

«Визирь.СКУД»

Программный комплекс системы видеоидентификации

Руководство администратора



СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ	4
1.1. Общие положения	4
1.2. Правообладатель	4
1.3. Соглашения и обозначения	4
2. ОБЩИЕ СВЕДЕНИЯ	6
2.1. Сведения о программе и изготовителе	6
2.2. Техническая поддержка	6
2.3. Назначение и функции	6
3. НАСТРОЙКА СИСТЕМЫ	8
3.1. Настройка Сервиса УТ	8
3.1.1. Общая информация	8
3.1.2. Настройки Сервиса УТ	9
3.2. Настройка сервисов на объекте заказчика	14
3.2.1. Настройка сервиса cbs-management-service	15
3.2.2. Настройка сервиса idp-organization-service	17
3.2.3. Настройка сервиса sberid-smartbio-integration-service	18
3.2.4. Настройки сервиса terminal-proxy-manager-service	20
3.3. Инициализация терминала	21
3.4. Активация терминала	21
3.5. Настройка терминала	25
3.6. Дополнительная информация	32
3.6.1. Создание клиентов в Keycloak	32
3.6.2. Создание пользователей Сервиса УТ в Keycloak	39
3.6.3. Просмотр лог-файлов Сервиса УТ	42
4. РАБОТА СИСТЕМЫ	46



4.1.	Регистрация пользователей в системе (онбординг).....	46
4.1.1.	Работа с терминалом.....	47
4.2.	Биометрический проход.....	57
4.3.	Проход по карте (RFID).....	59
5.	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ.....	62
5.1.	Модуль взаимодействия с MDM.....	62
5.2.	Расширенное логирование по каждому терминалу.....	63
5.3.	Групповое изменение настроек для группы терминалов.....	63
5.4.	Соответствие настроек терминала и Сервера УТ.....	64
5.5.	Иерархическая структура вложенных папок.....	66
5.6.	Режимы терминала.....	67
5.7.	Выгрузка данных о биометрических терминалах.....	68
5.8.	Ролевая модель.....	69
5.9.	Создание типовых настроек.....	70
5.10.	Обновление рутовых сертификатов терминала.....	70



1. ВВЕДЕНИЕ

1.1. Общие положения

Данное руководство содержит сведения, необходимые для настройки **Программного комплекса системы видеоидентификации Визирь.СКУД** (далее – ПО, программа, система), предназначенного для проведения операций верификации и идентификации лиц.

Настоящее руководство не заменяет учебную, справочную литературу и руководства от производителей операционной системы и общего программного обеспечения.

1.2. Правообладатель

Правообладателем **Программного комплекса системы видеоидентификации «Визирь.СКУД»** является ООО «ЦРТ».

Все остальные названия компаний и названия продуктов, упомянутые в документе, являются собственностью их соответствующих владельцев.

Ни одна из частей этого документа не подлежит воспроизведению, передаче, хранению в поисковой системе или переводу на какой-либо язык в любой форме, любыми средствами без письменного разрешения общества с ограниченной ответственностью «Центр речевых технологий».

1.3. Соглашения и обозначения

В руководстве приняты следующие типографские соглашения:

Формат	Описание
Обычный	Основной текст документа.
<i>Курсив</i>	Применяется для выделения первого появления <i>термина</i> , значение которого поясняется здесь же или даётся в приложении. Также применяется для оформления <i>примечаний</i> .
Полужирный	Применяется для написания наименований программных компонентов , наименований управляющих и информационных элементов интерфейса (заголовки , кнопки и т.п.), а также компонентов системы (Центральный сервер , Подсистема обработки видеопотоков и т.п.). Также применяется для привлечения внимания .
<i>Полужирный курсив</i>	Применяется для написания <i>имен файлов</i> и <i>путей доступа</i> к ним.



Формат	Описание
<u>Подчёркнутый синий</u>	Применяется для обозначения внешних ссылок , ссылок на разделы текущего документа, а также адресов URL-запросов для работы с API.

Словосочетание «выбрать, выделить, нажать объект (или нажать на объект)» означает: «навести указатель манипулятора типа «мышь» на объект, и нажать кнопку манипулятора».

Выбор меню, который показан при помощи стрелки **>**, например, текст **Файл > Выход**, должен пониматься так: выбрать меню **Файл**, затем команду **Выход** из меню **Файл**.

Ниже приведены примеры оформления материала руководства, указывающие на важность сведений.



Ссылки на другие документы в основном тексте.



Примечания; важные сведения; указания на действия, которые необходимо выполнить в обязательном порядке.



Требования, несоблюдение которых может привести к некорректной работе, повреждению или выходу из строя изделий или программного обеспечения.



2. ОБЩИЕ СВЕДЕНИЯ

2.1. Сведения о программе и изготовителе

Наименование: Программный комплекс системы видеоидентификации Визирь.СКУД

Изготовитель: Общество с ограниченной ответственностью «Центр речевых технологий»

Адрес: 194044, г. Санкт-Петербург, Выборгская наб., д. 45, лит. Е

Телефон: +7 (812) 325-88-48

Факс: +7 (812) 327-92-97

2.2. Техническая поддержка

Адрес службы сервисного обслуживания и технической поддержки в интернете:

Email: st-support@speechpro.com

Веб-сайт: <http://www.speechpro.ru/>

При обращении в службу технической поддержки необходимо предоставить подробное описание возникшей проблемы.

Предварительно подготовьте следующую информацию:

- тип компьютера и сведения об его конфигурации;
- название и версия используемой операционной системы;
- log-файлы.

2.3. Назначение и функции

Программный комплекс системы видеоидентификации «Визирь.СКУД» позволяет детектировать лица, находящиеся перед камерой мобильного устройства, проводить сравнение детектированных лиц с заранее созданной картотекой лиц, передавать управляющие команды на реле мобильного устройства, а также обеспечивает информирование о разрешении/запрете прохода через турникет/запирающее устройство. Предназначен для проведения операций верификации и идентификации лиц.

Основные функциональные возможности программы:

- Бесконтактная биометрическая идентификация по лицу;
- Верификация владельцев пропусков;
- Управление реле устройства;
- Ведение картотеки лиц;



- Фиксация времени прохода;
- Уведомление о наступлении события.

MDM-система, входящая в состав ПО, обеспечивает:

- Удаленное управление ПО: дистанционную установку, настройку рабочих приложений и обновление ОС на мобильных устройствах;
- Защиту соединений: установку и ротацию mTLS-сертификатов, а также автоматическое обновление корневых сертификатов ГОСТ;
- Администрирование парка устройств: организацию иерархической структуры, группировку мобильных устройств и реализацию ролевой модели доступа.

ПО поддерживает интеграцию с коммерческой биометрической системой **Сбер**.

Интеграция с КБС позволяет реализовывать сценарии биометрической аутентификации для прохода на объекты, оснащенные СКУД, с использованием биометрических моделей (векторов), централизованно хранящихся в единой биометрической системе (ЕБС).

Таким образом, интеграция с КБС **Сбер** позволяет использовать биометрический СКУД в соответствии со статьей 16 ФЗ № 572 от 29.12.2022 "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации".



3. НАСТРОЙКА СИСТЕМЫ

Общая схема взаимодействия компонентов приведена на рисунке ниже.

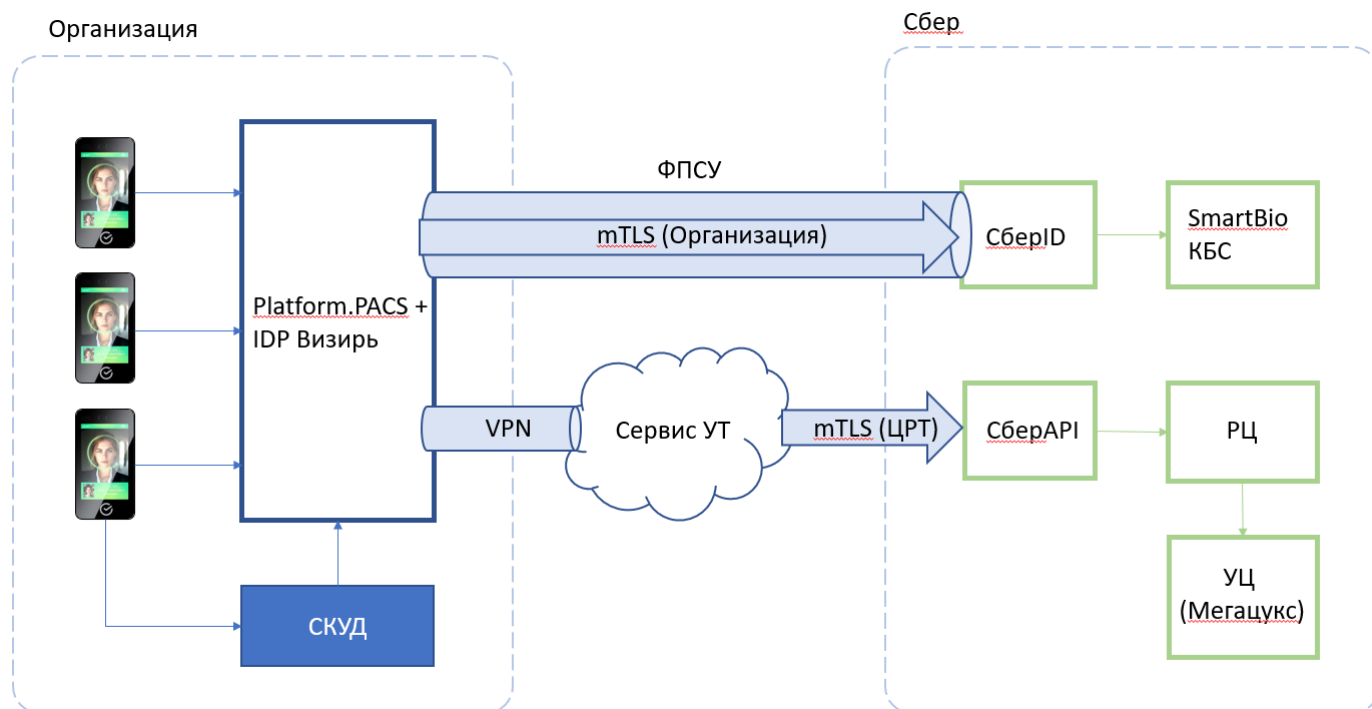


Рисунок 1 – Общая схема взаимодействия

Общий алгоритм настройки интеграции:

1. Настройте **Сервис УТ** (см. [Настройка Сервиса УТ](#)).
2. Установите и настройте сервисы на объекте заказчика (см. [Настройка сервисов на объекте заказчика](#)).
3. Инициализируйте терминал (см. [Инициализация терминала](#)).
4. Активируйте терминал (см. [Активация терминала](#)).
5. Настройте приложение на терминале (см. [Настройка терминала](#)).
6. Работайте с системой (см. [РАБОТА СИСТЕМЫ](#)).

3.1. Настройка Сервиса УТ

3.1.1. Общая информация

Сервис УТ (terminal-manager-service) предназначен для **активации** терминалов и доставки на терминал **сертификатов** и списков отозванных сертификатов из РЦ Сбер.



Сервис УТ устанавливается в облачном сервисе (за пределами организации, пользующейся терминалами).

Сервис УТ обменивается данными с терминалами через дополнительный **Сервис интеграции с УТ (terminal-proxy-manager-service)**.

Сервис интеграции с УТ устанавливается в контуре организации, пользующейся терминалами, и входит в состав поставки (bundle) **IDP Визирь**.

3.1.2. Настройки Сервиса УТ

Для доступа к настройкам **Сервиса УТ**:

- Авторизуйтесь в облачном сервисе, где развернут **Сервис УТ**;
- В меню **Service List** выберите **Cloud Container Engine** (рис. 2);

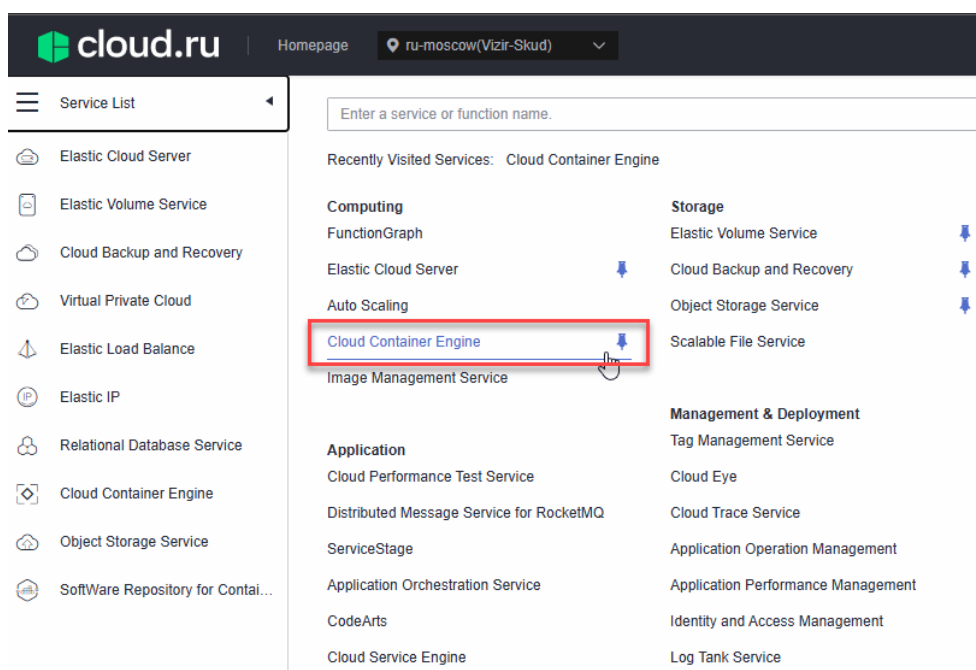


Рисунок 2 – **Cloud Container Engine**

- В открывшемся окне на вкладке **Clusters** перейдите в проект **cce-cluster** (рис. 3);

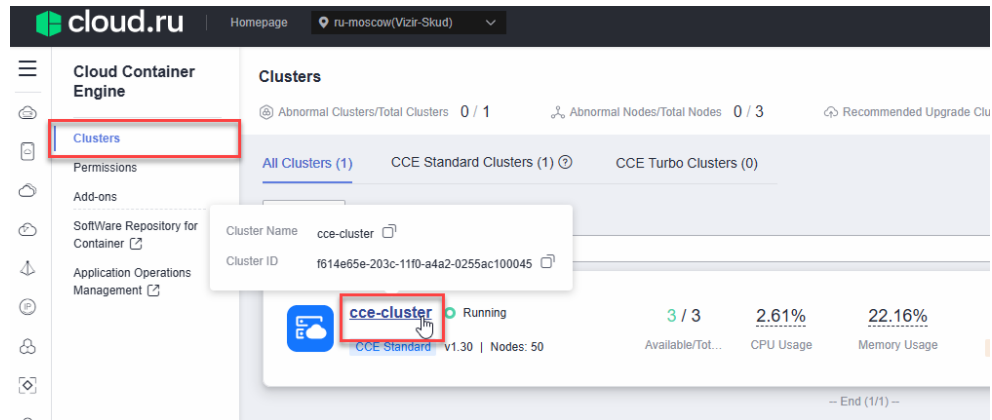


Рисунок 3 – cce-cluster

- Перейдите во вкладку **Workloads > Deployments** и в строке **terminal-manager-back** нажмите кнопку **More > Edit YAML** (рис. 4);

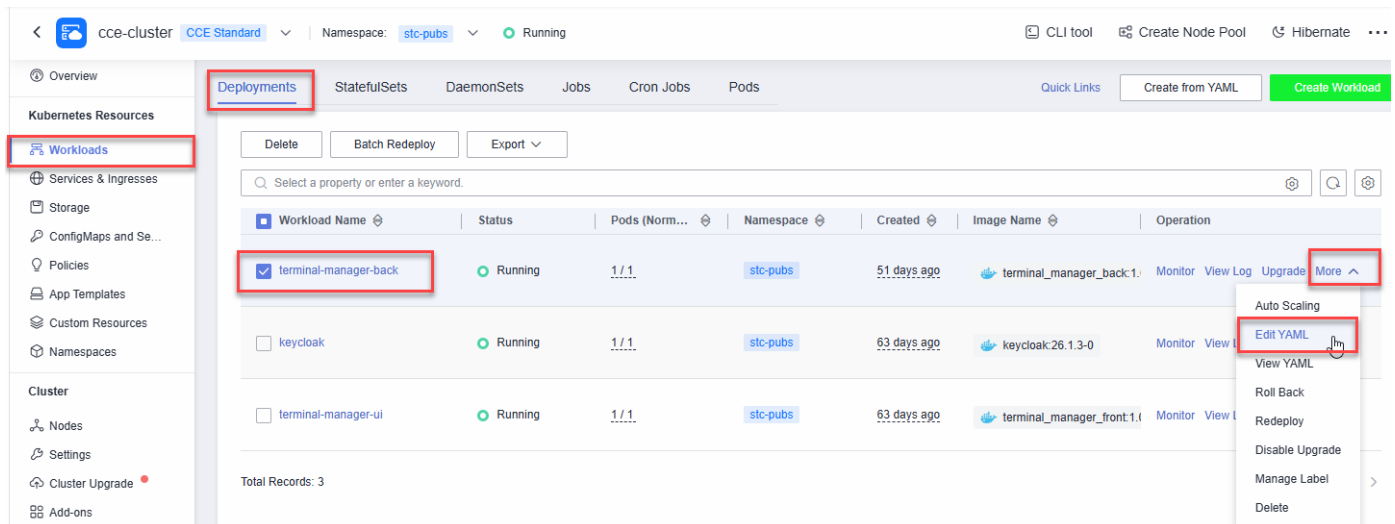


Рисунок 4 – Edit YAML

- В открывшемся окне настроек измените / добавьте необходимые параметры (рис. 5).

