользователя следует выполнить следующие действия, строго соблюдая их последовательность:

- переключиться на пользователя `postgres` (через пользователя `root`):

```
sudo su postgres
```

- запустить терминальный клиент СУБД:

```
psql
```

- используя интерактивный интерфейс терминального клиента СУБД, удалить БД:

```
postgres=# DROP DATABASE termidesk;
```

- удалить роль пользователя БД:

```
postgres=# DROP ROLE termidesk;
```

- выйти из интерактивного интерфейса терминального клиента СУБД:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

- удалить оставшийся каталог с файлами, содержащими переменные для подключения к БД, сертификат и ключ:

```
sudo rm -R /etc/opt/termidesk-vdi
```

где:

`-R` - ключ для рекурсивного действия. Будут удалены все вложенные подкаталоги.

8 . ЛИЦЕНЗИРОВАНИЕ

8.1 . 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 соглашение 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 17).

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

Для получения системных UUID узлов, установленных как в комплексном, так и в распределенном варианте, следует:

- открыть «Портал администратора» Termidesk;
- 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
```

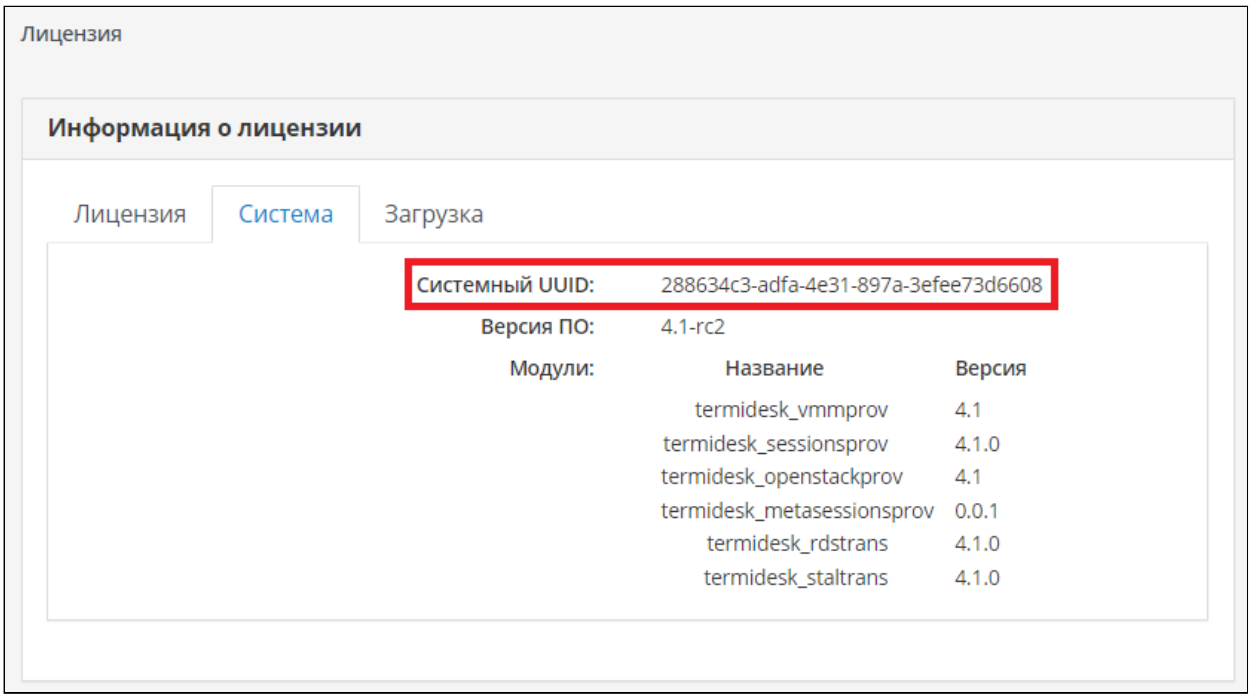

Рисунок 17 – Расположение информации о системном UUID

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».

8.2 . 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 18), а затем нажать экранную кнопку **[Загрузить]**.

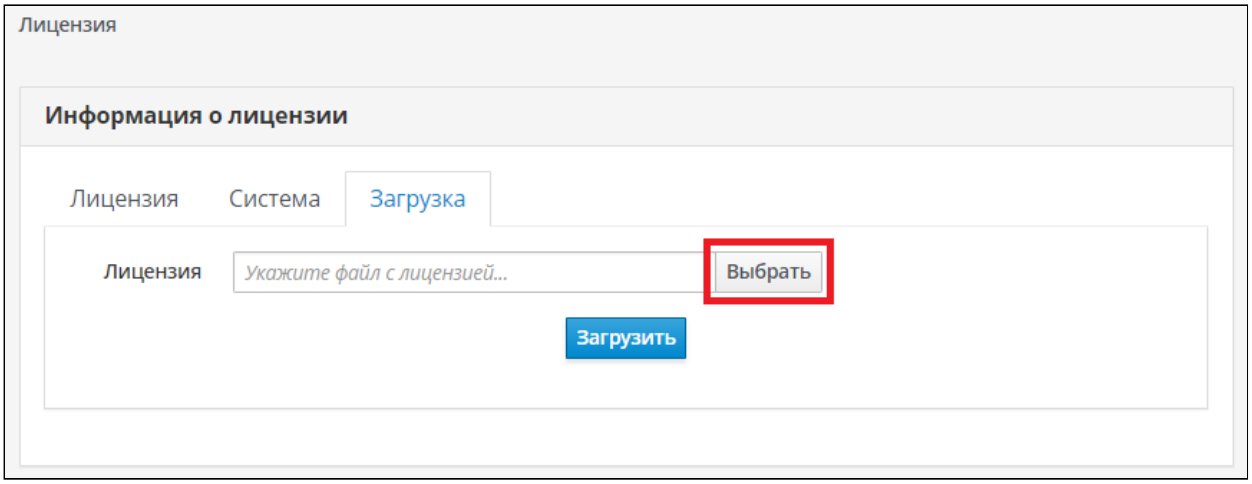

Рисунок 18 – Окно добавления файла с лицензией

8.3 . 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.

9 . ПЕРЕЧЕНЬ ТЕРМИНОВ

Термин	Определение
Компонент «Агент»	Собирательное название для следующих компонентов Termidesk: ▪ «Агент виртуального рабочего места»; ▪ «Агент узла виртуализации»; ▪ «Сессионный агент»; ▪ «Видеоагент»; ▪ «Агент виртуальных смарт-карт». Самостоятельный компонент, отвечающий за контролируемую доставку РМ, взаимодействие с «Универсальным диспетчером» и «Менеджером рабочих мест»
Компонент «Агент виртуальных смарт-карт»	Компонент Termidesk. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление подключенных к пользовательской рабочей станции смарт-карт в ВРМ
Компонент «Агент виртуального рабочего места»	Компонент Termidesk. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет взаимодействие с «Универсальным диспетчером», конфигурирует ВРМ, фиксирует действия пользователя, реализует передачу управляющих сообщений
Компонент «Агент узла виртуализации»	Компонент Termidesk. Устанавливается на узел виртуализации, взаимодействует с гипервизором через модуль `libvirt`
