РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Серия устройств контроля доступа по венам пальцев

Версия: 1.0.1

Дата: янв., 2019

Обзор Руководства

В этом документе описываются пользовательские интерфейсы и функции меню серии устройств контроля доступа по венам пальцев. Этот документ может использоваться в сочетании с программным обеспечением Access3.5. Для установки продукта, пожалуйста, смотрите руководство по началу работы устройства.

- Изображения в этом руководстве могут не соответствовать изображению вашего устройства; дисплей текущего устройства имеет преимущественную силу.
- Только некоторые устройства оснащены функциями со ★; текущее устройство имеет преимущественную силу.

Важное Заявление

Пожалуйста, внимательно прочитайте это руководство, чтобы не повредить устройство перед использованием. Напоминаем, что при правильном использовании вы можете испытать хороший эффект и скорость верификации.

Никакая часть этого документа не может быть извлечена или передана каким-либо образом без предварительного письменного согласия нашей компании.

Описанная в данном руководстве лицензия может содержать программное обеспечение, принадлежащее нашей компании или лицензиарам, обладающим авторскими правами. После того, как это разрешено кредиторами, никто не может копировать, распространять, изменять, извлекать, декомпилировать, разбирать, декодировать, осуществлять обратный инжиниринг, аренду, передачу, сублицензию Такое программное обеспечение в любой форме или поведения, нарушающего авторские права на программное обеспечение, за исключением случаев, но ограничения, налагаемые на закон, исключаются..



В связи с постоянным обновлением продуктов, компания не может выпускать фактический продукт полностью в соответствии с информацией в документе, а также не несет ответственность за любой спор, вызванный различием между фактическими техническими параметрами и информацией в этом документе. Приносим свои извинения за любые изменения без предварительного уведомления.

Содержание

1. Инструкция по применению 3

1.1 Функции устройства 3
1.2 Режимы регистрации и верификации по венам и отпечаткам пальцев★ 4
1.3 Способы прижима отпечатка пальца★ 7
1.4 Использование сенсорного датчика 7
1.5 Режимы верификации 8
1.5.1 Верификация по венам и отпечаткам пальцев★ 8
1.5.2 Верификация по паролю 10
1.5.3 Верификация по карте★ 12
1.5.4 Комбинированная верификация 12
1.5.5 Комбинированная верификация для разблокировки 13
1.6 Внешний вид устройства и клеммные колодки 15
1.6.1 Внешний вид устройства 15
1.6.2 Клеммные колодки 16
1.7 Начальный интерфейс 17

2. Главное меню 19

3. Управление пользователями 22

3.1 Добавление пользователей 22
3.1.1 Ввод идентификатора пользователя 23
3.1.2 Ввод имени 24
3.1.3 Роль пользователя 25
3.1.4 Регистрация вены и отпечатка пальца 26
3.1.5 Регистрация номера карты★ 28
3.1.6 Регистрация пароля 28
3.1.7 Настойка уровня контроля доступа 29
3.2 Все пользователи 31
3.2.1 Запрос пользователя 32
3.2.2 Редактирование / удаление пользователя 32
3.3 Стиль отображения 34

4. Роль пользователя 36

5. Настройки связи 40

5.1 Настройки Ethernet 40
5.2 Настройки последовательной связи 41
5.3 Подключение ПК 42
5.4 Установка Wiegand 43
5.4.1 Вход Wiegand 43
5.4.2 Выход Wiegand 46
5.4.3 Формат карты определяется автоматически 47

