Центр
Управления
Гетерогенными
Инфраструктурами

СУУ СКЗИ. Инструкция по запуску продукта в демо-зоне

ООО «Клируэй Текнолоджис»

2026

Оглавление

1 Введение

Настоящий документ содержит информацию о процессе установки «Системы учета и управления криптографическими средствами защиты информации» (СУУ СКЗИ), на ОС «Astra Linux 1.8» (далее система), а также инструкцию для доступа к уже готовому демо-стенду. На демо-стенде можно ознакомиться с функциональностью системы и протестировать её возможности.

> ⚠ Для выполнения всех действий требуются права локального администратора (Windows) или root (Linux).

2 Служба поддержки

По всем вопросам, связанных с установкой системы и доступу к демо-стенду, следует обращаться в техническую поддержку к сервисным инженерам.

Техническая поддержка работает круглосуточно и доступна по следующим каналам связи:

- Телефон: +7 (495) 142-41-42
- Email: support@clearwayintegration.com

3 Использование демо-стенда системы

3.1 Общая информация

Демо-стенд системы расположен во внутреннем контуре компании. Система развернута в минимальной версии и включает в себя сервер приложений, на котором находятся сервисы СКЗИ, сервер Keycloak, сервер PostgreSQL, сервер Active Directory. Для доступа к демо-стенду необходимо настроить VPN, добавить в доверенные сертификаты и перейти на веб-интерфейс управления системой (см. раздел Вход в веб-интерфейс системы).

3.2 Пререквизиты

Программное обеспечение

VPN-клиент	Cisco AnyConnect Secure Mobility Client https://vpn.clearwayintegration.com
Веб-браузер	Любой современный браузер для доступа к интерфейсам управления
Операционная система	Windows или Linux (поддерживаются Debian/Ubuntu и RHEL/CentOS/Fedora)

Требования к аппаратным ресурсам

CPU	2 ядра
RAM	8 GB
HDD	70 GB

Учетные записи

	Назначение УЗ	Учетная запись	Пароль
1	VPN Адрес шлюза для VPN: 82.142.150.30	Для подключения по VPN запросите учетные данные администратора у сотрудников технической поддержки.	
2	Портал СУУ СКЗИ	min-skzi	pctVv5bS3oHuz8E

Сертификаты безопасности

Для корректной работы браузера и отсутствия ошибок SSL на компьютере, который используется для подключения к демо-стенду, необходимо установить следующие сертификаты:

- Root CA Cert (корневой сертификат);
- Sub CA Cert (промежуточный сертификат).

Целевые ресурсы

После настройки доступ осуществляется по адресам:

- Keycloak: https://min-klck.tst.itc.internal
- Web-интерфейс СКЗИ: https://min-skzi.tst.itc.internal

3.3 Схема развертывания компонентов продукта на демо-стенде

Ниже представлена схема компонентов системы, развернутой по https://min-klck.tst.itc.internal

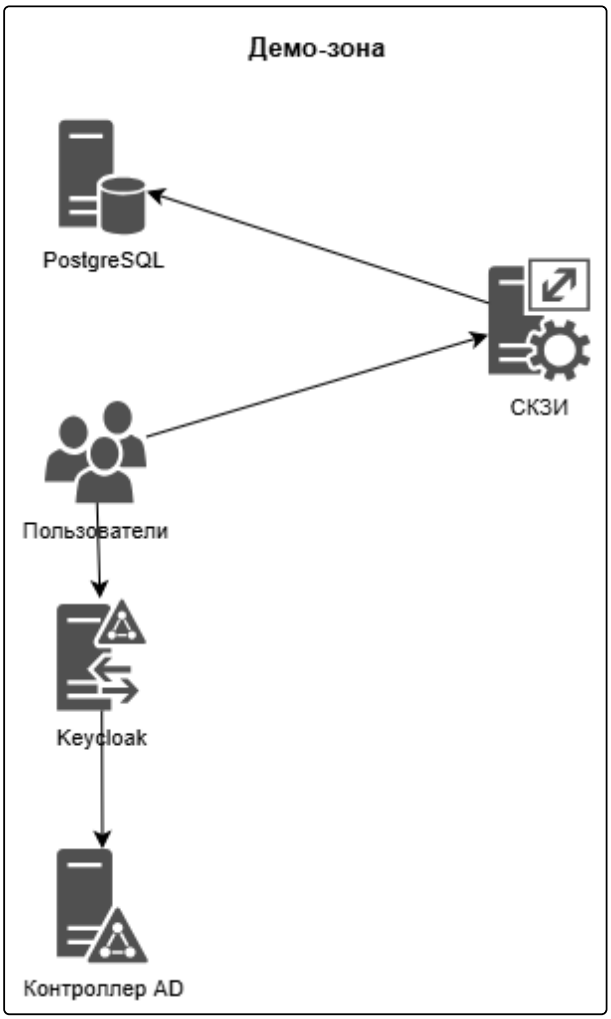


Рисунок 1 Схема компонентов СУУ СКЗИ

	Система	Имя сервера	IP-адрес	CPU	RAM GB	HDD GB
1	Контроллер AD	tst-dc1.tst.itc.internal	192.168.60.101	1	4	100
2	Keycloack	min-klck.tst.itc.internal	192.168.60.76	1	2	20
3	БД PostgreSQL	min-pgs.tst.itc.internal	192.168.60.77	2	8	70
4	СКЗИ	min-skzi.tst.itc.internal	192.168.60.85	2	4	30

1. Хост min-skzi.tst.itc.internal - на этом хосте установлены сервисы СУУ СКЗИ:

	Имя сервиса	Назначение
1	itcagentd	Агент ЦУГИ
2	nginx	Web-сервер, реверс-прокси, балансировщик
3	itcsrvd	Мост между агентами и сервером управления
4	itcdispd	Диспетчер агентов
5	ITC.Api.Collreg	Провайдер коллекций
6	itcmsgd	Брокер сообщений NATS
7	ITC.Api.AppStore	Магазин приложений для АРМов
8	ITC.Api.MailOutbox	Сервис отправки уведомлений по электронной почте (статусы заявок, результаты тестирования, напоминания и др.).
9	itc.api.edusurvey.service	Обучение и тестирование пользователей
10	itc.api.scriptlauncher.service	Интеграционный сервис, отвечающий за взаимодействие с системой МИУ и агентами на конечных устройствах: отправка команд инвентаризации и сбор данных об установленных СКЗИ.
11	itc.api.skzi.controlpanel.service	Веб-интерфейс системы: содержит административную консоль и личный кабинет пользователя. Через него осуществляется управление СКЗИ, просмотр статусов, прохождение тестирования и подача заявок.

	Имя сервиса	Назначение
12	itc.api.skzi.service	Основной сервер приложений (BackEnd), реализующий бизнес-логику СКЗИ: управление ключами, политиками, жизненным циклом средств, интеграция с другими сервисами.

2. Хост min-klck.tst.itc.internal - на этом хосте установлена система управления идентификацией и доступом Keycloak:

KeyCloak 26.0.7	Идентификация и управления доступом

3. Хост min-pgs.tst.itc.internal - на этом хосте установлена СУБД PostgreSQL:

PostgreSQL 15.14	Хранение данных

4. Список БД для функционирования данного ППО:

skzi
skzi-audit
skzi-mailoutbox
skzi_appstore
skzi_collreg
skzi_dispd

5. Хост min-dc.tst.itc.internal - на этом хосте установлен Контроллер AD:

ActiveDirectory	Служба каталогов

3.4 Настройка доступа к демо-стенду

Для настройки доступа к веб-интерфейсу управления системой выполните следующие шаги.