Базовое виртуальное рабочее место	Также: золотой образ, базовый образ. Подразумевает собой образ диска ВМ с предустановленным прикладным ПО и установленным «Агентом виртуального рабочего места». Этот образ далее будет использоваться для создания ВРМ для пользователей
Балансировщик нагрузки	Самостоятельный компонент, отвечающий за распределение нагрузки на множество «Универсальных диспетчеров» и «Шлюзов»
Компонент «Видеоагент»	Компонент Termidesk. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление видеокамеры с пользовательской рабочей станции в ВРМ
Виртуальное рабочее место	Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО. Подключение к ВРМ происходит через протоколы удаленного доступа
Рабочее место	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 терминальном сервере приложениям
Гостевая ОС	ОС, функционирующая на ВМ
Домен аутентификации	Способ проверки субъектов и их полномочий
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 служб после установки: `termidesk-celery-beat.service` и `termidesk-celery-worker.service`
Компонент «Оркестратор»	Компонент Termidesk. Самостоятельный компонент, отвечающий за согласованную работу всех компонентов программного комплекса при децентрализованном развертывании, для нужд отказоустойчивости и комплексирования с облачными службами
Поставщик ресурсов	ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ

Термин	Определение
Протокол доставки	Поддерживаемый в Termidesk протокол удаленного доступа к РМ
Связанный клон	Способ организации ВРМ на основе единого образа с возможностью экономии дискового пространства за счет технологии «копирование при записи» и ускорения операций возврата к базовому состоянию, установки дополнительного ПО и обновлений
Компонент «Сессионный агент»	Компонент Termidesk. Устанавливается на терминальный сервер (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям
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`
Фонд рабочих мест	Совокупность подготовленных РМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей
Шаблон рабочего места	Параметры конфигурации РМ для использования в фонде РМ
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`
Компонент «Сервер терминалов Astra Linux»	Компонент Termidesk. Также: STAL. Обеспечивает подключение пользовательских рабочих станций к РМ с ОС Astra Linux Special Edition через сеанс удаленного терминала
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 - и «Портала администратора», и «Портала пользователя». При этом активируется доступ ко всем модулям документации по командам REST API, предоставляемым интерфейсом `swagger`
Ключ	Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом
Сертификат	Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу
Комплексная установка	Установка основных компонентов Termidesk на одном узле
Распределенная установка	Установка основных компонентов Termidesk на разных узлах

