

# Руководство пользователя

## SenseFP M2 & SenseFace M2F-LR

Дата: февраль 2025

Версия документа: 1.0

## Содержание

<b>1 ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ .....</b>	<b>5</b>
1.1 Положение пальца .....	5
1.2 Поза, положение тела и выражение лица★ .....	5
1.3 Регистрация шаблона лица★ .....	6
1.4 Интерфейс ожидания.....	7
1.5 Режим T9.....	8
1.6 Режим верификации.....	9
1.6.1 Верификация по отпечатку пальца.....	9
1.6.2 Верификация по карте.....	10
1.6.3 Верификация по лицу★ .....	11
1.6.4 Верификация по паролю.....	12
1.6.5 Комбинированная верификация.....	13
<b>2 ГЛАВНОЕ МЕНЮ.....</b>	<b>15</b>
<b>3 УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ.....</b>	<b>17</b>
3.1 Регистрация пользователя.....	17
3.1.1 ID и имя пользователя.....	17
3.1.2 Роль пользователя.....	17
3.1.3 Режим проверки (Verification Mode).....	18
3.1.4 Регистрация отпечатка пальца.....	18
3.1.5 Регистрация шаблона лица★ .....	18
3.1.6 Карта.....	19
3.1.7 Пароль.....	19
3.1.8 Фото профиля★ .....	20
3.2 Поиск пользователей.....	20
3.3 Редактирование пользователя.....	21
3.4 Удаление пользователя.....	21
3.5 Стиль отображения.....	22
<b>4 РОЛИ ПОЛЬЗОВАТЕЛЕЙ.....</b>	<b>23</b>
<b>5 НАСТРОЙКИ СВЯЗИ.....</b>	<b>24</b>
5.1 Настройки сети.....	24
5.2 Подключение к ПК.....	25
5.3 Беспроводная сеть★ .....	25
5.4 Настройки облачного сервера.....	27
5.5 Диагностика сети.....	28
<b>6 СИСТЕМНЫЕ НАСТРОЙКИ.....</b>	<b>29</b>
6.1 Дата и время.....	29
6.2 Учет рабочего времени (Attendance.....	30
6.3 Параметры шаблона лица★ .....	31

6.4	Параметры отпечатков пальцев.....	33
6.5	Настройки типа устройства.....	34
6.6	Настройки безопасности.....	34
6.7	Обновление через USB.....	35
6.8	Онлайн-обновление прошивки.....	35
6.9	Сброс к заводским настройкам.....	36
<b>7</b>	<b>ПЕРСОНАЛИЗАЦИЯ НАСТРОЕК.....</b>	<b>37</b>
7.1	Настройки пользовательского интерфейса.....	37
7.2	Настройки звука.....	38
7.3	Расписание звонков.....	38
7.4	Настройки состояний отметки.....	39
7.5	Назначение клавиш быстрого доступа.....	40
<b>8</b>	<b>УПРАВЛЕНИЕ ДАННЫМИ.....</b>	<b>42</b>
<b>9</b>	<b>КОД РАБОТЫ.....</b>	<b>44</b>
9.1	Добавление кода работы.....	44
9.2	Все коды работы.....	44
9.3	Настройки кода работы.....	45
<b>10</b>	<b>КОНТРОЛЬ ДОСТУПА .....</b>	<b>46</b>
10.1	Настройки контроля доступа.....	46
<b>11</b>	<b>МЕНЕДЖЕР USB.....</b>	<b>47</b>
11.1	Загрузка на USB.....	47
11.2	Выгрузка с USB.....	48
11.3	Настройки загрузки.....	48
<b>12</b>	<b>ПОИСК ОТМЕТОК.....</b>	<b>49</b>
<b>13</b>	<b>АВТОТЕСТ.....</b>	<b>50</b>
<b>14</b>	<b>СИСТЕМНАЯ ИНФОРМАЦИЯ.....</b>	<b>51</b>
<b>15</b>	<b>ПОДКЛЮЧЕНИЕ К ПО ZKBIO TIME.....</b>	<b>52</b>
15.1	Добавление устройства в программу.....	52
15.2	Добавление сотрудников в программу.....	53
<b>16</b>	<b>Подключение к приложению ZKBio Zlink .....</b>	<b>55</b>
16.1	Вход в приложение.....	55
16.2	Добавление устройства в приложении.....	56
16.3	Добавление пользователя.....	57
16.4	Настройка уровней доступа.....	58
16.5	Регистрация режима верификации в приложении.....	58

<b>ПРИЛОЖЕНИЕ 1 .....</b>	<b>62</b>
Требования к живой регистрации и шаблонам лиц★ в видимом свете★ .....	62
Требования к цифровому шаблону лица в видимом спектре★ .....	63

# 1 ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ

Перед ознакомлением с функциями устройства рекомендуется изучить основные принципы работы.

## 1.1 Положение пальца

**Рекомендуемые пальцы:** Указательный, средний или безымянный. Избегайте использования большого пальца или мизинца, так как их сложно правильно расположить на сканере.

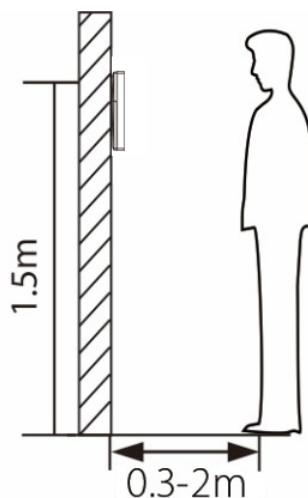


**Примечание:** При регистрации и идентификации правильно прикладывайте палец к сканеру. Компания не несет ответственности за проблемы с распознаванием, вызванные неправильным использованием. Мы оставляем за собой право окончательного толкования и внесения изменений в данное руководство.

## 1.2 Поза, положение тела и выражение лица★

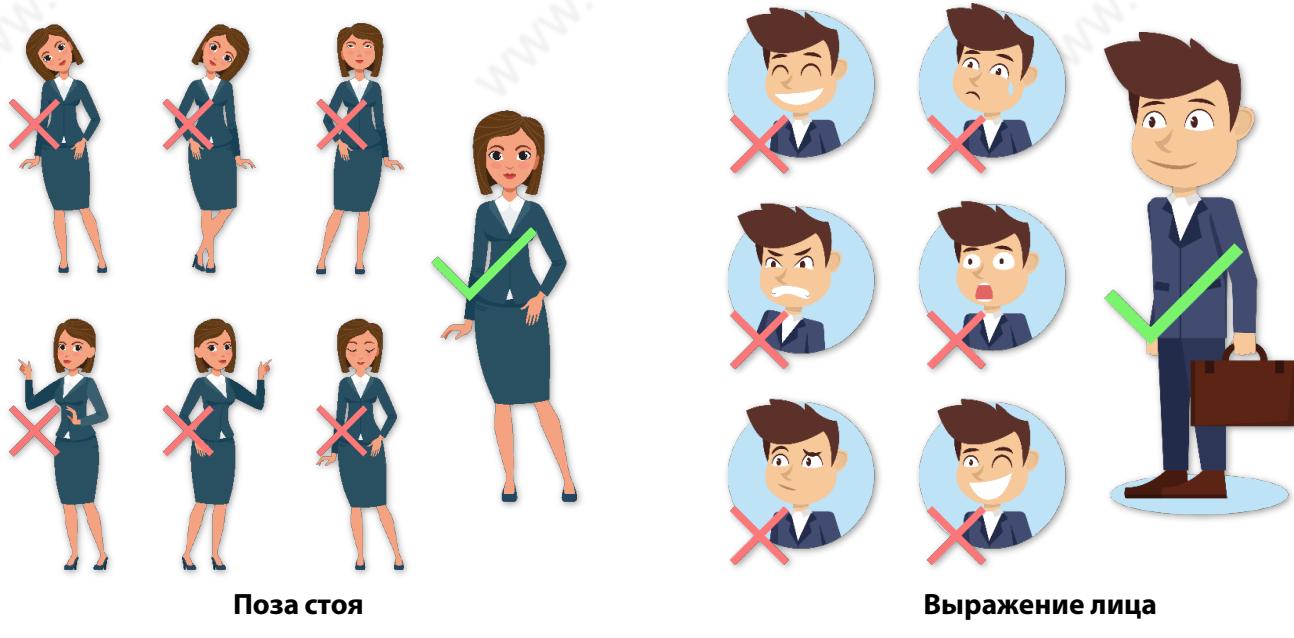
(Примечание: Только для устройств с камерой.)

### ➤ Рекомендуемое расстояние



Для пользователей ростом 1,55–1,85 м оптимальное расстояние до устройства — 0,3–2 м. Для улучшения качества изображения можно немного отодвинуться или приблизиться.

➤ **Рекомендуемая поза и выражение лица:**



**Примечание:** Во время регистрации и верификации сохраняйте естественное выражение лица и позу.

### 1.3 Регистрация шаблона лица★

(Примечание: Только для устройств с камерой.)

Убедитесь, что лицо находится в центре экрана во время регистрации. Смотрите прямо в камеру и не двигайтесь в процессе. Экран должен отображаться, как показано ниже:



#### Правильный метод регистрации и аутентификации лица

➤ **Рекомендации по регистрации шаблона лица:**

- При регистрации шаблона лица соблюдайте дистанцию 40–80 см между устройством и лицом.
- Не меняйте выражение лица (избегайте улыбок, нахмуренных бровей, подмигиваний и т.д.)
- Если не следовать инструкциям на экране, процесс может затянуться или завершиться ошибкой.

- Не закрывайте глаза и брови.
- Не используйте головные уборы, маски, солнцезащитные или обычные очки.
- В кадре должен находиться только один человек.
- Пользователям в очках рекомендуется зарегистрировать два шаблона: с очками и без.

#### ➤ Рекомендации по аутентификации:

- Убедитесь, что лицо полностью находится в пределах направляющих линий на экране устройства.
- При смене очков аутентификация может быть неудачной: если зарегистрирован шаблон без очков, выполняйте аутентификацию без очков; если зарегистрирован шаблон с очками, используйте те же очки.
- Если лицо частично закрыто головным убором, маской, повязкой или солнцезащитными очками, аутентификация может быть неудачной — не закрывайте лицо и обеспечьте видимость бровей для распознавания.

## 1.4 Интерфейс ожидания

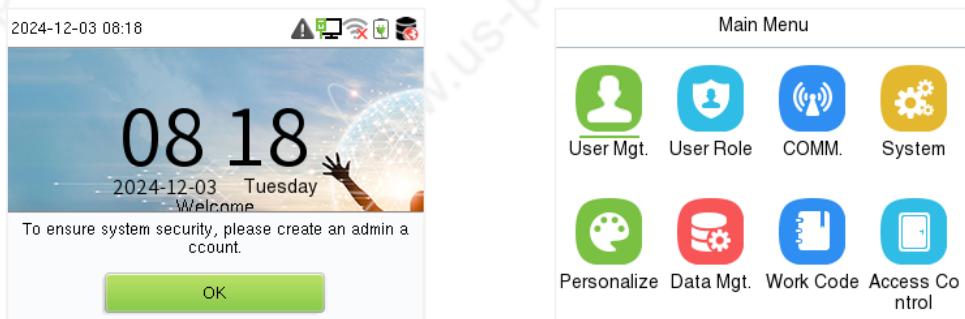
Устройство оснащено 2.8-дюймовым цветным экраном, управление осуществляется через клавиатуру. После включения отображается интерфейс ожидания:



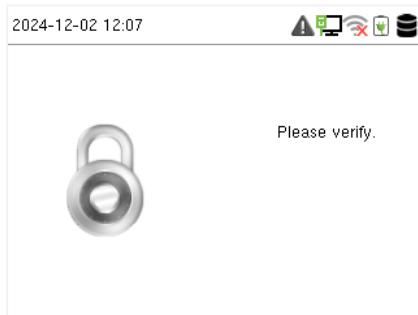
- Нажмите любую цифру для ввода **ID пользователя** (User ID)



- Если суперадминистратор не назначен, нажмите **M/OK** для доступа к меню.



- После добавления суперадминистратора на устройство требуется его верификация для доступа к функциям меню.



**Примечание:** Для безопасности устройства рекомендуется **сразу назначить суперадминистратора.**

- На интерфейсе ожидания также отображаются и могут быть использованы параметры состояния доступа. Соответствующие сочетания клавиш отображаются на экране при нажатии соответствующих горячих клавиш на клавиатуре (как показано на изображении ниже). Подробный способ работы см. в разделе «Сочетания клавиш».



## 1.5 Режим T9

Режим T9 позволяет вводить прописные, строчные и специальные символы в текстовых полях.

Для ввода букв и специальных символов нажмите соответствующую клавишу один раз (одно нажатие - один символ). Чтобы активировать режим T9, нажмите клавишу < ► > в текстовом поле.

- Перейдите в нужное поле и нажмите <M/OK>.



- Каждая клавиша клавиатуры содержит несколько букв (например, клавиша **3** соответствует символам **D, E, F**). Для ввода буквы **F** нажмите **3 три раза**. Система определяет вводимый символ путем сравнения количества нажатий с внутренним синтаксическим словарем.
- Для переключения между режимами ввода (прописные/строчные/специальные символы) нажмите клавишу < **►** >
- Для ввода специального символа нажмите соответствующую клавишу один раз. Например, чтобы ввести «@», нажмите **2 один раз**.
- После завершения ввода нажмите клавишу <**М/OK**> дважды для сохранения.

## 1.6 Режим верификации

### 1.6.1 Верификация по отпечатку пальца

#### ➤ Режим 1:N (один ко многим)

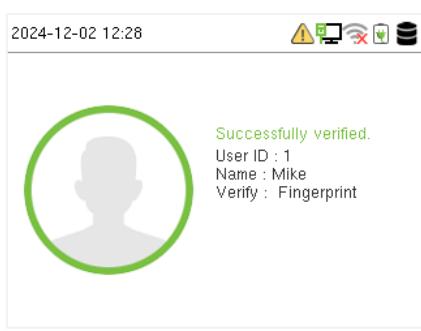
Устройство сравнивает текущий отпечаток пальца со всеми сохраненными в базе данных.

Для аутентификации пользователю необходимо приложить палец к сканеру.

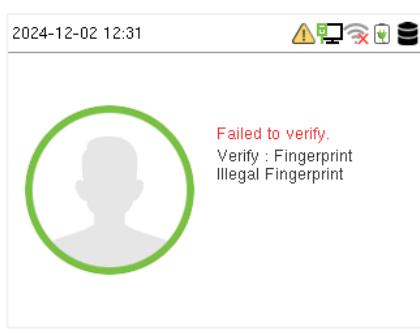
Для корректного сканирования следуйте рекомендованной методике расположения пальца.

Подробные инструкции см. в разделе «Позиционирование пальца».

Успешная верификация:



Неудачная верификация:



#### ➤ Режим 1:1 (один к одному)

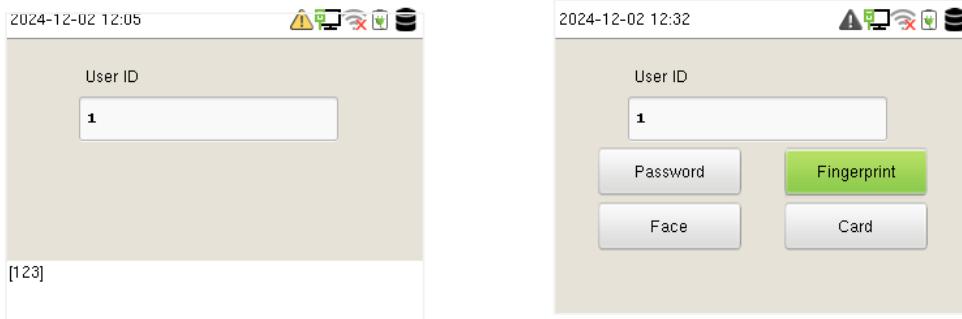
Устройство сравнивает текущий отпечаток пальца с отпечатками, привязанными к введенному с клавиатуры идентификатору пользователя (User ID).

В случае если пользователю не удалось получить доступ с использованием метода аутентификации 1:N, он может попытаться подтвердить личность с помощью режима верификации 1:1.

Введите идентификатор пользователя (User ID) и нажмите **М/ОК** для перехода в режим верификации отпечатка пальца 1:1.

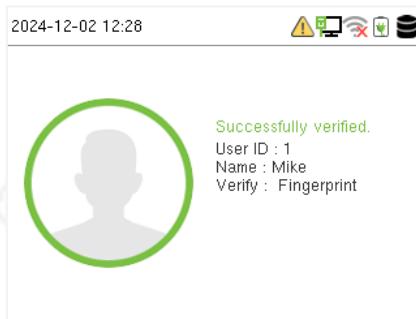
Если пользователь зарегистрировал карту, лицо и пароль в дополнение к отпечатку пальца, а метод верификации установлен на **Пароль/Отпечаток/Карта/Лицо** ★, на экране появится меню выбора.

Выберите Отпечаток пальца, чтобы перейти в соответствующий режим верификации.

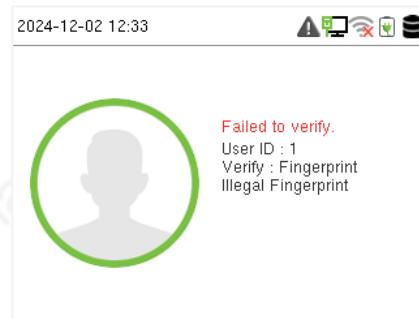


Приложите палец для верификации.

Верификация успешна:



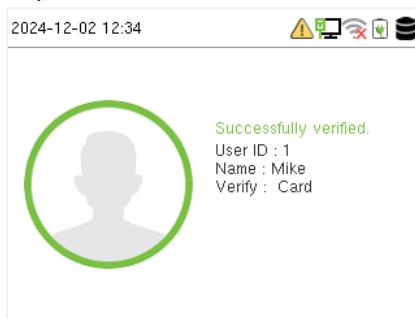
Верификация не выполнена:



## 1.6.2 Верификация по карте

### ➤ Верификация карты по методу 1:N (один ко многим)

Режим верификации карт 1:N выполняет сравнение номера карты, находящейся в зоне считывания, со всеми зарегистрированными в устройстве номерами карт. При верификации карты отображается следующий экран:



### ➤ Режим верификации карты 1:1

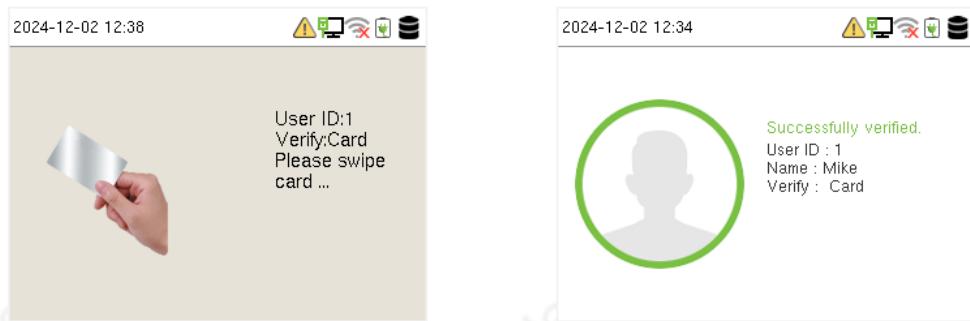
В режиме верификации 1:1 система сравнивает номер карты в зоне считывания с номером, привязанным к зарегистрированному в устройстве ID пользователя.