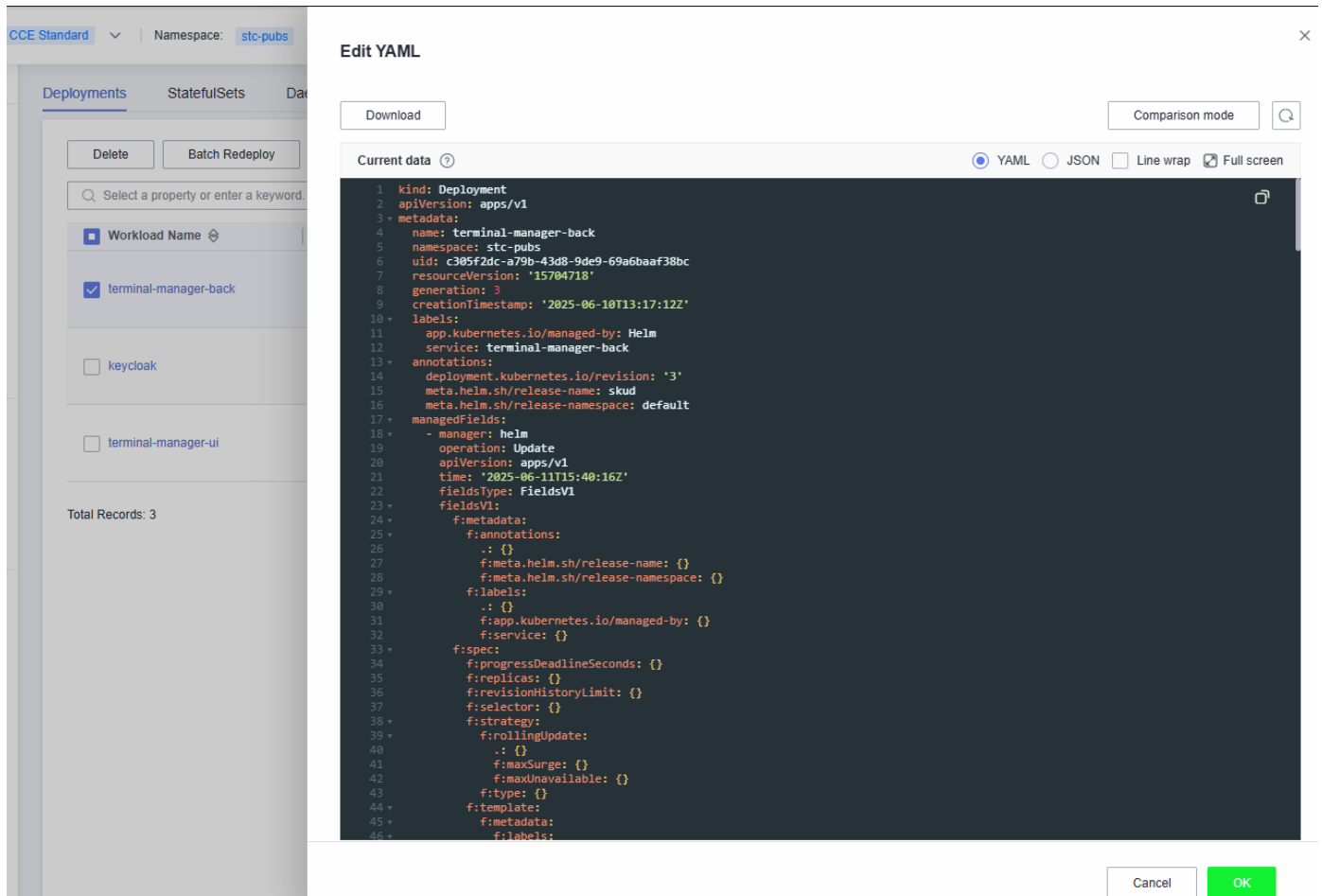


Рисунок 5 – Edit YAML



Все возможные параметры приведены в таблице ниже. При этом в настройках сервиса отображаются **не все параметры** (отсутствующие в настройках параметры применены со значениями по умолчанию, см. таблицу ниже). При необходимости изменить значения таких параметров **вручную добавьте их в настройки** с нужными значениями в формате:

- name: **Имя_параметра_из_таблицы**

value: 'Значение_параметра'

Например:

- name: **TERMINAL_HEARTBEAT_TASK_RUN_TIMEOUT_SEC**

value: '10'



Название	Значение по умолчанию	Описание
Общие настройки		
SERVER_PORT	9197	Порт Сервиса УТ .
TERMINAL_HEARTBEAT_TASK_RUN_TIMEOUT_SEC	5	Таймаут между запусками задания проверки состояния терминалов (в секундах).
ACTIVATION_CODE_RETRY_COUNT	3	Количество попыток ввода кода активации перед переводом устройства в статус Deactivated .
ACTIVATION_CODE_EXPIRED_HOURS	24	Время активности кода активации (в часах), по истечении которого код обновляется, если не был применен.
DEACTIVATION_TIME_HOURS	24	Время, через которое устройство деактивируется, если его состояние Stale (в часах).
HEARTBEAT_REQUEST_FREQUENCY_SECONDS	60	Частота получаемых heartbeat запросов (в секундах).
HEARTBEAT_TERMINAL_STALE_SECONDS	120	Время с момента последнего запроса heartbeat, через которое устройство переходит в состояние Stale (в секундах).
SBER_RC_REGISTER_TASK_RETRY_TIME_SEC	5	Частота попыток регистрации терминала в Сбер ПЦ, если запрос завершился ошибкой (в секундах).
SBER_RC_SYNC_TASK_RETRY_TIME_SEC	5	Частота попыток синхронизации терминала в Сбер ПЦ, если запрос завершился ошибкой (в секундах).
SBER_RC_SEARCH_CERT_TASK_RETRY_TIME_SEC	60	Частота попыток получения сертификата терминала в Сбер ПЦ, если запрос завершился ошибкой (в секундах).
SBER_RC_CERTIFICATE_TASK_RETRY_TIME_SEC	10	Частота попыток отправки CSR терминала в Сбер ПЦ, если запрос завершился ошибкой (в секундах).
SBER_RC_CRL_TASK_RETRY_TIME_SEC	60	Частота попыток получения CRL от Сбер ПЦ (в секундах).
INVALID_CERTIFICATE_TASK_RETRY_TIME_HOURS	12	Период проверки действительности сертификата терминала (в часах).
LIMIT_COUNT_REQUEST_CSR	14	Количество попыток отправки csr запроса.
LIMIT_PERIOD_REFRESH	1m	Период, за который возможно сделать n попыток отправки CSR-запроса. Возможные единицы измерения: ms (миллисекунды), s (секунды), m (минуты), h (часы).
TIME_DURATION	0	Задержка перед отправкой запроса (CSR). Возможные единицы измерения: ms (миллисекунды), s (секунды), m (минуты), h (часы).
GENERAL_LIMIT_COUNT_REQUEST	10	Количество попыток отправки запросов в Сбер (не CSR).



GENERAL_LIMIT_PERIOD_REFRESH	1s	Период, за который можно сделать n попыток отправки запроса (не CSR). Возможные единицы измерения: ms (миллисекунды), s (секунды), m (минуты), h (часы).
GENERAL_TIME_DURATION	0	Задержка перед отправкой запроса (не CSR). Возможные единицы измерения: ms (миллисекунды), s (секунды), m (минуты), h (часы).
FEIGN_CLIENT_CONNECTION_TIMEOUT_MS	10000	Таймаут подключения при обращении к СберПЦ (в миллисекундах).
FEIGN_CLIENT_READ_TIMEOUT_MS	90000	Таймаут ожидания данных при обращении к СберПЦ (в миллисекундах).
REGISTRATION_CENTER_URL	https://mc.api.sberbank.ru:443/prod/crt/bioscud/v1	Адрес сервиса СберПЦ.
LOGGER_FILE_PATH	terminal-manager-impl/src/main/resources/logger/logback.xml	Путь до файла с настройками логирования.
SWAGGER_ENABLED	true	Флаг для включения / отключения отображения интерфейса Swagger Сервиса УТ .
Настройки БД		
DB_URL	jdbc:postgresql://localhost:5444/postgres	URL для подключения к БД Сервиса УТ .
DB_USERNAME	postgres	Логин для подключения к БД Сервиса УТ .
DB_PASSWORD	123	Пароль для подключения к БД Сервиса УТ .
DB_CONNECTION_TIMEOUT_MS	20000	Таймаут подключения к БД.
Настройки авторизации Сервиса УТ		
KEYCLOAK_CERTS_URL	http://localhost:8080/realms/master/protocol/openid-connect/certs	Ссылка для получения публичных ключей.
KEYCLOAK_CERT_ALGORITHMS	RS256, RS512	Используемые алгоритмы шифрования.
SWAGGER_KEYCLOAK_URL	http://Server_name:8443/realms/master/protocol/openid-connect	URL openid-connect keycloak.



SECURITY_WHITELIST_LOCATION	terminal-manager-impl/src/main/resources/whitelist/whitelist.json	Путь до файла с разграничениями по ролям.
Настройки авторизации в системе Сбер		
SSL_CLIENT_ENABLED	true	Флаг для использования ssl при обращении к системе Сбер.
KEYSTORE_CERTIFICATE_PATH	terminal-manager-impl/src/main/resources/keystore/certificate_590fb22f-ff1f-43d0-814e-c8469dbc19b9.p12	Путь до файла сертификата Сбер (.p12). ВАЖНО: Сертификат активен в течение 1 года. До окончания периода активности сертификат необходимо обязательно перевыпустить в личном кабинете SberApi и заменить на сервере. Для перевыпуска сертификата необходимо обратиться к ответственному сотруднику (владелец продукта, Product Owner).
KEYSTORE_PASSWORD		Пароль от сертификата.
TRUSTSTORE_CERTIFICATE_PATH	terminal-manager-impl/src/main/resources/keystore/sber.crt	Путь до сертификата Сбер (для получения сертификата необходимо перейти по адресу https://mc.api.sberbank.ru/ и скачать сертификат в разделе защищенного подключения). ВАЖНО: не изменяйте значение параметра без дополнительных указаний от Сбера или команды разработки продукта.
TOKEN_CACHE_TIME_SEC	55	Время хранения токена доступа в кеше (в секундах).
TOKEN_REQUEST_SEC	45	Частота получения токена в Сбер ПЦ (в секундах).
SBER_TOKEN_URL	https://mc.api.sberbank.ru:443/prod/tokens/v3/oauth	Ссылка на получение токена. ВАЖНО: не изменяйте значение параметра без дополнительных указаний от Сбера или команды разработки продукта.
CLIENT_ID		ID клиента для авторизации. Значение параметра получает ответственный сотрудник (Product Owner) при подключении системы в личном кабинете SberApi.
CLIENT_SECRET		Secret клиента для авторизации. Значение параметра получает ответственный сотрудник (Product Owner) при подключении системы в личном кабинете SberApi.
GRANT_TYPE	client_credentials	Тип авторизации. ВАЖНО: не изменяйте значение параметра без дополнительных указаний от Сбера или команды разработки продукта.
SCOPE	auth://crt/bioscud	Ресурсы и данные, к которым предоставляется доступ. ВАЖНО: не изменяйте значение параметра без дополнительных указаний от Сбера или команды разработки продукта.

3.2. Настройка сервисов на объекте заказчика

Общий алгоритм установки и настройки сервисов системы:



1. Установите сервисы системы.
2. Создайте в картотеке ПК **Визирь.СКУД** шаблон, содержащий поля с именем **Bio** (тип поля – **Флаг**) и **PassId** (тип поля – **Строка**). Имена полей шаблона должны **обязательно** совпадать с именами, указанными в настройках сервиса **idp-organization-service** (см. [Настройка сервиса idp-organization-service](#)).
3. Настройте сервис **cbs-management-service** (см. [Настройка сервиса cbs-management-service](#)).
4. Настройте сервис **idp-organization-service** (см. [Настройка сервиса idp-organization-service](#)).
5. Настройте сервис **sberId-smartbio-integration-service** (см. [Настройка сервиса sberid-smartbio-integration-service](#)).
6. Настройте сервис **terminal-proxy-manager-service** (см. [Настройки сервиса terminal-proxy-manager-service](#)).

3.2.1. Настройка сервиса cbs-management-service

Для настройки параметров сервиса **cbs-management-service**:

1. Откройте файл **appsettings.json**, расположенный в каталоге **cbs-management-service** на вкладке **Key/Value** web-интерфейса **Consul**. Для перехода в web-интерфейс **Consul** введите в адресной строке браузера адрес в формате **Адрес_или_Имя_компьютера:8500**.
2. В файле **appsettings.json**:
 - В блоке параметров **users-service**:
 - В параметрах **ClientId** и **ClientSecret** укажите значение **acis**;
 - В параметрах **ApiName** и **ApiSecret** укажите значение **acis-service**.
 - В блоке параметров **cbs-management-service** в параметре **SberIdSmartBioServiceUrl** укажите адрес сервиса **sberid-smartbio-integration-service**.

Основные параметры сервиса **cbs-management-service** приведены в таблице ниже.

Таблица 1 – Настройки сервиса **cbs-management-service**

Название	Значение по умолчанию	Описание
CbsTimeout	00:00:05.000	Время ожидания ответа от сервиса интеграции с системой Сбер. Если аутентификация в системе Сбер проходит дольше указанного времени, пользователь будет получать отказ по причине таймаута. В лог-файлах сервиса cbs-management-service в этом случае отображается следующая ошибка: 408 Request timed out 00:00:05 seconds. Parameter `CbsTimeout` in settings



Название	Значение по умолчанию	Описание
MaxDegreeOfParallelism	2	Количество одновременно выполняемых параллельных потоков, которые будут обрабатывать лучший кадр (bestshot). Рекомендуемое значение параметра – не более количества ядер процессора компьютера.
PlaceholderPhotoCardPath	"Resources/placeholder_face.png"	Системная фотография-заглушка для обеспечения корректной работы системы. Размер изображения менее 4 Кбайт. Это изображение предназначено для прикрепления к тем карточкам, где будет отсутствовать фотография, для возможности прикрепления события идентификации. По умолчанию данное изображение размещено в дистрибутиве проекта.
SendIdentInfoToWS	true	Параметр для отключения проверки подключенных по WebSocket устройств и отправки в WebSocket сообщений. – true – требуется подключение клиентского приложения по WebSocket. Сервис отправляет сообщения IdentificationStarted и IdentificationResult по WebSocket. Внешняя система может использовать данные сообщения как один из методов интеграции; – false – подключение клиентского приложения по WebSocket не требуется, информацию о событии идентификации можно увидеть в web-интерфейсе ПК Визирь.СКУД или в лог-файлах.
CheckIdentInIDP	true	Параметр для отключения проверки событий Ident на наличие связи идентификаторов в сервисе idp-organization-service после получения события идентификации. – true – при ответе от сервиса интеграции с КБС со статусом "Ident" будет проводиться проверка наличия существующей связи с картотекой в ПК Визирь.СКУД, а также (при наличии возможности) будет отправлено событие об идентификации в ПК Визирь.СКУД; – false – при ответе от сервиса интеграции с КБС со статусом "Ident" не будет проводиться проверка наличия связи с картотекой в ПК Визирь.СКУД и не будет отправляться событие об идентификации в ПК Визирь.СКУД.
CheckIdentAccessProfiles	false	Параметр для включения проверки профиля доступа в методе биометрической аутентификации. – true – при ответе от сервиса интеграции с КБС со статусом "Ident" и при наличии связи с карточкой в ПК Визирь.СКУД, в методе биометрической аутентификации проверяется профиль доступа карточки; – false – в методе биометрической аутентификации не проверяется профиль доступа.
users-service		Адрес сервиса users-service .
events-service		Адрес сервиса events-service .
camera-service		Адрес сервиса camera-service .
person-cards-service		Адрес сервиса person-cards-service .
physical-access-profiles-service		Адрес сервиса physical-access-profiles-service .



Название	Значение по умолчанию	Описание
idp-organization-service		Адрес сервиса idp-organization-service .
SberIdSmartBioServiceUrl		Адрес сервиса sberid-smartbio-integration-service .

3.2.2. Настройка сервиса idp-organization-service

Для настройки параметров сервиса **idp-organization-service**:

- Откройте файл **appsettings.json**, расположенный в каталоге **idp-organization-service** на вкладке **Key/Value** web-интерфейса **Consul**. Для перехода в web-интерфейс **Consul** введите в адресной строке браузера адрес в формате **Адрес_или_Имя_компьютера:8500**.
- В файле **appsettings.json**:
 - Убедитесь, что значения параметров **CardNumberFieldName** и **BioFieldName** соответствуют названиям полей шаблона, созданного в web-интерфейсе ПК **Визирь** (см. [Настройка сервисов на объекте заказчика](#));
 - В блоке параметров **users-service**:
 - В параметрах **ClientId** и **ClientSecret** укажите значение **acis**;
 - В параметрах **ApiName** и **ApiSecret** укажите значение **acis-service**.

Основные параметры сервиса **idp-organization-service** приведены в таблице ниже.

Таблица 2 – Настройки сервиса **idp-organization-service**

Название	Значение по умолчанию	Описание
CardNumberFieldName	PassId	Имя поля шаблона, используемое для задания номера карты (пропуска) PassId.
BioFieldName	Bio	Имя поля шаблона, используемое для передачи признака наличия связи идентификатора карточки с КБС Id.
SyncPeriod	00:20:00.000	Частота актуализации (синхронизации) данных.
user-service		Параметры подключения к сервису users-service .
person-cards-service	http://<host_vizir>/person-cards-service	Адрес сервиса к person-cards-service , где host_vizir – доменное имя/адрес сервера, на котором развернут ПК Визирь.СКУД .
audit-service		Адрес сервиса audit-service .
DbSettings		Параметры подключения к базе данных.



3.2.3. Настройка сервиса sberid-smartbio-integration-service

Для настройки параметров сервиса **sberid-smartbio-integration-service**:

1. Откройте файл **appsettings.json**, расположенный в каталоге **sberid-smartbio-integration-service** на вкладке **Key/Value** web-интерфейса **Consul**. Для перехода в web-интерфейс **Consul** введите в адресной строке браузера адрес в формате **Адрес_или_Имя_компьютера:8500**.
2. В файле **appsettings.json**:
 - Настройте параметры интеграции с КБС (запросите значения параметров у менеджера КБС);
 - Установите значение параметра **DemoModeEnable = false**;
 - В блоке параметров **users-service**:
 - В параметрах **ClientId** и **ClientSecret** укажите значение **acis**;
 - В параметрах **ApiName** и **ApiSecret** укажите значение **acis-service**.

Основные параметры сервиса **sberid-smartbio-integration-service** приведены в таблице ниже.

Таблица 3 – Настройки сервиса **sberid-smartbio-integration-service**

Название	Значение по умолчанию	Описание
EnableSberTokenCaching	false	Параметр для активации / деактивации кеширования токена accessToken операции OAuth. Рекомендуемое значение – true. – true – использовать кеширование accessToken операции OAuth. В этом случае при отправке запроса на аутентификацию лучшего кадра, токен accessToken операции OAuth будет взят из кэша. При отсутствии в кэше токена, он будет запрошен в обычном режиме. Таким образом, несколько запросов на аутентификацию лучшего кадра могут использовать один accessToken операции OAuth; – false – кеширование accessToken операции OAuth не производится. В этом случае при каждом запросе на аутентификацию лучшего кадра будет отправляться запрос на получение accessToken операции OAuth.
TimeStoreTokenInCache	00:04:55.000	Время хранения accessToken операции OAuth в кэше. По умолчанию установлено оптимальное (рекомендуемое) значение. Параметр используется при установленном значении EnableSberTokenCaching = true.
TokenRenewalPeriod	00:04:45.000	Период времени, через который будет запрошен новый токен accessToken операции OAuth и помещен в кэш. При этом произойдет замена хранящегося в кэше accessToken. Функция отзыва accessToken не вызывается. По умолчанию установлено оптимальное (рекомендуемое) значение. Параметр используется при установленном значении EnableSberTokenCaching = true.



Название	Значение по умолчанию	Описание
SberTokenServiceUrl	https://oauth.sber.ru	URL адрес API СберID для авторизации.
SberBiometricAuthServiceUrl	https://100.73.141.17/	URL адрес API СберID для биометрического запроса.
OAuthPath	ru/prod/tokens/v2/oauth	Путь (часть URL адреса) для формирования первого запроса (получения токена доступа, access_token).
AuthenticatePath	api/v1/skud/auth-bio	Путь (часть URL адреса) для формирования второго запроса (на биометрическую аутентификацию).
ClientId	00000000-0000-0000-0000-000000000000	Идентификатор клиента, созданного в КБС Сбер SmartFace для получения токена авторизации. Значение параметра получает представитель Организации при подключении системы в личном кабинете SberApi .
ClientSecret	00000000-0000-0000-0000-000000000000	Секретная фраза для ClientId. Значение параметра получает представитель Организации при подключении системы в личном кабинете SberApi .
CertificatePassword	password	Данные доступа Организации, подключенной к СберID (пароль к сертификату). Значение параметра получает представитель Организации при подключении системы в личном кабинете SberApi .
CertificatePath	/var/cert/certificate_00000000-0-0000-0000-0000-000000000000.p12	Путь к сертификату на сервере. На хосте сертификат должен находиться в директории /opt/stc/cert . Значение параметра получает представитель Организации при подключении системы в личном кабинете SberApi . ВАЖНО: Сертификат активен в течение 1 года. До окончания периода активности сертификат необходимо обязательно перевыпустить в личном кабинете SberApi и заменить на сервере.
TimeoutFromSberId	00:00:10.000	Время в секундах, в течение которого сервис будет ожидать ответ от СберID .
GrantType	client_credentials	Данные для отправки запроса на аутентификацию (первый запрос): тип разрешения. ВАЖНО: не изменяйте значение параметра без дополнительных указаний от Сбера или команды разработки продукта.
Scope	api/v1/skud/auth-bio	Данные для отправки запроса на аутентификацию (первый запрос): область видимости (scope), которая предоставляется Клиенту. ВАЖНО: не изменяйте значение параметра без дополнительных указаний от Сбера или команды разработки продукта.
FormatType	jpeg	Данные для отправки CMS-пакета (запрос authenticate – биометрическая аутентификация, второй запрос). Допустимый формат – только jpeg . ВАЖНО: не изменяйте значение параметра без дополнительных указаний от Сбера или команды разработки продукта.
Channel	CRTDEMO	Данные для отправки CMS-пакета (запрос authenticate – биометрическая аутентификация, второй запрос): канал.



