Центр

Управления

Гетерогенными

Инфраструктурами

Руководство по установке Clearway CA 26.2.0 с помощью инсталлятора

ООО «Клируэй Текнолоджис»

2026

Оглавление

1 Введение

Настоящий документ — пошаговое руководство по установке Clearway CA с помощью графического инсталлятора. Инсталлятор — самодостаточное веб-приложение (backend на ASP.NET Core, интерфейс на Angular), которое запускается на рабочем месте оператора и разворачивает компоненты Clearway CA на целевые серверы под управлением ОС Linux по протоколу SSH. Сам инсталлятор на целевые серверы не устанавливается — он оркеструет установку.

> **Важно**
>
> Компоненты Clearway CA устанавливаются только на серверы под управлением ОС Linux. Установка на другие операционные системы, в том числе Windows, не поддерживается и невозможна.

Инсталлятор запускается локально; веб-интерфейс мастера открывается в браузере по адресу вида https://localhost:5224/installer. Версии инсталлятора и дистрибутива отображаются в правом нижнем углу окна мастера (в приведённых примерах — дистрибутив 26.1.0)

Для установки потребуются:

- целевые серверы под управлением поддерживаемой ОС Linux (см. требования к программному и аппаратному обеспечению) с сетевым доступом с рабочего места оператора;
- доступ по SSH к каждому целевому серверу (учётная запись с правами sudo — по паролю или по SSH-ключу);
- сетевая доступность сервера СУБД PostgreSQL (для компонентов, использующих базу данных);
- заранее согласованные параметры развёртывания: имена серверов (FQDN), технологическая учётная запись-владелец (по умолчанию itc-svc), каталог установки (по умолчанию */opt/itc*), параметры подключения к каталогу LDAP/Active Directory (для сервиса аутентификации).

Лицензионное соглашение (EULA):

Если условия EULA ещё не приняты, при открытии веб-интерфейса инсталлятор автоматически показывает Лицензионное соглашение с конечным пользователем на использование программного комплекса «Clearway CA». До принятия соглашения выбор и установка компонентов недоступны.

Ознакомьтесь с текстом соглашения, установите флажок «Я принимаю условия лицензионного соглашения» и нажмите «Принимаю». Кнопка «Принимаю» доступна только при установленном флажке. При нажатии «Отклонить» работа с мастером не начинается, а соглашение отображается повторно.

В режиме CLI текст EULA выводится постранично: нажмите Enter, чтобы перейти к следующей странице, или Q, чтобы перейти к запросу о принятии соглашения. Для продолжения установки подтвердите принятие EULA; при отказе инсталлятор завершает работу.

Совместимость с дистрибутивами Linux:

Инсталлятор проверен со следующими дистрибутивами Linux:

ОС	Версия	Совместимость
Astra Linux	1.7.5.9	Подтверждена

ОС	Версия	Совместимость
Astra Linux	1.8.1.6	Подтверждена
Ubuntu Server	24.04.03	Подтверждена
ОС Альт	11.0 (несертифицированная)	Подтверждена
ОС Альт	10.2.2 (сертифицированная)	Ограниченно совместима; требуются права sudo
РЕД ОС	8.0.2	Подтверждена
Debian	—	Ограниченно совместима; требуются права sudo

Запуск инсталлятора:

1. На рабочем месте оператора под управлением ОС Linux запустите "ITC.Installer". Инсталлятор запускается от имени обычного пользователя; применять sudo для запуска не требуется.
2. Откройте в браузере адрес https://localhost:5224/installer.

На главной странице отображаются все компоненты (о компонентах см. в описании архитектуры Clearway CA). Чтобы начать установку, выберите компонент и нажмите «Продолжить».

Запуск без графического интерфейса (режим CLI):

Инсталлятор можно использовать и без графического интерфейса — в режиме командной строки (CLI). Это удобно для установки на серверах без графической среды и для автоматизации развёртывания.

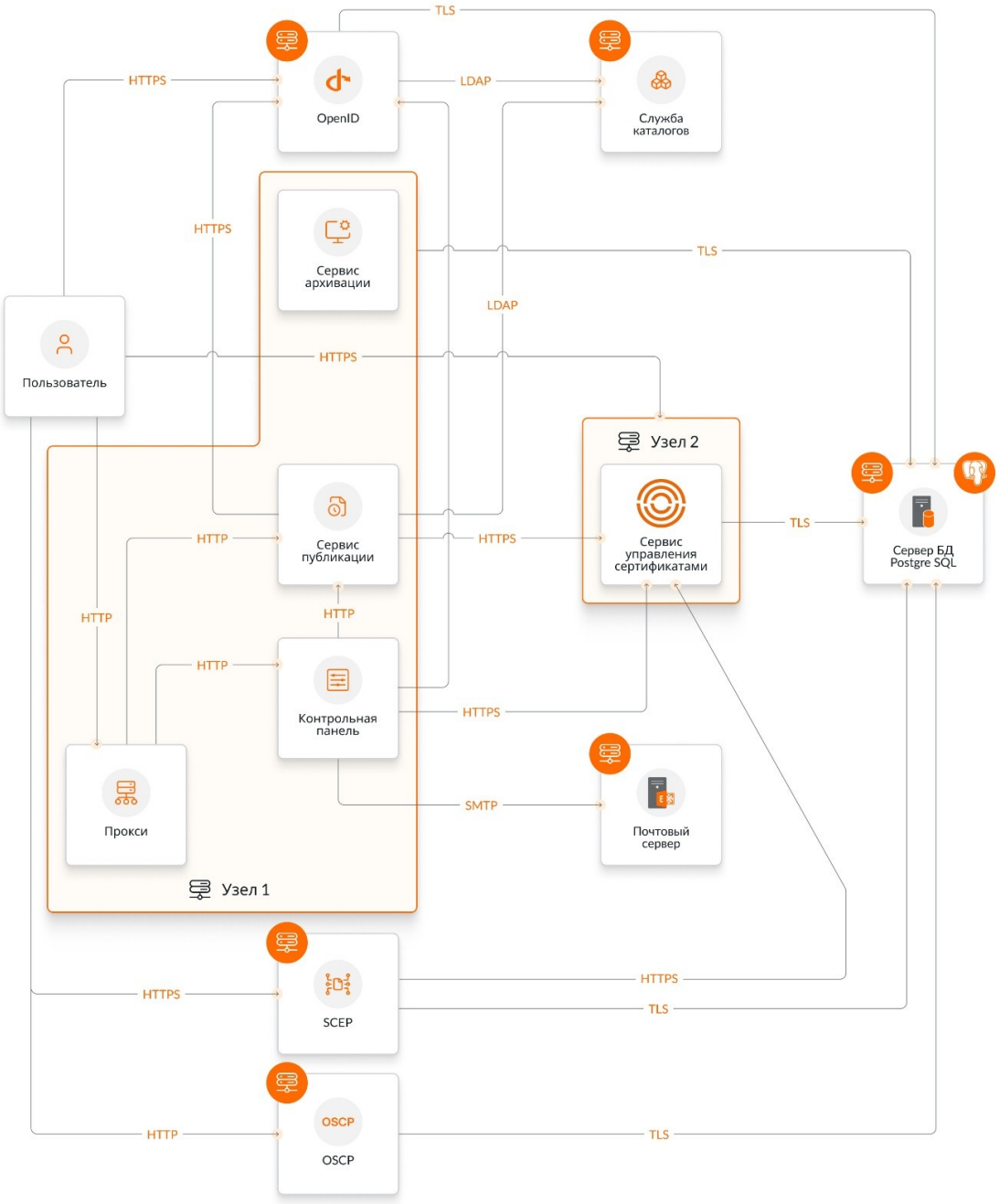
Чтобы запустить инсталлятор в режиме CLI, добавьте параметр cli к команде запуска исполняемого файла:

```
itc-installer cli
```

Последовательность действий в CLI-режиме та же, что и в графическом мастере, и повторяет описанные далее этапы: выбор группы и компонента → подключение к целевому серверу по SSH → ввод параметров компонента (переменных) → проверка и, при необходимости, настройка пререквизитов → установка и получение результатов. Значения по умолчанию, состав проверок пререквизитов и файлы-результаты компонентов совпадают с приведёнными в настоящем руководстве для графического режима.

2 Архитектура Clearway CA

Clearway CA состоит из набора компонентов, схема развертывания и взаимодействия которых представлена ниже.



Рекомендуемая схема развертывания (из двух узлов)

Краткое описание компонентов, входящих в состав Clearway CA, приведено в таблице ниже:

Компонент	Назначение
Сервис управления сертификатами — ядро ЦС (minica)	Сетевой REST-сервис удостоверяющего центра: выпуск и отзыв X.509-сертификатов по шаблонам, ведение CRL/DeltaCRL, ролевая модель на JWT. Одна программа работает и корневым, и выдающим ЦС — роль определяется конфигурацией. Конфигурация — *minica.yml*
Сервис аутентификации OpenID (openid)	OpenID Connect провайдер (форк Dex): единый вход для компонентов, аутентификация через LDAP/Active Directory, маппинг групп каталога на роли Clearway CA, выдача access/refresh-токенов
Контрольная панель (ControlPanel)	Графическая панель управления ЦС: серверная часть ASP.NET (ITC.Api.MiniCA.ControlPanel), одностраничное приложение (ITC.MiniCA.Spa) и конфигурация Nginx (обратный прокси и раздача статики). Вход по OpenID/JWT
Сервис публикации (Publication)	Сервис ITC.Api.MiniCA.Publication: публикация сертификатов и CRL на точки распространения, в том числе в каталог LDAP, по настраиваемым заданиям
OCSP-респондер (mOCSP)	Сервис mocsp: проверка статуса сертификатов в реальном времени по протоколу OCSP; статусы читаются из БД ЦС
Сервис архивации (Archiver)	Сервис ITC.Api.MiniCA.Archiver: перенос истекших сертификатов из рабочей БД ЦС в отдельную архивную БД по расписанию (@daily)
SCEP-адаптер (scepAdapter)	Сервис itc.acm.scepAdapter.clearwayCa: выпуск и обновление сертификатов для сетевых устройств по протоколу SCEP; аутентификация через OpenID, локальное состояние в SQLite
Точка распространения CRL и сертификатов (CDP)	Веб-сервер Nginx, раздающий по HTTP статические файлы CRL (CDP) и сертификатов ЦС (AIA) из каталогов публикации
Консольный клиент (mclient)	CLI для обращения к ядру ЦС: выпуск сертификатов, управление шаблонами, работа с JWT. Права клиента ограничены ролью в его токене

Внешние компоненты, с которыми взаимодействует Clearway CA:

Компонент	Краткое описание
Прокси	Сетевой сервис проксирования. При обращении клиентов по HTTPS он выполняет TLS-терминацию, при необходимости отдает статические ресурсы и маршрутизирует запросы к серверным API-компонентам
Сервер БД	Сервер СУБД, совместимый с PostgreSQL
Служба каталогов	Программный комплекс, который хранит и организует информацию о пользователях компьютерной сети и сетевых ресурсах
Почтовый сервер	SMTP-сервис, предназначенный для передачи электронной почты

Схема развертывания:

Компоненты можно размещать как на одном сервере, так и распределять по нескольким узлам. Типовые конфигурации:

- Базовая (1 сервер): ядро ЦС, PostgreSQL и необходимые сервисы (OpenID, Контрольная панель, OCSP, CDP, при необходимости SCEP) устанавливаются на одну машину. Подходит для стендов, пилотов и небольших инсталляций.
- Без резервирования (2 сервера): один сервер несет корневой ЦС (как правило, вынесенный и оффлайновый), второй — выдающий ЦС с сопутствующими сервисами и БД. Разделение снижает риски компрометации корневого ключа.
- Распределенная: каждая функциональная группа (корневой ЦС, выдающий ЦС, аутентификация OpenID, Контрольная панель, публикация, OCSP, архивирование, SCEP, CDP) выносится на отдельные серверы; БД разворачиваются на выделенных узлах PostgreSQL. Обеспечивает масштабирование и изоляцию ролей.

Развертывание выполняется веб-мастером установки, который оркестрирует установку компонентов на целевые серверы по SSH. Мастер сам на целевые серверы не устанавливается.

3 Требования к программному и аппаратному обеспечению

В разделе приведены требования к операционной системе, аппаратным ресурсам, системному ПО, СУБД, рабочим местам администратора и оператора, сетевым портам и технологической учетной записи, необходимые для установки и эксплуатации Clearway CA 26.1.0.

Операционная система:

Установщик определяет семейство ОС автоматически (altlinux, redos, прочие — семейство Debian, включая Astra Linux) и выбирает менеджер пакетов (apt или dnf). На всех узлах должно быть настроено единое системное время (NTP): проверка меток времени в запросах к ЦС использует окно рассогласования max-dt-sec = 600 (±10 минут); при большем расхождении запрос отклоняется.

Аппаратные требования:

Приведенные конфигурации виртуальных ресурсов (vCPU / vRAM / vHDD) рассчитаны на разную нагрузку по числу выпускаемых сертификатов.

Минимальная конфигурация — один сервер, все компоненты Clearway CA и СУБД PostgreSQL:

Узел	Компоненты	vCPU / vRAM / vHDD	Нагрузка
Единый сервер	Все компоненты + СУБД	4 / 4 ГБ / 256 ГБ	до 100 сертификатов в сутки

Базовая конфигурация — один сервер, все компоненты и СУБД, повышенная нагрузка:

Узел	Компоненты	vCPU / vRAM / vHDD	Нагрузка
Единый сервер	Все компоненты + СУБД	4 / 8 ГБ / 512 ГБ	до 5000 сертификатов в сутки

Типовая конфигурация — компоненты разнесены по отдельным узлам:

Узел	Компоненты	vCPU / vRAM / vHDD	Системное ПО
Центр сертификации	Сервис управления сертификатами (ЦС)	2 / 2 ГБ / 80 ГБ	PostgreSQL
Аутентификация	OpenID	2 / 2 ГБ / 40 ГБ	PostgreSQL
Вспомогательные сервисы	Контрольная панель, публикация, архиватор, OCSP, SCEP, CDP	2 / 4 ГБ / 40 ГБ	PostgreSQL, nginx, SMTP-сервер

Каталог журналов ЦС (*/opt/itc/minica/logs*) рекомендуется размещать на разделе с запасом свободного места и контролировать его заполнение средствами ОС.

Системное ПО:

На серверных узлах устанавливается следующее ПО (как правило, из репозитория ОС или из состава поставки):

ПО	Минимальная версия	Назначение
.NET (ASP.NET Core Runtime)	8.0	Среда выполнения .NET-сервисов (контрольная панель, публикация, архиватор). Компоненты SCEP, OCSP и ядро ЦС поставляются как самодостаточные (self-contained) сборки и отдельной установки .NET не требуют
nginx	из репозитория	Обратный прокси и TLS-терминация для веб-сервисов (контрольная панель, публикация, SCEP, CDP)
curl	из репозитория	Обращения к API системы из скриптов
jq	из репозитория	Обработка JSON при формировании токенов и настройке сервисов
OpenSSL	из репозитория	Генерация ключей, запросов (CSR) и сертификатов на узлах ЦС
psql (клиент PostgreSQL)	не ниже версии сервера БД	Создание и обслуживание БД и таблиц

СУБД PostgreSQL:

Состояние ЦС, сервиса аутентификации и архиватора хранится в PostgreSQL.

- Поддерживаемые версии — PostgreSQL 11–18; минимально допустимая — 11.
- При установке мастер автоматически подбирает наибольшую доступную версию из диапазона (от 18 к 11); если ни одна не обнаружена, используется запасное значение 16.
- Та же логика применяется к БД сервиса аутентификации (OpenID).

Для отказоустойчивого развертывания PostgreSQL поддерживается работа в кластере на базе etcd и patroni (устанавливаются из репозитория ОС на узлах СУБД).

Подключение сервисов к БД по умолчанию разрешено без TLS (database.allow-without-tls: true). Для защищенного состояния канал "сервис–БД" следует переводить на TLS (allow-without-tls: false, sslmode=verify-full). Подробнее см. в разделе настройки конфигурации ЦС.

АРМ администратора и оператора:

Рабочее место — ПК под управлением любой ОС, поддерживающей рекомендуемый браузер и допускающей применение мер защиты информации.

Параметр	Значение
Ядер / частота	2 / не менее 2 ГГц
RAM	4 ГБ
Диск	80 ГБ SSD
Браузер	Google Chrome версии не ниже 113 или браузер на базе Chromium (Microsoft Edge, Яндекс.Браузер)

Дополнительное ПО для АРМ администратора:

ПО	Минимальная версия	Назначение
DBeaver (+ утилиты pg_dump, pg_dumpall, pg_restore, psql, драйвер PostgreSQL)	21.3.1	Настройка и обслуживание БД
WinSCP	5.13.7	Доступ к файлам серверов
PuTTY	0.70	Доступ к серверам по SSH
Google Chrome	113	Доступ к веб-интерфейсу системы

Сетевые порты:

Для настройки правил межсетевого экрана используются перечисленные ниже порты. Веб-сервисы публикуются через Nginx (порт 443, TLS), а сами приложения слушают локальные порты и извне напрямую недоступны.

Служба / узел	Порт/протокол	Назначение
Веб-интерфейс (Nginx)	80/tcp, 443/tcp	Доступ к веб-консоли; на 443 — TLS. Порт 80 используется, в частности, точкой распространения CRL (CDP)
Центр сертификации (ЦС)	9443/tcp	Защищенный интерфейс ЦС (mTLS); обращения mclient и сервисов к ЦС
Аутентификация (OpenID)	443/tcp	HTTPS OIDC-провайдера
Аутентификация (OpenID)	5559/tcp	Служебный HTTP-интерфейс администрирования
Аутентификация (OpenID)	5432/tcp	Подключение к БД OpenID (PostgreSQL)

Служба / узел	Порт/протокол	Назначение
SCEP-адаптер	8440/tcp	Локальный порт приложения SCEP (публикуется через Nginx: *https://<fqdn>/api/scep*)
Серверы продукта (ОС)	22/tcp	Администрирование по SSH (OpenSSH)
Сервер БД	5432/tcp	Подключение к PostgreSQL для настройки и сопровождения

Внутренние порты .NET-сервисов (контрольная панель — 8407, публикация — 9407, OCSP — 8888) используются только для локального проксирования через Nginx и в правилах внешнего брандмауэра, как правило, не открываются.

Требования к учетной записи:

Все серверные сервисы Clearway CA работают от имени **технологической учетной записи-владельца** (по умолчанию itc-svc), а не от root. Каталог установки по умолчанию — */opt/itc* (для ЦС — */opt/itc/minica*), владельцем каталога должна быть эта учетная запись.

Сервисы запускаются как **пользовательские systemd-юниты** (`systemctl --user`), поэтому для учетной записи-владельца обязательны:

- включенный режим сохранения сеанса — `enable-linger` (`loginctl enable-linger <учетная запись>`), иначе пользовательские юниты не стартуют при отсутствии интерактивного входа;
- настроенное окружение для управления юнитами — переменные XDG_RUNTIME_DIR и (при необходимости) DBUS_SESSION_BUS_ADDRESS, прописываемые в *~/.bashrc*.

```
# Проверка режима linger для учетной записи-владельца
loginctl show-user itc-svc | grep Linger
# ожидается Linger=yes
# Включение при необходимости
loginctl enable-linger itc-svc
```

Наличие учетной записи, каталога установки, корректного владельца, режима linger, а также OpenSSL и Nginx проверяется установщиком на этапе контроля пререквизитов; при отсутствии предлагается автоматическое исправление.

4 Общие сведения о мастере установки

Установка выполняется по сценариям — группам установки. Группа объединяет компоненты, которые устанавливаются в строгом порядке (например: база данных → сервис → его настройка). Инсталлятор поддерживает 9 групп: Корневой ЦС, Выдающий ЦС, Аутентификация (OpenID), Контрольная панель, Сервис публикации, OCSP, Архиватор, SCEP и MS-WSTEP. Порядок развёртывания в общем случае: сначала Корневой и/или Выдающий ЦС, затем аутентификация и остальные сервисы.

Важно

На изображениях возможно отображение другой версии инсталлятора. Это не влияет на актуальность инструкции: интерфейс и шаги работы совпадают.

Ограничения совместного размещения

Графический инсталлятор не поддерживает установку следующих пар компонентов на один целевой сервер (ВМ):

- «Корневой ЦС» и «Выдающий ЦС»;
- «Контрольную панель» и «Аутентификацию (OpenID)»;
- «SCEP» и «Аутентификацию (OpenID)».

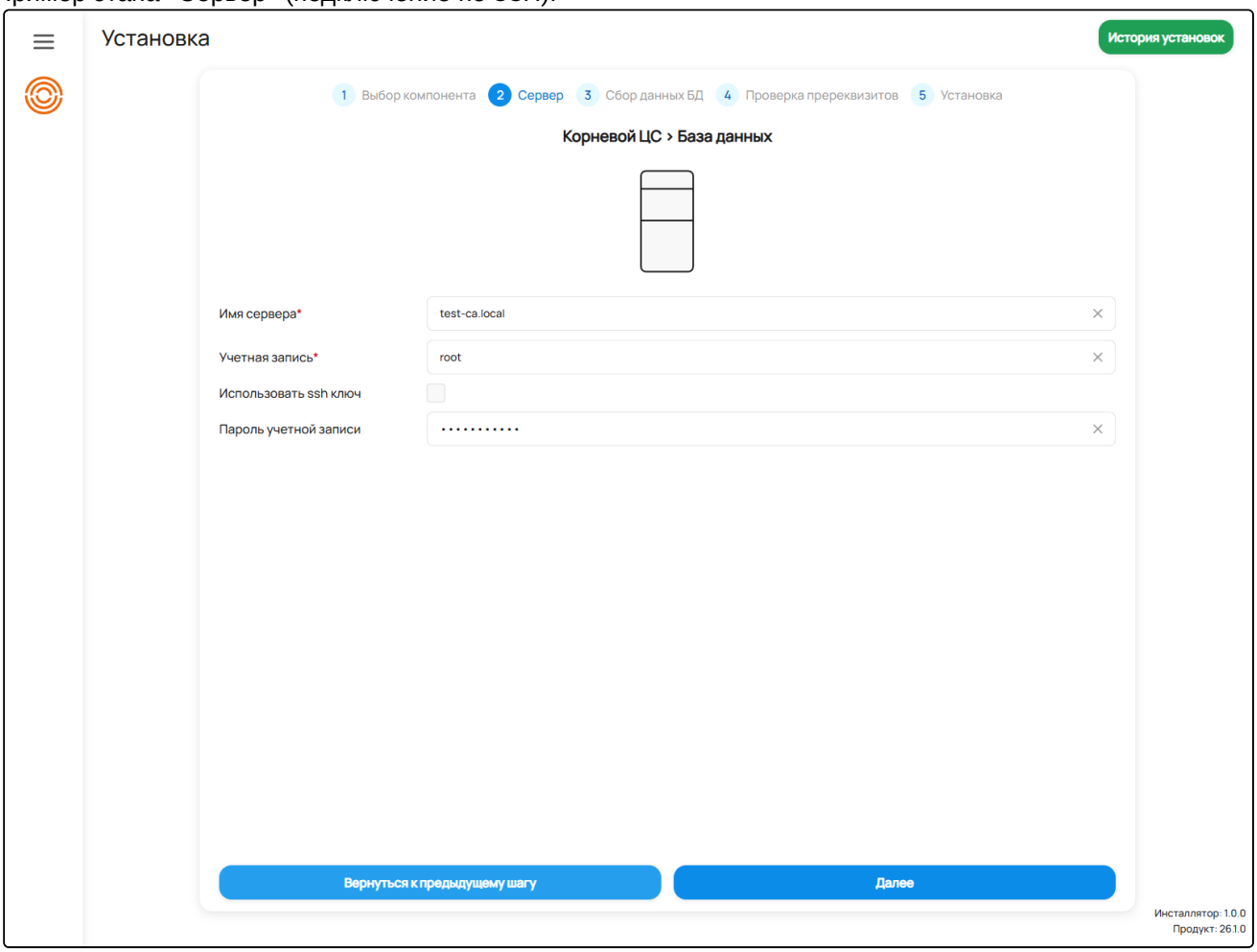
Для компонентов каждой пары укажите разные целевые серверы на этапе «Сервер». Вариант совместного размещения с ручным изменением портов не входит в сценарий графической установки и в этом руководстве не рассматривается.

Этапы мастера:

Установка каждого компонента проходит через последовательность этапов, отображаемых в верхней части окна:

1. Выбор компонента — выбор группы и компонента для установки.
2. Сервер — подключение к целевому серверу по SSH: имя сервера, учётная запись и пароль (либо флажок «Использовать ssh ключ»).
3. Сбор данных — ввод параметров компонента (переменных): имена, пути, учётные данные БД, адреса сервисов и т. п. Часть параметров подставляется значениями по умолчанию; расширенные параметры доступны при необходимости.
4. Проверка пререквизитов — автоматическая проверка готовности сервера (версия ОС, права sudo, сетевой доступ, каталог установки, зависимости). Успешные проверки помечаются состоянием «Проверено».
5. Установка — выполнение установки на сервере и вывод результата.

Пример этапа «Сервер» (подключение по SSH):



Если страница мастера перестала обновляться

Страница мастера может перестать обновляться из-за обрыва связи с инсталлятором. Само по себе это не означает, что целевой сервер недоступен.

Если ход выполнения не меняется:

1. Обновите страницу в браузере клавишей `F5`.
2. После загрузки страницы заново запустите шаг, который выполнялся до обновления.
3. Убедитесь, что мастер снова отображает ход выполнения.

Пропуск необязательных компонентов:

В инсталляторе 1.3.0 можно пропустить отдельный компонент группы целиком, но не отдельный экран этого компонента («Сервер», «Сбор данных», «Проверка пререквизитов» и т. п.). Выберите компонент, для которого разрешён пропуск, нажмите значок со стрелкой пропуска в линейке компонентов и подтвердите запрос «Пропустить компонент?». Проверки, команды и установка этого компонента не выполняются; мастер переходит к следующему компоненту, а в истории появляется запись со статусом Skipped.

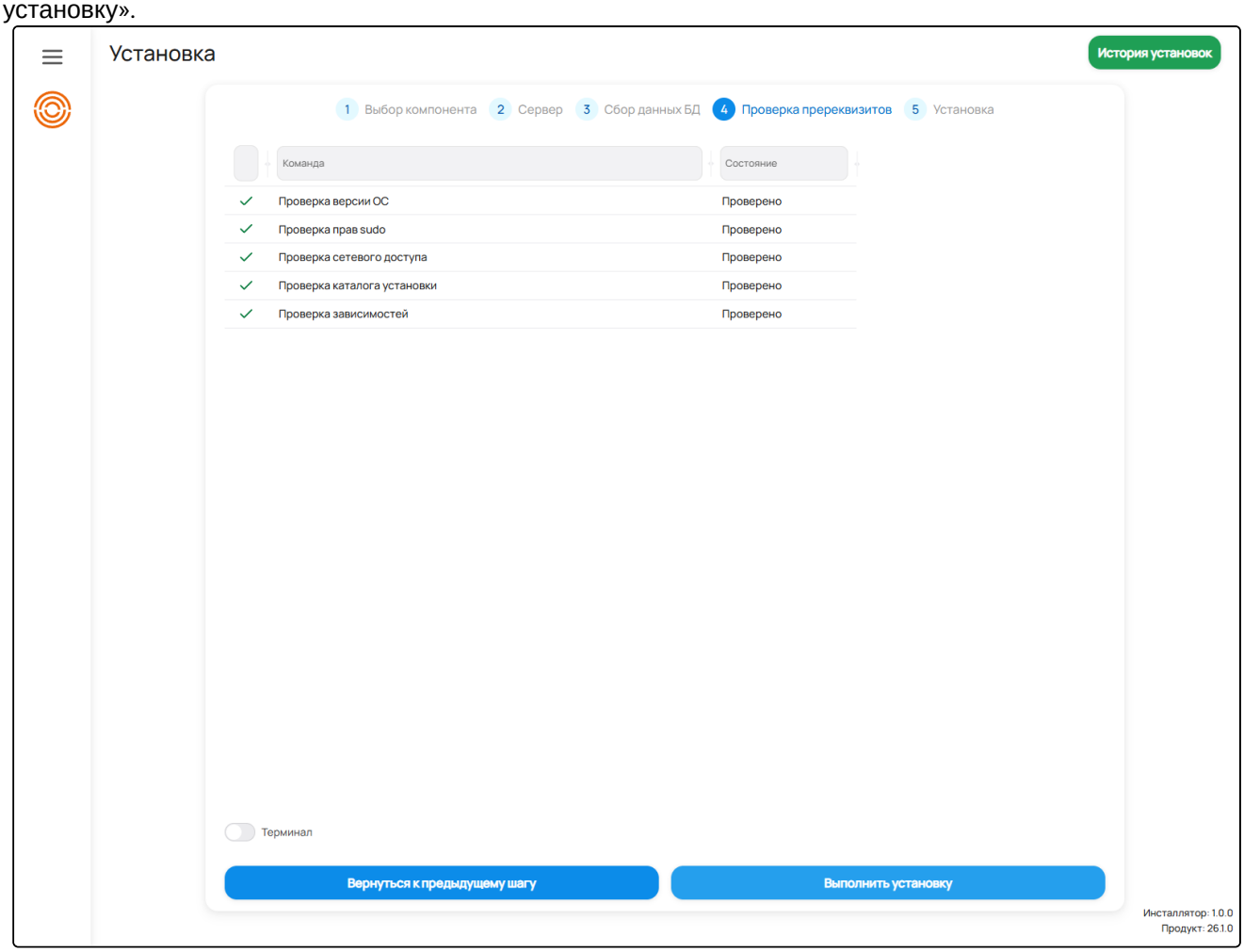
Пропускайте компонент только в том случае, если его результат уже получен, подготовлен вне инсталлятора либо сохранён после предыдущего выполнения. Инсталлятор не создаёт пропущенные артефакты автоматически: в следующих шагах их необходимо загрузить вручную или заранее разместить на целевом сервере.

- Выдающий ЦС — «Выпуск сертификата»;

- Сервис публикации — «Выпуск запроса на TLS» и «Выпуск сертификата»;
- MS-WSTEP — «Выпуск запроса для TLS» и «Выпуск сертификата».

Проверка и настройка пререквизитов:

На этапе «Проверка пререквизитов» инсталлятор проверяет готовность целевого сервера. Если какая-либо проверка не пройдена, становится доступна кнопка «Выполнить настройку пререквизитов» — инсталлятор автоматически устраняет проблему (создаёт учётную запись, каталог, устанавливает недостающие пакеты и т. п.). Когда все проверки в состоянии «Проверено», нажмите «Выполнить установку».



Если настройка пререквизитов не продолжается

При установке пакетов может потребоваться интерактивный ввод. В этом случае интерфейс мастера может перестать обновляться.

1. Включите переключатель «Терминал» в мастере и скопируйте команду, на которой остановилось выполнение.
2. Подключитесь по SSH к целевому серверу.
3. Перед ручным запуском убедитесь, что такая же команда больше не выполняется на сервере.
4. Выполните скопированную команду, ответьте на появившиеся запросы и дождитесь её завершения.

5. Вернитесь в мастер и проверьте, что этап настройки пререквизитов больше не заблокирован.

Передача результатов между компонентами:

Результаты одних компонентов используются другими: запрос на сертификат (CSR), выпущенный сертификат, файлы JWT и ключи, полученные на предыдущих шагах, автоматически подставляются в качестве значений по умолчанию для последующих компонентов группы. Например, запрос TLS формируется отдельным компонентом, подписывается на ЦС, а затем используется при установке сервиса.

Дополнительные возможности:

- переключатель «Терминал» на этапах установки показывает журнал выполняемых на сервере команд;
- кнопка «История установок» открывает историю ранее выполненных установок с введёнными параметрами;
- кнопка «Вернуться к предыдущему шагу» позволяет вернуться к предыдущему этапу и скорректировать данные.

Файлы — результаты компонентов:

Часть компонентов формирует файлы, которые используются последующими компонентами. В рамках одной сессии мастер подставляет их автоматически; при установке в разных сессиях сохраните файлы и передайте вручную на нужном шаге.

Раздел	Пункт	Файлы	Описание
Корневой ЦС	ЦС	root-ca.crt, root-ca-tls.crt	самоподписанный сертификат корневого ЦС и TLS-сертификат его сервера
Выдающий ЦС	ЦС	sub-ca.csr	запрос на выпуск сертификата выдающего ЦС (передаётся на корневой ЦС для подписи)
Выдающий ЦС	Выпуск сертификата	sub-ca.crt	сертификат выдающего ЦС, выпущенный по запросу
Выдающий ЦС	Настройка ЦС	sub-ca.crt, sub-ca-tls.crt	установленный сертификат выдающего ЦС и TLS-сертификат его сервера
КП / Сервис публикации	Выпуск запроса для TLS	tls.req	запрос на выпуск TLS-сертификата компонента
КП / Сервис публикации	Выпуск JWT	<сервис>.jwt, <сервис>.encrypted.key	JWT-токен и зашифрованный ключ для подключения компонента к ЦС
OCSP	OCSP	mocsp.csr	запрос на выпуск сертификата OCSP-сервиса

Раздел	Пункт	Файлы	Описание
OCSP	Выпуск сертификата	mocsp.crt	сертификат OCSP-сервиса, выпущенный по запросу

5 Параметры по умолчанию

Для части параметров мастер предзаполняет значения по умолчанию — рекомендуется использовать их. Пароли и парольные фразы всегда задаются вручную.

Параметр	Значение по умолчанию
Технологическая учётная запись	itc-svc
Учётная запись в БД	cwica
Имя базы данных ЦС	cwica
Порт сервера БД	5432
Subject корневого ЦС	CN=RootCA,O=Company,C=RU
Subject выдающего ЦС	CN=Issuing CA,O=Company,C=RU
Путь к папке установки ЦС	/opt/itc/minica
Путь к папке установки Контрольной панели / Сервиса публикации	/opt/itc
Путь к папке установки точки распространения (CDP)	/opt/itc/web
Путь к папке установки OCSP	/opt/itc/ocsp
Идентификатор клиента OpenID	itc-clearway (регистрируется сервисом OpenID; Контрольная панель использует это же значение)
Идентификатор роли администратора	admin
Alias сервера	определяется автоматически командой hostname
Имя файла сертификата	cert (если не передан CSR)
Имя шаблона сертификата	tls / subca / ocsp (в зависимости от сценария)
Наименование сервиса JWT	control-panel / publication-service / service (в зависимости от сценария)

Пример: на этапе «Сбор данных БД» компонента «База данных» параметры «Учётная запись в БД» и «Имя базы данных ЦС» имеют значение по умолчанию cwica — используйте его; «Пароль учётной записи PostgreSQL» задайте самостоятельно.

6 Проверка пререквизитов — список проверок

Перед установкой каждого компонента на этапе «Проверка пререквизитов» мастер проверяет готовность сервера и при необходимости подготавливает его. У каждого компонента свой набор проверок.

Статусы проверки: «В процессе» — условие проверяется; «Ожидание» — условие ожидает проверки; «Проверено» — условие выполнено; «Отсутствует» — условие не соблюдено. Если проверка не пройдена, нажмите «Выполнить настройку пререквизитов» — мастер устранит замечание автоматически; когда все проверки в состоянии «Проверено», нажмите «Выполнить установку». Чтобы видеть выполняемые команды, включите переключатель «Терминал».

Проверка	**Что означает**	**Ожидаемый результат**	**Как исправить (команда)**
Наличие учётной записи $USER_NAME	На сервере должен существовать пользователь, от имени которого работает сервис	Учётная запись существует	sudo adduser --disabled-password --gecos "" $USER_NAME
Наличие папки $PATH	Должна существовать папка для файлов компонента	Папка существует	sudo mkdir -p $PATH
Права на папку $PATH	Папка установки принадлежит технологической учётной записи	Владелец и группа: $USER_NAME:$USER_NAME	sudo chown $USER_NAME:$USER_NAME $PATH
Состояние enable-linger для $USER_NAME	Пользовательские сервисы должны работать после выхода из SSH-сессии	Linger=yes	sudo loginctl enable-linger $USER_NAME
Наличие OpenSSL	Требуется для работы с ключами, CSR и сертификатами	OpenSSL установлен и доступен	sudo apt install openssl -y
Установка PostgreSQL	На сервере БД должен быть установлен PostgreSQL	Команда psql доступна	sudo apt install postgresql postgresql-contrib -y
Наличие УЗ в PostgreSQL	Должен существовать пользователь БД для ЦС	Пользователь существует	sudo -u postgres psql -c "CREATE USER \"$PG_USERNAME\" WITH PASSWORD '$PG_PASSWORD';"
Наличие базы данных	Должна существовать база данных ЦС	База существует	sudo -u postgres psql -c "CREATE DATABASE $PG_DB OWNER \"$PG_USERNAME\";"

Проверка	Что означает	Ожидаемый результат	Как исправить (команда)
Отсутствие таблиц в БД	Перед инициализацией база должна быть пустой	В схеме public нет таблиц	sudo -u postgres psql -d $PG_DB -c "DROP SCHEMA public CASCADE; CREATE SCHEMA public;"
Права пользователя в PostgreSQL	Пользователь БД имеет права CONNECT, CREATE, USAGE	Права выданы	GRANT CONNECT, CREATE ON DATABASE "$PG_DB" TO "$PG_USERNAME"; GRANT USAGE, CREATE ON SCHEMA public TO "$PG_USERNAME";
Подключение к базе данных	Компонент может подключиться к БД с указанными параметрами	Подключение успешно	Проверьте адрес, порт, имя БД, пользователя, пароль и доступность PostgreSQL
Установка Nginx	На сервере установлен и запущен Nginx	Nginx установлен, включён и запущен	sudo apt install nginx -y && sudo systemctl enable --now nginx
Установка ЦС	ЦС установлен и доступен через mclient	$PATH/mclient ping выполняется успешно	Проверьте, что сервис minica.service запущен, а путь к mclient указан верно

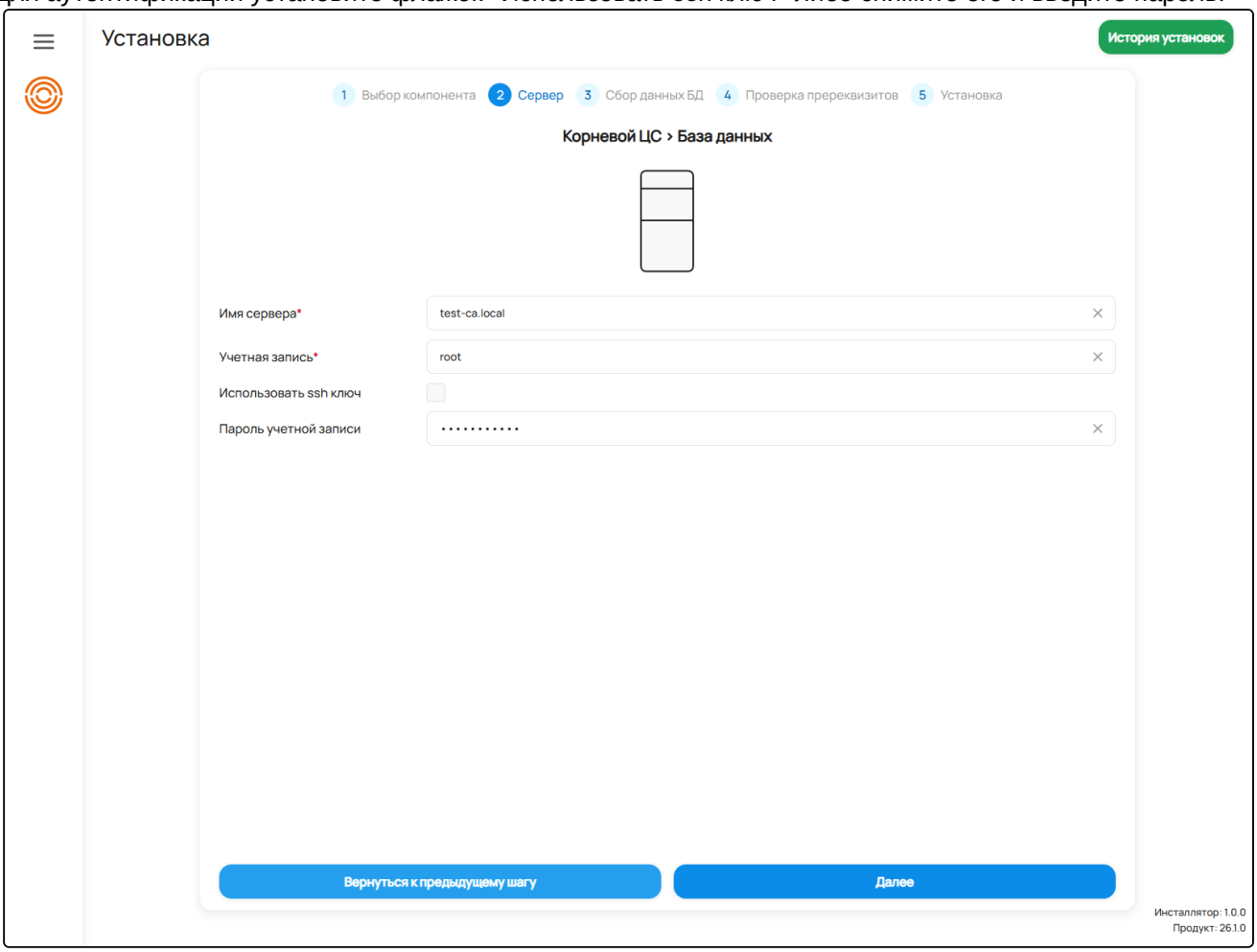
7 Корневой ЦС

Группа разворачивает самодостаточный корневой центр сертификации Clearway CA — вершину доверия всей инфраструктуры. Установка выполняется в два шага строго по порядку: сначала База данных (PostgreSQL со схемой ЦС), затем Корневой ЦС (сервис MiniCA, самоподпись корневого сертификата, включение TLS). Мастер подключается к целевому серверу по SSH и выполняет все действия от имени технологической учётной записи itc-svc; каталог установки по умолчанию — */opt/itc/minica*.

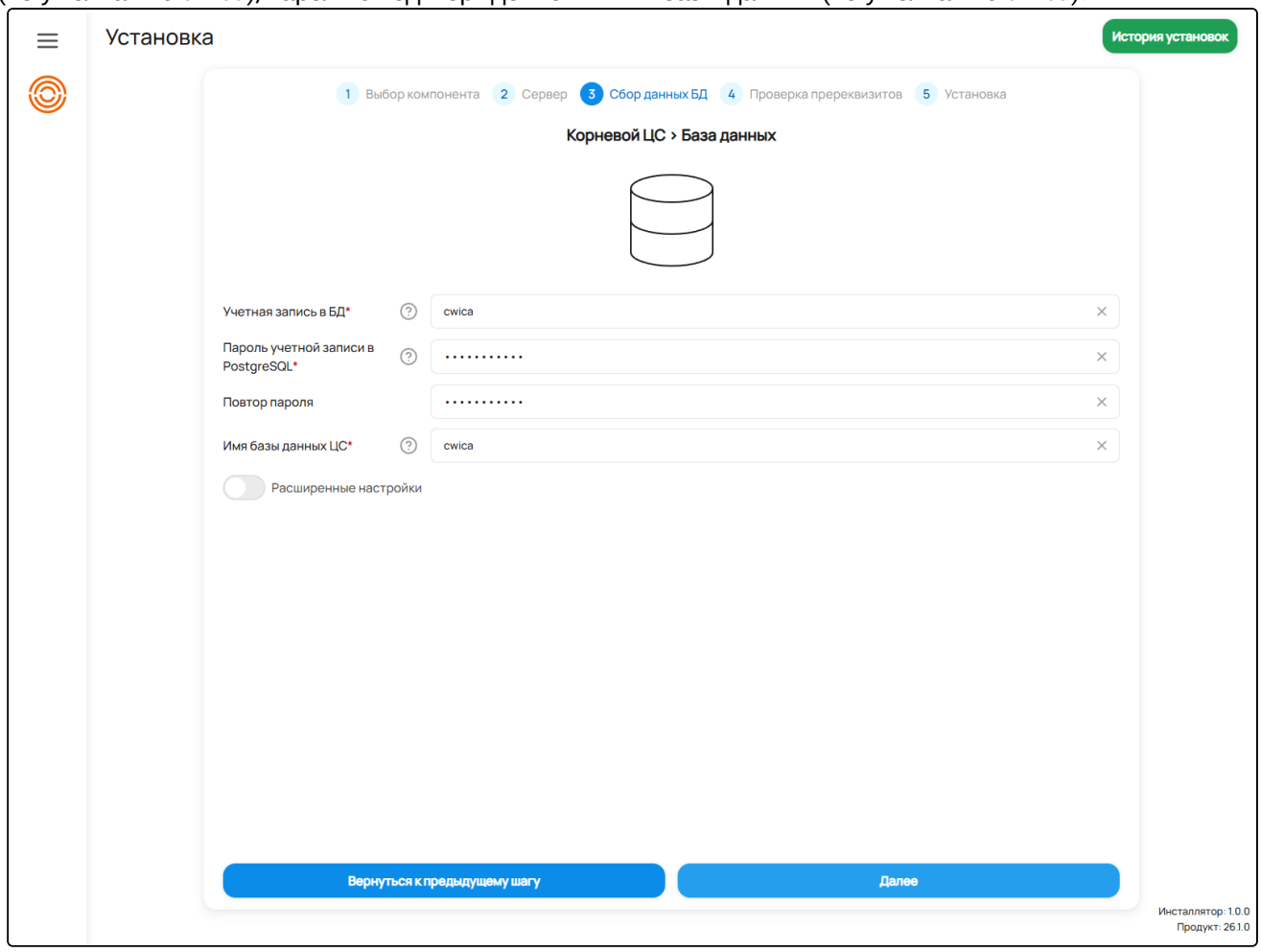
7.1 База данных

Разворачивает БД центра сертификации на PostgreSQL: создаёт учётную запись-владельца, базу и применяет схему ЦС (таблицы запросов, сертификатов, CRL, шаблонов, токенов и журнала событий).

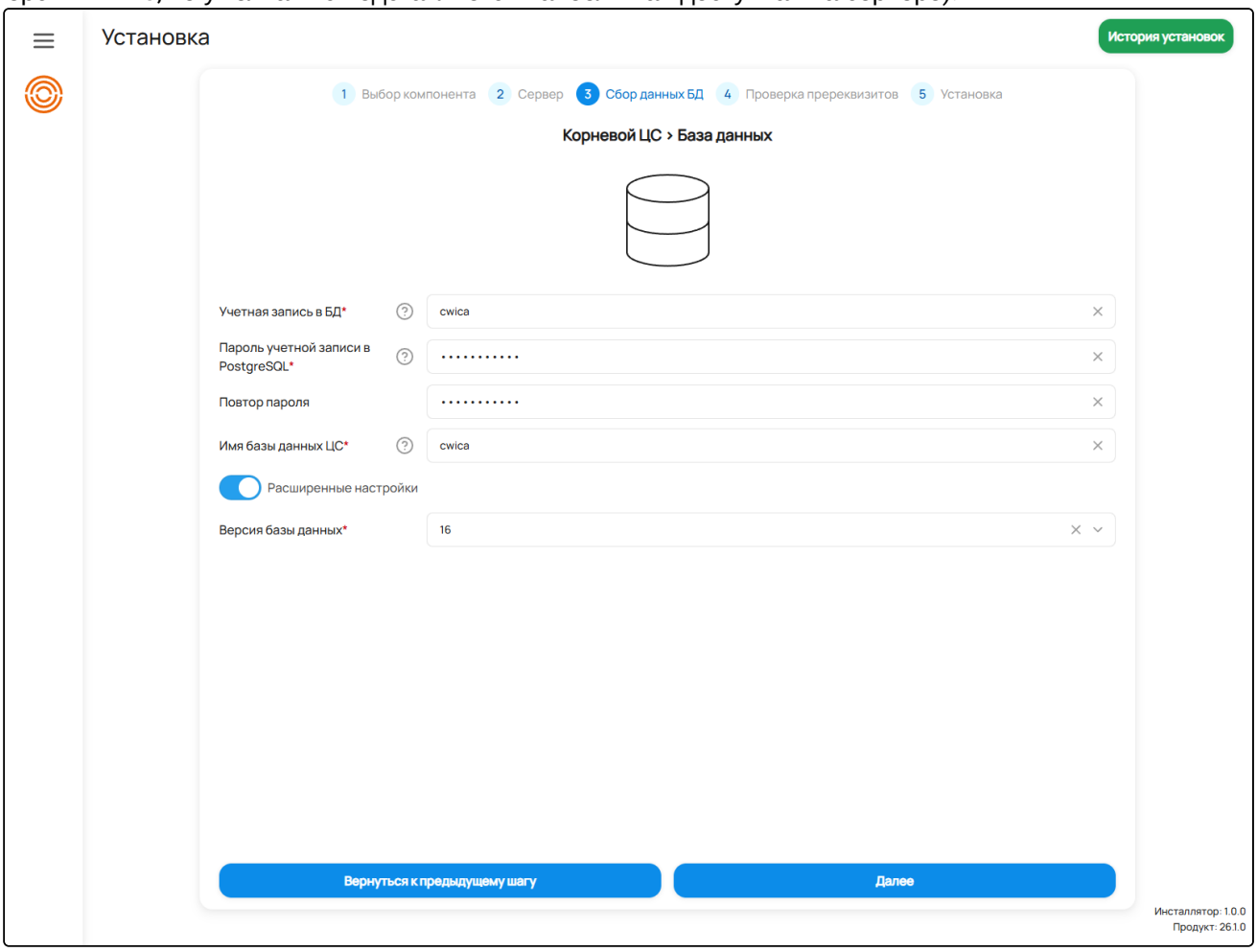
Шаг 1. Сервер. Укажите адрес сервера базы данных и параметры SSH-подключения: в поле «Имя сервера» введите FQDN или IP целевого узла, в поле «Учётная запись» — имя пользователя для входа. Для аутентификации установите флажок «Использовать ssh ключ» либо снимите его и введите пароль.



Шаг 2. Сбор данных БД. Заполните параметры создаваемой базы: имя пользователя-владельца БД (по умолчанию cwica), пароль с подтверждением и имя базы данных (по умолчанию cwica).

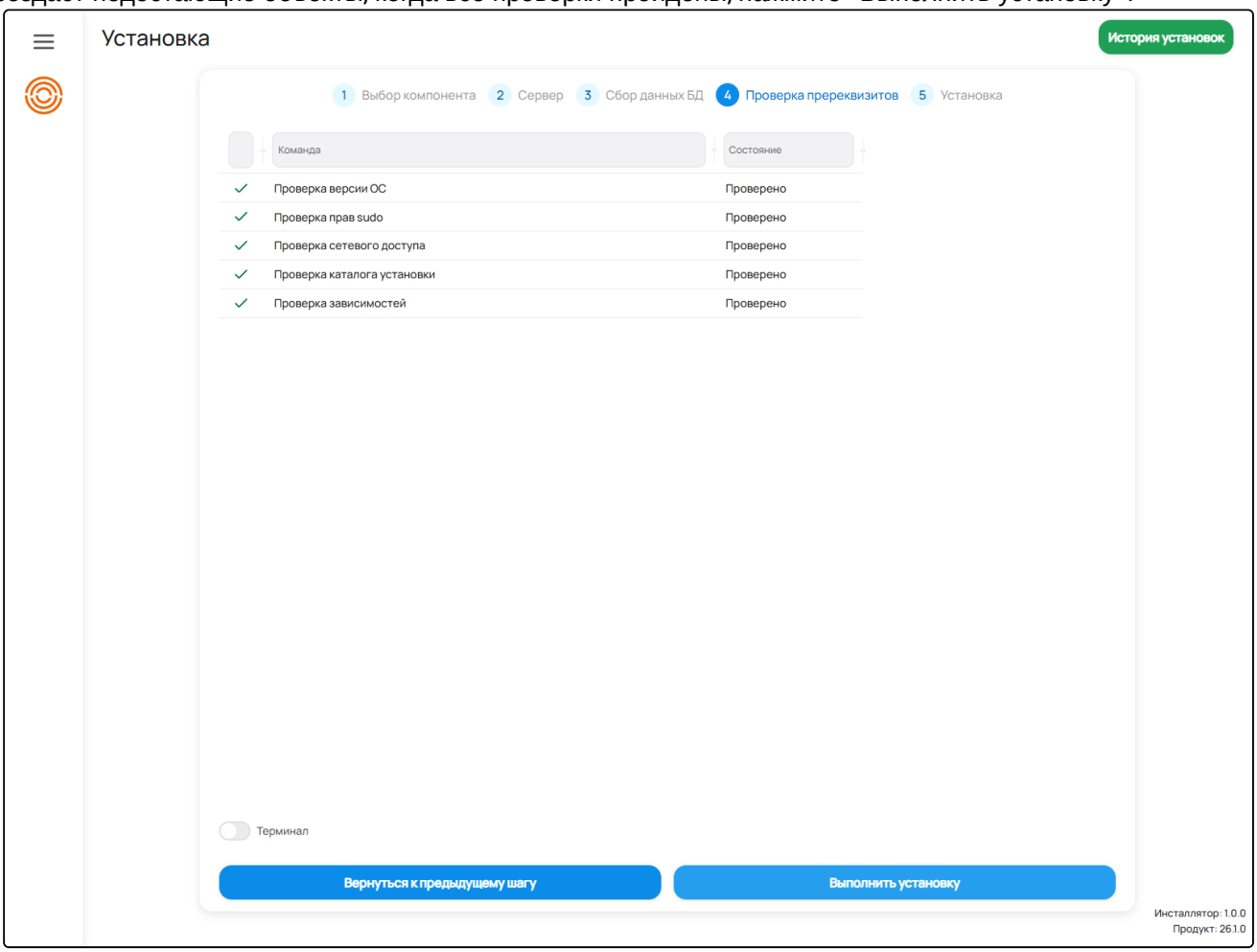


Прокрутите форму ниже и выберите версию PostgreSQL из выпадающего списка (поддерживаются версии 11–18; по умолчанию подставляется наибольшая доступная на сервере).

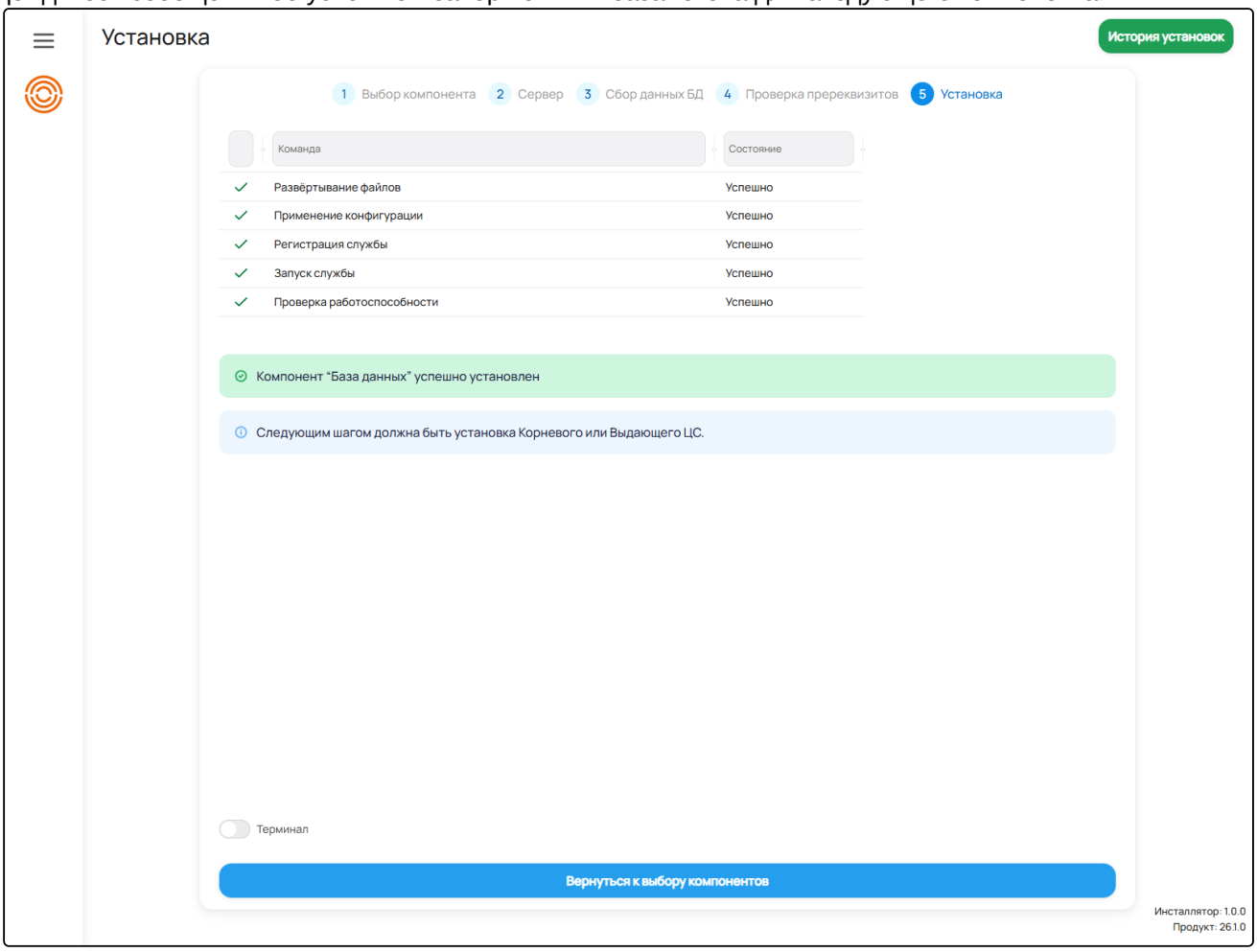


Шаг 3. Проверка пререквизитов. Мастер выводит таблицу проверок: установлен ли PostgreSQL, существуют ли учётная запись и база, свободна ли схема и выданы ли права пользователю. Если есть незакрытые пункты, нажмите «Выполнить настройку пререквизитов» — установщик установит СУБД и

создаст недостающие объекты; когда все проверки пройдены, нажмите «Выполнить установку».



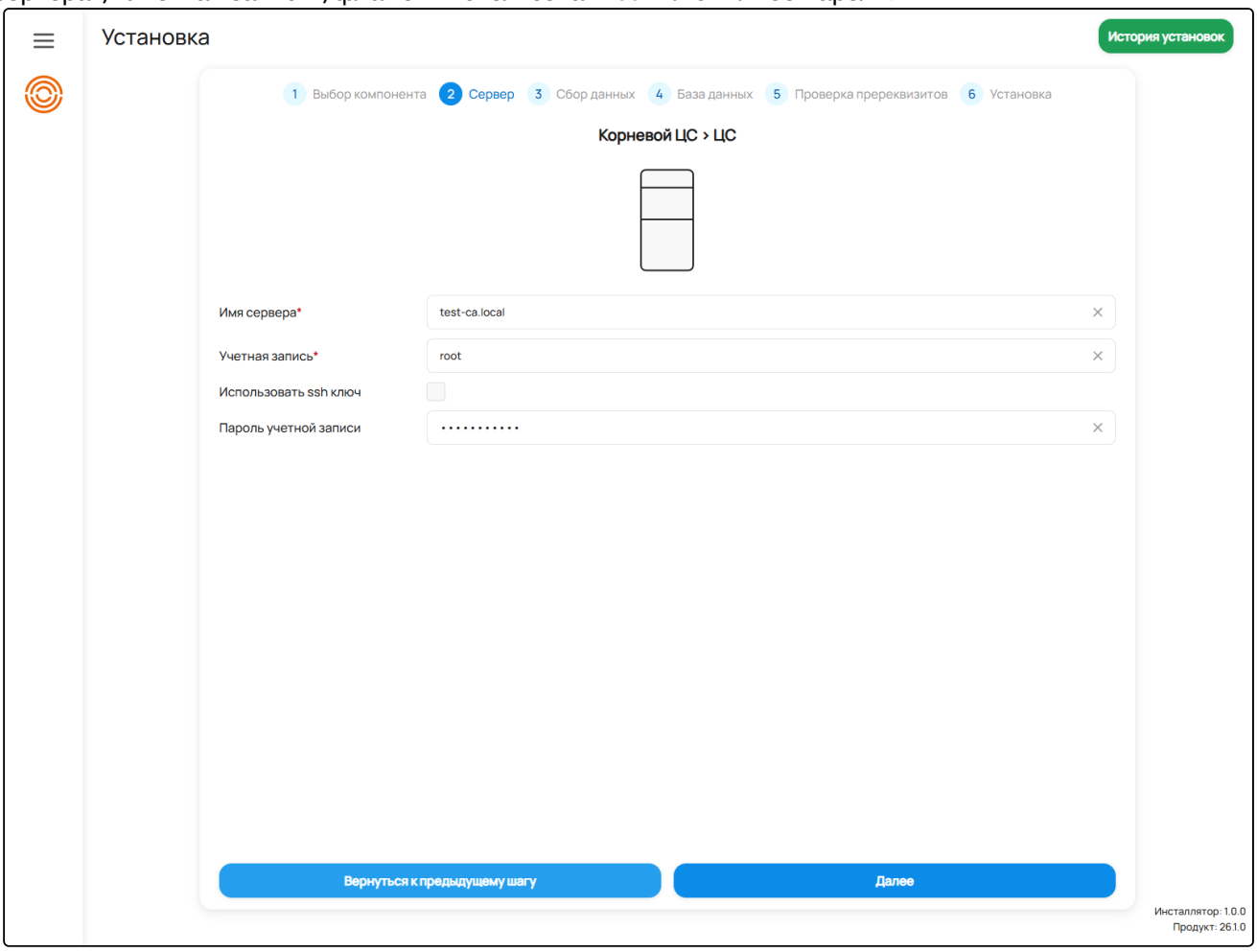
Шаг 4. Установка и результат. Установщик применяет схему ЦС к базе (создаёт таблицы и типы). Дождитесь сообщения об успешном завершении — база готова для следующего компонента.



7.2 Корневой ЦС

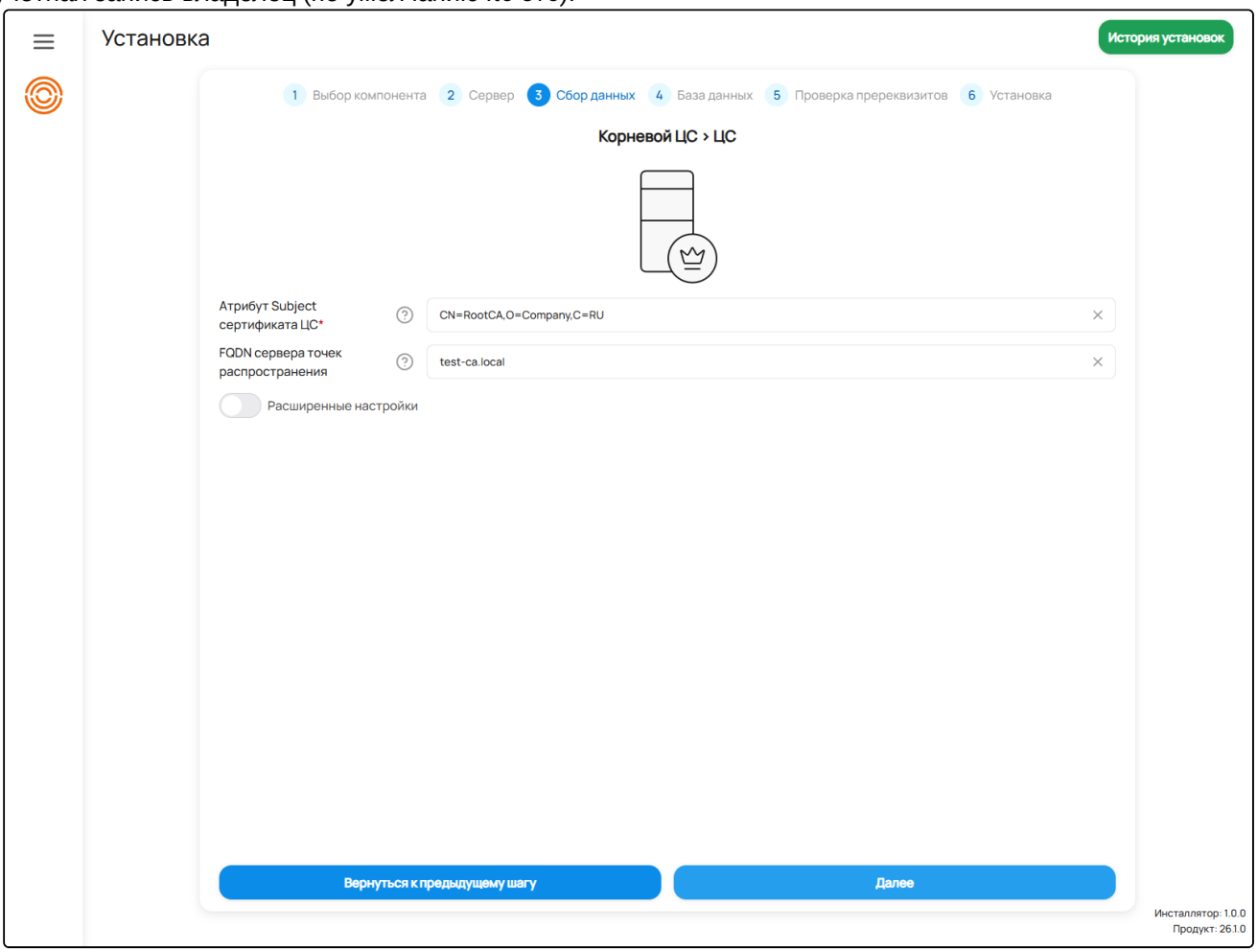
Разворачивает сервис MiniCA, самоподписывает корневой сертификат (RSA-4096, срок ~8 лет), включает TLS и заводит базовые шаблоны выпуска. Это ядро доверия — все нижестоящие ЦС и сервисы проверяются по нему.

Шаг 1. Сервер. Укажите сервер, на который устанавливается корневой ЦС, и параметры SSH: «Имя сервера», «Учётная запись», флажок «Использовать ssh ключ» либо пароль.



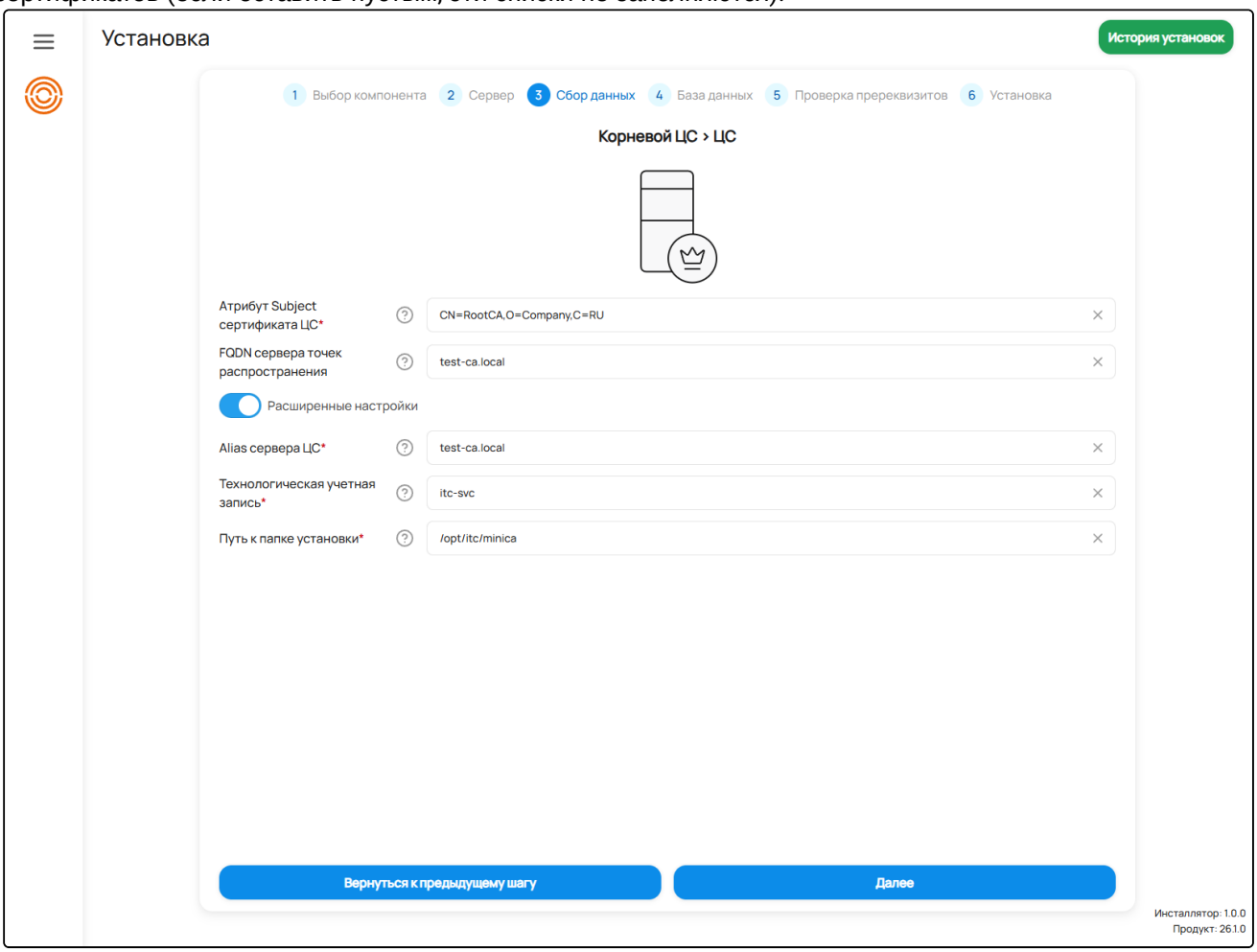
Шаг 2. Сбор данных. Заполните параметры корневого ЦС: «Subject» – различительное имя корневого сертификата (по умолчанию CN=RootCA,O=Company,C=RU); «HOSTNAME» – алиас, на который выпускается TLS-сертификат и по которому обращается mclient; «USER_NAME» – технологическая

учётная запись-владелец (по умолчанию itc-svc).



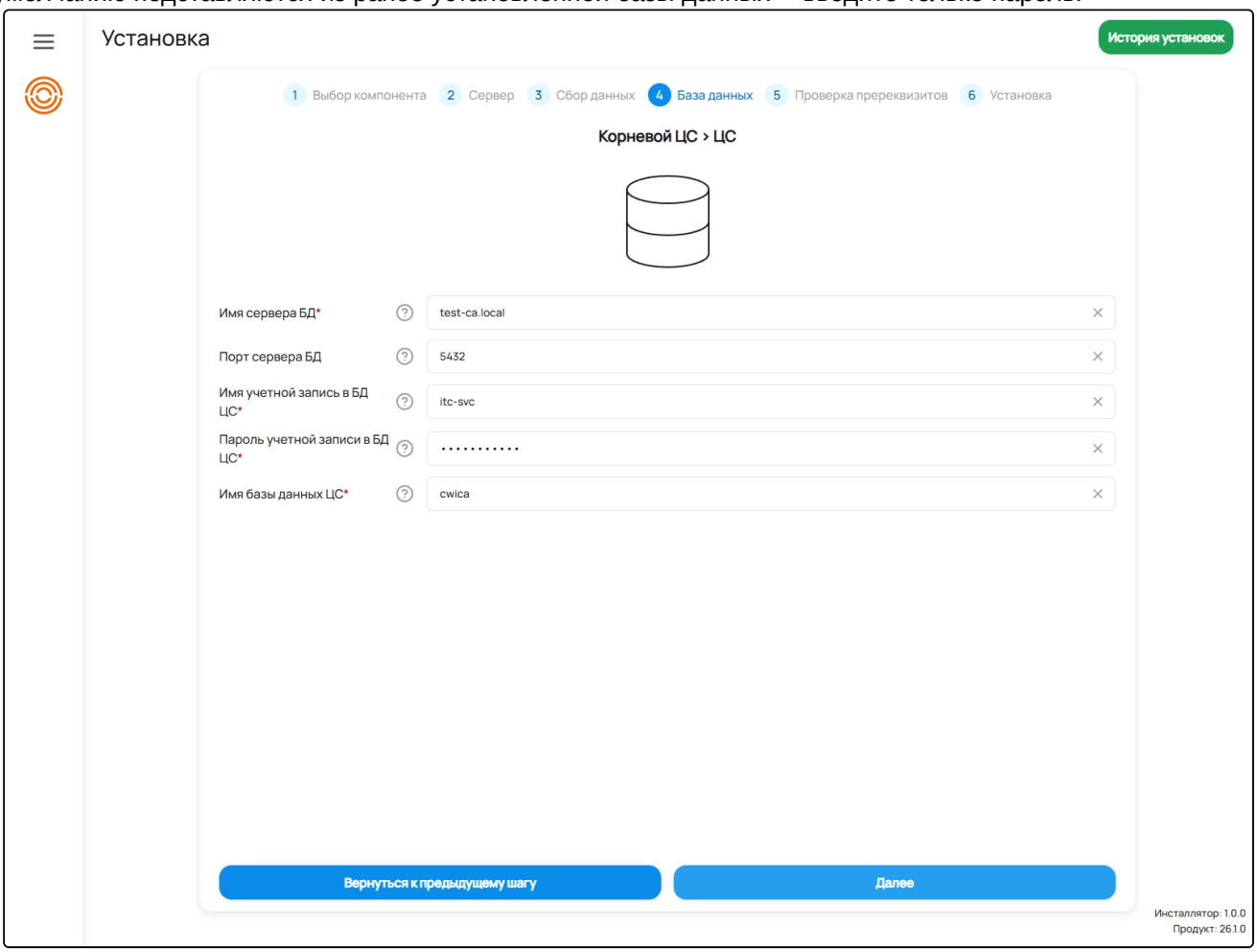
Прокрутите ниже и задайте каталог установки «PATH» (по умолчанию /opt/itc/minica) и «CDP_SERVER_NAME» — FQDN, который прописывается в точки распространения CRL/AIA выпускаемых

сертификатов (если оставить пустым, эти списки не заполняются).



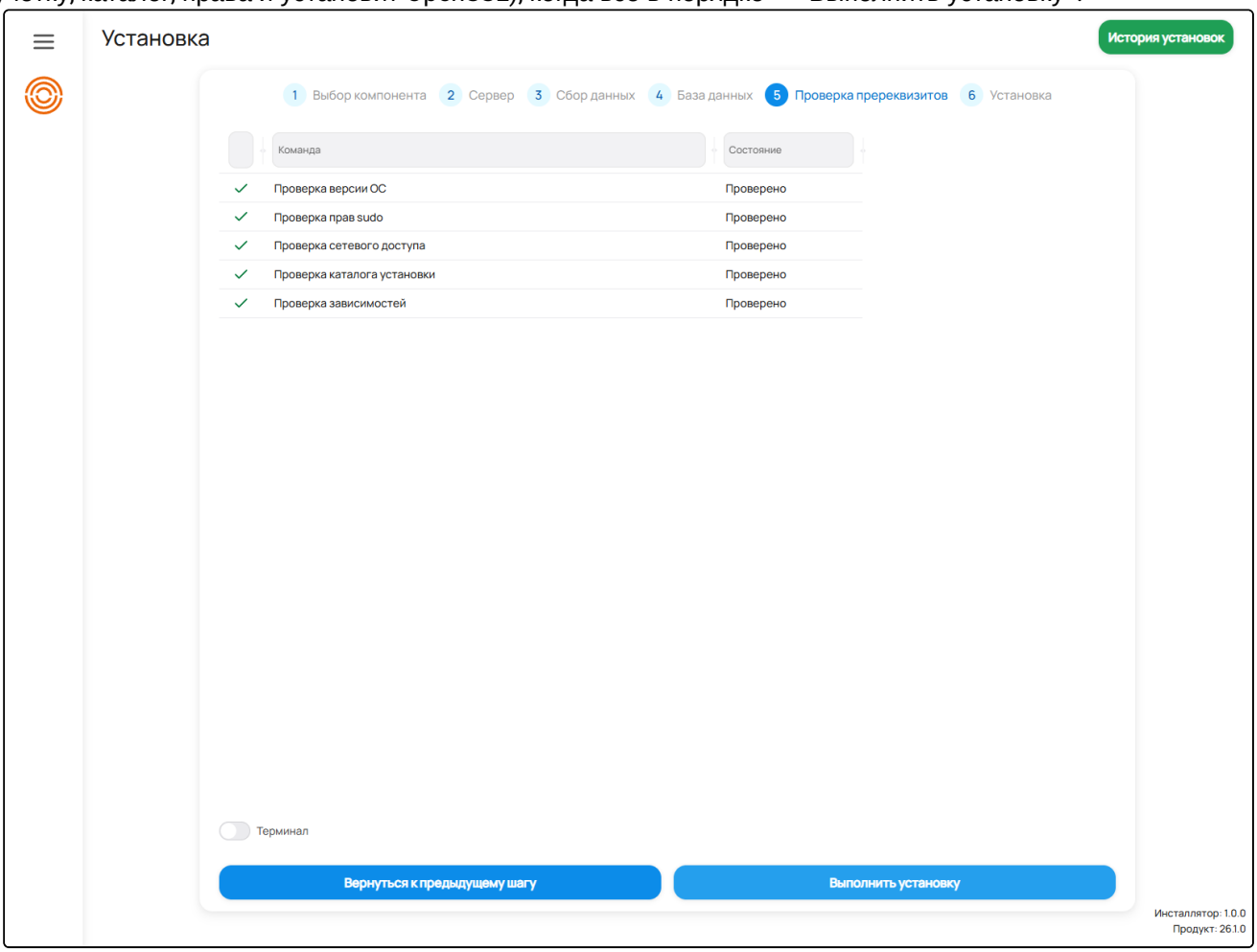
Шаг 3. База данных. Укажите параметры подключения к базе, созданной на предыдущем компоненте: хост, порт (5432), пользователя, пароль и имя БД. Значения хоста, пользователя и имени базы по

умолчанию подставляются из ранее установленной базы данных — введите только пароль.



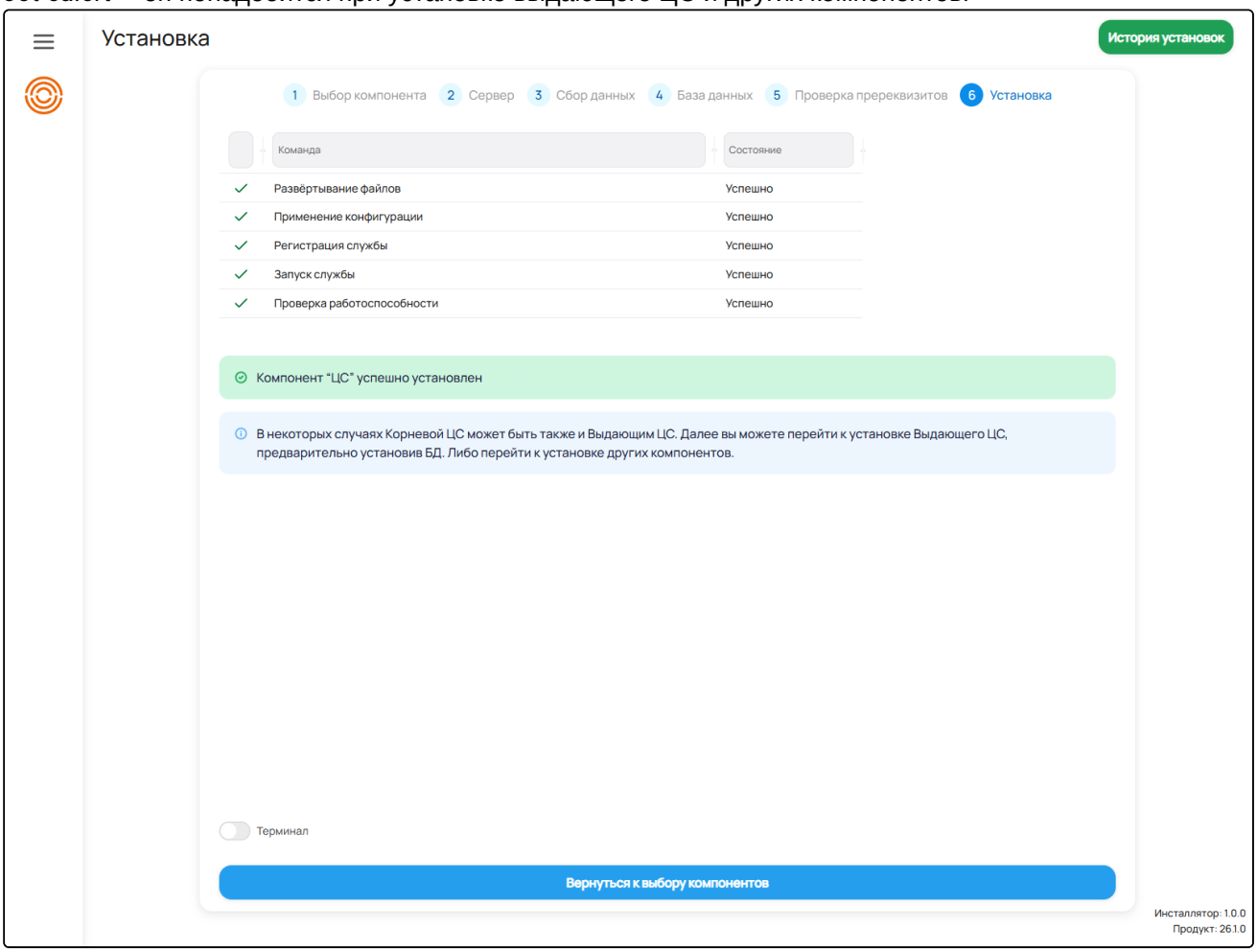
Шаг 4. Проверка пререквизитов. Мастер проверяет: наличие учётной записи itc-svc, каталога установки и его владельца, включение linger для пользователя, наличие OpenSSL и доступность базы данных. При незакрытых пунктах нажмите «Выполнить настройку пререквизитов» (установщик создаст

учётку, каталог, права и установит OpenSSL); когда всё в порядке — «Выполнить установку».



Шаг 5. Установка и результат. Установщик заливает бинарные файлы и конфиг minica.yml, самоподписывает корневой сертификат, поднимает пользовательский сервис minica, заводит шаблоны (tls, subca, ocsp), выпускает TLS-сертификат и включает HTTPS. По завершении доступны для скачивания результаты — корневой сертификат root-ca.crt и его TLS-сертификат root-ca-tls.crt; сохраните

root-ca.crt – он понадобится при установке выдающего ЦС и других компонентов.



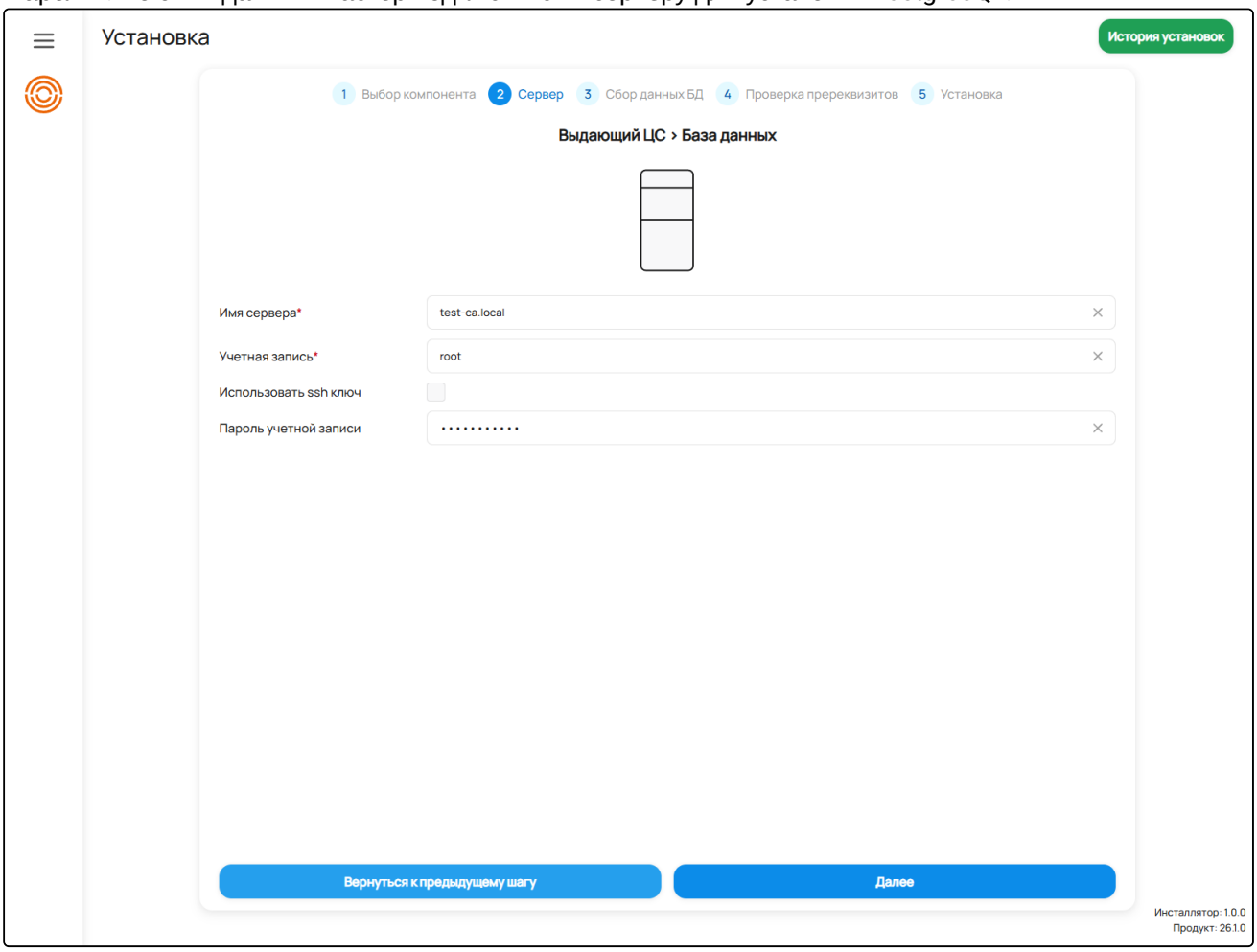
8 Выдающий ЦС

Группа разворачивает подчинённый (выдающий) центр сертификации Clearway CA, который выпускает конечные сертификаты по цепочке доверия от корневого ЦС. Установка выполняется удалённо по SSH и проходит четыре компонента строго по порядку: База данных (PostgreSQL для ЦС), Выдающий ЦС (развёртывание сервиса и выпуск запроса на сертификат CA), Выпуск сертификата (подпись этого запроса на корневом ЦС) и Настройка (загрузка подписанного сертификата, сборка цепочки и запуск сервиса). Технологическая учётная запись по умолчанию — itc-svc, каталог установки ЦС — */opt/itc/minica*, главный конфигурационный файл — *conf/minica.yml*.

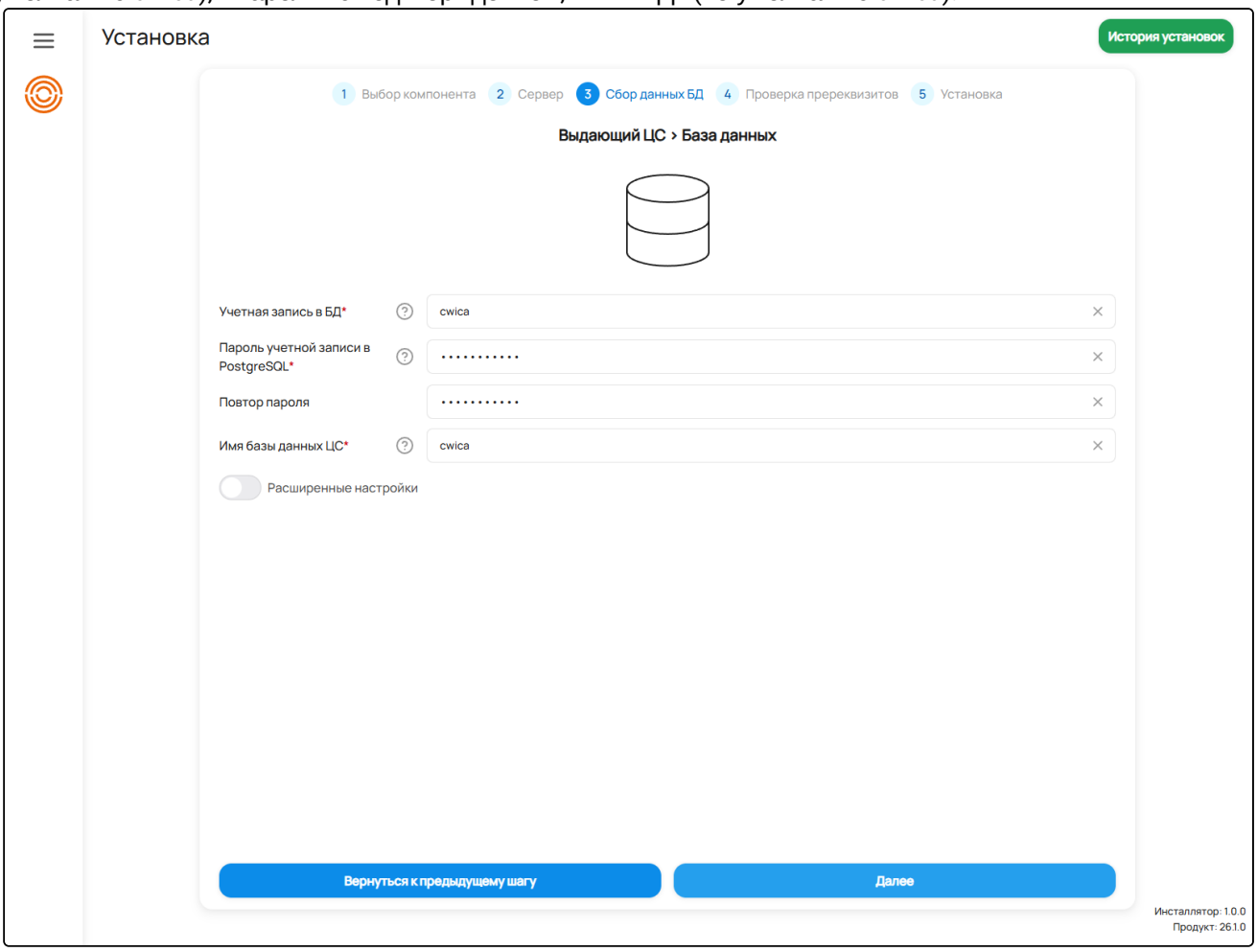
8.1 База данных

Разворачивает базу данных выдающего ЦС на PostgreSQL: устанавливает СУБД (если нужно), создаёт владельца, базу и схему MiniCA.

