**АКЦИОНЕРНОЕ ОБЩЕСТВО "СОЦИАЛЬНАЯ КАРТА"**

|  |  |
| --- | --- |
|  | **УТВЕРЖДАЮ**  Генеральный директор  АО "Социальная Карта"  А. А. Бунятян  "\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023г. |

**АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДЕТЕКТИРОВАНИЯ И РАСПОЗНАВАНИЯ НА ОСНОВЕ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ «Face2Pass.Терминал»**

РУКОВОДСТВО АДМИНСТРАТОРА

1101690000940.05.11.01 Ф001 ИЗ-ЛУ

ЛИСТ УТВЕРЖДЕНИЯ

|  |  |
| --- | --- |
| **СОГЛАСОВАНО**  Руководитель направления развития биометрии | Т. В. Шипунов |

2024

**АКЦИОНЕРНОЕ ОБЩЕСТВО "СОЦИАЛЬНАЯ КАРТА"**

|  |  |
| --- | --- |
| УТВЕРЖДЕН 1101690000940.05.11.01 Ф001 ИЗ-ЛУ |  |

**АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДЕТЕКТИРОВАНИЯ И РАСПОЗНАВАНИЯ НА ОСНОВЕ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ «Face2Pass.Терминал»**

РУКОВОДСТВО АДМИНСТРАТОРА

1101690000940.05.11.01 Ф001 ИЗ

Листов: 19

2024

**АННОТАЦИЯ**

Настоящий документ является руководством системного программиста по установке автоматизированной системы детектирования и распознавания на основе биометрической идентификации «Face2Pass.Терминал» (далее по тексту - Система).

В данном руководстве приводится следующая информация:

В разделе "Назначение и условия применения" указаны назначение и функции программы и сведения о технических и программных средствах, обеспечивающих выполнение данной программы, а также требования к персоналу.

В разделе "Описание операций" приведено описание способов проверки, позволяющих дать общее заключение о работоспособности программы (контрольные примеры, методы прогона, результаты).

Документ разработан в соответствии с требованиями следующих документов:

* ГОСТ Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»;
* ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
* ГОСТ 2.105-95 «Единая система конструкторской документации. Общие требования к текстовым документам».

**СОДЕРЖАНИЕ**

[1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ 5](#_Toc137124482)

[1.1. Область применения 5](#_Toc137124483)

[1.2. Краткое описание возможностей 5](#_Toc137124484)

[1.3. Интеграция со СКУД Системами 5](#_Toc137124485)

[1.4. Уровень подготовки пользователей. 5](#_Toc137124486)

[2. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ 6](#_Toc137124487)

[2.1. Виды деятельности, функции, для автоматизации которых предназначено данное средство автоматизации 6](#_Toc137124488)

[2.2. Условия, при соблюдении которых обеспечивается применение средства автоматизации в соответствии с назначением 6](#_Toc137124489)

[2.2.1. Требования к программному обеспечению 6](#_Toc137124490)

[2.2.2. Требования к техническому обеспечению 7](#_Toc137124491)

[2.3. Требования к персоналу (системному программисту) 7](#_Toc137124492)

[3. УСТАНОВКА СИСТЕМЫ 8](#_Toc137124493)

[3.1. Установка в автоматическом режиме 8](#_Toc137124494)

[3.1.1. Автоматическая установка ядра ИС 8](#_Toc137124495)

[3.1.2. Автоматическая установка локальной части ИС 8](#_Toc137124496)

[4. ПОДГОТОВКА К РАБОТЕ И ПРОВЕРКА РАБОТОСПОСОБНОСТИ 9](#_Toc137124497)

[4.1. Общее описание конфигурационных файлов 9](#_Toc137124498)

[4.2. Проверка работоспособности 10](#_Toc137124499)

[4.2.1. Проверка работоспособности Серверной части 10](#_Toc137124500)

[5. ОПИСАНИЕ ОПЕРАЦИЙ 11](#_Toc137124501)

[5.1. Авторизация в Системе 11](#_Toc137124502)

[5.2. Главная страница Системы 11](#_Toc137124503)

[5.3. Регистрация нового администратора/оператора в Системе 11](#_Toc137124504)

[5.3.1. Создание администратора 11](#_Toc137124505)

[5.4. Пользователи Системы 12](#_Toc137124506)

[5.4.1. Регистрация нового пользователя в Системе 13](#_Toc137124507)

[5.5. Отчеты формируемые Системой 14](#_Toc137124508)

[5.6. Добавление точек прохода 14](#_Toc137124509)

[5.6.1. Добавление устройства 14](#_Toc137124510)