1. Запросите учетные данные для VPN у сотрудников технической поддержки.
2. Авторизуйтесь по VPN.
3. Добавьте в доверенные необходимые сертификаты для ОС Windows / ОС Linux.

3.4.1 Настройка VPN

Доступ во внутренний контур компании обеспечивается с помощью программы Cisco AnyConnect Secure Mobility Client.

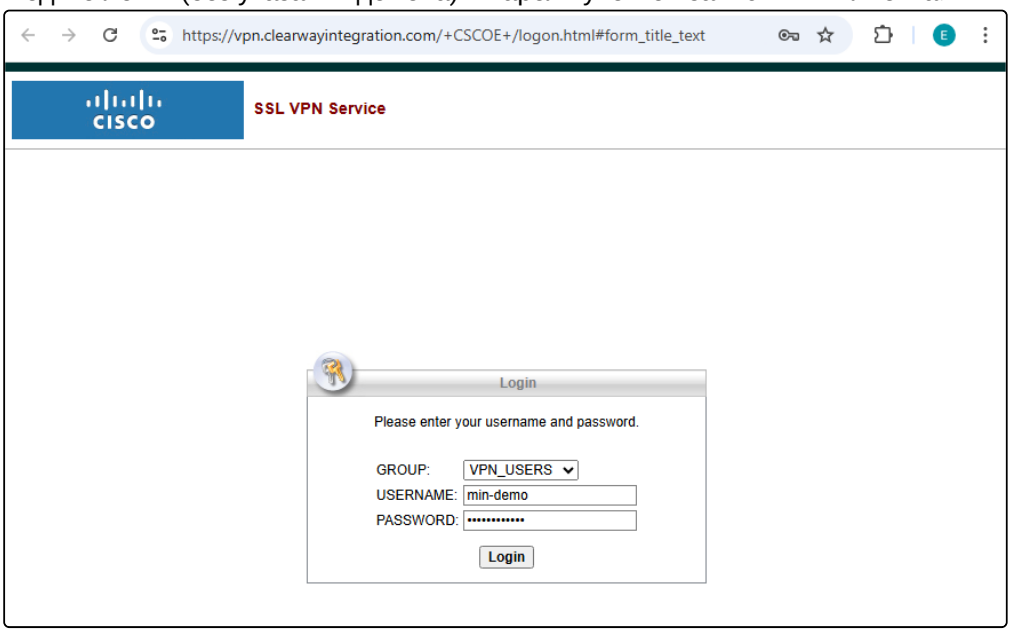
Перед началом установки убедитесь, что:

- вы выполняете инструкцию на рабочем компьютере, на котором будет осуществляться VPN-подключение к ресурсам компании;
- у вас есть права локального Администратора (Windows) или sudo (Linux/macOS);
- отключены другие VPN-соединения.

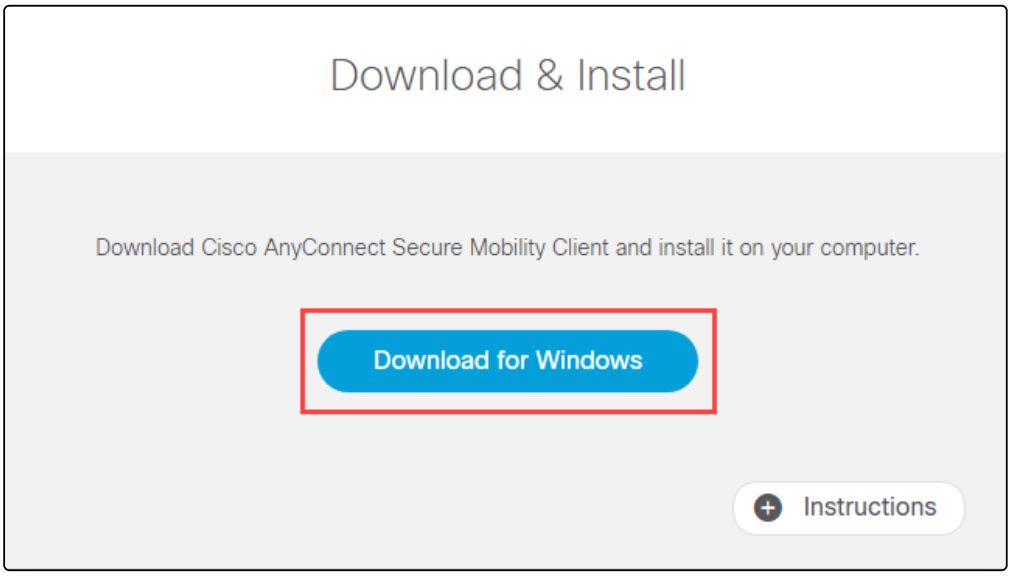
3.4.1.1 Первоначальная установка VPN-клиента

Если VPN-клиент Cisco AnyConnect уже установлен на вашем компьютере, пропустите этот раздел и перейдите к разделу Авторизация по VPN.

1. Откройте в браузере страницу https://vpn.clearwayintegration.com
   Введите логин (без указания домена) и пароль учетной записи VPN-клиента.

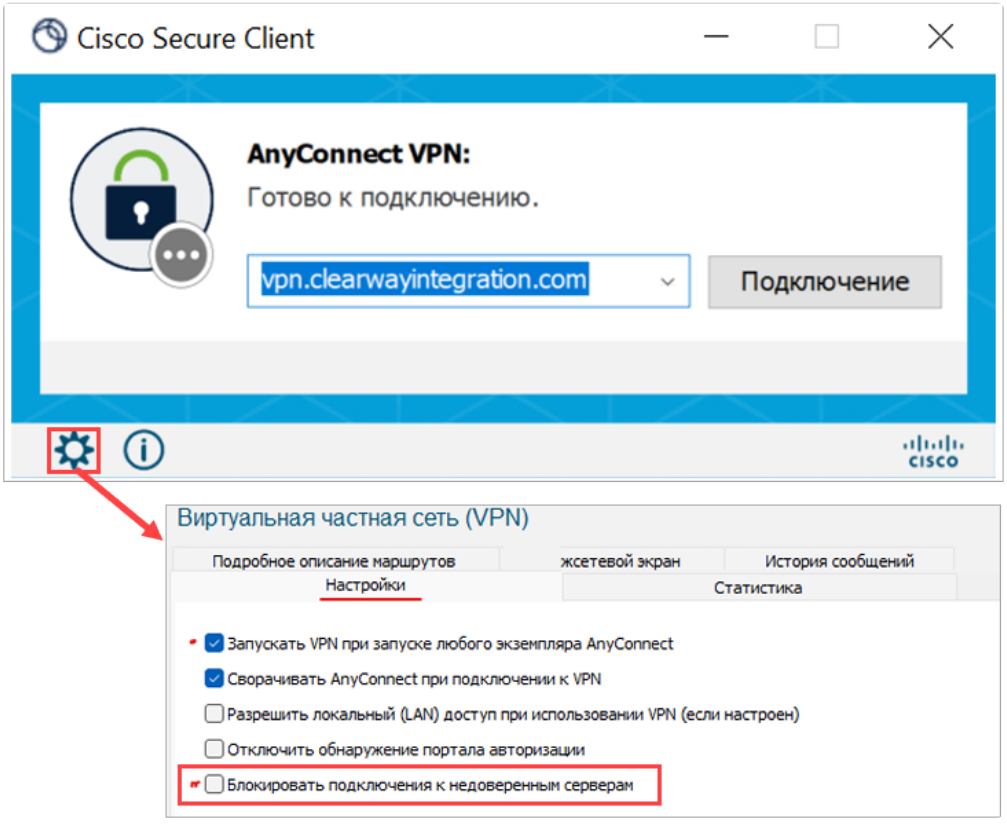


2. После успешной авторизации откроется окно с кнопкой для скачивания дистрибутива AnyConnect Secure Mobility Client.