6. Системные настройки 49

6.1 Настройки даты / времени 49
6.2 Настройка журналов доступа★ 50
6.3 Настройка параметров вен и отпечатков пальцев★ 51
6.4 Сброс до заводских настроек 52
6.5 Обновить USB 52
7. Настройки персонализации 54
7.1 Настройки пользовательского интерфейса 54
7.2 Настройки голоса 56
7.3 Настройки звонков 57
7.3.1 Новый график звонков 58
7.3.2 Все графики звонков 60
8. Управление данными 61
8.1 Удалить данные 61
8.2 Данные резервной копии 63
8.3 Восстановить данные 64
9. Контроль доступа 66
9.1 Настройки параметров контроля доступа 66
9.2 Настройки графиков 69
9.3 Настройки праздничных дней 71
9.3.1 Добавить праздничные дни 72
9.3.2 Включить праздничные дни 74
9.4 Настройки комбинированной верификации 74
9.5 Настройки запрета двойного прохода 76
10. Диспетчер USB 79
10.1 Загрузить на USB 79
10.2 Выгрузить с USB 80
11. Поиск событий учета рабочего времени 82
12. Автоматическое тестирование 83
13. Информация о системе 85
14. Приложения 88
Приложение 1 Инструкции ввода текста 88
Приложение 2 USB 89
Приложение 3 Введение в Wiegand 90
Приложение 3.1 Введение в Wiegand 26 91
Приложение 3.2 Введение в Wiegand 34 93
Приложение 4 Настройки запрета двойного прохода 96
Заявление о правах человека и конфиденциальности 100
Описание экологичного использования 101

1. Инструкция по применению

Не подвергайте устройство воздействию сильного прямого солнечного света, поскольку сильный свет оказывает неблагоприятное воздействие на коллектор отображения вен. Рабочая температура устройства колеблется от 0 до 40°C, и теплоотдача устройства может снизить его производительность, что приведет к снижению скорости отклика и скорости прохождения. Если устройство необходимо использовать на открытом воздухе, рекомендуется использовать корпус или теплоизлучающее оборудование.

Рекомендуемая высота установки (вертикальное расстояние от земли до дверного звонка) устройства составляет 1,4 м в зависимости от группы пользователей с высотой от 1,55 до 1,75 м. Высота установки может быть отрегулирована на основе средней высоты пользователя, так чтобы пользователи было удобно прижимать вены и пальцы.

1.1 Функции устройства

- Специальные функции (приложение логики прошивки)

1. Функция вены пальца

Технология идентификации вен пальцев - это новая технология идентификации биологических характеристик. Он распознает идентичность, используя изображения распределения вен в пальцах, и обладает характеристиками уникальности, стабильности, высокой точности идентификации и защиты от подделок.

Функция «Вена пальца» поддерживает регистрацию, удаление, верификацию, а также загрузку и выгрузку шаблонов вены пальца через USB-диск или программное обеспечении.

2. Контроль доступа пользователя

Логика управления доступом, использующая контроллер, имеет следующие функции:

Установка действительных дат пользователей

Установка периодов времени действия пользователей

(3) Поддержка нескольких методов верификации пользователя

(4) Установка периодов времени действия для дверей

(5) Установка периодов времени для открытия двери

(6) Установка периодов времени для праздников

(7) Настройка первой карты на нормальное открытие

(8) Установка периодов времени запрета двойного прохода

(9) Установка запрета двойного прохода на вход / выход

(10) Ведение записей контроллера контроля доступа

(11) Поддержка вспомогательного входа

(12) Поддержка функций главного и подчиненного блока Wiegand

3. Функция USB-диска

Вы можете загружать пользовательские данные и записи контроля доступа на USB-диск и загружать пользовательские данные, рекламные изображения и обои с USB-диска на устройство.

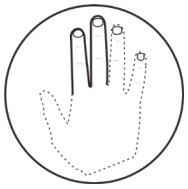
4. Связь через RS485 или Ethernet

Устройство связывается с программным обеспечением Access3.5 по протоколу RS485 или Ethernet (TCP / IP).

1.2 Режимы регистрации и верификации по венам и отпечаткам пальцев★

Примечание: при регистрации вены пальца устройство также регистрирует отпечаток выбранного пальца.

1. Рекомендуемые пальцы: указательный и средний пальцы



2. Расположение пальца

(1) Коснитесь кончиком пальца передней выемки коллектора отображения вены пальца, прижмите мякоть пальца к коллектору отпечатка пальца, чтобы устройство зафиксировало вену и отпечаток пальца.

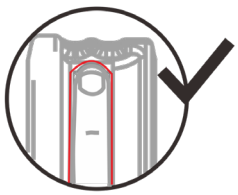


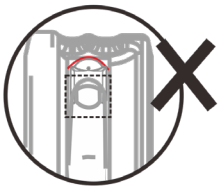
② Когда мякоть пальца соприкасается с датчиком, коллектор начинает фиксировать вену и отпечаток пальца.