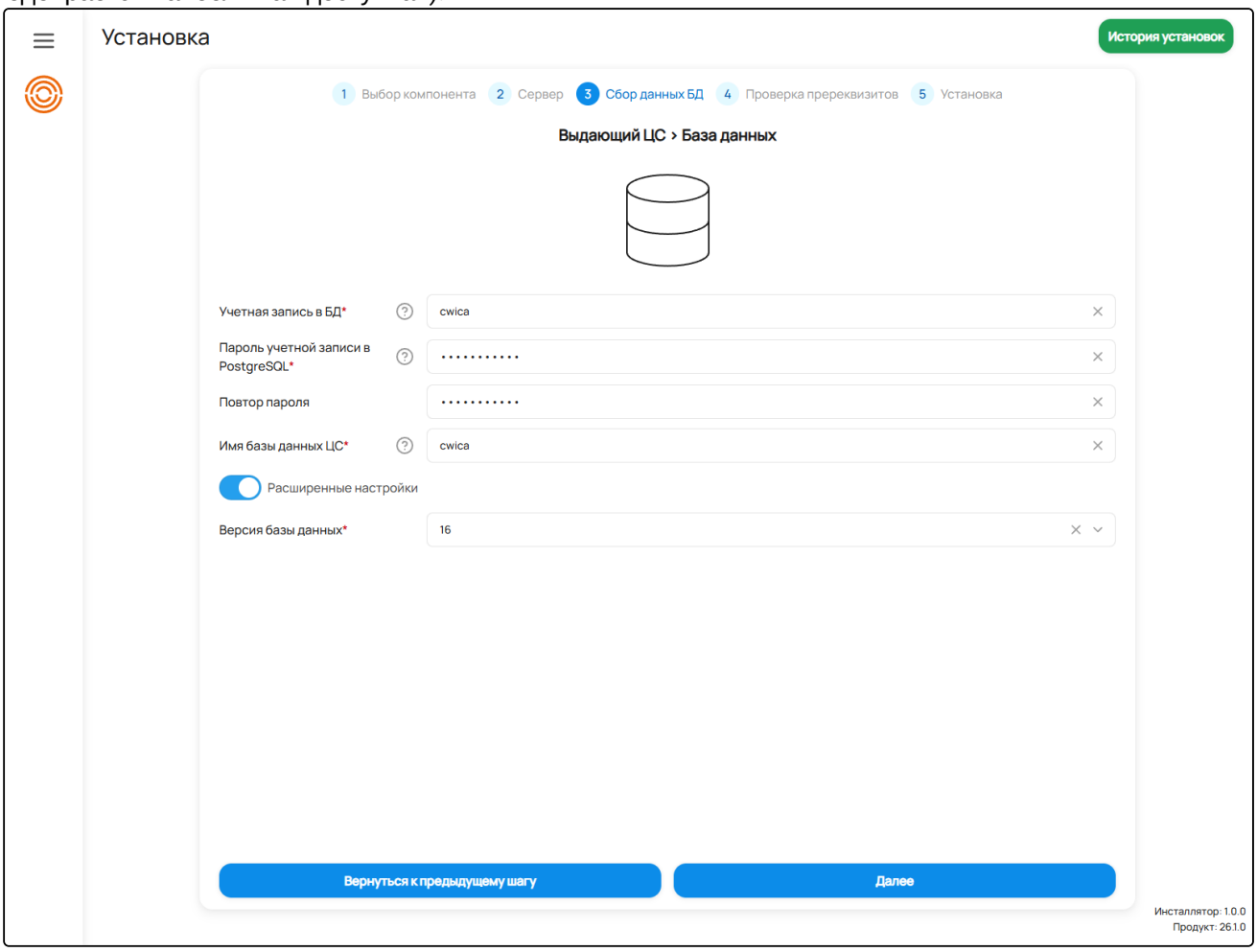
Шаг 1. Сервер. Укажите параметры подключения к серверу базы данных по SSH: «Имя сервера» (адрес хоста), «Учётная запись» и способ входа — установите флажок «Использовать ssh ключ» либо введите «Пароль». По этим данным мастер подключится к серверу для установки PostgreSQL.



Шаг 2. Сбор данных БД. Заполните параметры базы данных: «Пользователь БД» (владелец, по умолчанию cwica), «Пароль» с подтверждением, «Имя БД» (по умолчанию cwica).

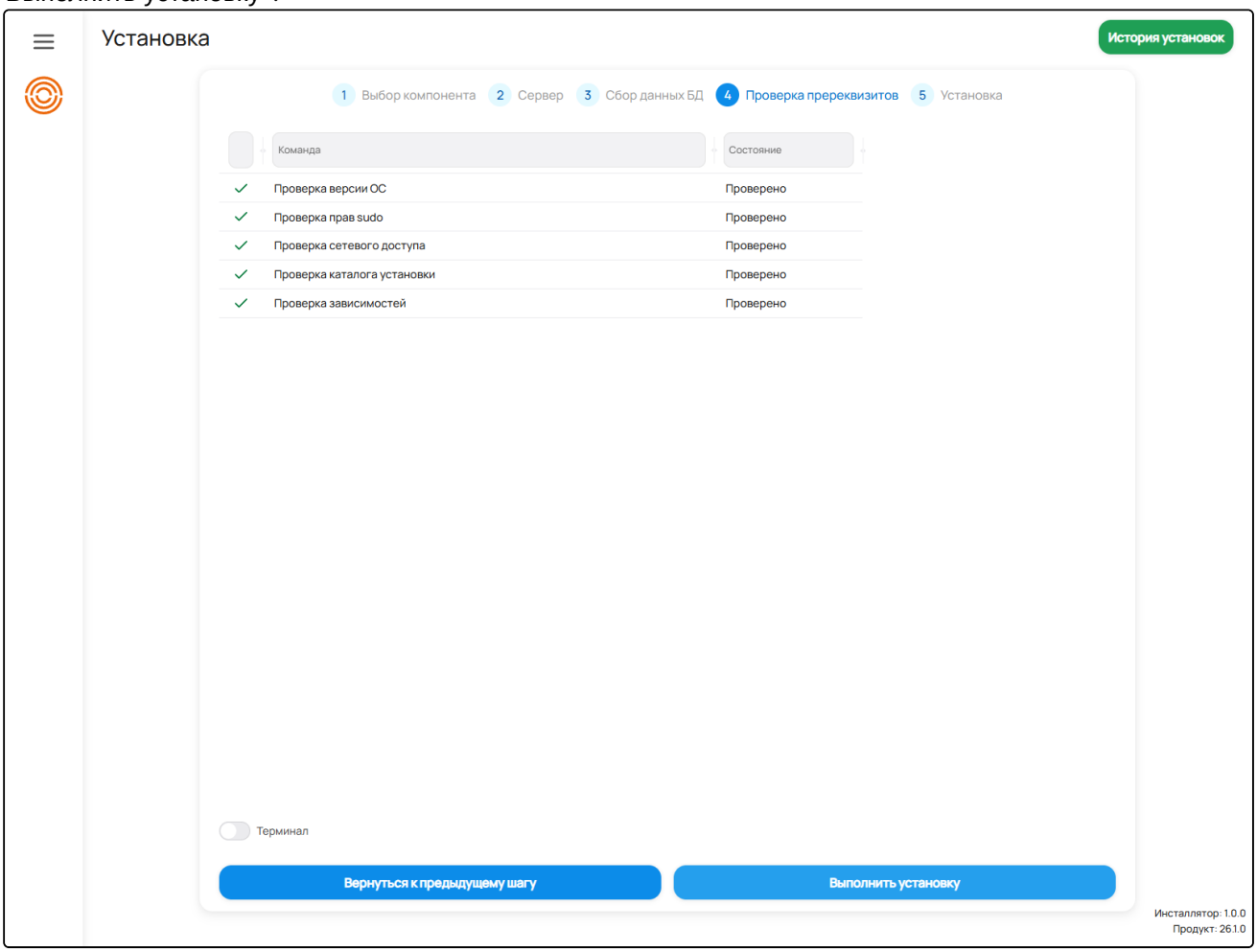


Прокрутите форму ниже, чтобы задать «Версию PostgreSQL» (поддерживаются 11–18; по умолчанию подбирается наибольшая доступная).

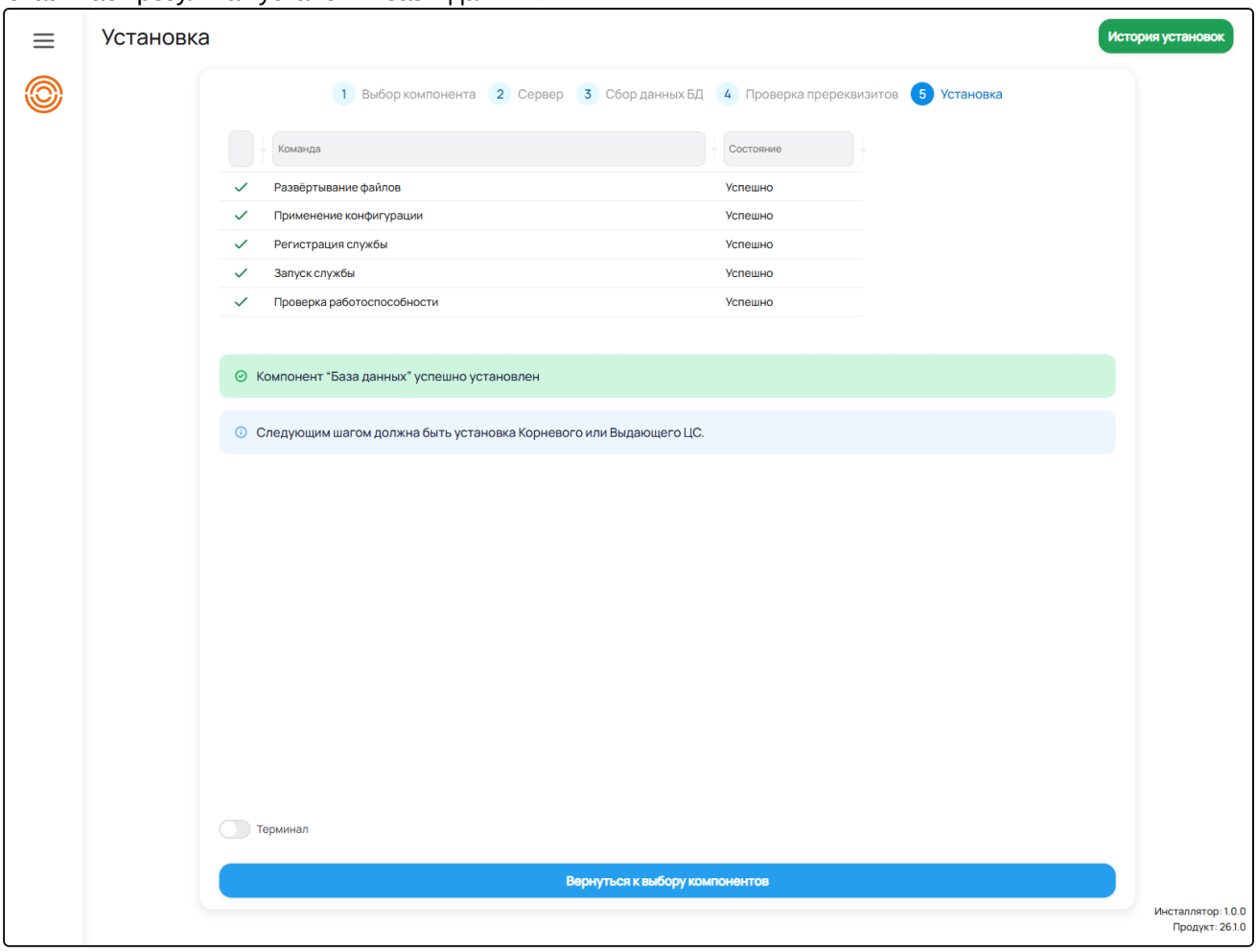


Шаг 3. Проверка пререквизитов. Мастер выводит таблицу проверок: установлен ли PostgreSQL, наличие учётной записи и базы данных, отсутствие таблиц, права пользователя. Если есть незакрытые пункты, нажмите «Выполнить настройку пререквизитов»; когда все проверки пройдены — нажмите

«Выполнить установку».



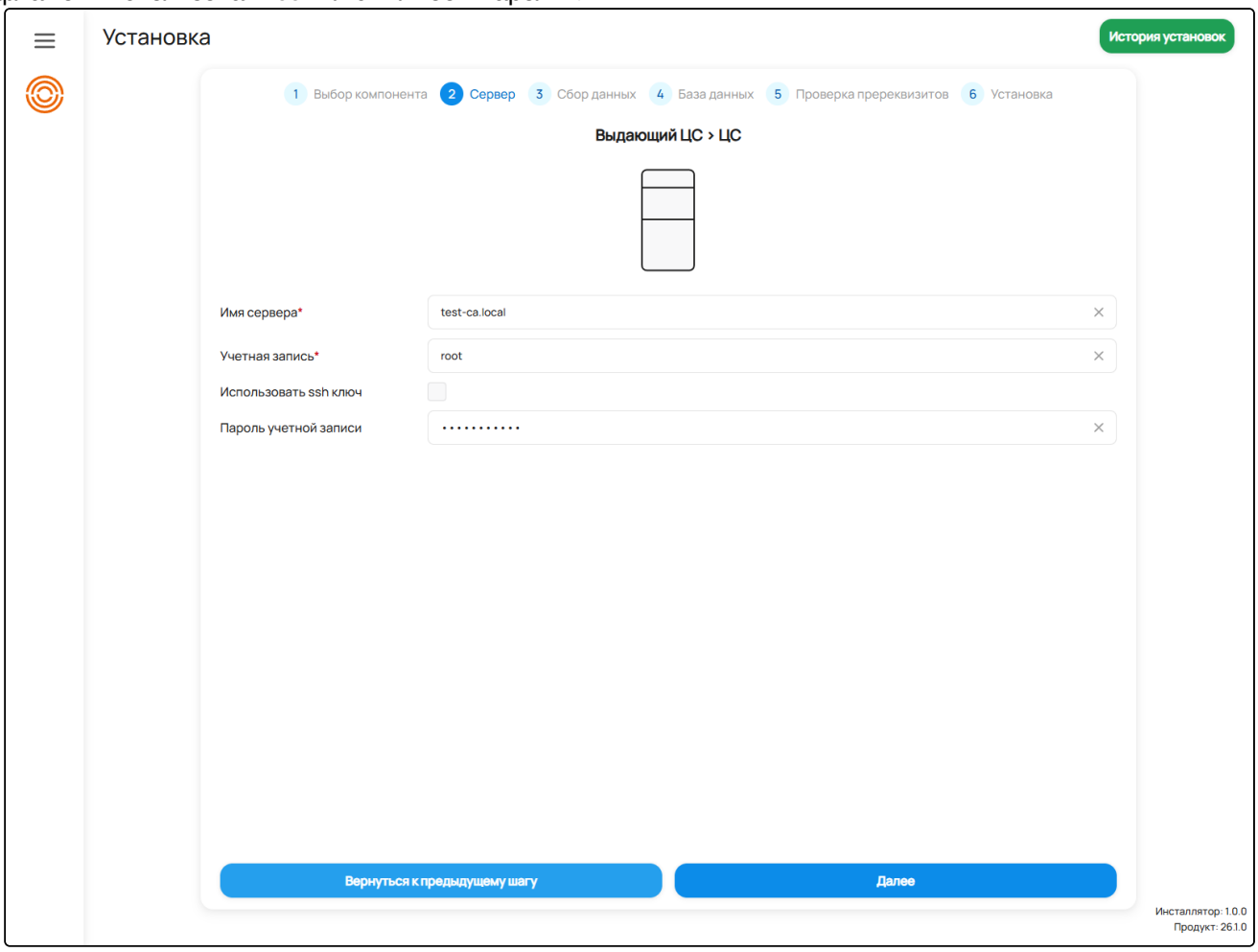
Шаг 4. Установка и результат. Мастер применяет схему MiniCA (таблицы csr, cert, crl, templ, jwt, evt) и показывает результат установки базы данных.



8.2 Выдающий ЦС

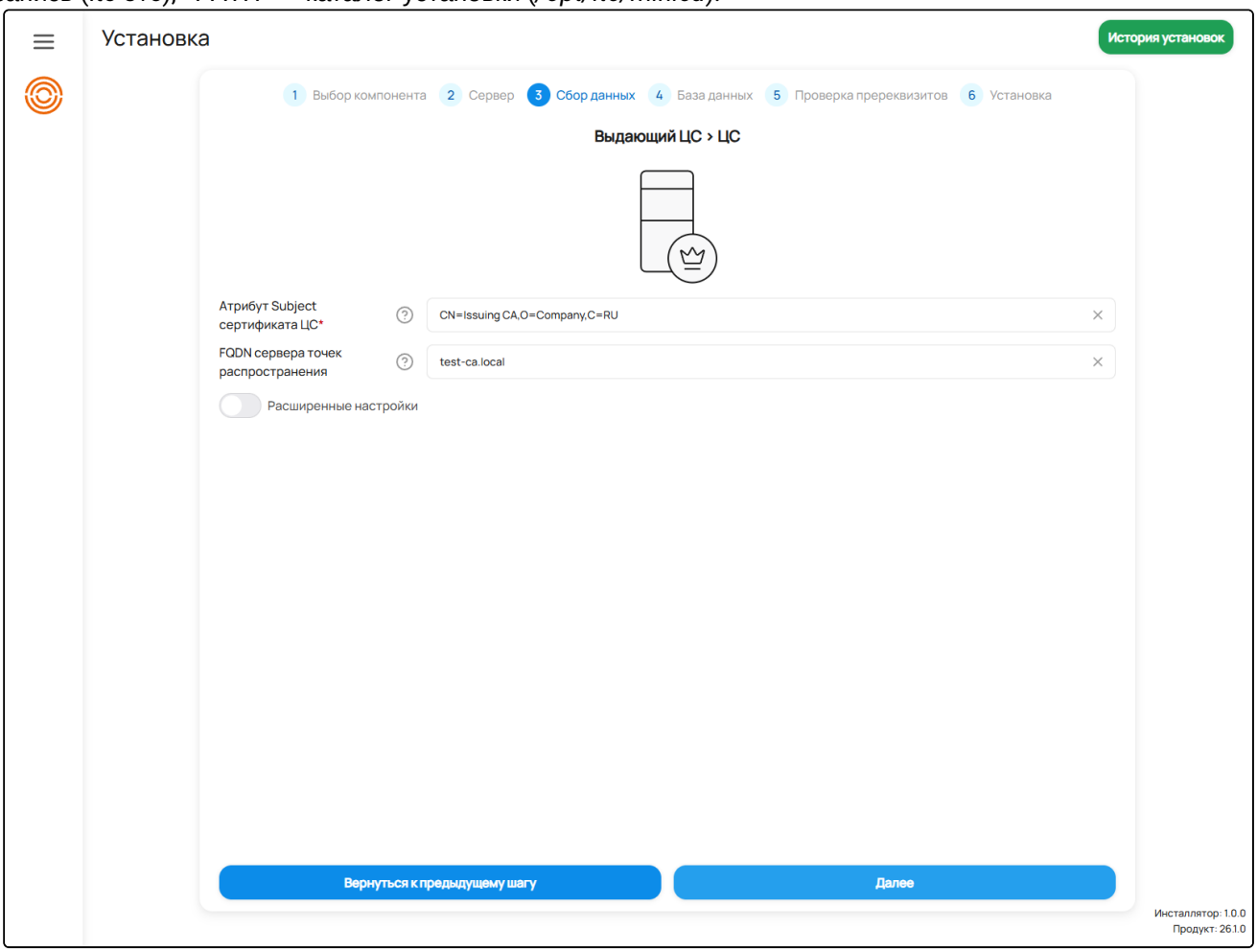
Разворачивает сервис выдающего ЦС на MiniCA и выпускает запрос на сертификат (CSR) для подписания на корневом ЦС; сам сертификат CA пока не создаётся, сервис останавливается до этапа настройки.

Шаг 1. Сервер. Укажите сервер выдающего ЦС: «Имя сервера», «Учётная запись» и способ входа — флажок «Использовать ssh ключ» либо «Пароль».



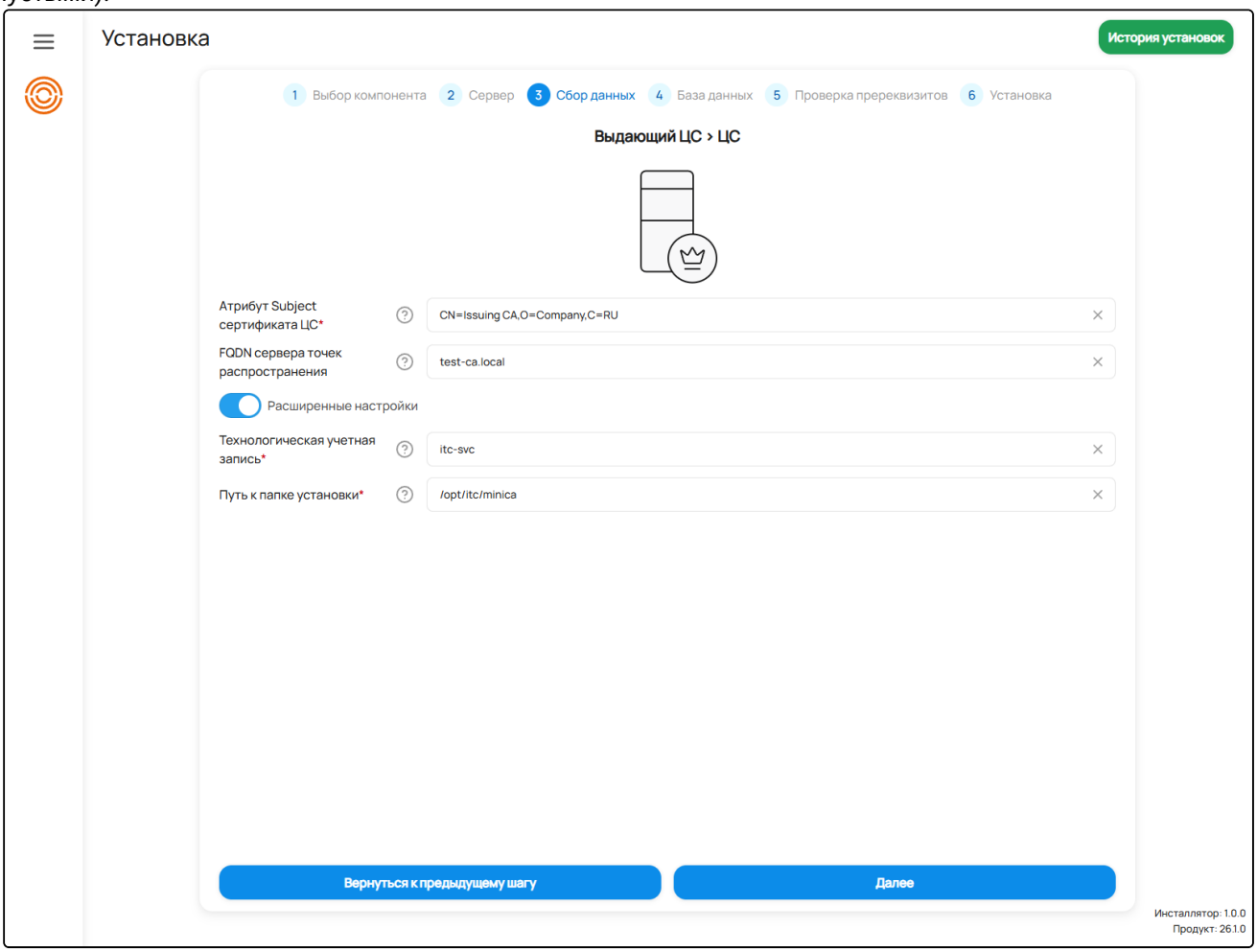
Шаг 2. Сбор данных. Заполните переменные ЦС: «Subject» — DN сертификата выдающего ЦС (по умолчанию CN=Issuing CA,O=Company,C=RU), «HOSTNAME» — имя, на которое выпускается TLS-сертификат и по которому mclient обращается к серверу, «USER_NAME» — технологическая учётная

запись (itc-svc), «PATH» – каталог установки (*/opt/itc/minica*).



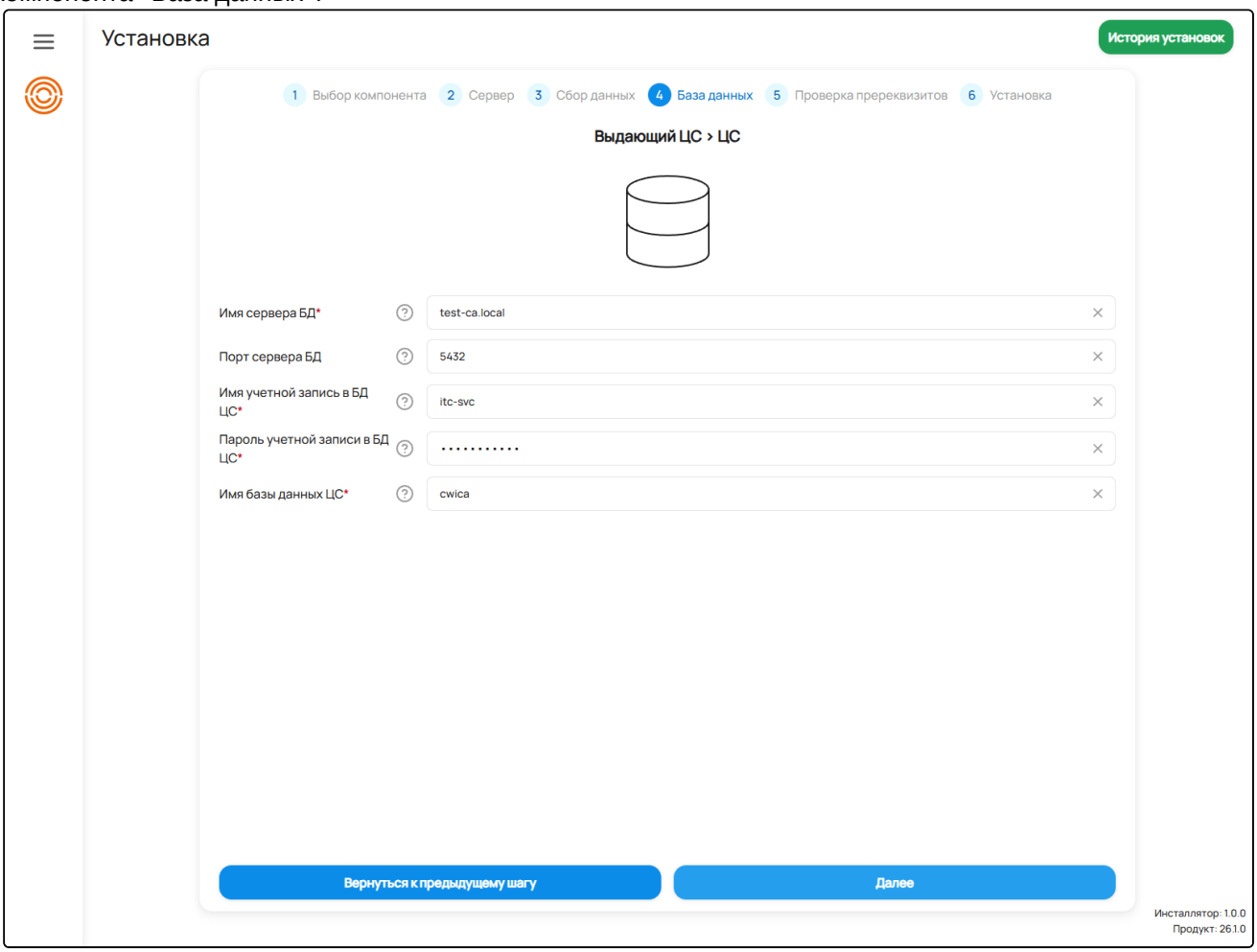
Прокрутите форму, чтобы указать «CDP_SERVER_NAME» – FQDN, который прописывается в точки распространения CRL и AIA выпускаемых сертификатов (если оставить пустым, эти списки будут

пустыми).



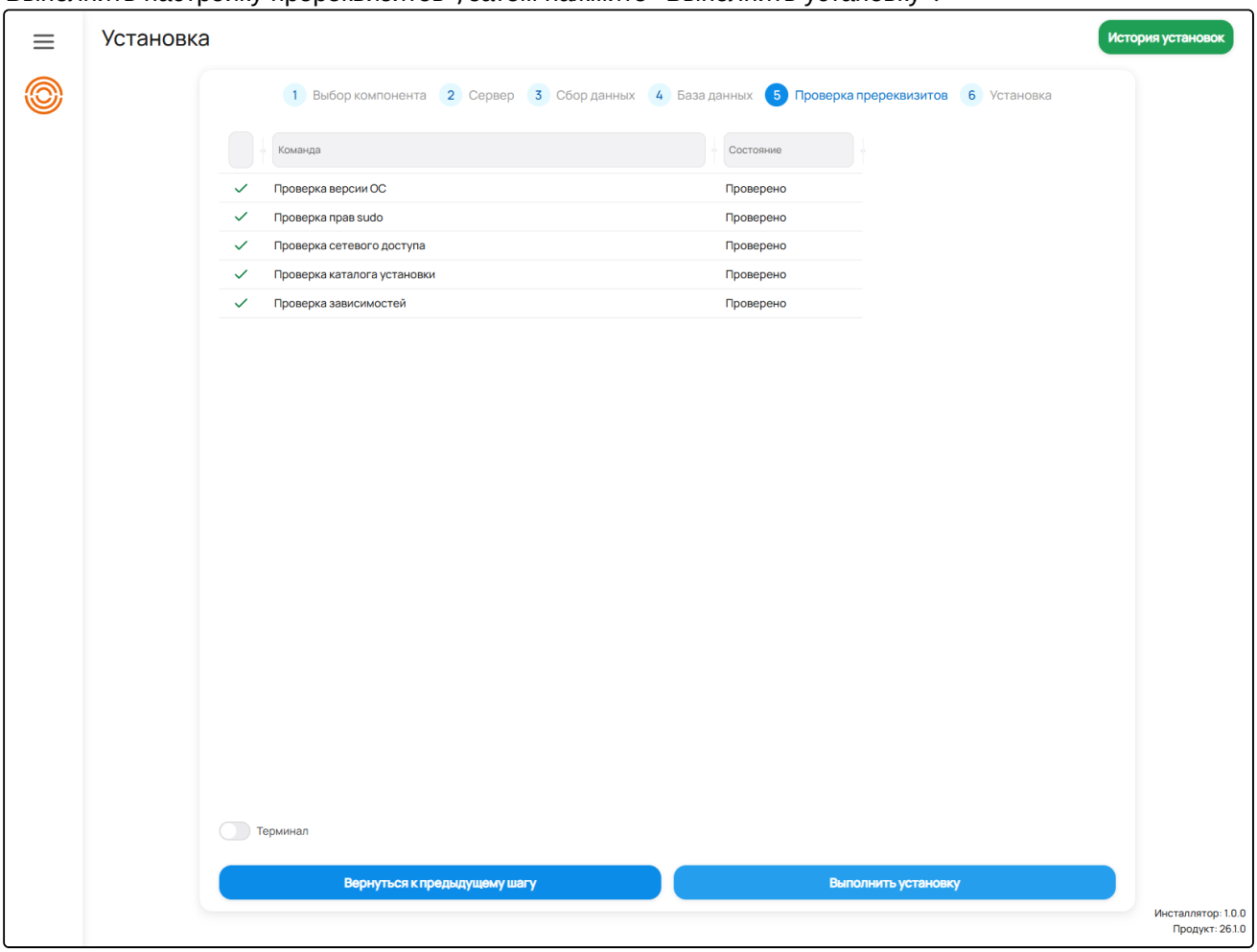
Шаг 3. База данных. Укажите параметры подключения к базе данных ЦС: хост, порт (5432), пользователь и пароль, имя БД. По умолчанию значения подставляются из ранее установленного

компонента «База данных».



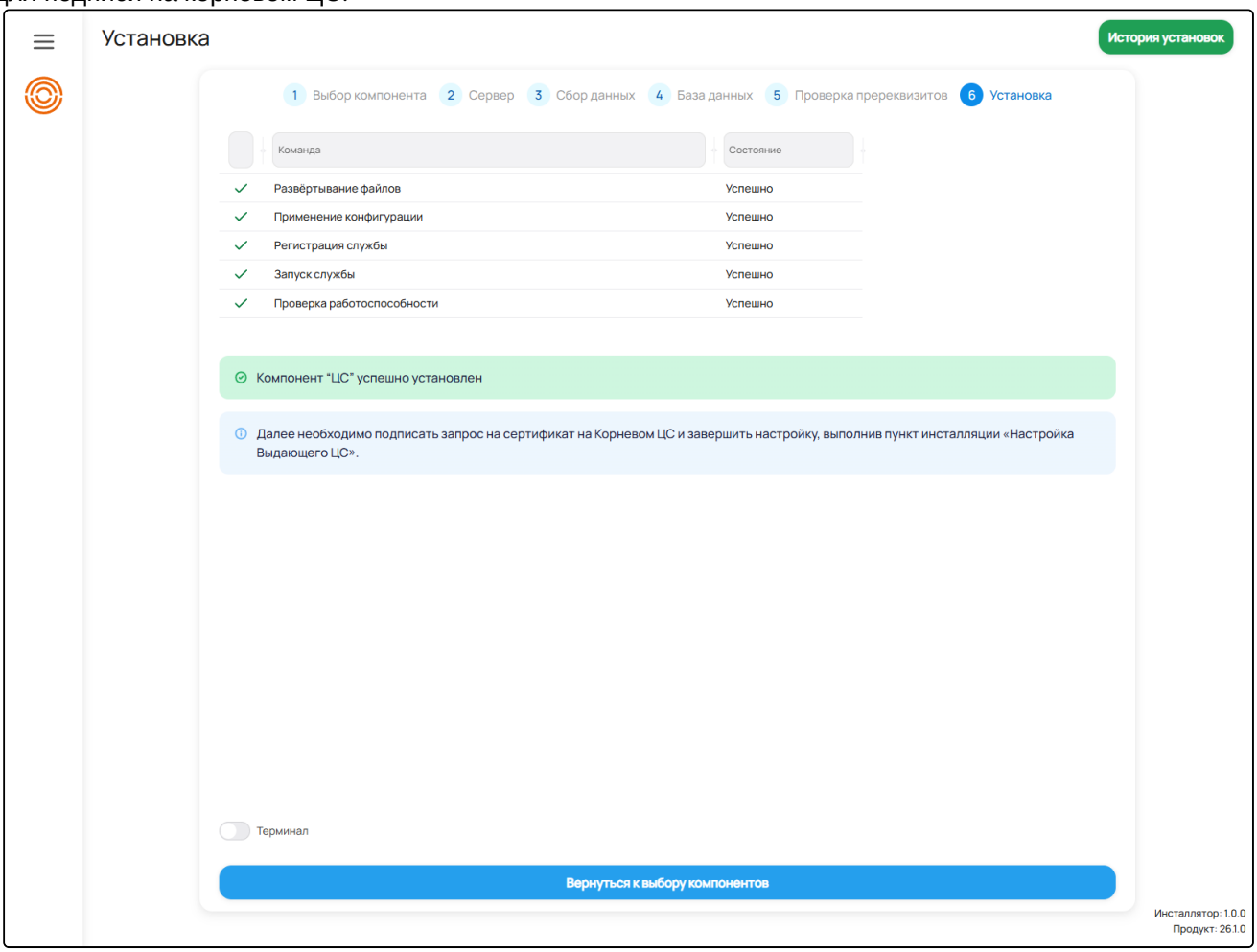
Шаг 4. Проверка пререквизитов. Мастер проверяет наличие учётной записи и каталога, права владельца, enable-linger, наличие OpenSSL и подключение к БД. Незакрытые пункты закройте кнопкой

«Выполнить настройку пререквизитов», затем нажмите «Выполнить установку».



Шаг 5. Установка и результат. Мастер разворачивает сервис, формирует ключ и запрос на сертификат CA. По завершении скачайте файл-результат — запрос sub-ca.csr; он потребуется на следующем шаге

для подписи на корневом ЦС.



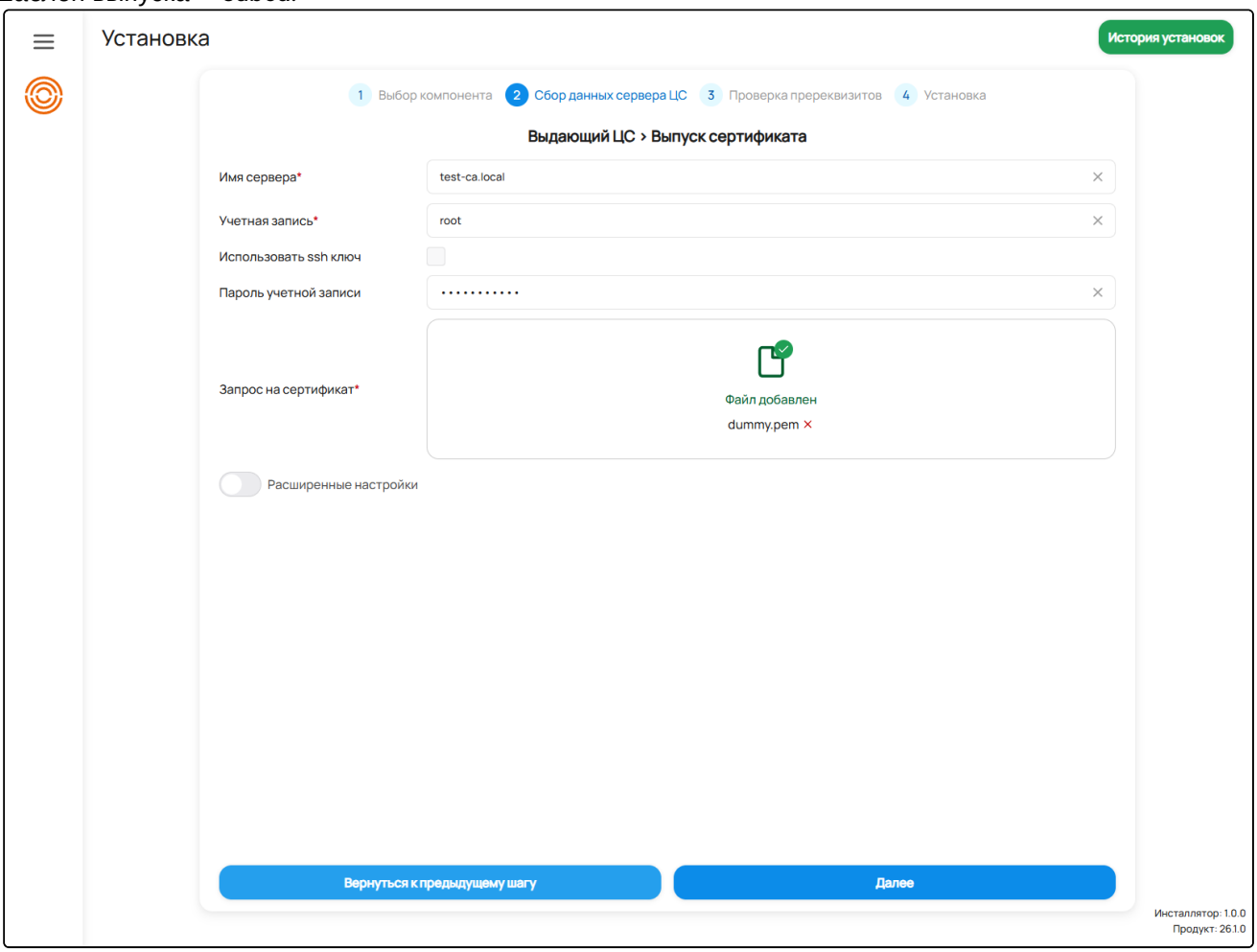
8.3 Выпуск сертификата

Служебный компонент: подключается к серверу корневого ЦС и через mclient подписывает запрос sub-ca.csr, выпуская сертификат выдающего ЦС.

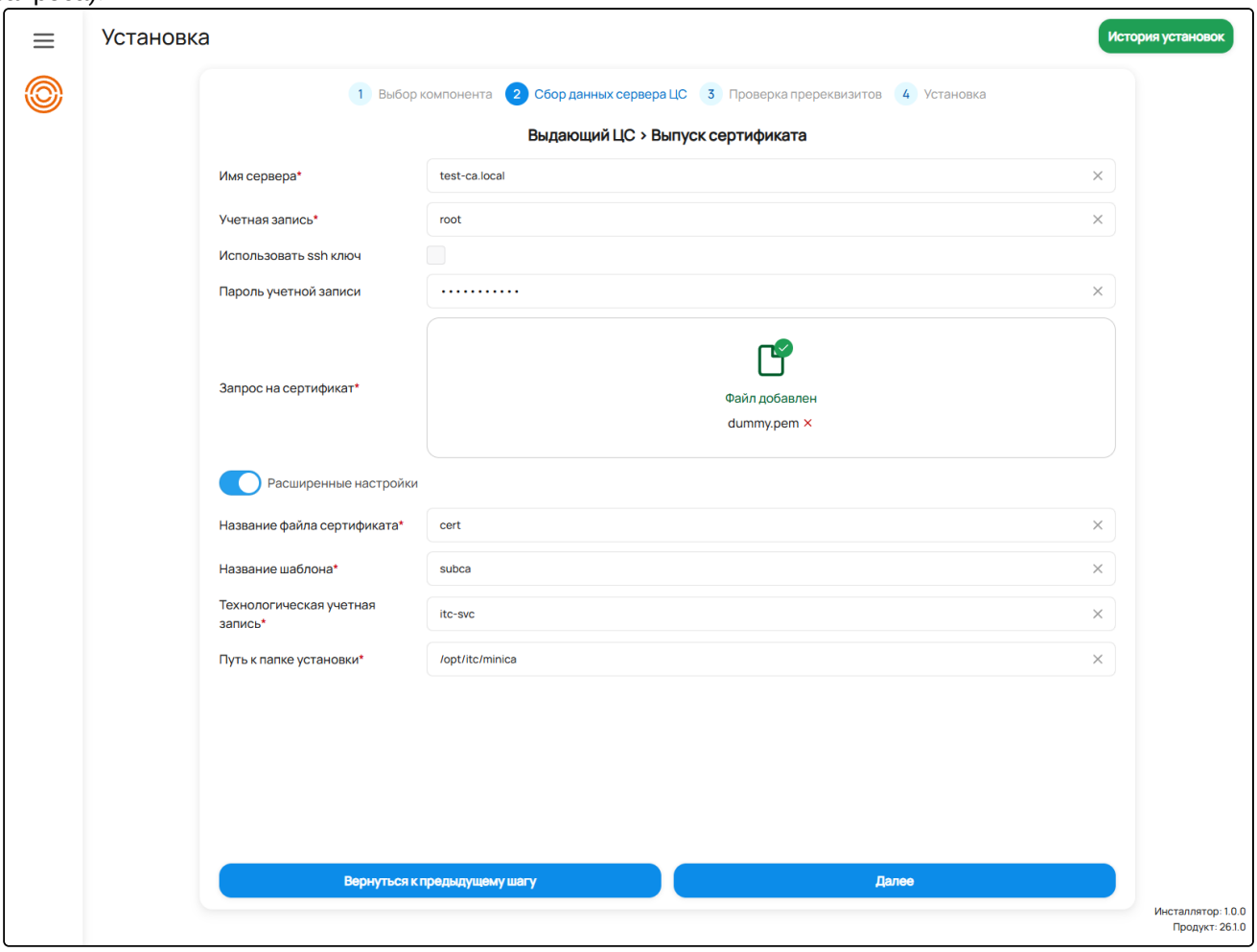
Когда можно пропустить: пропустите этот компонент, если сертификат выдающего ЦС подписывается во внешнем корневом ЦС, а не в Clearway CA. Скачайте файл sub-ca.csr, сформированный на предыдущем этапе, подпишите его во внешнем ЦС и на этапе «Настройка» вручную загрузите полученный сертификат в поле «CA». Сертификат должен соответствовать приватному ключу, оставшемуся на сервере выдающего ЦС.

Шаг 1. Сбор данных сервера ЦС. Укажите сервер корневого ЦС и его параметры: учётную запись USER_NAME, каталог PATH. В поле запроса подставляется CSR, полученный на предыдущем шаге;

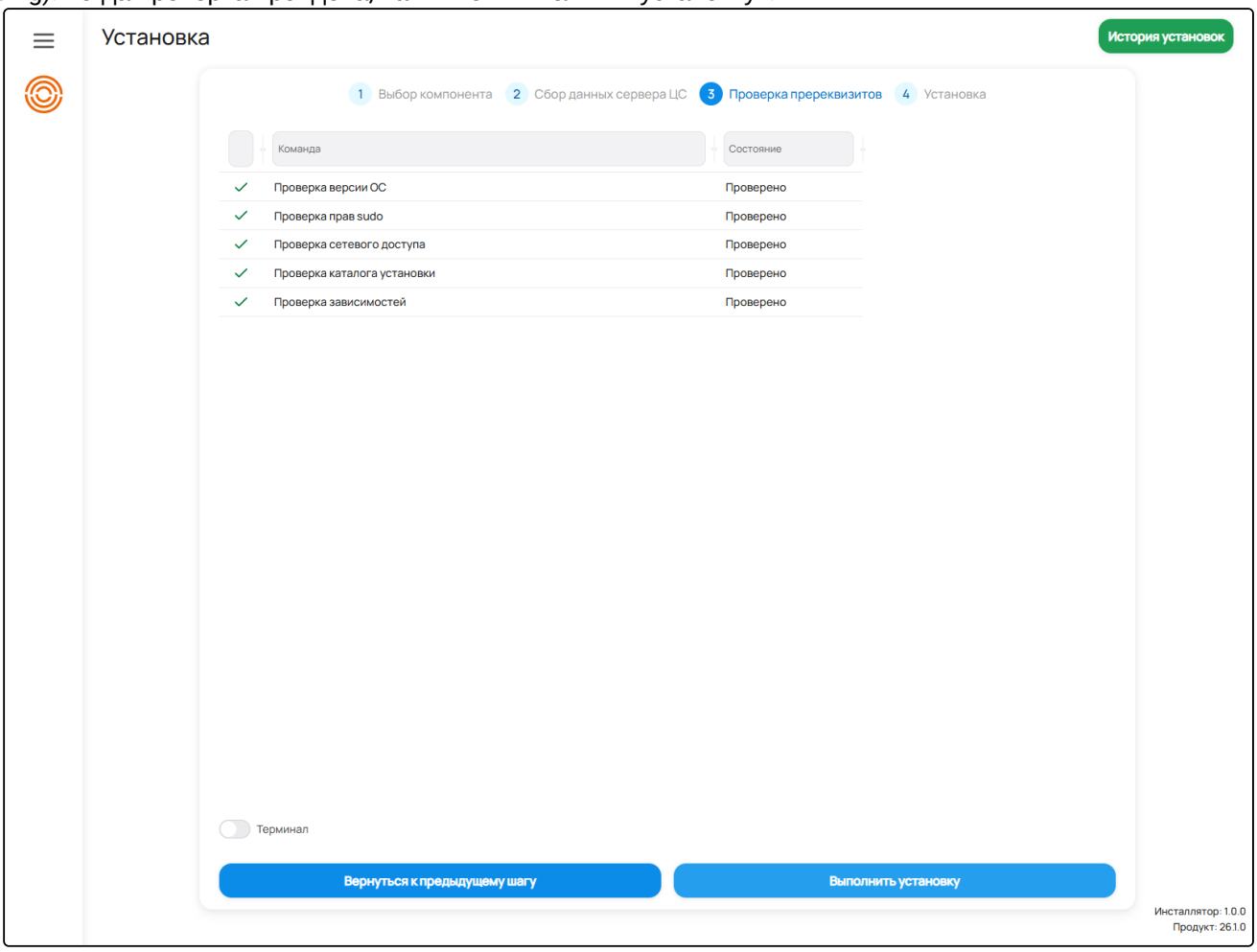
шаблон выпуска – subca.



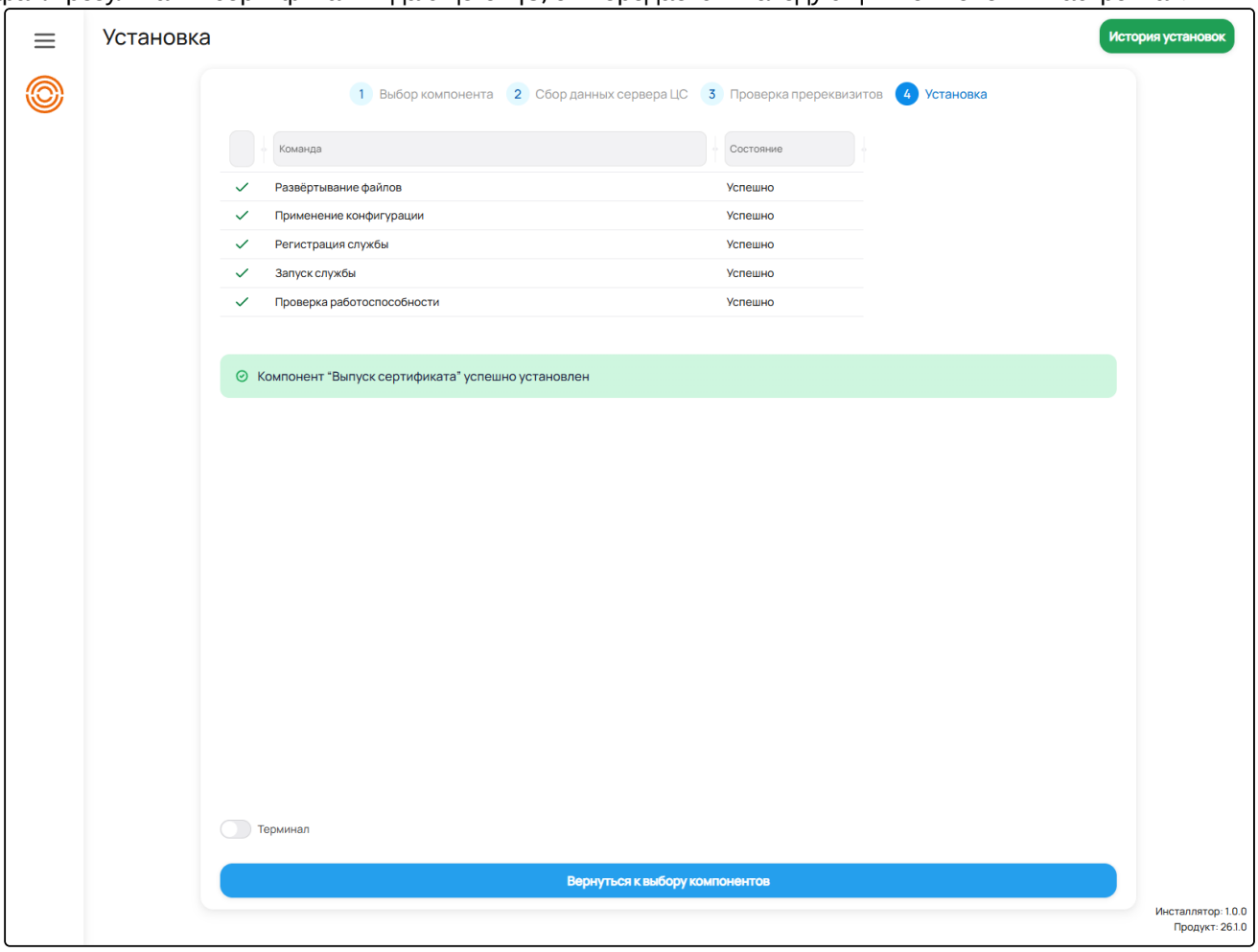
Прокрутите форму, чтобы проверить остальные поля выпуска (имя файла результата и содержимое запроса).



Шаг 2. Проверка пререквизитов. Мастер проверяет, что корневой ЦС установлен и доступен (mclient ping). Когда проверка пройдена, нажмите «Выполнить установку».



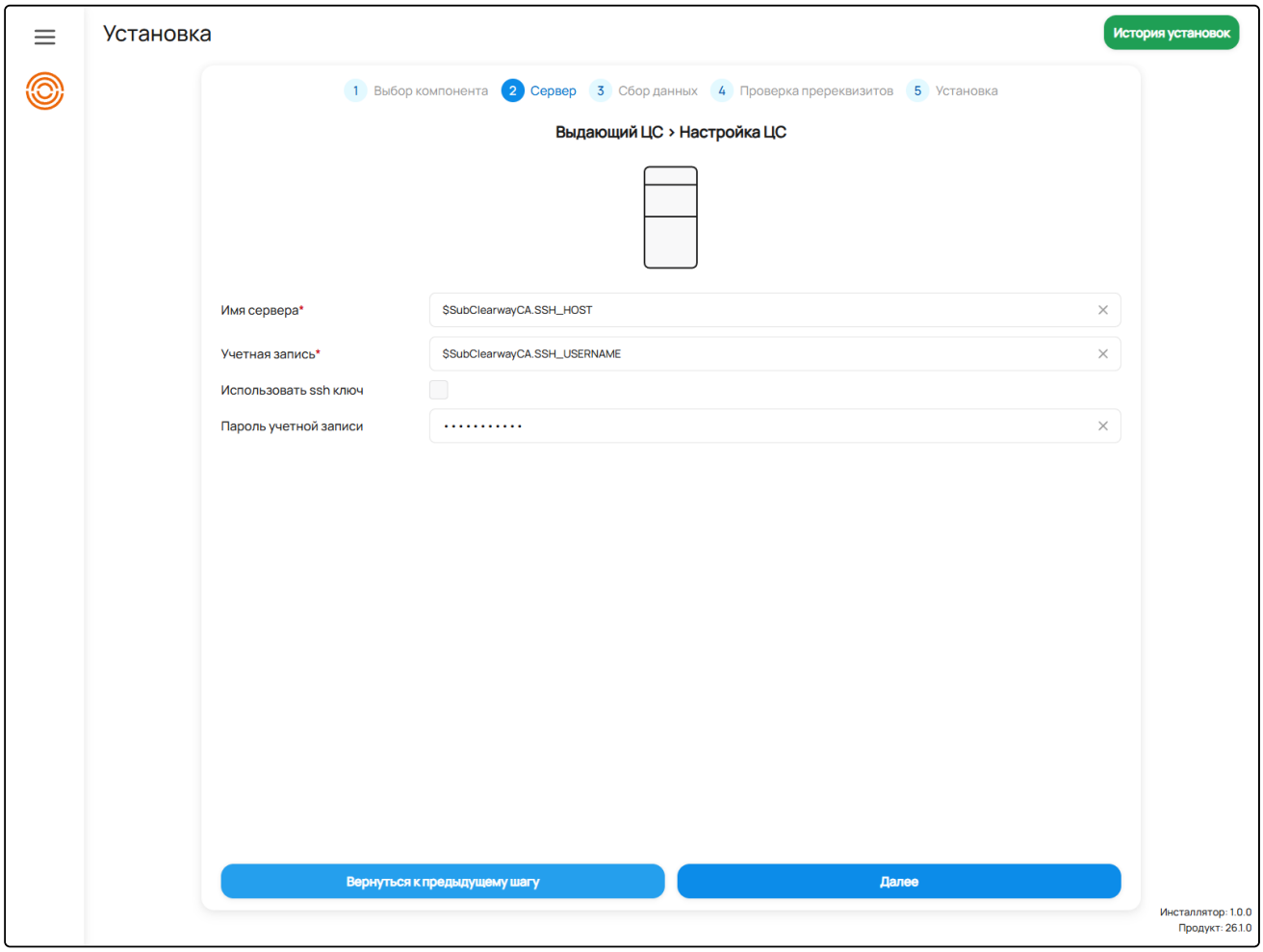
Шаг 3. Установка и результат. Корневой ЦС подписывает запрос и возвращает сертификат. Скачайте файл-результат — сертификат выдающего ЦС; он передаётся в следующий компонент «Настройка».



8.4 Настройка

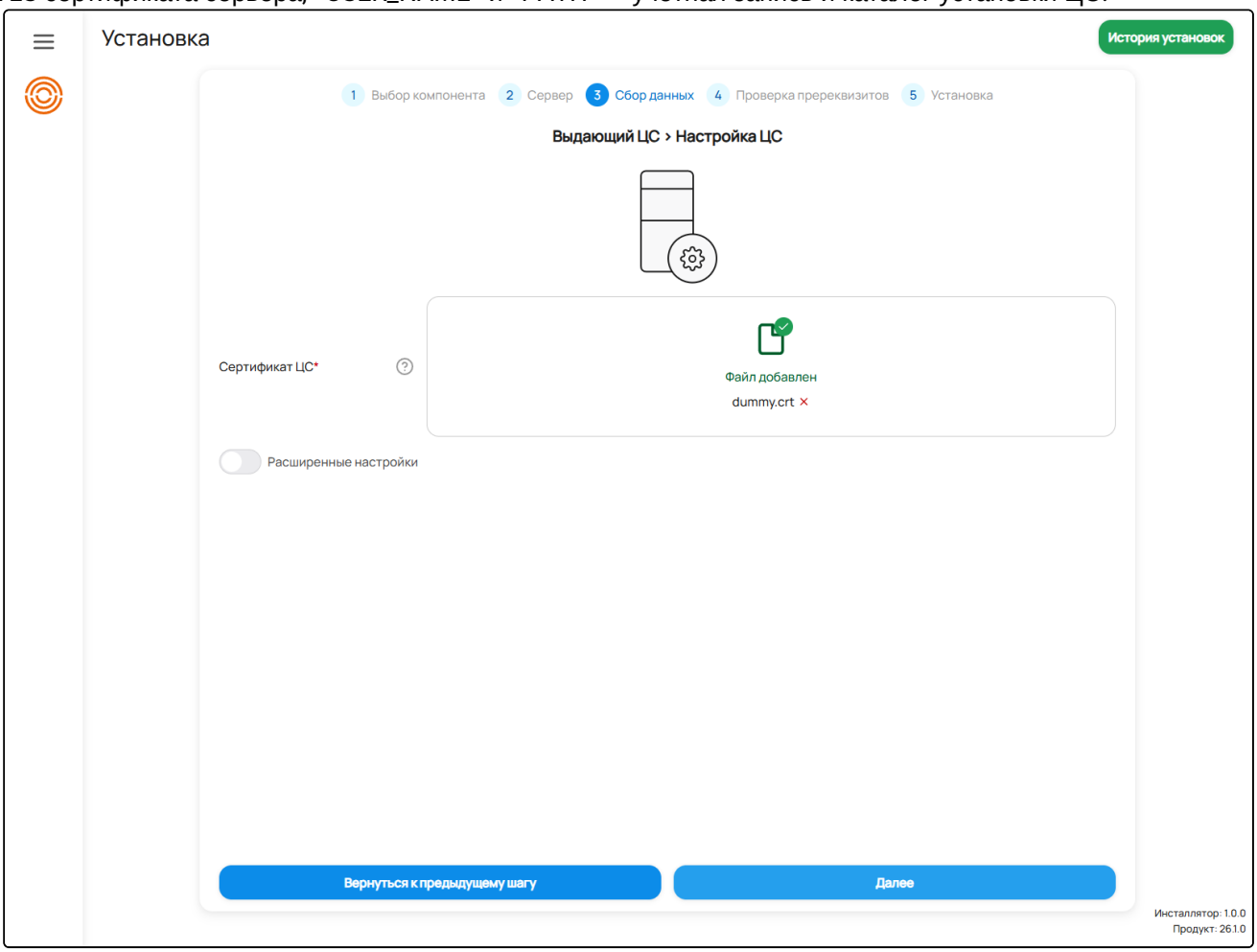
Завершает развёртывание: загружает подписанный сертификат на выдающий ЦС, собирает цепочку доверия chain.pem, включает TLS и запускает сервис.

Шаг 1. Сервер. Укажите сервер выдающего ЦС: «Имя сервера», «Учётная запись» и способ входа — флажок «Использовать ssh ключ» либо «Пароль». Обычно это тот же сервер, что и на этапе выпуска запроса.

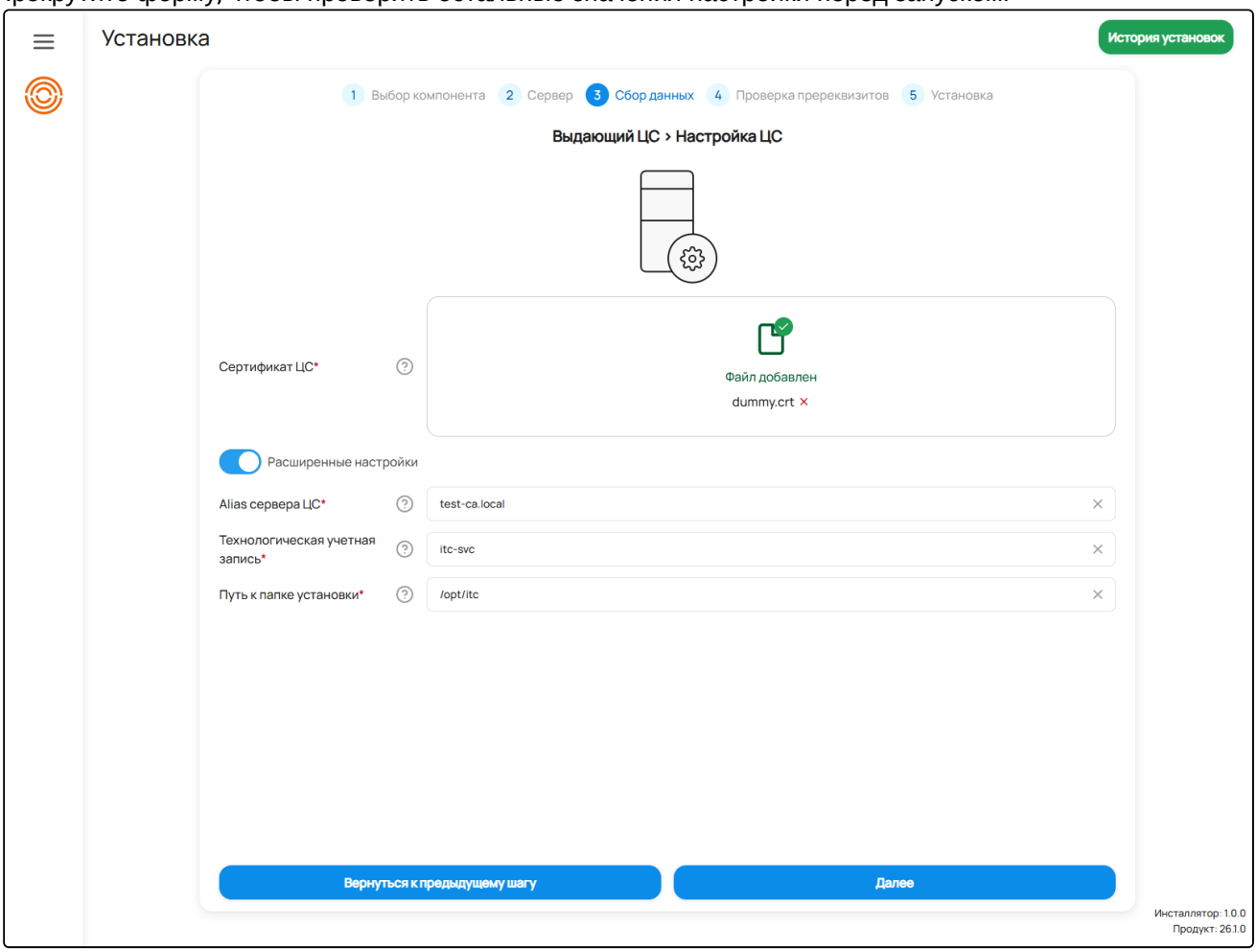


Шаг 2. Сбор данных. Укажите ключевые поля: «CA» — файл сертификата выдающего ЦС (по умолчанию берётся результат предыдущего шага «Выпуск сертификата»), «HOSTNAME» — имя для

TLS-сертификата сервера, «USER_NAME» и «PATH» – учётная запись и каталог установки ЦС.

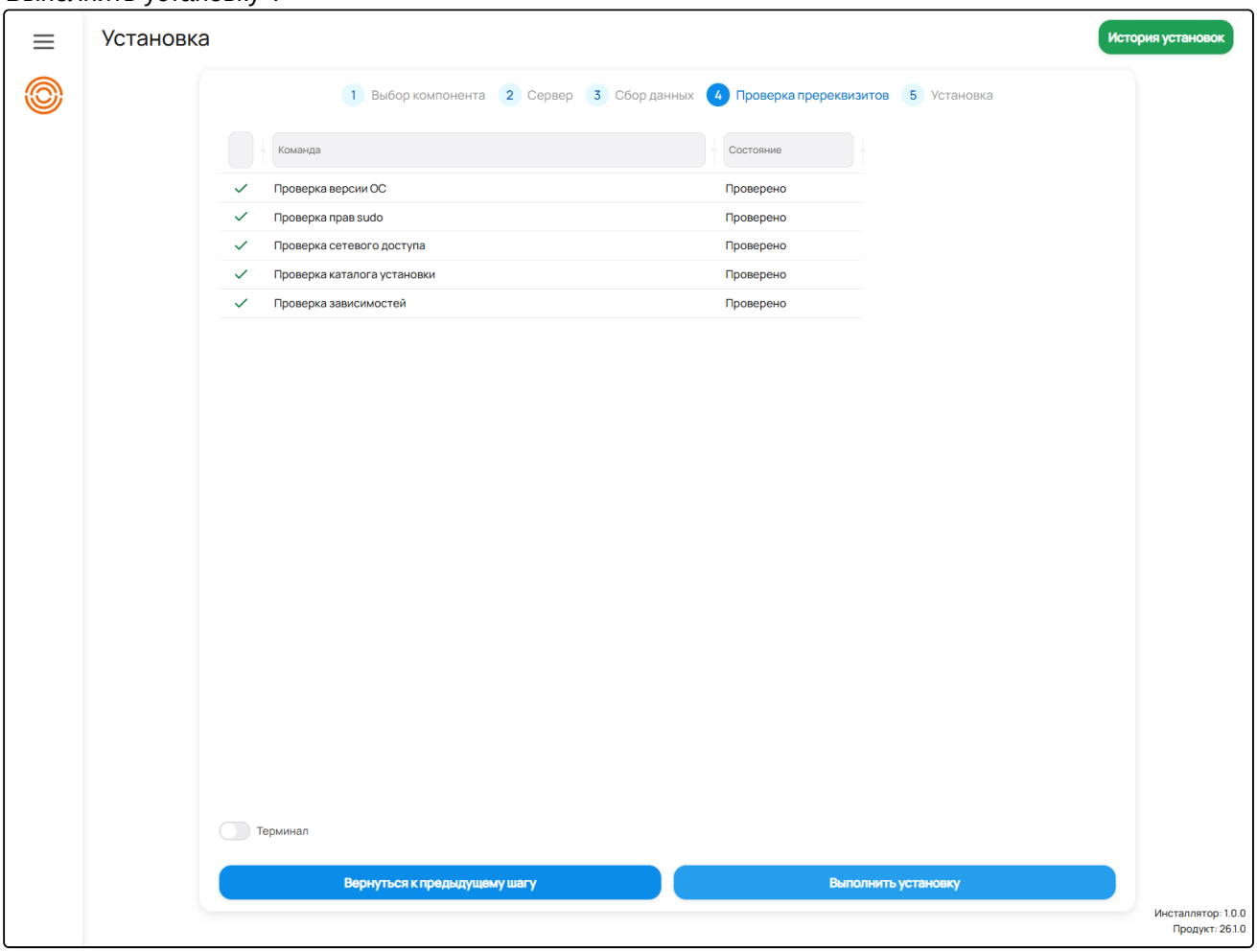


Прокрутите форму, чтобы проверить остальные значения настройки перед запуском.



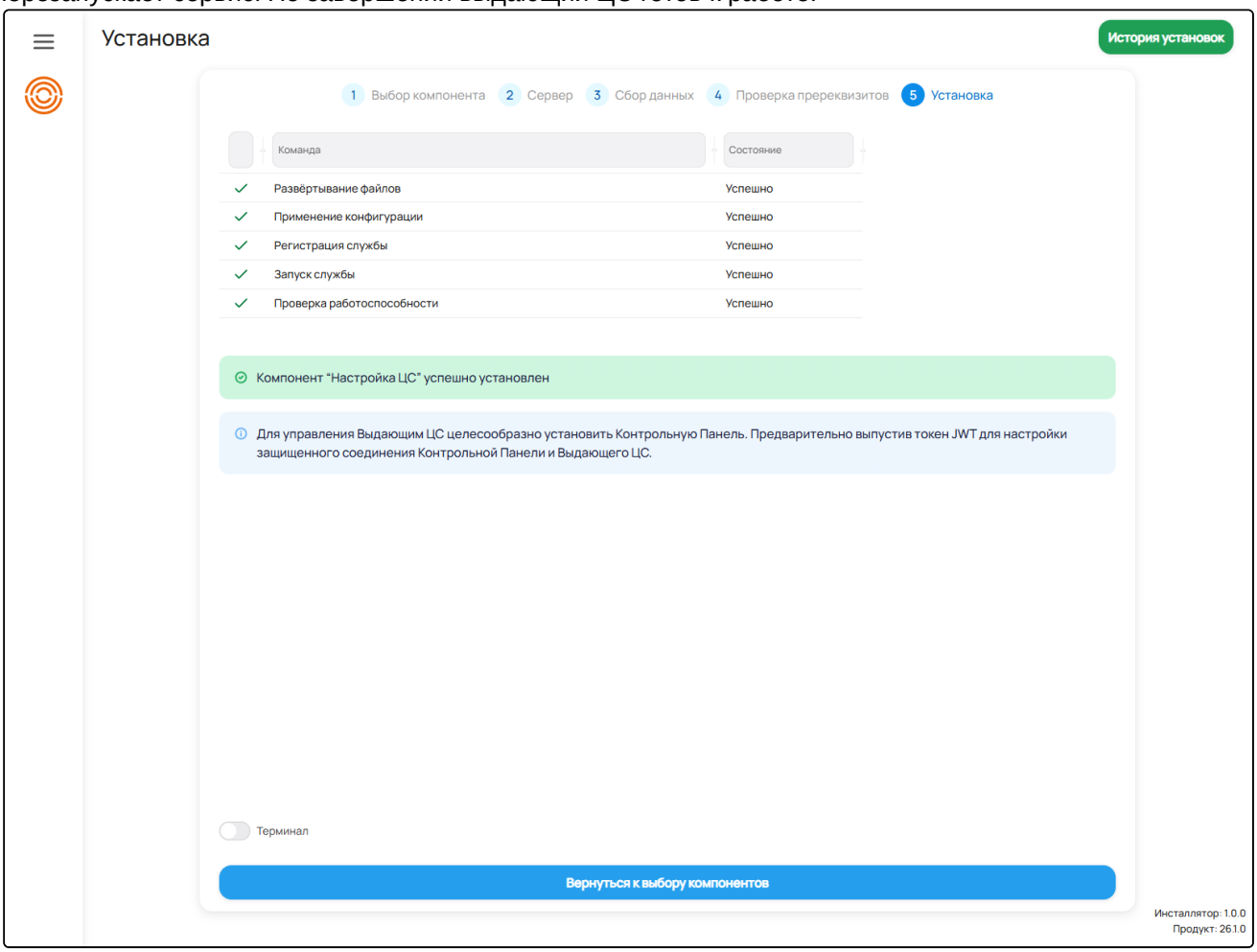
Шаг 3. Проверка пререквизитов. Мастер проверяет наличие учётной записи, каталога и прав. Незакрытые пункты закройте кнопкой «Выполнить настройку пререквизитов», затем нажмите

«Выполнить установку».



Шаг 4. Установка и результат. Мастер загружает сертификат в ca/ca.crt, собирает цепочку chain.pem (корневой + выдающий), включает TLS (https://<HOSTNAME>:9443), создаёт шаблоны выпуска и

перезапускает сервис. По завершении выдающий ЦС готов к работе.



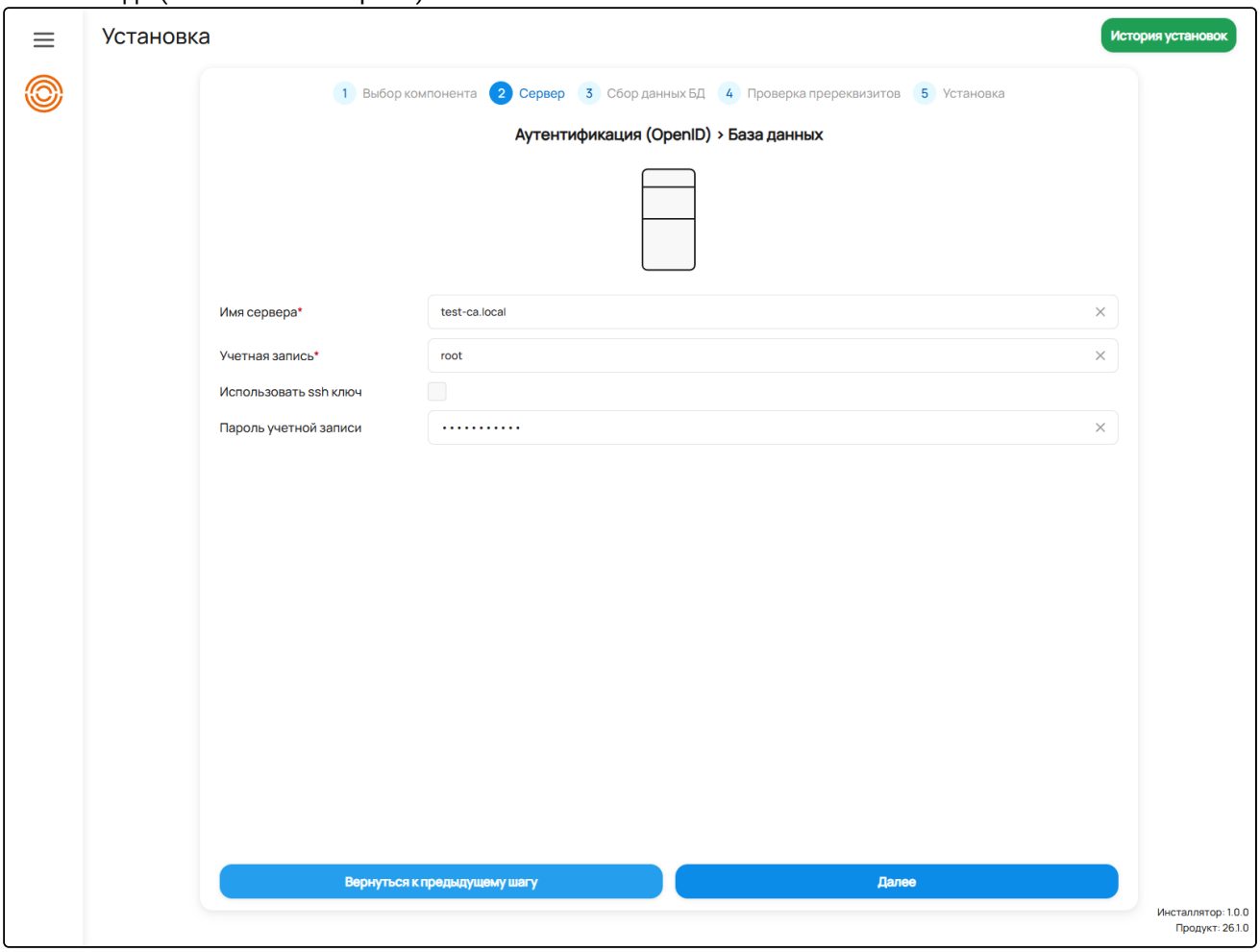
9 Аутентификация (OpenID)

Группа разворачивает провайдер аутентификации OpenID Connect — единую точку входа (Single Sign-On) для веб-сервисов Clearway CA (Контрольная панель, Сервис публикации, SCEP и др.). По умолчанию для входа используется встроенная статическая учётная запись администратора; интеграция с внешним каталогом LDAP/Active Directory выполняется отдельным необязательным компонентом. Компоненты устанавливаются в следующем порядке: «База данных» (создание базы PostgreSQL для сервиса), «Выпуск запроса на TLS» (генерация ключа и CSR), «Выпуск сертификата» (подпись CSR на действующем ЦС), «Установка» (развёртывание и запуск сервиса OpenID) и «Интеграция с LDAP» (необязательное подключение внешнего каталога пользователей и групп).

9.1 База данных

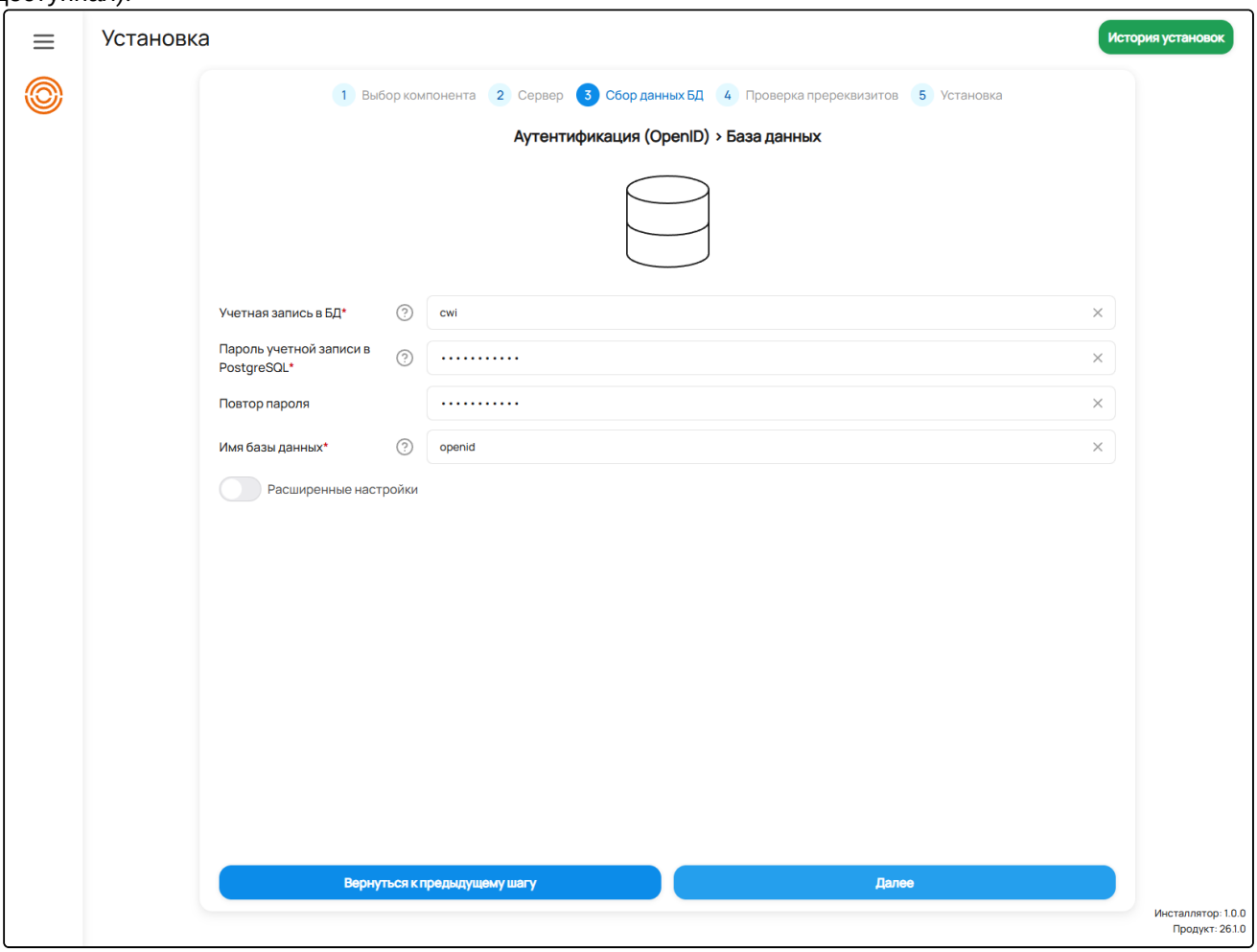
Компонент разворачивает базу данных PostgreSQL для сервиса OpenID: создаёт учётную запись-владельца, пустую базу и права. Таблицы (сессии, refresh-токены, ключи подписи) создаёт уже сам сервис при первом запуске.

Сервер. Укажите параметры SSH-подключения к серверу базы данных: имя сервера, учётную запись и способ входа (ssh-ключ или пароль).

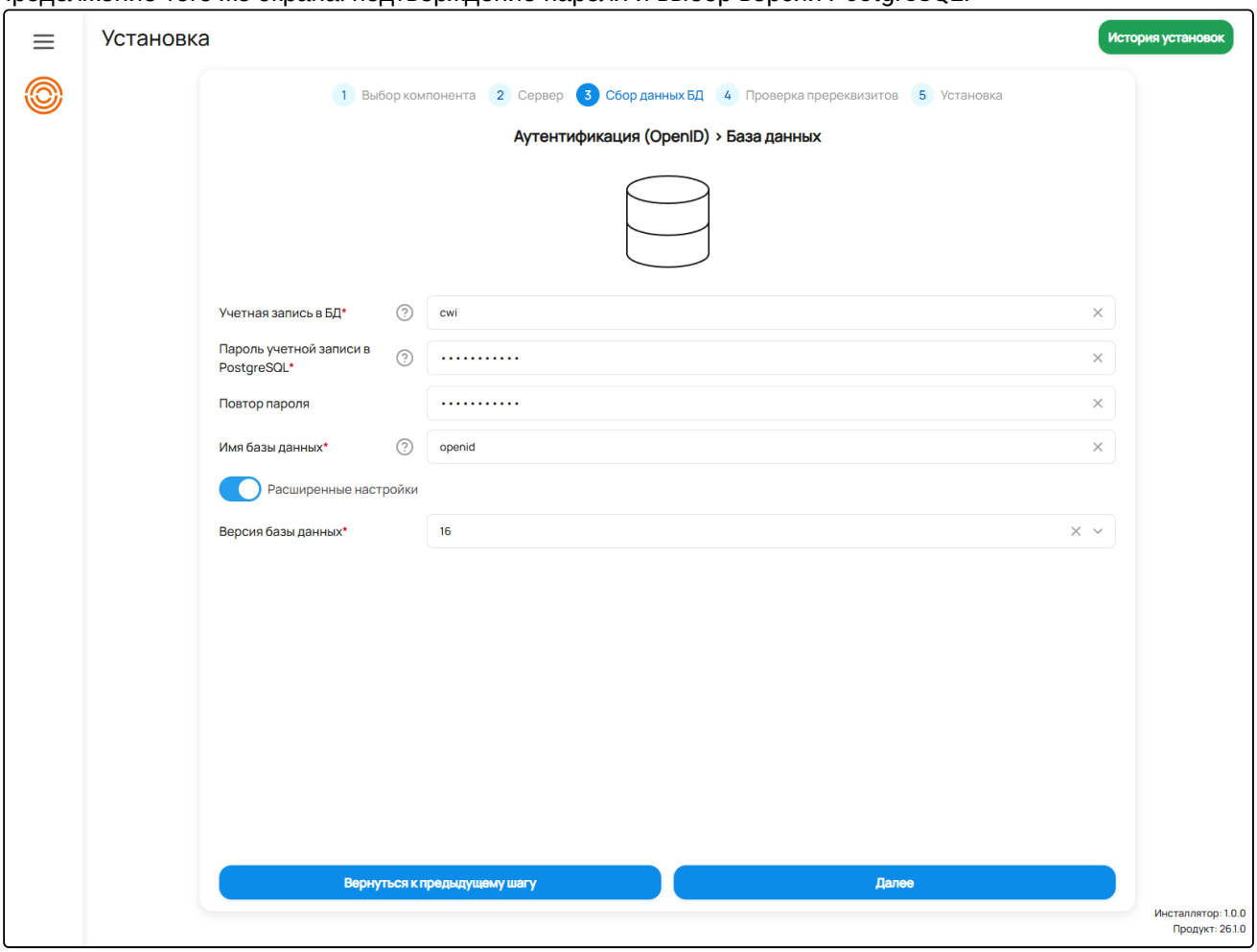


Сбор данных БД. Заполните параметры базы: PG_USERNAME — пользователь-владелец (по умолчанию cwi); PG_PASSWORD — пароль с подтверждением; PG_DB — имя базы (по умолчанию openid); PG_VERSION — версия PostgreSQL (поддерживаются 11–18, по умолчанию подбирается наибольшая

доступная).

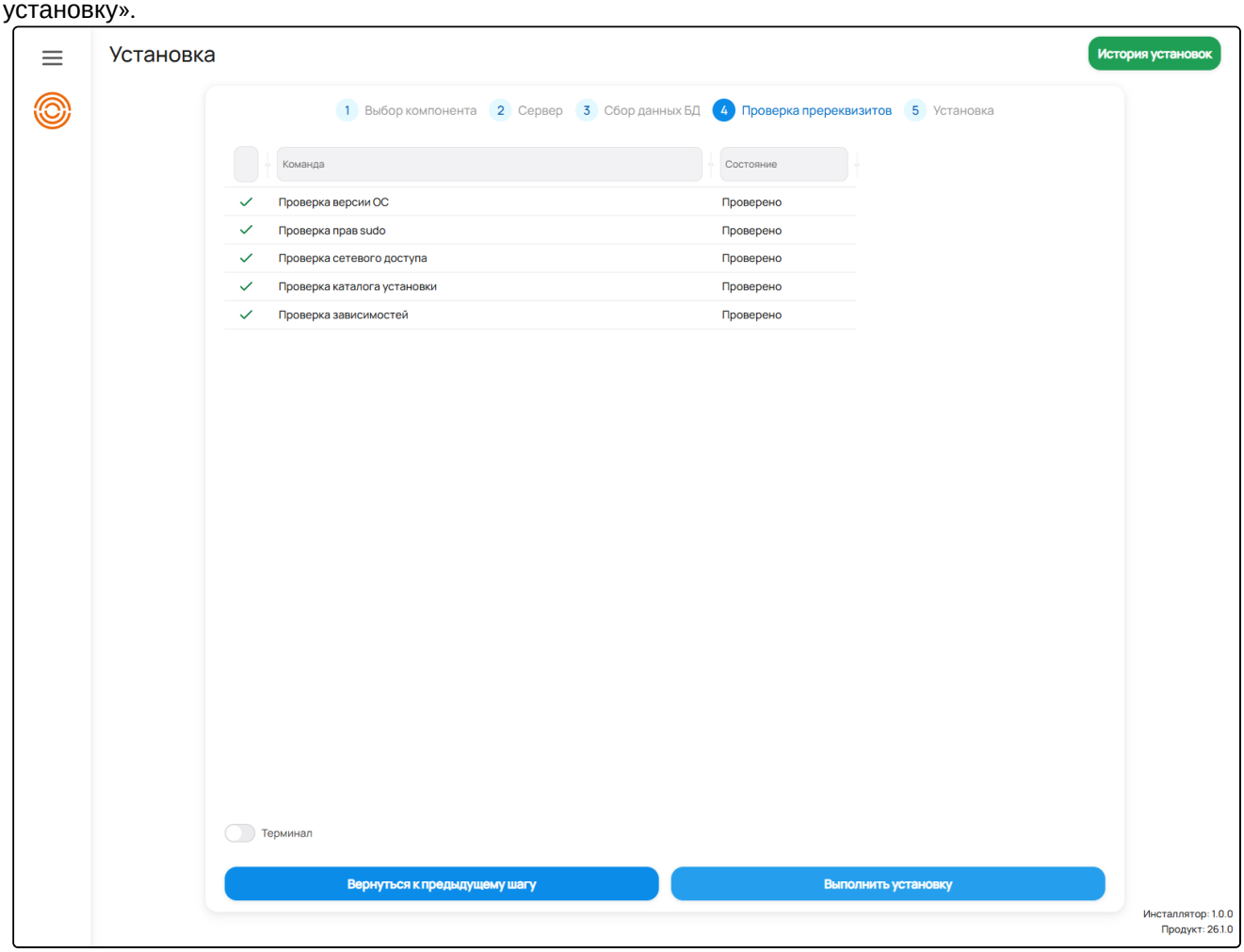

Установка
История установок
1 Выбор компонента
2 Сервер
3 Сбор данных БД
4 Проверка пререквизитов
5 Установка
Аутентификация (OpenID) › База данных
Учетная запись в БД*
cwi
Пароль учетной записи в PostgreSQL*
Повтор пароля
Имя базы данных*
openid
Расширенные настройки
Вернуться к предыдущему шагу
Далее
Инсталлятор: 1.0.0
Продукт: 26.1.0

Продолжение того же экрана: подтверждение пароля и выбор версии PostgreSQL.