10 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
БД	База данных
ВМ	Виртуальная машина
ВРМ	Виртуальное рабочее место
ЗПС	Замкнутая программная среда
КД	Контроллер домена
ОС	Операционная система
ПК СВ Брест	Программный комплекс «Средства виртуализации «Брест»
ПО	Программное обеспечение
РМ	Рабочее место
СУБД	Система управления базами данных
ЭЦП	Электронная цифровая подпись
API	Application Programming Interface (программный интерфейс приложения)
DHCP	Dynamic Host Configuration Protocol (протокол назначения сетевого адреса)
DNS	Domain Name System (система доменных имен)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
HTML	Hypertext Markup Language (язык гипертекстовой разметки)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
ID	Identification Data (идентификатор)
IP	Internet Protocol (межсетевой протокол)
KVM	Kernel Virtual Machine (виртуальная машина на основе ядра, технология аппаратной виртуализации)
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов)
MAC	Media Access Control (уникальный идентификатор сетевого устройства)
MS AD	Microsoft Acive Directory (служба каталогов Microsoft)
mTLS	Multiplexed Transport Layer Security (протокол, основанный на TLS с усиленной безопасностью)
NTP	Network Time Proetwork Time Protocol (протокол сетевого времени)
OU	Organizational Unit (организационная единица)
QEMU	Quick Emulator (средства эмуляции аппаратного обеспечения)
RADIUS	Remote Authentication Dial-In User Service (протокол, предоставляющий функции аутентификации, авторизации и учета)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)
REDIS	REmote DIctionary Service (резидентная СУБД)

Сокращение	Пояснение
RDS	Remote Desktop Services (службы удаленного рабочего стола Microsoft)
RDSH	Remote Desktop Session Host (хост сеансов удаленных рабочих столов)
RFC	Request for Comments (рабочее предложение Интернет)
RSA	Rivest, Shamir and Adleman (криптографический алгоритм с открытым ключом)
SPICE	Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)
SSL	Secure Sockets Layer (криптографический протокол)
STAL	Terminal Server Astra Linux (сервер терминалов Astra Linux)
TCP	Transmission Control Protocol (протокол управления передачей)
TLS	Transport Layer Security (протокол защиты транспортного уровня)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
UUID	Unique User Identifier (уникальный идентификатор пользователя)
vGPU	Virtual Graphics Processing Unit (виртуальный графический процессор)
VNC	Virtual Network Computing (система удаленного доступа к рабочему столу компьютера)
VRRP	Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности)

UVEON
Unified Virtualization
Experience, Opportunities, Now

© 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