

# Руководство пользователя

## Биометрический терминал доступа MA300

Дата: Март 2023

Версия документа: 3.1

Благодарим за выбор нашей продукции. Перед эксплуатацией внимательно ознакомьтесь с инструкцией. Следуйте указанным рекомендациям для обеспечения надлежащей работы изделия. Изображения в данном руководстве приведены исключительно в иллюстративных целях.

## СОДЕРЖАНИЕ

### 1 ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ..... 3

1.1	РАСПОЛОЖЕНИЕ ПАЛЬЦА НА СКАНЕРЕ.....	3
1.2	ИНСТРУКЦИЯ ПО ПРИКЛАДЫВАНИЮ КАРТЫ .....	4
1.3	МЕРЫ ПРЕДОСТОРОЖНОСТИ .....	4

### 2 ОПИСАНИЕ УСТРОЙСТВА КОНТРОЛЯ ДОСТУПА..... 5

2.1	ОБЗОР ФУНКЦИЙ УСТРОЙСТВА .....	5
2.2	ВНЕШНИЙ ВИД .....	6
2.3	РЕЖИМ ВЕРИФИКАЦИИ .....	8
2.4	КАРТА АДМИНИСТРАТОРА .....	9
2.5	ТАЙМАУТ ОПЕРАЦИИ .....	10

### 3 ОПЕРАЦИИ С УСТРОЙСТВОМ ..... 11

3.1	КАРТА АДМИНИСТРАТОРА.....	11
3.1.1	РЕГИСТРАЦИЯ КАРТЫ АДМИНИСТРАТОРА .....	11
3.1.2	РЕГИСТРАЦИЯ ОБЫЧНОГО ПОЛЬЗОВАТЕЛЯ .....	12
3.1.3	УДАЛЕНИЕ ОДНОГО ПОЛЬЗОВАТЕЛЯ. ....	18
3.2	ВЕРИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ.....	21
3.3	U-ДИСК (U-DISK) .....	23
3.4	ДАТЧИК ВСКРЫТИЯ КОРПУСА.....	24

### 4 ВЕБ-СЕРВЕР УСТРОЙСТВА..... 26

4.1	АВТОРИЗАЦИЯ .....	26
4.2	УСТРОЙСТВО .....	28
4.2.1	СОСТОЯНИЕ УСТРОЙСТВА .....	28
4.2.2	СМЕНА ПАРОЛЯ.....	28
4.3	НАСТРОЙКИ .....	29
4.3.1	ПАРАМЕТРЫ СВЯЗИ .....	29
4.3.2	НАСТРОЙКА ОБЛАКА .....	30

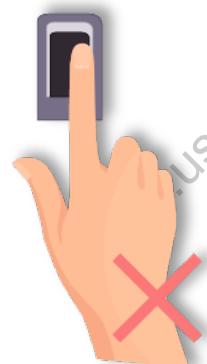
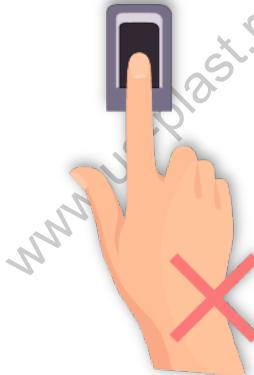
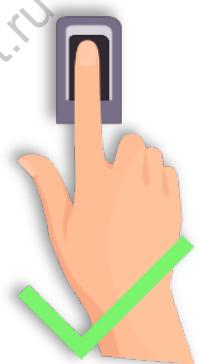
4.3.3	СИСТЕМНЫЕ НАСТРОЙКИ.....	31
4.3.4	УПРАВЛЕНИЕ ДАННЫМИ.....	31
4.3.5	ДАТА И ВРЕМЯ.....	32
4.3.6	ЖУРНАЛ ОПЕРАЦИЙ.....	32
4.3.7	НАСТРОЙКА WIEGAND.....	33
4.4	УПРАВЛЕНИЕ УСТРОЙСТВОМ.....	36
4.4.1	ОБНОВЛЕНИЕ И СБРОС .....	36
4.4.2	ЗАГРУЗКА СЕРТИФИКАТА.....	37
<b>5 ПОДКЛЮЧЕНИЕ К ПО ZKBIO CVACCESS.....</b>		<b>38</b>
5.1	ЗАДАТЬ АДРЕС СВЯЗИ.....	38
5.2	ДОБАВЛЕНИЕ УСТРОЙСТВА В ПРОГРАММУ .....	39
5.3	ДОБАВЛЕНИЕ ЛЮДЕЙ В ПРОГРАММУ.....	40
<b>6 ХАРАКТЕРИСТИКИ.....</b>		<b>42</b>

## 1 Инструкция по эксплуатации

Прежде чем приступить к изучению функций устройства, рекомендуется ознакомиться со следующими основными принципами.

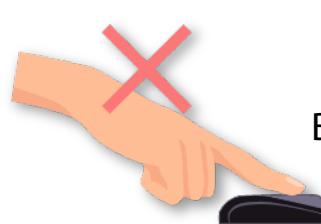
### 1.1 Расположение пальца на сканере

**Рекомендуемые пальцы:** для сканирования рекомендуется использовать указательный, средний или безымянный палец. Следует избегать использования большого пальца или мизинца, так как их сложно правильно расположить на сканере отпечатков.



Слишком низко

Слишком близко к краю



Вертикально

**Примечание:** При регистрации и идентификации отпечатков пальцев необходимо правильно прикладывать палец к сканеру. Наша компания не несет ответственности за проблемы с распознаванием, вызванные нарушением правил эксплуатации. За компанией сохраняется право окончательного толкования и внесения изменений в данное положение.

## 1.2 Инструкция по прикладыванию карты

Данное устройство интегрировано с бесконтактным модулем считывателя RF-карт и поддерживает карты ID, а также карты IC / HID (опционально). Предлагая несколько режимов верификации, таких как верификация по отпечатку пальца и по RF-карте, устройство удовлетворяет разнообразные потребности пользователей.

Проведите картой по области считывания в соответствии с голосовым указанием и уберите карту после того, как устройство ее считает. Область для проведения картой см. в разделе **2.2 Product Appearance (Внешний вид изделия)**.

## 1.3 Меры предосторожности

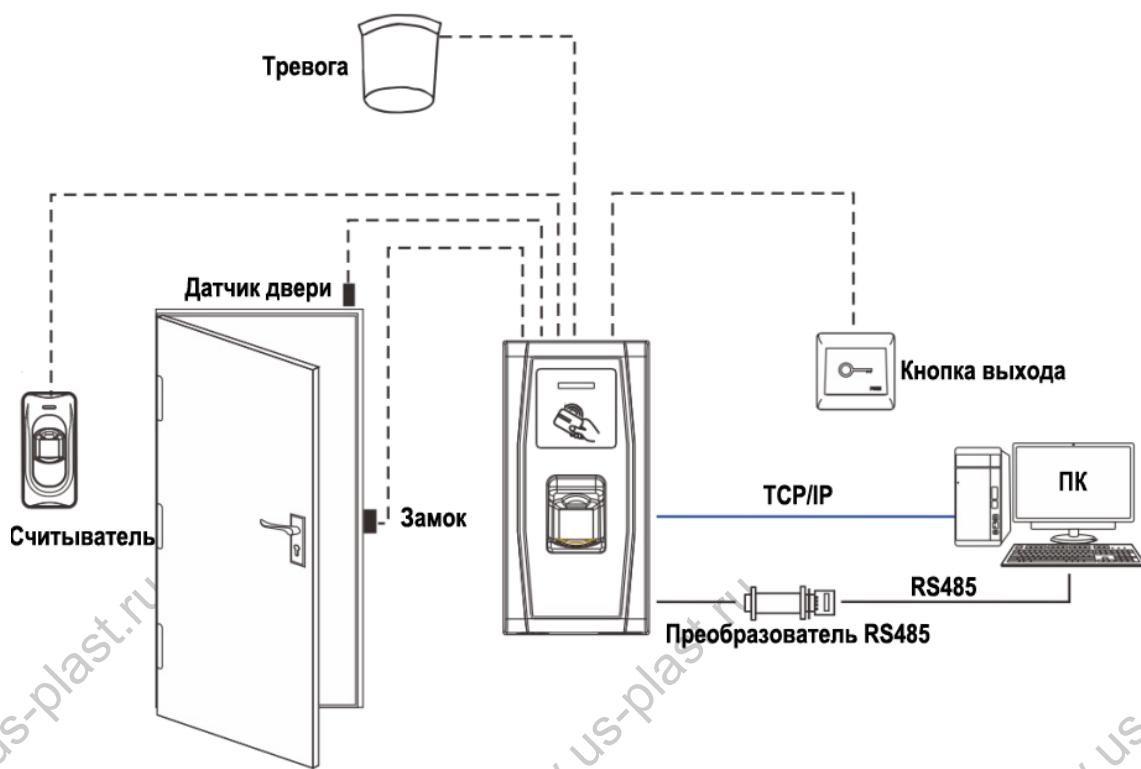
Необходимо защищать устройство от воздействия прямых солнечных лучей или сильного светового пучка, поскольку он значительно влияет на качество сканирования отпечатка пальца и приводит к сбою верификации. Для достижения наилучших результатов используйте устройство при температуре окружающей среды **от 0°C до 50°C**. Если устройство будет длительное время находиться на открытом воздухе, рекомендуется установить солнцезащитный козырек и системы охлаждения, поскольку экстремально высокие или низкие температуры снижают производительность устройства и приводят к высокому коэффициенту ложного отказа (FRR) и ложного доступа (FAR).

При установке устройства контроля доступа необходимо подключать кабель питания **после** подключения всех остальных кабелей. Если устройство работает некорректно, обязательно отключите питание перед проведением необходимой проверки. Обратите внимание, что любые работы под напряжением могут привести к повреждению устройства, и такой ущерб не покрывается стандартной гарантией.

## 2 Описание устройства контроля доступа

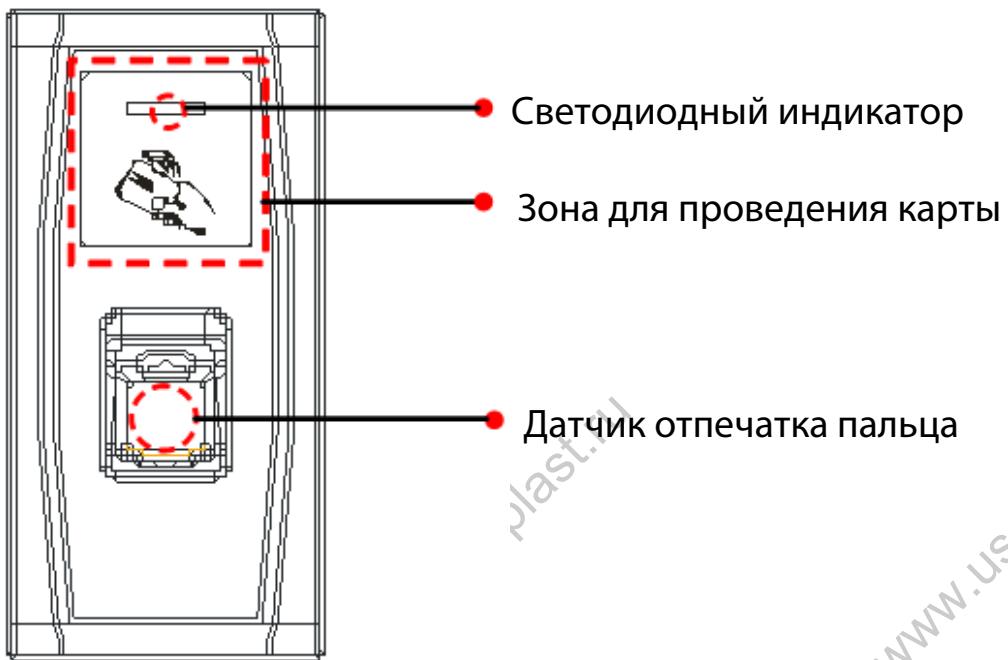
### 2.1 Обзор функций устройства

Устройство может использоваться совместно с электрозамком или контроллером доступа в качестве комбинированного устройства для считывания отпечатков пальцев и контроля доступа. Устройство поддерживает использование карт администратора и обладает простым и гибким управлением. С помощью карты администратора можно выполнять такие задачи, как автономная регистрация, регистрация пользователей и управление через U-disk. Благодаря голосовым подсказкам, которые проводят пользователя через все операции, устройству не требуется экран и клавиатура. Оно поддерживает несколько режимов связи. Работа с U-disk отличается простотой и удобством. Влагозащищенное исполнение и металлический корпус позволяют устройству выдерживать сильные механические воздействия без повреждений. Благодаря компактному и простому дизайну пользователь может подключить несколько устройств к ПК и осуществлять их мониторинг в реальном времени.