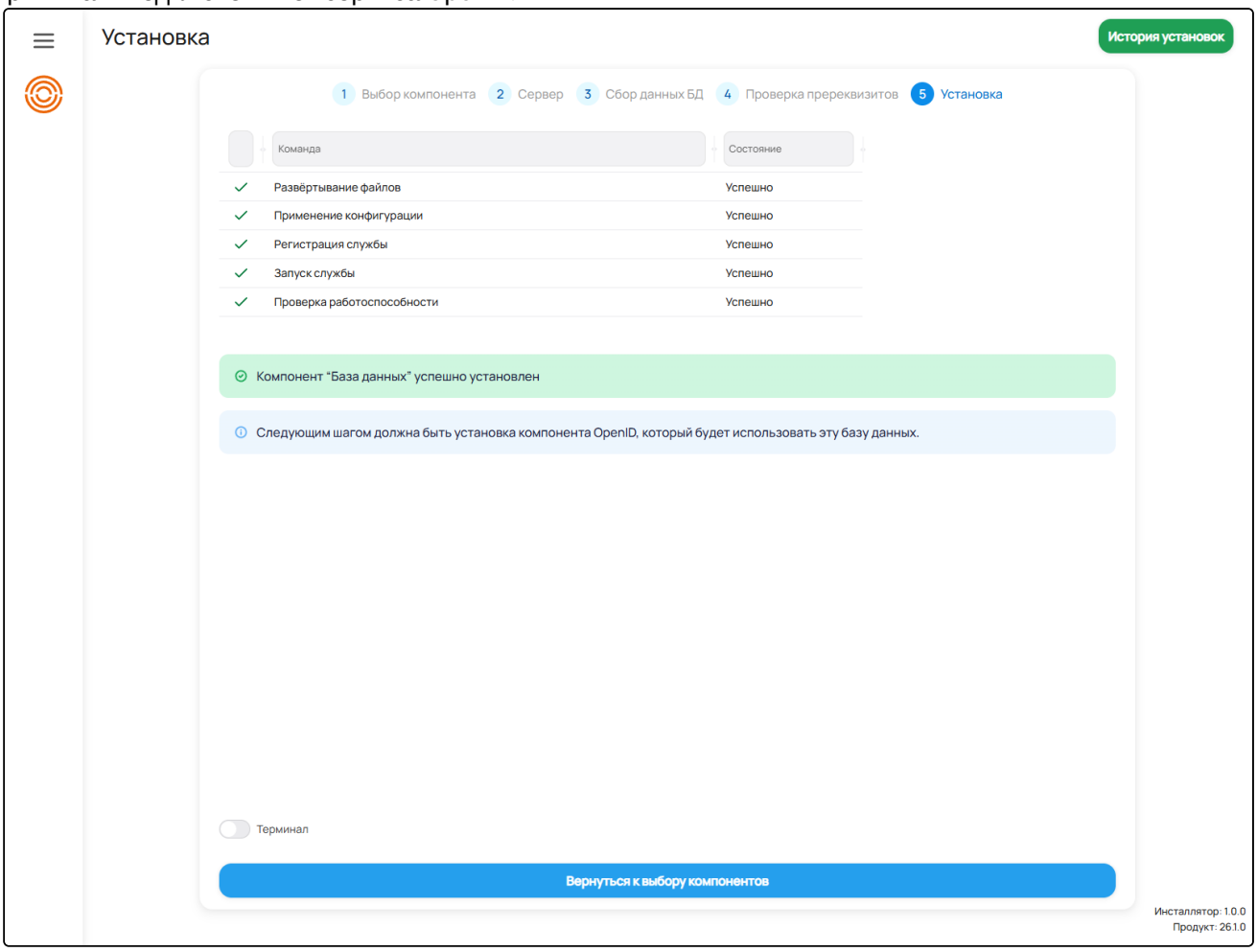


Проверка пререквизитов. Таблица проверок: установлен ли PostgreSQL, существуют ли учётная запись и база, права пользователя. Незакрытые пункты устраняются кнопкой «Выполнить настройку пререквизитов» (установка СУБД, создание пользователя и базы, выдача прав); затем — «Выполнить

установку».


Установка
История установок
1 Выбор компонента
2 Сервер
3 Сбор данных БД
4 Проверка пререквизитов
5 Установка
Команда
Состояние
Проверка версии ОС
Проверено
Проверка прав sudo
Проверено
Проверка сетевого доступа
Проверено
Проверка каталога установки
Проверено
Проверка зависимостей
Проверено
Терминал
Вернуться к предыдущему шагу
Выполнить установку
Инсталлятор: 1.0.0
Продукт: 26.1.0

Установка и результат. Мастер завершает подготовку базы. По окончании база openid готова принимать подключения от сервиса OpenID.

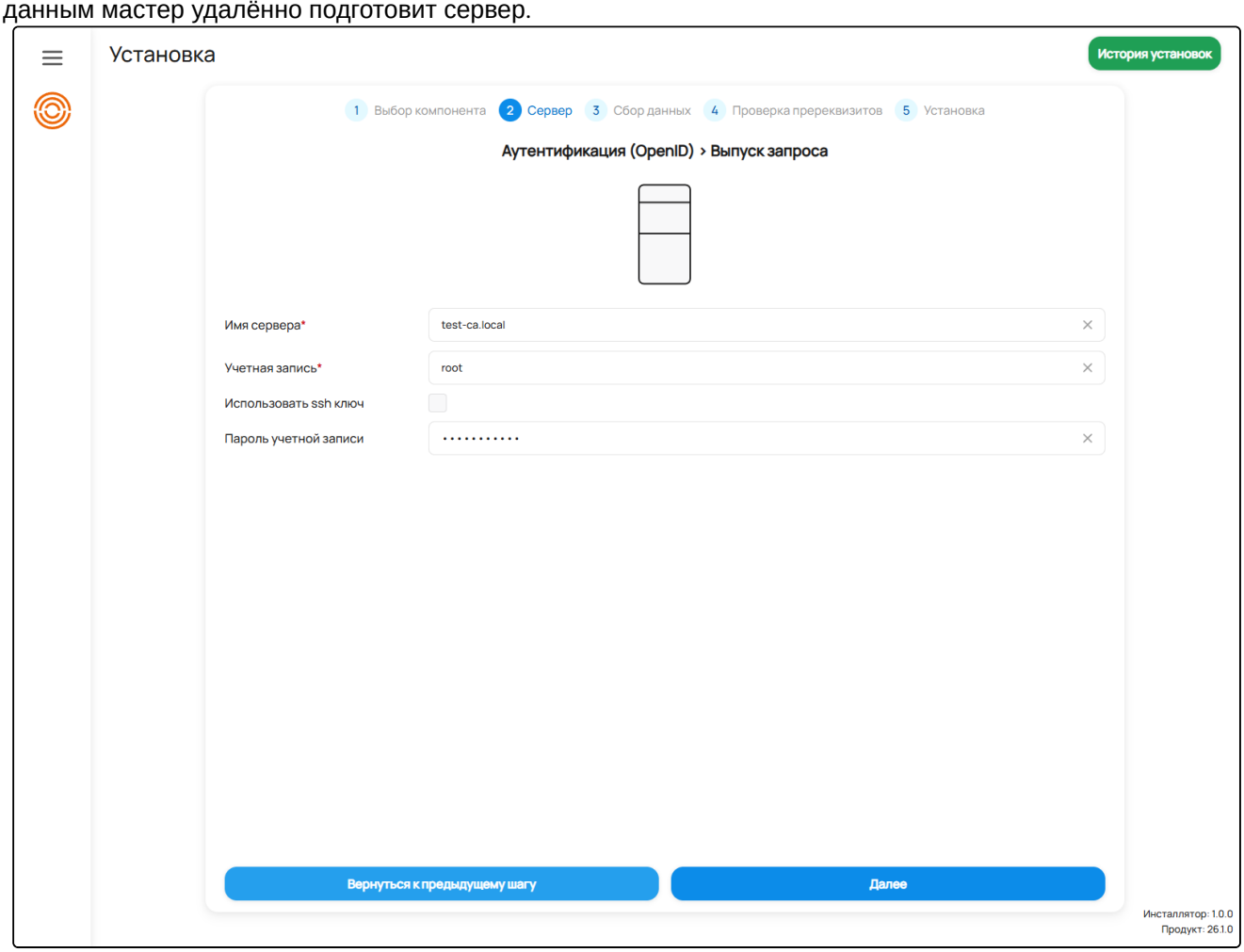


9.2 Выпуск запроса на TLS

Компонент генерирует на целевом сервере приватный ключ и запрос на сертификат (CSR) для TLS сервиса OpenID; сам сервис пока не устанавливается.

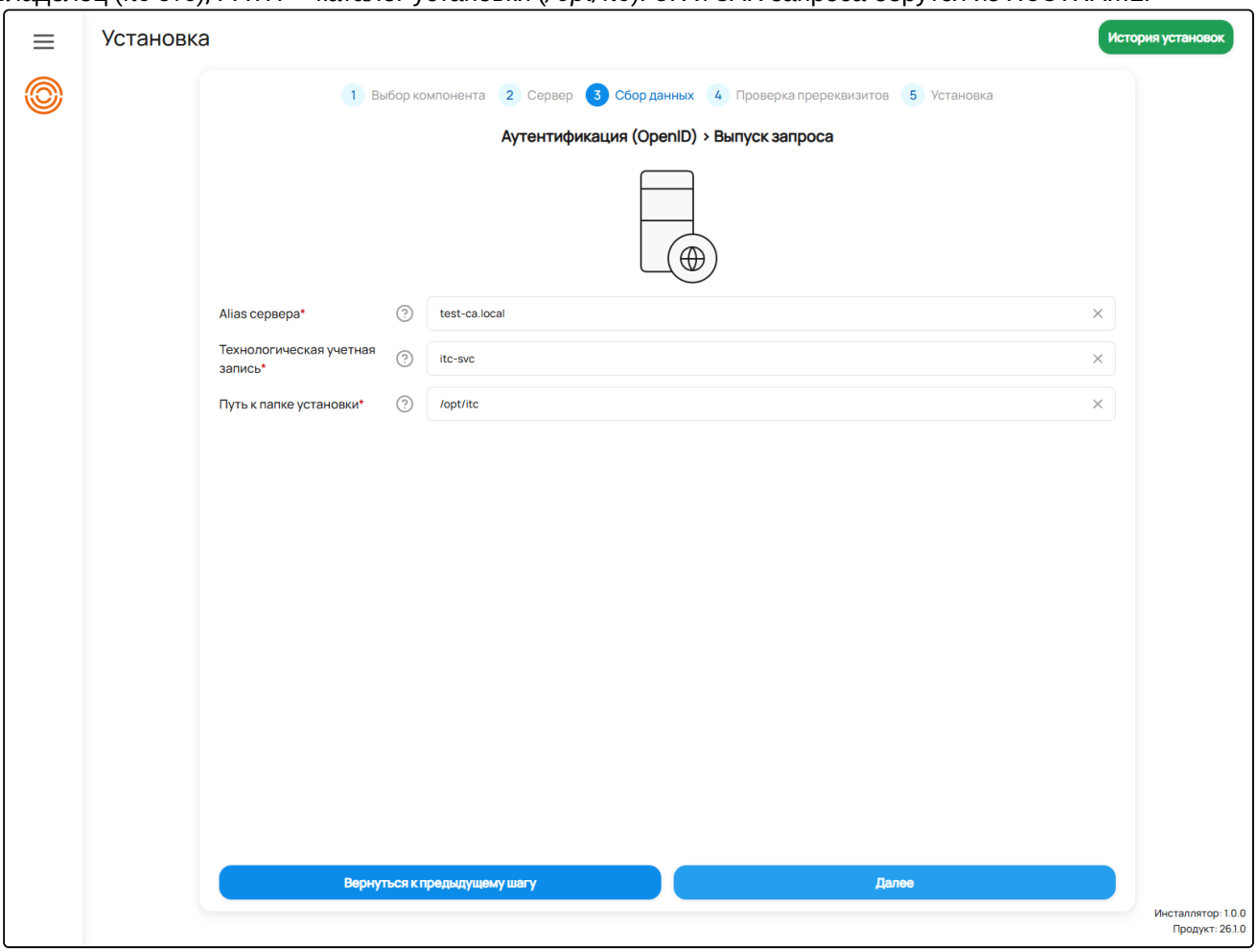
Сервер. Укажите параметры SSH-подключения к серверу, где будет работать OpenID: имя сервера (адрес), учётную запись и способ входа — флажок «Использовать ssh ключ» либо пароль. По этим

данным мастер удалённо подготовит сервер.



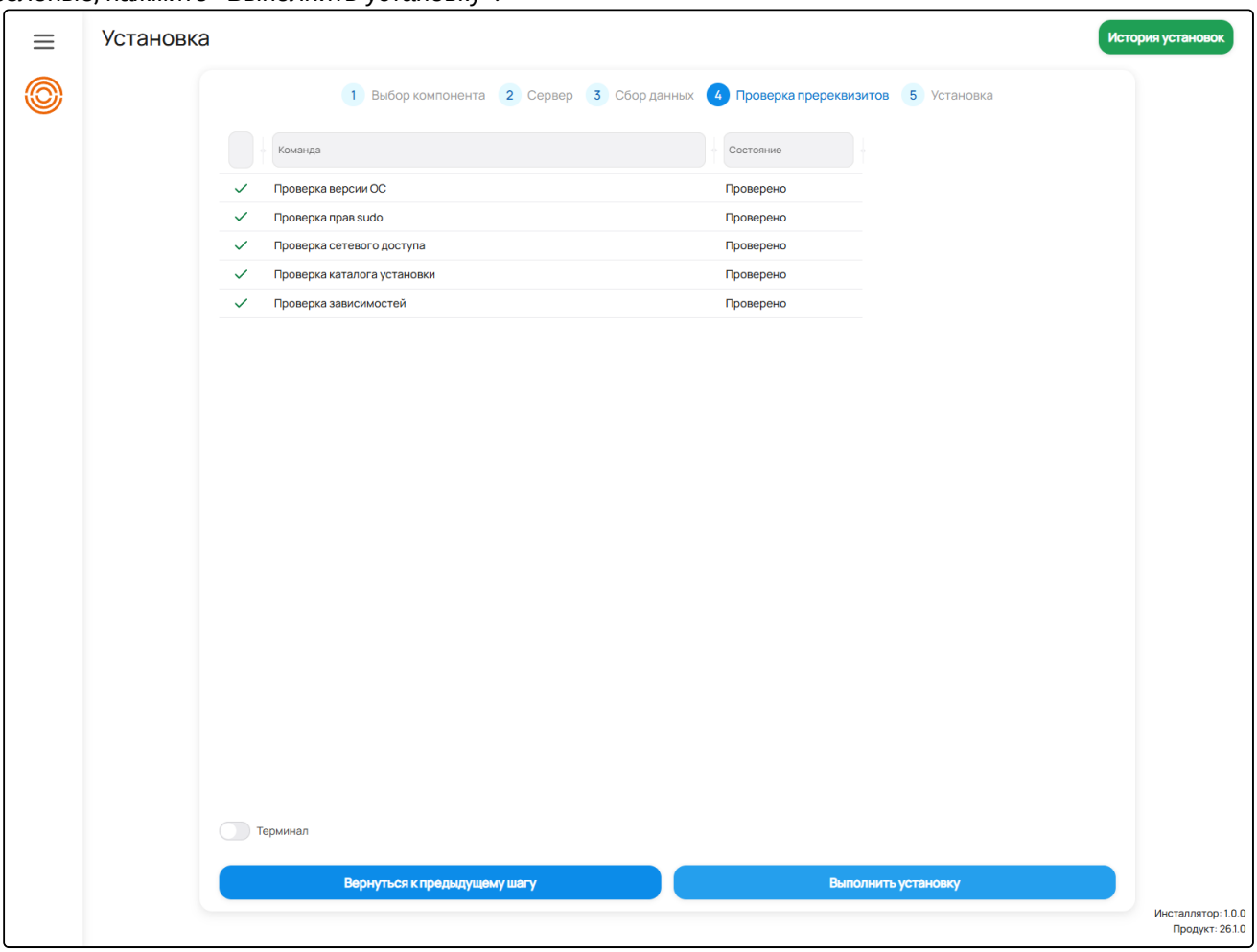
Сбор данных. Заполните переменные компонента: HOSTNAME — имя (alias), на которое выпускается TLS-сертификат (по умолчанию — имя сервера); USER_NAME — технологическая учётная запись-

владелец (itc-svc); PATH — каталог установки (*/opt/itc*). CN и SAN запроса берутся из HOSTNAME.



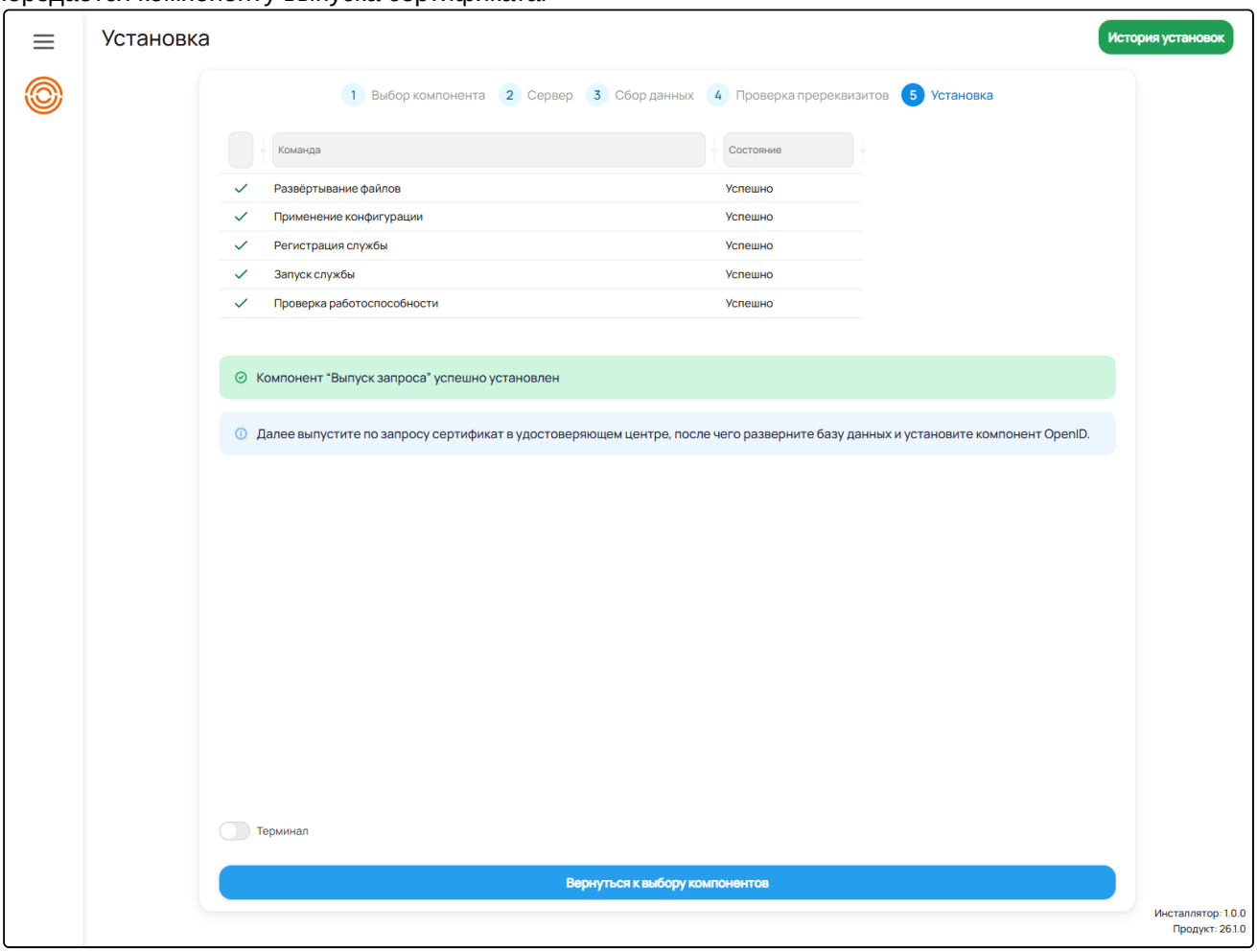
Проверка пререквизитов. Мастер выводит таблицу проверок: наличие учётной записи, каталога и корректных прав на него. Если какая-либо проверка не пройдена, нажмите «Выполнить настройку пререквизитов» — мастер создаст учётную запись, каталог и назначит права; когда все проверки

зелёные, нажмите «Выполнить установку».



Установка и результат. Мастер создаёт каталог certs, генерирует RSA-ключ openid-tls.key и формирует запрос openid-tls.csr. Результат — файл запроса openid-tls.csr — скачивается и на следующем шаге

передаётся компоненту выпуска сертификата.

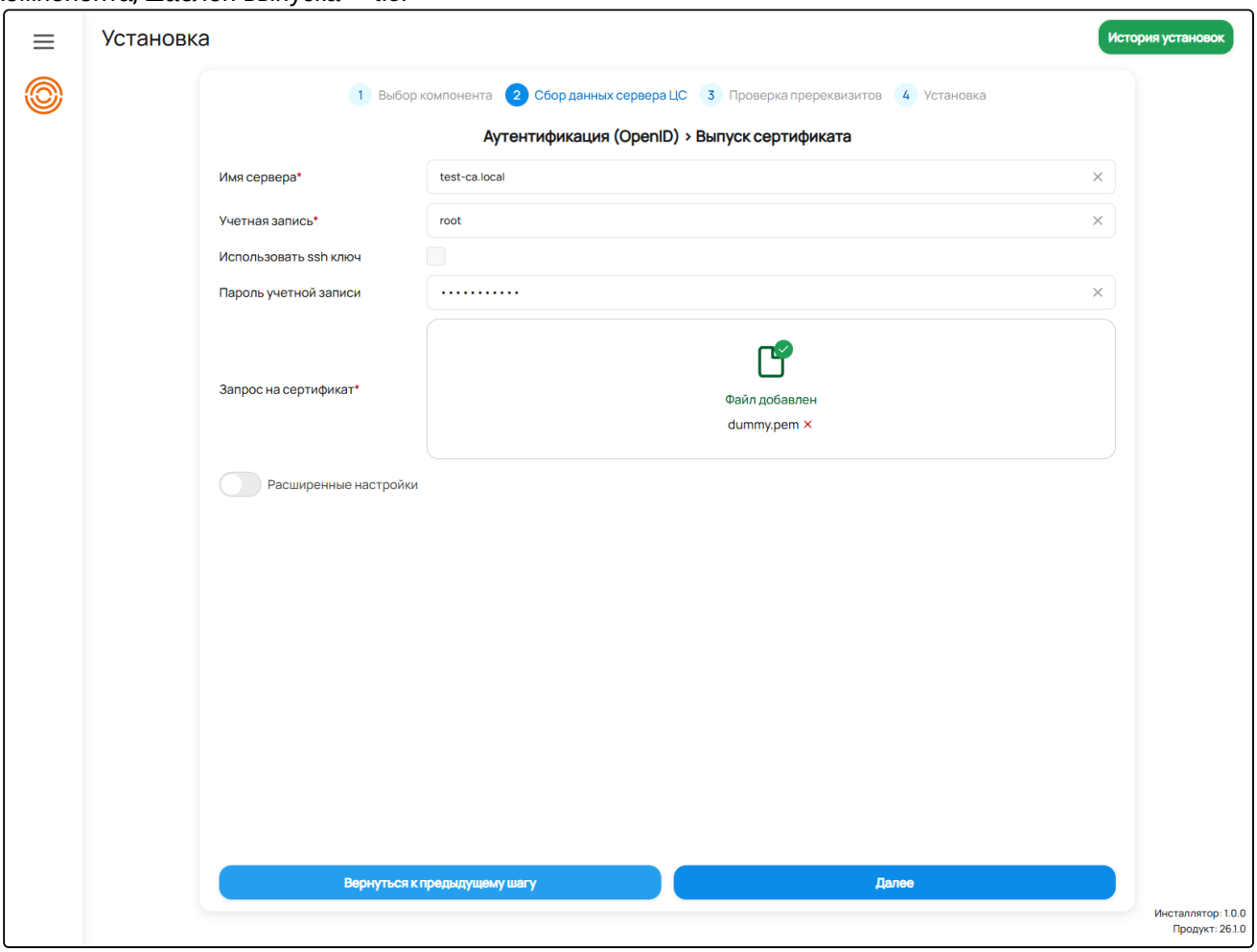


9.3 Выпуск сертификата

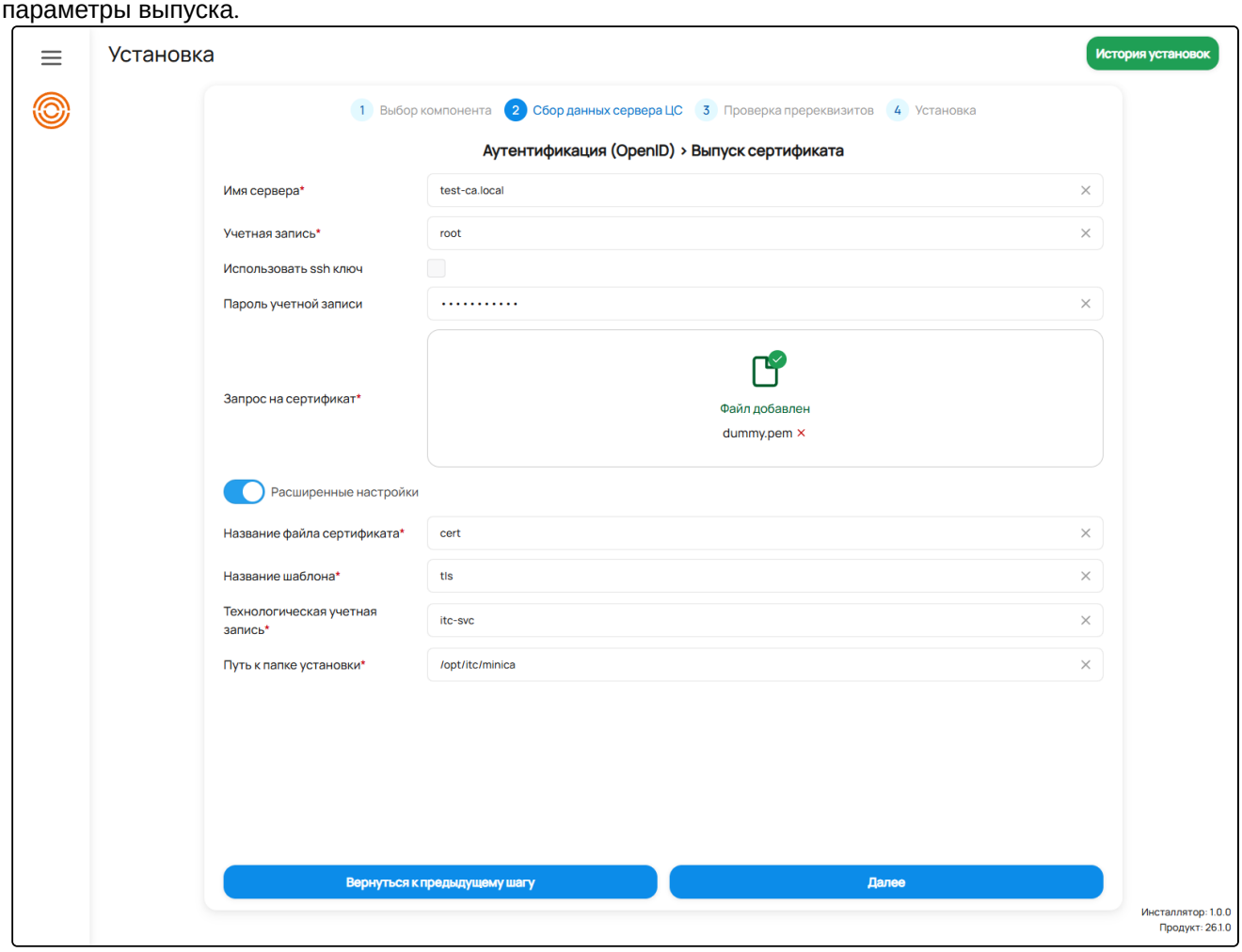
Служебный компонент: подключается к серверу действующего ЦС, передаёт туда запрос openid-tls.csr и выпускает по нему подписанный TLS-сертификат. Ничего постоянно на сервере не устанавливает.

Сбор данных сервера ЦС. Укажите сервер ЦС, на котором выполняется выпуск, и учётную запись/путь установки ЦС (USER_NAME, PATH — по умолчанию берутся из установленного выдающего или корневого ЦС). Запрос на сертификат подставляется автоматически как результат предыдущего

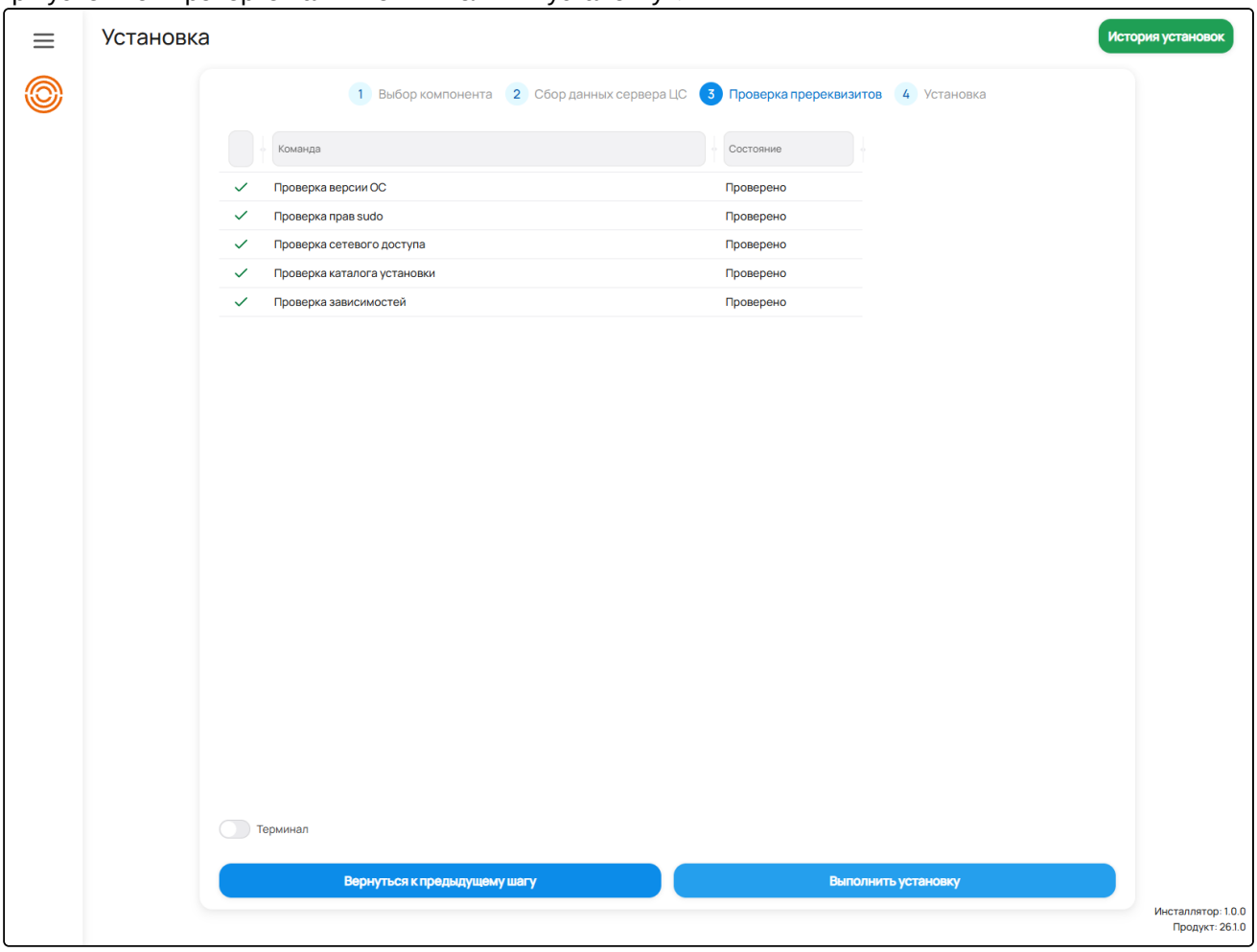
компонента; шаблон выпуска – tls.



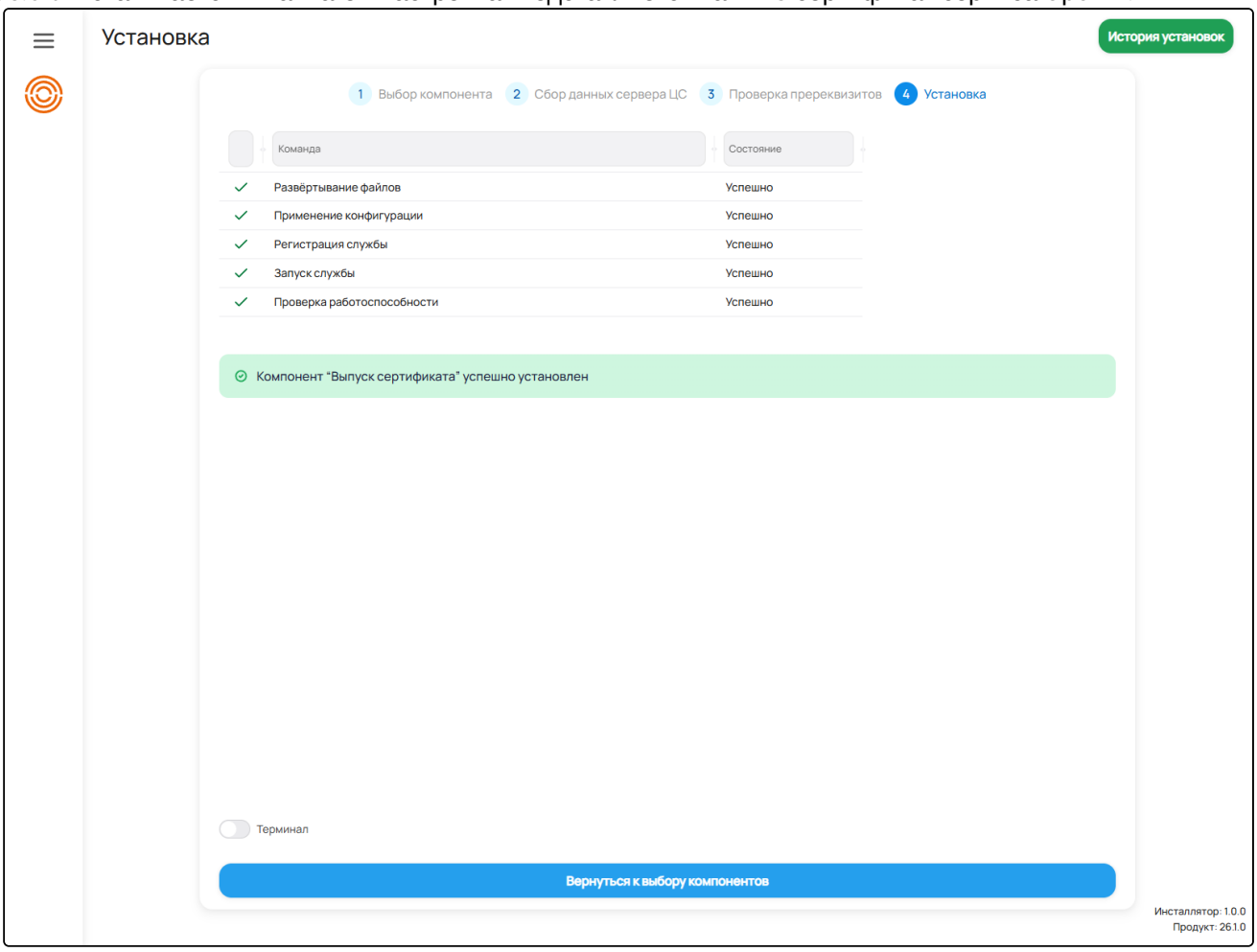
Продолжение того же экрана (прокрутка): проверьте подставленное содержимое запроса и остальные параметры выпуска.



Проверка пререквизитов. Мастер проверяет, что ЦС установлен и отвечает (проверка mclient ping). При успешной проверке нажмите «Выполнить установку».



Установка и результат. ЦС подписывает запрос и возвращает сертификат. Результат — файл openid-tls.crt — скачивается и на шаге «Настройка» подставляется как TLS-сертификат сервиса OpenID.

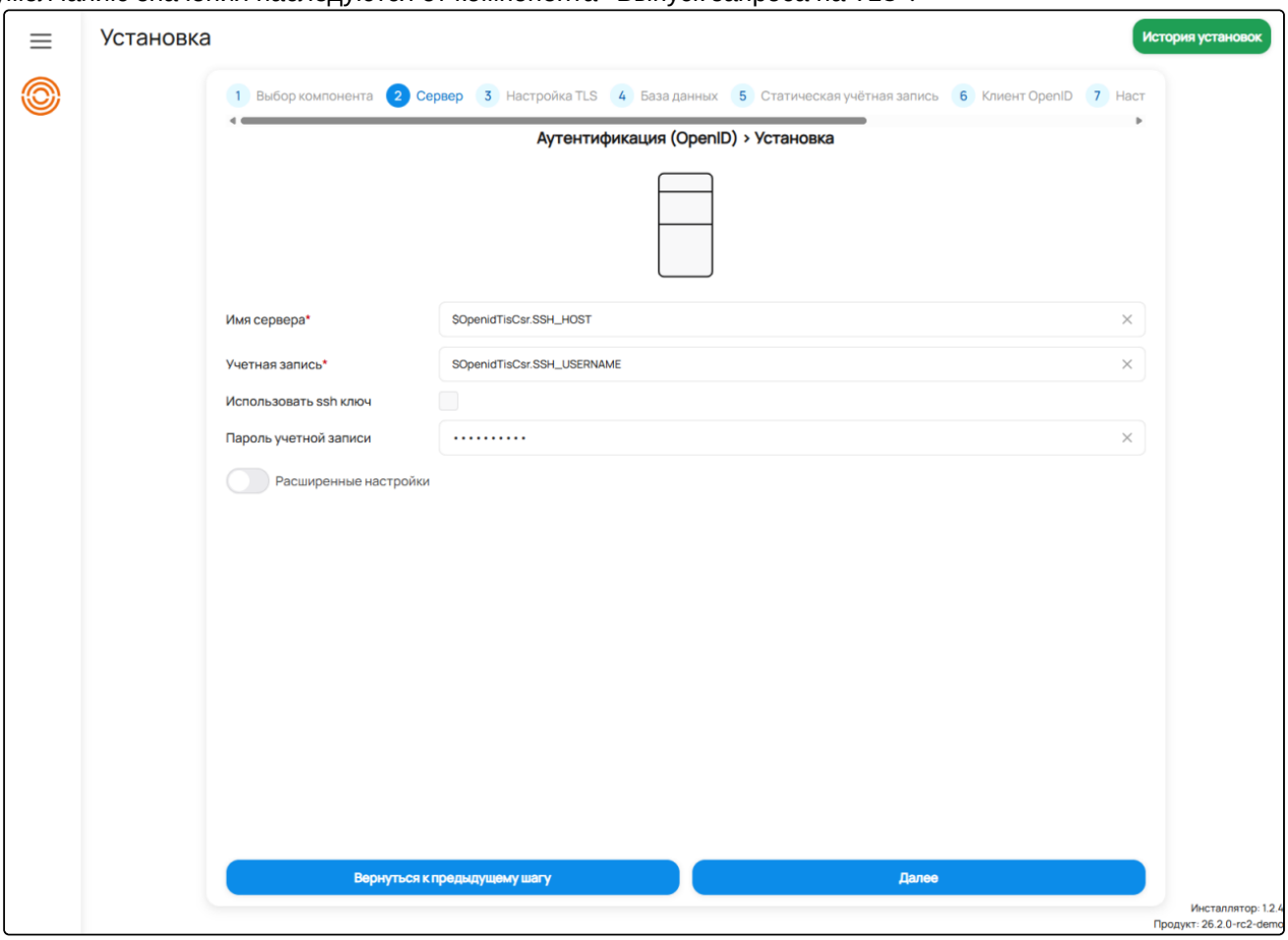


9.4 Установка

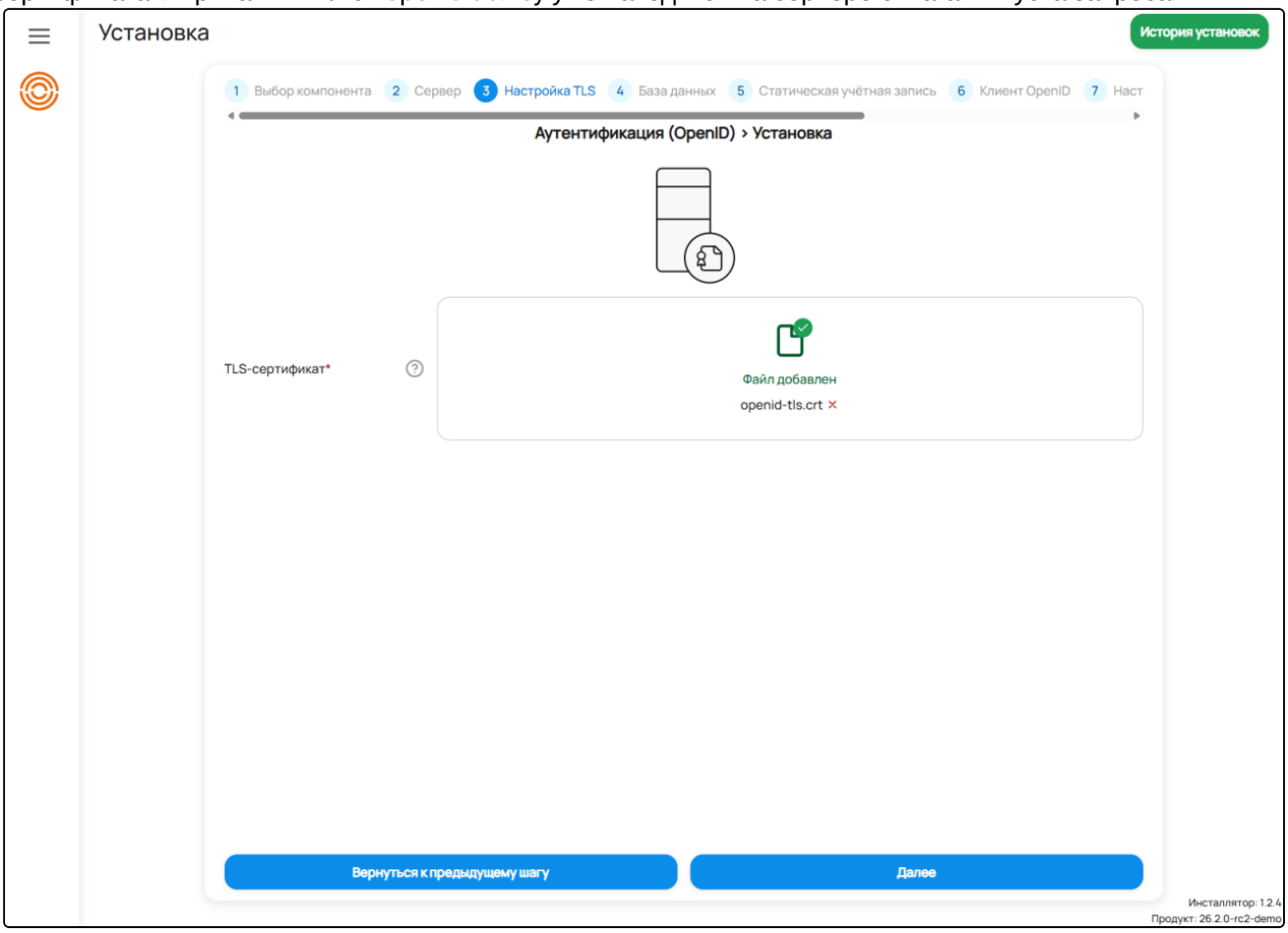
Завершающий компонент устанавливает и запускает сервис аутентификации OpenID Connect: разворачивает бинарный файл и конфигурацию в */opt/itc/openid*, регистрирует пользовательский systemd-сервис и открывает HTTPS-порт 443. Здесь задаются параметры подключения к базе данных, встроенная статическая учётная запись, клиент OpenID и время жизни токенов. Перед установкой должны быть развёрнута база данных OpenID и выпущен TLS-сертификат сервиса.

Сервер. Укажите параметры SSH-подключения к серверу, где будет работать сервис OpenID: имя сервера, учётную запись и способ входа — флажок «Использовать ssh ключ» либо пароль. По

умолчанию значения наследуются от компонента «Выпуск запроса на TLS».

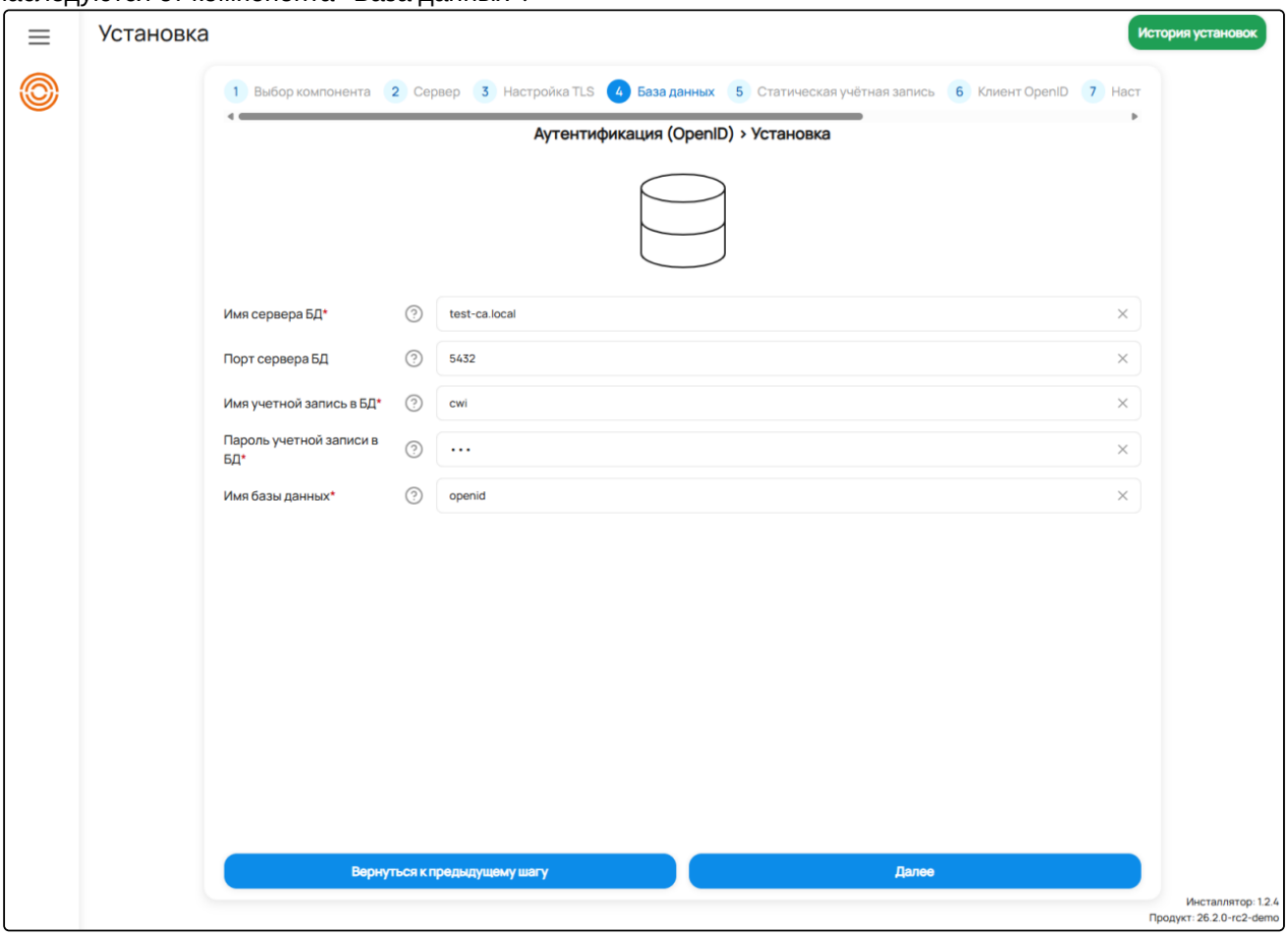


Настройка TLS. Подставьте TLS-сертификат сервиса — файл openid-tls.crt, полученный на шаге «Выпуск сертификата». Приватный ключ openid-tls.key уже находится на сервере с шага выпуска запроса.



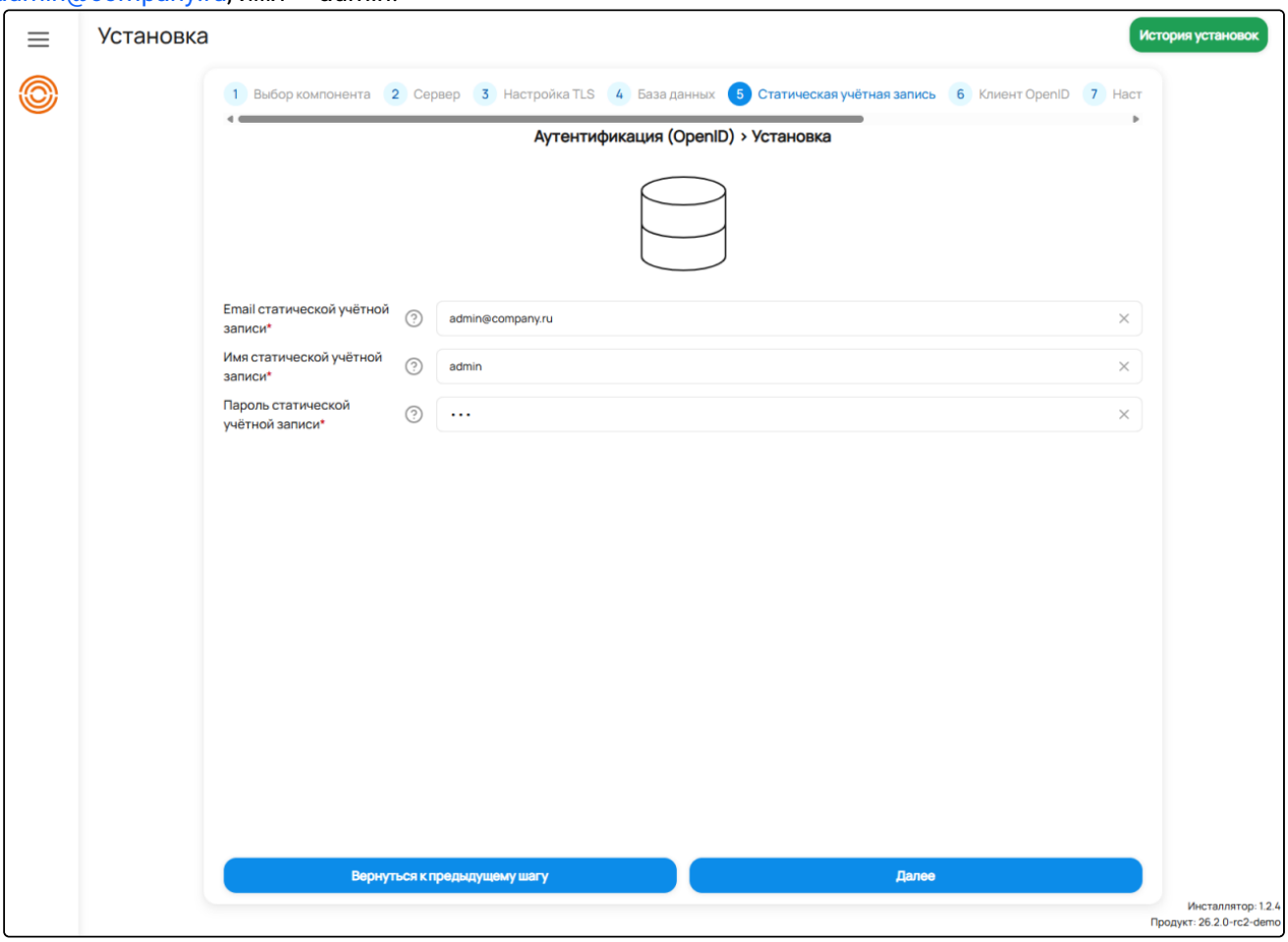
База данных. Укажите параметры подключения к базе OpenID: имя сервера БД и порт (5432), имя и пароль учётной записи PostgreSQL, имя базы данных. По умолчанию значения (кроме пароля)

наследуются от компонента «База данных».



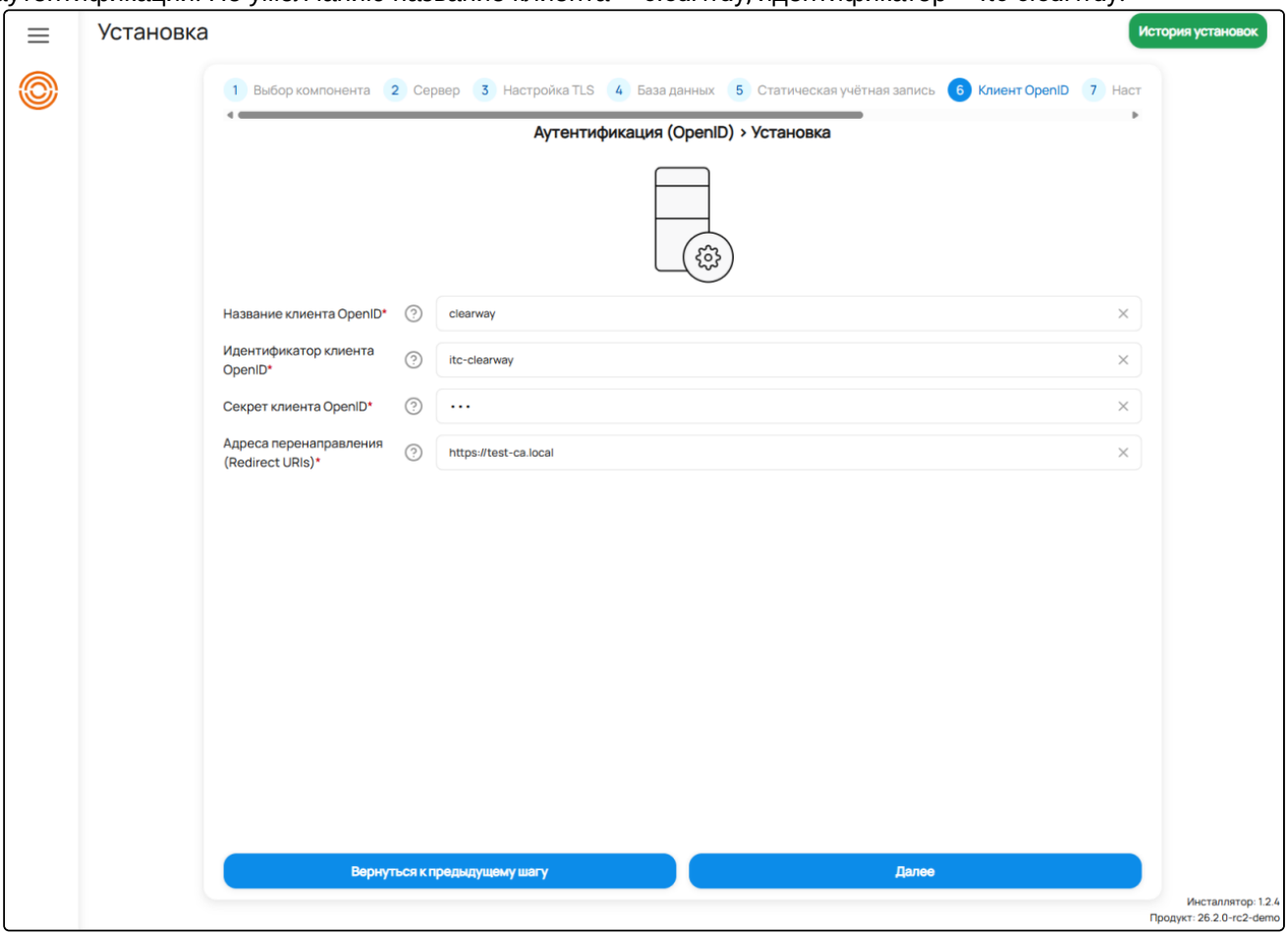
Статическая учётная запись. Задайте встроенную учётную запись администратора, позволяющую входить без внешнего каталога: Email (используется как логин), отображаемое имя и пароль. В конфигурацию сохраняется bcrypt-хэш пароля, открытый пароль не хранится. По умолчанию Email –

admin@company.ru, имя — admin.



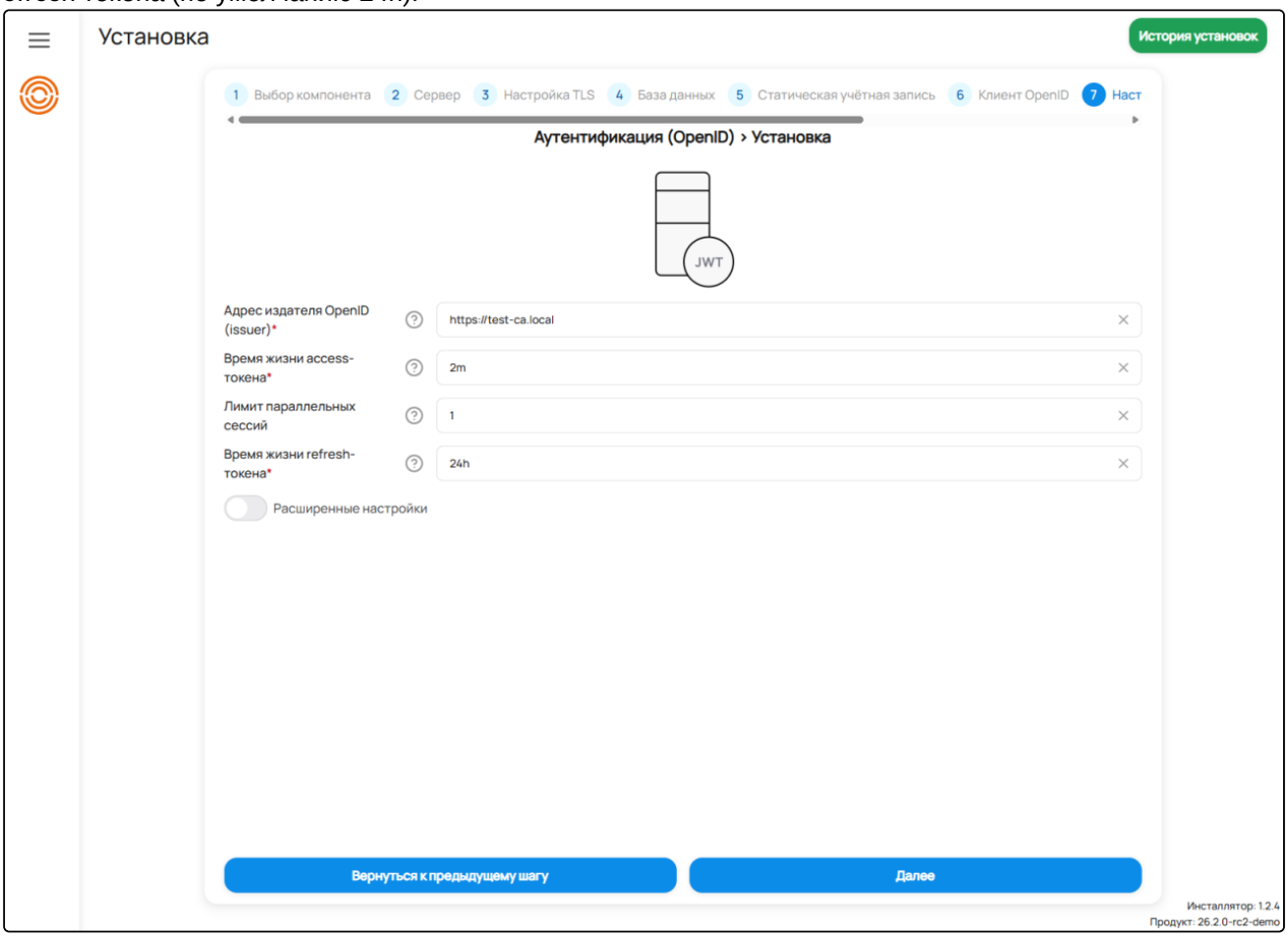
Клиент OpenID. Укажите название клиента, его идентификатор и секрет, а также адреса перенаправления (Redirect URIs), на которые провайдер возвращает пользователя после

аутентификации. По умолчанию название клиента — clearway, идентификатор — itc-clearway.



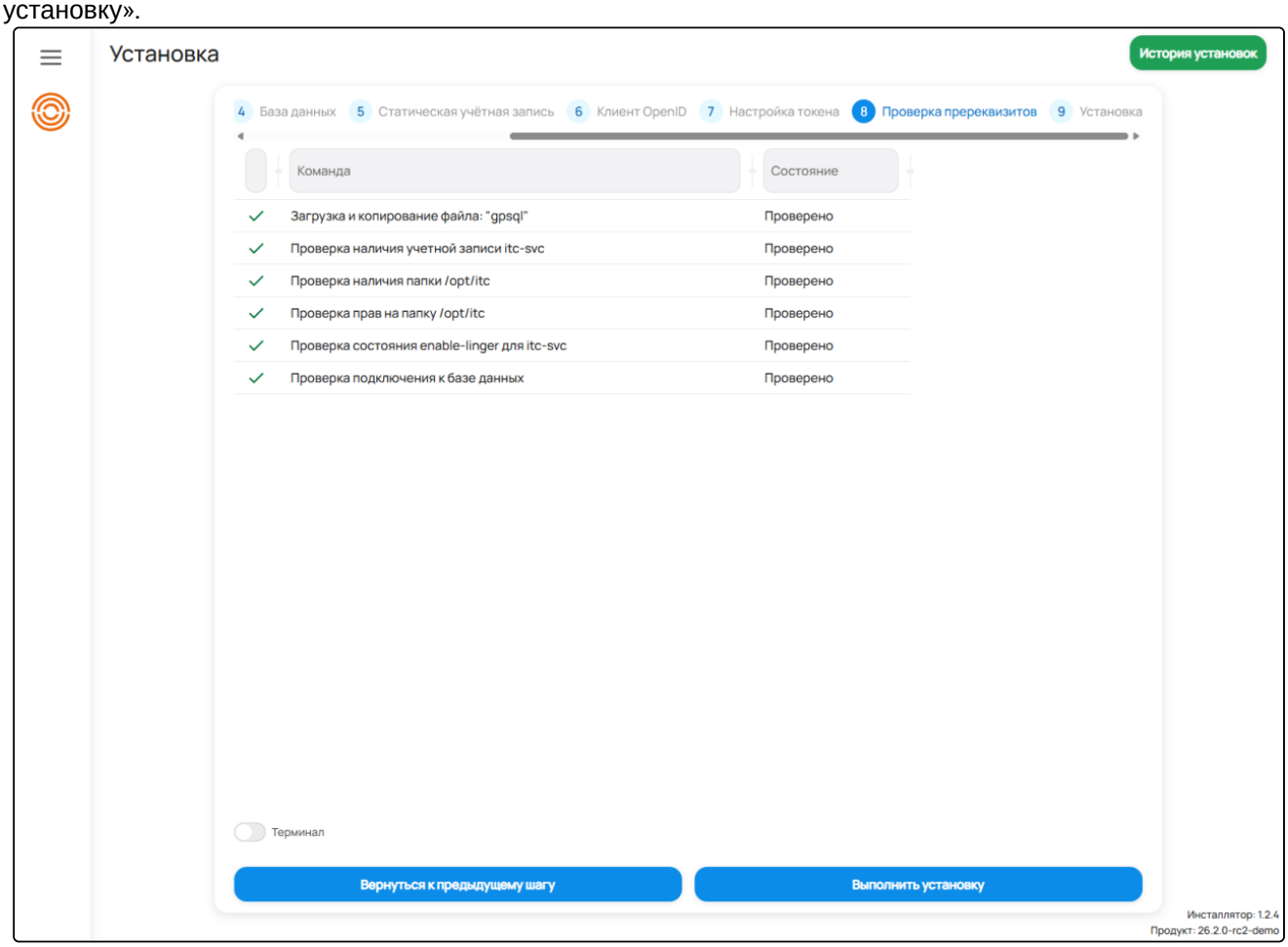
Настройка токена. Задайте адрес издателя токенов (issuer, по умолчанию https://<имя-сервера>), время жизни access-токена (по умолчанию 2m), лимит параллельных сессий пользователя и время жизни

refresh-токена (по умолчанию 24h).



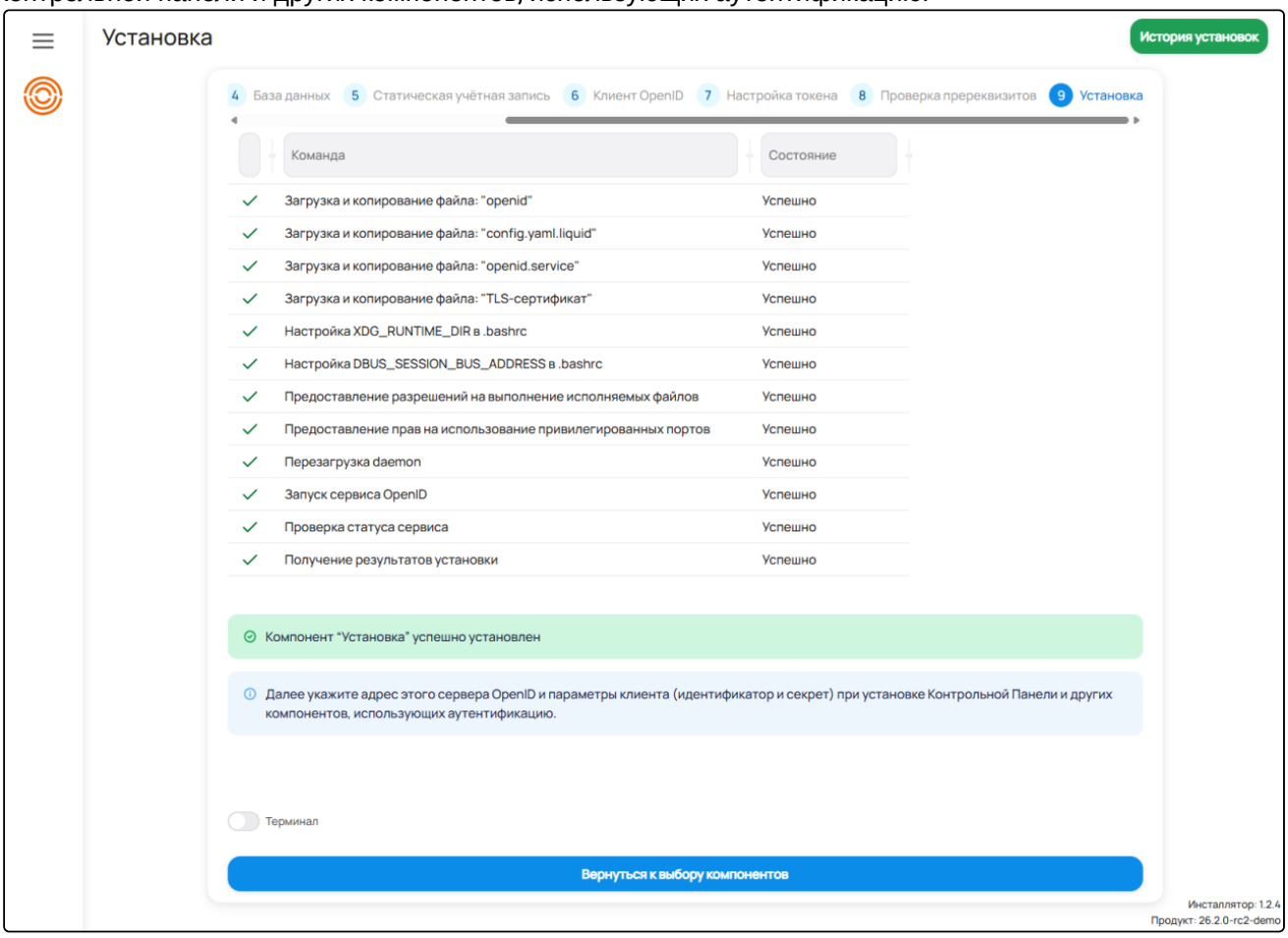
Проверка пререквизитов. Мастер выводит таблицу проверок: наличие учётной записи, каталога и прав на него, состояние enable-linger и подключение к базе данных. Незакрытые пункты устраняются кнопкой «Выполнить настройку пререквизитов»; когда все проверки пройдены — нажмите «Выполнить

установку».



Установка и результат. Мастер разворачивает бинарный файл и конфигурацию, назначает право на привязку к порту 443, регистрирует и запускает пользовательский сервис openid.service. По завершении провайдер аутентификации доступен по адресу https://<имя-сервера> и готов обслуживать вход в веб-сервисы Clearway CA. Адрес сервера OpenID и параметры клиента понадобятся при установке

Контрольной панели и других компонентов, использующих аутентификацию.

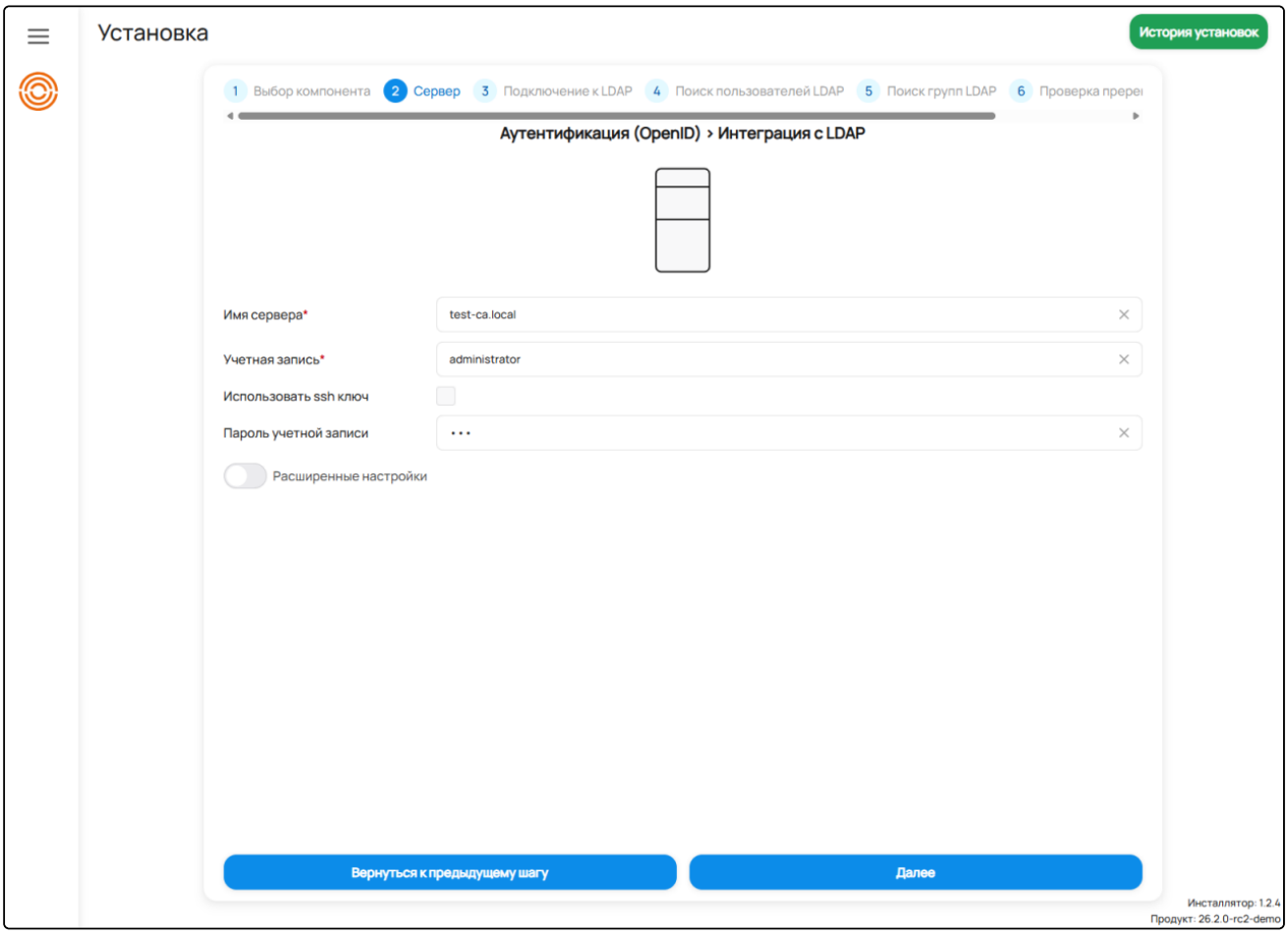


9.5 Интеграция с LDAP

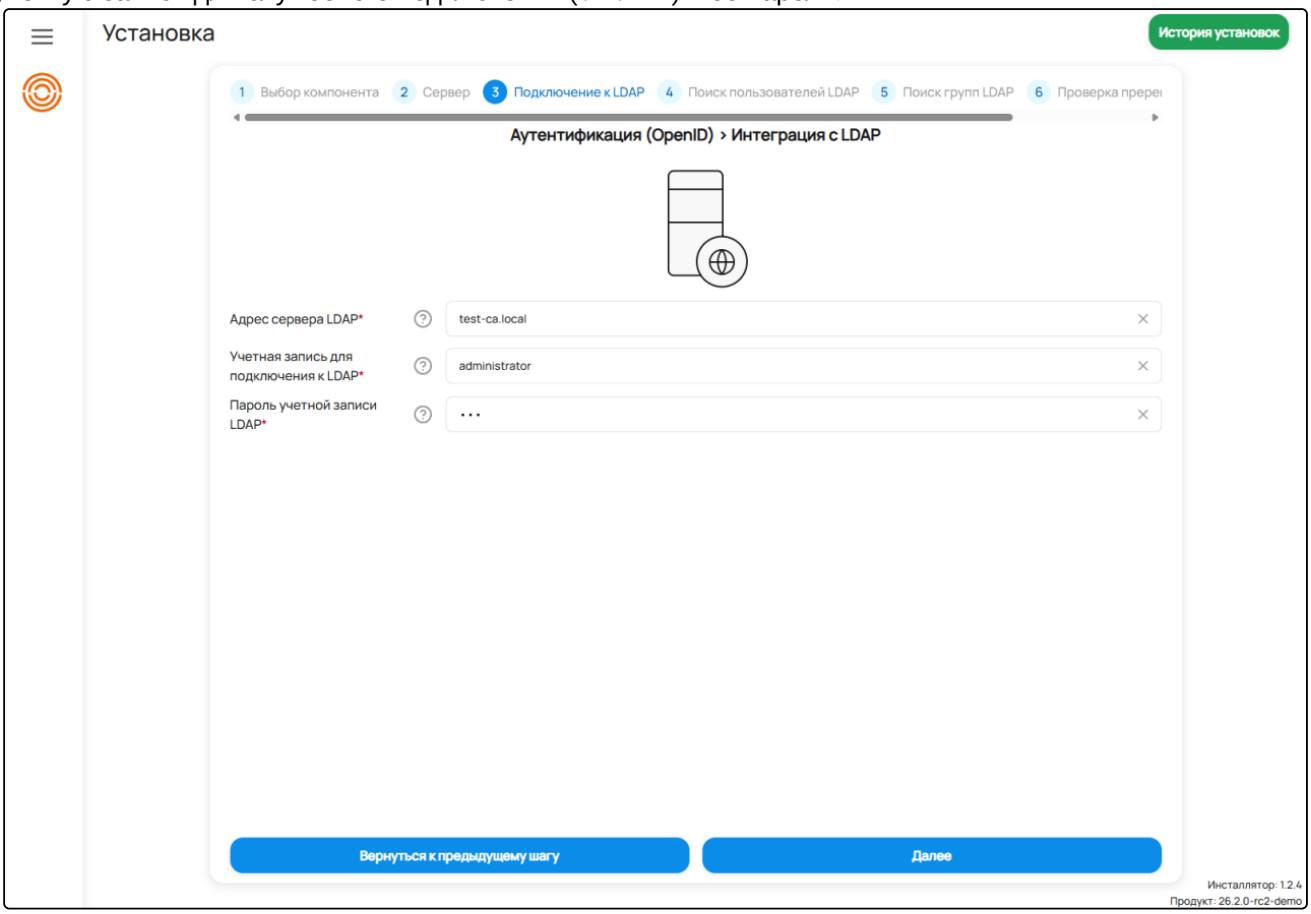
Необязательный компонент добавляет коннектор LDAP/Active Directory в конфигурацию уже установленного сервиса OpenID: настраивает периодический импорт пользователей и групп и сопоставление групп каталога с ролями Clearway CA. Встроенная статическая учётная запись при этом сохраняется. Перед установкой сервис OpenID должен быть установлен и запущен.

Сервер. Укажите параметры SSH-подключения к серверу с установленным сервисом OpenID: имя сервера, учётную запись и способ входа (ssh-ключ или пароль). По умолчанию параметры наследуются

от компонента «Установка».

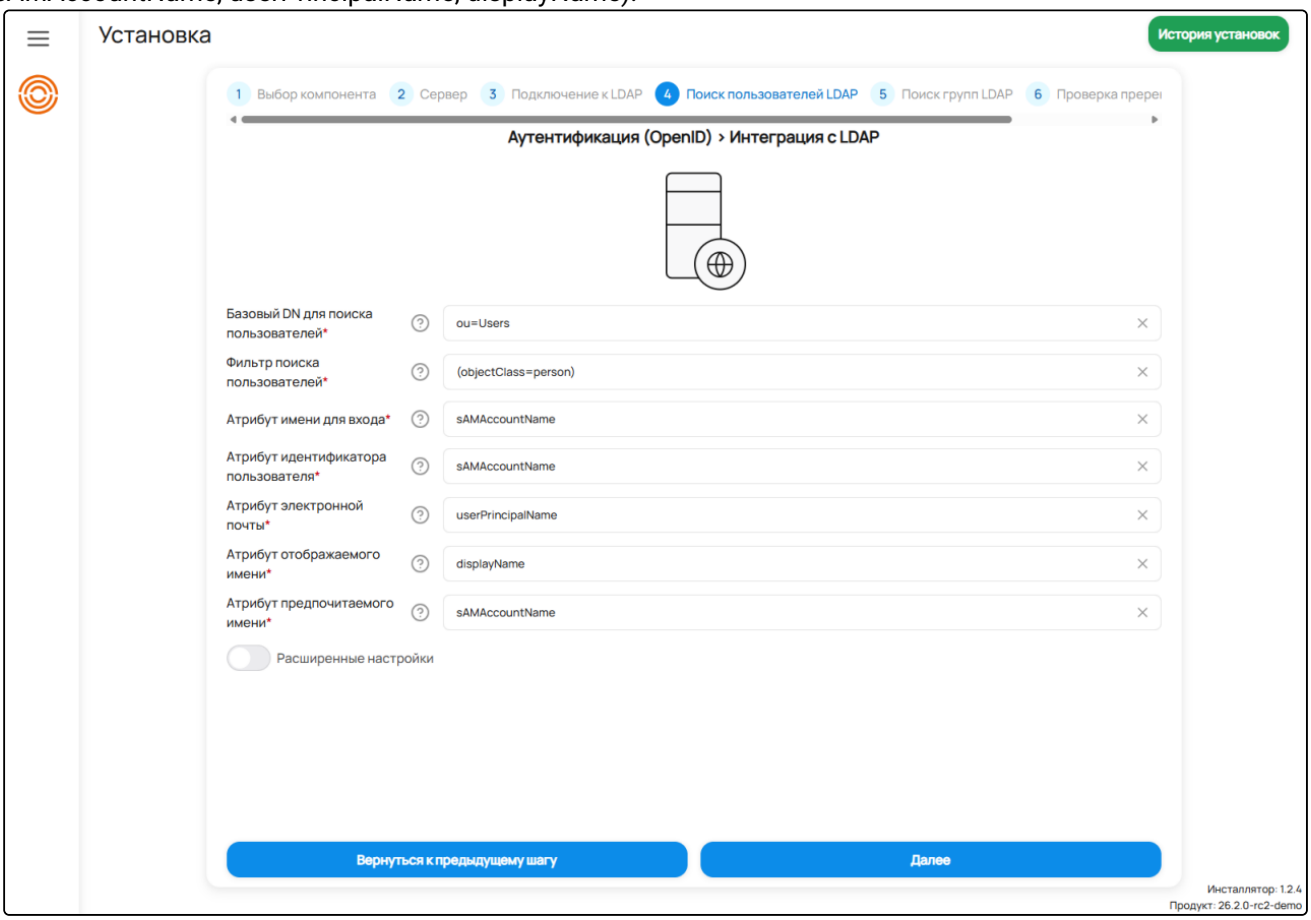


Подключение к LDAP. Задайте параметры каталога: адрес сервера LDAP/AD (формат <host>:<port>), учётную запись для служебного подключения (bind DN) и её пароль.



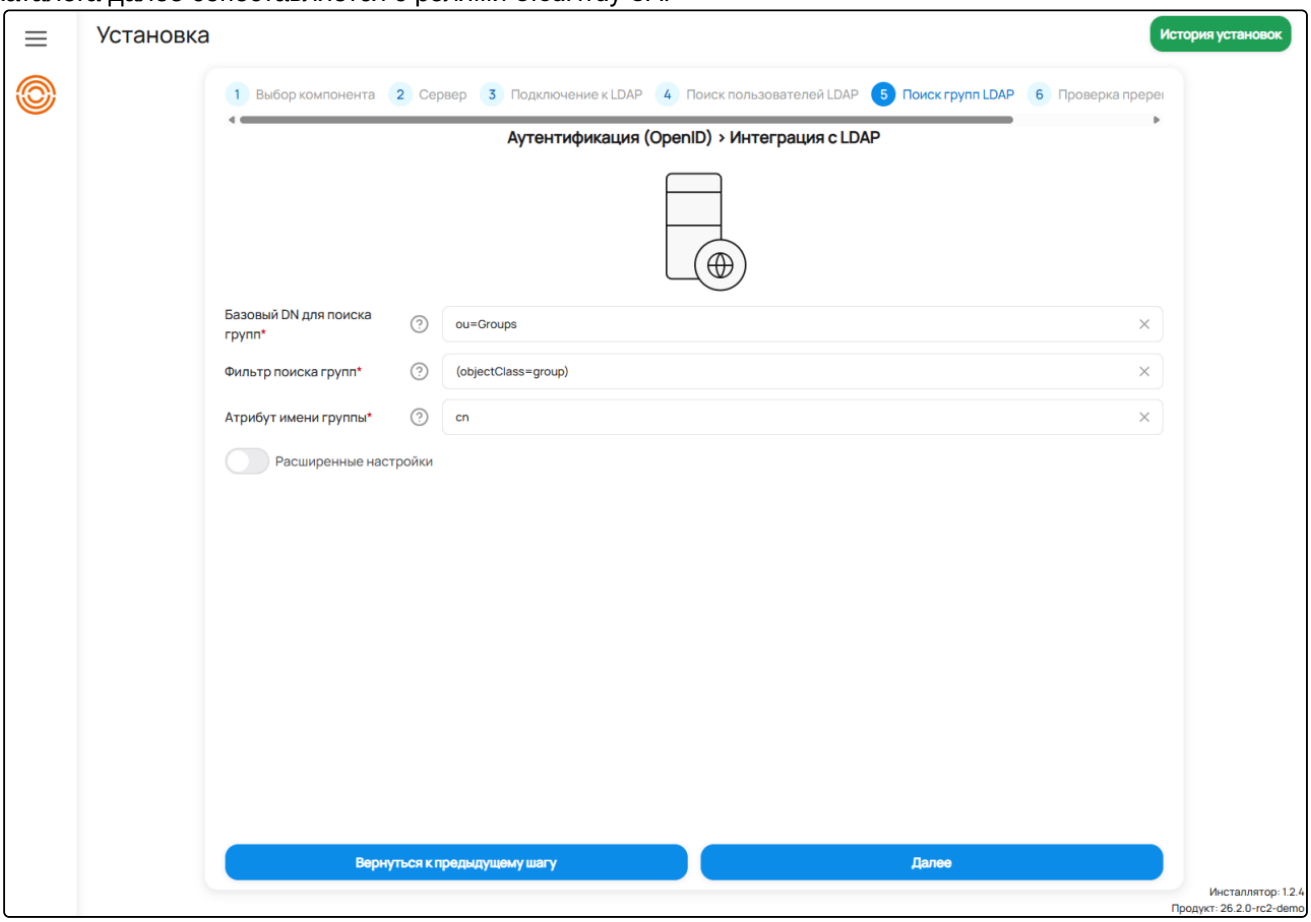
Поиск пользователей LDAP. Настройте импорт учётных записей: базовый DN поиска пользователей, фильтр отбора (по умолчанию (objectClass=person)) и атрибуты — имени для входа, идентификатора, электронной почты, отображаемого и предпочитаемого имени (для Active Directory обычно

sAMAccountName, userPrincipalName, displayName).



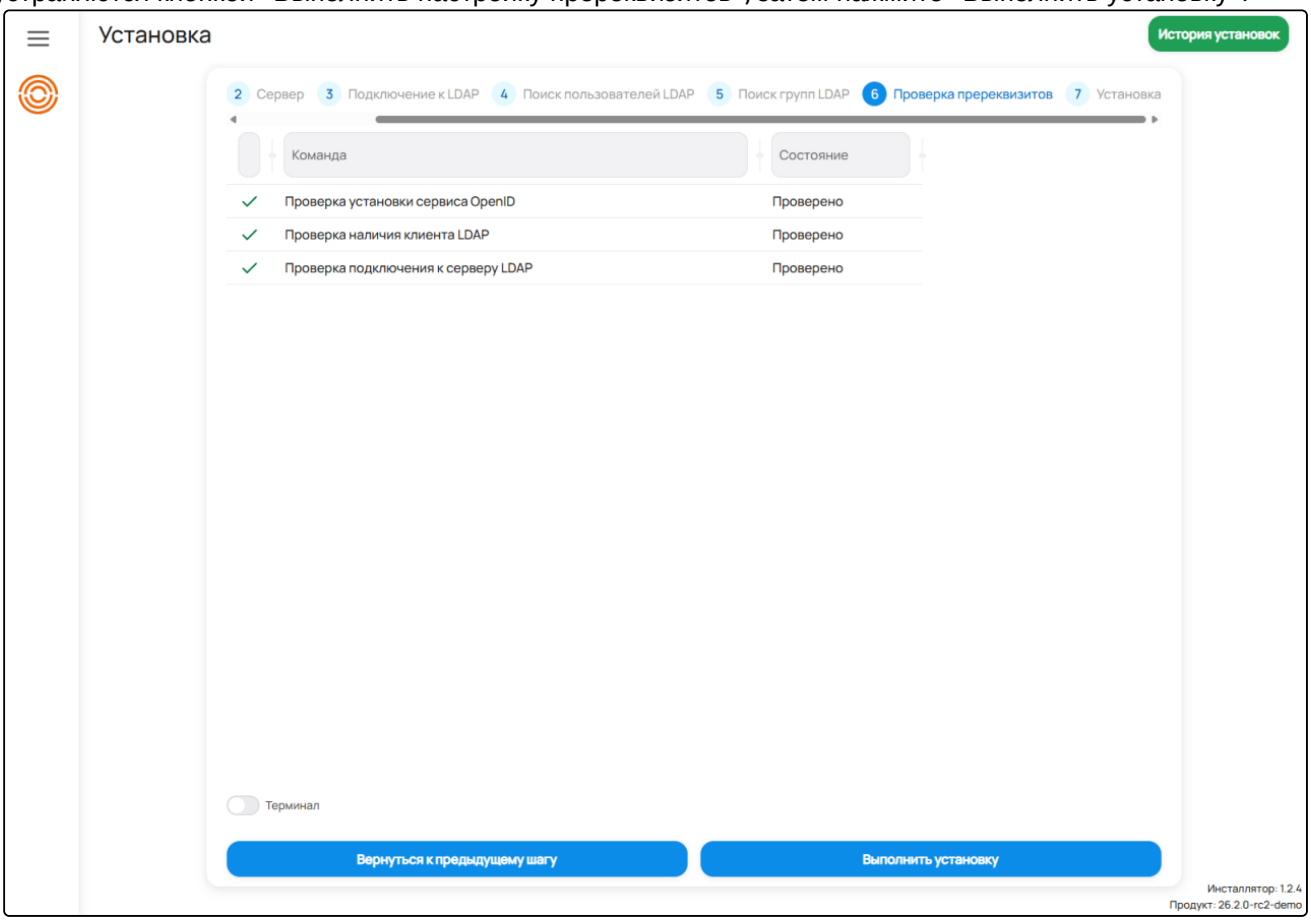
Поиск групп LDAP. Настройте импорт групп: базовый DN поиска групп, фильтр отбора (по умолчанию (objectClass=group)) и атрибут имени группы (для Active Directory обычно cn). Членство в группах

каталога далее сопоставляется с ролями Clearway CA.



