Центр
Управления
Гетерогенными
Инфраструктурами

ЛКПС. Инструкция по запуску продукта в демо-зоне

ООО «Клируэй Текнолоджис»

2026

Оглавление

1 Введение

Настоящий документ содержит информацию о процессе установки системы «Личного Кабинета Пользователя Сертификатов» (ЛКПС), 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 ЛКПС, 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 ЛКПС	min-audit	L9qsXUTwJAa8fdP

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 ЛКПС: https://min-lk.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.

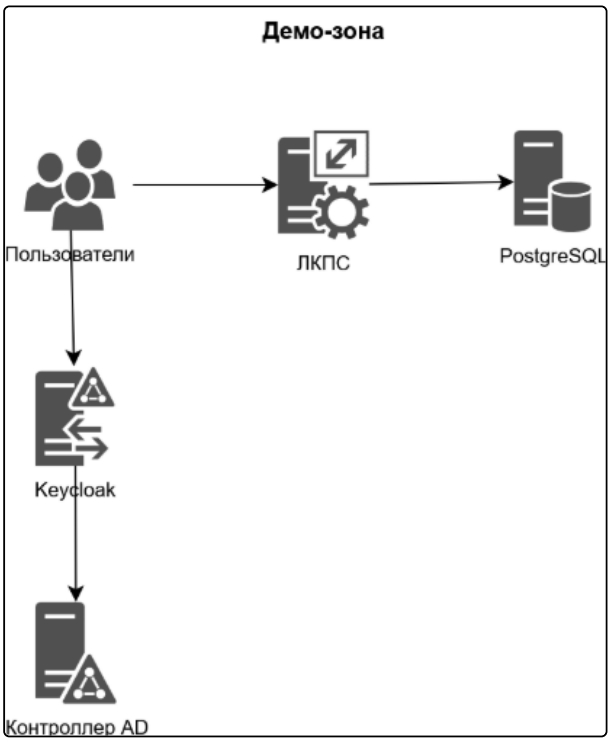


Рисунок 1 Схема компонентов ЛКПС

1. Хост min-lk.tst.itc.internal - на этом хосте установлены сервисы ЛКПС:

	Имя сервиса	Назначение
1	nginx	Web-сервер, реверс-прокси, балансировщик
2	ITC.Archiver	Сервис хранения архивных данных

	Имя сервиса	Назначение
3	ITC.Api.CertRkMon	Микросервис отслеживания отозванных сертификатов
4	ITC.Api.ContactBook	Сервис контактов пользователей
5	ITC.Api.CommonCore	Основной сервис Платформы
6	ITC.Api.Cpa.ControlPanel	Графический интерфейс ЛКПС
7	ITC.Api.Cpa	Сервис ЛКПС
8	ITC.Api.Isc	Сервис информационных систем
9	ITC.Api.MailOutbox	Отправка почтовых уведомлений
10	ITC.Api.Cpa.Workers	Сервис воркеров ЛКПС

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:

itc_cpa
itc_cpa_archiver
itc_cpa_certrkmon
itc_cpa_contact_book
itc_cpa_isc
itc_cpa_mailoutbox

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.

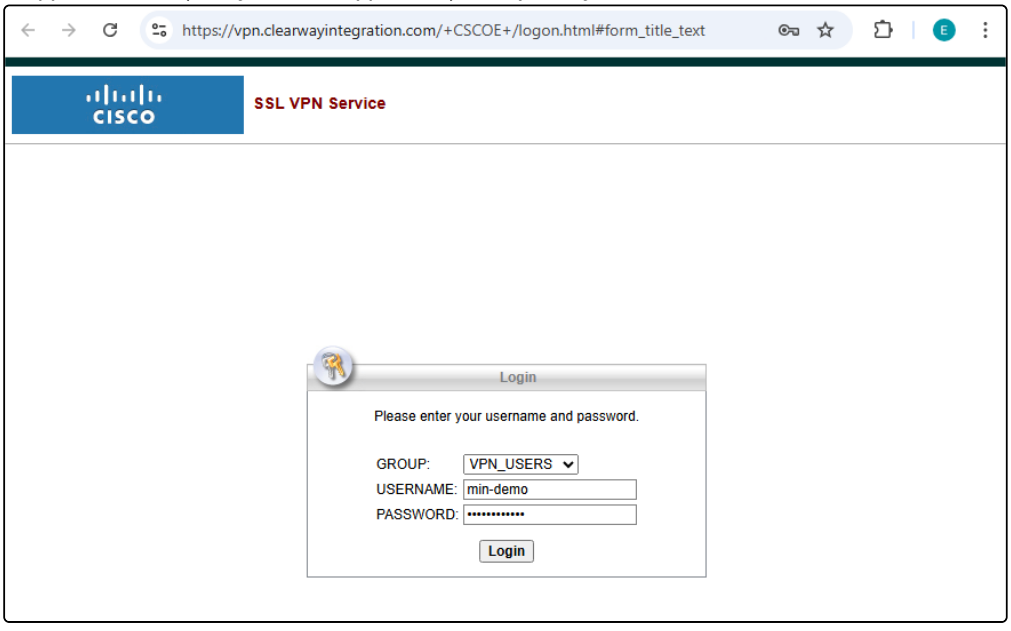
Перед началом установки убедитесь, что:

- 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.

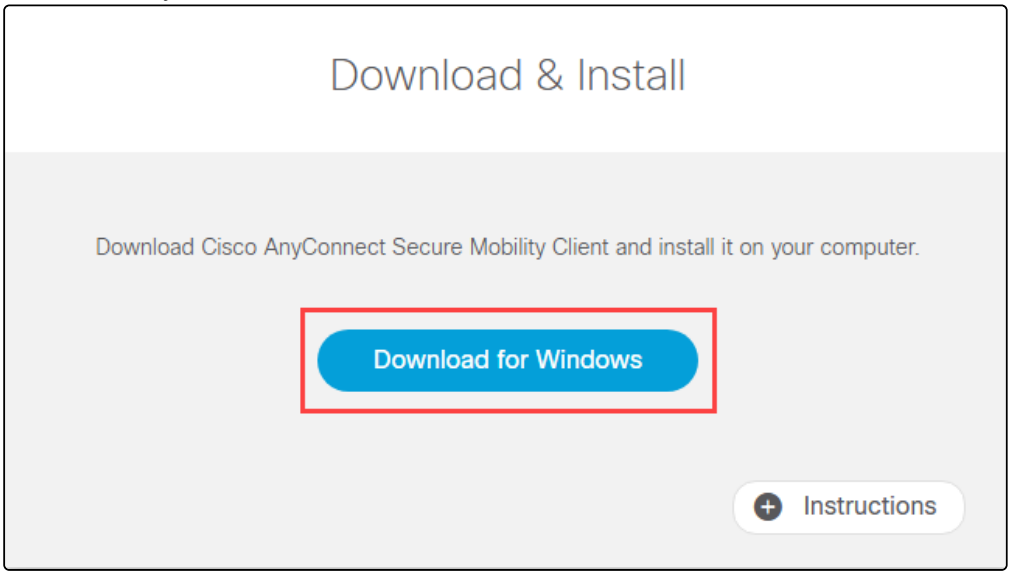
3.4.1.1 Первоначальная установка VPN-клиента

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.