Введите ID пользователя (user ID) и нажмите клавишу **М/ОК** для перехода в режим верификации 1:1



Если пользователь зарегистрировал отпечаток пальца, лицо и пароль в дополнение к карте, а метод верификации установлен на Пароль/Отпечаток/Карта/Лицо★, на экране появится следующее меню выбора. Выберите Карта (Card) для перехода в режим верификации по карте.

После успешной проверки система отобразит уведомление **"Верификация успешно пройдена"** (Successfully verified), как показано на изображении ниже:

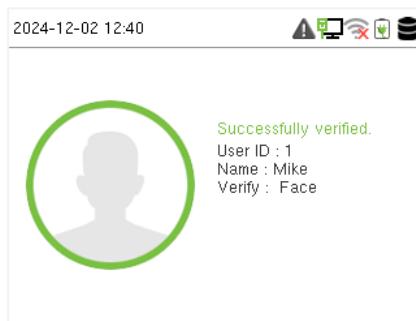


### 1.6.3 Верификация по лицу★

(Примечание: Только для устройств с камерой.)

#### ➤ Режим верификации по лицу 1:N

Устройство сравнивает полученное изображение лица со всеми зарегистрированными шаблонами в базе данных. Результат сравнения отображается во всплывающем окне.



#### ➤ Режим верификации по лицу 1:1

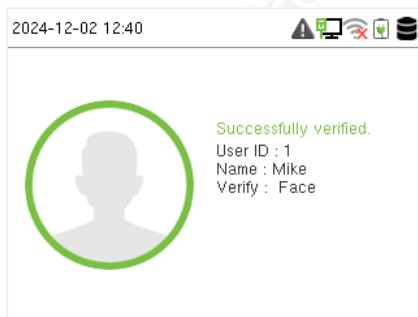
В данном режиме устройство сравнивает захваченное камерой лицо с шаблоном, привязанным к введенному ID пользователя. Введите **ID пользователя** (user ID) и нажмите **М/ОК** для перехода в режим верификации 1:1.



Если пользователь зарегистрировал отпечаток пальца, карту и пароль в дополнение к лицу, и выбран метод Пароль/Отпечаток/Карта/Лицо★. Выберите **Лицо** (Face) в меню выбора метода.



После успешной проверки система отобразит сообщение **"Верификация успешно пройдена"** (Successfully verified), как показано ниже:

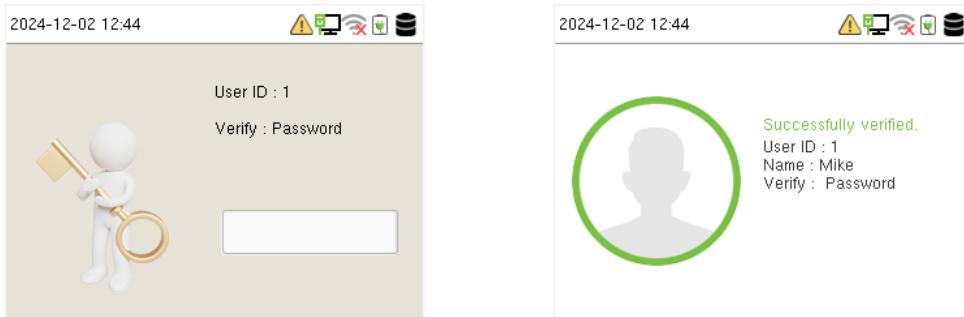


#### 1.6.4 Верификация по паролю

Устройство сверяет введённый пароль с зарегистрированным паролем и ID пользователя (User ID). Введите ID пользователя и нажмите **M/OK** для перехода в режим верификации пароля 1:1, затем снова введите ID пользователя и нажмите **M/OK**.

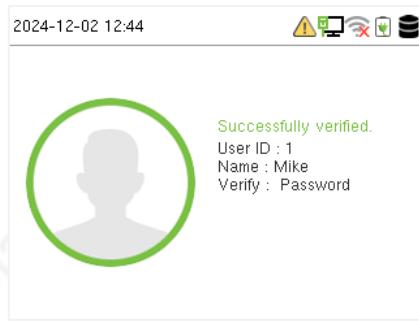


При настройке метода верификации "Пароль/Отпечаток/Карта/Лицо★" для пользователей, зарегистрировавших несколько идентификаторов (пароль, отпечаток пальца, карту и лицо), отображается экран выбора метода аутентификации. Выберите "Пароль" (Password) для перехода в режим проверки пароля.

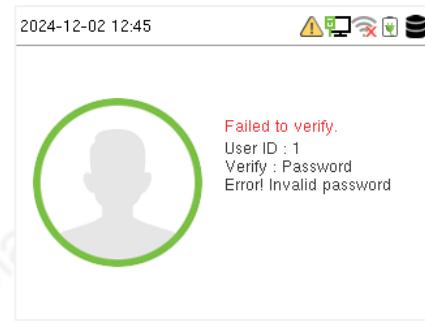


После ввода правильного и неправильного пароля отображается следующий экран:

Верификация успешна:



Верификация не пройдена:

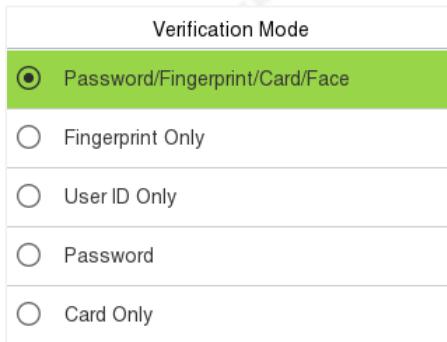


## 1.6.5 Комбинированная верификация

Для повышения безопасности устройство поддерживает использование нескольких методов верификации одновременно. Доступно 21 различных комбинаций проверки, как показано ниже:

**Обозначения комбинированной верификации:**

Символ	Описание	Пример
/	or или	Данный метод сравнивает введённые любые верификационные данные пользователя с сохранённым шаблоном верификации, привязанным к соответствующему ID персонала в устройстве.
+	and и	Данный метод сравнивает группу введенных верификационных данных пользователя со всеми шаблонами верификации, ранее сохраненными для данного ID персонала в устройстве.

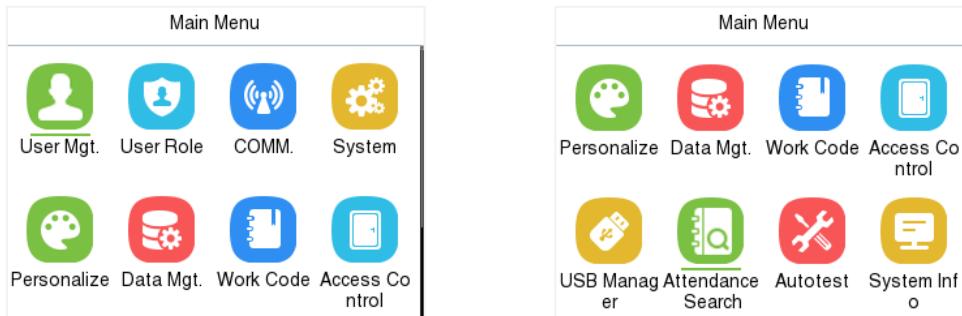


#### ➤ **Процедура настройки комбинированного режима верификации::**

- Комбинированная верификация требует, чтобы сотрудник зарегистрировал все указанные методы проверки. В противном случае сотрудники не смогут успешно пройти процесс комбинированной верификации.
- Например, если сотрудник зарегистрировал только данные лица, а в устройстве установлен режим верификации «Лицо + Пароль», он не сможет успешно завершить процесс верификации.
- Это происходит потому, что устройство сравнивает сканированный шаблон лица человека с зарегистрированными шаблонами верификации (как шаблон лица, так и пароль), ранее сохраненными для этого ID персонала в устройстве.
- Однако, поскольку сотрудник зарегистрировал только шаблон лица, но не пароль, верификация не будет завершена, и устройство отобразит сообщение «Верификация не пройдена» (Verification Failed).

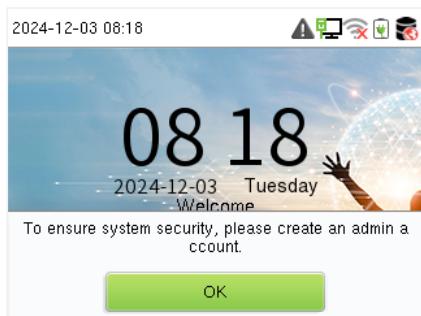
## 2 Главное меню

Нажмите **M/OK** для входа в **главное меню** (Main Menu). Доступны следующие разделы:



Раздел	Описание
<b>User Mgt.</b> Управление пользователями	Добавление, редактирование, просмотр и удаление пользователей
<b>User Role</b> Роли пользователей	Настройка прав доступа для пользовательских ролей
<b>COMM.</b> Настройка облачного сервиса	Настройка соответствующих параметров сети, подключения к ПК, беспроводной сети★, облачного сервера и диагностики сети.Ч
<b>System</b> Система	Для настройки параметров системы, включая дату и время, учет рабочего времени, параметры шаблонов лиц★ и отпечатков пальцев, настройки типа устройства, параметры безопасности, онлайн-обновление прошивки, обновление через USB и сброс к заводским настройкам
<b>Personalize</b> Персонализация	Настройка пользовательского интерфейса, голосовых оповещений, расписания звонков, параметров состояния отметки и назначения горячих клавиш
<b>Data Mgt.</b> Управление данными	Удаление всех соответствующих данных в устройстве
<b>Work Code</b> Коды работы	Настройка различных типов работ
<b>Access Control</b> Контроль доступа	Настройка параметров замка и соответствующего устройства контроля доступа
<b>USB Manager</b> USB-менеджер	Загрузка или выгрузка конкретных данных с помощью USB-накопителя
<b>Attendance Search</b> Поиск по событиям	Для запроса указанных журналов событий, проверки фотографий отметок★ и фотографий отметок из черного списка★
<b>Autotest</b> Автотест	Для автоматического тестирования работоспособности каждого модуля (ЖК-экран, аудиосистема, клавиатура, камера★, датчик отпечатков пальцев и часы реального времени)
<b>System Info</b> Информация	Для просмотра данных о емкости памяти, информации об устройстве и прошивке, а также политики конфиденциальности устройства

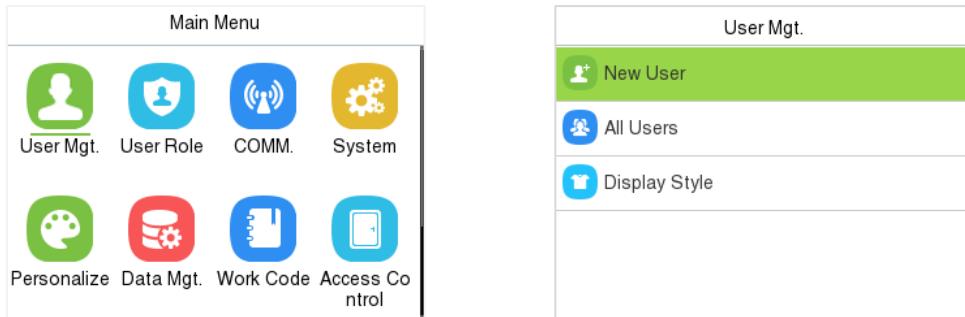
**Примечание:** При первом использовании продукта необходимо выполнить настройку с правами администратора. Нажмите **Управление пользователями** (User Mgt), чтобы добавить администратора или изменить права пользователя с помощью супер администратора. Если в продукте не настроен администратор, система будет отображать запрос на настройку администратора при каждом входе в меню устройства.



## 3 Управление пользователями

### 3.1 Регистрация пользователя

Когда устройство находится на начальном интерфейсе, нажмите **М/ОК** и перейдите в **Управление пользователями** (User Mgt.) > **Новый пользователь** (New User).



#### 3.1.1 ID и имя пользователя

Введите **ID пользователя** (User ID) и **имя** (Name).

New User	
User ID	1
Name	
User Role	Normal User
Verification Mode	Password/Fingerpr...
Fingerprint	0

#### Примечания:

- Имя пользователя может содержать максимум 34 символа
- Идентификатор пользователя (User ID) по умолчанию может содержать от 1 до 14 цифр, поддерживая как числа, так и буквенные символы.
- В процессе первоначальной регистрации вы можете изменить свой ID, однако после регистрации его изменение невозможно.
- Если появляется сообщение "**Дублируется**" (Duplicated!), необходимо выбрать другой ID, так как введенный User ID уже существует.

#### 3.1.2 Роль пользователя

На интерфейсе **Новый пользователь** (New User) выберите **Роль пользователя** (User Role), чтобы установить роль: **Обычный пользователь** (Normal User) или **Суперадминистратор** (Super Admin).

- Суперадминистратор** (Super Admin): обладает всеми правами управления устройством.
- Обычный пользователь** (Normal User): если Супер-администратор уже зарегистрирован в устройстве, обычные пользователи не смогут управлять системой и имеют доступ только к проверке аутентификации.
- Пользовательские роли** (User Defined Roles): Обычному пользователю также можно назначить пользовательскую роль — это настраиваемые роли, которые можно задать для обычного пользователя.

User Role
<input checked="" type="radio"/> Normal User
<input type="radio"/> Super Admin

**Примечание:** Если выбрана роль **Суперадминистратор**, пользователь должен пройти аутентификацию для доступа к главному меню. Аутентификация зависит от метода(ов), зарегистрированных супер-администратором. Подробнее см. Режим проверки (Verification Mode).

### 3.1.3 Режим проверки (Verification Mode)

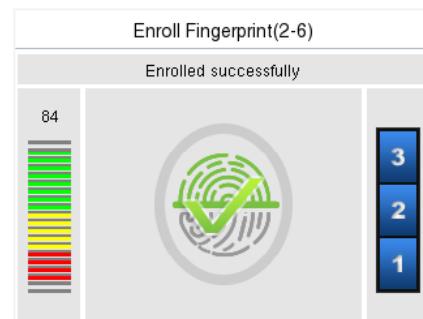
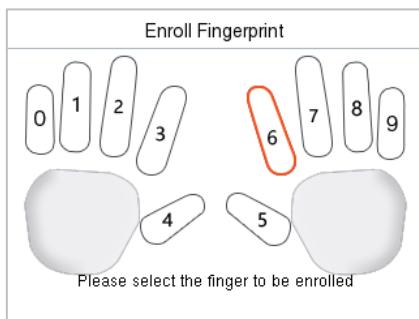
Выберите способ аутентификации пользователя. Доступно **21 различное сочетание методов** проверки. Подробности см. в разделе 1.6.5 Комбинированная проверка.

Verification Mode
<input checked="" type="radio"/> Password/Fingerprint/Card/Face
<input type="radio"/> Fingerprint Only
<input type="radio"/> User ID Only
<input type="radio"/> Password
<input type="radio"/> Card Only

### 3.1.4 Регистрация отпечатка пальца

Выберите **Отпечаток пальца** (Fingerprint) на интерфейсе **Новый пользователь**, чтобы перейти на страницу регистрации отпечатка..

- Выберите палец для регистрации.
- Приложите тот же палец к сканеру **три раза**.
- Зеленый индикатор означает успешную регистрацию отпечатка.



### 3.1.5 Регистрация шаблона лица★

Выберите **Лицо** (Face) на интерфейсе **Новый пользователь**, чтобы перейти на страницу регистрации лица.

- Повернитесь лицом к камере, разместите шаблон лица внутри белой направляющей рамки и оставайтесь неподвижным во время регистрации шаблона лица.

- При регистрации шаблона лица отображается индикатор выполнения, а при завершении процесса появляется сообщение **Шаблон успешно зарегистрирован** (Enrolled successfully).
- Если шаблон лица уже зарегистрирован в системе, отображается сообщение **"Дубликат лица"** (Duplicated Face). Интерфейс регистрации выглядит следующим образом:



### 3.1.6 Карта

Выберите **Карта** (Card) на интерфейсе **Новый пользователь**, чтобы перейти на страницу регистрации карты.

- В интерфейсе **"Карта"** (Card) проведите картой в зоне считывания. Регистрация карты будет выполнена успешно.
- Если карта уже зарегистрирована, появится сообщение **"Дубликат карты"** (Duplicate Card). Интерфейс регистрации выглядит следующим образом:



### 3.1.7 Пароль

Выберите Пароль (Password) на интерфейсе Новый пользователь, чтобы перейти на страницу регистрации пароля.

- Введите пароль и подтвердите его, затем нажмите **М/OK**.
- Если пароли не совпадают, устройство выведет сообщение **"Пароль не совпадает!"** (Password not match!), и потребуется повторное подтверждение.
- По умолчанию пароль может содержать **от 6 до 8 цифр**.

Password	
Please input	
<input type="text" value=" "/>	
Confirm (OK)	Cancel (ESC)

Password	
Please re-type the password.	
<input type="text" value="*****"/>	
Confirm (OK)	Cancel (ESC)

### 3.1.8 Фото профиля★

Выберите **Фото профиля** (Profile Photo) на интерфейсе Новый пользователь, чтобы перейти на страницу регистрации фото.



- Когда пользователь, зарегистрированный с фото, проходит аутентификацию, зарегистрированное фото отображается (включите Отображение фото пользователя в **[Система]** (System) > **[Посещаемость]** (Attendance)).
- Нажмите "Фото профиля" (Profile Photo) для активации камеры устройства, затем нажмите **М/OK** для съемки. Сделанное фото отобразится в верхнем левом углу экрана. Камера остается активной для возможности сделать дополнительные снимки при необходимости.

**Примечание:** При регистрации шаблона лица система автоматически сохраняет фото как фото профиля. Если фото профиля не зарегистрировано, система использует фото, сделанное при регистрации, по умолчанию.

## 3.2 Поиск пользователей

Когда устройство находится на начальном интерфейсе, нажмите **М/OK** и перейдите в **Управление пользователями** (User Mgt.) > **Все пользователи** (All Users).

- На интерфейсе "Список пользователей" (All Users) введите ключевое слово (ID, фамилия или полное имя) в строке поиска, и система найдет соответствующую информацию о пользователе.