## 2.2 Внешний вид

Вид спереди



- ❖ **LED Indicator (Светодиодный индикатор):** Светодиодный индикатор отображает результаты операций и аварийные состояния устройства, которые определяются следующим образом:

**Общие правила:** При успешном выполнении операции зеленый индикатор горит постоянно в течение одной секунды; в противном случае красный индикатор горит постоянно в течение одной секунды.

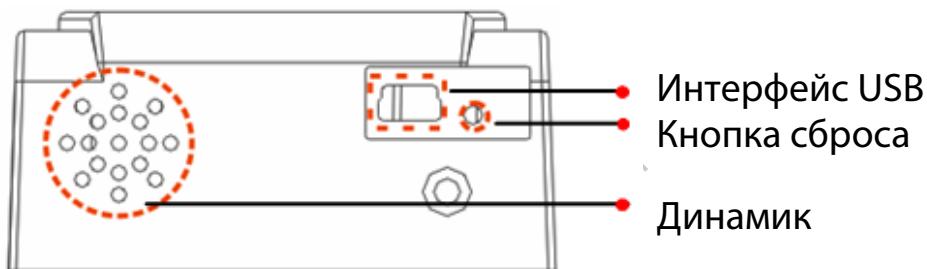
**Режим регистрации:** Зеленый светодиод мигает три раза с интервалом в три секунды.

**Удаление одного пользователя:** Красный светодиод мигает три раза с интервалом в три секунды.

**Режим верификации:** Зеленый светодиод мигает один раз с интервалом в две секунды.

- ❖ **Card Swiping Area (Зона для проведения карты):** Обозначена красной пунктирной рамкой, как показано на рисунке выше.
- ❖ **Fingerprint Sensor (Датчик отпечатка пальца):** Используется для сканирования и сравнения отпечатков пальцев, а также для удаления пользователей.

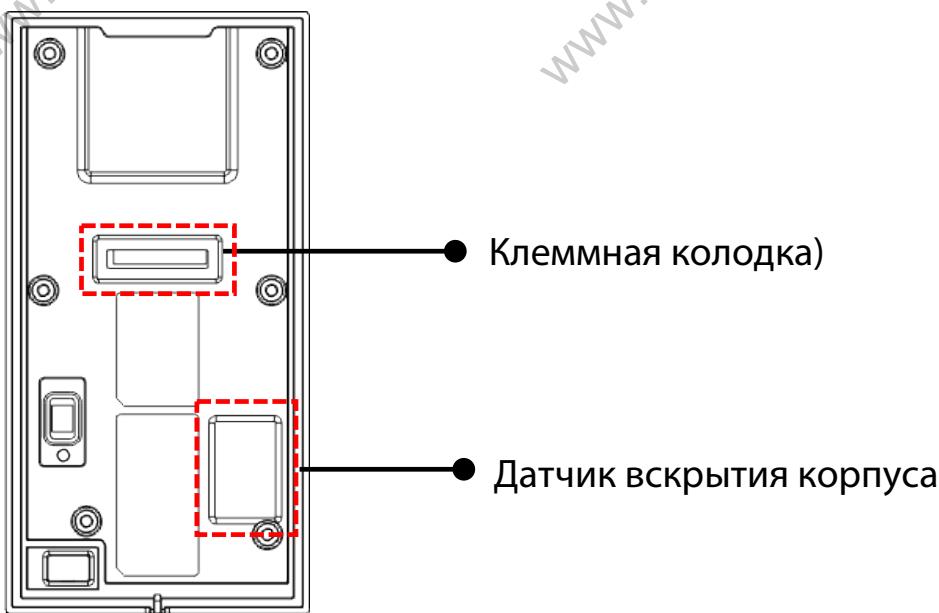
Вид снизу:



**USB Interface (Интерфейс USB):** Используется для подключения U-disk (USB-накопителя).

- ❖ **Reset Button (Кнопка сброса):** Используется для перезагрузки устройства.
- ❖ **Speaker (Динамик):** Используется для воспроизведения звукового сигнала и голосовых подсказок.
- Если пользователь проходит верификацию, динамик издает один звуковой сигнал и произносит "Thank you (Спасибо)".
- Если верификация по отпечатку пальца не прошла, динамик издает один звуковой сигнал и произносит "Please try again (Пожалуйста, попробуйте еще раз)".
- Если верификация по карте не прошла, динамик издает один звуковой сигнал и произносит "Please punch your card again (Пожалуйста, приложите карту еще раз)".
- Стандартные оповещения во время работы: Звуковой сигнал + голосовые подсказки.

Вид сзади:



- ❖ **Wiring Terminal (Клеммная колодка):** Служит для подключения кабелей к замку, источнику питания и ПК (подробная схема подключения приведена в Руководстве по установке).
- ❖ **Tamper Switch (Датчик вскрытия корпуса):** Используется для формирования сигнала тревоги о вскрытии. Подробности см. в разделе 3.4 Датчик вскрытия корпуса.

## 2.3 Режим верификации

**Режим верификации:** Если была выполнена регистрация или успешно зарегистрирована карта администратора, либо при любом таймауте операции, устройство переходит в режим верификации после включения.

Все пользователи могут подтвердить свою личность и разблокировать устройство в режиме верификации (администратор с картой администратора может разблокировать устройство только с помощью ранее зарегистрированных отпечатков пальцев); администратор может выполнять такие операции, как регистрация/удаление пользователей и управление через U-disk, с помощью карты администратора.

## 2.4 Карта администратора

Пользователи устройства делятся на администраторов и обычных пользователей.

- **Administrator (Администратор):** Администратору разрешено выполнять все операции, включая регистрацию или удаление пользователей (удаление всех других пользователей, кроме себя) и управление через U-disk. Права администратора устройства реализуются с помощью карты администратора.
- **Ordinary Users (Обычные пользователи):** Обычным пользователям разрешено только подтверждать свою личность и разблокировать устройство.

Карта администратора — это карта, специально выделенная для суперадминистратора. Для каждого устройства необходимо зарегистрировать карту администратора. Если карта администратора не зарегистрирована, выполнение любых операций невозможно, и система генерирует голосовую подсказку: "❗: "Please register the management card (Зарегистрируйте карту администратора)".



**Различные функции активируются разным количеством последовательных прикладываний карты администратора:**

### Без подключенного U-disk:

- Однократное прикладывание карты администратора переводит устройство в режим регистрации одного пользователя.
- Пятикратное последовательное прикладывание карты администратора переводит устройство в режим удаления одного пользователя.

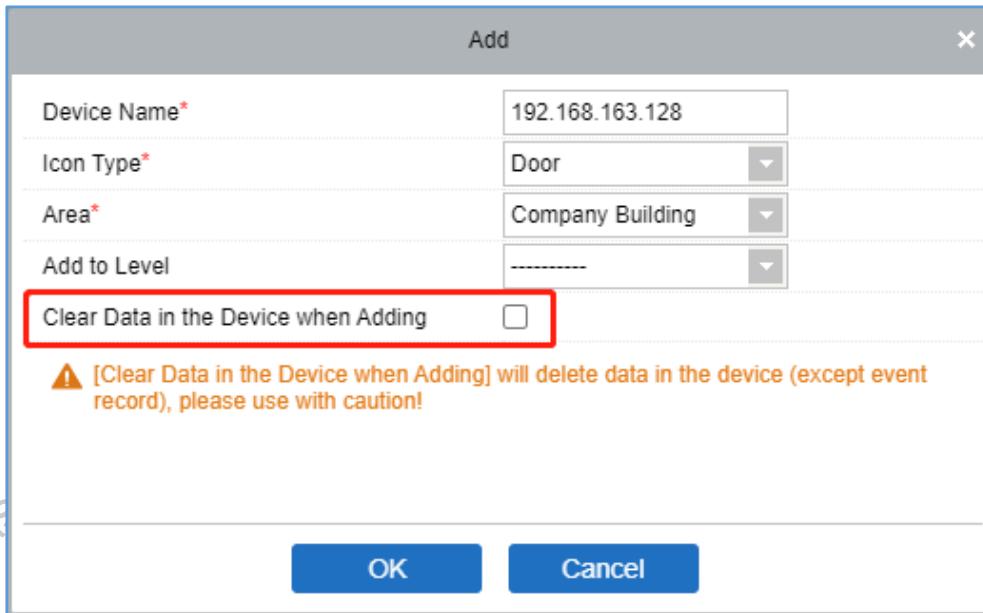
### С подключенным U-disk:

- Однократное прикладывание карты администратора переводит устройство в режим управления U-disk.

**Последовательные прикладывания:** Интервал между двумя прикладываниями подряд должен составлять менее **5 секунд**.

## Удалить карту администратора можно тремя способами:

- Программное обеспечение ZKBioAccess IVS: Установите флагок **Clear Data in the Device when Adding** (Очистить данные на устройстве при добавлении) при добавлении устройства в программу. Подробности см. в разделе 5.2.



• **Датчик вскрытия (Tamper switch):** Для восстановления заводских настроек устройства. Подробности см. в разделе 3.4.

- **Веб-сервер устройства (Webserver):** Для удаления всех данных на устройстве. Подробности см. в разделе 4.3.4.

Отпечатки пальцев пользователя, являющегося держателем карты администратора, могут быть зарегистрированы только через программное обеспечение. Подробности см. в разделе 5.3.

 **Примечание:** Пользователи, имеющие карту администратора, могут подтвердить свою личность и разблокировать устройство только с помощью ранее зарегистрированных отпечатков пальцев.

## 2.5 Таймаут операции

Таймаут операции по умолчанию составляет 30 секунд. Если при удалении/регистрации пользователя не производится никаких действий, система выдает напоминание каждые 10 секунд, а после трех напоминаний возвращается в режим верификации. Голосовая подсказка: "Operation timeout. The system returns to verification state (Таймаут операции. Система возвращается в режим верификации)".

## 3 Операции с устройством

### 3.1 Карта администратора

#### 3.1.1 Регистрация карты администратора

**Для регистрации карты администратора выполните следующие действия:**

1. Устройство автоматически проверяет, зарегистрирована ли карта администратора.
  2. Если устройство не обнаруживает зарегистрированную карту администратора, оно переходит в режим регистрации карты администратора. Затем перейдите к шагу 3; в противном случае перейдите к шагу 5.
3. После того как система произнесет голосовую подсказку "🗣: «Please register the management card (Зарегистрируйте карту администратора)», проведите картой по зоне считывания.

**Примечание:** Устройство будет оставаться в режиме регистрации карты администратора до тех пор, пока ваша карта не будет успешно зарегистрирована.

Если регистрация прошла успешно, система произносит голосовую подсказку: "🗣: "Registration is successful. The system returns to verification state (Регистрация успешно завершена. Система возвращается в режим верификации)".

После возвращения в режим верификации система произносит голосовую подсказку: "🗣: "Verify users. Please press your finger or punch your card (Верификация пользователей. Пожалуйста, приложите палец или приложите карту)".

**Блок-схема процесса регистрации карты администратора представлена ниже:**



### 3.1.2 Регистрация обычного пользователя

При каждом входе в режим регистрации может быть зарегистрирован только один пользователь. При регистрации нового пользователя система автоматически присваивает ему минимальный свободный идентификатор (ID). Каждый пользователь может зарегистрировать не более 10 отпечатков пальцев и одну карту.

**Для регистрации пользователя выполните следующие действия:**

1. В режиме верификации система переходит в режим регистрации обычного пользователя после однократного прикладывания карты администратора (В режиме регистрации однократное прикладывание карты администратора вернет вас в режим верификации).
2. После того как система произнесет голосовую подсказку "█: "Register users. Please press your finger or punch your card (Регистрация пользователей. Пожалуйста, приложите палец или приложите карту)", вы можете начать регистрацию пользователя. Возможны два варианта:



### (1) Сначала приложите карту

- a. Когда вы прикладываете новую карту и пользователь успешно регистрируется, устройство произносит голосовую подсказку "🗣: "User number \*\*. Registration is successful! (Пользователь номер. Регистрация успешна!)" ( означает идентификатор (ID), автоматически присвоенный пользователю системой; далее аналогично). После этого переходите к шагу **b**.
- b. После того как устройство произнесет голосовую подсказку "🗣: "Register. Please press your finger (Регистрация. Пожалуйста, приложите палец)" , система переходит в режим регистрации указанного отпечатка пальца. Приложите один и тот же палец к датчику трижды, следуя голосовым подсказкам.
- c. Если регистрация отпечатка пальца прошла успешно, система произносит голосовую подсказку "🗣: "Registration is successful. Register. Please press your finger (Регистрация успешна. Зарегистрируйте. Пожалуйста, приложите палец)" и сразу переходит в режим регистрации следующего отпечатка пальца. Если регистрация отпечатка пальца не удалась, система произносит голосовую подсказку: "Please press your finger again (Пожалуйста, приложите палец снова)" и повторяет шаг **b**.

d. Система автоматически возвращается в режим верификации, когда зарегистрированы 10 пальцев и карта, когда карта администратора приложена один раз или при таймауте операции.