3. Процедура верификации по венам



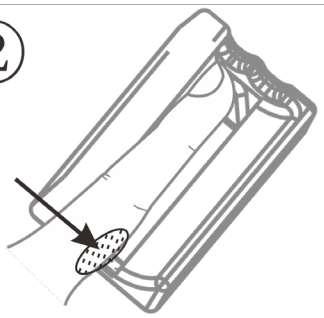
Убедитесь, что кончик пальца касается передней выемки отображения вены пальца, и прижмите мякоть пальца к коллектору отпечатка пальца.

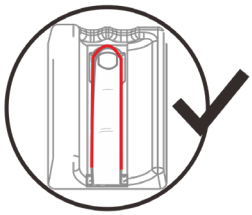


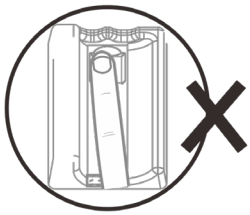


Убедитесь, что кончик пальца касается переднего конца коллектора отображения вен пальцев. В противном случае отображения вен и отпечатков пальцев не могут быть правильно

②



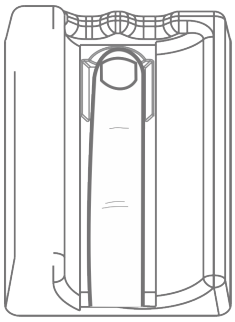


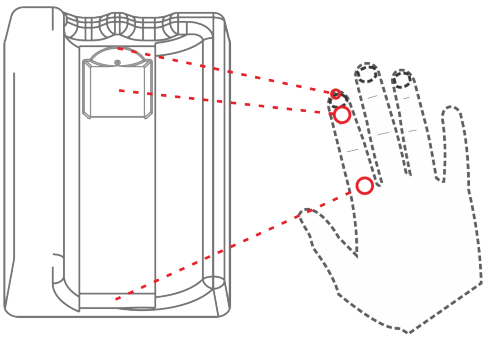


Расположите палец вдоль направляющей, удерживая его посередине так, чтобы мякоть пальца касалась датчика.

Правильные отображения вены и отпечатка пальца не могут быть зафиксированы, если палец наклонен.

③





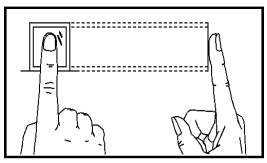
После того, как мякоть пальца соприкасается с датчиком, коллектор начинает собирать отображение вены пальца. Держите палец на месте, пока не услышите звук «Бип», а затем уберите палец.

- Распрямите руку естественно без напряжения.
- Распрямите палец и постарайтесь не сгибать и не поворачивать его.
- Вам не нужно прижимать палец к коллектору с силой.

1.3 Способы прижима отпечатка пальца★

Рекомендуется использовать указательный, средний и безымянный пальцы. Избегайте использования большого и маленького пальцев.

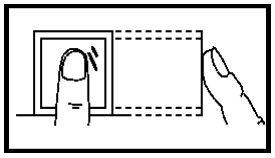
1. Правильная позиция прижима отпечатка пальца



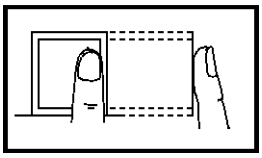
Прижмите палец горизонтально к датчику отпечатка пальца, нацеливаясь на центр датчика.

2. Неправильные позиции прижима отпечатка пальца:

