Центр
Управления
Гетерогенными
Инфраструктурами

МиУ. Инструкция по запуску продукта в демо-зоне

ООО «Клируэй Текнолоджис»

2026

Оглавление

1 Введение

Настоящий документ содержит информацию о процессе установки системы «Мониторинга и Управления» (МиУ) 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

Использование демо-стенда системы

2.1 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 МиУ, сервер Keycloak, сервер PostgreSQL, сервер ClickHouse, 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).

2.2 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	min-demo	+iSU5w1JU6E5
2	Портал МиУ	min-client	WydR5WG65s91f4l

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 адресу:

- Web-интерфейс МиУ: https://min-miu.tst.itc.internal.

2.3 Схема развертывания компонентов продукта на демо-стенде

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

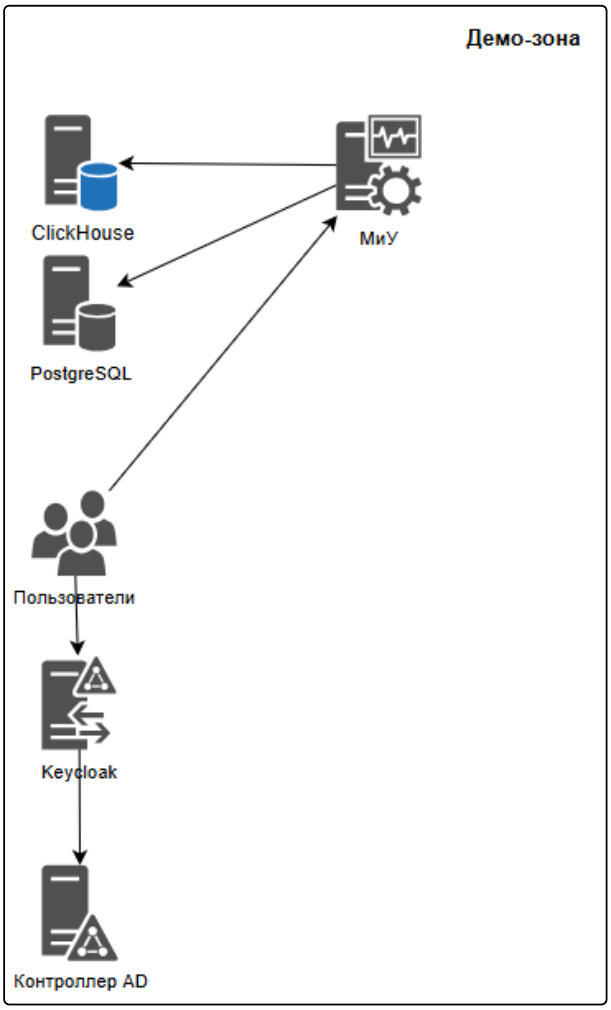


Рисунок 1 Схема компонентов МиУ

1. Хост min-miu.tst.itc.internal - на этом хосте установлены сервисы МиУ:

	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.Acl	Формирование ACL, Policies и других сущностей для отправки агентам
6	ITC.Api.Collreg	Провайдер коллекций

	Имя сервиса	Назначение
7	ITC.Api.TaskControl	Сервис пользовательских сценариев для агентов
8	ITC.Api.FileStorage	Файловое хранилище
9	ITC.Api.WsMam	Расчет и инвентаризация
10	ITC.Api.StructMon.WsMam.Host	Структурированный мониторинг
11	ITC.Api.WsMam.CVE.DistributionPoint	API для получения базы уязвимостей CVE
12	itcmsgd	Брокер сообщений NATS
13	ITC.Api.Integration	Сервис интеграции
14	ITC.Api.PermissionManager	Ролевая модель
15	ITC.Api.AppStore	Магазин приложений для АРМов
16	ITC.Api.InputRules	Правила проверки паролей и других текстовых данных
17	ITC.Api.SupportManager	Удаленная поддержки пользователей
18	ITC.Api.EDR.Rules	Создание правил
19	ITC.Api.MailOutbox	Отправка почтовых уведомлений
20	ITC.Api.Reporter	Сервис отчётов
21	ReportConstructor	Отчёты по данным инвентаризации
22	ITC.Api.LogsExporter	Для интеграции между хранилищем логов OpenSearch и сервером Syslog
23	marmdisp	Сервис проверки и реагирования
24	discovery	Обнаружение Мостов
25	ITC.Api.Platform.Core	Основной сервис Платформы

	Имя сервиса	Назначение
26	ITC.Api.WsMam.ControlPlane	BFF

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

Список БД для функционирования данного ППО:

miu_platformcore
miu_marmdisp
miu_discovery
miu_dispd
miu_acl
miu_collreg
miu_filestorage
miu_mam
miu_structmon
miu_controlplane
miu_taskcontrol
miu_supportmanager

miu_appstore
miu_inputrules
miu_mailoutbox
miu_reporter
miu_permissionmanager
miu_edr_rules

4. Хост min-ch.tst.itc.internal - на этом хоста установлена СУБД ClickHouse:

ClickHouse 25.3.2.39	Хранение данных

Список БД для функционирования данного ППО:

mon
crd
tco

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

ActiveDirectory	Служба каталогов

2.4 Настройка доступа к демо-стенду

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

1. Авторизуйтесь по VPN.
2. Добавьте в доверенные необходимые сертификаты для ОС Windows / ОС Linux.

