Центр
Управления
Гетерогенными
Инфраструктурами

ЕСАУС. Инструкция по запуску продукта в демо-зоне

ООО «Клируэй Текнолоджис»

2026

Оглавление

1 Введение

Настоящий документ содержит информацию о процессе установки «Единой Системы Автоматизированного Управления Сертификатами» (ЕСАУС) 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 ЕСАУС, сервер PostgreSQL, сервер Active Directory, выдающий и корневой ЦС (Clearway CA). 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 ЕСАУС	min-client	WydR5WG65s91f4l
3		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 ЕСАУС: https://min-esaus.tst.itc.internal.

3.3 Схема развертывания компонентов продукта на демо-стенде

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

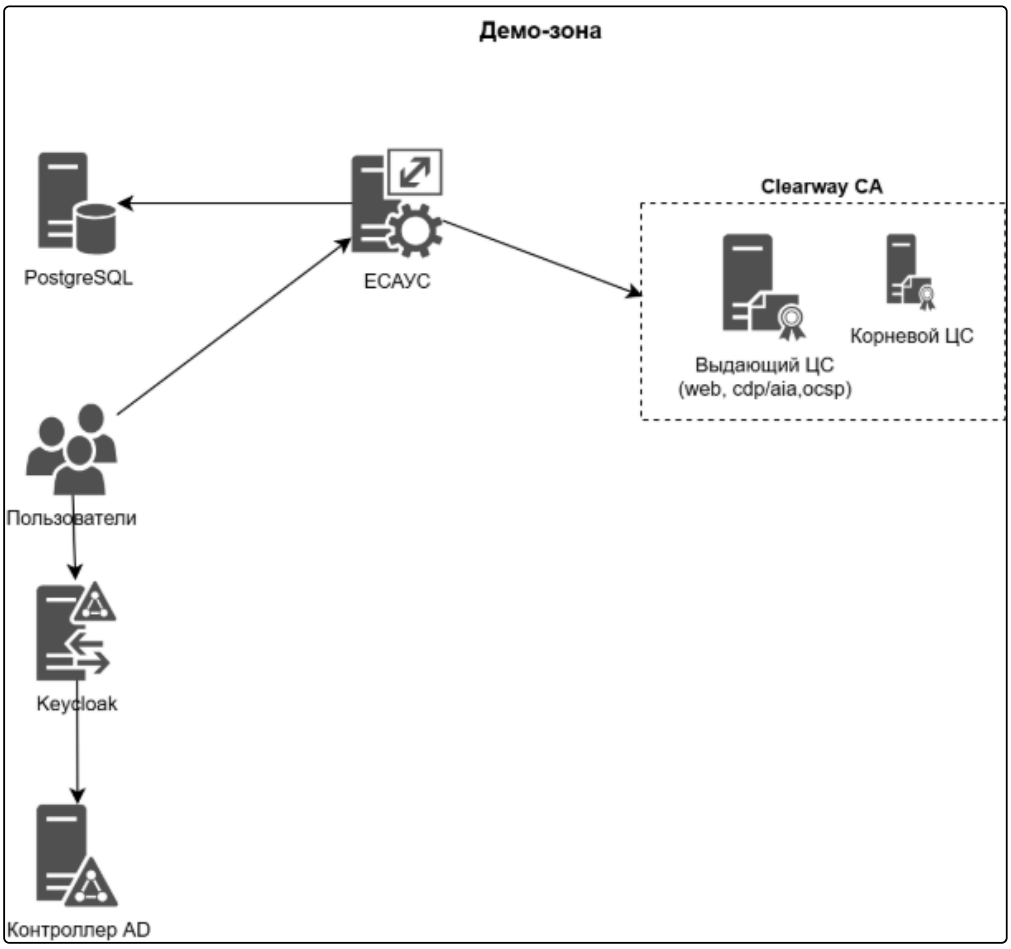


Рисунок 1 Схема компонентов ЕСАУС

```
192.168.60.76 min-klck.tst.itc.internal – на этом хосте запущена служба Keycloak. Keycloak – это открытое (Open Source) решение для управления идентификацией и доступом (Identity and Access Management, IAM), ориентированное на современные приложения и сервисы.
```

Оно обеспечивает единую точку аутентификации и авторизации, реализуя такие стандарты, как OpenID Connect, OAuth 2.0 и SAML 2.0. Рабочая директория /app/itc/

192.168.60.77 min-pgs.tst.itc.internal - на этом хосте запущена база данных Postgresql15. PostgreSQL 15 — это объектно-реляционная система управления базами данных (ОРСУБД) с открытым исходным кодом, представляющая собой конкретную мажорную версию (15) глобального проекта PostgreSQL.
Список БД для функционирования данного комплекса:

Name	Owner	Encoding	Collate	Ctype	ICU Locale	Locale Provider	Access privileges
cwica_archive	cwica	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	
cwica_root	cwica	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	
cwica_sub	cwica	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	
itc_acm	itc_svc	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	
itc_acm_agenttask	itc_svc	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	
itc_acm_collection	itc_svc	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	
itc_acm_collreg	itc_svc	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	
itc_acm_contactbook	itc_svc	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	
itc_acm_dispd	itc_svc	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	
itc_acm_isc	itc_svc	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	
itc_acm_issuenotifier	itc_svc	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	
itc_acm_mailoutbox	itc_svc	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	
keycloak	keycloak	UTF8	ru_RU.UTF-8	ru_RU.UTF-8		libc	

192.168.60.101 tst-dc1.tst.itc.internal - на этом хосте запущен контроллер домена AD. Контроллер домена Active Directory (Domain Controller, DC) — это сервер, на котором развернута и выполняется служба Active Directory Domain Services (AD DS).
Он является центральным компонентом сетевой инфраструктуры Windows, реализующим управление идентификацией и доступом на уровне домена.
Domain tst.itc.internal. NetBios tst.