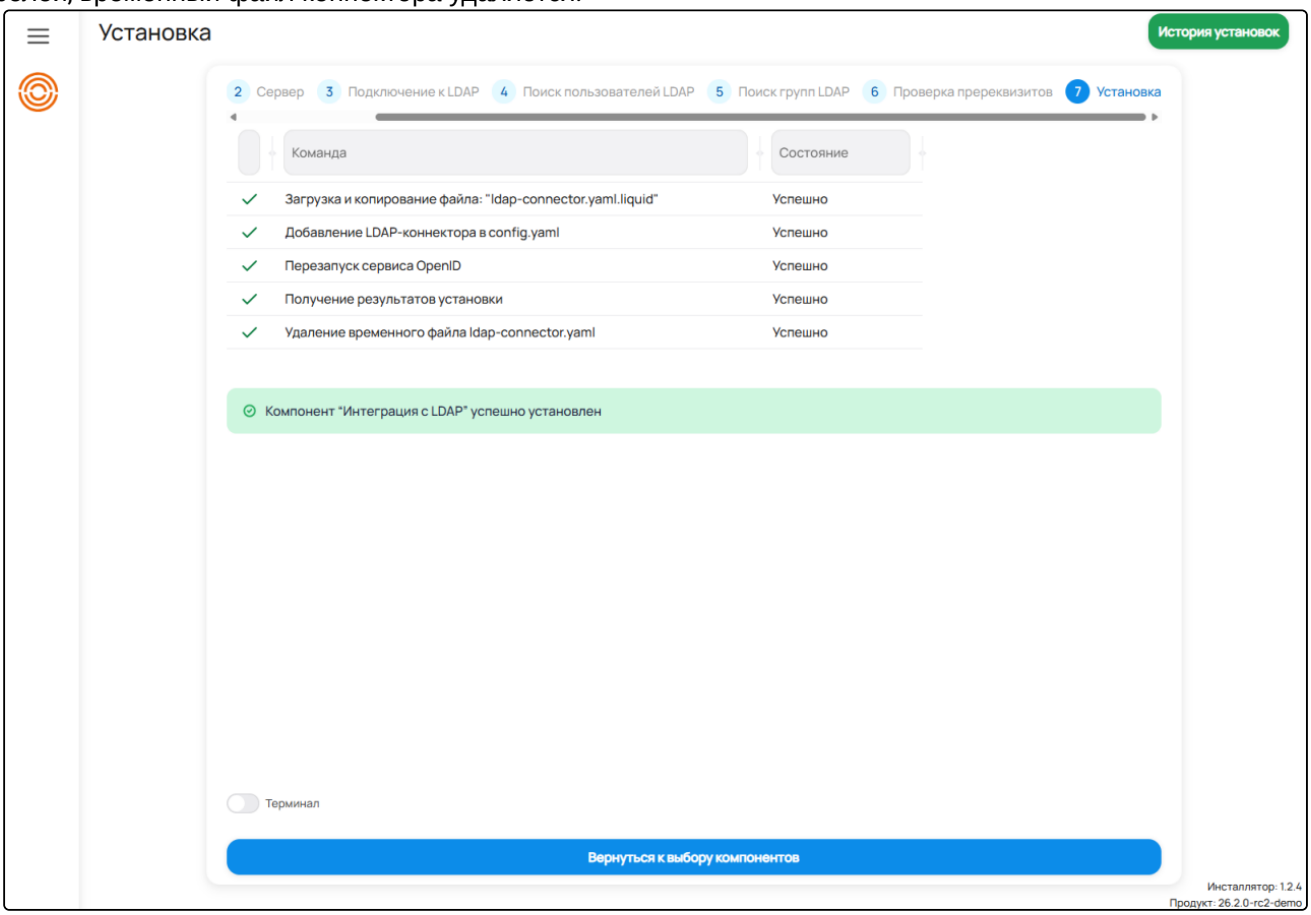
Проверка пререквизитов. Мастер проверяет, что сервис OpenID установлен и запущен, наличие клиента ldapsearch и доступность сервера LDAP с указанными учётными данными. Незакрытые пункты

устраняются кнопкой «Выполнить настройку пререквизитов»; затем нажмите «Выполнить установку».



Установка и результат. Мастер добавляет секцию коннектора LDAP в config.yaml сервиса OpenID и перезапускает его. По завершении пользователи и группы каталога доступны для входа и назначения

ролей; временный файл коннектора удаляется.



10 MS-WSTEP

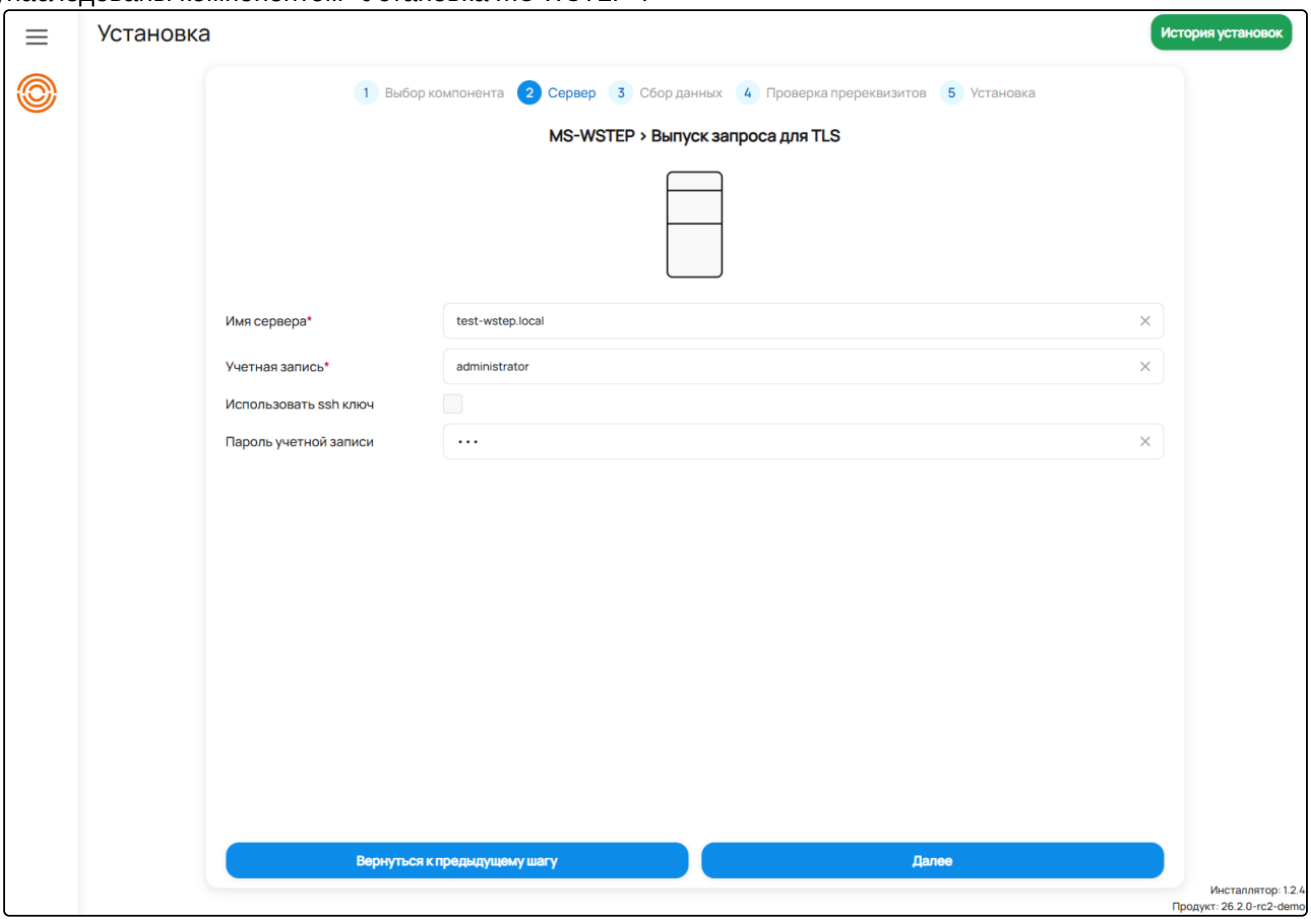
Группа устанавливает службы CEP и CES для регистрации сертификатов Microsoft и их взаимодействия с Clearway CA. Компоненты выполняются последовательно: выпуск TLS-запроса, выпуск сертификата, установка MS-WSTEP, выпуск JWT и настройка MS-WSTEP.

10.1 Выпуск запроса для TLS

Компонент создаёт на сервере каталог $PATH/itc/certs, приватный ключ nginx-tls.key и запрос nginx-tls.csr для имени $HOSTNAME. Приватный ключ остаётся на сервере, CSR передаётся компоненту выпуска сертификата.

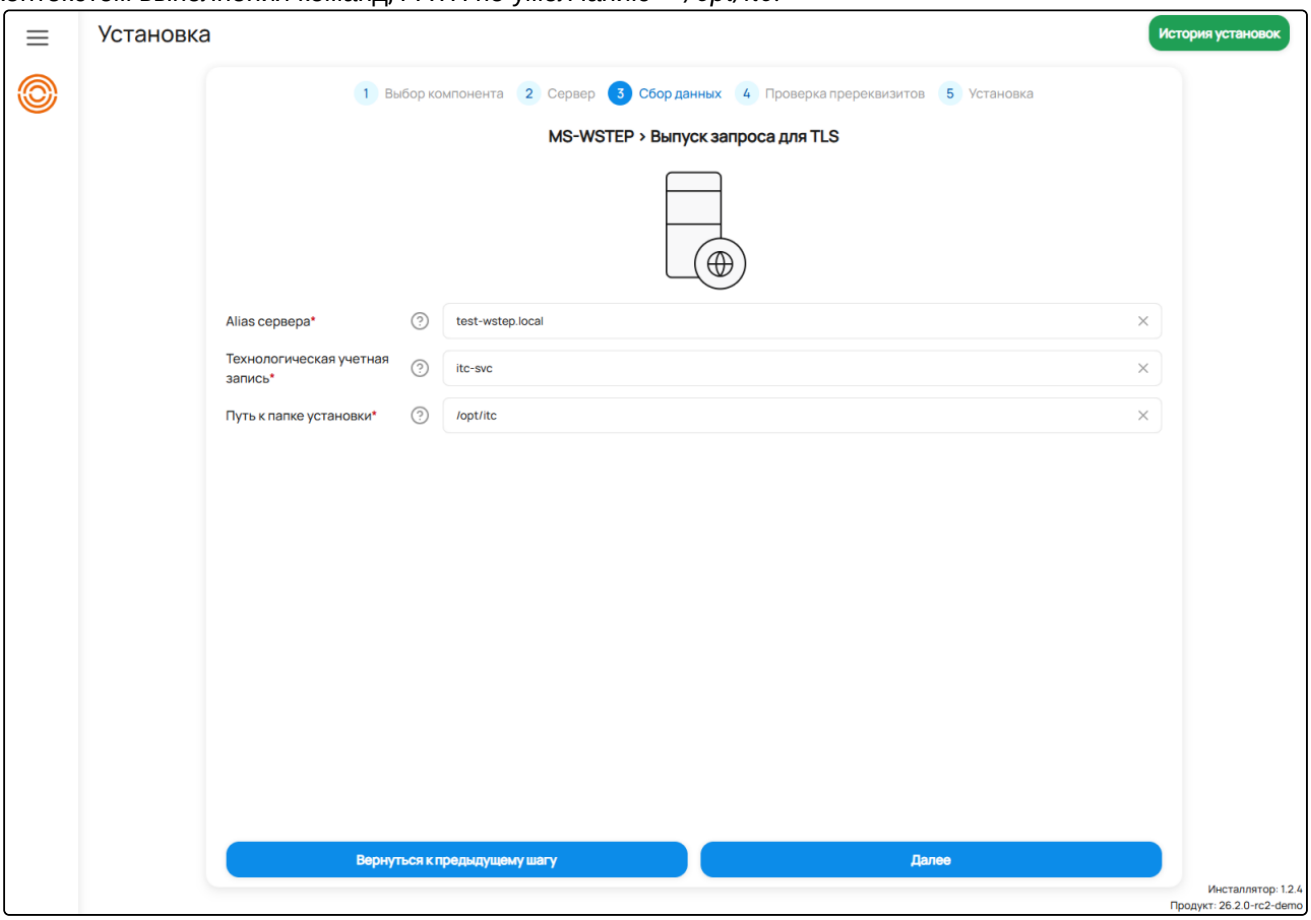
Когда можно пропустить: пропустите этот компонент, если приватный ключ и запрос на TLS-сертификат уже подготовлены на целевом сервере. Приватный ключ должен находиться в $PATH/itc/certs/nginx-tls.key. Если сертификат будет выпускаться Clearway CA, на следующем этапе вручную загрузите подготовленный CSR; если готовый сертификат уже есть, можно пропустить и этап «Выпуск сертификата». На этапе «Установка MS-WSTEP» вручную укажите параметры целевого сервера, HOSTNAME, USER_NAME и PATH.

Сервер. Укажите SSH-адрес целевого сервера и учётную запись подключения. Эти параметры будут унаследованы компонентом «Установка MS-WSTEP».



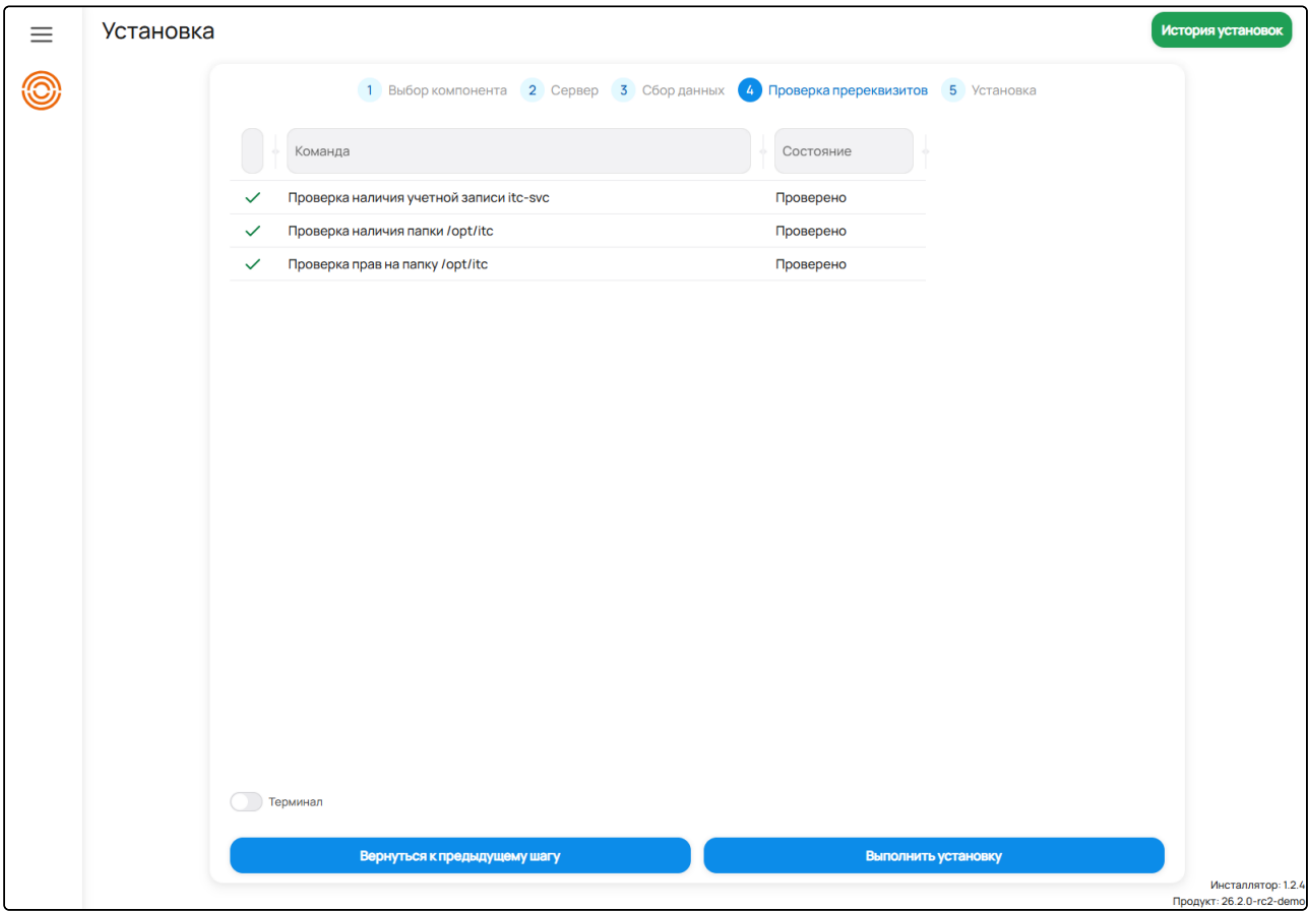
Сбор данных. HOSTNAME задаёт CN и DNS subjectAltName будущего TLS-сертификата; если поле не менять, используется hostname ОС. USER_NAME (по умолчанию itc-svc) станет владельцем каталога и

контекстом выполнения команд, PATH по умолчанию – */opt/itc*.



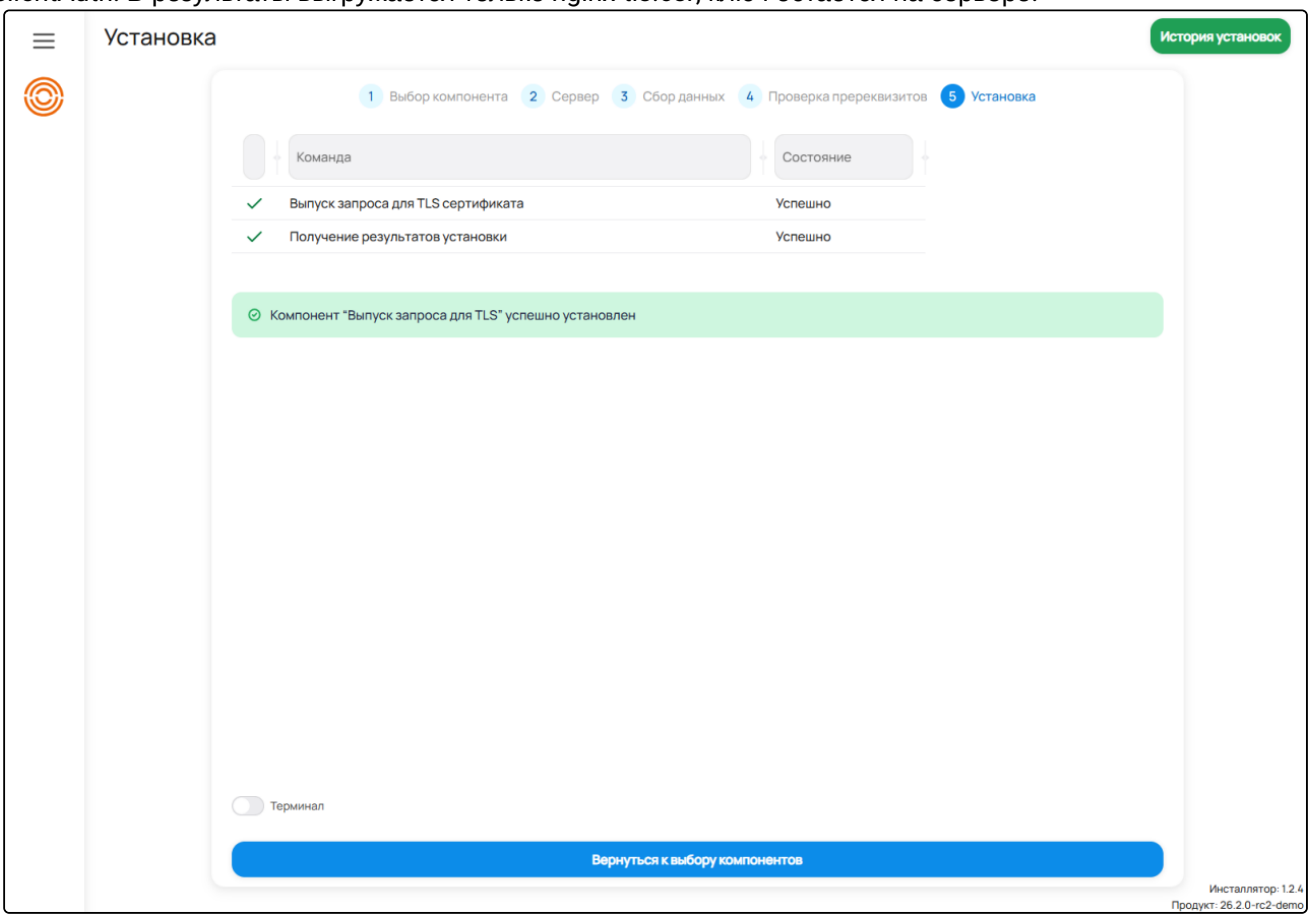
Проверка пререквизитов. Проверяется существование $USER_NAME, каталога $PATH и владение каталогом со стороны $USER_NAME. Настройка пререквизитов при необходимости создаёт

пользователя и каталог и выполняет chown.



Установка и результат. Выполняется openssl req: создаются незашифрованный приватный ключ $PATH/itc/certs/nginx-tls.key и CSR nginx-tls.csr с SHA-256, CN/SAN=$HOSTNAME и назначениями serverAuth/

clientAuth. В результаты выгружается только nginx-tls.csr; ключ остаётся на сервере.



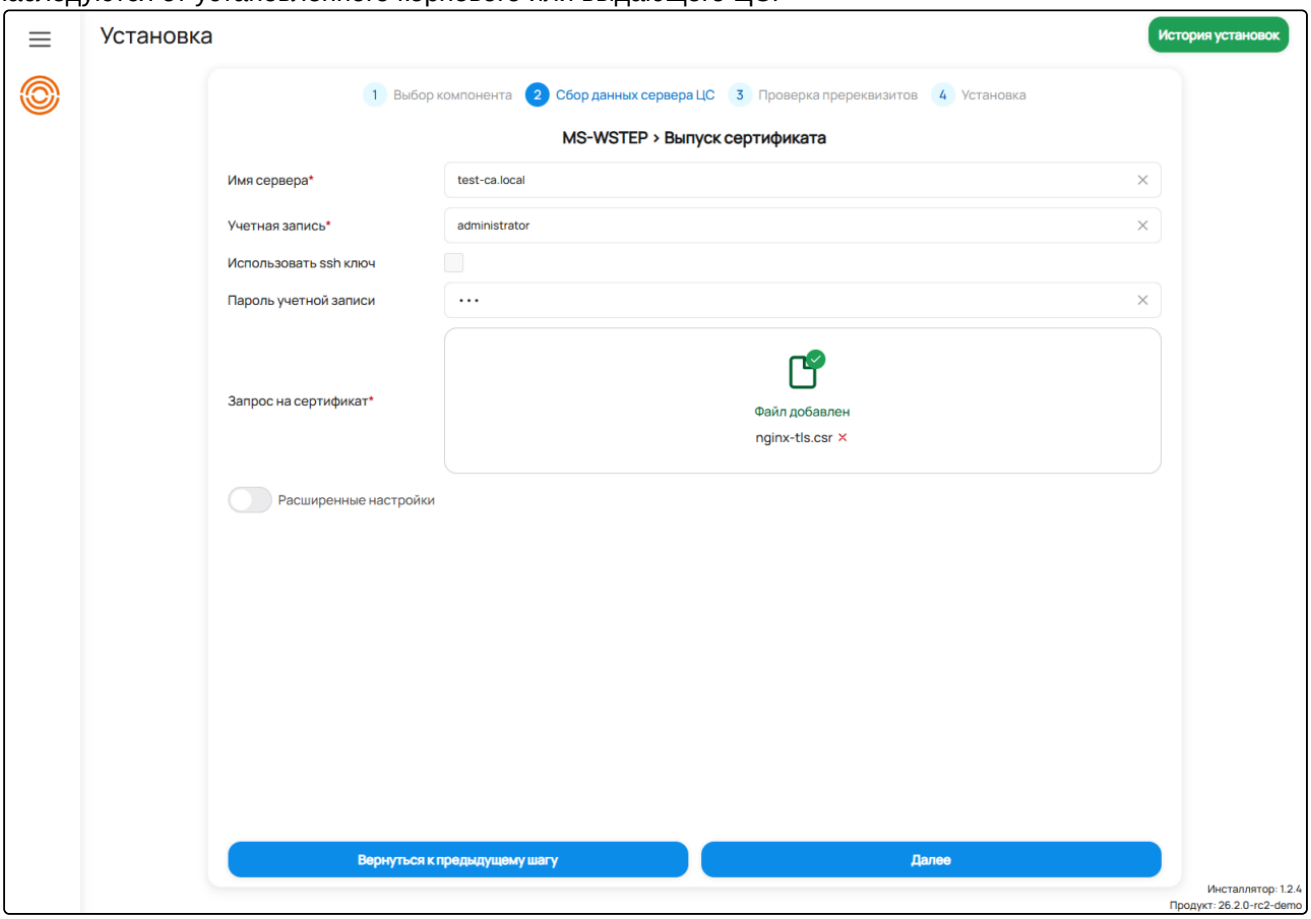
10.2 Выпуск сертификата

Компонент подключается к установленному Clearway CA и через mclient выпускает по nginx-tls.csr сертификат с шаблоном tls. Готовый nginx-tls.crt передаётся компоненту установки MS-WSTEP.

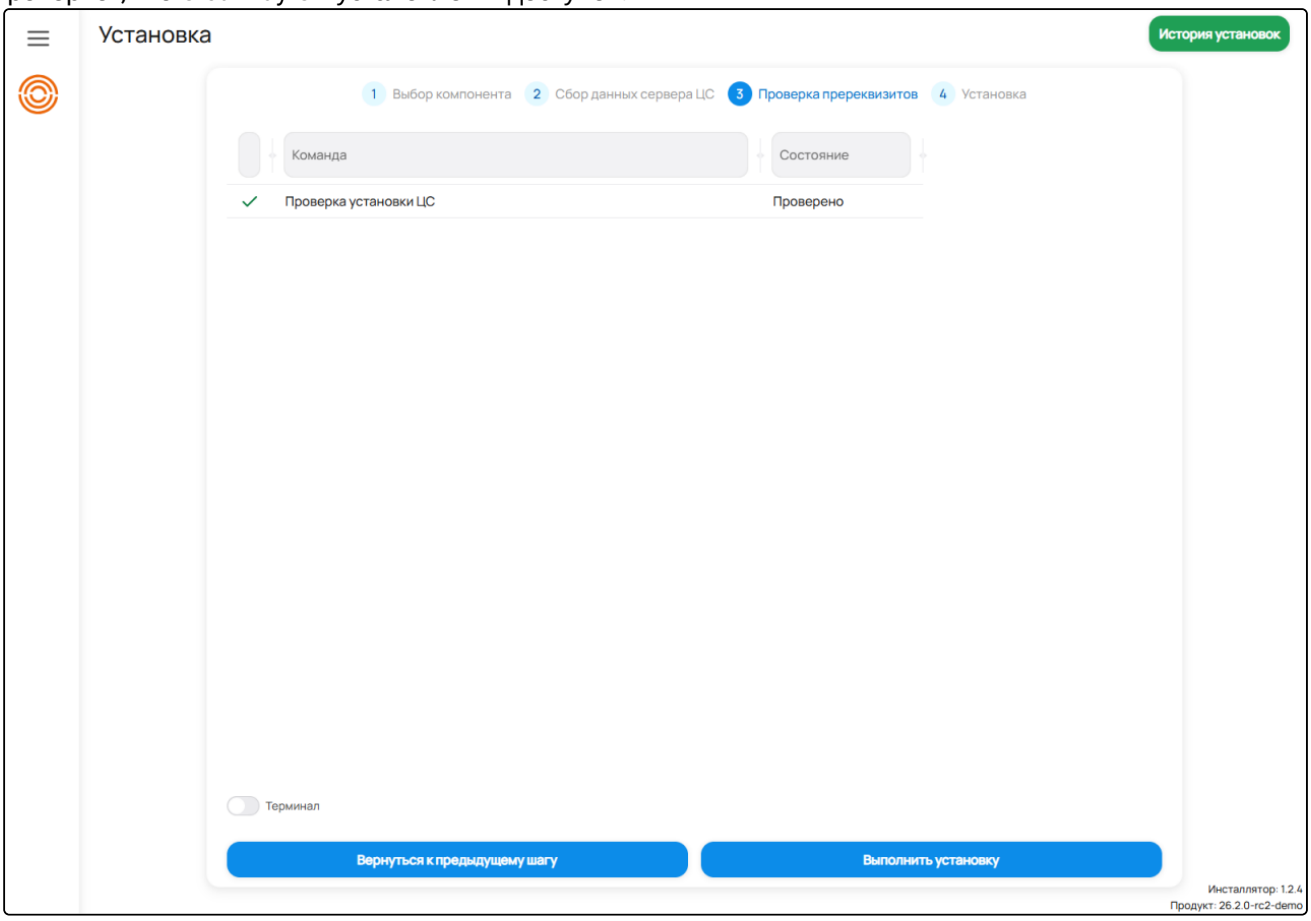
Когда можно пропустить: пропустите этот компонент, если действующий TLS-сертификат для MS-WSTEP уже выпущен. На этапе «Установка MS-WSTEP» вручную загрузите его в поле «TLS-сертификат» (CERTIFICATE_NGINX). Сертификат должен соответствовать имени HOSTNAME и приватному ключу $PATH/itc/certs/nginx-tls.key.

Сбор данных сервера ЦС. CSR предыдущего компонента загружается во временный файл. Имя результата берётся из имени CSR, шаблон выпуска для MS-WSTEP — tls; USER_NAME и PATH

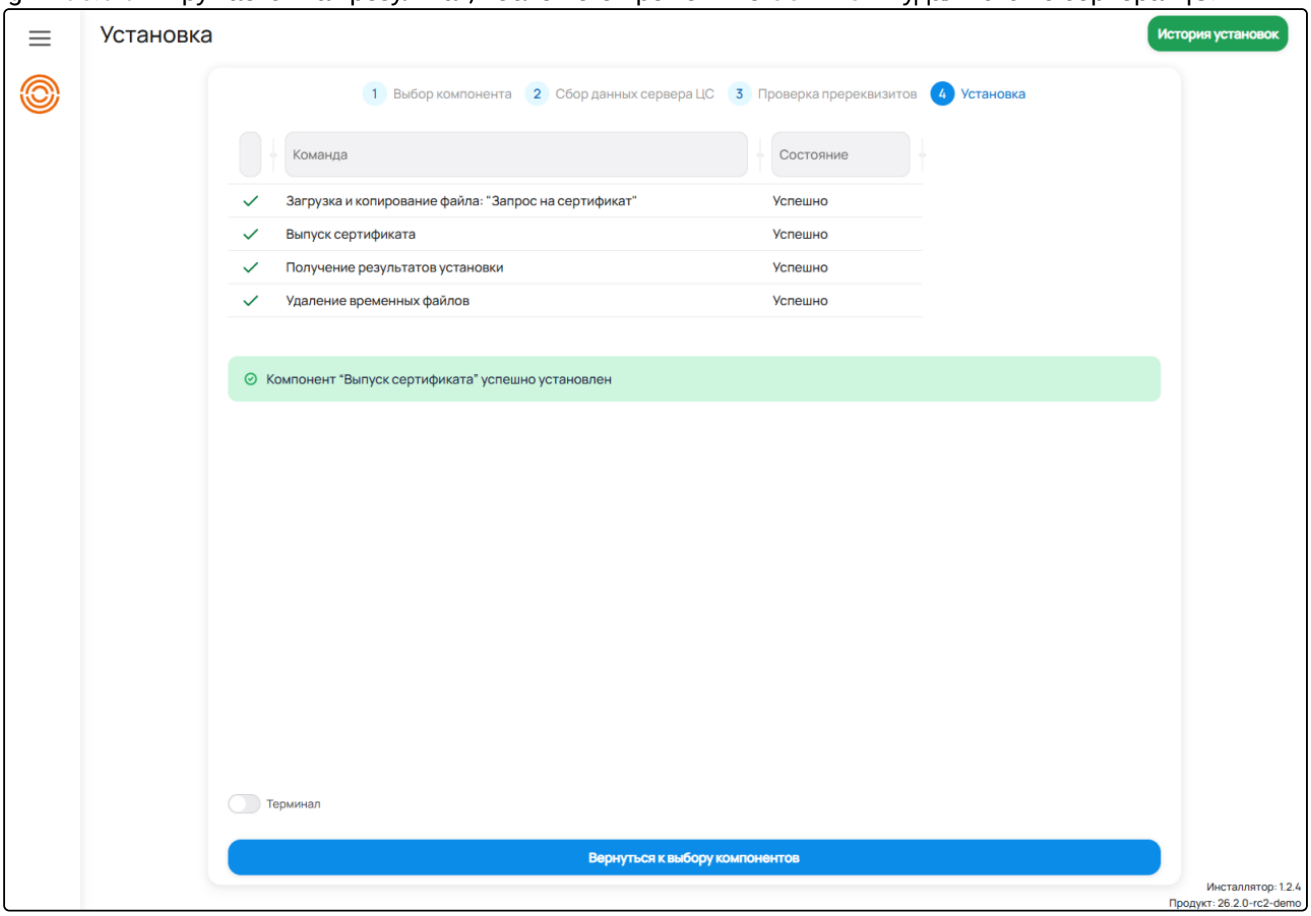
наследуются от установленного корневого или выдающего ЦС.



Проверка пререквизитов. Команда $PATH/mclient ping с конфигурацией $PATH/conf/mclient.yml проверяет, что Clearway CA установлен и доступен.



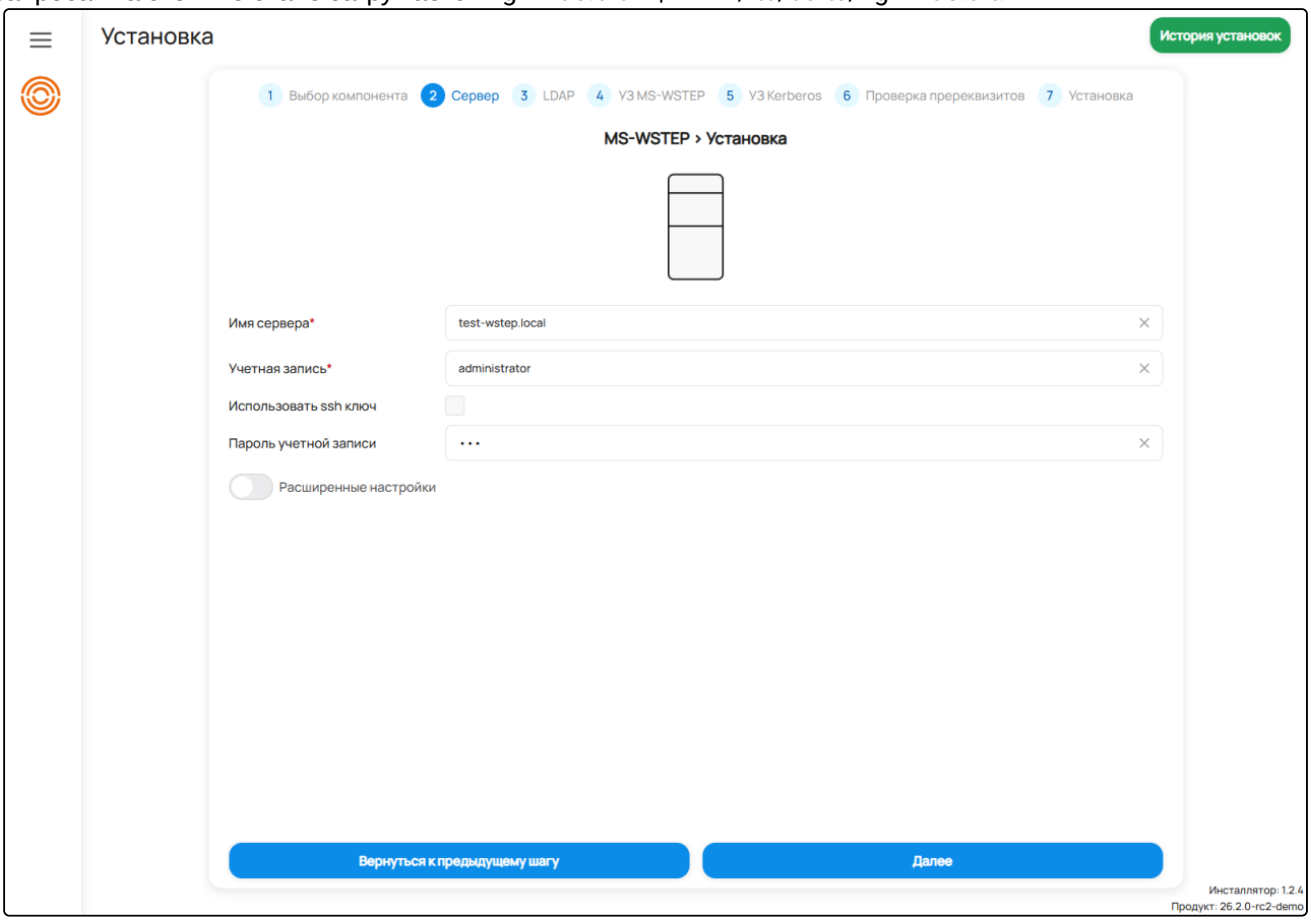
Установка и результат. Команда mclient ca выпускает по CSR сертификат с шаблоном tls. Сертификат nginx-tls.crt выгружается как результат, после чего временные CSR и CRT удаляются с сервера ЦС.



10.3 Установка MS-WSTEP

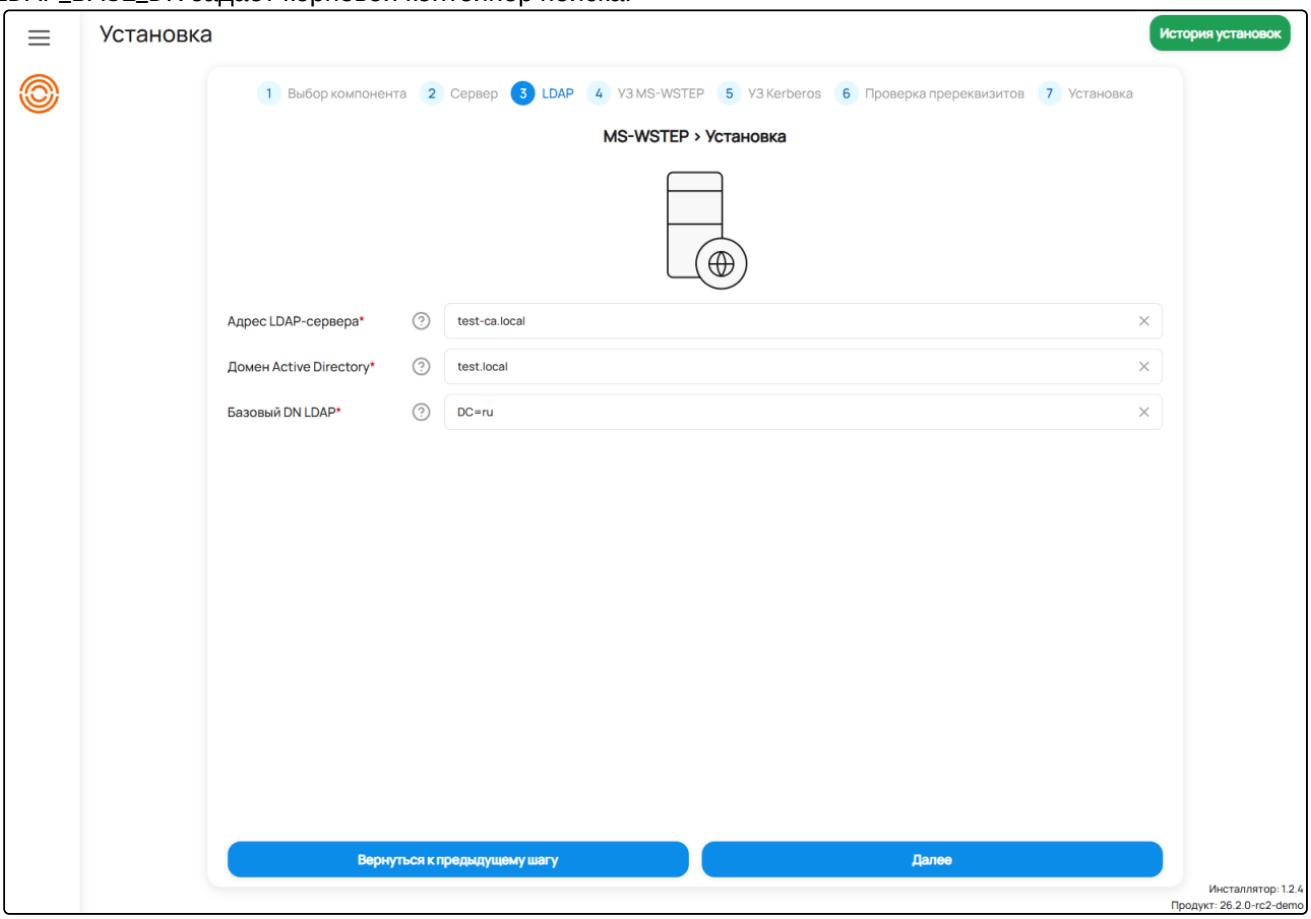
Компонент вводит сервер в домен Active Directory, настраивает Kerberos и LDAP, разворачивает Nginx и две пользовательские службы: CEP для публикации политик и CES Adapter для выпуска сертификатов через Clearway CA.

Сервер. SSH-параметры, HOSTNAME, USER_NAME и PATH наследуются от компонента выпуска TLS-запроса. На этом же этапе загружается nginx-tls.crt в $PATH/itc/certs/nginx-tls.crt.

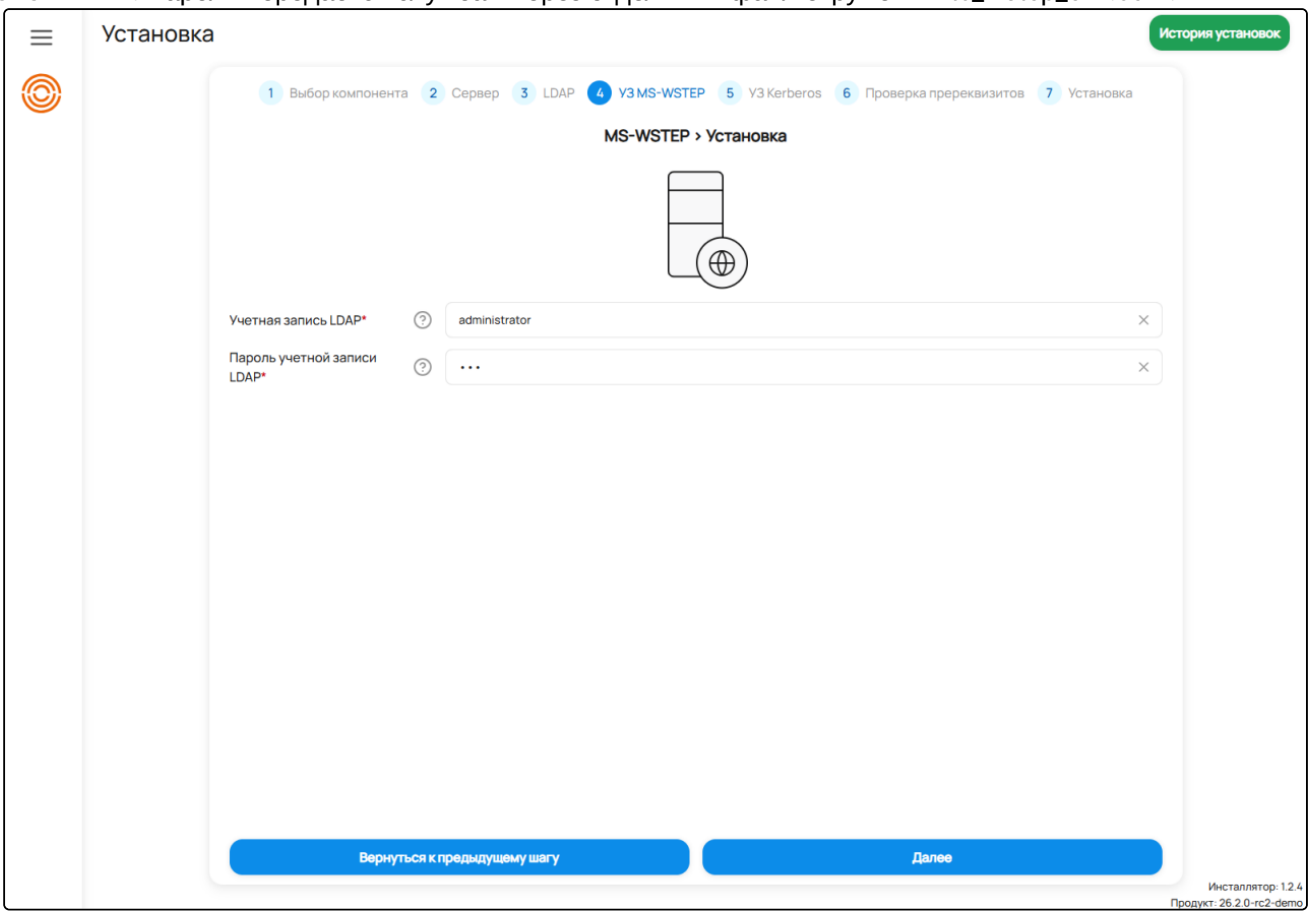


LDAP. LDAP_HOST — домен-контроллер, к которому CEP/CES обращаются за шаблонами, точками выдачи и пользователями. AD_DOMAIN используется для ввода сервера в домен и Kerberos,

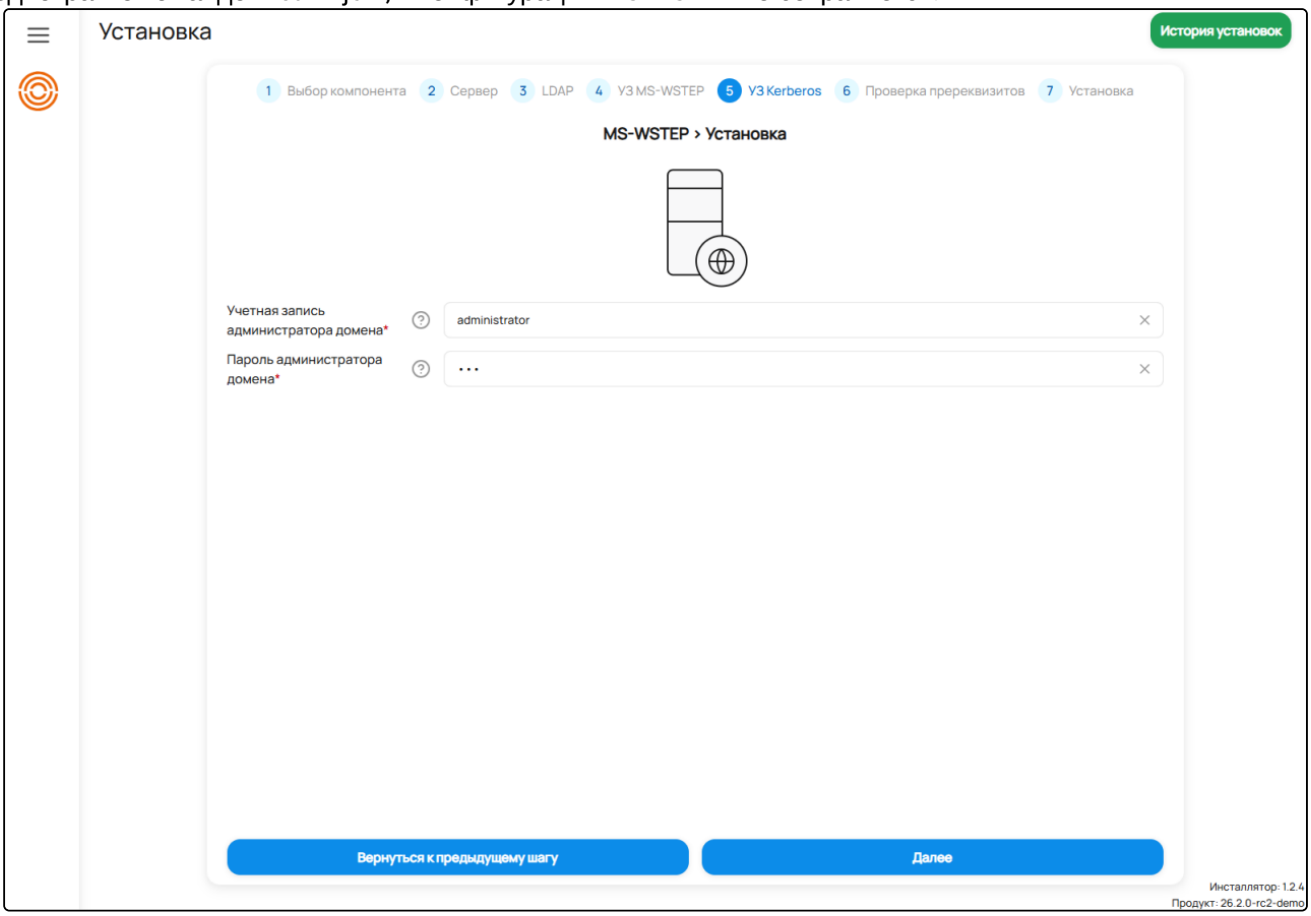
LDAP_BASE_DN задаёт корневой контейнер поиска.



УЗ MS-WSTEP. LDAP_LOGIN и LDAP_PASSWORD задают сервисную учётную запись подключения CEP/CES к LDAP. Пароль передаётся службам через отдельный файл окружения itc_wstep_env.conf.

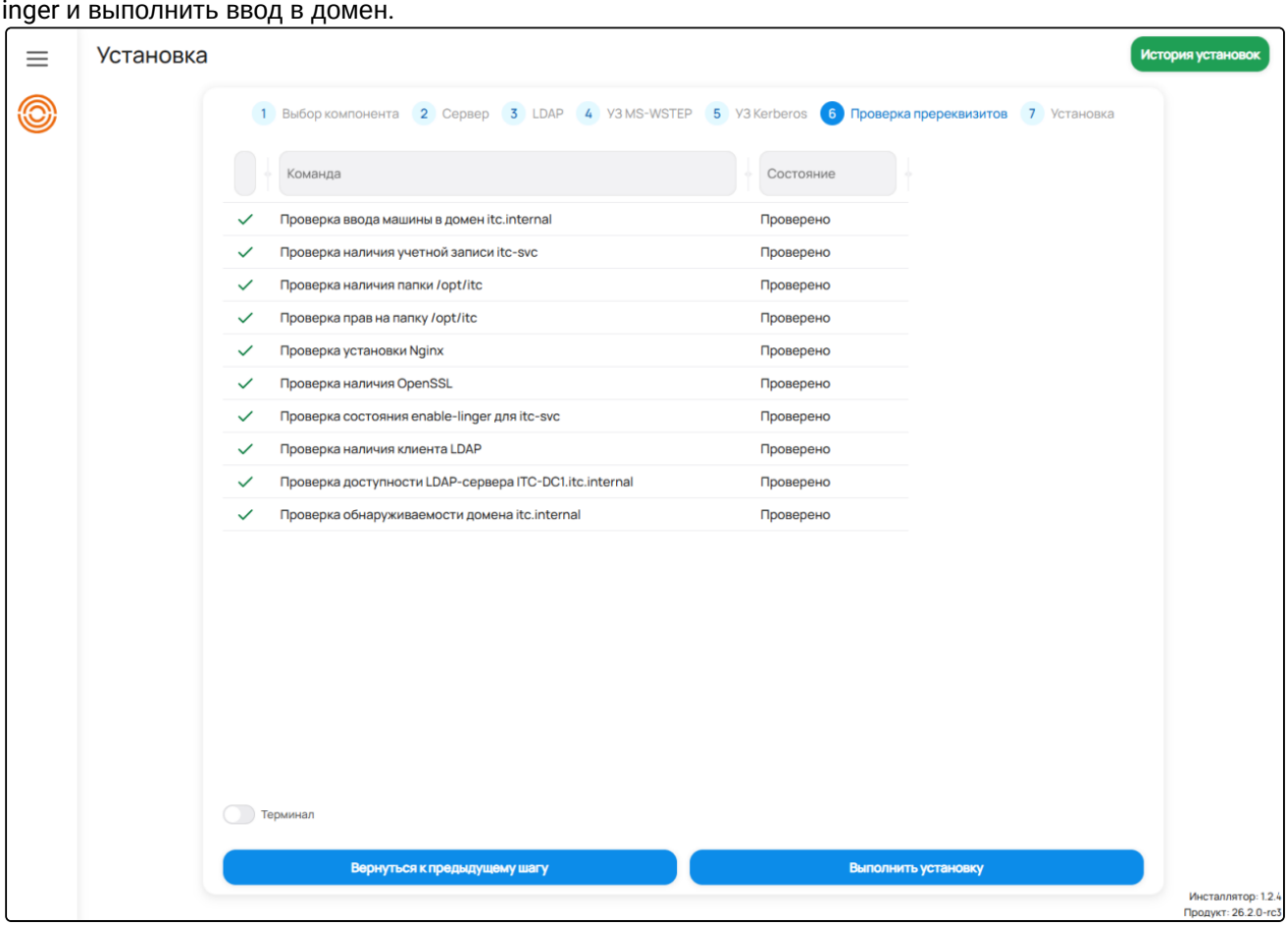


УЗ Kerberos. KRB_AD_ADMIN должен иметь право вводить компьютеры в домен. Пароль используется однократно командой realm join, в конфигурации MS-WSTEP не сохраняется.



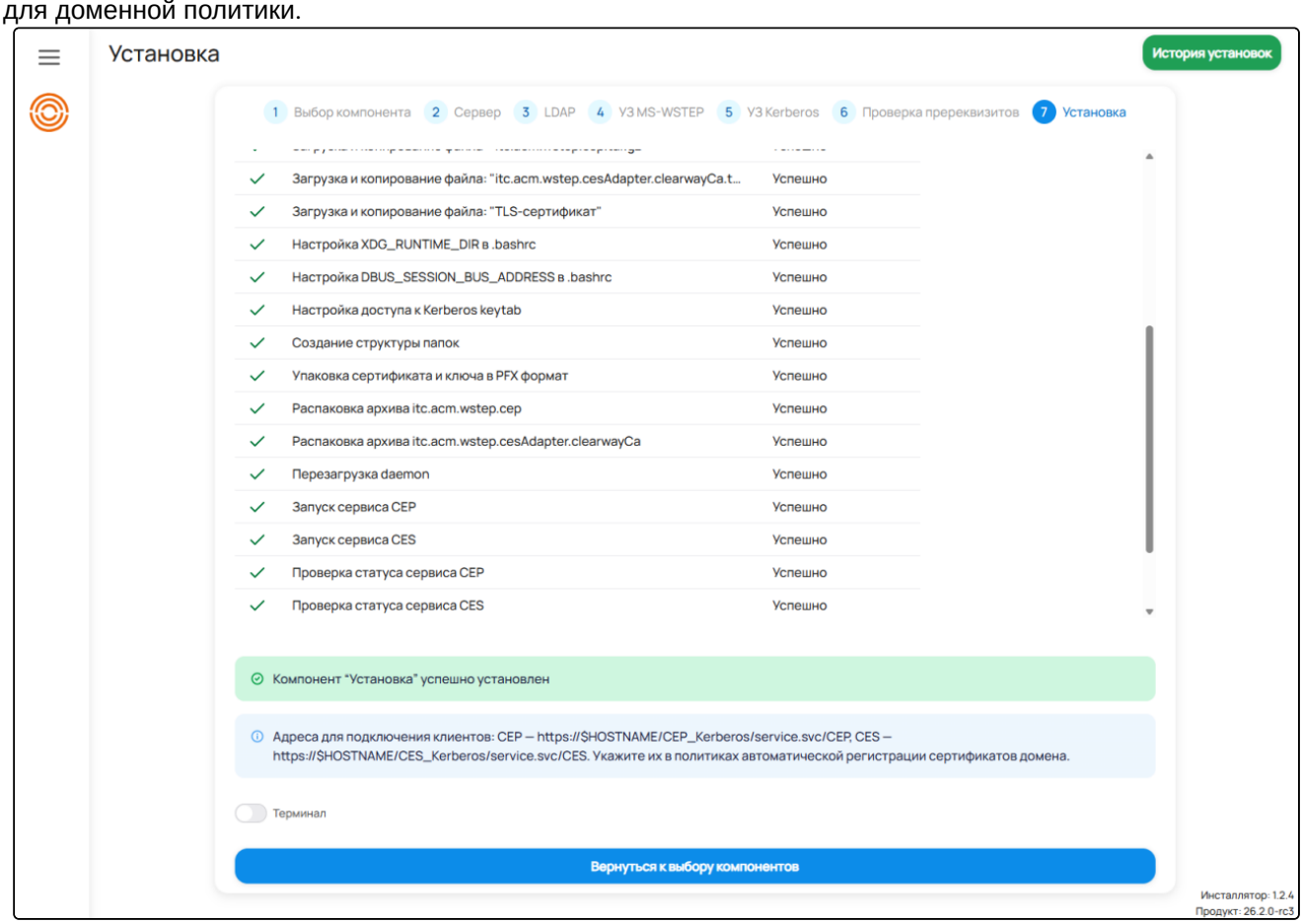
Проверка пререквизитов. Проверяются членство сервера в домене и */etc/krb5.keytab*, учётная запись и каталог, права, Nginx, OpenSSL, enable-linger, ldapsearch, доступность LDAP и обнаруживаемость домена через realm discover. Настройка может установить пакеты, создать пользователя и каталог, включить

linger и выполнить ввод в домен.



Установка и результат. Настраиваются XDG_RUNTIME_DIR и D-Bus, доступ itc-svc к Kerberos keytab, каталоги и конфигурации CEP/CES. TLS-сертификат и оставшийся на сервере ключ упаковываются в nginx-tls.pfx; распаковываются приложения CEP и CES Adapter, регистрируются и запускаются wstepCep.service и wstepCesAdapter.service, настраивается Nginx. Результат содержит адреса CEP и CES

для доменной политики.

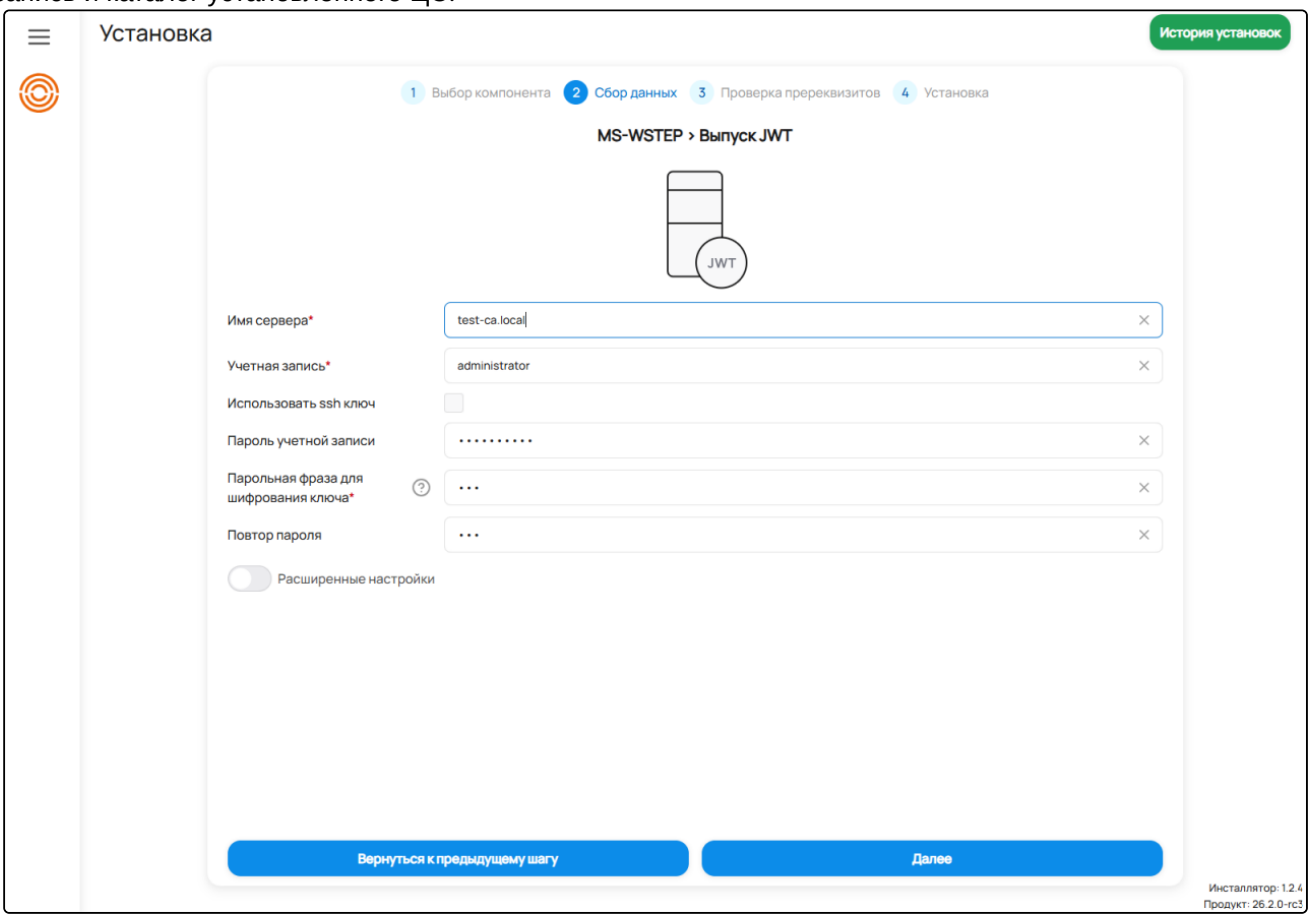


10.4 Выпуск JWT

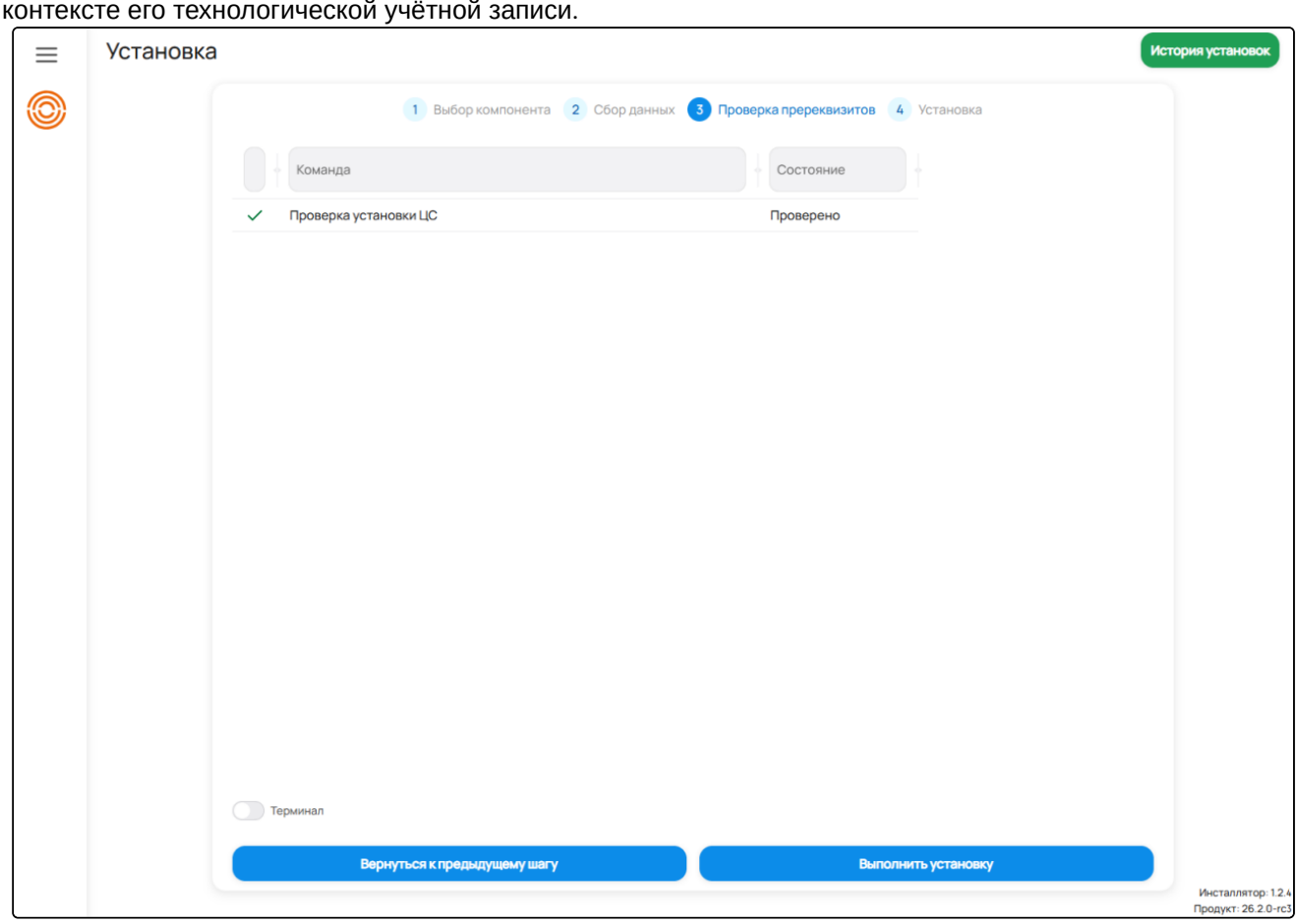
Компонент создаёт для сервиса ms-wstep JWT и зашифрованный приватный ключ, используемые CES Adapter для аутентификации и авторизации при обращении к Clearway CA.

Сбор данных. Для сервиса NAME_SERVICE=ms-wstep задаётся парольная фраза шифрования ключа; расширенные параметры определяют роль JWT (по умолчанию admin), технологическую учётную

запись и каталог установленного ЦС.

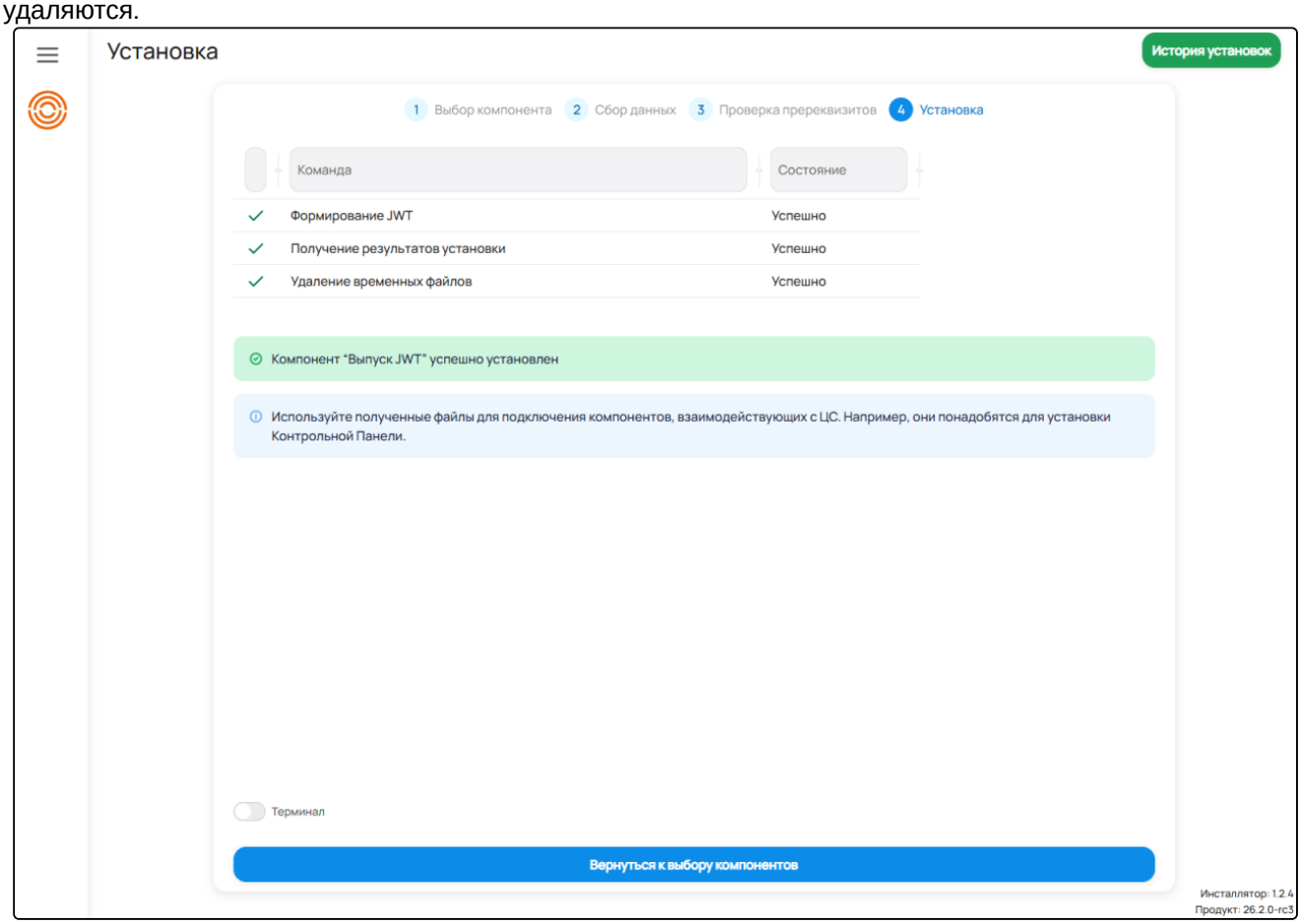


Проверка пререквизитов. Команда mclient ping проверяет доступность установленного Clearway CA в контексте его технологической учётной записи.



Установка и результат. Генерируются RSA-ключ и самоподписанный сертификат, затем mclient mkjwt создаёт токен с именем ms-wstep и выбранной ролью. Приватный ключ преобразуется в PKCS#8 и шифруется AES-256-CBC. Выгружаются ms-wstep.encrypted.key и ms-wstep.jwt; временные файлы

удаляются.

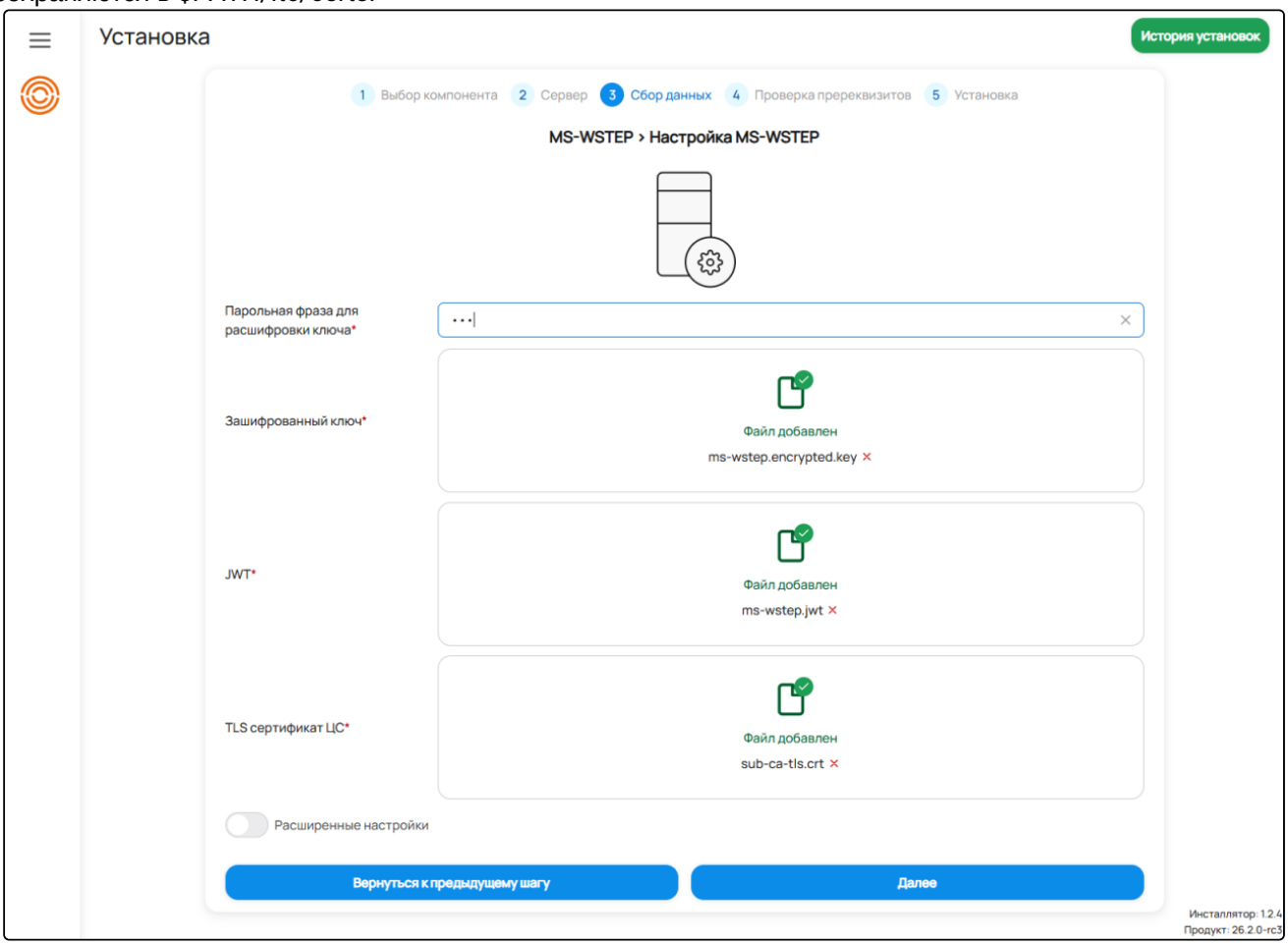


10.5 Настройка MS-WSTEP

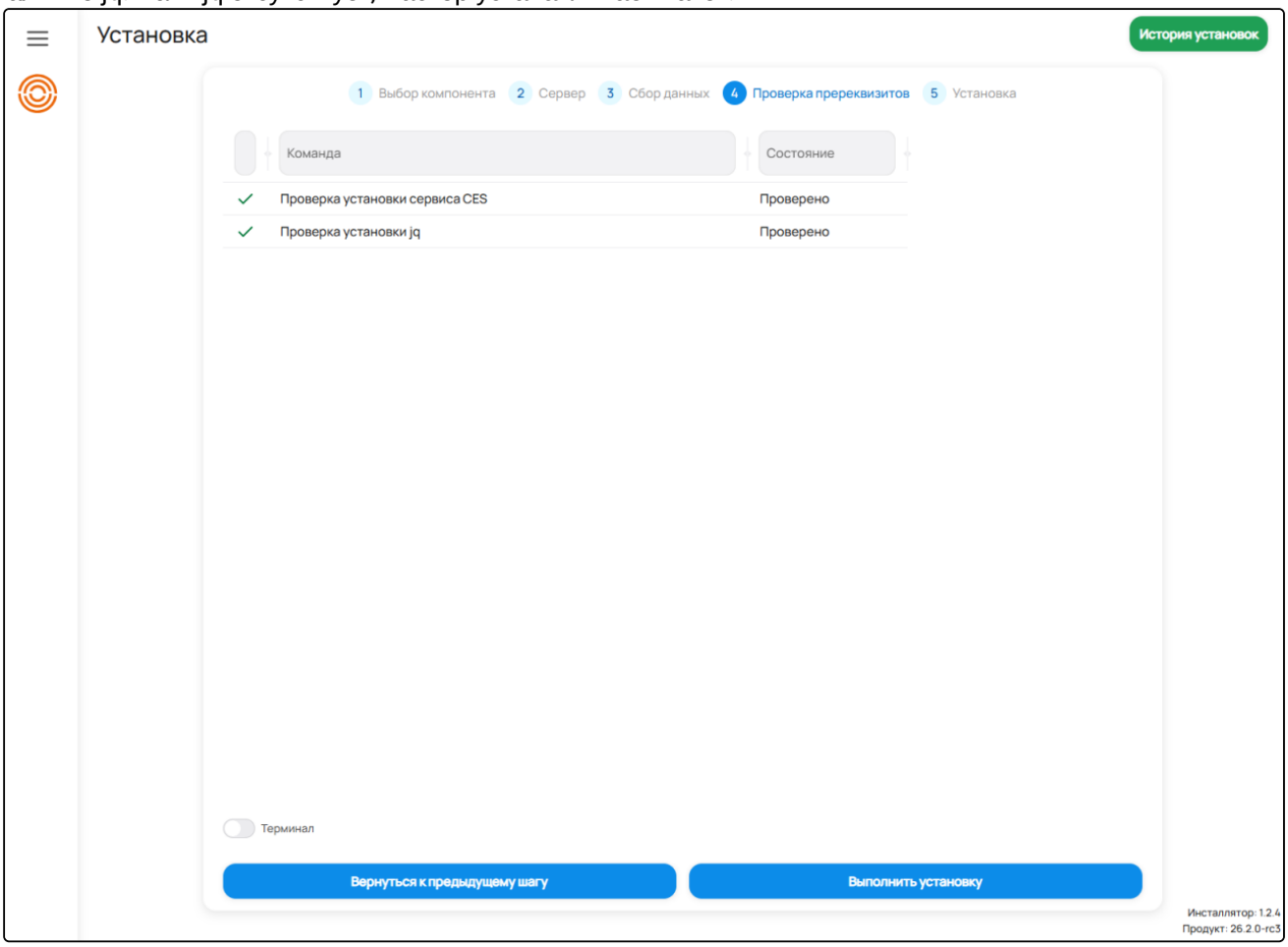
Компонент добавляет параметры Clearway CA в конфигурацию CES Adapter, устанавливает ключ, JWT и TLS-сертификат ЦС, перезапускает CES и формирует файлы регистрации политики сертификатов в Active Directory.

Сбор данных. Укажите парольную фразу от выпущенного ключа и загрузите ENCRYPTED_KEY, JWT и TLS-сертификат Clearway CA. NAME_CA и HOSTNAME_CA определяют имя кластера и адрес ЦС; файлы

сохраняются в $PATH/itc/certs.

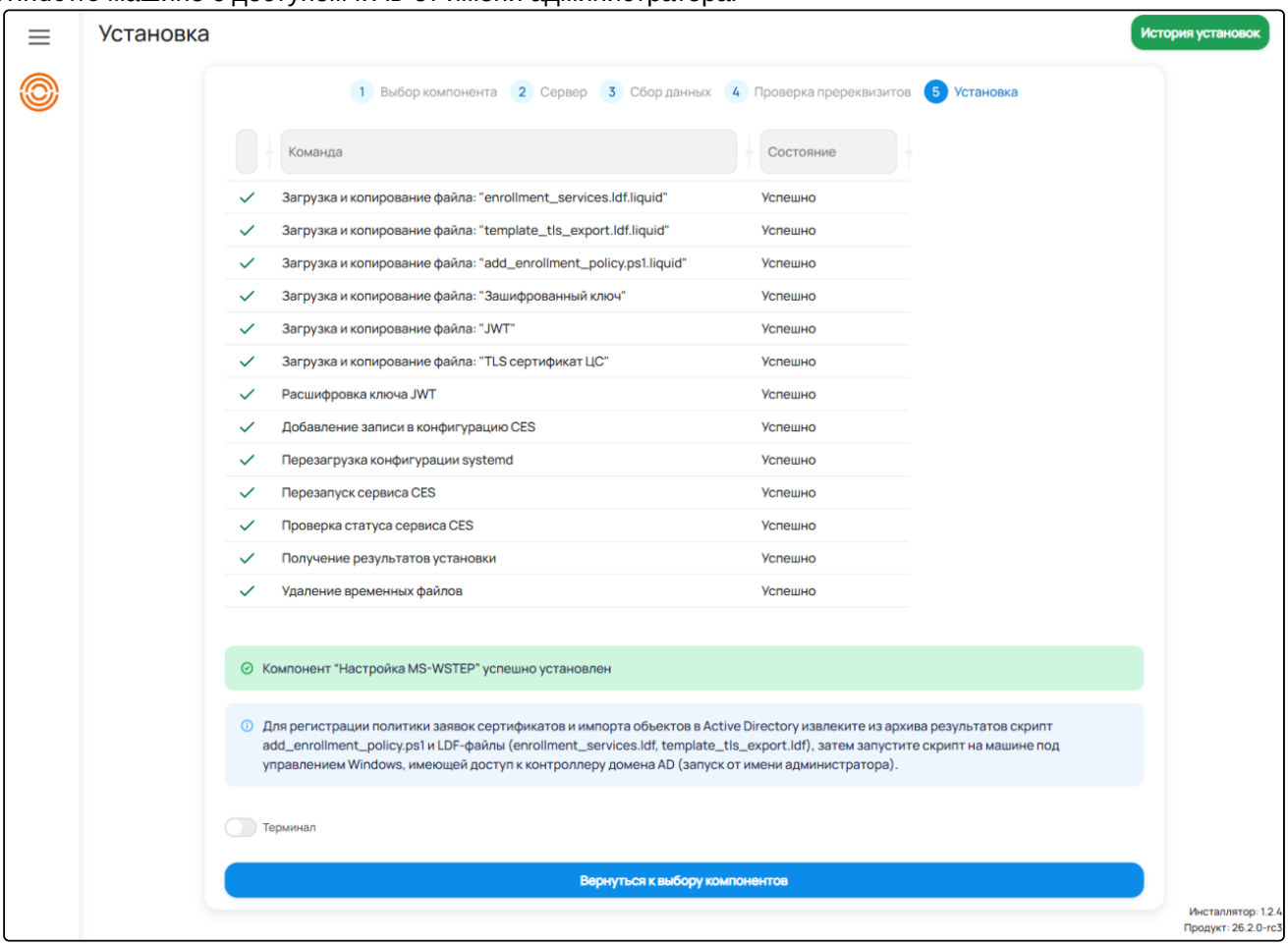


Проверка пререквизитов. Проверяется активность пользовательской службы wstepCesAdapter.service и наличие jq. Если jq отсутствует, мастер устанавливает пакет.



Установка и результат. Ключ JWT расшифровывается, а jq добавляет в конфигурацию CES Adapter кластер Clearway CA, шаблон tls, URL https://$HOSTNAME_CA:9443 и пути к TLS-сертификату, ключу и JWT. Затем выполняются systemctl --user daemon-reload, перезапуск и проверка CES. В результаты выгружаются enrollment_services.ldf, template_tls_export.ldf и add_enrollment_policy.ps1; их запускают на

Windows-машине с доступом к AD от имени администратора.



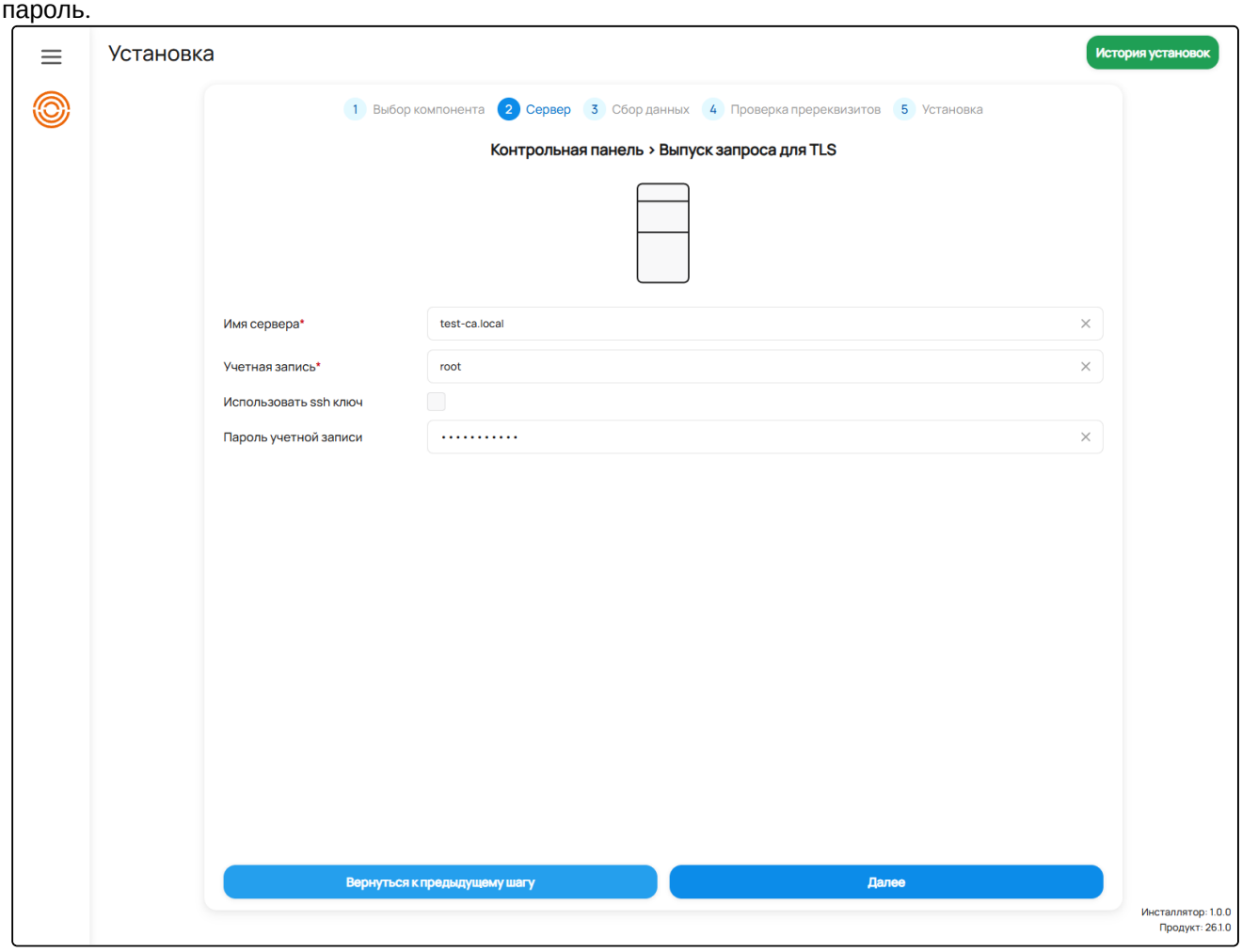
11 Контрольная панель

Группа разворачивает графическую панель управления центром сертификации — веб-интерфейс оператора, работающий за Nginx с входом через OpenID/JWT. Компоненты устанавливаются в следующем порядке: «Выпуск запроса на TLS» (nginx-tls.csr), «Выпуск сертификата» (подпись CSR на ЦС), «Контрольная панель» (backend на порту 8407 и SPA), «Выпуск JWT» (учётные данные для доступа панели к ЦС) и «Настройка» (регистрация ЦС в панели). Каждый компонент передаёт результат-файл следующему.