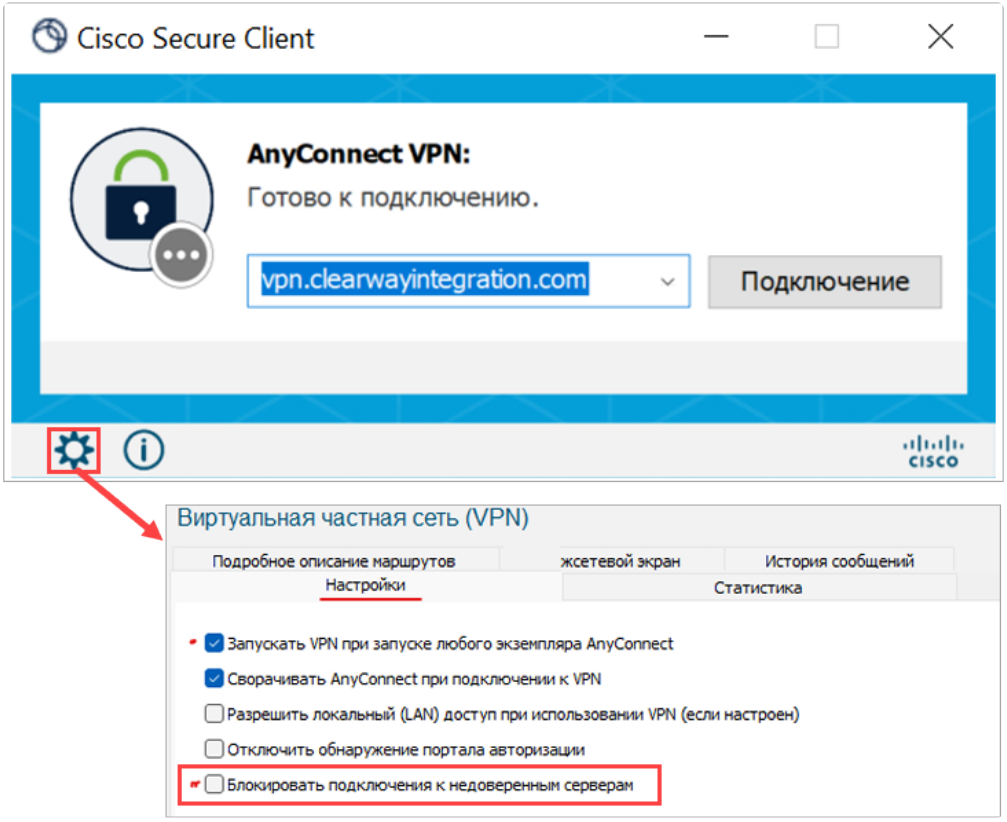


2. После успешной авторизации откроется окно с кнопкой для скачивания дистрибутива AnyConnect Secure Mobility Client.



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

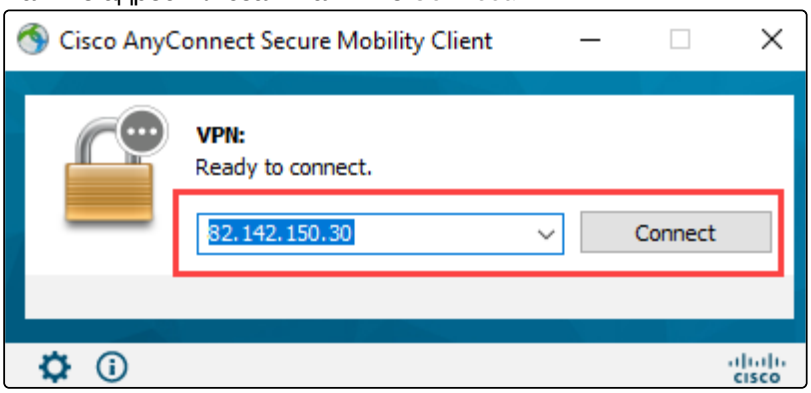
3. Скачайте и установите Cisco AnyConnect, следуя указаниям мастера установки.
4. Запустите клиент Cisco AnyConnect.
5. Откройте настройки (значок шестеренки) и снимите флажок "Блокировать подключения к недоверенным серверам", затем закройте окно настроек.



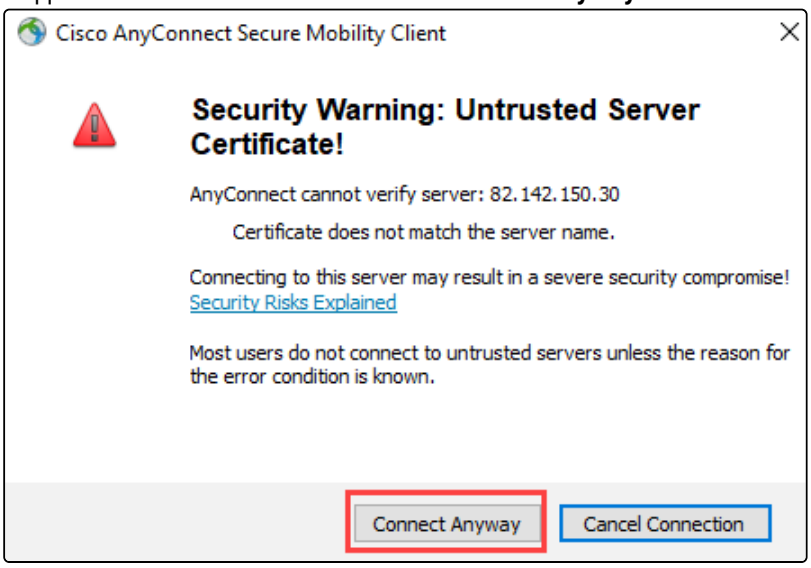
3.4.1.2 Авторизация по VPN

Для подключения к VPN выполните следующие действия.

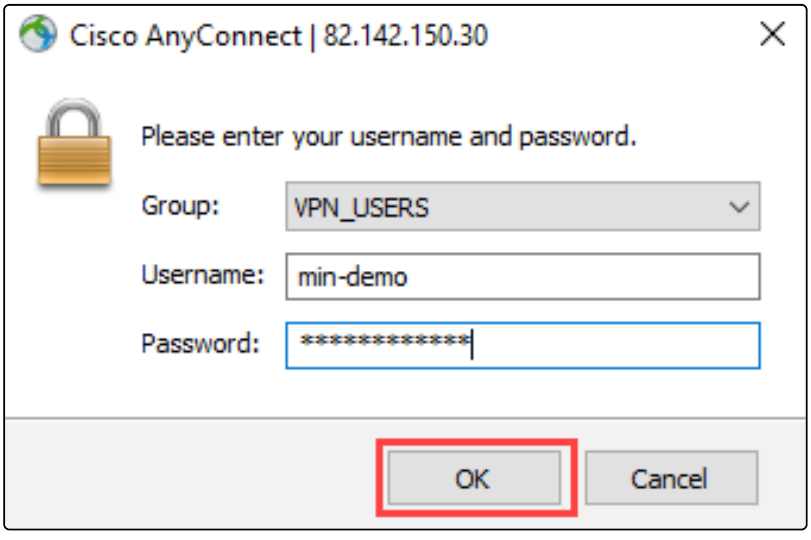
1. Запустите VPN-клиент Cisco AnyConnect.
2. Укажите адрес шлюза и нажмите **Connect**.



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**.

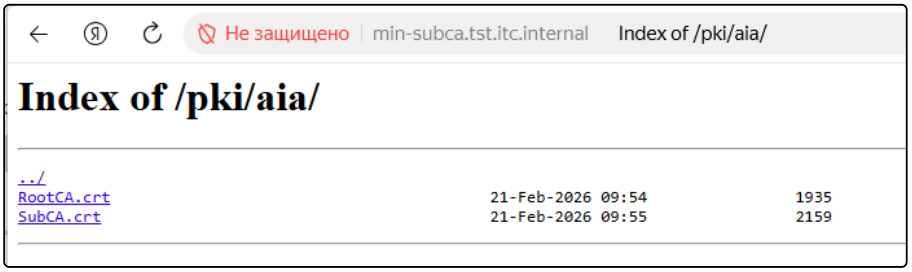


4. Укажите логин и пароль учетной записи VPN-клиента, в поле "Группа" выберите "VPN_USERS".
5. Нажмите кнопку **OK**.