Название	Значение по умолчанию	Описание
DemoModeEnable	false	Флаг для переключения работы сервиса в Демо-режим . Демо-режим предполагает отправку двух типов сообщений, при любых входных лучших кадрах (bestshot): – Отправка сообщений Ident при DemoModelIdentResponse: true (см. параметр ниже); – Отправка сообщений Noident при DemoModelIdentResponse: false (см. параметр ниже).
DemoModelIdentResponse	true	Переключение режима работы (при работе в Демо-режиме): – true – отправка сообщений Ident; – false – отправка сообщений Noident.
DemoModeCloudId	00000000-0000-0000-0000-000000000000	При DemoModelIdentResponse: true данное значение будет возвращено как CloudId .
DemoModeCloudIdAlt	["00000000-0000-0000-0000-000000000000", "00000000-0000-0000-0000-000000000000"]	При DemoModelIdentResponse: true данное значение будет возвращено как CloudIdAlt .

3.2.4. Настройки сервиса terminal-proxy-manager-service

Для настройки параметров сервиса **terminal-proxy-manager-service** откройте файл **appsettings.json**, расположенный в каталоге **terminal-proxy-manager-service** на вкладке **Key/Value** web-интерфейса **Consul**. Для перехода в web-интерфейс **Consul** введите в адресной строке браузера адрес в формате **Адрес_или_Имя_компьютера:8500**.

Основные параметры сервиса **terminal-proxy-manager-service** приведены в таблице ниже.

Таблица 4 – Настройки сервиса **terminal-proxy-manager-service**

Название	Значение по умолчанию	Описание
UseMtls	true	Параметр для использования протокола mTLS при подключении к Сервису УТ .
CertificatePassword	password	Пароль для доступа к контейнеру с сертификатом и закрытым ключом.
CertificatePath	/var/cert/certificate_00000000-0000-0000-0000-	Путь к контейнеру с сертификатом и закрытым ключом. Контейнер имеет формат p12 . На хосте сертификат должен находиться в директории /opt/stc/cert/ .



Название	Значение по умолчанию	Описание
	000000000000.p12	
RetryFrequency	00:00:10.000	Частота повторных запросов в случае, когда метод, вызванный в Сервисе УТ , вернул ошибку.
ServiceHeartbeatFrequency	00:01:00.000	Частота отправки пакетов heartbeat в Сервис УТ . Значение параметра должно совпадать со значением параметра HEARTBEAT_REQUEST_FREQUENCY_SECONDS в настройках Сервиса УТ (см. Настройки Сервиса УТ).
TokenExpirationBuffer	00:00:05.000	Временной буфер перед истечением срока действия токена. Пример: если срок действия токена 60 секунд, то в кэше токен будет находиться меньше на указанное в параметре TokenExpirationBuffer время.
KeycloakUrl	https://localhost:8443	URL-адрес службы аутентификации Keycloak . Сервис Keycloak расположен в облачном сервисе, где развернут Сервис УТ . Для подключения к Keycloak укажите адрес https://auth.cbs.speechpro.com .
KeycloakTokenEndpoint	realms/master/protocol/openid-connect/token	Путь к конечной точке получения токена Keycloak .
KeycloakClientId		Идентификатор клиента для аутентификации в Keycloak (см. Создание клиентов в Keycloak).
KeycloakClientSecret		Секретный ключ клиента для аутентификации в Keycloak (см. Создание клиентов в Keycloak).
terminal-manager-service	http://localhost/terminal-manager-back/	Адрес Сервиса УТ ("back" часть). Для подключения к Сервису УТ укажите адрес https://api.cbs.speechpro.com/terminal-manager-back .



Для выпуска клиентского сертификата необходимо воспользоваться соответствующей инструкцией.

3.3. Инициализация терминала

Для корректной работы на терминал должны быть предварительно загружены соответствующие крипто-данные. Процесс переноса крипто-данных на терминал подробно описан в документе **Автоматизированный скрипт инициализации терминалов на АРМ Оператора. Описание работы.**

3.4. Активация терминала

Для активации терминала:

1. Перейдите в web-интерфейс **Сервиса УТ**.



2. В открывшемся окне нажмите кнопку **SIGN IN** (рис. 6).

Welcome to Terminal Manager Service

SIGN IN

Рисунок 6 – Вход в web-интерфейс **Сервиса УТ**

3. В открывшемся окне авторизации введите **имя** и **пароль** пользователя и нажмите кнопку **Sign in** (рис. 7).



Авторизация производится через сервис **Keycloak**. Для возможности авторизации, в сервисе **Keycloak** должны быть созданы учетные записи соответствующих пользователей / операторов (см. [Создание пользователей Сервиса УТ в Keycloak](#)).

KEYCLOAK

Sign in to your account

Username or email

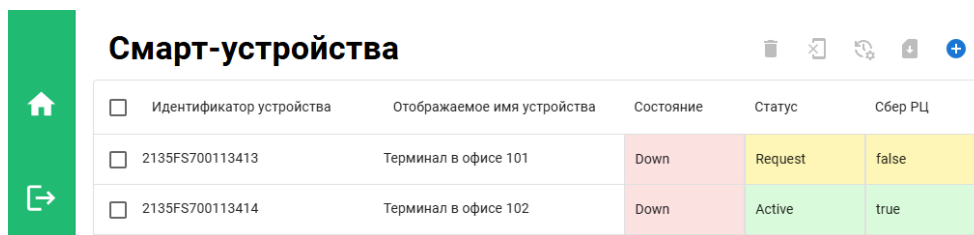
Password

Sign In

Рисунок 7 – Окно авторизации



4. В открывшемся окне нажмите кнопку , расположенную в правом верхнем углу экрана (рис. 8).

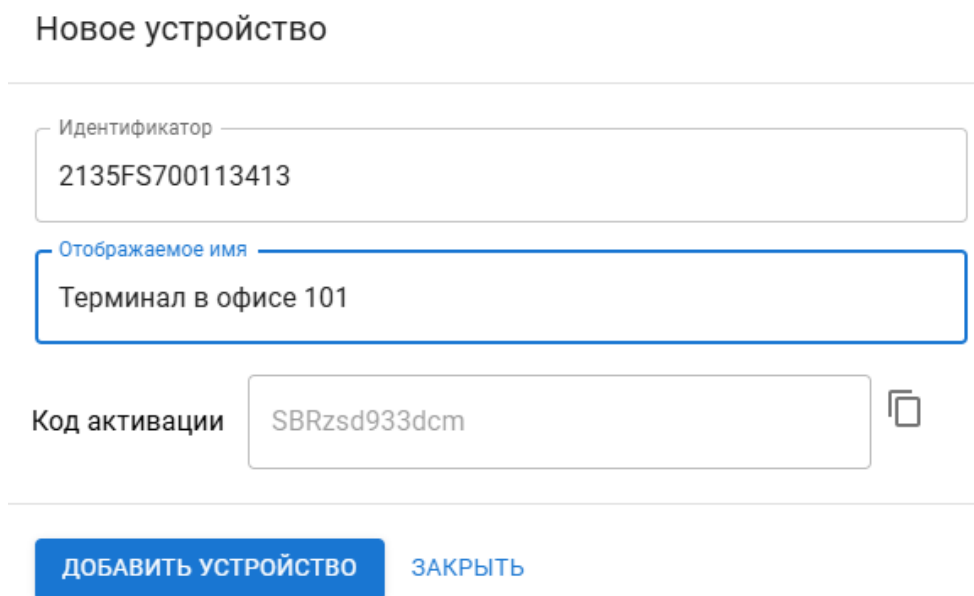


The interface shows a sidebar with a home icon and a right arrow icon. The main area is titled 'Смарт-устройства' and contains a table with columns: 'Идентификатор устройства', 'Отображаемое имя устройства', 'Состояние', 'Статус', and 'Сбор РЦ'. There are two rows of data.

☐	Идентификатор устройства	Отображаемое имя устройства	Состояние	Статус	Сбор РЦ
☐	2135FS700113413	Терминал в офисе 101	Down	Request	false
☐	2135FS700113414	Терминал в офисе 102	Down	Active	true

Рисунок 8 – Список устройств

5. В открывшемся окне (рис. 9) заполните следующие поля:
- **Идентификатор** – укажите **SN** (серийный номер) терминала. **SN указан на корпусе устройства;**
 - **Отображаемое имя** – укажите имя устройства, которое будет отображаться в web-интерфейсе системы;
 - Скопируйте или запишите **автоматически** сгенерированный **Код активации** – он потребуется на следующих шагах;
 - После ввода данных нажмите кнопку **Добавить устройство**.



The form is titled 'Новое устройство'. It contains three input fields: 'Идентификатор' with the value '2135FS700113413', 'Отображаемое имя' with the value 'Терминал в офисе 101', and 'Код активации' with the value 'SBRzsd933dcm'. There is a copy icon next to the activation code field. At the bottom, there are two buttons: 'ДОБАВИТЬ УСТРОЙСТВО' and 'ЗАКРЫТЬ'.

Новое устройство

Идентификатор
2135FS700113413

Отображаемое имя
Терминал в офисе 101

Код активации
SBRzsd933dcm

ДОБАВИТЬ УСТРОЙСТВО ЗАКРЫТЬ

Рисунок 9 – Добавление устройства

6. В результате устройство будет добавлено в список устройств (рис. 10). При этом:



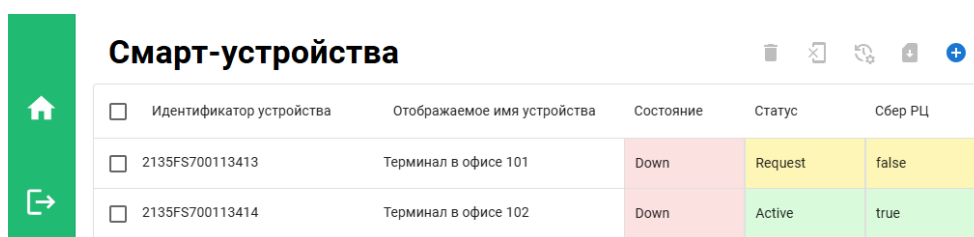
- Для **просмотра параметров** добавленного устройства нажмите на устройство (одинарный щелчок левой кнопкой мыши);
- Для **деактивации** устройства выберите устройство в списке (установите флаг ) и нажмите кнопку  в правом верхнем углу экрана;
- Для **удаления** устройства выберите устройство в списке (установите флаг ) и нажмите кнопку  в правом верхнем углу экрана;
- Для **выхода** из web-интерфейса **Сервиса УТ** нажмите кнопку .

В поле **Состояние** отображается информация об активности терминала со стороны самого устройства, корректности его работы и наличии связи с сервером:

- **Down** – устройство деактивировано или еще не активировано;
- **Live** – устройство доступно, присылает heartbeat, работает без ошибок;
- **Error** – устройство доступно, присылает heartbeat, но работает с ошибкой;
- **Stale** – устройство не присылает heartbeat.

В поле **Статус** отображается информация о статусе терминала со стороны **Сервиса УТ**:

- **Request** – устройство добавлено администратором в **Сервис УТ**, ожидается активация со стороны терминала;
- **Active** – устройство активировано;
- **Deactivated** – устройство деактивировано администратором или автоматически после определенного времени в состоянии **Stale**.



Идентификатор устройства	Отображаемое имя устройства	Состояние	Статус	Сбор РЦ
2135FS700113413	Терминал в офисе 101	Down	Request	false
2135FS700113414	Терминал в офисе 102	Down	Active	true

Рисунок 10 – Список устройств

7. На терминале:

- Откройте установленное приложение **CBS Client** из списка приложений мобильного устройства.
- В открывшемся окне укажите данные для активации терминала (рис. 11, **1**):



- В поле **Введите адрес сервера** укажите адрес сервиса **terminal-proxy-manager-service**;
- В поле **Введите код активации** введите код активации устройства, полученный на шаге 5.
- Нажмите кнопку **Активировать**.

При активации терминал получает сертификат и список отозванных сертификатов (рис. 11, **2** и **3**). Если криптоданные получены успешно, терминал переходит в рабочий режим (рис. 11, **4**).

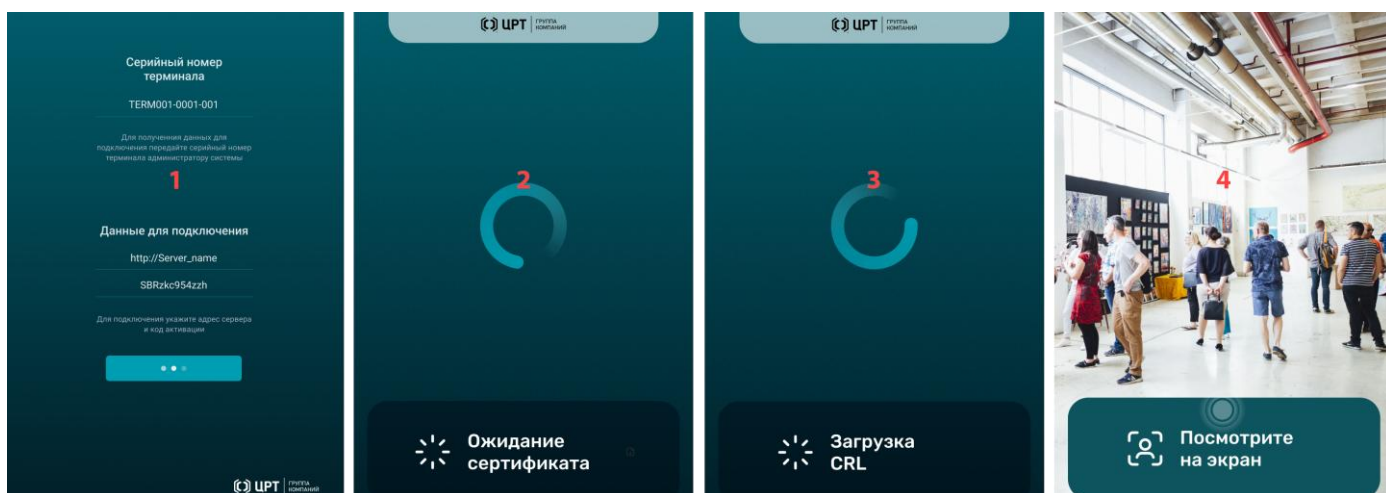


Рисунок 11 – Активация терминала

3.5. Настройка терминала

Настройте терминал, используемый для распознавания лиц:

1. Откройте установленное приложение **CBS Client** из списка приложений терминала.
2. Перейдите в настройки приложения: для этого нажмите на экран устройства 5 раз подряд. В открывшемся окне введите PIN-код. По умолчанию PIN-код состоит из 6 символов: 3 первых и 3 последних символа серийного номера терминала.

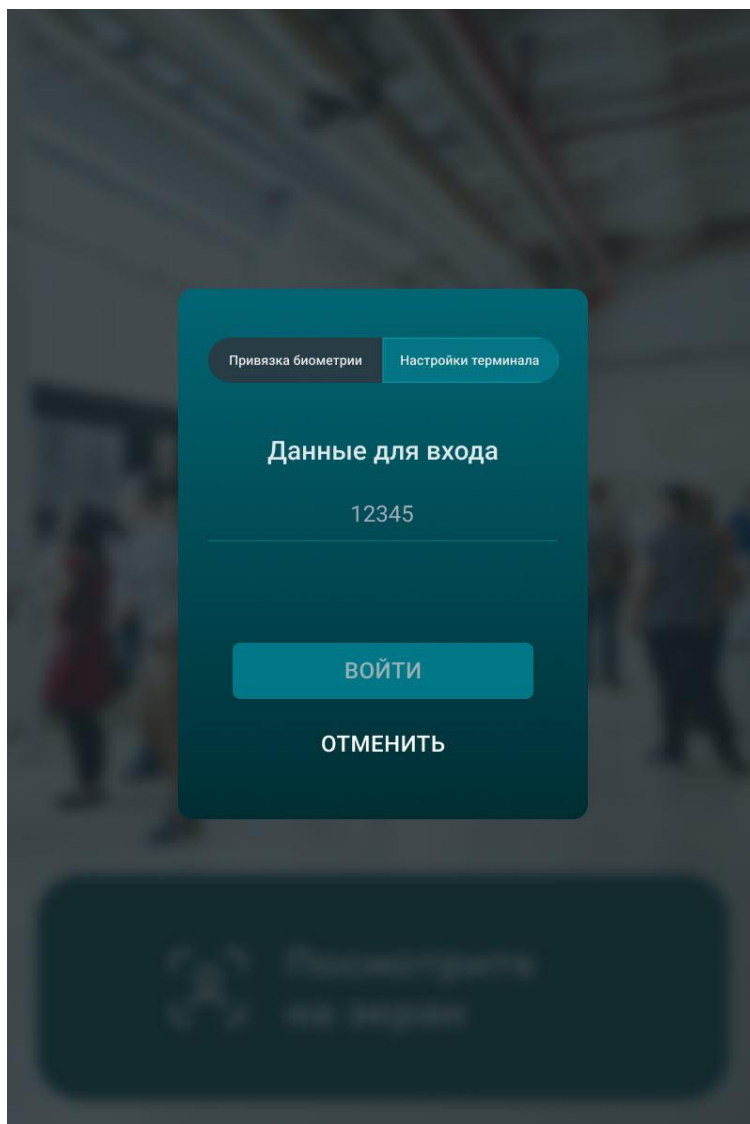


Рисунок 12 – Настройки терминала

Таблица 5 – Настройки мобильного приложения

Название	Описание
Идентификатор устройства	ID мобильного устройства (требуется для добавления устройства в web-интерфейсе Сервиса УТ).
Настройки работы с лицами	
Размер лица, px	Минимальный детектируемый размер лица (в пикселях).
Порог качества детекции, %	Порог детектирования лиц (в процентах). Служит для отсеивания событий со слишком низким качеством. Диапазон значений – от 0 до 100.



Название	Описание
Порог срабатывания liveness, %	Порог срабатывания детектора Liveness. Диапазон значений – от 0 до 100 (где 0 означает, что проверка на Liveness отключена). Обратите внимание! Для ускорения работы с лицами с различными портретными характеристиками (очки, борода, отсутствие волос на голове и т.д.) рекомендуется устанавливать значение 60 .
Наклон вбок (Roll), %	Порог угла наклона лица вбок (в радианах). Лицо в фокусе камеры не будет задетектировано, если оно будет наклонено в бок больше настроенного угла.
Наклон вперед (Pitch), %	Порог угла наклона лица вперед (в радианах). Лицо в фокусе камеры не будет задетектировано, если оно будет наклонено вперед больше настроенного угла.
Поворот (Yaw), %	Порог угла поворота лица (в радианах). Лицо в фокусе камеры не будет задетектировано, если оно будет повернуто больше настроенного угла.
Размытие (Blur), %	Порог размытия изображения лица. Лицо в фокусе камеры будет задетектировано , если полученное значение будет больше настроенного значения.
Освещение (Light), %	Порог освещенности лиц. Лицо в фокусе камеры не будет задетектировано, если оно будет освещено меньше настроенного значения.
Яркость (Brightness), %	Порог яркости лиц. Лицо в фокусе камеры не будет задетектировано, если яркость изображения будет больше настроенного значения.
Порог качества изображения, %	Порог качества изображения лица. Лицо в фокусе камеры не будет задетектировано, если качество изображения будет меньше настроенного значения.
Порог наличия очков (Glasses), %	Порог наличия на лице очков. При значении 100 лицо будет задетектировано независимо от наличия / отсутствия на нем очков.
Порог наличия маски (Mask)	Порог наличия на лице маски. При значении 100 лицо будет задетектировано независимо от наличия / отсутствия на нем маски.
Порог наличия головного убора (Hat)	Порог наличия головного убора. При значении 100 лицо будет задетектировано независимо от наличия / отсутствия головного убора.
Порог наличия головного платка (Shawl)	Порог наличия головного платка. При значении 100 лицо будет задетектировано независимо от наличия / отсутствия головного платка.