## (2) Сначала приложите палец(цы)

- a. Трижды приложите один и тот же палец к датчику, следуя голосовым подсказкам и правильно размещая палец. Если регистрация отпечатка пальца прошла успешно, система произносит голосовую подсказку "🗣: "User number \*\*. Registration is successful (Пользователь номер \*\*. Регистрация успешна)" и вы можете перейти к шагу **b**. Если регистрация отпечатка не удалась, система произносит голосовую подсказку "🗣: "Please press your finger again (Пожалуйста, приложите палец снова)" и возвращается в режим регистрации, ожидая приложения пальца или карты.
- b. После произнесения голосовой подсказки: "🗣: "Register. Please press your finger or punch your card (Регистрация. Пожалуйста, приложите палец или приложите карту)", система переходит в режим регистрации информации указанного пользователя, ожидая приложения новой карты или пальца.
- c. Если регистрация карты прошла успешно, система произносит голосовую подсказку: "🗣: "Registration is successful. Register. Please press your finger (Регистрация успешна. Зарегистрируйте. Пожалуйста, приложите палец)" и сразу переходит в режим регистрации отпечатка пальца. Если вы приложите ранее незарегистрированный палец и он будет успешно зарегистрирован, система произнесет голосовую подсказку: "🗣: "Registration is successful. Please press your finger or punch your card (Регистрация успешна. Пожалуйста, приложите палец или приложите карту)", и вы можете продолжить регистрацию новых отпечатков пальцев и карты. После регистрации 10 отпечатков пальцев, если ваша карта еще не зарегистрирована, система произнесет голосовую подсказку "🗣: "Register. Please punch your card (Регистрация. Пожалуйста, приложите карту)" для регистрации карты.

d. Система автоматически возвращается в режим верификации, когда зарегистрированы 10 пальцев и карта, когда карта администратора приложена один раз или при таймауте операции.

3. Если пользователю уже присвоен ID, то для регистрации отпечатков пальцев или карты возможны следующие два варианта:

**(1) Регистрация отпечатка(ов) пальца при уже зарегистрированной карте**

- a. После прикладывания зарегистрированной карты система произнесет голосовую подсказку: ">User number \*\*. Register. Please press your finger (Пользователь номер . Зарегистрируйте. Пожалуйста, приложите палец)" ( означает ID, присвоенный пользователю; далее аналогично) и перейдет в режим регистрации отпечатка пальца. Регистрируемые отпечатки пальцев заменят все предыдущие.
- b. Трижды приложите один и тот же палец к датчику, следуя голосовым подсказкам и правильно размещая палец. Если регистрация отпечатка пальца прошла успешно, система произносит голосовую подсказку "Registration is successful. Please press your finger (Регистрация успешна. Пожалуйста, приложите палец)" и переходит к регистрации следующего отпечатка.
- c. Система автоматически возвращается в режим верификации, когда зарегистрированы 10 пальцев, когда карта администратора приложена один раз или при таймауте операции.

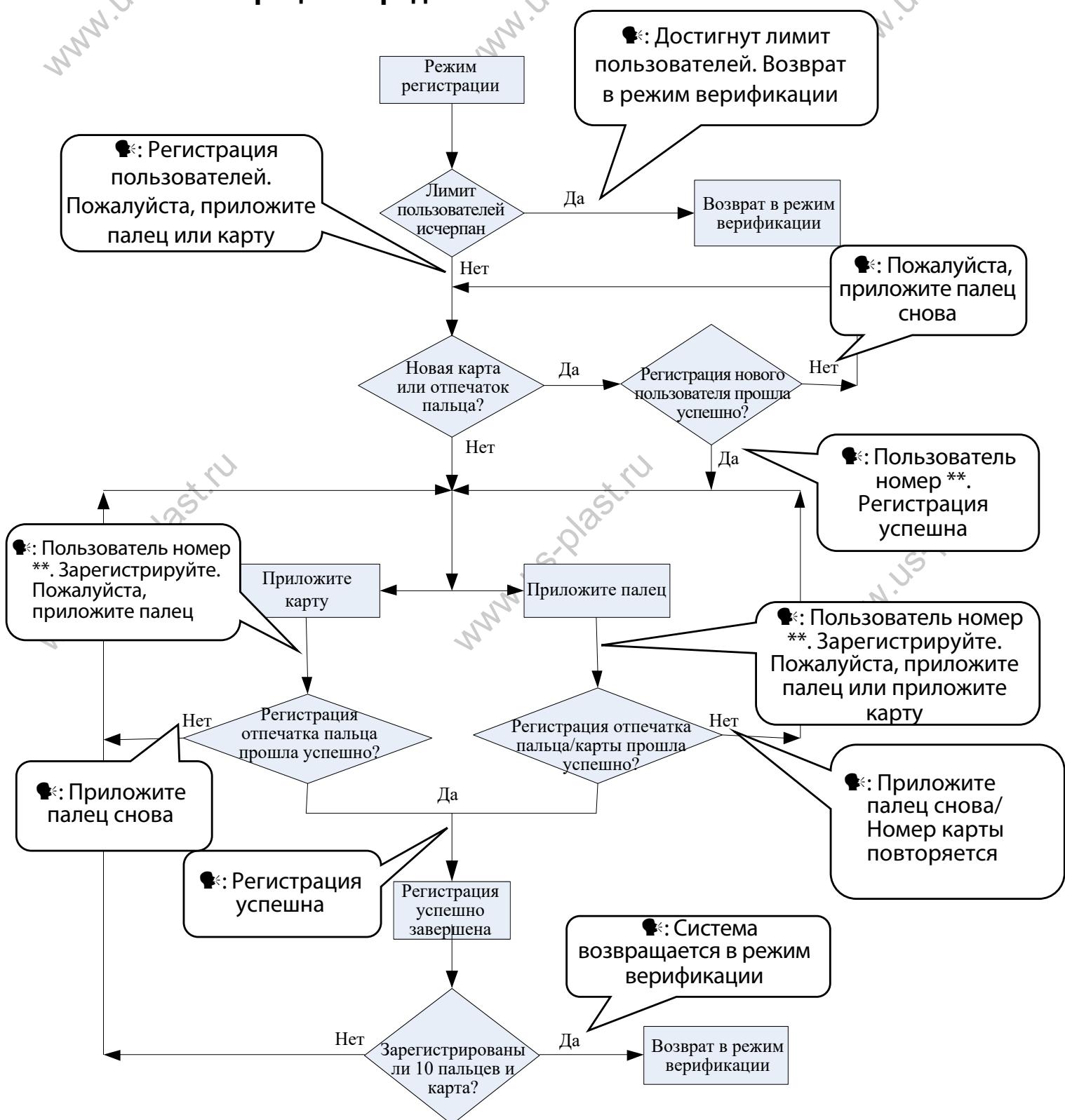
**Примечания:**

- Отпечатки пальцев, зарегистрированные на этом шаге, заменят все ранее зарегистрированные отпечатки данного пользователя.
- В этом режиме невозможно зарегистрировать отпечаток пальца пользователя, имеющего карту администратора, так как прикладывание карты администратора автоматически вернет систему в режим верификации.

## (2) Регистрация карты и отпечатка(ов) пальца при уже зарегистрированном отпечатке(ах) пальца

- a. Трижды приложите палец с уже зарегистрированным отпечатком, следуя голосовым подсказкам. Если при каждой попытке система идентифицирует вас как одного и того же человека, она переходит в режим регистрации отпечатка пальца.
- b. После произнесения голосовой подсказки "⌚: "User number \*\*. Register. Please press your finger or punch your card (Пользователь номер \*\*. Зарегистрируйте. Пожалуйста, приложите палец или приложите карту)", система начинает регистрацию вашего отпечатка пальца или карты. Отпечатки пальцев, зарегистрированные на этом шаге, заменят все предыдущие отпечатки данного пользователя.
- c. Если регистрация карты прошла успешно, система произносит голосовую подсказку "⌚: "Registration is successful. Register. Please press your finger (Регистрация успешна. Зарегистрируйте. Пожалуйста, приложите палец)" и сразу переходит в режим регистрации отпечатка пальца. Если вы приложите ранее незарегистрированный палец и он будет успешно зарегистрирован, система произнесет голосовую подсказку: "⌚: "Registration is successful. Please press your finger or punch your card (Регистрация успешна. Пожалуйста, приложите палец или приложите карту)", и вы можете продолжить регистрацию новых отпечатков пальцев и карты. После регистрации 10 отпечатков пальцев, если ваша карта еще не зарегистрирована, система произнесет голосовую подсказку "⌚: "Register. Please punch your card (Регистрация. Пожалуйста, приложите карту)" для регистрации карты.
- d. Система автоматически возвращается в режим верификации, когда зарегистрированы 10 пальцев и карта, когда карта администратора приложена один раз или при таймауте операции.

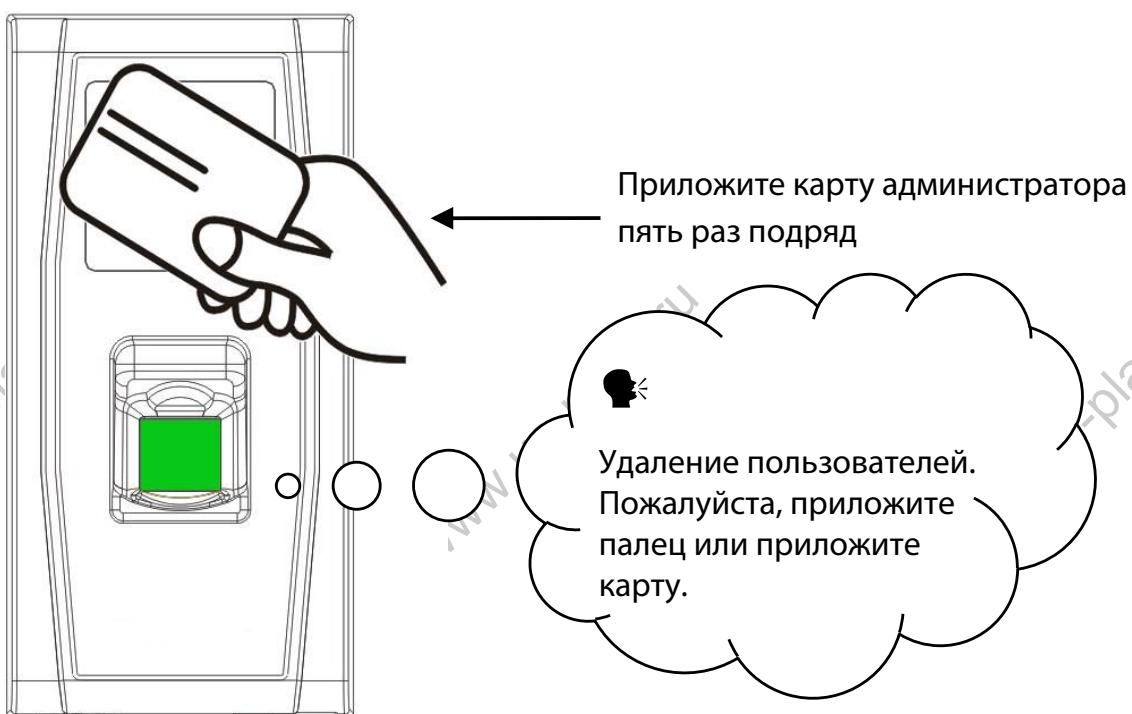
## Блок-схема процесса представлена ниже:



### 3.1.3 Удаление одного пользователя

#### Операция удаления одного пользователя (простой режим):

1. В режиме верификации приложите карту администратора пять раз подряд, чтобы войти в режим простого удаления одного пользователя (приложите карту еще один раз, чтобы вернуться в режим верификации).



2. Приложите палец к датчику отпечатков или проведите картой по считывателю.

##### (1) Удаление пользователя по отпечатку пальца:

Правильно приложите один из зарегистрированных пальцев к датчику. Если верификация прошла успешно, система произнесет голосовую подсказку "🗣: "User number \*\*. Deletion is successful. Delete users. Please press your finger or punch your card. (Пользователь номер . Удаление успешно. Удаление пользователей. Пожалуйста, приложите палец или приложите карту.)" ( указывает ID-номер пользователя) и автоматически вернется в режим удаления. Если верификация не удалась, система произнесет голосовую подсказку "🗣: "Please try again. (Пожалуйста, попробуйте еще раз.)".