3.4.2 Добавление сертификатов в доверенные

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

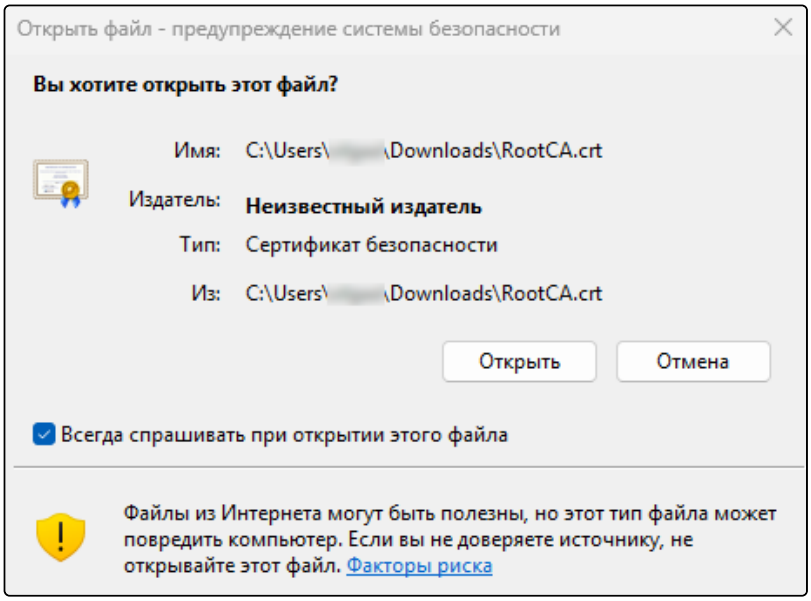


2. Скачайте на компьютер файлы сертификатов *RootCA.crt* и *SubCA.crt*.
3. Перейдите в директорию, куда вы сохранили файлы сертификатов.
4. Добавьте сертификаты, как описано ниже.
5. После добавления сертификатов закройте и заново откройте браузер, чтобы он подхватил новые сертификаты.

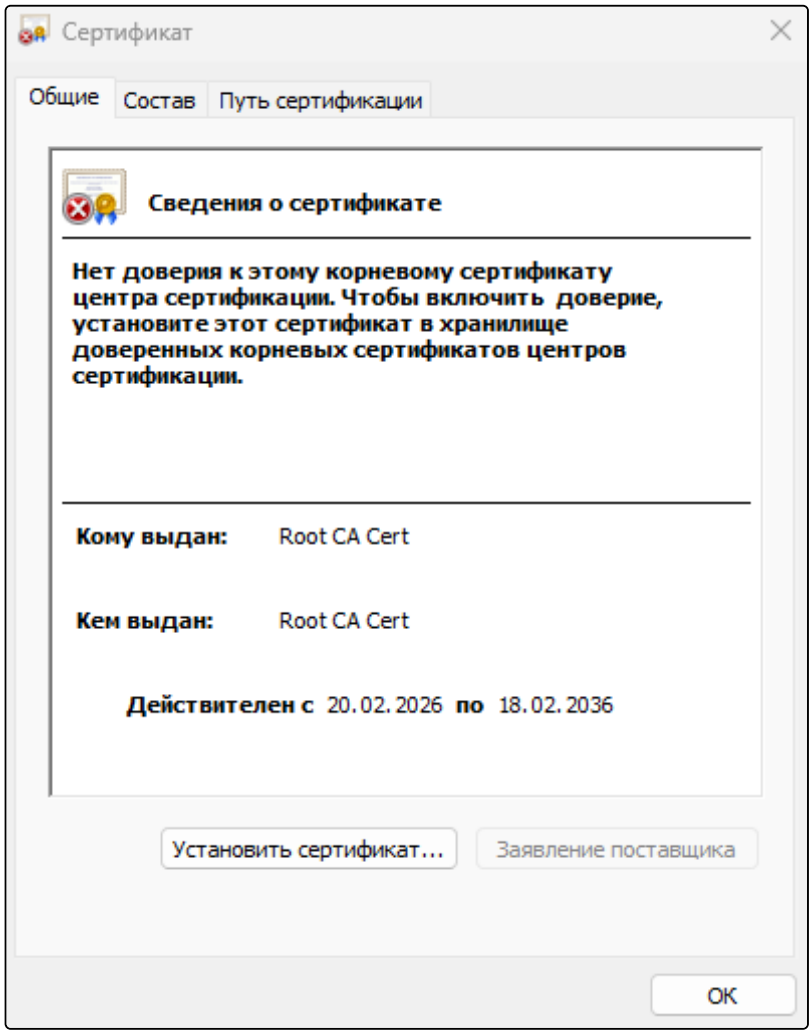
3.4.2.1 Добавление сертификатов для ОС Windows

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

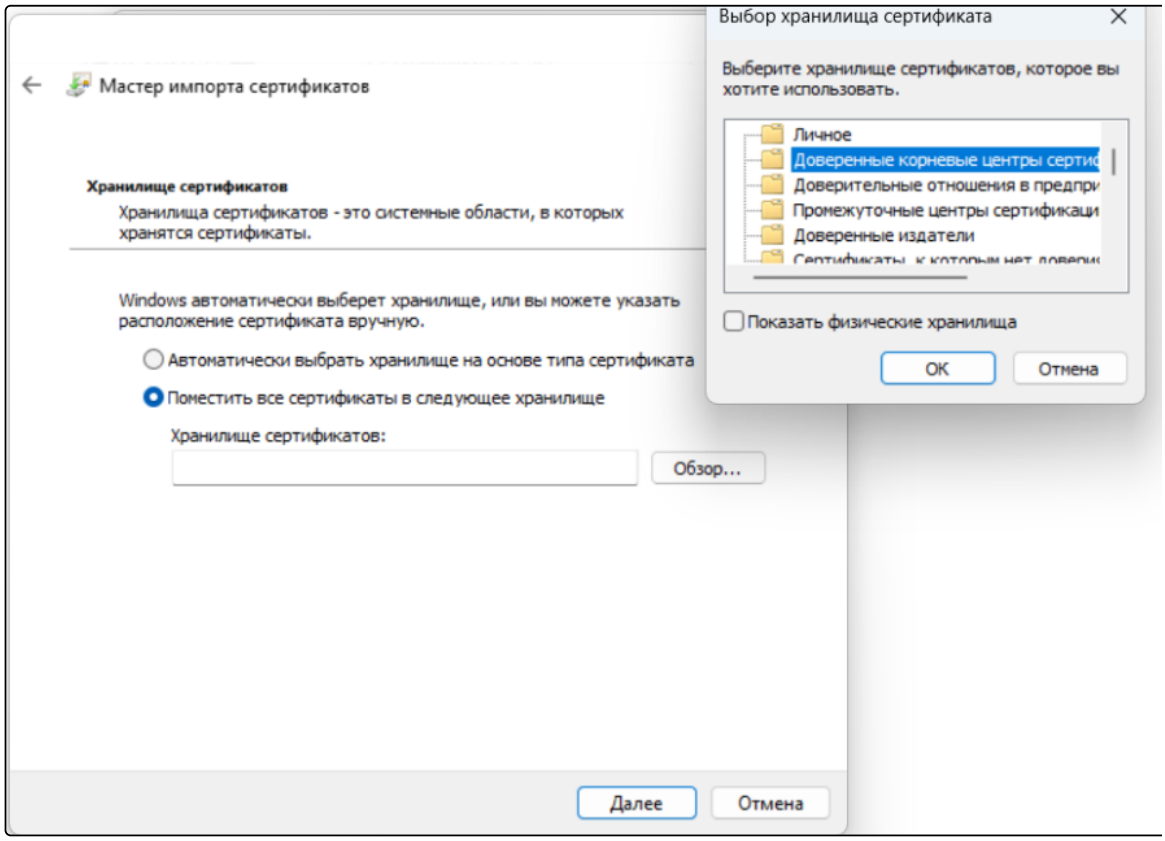
   a. Дважды нажмите на имя файла *RootCA.crt*, а затем в окне предупреждения системы безопасности нажмите **Открыть**.



   b. Нажмите **Установить сертификат**.



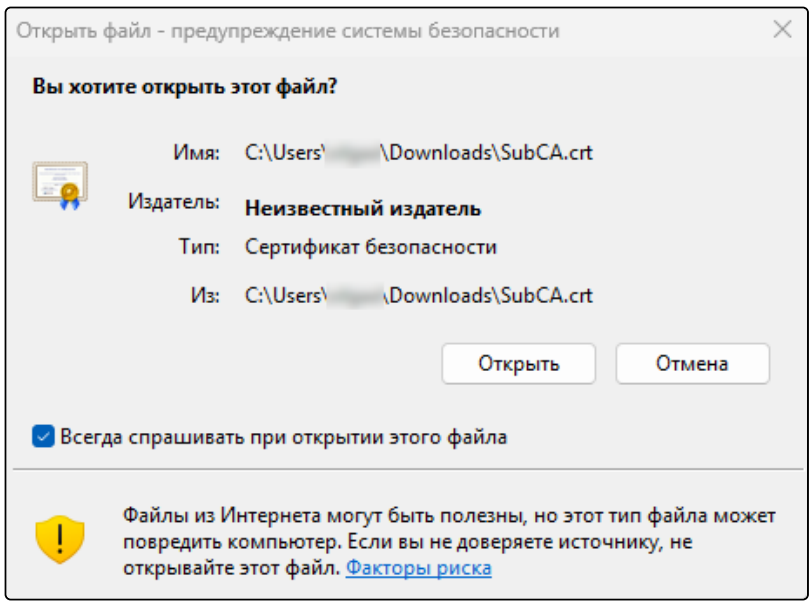
c. Нажмите **Далее**, выберите пункты, как показано на рисунке ниже. Затем нажмите **Далее**.