Название	Описание
Порог наличия солнцезащитных очков (Sunglasses), %	Порог наличия на лице солнцезащитных очков. При значении 100 лицо будет задетектировано независимо от наличия / отсутствия на нем солнцезащитных очков.
Порог перекрытия лица (Overlap), %	Порог перекрытия лица посторонними предметами. При значении 100 лицо будет задетектировано независимо от наличия / отсутствия посторонних предметов.
Очки (Eye Glasses), %	Порог наличия на лице очков. При значении 100 лицо будет задетектировано независимо от наличия / отсутствия на нем очков.
Открытость глаз (Eye open), %	Порог открытости глаз. При значении 0 лицо будет задетектировано независимо от степени открытости глаз.
Видимость глаз (Eye Obscureness), %	Порог видимости глаз (перекрытия глаз посторонними предметами). При значении 100 лицо будет задетектировано независимо от перекрытия глаз посторонними предметами.
Улыбка (Smile), %	Порог улыбки на лице. При значении 100 лицо будет задетектировано независимо от наличия / отсутствия на лице улыбки.
Открытость рта (Mouth open), %	Порог открытия рта. При значении 100 лицо будет задетектировано независимо от степени открытия рта.
Видимость рта (Mouth Obscureness), %	Порог видимости рта (перекрытия рта посторонними предметами). При значении 100 лицо будет задетектировано независимо от перекрытия рта посторонними предметами.
Рамка детекции	Включение / отключение отображения рамки вокруг лица при детекции.
Количество попыток перед отказом	Максимальное количество попыток отправки лучшего кадра на идентификацию. Возможные значения: 1-5. Рекомендуемое значение – 2. Алгоритм работы параметра: 1. Если значение параметра Количество попыток перед отказом равно 1, то, при получении события неидентификации с сервера отображается красный экран запрета прохода. 2. Если значение параметра Количество попыток перед отказом больше 1 (2...5), то накапливается необходимое количество дополнительных лучших кадров, и, при получении события неидентификации с сервера, происходит отправка на идентификацию следующего лучшего кадра. Следующий лучший кадр должен быть сформирован не позднее 2 секунд после предыдущего. 3. Во время всех попыток идентификации на устройстве отображается экран ожидания. 4. Варианты завершения данного цикла:



Название	Описание
	– Если в результате одной из попыток идентификации получено сообщение идентификации – номер карты сотрудника отправляется на контроллер СКУД, и, после получения ответа отображается соответствующий ответу контроллера результат на экране устройства (допуск или отказ в допуске); – Если в результате всех попыток идентификации с сервера было получено событие неидентификации – отображается красный экран запрета прохода; – Если не удалось собрать все необходимые лучшие кадры (например, плохие условия освещенности, пользователь отвернулся от экрана и прочее), а по отправленным лучшим кадрам вернулись неидентификации – через 2 секунды после формирования последнего лучшего кадра отображается красный экран запрета прохода. 5. Данный параметр распространяется только на отказы в проходе, получаемые с сервера (не распространяется на отказы контроллера СКУД).
Количество успешных bestshot перед отправкой	Максимальное количество зафиксированных лучших кадров перед отправкой кадра на идентификацию. Возможные значения: 1-5. Рекомендуемое значение – 2. На идентификацию отправляется самый последний сформированный лучший кадр.
Настройка интерфейсов и камеры	
Корректировка экспозиции	Переключатель для включения / отключения корректировки экспозиции изображения с камеры мобильного устройства. При активации данного параметра экспозиция камеры будет меняться автоматически. Рекомендуемое значение – параметр активирован.
Фиксирование фокуса	Переключатель для активации / деактивации фиксации фокусного расстояния камеры: – При активации параметра фокус камеры будет зафиксирован на расстоянии, указанном в параметре Фокусное расстояние, см. – При деактивации параметра используется автофокусировка камеры.
Фокусное расстояние, см	Расстояние от камеры терминала, на котором объект находится в фокусе камеры. Параметр используется при активированном параметре Фиксирование фокуса. Диапазон значений: 10-100 см.
Подсветка	Активация подсветки мобильного устройства.
Подсветка загорается при детекции	Переключатель для включения / отключения подсветки устройства при детектировании лица. При активации данной опции подсветка будет включаться только при



Название	Описание
	детектировании лица, в остальное время подсветка будет выключена.
Реле	Переключатель для включения / отключения управляющего реле устройства, используемого для управления подключенным турникетом (при наличии реле на устройстве).
Задержка реле, мс	Время, на которое происходит размыкание реле устройства (в миллисекундах). Значение параметра необходимо вычислять опытным путем в зависимости от конфигурации объекта. Возможные значения: 0 - 20 000 мс.
Wiegand	Переключатель для включения / отключения возможности подключения и передачи данных по интерфейсу Wiegand .
Система счисления кода wiegand	Используемая система счисления (система счисления, которая будет использоваться для распознавания кодов карт PassId). Возможные значения: – DEC (десятичная); – HEX (шестнадцатеричная).
Формат wiegand	Используемый формат Wiegand .
Задержка между отправкой карт, мс	Время в миллисекундах, на которое происходит задержка перед отправкой следующей карты доступа, если в PassId передано несколько карт доступа. Возможные значения: 0 - 5000. При значении параметра 0 следующая карта отправляется сразу после получения отрицательного ответа по ранее отправленной карте без дополнительных задержек. Во время отправки карт доступа отображается экран ожидания (включая время задержки).
Timeout ожидания ответа от контроллера, мс	Время в миллисекундах, в течение которого терминал ожидает ответ от контроллера СКУД после отправки номера карты по wiegand . При отсутствии ответа за указанное время, на терминале отображается сообщение об отказе в доступе. Возможные значения: 1000 - 10 000.
RFID	Переключатель для включения / отключения возможности прохода с помощью прикладывания карты к считывателю карт доступа (см. Проход по карте (RFID)). Обратите внимание: – Доступен только режим Однофакторный (ИЛИ), позволяющий проходить по лицу или карте; – Для работы в режиме Однофакторный (ИЛИ) обязательно должен быть активирован переключатель Wiegand.
Выводимая информация	



Название	Описание
Время отображения сообщения (мс)	Время (длительность) отображения сообщений на экране устройства (в миллисекундах).
Экран допуска	Переключатель для включения / отключения отображения экрана допуска при успешной идентификации лица.
Текст приветствия	Текст приветственного сообщения, отображаемого на экране устройства при успешной идентификации лица.
Экран отказа	Переключатель для включения / отключения отображения экрана отказа в доступе.
Сообщение при неидентификации	Текст сообщения, отображаемого на экране устройства при неидентификации лица.
Сообщение при отказе от контроллера	Текст сообщения, отображаемого на экране устройства при отказе в доступе от контроллера СКУД.
Экран ожидания	Переключатель включения / отключения отображения экрана ожидания. Данный переключатель, а также параметр Текст экрана ожидания (см. ниже) отображаются только при активированных переключателях Экран допуска и Экран отказа .
Текст экрана ожидания	Текст сообщения, отображаемого на экране устройства при ожидании ответа на запрос идентификации.
Системные настройки	
Частота отправки heartbeat (сек)	Интервал в секундах между отправкой пакетов HeartBeat (в секундах). Возможные значения: 1 - 100. Рекомендуемое значение – 10 секунд.
Time bomb (часы)	Время в часах, через которое произойдет деактивация терминала при отсутствии связи с сервером. Возможные значения: 1 - 24 000.
Редактирование картотеки	Переключатель для включения / отключения возможности редактирования картотеки. При активации параметра: 1. В разделе Картотека отображается кнопка для добавления новых карточек. 2. При просмотре карточки отображается кнопка Удалить карточку .
Инструкция СберID при онбординге	Активация / деактивация отображения инструкции по проверке профиля в СберID при работе в режиме регистрации пользователей в системе (онбординг): – Опция активирована – при нажатии на кнопку Привязать биометрию в карточке пользователя, отображается инструкция по проверке профиля в СберID (см. Проверка подключения биометрии в СберID);



Название	Описание
	– Опция деактивирована – при нажатии на кнопку Привязать биометрию в карточке пользователя, происходит переход к процессу аутентификации.
Название сервиса для отправки sms пакета	URL-адрес сервиса системы для отправки запроса с SMS пакетом при биометрическом проходе. При работе в режиме онбординга всегда используется сервис CBS-Management-Service .
Режим аутентификации по команде	При активированном переключателе терминал получает команду на аутентификацию по WebSocket от сервиса, указанного в параметре Название сервиса для соединения по WebSocket (см. ниже). При этом bestshot отправляются в сервис, указанный в параметре Название сервиса для отправки sms пакета . Режим аутентификации по команде используется при работе со СКУД Аспект .
Текст экрана ожидания аутентификации	Текст сообщения, отображаемого на экране терминала до появления по WebSocket команды на старт процесса детектирования лица.
Название сервиса для соединения по WebSocket	URL-адрес сервиса интеграции со СКУД, используемого при работе в Режиме аутентификации по команде .
Время ожидания лица, мс	Время ожидания лица в кадре для распознавания (в миллисекундах). По истечении времени ожидания лица отображается экран ожидания аутентификации. Возможные значения: 1000 - 10 000.
О приложении	
Пароль входа в настройки	Пароль (PIN-код) для входа в настройки терминала. Пароль формируется автоматически и по умолчанию состоит из 3 первых и 3 последних символов идентификатора терминала. Пароль можно редактировать. Требования к паролю: – Длина пароля – от 3 до 10 символов; – Допустимые символы: латинские буквы и цифры 0-9.
Версия приложения	Текущая версия установленного на устройство приложения (поле недоступно для редактирования).

3.6. Дополнительная информация

3.6.1. Создание клиентов в Keycloak

Для каждой организации, использующей терминалы, в сервисе **Keycloak** должны быть созданы соответствующие клиенты: необходимо создать клиента для сервиса **terminal-proxy-manager-service**, который устанавливается в контуре организации, пользующейся терминалами.

Для создания клиента организации:



1. Перейдите в **Keycloak**.
2. В открывшемся окне авторизации введите **имя** и **пароль** пользователя и нажмите кнопку **Sign in** (рис. 13).

KEYCLOAK

Sign in to your account

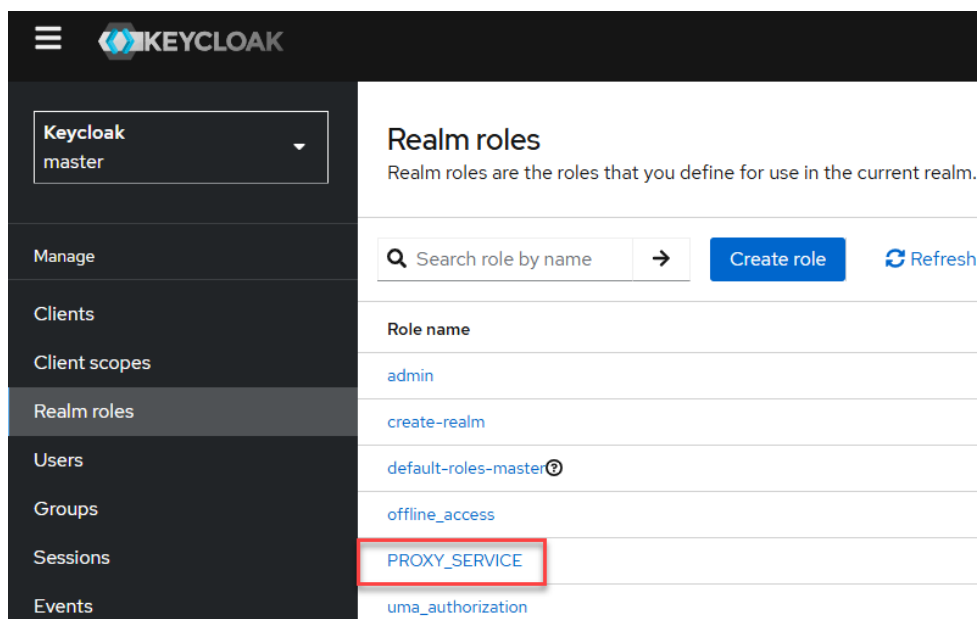
Username or email

Password

Sign In

Рисунок 13 – Окно авторизации

3. Перейдите на вкладку **Realm roles** и убедитесь, что создана роль **PROXY_SERVICE** (рис. 14).

Рисунок 14 – Вкладка **Realm roles**

4. Перейдите на вкладку **Clients** и нажмите кнопку **Create client**.
5. В открывшемся окне:
 - На вкладке **General settings** укажите **уникальное** имя создаваемого клиента в поле **Client ID** и нажмите кнопку **Next** (рис. 15);

[Clients](#) > Create client

Create client

Clients are applications and services that can request authentication of a user.

1 General settings

2 Capability config

3 Login settings

Client type ⓘ

OpenID Connect

Client ID * ⓘ

terminal-proxy-manager-service_Company_name

Name ⓘ

Description ⓘ

Always display in UI ⓘ ☐ Off

Back

Next

Cancel

Рисунок 15 – Вкладка **General settings**

- На вкладке **Capability config** активируйте опции **Client authentication** и **Service accounts roles** и нажмите кнопку **Next** (рис. 16);

[Clients](#) > Create client

Create client

Clients are applications and services that can request authentication of a user.

1 General settings

2 Capability config

3 Login settings

Client authentication ☒ On

Authorization ☐ Off

Authentication flow

☒ Standard flow

☐ Implicit flow

☐ OAuth 2.0 Device Authorization Grant

☐ OIDC CIBA Grant

☒ Direct access grants

☒ Service accounts roles

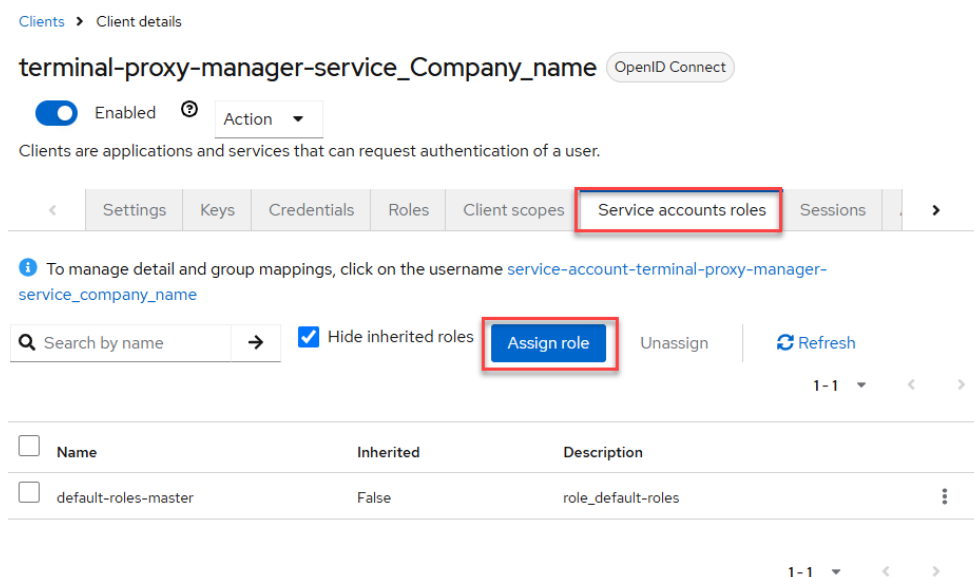
Back

Next

Cancel

Рисунок 16 – Вкладка **Capability config**

- На вкладке **Login settings** нажмите кнопку **Save**;
- 6. Будет открыто окно с параметрами созданного клиента. Перейдите на вкладку **Service accounts roles** и нажмите кнопку **Assign role** (рис. 17).

Рисунок 17 – Вкладка **Service accounts roles**

7. В открывшемся окне (рис. 18):

- Установите значение фильтра **Filter by realm roles** в левом верхнем углу окна;
- Выберите роль **PROXY_SERVICE**;
- Нажмите кнопку **Assign**.



Assign roles to terminal-proxy-manager-service_Company_name

Filter by realm roles

Search by role name

Refresh

☐	Name	Description
☐	admin	role_admin
☐	create-realm	role_create-realm
☐	offline_access	role_offline-access
☒	PROXY_SERVICE	–
☐	uma_authorization	role_uma_authorization

Assign

Cancel

Рисунок 18 – Выбор роли

8. Перейдите на вкладку **Advanced**. В открывшемся окне (рис. 19):

- В группе настроек **Advanced settings** установите для параметра **Access Token Lifespan** значение **Expires in 1 Hours**;
- Нажмите кнопку **Save**, расположенную в группе настроек **Advanced settings**.

Advanced settings

This section is used to configure advanced settings of this client related to OpenID Connect protocol

Access Token Lifespan ?

Expires in

1

Hours

Client Session Idle ?

Inherits from realm settings

Client Session Max ?

Inherits from realm settings

Client Offline Session Idle ?

Inherits from realm settings

Рисунок 19 – **Advanced settings**

9. Перейдите в настройки сервиса **terminal-proxy-manager-service**, установленного в контуре организации, пользующейся терминалами.



10. В настройках сервиса **terminal-proxy-manager-service**:

- В параметре **KeycloakUrl** укажите адрес сервиса **Keycloak**;
- В параметре **terminal-manager-service** укажите адрес сервиса **terminal-manager-service**, установленного в облачном сервисе;
- В параметре **KeycloakClientId** укажите значение, указанное в поле **Client ID** на шаге 5;
- В параметре **KeycloakClientSecret** укажите значение параметра **Client Secret**, расположенного в настройках созданного клиента на вкладке **Credentials** (рис. 20).

Clients > Client details

terminal-proxy-manager-service_Company_name OpenID Connect ☒ Enabled ⓘ Action ▾

Clients are applications and services that can request authentication of a user.

Settings Keys **Credentials** Roles Client scopes Service accounts roles Sessions Advanced Events

Client Authenticator ⓘ Client Id and Secret ▾

Save

Client Secret ⓘ BwgtuMlaNe0TgYDE8eSjUdLDwK2shG4n ⓘ Copy Regenerate

Registration access token ⓘ [Redacted] ⓘ Copy Regenerate

Рисунок 20 – Вкладка **Credentials**

3.6.2. Создание пользователей Сервиса УТ в Keycloak

Для возможности авторизации, необходимо создать соответствующие учетные записи пользователей.

Для создания учетной записи:

1. Перейдите в **Keycloak**.
2. В открывшемся окне авторизации введите **имя** и **пароль** пользователя и нажмите кнопку **Sign in** (рис. 21).