2.4.1 Настройка VPN

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

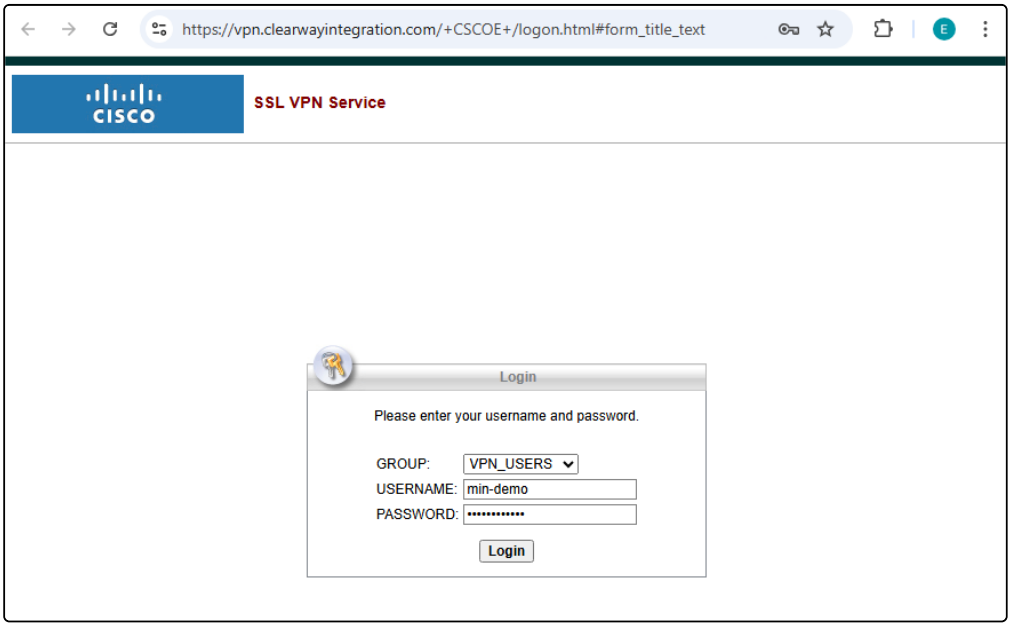
Перед началом установки убедитесь, что:

- 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.

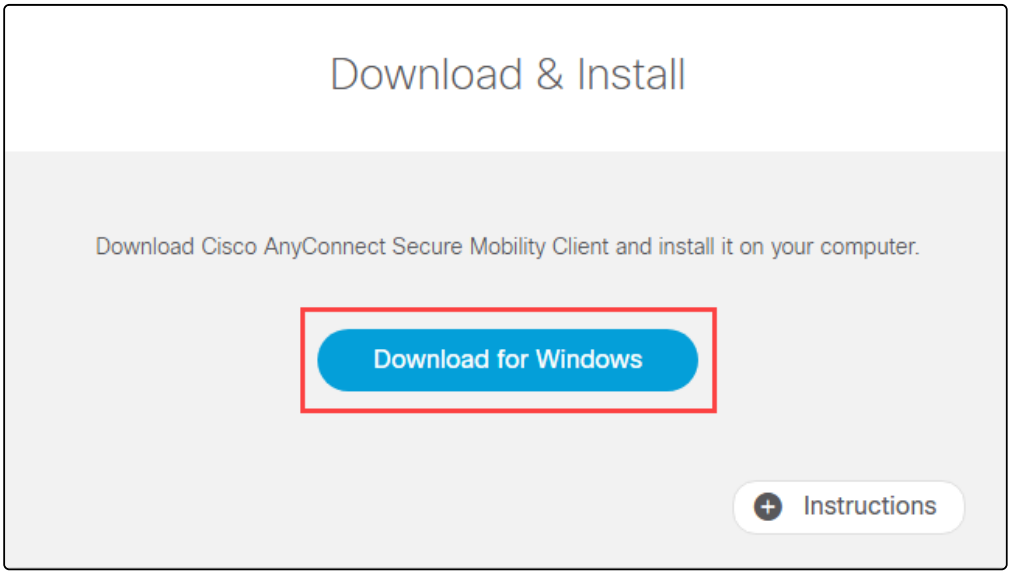
2.4.1.1 Первоначальная установка VPN-клиента

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.



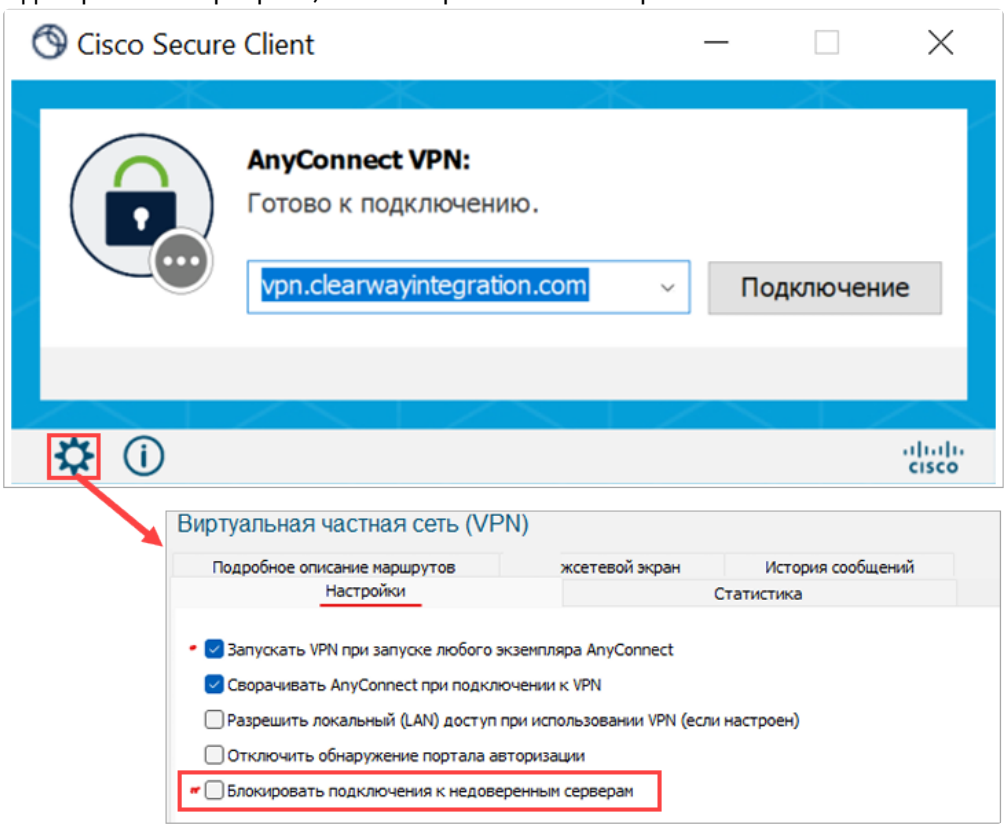
2. После успешной авторизации откроется окно с кнопкой для скачивания дистрибутива AnyConnect Secure Mobility Client.



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

3. Скачайте и установите Cisco AnyConnect, следуя указаниям мастера установки.