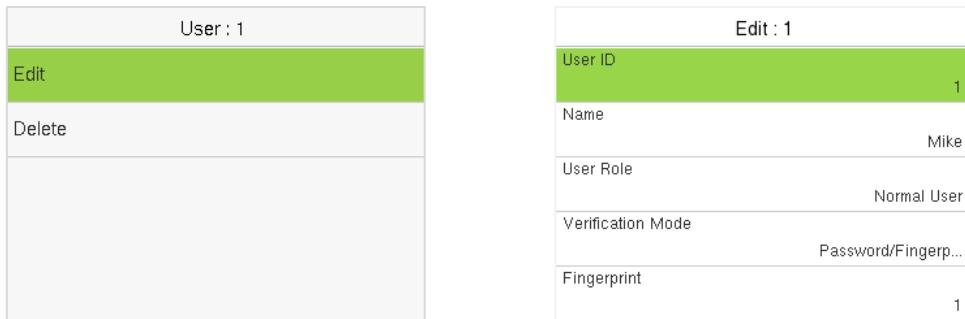
User Mgt.	
	New User
	All Users
	Display Style

All Users	
1	█ ⚡
2	█ ⚡
3	█
4	█
<input type="text" value="Search"/>	

### 3.3 Редактирование пользователя

На интерфейсе "Список пользователей" (All Users) выберите нужного пользователя из списка, нажмите **М/ОК**, затем выберите "Редактировать" (Edit), чтобы изменить информацию о пользователе.



**Примечание:** Процесс редактирования пользователя аналогичен добавлению пользователя, за исключением того, что ID пользователя нельзя изменить при редактировании. Подробный процесс см. в разделе "Управление пользователями".

### 3.4 Удаление пользователя

На интерфейсе "Все пользователи" (All Users) выберите нужного пользователя из списка, нажмите **М/ОК**, затем выберите "Удалить" (Delete), чтобы удалить пользователя или конкретную информацию о пользователе из устройства. На интерфейсе "Удаление" (Delete) выберите нужную операцию и нажмите **М/ОК** для подтверждения удаления.

#### ➤ Доступные операции удаления:

**Удалить пользователя** (Delete User): Вся информация о пользователе будет удалена (пользователь удаляется полностью).

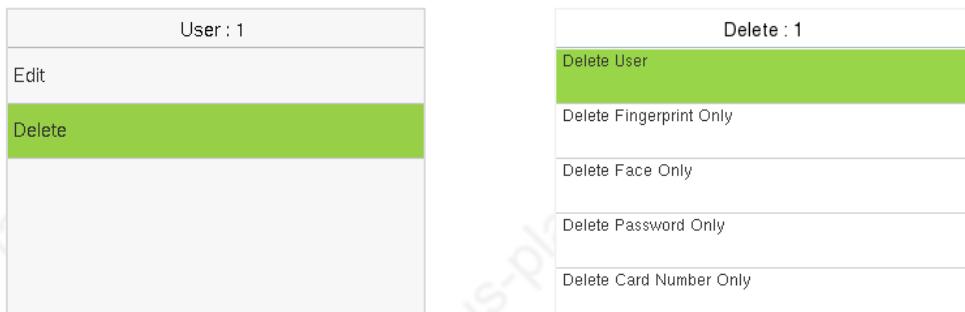
**Удалить только отпечаток пальца** (Delete Fingerprint Only): Удаляет данные отпечатка пальца выбранного пользователя.

**Удалить только лицо★** (Delete Face Only★): Удаляет шаблон лица выбранного пользователя.

**Удалить только пароль** (Delete Password Only): Удаляет пароль выбранного пользователя.

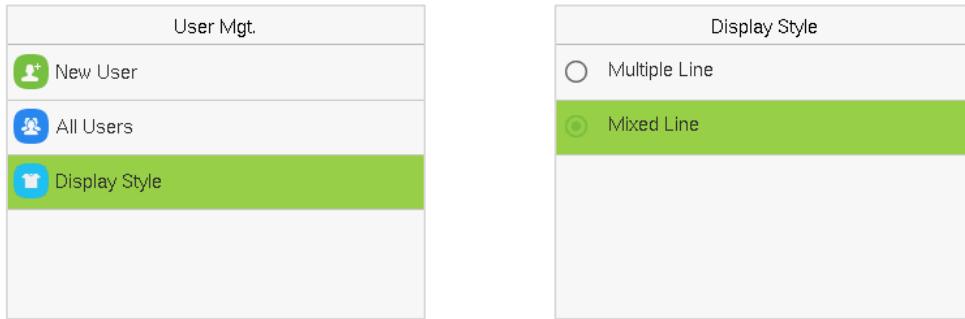
**Удалить только номер карты** (Delete Card Number Only): Удаляет информацию о карте выбранного пользователя.

**Удалить только фото профиля★** (Delete Profile Photo Only★): Удаляет фото профиля выбранного пользователя.



### 3.5 Стиль отображения

Когда устройство находится на начальном интерфейсе, нажмите **M/OK** и перейдите в "Управление пользователями" (User Mgt.) > "Стиль отображения" (Display Style).



Доступны следующие стили отображения:

Многострочный (Multiple Line):



Смешанный (Mixed Line):



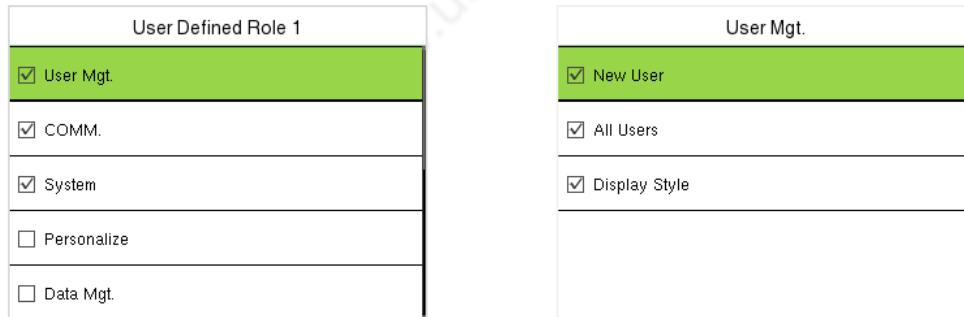
## 4 Роли пользователей

Функция "**Роли пользователей**" (User Role) позволяет назначать определенные права доступа пользователям в соответствии с требованиями.

- Когда устройство находится на начальном интерфейсе, нажмите **M/OK** и перейдите в "**Роли пользователей**" (User Role) > "**Пользовательские роли**" (User Defined Role), чтобы настроить права доступа.
- Область разрешений для пользовательской роли может быть разделена на 3 уровня, определяющих доступ к функциям меню.



- Выберите "**Определить роль пользователя**" (Define User Role), назначьте необходимые привилегии для новой роли и нажмите **M/OK**.
- Сначала выберите нужную функцию из **главного меню**, затем нажмите **M/OK** и выберите соответствующие подменю из списка.



### Примечание:

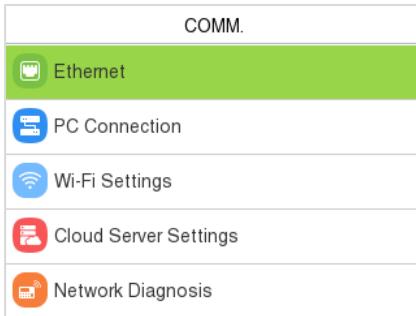
Если функция Роли пользователей активирована на устройстве, перейдите в **Управление пользователями** (User Mgt.) > **Новый пользователь** (New User) > **Роль пользователя** (User Role), чтобы назначить созданные роли пользователям.

Если в устройстве не зарегистрирован супер-администратор, при попытке включения функции Роли пользователей появится сообщение: "**Сначала зарегистрируйте суперадминистратора!** (Please enroll super admin first!)".

## 5 Настройки связи

Настройки связи используются для установки параметров сети, подключения к ПК, Wi-Fi★, облачного сервера и диагностики сети.

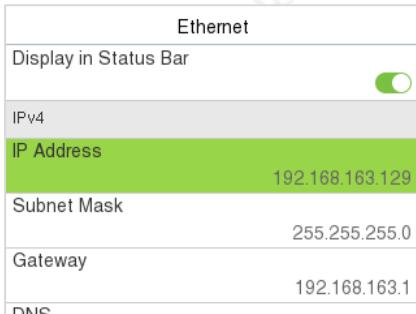
Когда устройство находится на начальном интерфейсе, нажмите **M/OK** и выберите **COMM**.



### 5.1 Настройки сети

Если устройству необходимо взаимодействовать с ПК через Ethernet, требуется настроить параметры сети и убедиться, что устройство и ПК находятся в одной подсети.

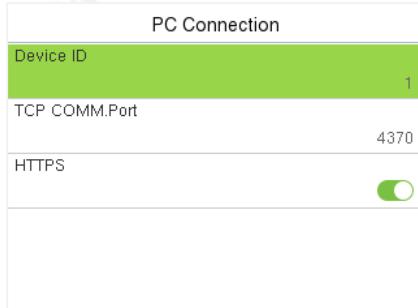
Выберите **Ethernet** в меню **COMM. Settings** для настройки.



Название функции	Описание
<b>Display in Status Bar</b> Отображение в строке состояния	Включите, чтобы отображать значок сети в строке состояния.
<b>IP Address</b> IP-адрес	По умолчанию: 192.168.1.201. Может быть изменен в зависимости от сети.
<b>Subnet Mask</b> Маска подсети	По умолчанию: 255.255.255.0. Может быть изменена.
<b>Gateway</b> Шлюз	По умолчанию: 0.0.0.0. Может быть изменен.
<b>DNS</b>	По умолчанию: 0.0.0.0. Может быть изменен.
<b>DHCP</b>	Протокол динамической настройки узла для автоматического назначения IP-адресов.

## 5.2 Подключение к ПК

Выберите **PC Connection** в меню **COMM. Settings** для настройки параметров



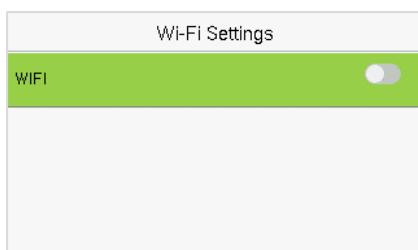
Название функции	Описание
<b>Device ID</b> ID устройства	Уникальный номер устройства должен находиться в диапазоне от 1 до 254.
<b>TCP COMM. Port</b> TCP порт связи	Значение TCP-порта по умолчанию: 4370. Оно может быть изменено в зависимости от конфигурации сети.
<b>HTTPS</b>	<p>Пользователи могут активировать протокол HTTPS, обеспечивающий безопасную и зашифрованную передачу данных, гарантируя защиту информации за счет аутентификации и шифрования соединения.</p> <p>Функция включена по умолчанию. Её можно активировать или деактивировать через интерфейс меню. При изменении статуса HTTPS устройство выводит предупреждение системы безопасности и выполняет перезагрузку после подтверждения.</p>

## 5.3 Беспроводная сеть★

Устройство поддерживает Wi-Fi модуль (встроенный или внешний), позволяющий подключаться к беспроводным сетям.

Модуль Wi-Fi обеспечивает передачу данных через беспроводную сеть (Wireless Fidelity) и создает беспроводную сетевую среду. По умолчанию Wi-Fi включен в устройстве. Если использование Wi-Fi сети не требуется, вы можете переключить кнопку в положение "Отключить".

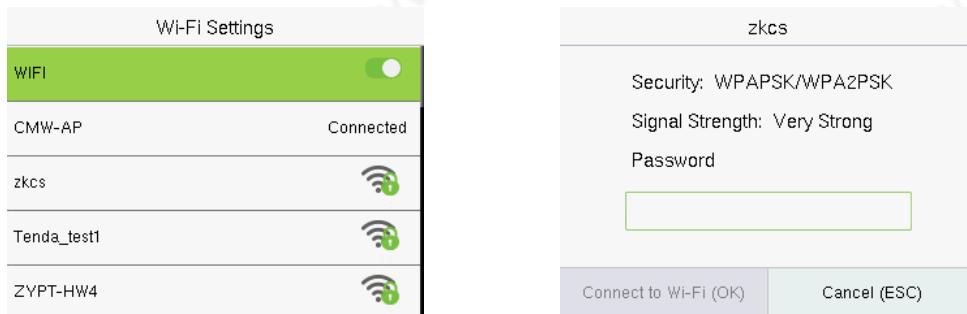
Выберите **Wi-Fi Settings** в меню **COMM. Settings** для настройки.



### ➤ Поиск сети Wi-Fi

- Wi-Fi включен по умолчанию. Используйте  для включения или отключения Wi-Fi.
- После включения Wi-Fi устройство выполнит поиск доступных сетей в пределах зоны действия.

- Выберите нужное имя Wi-Fi сети из списка доступных, введите правильный пароль в соответствующем поле и нажмите **М/OK** для подтверждения.



**Wi-Fi включен:** Выберите нужную сеть из списка найденных сетей.

Нажмите на поле ввода пароля, введите пароль, затем нажмите **М/OK**.

- При успешном подключении к Wi-Fi на начальном экране отобразится значок Wi-Fi.

#### ➤ Ручное добавление Wi-Fi сети

Wi-Fi сеть также можно добавить вручную, если нужная сеть не отображается в списке.



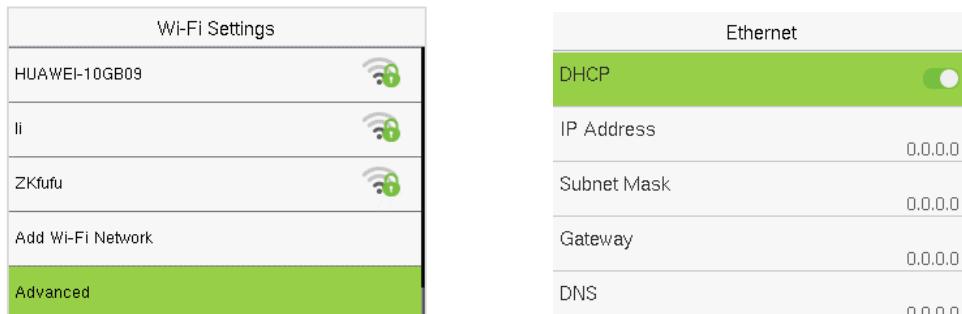
Нажмите «**Добавить сеть Wi-Fi**» (Add WiFi Network) для ручного ввода параметров сети.

На данном интерфейсе введите параметры Wi-Fi сети (добавляемая сеть должна существовать).

**Примечание:** После ручного добавления сети выполните поиск для подключения.

#### ➤ Дополнительные настройки

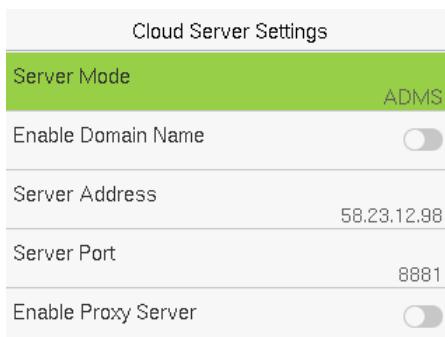
В меню **Wireless Network** нажмите **Advanced** для настройки параметров:



Название функции	Описание
<b>DHCP</b>	Протокол динамической конфигурации узла автоматически назначает IP-адреса сетевым клиентам. При включенном DHCP ручная настройка IP-адреса недоступна.
<b>IP Address</b> IP-адрес	IP-адрес для Wi-Fi сети по умолчанию: 0.0.0.0. Адрес может быть изменен в зависимости от конфигурации сети.
<b>Subnet Mask</b> Маска подсети	Маска подсети Wi-Fi сети по умолчанию: 255.255.255.0. Она может быть изменена в зависимости от конфигурации сети.
<b>Gateway</b> Шлюз	Адрес шлюза по умолчанию: 0.0.0.0. Может быть изменен в соответствии с конфигурацией сети.
<b>DNS</b>	DNS-адрес по умолчанию: 0.0.0.0. Может быть изменен в соответствии с конфигурацией сети.

## 5.4 Настройки облачного сервера

Выберите "**Настройка облачного сервера**" (Cloud Server Setting) в меню **Comm. Settings** для подключения к серверу ADMS.



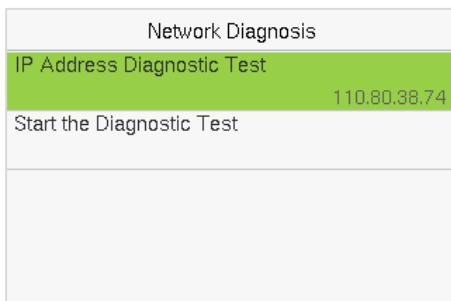
Название функции	Описание	
<b>Enable Domain Name</b> Включить доменное имя	<b>Server Address</b> Адрес сервера	При включении этой функции будет использоваться режим доменного имени "https://..." (например, https://www.XYZ.com), где "XYZ" обозначает доменное имя (активно при включенном режиме).
<b>Disable Domain Name</b> Отключить доменное имя	<b>Server Address</b>	IP-адрес сервера ADMS
	<b>Server Port</b> Порт сервера	Порт, используемый сервером ADMS
<b>Enable Proxy Server</b> Включить прокси-сервер		При включении прокси-сервера необходимо указать его IP-адрес и номер порта.

**Примечание:** Если устройство использует **BEST Protocol**, настройки облачного сервера не требуются.

## 5.5 Диагностика сети

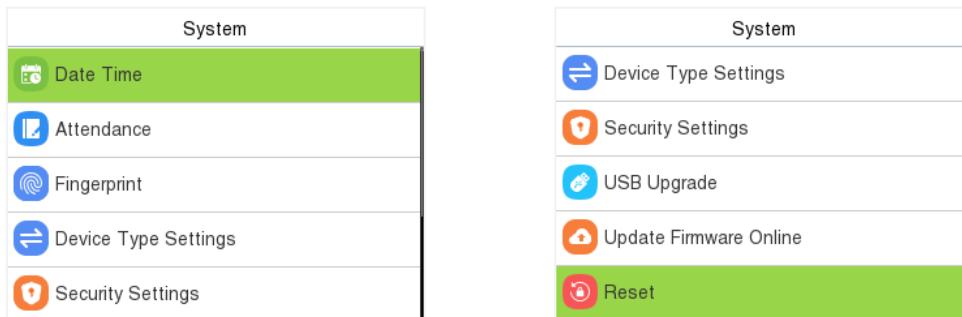
Позволяет настроить параметры диагностики сети.

Выберите "Диагностика сети" (Network Diagnosis) в меню **COMM. Settings**, введите IP-адрес для проверки и нажмите "Запустить диагностический тест" (Start the Diagnostic Test), чтобы проверить возможность подключения к устройству.