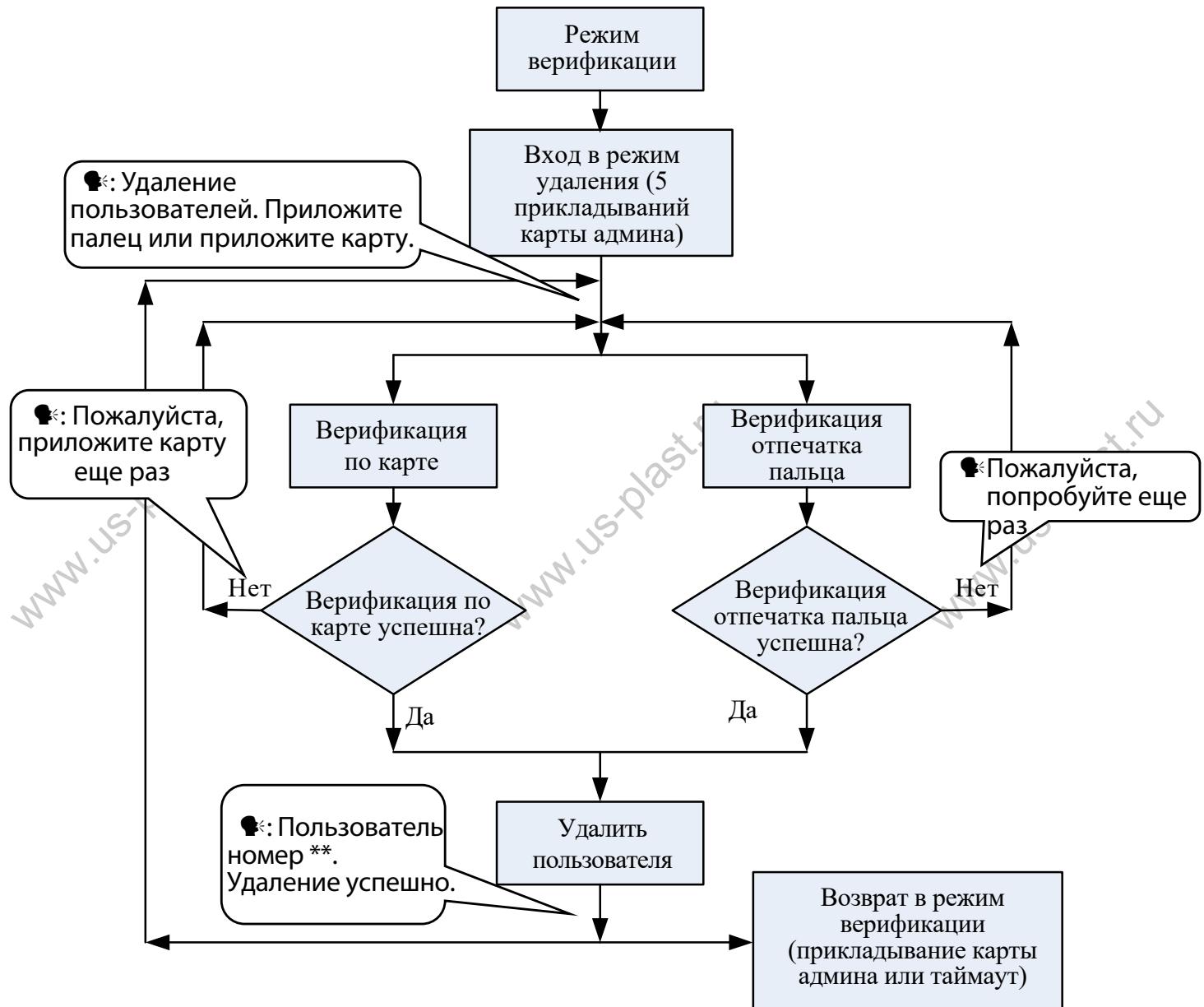
**(2) Проведите картой по считывателю для удаления пользователя.**

Проведите зарегистрированную карту по считывателю. Если верификация прошла успешно, система произнесет голосовую подсказку “: "User number \*\*. Deletion is successful. Delete users. Please press your finger or punch your card. (Пользователь номер \*\*). Удаление успешно. Удаление пользователей. Пожалуйста, приложите палец или приложите карту.)" и автоматически вернется в режим удаления. Если верификация не удалась, система произнесет голосовую подсказку “: "Please punch your card again. (Пожалуйста, приложите карту еще раз.)".

3. Если вы приложите карту администратора еще один раз или произойдет таймаут операции, система вернется в режим верификации.



**Примечание:** В режиме простого удаления одного пользователя нельзя удалить держателя карты администратора, так как прикладывание карты администратора вернет систему в режим верификации.

**Процедура простого удаления одного пользователя:**

## 3.2 Верификация пользователя

### Порядок действий:

1. Когда устройство находится в режиме верификации, система произносит голосовую подсказку "🗣: "Verify users. Please press your finger or punch your card. (Верификация пользователей. Пожалуйста, приложите палец или приложите карту.)"
2. Начало верификации пользователя. Устройство поддерживает два режима верификации: по отпечатку пальца и по карте.

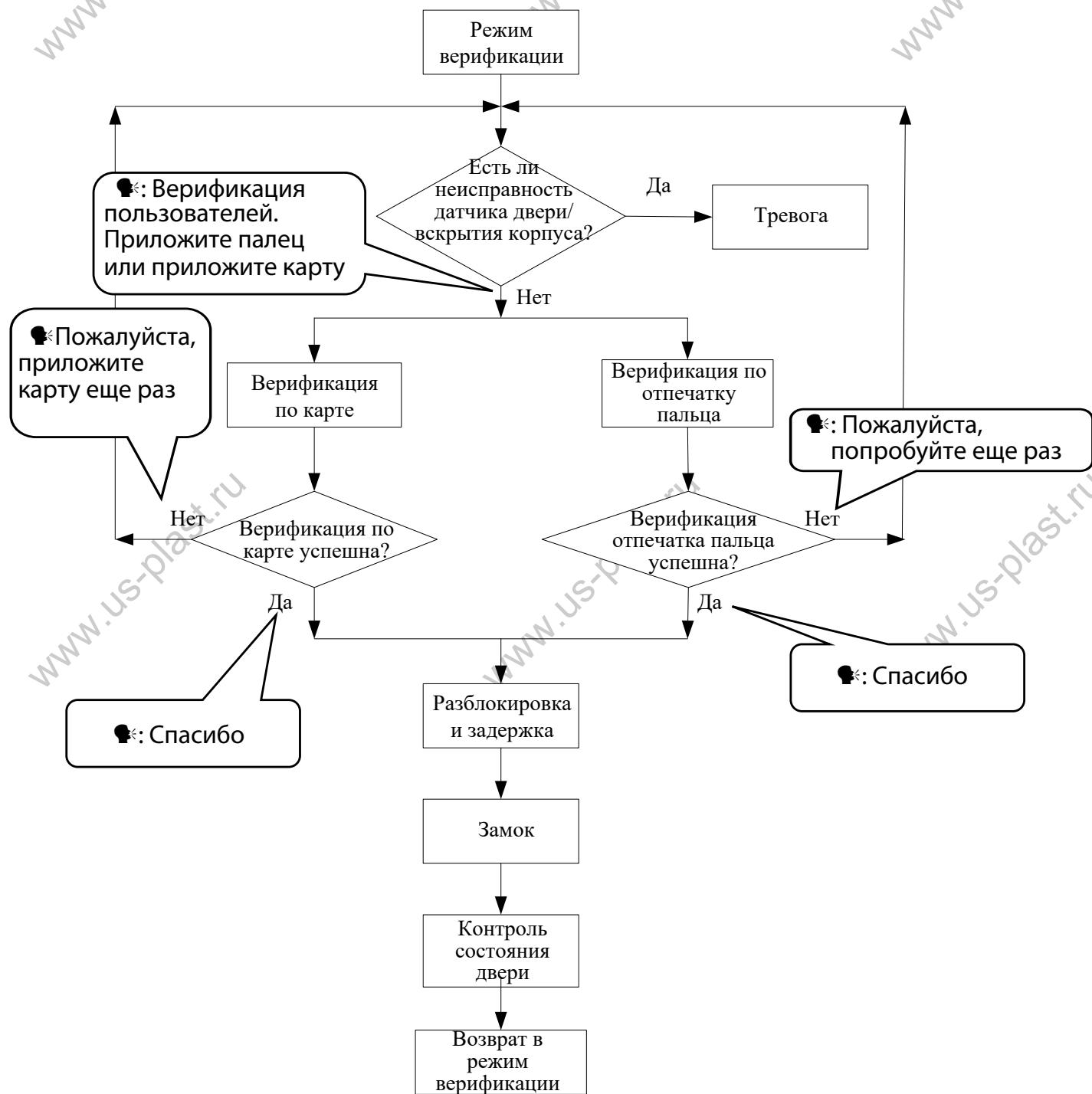
#### (1) Верификация по отпечатку пальца

Правильно приложите палец к датчику отпечатков. Если верификация прошла успешно, система произносит голосовую подсказку "🗣: "Thank you. (Спасибо.)" и одновременно формирует сигнал разблокировки. Если верификация не удалась, система произносит голосовую подсказку "🗣: "Please try again. (Пожалуйста, попробуйте еще раз.)"

#### (2) Верификация по карте

Проведите картой по считывателю. Если верификация прошла успешно, система произносит голосовую подсказку "🗣: "Thank you. (Спасибо.)" и одновременно формирует сигнал разблокировки. Если верификация не удалась, система произносит голосовую подсказку "🗣: "Please punch your card again. (Пожалуйста, приложите карту еще раз.)"

**Блок-схема процесса верификации пользователя представлена ниже:**



**Примечание:** Администратор может разблокировать устройство с помощью своих зарегистрированных отпечатков пальцев, а не карты администратора.

### 3.3 U-диск (U-disk)

Пользователь может выполнять загрузку журналов событий, выгрузку/загрузку данных пользователей и обновление микропрограммы (прошивки) через U-disk.

- a. **Download Records (Загрузка журналов событий):** Загрузка журналов доступа всех пользователей с устройства на U-disk.
- b. **Download Users (Выгрузка данных пользователей):** Загрузка всей пользовательской информации (например, отпечатков пальцев, номеров карт) с устройства на U-disk.
- c. **Upload Users (Загрузка данных пользователей):** Загрузка пользовательской информации с U-disk на устройство.
- d. **Upgrade Firmware (Обновление микропрограммы):** Обновление прошивки устройства через U-disk.

#### Операции с U-disk:

Если подключить U-disk к устройству, система автоматически поочередно предложит доступные операции.

- (1) После подключения U-disk к устройству приложите карту администратора один раз, чтобы войти в режим управления U-disk.
- (2) Система произносит голосовую подсказку ": \*\*\*\*. Please punch your management card for confirmation. (. Пожалуйста, приложите карту администратора для подтверждения.)" (\*\*\*\* означает четыре пункта операций **a-d** по порядку; далее аналогично).
- (3) Если вы хотите выполнить операцию, приложите карту администратора для подтверждения. Если операция успешна, система произносит голосовую подсказку ": The operation is successful. (Операция выполнена успешно.)" и предлагает перейти к следующему шагу.

После выполнения всех четырех пунктов система произносит "❗: *The system returns to verification state.* (Система возвращается в режим верификации.)". Если операция не удалась, система произносит "❗: "The operation fails. The system returns to verification state. (Ошибка операции. Система возвращается в режим верификации.)".

- (4) Если вы не приложите карту администратора, система автоматически пропустит этот шаг через 5 секунд и предложит следующий. После выполнения всех четырех пунктов система автоматически возвращается в режим верификации.



Не обновляйте микропрограмму (прошивку) самостоятельно, так как это может вызвать проблемы и нарушить нормальную работу устройства. Для технической поддержки или уведомления об обновлениях обращайтесь к нашим дистрибуторам.

### 3.4 Датчик вскрытия корпуса

Датчик вскрытия корпуса нажимается и удерживается задней крышкой. При разборке устройства датчик освобождается и отправляет сигнал тревоги.

**Сброс сигнала тревоги:** Пользователь может сбросить сигнал тревоги, вернув магнит на датчик вскрытия.

**Восстановление заводских настроек:** Заводские настройки можно восстановить с помощью датчика вскрытия.

Процедура восстановления заводских настроек: Включите устройство. После голосовой подсказки "Verify users. Please press your finger or punch your card (Верификация пользователей. Пожалуйста, приложите палец или приложите карту)" в течение 30, но не более 60 секунд, приложите магнит к датчику вскрытия шесть раз.

После успешного восстановления устройство автоматически перезагрузится и произнесет подсказку: *"Please register the management card (Зарегистрируйте карту администратора)"*.



### Примечания:

1. Все пользовательские данные будут удалены, включая данные администратора и обычных пользователей.
2. IP-адрес устройства и пароль для входа в веб-сервер будут сброшены на значения по умолчанию.