[5.6.2. Добавление групп устройств 15](#_Toc137124511)

[5.7. Группы доступа 15](#_Toc137124512)

[6. АВАРИЙНЫЕ СИТУАЦИИ 16](#_Toc137124513)

[7. ПЕРЕЧЕНЬ ТЕРМИНОВ 17](#_Toc137124514)

[8. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ 18](#_Toc137124515)

# ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

## Область применения

Автоматизированная система детектирования и распознавания на основе биометрической идентификации «Face2Pass.Терминал» входит в состав программно-аппаратного комплекса «Face2Pass». Предназначена для определения нахождения перед биометрическим терминалом живого человека, считывания QR кода, передачи биометрического образца, последующего получения и отображения уровня доступа, отправке сигнала в СКУД.

Система разработана с использованием методов на основе компьютерного зрения, которое обеспечивает высокую точность определения живого человека перед камерой.

## Краткое описание возможностей

Система предоставляет следующие возможности:

* взаимодействия с пользователем посредством отображения ошибок настройки;
* взаимодействия с пользователем посредством отображения уровня доступа;
* Работу с несколькими камерами[[1]](#footnote-1);
* Отсечения несанкционированного доступа с помощью электронных или бумажных фотографий при запуске[[2]](#footnote-2);
* Обеспечение доступа с помощью второго фактора: QR код, карты доступа и прочие[[3]](#footnote-3).

## Интеграция со СКУД Системами

В рамках ПАК «Face2Pass» имеет в своем составе сервер интеграции и может быть интегрирован со СКУД поддерживающие протоколы PERCO, Wiegand26, Bosh, Honeywell

## Уровень подготовки пользователей.

Пользователям не нужно проходить никакую дополнительную подготовку для работы с Системой.

# НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

## Виды деятельности, функции, для автоматизации которых предназначено данное средство автоматизации

Система позволяет автоматизировать следующие виды деятельности:

* Идентификация подмены документа доступа
* Получение уровня доступа Пользователей ПАК «Face2Pass»
* Распознавание и сопоставление QR кодов с мобильных устройств

Система может встраиваться в работу сторонних систем и устанавливаться для обеспечения автоматической работы в составе ПАК «Face2Pass». Взаимодействие со сторонними системами (вход и выход данных) выполняется без участия пользователя – через API.

## Условия, при соблюдении которых обеспечивается применение средства автоматизации в соответствии с назначением

Система может использоваться в следующих вариантах исполнения:

а) Х64 – в виде ПО установленного на компьютер с архитектурой x64 и подключением к камере с rtsp потоком[[4]](#footnote-4);

б) АРМ – в виде ПО установленного на биометрические терминалы Inoface.

Условием применения Системы является наличие у устройства, на котором будет производиться установка, функцией доступа в локальную сеть или сеть Интернет.

Во всех вариантах исполнения Системы предъявляются следующие минимальные требования:

− Требования к программному обеспечению;

− Требования к техническому обеспечению.

### Требования к программному обеспечению

К программному обеспечению для работы Системы предъявляются минимальные требования, перечисленные в таблице 1

Таблица 1 – Требования к конфигурации программного обеспечения клиентской части

|  |  |
| --- | --- |
| Компонент | Конфигурация |
| Операционная система | Ubuntu Linux 18.04 LTS или Ubuntu Linux 20.04 LTS |
| Общесистемное ПО | OpenCV 4.4 |

### Требования к техническому обеспечению

Для работы Системы конфигурация устройства должны удовлетворять минимальным требованиям к конфигурации аппаратного обеспечения, перечисленным в таблице 2.

Таблица 2 – Требования к конфигурации аппаратного обеспечения клиентской части

|  |  |
| --- | --- |
| Компонент | Минимальная конфигурация |
| Процессор | Intel Core i3-10-го поколения или ARMv8 Nvidia |
| Оперативная память | 4 Гб RAM |
| Жесткий диск | 32 ГБ HDD/SDD/SDCard |
| Видеоадаптер | встроен в системную плату |
| Сетевая плата | Ethernet 100 Мбит |
| Дополнительное оборудование | Монитор SVGA1280x1024, мышь, клавиатура |

## Требования к персоналу (системному программисту)

Системный программист должен иметь минимум среднее техническое образование.