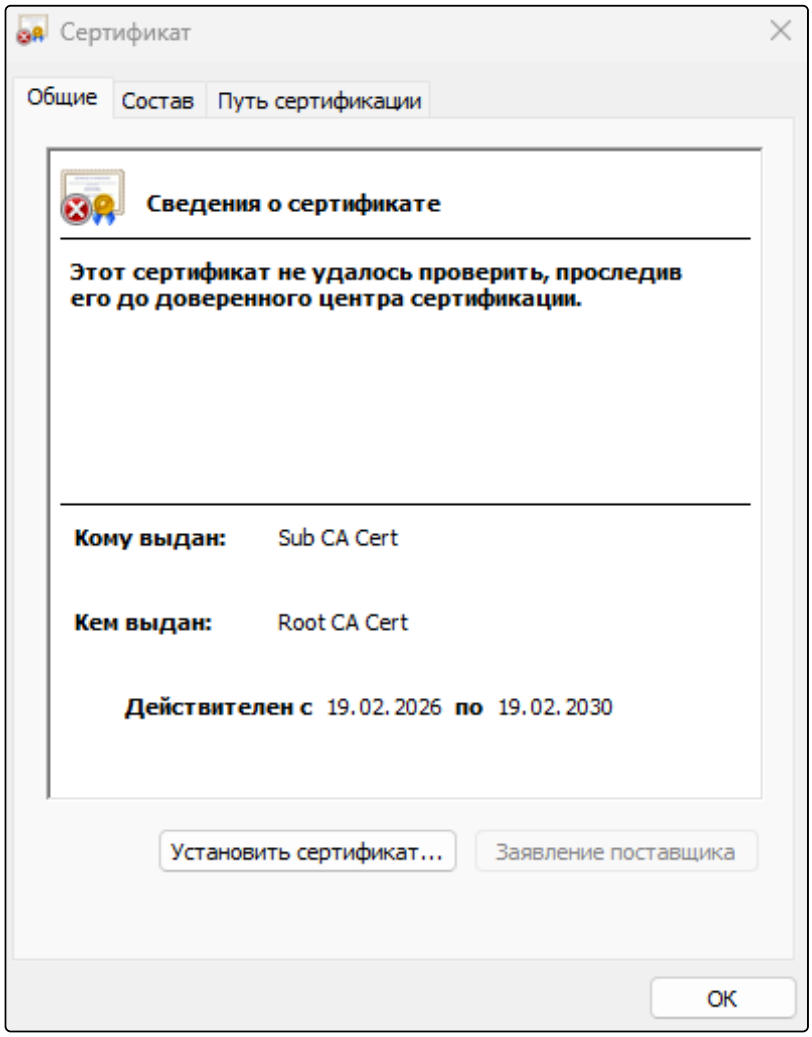
d. Нажмите **Готово**, а затем в окне предупреждения системы безопасности нажмите **Да**.

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

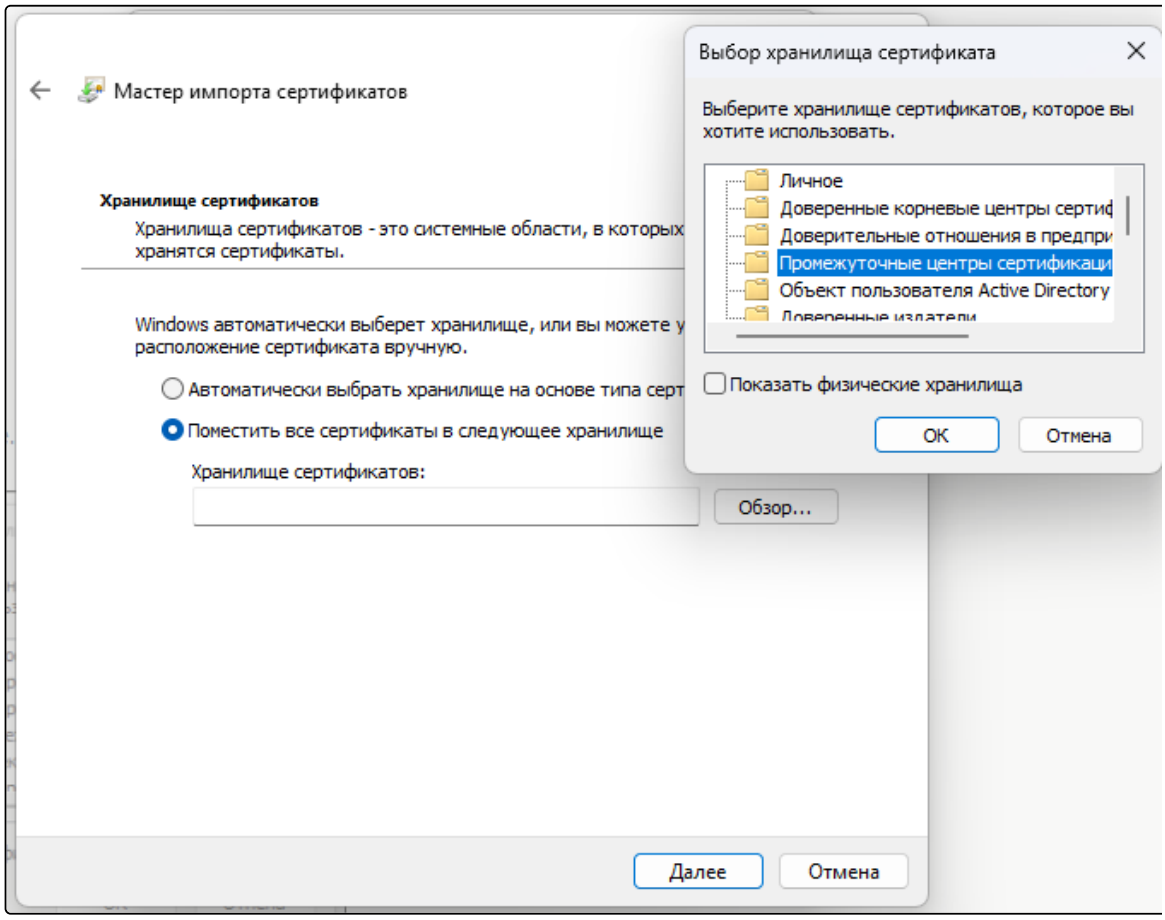
a. Дважды нажмите на имя файла *SubCA.crt*, а затем в окне предупреждения системы безопасности нажмите **Открыть**.



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 следующую ссылку https://min-lk.tst.itc.internal и нажмите **Enter.**
3. В появившемся окне входа заполните соответствующие поля, используя данные из таблицы Учетные записи.