Клиент выбирается автоматически для той ОС, в которой открыт браузер.

3. Скачайте и установите Cisco AnyConnect, следуя указаниям мастера установки.
4. Запустите клиент Cisco AnyConnect.
5. Откройте настройки (значок шестеренки) и снимите флажок "Блокировать подключения к недоверенным серверам", затем закройте окно настроек.

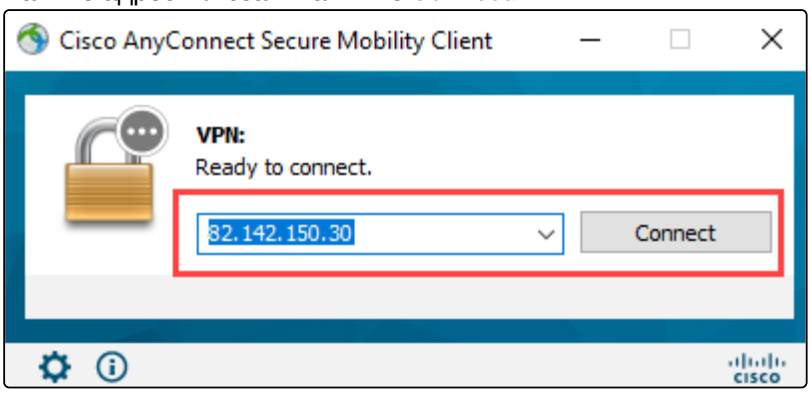


3.4.1.2 Авторизация по VPN

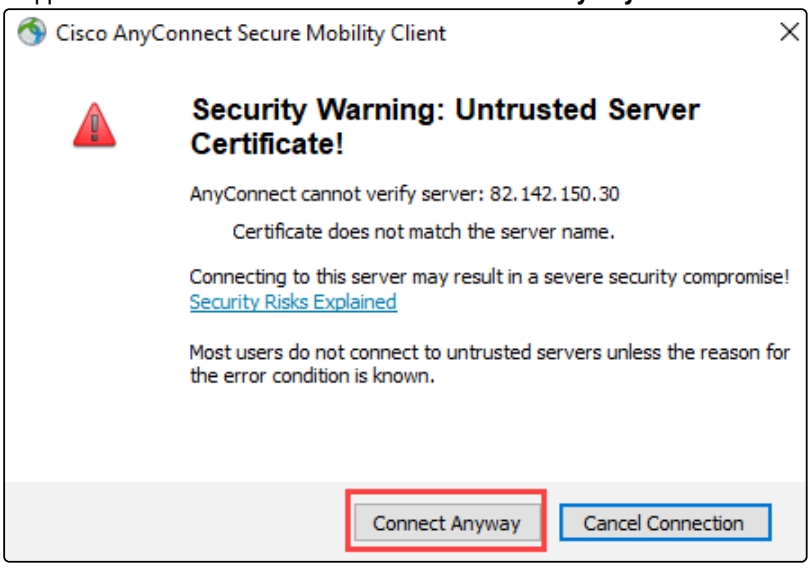
Для подключения к VPN выполните следующие действия.

1. Запустите VPN-клиент Cisco AnyConnect.

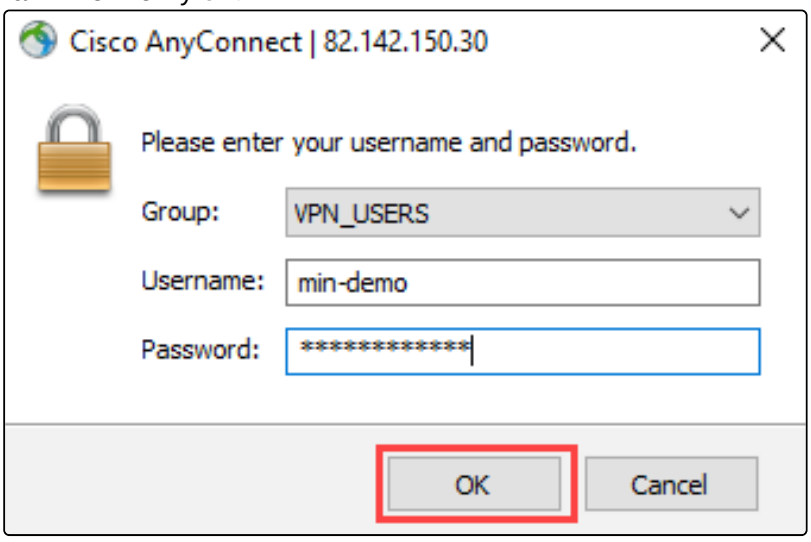
2. Укажите адрес шлюза и нажмите **Connect**.



3. При подключении к демо-стенду вы можете увидеть предупреждение, что сертификат внутреннего корпоративного ресурса не является доверенным для вашего компьютера. Это не означает, что соединение небезопасно. Нажмите **Connect Anyway**.

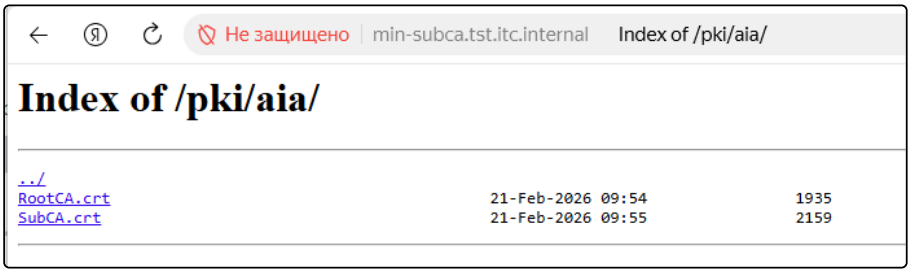


4. Укажите логин и пароль учетной записи VPN-клиента, в поле "Группа" выберите "VPN_USERS".
5. Нажмите кнопку **OK**.



3.4.2 Добавление сертификатов в доверенные

1. Откройте браузер и перейдите по ссылке http://min-subca.tst.itc.internal/pki/aia/.

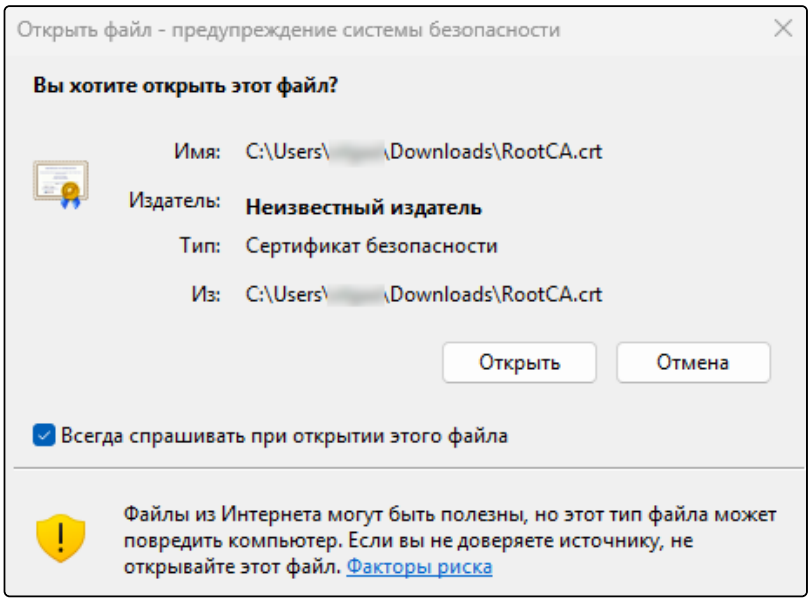


2. Скачайте на компьютер файлы сертификатов *RootCA.crt* и *SubCA.crt*.
3. Перейдите в директорию, куда вы сохранили файлы сертификатов.
4. Добавьте сертификаты, как описано ниже.
5. После добавления сертификатов закройте и заново откройте браузер, чтобы он подхватил новые сертификаты.