В перечень задач, выполняемых системным программистом, должны входить:

* задача поддержания работоспособности технических средств;
* задача установки (инсталляции) и подержания работоспособности системных программных средств - операционной системы;
* задача установки (инсталляции) и подержания работоспособности программного обеспечения OpenCV;
* задача установки (инсталляции) и подержания работоспособности Автоматизированной системы детектирования и распознавания контроля и управления доступом на основе биометрической идентификации «Face2Pass.Терминал»

# УСТАНОВКА СИСТЕМЫ

Прежде чем начать использовать ПО, необходимо подготовить устройство и установить операционную систему. В этом разделе описаны шаги по скачиванию образа, записи его на флеш-карту и первоначальному запуску устройства.

## Шаги подготовки

#### Скачивание образа с сайта

Перейдите на официальный сайт распространения ПО по полученной ссылке и скачайте актуальный образ себе на компьютер

#### Запись образа на флеш-карту

**Важно**: В данной инструкции не рассматривается установка стороннего ПО Balena Etcher. Предполагается, что Balena Etcher уже установлен на вашем компьютере.

1. Подключите флеш-карту размером не менее 16 ГБ к компьютеру.
2. Откройте программу Balena Etcher.
3. Выберите скачанный образ операционной системы как источник.
4. Выберите подключенную флеш-карту как целевой диск.
5. Нажмите кнопку "Flash" для начала записи образа на флеш-карту.
6. Дождитесь завершения процесса. Программа уведомит вас об успешном завершении.

#### 3. Установка флеш-карты в Биометрический терминал

1. Отключите питание от биометрического терминала, если оно подключено.
2. Откройте корпус биометрического терминала и найдите слот для флеш-карты.
3. Вставьте подготовленную флеш-карту в слот до упора.
4. Закройте корпус биометрического терминала.

#### 4. Подача питания на устройство

1. Подключите кабель питания к биометрическому терминалу.
2. Включите питание.
3. Дождитесь загрузки операционной системы.

После выполнения этих шагов, Биометрический терминал будет готов к использованию. Переходите к следующему разделу инструкции для настройки и запуска ПО.

# ПОДГОТОВКА К РАБОТЕ И ПРОВЕРКА РАБОТОСПОСОБНОСТИ

## Общее описание конфигурационных файлов

Настройки приложений хранятся в конфигурационных JSON файлах каждого приложения, которые имеют стандартную структуру.

В общем файле должны быть заданы параметры доступа к сервисам системной платформы. У каждого сервиса свои параметры для работы с компонентами. Поскольку компоненты Системы имеют схожую структуру, ниже описание переменных окружения расположенные в файлах JSON в приложениях ИС.

Пример конфигурационного файла приложения VisionModule

"currentTarget": "csi\_inno" - текущий таргет  
"debugMode": false, - режим дебага, добавляет окно с отображением информации о детекции, инфраспуфе и пейпер спуфе. True - живое лицо, False - спуф.  
"enableInfraSpoof": true, - включить/выключить инфраспуф. true - включить, false - выключить.  
"enablePaperSpoof": true, - включить/выключить пейперспуф. true - включить, false - выключить.  
"paperSpoofVersion": 1, - версия пейперспуфа. 1 - пейперспуф использующий изображение с инфракрасной и оптической камеры(ВАЖНО: работает только вместе со включенным инфраспуфом). 2 - пейперспуф на основе оптической камеры и дополнения лица.  
    "paperSpoofV2ModelPadSize": 30, - процент дополнения для 2 пейперспуфа. \*др\*  
    "PaperSpoofV2Path": "models/mobnet\_v9\_mm\_cefa\_epoch\_6.onnx", - путь до модели для 1 пейперспуфа. \*др\*

## Первый запуск и калибровка камер

После первоначальной загрузки системы, вам будет предложено откалибровать камеры для обеспечения корректной работы детекции человека. В этом разделе описаны шаги по калибровке камер.

Шаги калибровки камер

1. Распечатайте "шахматную доску" предоставленную в приложении на листе формата A4.

2. Подключите биометрический терминал сети питания 220В

3. Процесс калибровки

Убедитесь, что камеры Биометрическому терминалу направлены на область, где будет размещена "шахматная доска". Поместите распечатанную "шахматную доску" перед камерами так, чтобы она была хорошо видна на обоих камерах.

Камеры начнут анализировать изображение с "шахматной доской". Когда калибровка будет завершена, окна камер на экране моргнут зеленым цветом.

У вас будет 30 секунд для проверки правильности настройки. Если все в порядке, переходите к следующему шагу. Если качество изображения неудовлетворительное, повторите процесс калибровки.

После успешной калибровки камер, перезапустите биометрический терминал.

Отключите питание и снова включите устройство.

Дождитесь загрузки системы.

Теперь камеры биометрический терминал готов к использованию. Переходите к следующему разделу инструкции для настройки и запуска основного ПО.