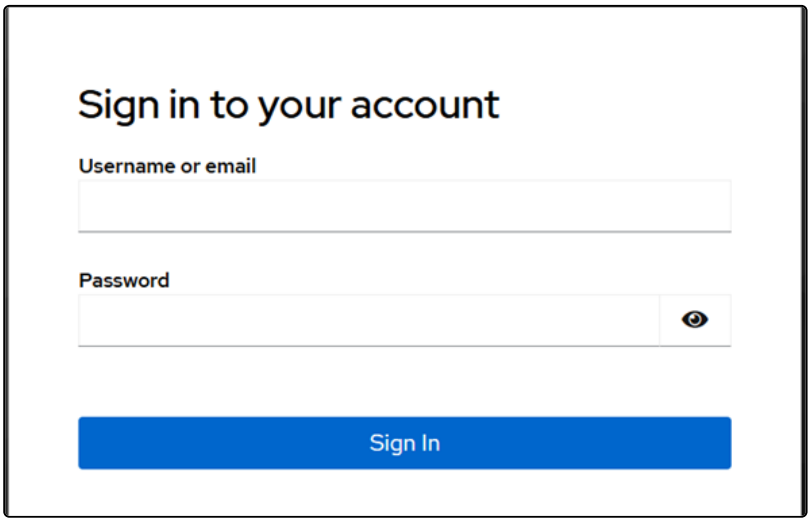


Рисунок 2 Окно входа

4. После ввода данных нажмите кнопку входа для доступа к главной странице системы. Откроется Главная страница портала ЛКПС:

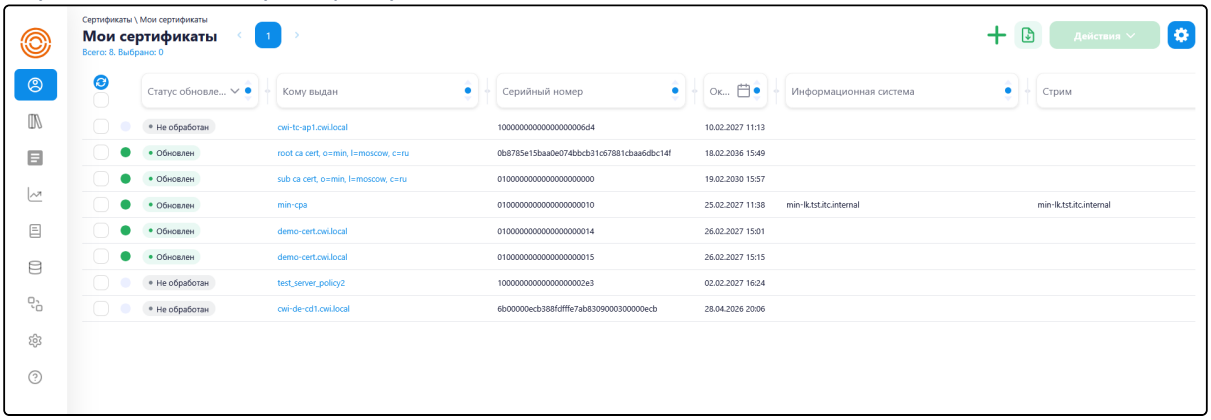


Рисунок 3 Главная страница портала ЛКПС

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-lk.tst.itc.internal -l administrator
```

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

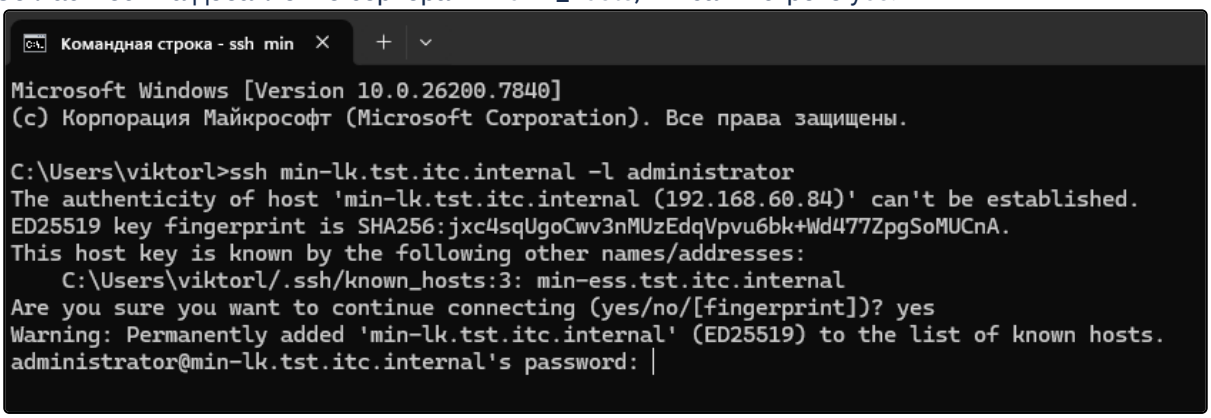


Рисунок 4 Добавление сервера в know_hosts

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 Импорт сертификатов в ЛКПС

Для выполнения данной проверки, потребуется сертификат. Можете использовать свой сертификат или воспользоваться данным сертификатом для теста:

```
-----BEGIN CERTIFICATE-----
MIIEtTCCA52gAwIBAgILEAAAAAAAAAAAAYMwDQYJKoZIhvcNAQELBQAwgZYxCzAJ
BgNVBAYTAlJVMQ8wDQYDVQQIDAZNb3Njb3cxHTAbBgNVBAoMFENsZWFyd2F5IElu
dGVncmF0aW9uMRowGAYDVQQLDBFJVEMtTUNBMS1JbnRlcm5hbDEaMBgGA1UEAwwR
SVRDLU1DQTEtSW50ZXJuYWwxHzAdBgkqhkiG9w0BCQEWEHNzbEBpdGMuaW50ZXJu
YWwwHhcNMjYwMTEwMTAyMjI4WhcNMjcwMTEwMTEyMjI4WjAsMSowKAYDVQQDEyFr
bm93bGVkZ2UuY2xlYXJ3YXlpbnRlZ3JhdGlvbi5jb20wggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDfcxEfZD23RFUFFhNL1O06T7foxhLNmdJrU2JjAwfh
N+ph3OtLZA2EIkFvfjBX++Ak3rt/Kkky+ZPKBTIWM34tji8aqhOsB8IAYTWZ4CFJ
KFQA6NmWaiWQN6KqSEXLoVkNaF6T93d5O1ayxJIstHiuaa4F5LBl2X4fw2P/MQqk
xac6O72z/Sv/s5JxhnAwG7dKvrF7NPxEezNF1b4IevyLU2IlYbWWymrb9Z/fxQGI
QYzOck5rAIe/MrT1fV89lNoaQjDFq/TZMx8AxkgHQTOVUrdJOv0Ftg9B3AInfkMC
OOPPdpgUPfte7zAeXr19JC/85cBfbQdJDB5P4wUqokGvAgMBAAGjggFrMIIBZzAO
BgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB0G
A1UdDgQWBBRcxv9054cNWDjGcdV5n8ElqYrzezAfBgNVHSMEGDAWgBSrsDgaitBG
yf2icV1+kUtA0MWK4zBOBgNVHR8ERzBFMEOgQaA/hj1odHRwOi8vaXRjLWVzYXUt
YjEuaXRjLmludGVybmFsL3BraS9jZHAvaXRjLWludGVybmFsLW1jYTEuY3JsMFkG
CCsGAQUFBwEBBE0wSzBJBggrBgEFBQcwAoY9aHR0cDovL2l0Yy1lc2F1LWIxLml0
Yy5pbnRlcm5hbC9wa2kvYWlhL2l0Yy1pbnRlcm5hbC1tY2ExLmNydDBLBgNVHREE
RDBCgiFrbm93bGVkZ2UuY2xlYXJ3YXlpbnRlZ3JhdGlvbi5jb22CHWtub3dsZWRn
ZS5sYWIuaXRjLmludGVybmFsZGV2MA0GCSqGSIb3DQEBCwUAA4IBAQCdEWsq/YqD
2twhgDdbzpC5kU5gj/Rxuuw02ysZJXZ4Vme25jkPv7QwG39v5vv3RnLCZCOgk7rE
OHDXp/+kHZ2RKcG6+suyMfxwrjHt1CCv8+3kTDl0E9V9cj/g2aA64SgRCYHhnlMj
PY5B64xGK/yFjGrr1Z9LB3Q155vabqOSqFQ3ewURwSKSIoYQTNNhrt8+9/RFSFRI
GFlkJvyLXv+cgxf4xEHBZfTXXnoGYzpObJxhyqfdg8ntKrpFGcSjK5gOmJq51Kav
OW1qdtnGigu3MzsRxYYj1AElZhLO4HDBfXJfufQipcU10s0SF/Ht6Lk2B9xrJTRV
SaJ9umdlQVXu
-----END CERTIFICATE-----
```

1. В адресную строку введите ссылку https://min-lk.tst.itc.internal и нажмите Enter.
2. Перейдите в **Мои сертификаты** и нажмите кнопку **Добавить сертификат**. Откроется модальное окно для импорта сертификата.

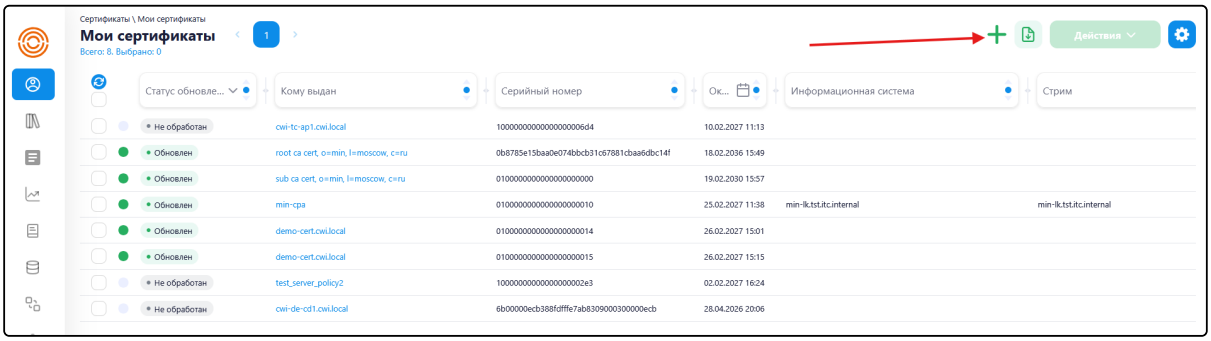


Рисунок 6 Расположение кнопки "Добавить сертификат"

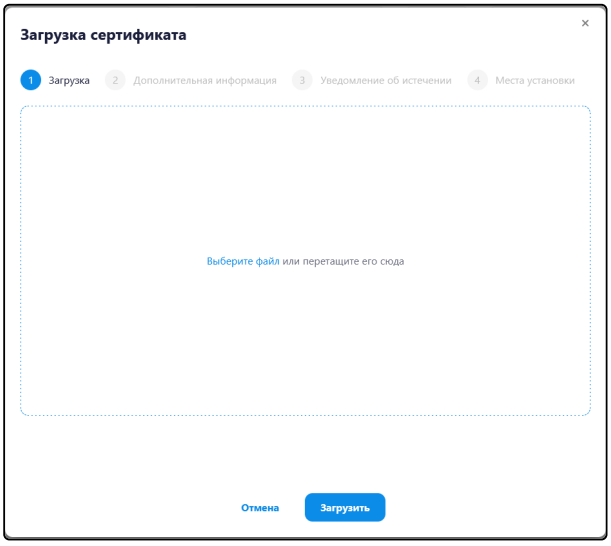


Рисунок 7 Модальное окно для импорта сертификатов