192.168.60.79 min-rootca.tst.itc.internal - на этом хосте запущена служба ClearwayCA, хост выполняет функцию коревого УЦ. ClearwayCA — это программный продукт, реализующий функции Корневого (головного) Удостоверяющего центра (Корневого УЦ) в иерархической инфраструктуре открытых ключей (PKI), предназначенной для выпуска и управления SSL/TLS сертификатами. Рабочая директория /app/itc/

```
192.168.60.80 min-subca.tst.itc.internal – на этом хосте запущены службы ClearwayCA,
ClearwayCA-WEB, ClearwayCA-Publication, ClearwayCA-Archiver, ClearwayCA-OCSP и nginx для
проксирования: хост выполняет функцию выдающего УЦ, Панель управления УЦ,
Выпуск публикации CRL, выполняет функцию OCSP, выполняет функцию распространения CDP/AIA.
ClearwayCA – это программный продукт, реализующий функции Выдающего Удостоверяющего центра
 (Выдающего УЦ) в иерархической инфраструктуре открытых ключей (PKI), предназначенной для
выпуска и управления SSL/TLS сертификатами
Рабочая директория /app/itc/.
```

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.

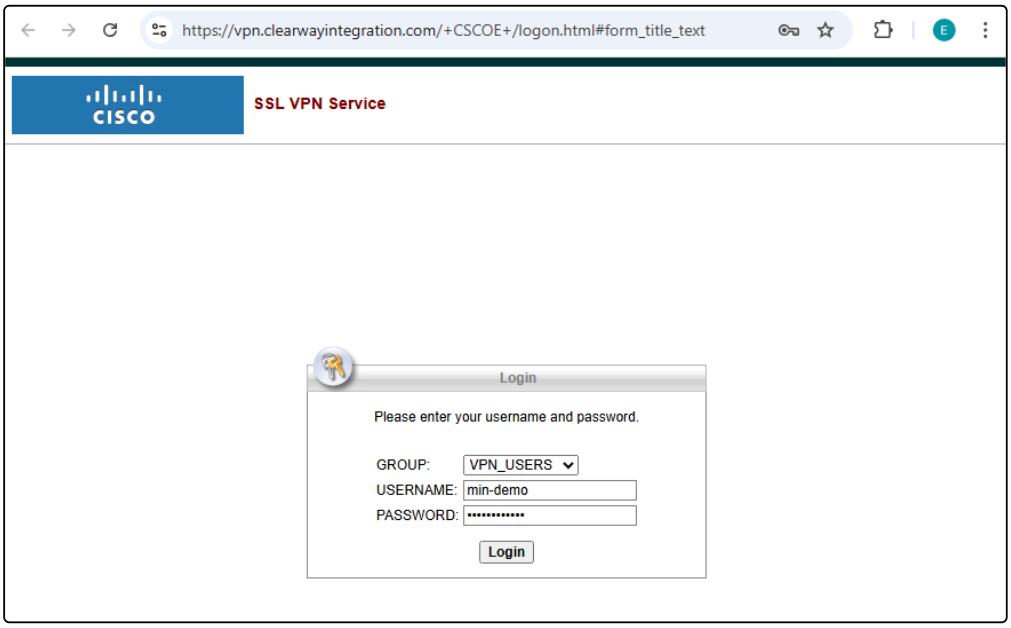
Перед началом установки убедитесь, что:

- 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.

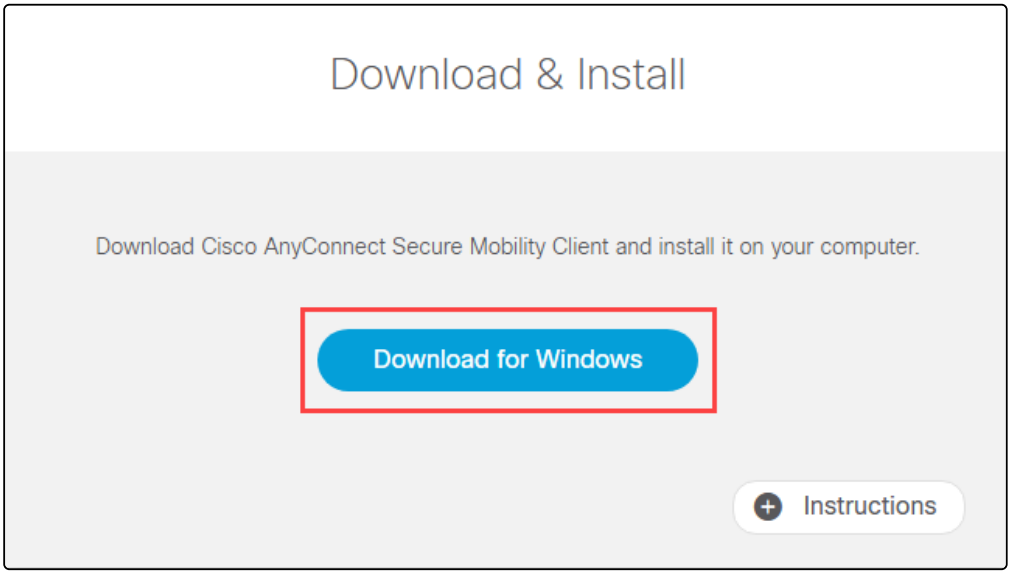
3.4.1.1 Первоначальная установка VPN-клиента

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.