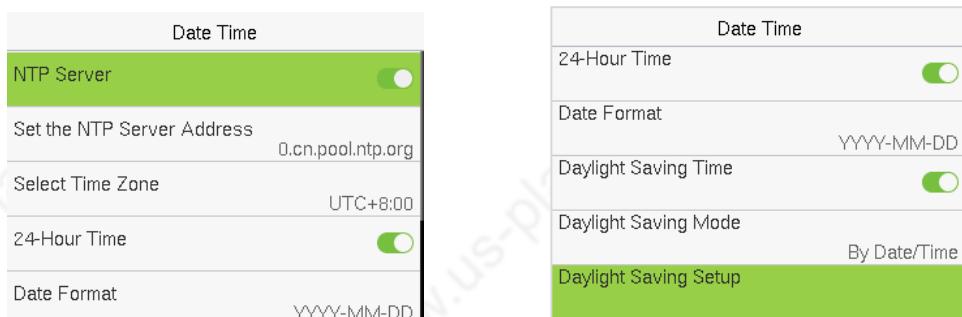
## 6 Системные настройки

Настройте параметры системы для оптимизации работы устройства. Когда устройство находится на начальном интерфейсе, нажмите **M/OK** и выберите "Система" (System).



### 6.1 Дата и время

Выберите "Дата и время" (Date Time) в меню "Система" (System) для настройки даты и времени.



- Нажмите «**Сервер NTP**» (NTP Server) для активации автоматической синхронизации времени по указанному адресу сервера.
- Нажмите «**Ручная установка даты и времени**» (Manual Date and Time) для ручной настройки, затем подтвердите выбор нажатием **M/OK** для сохранения.
- Нажмите «**Выбор часового пояса**» (Select Time Zone) для ручного указания часового пояса устройства.
- Для включения/отключения 24-часового формата времени выберите соответствующий пункт. При активации нажмите "Формат даты" (Date Format) для настройки отображения даты.
- Нажмите «**Летнее время**» (Daylight Saving Time) для включения или отключения функции. При активации нажмите «**Режим летнего времени**» (Daylight Saving Mode) для выбора режима, затем «**Настройка летнего времени**» (Daylight Saving Setup) для установки времени перехода.



Режим недели



Режим даты

- При восстановлении заводских настроек будут сброшены форматы времени (24-часовой) и даты (ГГГГ-ММ-ДД), но текущие дата и время устройства не изменятся.

**Примечание:** Если пользователь изменит время устройства (было: 15 марта 2019, 18:35) на 1 января 2020, 18:30, то после сброса к заводским настройкам время останется 1 января 2020, 18:30.

## 6.2 Учет рабочего времени (Attendance)

Выберите "Учет рабочего времени" (Attendance) в меню **System**.

Attendance	
Duplicate Punch Period(m)	1
Camera Mode	No photo
Display User Photo	<input checked="" type="checkbox"/>
Alphanumeric User ID	<input checked="" type="checkbox"/>
Attendance Log Alert	99

Attendance	
Periodic Del of T&A Data	Disabled
Periodic Del of T&A Photo	99
Periodic Del of Blocklist Photo	99
Authentication Timeout(s)	3
Recognition Interval(s)	1

Название функции	Описание
<b>Duplicate Punch Period(m)</b> Интервал повторной отметки (мин)	Повторные отметки в течение заданного интервала (1–999999 мин) не сохраняются.
<b>Camera Mode★</b> Режим камеры	Функция отключена по умолчанию. При включении появляется предупреждение системы безопасности, а звук затвора камеры становится обязательным. Режимы работы: <b>Без фото (No photo):</b> фотография не делается при верификации. <b>Съемка без сохранения (Take photo, no save):</b> фото делается, но не сохраняется. <b>Съемка с сохранением (Take photo and save):</b> сохраняются все фото, сделанные при верификации. <b>Сохранение при успехе (Save on successful verification):</b> фото сохраняется только при успешной верификации. <b>Сохранение при ошибке (Save on failed verification):</b> фото сохраняется только при неудачной верификации.
<b>Display User Photo</b> Отображение фото пользователя	Данная функция по умолчанию отключена. При включении появится предупреждение системы безопасности.
<b>Alphanumeric User ID</b> Буквенно-цифровой идентификатор пользователя	Активация/деактивация буквенно-цифрового формата для ID пользователя
<b>Attendance Log Alert</b> Оповещение о записи отметки	При достижении максимального установленного предела записей посещаемости устройство автоматически отображает предупреждение о заполнении памяти. Пользователь имеет возможность отключить данную функцию или установить допустимое значение в диапазоне от 1 до 9999.
<b>Periodic Del of T&amp;A Data</b> Период удаления данных учета рабочего времени	При достижении максимального объема памяти устройство автоматически удаляет часть старых записей посещаемости. Пользователь может отключить эту функцию или установить допустимое значение в диапазоне от 1 до 999 записей.
<b>Periodic Del of T&amp;A Photo★</b> Период удаления фото учета рабочего времени	При заполнении памяти до максимального объема устройство автоматически удаляет часть старых фотографий отметок. Пользователь может отключить данную функцию или задать количество сохраняемых фотографий от 1 до 99.

<b>Periodic Del of Blocklist Photo★</b> Автоматическое удаление фото отметок	При достижении максимального объема хранения устройство автоматически удаляет часть старых фотографий из чёрного списка. Пользователь может отключить эту функцию или задать количество сохраняемых фотографий (от 1 до 99).
<b>Authentication Timeout(s)</b> Таймаут аутентификации (сек)	Параметр определяет время (в секундах), в течение которого отображается сообщение об успешной проверке. Допустимый диапазон значений: от 1 до 9 секунд.
<b>Recognition Interval(s) ★</b> Интервал распознавания (сек)	При установке интервала (например, 5 секунд) система будет проверять лицо каждые 5 секунд. Допустимые значения: 0 (непрерывное распознавание) или 1-9 секунд (периодические проверки).

## 6.3 Параметры шаблона лица★

Выберите **Face** в меню **System** для настройки.



Название функции	Описание
<b>1:N Threshold</b> Порог верификации 1:N	Проверка будет успешной только в том случае, если сходство между полученным изображением лица и всеми зарегистрированными шаблонами лиц превысит установленное значение. Допустимое значение находится в диапазоне от 0 до 100. Чем выше пороговые значения, тем ниже вероятность ошибочной оценки, тем выше вероятность отклонения, и наоборот. Рекомендуемое значение по умолчанию: 40.
<b>1:1 Threshold</b> Порог верификации 1:1	В данном режиме верификация считается успешной только при превышении установленного процента совпадения между текущим изображением лица и зарегистрированным шаблоном пользователя. Диапазон значений: 0-100. Чем выше порог, тем ниже вероятность ошибочного распознавания, но выше процент отказов, и наоборот. Рекомендуемое значение по умолчанию: 30.

<b>Face Enrollment Threshold</b> Порог регистрации лиц	Во время регистрации шаблона лица используется сравнение 1:N для определения, был ли пользователь зарегистрирован ранее. Если степень сходства между полученным изображением лица и всеми зарегистрированными шаблонами превышает данный порог, это означает, что шаблон лица уже зарегистрирован в системе.
<b>Image Quality</b> Качество изображения	Качество изображения для регистрации и сравнения лиц. Чем выше значение, тем более чёткое изображение требуется.
<b>Facial Recognition Distance</b> Дистанция распознавания лица	Чем дальше находится человек, тем меньше размер его лица и тем меньше пикселей обрабатывает алгоритм. Настройка данного параметра позволяет регулировать максимальную дистанцию для распознавания лиц.
<b>LED Light Trigger Value</b> Порог активации LED-подсветки	Данный параметр регулирует включение и выключение светодиодной подсветки. Чем выше установленное значение, тем чаще будет активироваться и деактивироваться подсветка.
<b>Live Detection</b> Живое обнаружение	Система выявляет попытки обмана с помощью анализа изображений в видимом спектре, определяя, является ли предоставленный биометрический образец реальным человеком или подделкой.
<b>Live Detection Threshold</b> Порог обнаружения в реальном времени	Параметр определяет, является ли полученное изображение в видимом спектре реальным человеком. Чем выше значение, тем эффективнее защита от спуфинга с использованием видимого света.
<b>Anti-spoofing Using NIR</b> Защита от подмены данных с NIR	Использование ближнего инфракрасного спектрального изображения для выявления и предотвращения атак с использованием поддельных фотографий и видеозаписей.
<b>Binocular Live Detection Threshold</b> Порог биокулярного обнаружения	Параметр позволяет определить, является ли изображение в ближнем инфракрасном спектре поддельным. Чем выше значение, тем эффективнее защита от спуфинга с использованием ближнего ИК-спектра.
<b>Face AE</b> Автоэкспозиция для лиц	При нахождении лица перед камерой в режиме Face AE яркость области лица увеличивается, тогда как остальные участки изображения становятся темнее.
<b>WDR</b>	Технология широкого динамического диапазона (WDR) балансирует освещение и расширяет видимость изображения в видеонаблюдении при работе в условиях высокой контрастности, улучшая распознавание объектов как в ярких, так и в темных участках сцены.
<b>Anti-flicker Mode</b> Режим подавления мерцания	Режим применяется при отключенной функции WDR и помогает устраниТЬ мерцание, возникающее при совпадении частоты обновления экрана устройства с частотой импульсов освещения.
<b>Face Algorithm</b> Распознавания лиц	Содержит информацию о работе алгоритма обработки лиц и позволяет приостановить обновление лицевых шаблонов.

**Примечание:** Неправильная настройка параметров может ухудшить работу устройства. Изменяйте их только под руководством службы поддержки.

➤ **Процесс настройки точности распознавания:**

- В системном меню выберите пункт "Лицо" (Face), затем активируйте переключатель "Защита от спуфинга с использованием NIR" (Anti-Spoofing using NIR) для включения защиты от подделок.
- В главном меню выберите **Autotest > Test Face** для запуска процедуры тестирования системы распознавания лиц.
- Трижды нажмите на показатели в правом верхнем углу экрана – появится красная прямоугольная рамка, указывающая на начало корректировки параметров.

- Соблюдайте расстояние в длину руки между устройством и лицом. Для точного распознавания рекомендуется избегать резких или широких движений головой.

## 6.4 Параметры отпечатков пальцев

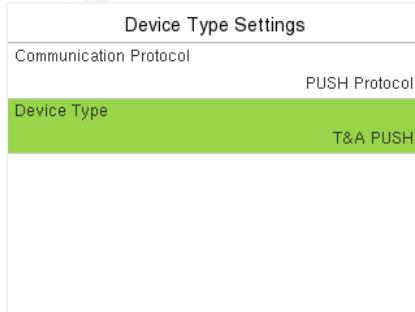
Выберите "Отпечатки пальцев" (Fingerprint) в меню **System** для настройки параметров отпечатков пальцев.



Название функции	Описание
<b>1:1 Threshold</b> Порог верификации 1:1	Проверка считается успешной только в случае, если степень совпадения между считанными данными отпечатка пальца и сохраненным шаблоном, привязанным к введенному ID пользователя, превышает установленное пороговое значение.
<b>1:N Threshold</b> Порог идентификации 1:N	Проверка считается успешной только при превышении установленного порога совпадения между считанными данными отпечатка и всеми сохранёнными в устройстве шаблонами.
<b>FP Sensor Sensitivity</b> Чувствительность датчика отпечатков	Параметр настраивает чувствительность сканирования отпечатков. Рекомендуется уровень " <b>Средний</b> " (Medium). В сухих условиях, когда скорость обнаружения снижается, установите значение " <b>Высокий</b> " (High). При высокой влажности, затрудняющей распознавание, используйте уровень " <b>Низкий</b> " (Low).
<b>1:1 Retry Attempts</b> Количество попыток при 1:1	Позволяет повторить попытку сканирования, если пользователь забыл зарегистрированный палец или приложил его неправильно, без повторного ввода ID.
<b>Fingerprint Algorithm</b> Алгоритм отпечатков пальцев	По умолчанию используется ZKFinger VX13.0. Доступно переключение на ZKFinger VX10.0.
<b>Fingerprint Image</b> Отображение изображения отпечатка	Функция по умолчанию отключена. После её отключения изображение отпечатка пальца не будет отображаться при регистрации и верификации отпечатков пальцев. Интерфейс меню позволяет включить или отключить эту функцию, при переключении появляются запросы безопасности. Доступны четыре варианта: <b>Show for Enroll (Показывать при регистрации)</b> — отображение только во время записи отпечатка; <b>Show for Match (Показывать при проверке)</b> — только во время верификации; <b>Always Show (Показывать всегда)</b> — в обоих режимах; <b>None (Не показывать)</b> — полное отключение отображения.

## 6.5 Настройки типа устройства

Выберите **Device Type Settings (Настройки типа устройства)** в меню **System** для настройки параметров устройства.

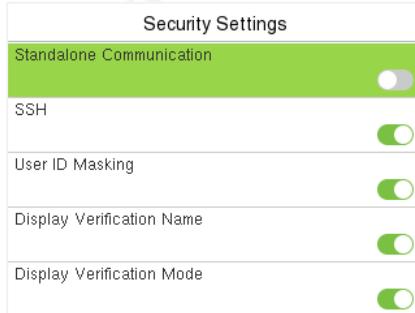


Название функции	Описание
<b>Communication Protocol</b> Настройка протокола связи	Установите протокол связи устройства: PUSH Protocol или BEST Protocol. (Протокол BEST предназначен для работы с ZKBio Zlink. Подробности см. в разделах "16. Подключение к ZKBio Zlink App" и "17. Подключение к ZKBio Zlink Web".)
<b>Device Type</b> Тип устройства	По умолчанию используется T&A PUSH. Данный параметр не подлежит изменению.

**Примечание:** После изменения типа устройства все данные будут удалены, устройство перезагрузится, а некоторые функции автоматически адаптируются под новый режим работы.

## 6.6 Настройки безопасности

Выберите **Security Settings (Настройки безопасности)** в меню **System** для настройки параметров безопасности.



Название функции	Описание
<b>Standalone Communication</b> Автономный режим связи	По умолчанию отключена. Управление (включение/отключение) осуществляется через интерфейс меню. При активации появляется предупреждение системы безопасности, после подтверждения которого устройство перезагружается.
<b>SSH</b>	Устройство не поддерживает Telnet, поэтому для удаленной отладки обычно используется SSH. По умолчанию SSH включен. Статус можно изменить в меню. При включении отображается предупреждение безопасности, но перезагрузка устройства не требуется.
<b>User ID Masking</b> Маскировка ID пользователя	После активации идентификатор пользователя частично скрывается при отображении результатов верификации (функция доступна только для ID длиной более 2 символов). По умолчанию включена.

<b>Display Verification Name</b> Отображение имени при верификации	При включении функции после подтверждения идентификации будет отображаться имя пользователя. При отключении имя отображаться не будет.
<b>Display Verification Mode</b> Отображение метода верификации	Активация функции позволяет показывать способ идентификации (например, по лицу или отпечатку) в результатах проверки. При деактивации эта информация скрывается.
<b>Save Photo as Template</b> Сохранение фото как шаблон	Отключение данной функции потребует повторной регистрации лицевых шаблонов после обновления алгоритма распознавания.

## 6.7 Обновление через USB

Выберите **USB Upgrade (USB-обновление)** в меню **System**.

Программное обеспечение устройства может быть обновлено с использованием файла прошивки на USB-накопителе. Перед выполнением данной операции необходимо убедиться, что USB-накопитель содержит корректный файл обновления и правильно подключен к устройству.

При отсутствии подключенного USB-накопителя система выведет соответствующее сообщение после нажатия пункта "**USB Upgrade**" в системном меню.



**Примечание:** Для получения файла обновления обратитесь в службу технической поддержки. Обновление прошивки не рекомендуется выполнять в штатных условиях эксплуатации.

## 6.8 Онлайн-обновление прошивки

Выберите **Update Firmware Online (Обновление прошивки онлайн)** в меню **System**.

При включении функции **Enable Firmware Update Online** система выведет предупреждение о потенциальных рисках для безопасности данных, требующее обязательного подтверждения пользователем вручную.



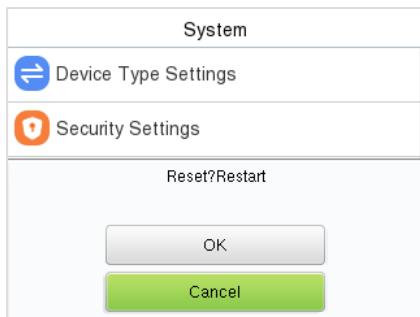
При нажатии **Check for Updates** могут возникнуть три возможных сценария:

- При неудачном запросе интерфейс отобразит сообщение **Query Failed (Ошибка запроса)**.
- Если текущая версия прошивки устройства актуальна, появится уведомление **Already the Latest Version (Уже установлена последняя версия)**.
- В случае устаревшей версии прошивки система отобразит номер новой версии и список изменений, после чего пользователь сможет выбрать необходимость обновления до последней версии.

## 6.9 Сброс к заводским настройкам

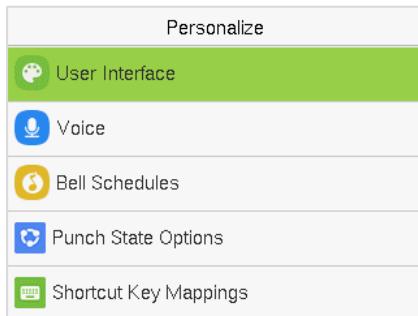
Функция "Сброс к заводским настройкам" восстанавливает параметры устройства, такие как настройки связи и системные настройки, до значений по умолчанию (эта функция не удаляет зарегистрированные пользовательские данные).

Выберите **Reset** (Сброс) в интерфейсе **System** (Система) и нажмите **M/OK**, чтобы восстановить заводские настройки по умолчанию.



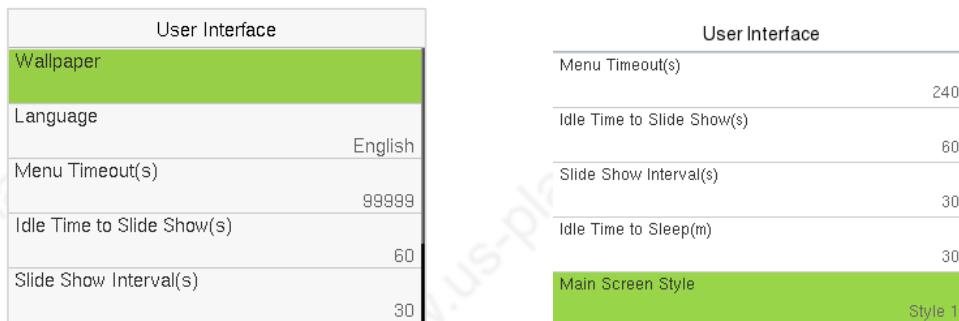
## 7 Персонализация настроек

Когда устройство находится на начальном интерфейсе, нажмите **M/OK** и выберите **Personalize** (**Персонализация**), чтобы настроить параметры интерфейса, звука, звонка, состояния удара и назначения клавиш быстрого доступа.