## Проверка работоспособности

### Проверка работоспособности. Успешный запуск.

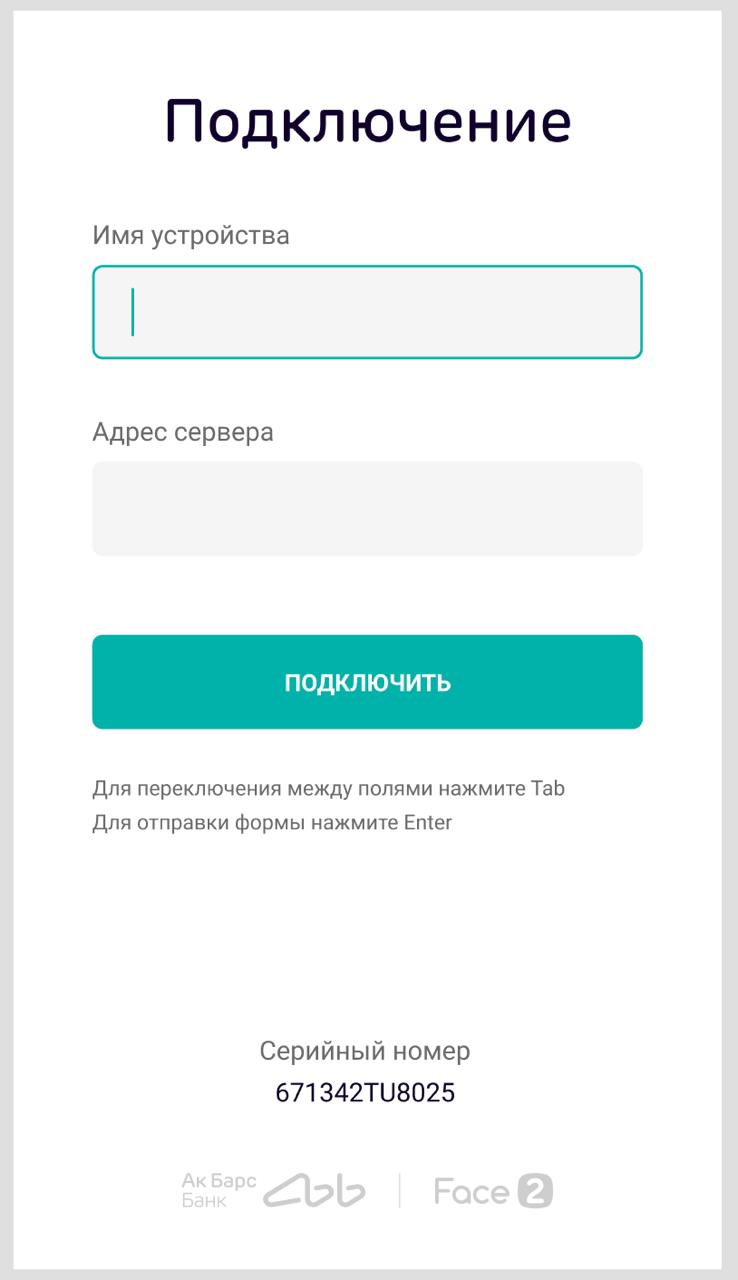
Во второй и последующие запуски система должна автоматически выходить на рабочий режим детектирования.



# ОПИСАНИЕ ОПЕРАЦИЙ

### Подключение к Серверу

В случае если предварительно в образе не были прописаны ключи авторизации в Системе Face2Pass биометрический терминал предложит произвести настройку терминала.



В таком случае раскройте корпус биометрического терминала, подключите клавиатуру и следуйте шагам настройки отображенных на экране.

На последнем экране будет указано что терминал сконфигурирован и ожидает подключения.



Следующим шагом необходимо подключиться к информационной Центральному серверу системы Face2Pass, перейти в настройки групп устройств и произвести авторизацию Биометрического терминала

### Изменение адреса терминала через командную строку

В случае если биометрический терминал переустанавливается на другой объект рекомендуется заново прошивать флеш-карту. Однако бывают моменты, когда нет возможности прошивки флеш-карты, в таких случаях допускается изменение конфигурационных файлов на биометрическом терминале. Для этого необходимо подключиться с рабочей станции сотрудника к терминалу и внести изменеия в конфигурационный файл.

В качестве рабочих станций пользователей могут использоваться любые персональные компьютеры, которые:

* имеют доступ до порта 22 биометрического терминала, на котором произведена установка ;
* оснащены интернет-браузером Google Chrome версии 81 или выше;
* оснащены ssh клиентом Pyttu или иным другим

Минимальная пропускная способность канала доступа для подключения одной точки доступа – не менее 10 Мбит/сек.