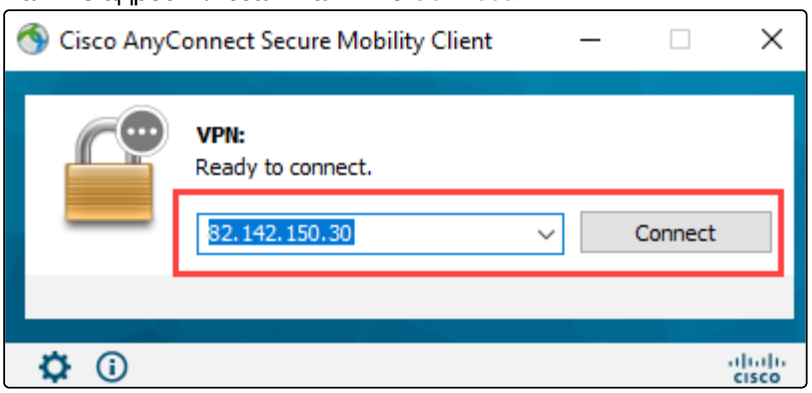
4. Запустите клиент Cisco AnyConnect.
5. Откройте настройки (значок шестеренки) и снимите флажок "Блокировать подключения к недоверенным серверам", затем закройте окно настроек.



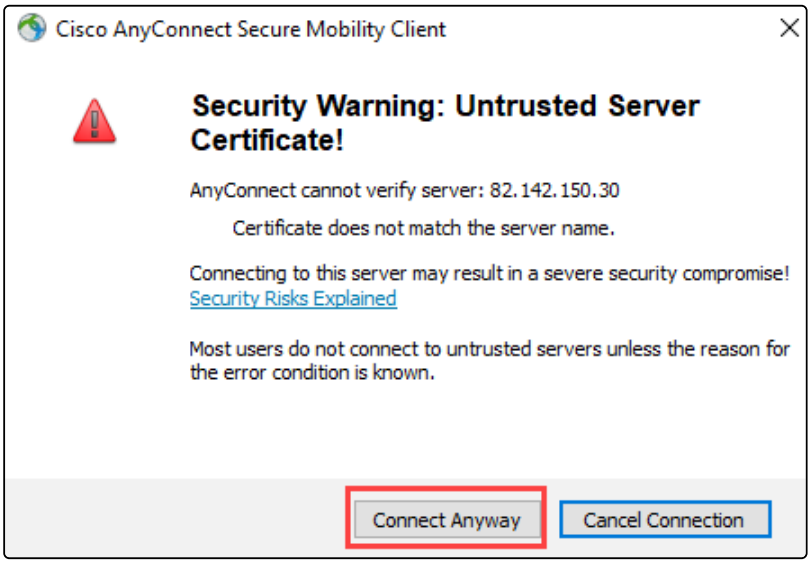
2.4.1.2 Авторизация по VPN

Для подключения к VPN выполните следующие действия.

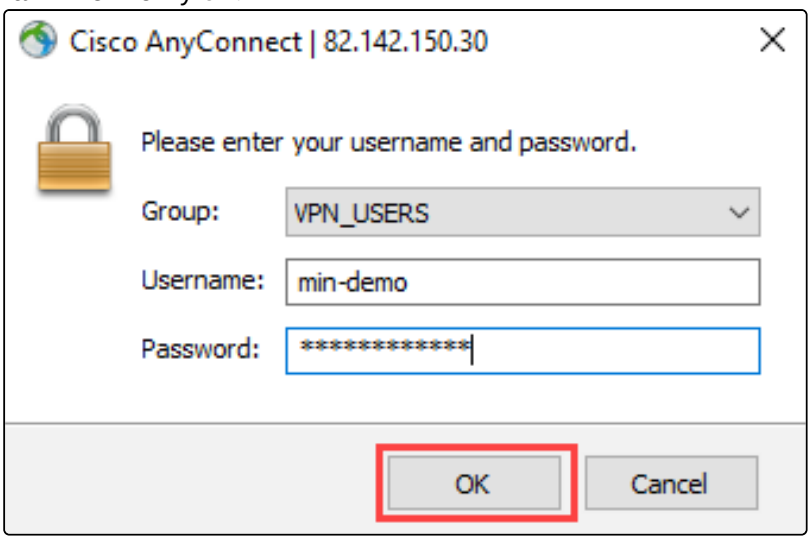
1. Запустите VPN-клиент Cisco AnyConnect.
2. Укажите адрес шлюза и нажмите **Connect**.



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**.

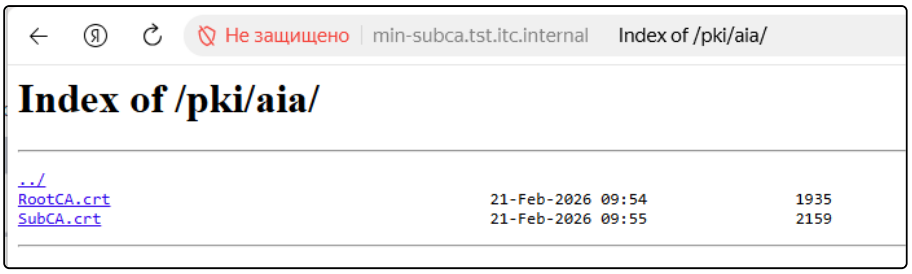


4. Укажите логин и пароль учетной записи VPN-клиента, в поле "Группа" выберите "VPN_USERS".
5. Нажмите кнопку **OK**.