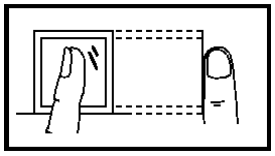
Вертикальная



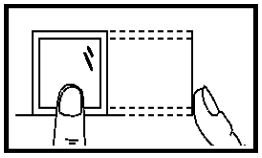
Сбоку



Под углом

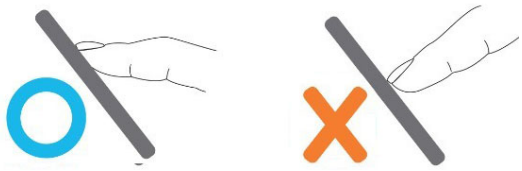


Слишком смещена книзу

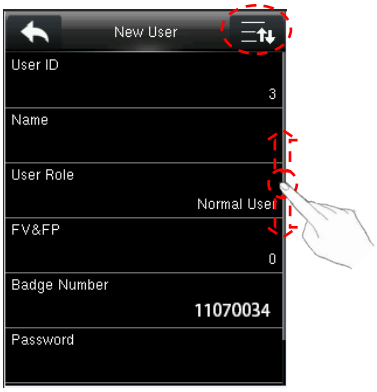


1.4 Использование сенсорного датчика

Вы можете прижать палец к сенсорному экрану или прижать и сдвинуть его, используя мякоть пальца. Прижатие к экрану кончика пальца или ногтя может повредить экран.



Нажмите на , чтобы прокрутить экран вверх или вниз, или перетащите полосу прокрутки справа.



1.5 Режимы верификации

1.5.1 Верификация по венам и отпечаткам пальцев★

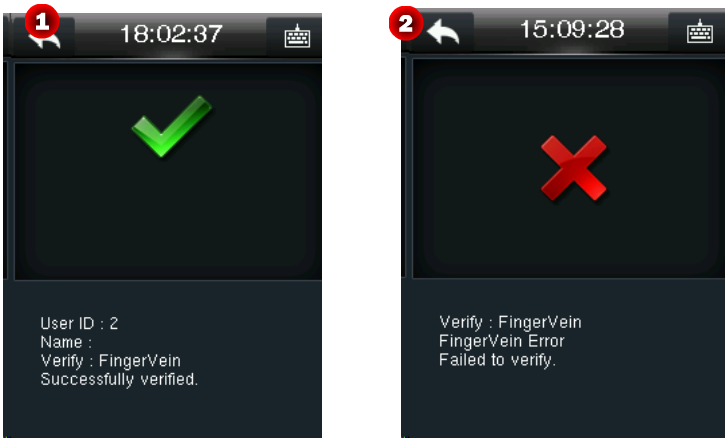
◆ Верификация 1:N

Отображение вен и отпечатков пальца, зарегистрированные коллектором сравниваются с отображениями вен и отпечатков пальцев, хранящихся на устройстве.

1. Устройство автоматически определяет вену пальцев или другие режимы верификации. Когда палец соприкасается с датчиком вены пальца, устройство переходит в режим верификации вены и отпечатка пальца. (Примечание: положение датчика вен см. 1.6.1 «Изображение устройства»).

2. Прижмите палец к коллектору правильно. Для детальной информации см. 1.2 «Режимы регистрации и верификации по венам и отпечатку пальцев».

3. После того, как устройство выдает звук «Бип», уберите палец. Если проверка прошла успешно, устройство воспроизводит голосовую подсказку «Спасибо» и «Верификация прошла успешно» отображается на экране. Если верификация не удалась, устройство воспроизводит голосовую подсказку «Пожалуйста, прижмите палец» и «Верификация не удалась» отображается на экране.



◆ **Верификация 1:1**

Отображение вены пальца и отображение отпечатка пальца, зарегистрированные в настоящее время коллектором, сравниваются с отображением пальца и отображением отпечатка пальца, связанным с идентификатором пользователя, введенным с клавиатуры. Этот режим используется, когда пользователи испытывают трудности при верификации вен на пальцах и отпечатков пальцев.

1. На начальном интерфейсе нажмите , чтобы войти в интерфейс для ввода идентификатора пользователя.

2. Введите идентификатор пользователя и нажмите «ОК» (см. Рис. 2), чтобы войти в интерфейс выбора режима верификации.