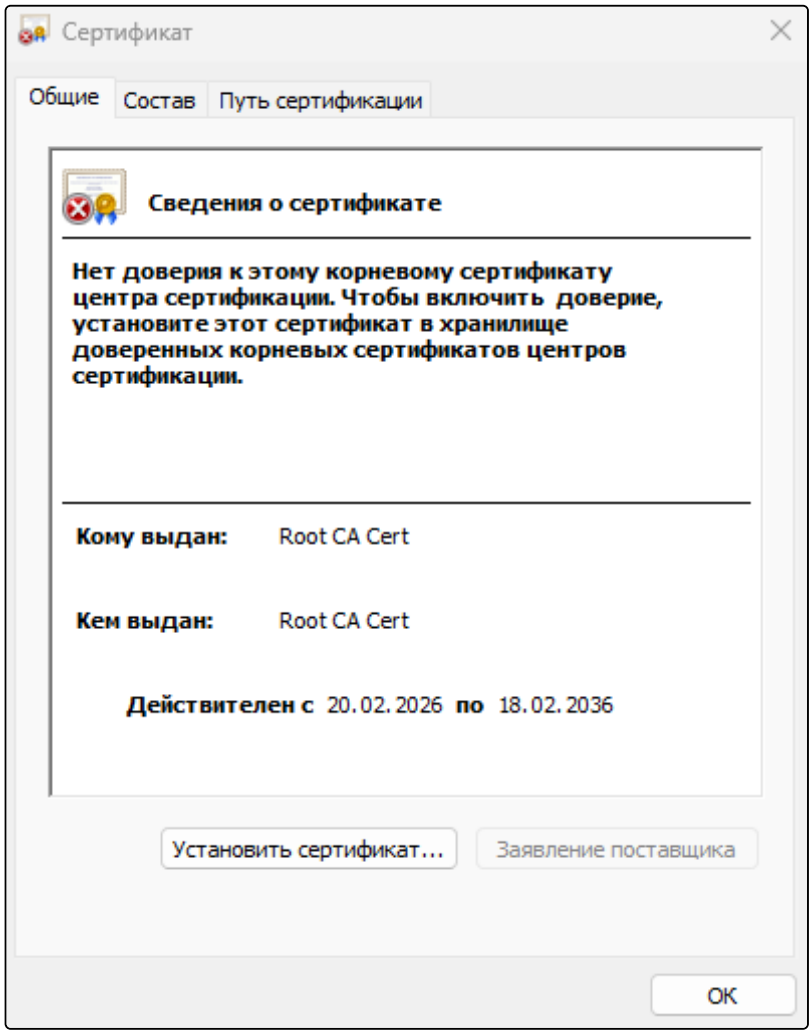
3.4.2.1 Добавление сертификатов для ОС Windows

1. Добавьте корневой сертификат *RootCA.crt* в доверенные корневые центры сертификации.

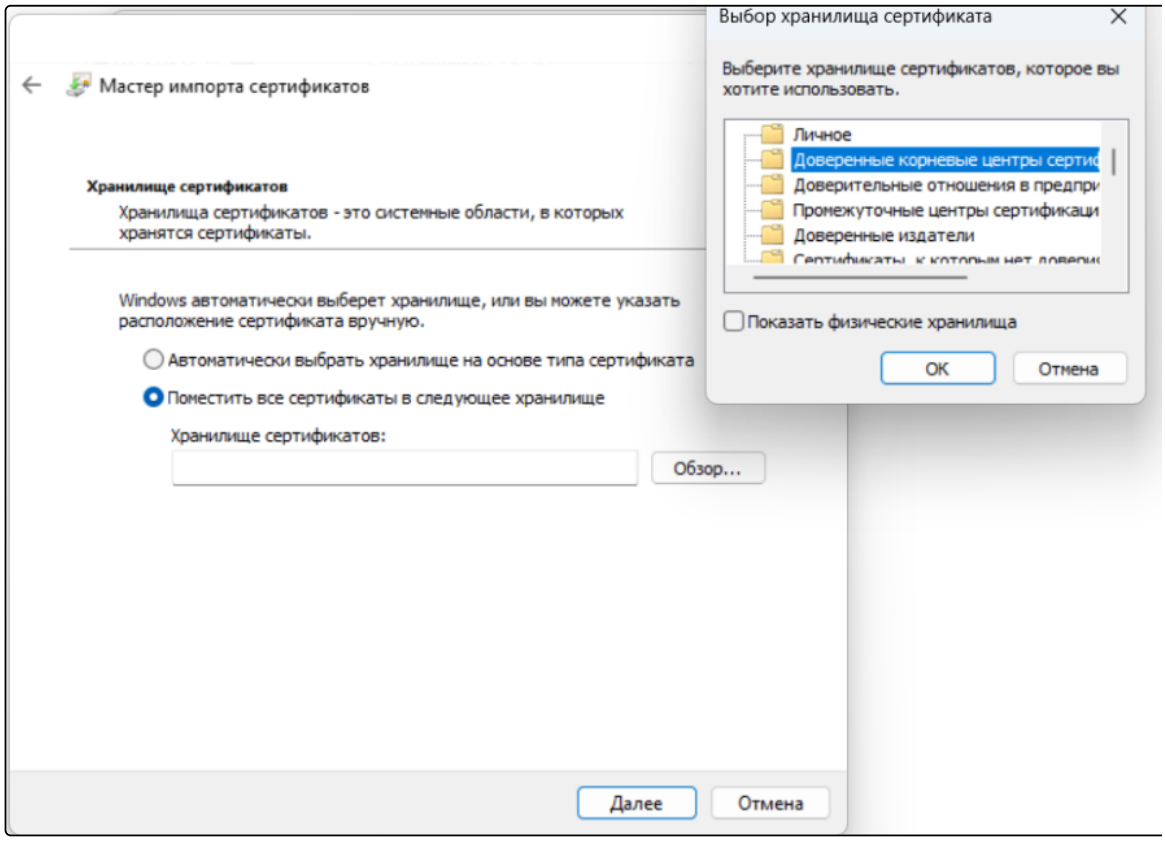
   a. Дважды нажмите на имя файла *RootCA.crt*, а затем в окне предупреждения системы безопасности нажмите **Открыть**.



   b. Нажмите **Установить сертификат**.