### 7.1 Настройки пользовательского интерфейса

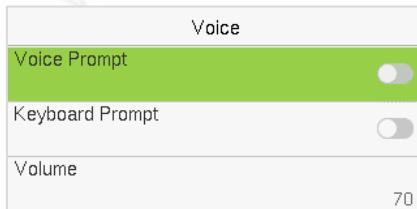
Выберите **User Interface** (**Пользовательский интерфейс**) в меню **Personalize** (**Персонализация**), чтобы настроить стиль отображения главного интерфейса.



Название функции	Описание
<b>Wallpaper</b> Обои	Позволяет выбирать изображение для главного экрана согласно предпочтениям пользователя.
<b>Language</b> Язык	Определяет язык интерфейса устройства.
<b>Menu Timeout (s)</b> Таймаут меню (сек)	При отсутствии действий в течение заданного времени (от 60 до 99999 секунд) система автоматически возвращается к начальному экрану. Функция может быть отключена.
<b>Idle Time to Slide Show (s)</b> Время до запуска слайд-шоу (сек)	Активирует слайд-шоу при бездействии пользователя в течение установленного периода (от 3 до 999 секунд). Возможно отключение функции.
<b>Slide Show Interval (s)</b> Интервал слайд-шоу (сек)	Определяет время переключения между изображениями в слайд-шоу (от 3 до 999 секунд). Функция поддерживает отключение.
<b>Idle Time to Sleep (m)</b> Время до перехода в спящий режим (мин)	Переводит устройство в режим ожидания при бездействии (от 1 до 999 минут), если активирована соответствующая функция.
<b>Main Screen Style</b> Стиль главного экрана	Позволяет выбрать оформление основного интерфейса по предпочтениям пользователя.

## 7.2 Настройки звука

Перейдите в меню **Personalize (Персонализация)**, выберите пункт **Voice (Голос)** для настройки голосовых параметров системы.



Название функции	Описание
<b>Voice Prompt</b> Голосовые подсказки	Функция включает или отключает звуковые оповещения при выполнении операций.
<b>Touch Prompt</b> Звук нажатий	Параметр активирует или деактивирует звуковое сопровождение нажатий на клавиатуре.
<b>Volume</b> Громкость	Регулирует уровень громкости устройства с диапазоном значений от 0 до 100.

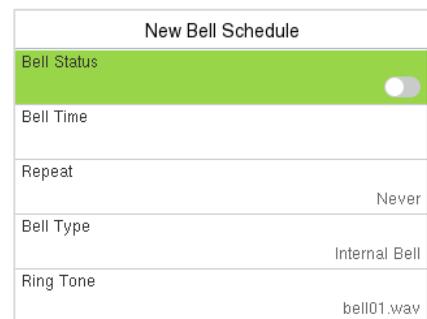
## 7.3 Расписание звонков

Выберите **Bell Schedules (Расписание звонков)** в меню **Personalize (Персонализация)** для настройки параметров звонка.



### ➤ Новое расписание звонка

Выберите **New Bell Schedule (Новое расписание звонка)** в интерфейсе **Bell Schedule** (Расписание звонков) для добавления нового расписания.



Название функции	Описание
<b>Bell Status</b> Состояние звонка	Переключатель для активации/деактивации функции звонка.
<b>Bell Time</b> Время звонка	При установке времени устройство автоматически активирует звонок в заданный период.
<b>Repeat</b> Повторение	Устанавливает количество повторений запланированного звонка.

<b>Bell Type</b> Тип звонка	Выбор типа сигнала: внутренний звонок, внешний звонок или оба варианта одновременно.
<b>Ring Tone</b> Мелодия звонка	Настройка звукового сигнала для оповещения.
<b>Internal Bell Delay(s)</b> Задержка внутреннего звонка (сек)	Установка интервала повторения внутреннего сигнала. Допустимый диапазон значений: от 1 до 999 секунд.

➤ **Все расписания звонков** (All Bell Schedules):

Для просмотра всех запланированных звонков перейдите в интерфейс **Bell Schedules** (Расписание звонков) и выберите **All Bell Schedules** (Все расписания звонков)

➤ **Редактирование запланированного звонка** (Edit the Scheduled Bell):

В интерфейсе **All Bell Schedules** (Все расписания звонков) выберите нужное расписание и нажмите **Edit** (Редактировать). Процесс редактирования аналогичен созданию нового расписания.

➤ **Удаление звонка** (Delete a Bell):

В интерфейсе **All Bell Schedules** (Все расписания звонков) выберите нужное расписание, нажмите **Delete** (Удалить), затем подтвердите действие кнопкой M/OK для удаления выбранного звонка.

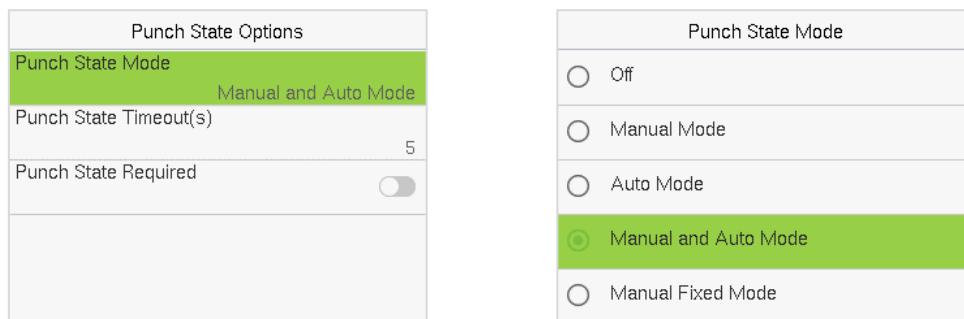
➤ **Дополнительные настройки** (Options):

В интерфейсе **Bell Schedule** (Расписание звонков) выберите **Options** (Опции) для настройки внешнего вывода звонка (терминал NCI/NO1), который по умолчанию отключен.

**Примечание:** Внешний звонок и замок являются взаимоисключающими функциями. При активации внешнего звонка убедитесь в правильности подключения проводов.

## 7.4 Настройки состояний отметки

Выберите **Punch States Options** (Настройки состояний отметки) в меню **Personalize** (Персонализация) для конфигурации параметров состояния отметки.



Название функции	Описание
<b>Punch State Mode</b> Режим состояния отметки	<p><b>Off:</b> Деактивирует функцию состояния отметки. В этом случае назначенная клавиша в меню <b>Shortcut Key Mappings</b> (Назначение горячих клавиш) становится неактивной.</p> <p><b>Manual Mode:</b> Переключение клавиши состояния отметки вручную. Клавиша исчезнет после истечения времени, заданного в параметре <b>Punch State Timeout</b> (Таймаут состояния отметки).</p> <p><b>Auto Mode:</b> Клавиша состояния отметки автоматически переключается на заданное состояние согласно расписанию, которое можно настроить в меню <b>Shortcut Key Mappings</b> (Назначение клавиш быстрого доступа)</p>

	<p><b>Manual and Auto Mode:</b> На главном экране отображается клавиша автоматического переключения состояния отметки, но пользователи также могут вручную выбрать альтернативный статус отметки. После истечения таймаута клавиша вернется в автоматический режим.</p> <p><b>Manual Fixed Mode:</b> После ручной установки состояния отметки функция остается неизменной до следующего ручного переключения.</p> <p><b>Fixed Mode:</b> Отображается только фиксированная клавиша состояния отметки. Пользователи не могут изменить статус нажатием других клавиш.</p>
<b>Punch State Timeout(s)</b> Таймаут состояния отметки (сек)	Определяет продолжительность отображения состояния отметки. Допустимый диапазон значений: от 5 до 999 секунд.
<b>Punch State Required</b> Обязательное указание состояния	<p>Параметр определяет необходимость выбора состояния посещаемости после верификации:</p> <p><b>ON:</b> Требуется выбор состояния после подтверждения личности.</p> <p><b>OFF:</b> Выбор состояния не требуется.</p>

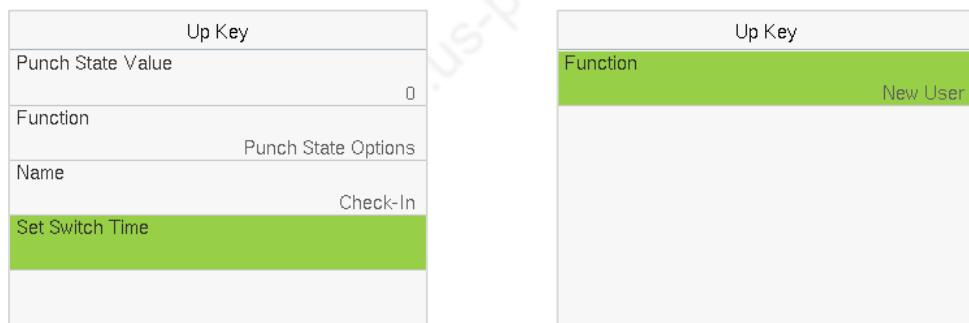
## 7.5 Назначение клавиш быстрого доступа

Пользователи могут назначать клавиши быстрого доступа для статусов отметки и функциональных клавиш, которые будут отображаться на главном экране. При нажатии этих клавиш будет сразу отображаться соответствующий статус отметки или функциональный интерфейс.

Выберите **Shortcut Key Mappings** (Назначение клавиш быстрого доступа) on the **Personalize** (Персонализация) interface to set the required shortcut keys.

Shortcut Key Mappings	
Up Key	Check-In
Down Key	Check-Out
Left Key	Overtime-In
Right Key	Overtime-Out

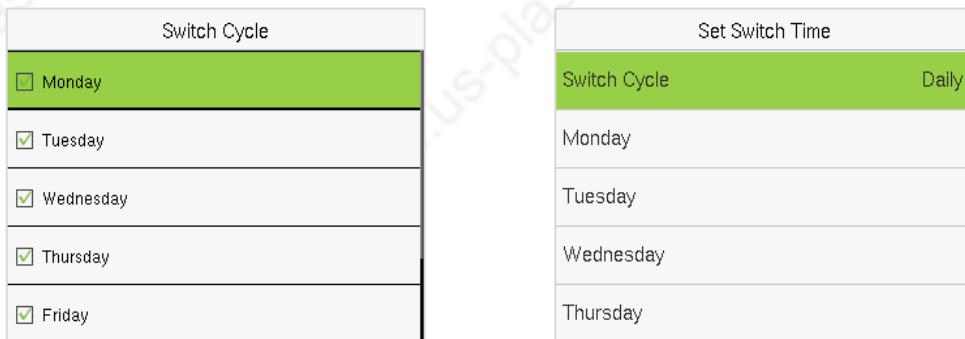
- В интерфейсе **Shortcut Key Mappings** (Назначение клавиш быстрого доступа) выберите нужную клавишу для настройки.
- В интерфейсе **Shortcut Key** (Клавиша быстрого доступа) нажмите **Function** (Функция) чтобы задать действие клавиши (состояние отметки или функциональная клавиша).
- Если клавиша назначена как функциональная (например, "Новый пользователь", "Все пользователи" и т. д.), настройка завершена (см. изображение ниже).



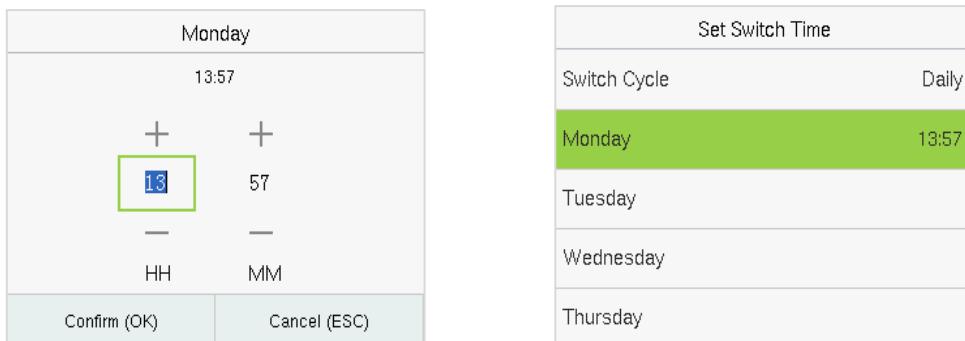
- Если клавиша назначена как состояние отметки (например, "Вход", "Выход" и т. д.), необходимо задать значение состояния отметки (допустимые значения 0–250) и название.

## ➤ Настройка времени переключения

- Время переключения настраивается в соответствии с параметрами состояния отметки.
- При установке режима **Punch State Mode** состояния отметки в автоматический (**Auto Mode**) необходимо задать время переключения.
- В интерфейсе **Shortcut Key** (Горячие клавиши) используйте опцию **Set Switch Time** (Установить время переключения) для соответствующей настройки.
- В интерфейсе **Switch Cycle** (Цикл переключения) выберите дни недели для активации (понедельник, вторник и другие), как показано на приведенном изображении.



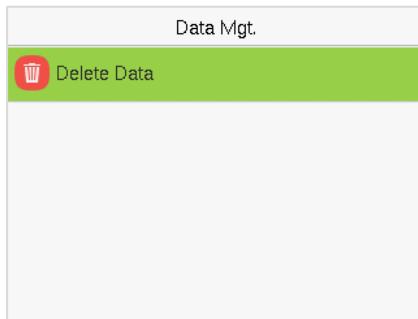
- После выбора цикла задайте время переключения для каждого дня и нажмите **М/ОК** для подтверждения (см. изображение ниже).



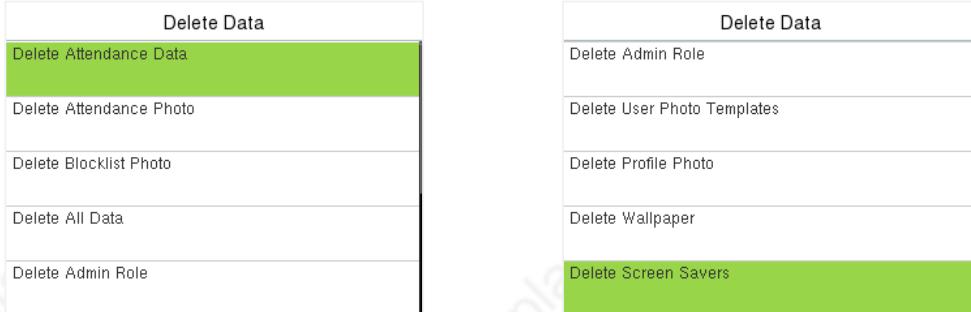
**Примечание:** Если функция установлена как "Не определена", устройство не активирует клавишу состояния отметки.

## 8 Управление данными

Когда устройство находится на начальном интерфейсе, нажмите **M/OK** и выберите **Data Mgt.** (Управление данными) для управления соответствующей информацией в устройстве

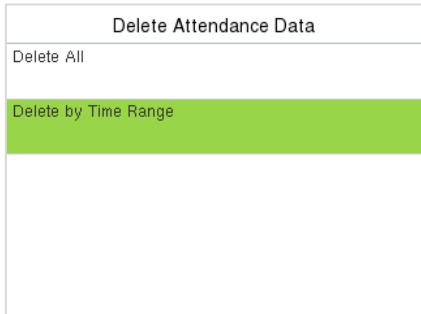


Выберите **Delete Data** (Удаление данных) в **Data Mgt.** (Управление данными) для удаления необходимых данных.

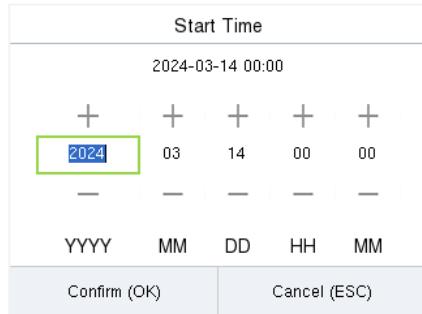


Название функции	Описание
<b>Delete Attendance Data</b> Удалить данные отметок	Удаление данных посещаемости.
<b>Delete Attendance Photo★</b> Удалить фото отметок	Удаление фотографий отметок указанных сотрудников.
<b>Delete Blocklist Photo★</b> Удалить фото из чёрного списка	Удаление фотографий, сделанных при неудачной верификации.
<b>Delete All Data</b> Удалить все данные	Удаление информации и журналов отметок всех зарегистрированных пользователей.
<b>Delete Admin Role</b> Удалить права администратора	Удаление всех административных привилегий.
<b>Delete User Photo Templates★</b> Удалить шаблоны фото пользователей	Удаление шаблонов фотографий пользователей в устройстве. При удалении появляется предупреждение: <b>"Face re-registration is required after an algorithm upgrade."</b> ("После обновления алгоритма потребуется повторная регистрация лиц.")
<b>Delete Profile Photo</b> Удалить профильные фото	Удаление всех фотографий пользователей в устройстве.
<b>Delete Wallpaper</b> Удалить обои	Удаление всех обоев в устройстве.
<b>Delete Screen Savers</b> Удалить заставки	Удаление заставок экрана в устройстве.

Пользователь может выбрать **Delete All** (Удалить всё) или **Delete by Time Range** (Удалить по временному диапазону) при удалении данных отметок, фотографий отметок★ или фотографий из чёрного списка★. При выборе **Delete by Time Range** (Удалить по временному диапазону) необходимо задать конкретный период времени для удаления всех данных за указанный срок.



Выберите **Delete by Time Range**.  
(Удалить по временному диапазону)

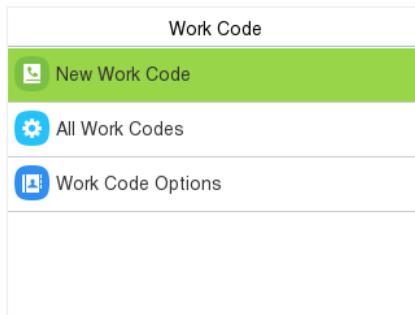


Установите временной диапазон  
и нажмите **M/OK**.

## 9 Код работы

Заработка плата сотрудников зависит от их записей посещаемости. Сотрудник может быть занят в нескольких видах работ, которые могут меняться со временем. Поскольку оплата варьируется в зависимости от типов работ, терминал FFR предоставляет параметр для указания соответствующего типа работы для каждой записи посещаемости, чтобы упростить анализ различных ситуаций при обработке данных посещаемости.

Выберите **Work Code** (Код работы) в главном меню устройства.



### 9.1 Добавление кода работы



Пункт меню	Описание
<b>ID</b>	Цифровой код работы. Пользователь может установить значение от 1 до 99999999.
<b>Name</b> Название	Наименование кода работы.