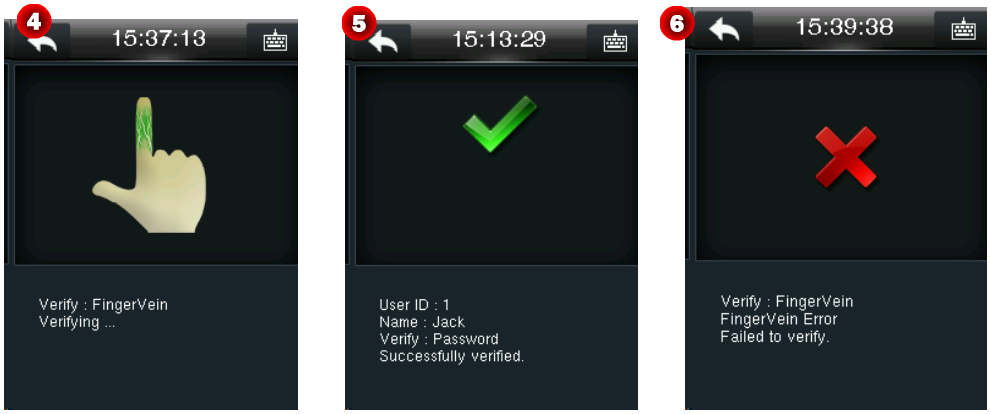
☺**Примечание:** если выдается «Нет данных регистрации», идентификатор пользователя не существует.

3. Нажмите на значок вены пальцев (см. Рис. 3), чтобы войти в интерфейс верификации 1:1 вены пальцев (отпечатков пальцев).



4. Прижмите палец к коллектору правильно. Подробнее см. 1.2 «Режимы регистрации и верификации вен и отпечатков пальцев».

5. После того, как устройство издаст звук «Бип», уберите палец. Если верификация прошла успешно, устройство воспроизводит голосовую подсказку «Спасибо», а «Верификация прошла успешно» отображается на экране (см. Рис. 5). Если верификация не удалась, устройство воспроизводит голосовую подсказку «Пожалуйста, прижмите палец», а «Верификация не удалась» отображается на экране (см. Рис. 6).



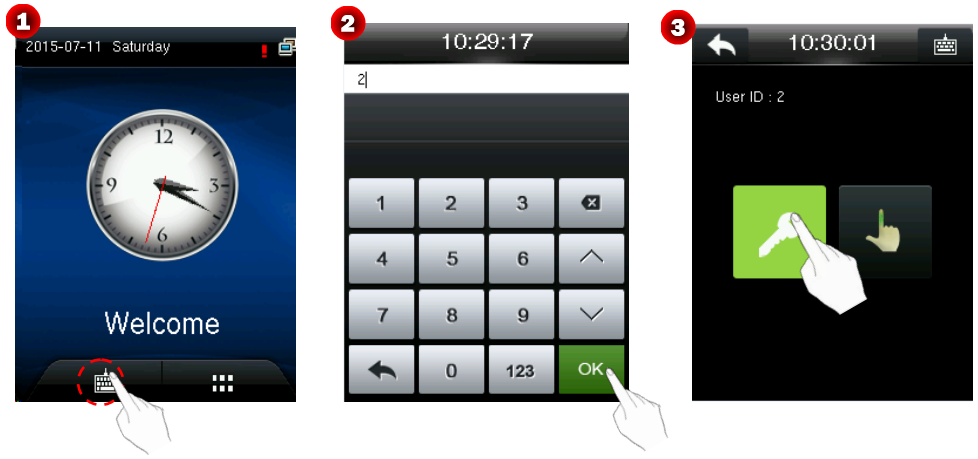
1.5.2 Верификация по паролю

1. На начальном интерфейсе нажмите , чтобы войти в интерфейс для ввода идентификатора пользователя.

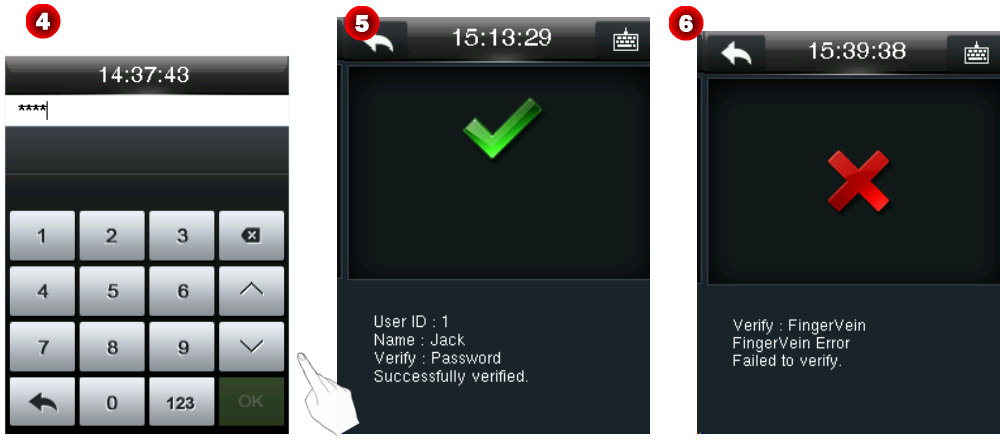
2. Введите идентификатор пользователя и нажмите «OK» (см. Рис. 2), чтобы войти в интерфейс для выбора режима верификации.