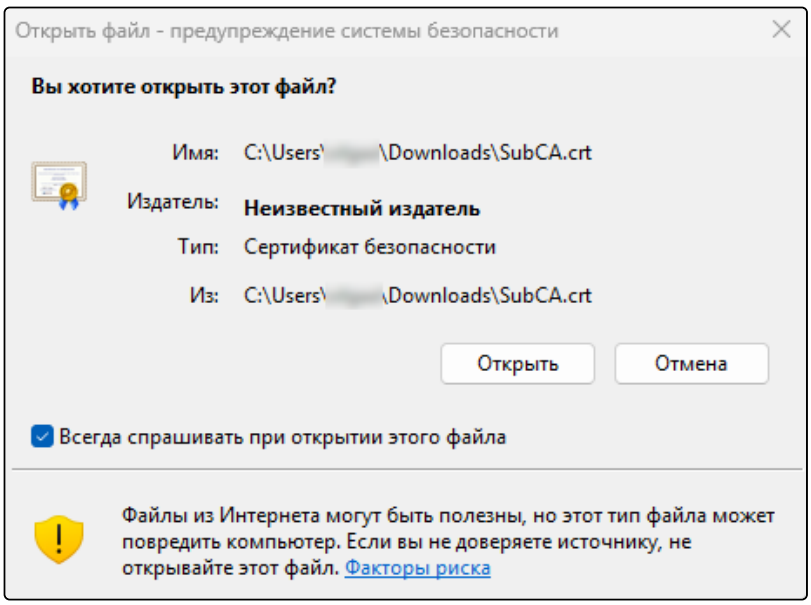
c. Нажмите **Далее**, выберите пункты, как показано на рисунке ниже. Затем нажмите **Далее**.



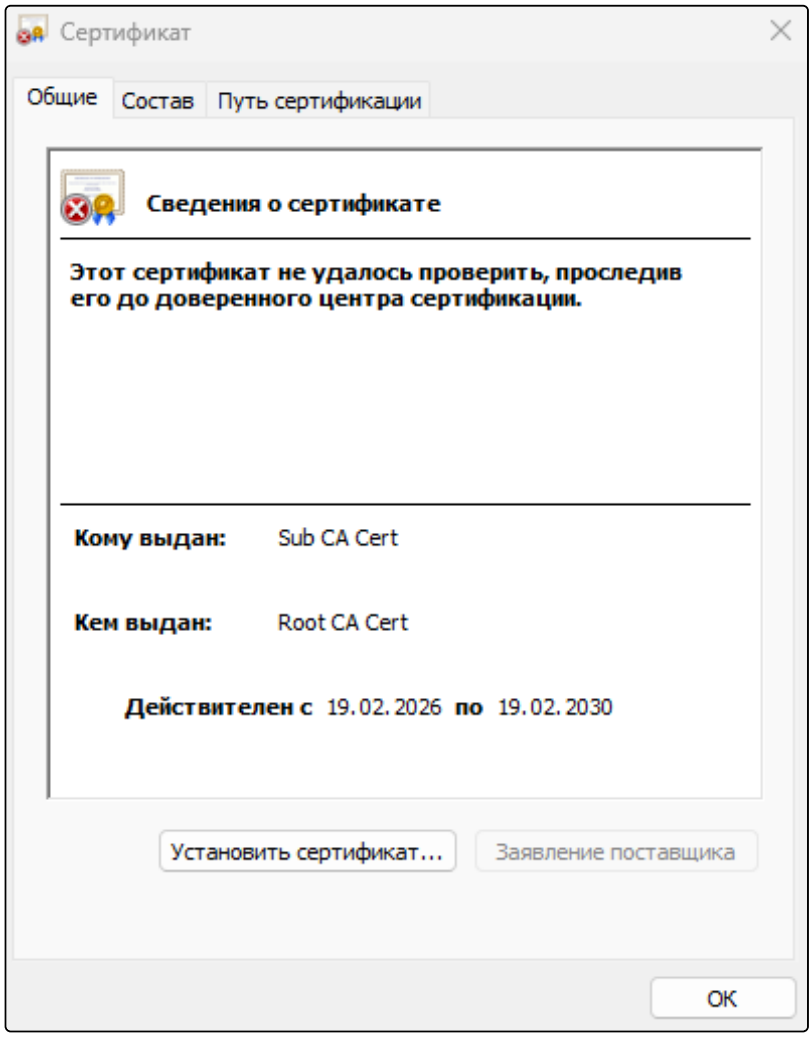
d. Нажмите **Готово**, а затем в окне предупреждения системы безопасности нажмите **Да**.

2. Добавьте промежуточный сертификат *SubCA.crt* в промежуточные центры сертификации:

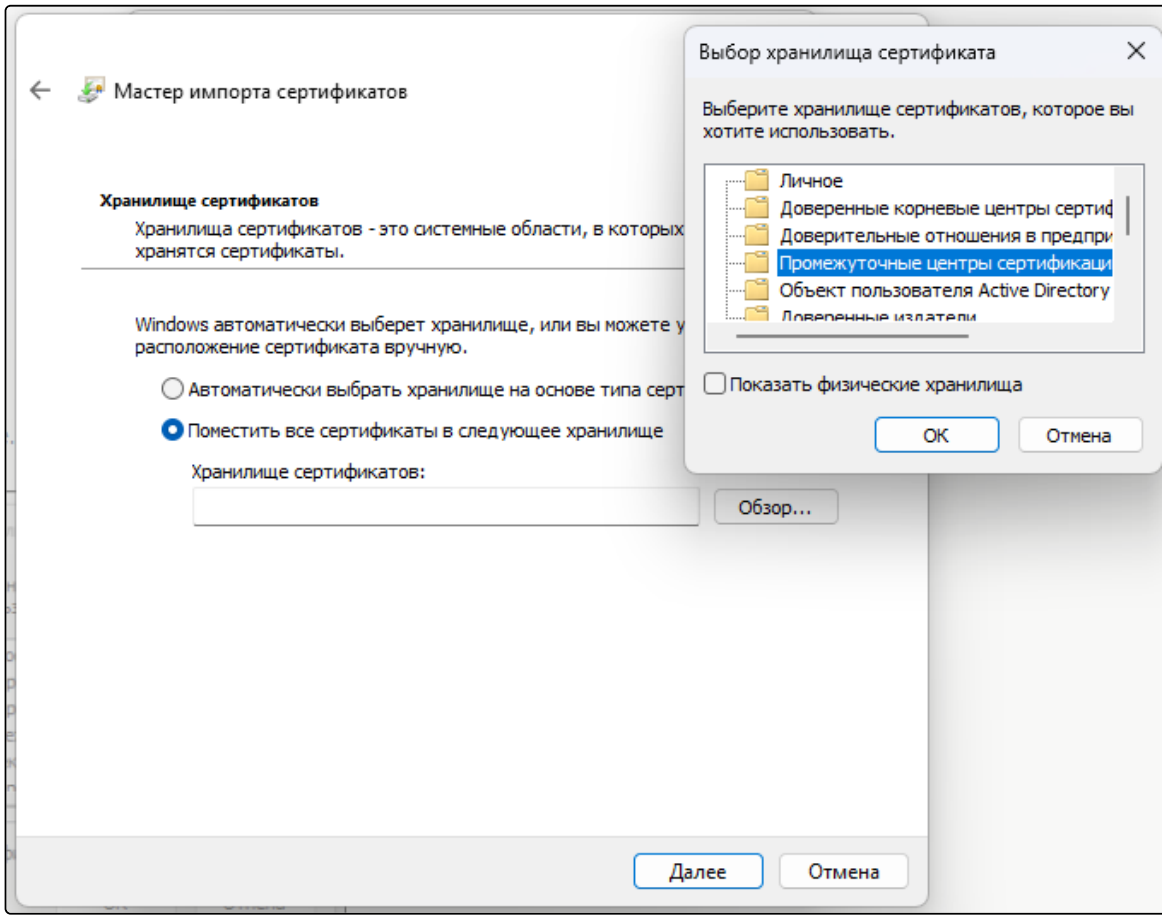
a. Дважды нажмите на имя файла *SubCA.crt*, а затем в окне предупреждения системы безопасности нажмите **Открыть**.



b. Нажмите **Установить сертификат**.



c. Нажмите **Далее**, выберите пункты, как показано на рисунке ниже. Затем нажмите **Далее**.



d. Нажмите **Готово**, а затем в окне предупреждения системы безопасности нажмите **Да**.