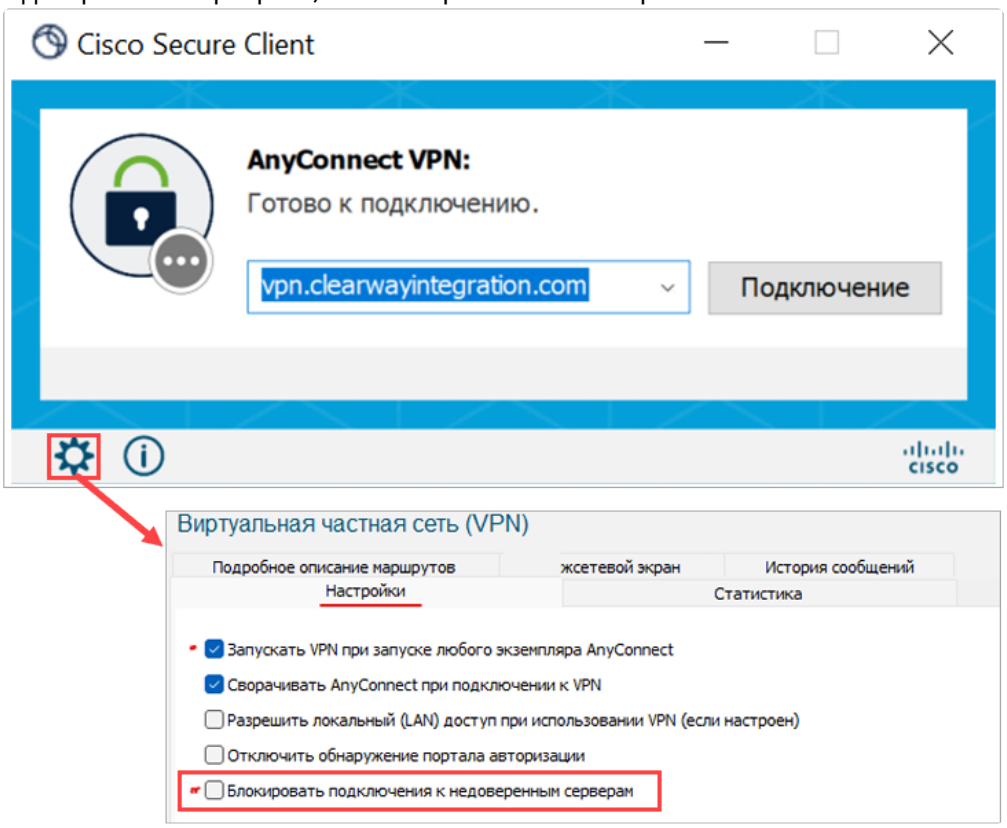
2. После успешной авторизации откроется окно с кнопкой для скачивания дистрибутива AnyConnect Secure Mobility Client.



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.

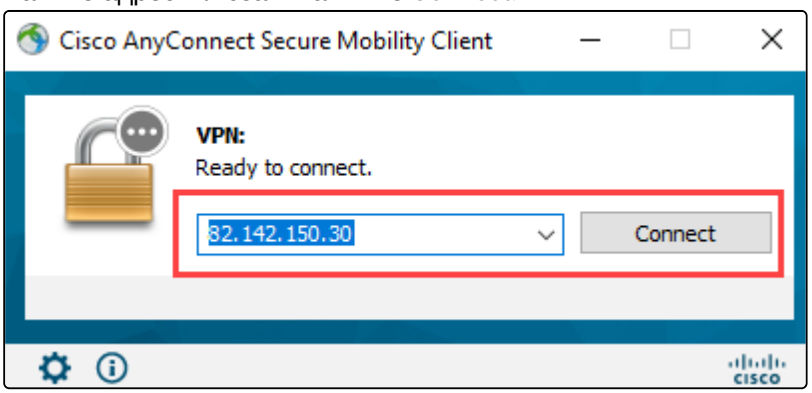
5. Откройте настройки (значок шестеренки) и снимите флажок "Блокировать подключения к недоверенным серверам", затем закройте окно настроек.



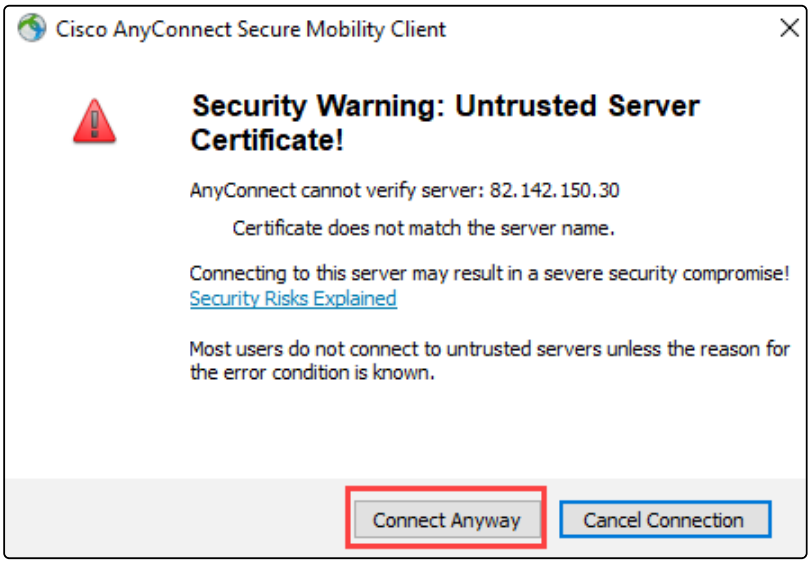
3.4.1.2 Авторизация по VPN

Для подключения к VPN выполните следующие действия.