☺**Примечание:** если выдается «Нет данных регистрации», идентификатор пользователя не существует.

3. Нажмите значок ключа (см. Рис. 3), чтобы войти в интерфейс верификации по паролю.



4. В появившемся интерфейсе введите пароль и нажмите OK. Если верификация прошла успешно, устройство воспроизводит голосовую подсказку «Спасибо», а «Успешно проверено» отображается на экране. Если верификация не удалась, устройство воспроизводит голосовую подсказку «Неверный пароль», а «Верификация не удалась» отображается на экране.



1.5.3 Верификация по карте★

1. Функция карты является опциональной. Только устройства со встроенными карточными модулями оснащены функцией верификации по карте. Некоторые устройства поддерживают карты Mifare в качестве идентификационных карт.

2. Если верификация прошла успешно, устройство воспроизводит голосовую подсказку «Спасибо», а «Верификация прошла успешно» отображается на экране. Если верификация не удалась, устройство выдает голосовую подсказку «УУ», а «Верификация не удалась» отображается на экране.



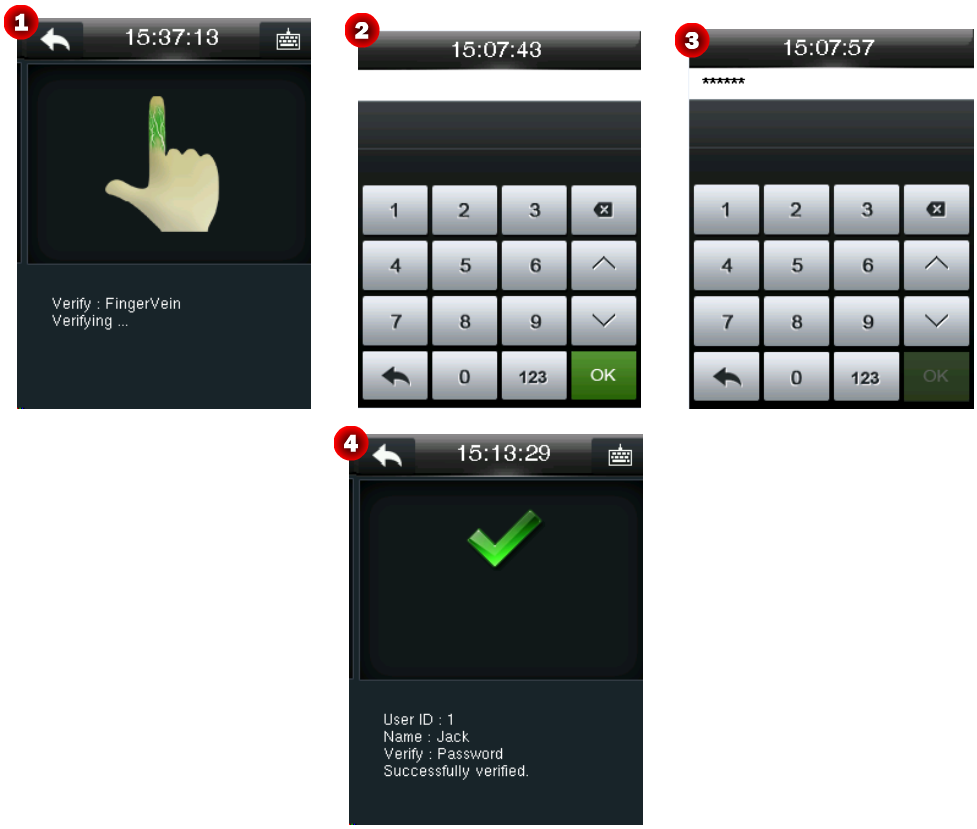
1.5.4 Комбинированная верификация

Устройство поддерживает комбинированную верификацию, например, вену пальца и пароль, при которой устройство должно верифицировать пароль / вену пальца после того, как пользователь пройдет верификацию вен / пальца.