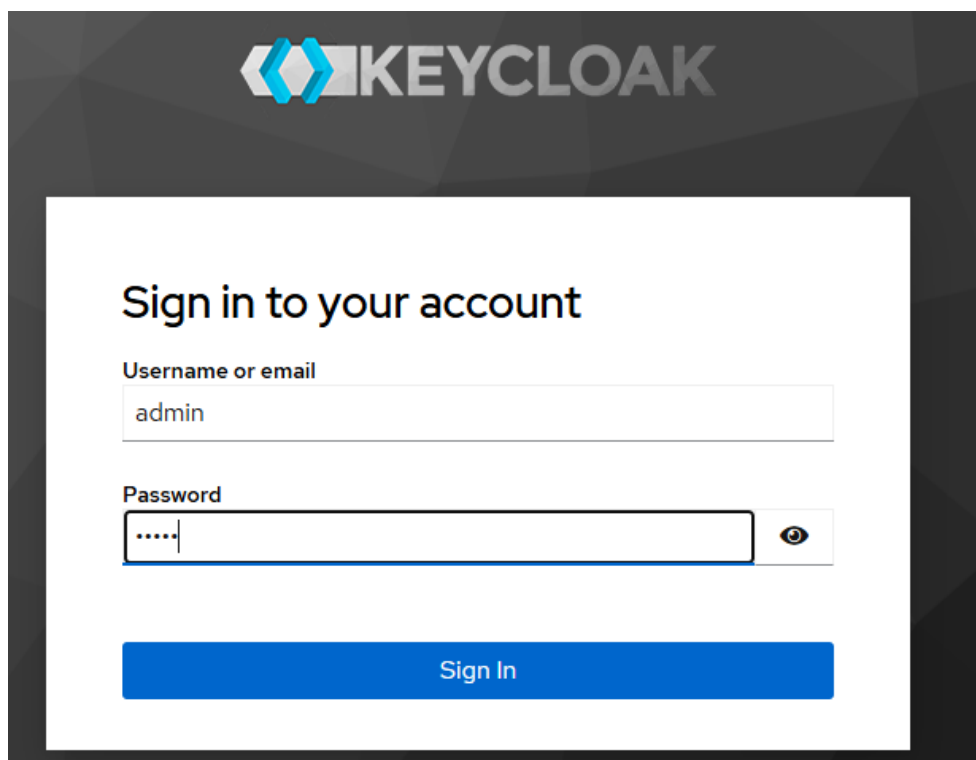
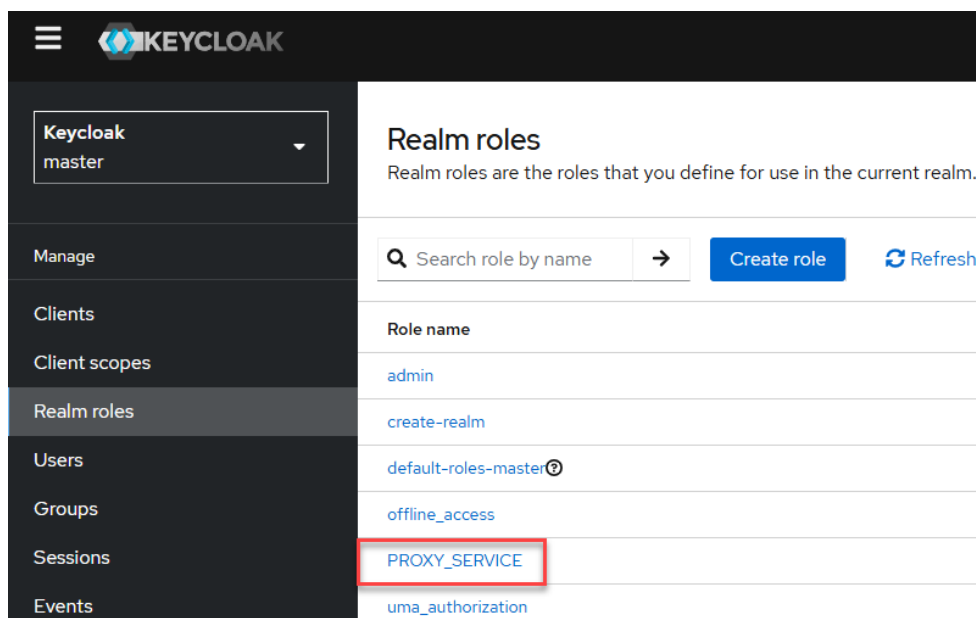


Рисунок 21 – Окно авторизации

3. Перейдите на вкладку **Realm roles** и убедитесь, что создана роль **PROXY_SERVICE** (рис. 22).

Рисунок 22 – Вкладка **Realm roles**

4. Перейдите на вкладку **Users** и нажмите кнопку **Add user**.



5. В открывшемся окне укажите **уникальное** имя создаваемого пользователя в поле **Username** и нажмите кнопку **Create** (рис. 23);

Рисунок 23 – Создание пользователя

6. Будет открыто окно с параметрами созданного пользователя. Перейдите на вкладку **Role mapping** и нажмите кнопку **Assign role** (рис. 24).

Рисунок 24 – Вкладка **Role mapping**

7. В открывшемся окне (рис. 25):
- Установите значение фильтра **Filter by realm roles** в левом верхнем углу окна;
 - Выберите роль **PROXY_SERVICE**;



- Нажмите кнопку **Assign**.

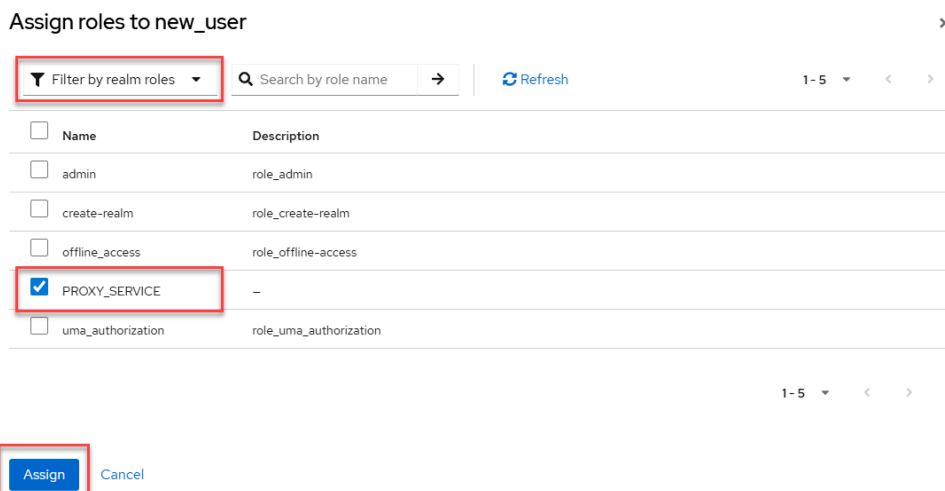


Рисунок 25 – Выбор роли

3.6.3. Просмотр лог-файлов Сервиса УТ

Для просмотра лог-файлов **Сервиса УТ**:

- Авторизуйтесь в облачном сервисе, где развернут **Сервис УТ**;
- В меню **Service List** выберите **Cloud Container Engine** (рис. 26);

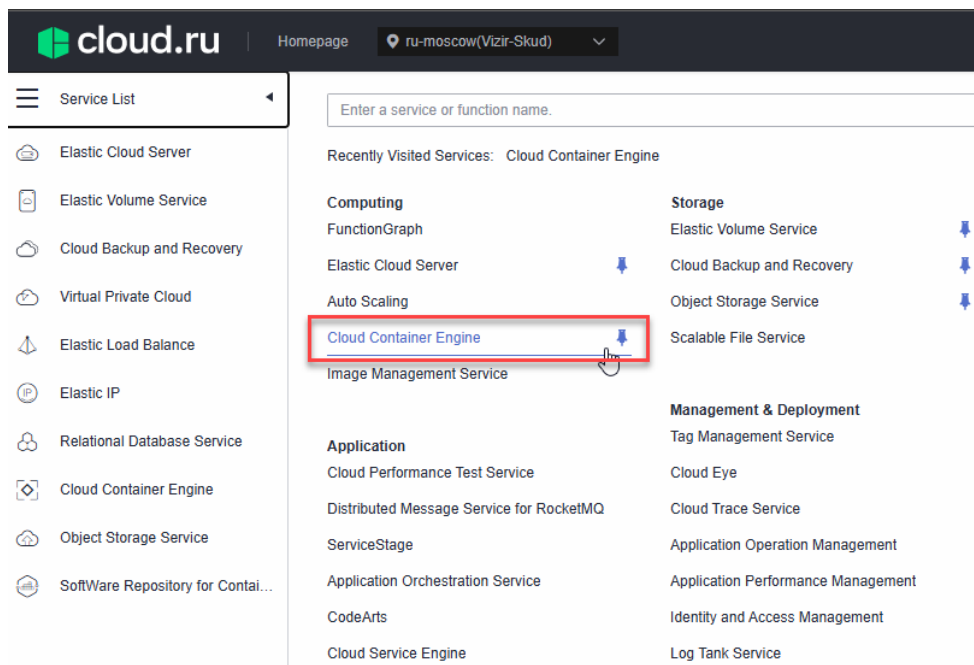


Рисунок 26 – Cloud Container Engine

- В открывшемся окне на вкладке **Clusters** перейдите в проект **cce-cluster** (рис. 27);

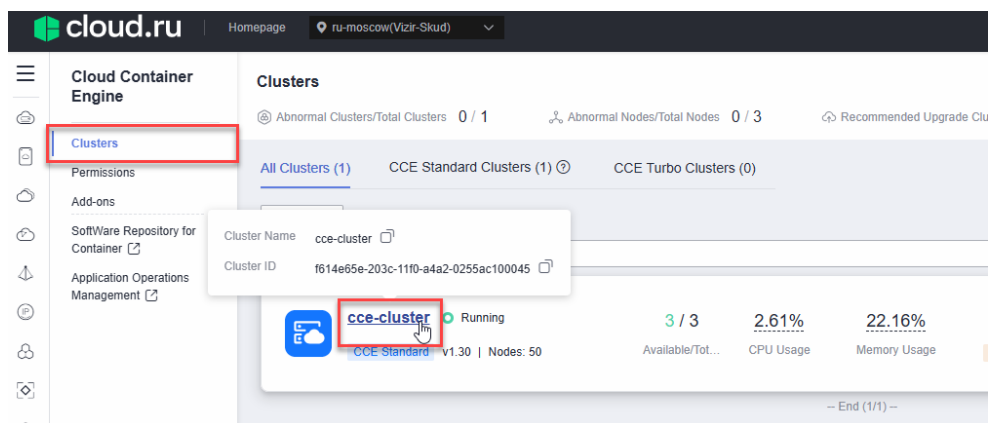


Рисунок 27 – cce-cluster

– Перейдите во вкладку **Workloads > Deployments** и в строке **terminal-manager-back** нажмите кнопку **View Log** (рис. 28).

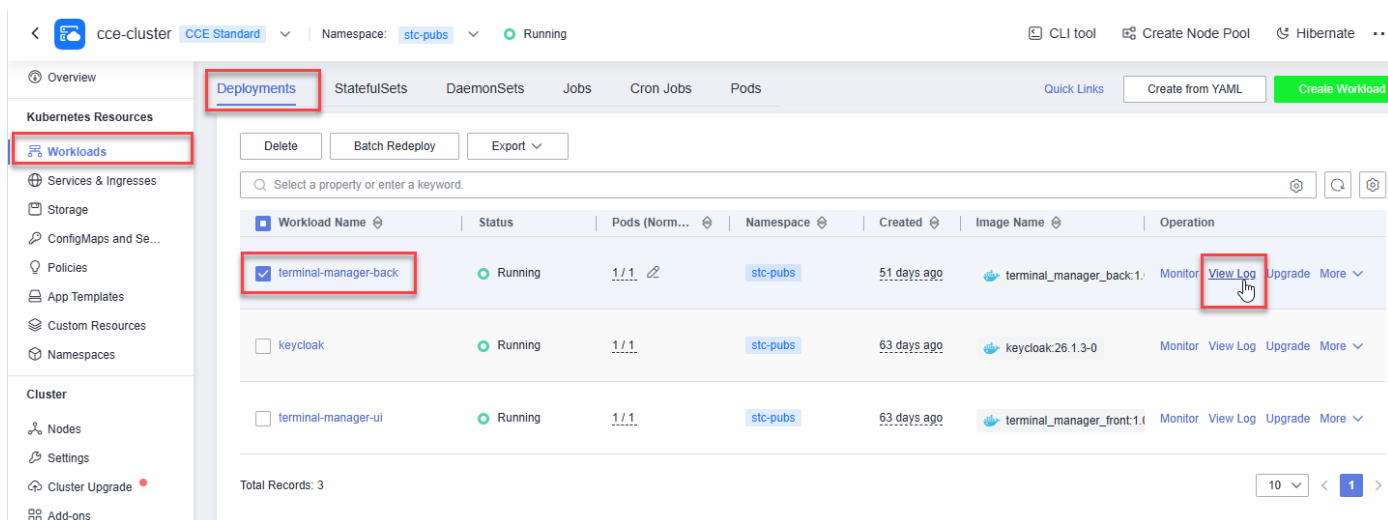


Рисунок 28 – View Log

В результате в правой части экрана будет отображена область, содержащая лог-файл сервиса (рис. 29, 1).

При наличии нескольких экземпляров сервиса, выберите нужный контейнер в поле **Pod** (рис. 29, 2).



Параметры логирования (см. [Параметры логирования](#)) настраиваются в конфигурационном файле **logback.xml**. Для доступа к файлу перейдите во вкладку **ConfigMaps and Secrets** и в строке **terminal-manager-back-configmap** нажмите кнопку **Edit YAML**. После редактирования файла необходимо перезапустить сервис. Для этого во вкладке **Workloads > Pods** выберите (установите чекбокс) сервис **terminal-manager-back...** и нажмите кнопку **Delete**. В открывшемся диалоговом окне подтвердите удаление.

The screenshot shows the Kubernetes UI interface. On the left, the 'Deployments' tab is active, showing a list of workloads. The 'terminal-manager-back' workload is selected. On the right, the 'View Log' dialog is open, displaying a list of log entries. The 'Pod' dropdown is set to 'terminal-manager-back' and the 'Container' dropdown is set to 'terminal-m...'. The log entries show messages from the 'SberAuthService'.

Рисунок 29 – Просмотр лог-файлов Сервиса УТ

3.6.3.1. Параметры логирования

Параметры логирования настраиваются в конфигурационном файле **logback.xml**. Основные параметры логирования:

- **ru.sber.umscud.terminal_manager_impl** – логирование работы Сервиса УТ (основные уровни логирования – INFO, DEBUG);
- **org.hibernate.SQL** – логирование запросов к БД (основные уровни логирования – INFO, DEBUG);
- **org.apache.hc.client5.http.wire** – логирование исходящих/входящих запросов с помощью **apache client** (основные уровни логирования – INFO, DEBUG; при использовании уровня INFO логи не отображаются в потоке вывода);



- **feign** – логирование исходящих/входящих запросов **feign client** (основные уровни логирования – INFO, DEBUG; при использовании уровня INFO логи не отображаются в потоке вывода).

Доступны следующие типы вывода логов:

- **ELASTIC** – отправка логов в **elasticsearch**;
- **STDOUT** – вывод логов в стандартный поток вывода;
- **STDERR** – вывод логов в поток вывода ошибок.

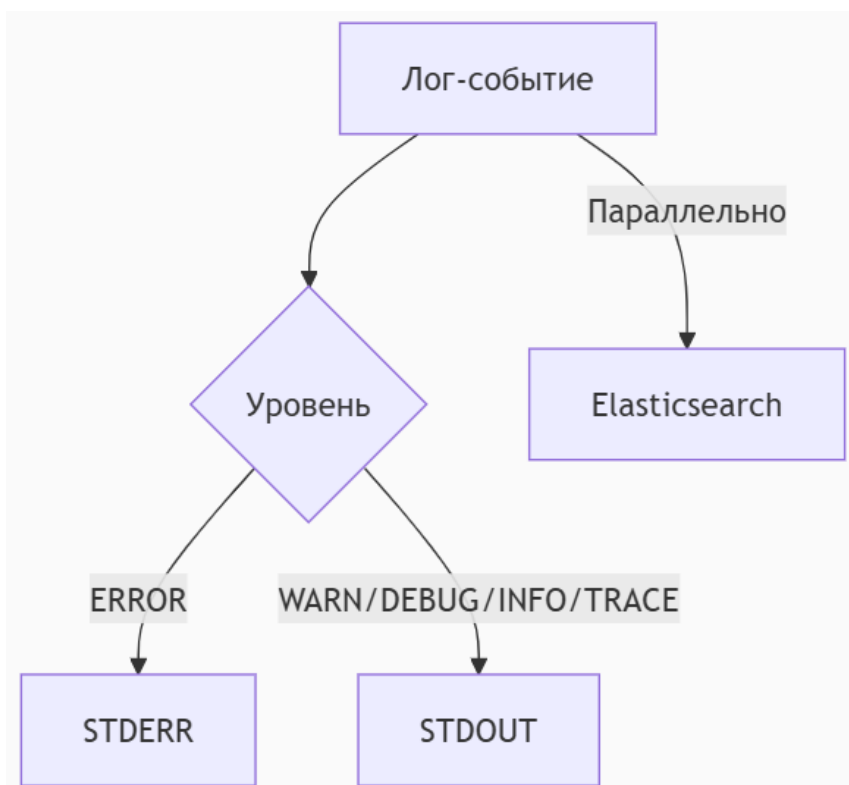


Рисунок 30 – Схема логирования работы Сервиса УТ



4. РАБОТА СИСТЕМЫ

4.1. Регистрация пользователей в системе (онбординг)

Для работы интеграции ПК **Визирь.СКУД** с КБС **Сбер** необходимо выполнить регистрацию пользователя, предварительно сдавшего биометрические данные в ЕБС, в картотеке ПК **Визирь.СКУД**.

Алгоритм работы по данному сценарию:

1. **Визирь.СКУД** устанавливается и настраивается на объекте (см. [Настройка сервисов на объекте заказчика](#)).
2. Если предполагается работа с внешней СКУД – настраивается синхронизация картотек СКУД, установленной на объекте и ПК **Визирь.СКУД** (шаги 1 PassId и CardId + PassId на схеме ниже).
3. Синхронизированная картотека отображается на терминале – шаг 2 CardId на схеме ниже.
4. Пользователь подходит к биометрическому терминалу и выбирает нужную карточку из картотеки на планшете (шаг 3 на схеме ниже).
5. Пользователь смотрит в камеру терминала (шаг 4 на схеме ниже). При этом:
 - анализируется видеопоток;
 - детектируется лицо;
 - проводится оценка качества детекции;
 - проводится оценка портретных характеристик;
 - формируется лучший кадр (bestshot).
6. Сформированный лучший кадр (bestshot) передается на аутентификацию в КБС **Сбер** (шаг 5 на схеме ниже).
7. Если пользователь успешно аутентифицирован, в сервис **cbs-management-service** возвращается идентификатор пользователя из КБС (**CloudId**, шаг 6 на схеме ниже).
8. Идентификатор из КБС вместе с идентификатором карточки пользователя передается в сервис **idp-organization-service** (шаг 7 на схеме ниже).
9. **idp-organization-service** сохраняет связку идентификаторов в БД и передает в ПК **Визирь.СКУД** признак наличия биометрии у данного пользователя (шаги 8 и 9 на схеме ниже).
10. Результат связывания идентификаторов передается на терминал (шаг 10 на схеме ниже).