11.1 Выпуск запроса на TLS

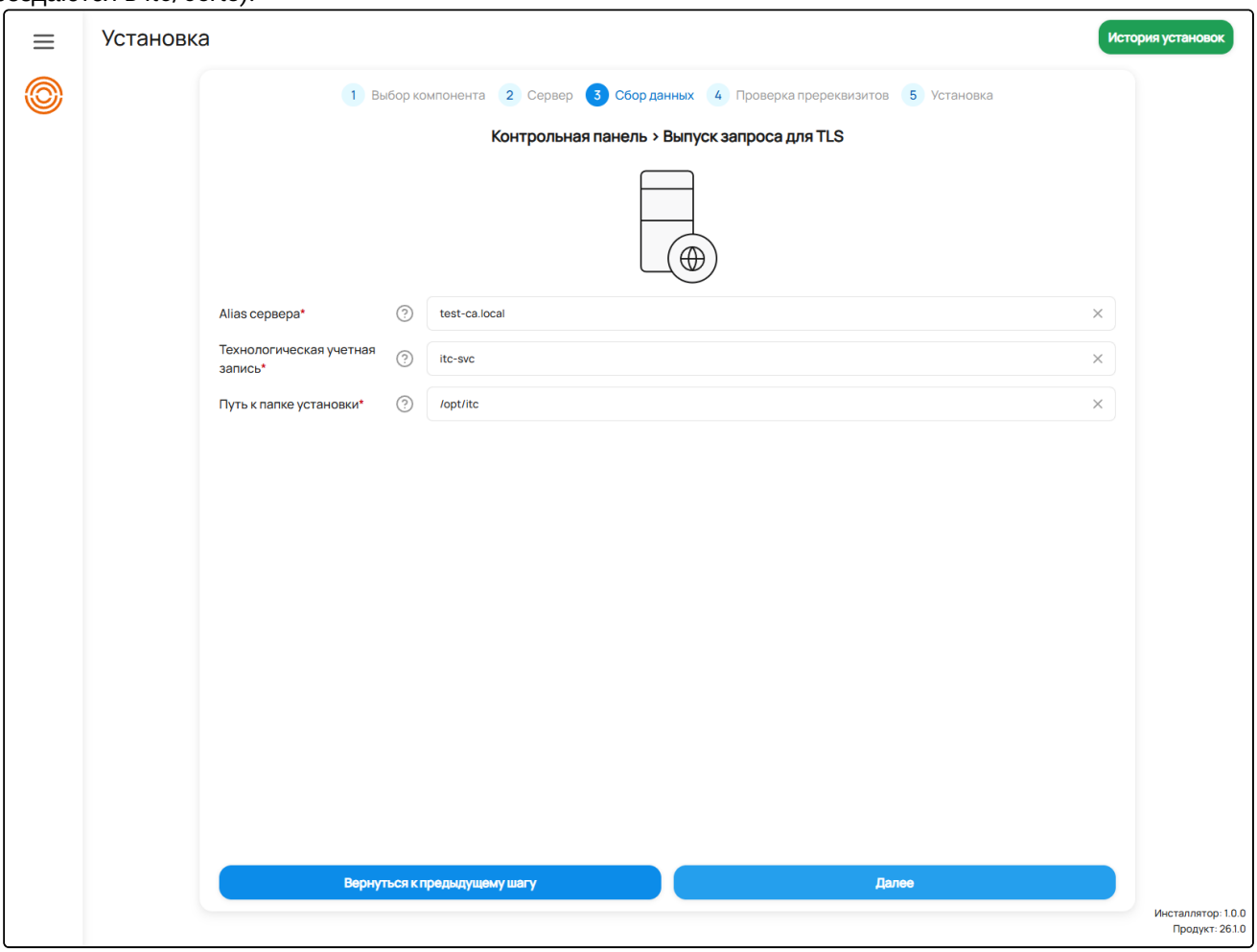
Компонент генерирует на сервере приватный ключ и запрос на сертификат (CSR) для TLS-соединения Nginx.

Сервер. Укажите параметры подключения по SSH к серверу Контрольной панели: имя сервера (Host) и учётную запись. Для входа установите флажок «Использовать ssh ключ» либо снимите его и введите пароль.



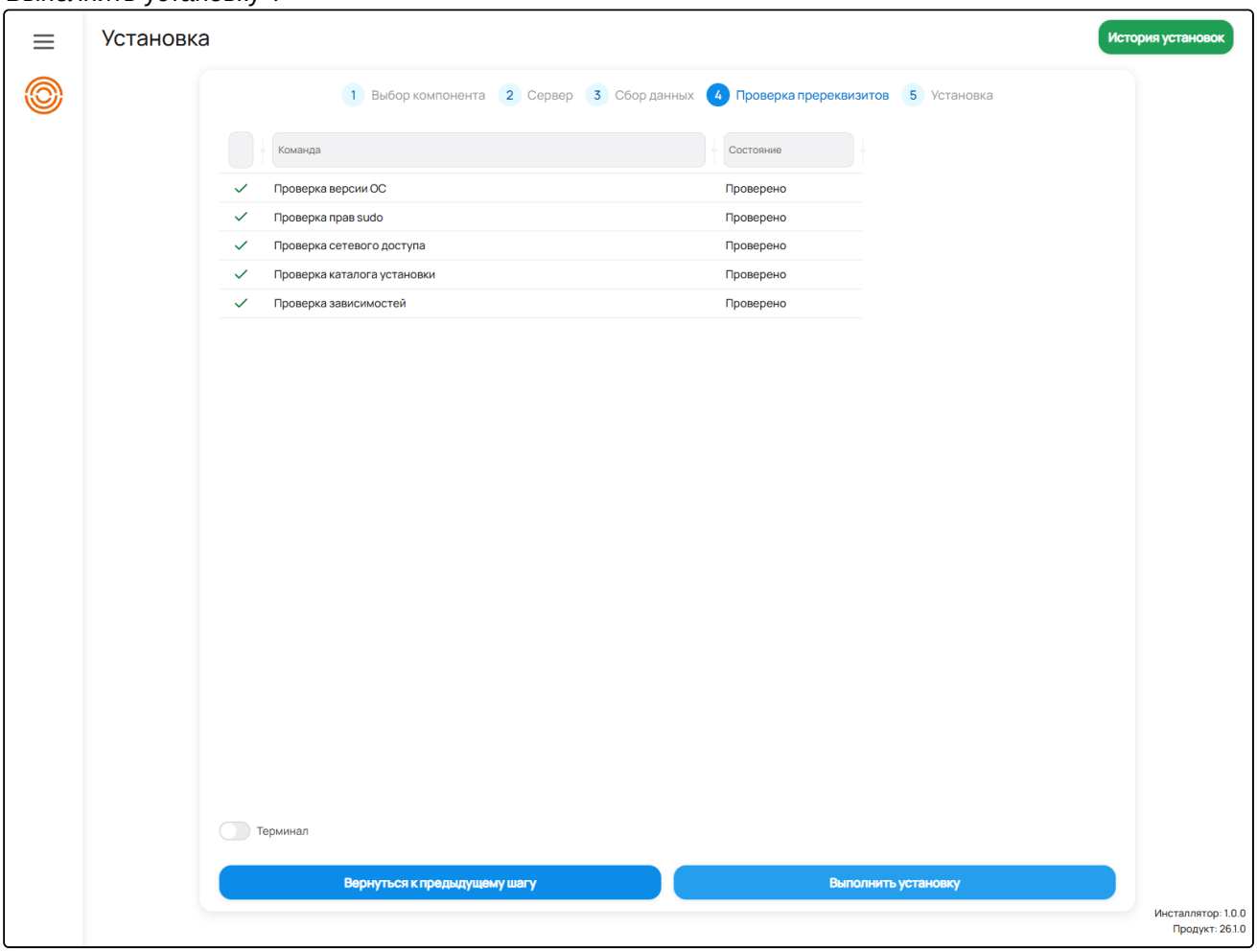
Сбор данных. Заполните переменные компонента: HOSTNAME — имя (alias), на которое выпускается TLS-сертификат (по умолчанию берётся имя хоста ОС); USER_NAME — технологическая учётная запись-владелец (по умолчанию itc-svc); PATH — каталог установки (по умолчанию */opt/itc*; ключ и CSR

создаются в itc/certs).



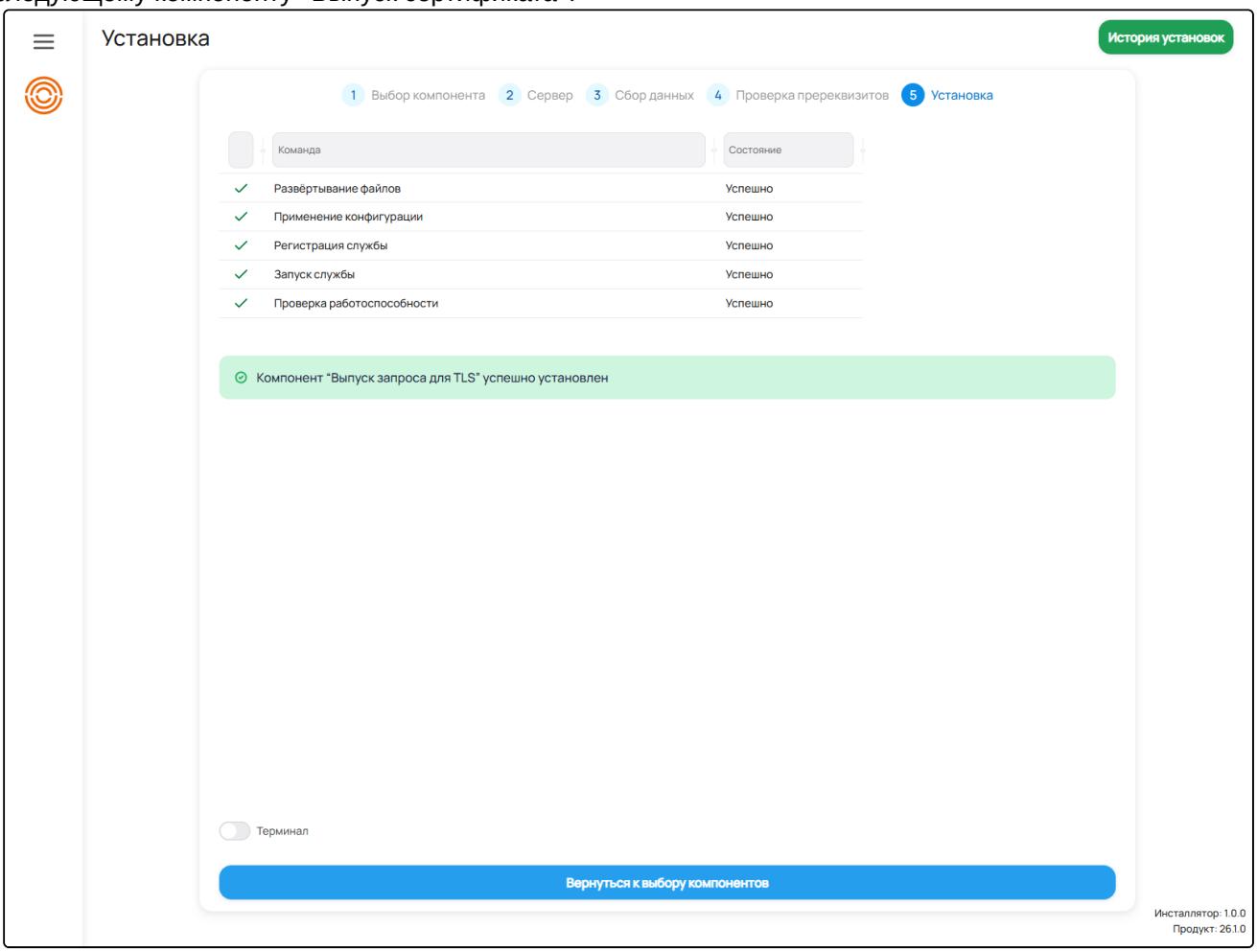
Проверка пререквизитов. В таблице показаны проверки: наличие учётной записи $USER_NAME, наличие каталога и корректность прав на него. Если какие-то проверки не пройдены, нажмите «Выполнить настройку пререквизитов» (будут созданы учётка, каталог и права), иначе нажмите

«Выполнить установку».



Установка и результат. Мастер выполняет openssl req и формирует ключ nginx-tls.key (остаётся на сервере) и запрос nginx-tls.csr. По завершении скачайте файл-результат CSR — он понадобится

следующему компоненту «Выпуск сертификата».

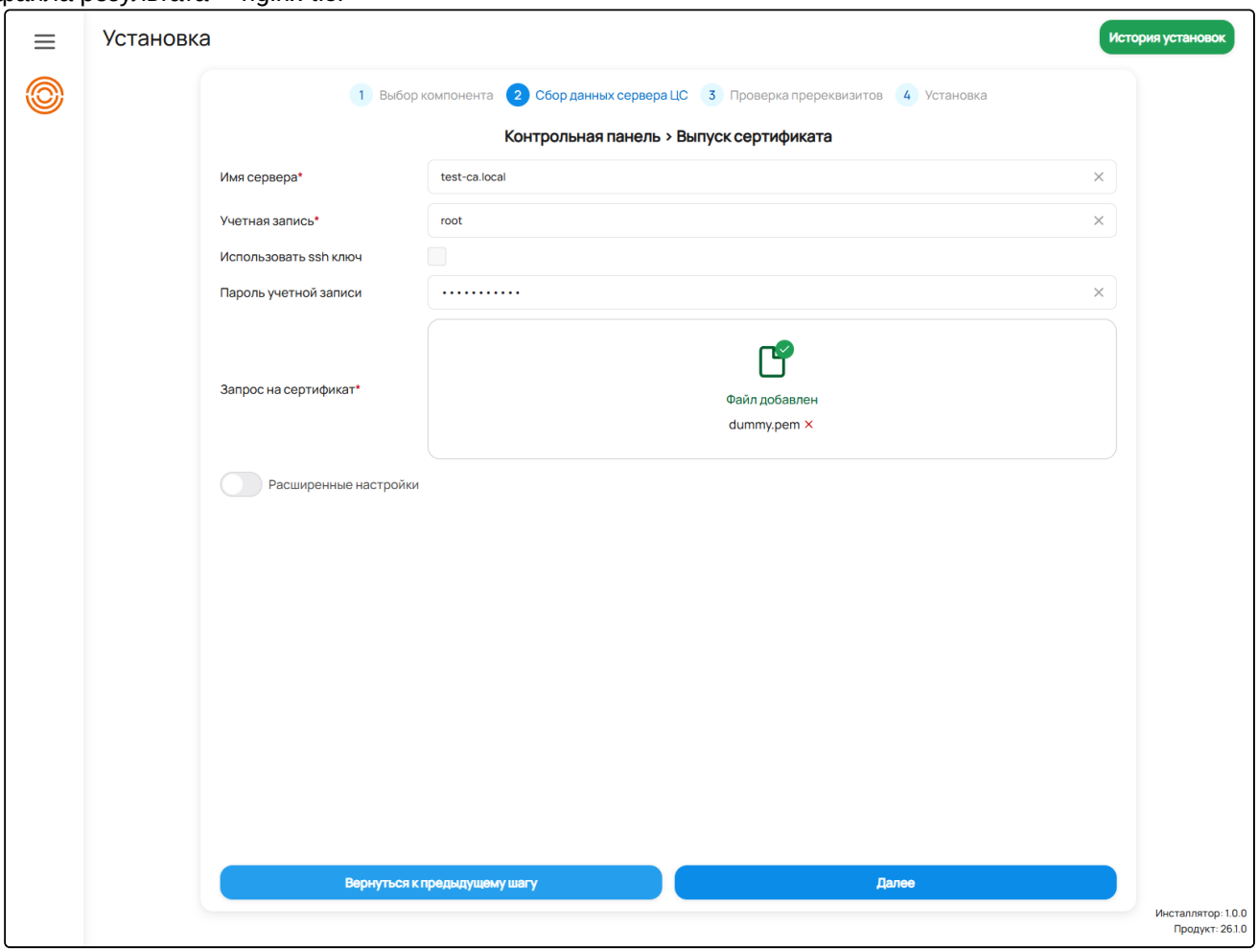


11.2 Выпуск сертификата

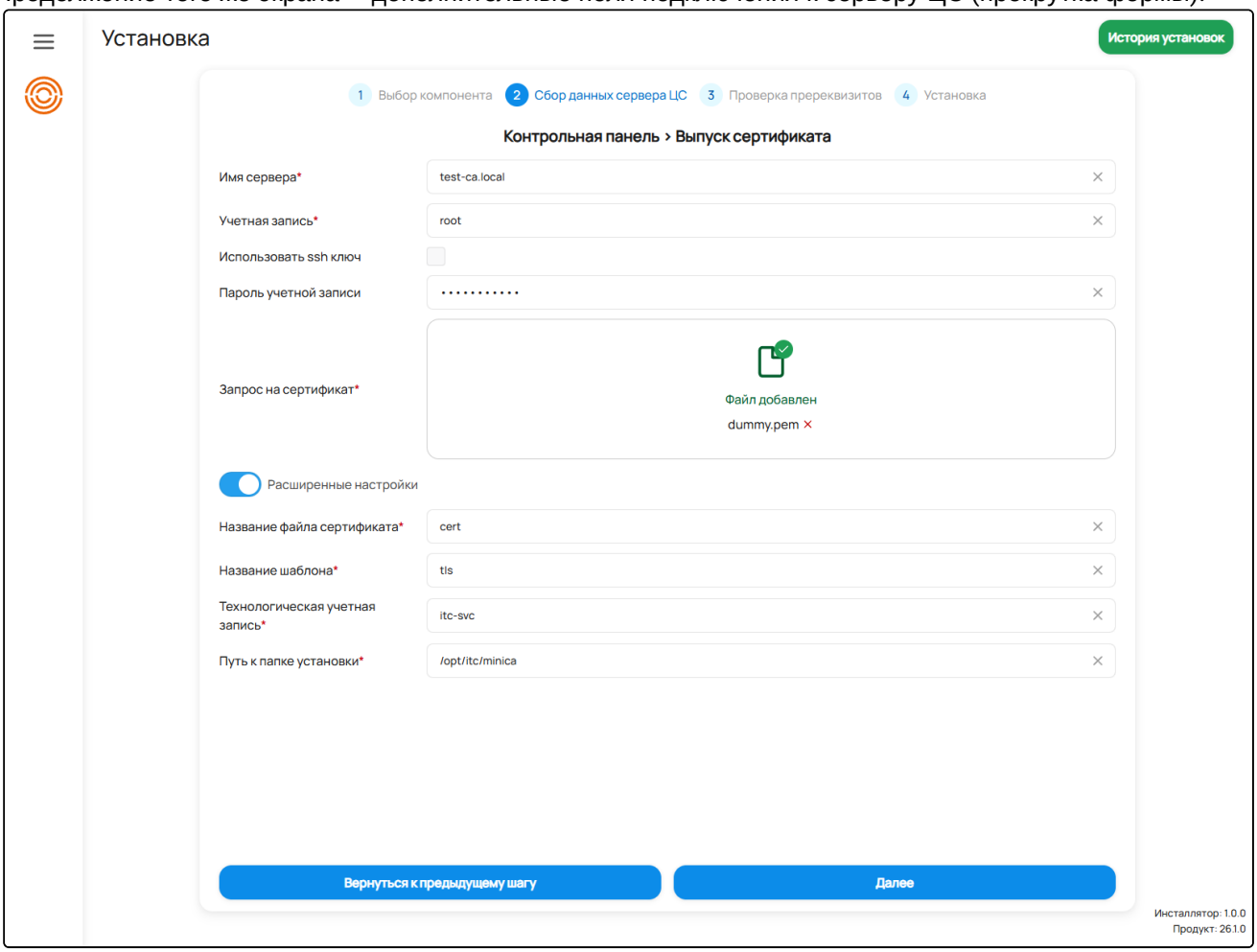
Служебный компонент подключается к серверу центра сертификации и через mclient подписывает ранее выпущенный CSR, возвращая готовый TLS-сертификат.

Сбор данных сервера ЦС. Укажите данные для подключения к серверу ЦС и параметры выпуска: загружаемый CSR (по умолчанию берётся результат nginx-tls.csr предыдущего компонента), учётную запись USER_NAME и каталог ЦС PATH (по умолчанию */opt/itc/minica*). Шаблон выпуска — tls, имя

файла результата – nginx-tls.

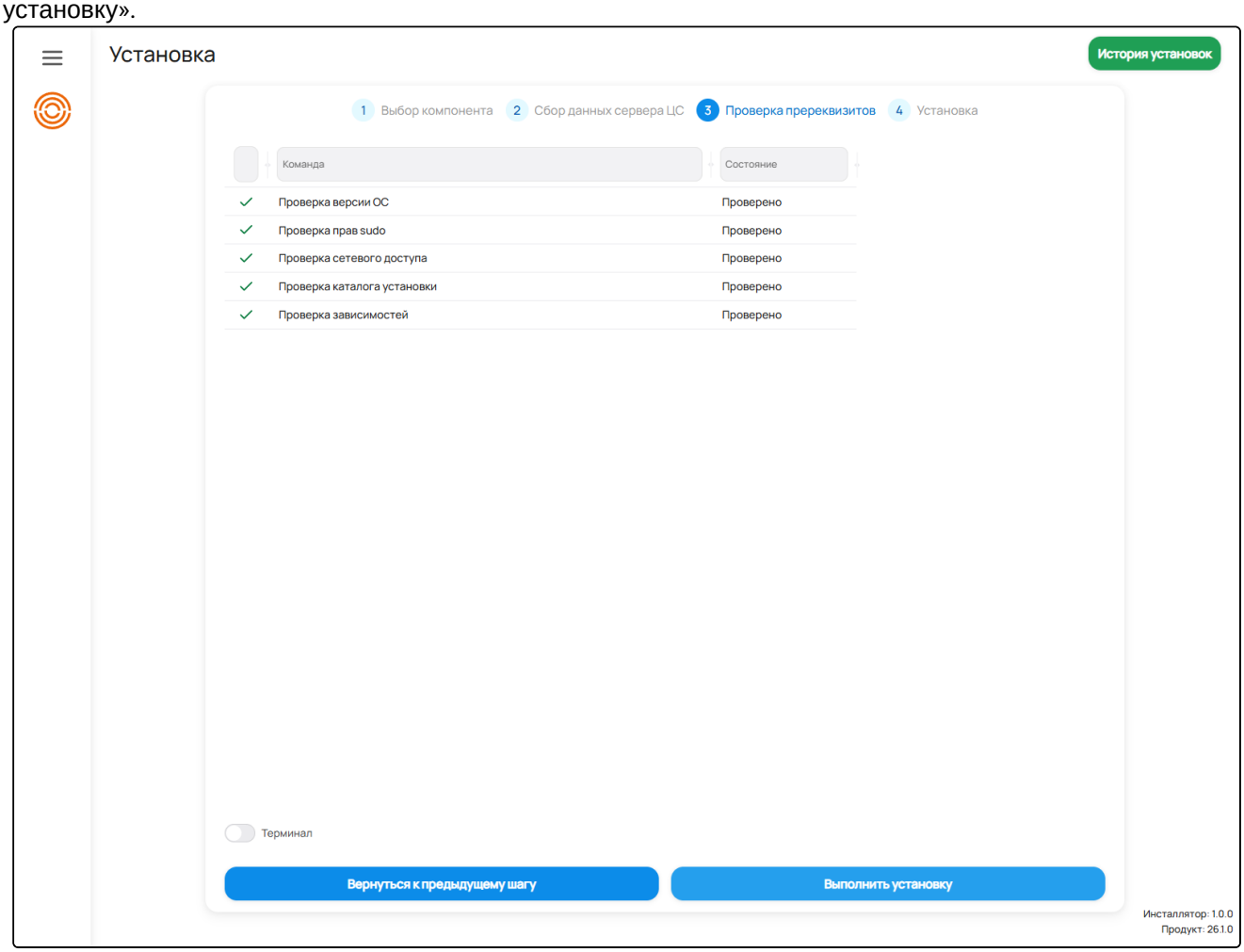


Продолжение того же экрана – дополнительные поля подключения к серверу ЦС (прокрутка формы).

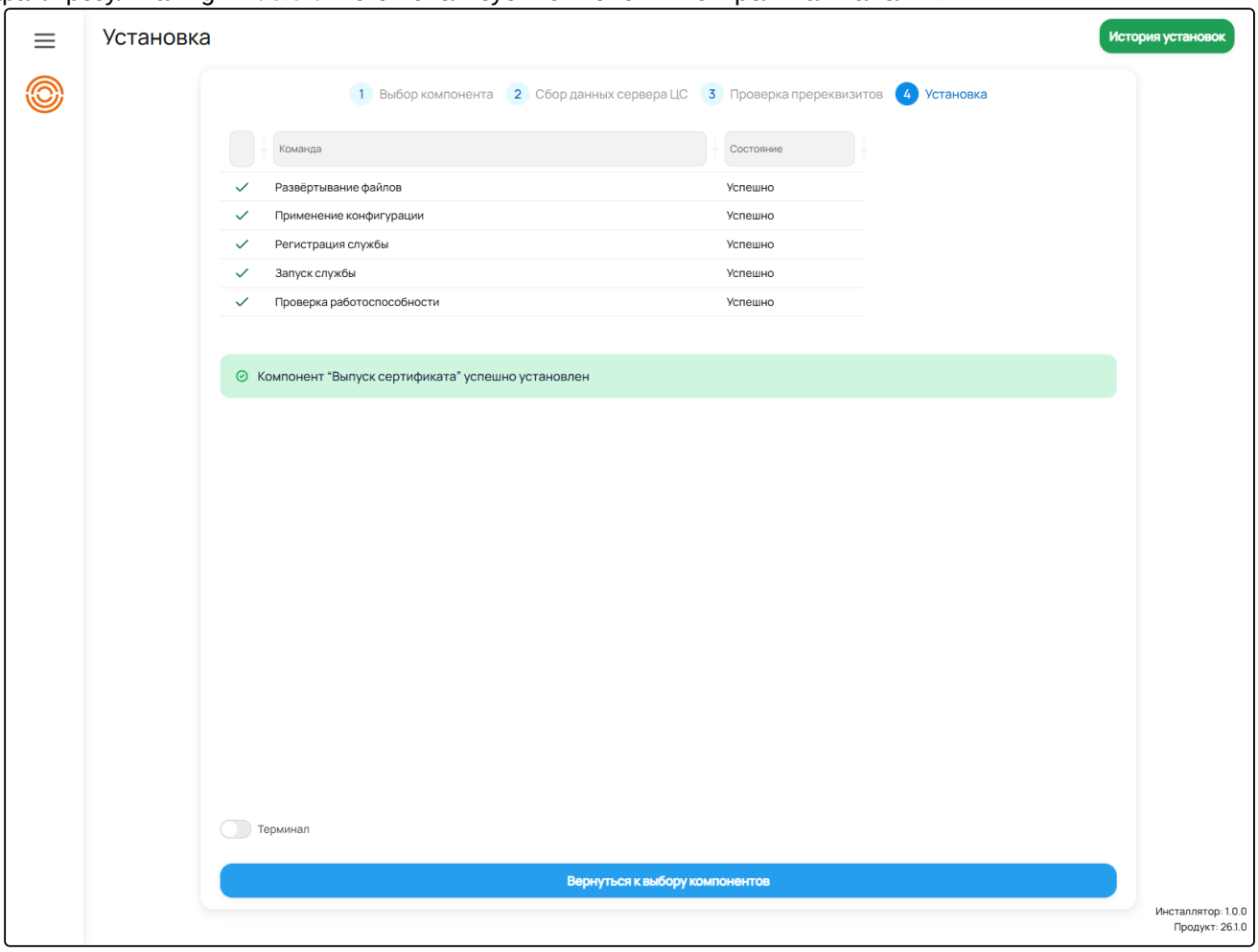


Проверка пререквизитов. Проверяется доступность центра сертификации командой mclient ping (с конфигом MCLIENT_CONF=$PATH/conf/mclient.yml). Если проверка пройдена, нажмите «Выполнить

установку».


Установка
История установок
1 Выбор компонента
2 Сбор данных сервера ЦС
3 Проверка пререквизитов
4 Установка
Команда
Состояние
Проверка версии ОС
Проверено
Проверка прав sudo
Проверено
Проверка сетевого доступа
Проверено
Проверка каталога установки
Проверено
Проверка зависимостей
Проверено
Терминал
Вернуться к предыдущему шагу
Выполнить установку
Инсталлятор: 1.0.0
Продукт: 26.1.0

Установка и результат. Мастер выполняет mclient ca … -template tls и выпускает сертификат. Скачайте файл-результат nginx-tls.crt — его использует компонент «Контрольная панель».

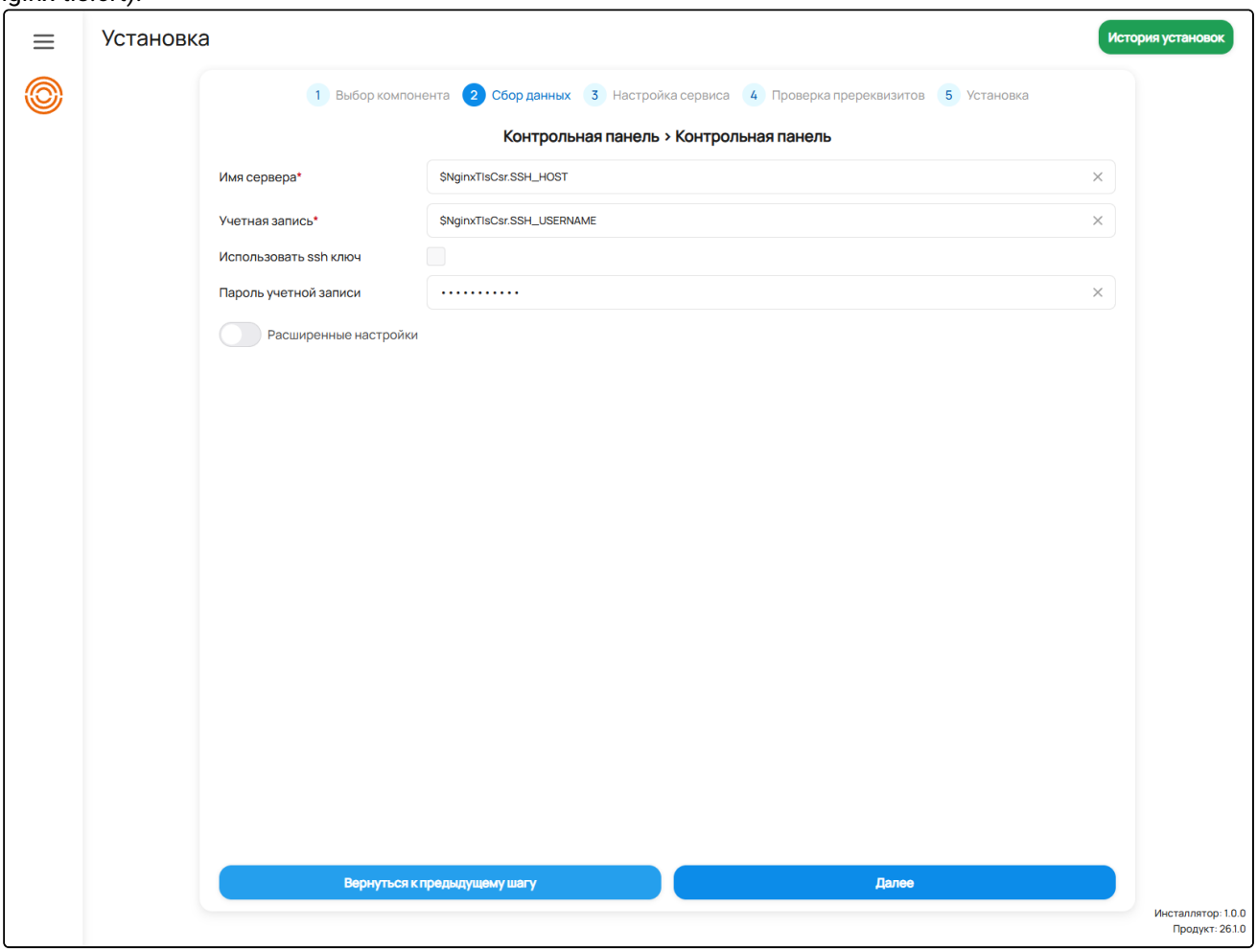


11.3 Контрольная панель

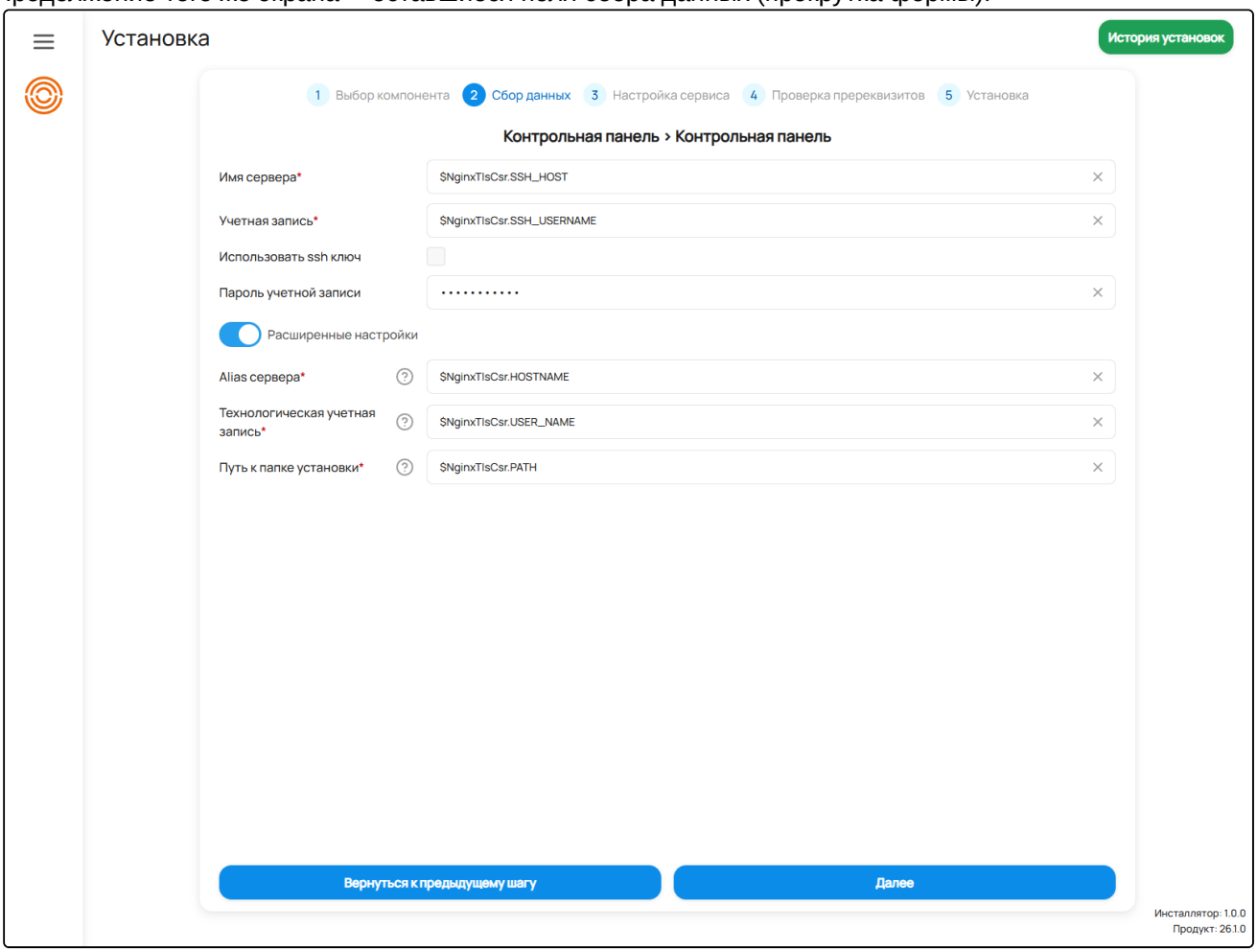
Компонент разворачивает backend панели управления (ASP.NET, порт 8407), статическое приложение SPA и конфигурацию Nginx для доступа оператора.

Сбор данных. Заполните основные параметры: HOSTNAME, USER_NAME и PATH (по умолчанию подставляются из компонента «Выпуск запроса на TLS»), а также TLS-сертификат Nginx CERTIFICATE_NGINX (по умолчанию результат nginx-tls.crt из «Выпуска сертификата», сохраняется как

nginx-tls.crt).

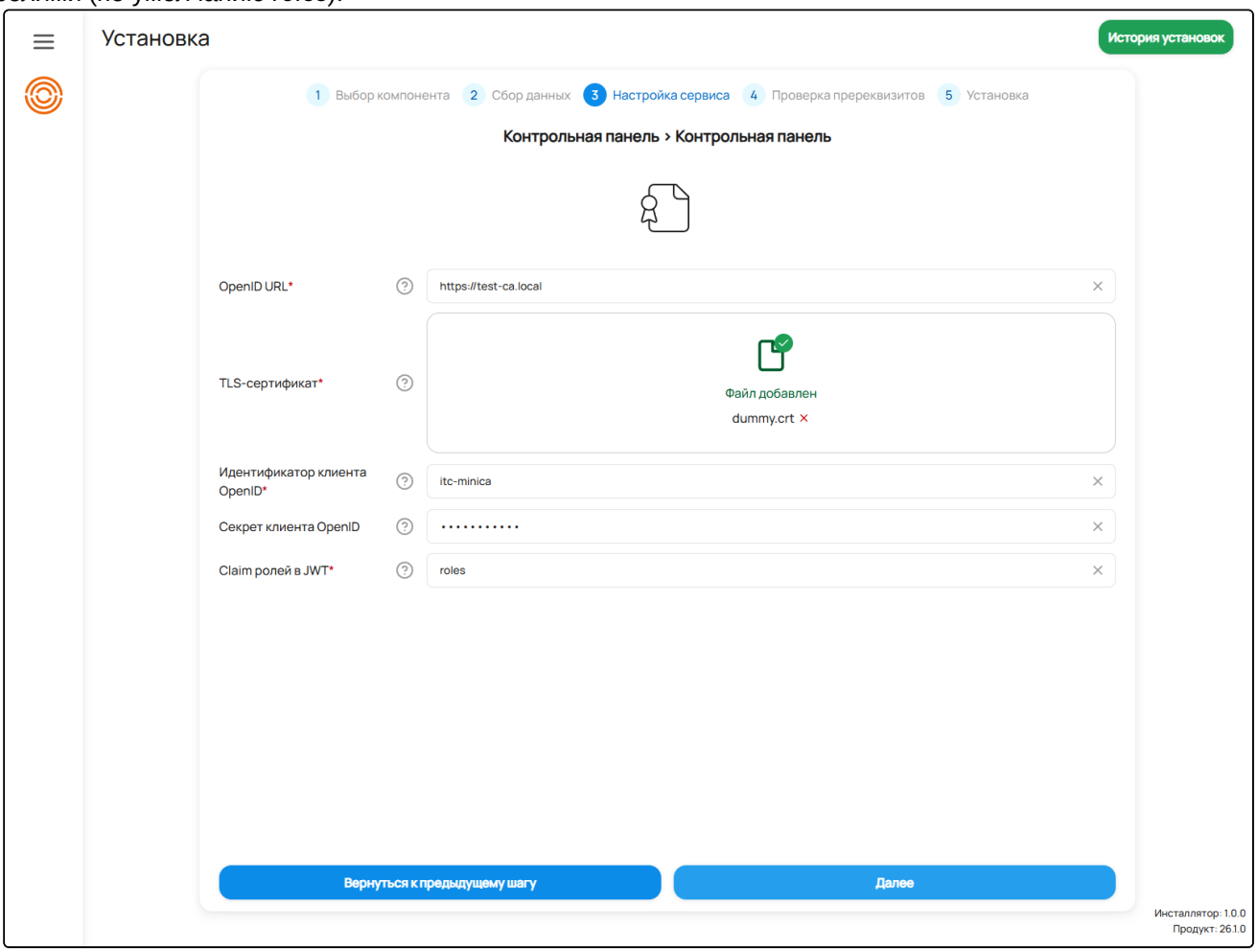


Продолжение того же экрана — оставшиеся поля сбора данных (прокрутка формы).



Настройка сервиса. Задайте параметры аутентификации: AUTH_URL — адрес провайдера OpenID (issuer сервиса аутентификации); AUTH_CLIENT_ID — идентификатор клиента (по умолчанию itc-clearway); AUTH_CLIENT_SECRET — секрет клиента (необязателен); JWT_ROLE_CLAIM — имя claim с

ролями (по умолчанию roles).



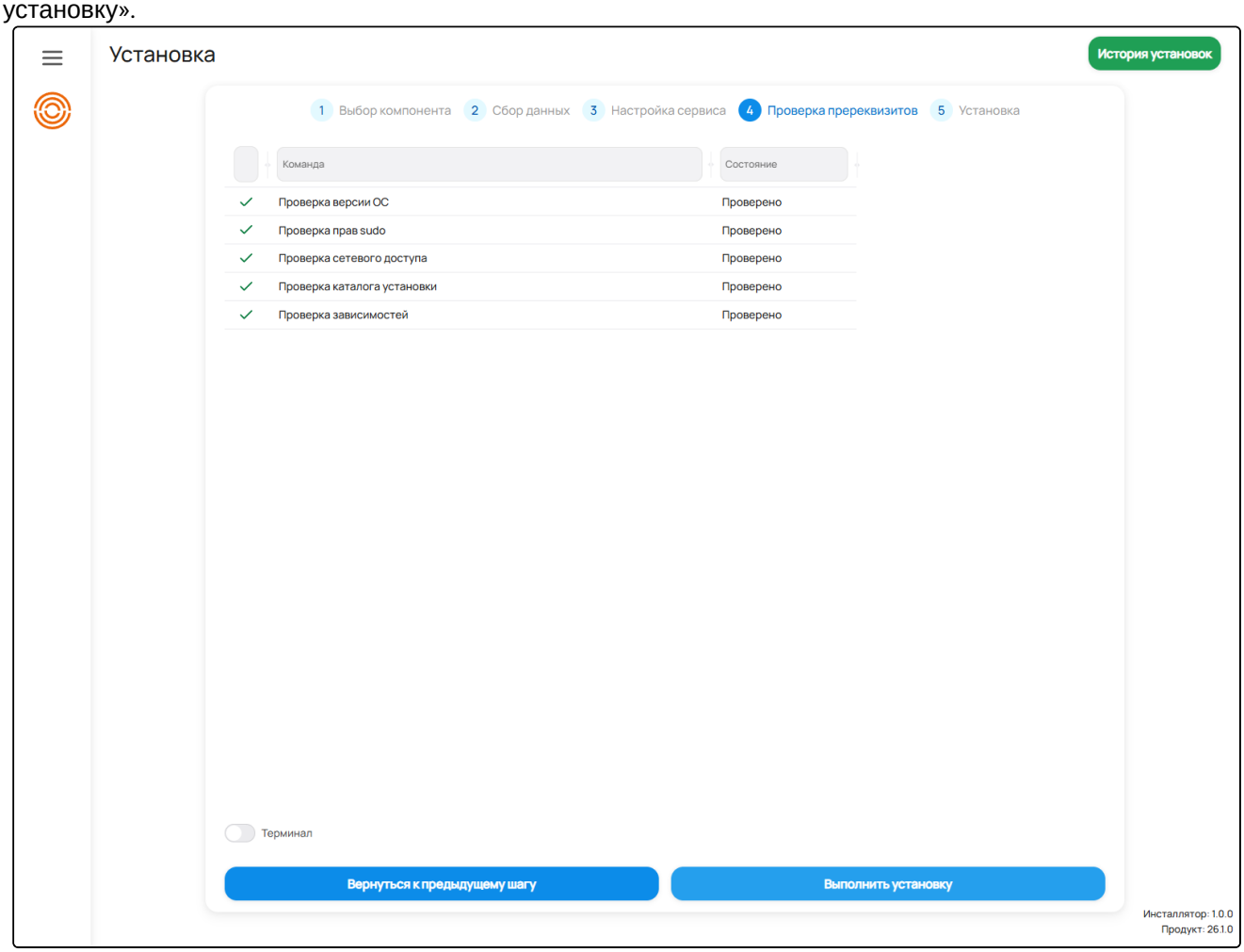
Как заполнить `AUTH_CLIENT_SECRET`

На этапе «Контрольная панель» новый секрет не создаётся. Значение зависит от используемого провайдера аутентификации:

Сценарий	**Значение** `AUTH_CLIENT_SECRET`
Установлен компонент «Аутентификация (OpenID)»	Укажите тот же секрет, который задали в блоке «Клиент OpenID». Поле оставлять пустым нельзя.
Компонент «Аутентификация (OpenID)» не устанавливается, используется другой провайдер	Укажите секрет из настроек клиента выбранного провайдера. Если клиент работает без секрета, оставьте поле пустым.

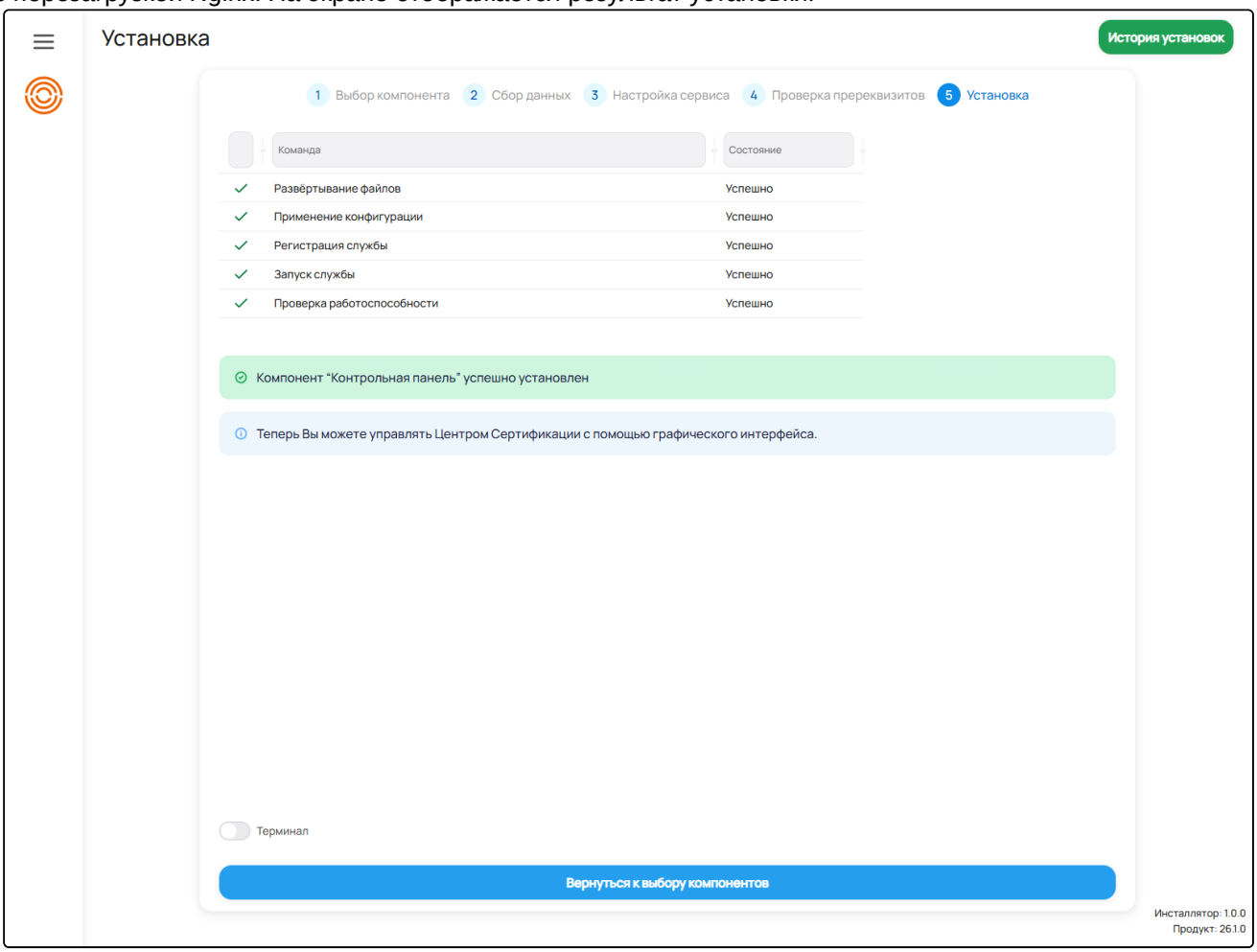
Проверка пререквизитов. В таблице проверяются учётная запись, каталог и права, установленный Nginx (systemctl is-active nginx) и включённый enable-linger. Если есть незакрытые проверки — нажмите «Выполнить настройку пререквизитов» (будет установлен Nginx и включён linger), иначе — «Выполнить

установку».



Установка и результат. Мастер распаковывает backend и SPA, поднимает пользовательский сервис controlPanel.service (порт 8407) и разворачивает конфигурацию Nginx (443, reverse-proxy на /api/minica)

с перезагрузкой Nginx. На экране отображается результат установки.

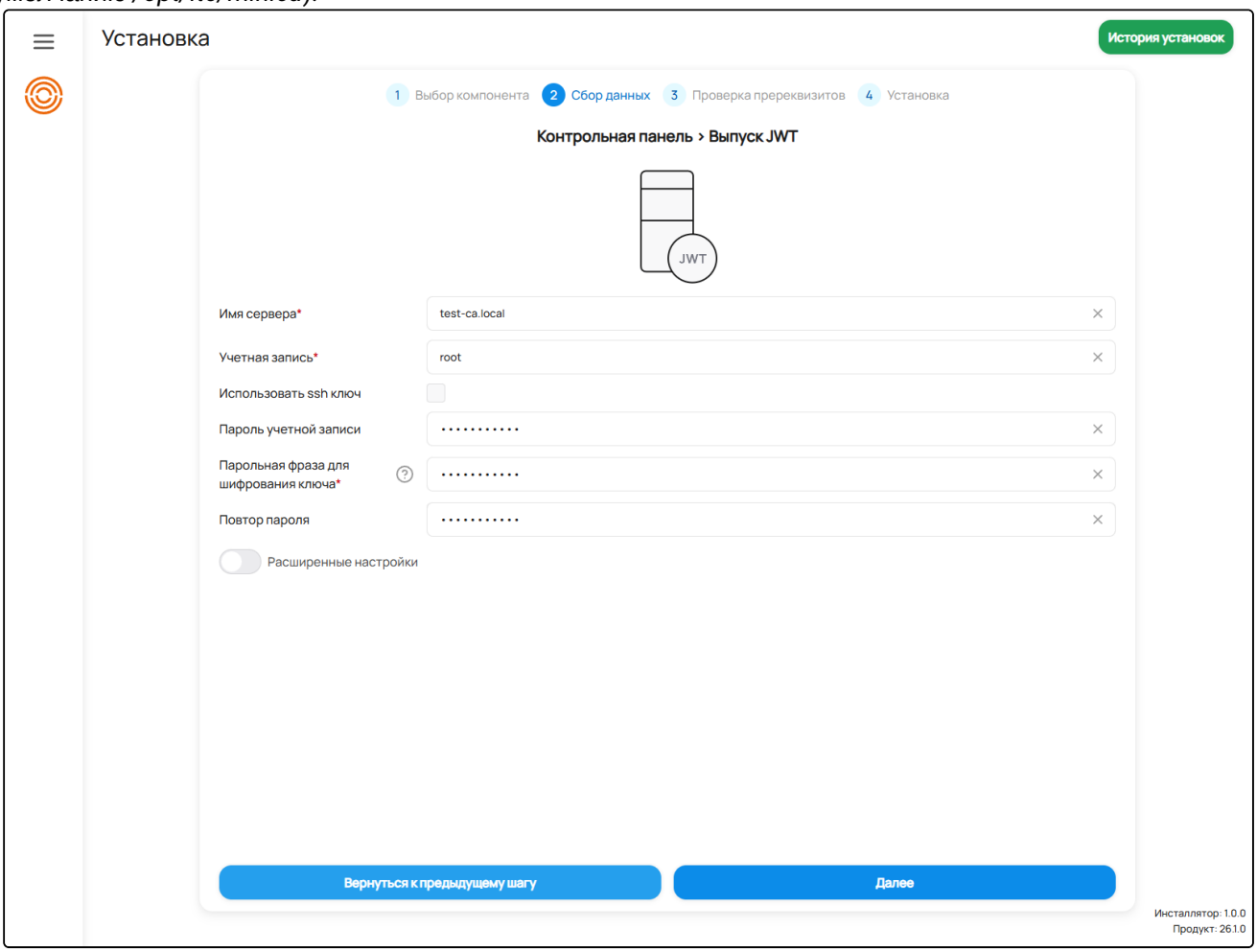


11.4 Выпуск JWT

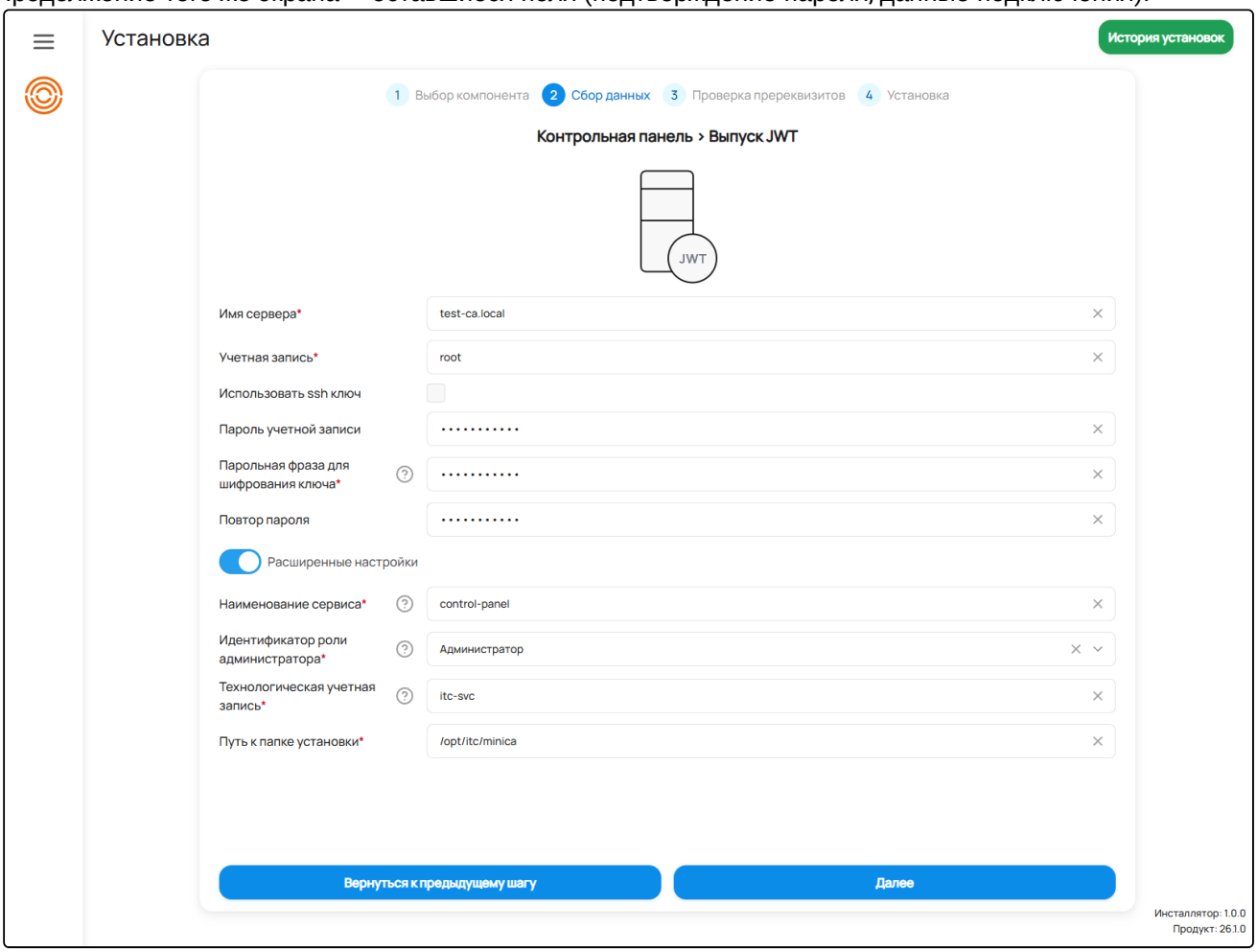
Компонент на действующем ЦС выпускает пару файлов авторизации — JWT-токен и зашифрованный приватный ключ, — с которыми Контрольная панель обращается к центру сертификации.

Сбор данных. Заполните параметры выпуска: NAME_SERVICE (для Контрольной панели по умолчанию control-panel); PASSWORD_KEY — пароль для шифрования приватного ключа (обязателен, с подтверждением); ROLE — роль токена (по умолчанию admin); USER_NAME и PATH сервера ЦС (по

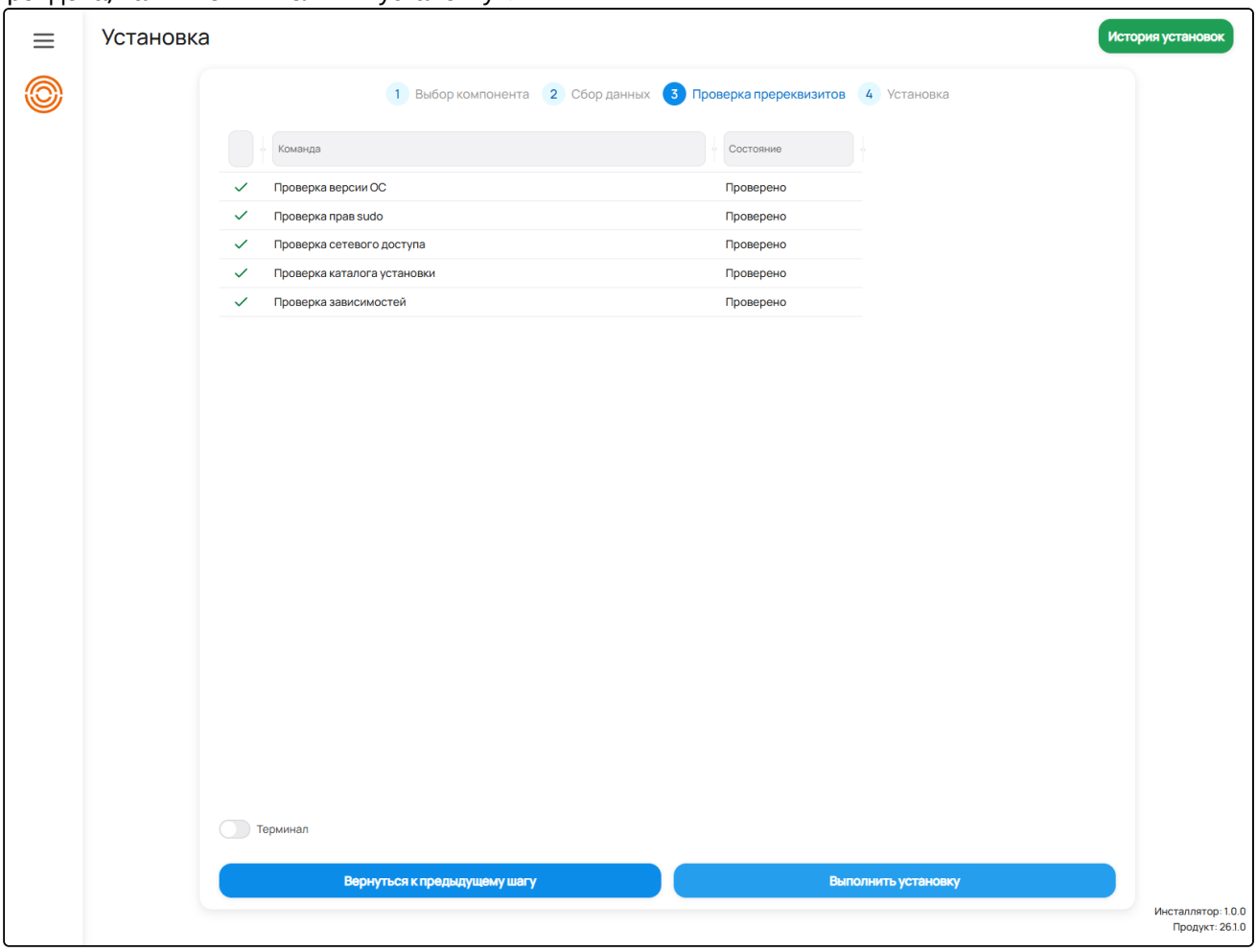
умолчанию */opt/itc/minica*).



Продолжение того же экрана – оставшиеся поля (подтверждение пароля, данные подключения).

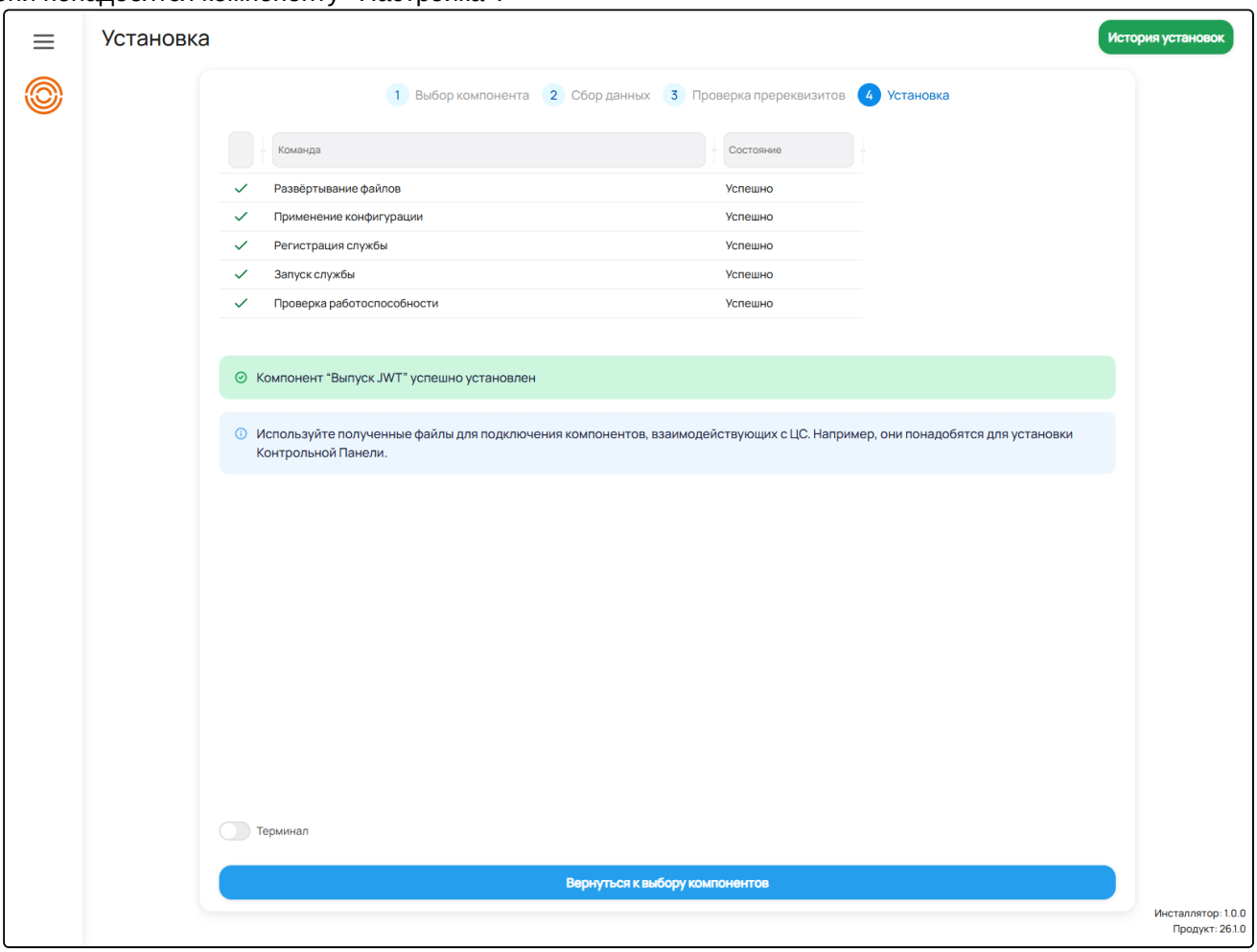


Проверка пререквизитов. Проверяется доступность ЦС командой mclient ping. Если проверка пройдена, нажмите «Выполнить установку».



Установка и результат. Мастер генерирует ключ, выпускает JWT (mclient mkjwt) и шифрует ключ (PKCS8/AES-256-CBC). Скачайте оба файла-результата — control-panel.jwt и control-panel.encrypted.key:

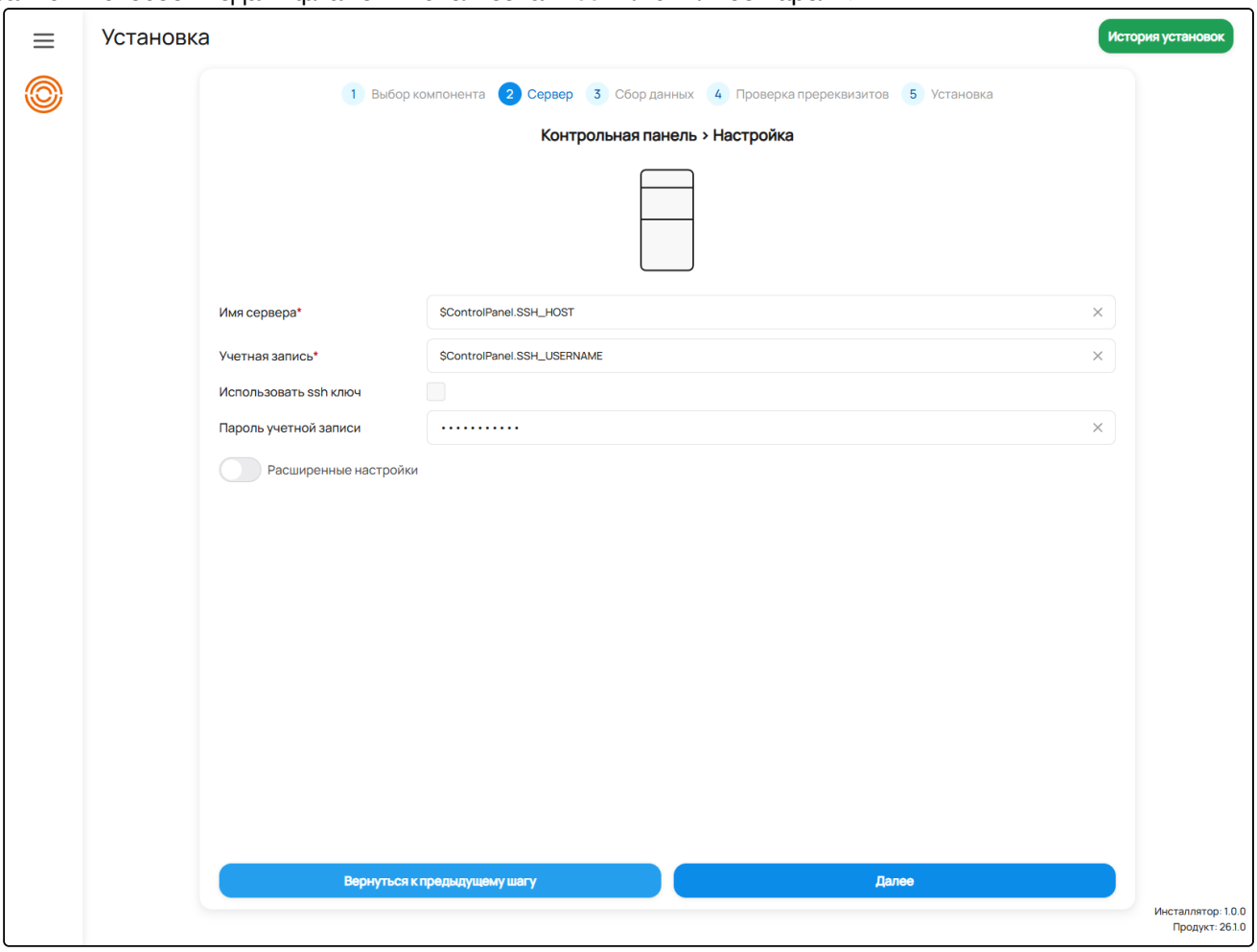
они понадобятся компоненту «Настройка».



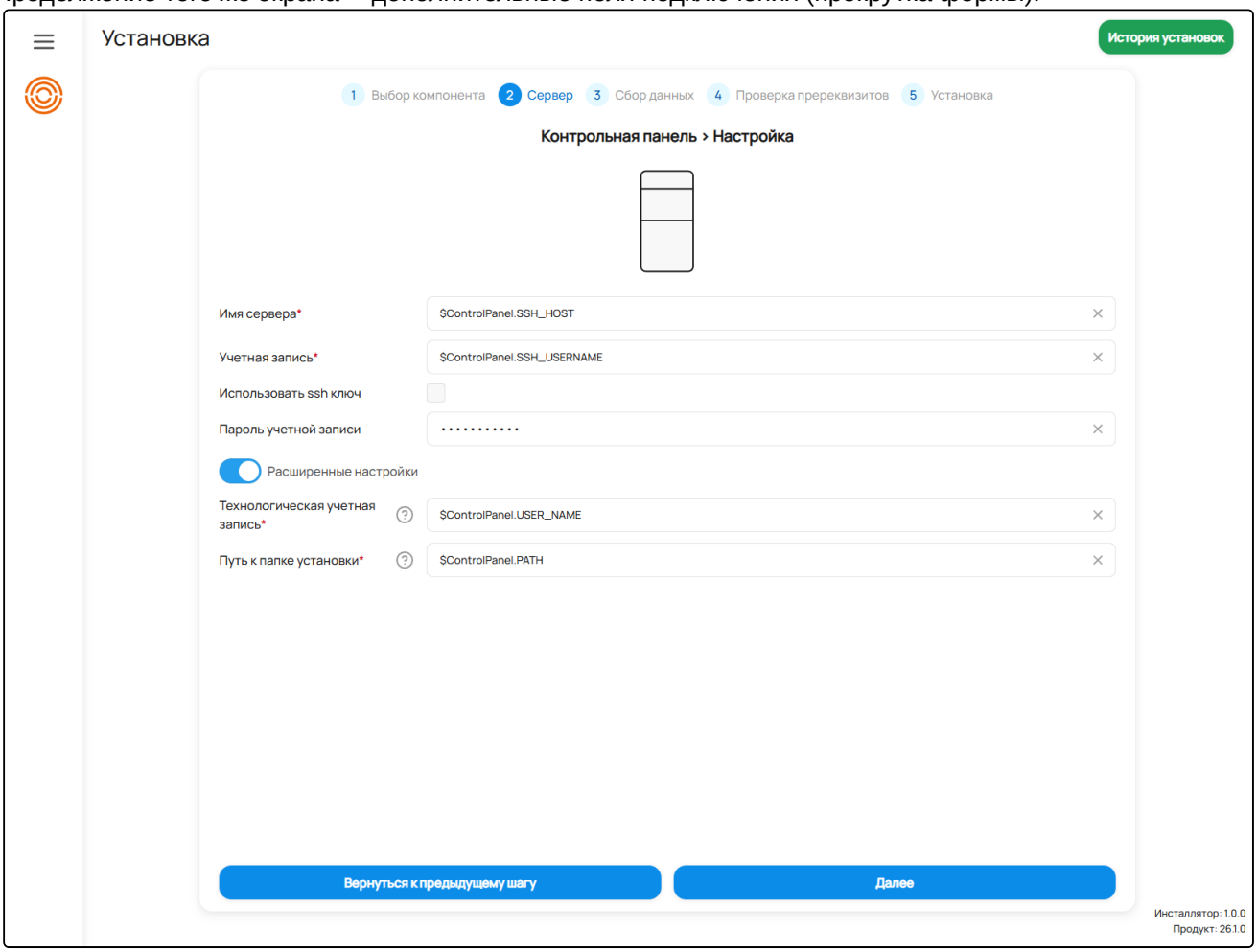
11.5 Настройка

Компонент подключает установленный центр сертификации к Контрольной панели: загружает учётные данные ЦС, расшифровывает ключ и регистрирует ЦС в конфигурации панели.

Сервер. Укажите параметры подключения по SSH к серверу Контрольной панели: имя сервера, учётную запись и способ входа — флажок «Использовать ssh ключ» либо пароль.

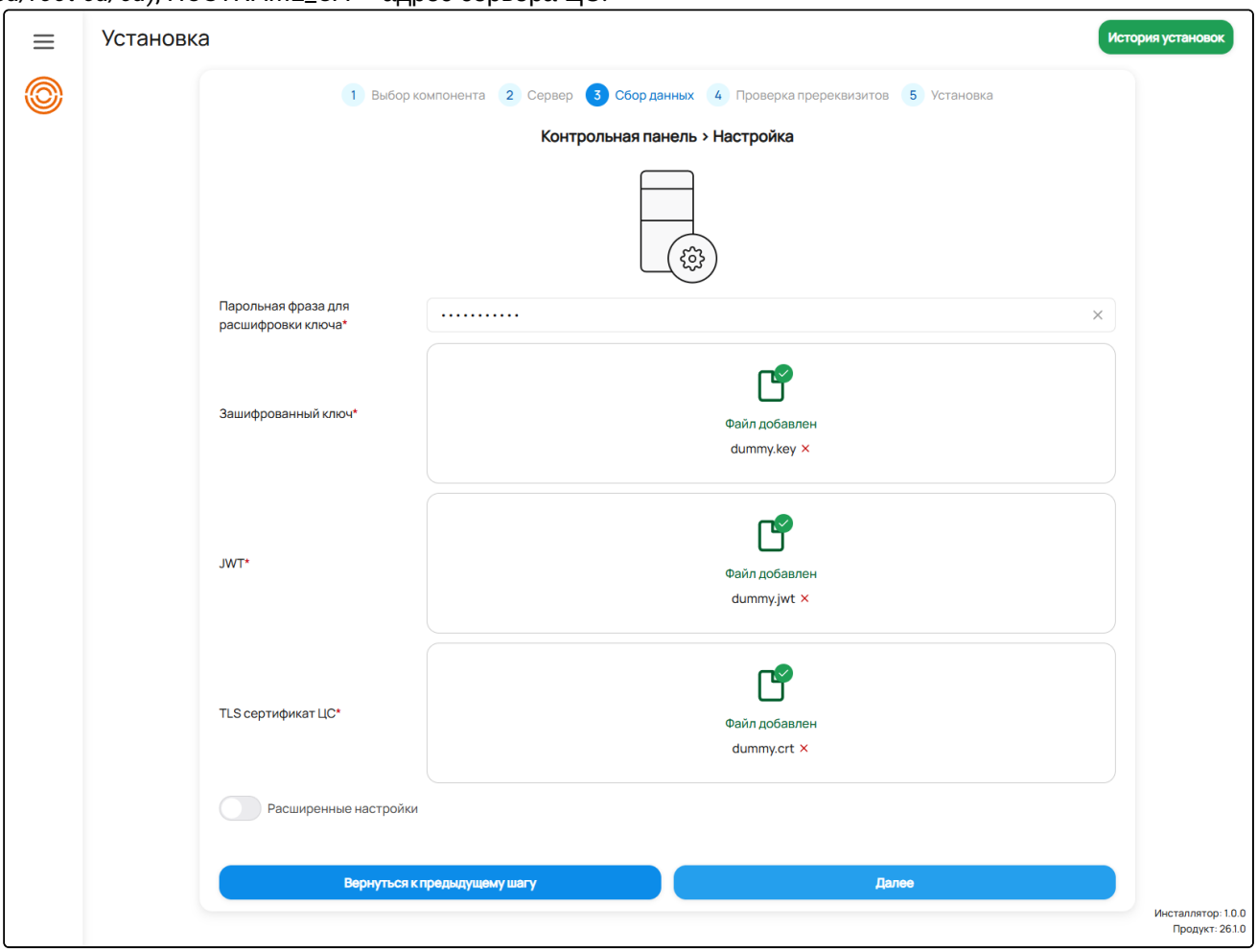


Продолжение того же экрана — дополнительные поля подключения (прокрутка формы).

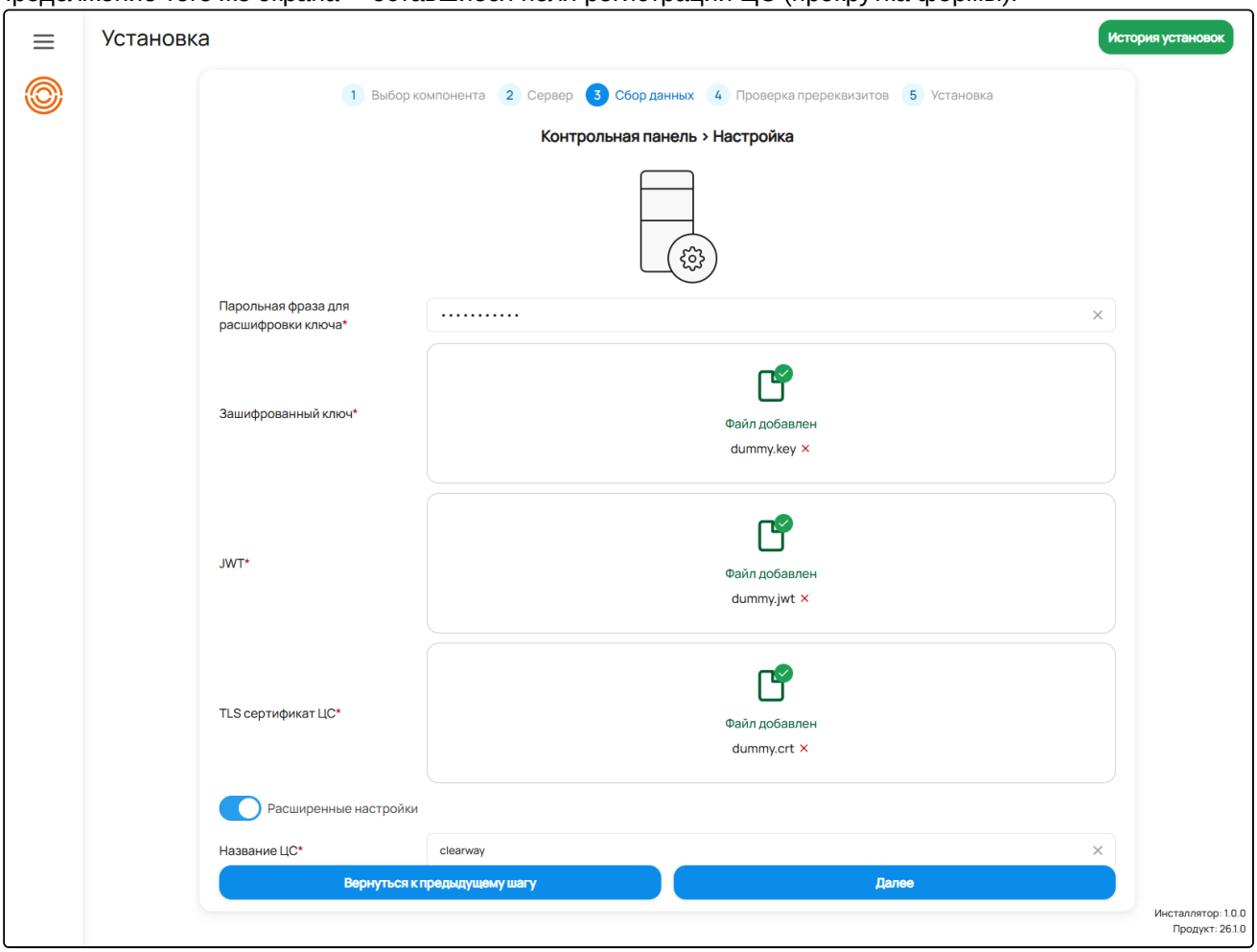


Сбор данных. Заполните параметры регистрации ЦС: PASSWORD_KEY — пароль для расшифровки ключа (тот же, что задан при выпуске JWT); ENCRYPTED_KEY и JWT — файлы control-panel.encrypted.key и control-panel.jwt из компонента «Выпуск JWT»; CA_TLS — TLS-сертификат ЦС; NAME_CA — имя ЦС (*sub-*

ca/root-ca/ca); HOSTNAME_CA — адрес сервера ЦС.



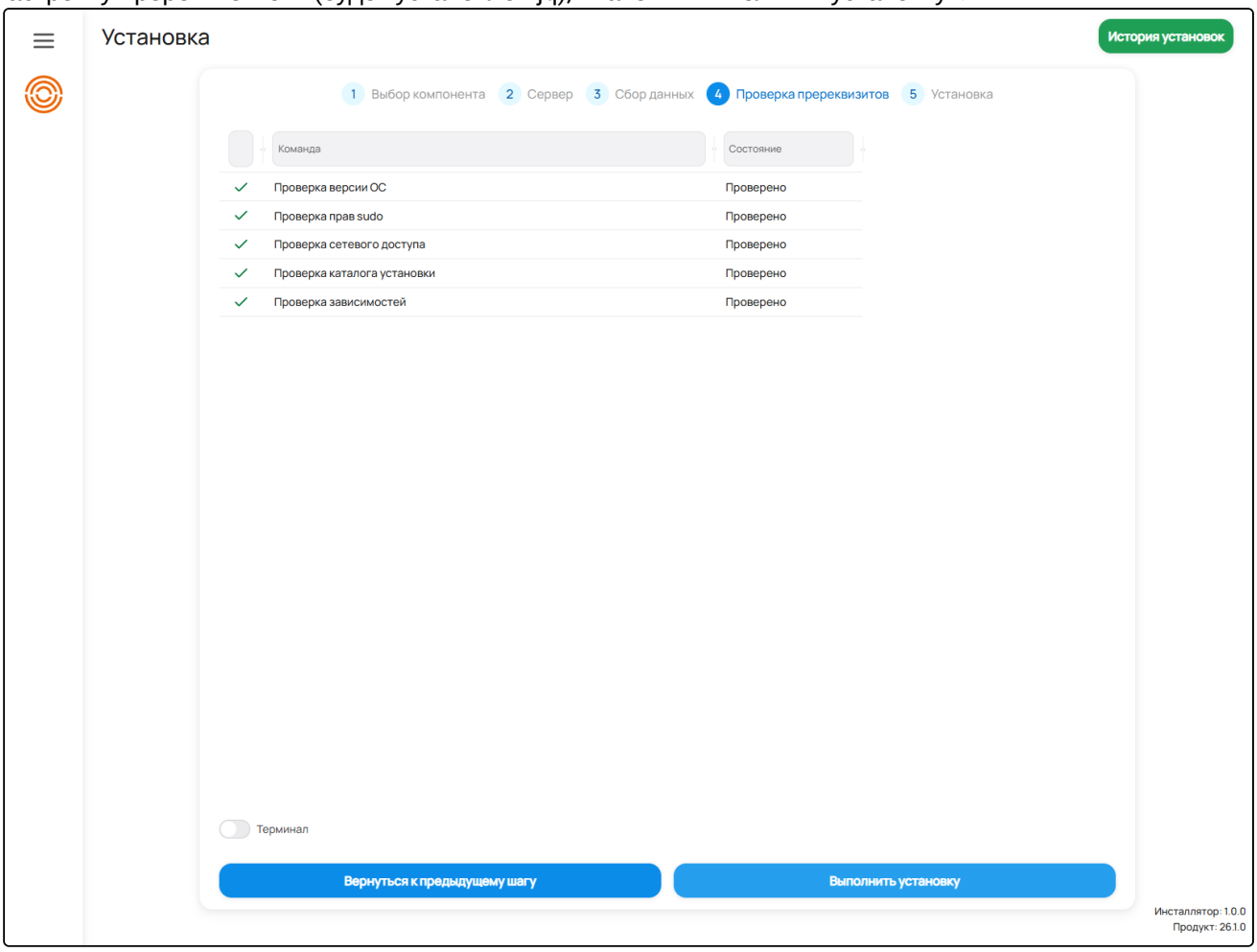
Продолжение того же экрана — оставшиеся поля регистрации ЦС (прокрутка формы).



Проверка пререквизитов. Проверяется, что сервис панели активен:

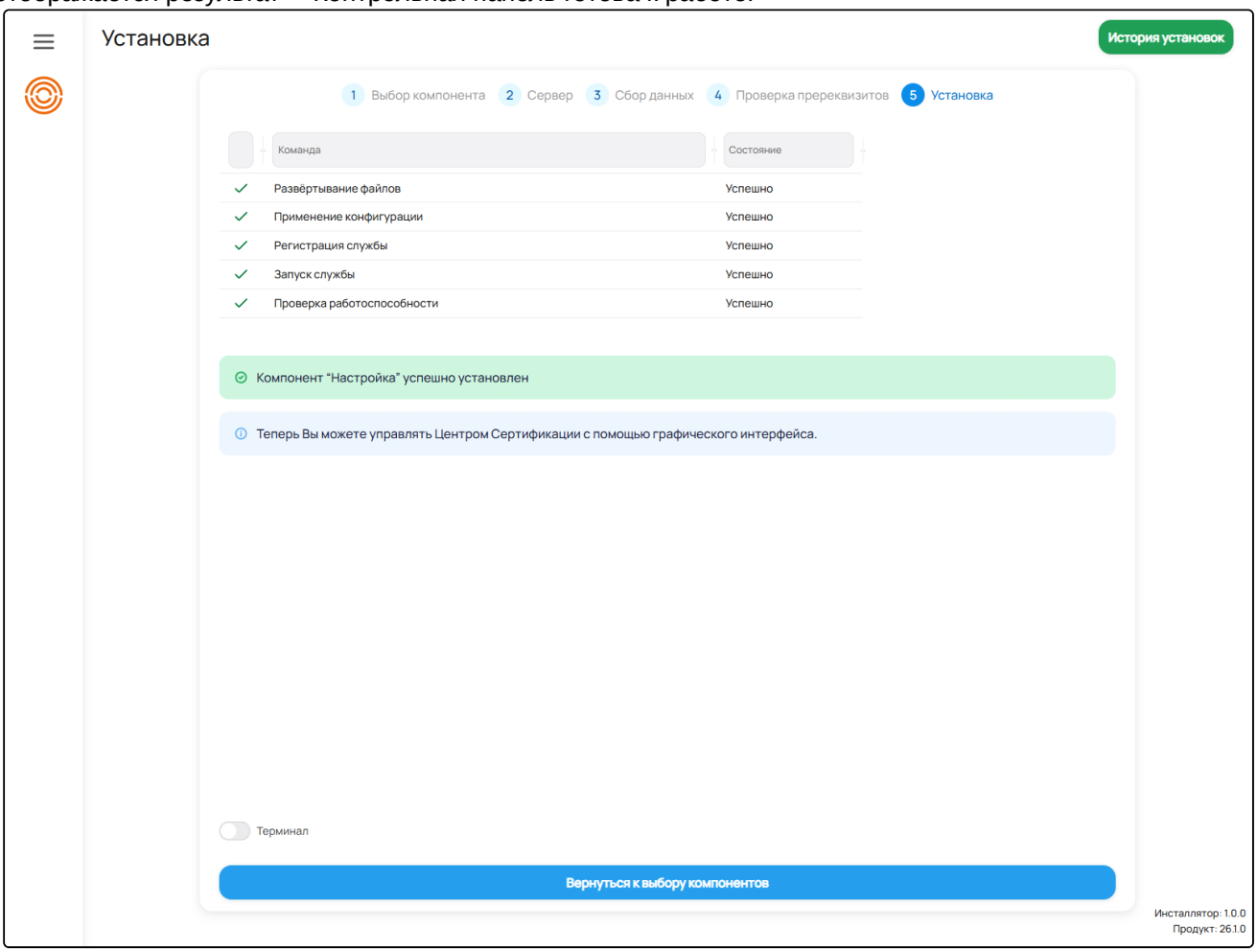
```
systemctl --user is-active controlPanel.service
```

Также проверяется, что установлена утилита jq. Если есть незакрытые проверки — нажмите «Выполнить настройку пререквизитов» (будет установлен jq), иначе — «Выполнить установку».



Установка и результат. Мастер расшифровывает ключ (openssl pkcs8) и через jq регистрирует ЦС в конфигурации панели (адрес https://$HOSTNAME_CA:9443, привязка TLS/подписи/JWT). На экране

отображается результат — Контрольная панель готова к работе.



11.6 Первое открытие Контрольной панели

Перед первым открытием Контрольной панели настройте доверие к TLS-сертификату OpenID. Без доверенной цепочки сертификатов вместо формы входа может остаться экран загрузки.

Подготовьте сертификаты в соответствии со схемой выпуска:

Файл	Когда нужен	Откуда взять	Куда установить
`openid-tls.crt`	TLS-сертификат OpenID самоподписанный	Результат выпуска TLS-сертификата OpenID, раздел 7.3	Доверенные корневые сертификаты
`root-ca.crt`	TLS-сертификат OpenID выпущен корневым или выдающим ЦС Clearway CA	Результат установки корневого ЦС, раздел 5.2	Доверенные корневые сертификаты
`sub-ca.crt`	Дополнительно, если TLS-сертификат OpenID выпущен выдающим ЦС	Результат выпуска сертификата выдающего ЦС, раздел 6.3	Промежуточные центры сертификации

Если сертификат OpenID выпущен внешним ЦС, используйте предоставленные им корневой и промежуточные сертификаты.

1. На компьютере, с которого будет открываться Контрольная панель, установите нужные сертификаты в хранилище, используемое браузером.
2. Перезапустите браузер, чтобы он перечитал доверенное х ранилище.
3. Возьмите значение `AUTH_URL`, указанное на шаге «Контрольная панель» при настройке аутентификации. Удалите завершающий символ `/`, если он есть, и откройте адрес:

   ```
   <AUTH_URL>/.well-known/openid-configuration
   ```

   Вместо `<AUTH_URL>` подставьте полное значение параметра, включая путь, если он есть.
4. Убедитесь, что JSON-документ с параметрами провайдера OpenID открывается без предупреждения о сертификате.
5. Откройте адрес Контрольной панели.

Важно. Не обходите предупреждение браузера и не отключайте проверку сертификатов. Если страница конфигурации OpenID по-прежнему открывается с предупреждением, проверьте, что установлена цепочка сертификатов именно того сервиса, адрес которого указан в `AUTH_URL`.