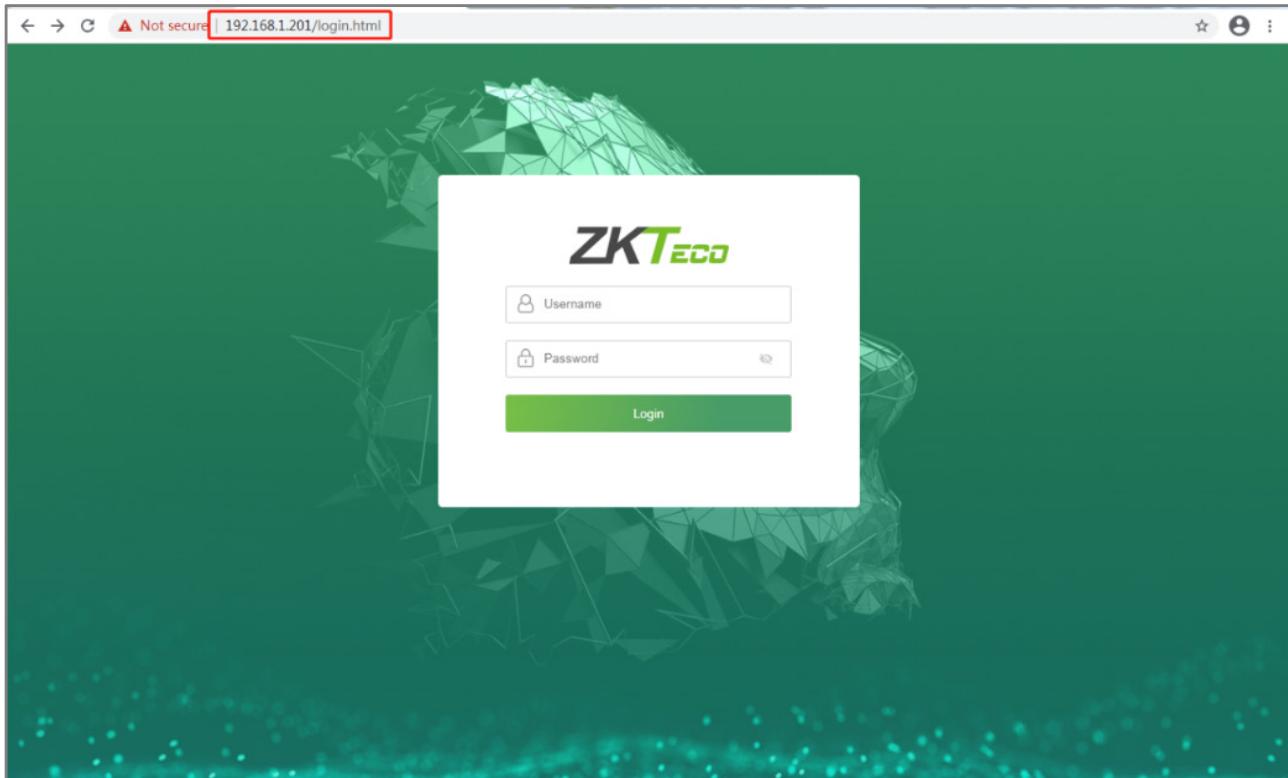
## 4 Веб-сервер устройства

Пользователь может открыть веб-приложение для настройки соответствующих параметров устройства.

### 4.1 Авторизация

Сначала подключите устройство к сети. Откройте браузер и введите адрес: **https://IP-адрес\_устройства**, чтобы перейти на интерфейс входа. (Например, IP-адрес устройства по умолчанию — **192.168.1.201**, тогда адрес веб-сервера: **https://192.168.1.201**).

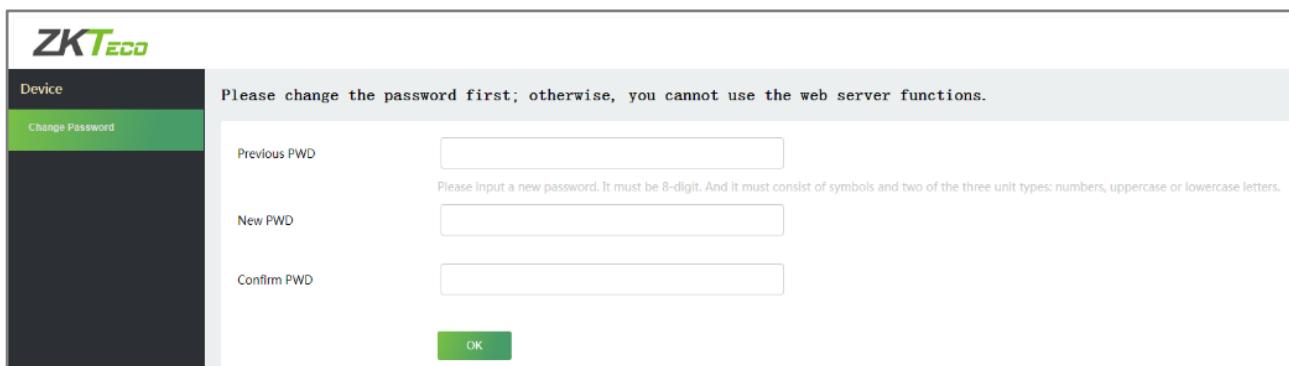
**Примечание:** IP-адрес вашего ПК и устройства должны находиться в одной подсети, иначе ссылка не откроется. Если вы изменили IP-адрес устройства в *Settings-Comm Settings* (*Настройки-Параметры связи*), адрес веб-сервера изменится соответствующим образом.



Введите **Username** (Имя пользователя) и **Password** (Пароль).

- Username (Имя пользователя): **admin** (по умолчанию)
- Password (Пароль): **admin@123** (по умолчанию)

После успешного входа система перенаправит на страницу смены пароля. Введите *Previous password* (Старый пароль), *New password* (Новый пароль) и подтвердите его в поле *Confirm your password* (Подтвердите новый пароль). Затем нажмите *OK*, как показано ниже:



#### Примечание:

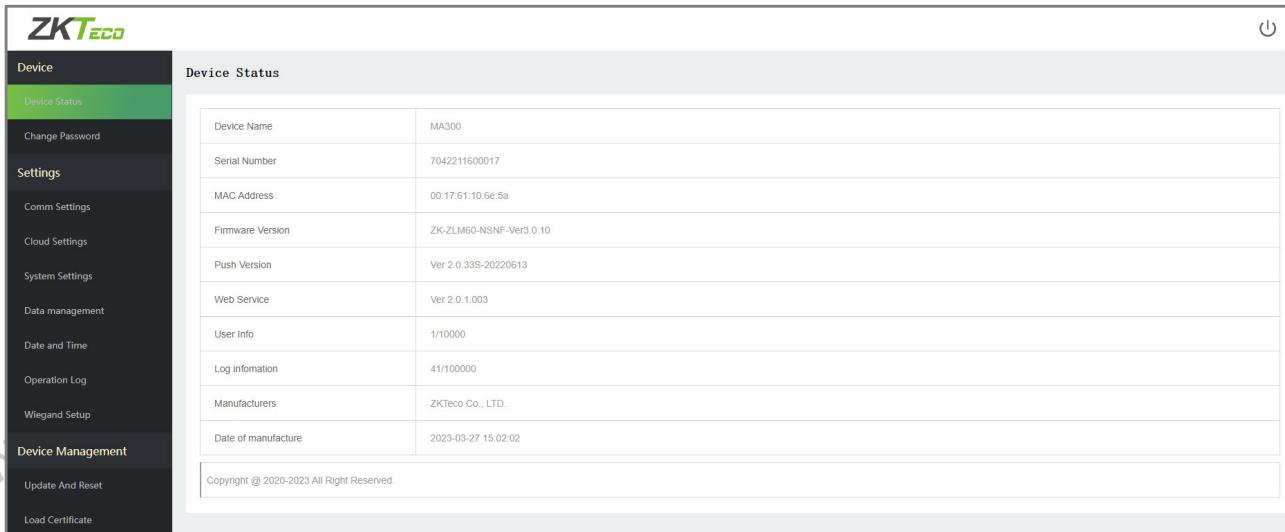
1. Пароль необходимо сменить при первом входе в систему.
2. Новый пароль должен содержать не менее 8 символов, включать специальные символы (например, @, #, \$) и как минимум два из трех типов символов: цифры, заглавные или строчные буквы.
3. Если вы забыли пароль от веб-сервера, восстановите заводские настройки через датчик вскрытия корпуса (tamper switch).  
Подробности см. в разделе 3.4.

После успешного изменения система вернется на интерфейс входа в систему.

## 4.2 Устройство

### 4.2.1 Состояние устройства

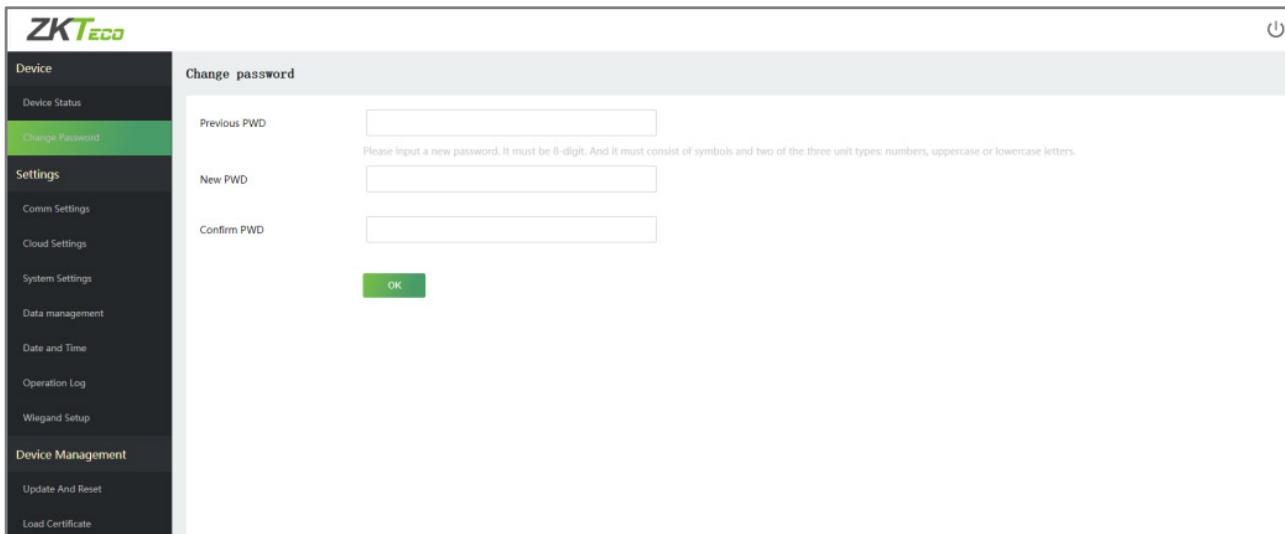
Нажмите *Device Status* (Состояние устройства), чтобы просмотреть *Device name* (Имя устройства), *Serial number* (Серийный номер), *MAC address* (MAC-адрес) и другую информацию о текущем устройстве.



Device Name	MA300
Serial Number	7042211600017
MAC Address	00:17:61:10:6e:5a
Firmware Version	ZK-ZLM60-NSNF-Ver3.0.10
Push Version	Ver 2.0.33S-20220613
Web Service	Ver 2.0.1.003
User Info	1/10000
Log information	41/100000
Manufacturers	ZKTeco Co., LTD.
Date of manufacture	2023-03-27 15:02:02

### 4.2.2 Смена пароля

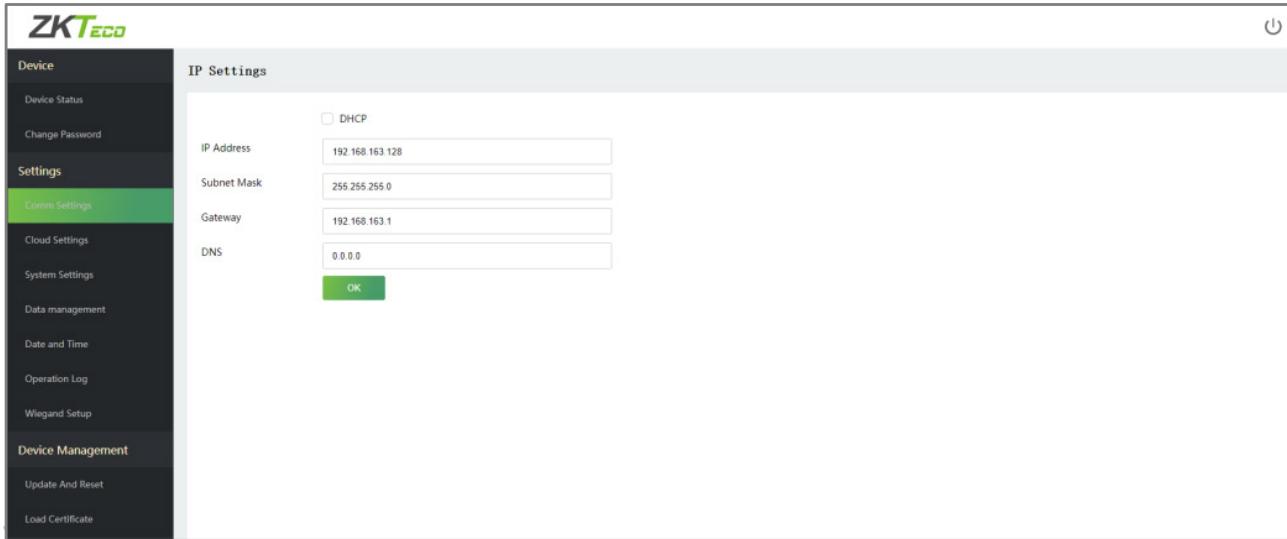
Нажмите *Change Password* (Смена пароля), чтобы изменить пароль пользователя. Введите *Previous password* (Старый пароль), *New password* (Новый пароль), подтвердите его в поле *Confirm the password* (Подтвердите пароль), затем нажмите *OK*.