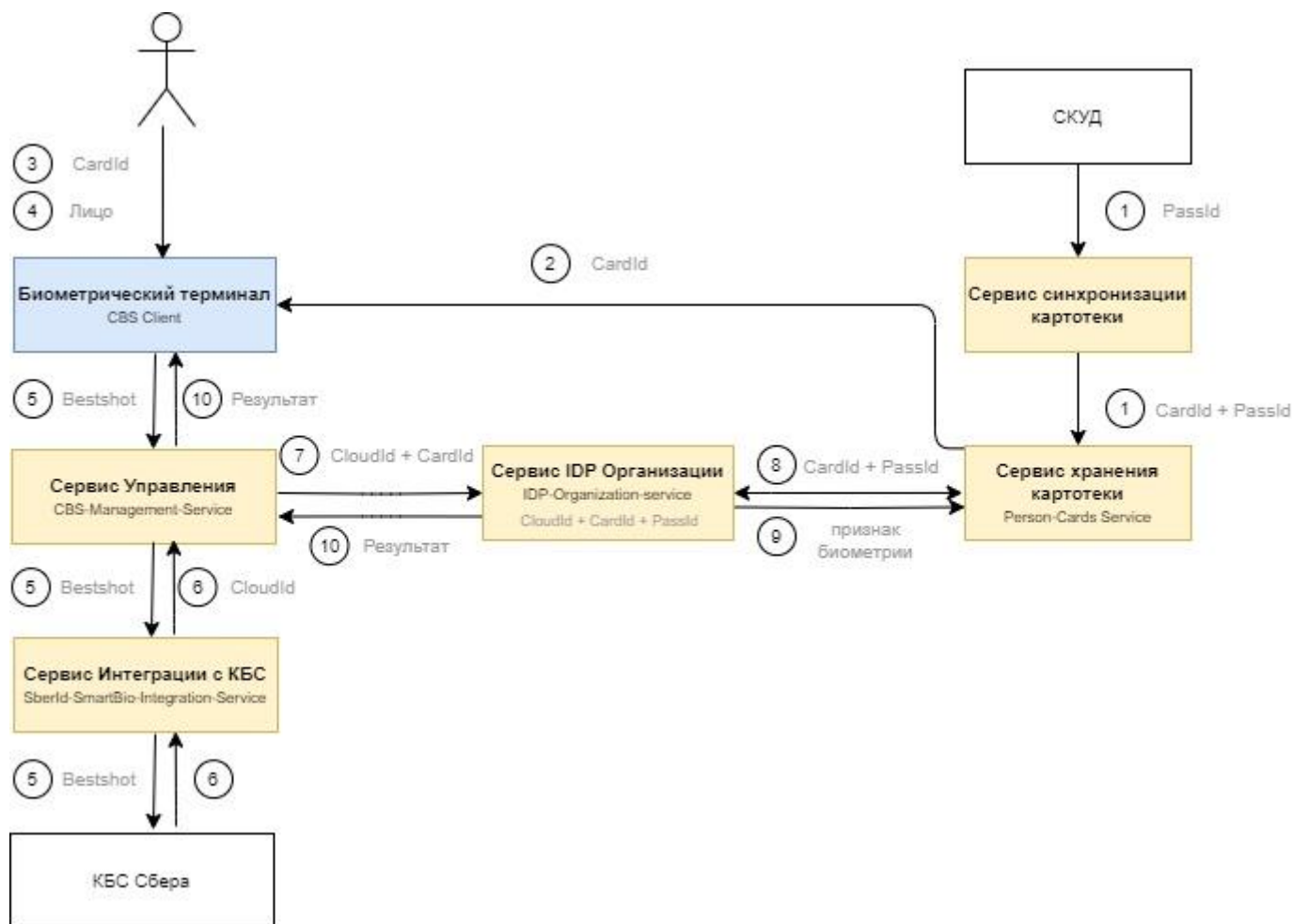


Рисунок 31 – Схема работы

4.1.1. Работа с терминалом

Общий алгоритм работы с терминалом:

1. Откройте установленное приложение **CBS Client** из списка приложений терминала.
2. Нажмите на экран устройства 5 раз подряд. В открывшемся окне (рис. 32):
 - Установите переключатель **Привязка биометрии / Настройки терминала** в положение **Привязка биометрии**;
 - Введите логин и пароль пользователя системы **Визирь.СКУД**.



Для входа в режим онбординга необходимо создать пользователя в **Конфигураторе** ПК **Визирь.СКУД** для каждого Администратора системы, который будет иметь доступ в данный раздел.

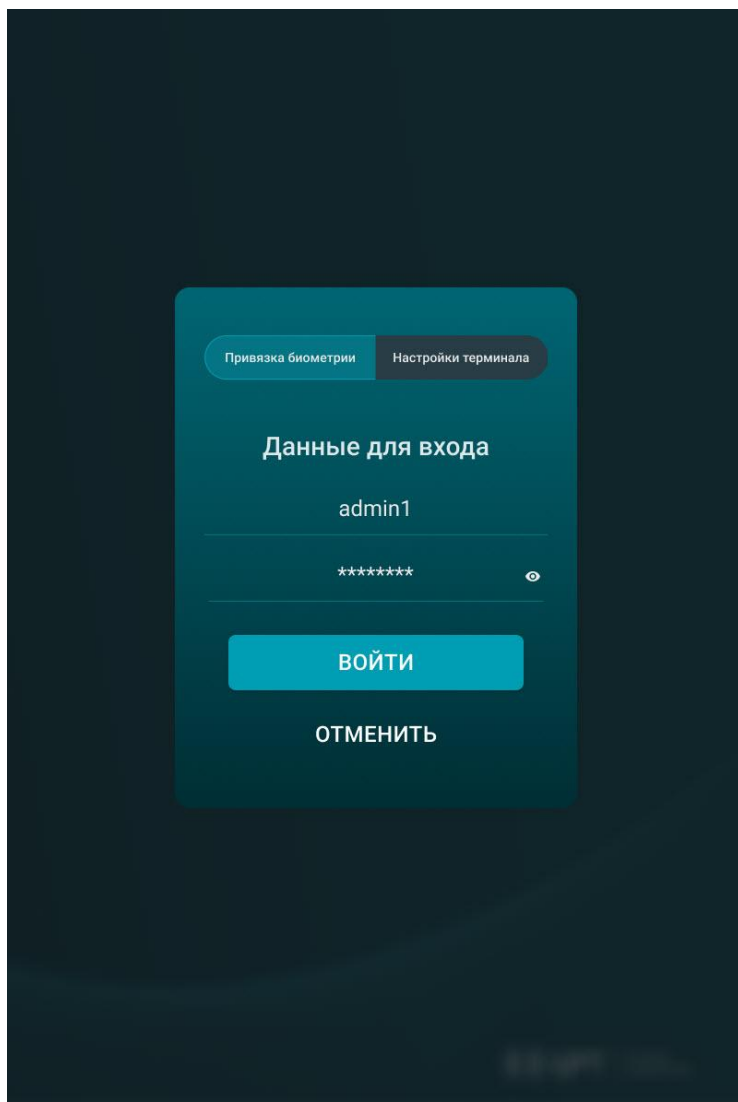


Рисунок 32 – Вход в настройки приложения

3. В открывшемся экране нажмите кнопку **Выбрать пользователя** (рис. 33).

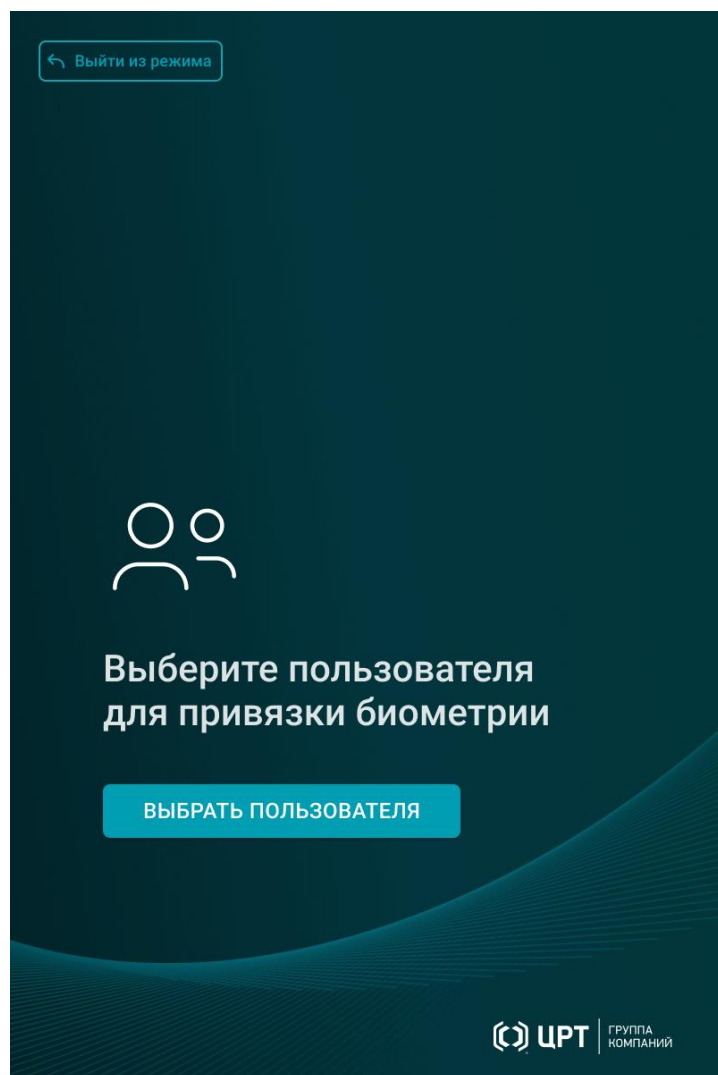


Рисунок 33 – Кнопка **Выбрать пользователя**

4. В открывшемся экране выберите нужную карточку в картотеке ПК **Визирь.СКУД**, к которой необходимо привязать ID пользователя из КБС (рис. 34). По умолчанию отображаются все доступные карточки в системе. Карточки, для которых уже привязана биометрия, имеют метку . Для фильтрации отображаемых карточек нажмите кнопку  и выберите нужную категорию (возможно выбрать либо **одну** необходимую категорию, либо **все** категории). Для выполнения текстового поиска по карточкам введите текст для поиска в области . В результате будут отображены только карточки, соответствующие условиям поиска. Поиск производится по именам карточек.

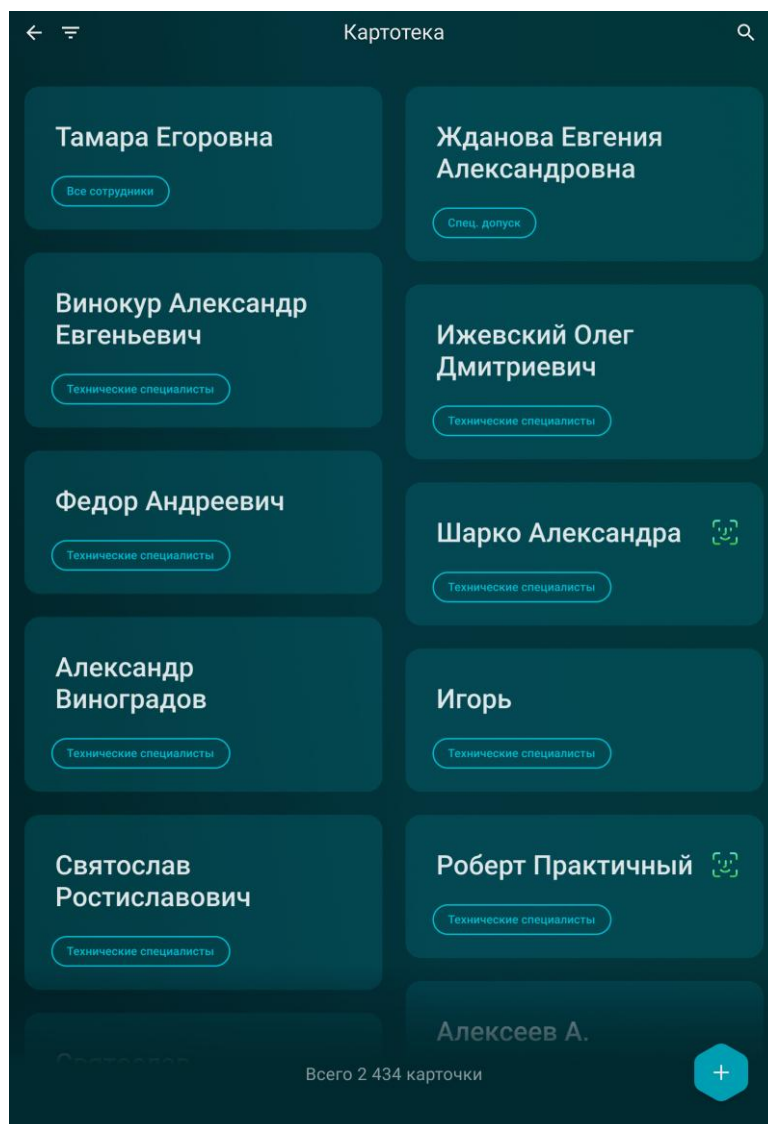


Рисунок 34 – Выбор карточки

5. В открывшемся экране:

- Если к карточке **уже привязана** биометрия, то, для повторной привязки, нажмите кнопку **Перепривязать биометрию** (рис. 35, **1**);
- Если к карточке **не привязана** биометрия, нажмите кнопку **Привязать биометрию** (рис. 35, **2**).

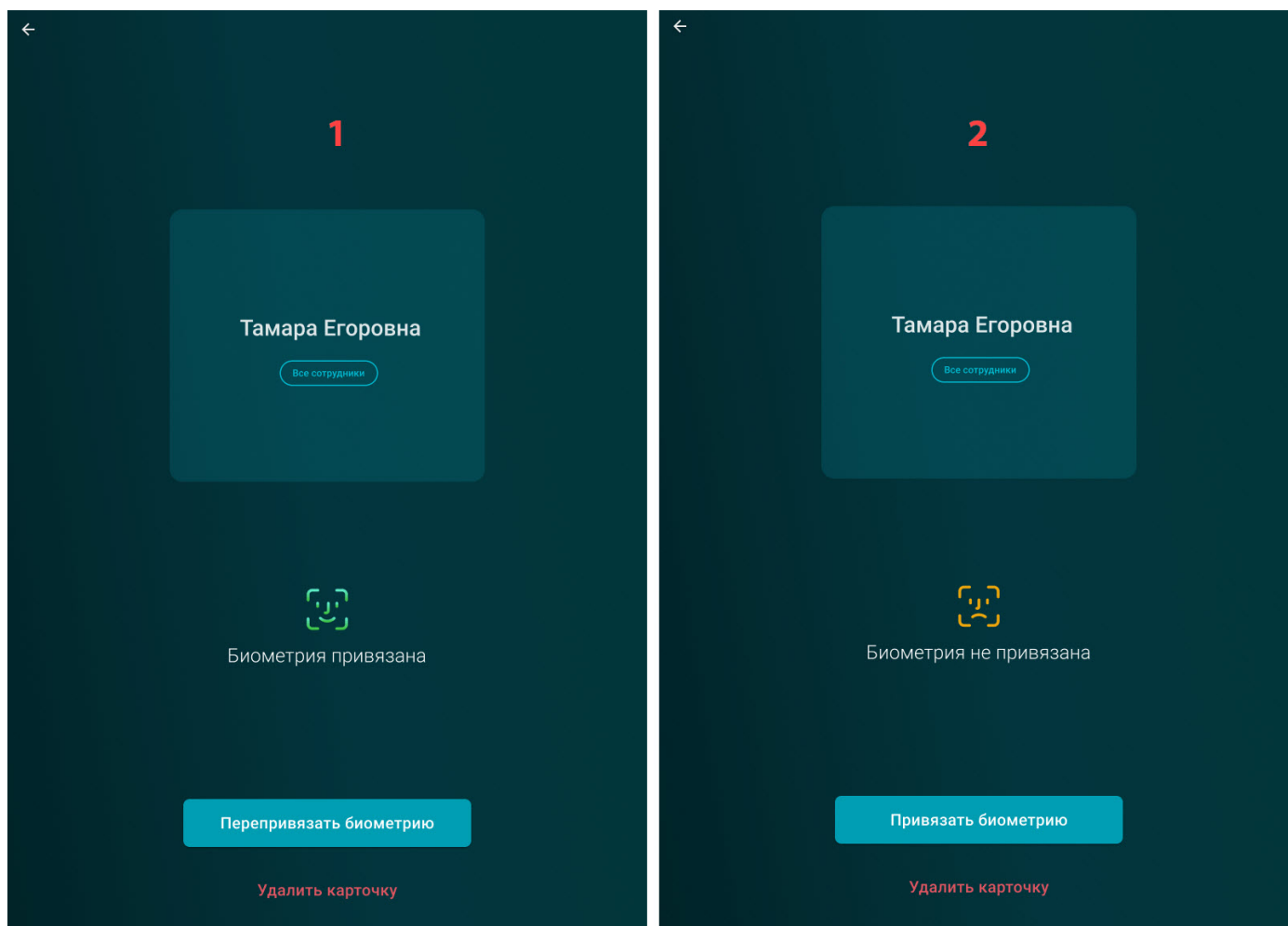


Рисунок 35 – Кнопки **Перепривязать биометрию / Привязать биометрию**

6. Поместите лицо человека, ID которого из КБС необходимо привязать к карточке, в фокус камеры терминала (рис. 36).

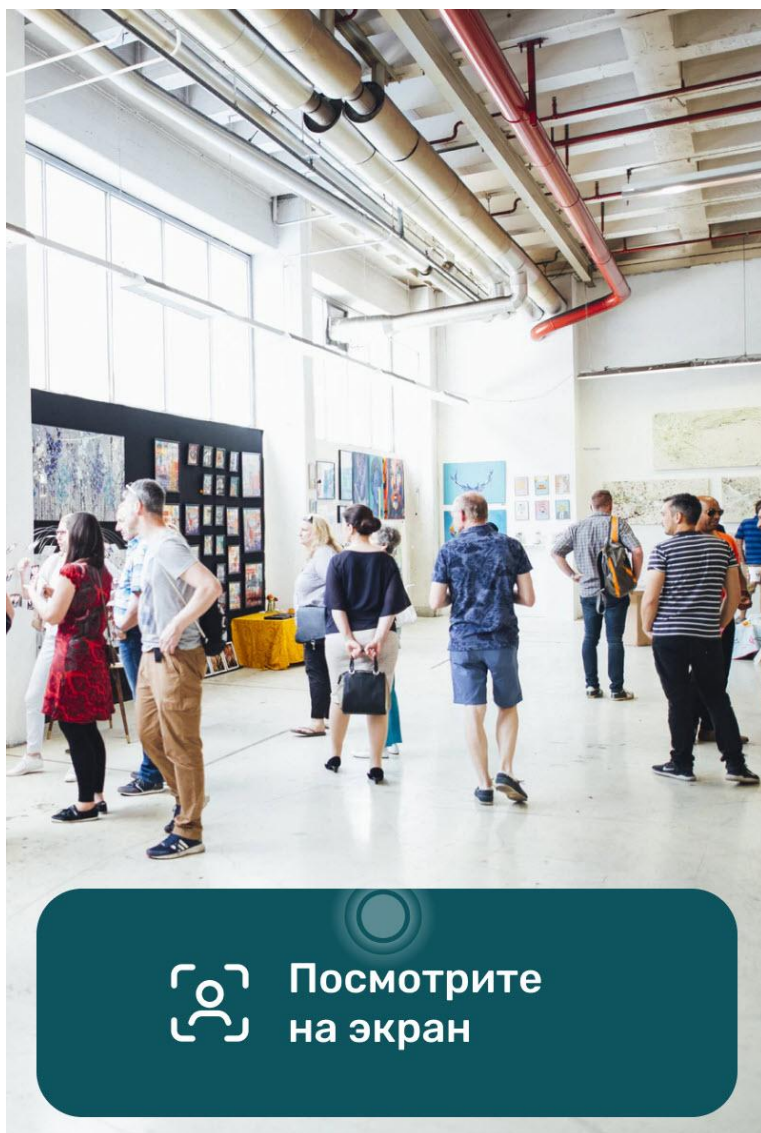


Рисунок 36 – Окно **Посмотрите на экран**

7. При успешной привязке ID будет отображено соответствующее сообщение (рис. 37).

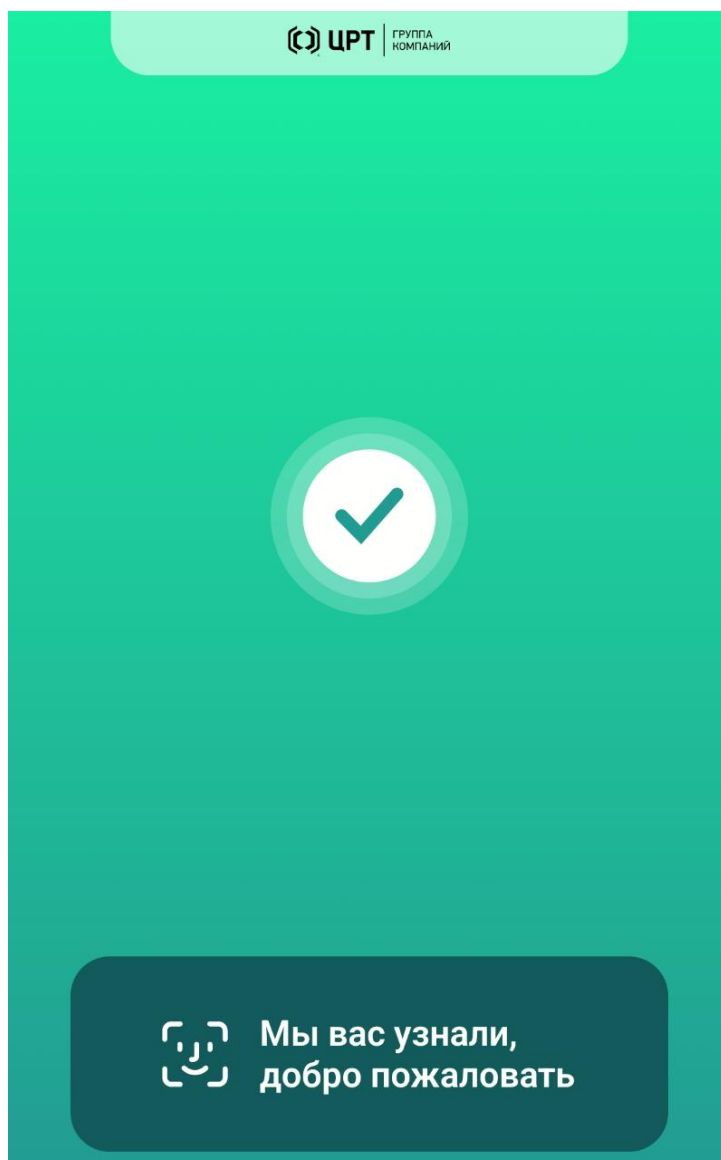


Рисунок 37 – Сообщение при успешной привязке ID

8. При ошибке будет отображено соответствующее сообщение (рис. 38).