12 Сервис публикации

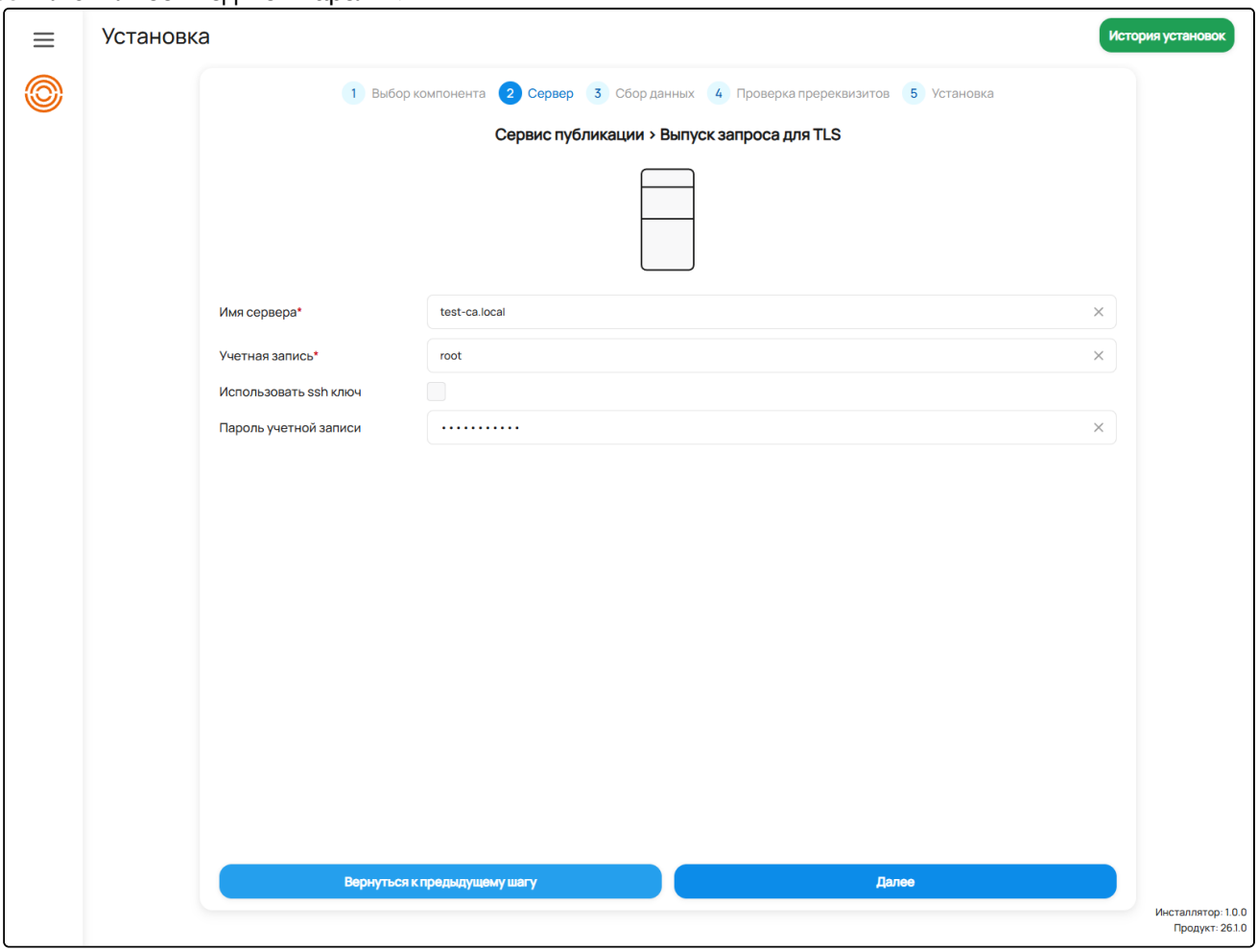
Группа разворачивает веб-сервис публикации сертификатов и списков отзыва (CRL) на точки распространения, доступный через Nginx по HTTPS с авторизацией OpenID/JWT. Компоненты устанавливаются в следующем порядке: Выпуск запроса на TLS (генерация ключа и CSR для Nginx), Выпуск сертификата (подпись CSR на действующем ЦС), Сервис публикации (установка .NET-сервиса за Nginx) и Выпуск JWT (создание токена и ключа для доступа сервиса к ЦС).

12.1 Выпуск запроса на TLS

Компонент генерирует на целевом сервере приватный ключ и запрос на сертификат (CSR) для TLS Nginx; сам сервис не устанавливается.

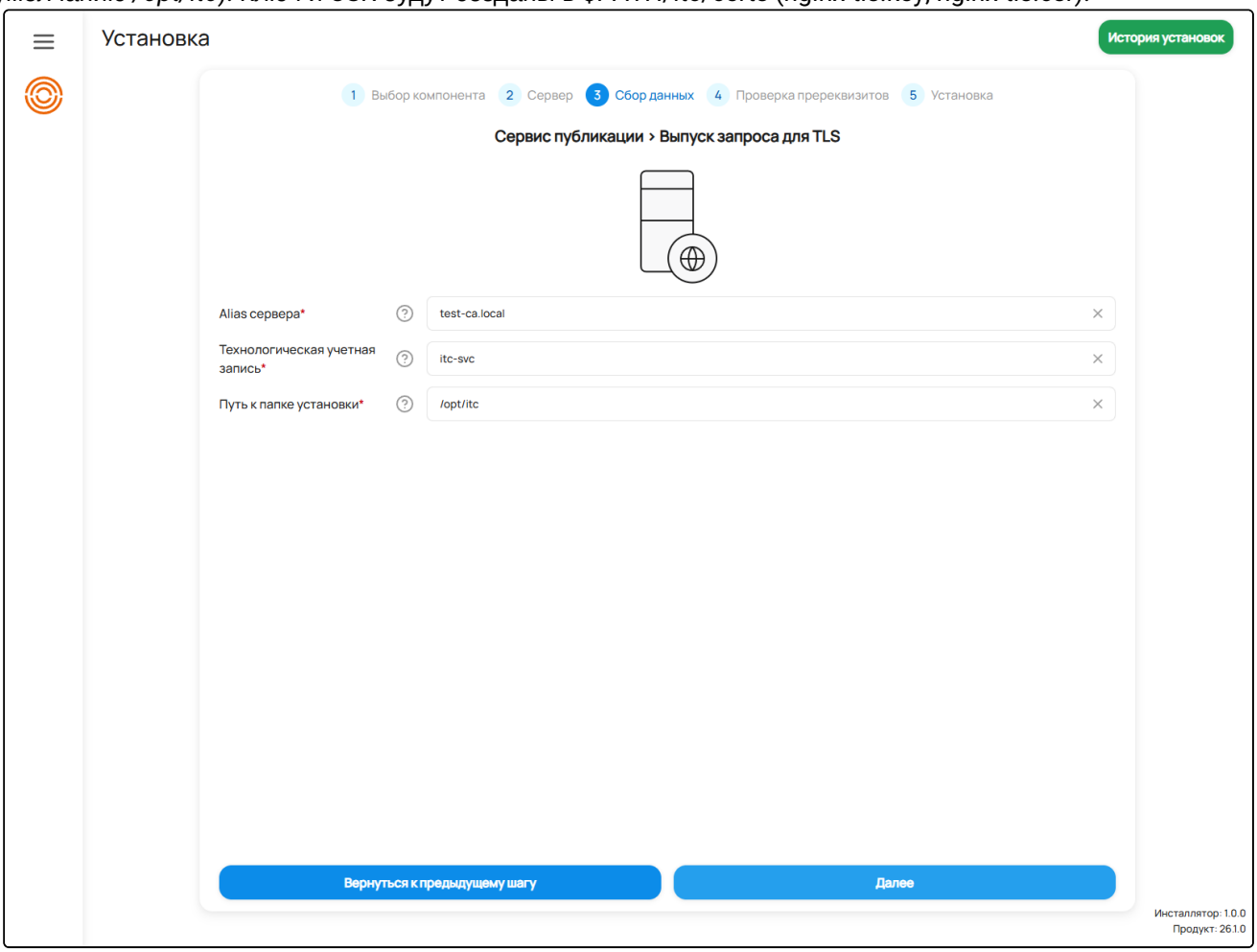
Когда можно пропустить: пропустите этот компонент, если приватный ключ и запрос на TLS-сертификат уже подготовлены на целевом сервере, например при повторной установке или по корпоративной процедуре PKI. Приватный ключ должен находиться в $PATH/itc/certs/nginx-tls.key. Если сертификат будет выпускаться Clearway CA, на следующем этапе вручную загрузите подготовленный CSR; если готовый сертификат уже есть, можно пропустить и этап «Выпуск сертификата».

Подключение к серверу. Укажите адрес целевого сервера в поле «Имя сервера», технологическую «Учётную запись» (по умолчанию itc-svc) и способ входа по SSH — установите флажок «Использовать ssh ключ» либо введите «Пароль».



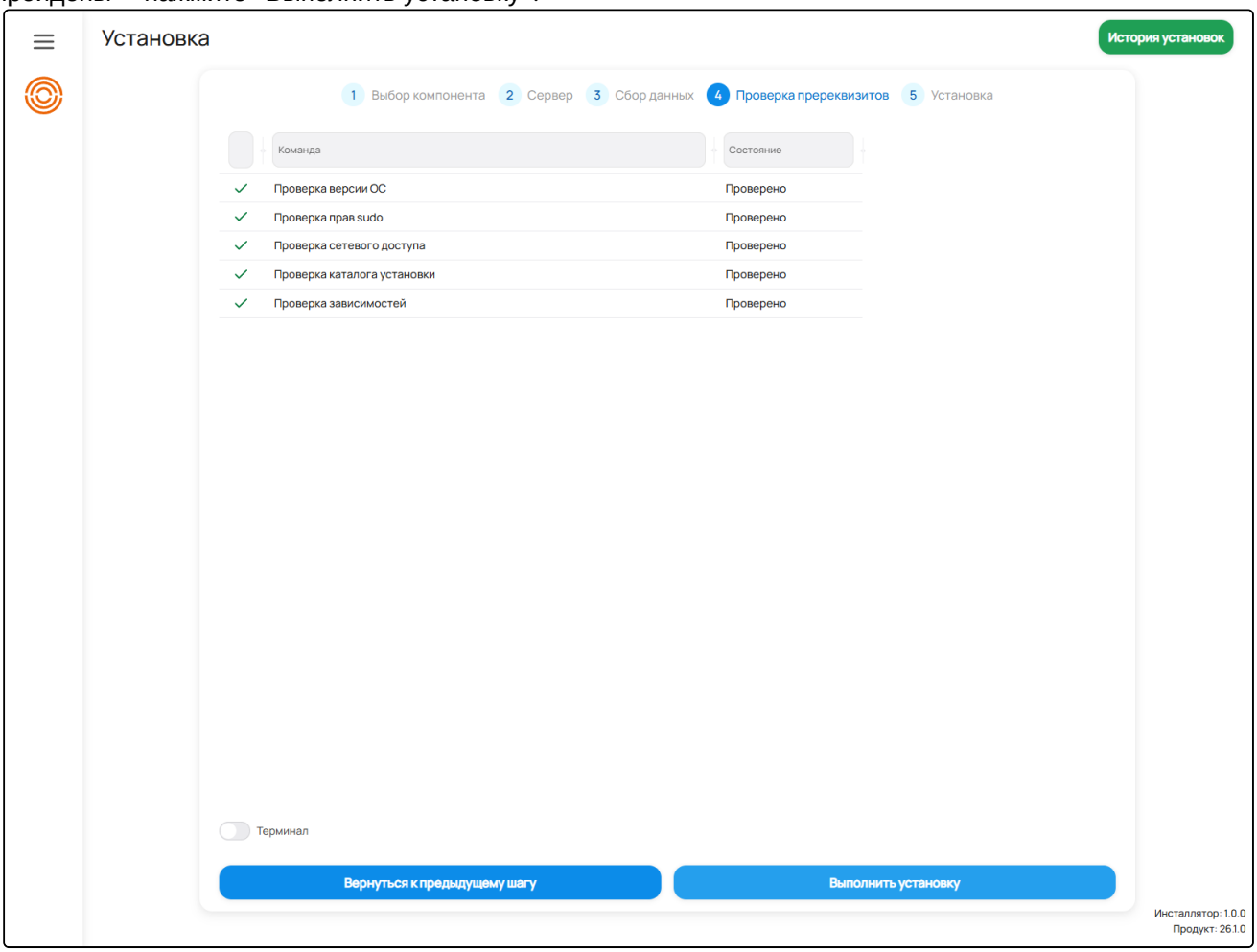
Сбор данных. Заполните параметры запроса: HOSTNAME (имя, попадающее в CN/SAN сертификата; по умолчанию имя хоста ОС), USER_NAME (учётка-владелец, itc-svc) и PATH (каталог установки, по

умолчанию */opt/itc*). Ключ и CSR будут созданы в $PATH/itc/certs (nginx-tls.key, nginx-tls.csr).



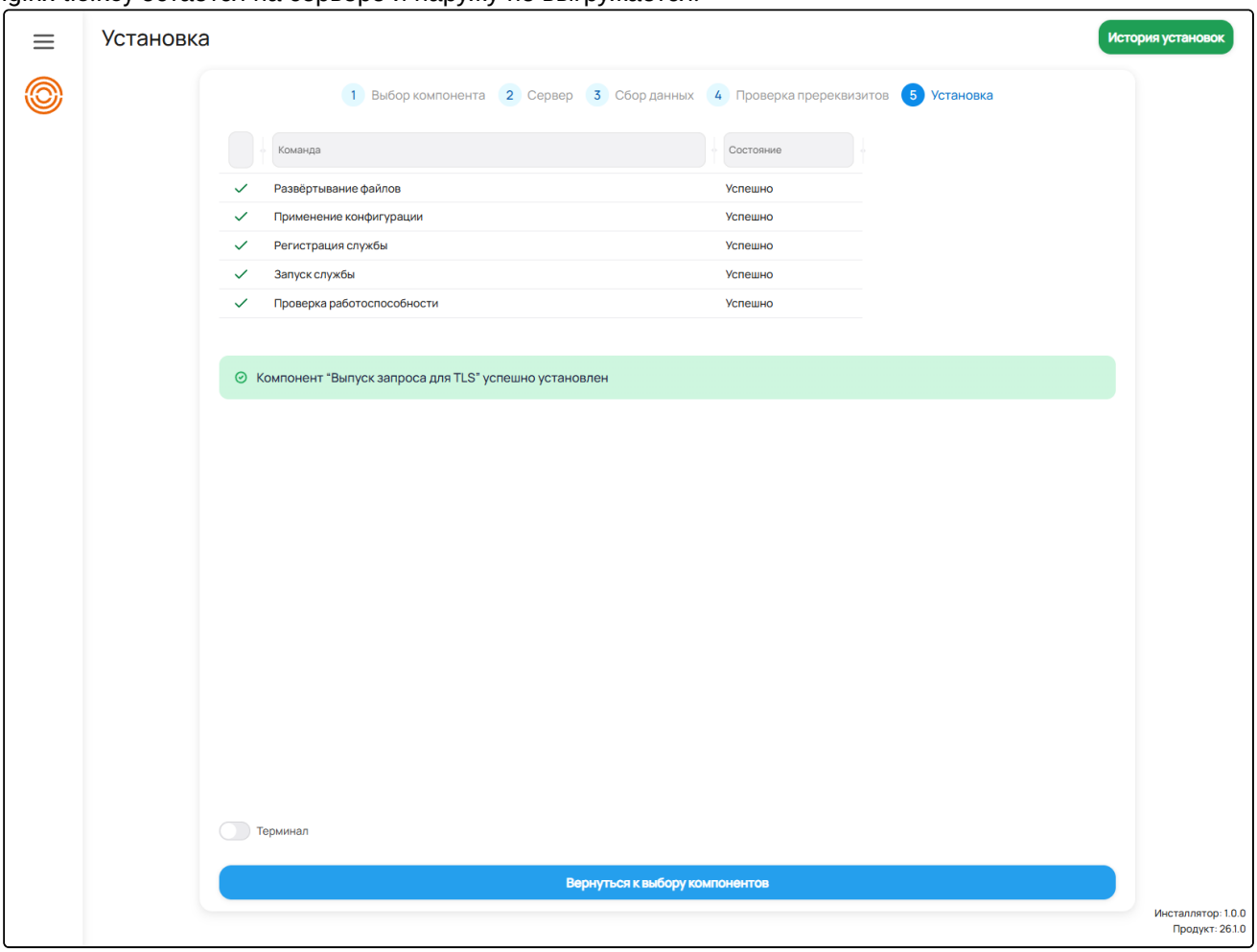
Проверка пререквизитов. Мастер проверяет наличие учётной записи, каталога и прав на него. Если есть незакрытые проверки — нажмите «Выполнить настройку пререквизитов»; когда все проверки

пройдены — нажмите «Выполнить установку».



Установка и результат. Выполняется генерация ключа и CSR. По завершении скачайте файл-результат nginx-tls.csr — он потребуется следующему компоненту для выпуска сертификата. Приватный ключ

nginx-tls.key остаётся на сервере и наружу не выгружается.



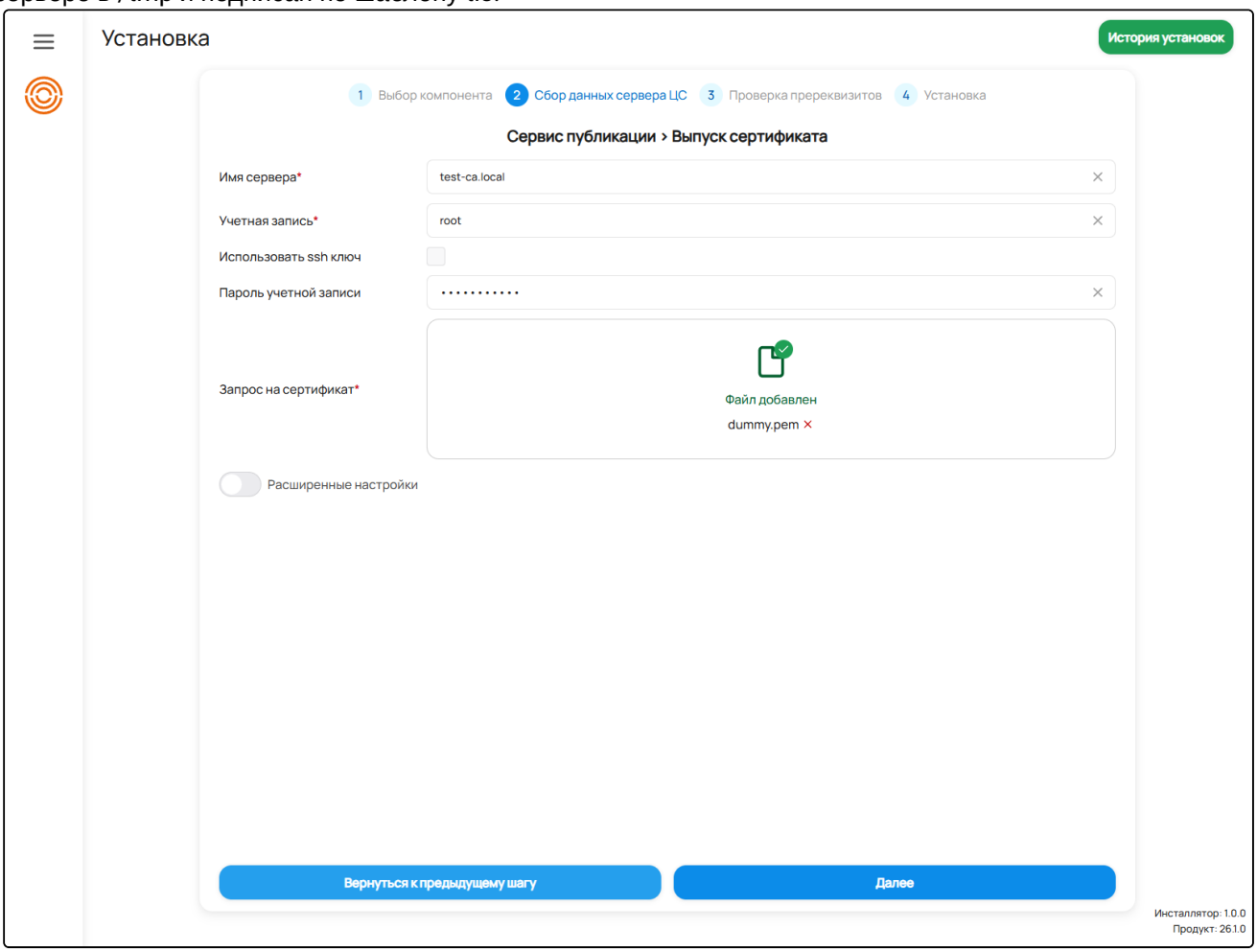
12.2 Выпуск сертификата

Служебный компонент подключается по SSH к серверу ЦС и через mclient выпускает подписанный TLS-сертификат по загруженному CSR.

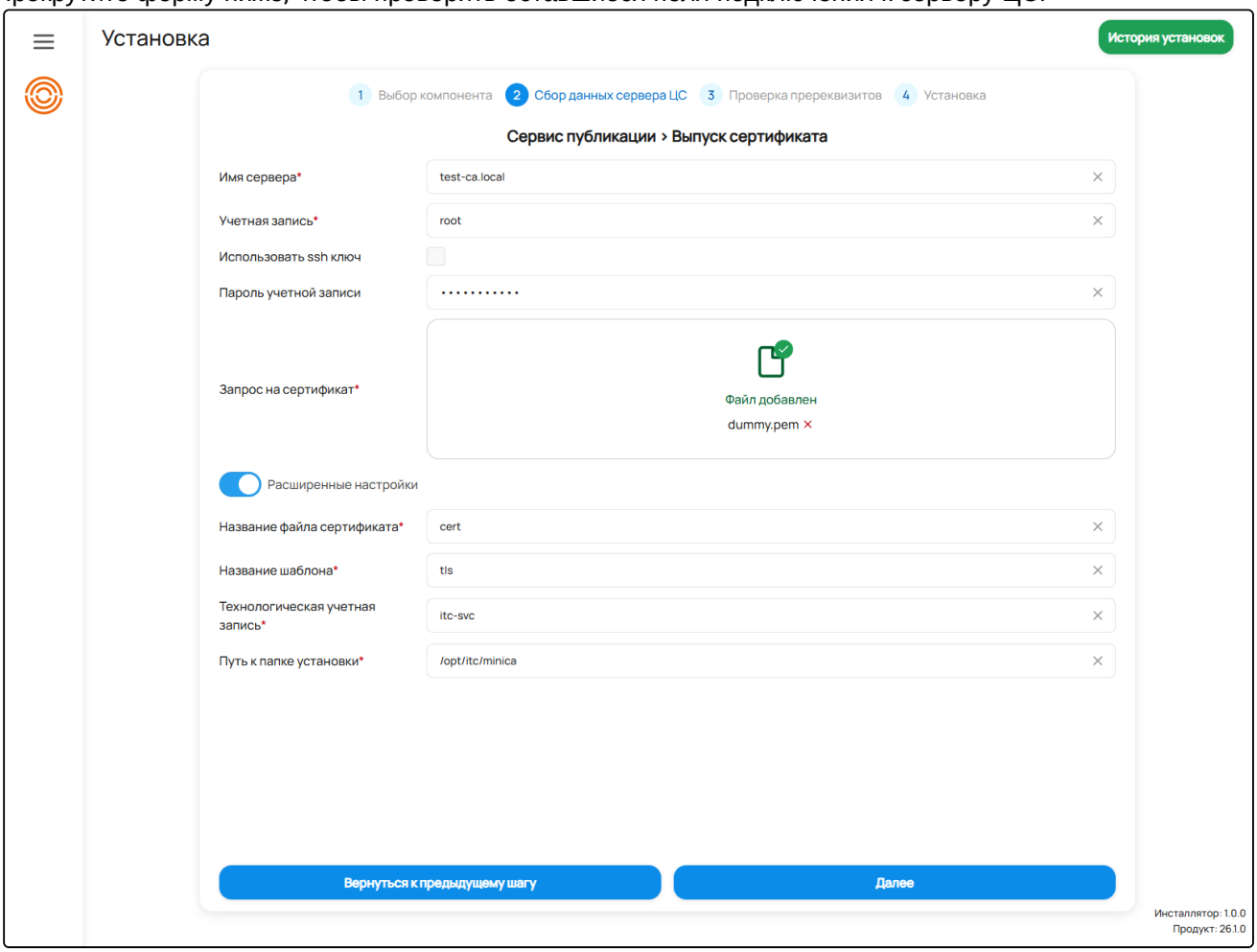
Когда можно пропустить: пропустите этот компонент, если действующий TLS-сертификат для сервиса уже выпущен внешним ЦС или был получен ранее. На этапе «Сервис публикации» вручную загрузите его в поле «TLS-сертификат» (CERTIFICATE_NGINX). Сертификат должен соответствовать имени HOSTNAME и приватному ключу $PATH/itc/certs/nginx-tls.key.

Сбор данных сервера ЦС. Укажите сервер действующего ЦС и учётные данные для SSH-подключения, а также каталог ЦС (PATH, по умолчанию */opt/itc/minica*) и учётку USER_NAME. В поле CSR подставляется результат предыдущего компонента (nginx-tls.csr); он будет помещён на

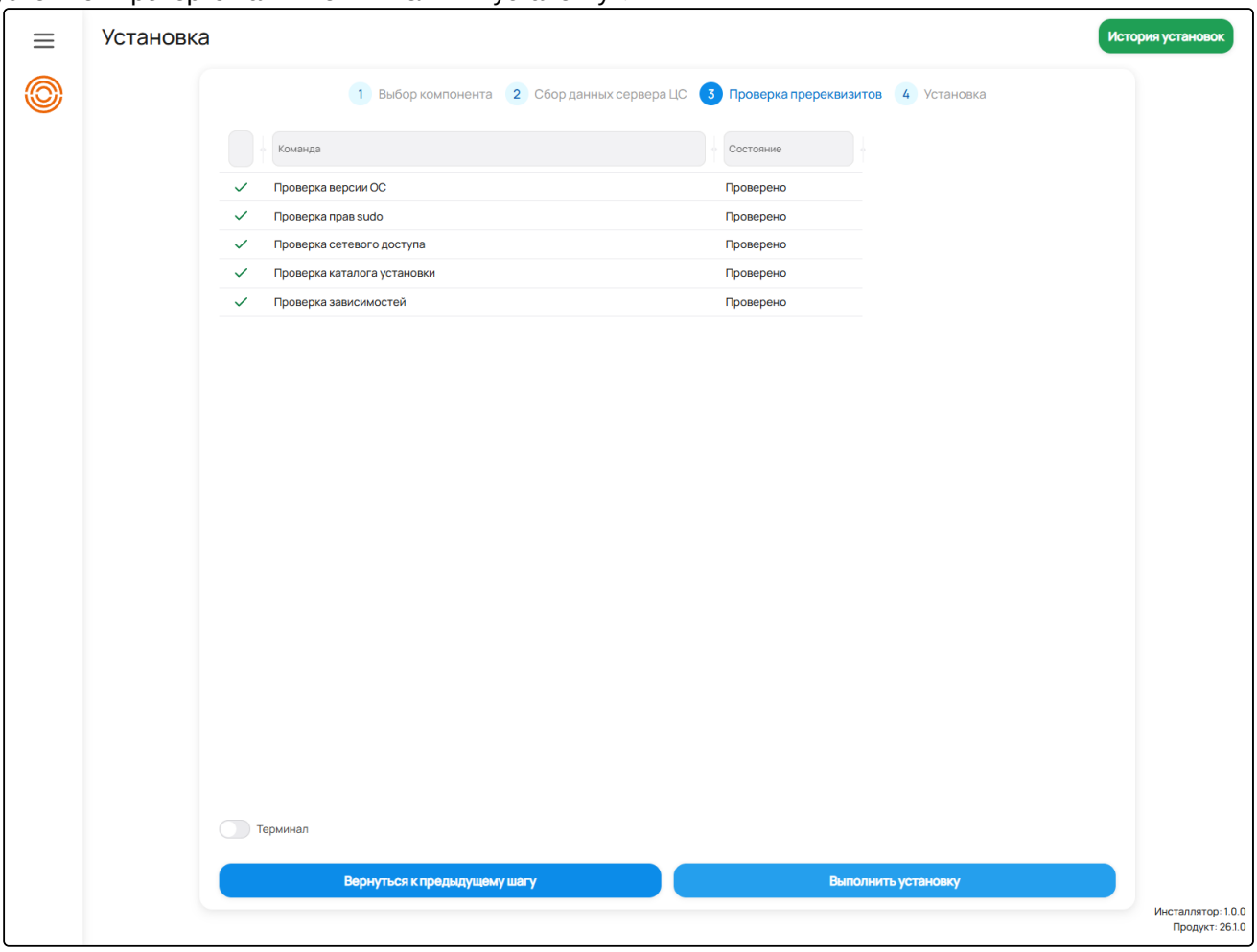
сервере в /tmp и подписан по шаблону tls.



Прокрутите форму ниже, чтобы проверить оставшиеся поля подключения к серверу ЦС.

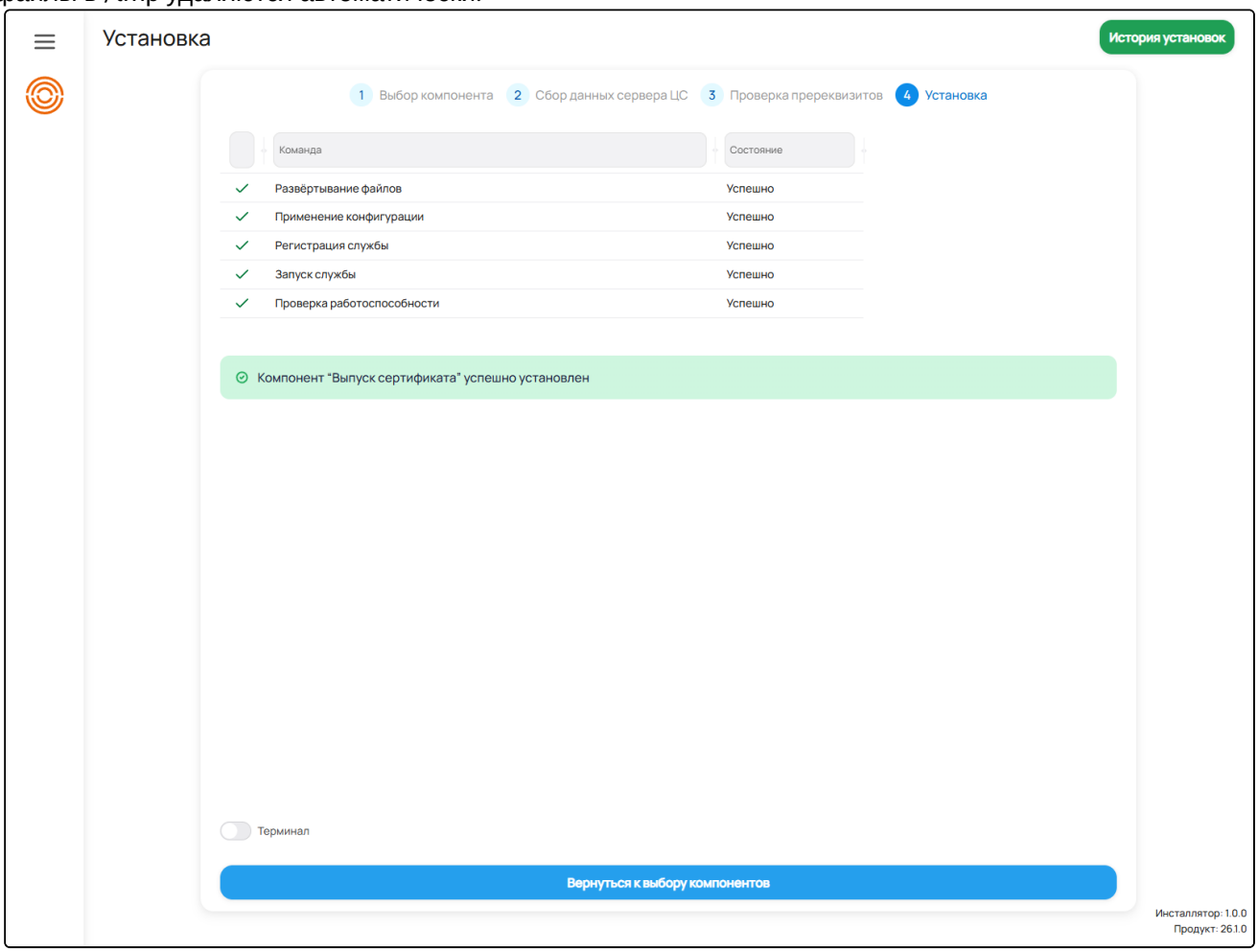


Проверка пререквизитов. Мастер проверяет, что ЦС установлен и отвечает (mclient ping). При успешной проверке нажмите «Выполнить установку».



Установка и результат. ЦС подписывает запрос и возвращает сертификат. Скачайте файл-результат nginx-tls.crt — он будет передан компоненту «Сервис публикации» для настройки TLS Nginx. Временные

файлы в /tmp удаляются автоматически.

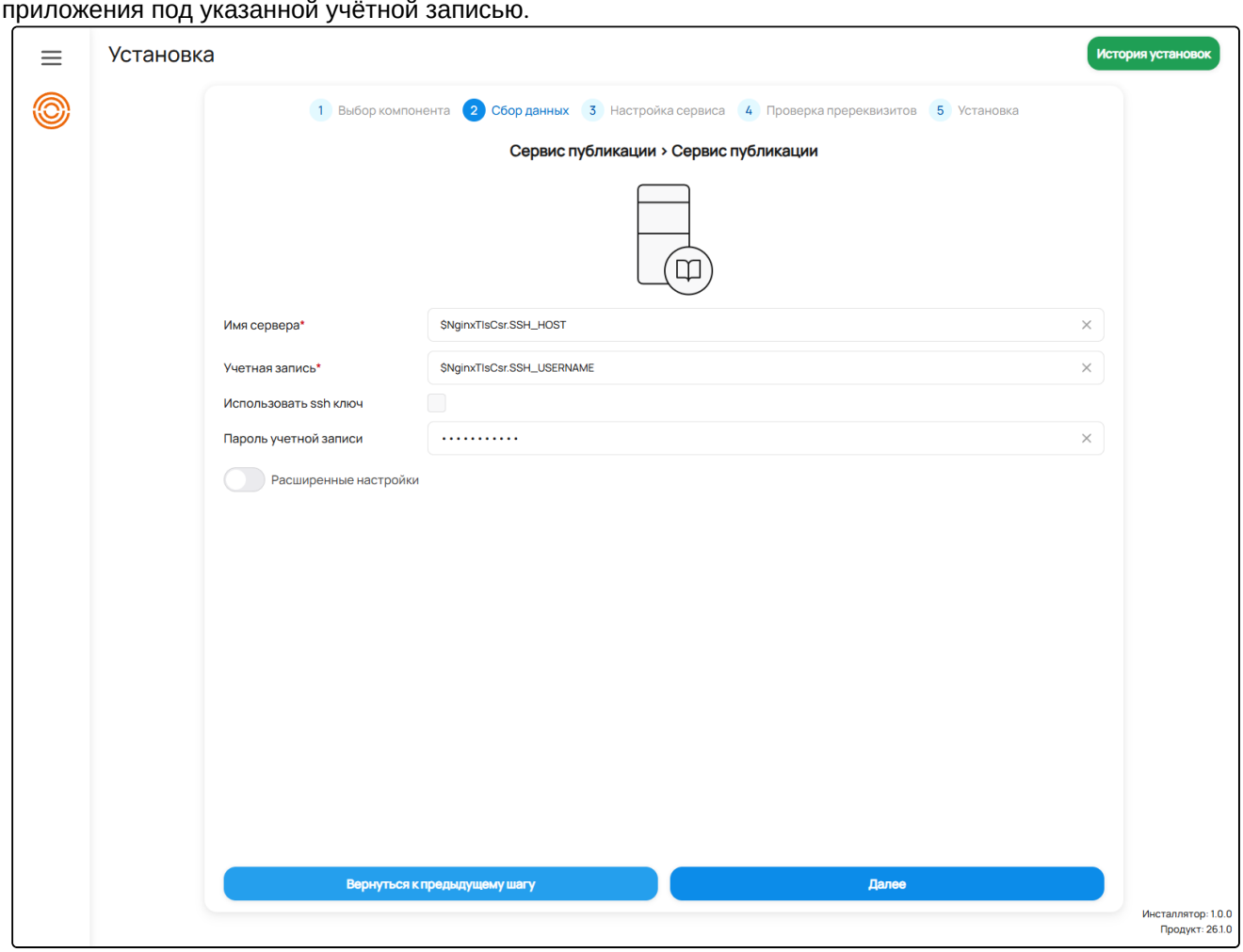


12.3 Сервис публикации

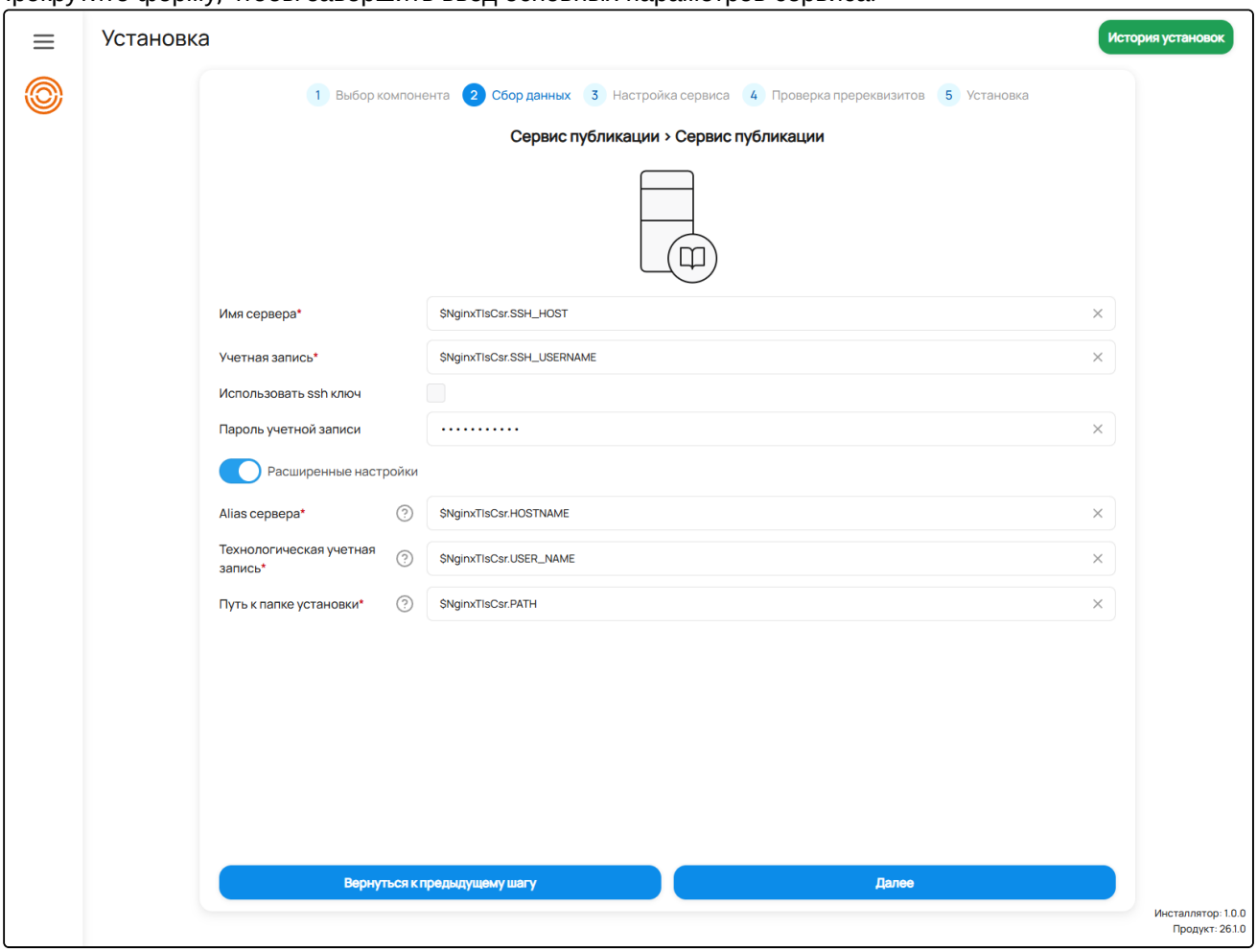
Компонент устанавливает .NET-сервис ITC.Api.MiniCA.Publication (порт 9407) как пользовательский systemd-сервис и публикует его через Nginx (TLS 443, путь */api/publication*).

Сбор данных. Заполните основные параметры сервиса: HOSTNAME, USER_NAME и PATH (подставляются из компонента выпуска запроса на TLS). Служба разворачивается в каталоге

приложения под указанной учётной записью.

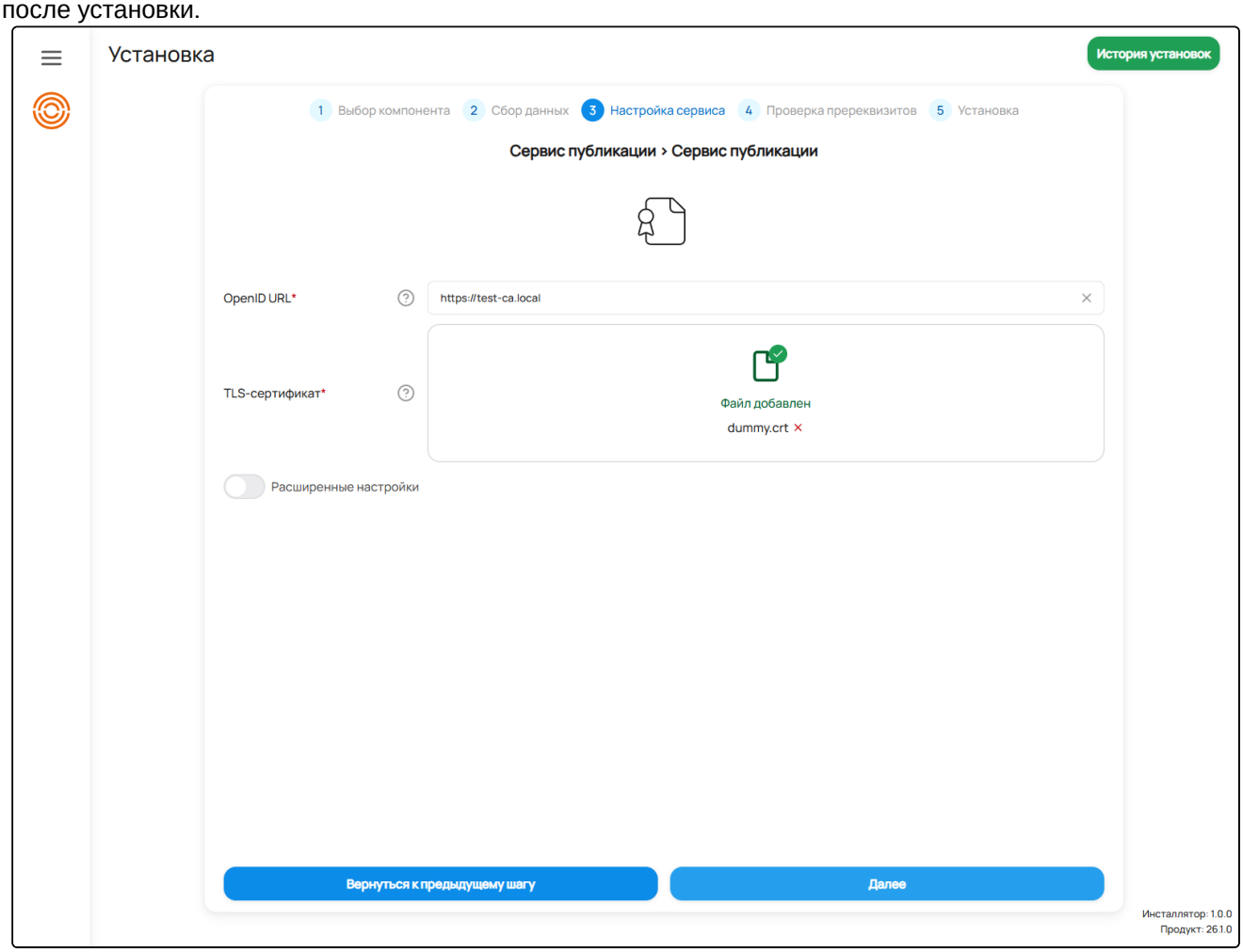


Прокрутите форму, чтобы завершить ввод основных параметров сервиса.

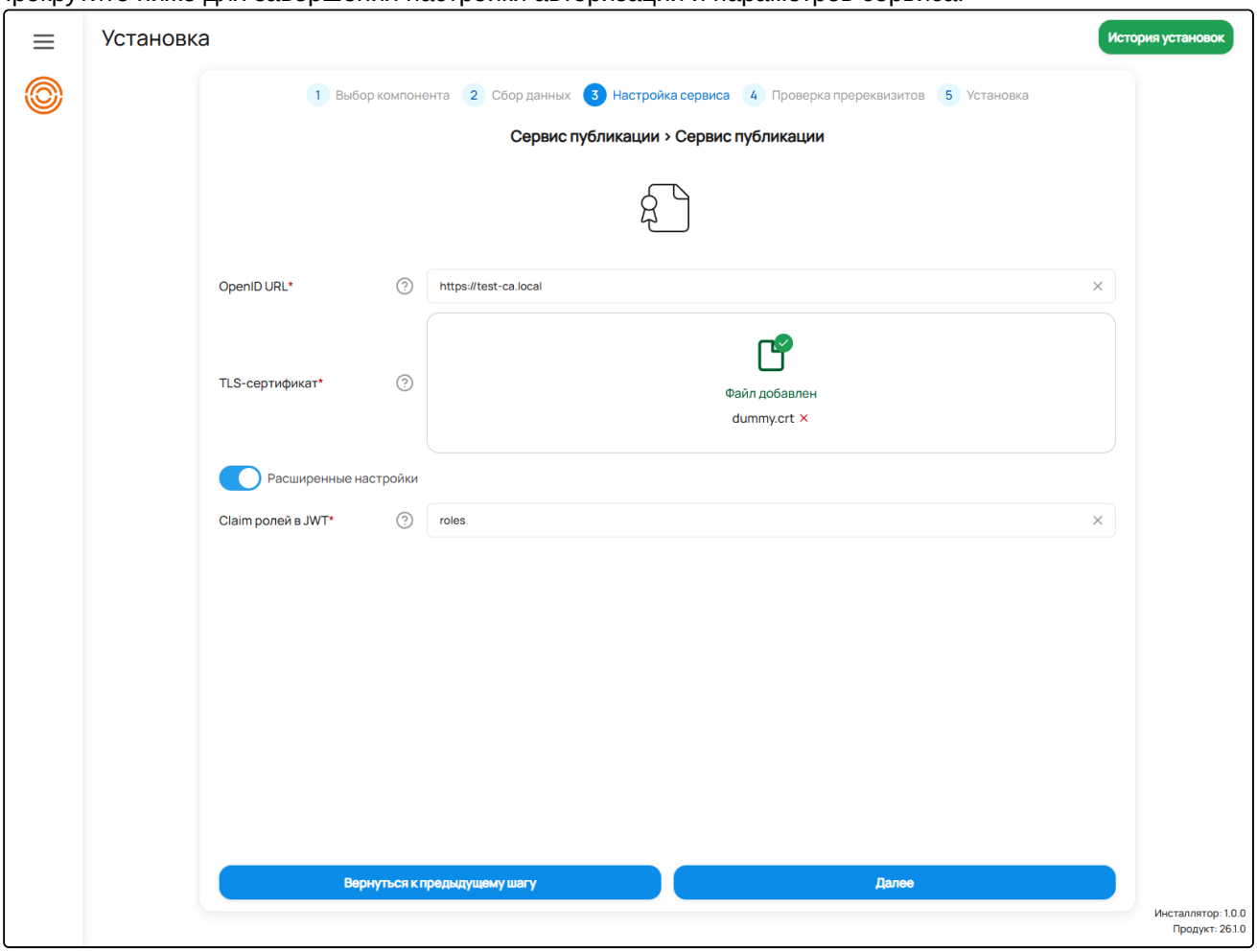


Настройка сервиса. Задайте параметры авторизации: AUTH_URL — адрес провайдера OpenID (из компонента аутентификации), JWT_ROLE_CLAIM — имя claim с ролями (по умолчанию roles), и CERTIFICATE_NGINX — TLS-сертификат Nginx (подставляется nginx-tls.crt, полученный на предыдущем шаге). Задания публикации CRL и сертификатов остаются пустыми и настраиваются пользователем

после установки.

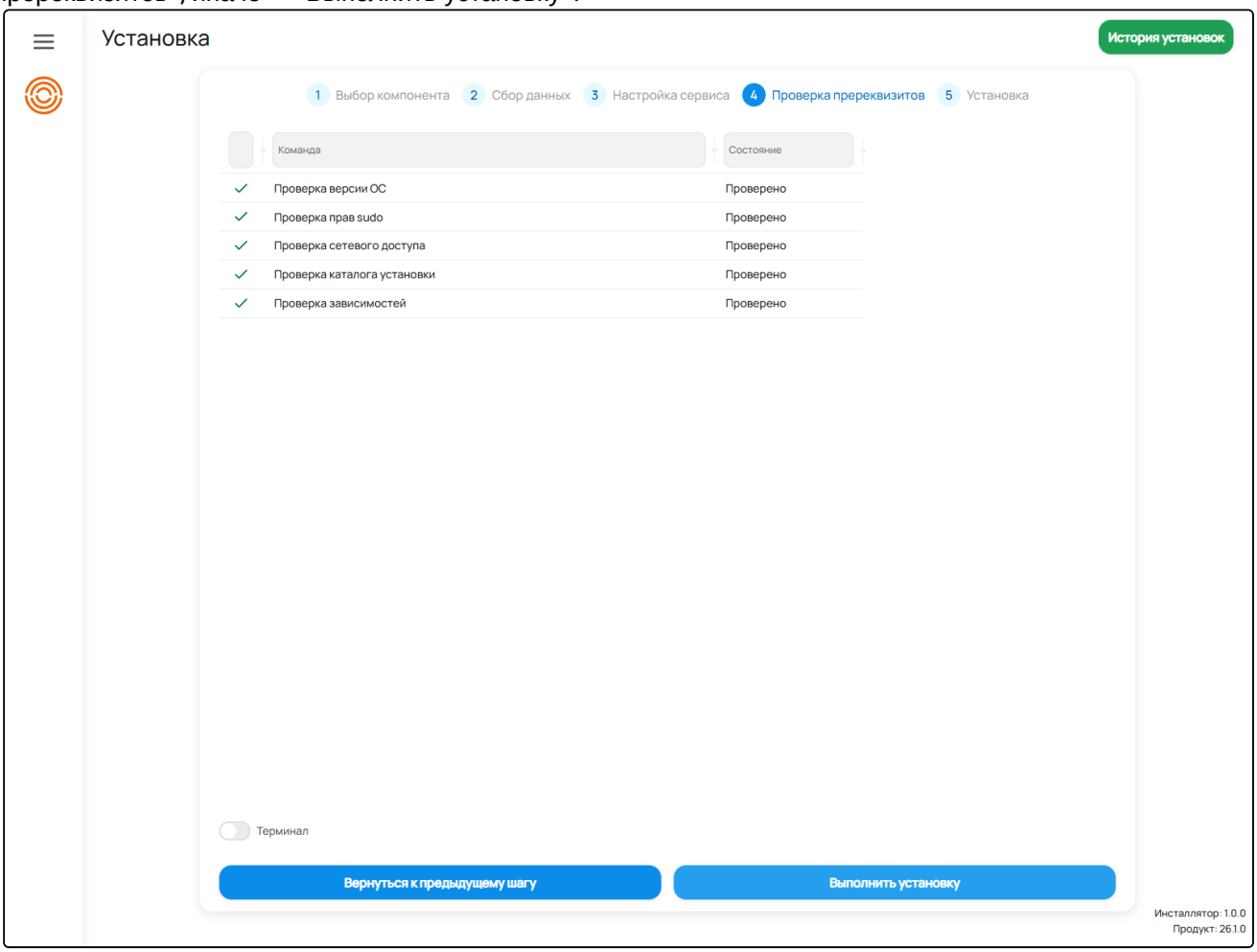


Прокрутите ниже для завершения настройки авторизации и параметров сервиса.

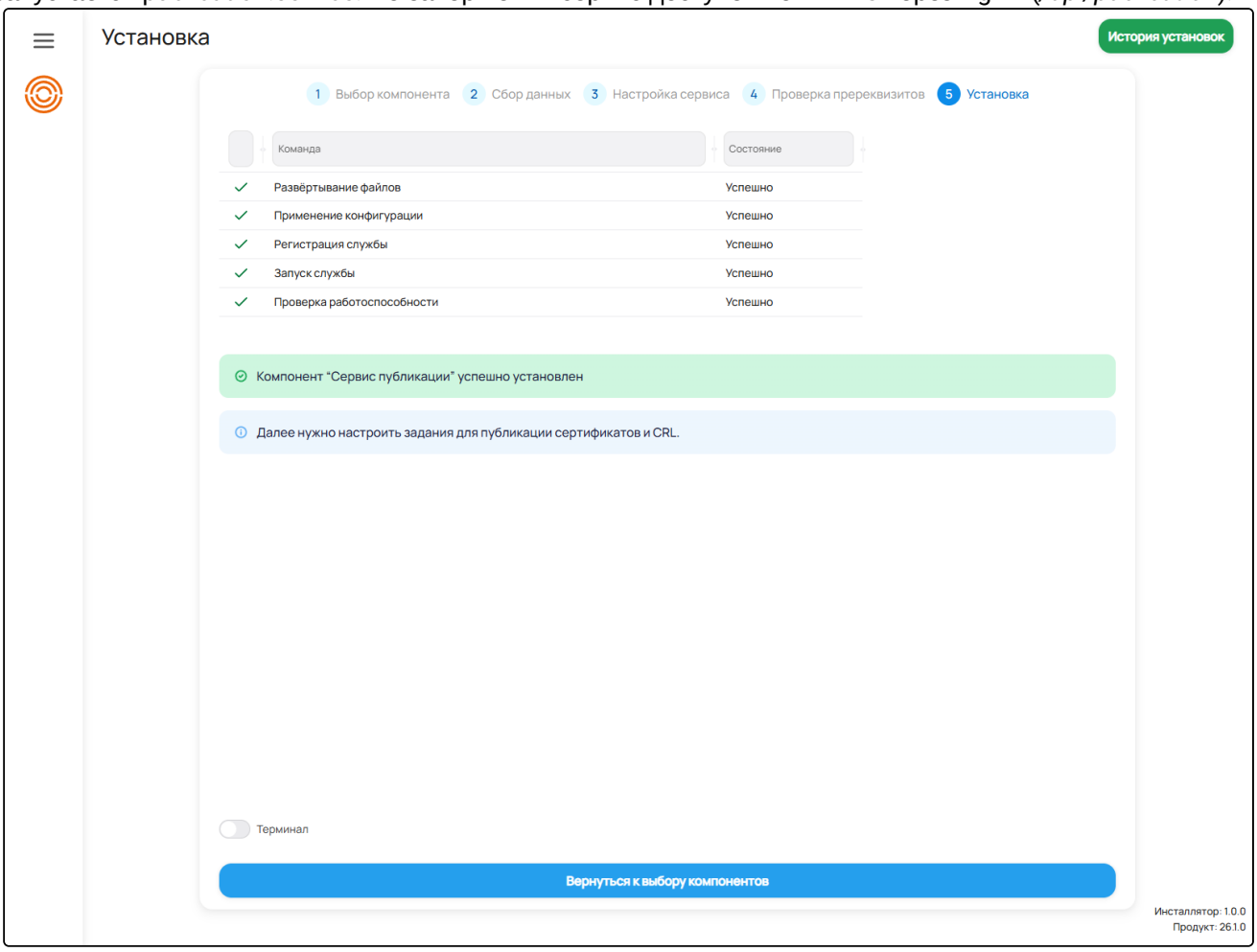


Проверка пререквизитов. Мастер проверяет учётную запись, каталог и права, установленный Nginx и включённый enable-linger. Если есть незакрытые проверки — нажмите «Выполнить настройку

пререквизитов», иначе — «Выполнить установку».



Установка и результат. Разворачивается приложение из архива, копируется конфигурация Nginx и запускается publication.service. По завершении сервис доступен по HTTPS через Nginx (*/api/publication*).

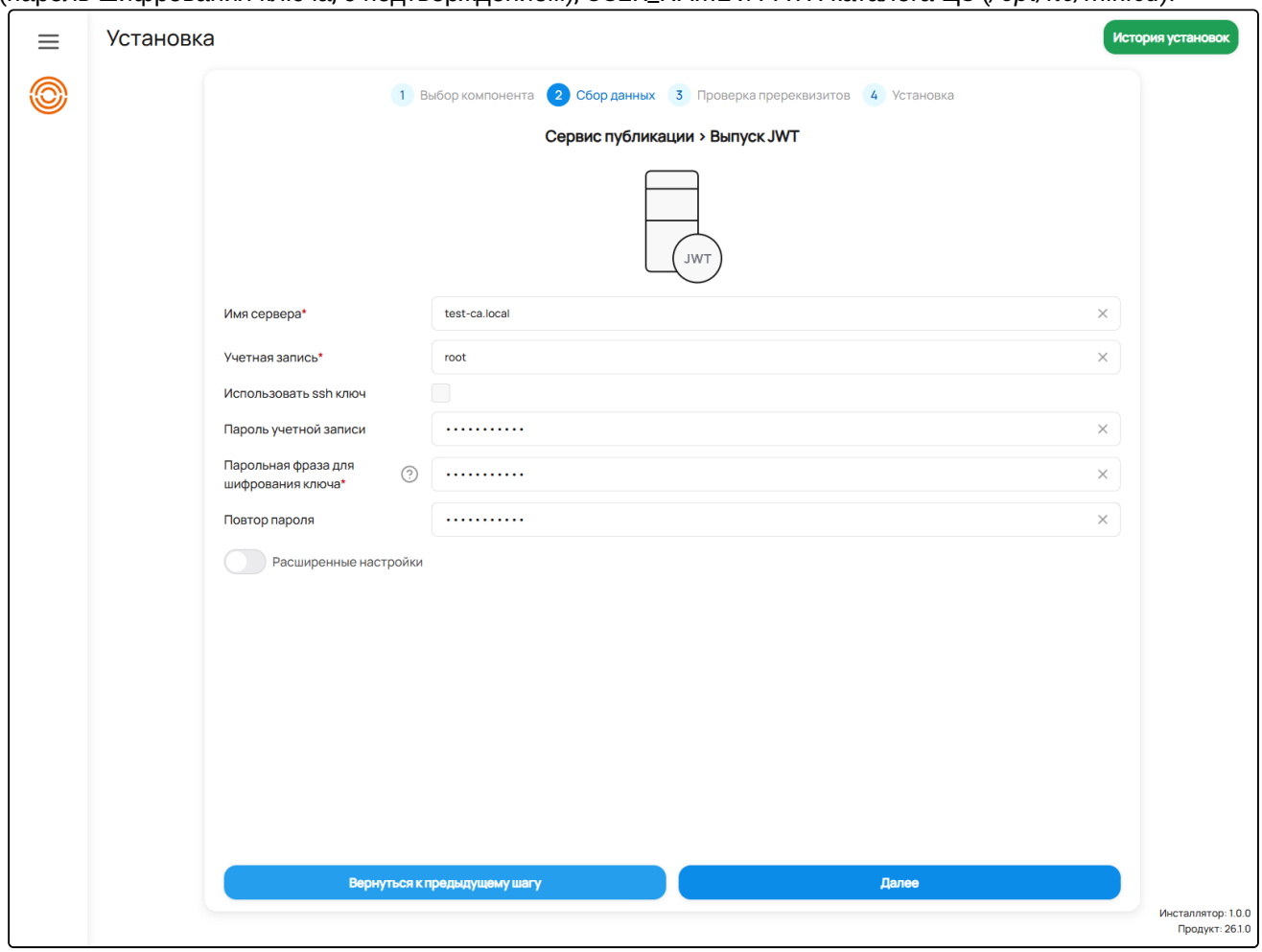


12.4 Выпуск JWT

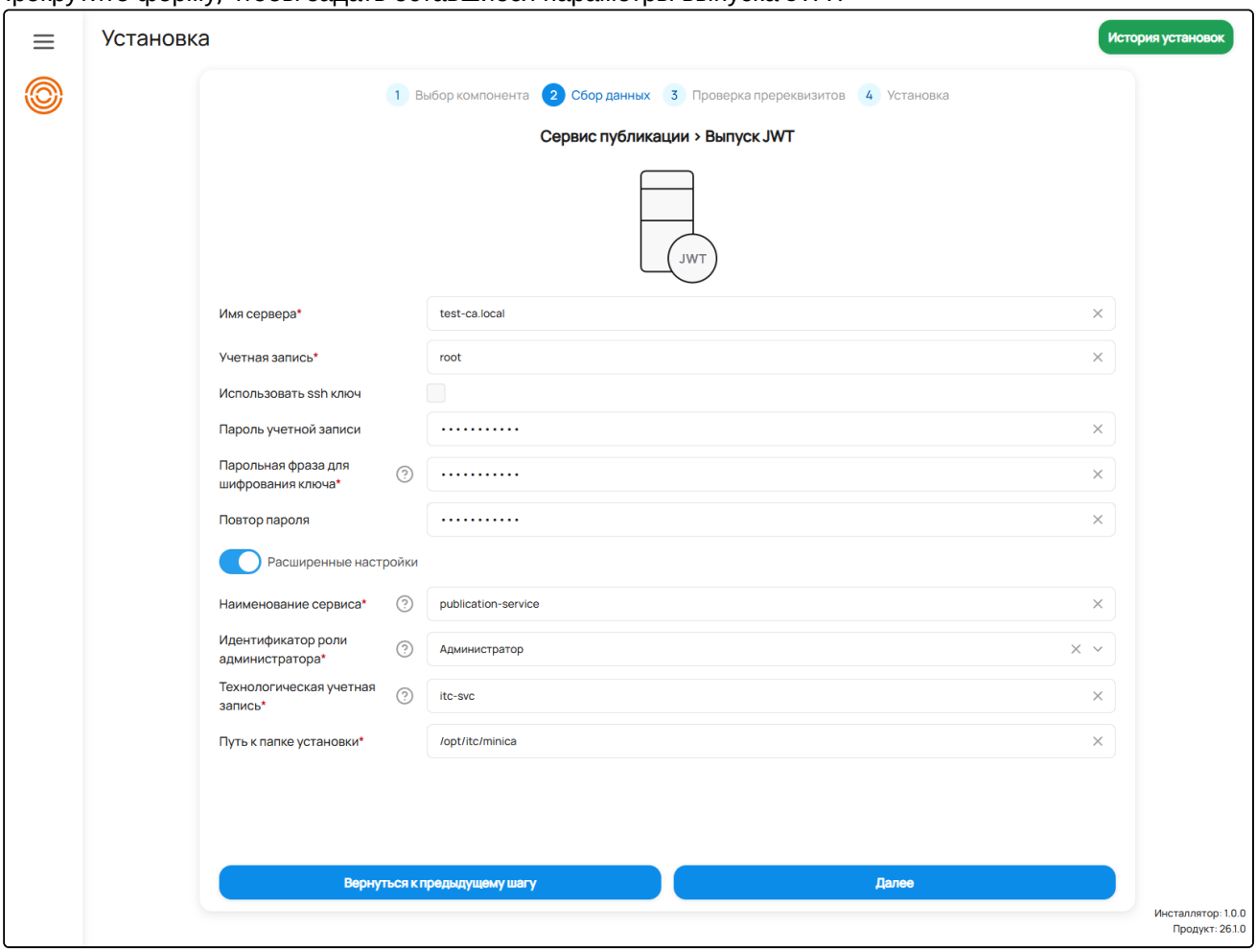
Компонент выпускает на действующем ЦС пару файлов авторизации — токен JWT и зашифрованный приватный ключ — для доступа сервиса публикации к ЦС.

Сбор данных. Укажите сервер ЦС и SSH-доступ, а также параметры выпуска: NAME_SERVICE (для сервиса публикации — publication-service), ROLE (роль токена, по умолчанию admin), PASSWORD_KEY

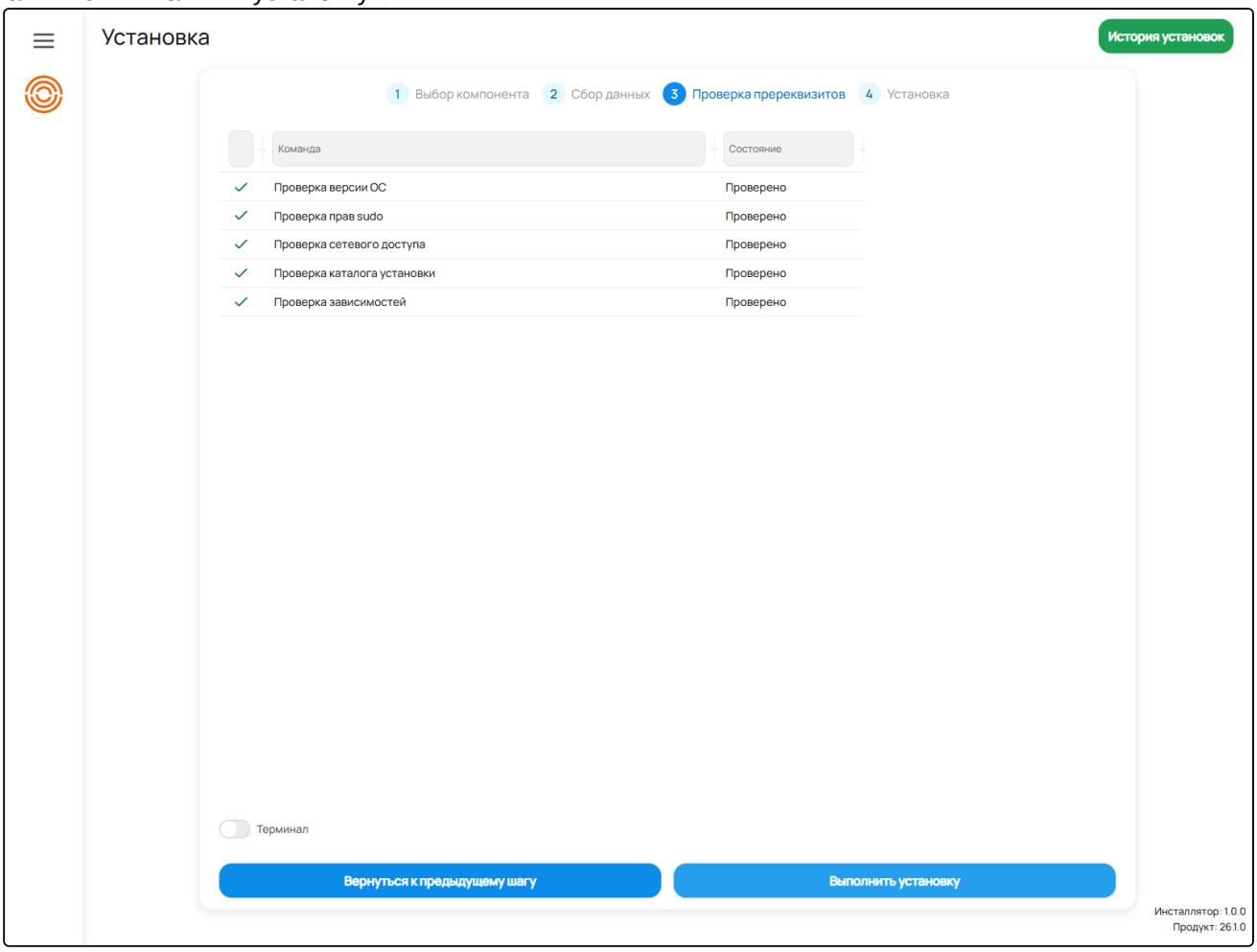
(пароль шифрования ключа, с подтверждением), USER_NAME и PATH каталога ЦС (*/opt/itc/minica*).



Прокрутите форму, чтобы задать оставшиеся параметры выпуска JWT.

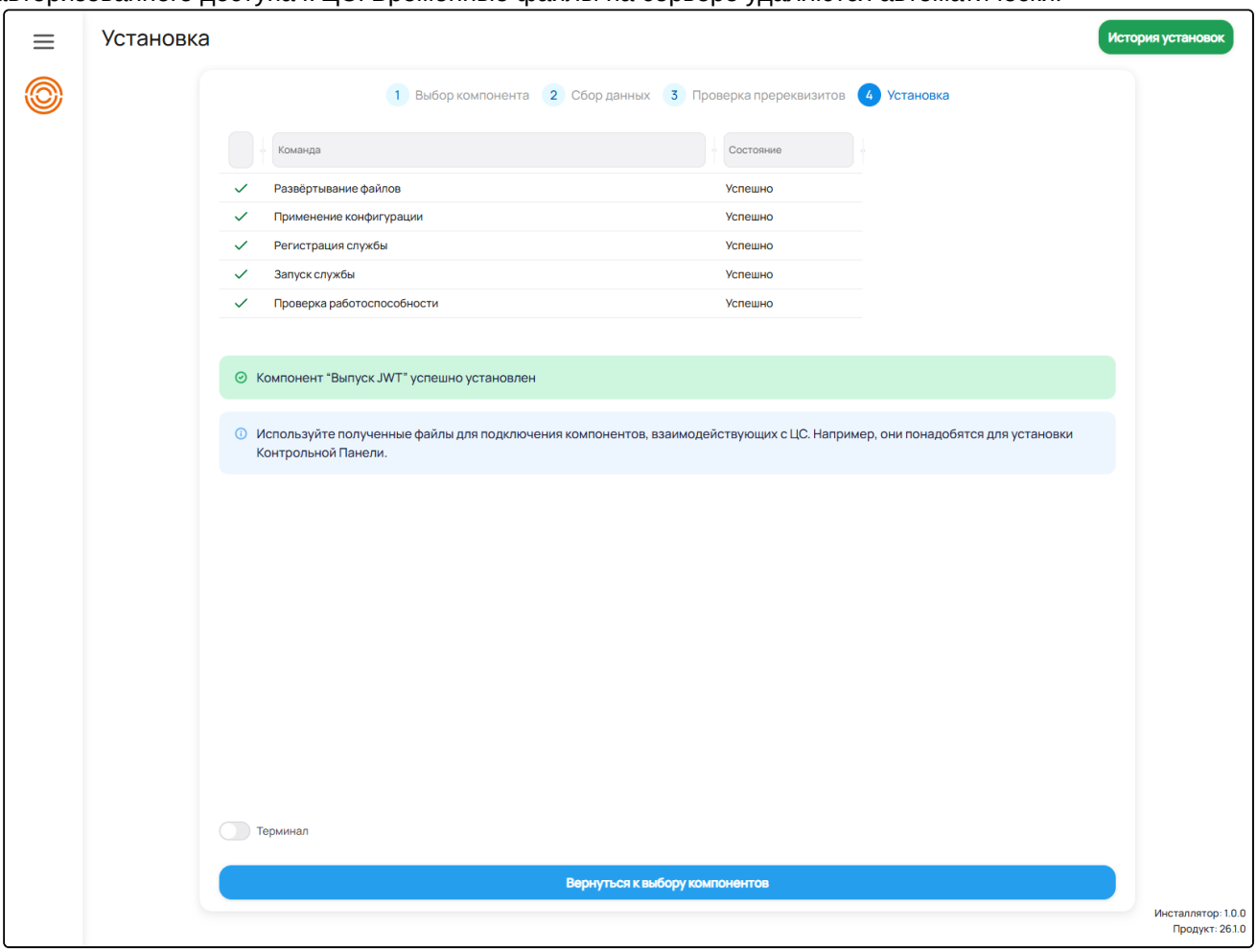


Проверка пререквизитов. Мастер проверяет доступность ЦС (mclient ping). При успешной проверке нажмите «Выполнить установку».



Установка и результат. ЦС формирует токен и зашифрованный ключ. Скачайте оба файла-результата — publication-service.jwt и publication-service.encrypted.key; они используются сервисом публикации для

авторизованного доступа к ЦС. Временные файлы на сервере удаляются автоматически.



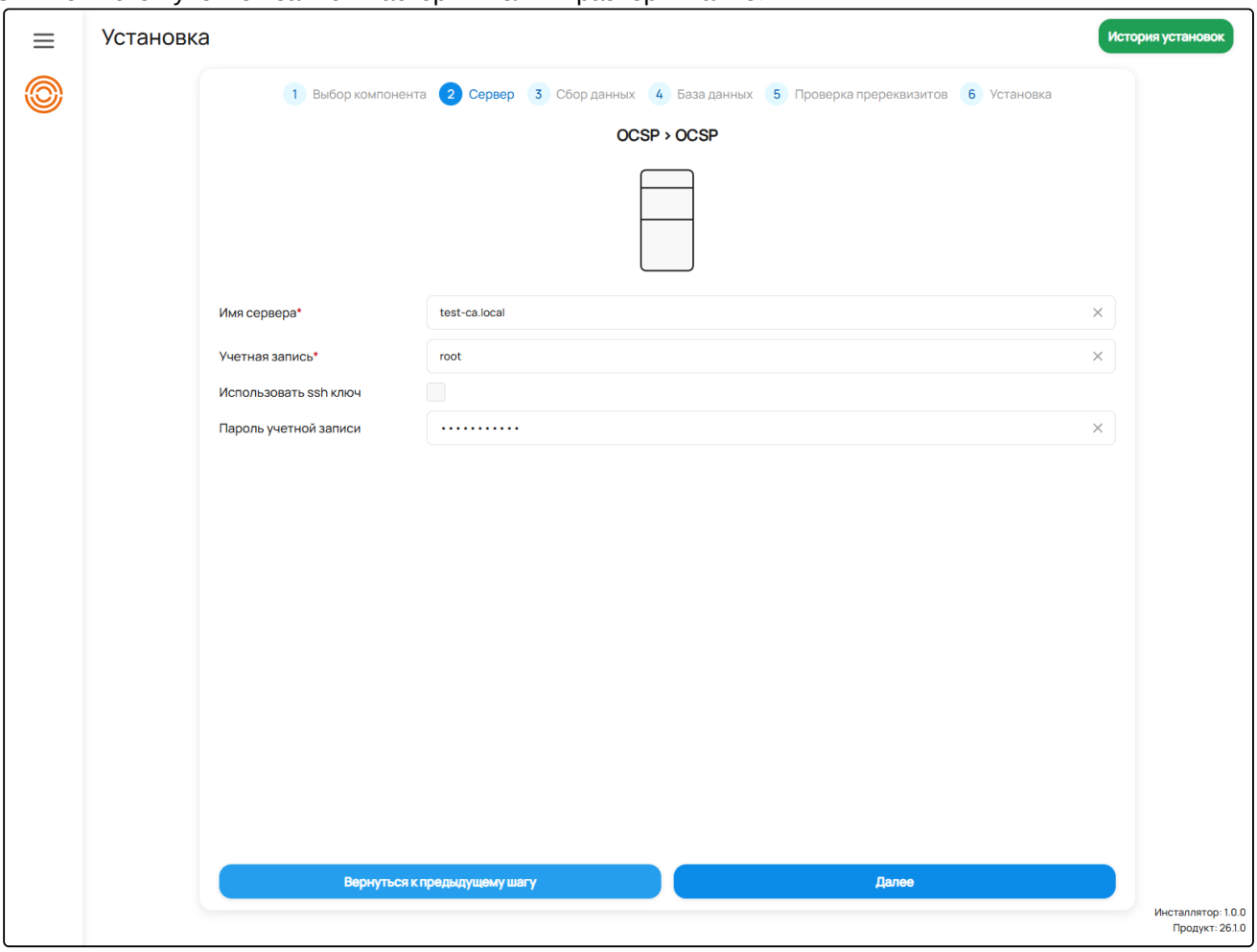
13 OCSP

Группа разворачивает службу проверки статуса сертификатов по протоколу OCSP (респондер mOCSP), который в реальном времени отвечает на запросы о действительности сертификатов, читая их статусы из базы данных ЦС. Компоненты устанавливаются в следующем порядке: OCSP (развёртывание сервиса mOCSP и выпуск запроса на сертификат подписи), Выпуск сертификата (подпись этого запроса на действующем ЦС) и Настройка OCSP (установка выпущенного сертификата подписи и запуск сервиса).

13.1 OCSP

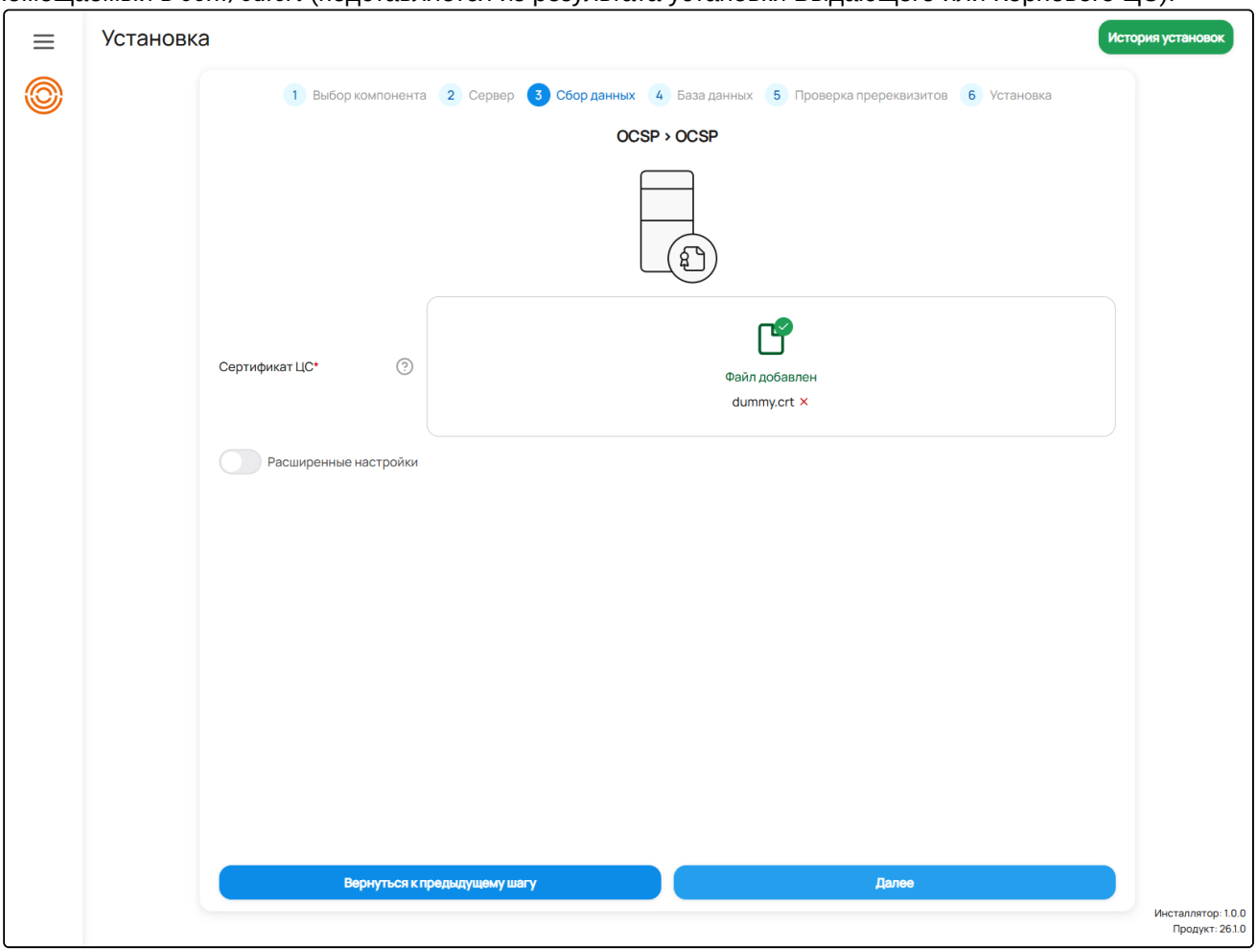
Устанавливает бинарь mocsp и конфигурацию в каталог */opt/itc/ocsp*, поднимает пользовательский systemd-сервис mocsp и на этом этапе формирует запрос (CSR) на сертификат, которым будут подписываться OCSP-ответы.

Сервер. Укажите параметры подключения к целевому серверу по SSH: имя сервера (адрес), учётную запись и способ аутентификации — установите флажок «Использовать ssh ключ» либо введите пароль. От имени этой учётной записи мастер выполнит развёртывание.

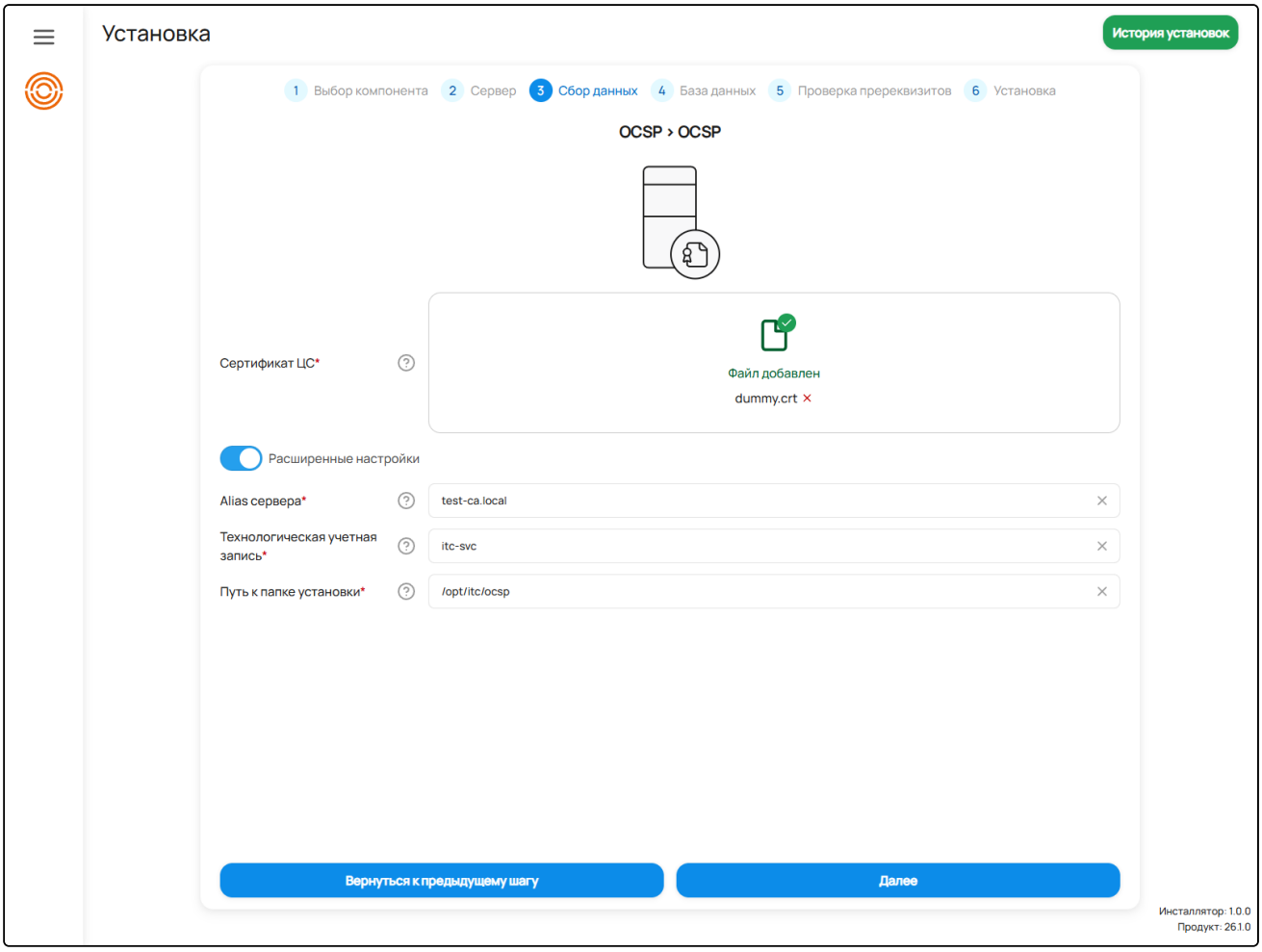


Сбор данных. Заполните параметры сервиса OCSP: HOSTNAME (имя сервера, используется как CN/SAN сертификата подписи), USER_NAME — технологическая учётная запись-владелец (по умолчанию itc-svc), PATH — каталог установки (по умолчанию */opt/itc/ocsp*) и CERTIFICATE_CA — сертификат ЦС,

помещаемый в *conf/ca.crt* (подставляется из результата установки Выдающего или Корневого ЦС).

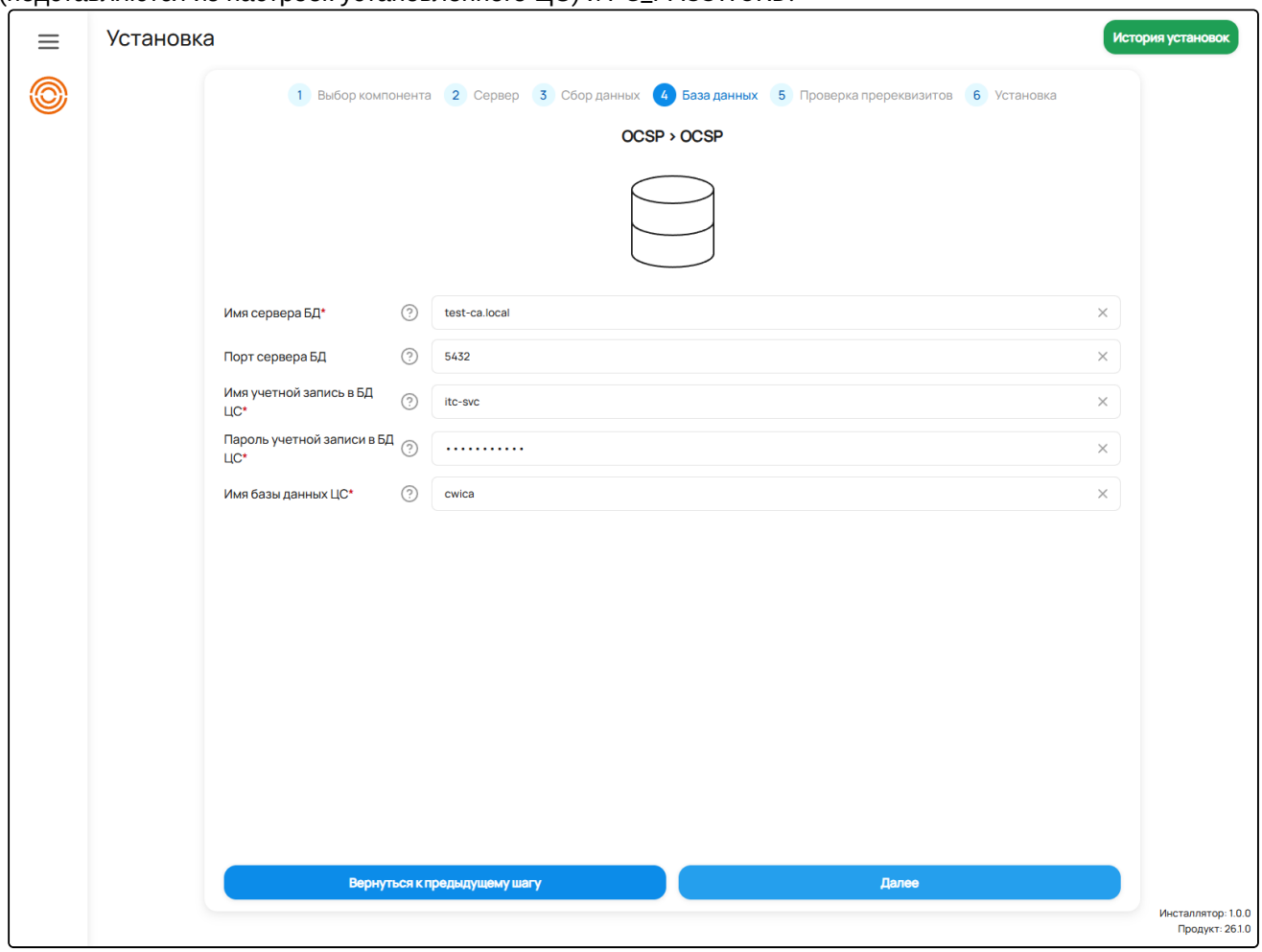


Прокрутите экран, чтобы проверить и при необходимости скорректировать оставшиеся значения этого шага.