3.4.2.2 Добавление сертификата для ОС Linux

3.4.2.2.1 Метод 1. Использование update-ca-certificates (Debian/Ubuntu)

1. Скопируйте сертификат в нужную директорию:

```
sudo cp your-ca-certificate.crt /usr/local/share/ca-certificates/
```

2. Обновите хранилище сертификатов:

```
sudo update-ca-certificates
```

3. Проверьте добавление сертификата:

```
ls -la /etc/ssl/certs/ | grep your-certificate
```

3.4.2.2.2 Метод 2. Ручное добавление (RHEL/CentOS/Fedora)

1. Скопируйте сертификат:

```
sudo cp your-ca-certificate.crt /etc/pki/ca-trust/source/anchors/
```

2. Обновите хранилище сертификатов:

```
sudo update-ca-trust
```

3. Проверьте добавление сертификата:

```
ls -la /etc/pki/ca-trust/extracted/openssl/
```

3.5 Вход в веб-интерфейс демо-стенда

Для начала работы с веб-интерфейсом системы выполните следующие шаги:

Предварительные требования
Убедитесь, что ваше рабочее место подключено к корпоративной сети через VPN (см. раздел Настройка доступа), так как адрес находится во внутреннем контуре.

Порядок действий

1. Откройте используемый веб-браузер (например, Google Chrome, MS Edge или Яндекс.Браузер).
2. В адресную строку введите https://min-skzi.tst.itc.internal и нажмите **Enter**.
3. В появившемся окне входа заполните соответствующие поля, используя данные из таблицы Учетные записи.

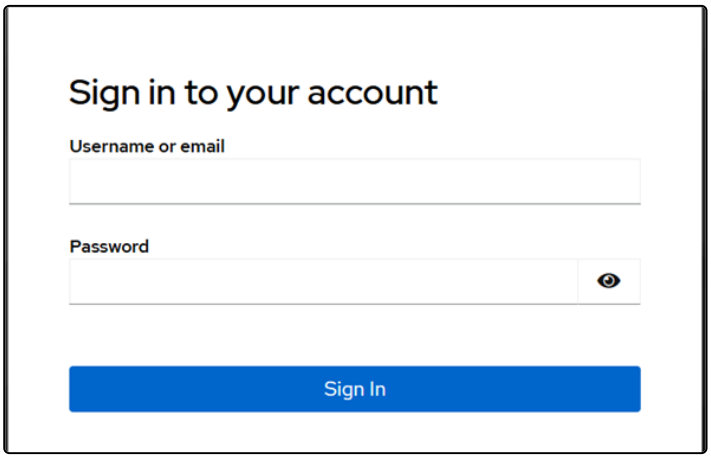


Рисунок 2 Окно входа

4. После ввода данных нажмите кнопку входа для доступа к главной странице системы. Откроется главная страница портала СУУ СКЗИ:

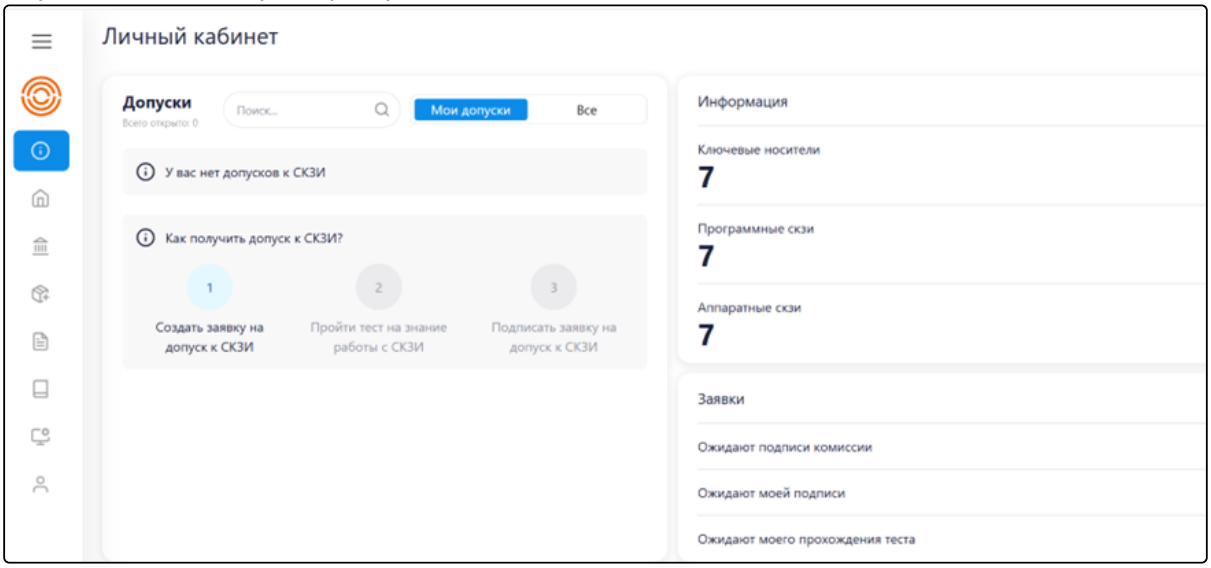


Рисунок 3 Главная страница портала СУУ СКЗИ

3.6 Подключение к демо-стенду через SSH

Для подключения к демо-стенду через SSH запросите учетные данные администратора у сотрудников технической поддержки.

Для подключения можно использовать стандартный SSH-клиент (OpenSSH), который вызывается через командную строку (cmd) для Windows или использовать стандартный терминал для Linux.

1. Введите команду для подключение к машине демо-стенда по SSH:

```
ssh min-miu.tst.itc.internal -l administrator
```

2. Согласитесь на добавление сервера в known_hosts, вписав в строке yes.

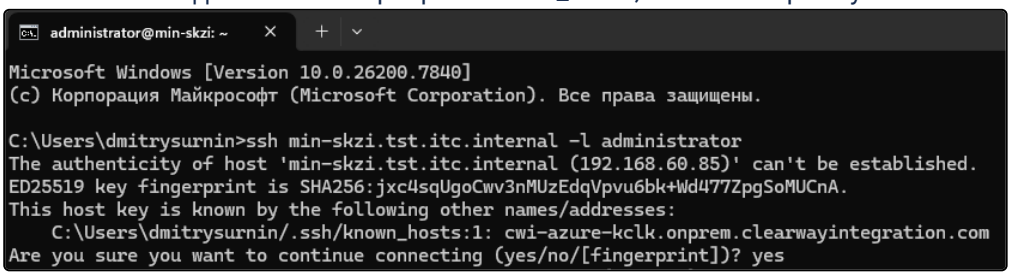


Рисунок 4 Добавление сервера в know_hosts

3. Введите пароль от учетной записи administrator.
4. При успешном подключении вы увидите информацию о предыдущем входе пользователя, а в начале строки появится имя пользователя и имя сервера.