2.4.2 Добавление сертификатов в доверенные

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



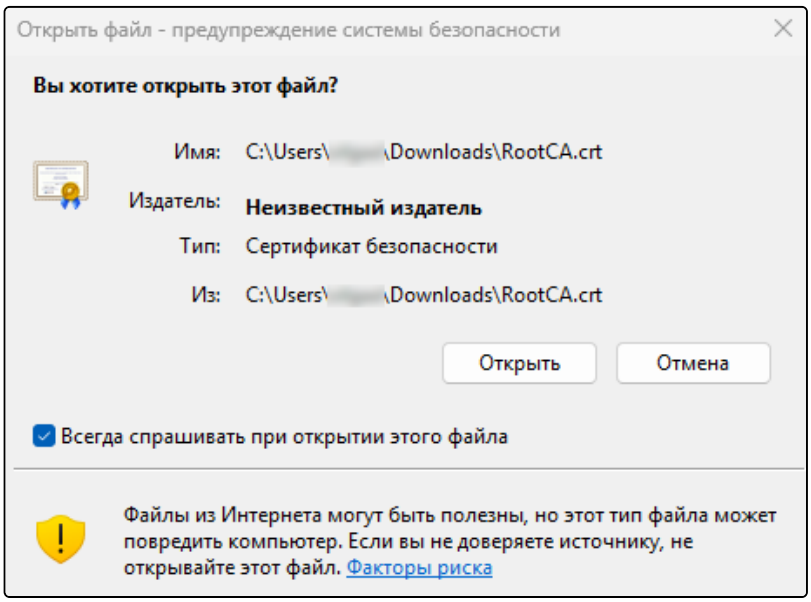
2. Скачайте на компьютер файлы сертификатов *RootCA.crt* и *SubCA.crt*.
3. Перейдите в директорию, куда вы сохранили файлы сертификатов.

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

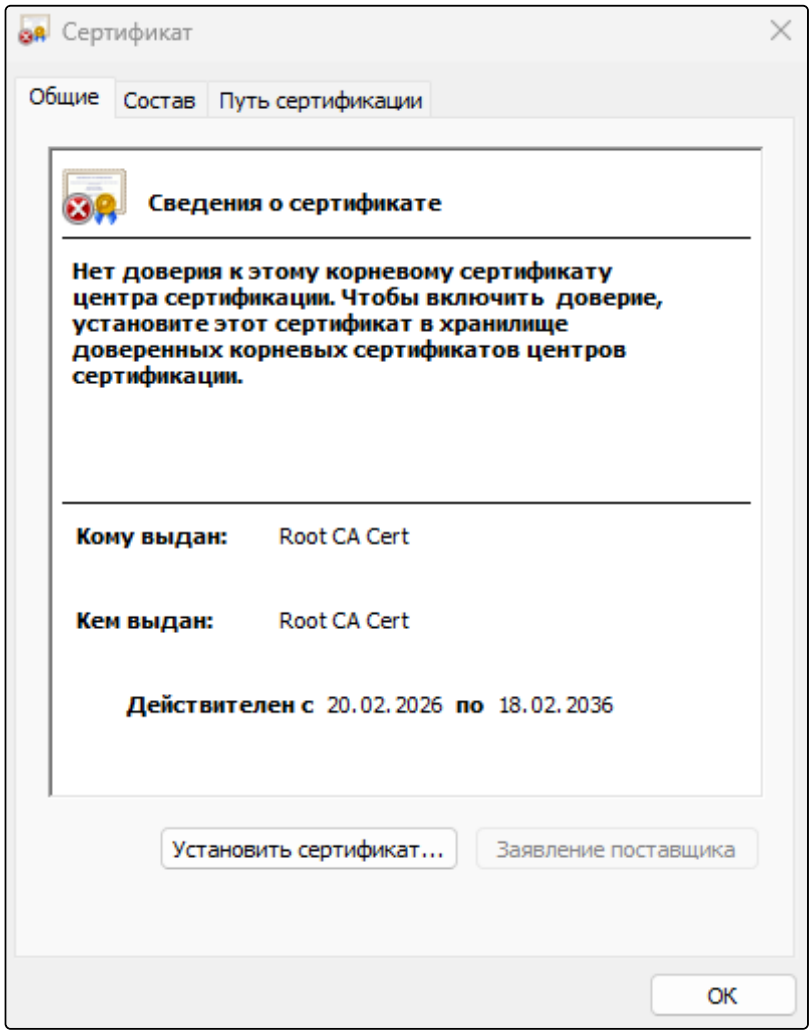
2.4.2.1 Добавление сертификатов для ОС Windows

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

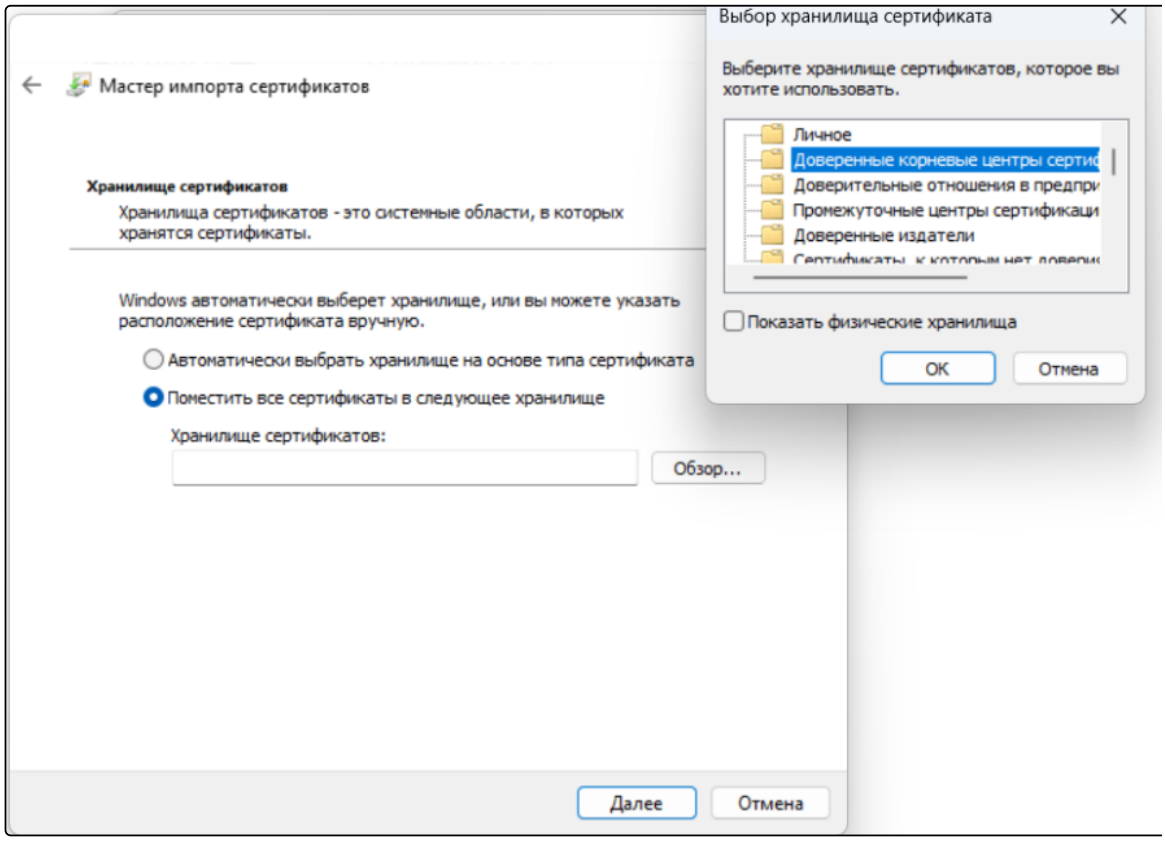
    a. Дважды нажмите на имя файла *RootCA.crt*, а затем в окне предупреждения системы безопасности нажмите **Открыть**.