Взять, к примеру, верификацию вены и пароля. Предположим, что пользователь сначала выполняет верификацию вены пальцев.

1. Правильно прижмите палец к коллектору. Подробнее см. 1.2 «Режимы регистрации и проверки вен и отпечатков пальцев».

2. После того, как устройство издаст звук «Бип», уберите палец. После того, как верификация вены / пальца пройдена, отображается интерфейс верификации пароля (см. Рис. 2).



3. Введите правильный пароль и нажмите **OK**. Если верификация успешно прошла и отображается «Верификация прошла успешно» (см. Рис. **4**).

✍**Примечание:** Пользователи могут устанавливать режимы проверки по мере необходимости. Для конкретных операций, см. 9.1 «Параметры контроля доступа».

1.5.5 Комбинированная верификация для разблокировки

✍Примечания:

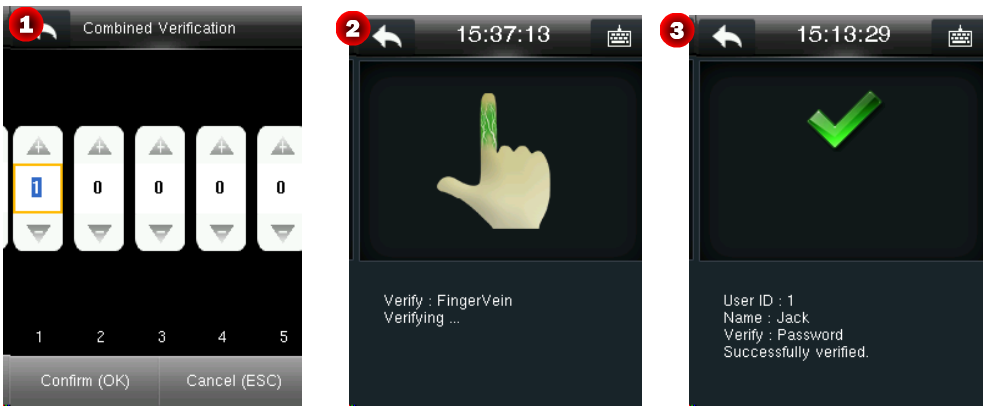
(1) Подробнее о том, как установить комбинированную верификацию для разблокировки, см. в 9.4 «Комбинированные настройки для разблокировки».

(2) В интерфейсе добавления / редактирования пользователя администраторы могут указать группу, к которой принадлежит пользователь, и добавить пользователя в

группу для разблокировки. Подробные способы работы см. В разделе 3.1.7 «Установка уровня контроля доступа».

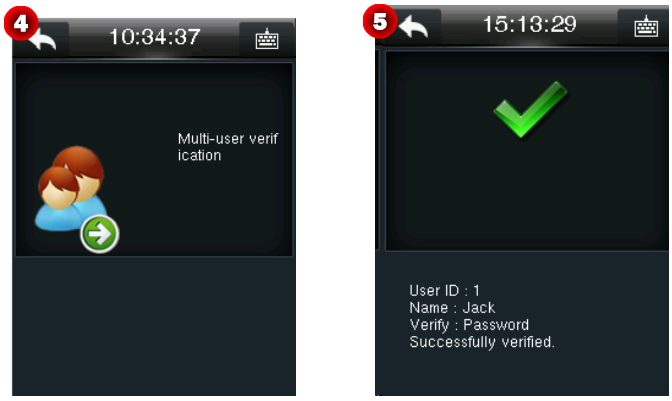
Например, добавьте к комбинации разблокировки, запрашивающей одновременную верификацию группы пользователей 1 и группы пользователей 2 (см. **Рис. 1**), и добавьте пользователей в группы пользователей для разблокировки.