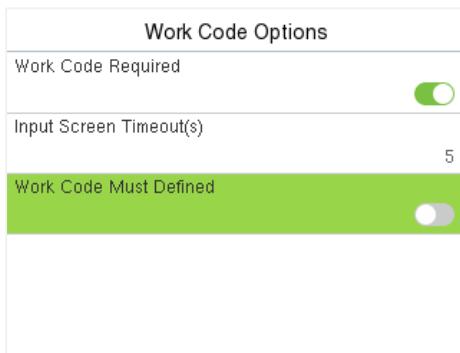
### 9.2 Все коды работы

В разделе **All Work Codes** (Все коды работы) можно просматривать, редактировать и удалять коды работ. Процесс редактирования аналогичен добавлению, за исключением того, что ID нельзя изменить.

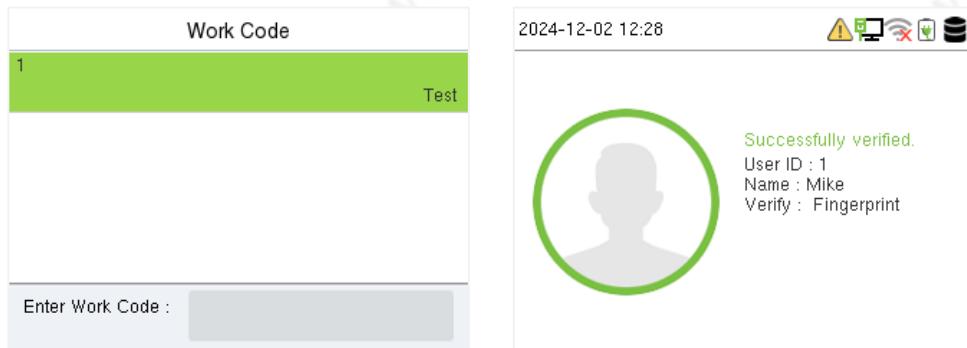


### 9.3 Настройки кода работы

Позволяет установить, является ли ввод кода работы обязательным и должен ли введенный код существовать при аутентификации.



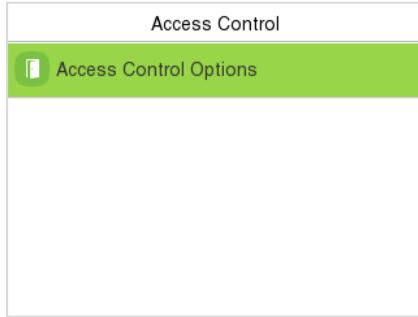
При верификации **1:N** или **1:1** система автоматически отобразит следующее окно. Для успешной верификации вручную выберите соответствующий код работы.



**Примечание:** Настройки кода работы влияют на процесс верификации и последующую обработку данных посещаемости для расчета заработной платы.

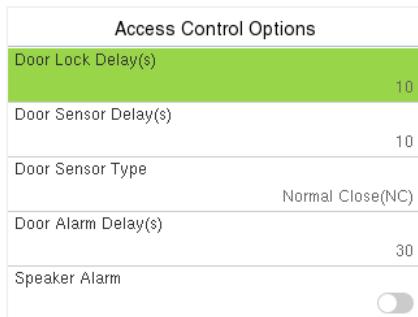
## 10 Контроль доступа

Когда устройство находится на начальном интерфейсе, нажмите **M/OK** и выберите **Access Control** (Контроль доступа) для настройки управления замками и других параметров, связанных с системой контроля доступа.



### 10.1 Настройки контроля доступа

Выберите **Access Control Options** (Настройки контроля доступа) в интерфейсе **Access Control** "Контроль доступа" для установки параметров управления замком терминала и связанного оборудования.

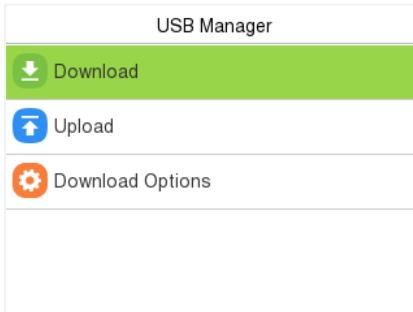


Название функции	Описание
<b>Door Lock Delay (s)</b> Задержка замка двери (с)	Время, в течение которого устройство удерживает электронный замок в открытом состоянии. Допустимые значения: 1-10 секунд; 0 означает отключение функции.
<b>Door Sensor Delay (s)</b> Задержка датчика двери (с)	Если дверь не заблокирована и остается открытой в течение заданного времени (Задержка датчика двери), срабатывает сигнализация. Допустимые значения: 1-255 секунд.
<b>Door Sensor Type</b> Тип датчика двери	Доступны три типа датчиков: <b>Нет</b> , <b>Нормально открытый (NO)</b> и <b>Нормально закрытый (NC)</b> . <b>None:</b> датчик двери не используется <b>Normally Open(NO):</b> дверь остается открытой при подаче питания <b>Normally Closed(NC):</b> дверь остается закрытой при подаче питания
<b>Door Alarm Delay(s)</b> Задержка сигнализации двери (с)	При несоответствии состояния датчика двери заданному типу датчика сигнализация срабатывает через указанное время (0-999 секунд).
<b>Speaker Alarm</b> Звуковая сигнализация	Включает звуковую сигнализацию при несанкционированном доступе. Сигнализация отключается при закрытии двери или успешной верификации.

## 11 Менеджер USB

Вы можете импортировать информацию о пользователях и данные посещаемости с устройства на компьютер через USB-накопитель для последующей обработки или выполнить резервное копирование данных на другие устройства.

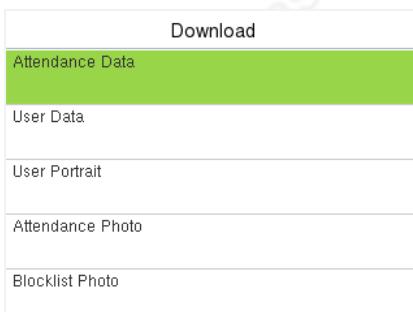
Перед загрузкой/выгрузкой данных вставьте USB-накопитель в соответствующий разъем. Выберите **USB Manager** (Менеджер USB) в главном меню.



**Примечание:** Для загрузки данных поддерживаются только USB-накопители в формате FAT32.

### 11.1 Загрузка на USB

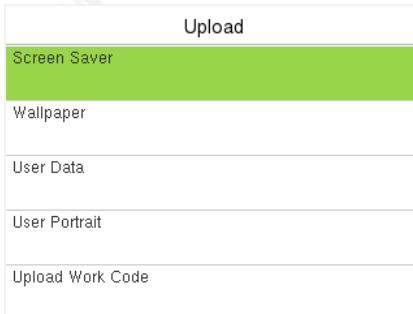
В интерфейсе **USB Manager** (Менеджер USB) выберите **Download** (Загрузить).



Название функции	Описание
<b>Attendance Data</b> Данные посещаемости	Выгрузка всех данных посещаемости за указанный период на USB-накопитель.
<b>User Data</b> Данные пользователей	Выгрузка всей информации о пользователях с устройства на USB-накопитель.
<b>User Portrait</b> Портреты пользователей	Выгрузка всех фотографий пользователей с устройства на USB-накопитель.
<b>Attendance Photo★</b> Фото отметок	Выгрузка всех фотографий, сделанных при отметке, на USB-накопитель.
<b>Blocklist Photo★</b> Фото из черного списка	Выгрузка фотографий, сделанных при неудачных попытках верификации.
<b>Work Code</b> Коды работ	Выгрузка всех кодов работ с устройства на USB-накопитель.

## 11.2 Выгрузка с USB

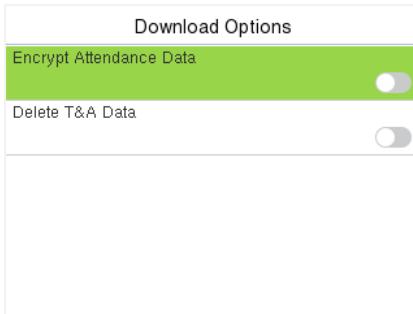
В интерфейсе **USB Manager** (Менеджер USB) выберите **Download** (Выгрузить).



Название функции	Описание
<b>Screen Saver</b> Заставки	Загрузка заставок с USB-накопителя на устройство. Можно выбрать отдельные изображения или загрузить все.
<b>Wallpaper</b> Обои	Загрузка обоев с USB-накопителя на устройство. Изображения будут отображаться на экране.
<b>User Data</b> Данные пользователей	Загрузка информации о пользователях с USB-накопителя на устройство.
<b>User Portrait</b> Портреты пользователей	Загрузка фотографий пользователей с USB-накопителя на устройство.
<b>Upload Work Code</b> Коды работ	Загрузка кодов работ с USB-накопителя на устройство.

## 11.3 Настройки загрузки

В интерфейсе **USB Manager** (Менеджер USB) выберите **Download Options** (Настройки загрузки).



Название функции	Описание
<b>Encrypt Attendance Date</b> Шифрование данных	Данные посещаемости шифруются при передаче
<b>Delete T&amp;A Data</b> Удаление данных после загрузки	Данные посещаемости автоматически удаляются с устройства после успешной выгрузки.

(★ - Функции, отмеченные звёздочкой, могут быть недоступны в некоторых моделях устройства)

## 12 Поиск отметок

После успешной верификации пользователя журнал событий сохраняется в устройстве. Данная функция позволяет просматривать записи о посещаемости.

Когда устройство находится на начальном интерфейсе, нажмите **M/OK** и выберите **Attendance Search** (Поиск отметок) для просмотра нужных записей.



Процесс поиска фотографий отметок★ и фотографий из черного списка★ аналогичен поиску в журнале событий. Ниже приведен пример поиска записей посещаемости.

В интерфейсе **Attendance Search** (Поиск отметок) выберите **Attendance Record** (Записи посещаемости)

User ID	
Right key to switch input method, Left key to back space	
Confirm (OK)	Cancel (ESC)

Time Range	
<input checked="" type="radio"/> Today	
<input type="radio"/> Yesterday	
<input type="radio"/> This Week	
<input type="radio"/> Last Week	
<input type="radio"/> This Month	

1. Введите **ID пользователя** для поиска и нажмите **M/OK**. Для поиска всех записей оставьте поле пустым.

2. Выберите временной диапазон для поиска.

Personal Record Search		
Date	User ID	Time
07-31		Number of Rec...:1
	1	15:19

Prev : Left Key Next : Right Key Details : OK

Personal Record Search		
User ID	Time	
1	07-31 15:19	

Name :  
Punch State : 255  
Verification Mode : Face

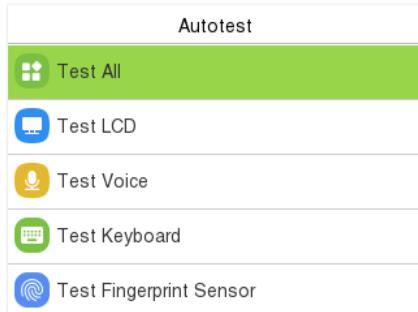
3. После завершения поиска выделенные зеленым записи можно просмотреть детально.

4. На экране отобразятся подробные данные выбранной записи.

## 13 Автотест

Когда устройство находится на начальном интерфейсе, нажмите **M/OK** и выберите **Autotest** (Автотест) для автоматической проверки работоспособности модулей:

LCD-экрана, звука, клавиатуры, сканера отпечатков, камеры★ и часов реального времени (RTC).

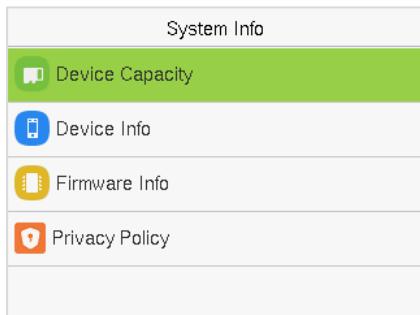


Название функции	Описание
<b>Test All</b> Тест всех модулей	Комплексная проверка LCD, звука, камеры и RTC.
<b>Test LCD</b> Тест LCD	Проверка качества отображения цветов (полноцветные, белые и черные экраны).
<b>Test Voice</b> Тест звука	Проверка целостности аудиофайлов и качества воспроизведения.
<b>Test Keyboard</b> Тест клавиатуры	Функция проверяет работоспособность всех клавиш. В интерфейсе <b>Test Keyboard</b> (Тест клавиатуры) нажмите любую клавишу для сверки соответствия между нажатой клавишей и отображаемым на экране символом. Нажатые клавиши подсвечиваются зеленым. Для выхода нажмите <b>ESC</b> .
<b>Test Fingerprint Sensor</b> Тест сканера отпечатков	Для проверки работы сканера приложите палец к сенсору. Система отобразит полученное изображение отпечатка на экране, позволяя оценить его четкость и качество распознавания.
<b>Cam Test★</b> Тест камеры	Проверка четкости фотографий, сделанных камерой (аналогично "Тесту лица").
<b>Test Clock RTC</b> Тест часов (RTC)	Проверка точности хода часов с использованием секундомера. Нажмите <b>M/OK</b> для запуска/остановки.

(★ - Функции, отмеченные звёздочкой, могут быть недоступны в некоторых моделях устройства)

## 14 Системная информация

Когда устройство находится на начальном интерфейсе, нажмите **M/OK** и выберите **System Info** (Системная информация) для просмотра состояния памяти, информации о версиях устройства, данных прошивки и политики конфиденциальности.



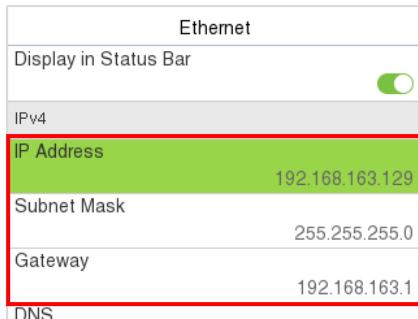
Название функции	Описание
<b>Device Capacity</b> Емкость устройства	Отображает текущее использование памяти: данные пользователей, пароли, шаблоны лиц★, отпечатков и карт, записи посещаемости, фотографии отметок и черного списка★, профильные фото.
<b>Device Info</b> Информация об устройстве	Отображает: название устройства, серийный номер, MAC-адрес, алгоритмы обработки отпечатков и шаблонов лиц★, информацию о платформе, версии MCU, BAT MCU и производителе.
<b>Firmware Info</b> Информация о прошивке	Отображает версию прошивки и другую информацию о версиях компонентов.
<b>Privacy Policy</b> Политика конфиденциальности	Политика отображается при первом включении устройства. После подтверждения ознакомления « <b>I have read it</b> » (Я прочитал) доступны все функции. Просмотреть политику можно в разделе <b>System Info</b> (Системная информация) > <b>Privacy Policy</b> (Политика конфиденциальности). Экспорт текста политики на USB-носитель невозможен.  <b>Примечание:</b> Текст текущей политики конфиденциальности доступен только на китайском (упрощенное письмо) и английском языках. Перевод на другие языки находится в процессе разработки и будет дополняться в следующих версиях.

## 15 Подключение к ПО ZKBio Time

### 15.1 Добавление устройства в программу

1. В главном меню выберите **COMM. > Ethernet** для настройки IP-адреса и шлюза устройства.

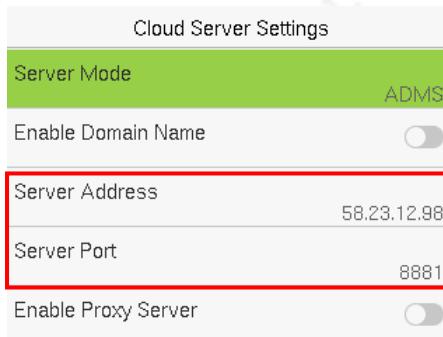
**Примечание:** Настроенный IP-адрес должен обеспечивать соединение с сервером времени ZKBio.



2. В главном меню выберите **COMM. > Cloud Server Settings** (Настройки облачного сервера) для указания адреса сервера и порта подключения.

**Server Address** (Адрес сервера): Укажите IP-адрес сервера ZKBio Time

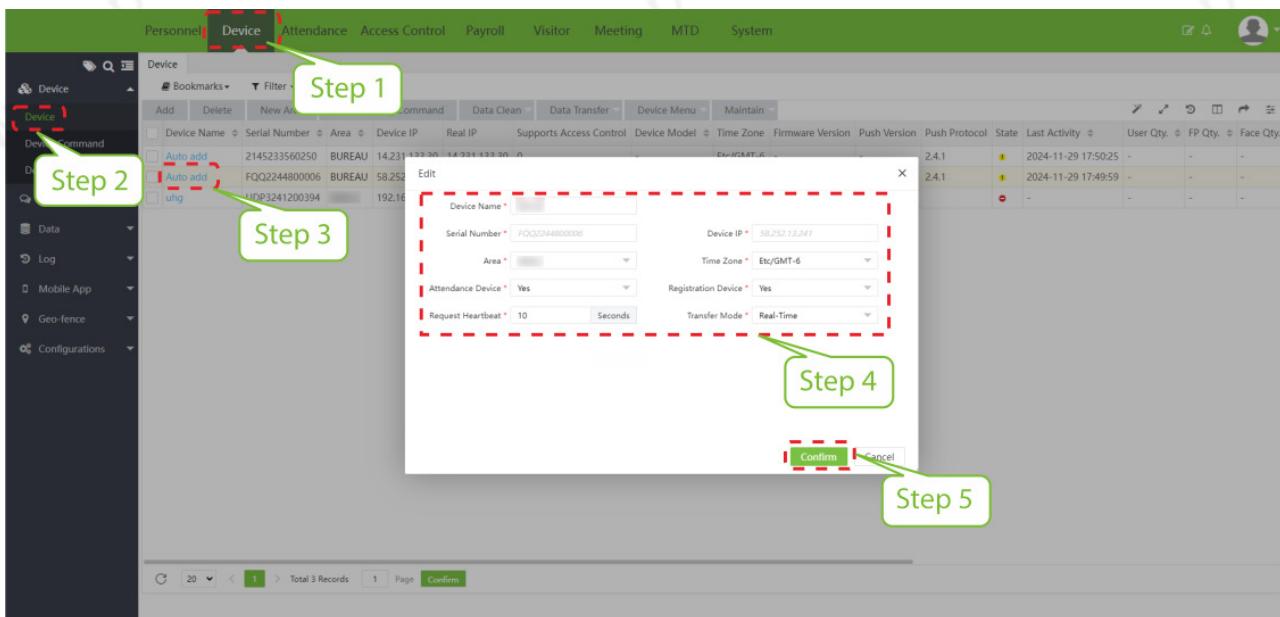
**Server Port** (Порт сервера): Укажите порт сервера ZKBio Time



3. После настройки устройство автоматически появится в ПО ZKBio Time. Для завершения подключения:

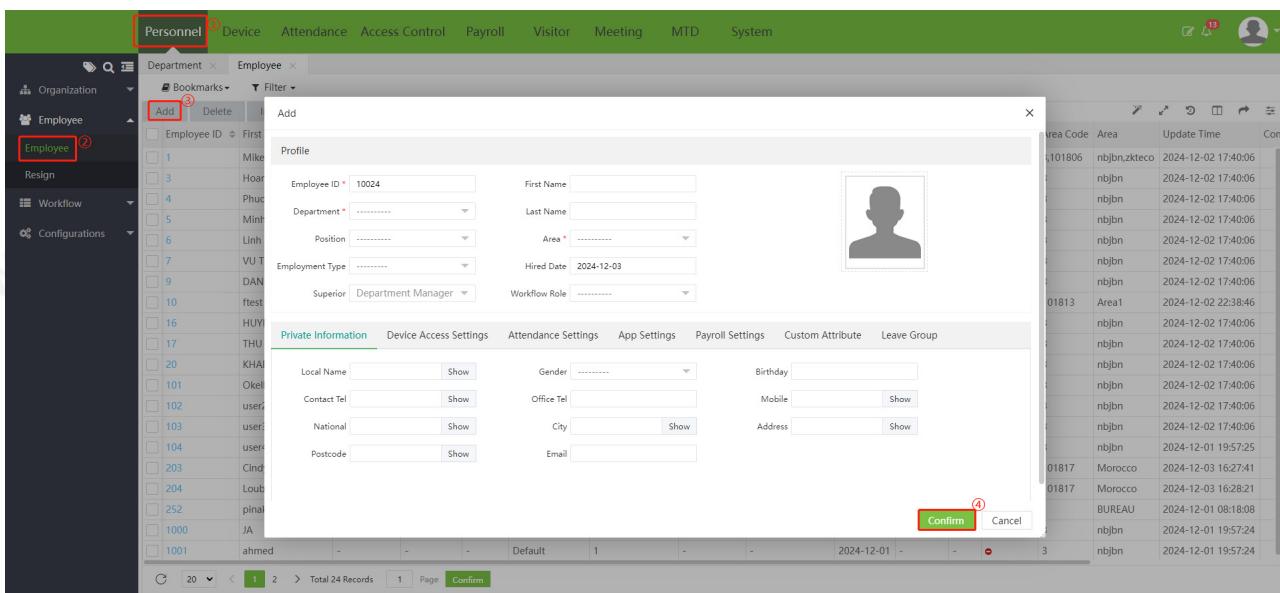
В ZKBio Time перейдите **Device** (Устройство) > **Device > Device**, выберите нужное устройство из списка, затем измените значения полей **Device Name** (Название устройства) и **Area** (Зона).