    b. Нажмите **Установить сертификат**.



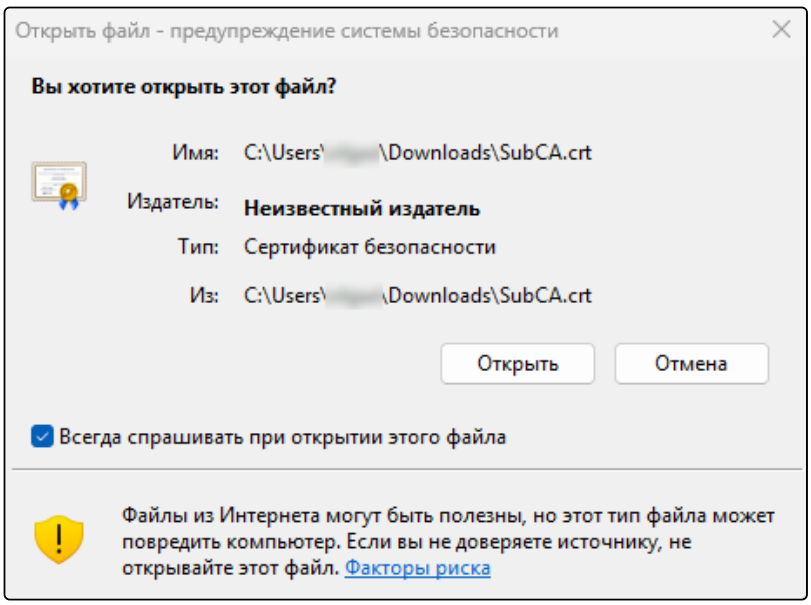
c. Нажмите **Далее**, выберите пункты, как показано на рисунке ниже. Затем нажмите **Далее**.



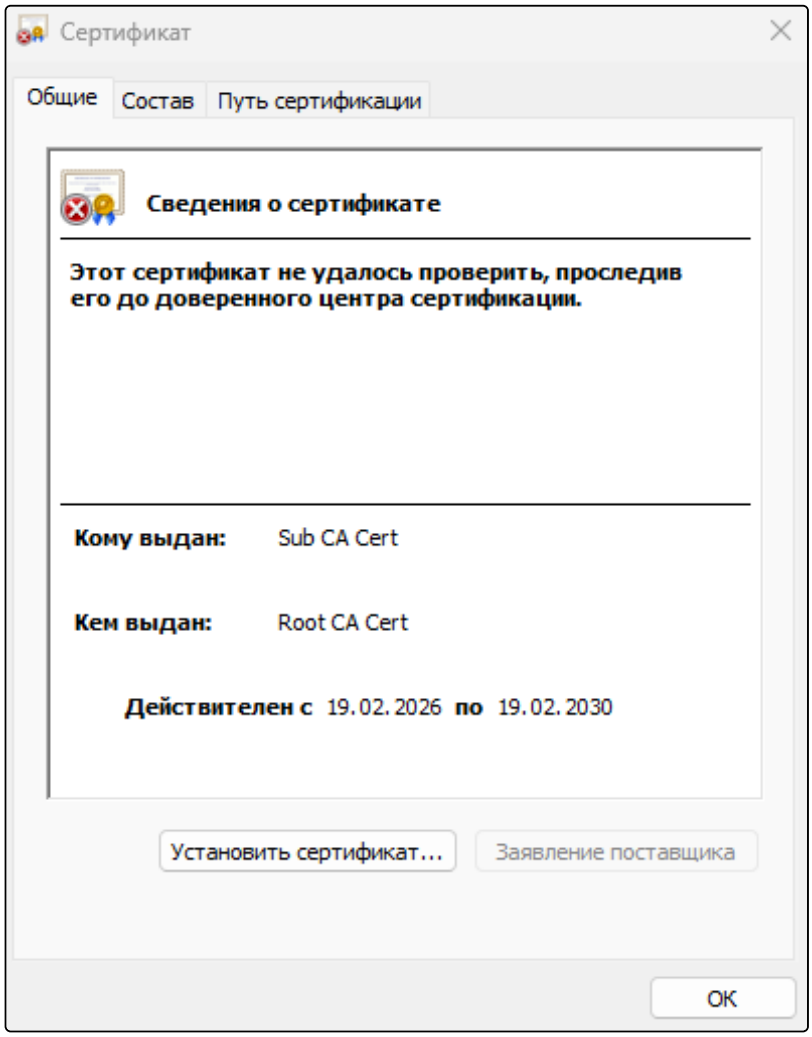
d. Нажмите **Готово**, а затем в окне предупреждения системы безопасности нажмите **Да**.