Рисунок 5 Успешное подключение по ssh

4 Проверка работы ПО

4.1 Проверка создания Поставщика

1. В адресную строку введите ссылку https://min-skzi.tst.itc.internal и нажмите Enter.
2. В левом меню выберите пункт **Объекты учета**-> **Поставщик.**
3. В правом верхнем углу нажмите на кнопку **+.**
4. В открывшейся форме **Добавление нового поставщика** заполните поля:
   a. в поле **Название поставщика** впишите название поставщика
   b. в поле **ИНН** впишите номер ИНН поставщика
   c. в поле **ОГРН** впишите номер ОГРН поставщика
5. В правом верхнем углу формы **Добавление нового поставщика** нажмите на кнопку с изображением **Дискета (сохранить)** для сохранения карточки.
6. Ожидаемый результат: не должно быть ошибок.
7. В правом верхнем углу формы нажать на кнопку **X** (Закрыть).
8. Ожидаемый результат: карточка Поставщики отображается в списке.

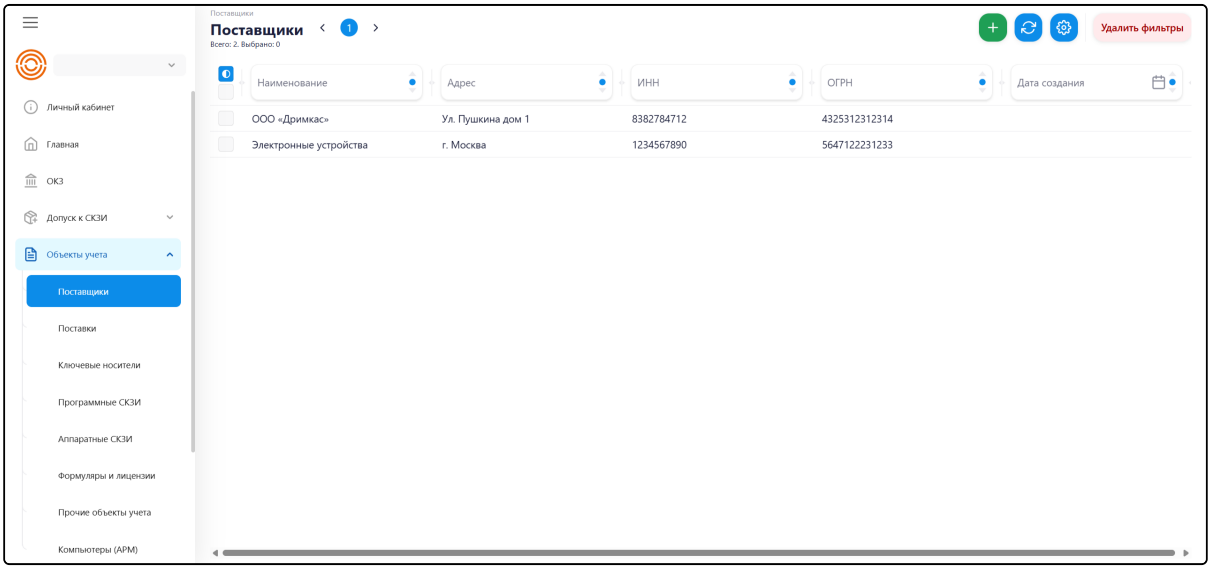


Рисунок 6 Карточка Поставщики

4.2 Проверка создания Поставки и пакета

4.2.1 Проверка создания Поставки

1. В адресную строку введите ссылку https://min-skzi.tst.itc.internal и нажмите Enter.
2. В левом меню выберите пункт **Объекты учета**-> **Поставки.**
3. В правом верхнем углу нажмите на кнопку **+.**

4. В открывшейся форме **Добавление поставки** заполните поля:
   a. в поле **Название поставки** впишите название
   b. в поле **Номер поставки** впишите номер
   c. в поле **Дата поставки** впишите дату
   d. в поле **Поставщик** выберите значение из списка
   e. в поле **Передаточный документ** впишите информацию о документе
   f. в поле **ОКЗ** выберите значение из списка
   g. в поле **Информировать об истечении за (в днях)** укажите число
5. В правом верхнем углу формы **Добавление поставки** нажмите на кнопку с изображением **Дискета (сохранить)** для сохранения карточки.
6. Ожидаемый результат: не должно быть ошибок.
7. В правом верхнем углу формы **Добавление поставки** нажать на кнопку **X** (Закрыть) и Подтвердить закрытие.
8. Ожидаемый результат: карточка Поставщики отображается в списке.

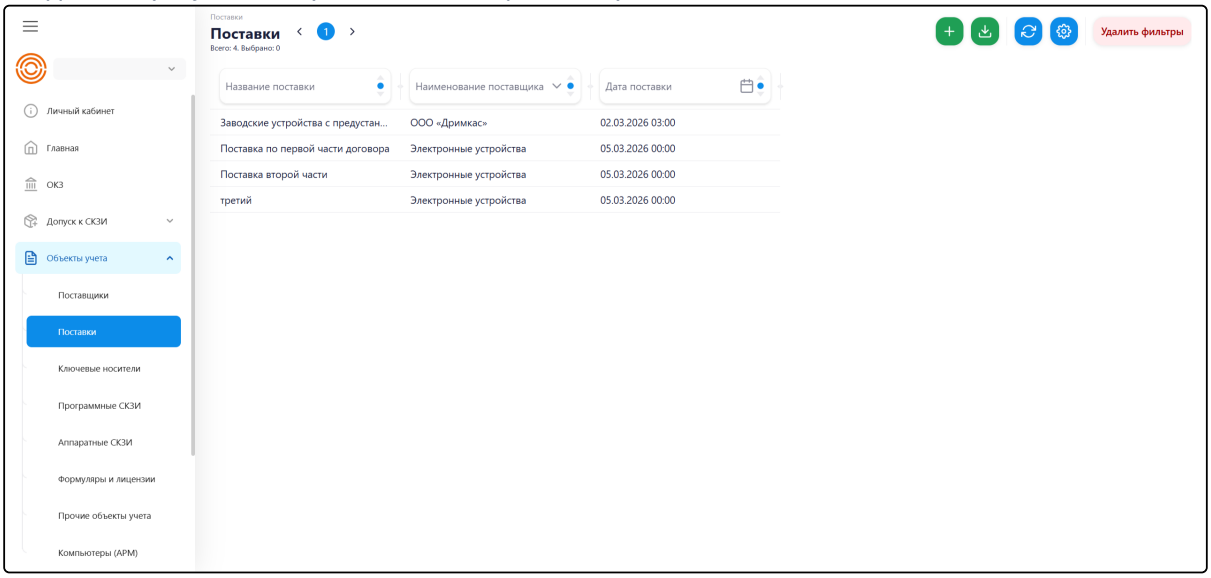


Рисунок 7 Карточка Поставки

4.2.2 Проверка создания пакета

1. В адресную строку введите ссылку https://min-skzi.tst.itc.internal и нажмите Enter.
2. Откройте в списке **Поставки** щелчком мыши требуемую поставку.
3. В открывшейся форме выберите вкладку **Пакеты.**
4. В открывшейся вкладке **Пакеты** нажмите на кнопку **Добавить.**
5. В открывшейся форме **Состав пакета** заполните поле:
   a. в поле **Наименование** впишите название пакета
6. В правом верхнем углу формы **Состав пакета** нажмите на кнопку с изображением **Дискета (сохранить)** для сохранения карточки.
7. Ожидаемый результат: не должно быть ошибок.