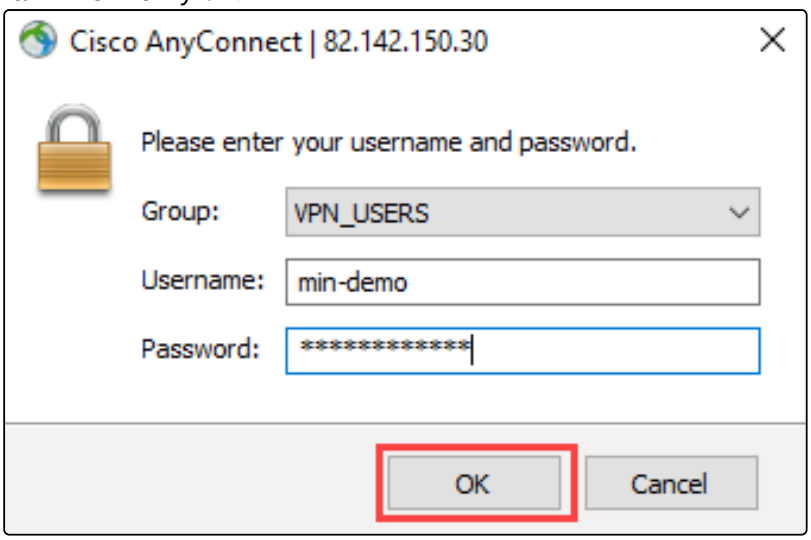
1. Запустите VPN-клиент Cisco AnyConnect.
2. Укажите адрес шлюза и нажмите **Connect**.



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**.

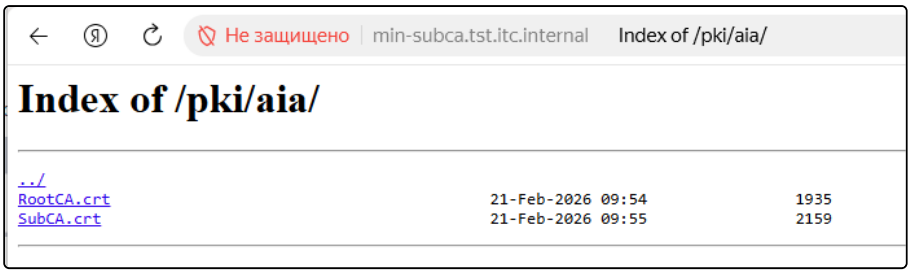


4. Укажите логин и пароль учетной записи VPN-клиента, в поле "Группа" выберите "VPN_USERS".
5. Нажмите кнопку **OK**.



3.4.2 Добавление сертификатов в доверенные

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



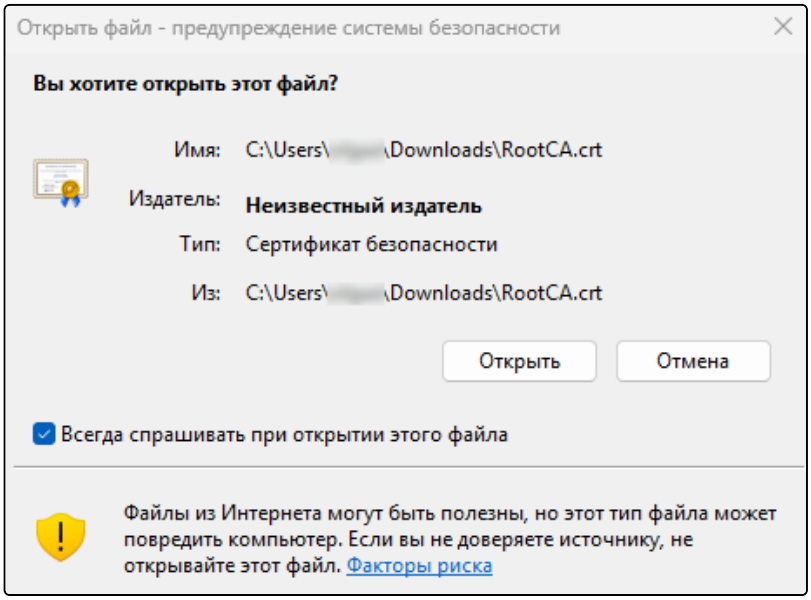
2. Скачайте на компьютер файлы сертификатов *RootCA.crt* и *SubCA.crt*.
3. Перейдите в директорию, куда вы сохранили файлы сертификатов.

4. Добавьте сертификаты, как описано ниже.
5. После добавления сертификатов закройте и заново откройте браузер, чтобы он подхватил новые сертификаты.