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

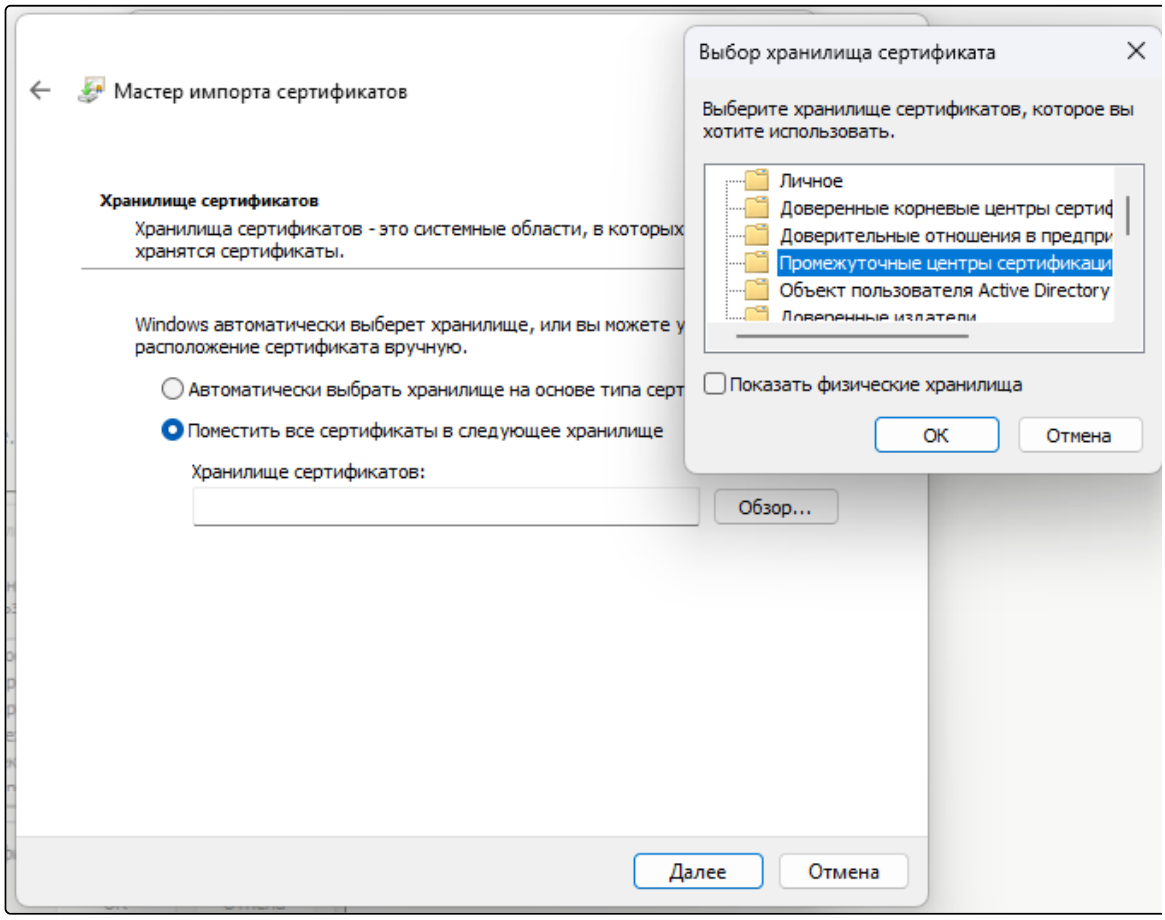
a. Дважды нажмите на имя файла *SubCA.crt*, а затем в окне предупреждения системы безопасности нажмите **Открыть**.



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**.

2.4.2.2 Добавление сертификата для ОС Linux

2.4.2.2.1 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
```

2.4.2.2.2 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/
```

2.5 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-miu.tst.itc.internal и нажмите **Enter.**
3. В появившемся окне входа заполните соответствующие поля, используя данные из таблицы Учетные записи.

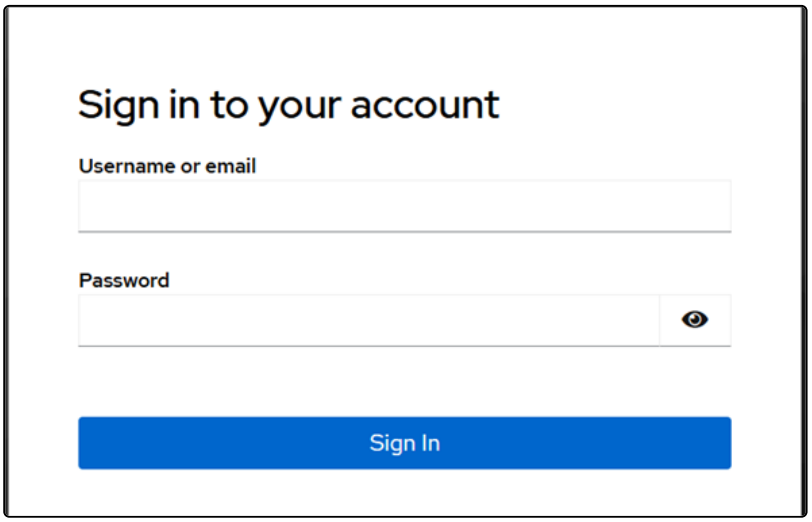


Рисунок 2 Окно входа

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

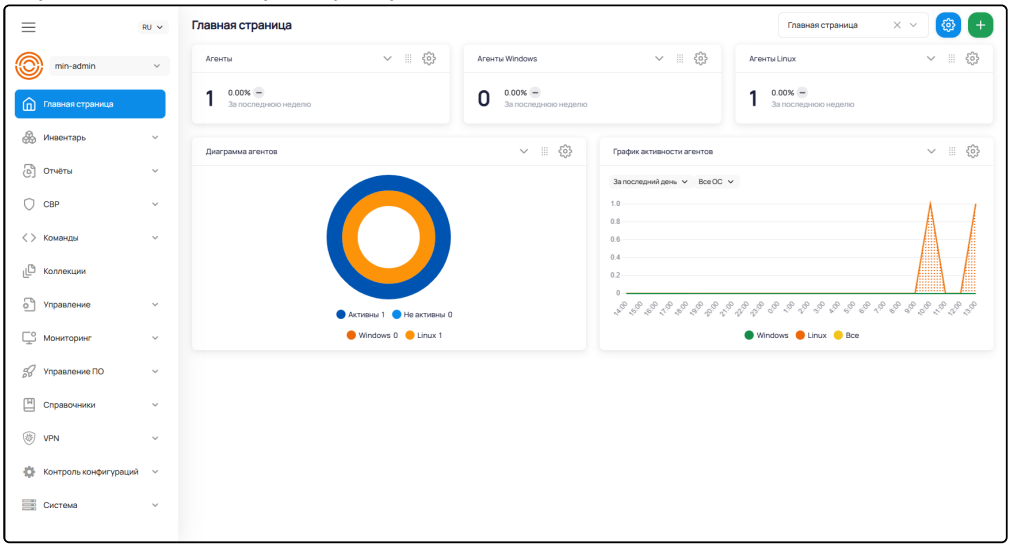


Рисунок 3 Главная страница портала МиУ

2.6 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.