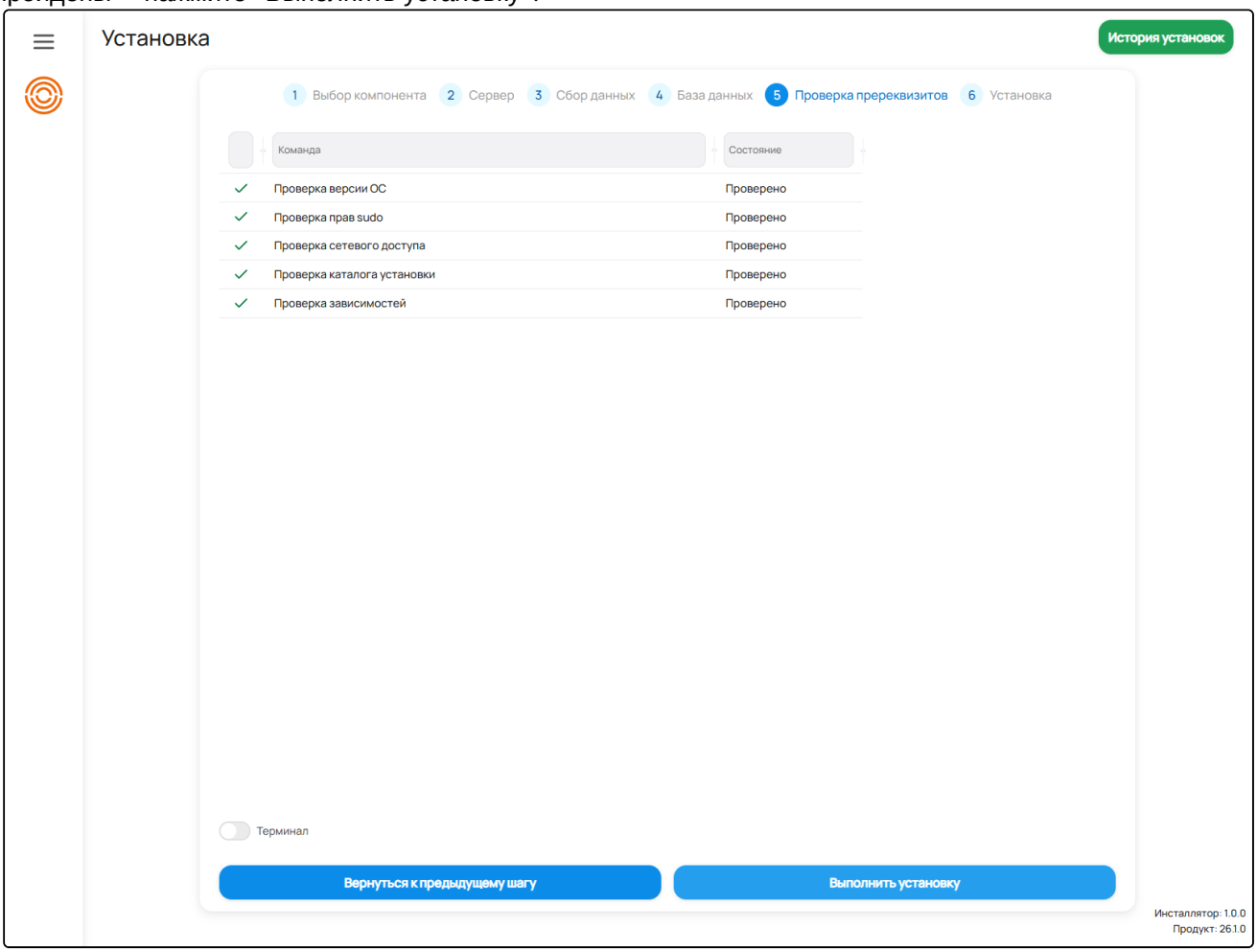
База данных. Задайте параметры подключения к базе данных ЦС, из которой mOCSP берёт статусы сертификатов: PG_HOST (адрес сервера БД), PG_PORT (по умолчанию 5432), PG_USERNAME, PG_DB

(подставляются из настроек установленного ЦС) и PG_PASSWORD.



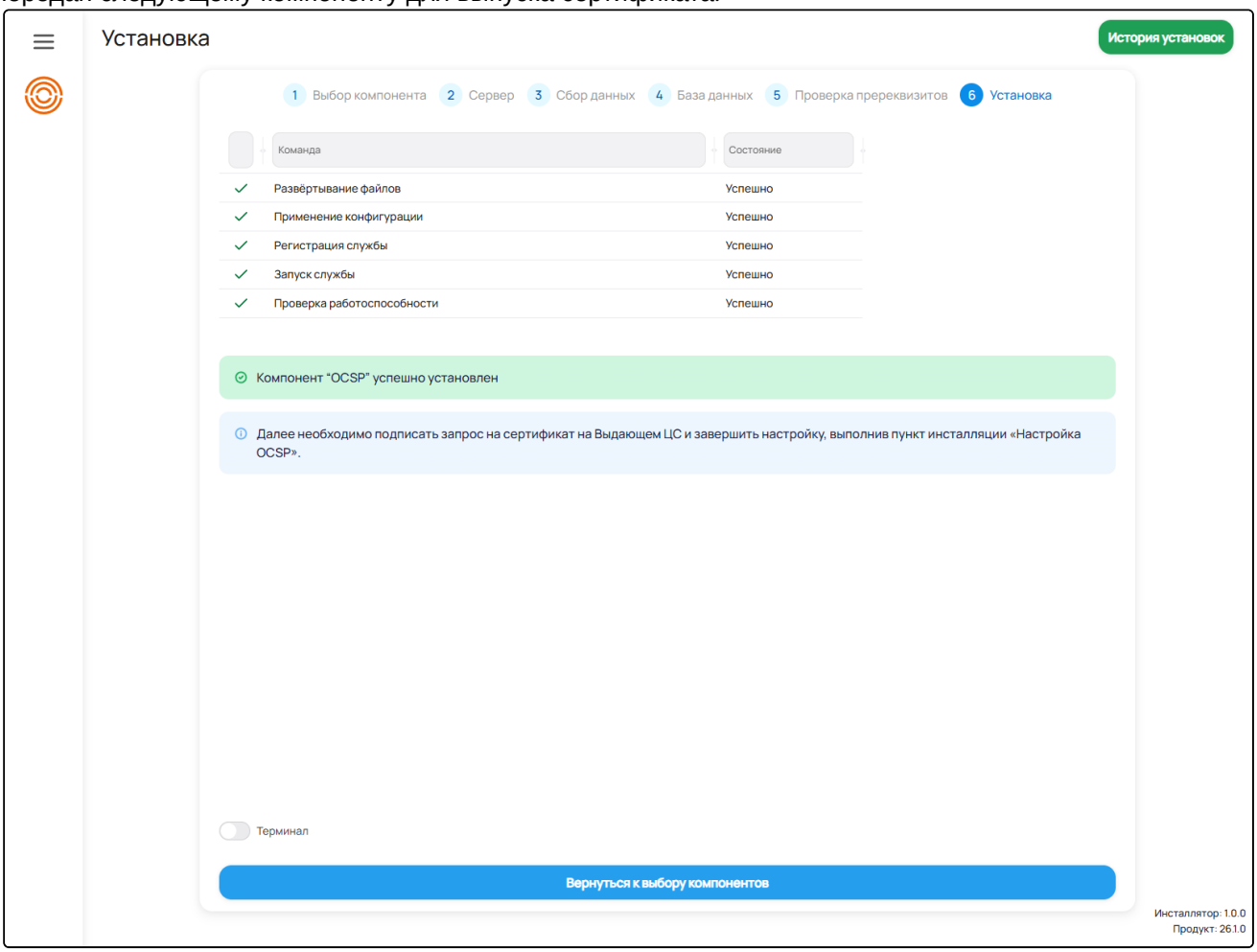
Проверка пререквизитов. Мастер проверяет наличие технологической учётной записи, каталога установки и прав на него, включённый linger для пользовательских служб, а также доступность БД ЦС. Если есть незакрытые проверки, нажмите «Выполнить настройку пререквизитов»; когда все проверки

пройдены — нажмите «Выполнить установку».



Установка и результат. Мастер разворачивает сервис mOCSP и генерирует запрос на сертификат подписи. По завершении становится доступен файл-результат mocsp.csr — скачайте его: он будет

передан следующему компоненту для выпуска сертификата.

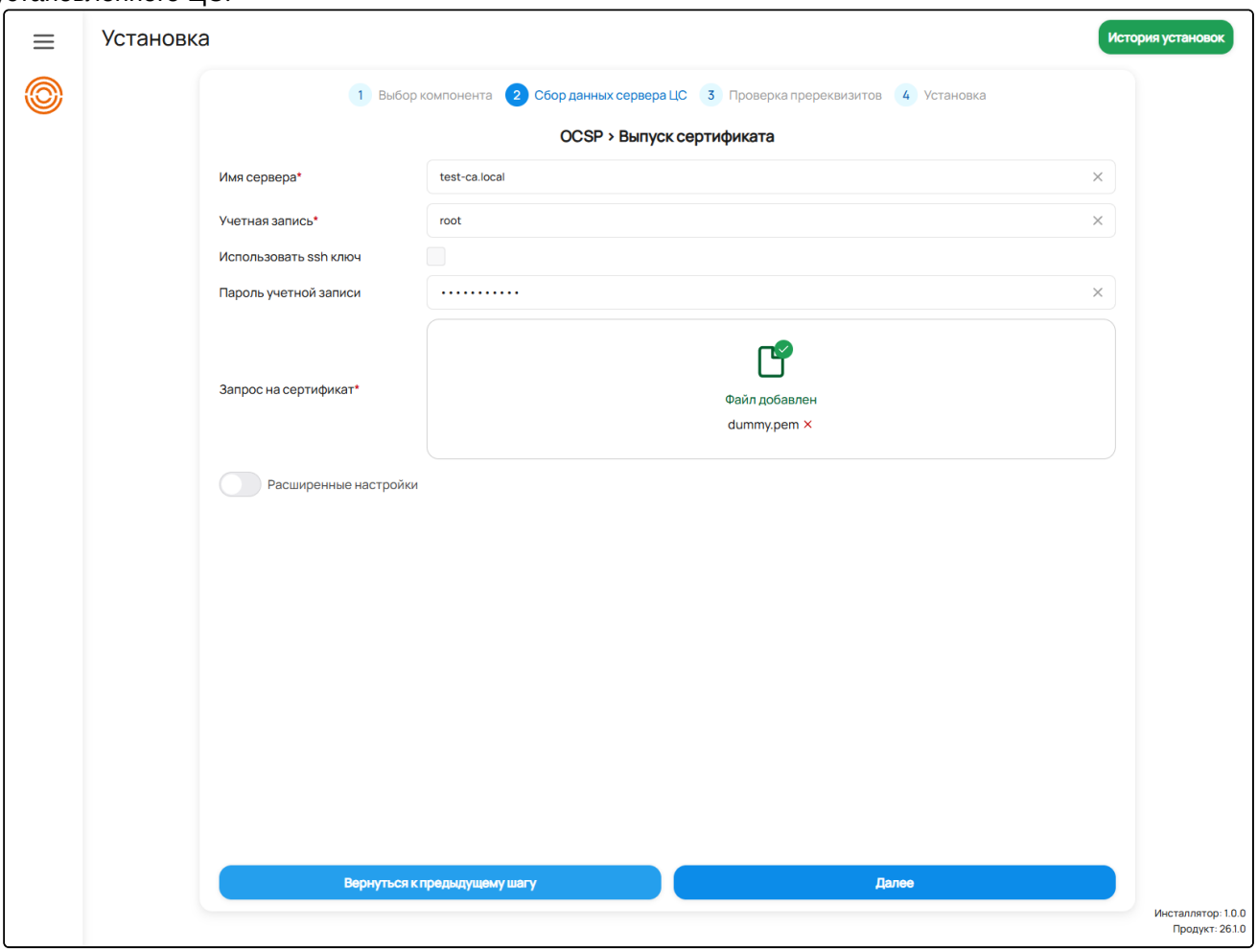


13.2 Выпуск сертификата

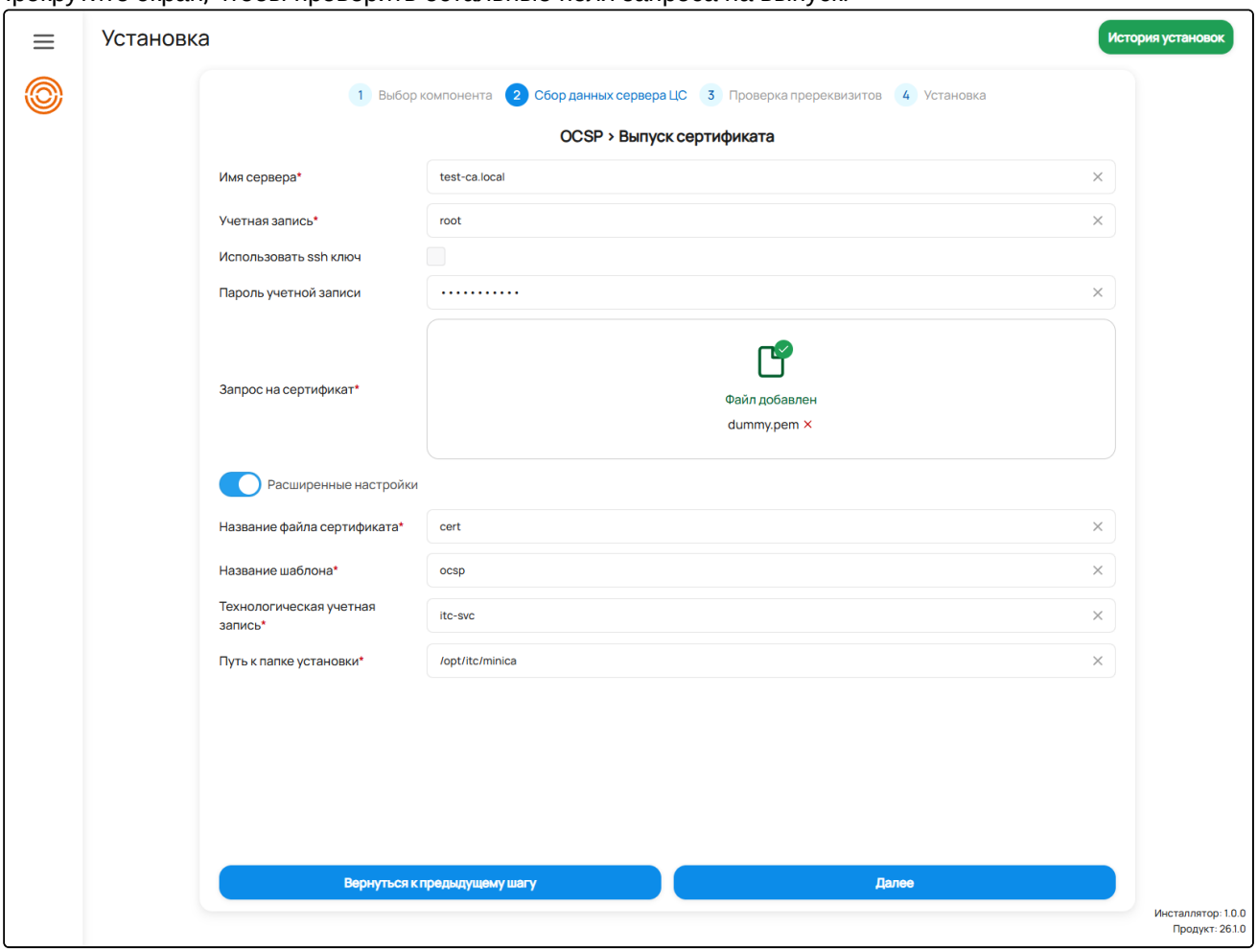
Служебный компонент: подключается к серверу действующего ЦС и через mclient подписывает запрос mocsp.csr по шаблону ocsp, возвращая сертификат подписи OCSP-ответов.

Сбор данных сервера ЦС. Укажите данные сервера ЦС, на котором выпускается сертификат: имя файла (NAME_FILE), шаблон выпуска TEMPLATE (для OCSP — ocsp), содержимое запроса CSR (подставляется из результата mocsp.csr предыдущего компонента), а также USER_NAME и PATH

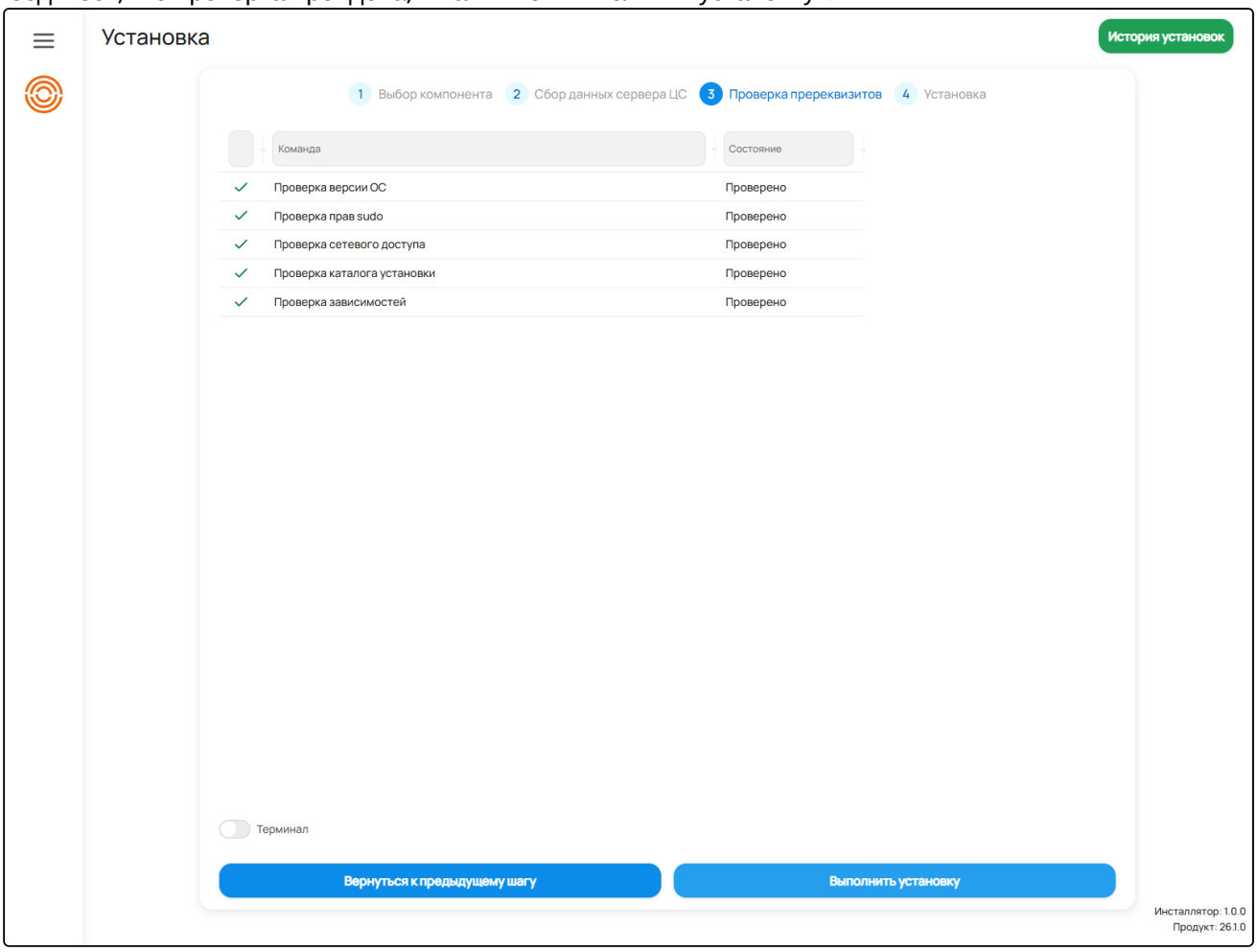
установленного ЦС.



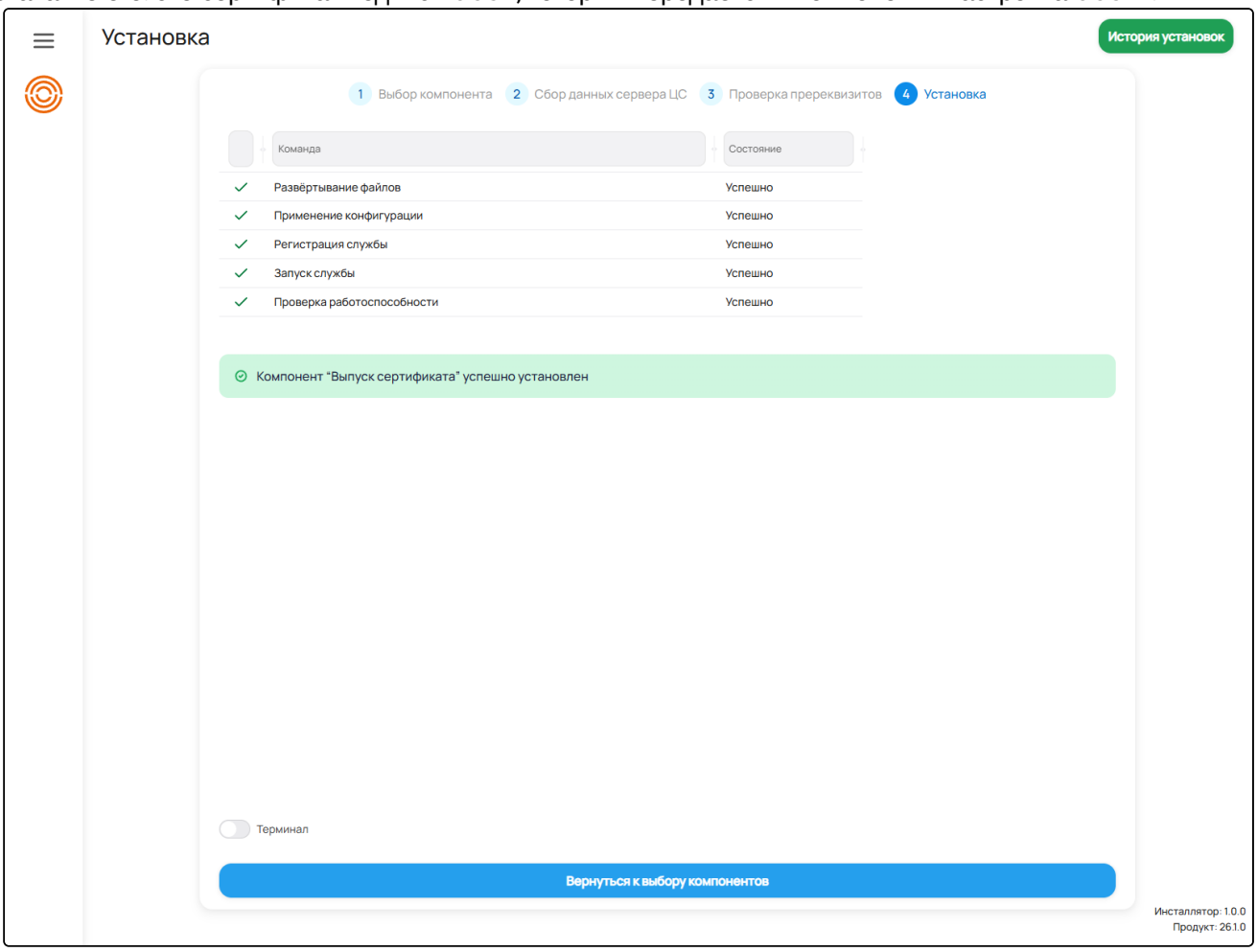
Прокрутите экран, чтобы проверить остальные поля запроса на выпуск.



Проверка пререквизитов. Мастер проверяет, что ЦС установлен и доступен (команда mclient ping). Убедитесь, что проверка пройдена, и нажмите «Выполнить установку».



Установка и результат. ЦС подписывает запрос, и мастер формирует файл-результат mocsp.crt — скачайте его: это сертификат подписи OCSP, который передаётся в компонент «Настройка OCSP».

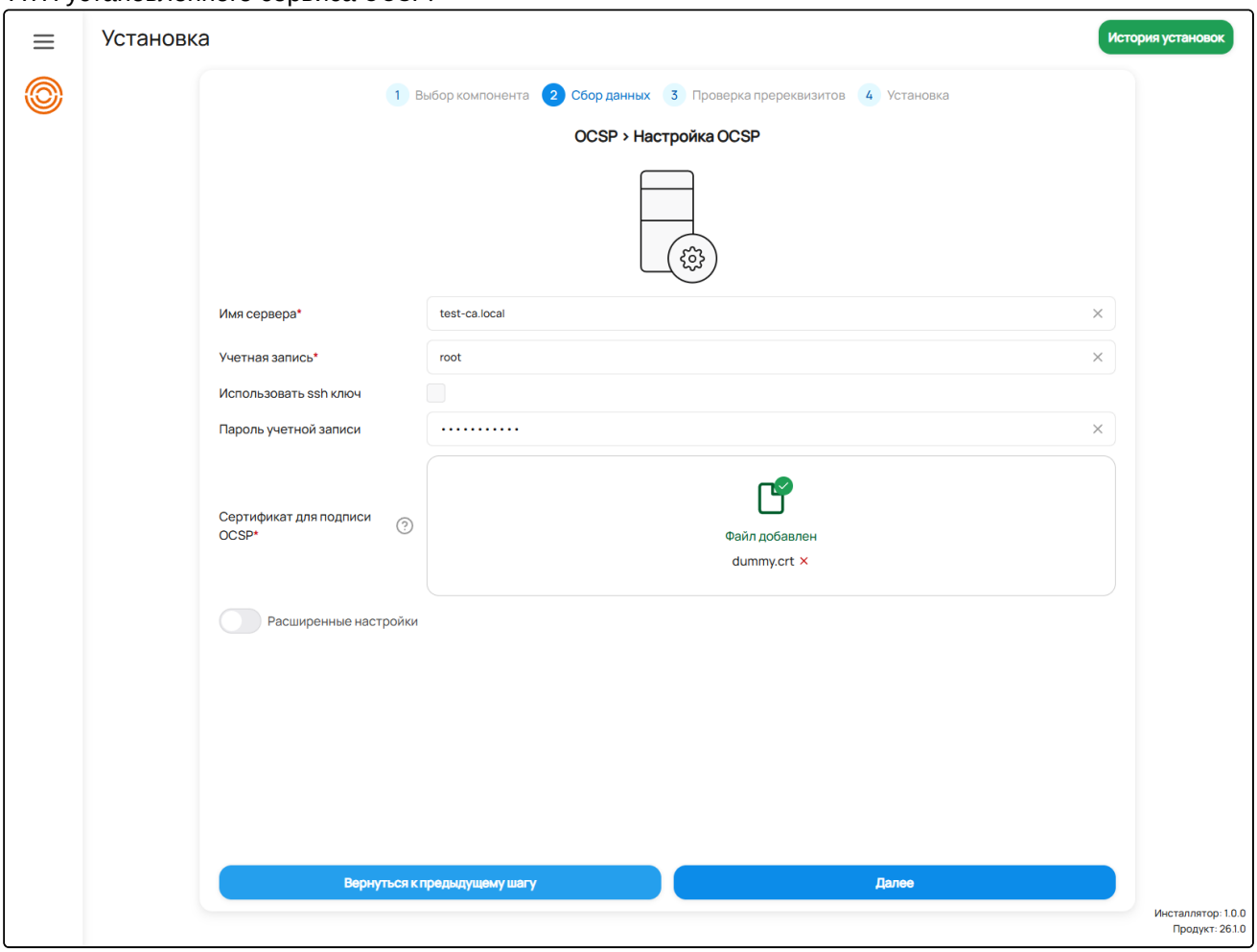


13.3 Настройка OCSP

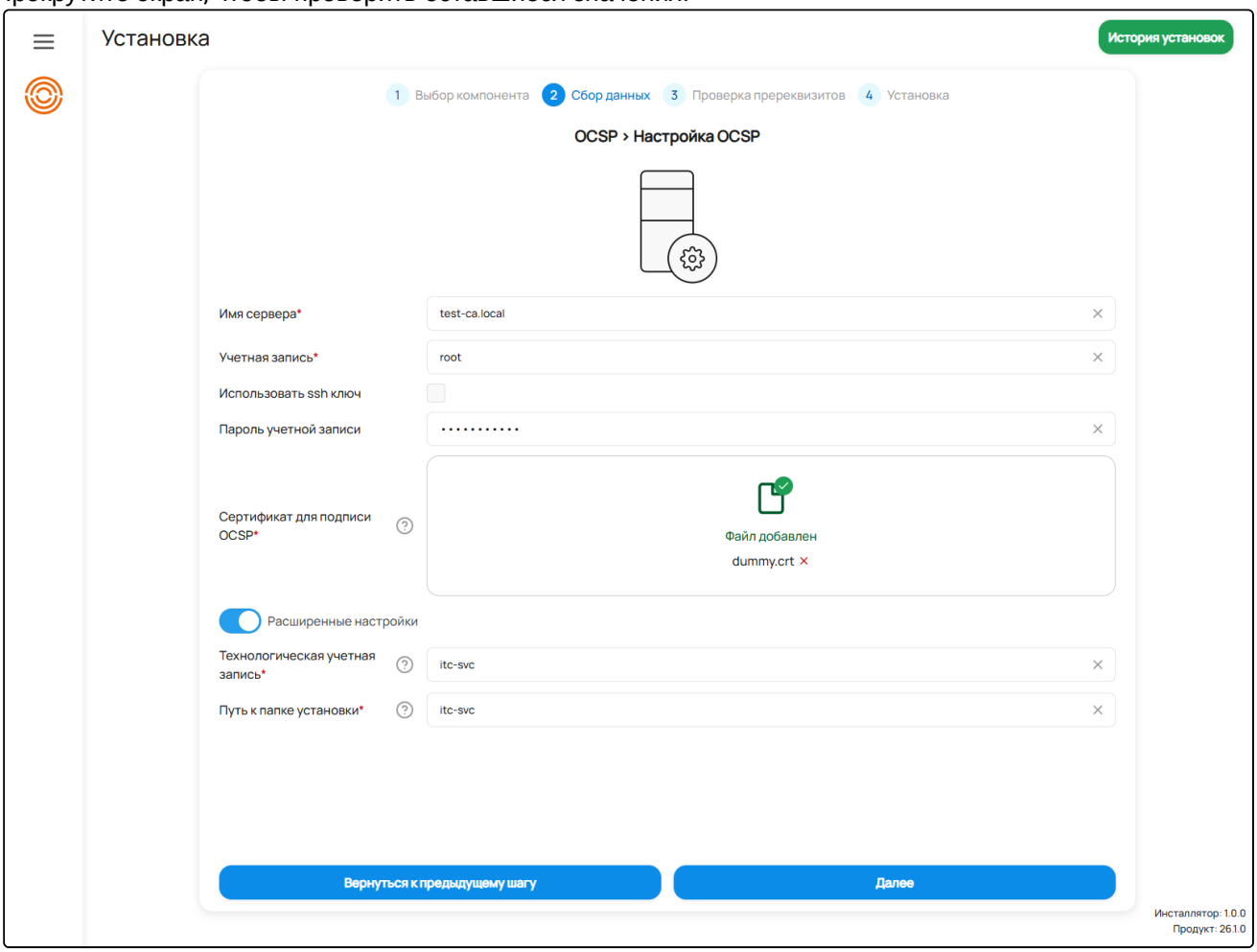
Завершающий компонент: загружает выпущенный сертификат подписи на развёрнутый сервис mOCSP, включает автозапуск и запускает службу.

Сбор данных. Укажите CERTIFICATE_OCSP — сертификат подписи OCSP-ответов, помещаемый в *conf/mocsp.crt* (подставляется из результата mocsp.crt предыдущего компонента), а также USER_NAME и

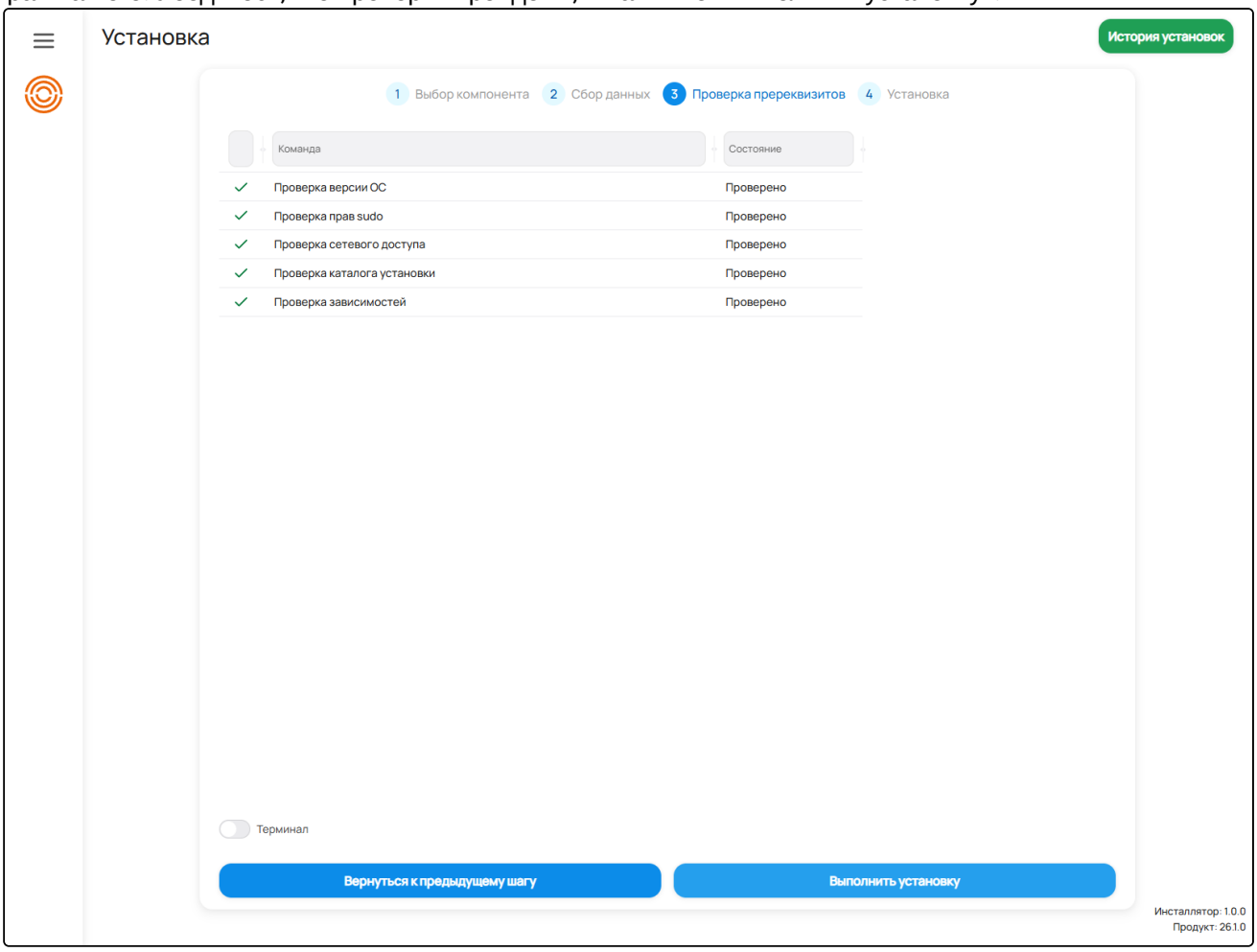
PATH установленного сервиса OCSP.



Прокрутите экран, чтобы проверить оставшиеся значения.

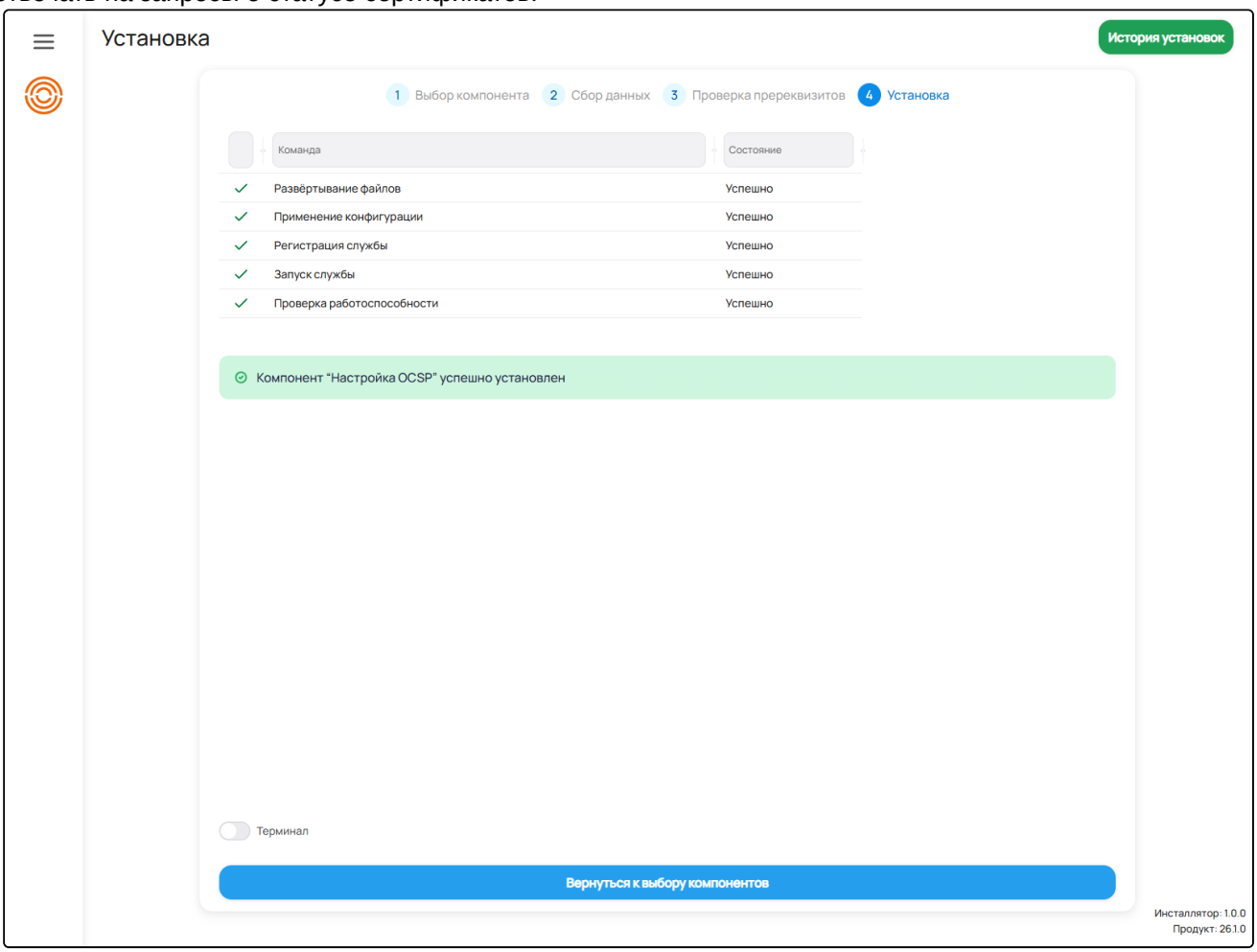


Проверка пререквизитов. Мастер проверяет наличие технологической учётной записи, каталога и прав на него. Убедитесь, что проверки пройдены, и нажмите «Выполнить установку».



Установка и результат. Мастер размещает сертификат подписи, включает автозапуск и (пере)запускает mocsp.service. На экране отображается результат установки — сервис OCSP готов

отвечать на запросы о статусе сертификатов.



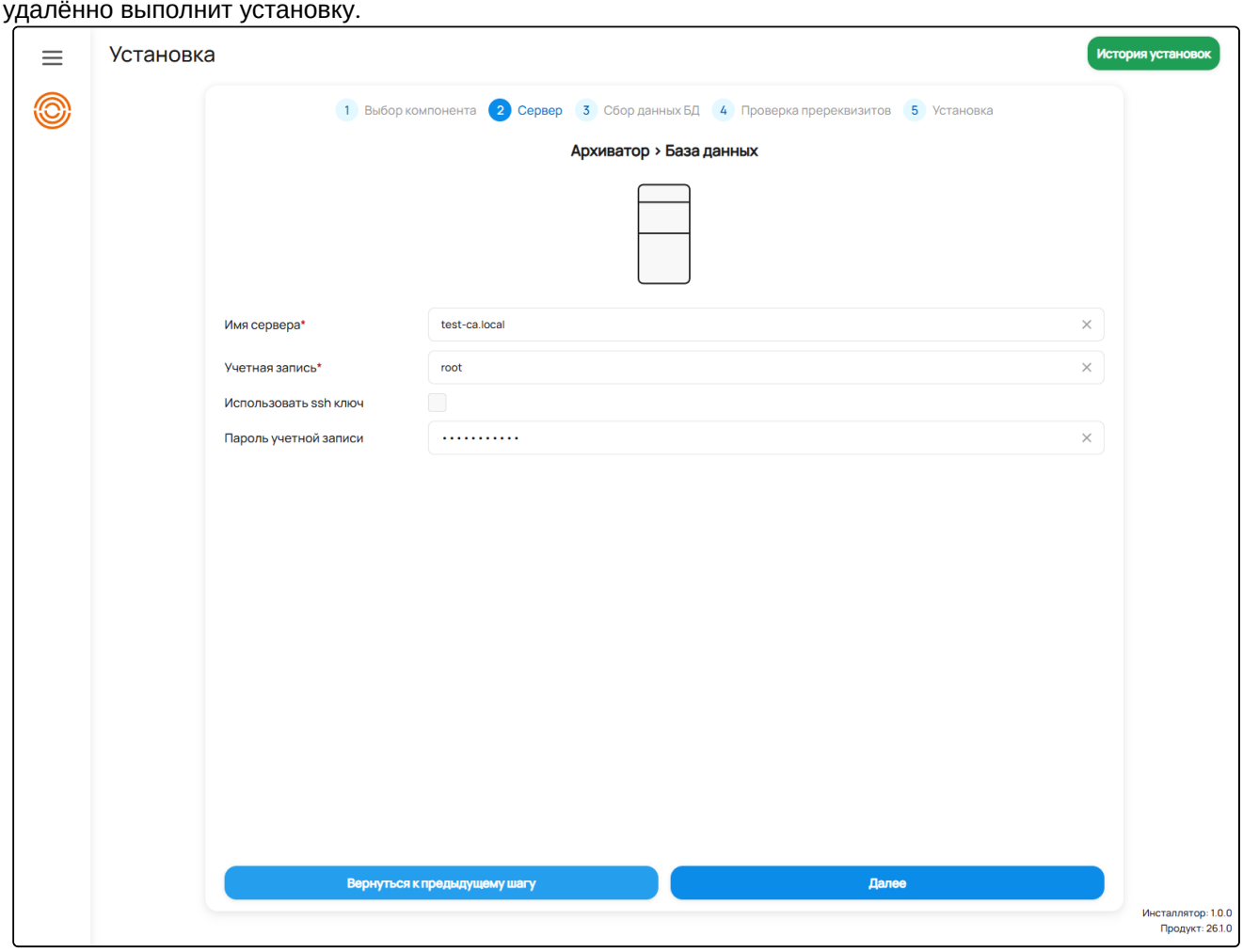
14 Архиватор

Группа «Архиватор» разворачивает служебный сервис, который по расписанию переносит устаревшие данные (в первую очередь истёкшие сертификаты) из рабочей базы данных ЦС в отдельную архивную базу, разгружая основную БД. Устанавливается двумя компонентами строго по порядку: сначала База данных (архивная БД на PostgreSQL), затем сам сервис **Архиватор** (ITC.Api.MiniCA.Archiver, пользовательский systemd-сервис, порт 9507, задание по cron @daily).

14.1 База данных

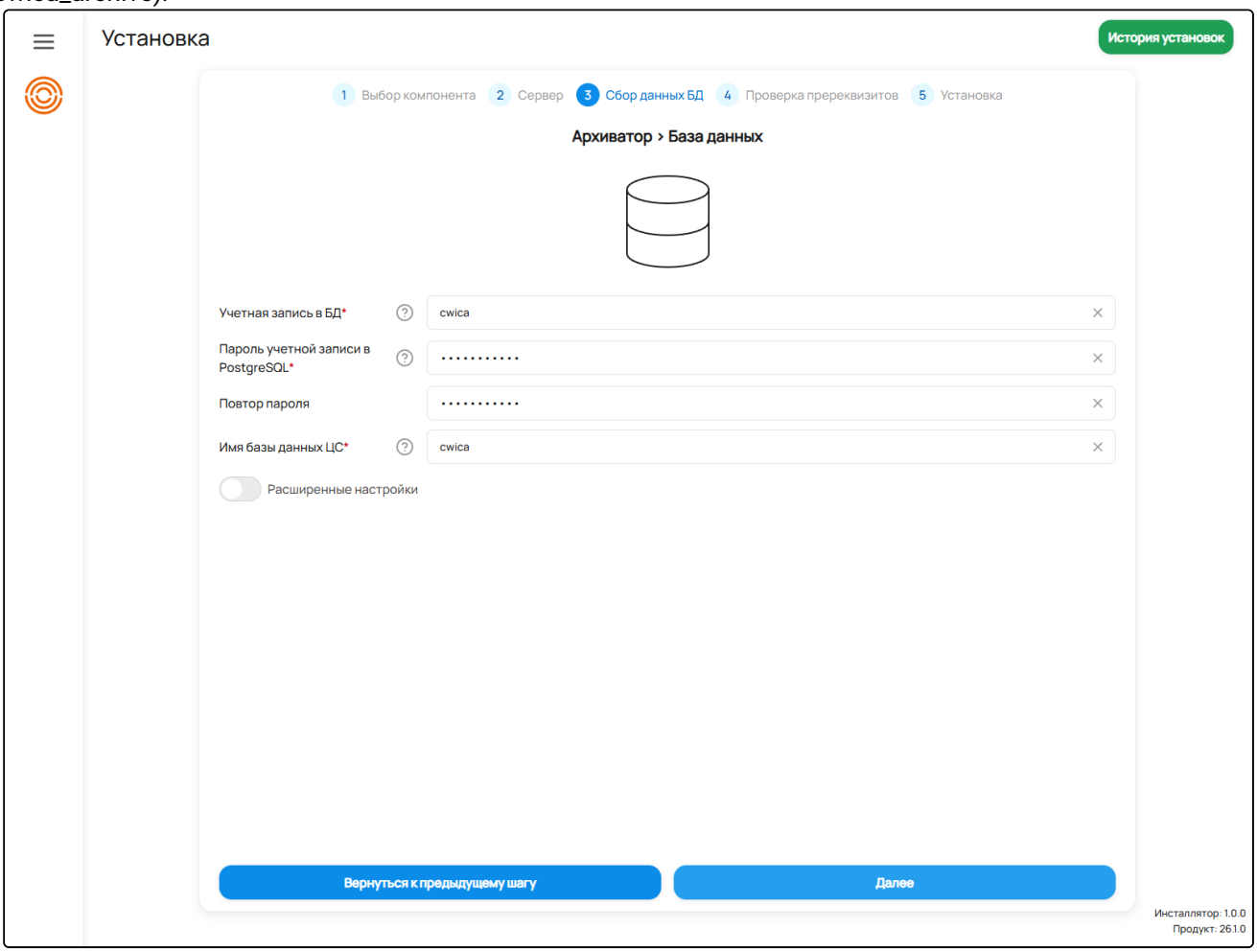
Разворачивает архивную базу данных на PostgreSQL: устанавливает при необходимости СУБД, создаёт учётную запись-владельца, саму базу и права доступа. По умолчанию имя архивной базы — cwica_archive.

Сервер. Укажите параметры SSH-подключения к серверу, где будет размещена архивная база: «Имя сервера» (адрес целевого хоста) и «Учётная запись» для входа. Для аутентификации установите флажок «Использовать ssh ключ» либо снимите его и введите пароль. По этим данным мастер удалённо выполнит установку.

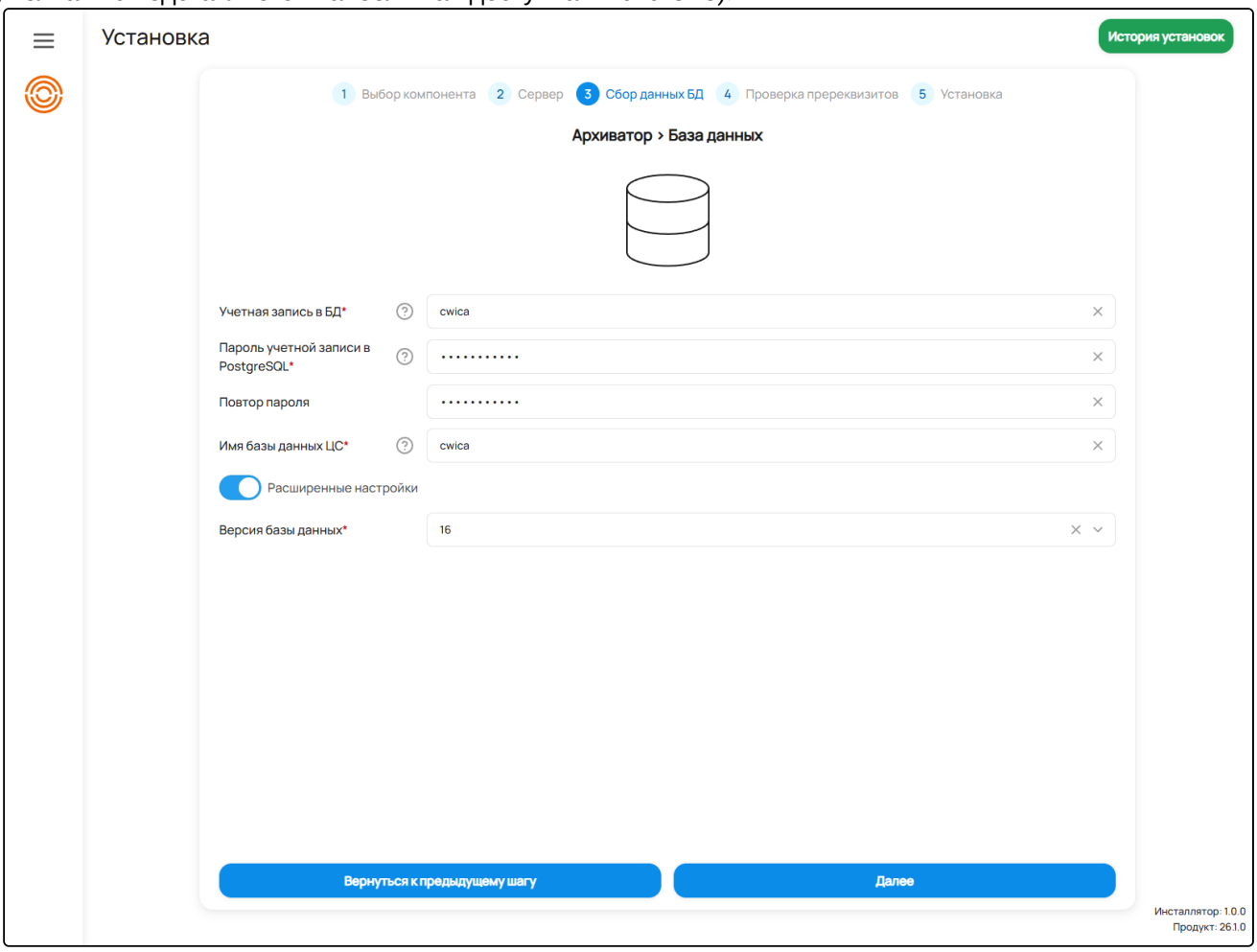


Сбор данных БД. Заполните параметры создаваемой базы: «Пользователь» (владелец БД, по умолчанию cwica), «Пароль» с подтверждением и «Имя базы данных» (для архива по умолчанию

cwica_archive).

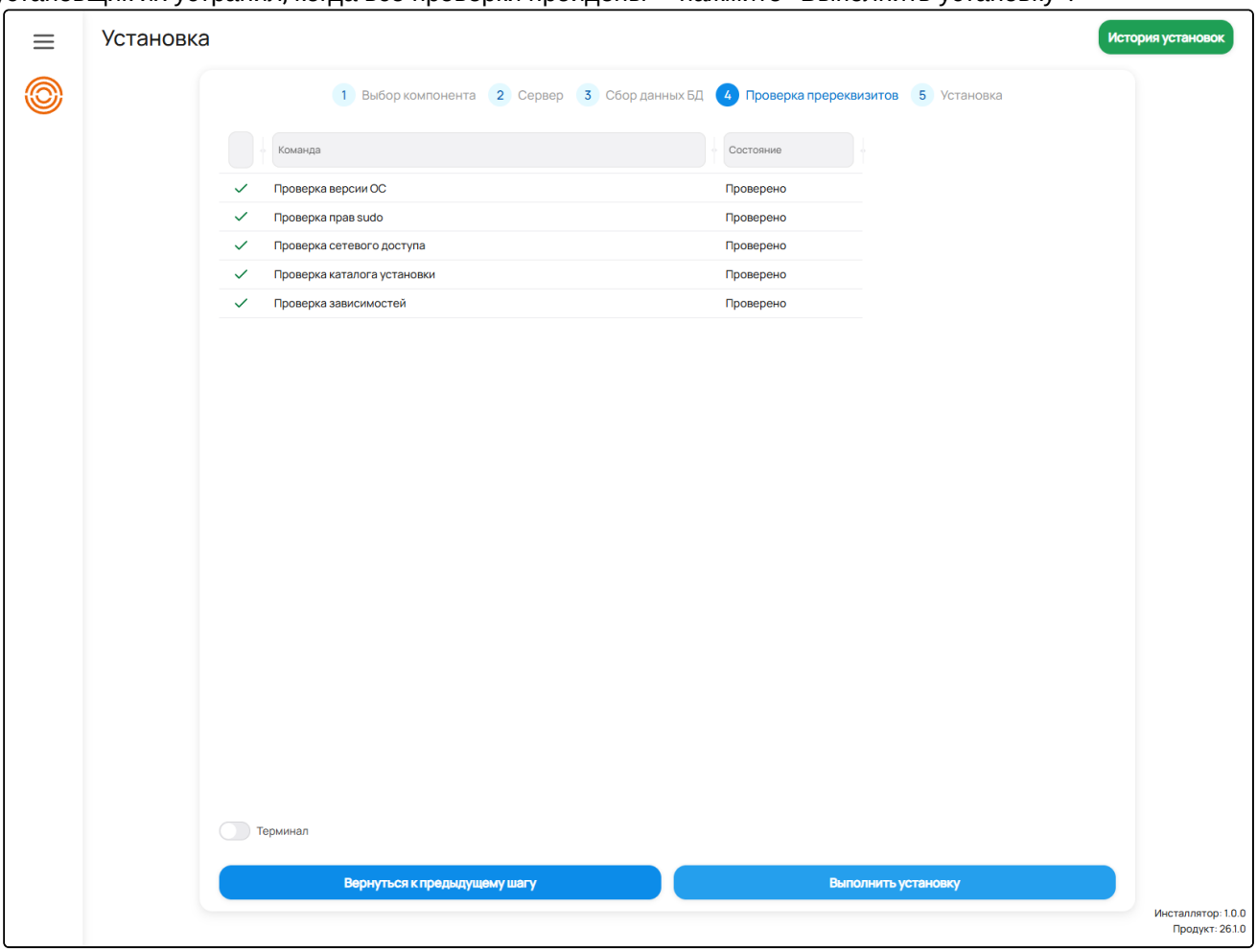


Прокрутите форму ниже и выберите «Версию PostgreSQL» из списка (поддерживаются версии 11–18; по умолчанию подставляется наибольшая доступная в системе).

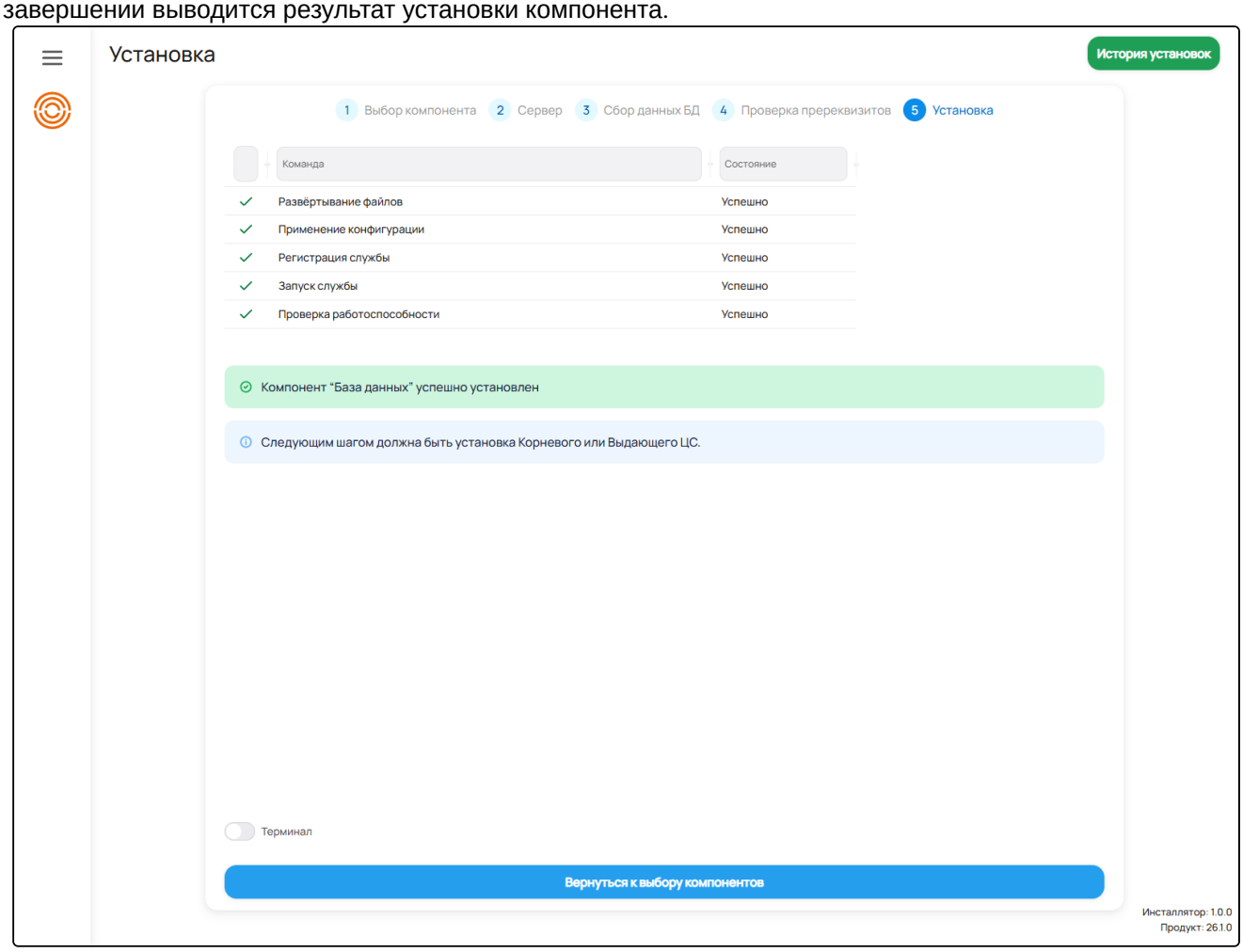


Проверка пререквизитов. Мастер выводит таблицу проверок: установлен ли PostgreSQL, существуют ли учётная запись-владелец и база данных, отсутствуют ли таблицы в целевой схеме, выданы ли права пользователю. Если есть незакрытые пункты, нажмите «Выполнить настройку пререквизитов», чтобы

установщик их устранил; когда все проверки пройдены – нажмите «Выполнить установку».



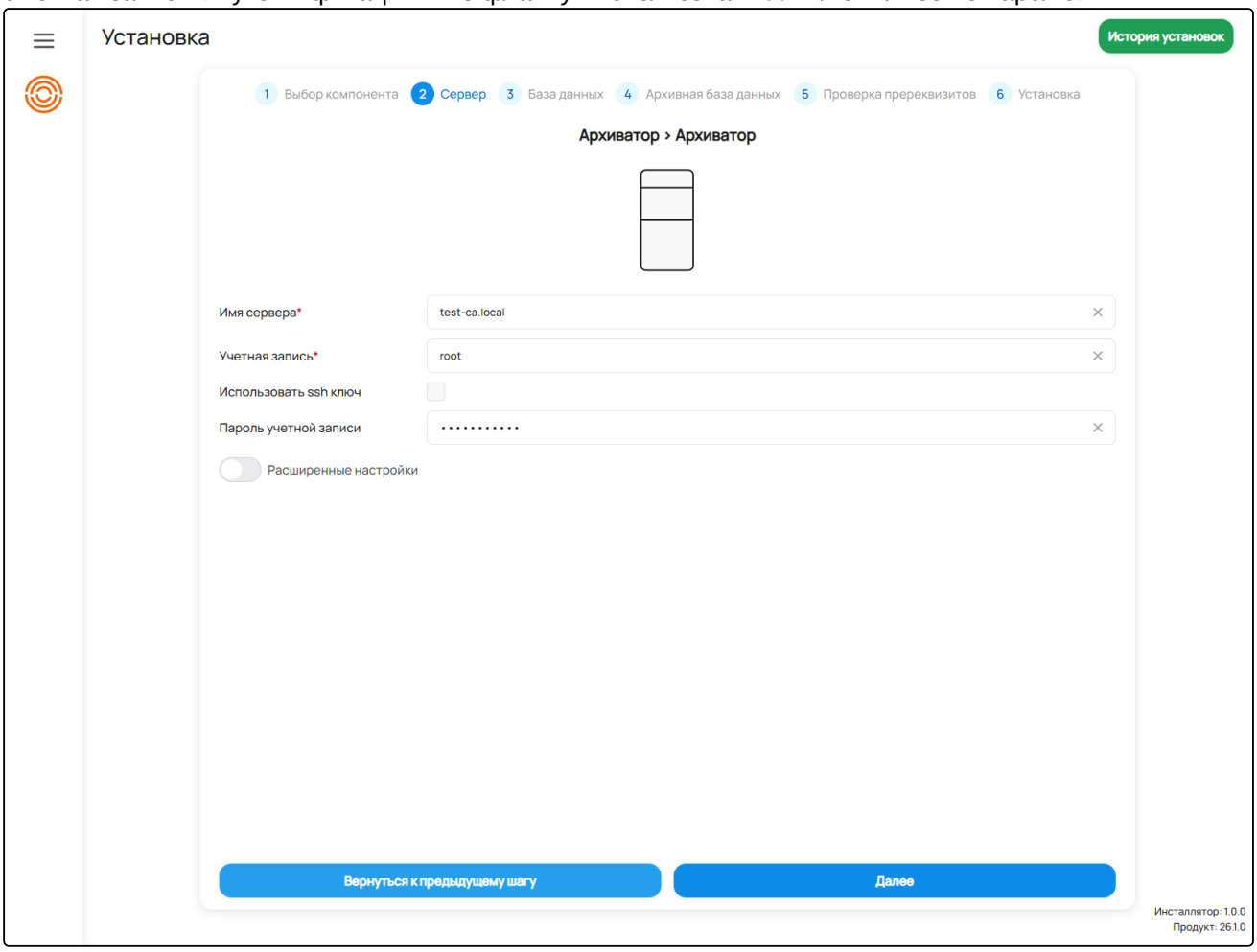
Установка и результат. Установщик применяет к базе схему и создаёт структуру таблиц. По завершении выводится результат установки компонента.



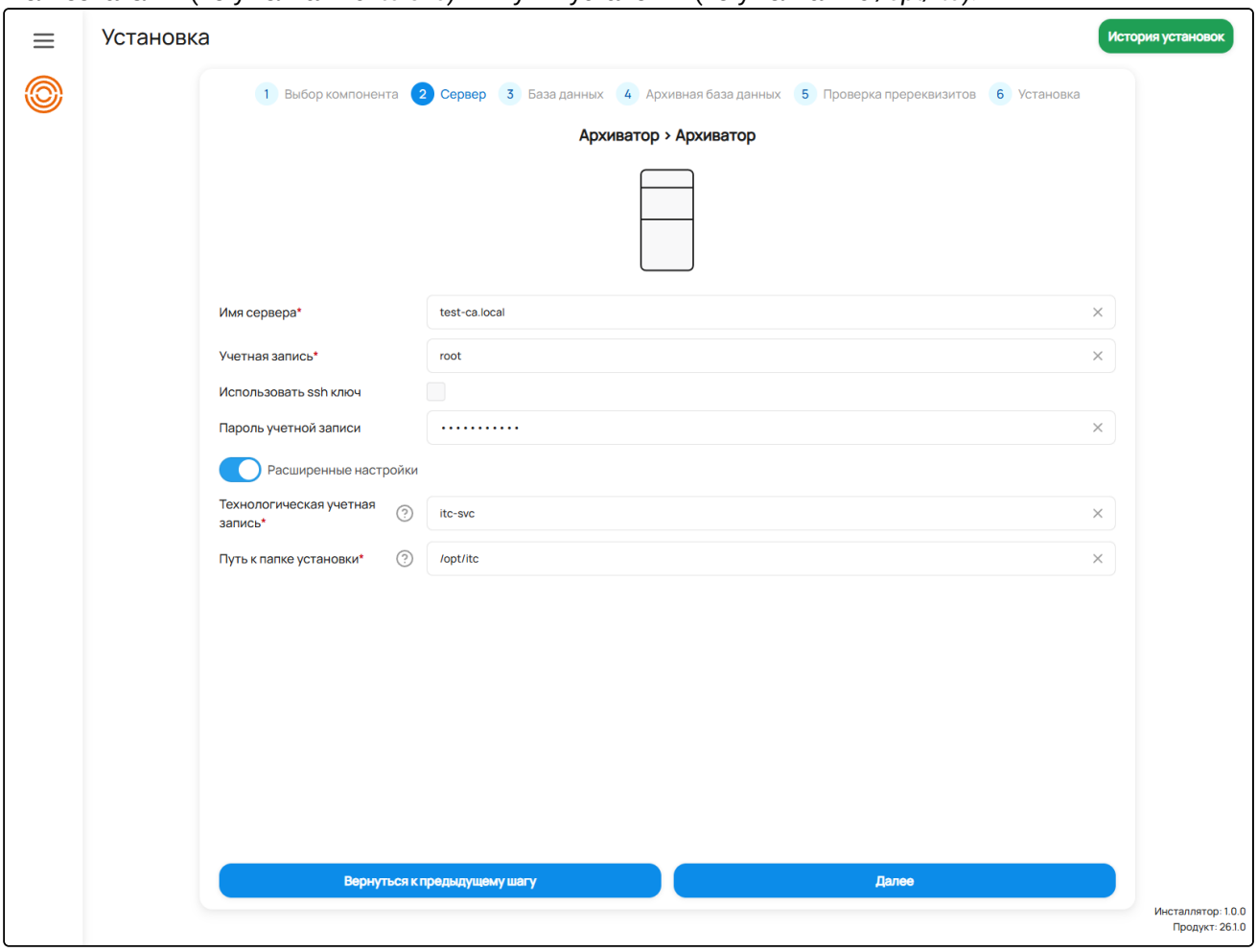
14.2 Архиватор

Устанавливает сервис архивирования, который по расписанию @daily подключается к рабочей базе ЦС (источник) и переносит устаревшие данные в архивную базу (приёмник).

Сервер. Задайте параметры SSH-подключения к серверу, на который ставится сервис: «Имя сервера» и «Учётная запись». Аутентификация – по флажку «Использовать ssh ключ» либо по паролю.

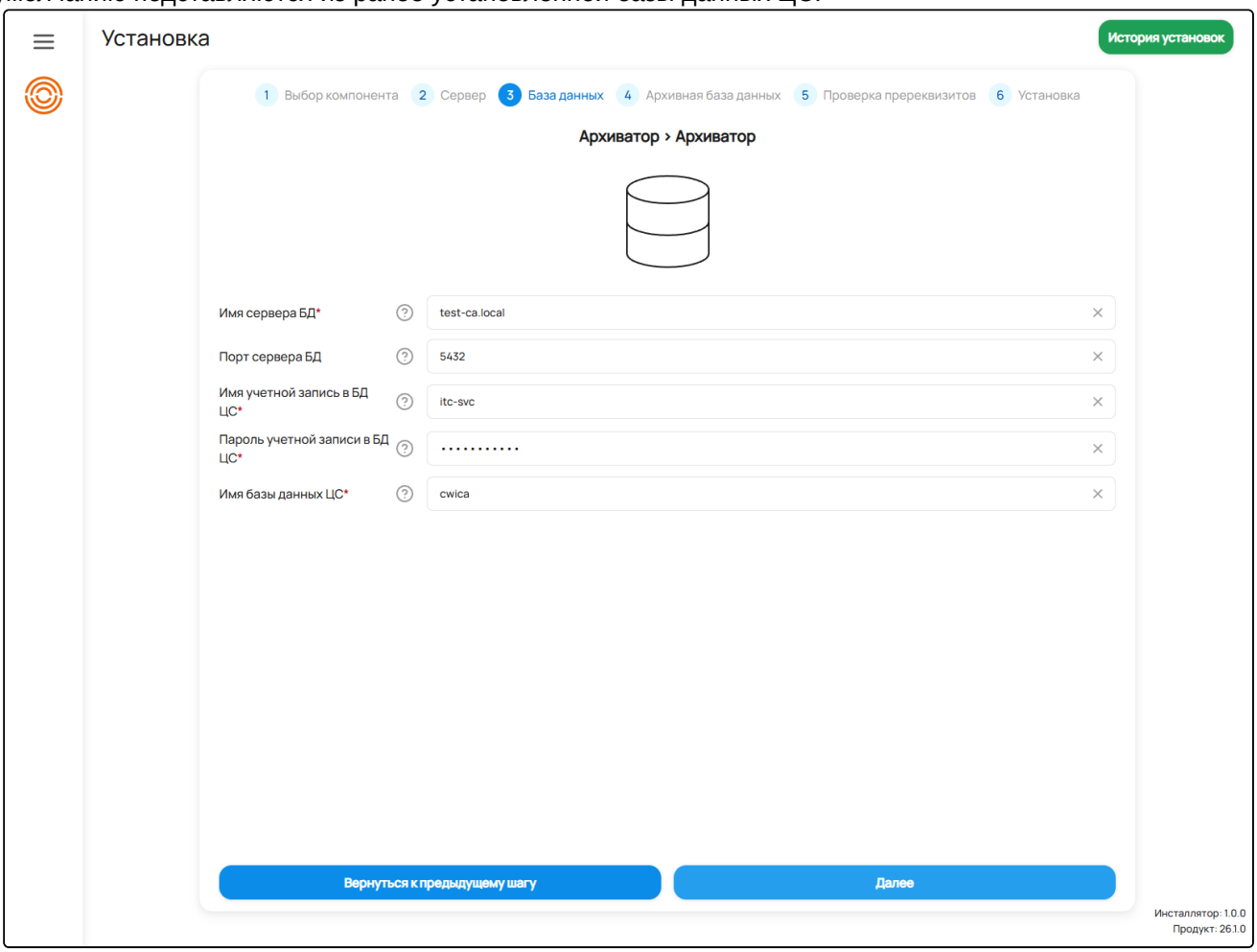


Ниже на этом же экране укажите технологическую учётную запись-владельца сервиса «Пользователь» (по умолчанию itc-svc) и «Путь» установки (по умолчанию */opt/itc*).



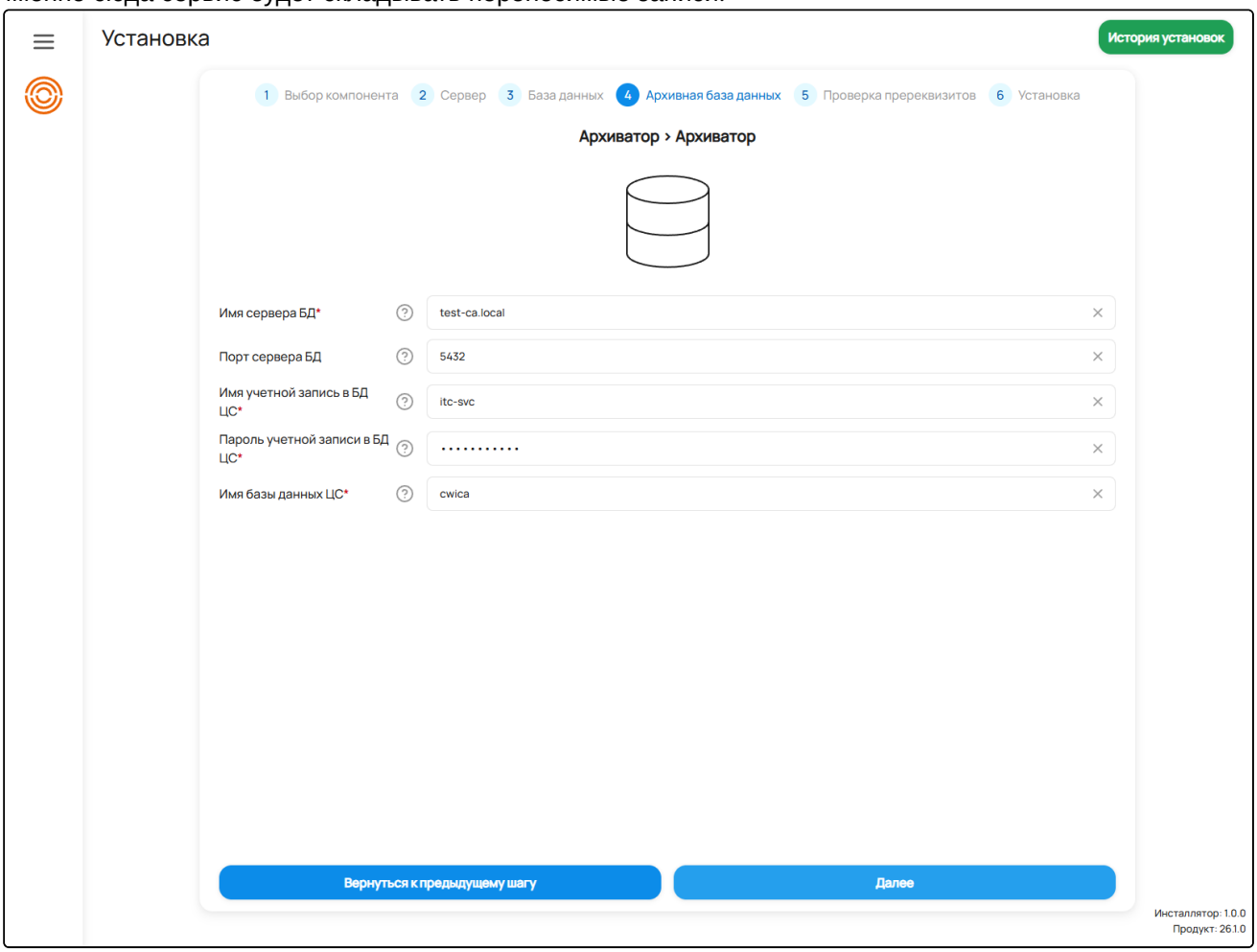
База данных (источник). Введите параметры подключения к рабочей базе ЦС, откуда будут переноситься данные: хост, порт (по умолчанию 5432), пользователь, пароль и имя базы. Значения по

умолчанию подставляются из ранее установленной базы данных ЦС.



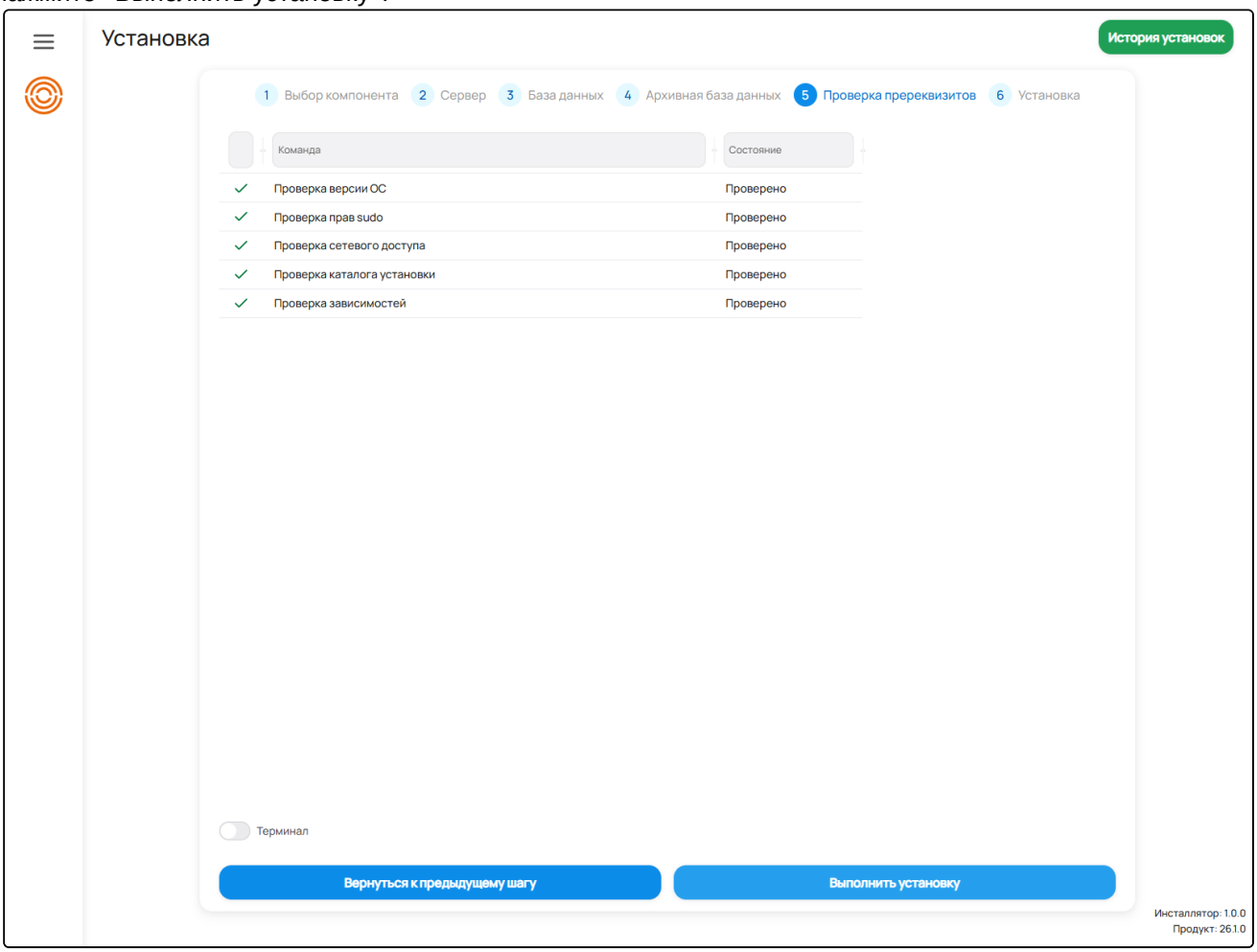
Архивная база данных (приёмник). Укажите параметры подключения к архивной базе, созданной на предыдущем компоненте: хост, порт (5432), пользователь (cwica), пароль и имя базы (cwica_archive).

Именно сюда сервис будет складывать переносимые записи.



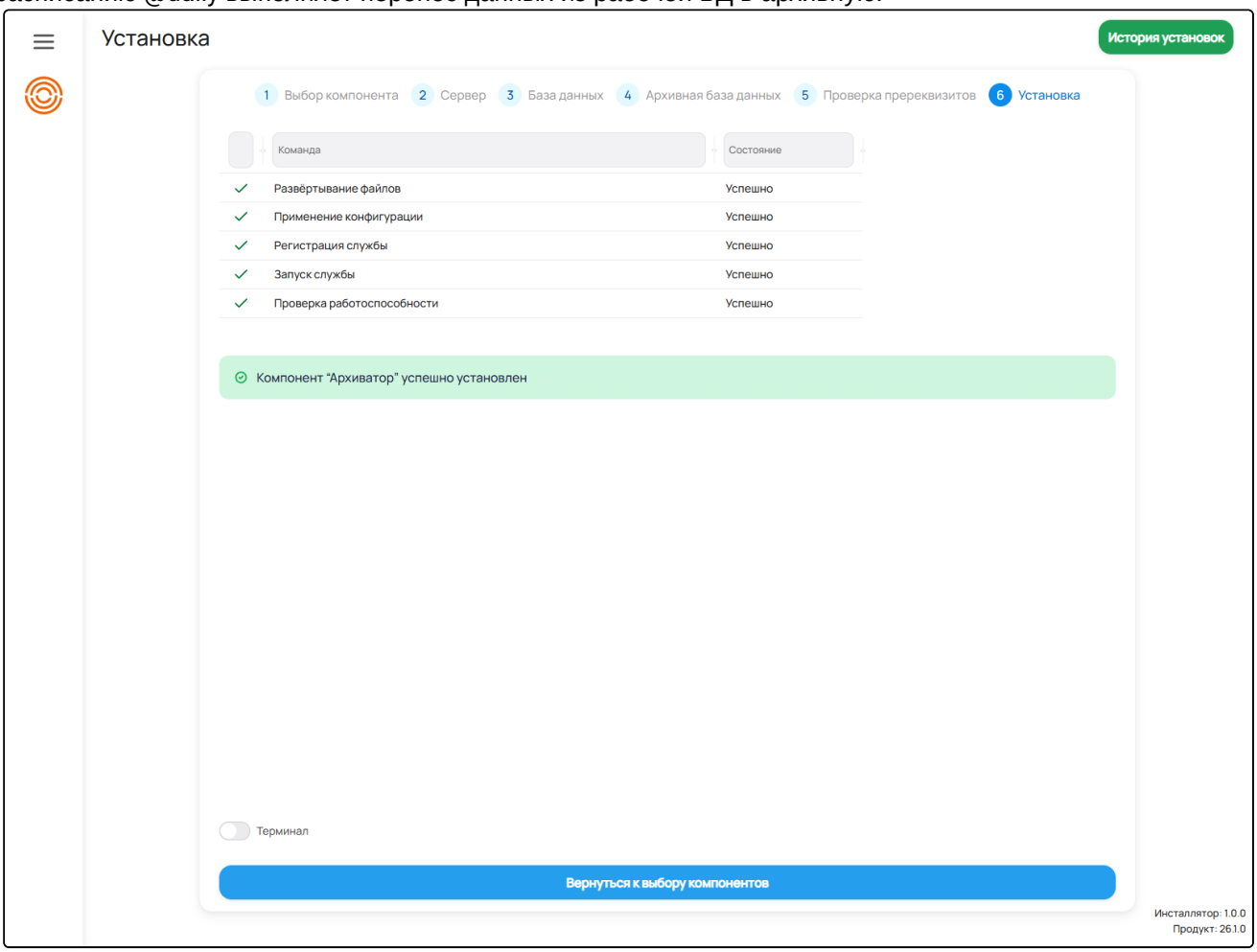
Проверка пререквизитов. Мастер проверяет наличие учётной записи, каталога установки и прав на него, включённый enable-linger, а также доступность рабочей и архивной баз данных. При наличии незакрытых пунктов нажмите «Выполнить настройку пререквизитов»; если все проверки пройдены –

нажмите «Выполнить установку».



Установка и результат. Установщик разворачивает файлы сервиса, регистрирует и запускает пользовательский systemd-юнит archiver.service и выводит результат. После этого сервис по

расписанию @daily выполняет перенос данных из рабочей БД в архивную.



15 SCEP

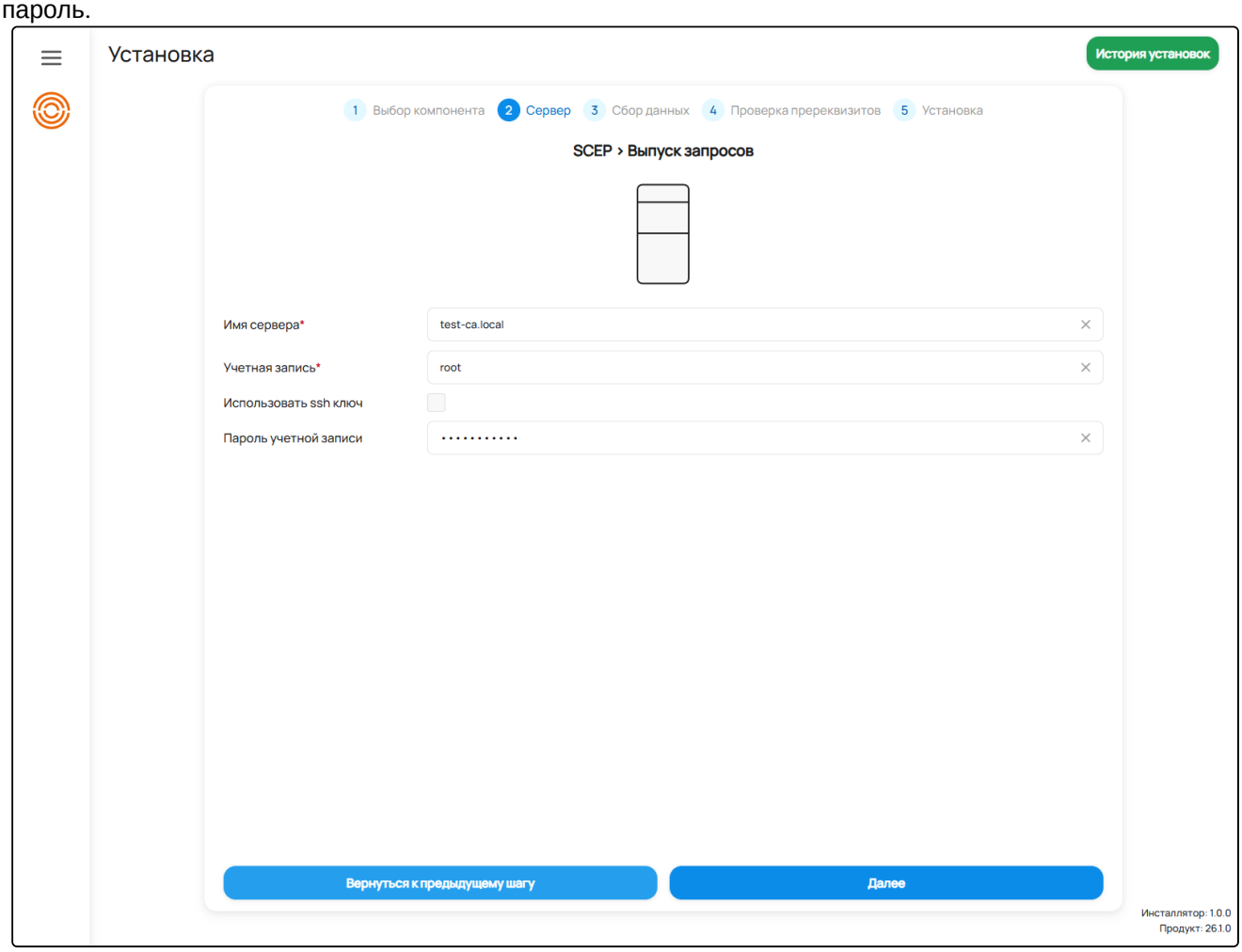
Группа разворачивает адаптер SCEP — сервис автоматического выпуска и обновления сертификатов для сетевых устройств по протоколу SCEP. Сервис публикуется через Nginx по HTTPS (внешний адрес устройств — https://<fqdn>/api/scep), аутентификация запросов выполняется через OpenID, состояние хранится в локальной базе SQLite. Компоненты устанавливаются в порядке: выпуск запросов на сертификаты (CSR), выпуск самих сертификатов на действующем ЦС, выпуск JWT для доступа к ЦС, установка сервиса SCEP и его финальная настройка.

Все компоненты работают от технологической учётной записи itc-svc, каталог установки по умолчанию — */opt/itc*.

15.1 Выпуск запросов

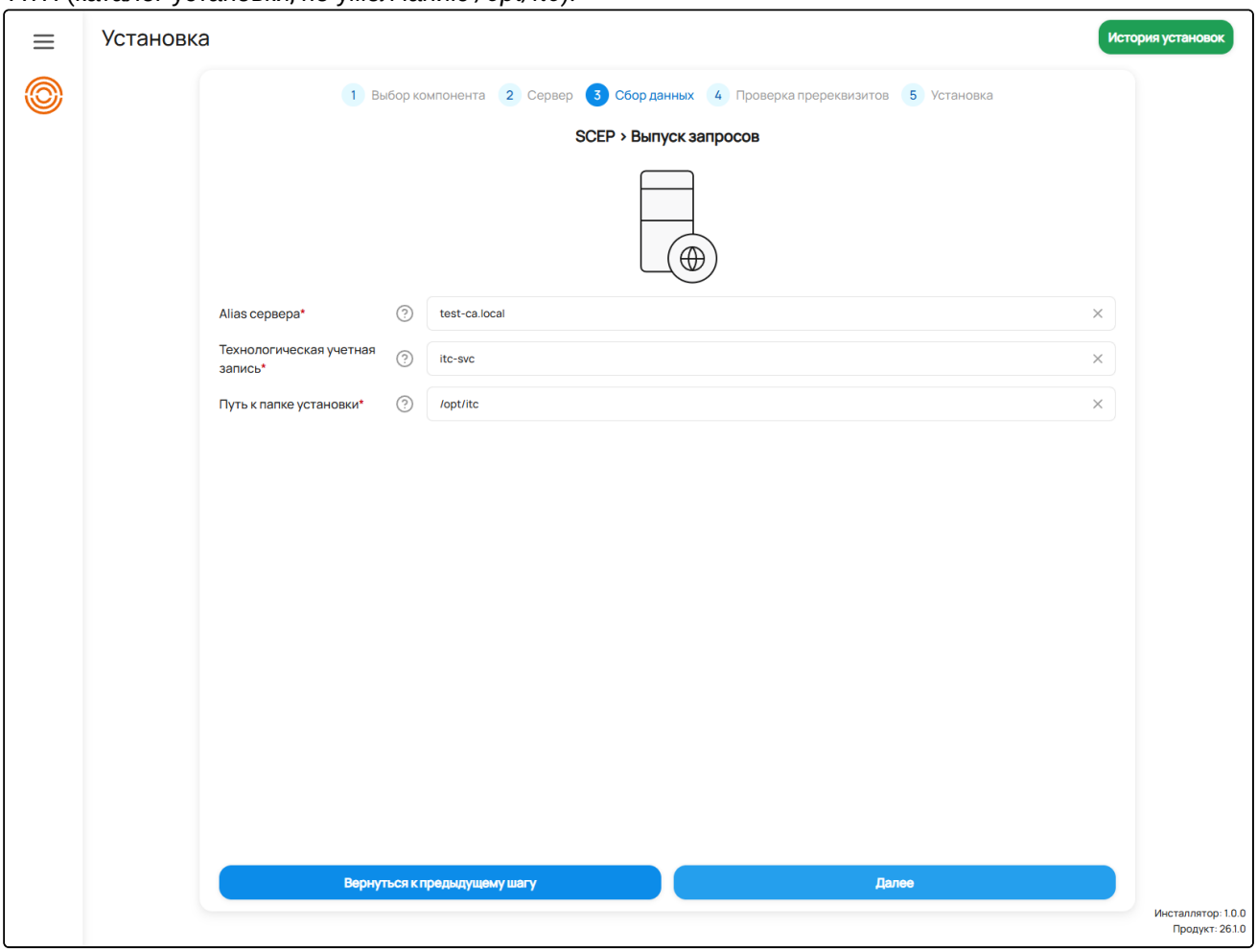
Компонент готовит сервер SCEP: генерирует два ключа и два запроса на сертификат (CSR) — для TLS Nginx и для подписи SCEP-ответов.