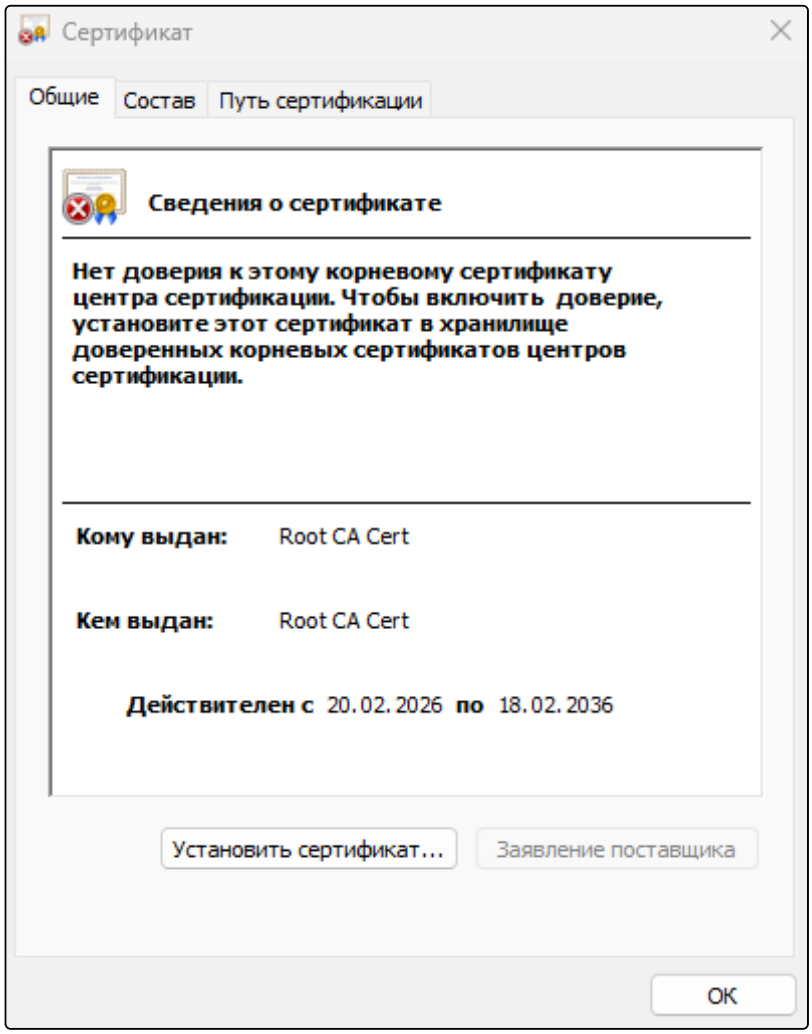
3.4.2.1 Добавление сертификатов для ОС Windows

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

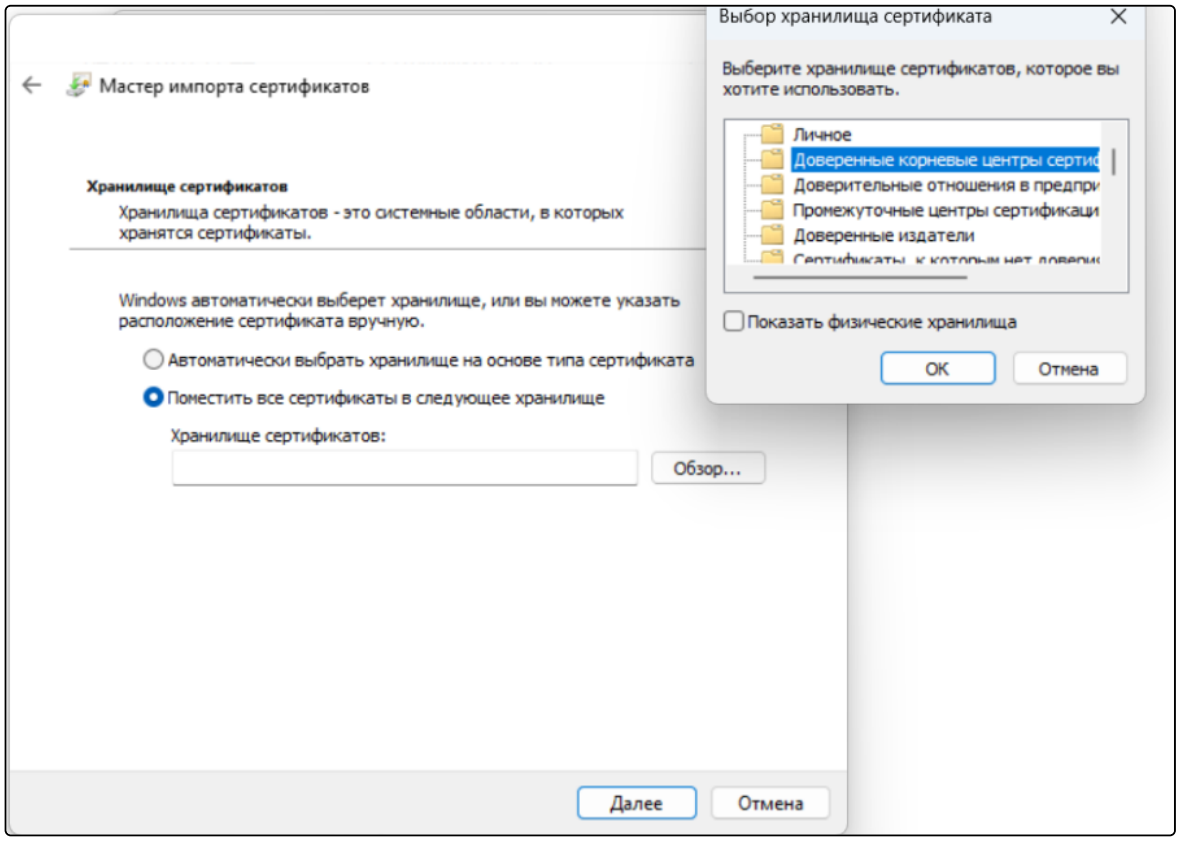
   a. Дважды нажмите на имя файла *RootCA.crt*, а затем в окне предупреждения системы безопасности нажмите **Открыть**.



   b. Нажмите **Установить сертификат**.