3. Перетащите или выберите файл сертификата в модальном окне и нажмите **Загрузить**. Будет выполнен переход к шагу 2.

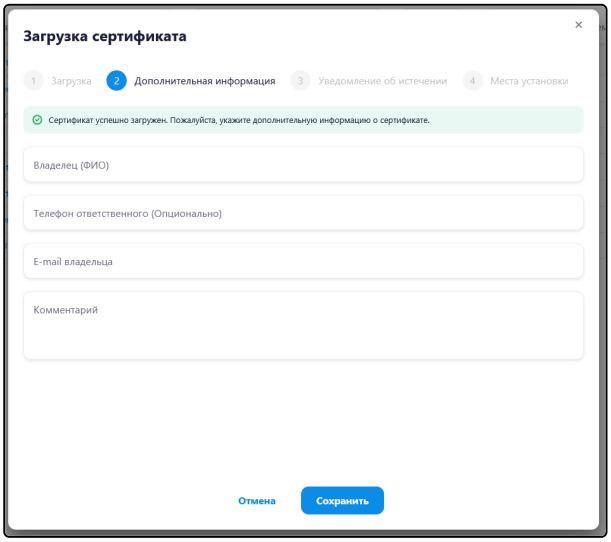


Рисунок 8 Шаг 2

4. Заполните обязательные поля валидными значениями и нажмите **Сохранить**. Будет выполнен переход к шагу 3.

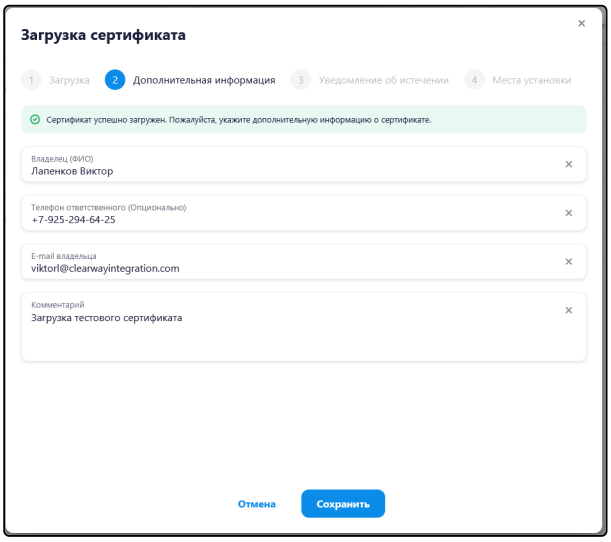


Рисунок 9 Загрузка сертификата (сохранение)

5. При необходимости измените дефолтное значение и нажмите кнопку **Подтвердить.** Будет выполнен переход к шагу 4.

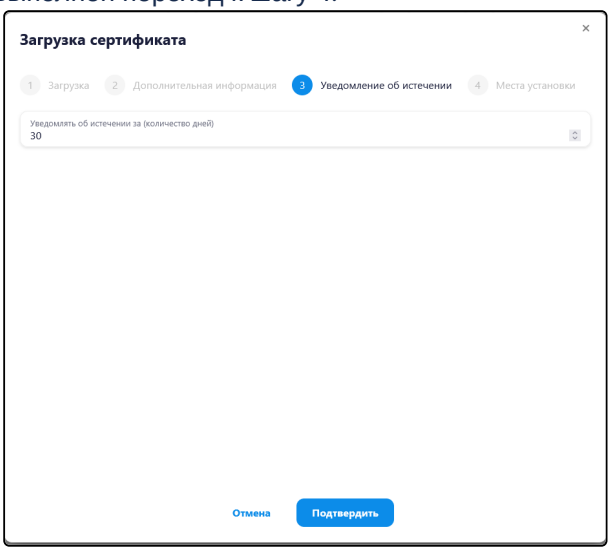


Рисунок 10 Загрузка сертификата (подтверждение)

6. Нажмите кнопку **Добавить место установки**. Откроется модальное окно, с выбором нового места установки. Введите в input валидное значение и нажмите **Подтвердить.**

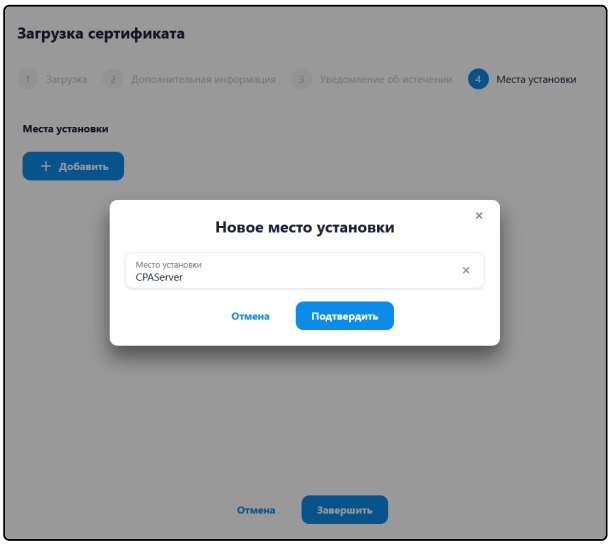


Рисунок 11 Загрузка сертификата (добавление места установки)

7. Нажмите кнопку **Завершить**, для завершения импорта. Произойдет переход в карточку добавленного сертификата.

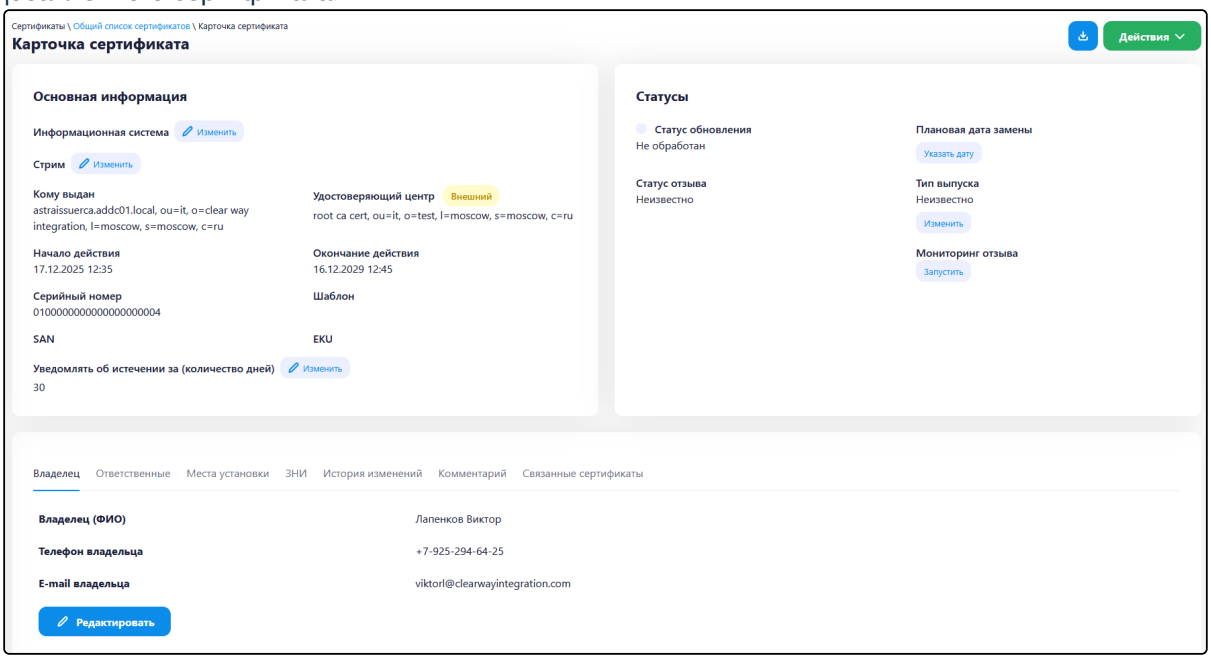


Рисунок 12 Карточка сертификата

4.2 Список моих сертификатов

Необходимо удостовериться, что реализован список **Мои сертификаты** (список сертификатов, по которым пользователь является ответственным).

1. В адресную строку введите ссылку https://min-lk.tst.itc.internal и нажмите Enter.
2. Перейдите в **Мои сертификаты** и проверьте, что выполнен переход на страницу. Должна открыться страница Мои сертификаты.

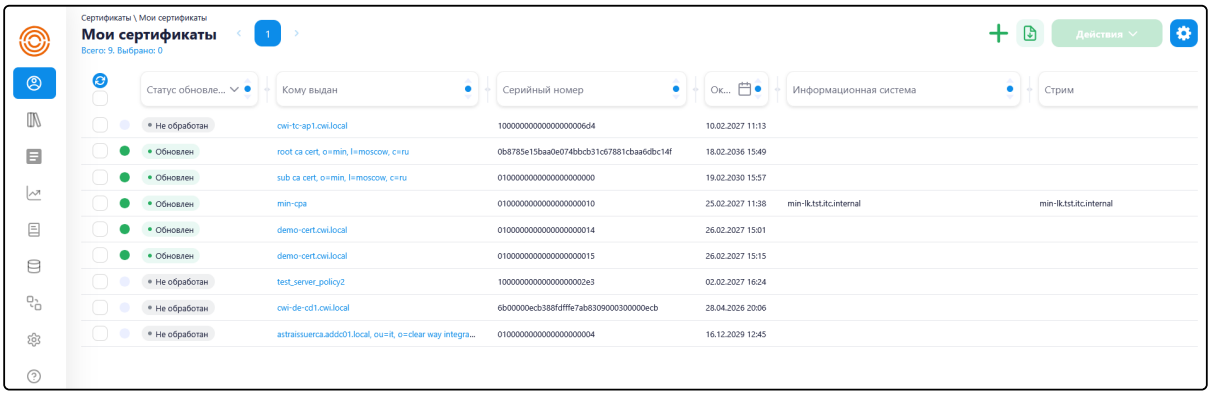


Рисунок 13 Страница "Мои сертификаты"

3. Зайдите в карточку сертификата и проверьте являетесь ли вы ответственными за данный сертификат.

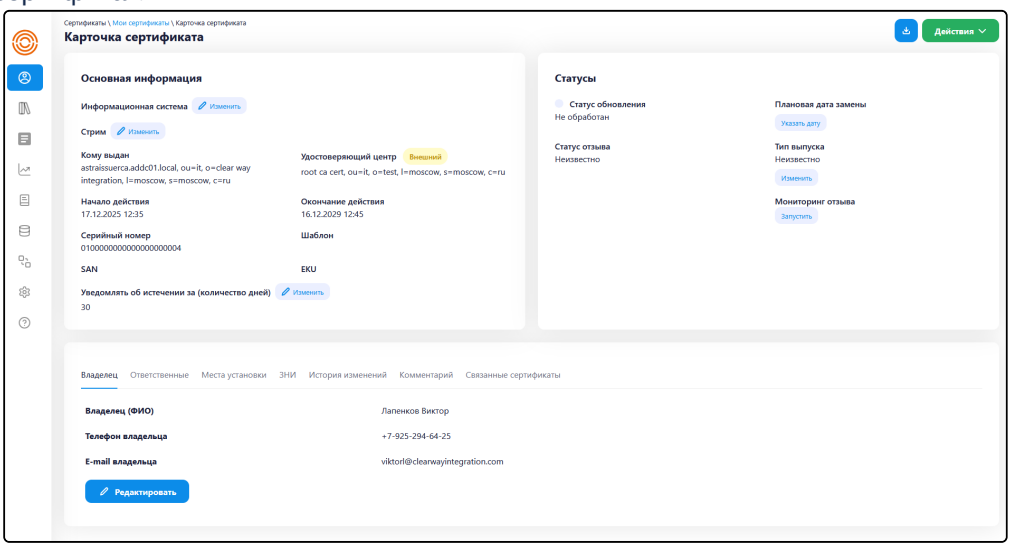


Рисунок 14 Проверка на ответственность за сертификат

4. Измените активную вкладку на **Ответственные**.

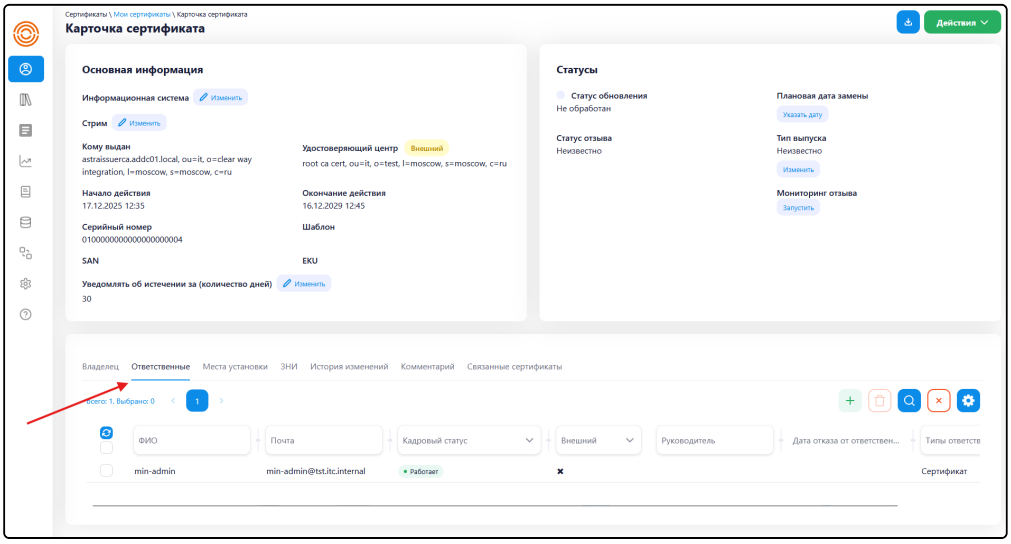


Рисунок 15 Вкладка "Ответственные"

5. Убедитесь, что пользователь является ответственным за сертификат.

4.3 Отчет по неклассифицированным сертификатам

1. В адресную строку введите ссылку https://min-lk.tst.itc.internal и нажмите Enter.
2. Перейдите во вкладку **Общий список сертификатов**.