# АВАРИЙНЫЕ СИТУАЦИИ

Система является сложным программным комплексом, установка и настройка которого осуществляется администратором Системы. Возможны следующие ситуации:

* при попытке отправить изменения в формах Система выводит сообщение «Не заполнены обязательные поля для заполнения». Для сохранения изменений в форме необходимо заполнить указанные поля. Поля, обязательные для заполнения, отмечены символом «\*»;
* Система выводит системные сообщения, описание которых отсутствует в Руководстве пользователя. При возникновении указанной ситуации необходимо сформировать снимок (скриншот) пользовательского интерфейса Системы или протоколировать текст сообщения, выводимого Системой. Далее необходимо направить письмо c описанием сообщения администратору Системы по следующему адресу: [support@face2.ru](mailto:support@face2.ru);
* Биометрический терминал выводит сообщение «Терминал не работает»



В рамках данной ошибки ниже должно быть пояснение какой из сервисов недоступен, который необходим для работы.

* + *Камера недоступна* – камера биометрического терминала не доступна или неверно сконфигурирована в файлах конфигурации.
  + *Сервер недоступен* – нет сетевого доступа с биометрического терминала до локального сервера Face2Pass
  + *СКД недоступен* - нет сетевого доступа с биометрического терминала до сервиса исполняющего роль интеграции с установленной СКД

На момент запуска терминала допускается появление этих ошибок в первые 30 секунд работы терминала в связи с задержкой проверок зависимых сервисов.

# ПЕРЕЧЕНЬ ТЕРМИНОВ

В тексте настоящего документа используются следующие термины:

**СКУД –**система контроля и управления доступом.

**АСКУД –** автоматизированная система контроля и управления доступом.

**АСКУД БИ –** автоматизированная система контроля и управления доступом на основе биометрической идентификации.

**Система** – автоматизированной системы детектирования и распознавания контроля и управления доступом на основе биометрической идентификации «Face2Pass.Терминал».

**Администратор** – роль пользователя, наделенная полными правами доступа к административному интерфейсу Системы, может управлять структурой Системы, управлять реестром пользователей, настраивать подключение Системы в сторонние программные комплексы и информационные системы, иметь доступ к остальным сервисам Системы.

**Пользователь** – физические лицо, заинтересованные в процессе биометрической идентификации и сопоставления с помощью Системы, а также получения доступа на территорию с помощью программно-аппаратного комплекса «Face2Pass».

**Серверная часть** – основные сервисы входящие в состав АСКУД БИ «Face2Pass» содержащие возможность управления и изменения параметрами Системы.

**Локальная часть** – сервисы входящие в состав АСКУД БИ «Face2Pass» не содержащие возможность управления и изменения параметрами Системы.

**Биометрический терминал** – «Терминал биометрический INOFACE-7», ИД №3539378 в каталоге продукции Минпромторга России.

# ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В тексте настоящего документа используются следующие сокращения на русском и английских языках:

АРМ – автоматизированное рабочее место

ВМ/VM – виртуальная машина, программная и/или аппаратная система, эмулирующая аппаратное обеспечение компьютера гостевой платформы и исполняющая программы для гостевой платформы на платформе хозяине или виртуализирующая некоторую платформу и создающая на ней среды, изолирующие друг от друга программы и даже операционные системы

ГОСТ – государственный стандарт

ЕБС – Единая биометрическая система Российской Федерации

ИС – информационная система

ПО – программное обеспечение

СПО – специальное программное обеспечение

API – Application programming interface, программный интерфейс приложения

HTTPS - HyperText Transfer Protocol Secure, протокол передачи данных с поддержкой шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов

SSH – Secure Shell, сетевой протокол, посредством которого два компьютера могут взаимодействовать и обмениваться данными.

*Лист регистрации изменений*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номера листов (страниц) | | | | | Всего листов (страниц) в документе | Номер доку-мента | Входящий № сопрово-дительного документа и дата | Подпись | Дата |
| Изм. | изменен-ных | заменен-ных | новых | аннулиро-ванных |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

1. При запуске на Биометрическом терминале Inoface [↑](#footnote-ref-1)
2. При запуске на Биометрическом терминале Inoface [↑](#footnote-ref-2)
3. Может использоваться стороннее программное обеспечение [↑](#footnote-ref-3)
4. Необходимо уточнять совместимость устройств [↑](#footnote-ref-4)