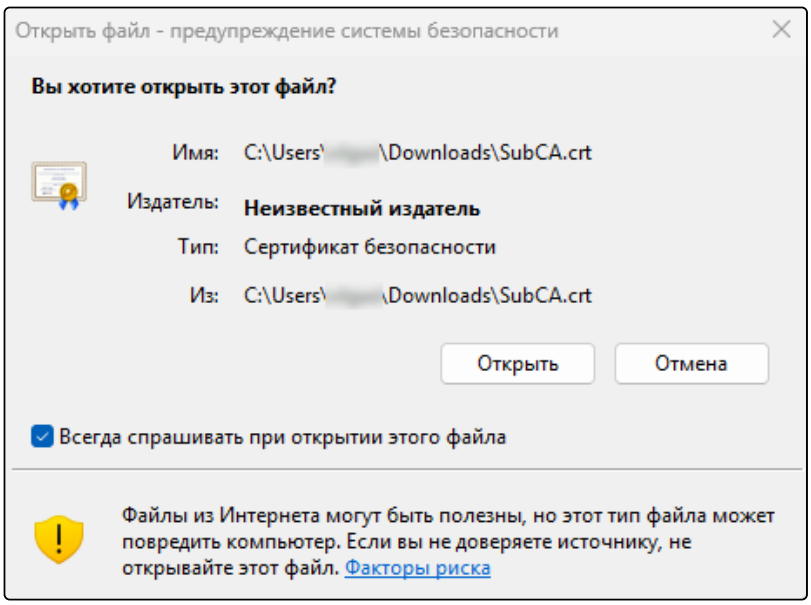
c. Нажмите **Далее**, выберите пункты, как показано на рисунке ниже. Затем нажмите **Далее**.



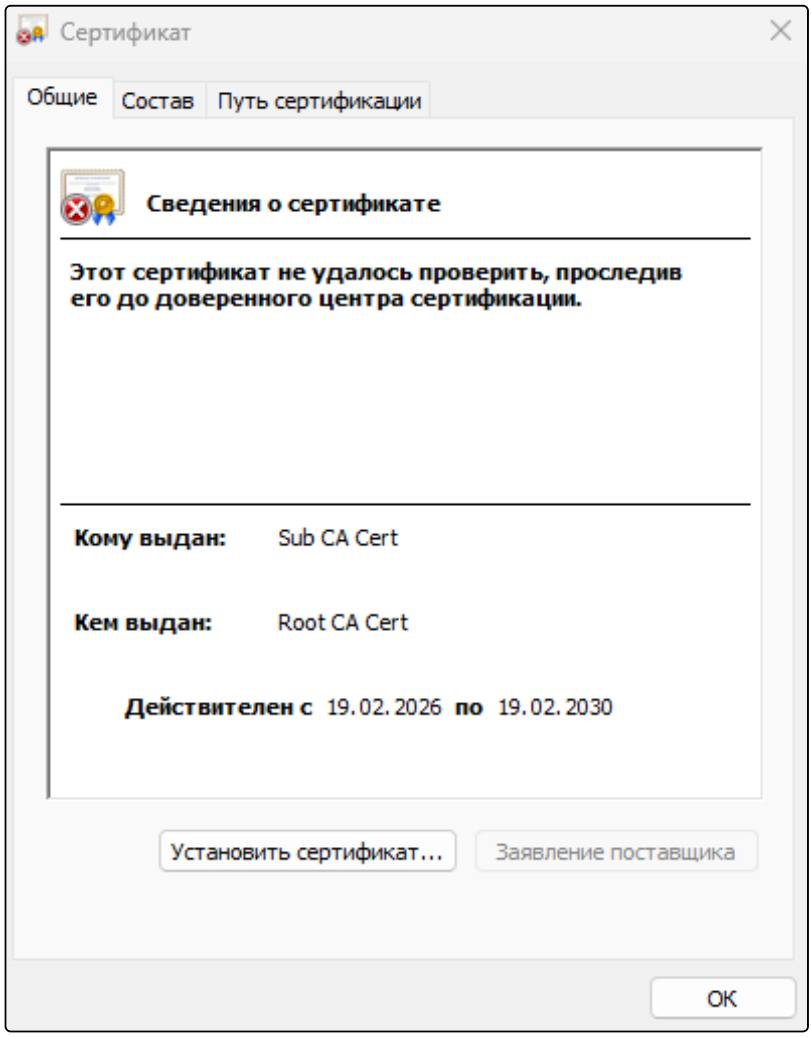
d. Нажмите **Готово**, а затем в окне предупреждения системы безопасности нажмите **Да**.