**Важно!** Автоматически добавленные устройства требуют ручного назначения зоны для работы с ПО.

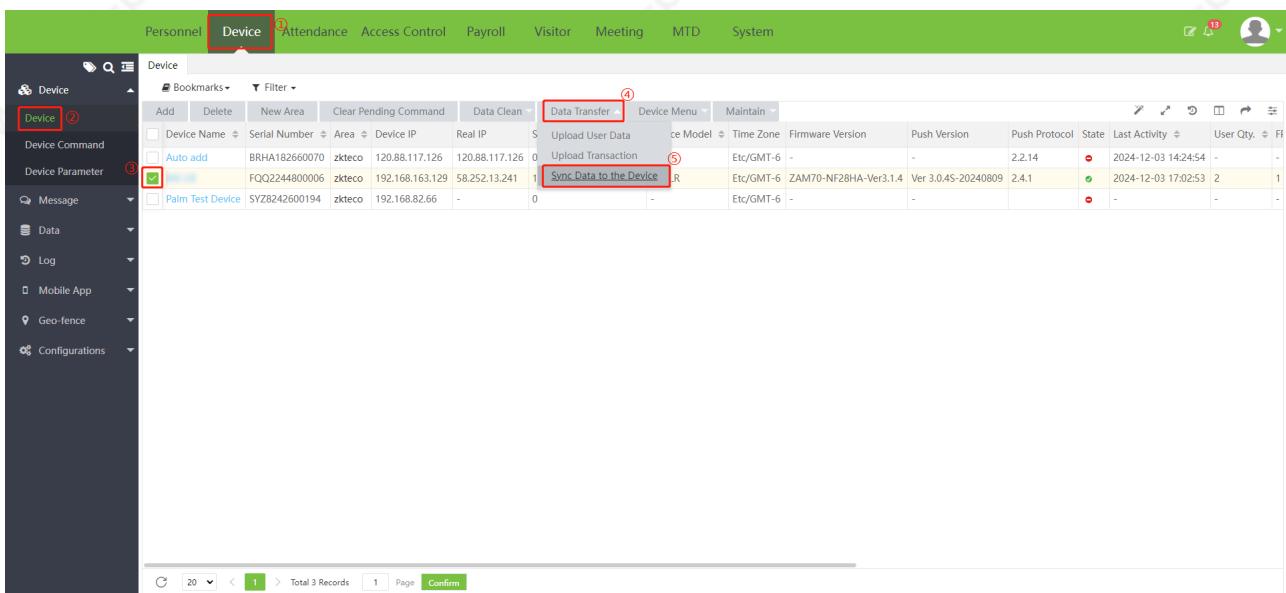


## 15.2 Добавление сотрудников в программу

1. Перейдите **Personnel** (Персонал) > **Employee** (Сотрудники) > **Employee** > **Add** (Добавить):



2. Заполните все обязательные поля и нажмите **Confirm** (Подтвердить) для завершения регистрации нового пользователя.
3. В меню программы выберите **Device** (Устройство) > **Device** > **Device**, выделите нужное устройство в списке, затем перейдите **Data Transfer** (Передача данных) > **Sync Data to the Device** (Синхронизировать данные с устройством) для загрузки всех данных, включая новых пользователей.



The screenshot shows the 'Device' tab selected in the top navigation bar. The main content area is titled 'Data Transfer' and contains a table with three rows of device data. The third row, for the device 'SVZ8242500194', has a 'Sync Data to the Device' button highlighted with a red box and a circled '5'. The table includes columns for Device Name, Serial Number, Area, Device IP, Real IP, Upload User Data, Device Model, Time Zone, Firmware Version, Push Version, Push Protocol, State, Last Activity, and User Qty. The bottom of the screen shows a navigation bar with a 'Confirm' button.

Device Name	Serial Number	Area	Device IP	Real IP	Upload User Data	Device Model	Time Zone	Firmware Version	Push Version	Push Protocol	State	Last Activity	User Qty.
BRHA182660070	zkteco	120.88.117.126	120.88.117.126	0	Upload Transaction	Etc/GMT-6	-	2.2.14	2024-12-03 14:24:54	-	-	-	-
FOQQ224800006	zkteco	192.168.163.129	58.252.13.241	1	Sync Data to the Device	Etc/GMT-6	ZAM70-NF28HA-Ver3.1.4	Ver 3.0.45-20240809	2.4.1	2024-12-03 17:02:53	2	1	-
Palm Test Device	SVZ8242500194	zkteco	192.168.82.66	-	0	Etc/GMT-6	-	-	-	-	-	-	-

## 16 Подключение к приложению ZKBio Zlink

Внешний вид интерфейса приложения может отличаться в зависимости от версии, и данная документация предназначена только для справочных целей. Для управления устройством через ZKBio Zlink необходимо изменить протокол связи устройства на BEST protocol. Подробные инструкции по настройке см. в разделе 6.5 Настройка типа устройства.

### ● Скачивание приложения ZKBio Zlink

Найдите приложение "ZKBio Zlink" в App Store (для iOS) или Google Play (для Android).

Альтернативно, отсканируйте QR-код ниже для прямой загрузки приложения.



Apple App Store

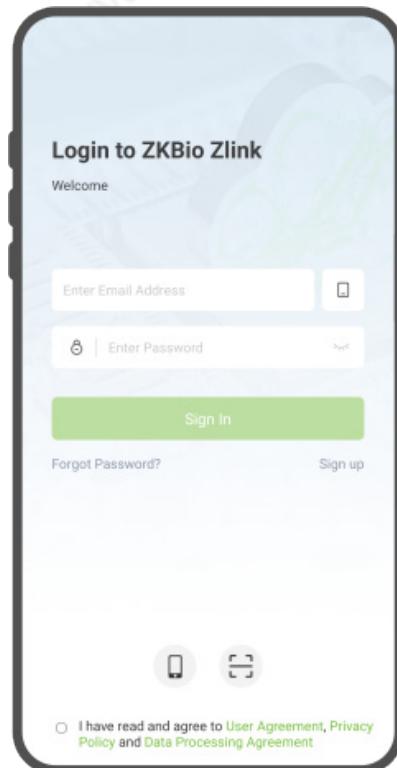


Google Play Store



### 16.1 Вход в приложение

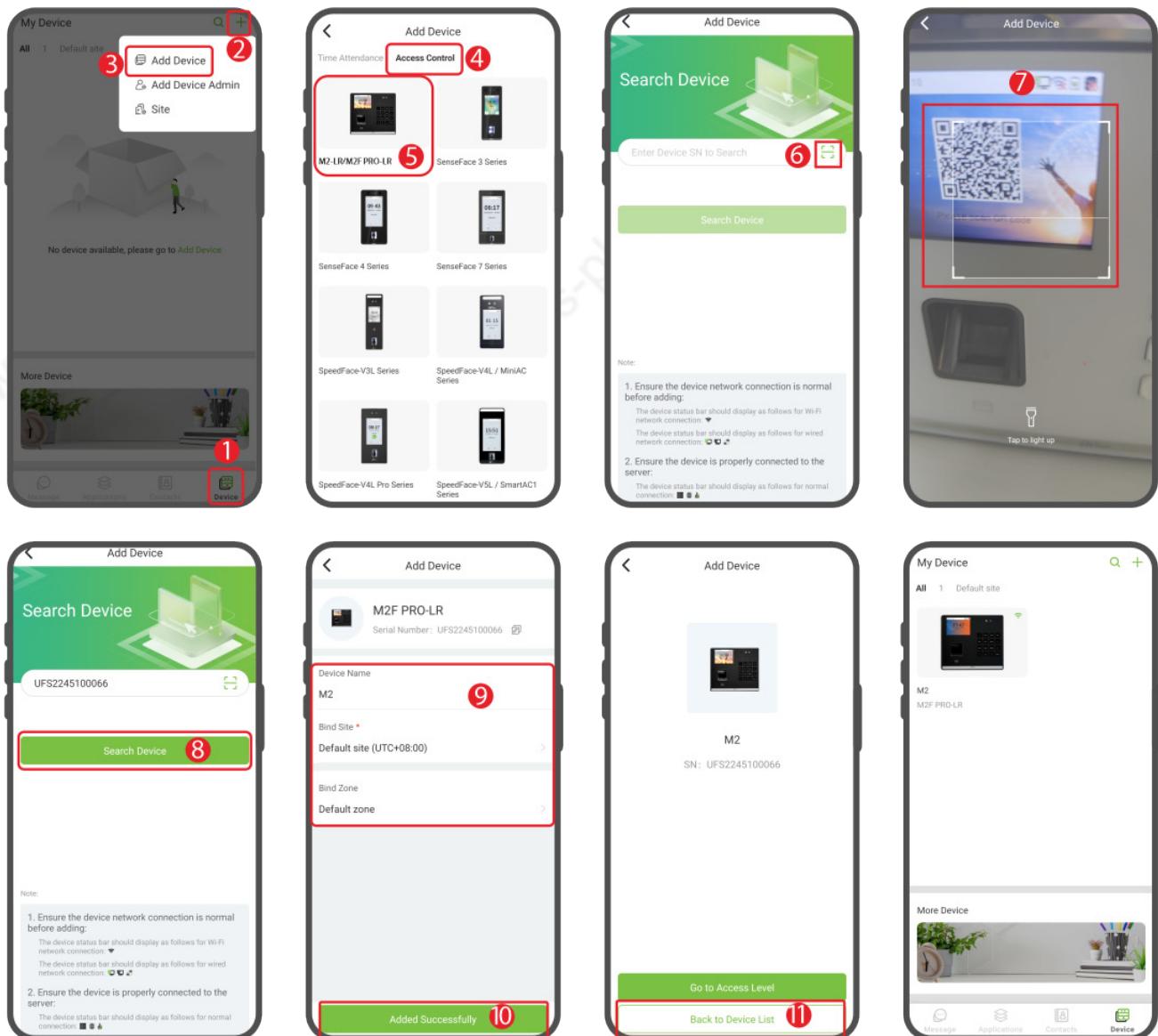
Введите ваш зарегистрированный аккаунт и пароль, поставьте галочку напротив пункта "**I have read and agree to User Agreement, Privacy Policy and Data Processing Agreement**" (Я прочитал и согласен с Пользовательским соглашением, Политикой конфиденциальности и Соглашением об обработке данных), затем нажмите "**Sign In**" (Войти) для доступа к приложению.



**Примечание:** Для получения информации о дополнительных функциях обратитесь к руководству пользователя приложения ZKBio Zlink.

## 16.2 Добавление устройства в приложении

- Откройте приложение ZKBio Zlink. Нажмите [Device] (Устройства) > + icon > [Add Device] (Добавить устройство) > [Access Control] (Контроль доступа) > [M2-LR/M2F PRO-LR]. (1,2,3,4,5)
- Нажмите  чтобы отсканировать QR-код. Серийный номер устройства автоматически отобразится в строке ввода. Нажмите [Search Device] (Найти устройство) для завершения процесса привязки.
- Введите название устройства, укажите площадку и зону его размещения, затем нажмите [Added Successfully] (Успешно добавлено) для завершения процедуры. Устройство подаст голосовое оповещение “Device is added successfully” (Устройство успешно добавлено), подтверждающее завершение процесса (9,10,11)
- Успешно добавленное устройство отобразится в списке интерфейса управления устройствами.



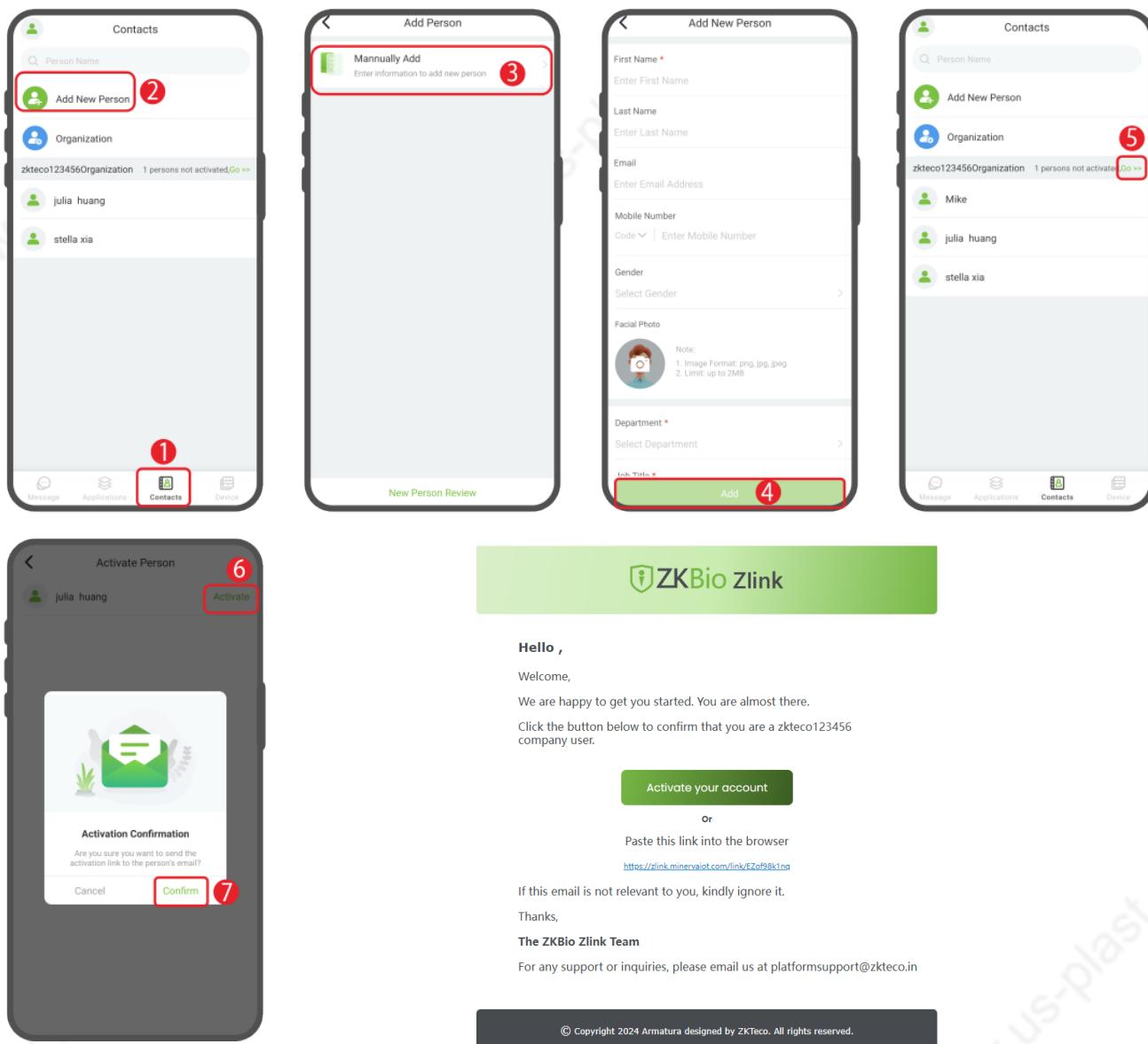
## 16.3 Добавление пользователя

### Создание новой учетной записи пользователя

- В главном меню выберите **[Contacts]** (Контакты) > **[Add New Person]** (Добавить пользователя) для перехода в интерфейс создания профиля. (1,2,3)
- Заполните обязательные поля: идентификатор пользователя, имя, контактные данные. Укажите действительный номер телефона или email для отправки ссылки активации. После заполнения нажмите **[Add]** (Добавить) для сохранения профиля. (4)
- Система подтвердит успешное добавление, и новый пользователь отобразится в списке персонала.