## 4.3 Настройки

### 4.3.1 Параметры связи

Если устройству необходимо взаимодействовать с сетью, требуется настроить параметры IP.



#### Описание полей:

**DHCP:** DHCP (Dynamic Host Configuration Protocol) динамически назначает IP-адреса клиентам через сервер. Если DHCP включен, IP-адреса нельзя задавать вручную.

**IP Address (IP-адрес):** Значение по умолчанию — 192.168.1.201. Можно изменить в соответствии с доступными сетевыми параметрами.

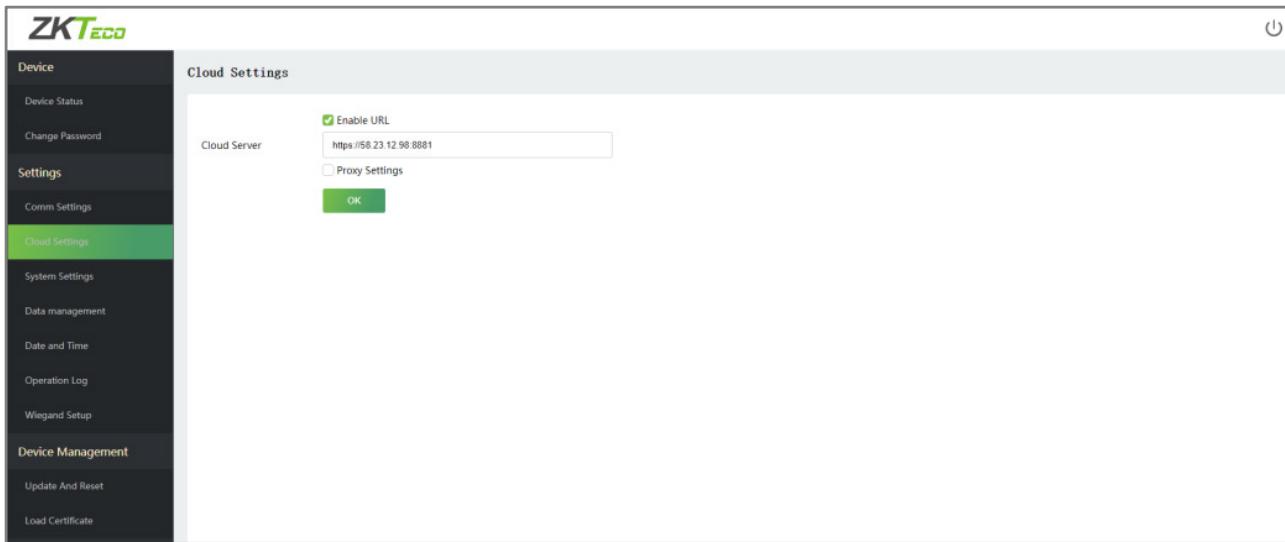
**Subnet Mask (Маска подсети):** Значение по умолчанию — 255.255.255.0. Можно изменить в соответствии с доступными сетевыми параметрами.

**Gateway (Шлюз):** Значение по умолчанию — 192.168.1.1. Можно изменить в соответствии с доступными сетевыми параметрами.

**DNS:** Адрес DNS по умолчанию — 0.0.0.0. Можно изменить в соответствии с конфигурацией сети.

## 4.3.2 Настройки облака

Подключение к облачному серверу осуществляется путем настройки параметров *Cloud Server Settings* (Параметры облачного сервера).



### Описание полей:

**Enable URL (Включить URL):** Эту настройку следует активировать, когда программное обеспечение работает в режиме HTTPS. Необходимо ввести полный адрес сервера и порт связи, как показано на рисунке выше.

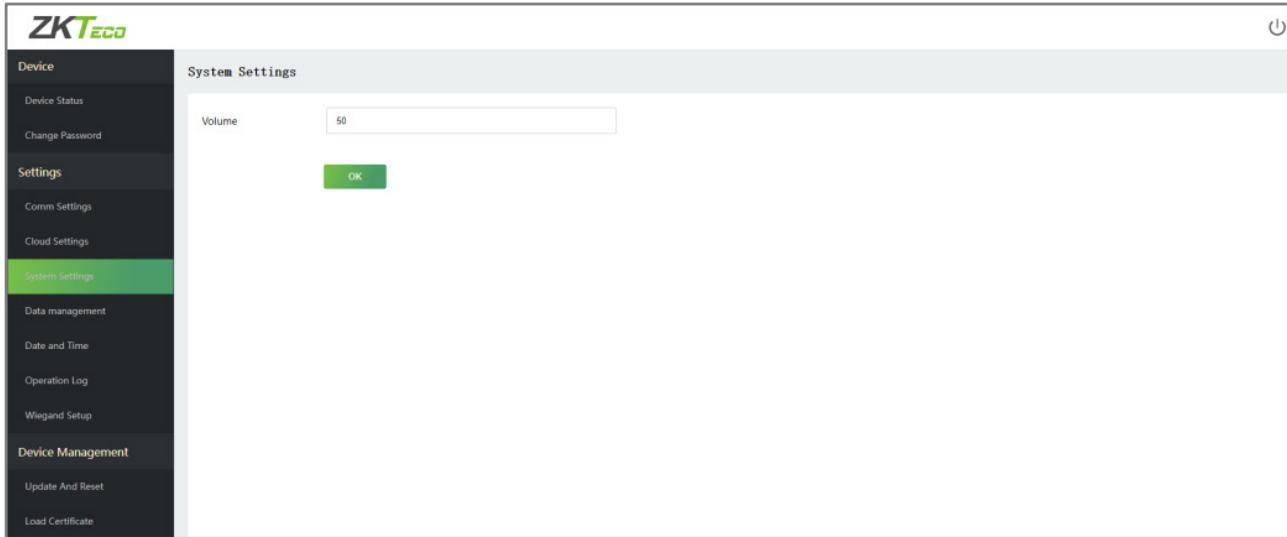
**Cloud Server (Облачный сервер):** IP-адрес сервера.

**Cloud Server Port (Порт облачного сервера):** Порт сервера.

**Proxy Settings (Настройки прокси-сервера):** IP-адрес и номер порта прокси-сервера задаются вручную при включении прокси.

### 4.3.3 Системные настройки

Нажмите *System Settings* (Системные настройки), чтобы настроить громкость устройства. Введите значение громкости и нажмите **OK**.

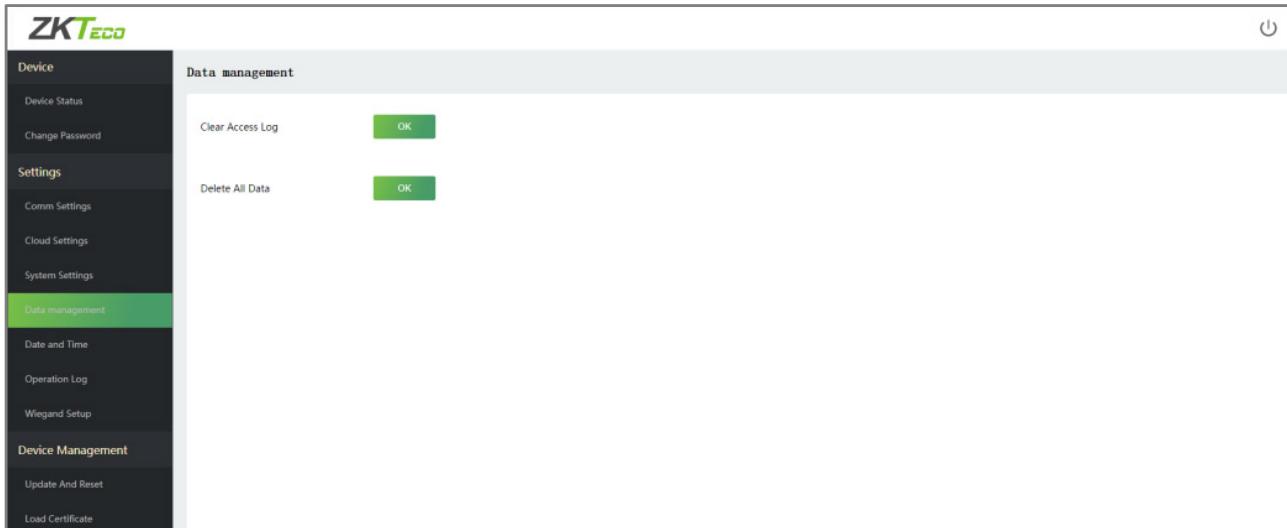


#### Описание полей:

**Volume (Громкость):** Регулировка громкости устройства. Значение может быть установлено в диапазоне от 0 до 100.

### 4.3.4 Управление данными

Нажмите *Data Management* (Управление данными), чтобы удалить соответствующие данные на устройстве.



#### Описание полей:

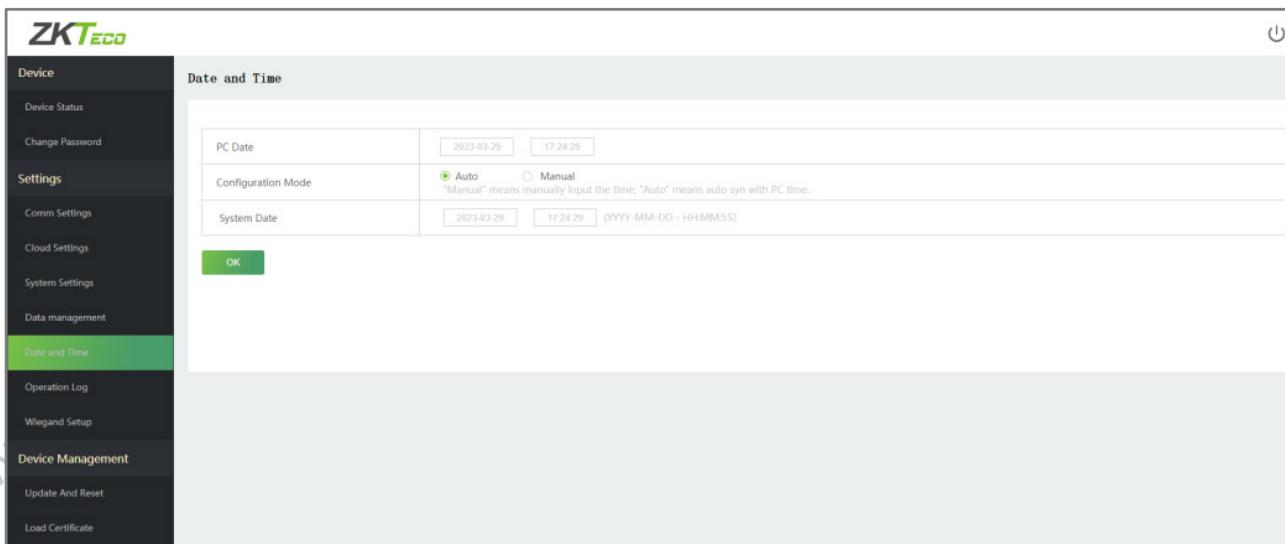
**Clear Access Log (Очистить журнал доступа):** Удаляет все записи журнала доступа.

**Delete All Data (Удалить все данные):** Удаляет все журналы и пользовательские данные (включая администратора)

и обычных пользователей). **Действуйте с осторожностью!** После успешного выполнения операции потребуется повторный вход в веб-сервер (Webserver).

### 4.3.5 Дата и время

Нажмите **Date and Time** (Дата и время), чтобы установить дату и время устройства.



#### Описание полей:

**Auto (Авто):** Автоматическая синхронизация с временем ПК.

**Manual (Вручную):** Требуется вручную ввести дату и время.

**Примечание:** Формат даты должен быть ГГГГ-ММ-ДД-ЧЧ:ММ:СС.

### 4.3.6 Журнал операций

Нажмите *Operation Log* (Журнал операций), чтобы просмотреть все журналы операций с устройством.

**Download (Скачать):** Выберите начальное и конечное время, затем нажмите *Download* (Скачать). Журнал операций за выбранный период будет автоматически загружен.

### 4.3.7 Настройка Wiegand

Нажмите Wiegand Setup (Настройка Wiegand), чтобы задать параметры ввода и вывода по стандарту Wiegand.