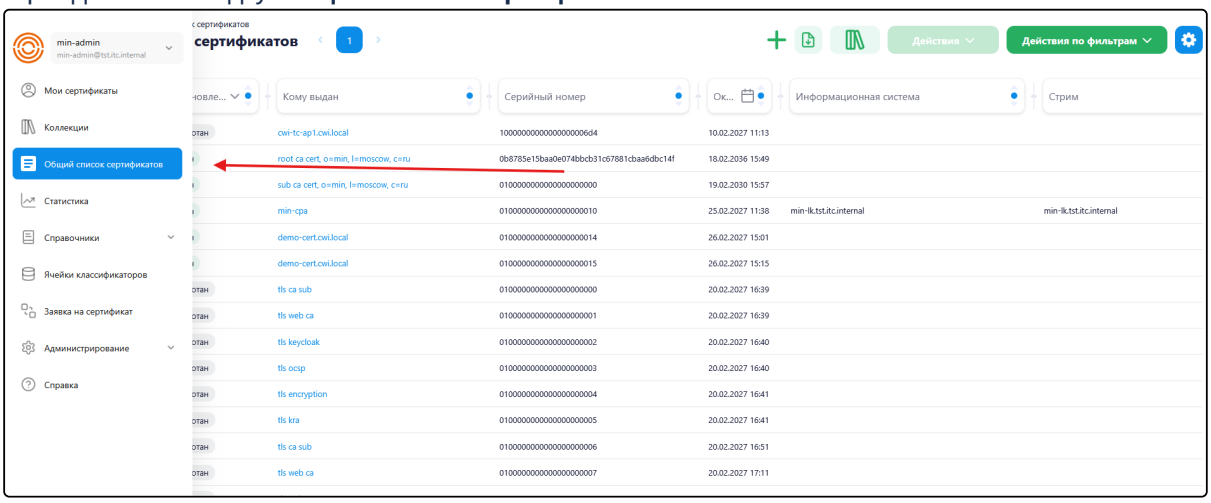


Рисунок 16 Вкладка "Общий список сертификатов"

3. В фильтрах найдите столбец **Ответственность за сертификат.**

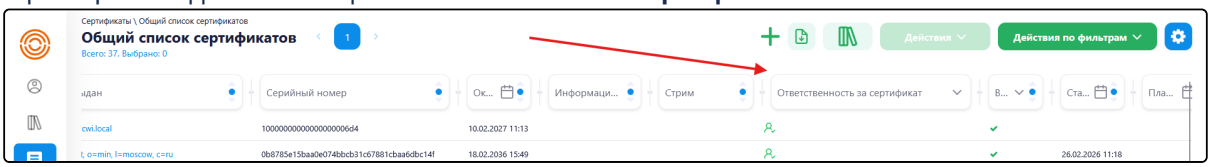


Рисунок 17 Ответственность за сертификат

4. В ниспадающем меню выберите **Никто не является ответственным**. В списке сертификатов должны остаться только сертификаты без ответственных.

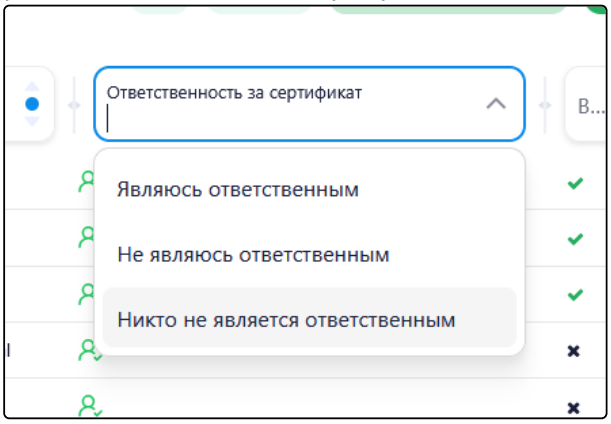


Рисунок 18 Выбор "Никто не является ответственным"

5. Нажмите кнопку выгрузки отчета. Дождитесь окончания скачивания отчета.

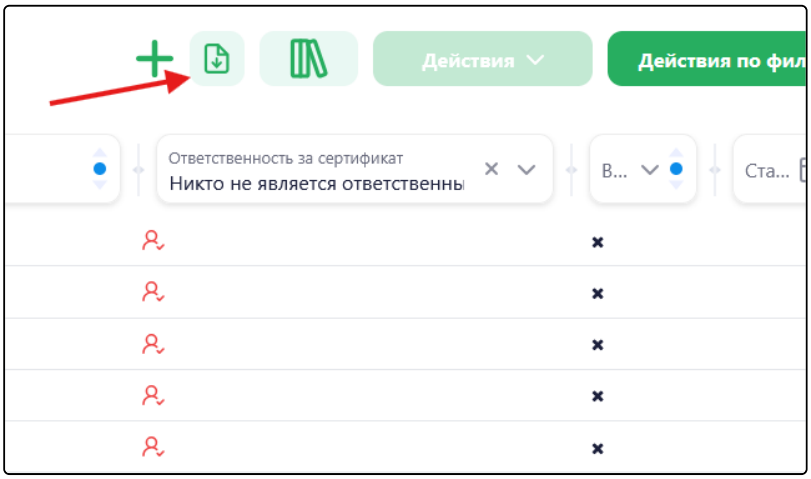


Рисунок 19 Кнопка "Выгрузка отчета"

6. Откройте скачанный отчет.

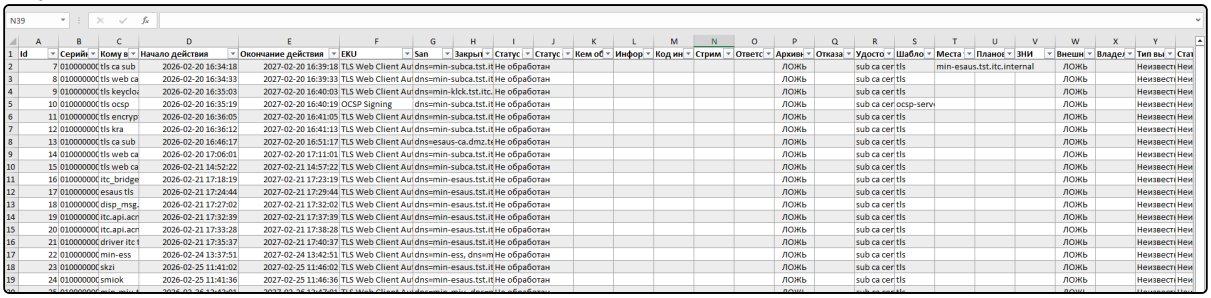


Рисунок 20 Отчет по сертификатам, у которых нет ни одного ответственного

4.4 Проверка статуса сервисов

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

1. Авторизуйтесь по ssh:

```
ssh min-lk.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 22 запущенных сервиса со статусом Active: active (running). ПО запущено и функционирует.

```
itc-svc@min-lk:/home/administrator$ systemctl list-units --user --type=service
  UNIT                           LOAD   ACTIVE SUB     DESCRIPTION
  itc.archiver.service           loaded active running itc.archiver
  itc.certrkmon.service          loaded active running itc.certrkmon
  itc.contactBook.service        loaded active running itc.contactBook
  itc.core.service               loaded active running itc.core
  itc.cpa.controlPanel.service loaded active running itc.cpa.controlPanel
  itc.cpa.service                loaded active running itc.cpa
  itc.cpa.workers.service        loaded active running itc.cpa.workers
  itc.isc.service                loaded active running itc.isc
  itc.mailoutbox.service         loaded active running itc.mailoutbox

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.
9 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
itc-svc@min-lk:/home/administrator$
```

Рисунок 21 Запущенные службы ЛКПС

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 запросите у сотрудников технической поддержки.