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

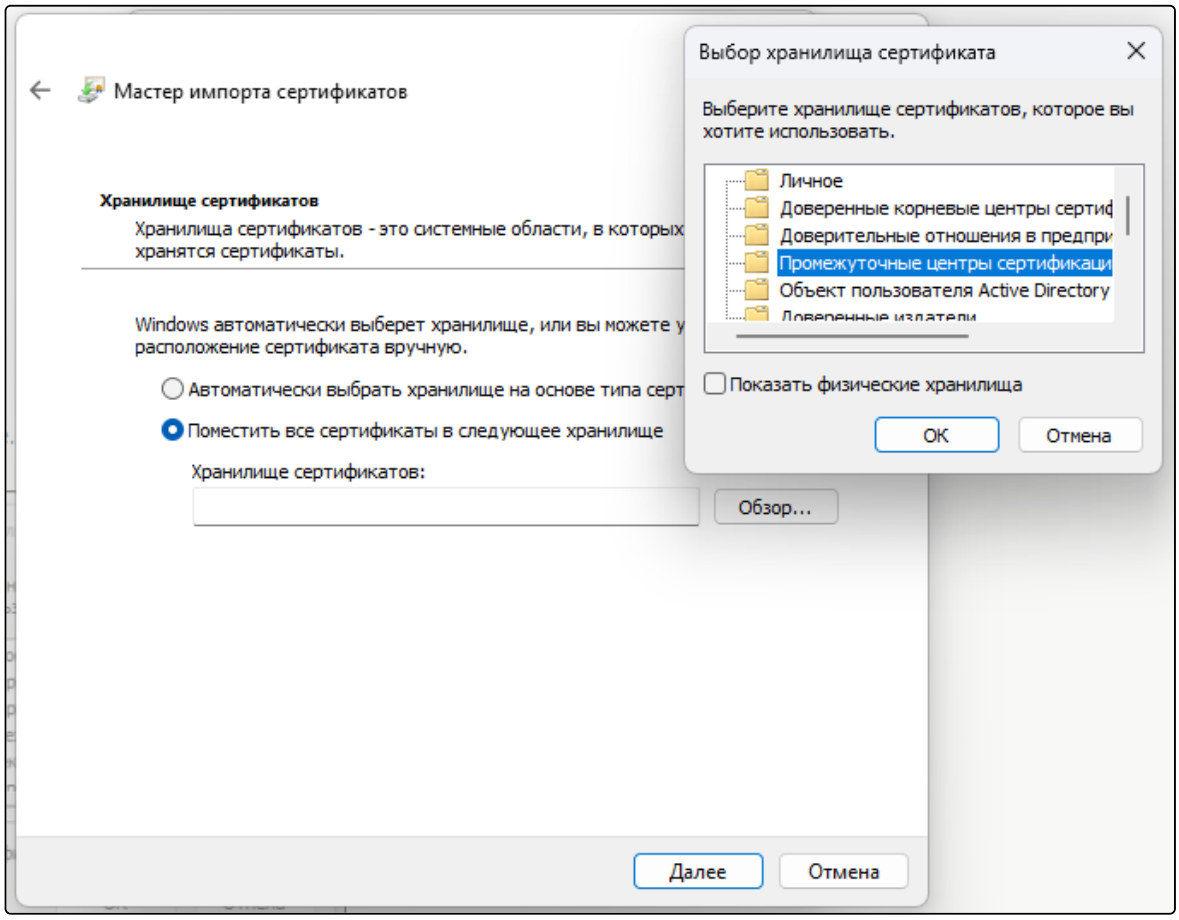
a. Дважды нажмите на имя файла *SubCA.crt*, а затем в окне предупреждения системы безопасности нажмите **Открыть**.