Сервер. Укажите параметры подключения к серверу SCEP по SSH: имя (адрес) сервера и учётную запись. Отметьте флажок «Использовать ssh ключ» для входа по ключу либо снимите его и введите пароль.



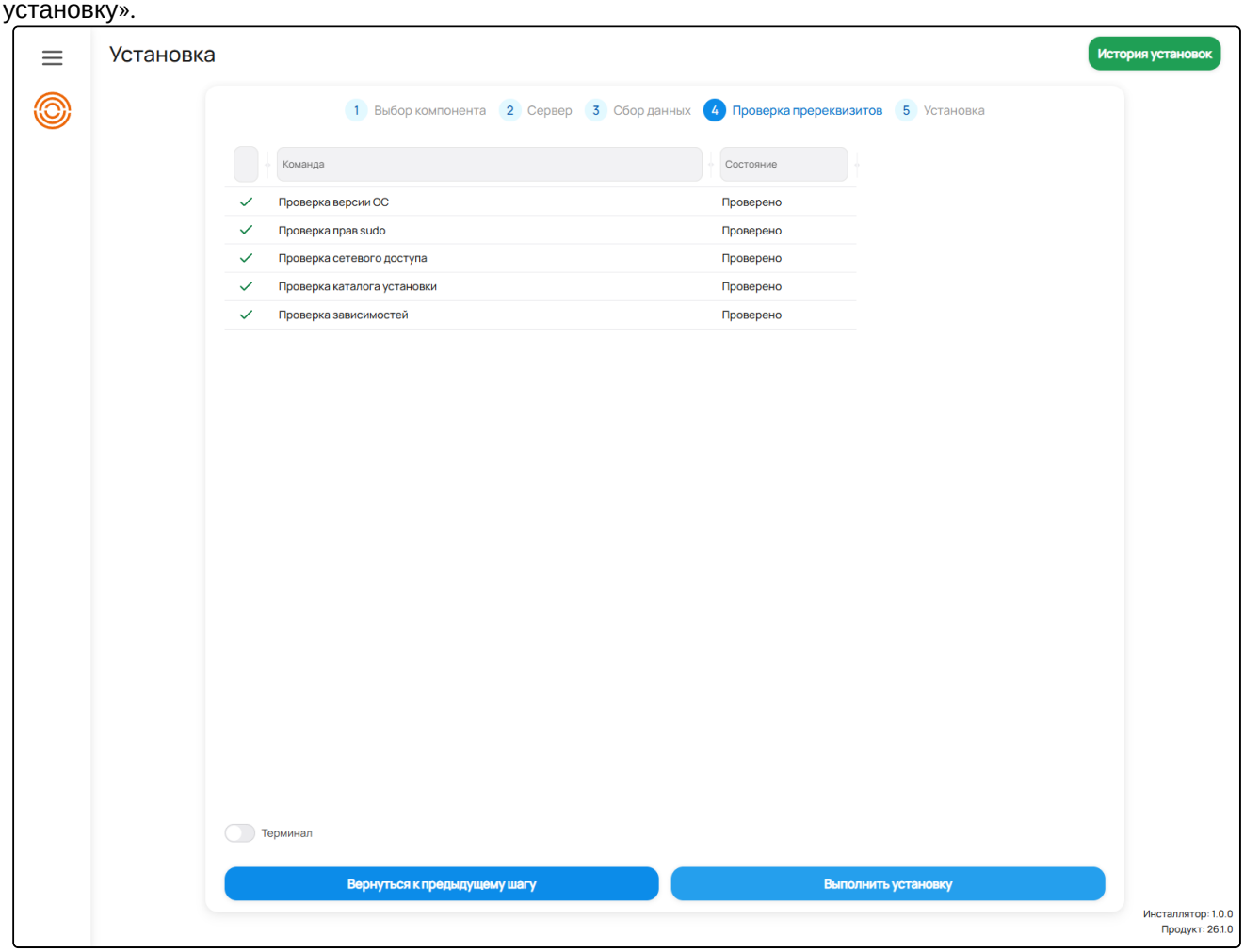
Сбор данных. Заполните переменные компонента: HOSTNAME (имя, на которое выпускаются сертификаты; по умолчанию имя хоста), USER_NAME (учётная запись-владелец, по умолчанию itc-svc) и

PATH (каталог установки, по умолчанию */opt/itc*).

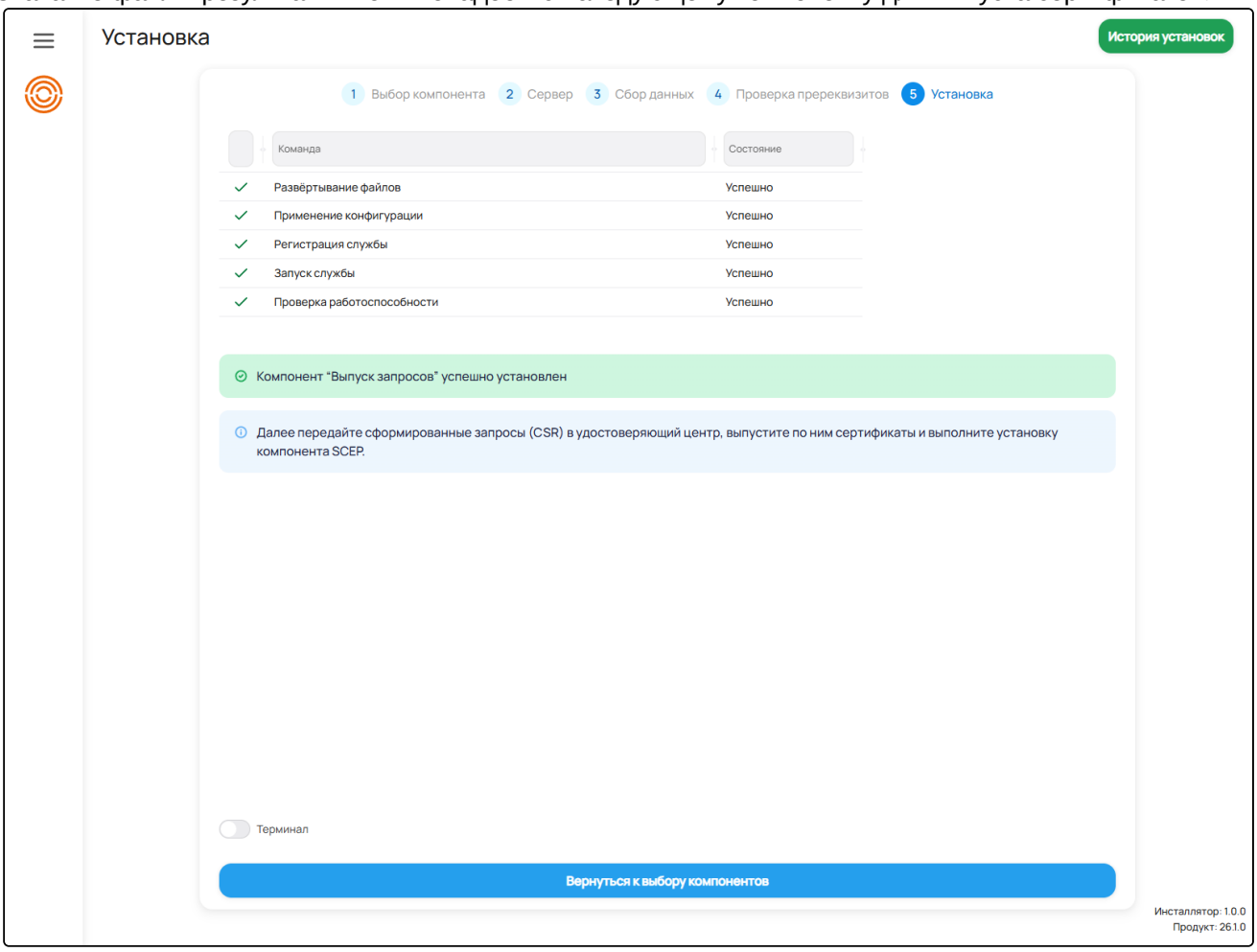


Проверка пререквизитов. Мастер проверяет наличие учётной записи, каталога и прав на него. Если есть незакрытые проверки — нажмите «Выполнить настройку пререквизитов», после чего — «Выполнить

установку».


Установка
История установок
1 Выбор компонента
2 Сервер
3 Сбор данных
4 Проверка пререквизитов
5 Установка
Команда
Состояние
Проверка версии ОС
Проверено
Проверка прав sudo
Проверено
Проверка сетевого доступа
Проверено
Проверка каталога установки
Проверено
Проверка зависимостей
Проверено
Терминал
Вернуться к предыдущему шагу
Выполнить установку
Инсталлятор: 1.0.0
Продукт: 26.1.0

Установка и результат. Формируются два CSR (nginx-tls.csr для TLS и scep.csr для подписи SCEP). Скачайте файлы-результаты — они понадобятся следующему компоненту для выпуска сертификатов.

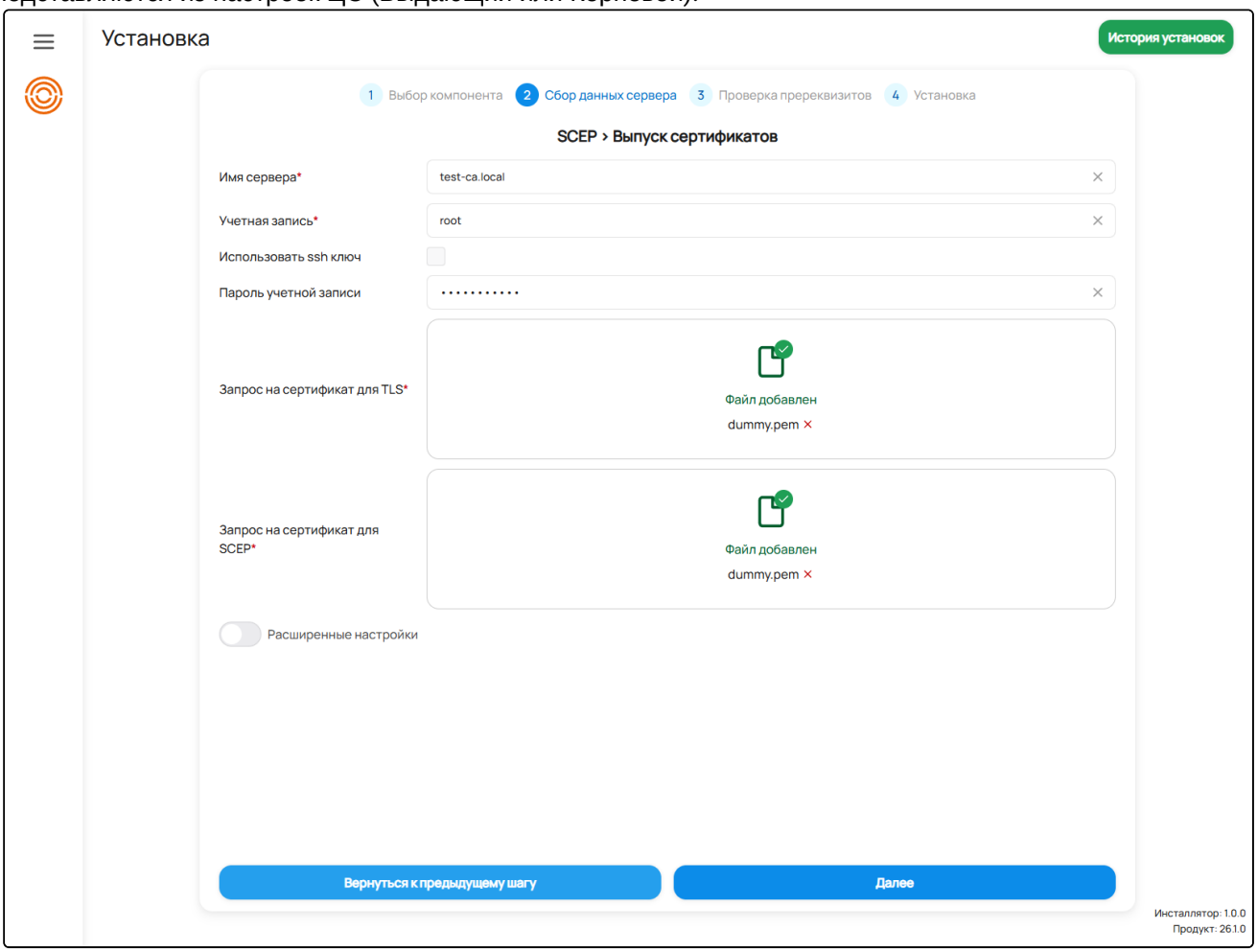


15.2 Выпуск сертификатов

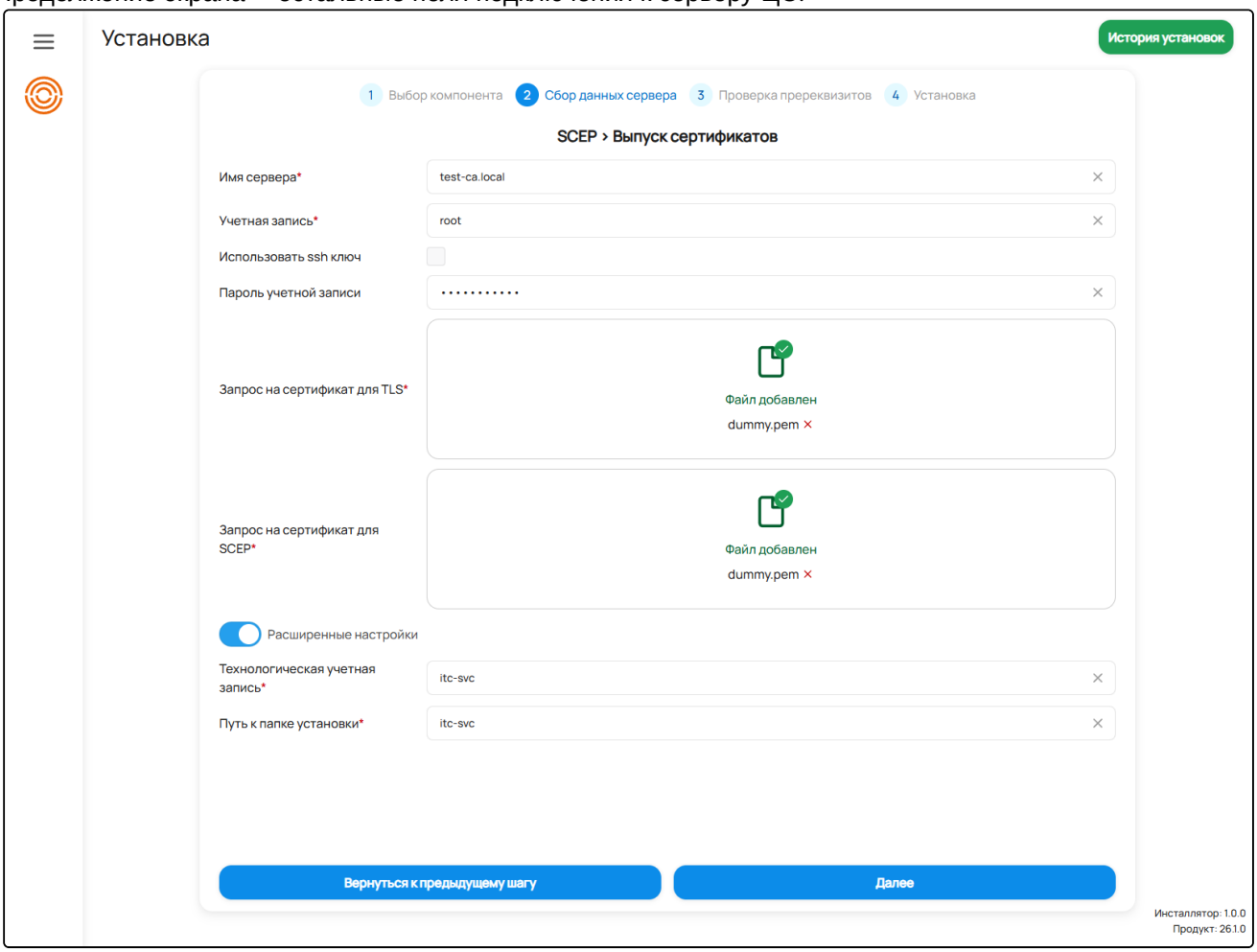
Компонент подключается к действующему ЦС и через mclient подписывает два сертификата по запросам из предыдущего шага — TLS и SCEP.

Сбор данных сервера ЦС. Укажите данные сервера ЦС и подставьте оба запроса: CSR_TLS (из результата nginx-tls.csr) и CSR_SCEP (из результата scep.csr). Учётная запись и каталог по умолчанию

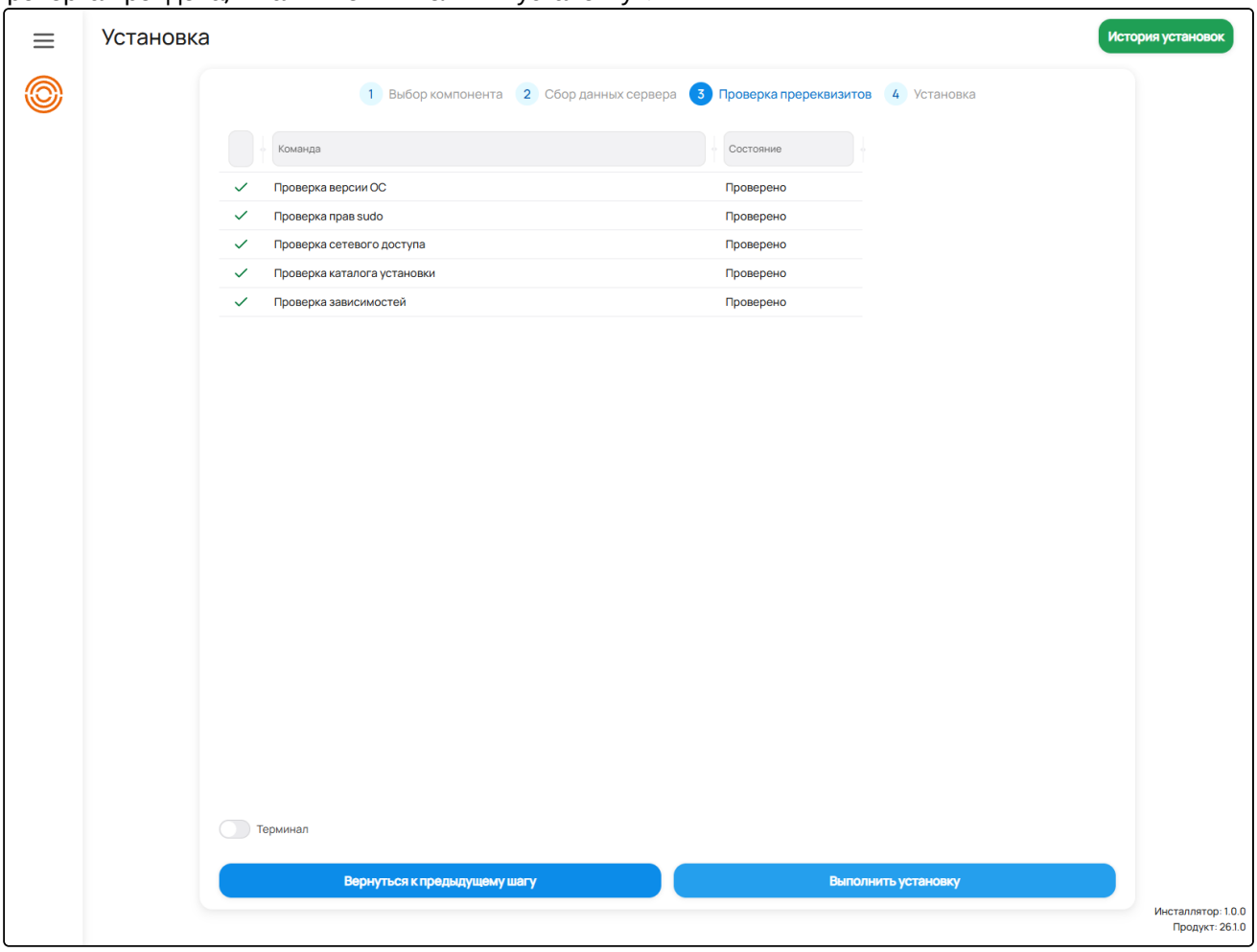
подставляются из настроек ЦС (Выдающий или Корневой).



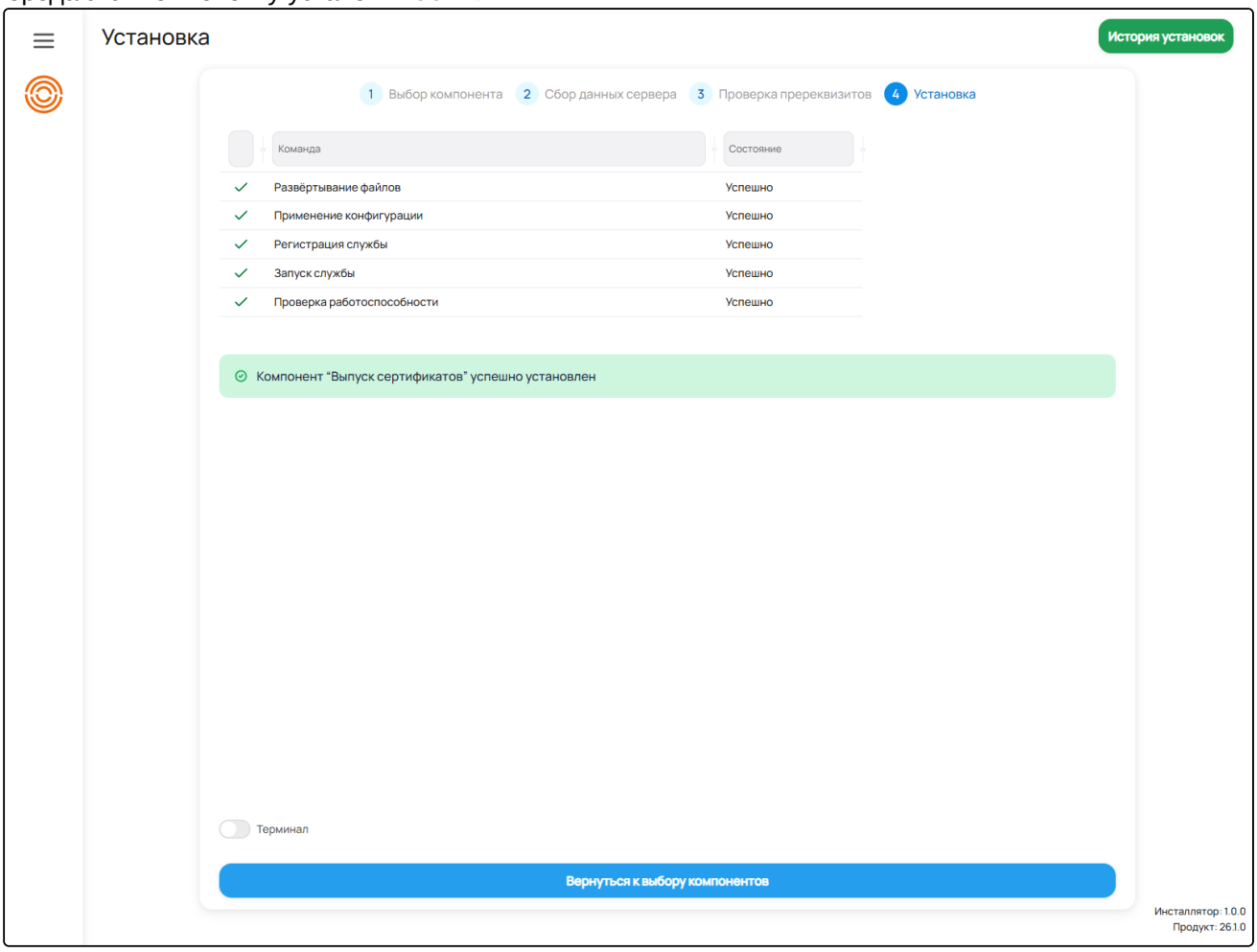
Продолжение экрана – остальные поля подключения к серверу ЦС.



Проверка пререквизитов. Проверяется, что ЦС установлен и доступен (mclient ping). Убедитесь, что проверка пройдена, и нажмите «Выполнить установку».



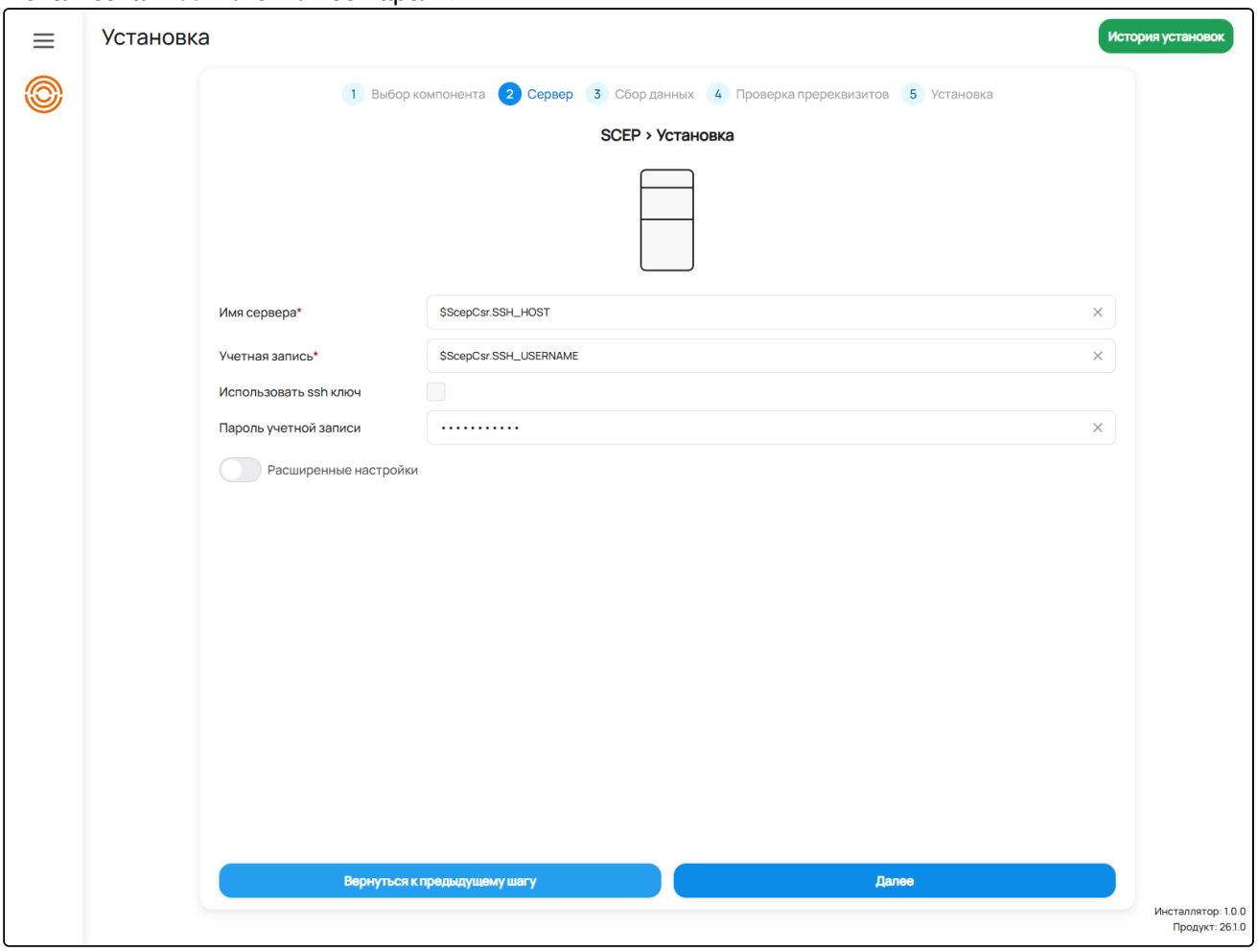
Установка и результат. ЦС выпускает сертификаты nginx-tls.crt и scep.crt. Скачайте оба файла — они передаются компоненту установки SCEP.



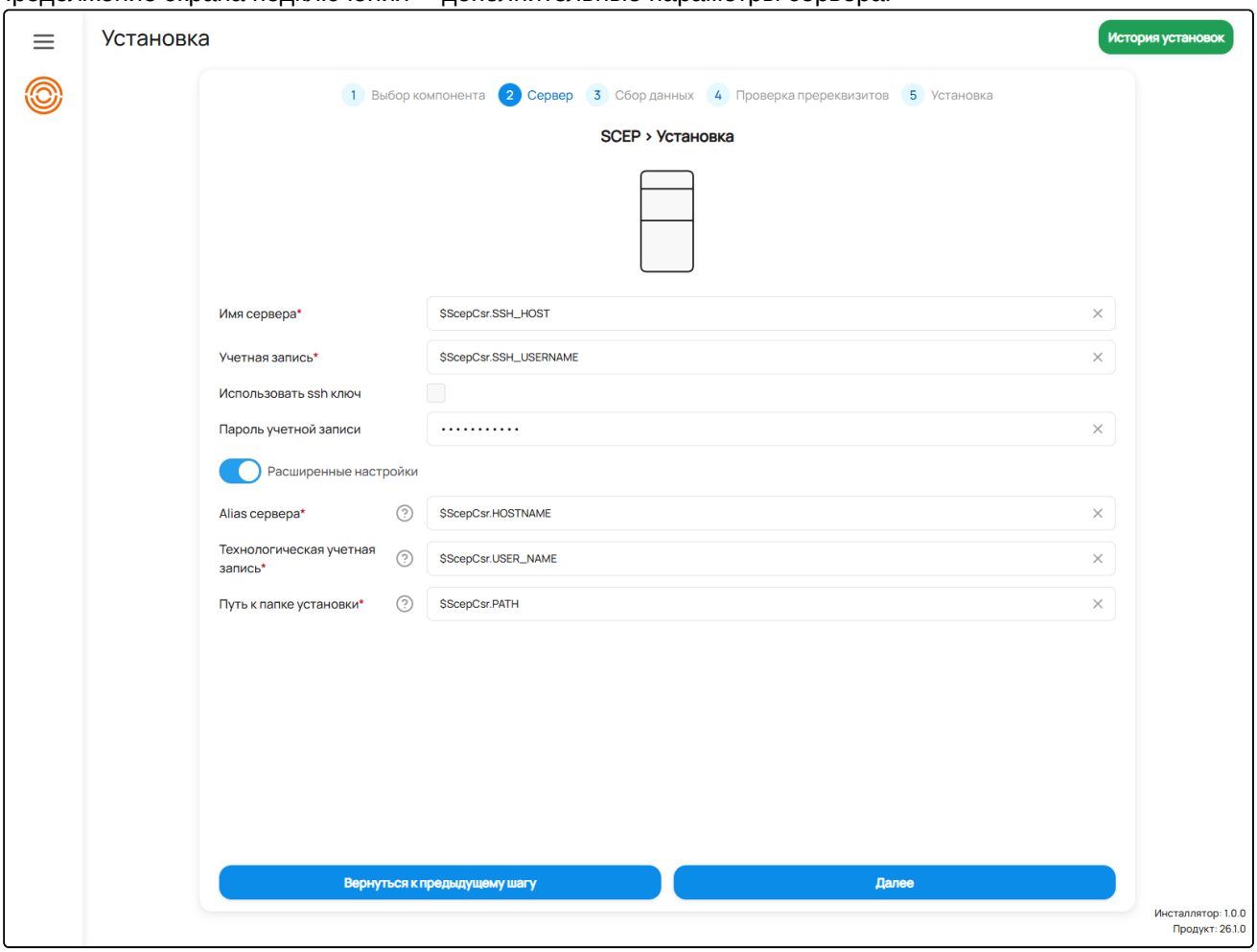
15.3 Установка

Компонент устанавливает сам сервис SCEP-адаптера как пользовательский systemd-сервис за Nginx.

Сервер. Укажите параметры SSH-подключения к серверу SCEP: имя сервера, учётную запись и флажок «Использовать ssh ключ» либо пароль.

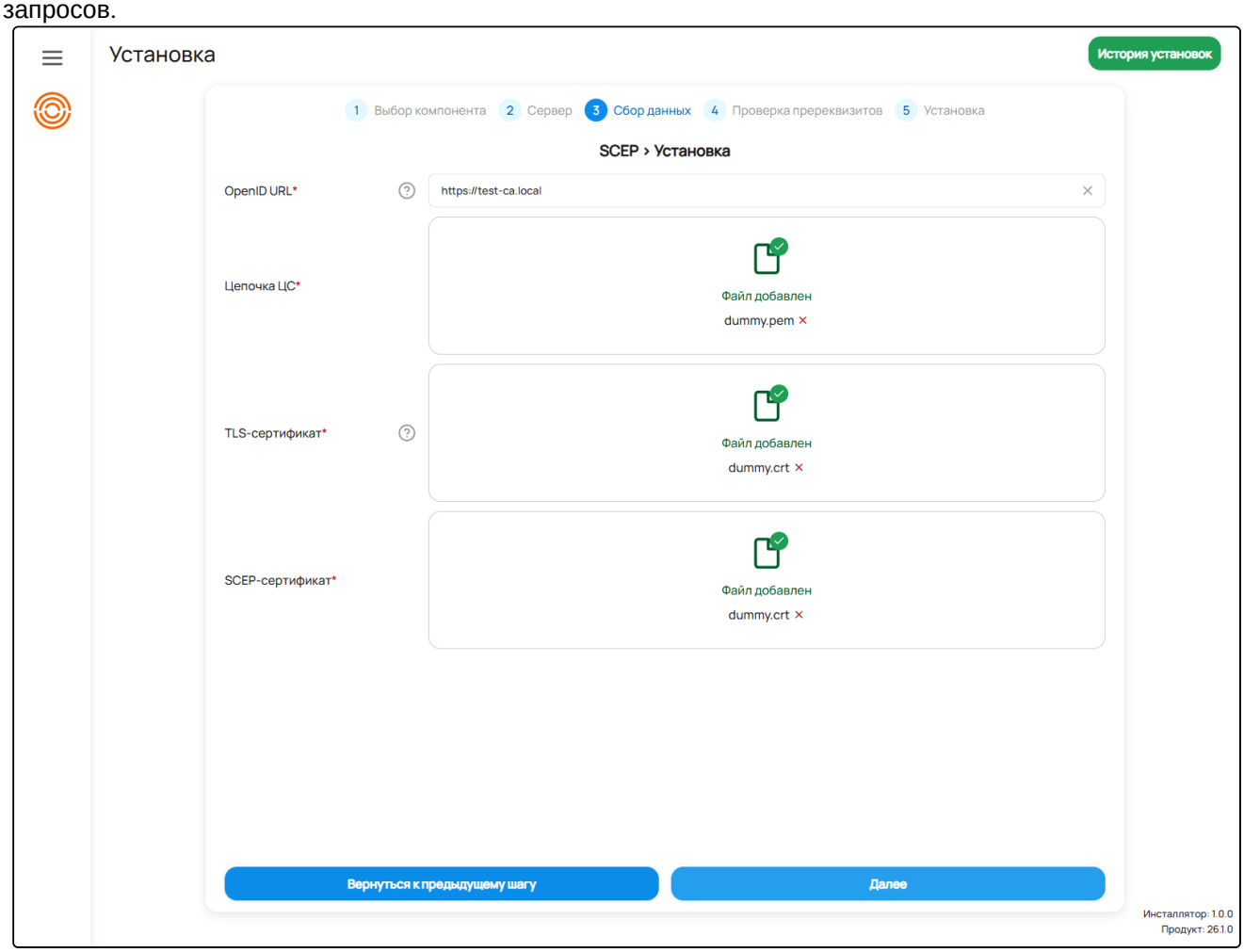


Продолжение экрана подключения – дополнительные параметры сервера.



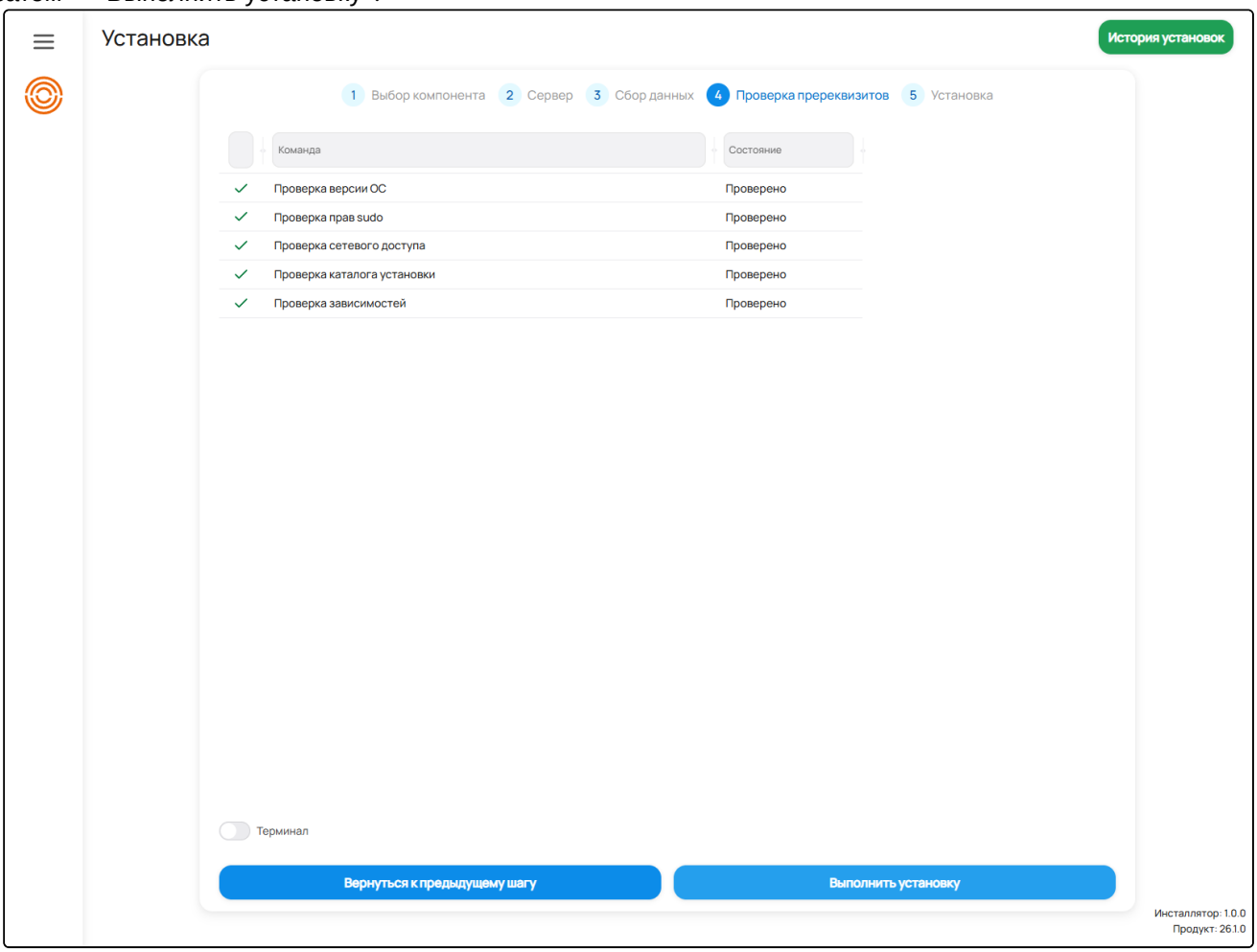
Сбор данных. Заполните переменные сервиса: AUTH_URL (адрес OpenID для аутентификации), CERTIFICATE_NGINX (сертификат nginx-tls.crt), CERTIFICATE_SCEP (сертификат scep.crt) и CHAIN (цепочка доверия ЦС scep-chain.pem). Учётная запись и каталог подставляются из настроек выпуска

запросов.

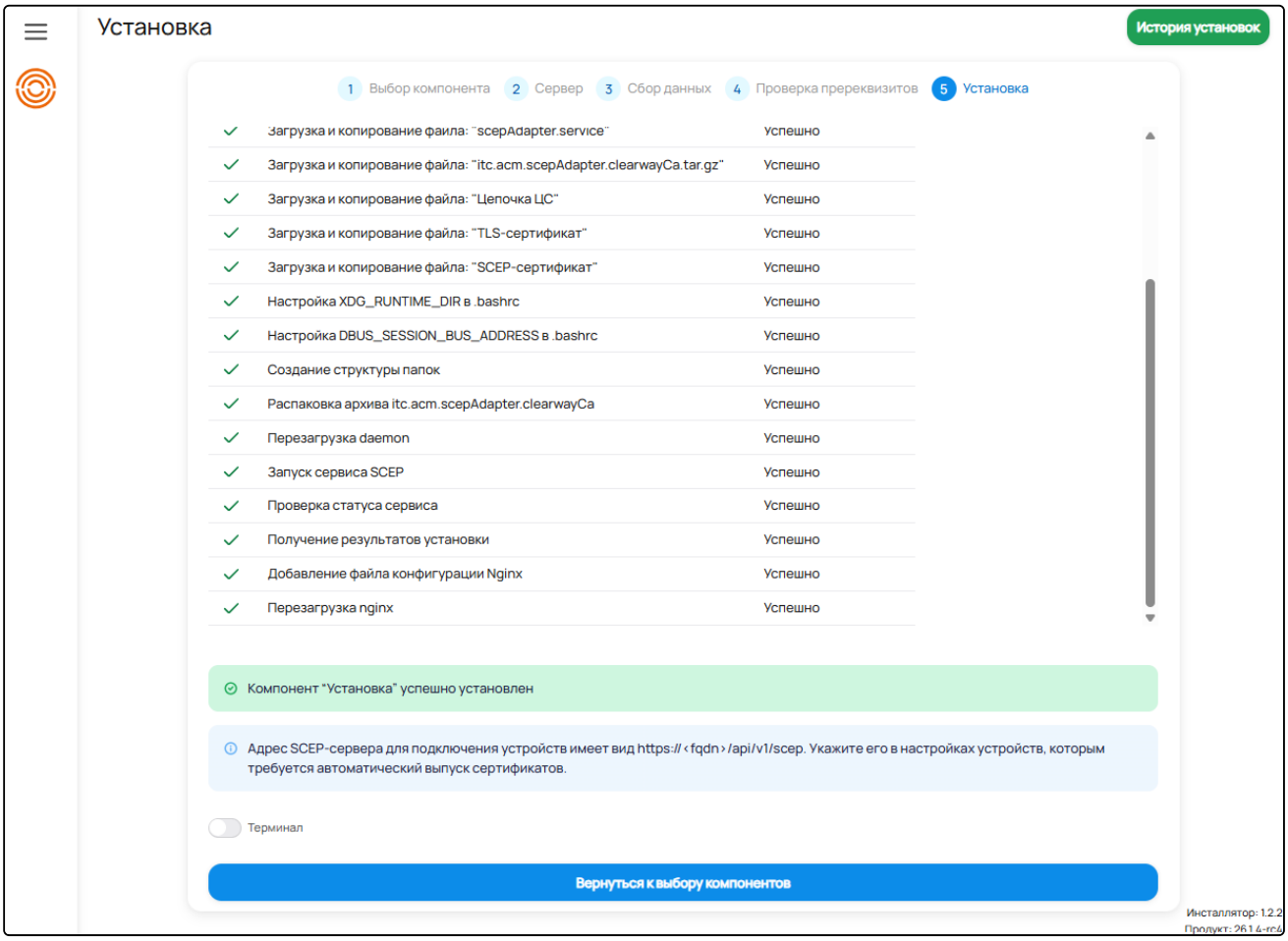


Проверка пререквизитов. Проверяются учётная запись, каталог и права, наличие и активность Nginx, включение enable-linger. При незакрытых проверках нажмите «Выполнить настройку пререквизитов»,

затем — «Выполнить установку».



Установка и результат. Разворачивается приложение адаптера, база SQLite (*/opt/itc/itc/sqlite/scep.db*), systemd-сервис scepAdapter.service и конфигурация Nginx (расположение: */api/scep*). Дождитесь успешного завершения.

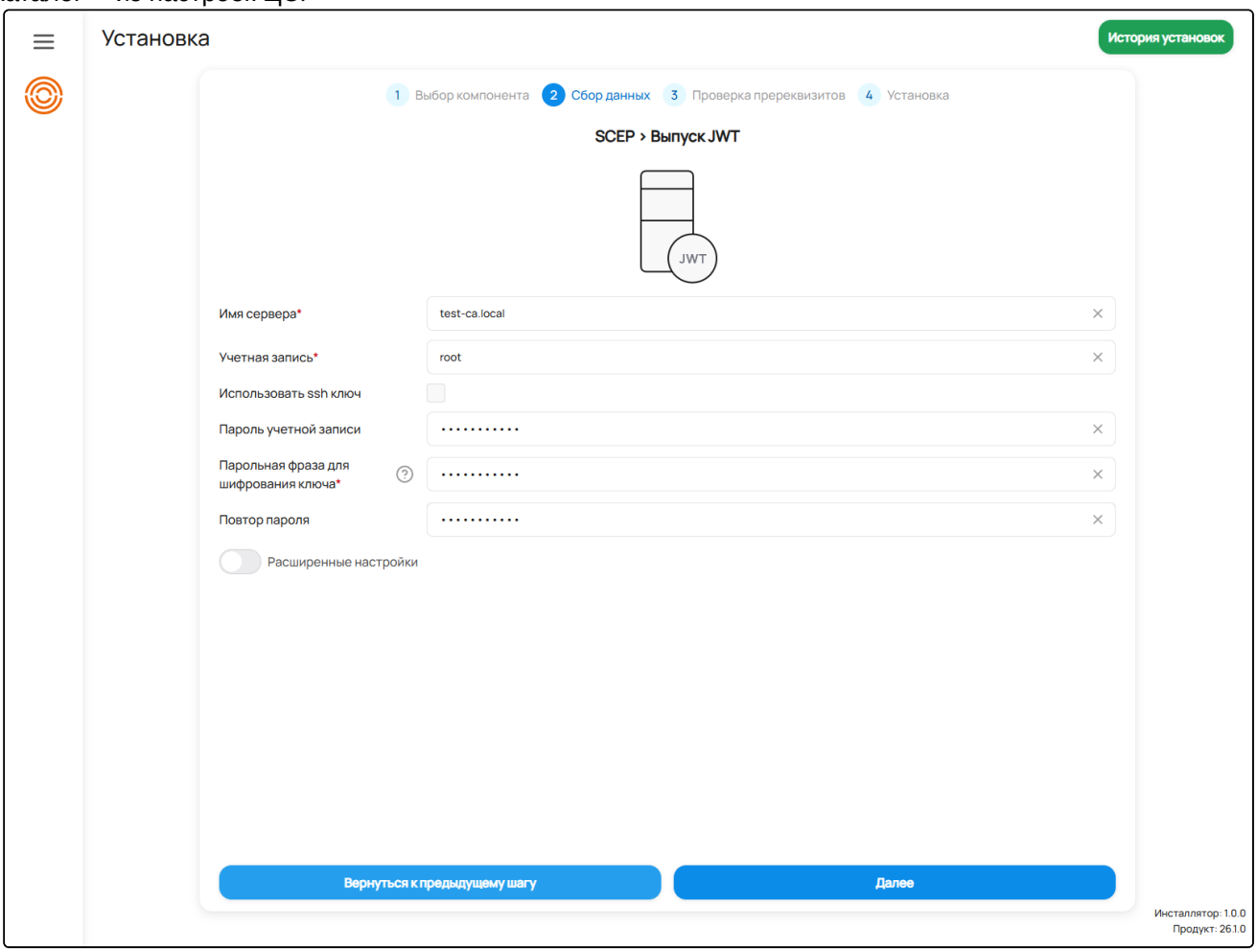


15.4 Выпуск JWT

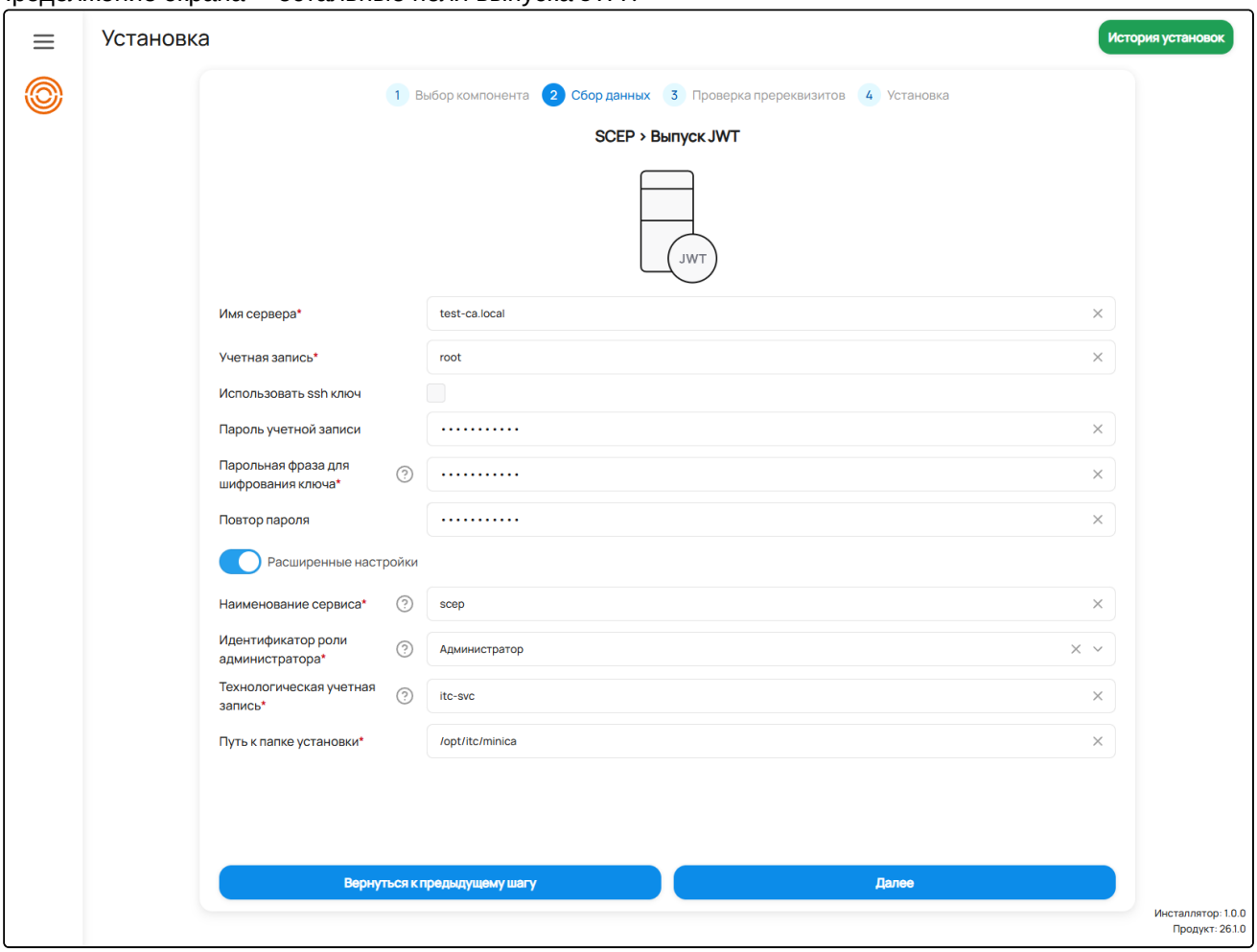
Компонент выпускает на действующем ЦС пару файлов авторизации для сервиса SCEP: JWT-токен и зашифрованный приватный ключ.

Сбор данных. Заполните переменные: ROLE (роль токена, по умолчанию admin), PASSWORD_KEY (пароль шифрования ключа, с подтверждением); имя сервиса подставляется как scep, учётная запись и

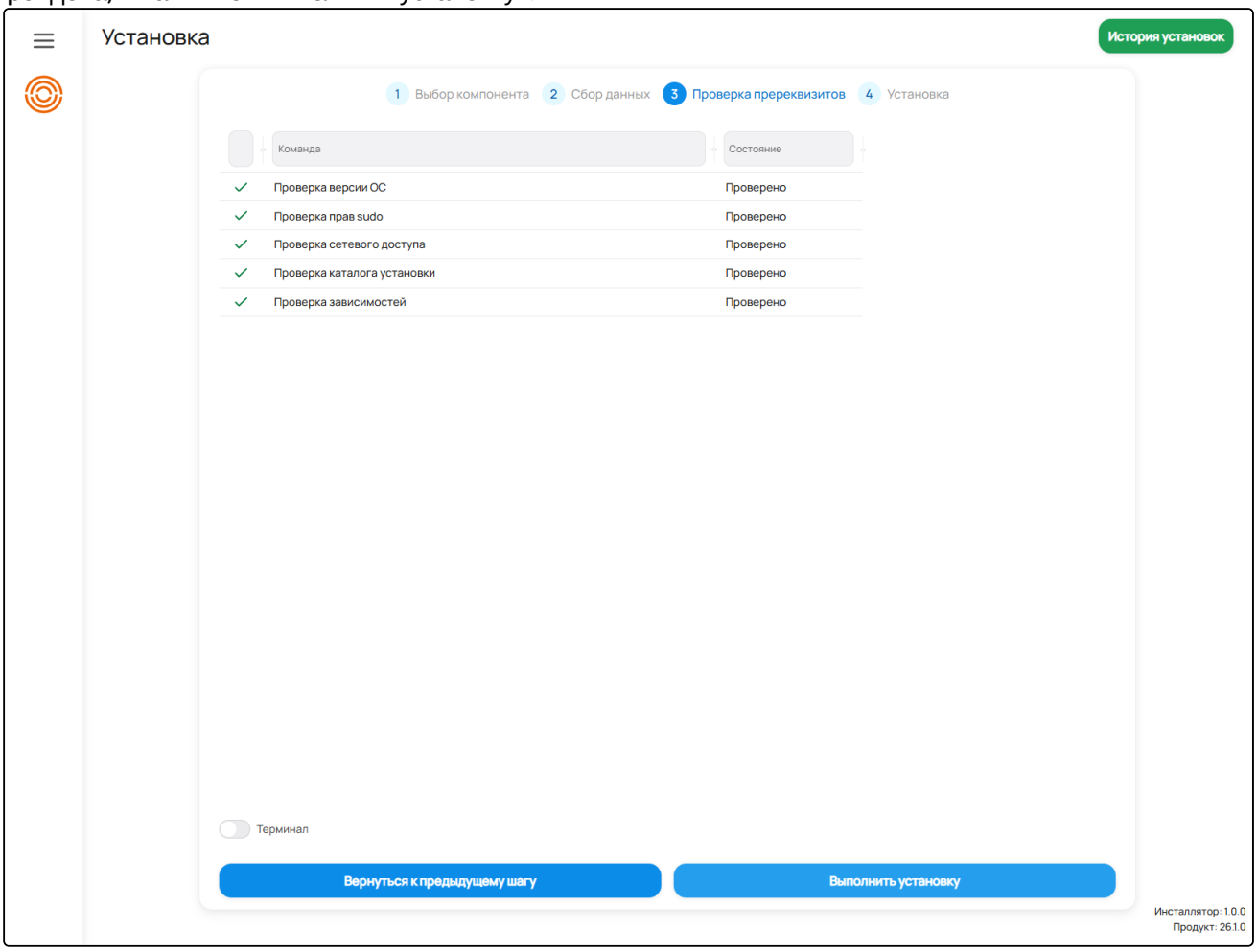
каталог – из настроек ЦС.



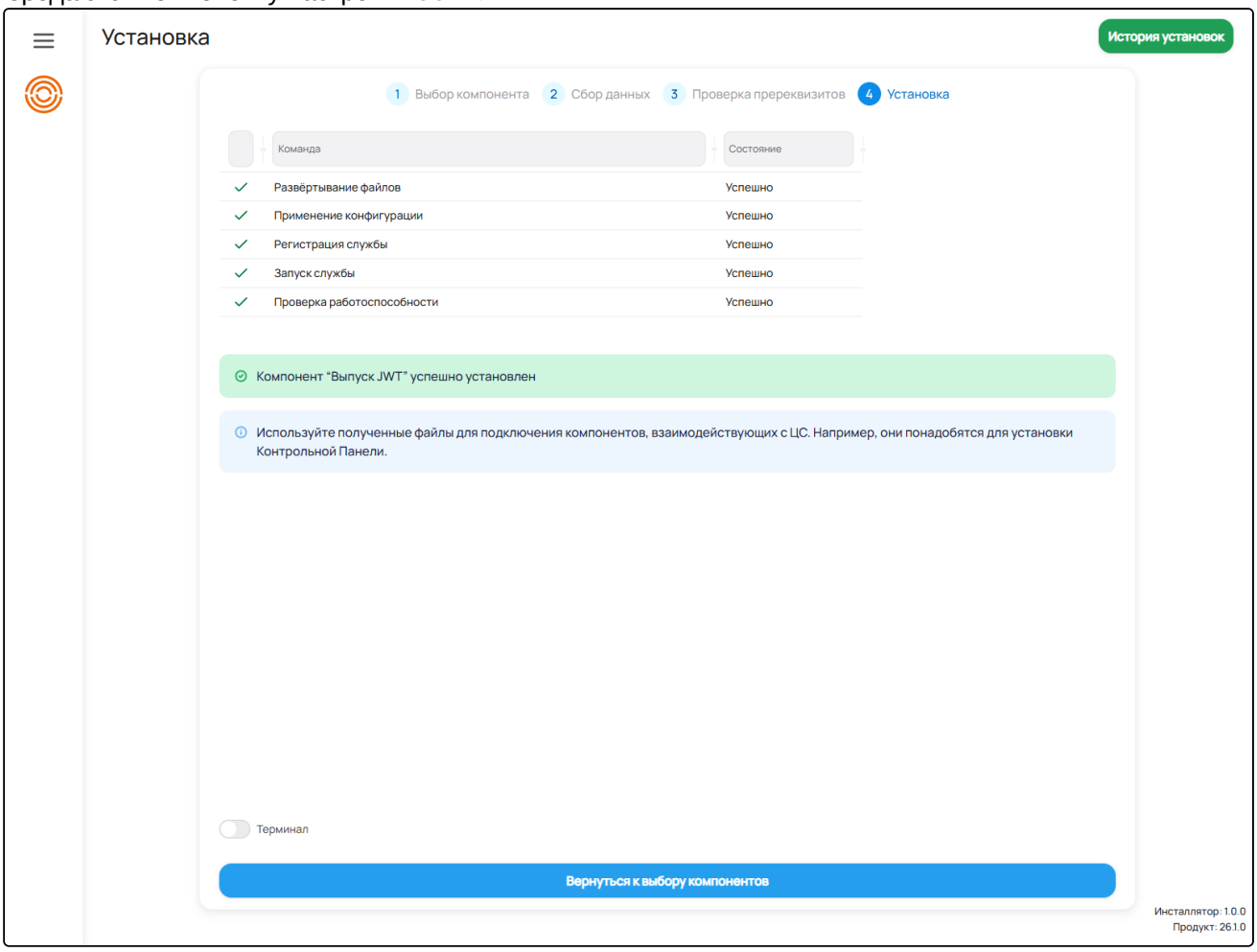
Продолжение экрана – остальные поля выпуска JWT.



Проверка пререквизитов. Проверяется доступность ЦС (mclient ping). Убедитесь, что проверка пройдена, и нажмите «Выполнить установку».



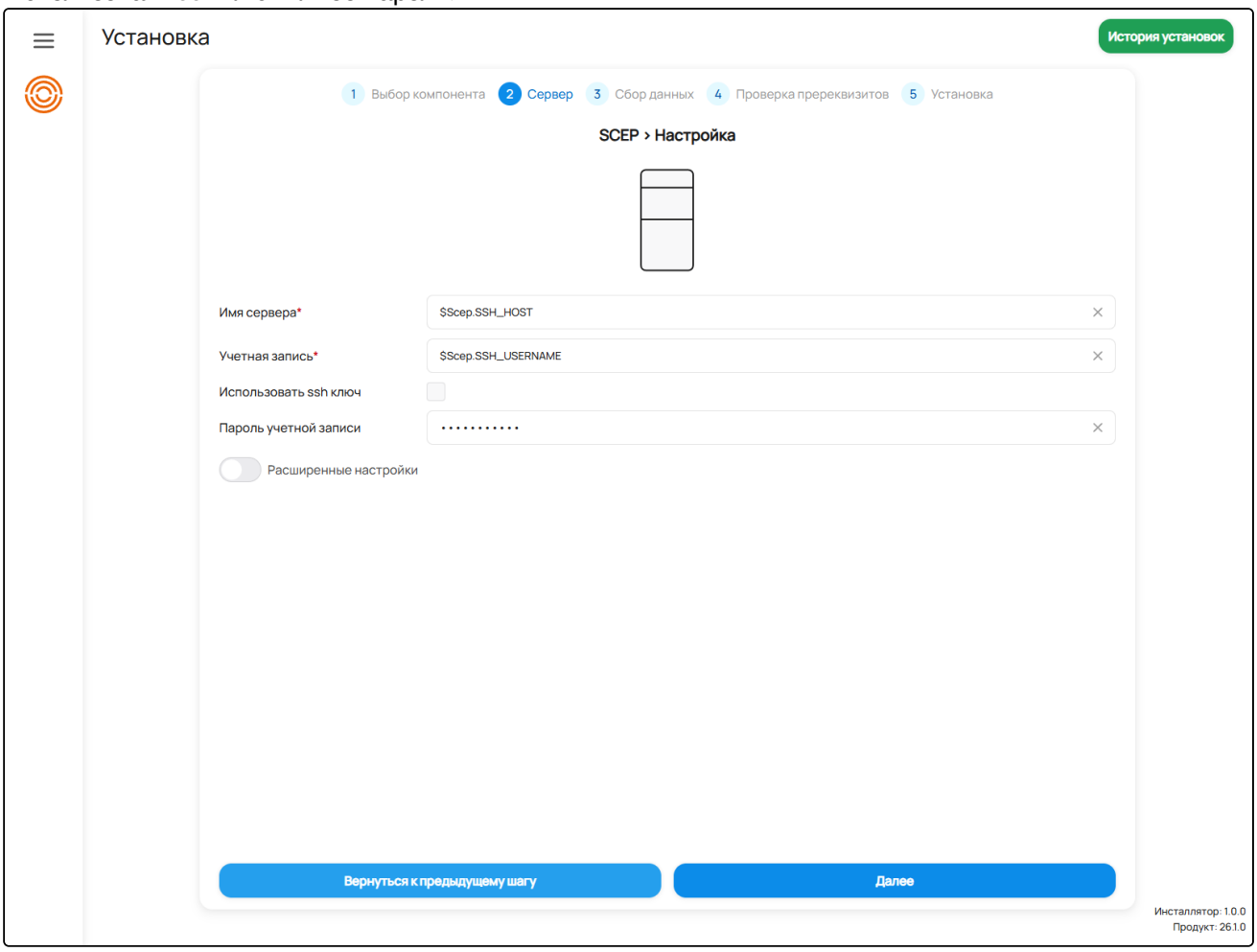
Установка и результат. Формируются файлы scep.jwt и scep.encrypted.key. Скачайте оба — они передаются компоненту настройки SCEP.



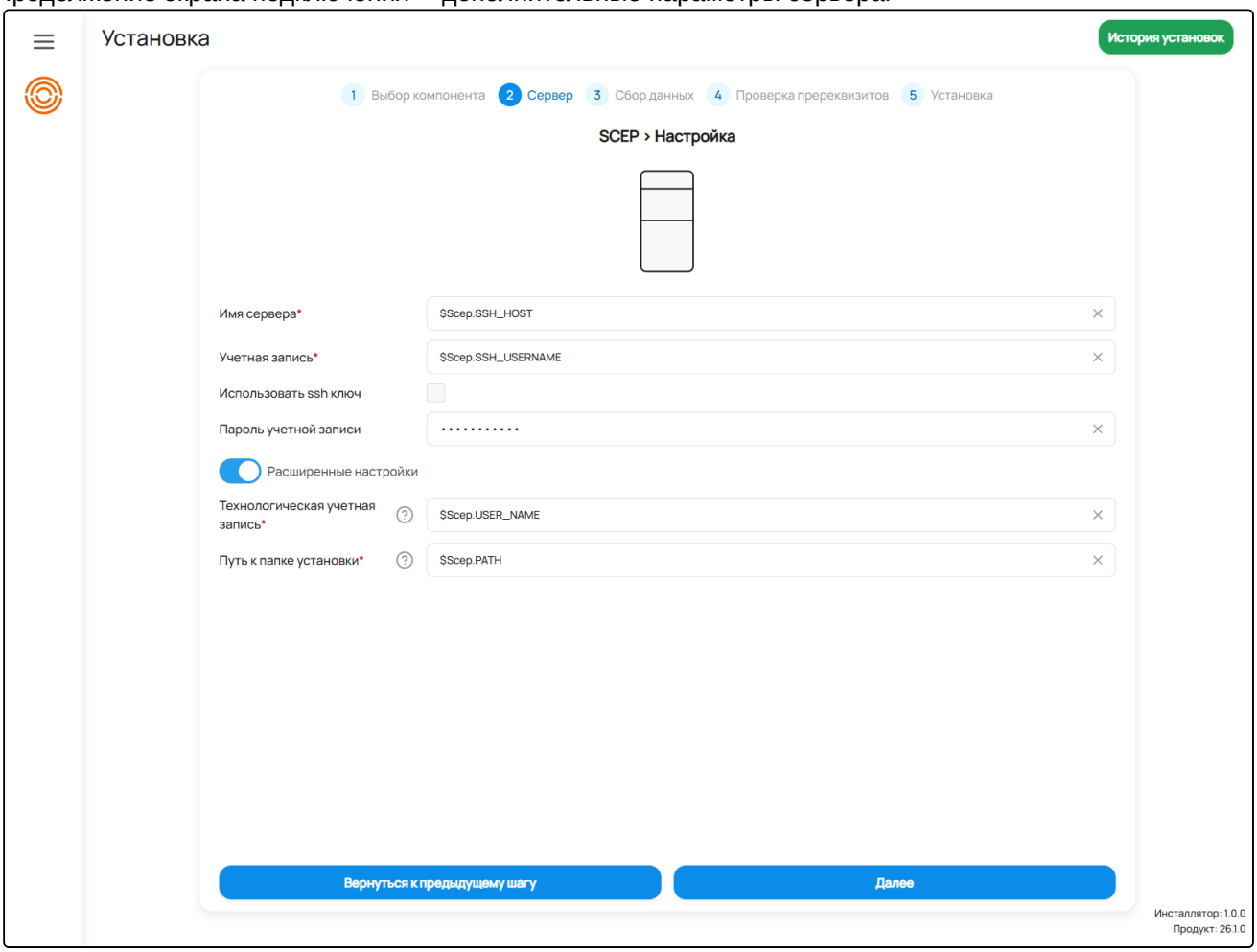
15.5 Настройка

Компонент донастраивает установленный SCEP-адаптер: размещает учётные данные ЦС, расшифровывает ключ и подключает ЦС к сервису.

Сервер. Укажите параметры SSH-подключения к серверу SCEP: имя сервера, учётную запись и флажок «Использовать ssh ключ» либо пароль.

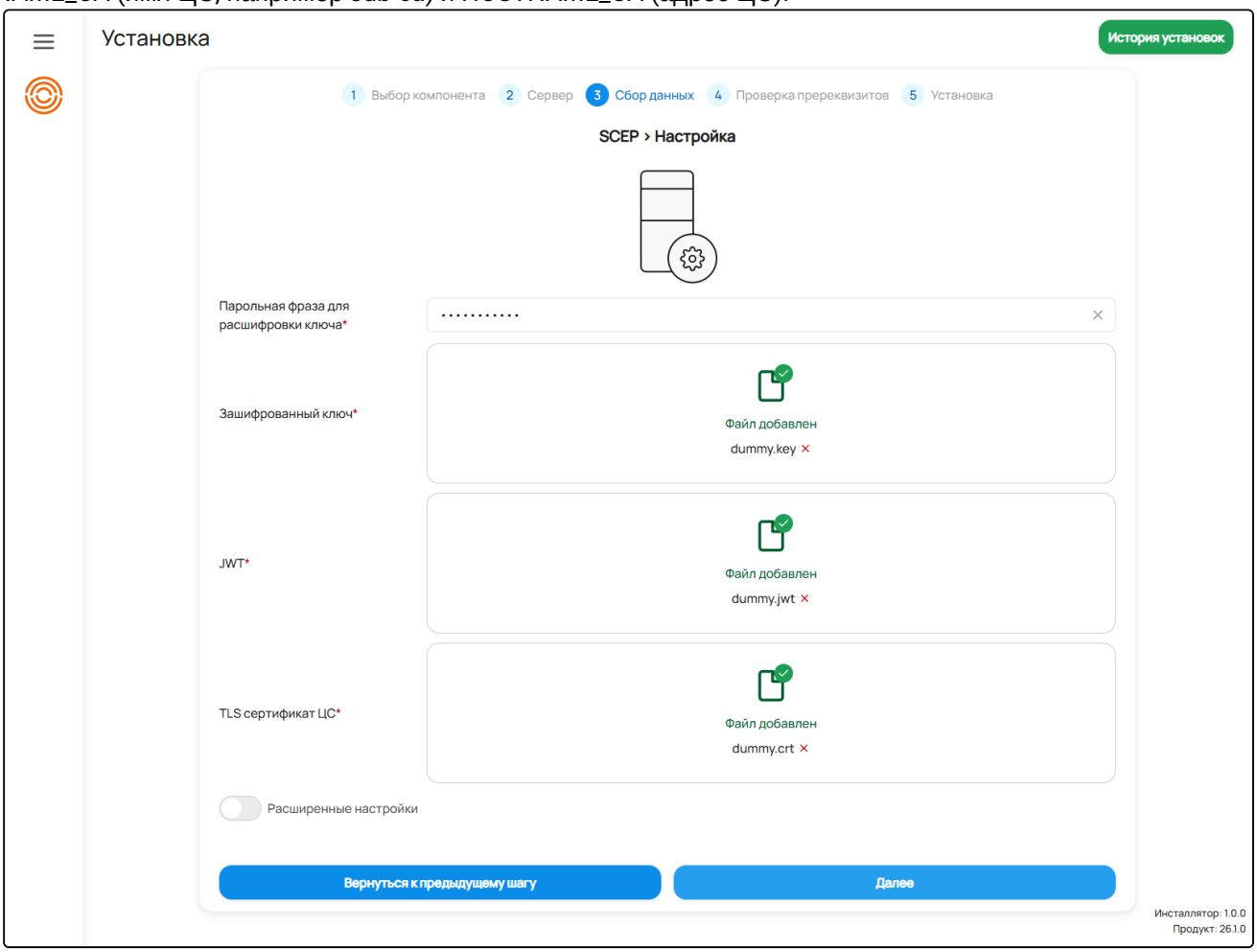


Продолжение экрана подключения – дополнительные параметры сервера.

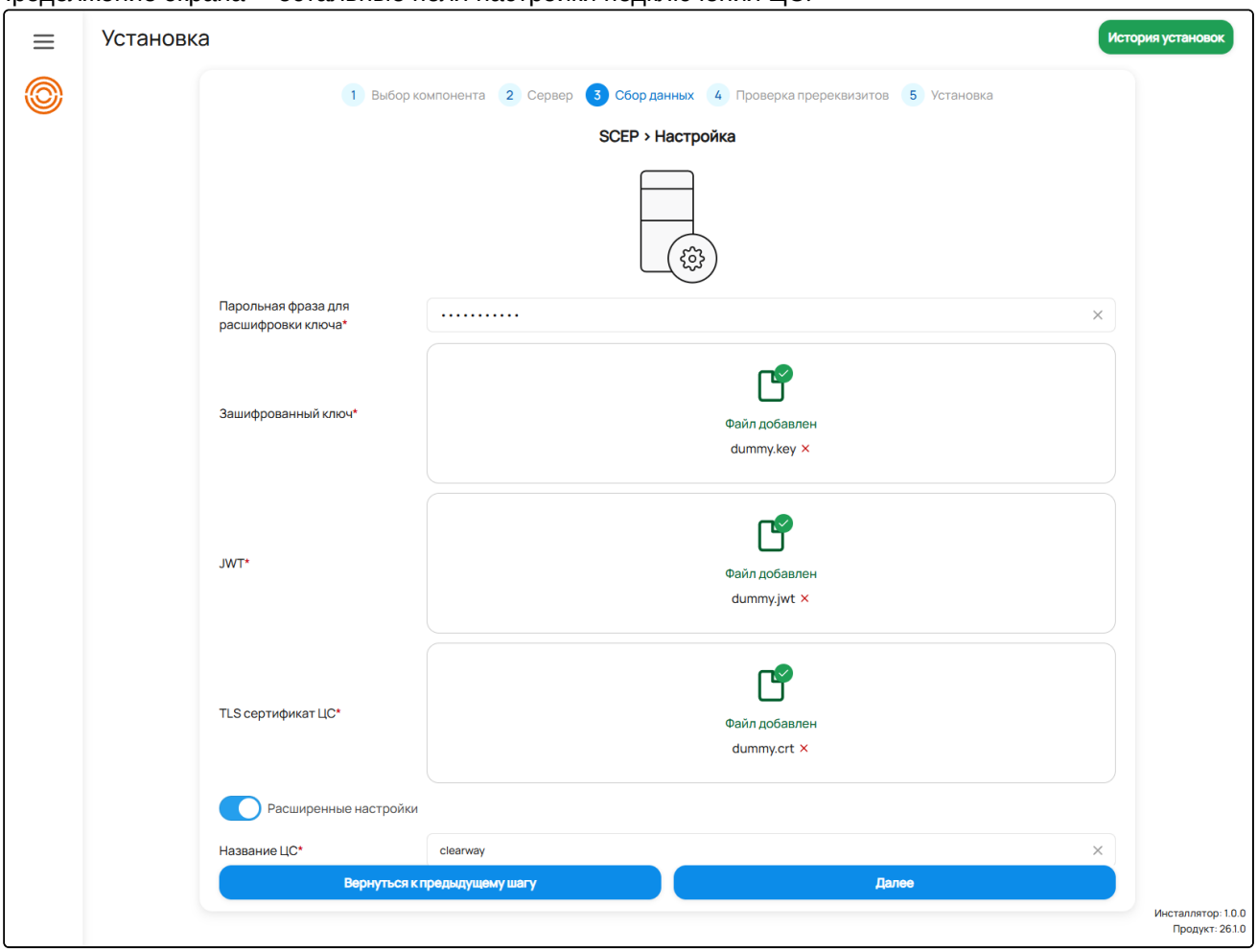


Сбор данных. Заполните переменные: ENCRYPTED_KEY (зашифрованный ключ scep.encrypted.key), JWT (токен scep.jwt), PASSWORD_KEY (пароль для расшифровки ключа), CA_TLS (TLS-сертификат ЦС),

NAME_CA (имя ЦС, например sub-ca) и HOSTNAME_CA (адрес ЦС).

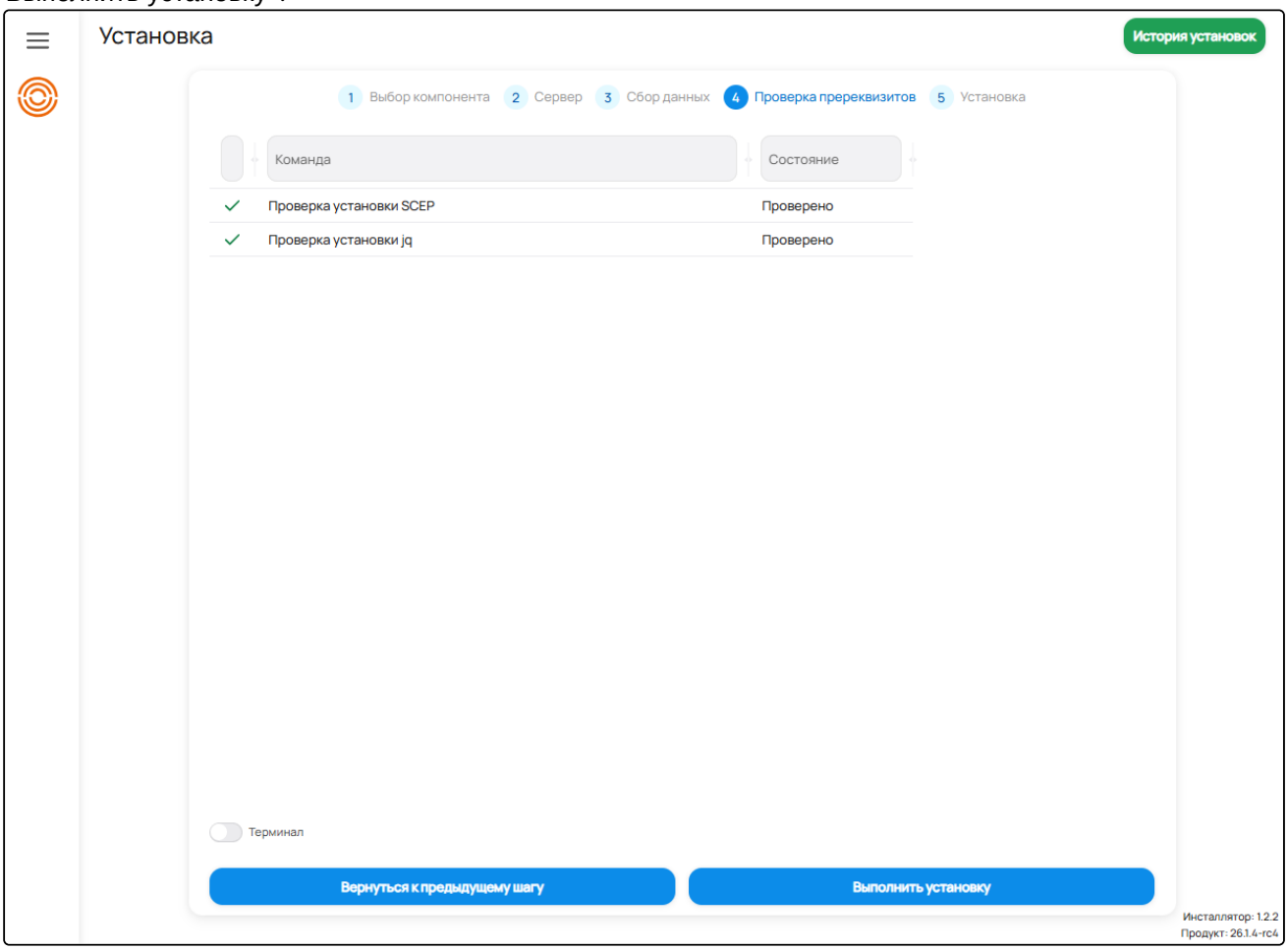


Продолжение экрана – остальные поля настройки подключения ЦС.

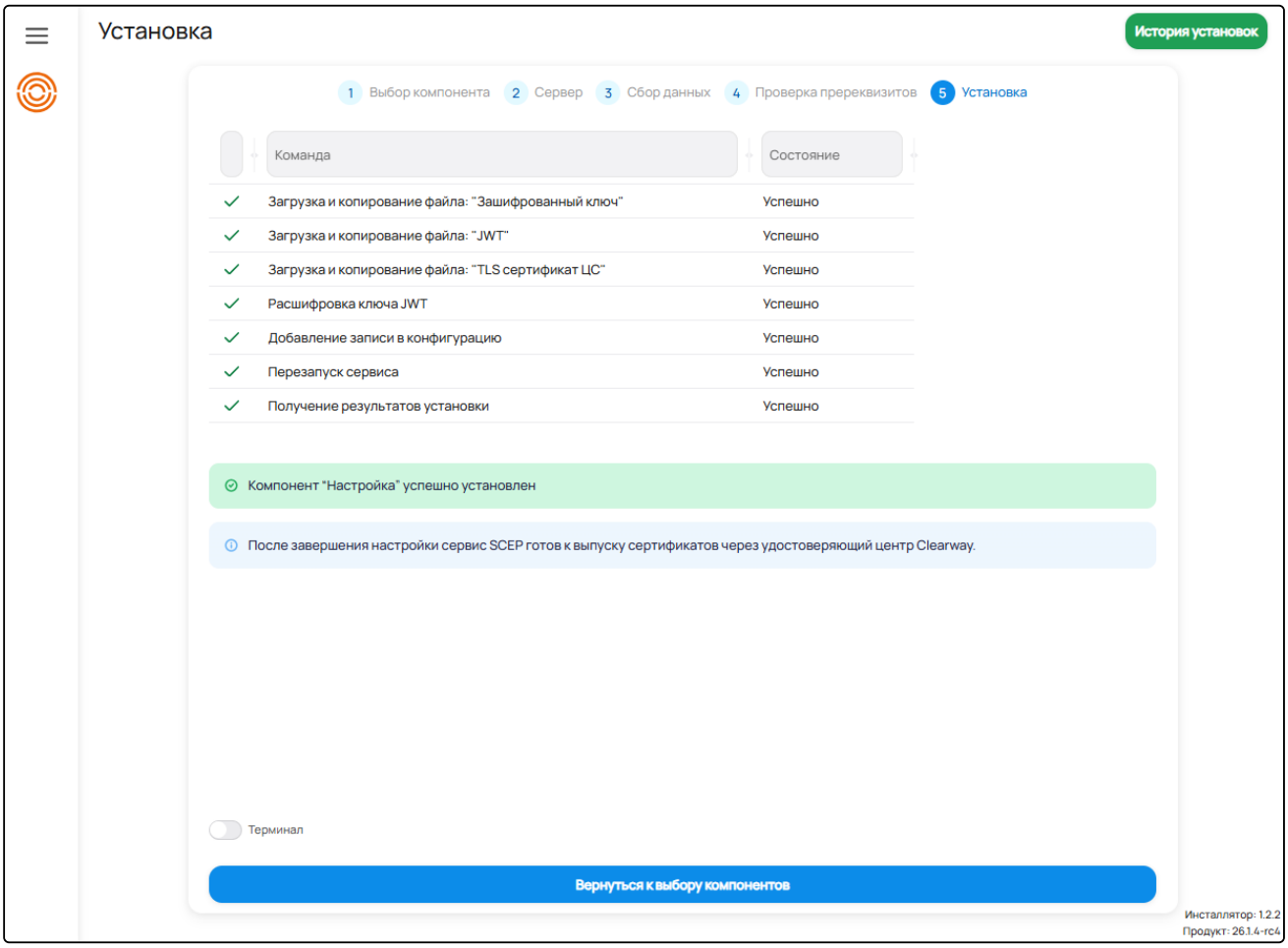


Проверка пререквизитов. Проверяется, что сервис SCEP активен (scepAdapter.service) и установлена утилита jq. При незакрытых проверках нажмите «Выполнить настройку пререквизитов», затем –

«Выполнить установку».



Установка и результат. Ключ расшифровывается, ЦС регистрируется в конфигурации адаптера (ClearwayCaClientConfig), сервис перезапускается. После успешного завершения сервис SCEP готов к работе.


Установка
История установок
1 Выбор компонента
2 Сервер
3 Сбор данных
4 Проверка пререквизитов
5 Установка
Команда
Состояние
Загрузка и копирование файла: "Зашифрованный ключ"
Успешно
Загрузка и копирование файла: "JWT"
Успешно
Загрузка и копирование файла: "TLS сертификат ЦС"
Успешно
Расшифровка ключа JWT
Успешно
Добавление записи в конфигурацию
Успешно
Перезапуск сервиса
Успешно
Получение результатов установки
Успешно
Компонент "Настройка" успешно установлен
После завершения настройки сервис SCEP готов к выпуску сертификатов через удостоверяющий центр Clearway.
Терминал
Вернуться к выбору компонентов
Инсталлятор: 1.2.2
Продукт: 26.1.4-rc4

16 Точка распространения CRL и сертификатов (CDP)

Компонент устанавливается отдельно (в мастере — «Остальные компоненты» → «Точка распространения CRL и сертификатов (web-сервер)»). Это HTTP-веб-сервер (Nginx), публикующий для клиентов:

- цепочку доверия — сертификаты ЦС (AIA, Authority Information Access);
- списки отозванных сертификатов (CRL, Certificate Revocation List).

Опубликованные файлы доступны по адресам http://<сервер>/cdp/ (списки отзыва) и http://<сервер>/aia/ (цепочка доверия). Путь установки по умолчанию — */opt/itc/web*, технологическая учётная запись — itc-svc.

Этапы: Выбор компонента → Сервер → Сбор данных → Проверка пререквизитов → Установка.

Сервер. Укажите имя сервера, учётную запись и способ подключения по SSH (пароль или SSH-ключ).

Сбор данных. Задайте параметры: «Alias сервера» (имя, по которому обращаются к точке распространения; если не указан — определяется командой hostname; поле доступно в расширенных настройках), «Технологическая учётная запись» (владелец папки установки) и «Путь к папке установки» (/opt/itc/web по умолчанию).

Проверка пререквизитов. Дождитесь завершения проверок; при незакрытых пунктах нажмите «Выполнить настройку пререквизитов», иначе — «Выполнить установку».

Установка. Мастер копирует конфигурацию nginx.conf, создаёт структуру каталогов публикации (cdp — для CRL, aia — для сертификатов), подключает конфигурацию Nginx (cdp.conf, ссылка в каталоге конфигураций Nginx) и перезагружает Nginx. По завершении выводится сообщение «Компонент … успешно установлен».

17 Обработка ошибок

Основные ошибки:

Ошибка	Причина	Как исправить
Cannot connect to database	Неверный пароль; PostgreSQL не запущен; неверный адрес или порт	Проверьте пароль; перезапустите PostgreSQL; проверьте сетевую конфигурацию
Certificate validation failed	TLS-сертификат и ключ не соответствуют друг другу	Заново скачайте оба файла и убедитесь в их соответствии
OpenID server unreachable	Адрес сервера OpenID недоступен или неверен	Проверьте URL в браузере и сетевую доступность сервера
Произошла ошибка при подключении!	Неверный пароль/имя сервера; не настроено SSH-подключение; отклонён проброс порта	Проверьте пароль и имя сервера; убедитесь в доступности SSH; в sshd_config целевого сервера добавьте строку GatewayPorts yes
Ошибка проверки установки PostgreSQL	Штатный скрипт установки PostgreSQL не подходит для данного дистрибутива	Установите PostgreSQL последней доступной версии вручную и продолжите установку
Ошибка проверки установки Nginx	Штатный скрипт установки Nginx не подходит для данного дистрибутива	Установите Nginx последней доступной версии вручную и продолжите установку

Ошибки Контрольной панели:

Симптом	Причина	Как исправить
После настройки КП не работает ЦС	С сервера КП недоступен сервер ЦС по FQDN/IP (значение поля «Url»)	Обеспечьте доступность сервера ЦС по FQDN (настройте DNS)
После настройки КП не работает ЦС	С сервера КП недоступен сервер OpenID по FQDN	Обеспечьте доступность сервера OpenID по FQDN
После настройки КП не работает ЦС	Неверный пароль в поле «Пароль»	Введите пароль, заданный на шаге «Выпуск JWT» установки КП
После настройки КП не работает ЦС	Переданы неверные файлы «Сертификат TLS» / «Зашифрованный приватный ключ» / «JWT»	Используйте файлы из шагов «Выпуск сертификата» и «Выпуск JWT» установки КП
«Красный» статус сервиса публикации	Сервис публикации не установлен	Установите сервис публикации через мастер

Симптом	Причина	Как исправить
«Красный» статус сервиса публикации	Неверная конфигурация	В /opt/itc/itc/config/itc_api_miniCA_controlPanel_config.json поле PublicationCrlUrl должно содержать адрес сервера публикации

18 История установок

Раздел «История установок» (кнопка в правом верхнем углу окна мастера) содержит справочную информацию о выполненных установках. В таблице отображаются:

- Компонент — название установленного компонента;
- Место установки — сетевой адрес сервера, на котором выполнялась установка;
- Дата — дата установки;
- Статус — результат: «Успешно», «Ошибка», «Приостановлено» или «Skipped» (Пропущено).

Доступны обновление данных, настройка отображаемых колонок и удаление фильтров. При выборе записи (ЛКМ) открывается подробная информация об установке по секциям: "Переменные" (введённые параметры), "Результат" (полученные файлы конфигураций и данных), "Пререквизиты" (состояние проверок на момент установки), "Установка" (состояние выполненных действий) и "Терминал" (журнал команд).