#### Описание полей:

**Wiegand Format (Формат Wiegand):** Может иметь значение 26 бит, 34 бита, 36 бит, 37 бит или 50 бит.

**Wiegand Bits (Биты Wiegand):** Количество бит данных Wiegand.

**Pulse Width(us) (Длительность импульса, мкс):** Длительность импульса, отправляемого по Wiegand. По умолчанию 100 микросекунд, может быть скорректирована в диапазоне от 20 до 100 микросекунд.

**Pulse Interval(us) (Интервал импульсов, мкс):** Значение по умолчанию — 1000 микросекунд, может быть скорректировано в диапазоне от 200 до 20000 микросекунд.

ID Type (Тип идентификатора): Выберите между User ID (ID пользователя) и card number (номером карты).

## Описание распространенных форматов Wiegand:

Формат Wiegand	Описание
<b>Wiegand26</b>	<p>EEEEEEEEEEEEEEEEEEEECCCCCO</p> <p>Состоит из 26-битного двоичного кода. 1-й бит является битом четности (even parity) для битов со 2-го по 13-й, а 26-й бит является битом нечетности (odd parity) для битов с 14-го по 25-й. Биты со 2-го по 25-й представляют собой номер карты.</p>
<b>Wiegand26a</b>	<p>ESSSSSSSCCCCCCCCCCCCCCCCCO</p> <p>Он состоит из 26-битного двоичного кода. 1-й бит является битом четности для битов со 2-го по 13-й, а 26-й бит является битом нечетности для битов с 14-го по 25-й. Биты со 2-го по 9-й представляют собой код объекта (site codes), а биты с 10-го по 25-й — номер карты.</p>
<b>Wiegand34</b>	<p>EEEEEEEEEEEEEEEEEEEECCCCCCCCCO</p> <p>Он состоит из 34-битного двоичного кода. 1-й бит является битом четности для битов со 2-го по 17-й, а 34-й бит является битом нечетности для битов с 18-го по 33-й. Биты со 2-го по 25-й представляют собой номер карты.</p>
<b>Wiegand34a</b>	<p>ESSSSSSSCCCCCCCCCCCCCCCCCO</p> <p>Он состоит из 34-битного двоичного кода. 1-й бит является битом четности для битов со 2-го по 17-й, а 34-й бит является битом нечетности для битов с 18-го по 33-й. Биты со 2-го по 9-й представляют собой код объекта, а биты с 10-го по 25-й — номер карты.</p>

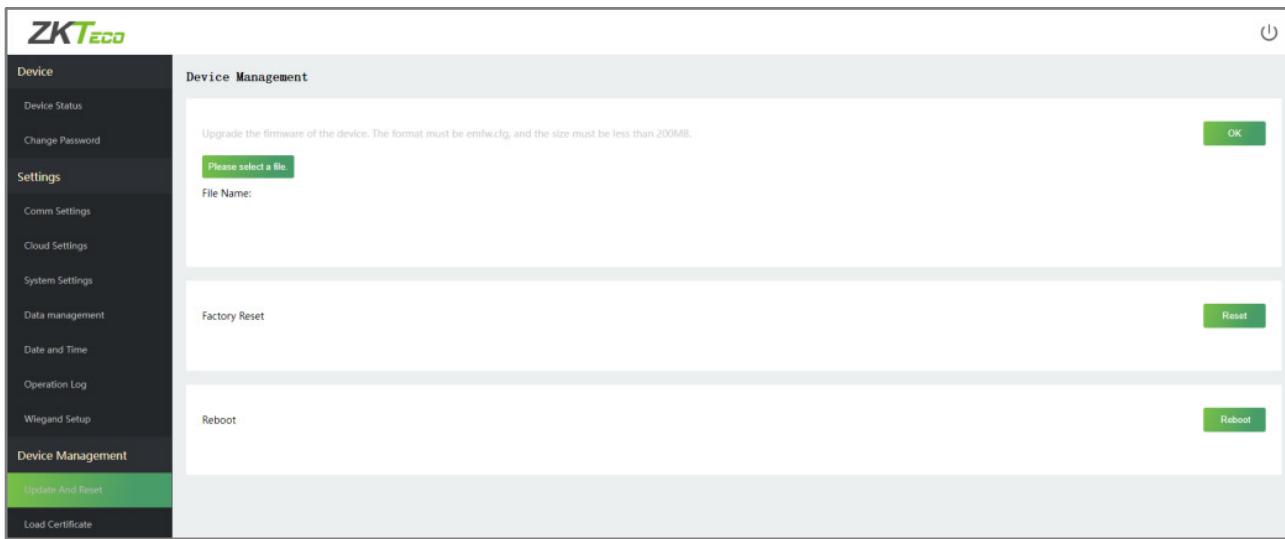
<b>Wiegand36</b>	<p>ОФФФФФФФФФФФФССССССССССССММЕ</p> <p>Он состоит из 36-битного двоичного кода. 1-й бит является битом нечетности для битов со 2-го по 18-й, а 36-й бит является битом четности для битов с 19-го по 35-й. Биты со 2-го по 17-й представляют собой код устройства. Биты с 18-го по 33-й представляют собой номер карты, а биты с 34-го по 35-й — код производителя.</p>
<b>Wiegand36a</b>	<p>ЕFFFFFFFFFFFCCCCCCCCCCCCCCCCCO</p> <p>Он состоит из 36-битного двоичного кода. 1-й бит является битом четности для битов со 2-го по 18-й, а 36-й бит является битом нечетности для битов с 19-го по 35-й. Биты со 2-го по 19-й представляют собой код устройства, а биты с 20-го по 35-й — номер карты.</p>
<b>Wiegand37</b>	<p>ОММММССССССССССССССССССССССССССЕ</p> <p>Он состоит из 37-битного двоичного кода. 1-й бит является битом нечетности для битов со 2-го по 18-й, а 37-й бит является битом четности для битов с 19-го по 36-й. Биты со 2-го по 4-й представляют собой код производителя. Биты с 5-го по 16-й представляют собой код объекта, а биты с 21-го по 36-й — номер карты.</p>
<b>Wiegand37a</b>	<p>ЕМММFFFFFFFFFFSSSSCCCCCCCCCCCCCO</p> <p>Он состоит из 37-битного двоичного кода. 1-й бит является битом четности для битов со 2-го по 18-й, а 37-й бит является битом нечетности для битов с 19-го по 36-й. Биты со 2-го по 4-й представляют собой код производителя. Биты с 5-го по 14-й представляют собой код устройства, биты с 15-го по 20-й — код объекта, а биты с 21-го по 36-й — номер карты.</p>

Wiegand50	<p>ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCC ССО</p> <p>Он состоит из 50-битного двоичного кода. 1-й бит является битом четности для битов со 2-го по 25-й, а 50-й бит является битом нечетности для битов с 26-го по 49-й. Биты со 2-го по 17-й представляют собой код объекта, а биты с 18-го по 49-й — номер карты.</p>
<p>"С" обозначает номер карты; "Е" — бит четности (Even parity bit); "О" — бит нечетности (Odd parity bit);</p> <p>"F" — код объекта (Facility code); "M" — код производителя (Manufacturer code);</p> <p>"Р" — бит четности (Parity bit); а "S" — код площадки (Site code).</p>	

## 4.4 Управление устройством

### 4.4.1 Обновление и сброс

Нажмите Update and Reset (Обновление и сброс), чтобы настроить параметры обновления устройства, сброса к заводским настройкам и перезагрузки.



#### Описание полей:

**Update (Обновление):** Нажмите *Please select a file* (Выберите файл). Формат файла должен быть *emfw.cfg*, а размер — менее 200 МБ.

Нажмите *OK*, чтобы выполнить операцию обновления микропрограммы (прошивки).

**Factory Reset (Сброс к заводским настройкам):** Функция сброса восстанавливает параметры устройства (такие как настройки связи и системные настройки) до заводских значений по умолчанию.



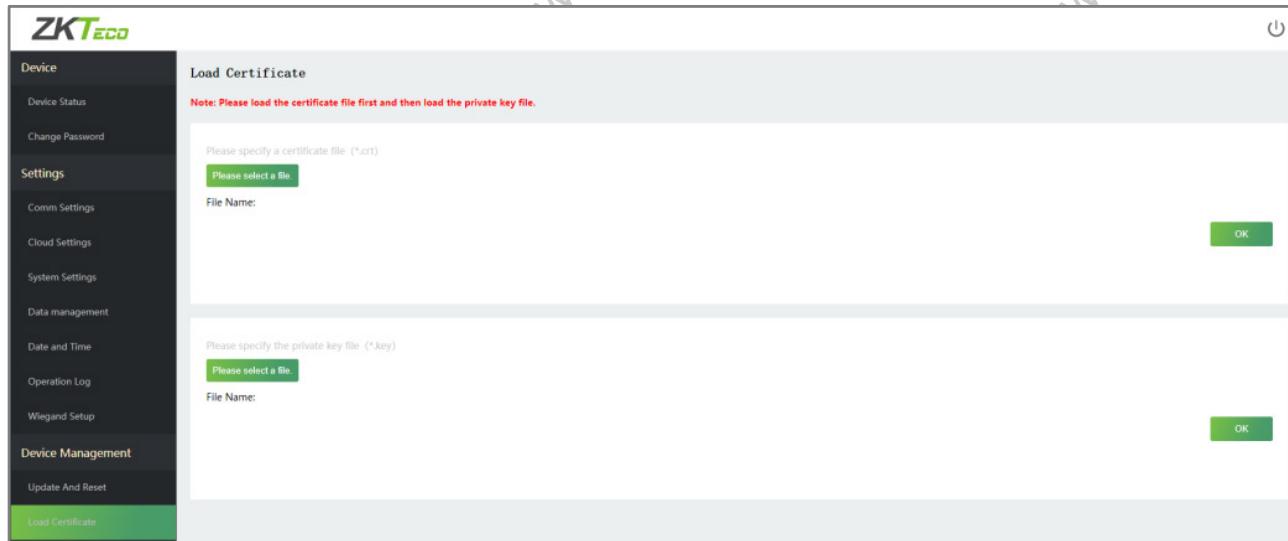
#### Примечание:

1. Пароль веб-сервера и IP-адрес устройства будут сброшены до значений по умолчанию.
2. Пользовательские данные удалены не будут.

**Reboot (Перезагрузка):** Перезапуск устройства.

#### 4.4.2 Загрузка сертификата

Нажмите *Load Certificate* ( Загрузить сертификат), чтобы загрузить файл сертификата устройства и файл закрытого ключа. Нажмите *Please select a file* (Выберите файл), загрузите файл сертификата и файл закрытого ключа, затем нажмите *OK*, чтобы завершить операцию загрузки файлов.

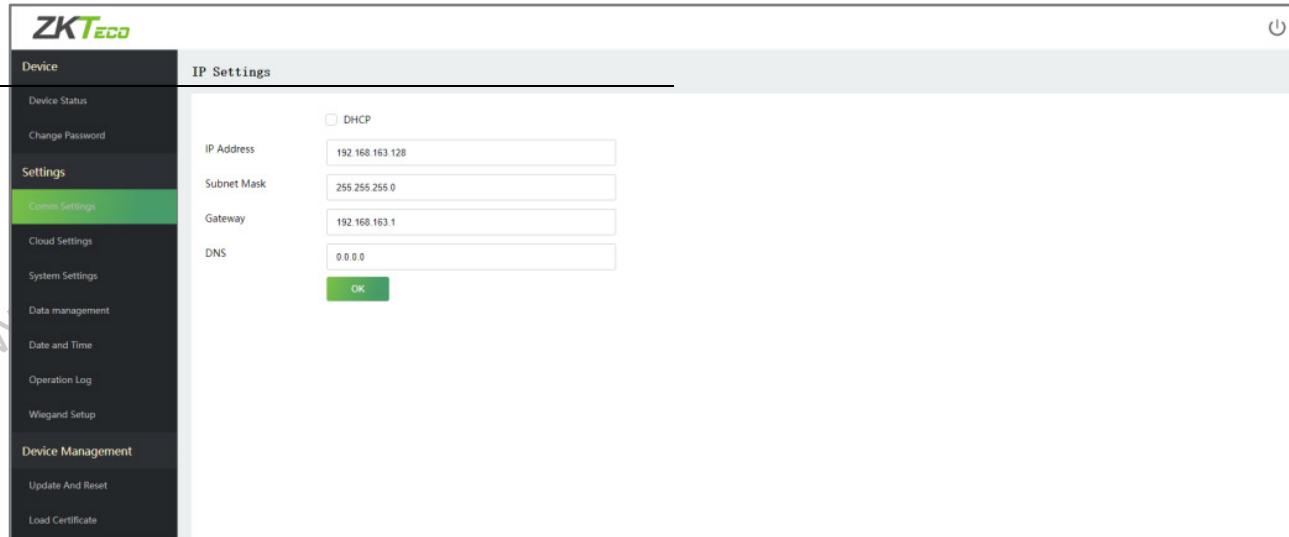


**Примечание:** Сначала загрузите файл сертификата, а затем файл закрытого ключа.

## 5. Подключение к ПО ZKBIO CVACCESS

### 5.1 Задать адрес связи

1. Войдите в веб-сервер (*Webserver*). Нажмите *Comm Settings* (Параметры связи), чтобы задать *IP address* (IP-адрес) и *Gateway* (Шлюз) устройства. (Примечание: IP-адрес должен обеспечивать связь с сервером ZKBIO CVACCESS).