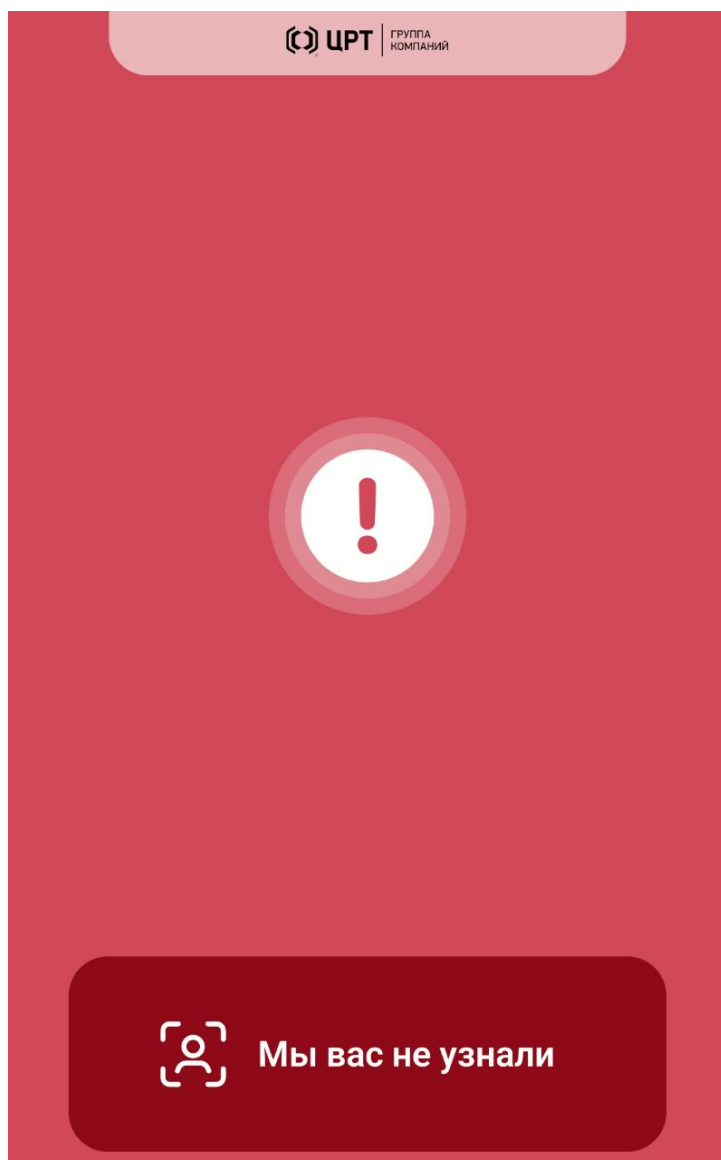


Рисунок 38 – Сообщение при ошибке

4.1.1.1. Добавление / удаление карточек

Возможна работа с картотекой ПК **Визирь.СКУД** (добавление и удаление карточек) в интерфейсе приложения **CBS Client**.

Алгоритм работы:

1. Активируйте опцию **Редактирование картотеки** в разделе **Системные настройки** настроек приложения.
2. Для **создания** новой карточки:
 - Перейдите в режим привязки биометрии (в список карточек).



- В открывшемся экране нажмите кнопку ;
 - В открывшемся экране укажите **имя** карточки и **категорию** (рис. 39, **1**);
 - Нажмите кнопку **Сохранить карточку**. Новая карточка появится в списке.
3. Для **удаления** карточки нажмите кнопку **Удалить карточку** в окне редактирования (рис. 39, **2**).
В открывшемся диалоговом окне подтвердите удаление.

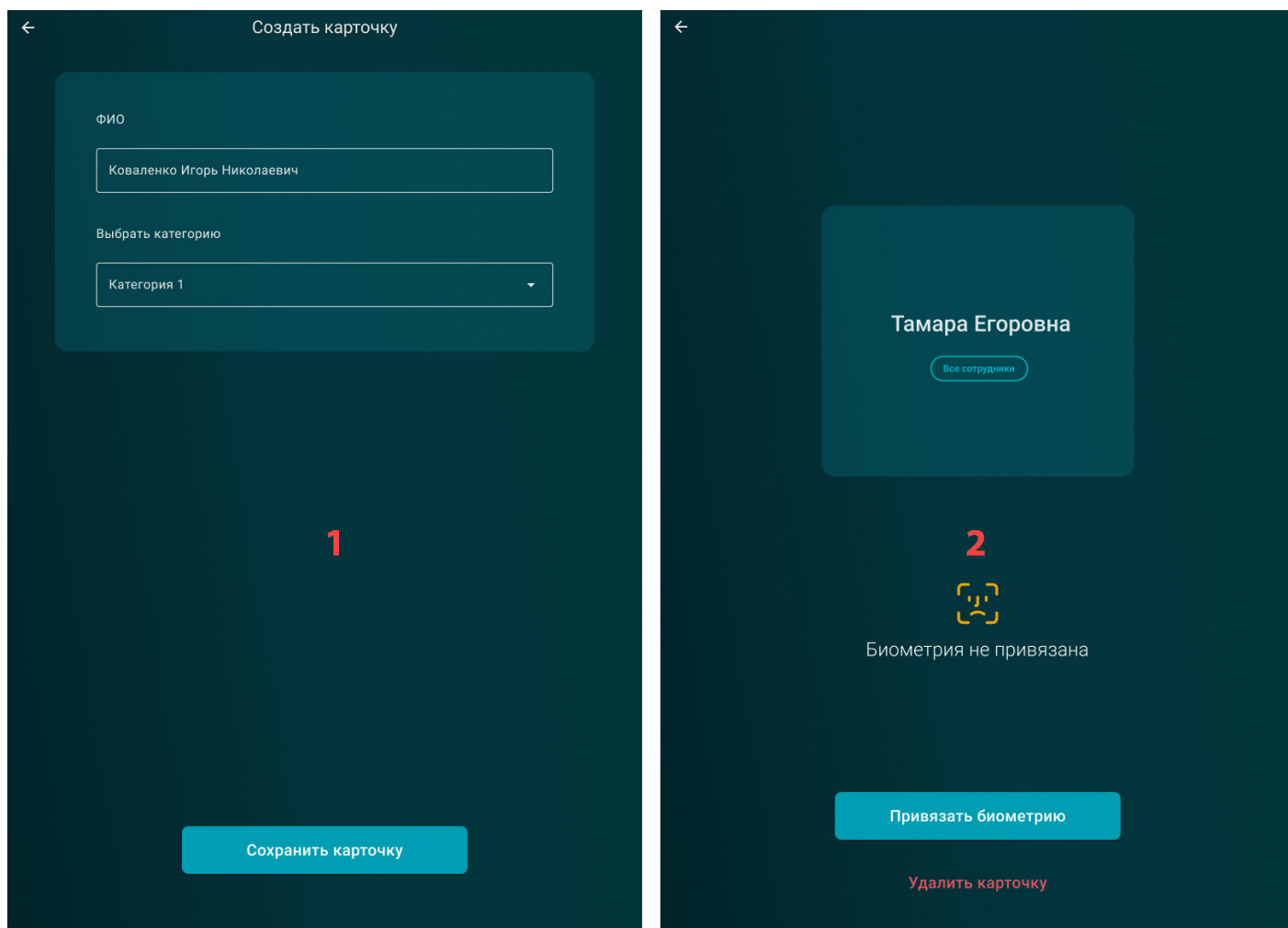


Рисунок 39 – Работа с карточками

4.1.1.2. Проверка подключения биометрии в СберId

Возможна проверка подключения биометрии в **СберId** в интерфейсе приложения **CBS Client**.

Алгоритм проверки:

1. Активируйте опцию **Инструкция СберId при онбординге** в разделе **Системные настройки** настроек приложения (см. [Настройка терминала](#)).



2. Находясь в режиме онбординга, выберите карточку пользователя для проведения процедуры проверки и нажмите кнопку **Привязать биометрию / Перепривязать биометрию** (см. [Работа с терминалом](#)).
3. В открывшемся окне (рис. 40, **1**) отсканируйте QR-код камерой своего мобильного телефона для входа в личный кабинет **СберId**.
4. При успешном входе в личный кабинет **СберId** нажмите кнопку **Я уже в личном кабинете СберId** (рис. 40, **1**).



Для **отмены проверки** на данном этапе (например, пользователь не смог зайти в личный кабинет **СберId**) нажмите кнопку **Проверить в другой раз**. В этом случае процесс онбординга будет **завершен**, и произойдет переход в окно выбора карточек в картотеке.

5. Проверьте, настроена ли биометрия, в соответствии с инструкцией на экране (рис. 40, **2**).
6. Если биометрия настроена, нажмите кнопку **Биометрия настроена** (рис. 40, **2**).



Для **отмены проверки** на данном этапе (например, пользователь не смог настроить биометрию) нажмите кнопку **Проверить в другой раз**. В этом случае процесс онбординга будет **завершен**, и произойдет переход в окно выбора карточек в картотеке.

7. В открывшемся окне нажмите кнопку **Перейти к привязке биометрии** (рис. 40, **3**). Будет открыт экран аутентификации для биометрической привязки биометрии. Дальнейший алгоритм аналогичен описанному в разделе [Работа с терминалом](#).



Для **отмены привязки биометрии** нажмите кнопку **Проверить в другой раз**. В этом случае процесс онбординга будет **завершен**, и произойдет переход в окно выбора карточек в картотеке.

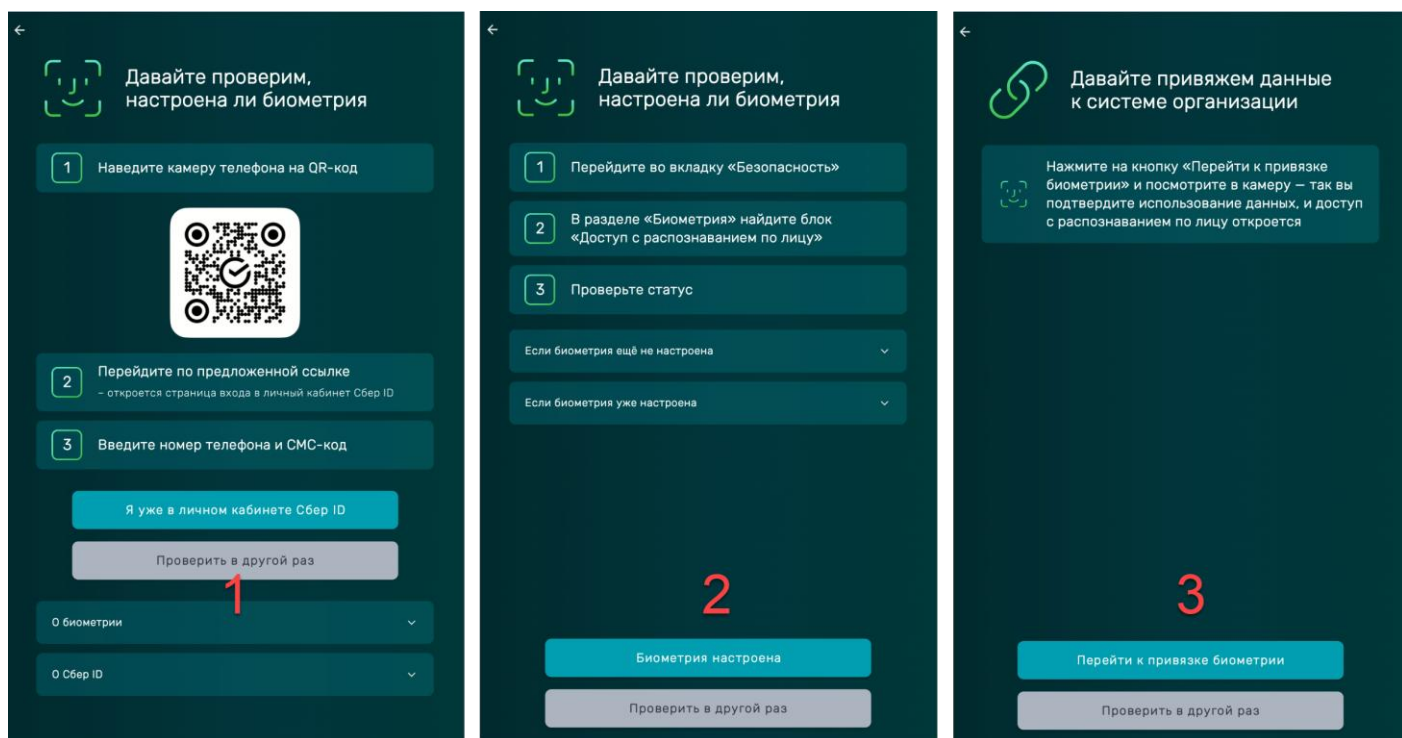


Рисунок 40 – Проверка подключения биометрии

4.2. Биометрический проход

Сценарий подразумевает, что обработка видео ведется на терминале.

Алгоритм работы по данному сценарию:

1. **Визирь.СКУД** устанавливается и настраивается на объекте (см. [Настройка сервисов на объекте заказчика](#)).
2. Предварительно настраивается интеграция со СКУД, установленной на объекте.
3. Предварительно выполняется регистрация пользователей, которые будут использовать СКУД для прохода на объект (см. [Регистрация пользователей в системе \(онбординг\)](#)).
4. Настраивается биометрический терминал (см. [Настройка терминала](#)).
5. Пользователь подходит к биометрическому терминалу (шаг 1 на схеме ниже). На терминале:
 - анализируется видеопоток;
 - детектируется лицо;
 - проводится оценка качества детекции;
 - проводится оценка портретных характеристик;
 - формируется лучший кадр (bestshot);
 - лучший кадр зашифровывается и подписывается.



6. Лучший кадр (bestshot) передается на сервер ПК **Визирь.СКУД** (шаг 2 на схеме ниже).
7. Лучший кадр (bestshot) передается на аутентификацию в КБС **Сбер** (шаг 3 на схеме ниже).
8. При успешной аутентификации пользователя в КБС **Сбер**, на сервер ПК **Визирь.СКУД** возвращается ID пользователя из КБС (шаги 4 на схеме ниже).
9. По идентификатору из КБС проверяется наличие связки данного идентификатора с карточкой в картотеке ПК **Визирь.СКУД**, а также запрашивается номер карты доступа данного пользователя (опционально) – шаг 5 на схеме ниже.
10. Если в системе включена проверка по профилям доступа – осуществляется проверка возможности доступа в соответствии с настроенными для данной карточки профилями (шаг 6 на схеме ниже).
11. Событие идентификации передается в ПК **Визирь.СКУД** (для интеграции через события идентификации и отображения событий в **Журнале событий** системы **Визирь.СКУД**) – шаг 7 на схеме ниже. Для просмотра событий в интерфейсе ПК **Визирь.СКУД** необходимо добавить соответствующее смарт-устройство в рабочую область, а также в дерево устройств и на карту.
12. Событие идентификации с необходимыми данными отправляется на терминал (шаг 8 на схеме ниже).
13. Терминал отправляет полученный номер карты доступа на контроллер СКУД для принятия решения о допуске (при интеграции с контроллером) – шаг 9 на схеме ниже.
14. Контроллер отправляет на терминал информацию о принятом решении допуска/отказа в допуске на объект (шаг 10 на схеме ниже).

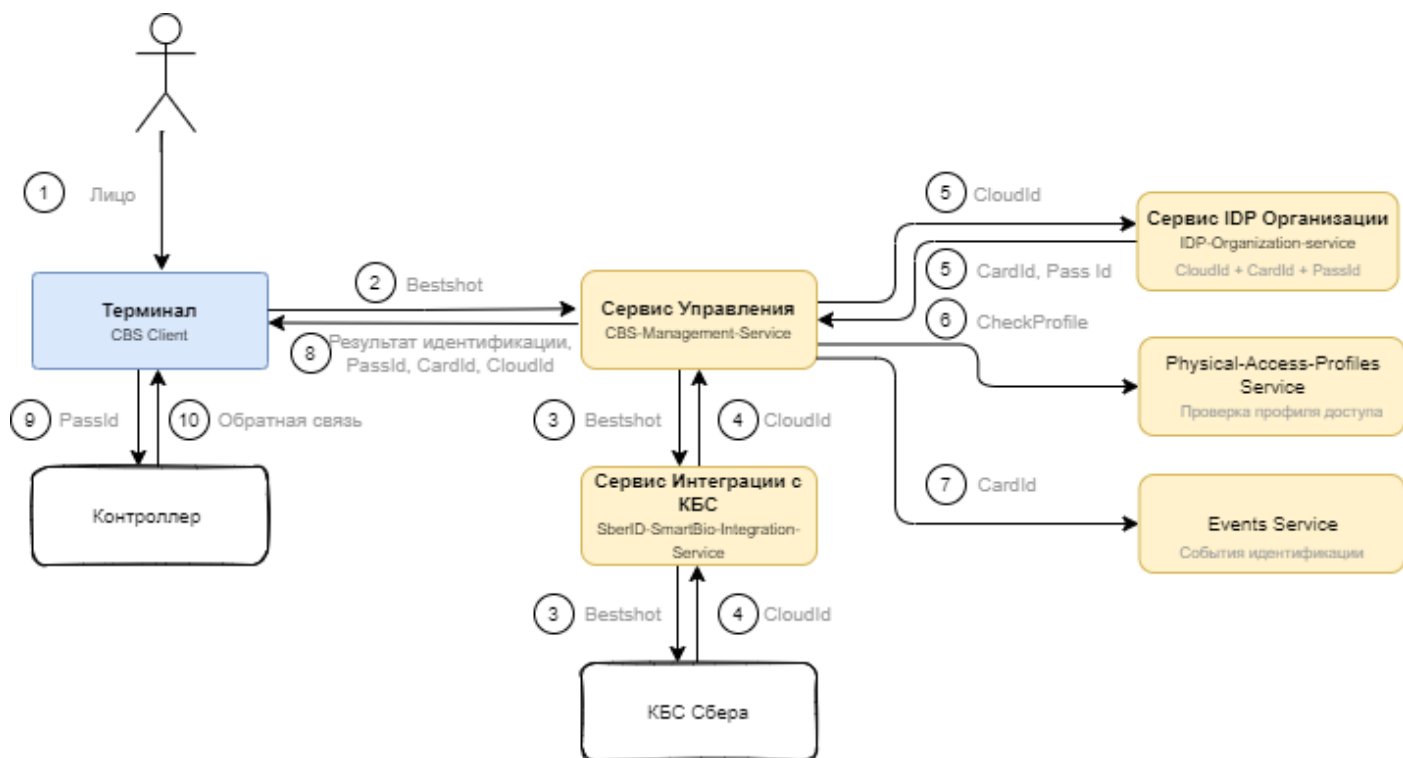


Рисунок 41 – Схема работы

4.3. Проход по карте (RFID)

Для возможности прохода с помощью прикладывания карты к считывателю карт доступа активируйте параметр **RFID > Однофакторный (ИЛИ)** в блоке **Настройка интерфейсов и камеры** в настройках терминала (см. [Настройка терминала](#)).