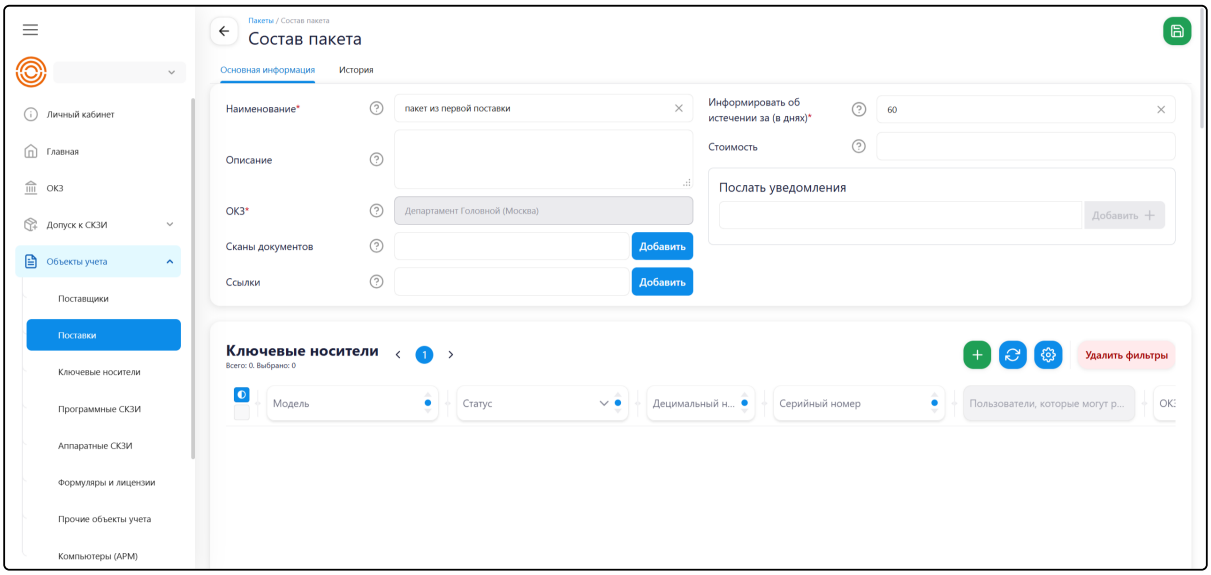


Рисунок 8 Карточка Состав пакета

4.3 Проверка создания ключевого носителя

1. В адресную строку введите ссылку https://min-skzi.tst.itc.internal и нажмите Enter.
2. В левом меню выберите пункт **Объекты учета**-> **Ключевые носители**.
3. В правом верхнем углу нажмите на кнопку **+.**
4. В открывшейся форме **Новый ключевой носитель** заполните поля:
   a. в поле **Модель** впишите модель ключевого носителя
   b. в поле **Серийный номер** впишите значение серийного номера
   c. в поле **Тип ключевого носителя** выберите значение из списка
   d. в поле **Подтип ключевого носителя** выберите значение из списка
   e. в поле **ОКЗ** выберите значение из списка
   f. в поле **Поставка** выберите значение из списка
   g. в поле **Пакет** выберите значение из списка
5. В правом верхнем углу формы **Новый ключевой носитель** нажмите на кнопку с изображением **Дискета (сохранить)** для сохранения карточки.
6. Ожидаемый результат: карточка Ключевые носители должна отобразиться в списке. Не должно быть ошибок.

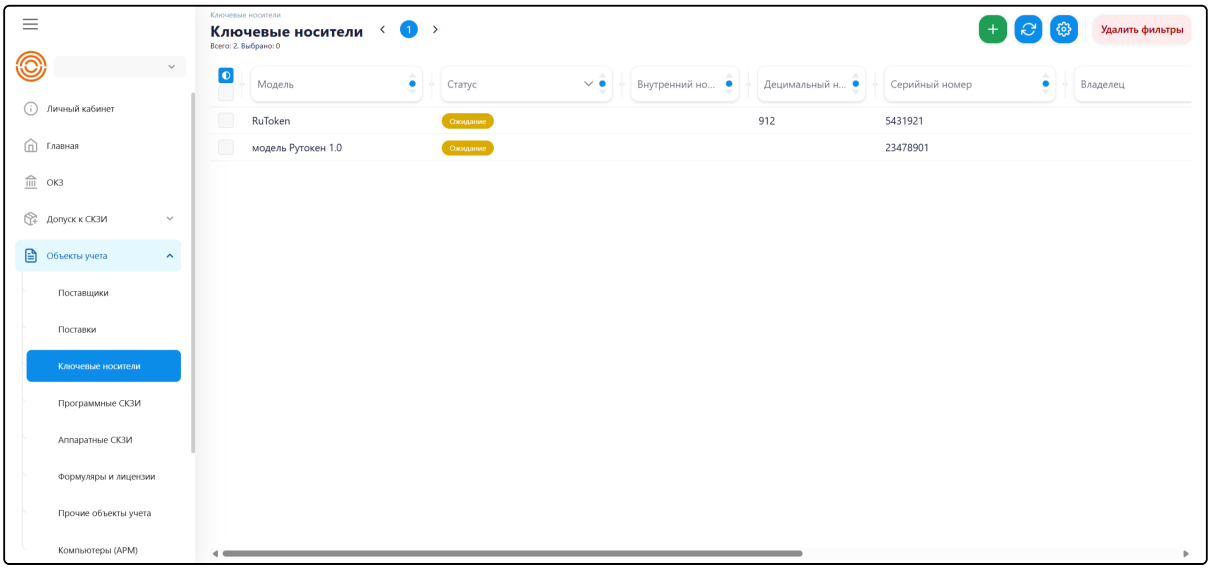


Рисунок 9 Карточка Ключевые носители

4.4 Проверка статуса сервисов

Для проверки статуса сервисов запросите учетные данные администратора у сотрудников технической поддержки.

1. Авторизуйтесь по ssh:

```
ssh min-skzi.tst.itc.internal -l administrator
```

2. Перейдите в контекст пользователя:

```
sudo -su itc-svc
```

3. Проверьте статус работы сервисов командой:

```
systemctl list-units --user --type=service
```

4. Ожидаемый результат: отображает 9 запущенных сервисов (itcagentd.service - failed - актуальный установлен под root и не виден данной командой) со статусом Active: active (running). ПО запущено и функционирует.

```
itc-svc@min-skzi:/home/administrator$ systemctl list-units --user --type=service
  UNIT                                LOAD   ACTIVE SUB     DESCRIPTION
  itc.api.appstore.service            loaded active running ITC.Api.AppStore
  itc.api.collreg.service             loaded active running ITC.Api.Collreg
  itc.api.edusurvey.service           loaded active running itc.api.edusurvey
  itc.api.scriptlauncher.service      loaded active running itc.api.scriptlauncher
  itc.api.skzi.controlpanel.service loaded active running itc.api.skzi.controlpanel
  itc.api.skzi.service                loaded active running itc.api.skzi
● itcagentd.service                   loaded failed failed  itcagentd
  itcdispd.service                    loaded active running itcdispd
  itcmsgd.service                     loaded active running itcmsgd
  itcsrvd.service                     loaded active running itcsrvd

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.
10 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
```

Рисунок 10 Запущенные службы СКЗИ

5 Самостоятельная установка

5.1 Системные требования

Подробный набор требований для развертывания системы содержится в документе «Описание технической архитектуры программного обеспечения» в разделе «Физическая архитектура».

5.2 Инструкции по установке

Подробные инструкции для развертывания компонентов системы содержатся в документе «Руководство администратора».