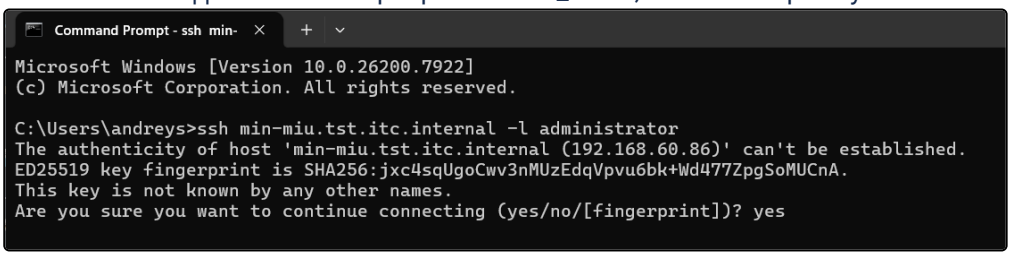


Рисунок 4 Добавление сервера в know_hosts

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

3 Проверка работы ПО

3.1 Проверка страницы агента

1. В адресную строку введите ссылку https://min-miu.tst.itc.internal и нажмите **Enter.**
2. В левом меню выберите пункт **Инвентарь** -> **Компьютеры**.
3. Выберите любой компьютер из списка.
4. Просмотрите вкладки на странице агента.
   Ожидаемый результат: не должно быть ошибок.

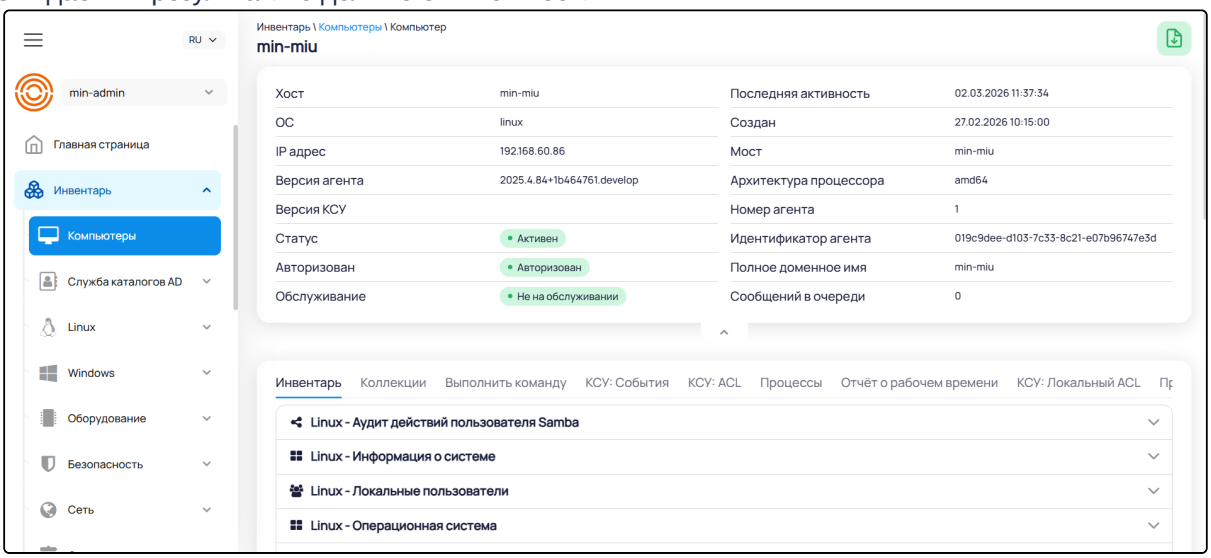


Рисунок 6 Карточка агента

3.2 Проверка работы интерактивных команд

1. В адресную строку введите ссылку https://min-miu.tst.itc.internal и нажмите **Enter.**
2. В левом меню выберите пункт **Инвентарь** -> **Компьютеры**.
3. Нажмите на имя компьютера из списка, чтобы перейти в карточку компьютера.
4. Выберите вкладку **Выполнить команду**.
5. Введите команду в поле **Команда**.
   Например: date
   Ожидаемый результат: команда должна вернуть результат выполнения в поле "Результат выполнения команд". Не должно быть ошибок.