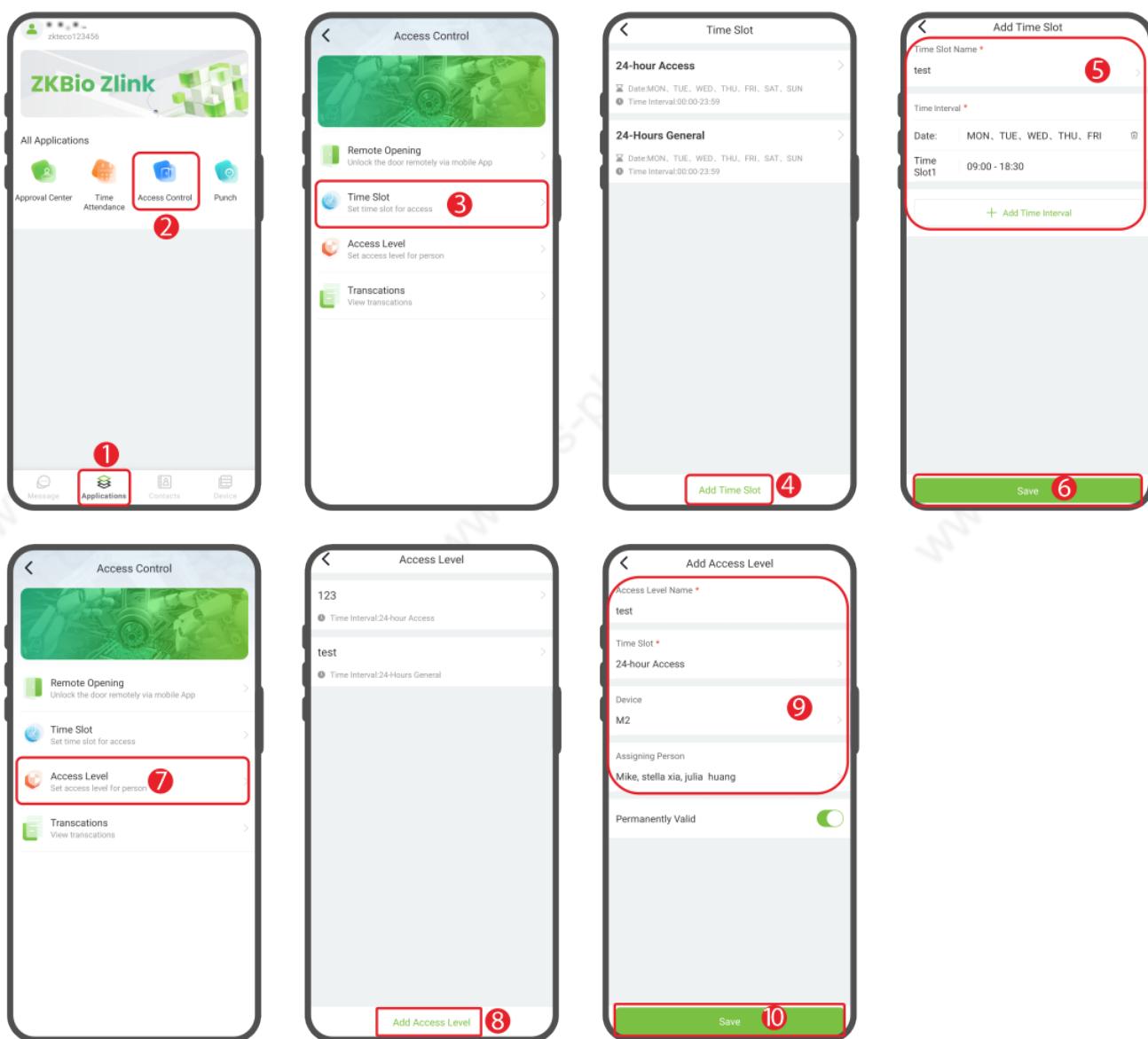
### Активация новой учетной записи пользователя

- Найдите добавленного пользователя в списке персонала, нажмите кнопку **[Go >>]** (Далее) затем выберите **[Activate]** (Активировать) для отправки ссылки активации учетной записи. (5,6,7)
- Выбранный пользователь получит электронное письмо с инструкциями по активации, которую необходимо завершить до начала работы с системой.



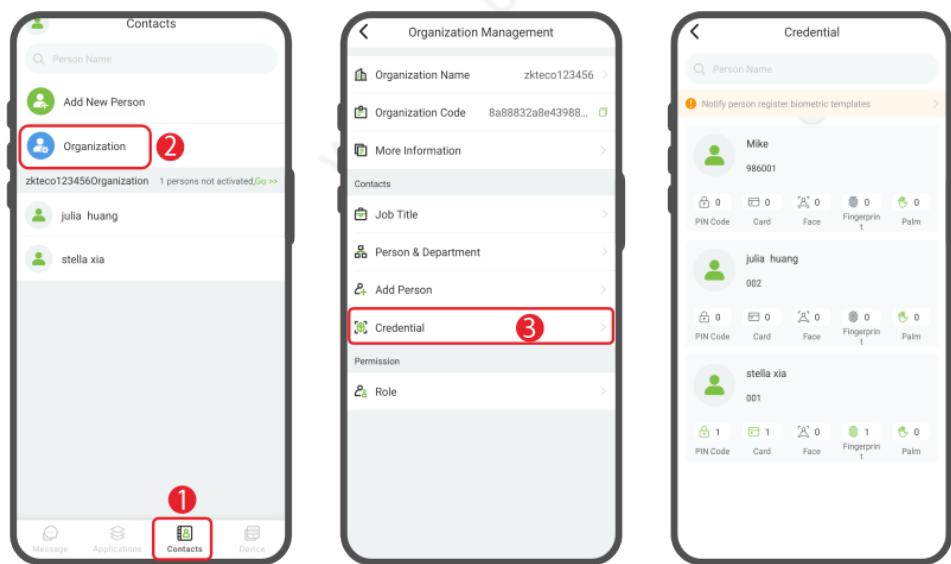
## 16.4 Настройка уровней доступа

- Выберите [Applications] (Приложения) > [Access Control] (Контроль доступа) > [Time Slot] (Временные интервалы) > [Add Time Slot] (Добавить интервал) для создания нового временного интервала. (1,2,3,4)
  - Укажите название и задайте временные границы, затем нажмите [Save] (Сохранить). Созданный интервал отобразится в списке. (5,6)
- Примечание:** В системе предустановлен интервал **24-hour Access** (Круглосуточный доступ).
- Для добавления уровня доступа нажмите [Access Level] (Уровень доступа) > [Add Access Level] (Добавить уровень) (7,8)
  - Заполните название, выберите временной интервал, устройство и пользователей, затем сохраните изменения для синхронизации уровня доступа с устройством. (9,10)



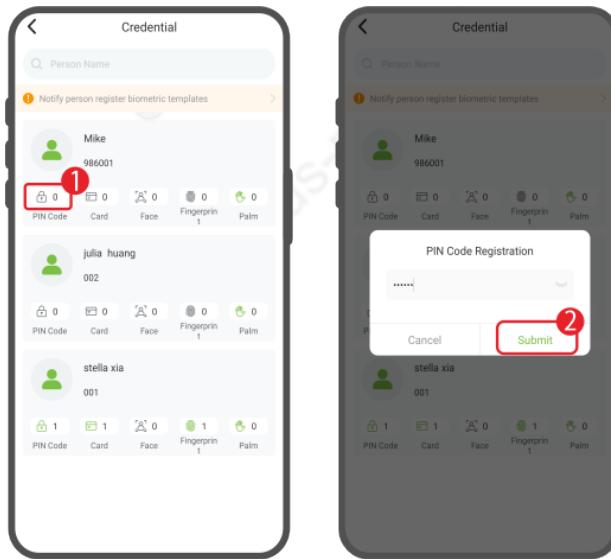
## 16.5 Регистрация режима верификации в приложении

После добавления пользователей на устройство можно зарегистрировать для них методы верификации. **Примечание:** Доступные методы зависят от функциональных возможностей устройства. Для настройки перейдите [Contacts] (Контакты) > [Organization] (Организация) > [Credential] (Учетные данные). (1,2,3)



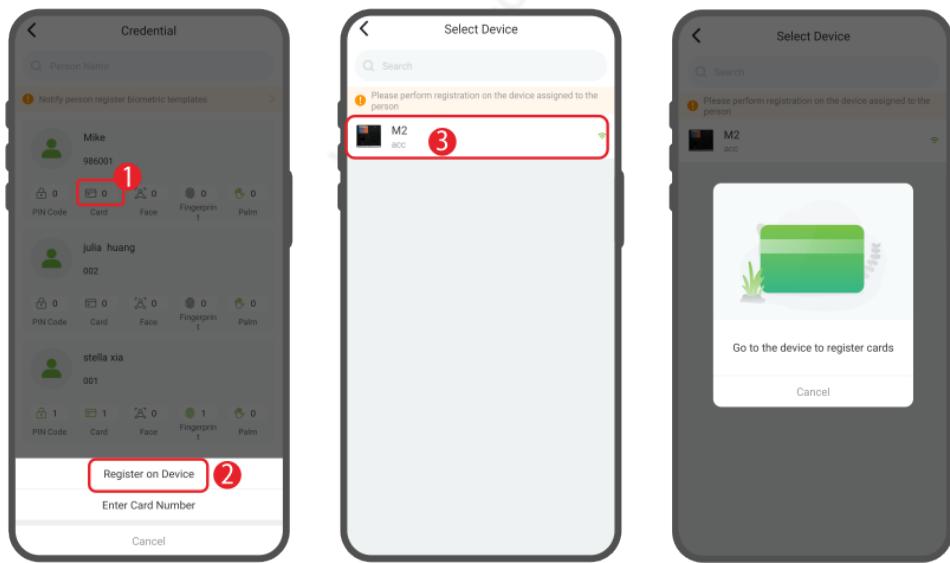
## Регистрация пароля

В интерфейсе Credential interface (Учетные данные), нажмите иконку добавить пароль, введите пароль во всплывающем окне и подтвердите действие кнопкой **[Submit]** (Отправить). (1,2)



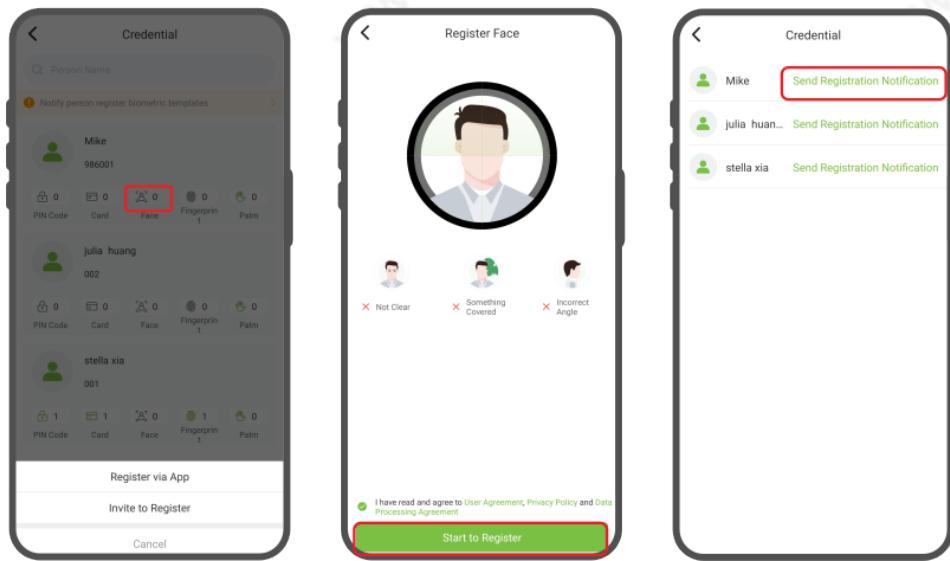
## Регистрация карты доступа

- В интерфейсе Credential interface (Учетные данные), нажмите иконку и выберите один из вариантов: Регистрация на устройстве или Ручной ввод номера карты (**Register on Device**). (1,2)
- Выберите устройство для регистрации – на его экране автоматически отобразится интерфейс **Enroll Card Number** (Добавление карты). Поместите карту в зону считывания, и после появления сообщения **“Card registered successfully”** (Карта успешно зарегистрирована) процесс будет завершен. (3)



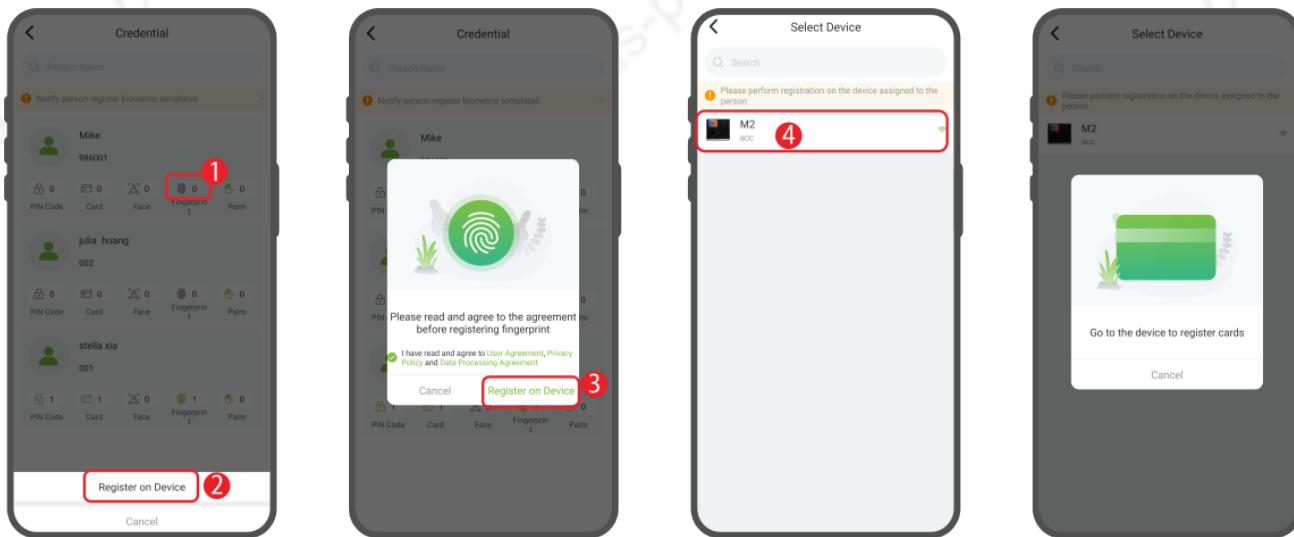
## Регистрация лица\*

- В интерфейсе **Credential interface** (Учетные данные), нажмите иконку  , затем выберите один из вариантов: Регистрация через приложение или Приглашение к регистрации. Для самостоятельной регистрации выберите **Register via App** (Регистрация через приложение) > **Start to Register** (Начать регистрацию) и выполните сканирование..
- Альтернативно, используйте **Invite to Register** (Приглашение к регистрации) > **Send Registration Notification** (Отправить уведомление) чтобы отправить пользователю инструкции для самостоятельной регистрации. (**Примечание:** Учетная запись пользователя должна быть предварительно активирована..)



## Регистрация отпечатка пальца

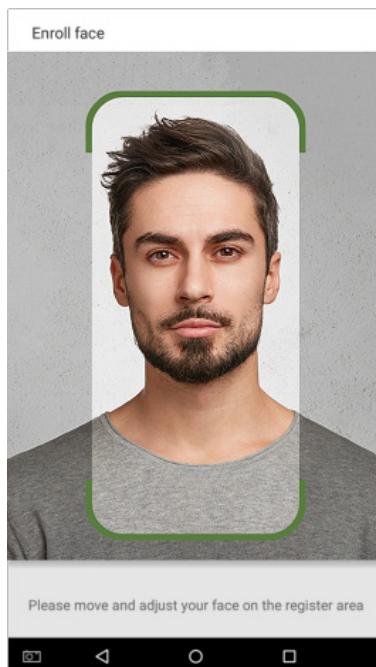
- В интерфейсе **Credential interface** (Учетные данные), нажмите иконку  , затем последовательно выберите: **Register on Device** (Регистрация на устройстве) > **Register on Device** (Зарегистрировать на устройстве). (1,2,3)
- Выберите устройство для регистрации – на его экране автоматически отобразится интерфейс "Регистрация отпечатка". Следуя инструкциям на экране, приложите палец к сканеру и повторите нажатие 3 раза. При появлении сообщения "**Enrolled successfully**" (Отпечаток успешно зарегистрирован), процесс будет завершен. (4)



## Приложение 1

### Требования к живой регистрации и шаблонам лиц★ в видимом свете

- 1) Рекомендуется проводить регистрацию в помещении с равномерным освещением, избегая затемненных или пересвеченных участков.
- 2) Не направляйте устройство на источники естественного света (окна/двери) или яркие искусственные источники.
- 3) Рекомендуется темная одежда, контрастирующая с фоном.
- 4) Лицо и лоб должны быть полностью открыты ( волосы не должны закрывать брови/лицо).
- 5) Сохраняйте нейтральное выражение лица (допустима легкая улыбка, но без закрытых глаз или наклона головы).
- 6) Для пользователей в очках требуется два шаблона: с очками и без.
- 7) Запрещены аксессуары, закрывающие лицо (шарфы, маски и пр.).
- 8) Располагайтесь строго напротив камеры, удерживая лицо в зоне захвата (см. пример ниже).
- 9) В зоне захвата должно находиться только одно лицо.
- 10) Оптимальное расстояние - 50-80 см (регулируется в зависимости от роста).



## Требования к цифровому шаблону лица в видимом спектре★

Цифровая фотография должна иметь четкие ровные края, быть цветной и сделанной в погрудном варианте (по плечи), на ней должен быть изображен только один человек без каких-либо графических пометок или водяных знаков, в повседневной одежде. Пользователи, которые носят очки, должны быть сфотографированы в них.

### ➤ **Рекомендации по расстоянию между глазами**

Оптимальное расстояние между глазами на изображении должно составлять 200 пикселей или более, минимально допустимое значение – не менее 115 пикселей.

### ➤ **Требования к мимике лица**

Рекомендуется нейтральное выражение лица или легкая улыбка с естественно открытыми глазами.

### ➤ **Требования к положению головы**

Горизонтальный угол поворота не должен превышать  $\pm 10^\circ$ , угол наклона вверх (элевация) и угол наклона вниз (депрессия) также должны находиться в пределах  $\pm 10^\circ$ .

### ➤ **Требования к аксессуарам**

Не допускается использование масок или цветных очков. Оправа очков не должна закрывать глаза и создавать блики. Для пользователей с массивной оправой рекомендуется зарегистрировать два шаблона: с очками и без них.

### ➤ **Требования к шаблону лица**

Шаблон должен содержать полное изображение лица с четкими контурами, реалистичными пропорциями, равномерным освещением без теней и бликов.

### ➤ **Требования к формату шаблона**

Допустимые форматы файлов: BMP, JPG или JPEG.

### ➤ **Требования к данным**

Данные должны соответствовать следующим условиям:

- 1) Белый фон и темная одежда.
  - 2) Режим 24-битного истинного цвета
  - 3) Шаблон в формате JPG сжатый до размера не более 20 КБ.
  - 4) Разрешение от 358×441 до 1080×1920 пикселей.
  - 5) Вертикальное соотношение головы и тела 2:1.
  - 6) Плечи должны быть видны и находиться на одном уровне.
  - 7) Глаза открыты с четко видимой радужной оболочкой.
  - 8) Нейтральное выражение лица или легкая улыбка (без показа зубов).
  - 9) Четкое изображение с естественными цветами, без резких теней, бликов или отражений.
- Контрастность и яркость должны быть сбалансированы.