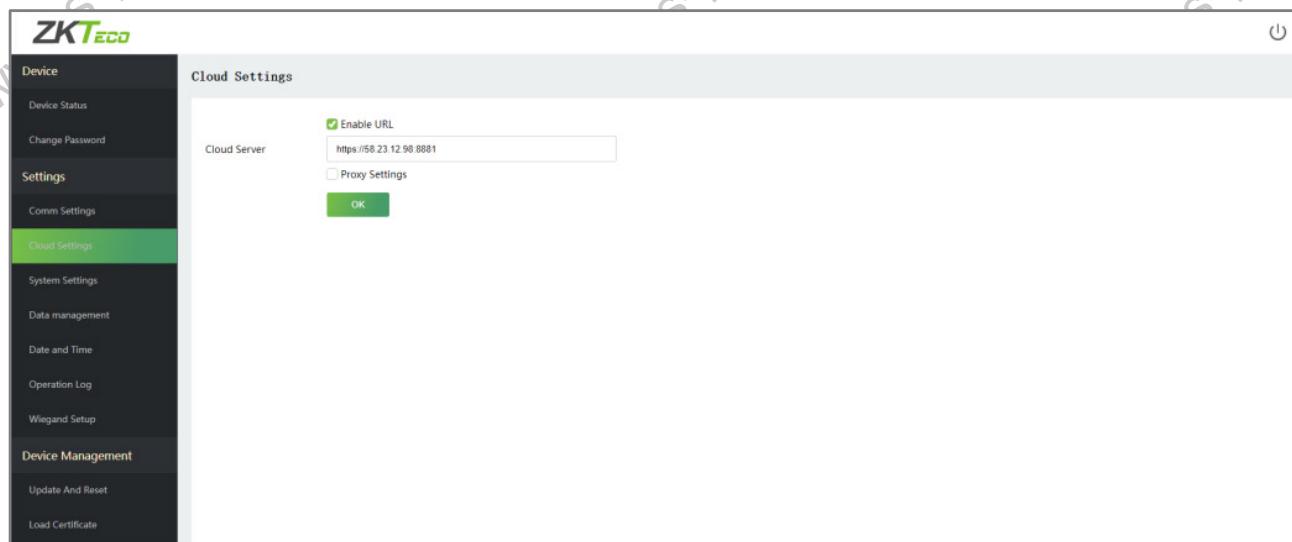


2. Нажмите *Cloud Settings* (Настройки облака), чтобы задать *Server address* (Адрес сервера) и *Server port* (Порт сервера).

**Enable URL (Включить URL):** Эту настройку следует активировать, когда программное обеспечение работает в режиме HTTPS. Необходимо ввести полный адрес сервера и порт связи, как показано на рисунке ниже.

**Cloud Server (Облачный сервер):** Установите IP-адрес сервера ZKBIO CVACCESS.

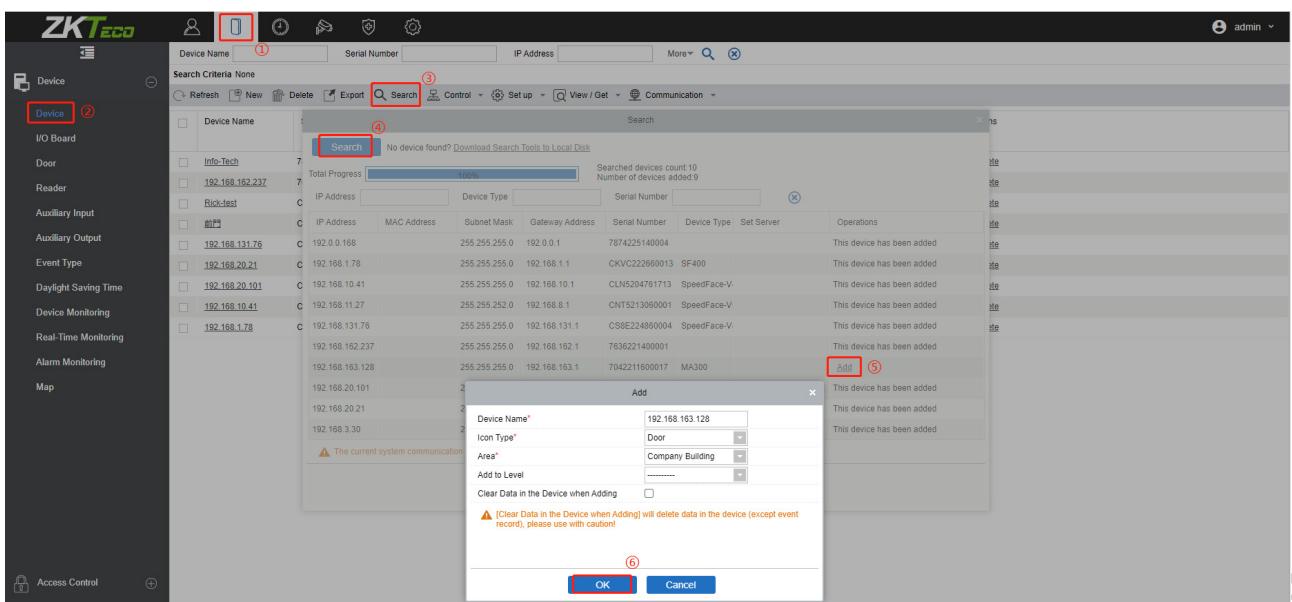
**Cloud Server Port (Порт облачного сервера):** Установите сервисный порт ZKBIO CVACCESS.



## 5.2 Добавление устройства в программу

Вы можете добавить устройство путем поиска. Процесс выглядит следующим образом:

1. Нажмите *Access* (Доступ) > *Device* (Устройство) > *Search* (Поиск), чтобы открыть интерфейс поиска.
2. Нажмите *Search* (Поиск), появится сообщение "*Searching...* (Выполняется поиск...)".
3. После завершения поиска будет отображен список контроллеров доступа и их общее количество.

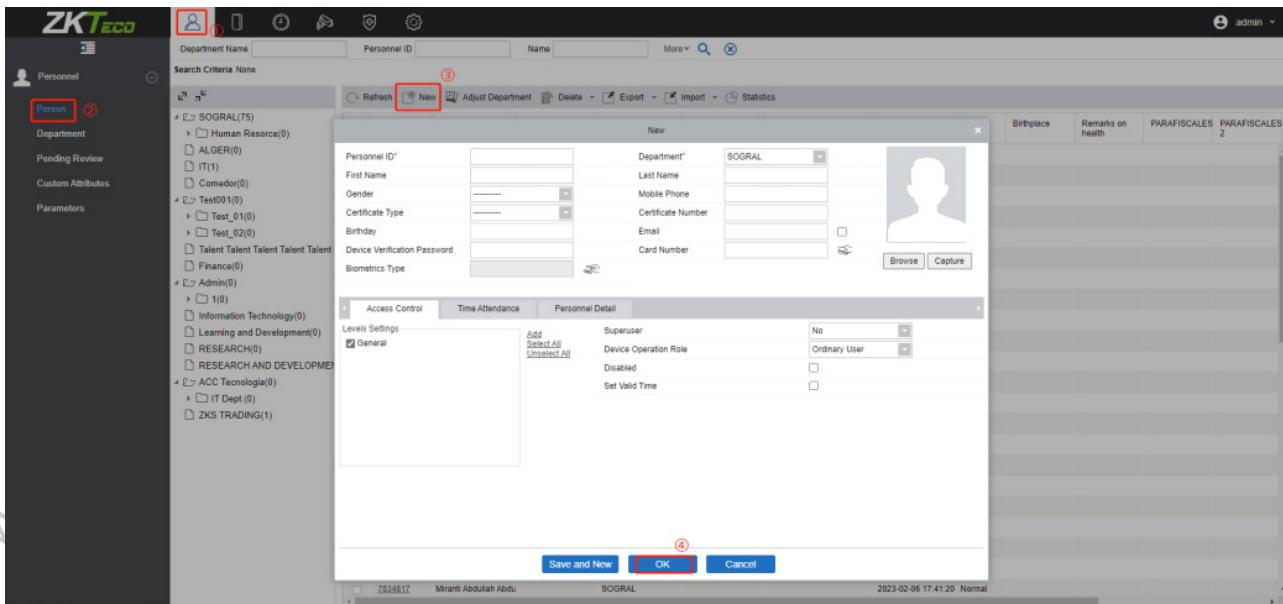


4. Нажмите *Add* (Добавить), чтобы добавить устройство..

5. После успешного добавления устройство отобразится в списке устройств.

## 5.3 Добавление людей в программу

1. Нажмите *Personnel* (Контингент) > *Person* (Человек) > *New* (Создать).



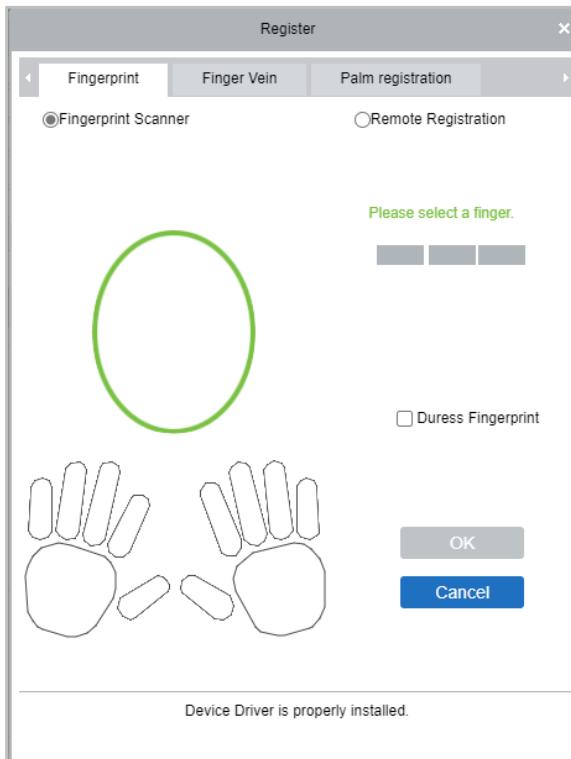
2. Введите необходимые данные пользователя и нажмите *OK*, чтобы сохранить запись.
3. Нажмите *Access* (Доступ) > *Device* (Устройство), отметьте устройство, с которым нужно работать, и нажмите *Control* (Управление) > *Synchronize All Data to Devices* (Синхронизировать все данные на устройства), чтобы синхронизировать все данные с устройством.

### ● Как зарегистрировать отпечатки пальцев пользователя, имеющего карту администратора?

1. Нажмите *Access* (Доступ) > *Device* (Устройство), отметьте устройство, с которым нужно работать, и нажмите *View/Get* (Просмотр/Получение) > *Get Personnel Information* (Получить информацию о людях), чтобы получить информацию о людях.
2. Нажмите *Personnel* (Контингент) > *Person* (Человек), выберите пользователя с *Personnel ID* (ID в контингенте), равным 1, чтобы перейти в интерфейс редактирования пользователя.

Нажмите значок  , чтобы зарегистрировать отпечаток пальца.

**(Примечание:** сначала необходимо подключить настольный сканер отпечатков пальцев к ПК).



3. После успешной регистрации нажмите *Access* (Доступ) > *Device* (Устройство), отметьте устройство, с которым нужно работать, и нажмите *Control* (Управление) > *Synchronize All Data to Devices* (Синхронизировать все данные на устройства), чтобы синхронизировать все данные с устройством.

#### **Примечание:**

1. Устройство MA300 в настоящее время не поддерживает онлайн-регистрацию отпечатков пальцев.
2. За подробными инструкциями по другим операциям обратитесь к ZKBIO CVACCESS User Manual (Руководству пользователя ZKBIO CVACCESS).

## 6 Характеристики

В следующей таблице перечислены основные функциональные параметры устройства.

Параметр	Описание
Питание	12V, 3A
Функции	Устройство контроля доступа, датчик двери/сигнализация/замок/кнопка выхода
	Один вход и один выход Wiegand
Кол-во пользователей	10,000 (отпечаток пальца и ID-карта)
Вместимость журнала	100,000 записей
Вместимость регистрируемого лица (отпечаток пальца/карта)	1,500 отпечатков / 10,000 карт
Режимы верификации	Карта ID (IC / HID), отпечаток пальца
Интерфейсы связи	TCP / IP, RS485
Динамик	Голосовые подсказки
LED	Двухцветная индикация (красный / зеленый)