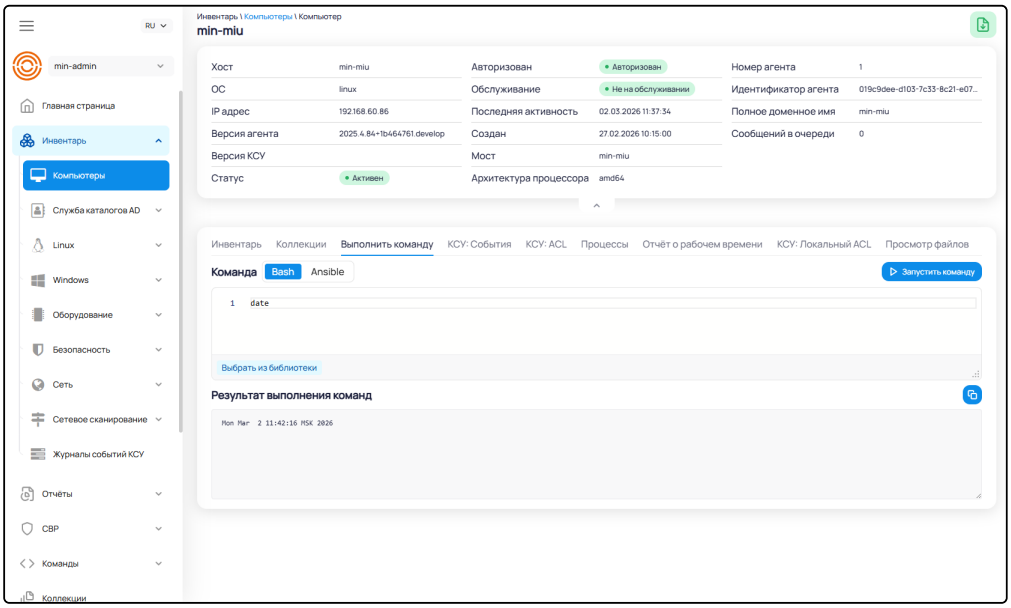


Рисунок 7 Работа интерактивных команд

3.3 Проверка создания коллекции и добавление агентов в коллекции

1. В адресную строку введите ссылку https://min-miu.tst.itc.internal и нажмите **Enter.**
2. В левом меню выберите пункт **Коллекции**.
3. Нажмите на плюсик в правом верхнем углу страницы коллекций.
4. В выпадающем списке выберите **Статическую**.
5. Впишите название коллекции в поле **Название**.
6. Нажмите на кнопку **Добавить АРМ +**.
7. Выберите из списка нужный АРМ.
8. Нажмите на кнопку **Добавить в коллекцию**.
9. Нажмите в правом верхнем углу на кнопку с изображением дискеты для сохранения коллекции.
   Ожидаемый результат: коллекция должна отобразиться в списке. Не должно быть ошибок.

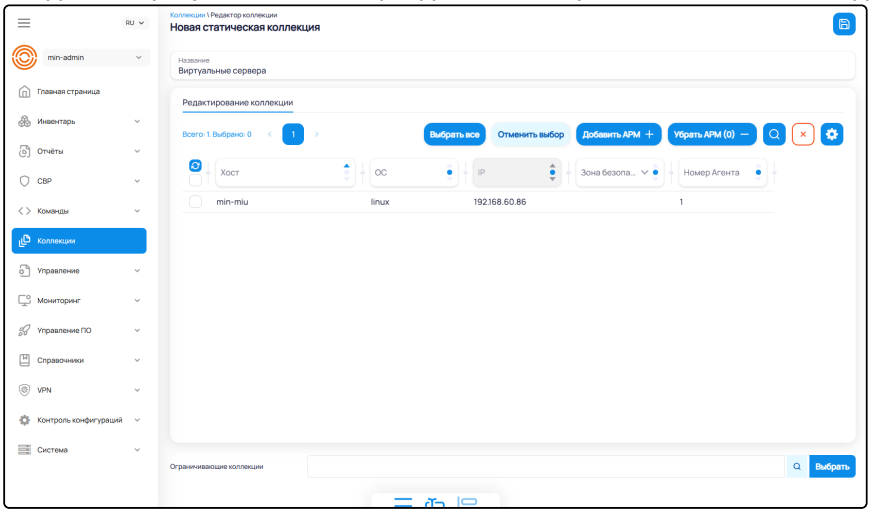


Рисунок 8 Создание статической коллекции

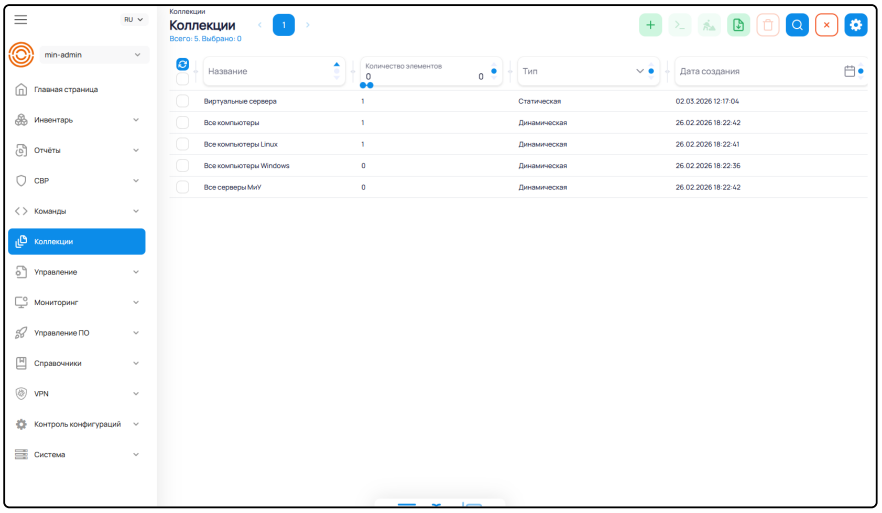


Рисунок 9 Отображение созданной статической коллекции в списке

3.4 Проверка статуса сервисов

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

1. Авторизуйтесь по ssh:

```
ssh min-miu.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-miu:~$ systemctl list-units --user --type=service
  UNIT                                LOAD   ACTIVE SUB     DESCRIPTION
  discovery.service                   loaded active running itc_api_discovery
  itc.api.acl.service                 loaded active running ITC.Api.Acl
  itc.api.appstore.service            loaded active running ITC.Api.AppStore
  itc.api.collreg.service             loaded active running ITC.Api.Collreg
  itc.api.controlPlane.service        loaded active running ITC.Api.ControlPlane
  itc.api.edr.rules.service           loaded active running ITC.Api.EDR.Rules
  itc.api.fileStorage.service         loaded active running ITC.Api.FileStorage
  itc.api.inputrules.service          loaded active running ITC.Api.InputRules
  itc.api.integration.service         loaded active running ITC.Api.Integration
  itc.api.mailOutbox.service          loaded active running itc.mailOutbox
  itc.api.permissionManager.service loaded active running ITC.Api.PermissionManager
  itc.api.platform.core.service       loaded active running ITC.Api.Platform.Core
  itc.api.reporter.service            loaded active running ITC.Api.Reporter
  itc.api.structmon.service           loaded active running ITC.Api.StructMon.WsMam.Host
  itc.api.supportManager.service      loaded active running ITC.Api.SupportManager
  itc.api.taskControl.service         loaded active running ITC.Api.TaskControl
  itc.api.wsmam.cve.dp.service        loaded active running ITC.Api.WsMam.CVE.DistributionPoint
  itc.api.wsmam.service               loaded active running ITC.Api.WsMam
  itcdispd.service                    loaded active running itcdispd
  itcmsgd.service                     loaded active running itcmsgd
  itcsrvd.service                     loaded active running itcsrvd
  marmdisp.service                    loaded active running marmdisp

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.
22 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 МиУ

4 Самостоятельная установка

4.1 Системные требования

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

4.2 Инструкции по установке

Подробные инструкции для развертывания компонентов системы запросите у сотрудников технической поддержки.