Обратите внимание:

1. При прикладывании карты к считывателю, если на терминале при этом **уже начался** процесс биометрической аутентификации и номер карты аутентифицированного лица **уже отправлен** по **wiegand**, прерывание процесса аутентификации **не производится**. В этом случае:
 - Если от контроллера пришло **разрешение** для отправленного в результате биометрической аутентификации номера карты, то отображается экран **Идентификация пройдена**, и сценарий завершается **без отправки** на контроллер приложенной к считывателю карты;
 - Если от контроллера пришел **отказ** для отправленного в результате биометрической аутентификации номера карты, то **продолжает отображаться экран ожидания**. При этом номер приложенной карты отправляется на контроллер по **wiegand** и ожидается ответ от контроллера СКУД. В зависимости от ответа отображается экран **Идентификация пройдена / Идентификация не пройдена**.



- Во всех остальных случаях, при прикладывании карты к считывателю **производится прерывание** текущего процесса и терминал переходит в режим работы с картами **RFID**, описанный ниже.

Алгоритм работы по данному сценарию:

- Пользователь подносит карту к RFID считывателю терминала.
- До получения ответа по интерфейсу **GPIO** на терминале отображается экран ожидания (рис. 42).

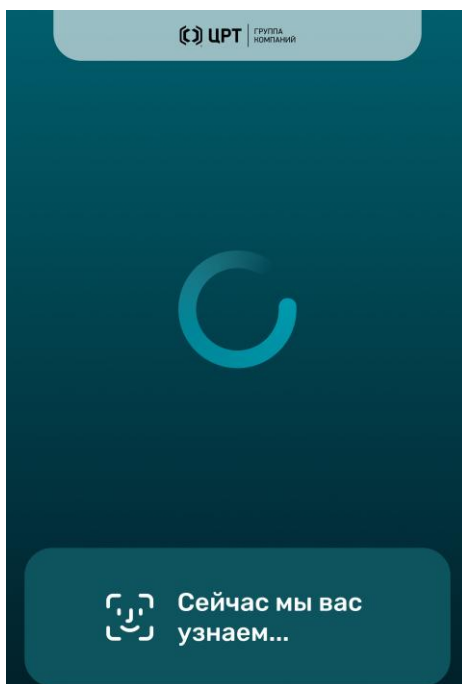


Рисунок 42 – Экран ожидания

- Полученный номер карты отправляется с терминала на контроллер по **wiegand**; терминал ожидает ответ от контроллера по интерфейсу **GPIO**. При этом, если во время прикладывания карты был начат процесс аутентификации, но карта аутентифицированного лица еще не отправлена на контроллер по **wiegand** – процесс аутентификации прерывается.
- При получении **разрешения** от контроллера отображается экран **Идентификация пройдена** (рис. 43, **1**). При получении **отказа** от контроллера отображается экран **Идентификация не пройдена** (рис. 43, **2**).

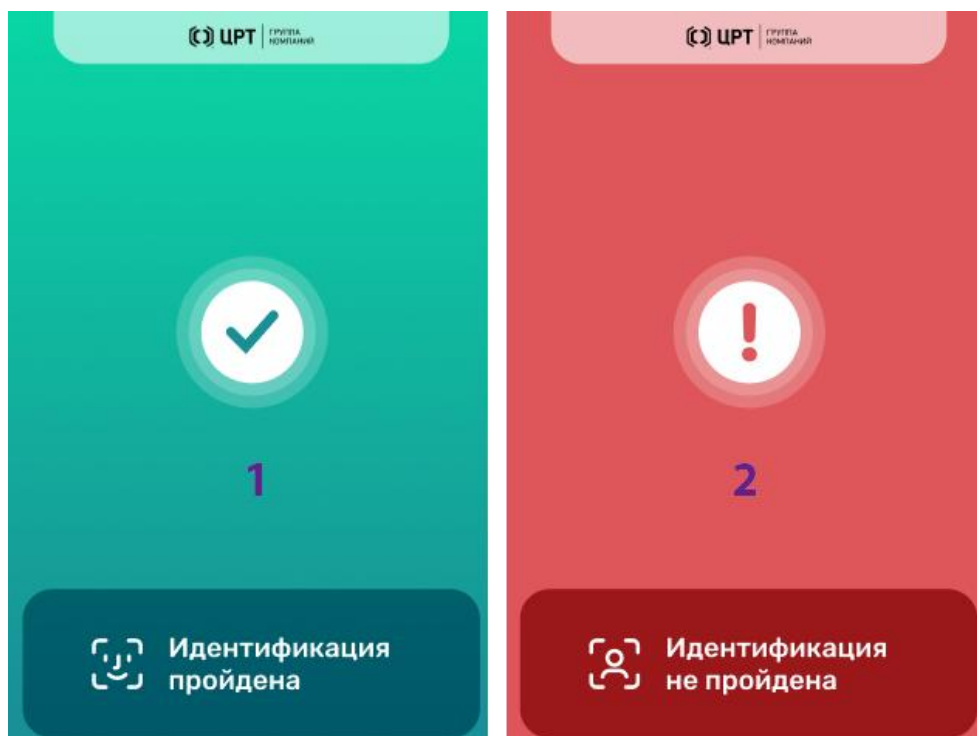


Рисунок 43 – Экраны разрешения / запрета прохода



5. ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

5.1. Модуль взаимодействия с MDM

Модуль взаимодействия с MDM обеспечивает интеграцию с инструментом удаленного управления, настройки и защиты мобильных устройств, а также расширяет возможности основной системы.

MDM обеспечивает:

- Удаленное управление ПО: дистанционную установку, настройку рабочих приложений и обновление ОС на мобильных устройствах.
- Защиту соединений: установку и ротацию mTLS-сертификатов, а также автоматическое обновление корневых сертификатов ГОСТ.
- Администрирование парка устройств: организацию иерархической структуры, группировку мобильных устройств и реализацию ролевой модели доступа.

Расширение функционала основной системы включает:

- Интеграцию со сторонними системами и СКУД:
 - Интеграцию со СКУД «Бастион» и расширение взаимодействия со СКУД Sigur.
 - Передачу данных по биометрическим терминалам в АС «Арсенал».
- Развитие логики работы оборудования и терминалов:
 - Расширение логики работы с Wiegand, GPIO и датчиками вскрытия (тамперами).
 - Синхронизацию структуры настроек между терминалом и Сервером УТ.
 - Расширение перечня режимов работы, профилей и функционала группового изменения настроек терминалов.
 - Реализацию режима ожидания на терминалах.
- Аппаратные и программные доработки мобильных устройств:
 - Встраивание SDK биометрического распознавания SmartBio (версий 1.31 и 1.33).
 - Добавление второго фактора аутентификации на мобильном устройстве для подтверждения прохода.
 - Расширение логики работы с Frida (анализ защищенности среды).
 - Управление дополнительными функциями камеры мобильного устройства.
- Интерфейс и системные функции:
 - Модификацию графического интерфейса приложения на мобильном устройстве.



- Локализацию интерфейса на английский язык.
- Расширение возможностей логирования работы приложений.

5.2. Расширенное логирование по каждому терминалу

Сервис УТ обеспечивает возможность изменения режима логирования по любому терминалу или группе терминалов для глубокого анализа и диагностики работы оборудования.

Варианты режимов логирования: INFO; ERROR; DEBUG.

Описание режимов ведения логов:

- INFO – Обычные сообщения о штатной работе приложения.
- ERROR – Предупреждения о нештатных ситуациях, которые не приводят к сбоям и ошибки, которые влияют на работу части функционала.
- DEBUG – Информация, полезная для отладки: переходы состояний, запросы на сервер и с сервера, запуск/остановка сервиса. Также включает в себя логи режимов INFO; ERROR.

Сервис запрашивает подтверждение при изменении режима логирования и рекомендует проверить наличие достаточного объёма свободного места в хранилище при активации опции записи в облачное хранилище.

Действия администратора по изменению режима логирования терминала записываются в журнал аудита для дальнейшего анализа.

Для активации режима логирования уровня DEBUG в сервисе УТ предварительно в поле для ввода необходимо ввести номера запроса на изменения (ЗНИ) или инцидента, в рамках которых активируется указанный режим. В поле для ввода номера ЗНИ/инцидента реализована проверка корректности номера. Номер ЗНИ/инцидента состоит из префикса "INC" или "С" и порядкового номера ЗНИ/инцидента длиной до 10 знаков (0-9).

При активации режимов логирования INFO или ERROR терминал или группа терминалов начинают запись логов в локальное хранилище терминала. При активации опции записи в облачное хранилище в меню режимов логирования сервиса УТ терминал или группа терминалов дополнительно отправляют логи в облачный бакет (S3). При активации режима логирования DEBUG опция записи в облачное хранилище активируется автоматически и становится недоступной для изменения в данном режиме, так как хранение логов уровня DEBUG на локальном хранилище терминала недопустимо. При нажатии кнопки "Очистить логи" в меню режимов логирования сервиса УТ терминал или группа терминалов производят удаление логов из локального хранилища.

5.3. Групповое изменение настроек для группы терминалов



Сервис УТ предоставляет возможность выбора группы терминалов для изменения настроек путём выбора отдельных терминалов.

Сервис обеспечивает групповое изменение настроек для группы терминалов.

Список доступных опций для групповых операций:

- Обновить;
- Применить профиль настроек;
- Изменить уровень логирования;
- Перезагрузить;
- Изменить режим устройства:
 - Активный;
 - Обслуживание;
 - Аварийный;
 - Заблокированный.
- Удалить.

Действия администратора по применению настроек терминала записываются в системный журнал для дальнейшего анализа и аудита.

5.4. Соответствие настроек терминала и Сервера УТ

Сервис УТ имеет доступ к изменению полного набора настроек мобильного приложения **Визирь.СКУД** (PACS Sber Client) на биометрическом терминале для удалённого администрирования.

Список настроек:

- Настройки работы с лицами:
 - Размер лица, px
 - Порог срабатывания liveness, %
 - Порог качества детекции, %
 - Наклон вбок (Roll), %
 - Наклон вперед (Pitch), %
 - Поворот (Yaw), %
 - Размытие (Blur), %
 - Освещение (Light), %
 - Яркость (Brightness), %



- Порог качества изображения, %
- Порог наличия очков (Glasses), %
- Порог наличия маски (Mask), %
- Порог наличия головного убора (Hat), %
- Порог наличия головного платка (Shawl), %
- Порог наличия солнцезащитных очков (Sunglasses), %
- Порог перекрытия лица (Overlap), %
- Очки (Eye Glasses), %
- Открытость глаз (Eye open), %
- Видимость глаз (Eye Obscureness), %
- Улыбка (Smile), %
- Открытость рта (Mouth open), %
- Видимость рта (Mouth Obscureness), %
- Рамка детекции
- Количество успешных bestshot перед отправкой
- Режим работы:
 - QR
 - RFID
 - Режим шлюзовой кабины:
 - Таймаут ожидания результата распознавания, сек
 - Сообщение приветствия для шлюзовой кабины
 - Настройка интерфейсов и камеры:
 - Отражать видеопоток
 - Подсветка:
 - Яркость подсветки, %
 - Подсветка загорается при детекции
 - Формат wiegand
 - Инверсия (Бастион)
 - Порт для RS-485



- Невалидные коды:
 - Код при неидентификации
 - Код при отказе по liveness
 - Количество попыток перед отказом
 - Длительность ожидания ответа контроллера
- Выводимая информация:
 - Время отображения сообщения (мс)
- Экран допуска:
 - Текст приветствия
- Экран отказа:
 - Сообщение при неидентификации
 - Сообщение при отказе от контроллера
 - Сообщение при отсутствии биометрии
- Экран ожидания:
 - Текст экрана ожидания
- О приложении:
 - Версия приложения

5.5. Иерархическая структура вложенных папок

Сервис УТ позволяет пользователям создавать и удалять папки для просмотра списка терминалов в виде древовидной структуры, где терминалы могут быть организованы в иерархическом порядке внутри вложенных папок.

Иерархическая структура объектов банка:

- Центральный аппарат (ЦА);
 - Объекты;
 - Терминалы на объекте.
- Территориальные банки (ТБ);
 - Объекты;
 - Терминалы на объекте.

Сервис позволяет пользователям перемещать терминалы между разными папками.



В интерфейсе сервиса на папках выводится следующая информация:

- Общее количество терминалов;
- Количество активных терминалов;
- Количество терминалов не в сети;
- Количество деактивированных терминалов.

Сервис обеспечивает разграничение прав доступа пользователей к папкам с терминалами. Папки имеют атрибут видимости, позволяющий настраивать доступ для определённых ролей из ролевой модели.

Действия администратора по созданию/изменению/удалению папок и изменению прав доступа записываются в системный журнал для дальнейшего анализа и аудита.

5.6. Режимы терминала

Сервис УТ

В интерфейсе сервиса УТ реализована функциональность для перевода терминала / группы терминалов в один из режимов работы:

- Активный;
- Обслуживание;
- Аварийный;
- Заблокированный.

При изменении режима терминала сервис УТ запрашивает подтверждение на выполнение операции.

Все события, связанные с изменением статуса терминала, логируются для дальнейшего анализа и аудита.

Биометрический терминал

Биометрический терминал переводится по команде сервиса УТ в один из режимов работы:

- Активный:
 - Терминал функционирует в штатном пропускном режиме.
 - Информационные сообщения реализуются всплывающими картинками с текстом.
 - В случае потери связи терминала с сервером на экране терминала отображается экран информационного сообщения.



- Обслуживание:
 - Терминал временно выведен из эксплуатации для проведения технического обслуживания. В этом режиме терминал не выполняет идентификацию лиц и не выводит всплывающих сообщений (об ошибках, потери связи, статусах распознавания и пр.).
 - На экране терминала отображается экран информационного сообщения.
 - На период действия режима проверка времени отсутствия соединения с сервером отключается.
- Аварийный:
 - Терминал временно выведен из эксплуатации по причине непредвиденных технических сбоев и временно не способен выполнять свои функции. В этом режиме терминал не выполняет идентификацию лиц и не выводит всплывающих сообщений (об ошибках, статусах распознавания и пр.).
 - На экране терминала отображается экран информационного сообщения.
 - На период действия режима проверка времени отсутствия соединения с сервером отключается.
- Заблокированный:
 - Терминал временно выведен из эксплуатации по причине административных действий. В этом режиме терминал не выполняет идентификацию лиц и не выводит всплывающих сообщений (об ошибках, статусах распознавания и пр.).
 - На экране терминала отображается экран информационного сообщения.

В случае перезагрузки терминал остается в прежнем режиме работы.

Не активированный терминал (до активации либо после деактивации) на экране отображает только экран информационного сообщения. Реализован механизм сворачивания экрана информационного сообщения при помощи сервисного пароля с возможностью его восстановления по кнопке или таймеру.

5.7. Выгрузка данных о биометрических терминалах

Реализован функционал сбора и обработки информации об устройствах СКУД (контроллерах и биометрических терминалах), осуществляется их привязка к объектам охраны (АС Арсенал), а также мониторинг их состояний.

Данные по биометрическим терминалам, в отличие от остального оборудования, выгружаются из сервиса terminal-manager.



В сервисе terminal-manager реализован сбор и хранение следующих данных по биометрическим терминалам:

- ID устройства [id]
- Наименование устройства [name]
- Тип устройства/оборудования (по умолчанию - биометрический терминал) [type]
- Год/дата установки [-]
- Производитель [manufacturer]
- Модель [model]
- Серийный номер [serialNumber]
- IP-адрес [ip]
- MAC [mac]
- Сегмент сети [subnetSegment]
- Домен [domain]
- Маска подсети [subnetMask]
- Версия прошивки [firmwareVersion]
- Открытые порты [openPorts]
- Тип порта [portType]
- Статус устройства [status]
- Состояние устройства [state]
- Режим подключения устройства (по умолчанию - Автоматический) [deviceConnectionMode]
- Место установки оборудования (Адрес) [address]
- Номер объекта охраны [nativeId]

5.8. Ролевая модель

Механизм распределения прав доступа к ресурсам и функциям системы подразумевает:

- предоставление пользователям прав, минимально необходимых для выполнения их функциональных обязанностей;
- сущности ролей и их связи с оператором, каждый оператор может получить только одну роль;
- охватывает все объекты системы и операции над ними, доступные пользователям всех категорий;



- реализован через роли и охватывает все объекты системы и операции над ними, доступные пользователям и администраторам всех категорий;
- задание параметров и ограничение прав экземпляра роли в рамках ролевой модели определяется пользователем с ролью с соответствующими полномочиями.

Роли имеют атрибуты видимости, позволяющие настраивать доступ к объектам системы и операциям над ними.

5.9. Создание типовых настроек

Сервис УТ обеспечивает возможность создавать профили настроек (для размещения на турникетах, на стене, в затемненном помещении и т.д.).

Профиль определяет все настраиваемые параметры терминала:

- Настройки работы с лицами;
- Дополнительные модальности;
- Настройка интерфейсов и камеры;
- Выводимая информация.

В интерфейсе сервиса есть возможность применять профили настроек для терминала или группы терминалов.

Действия администратора по применению профилей настроек терминала записываются в системный журнал для дальнейшего анализа и аудита.

5.10. Обновление рутовых сертификатов терминала

Алгоритм обновления:

- Генерация сертификатов в УЦ KC3 Encrypt и УЦ KC2 Devices Sign:
 - новый корневой сертификат открытого ключа шифрования УЦ KC3 Encrypt - root_cert_KC3.cer
 - на основе root_cert_KC3.cer формируется новый сертификат открытого ключа шифрования (ОКШ), подписанный на новом корневом сертификате открытого ключа шифрования -platform_cert.cer И/ИЛИ
 - новый корневой сертификат УЦ KC2 электронной подписи терминала УЦ KC2Devices Sign -root_cert_KC2.cer
- Формируется архив с артефактами обновления (new_cert);



- Архив с артефактами обновления подписывается доверенным сотрудником на ключе ЭП УЦ КСЗ для шифрования (УЦ КСЗ Encrypt) – подпись singКСЗ. Получаем подписанный архив new_cert_CMS.
- Подписанный архив с артефактами обновления вручную передается/нет на сервис МДМ через соответствующий UI;
- Через МДМ/вручную подписанный архив с артефактами обновления загружается на терминал в SmartBioCrypto;
- Проверяется совпадение OID в подписи с зафиксированным в коде OID внутри приложения SmartBioCrypto;
- Проверяется подпись (singКСЗ) архива, включая проверки цепочки сертификатов для доверенного УЦ КСЗ Encrypt и проверки текущего CRL УЦ КСЗ Encrypt;
- устанавливаются в доверенную зону на терминале:
 - новый корневой сертификат открытого ключа шифрования УЦ КСЗ Encrypt;
 - новый сертификат открытого ключа шифрования (ОКШ);
 - новый корневой сертификат УЦ КС2 электронной подписи терминала УЦ КС2 Devices Sign
- На терминал отправляется новый CRL УЦ КСЗ Encrypt, подписанный на новом корневом сертификате открытого ключа шифрования УЦ КСЗ;
- Определяется, какой CRL необходимо использовать на терминале двумя способами:
 - На основании математического сравнения подписей CRL и нового сертификата УЦ КСЗ Encrypt;
 - По совпадению идентификаторов центра сертификации: authorityKeyIdentifier (сертификат УЦ КСЗ Encrypt) = subjectKeyIdentifier (CRL)
- Проверка ранее загруженных сертификатов на отозванность на основании полученного CRL;
- Терминал переключается на работу на новых сертификатах;
- Терминал удаляет предыдущие/устаревшие корневые сертификаты из хранилища.

Санкт-Петербург

телефон: (812) 325-8848

факс: (812) 327-9297

Москва

телефон: (495) 669-7440

факс: (495) 669-7444

Дополнительная информация представлена на веб-сайте <http://www.speechpro.ru>.



Ни одна из частей этого документа не подлежит воспроизведению, передаче, хранению в поисковой системе или переводу на какой-либо язык в любой форме, любыми средствами без письменного разрешения ООО «ЦРТ».