«Визирь.СКУД»

Программный комплекс системы видеоидентификации

Модуль взаимодействия с MDM

Руководство администратора

ЦРТ | ГРУППА КОМПАНИЙ

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ 3
1.1. Общие положения 3
1.2. Правообладатель 3
1.3. Соглашения и обозначения 3
2. ОБЩИЕ СВЕДЕНИЯ 5
2.1. Сведения о программе и изготовителе 5
2.2. Техническая поддержка 5
2.3. Назначение и функции 5
3. РАБОТА СИСТЕМЫ 6
3.1. Общие сведения 6
3.2. Расширенное логирование по каждому терминалу 7
3.3. Групповое изменение настроек для группы терминалов 8
3.4. Соответствие настроек терминала и Сервера УТ 8
3.5. Иерархическая структура вложенных папок 10
3.6. Режимы терминала 11
3.7. Выгрузка данных о биометрических терминалах 12
3.8. Ролевая модель 13
3.9. Создание типовых настроек 14
3.10. Обновление рутовых сертификатов терминала 14

1. ВВЕДЕНИЕ

1.1. Общие положения

Данное руководство содержит сведения, необходимые для настройки **Модуля взаимодействия с MDM 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.
Курсив	Применяется для выделения первого появления *термина*, значение которого поясняется здесь же или даётся в приложении. Также применяется для оформления *примечаний*.
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**.
Полужирный курсив	Применяется для написания ***имен файлов*** и ***путей доступа*** к ним.

Формат	Описание
Подчёркнутый синий	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: Модуль взаимодействия с MDM программного комплекса 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

Модуль взаимодействия с 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.

3. РАБОТА СИСТЕМЫ

3.1. Общие сведения

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.

3.2. 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 "C" 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.

3.3. 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.

3.4. 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

3.5. 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.

3.6. 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.

3.7. 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]

3.8. 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.

3.9. 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.

3.10. Обновление рутовых сертификатов терминала

Алгоритм обновления:

- Генерация сертификатов в УЦ КС3 Encrypt и УЦ КС2 Devices Sign:
  - новый корневой сертификат открытого ключа шифрования УЦ КС3 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 КС2 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 КС3 для шифрования (УЦ КС3 Encrypt) – подпись singКС3. 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 (singКС3) архива, включая проверки цепочки сертификатов для доверенного УЦ КС3 Encrypt и проверки текущего CRL УЦ КС3 Encrypt;
- устанавливаются в доверенную зону на терминале:
  - новый корневой сертификат открытого ключа шифрования УЦ КС3 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 КС3 Encrypt, подписанный на новом корневом сертификате открытого ключа шифрования УЦ КС3;
- Определяется, какой CRL необходимо использовать на терминале двумя способами:
  - На основании математического сравнения подписей CRL и нового сертификата УЦ КС3 Encrypt;
  - По совпадению идентификаторов центра сертификации: authorityKeyIdentifier (сертификат УЦ КС3 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**.

© 2026 ООО «ЦРТ». Все права защищены.

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».