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

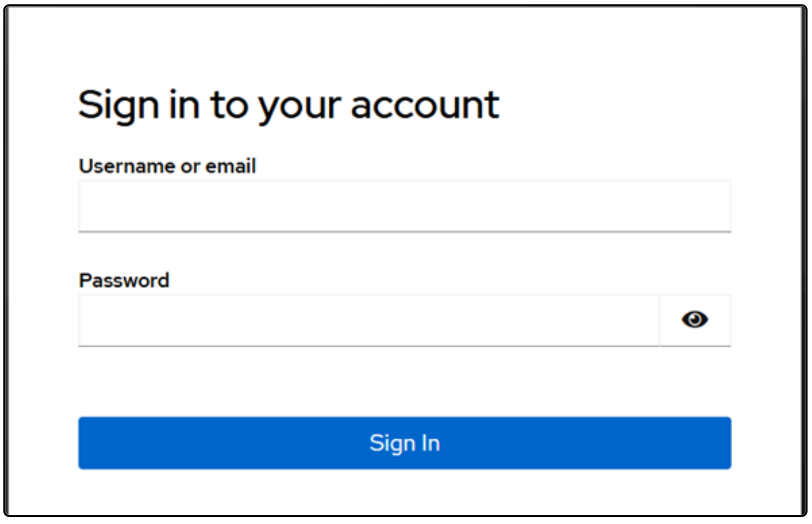


Рисунок 2 Окно входа

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

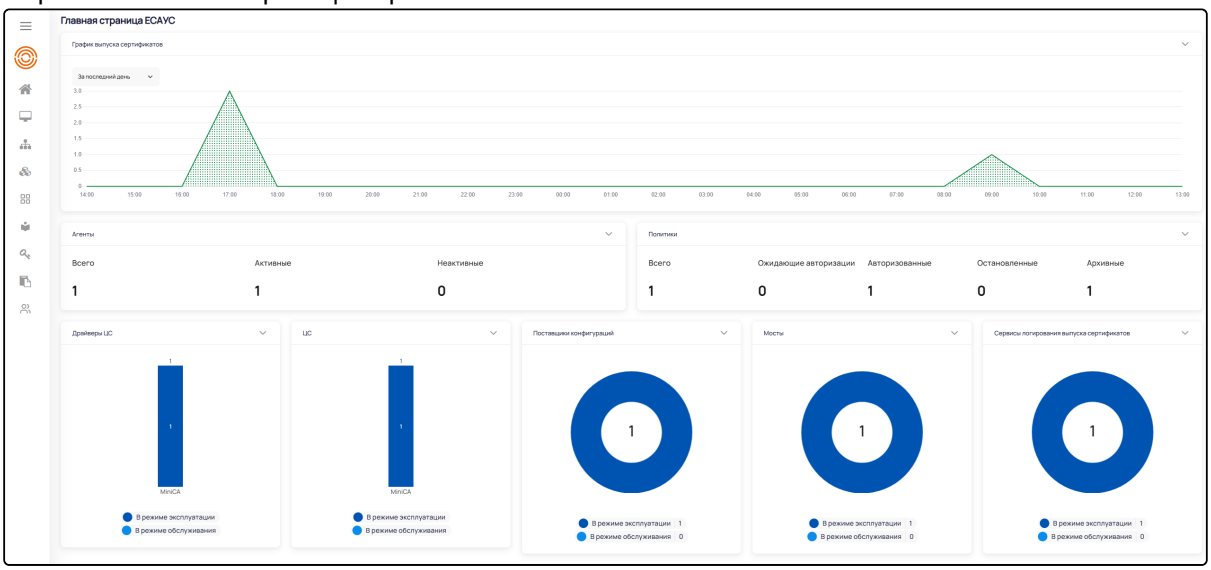


Рисунок 3 Главная страница портала ЕСАУС

3.6 Подключение к демо-стенду через SSH

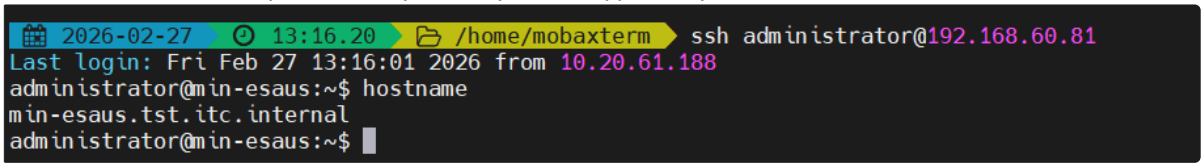
> Для подключения к демо-стенду через SSH запросите учетные данные администратора у сотрудников технической поддержки.

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

1. Откройте консоль с поддержкой работы ssh, введите адрес:

```
ssh administrator@min-esaus.tst.itc.internal
или
ssh administrator@192.168.60.81
```

2. В появившемся сообщении о запросе пароля введите пароль.



4 Проверка работы ПО

4.1 Проверка авторизации по web

1. В адресную строку введите https://min-esaus.tst.itc.internal и нажмите **Enter**.
2. Просмотрите вкладки на странице.
   Ожидаемый результат: не должно быть ошибок.

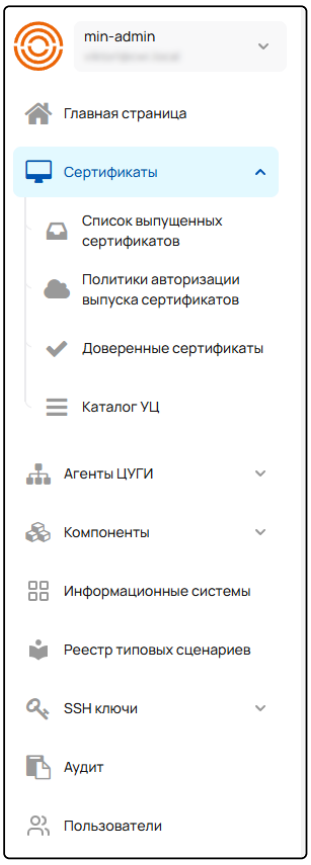


Рисунок 4 Главная страница ЕСАУС

4.2 Проверка статуса сервисов

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

1. Авторизуйтесь по ssh, ввести адрес в консоли:

```
ssh administrator@min-esaus.tst.itc.internal
```

2. Перейдите в контекст пользователя:

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

3. Перейдите в рабочую директорию:

```
itc-svc@min-esaus:/home/administrator$ cd /app/itc
itc-svc@min-esaus:/app/itc$
```

4. Проверьте статус работы служб командой:

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

5. Ожидаемый результат: отображает 15 запущенных служб со статусом Active: active (running). ПО запущено и функционирует.

```
itc-svc@min-esaus:/app/itc$ systemctl list-units --user --type=service
  UNIT                                LOAD   ACTIVE SUB     DESCRIPTION
  acmrequestsvalidator.service        loaded active running acmrequestsvalidator
  itc.acm.agentTasks.service          loaded active running itc.acm.agentTasks
  itc.acm.caDriver.service            loaded active running itc.acm.caDriver
  itc.acm.configDistributor.service loaded active running itc.acm.configDistributor
  itc.acm.controlPanel.service        loaded active running itc.acm.controlPanel
  itc.acm.issueNotifier.service       loaded active running itc.acm.issueNotifier
  itc.acm.logSink.service             loaded active running itc.acm.logSink
  itc.acm.logWorker.service           loaded active running itc.acm.logWorker
  itc.acm.sshm.service                loaded active running itc.acm.sshm
  itc.collreg.service                 loaded active running itc.collreg
  itc.contactBook.service             loaded active running itc.contactBook
  itc.core.service                    loaded active running itc.core
  itc.isc.service                     loaded active running itc.isc
  itc.mailOutbox.service              loaded active running itc.mailOutbox
  itcacmapi.service                   loaded active running itcacmapi
  itcagentd.service                   loaded active running ITC Management Agent
  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.
19 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
```

Рисунок 5 Запущенные службы ЕСАУС

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.