Предположим, что пользователь с идентификатором пользователя 1 принадлежит к группе пользователей 1, а пользователь с идентификатором пользователя 2 принадлежит к группе пользователей 2.



1. Пользователь с идентификатором пользователя 1 правильно нажимает пальцем на коллектор. Подробнее см. 1.2 «Режимы регистрации и проверки вен и отпечатков пальцев».

2. После того, как устройство издаст звук «Бип», уберите палец. После того, как верификация вены пальца прошла (см. Рис. 3), устройство отображает подсказку «Многопользовательская верификация» (см. Рис. 4).



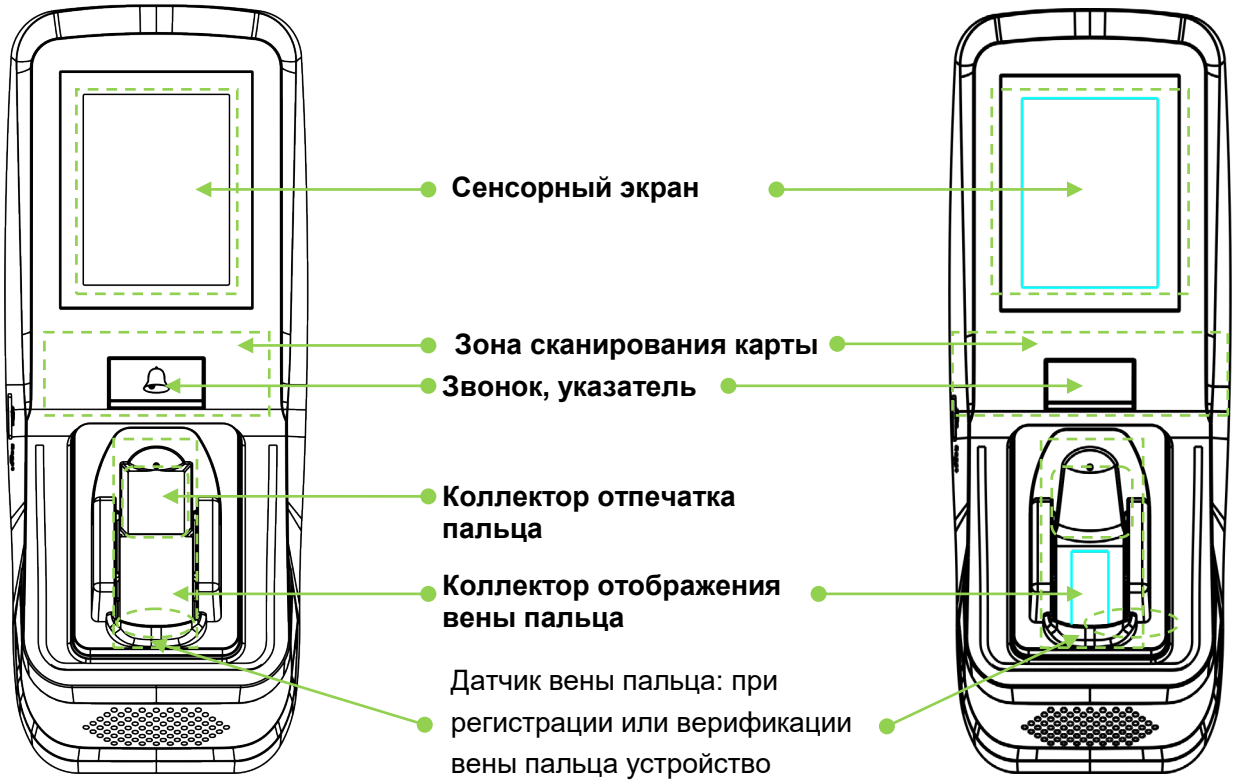
3. Пользователь с идентификатором пользователя 2 прижимает палец к коллектору правильно. После того, как устройство выдает звук «Бип», уберите палец. После успешной верификации на экране отображается «Верификация прошла успешно», а устройство выдает голосовую подсказку «Спасибо».

1.6 Внешний вид устройства и клеммные колодки

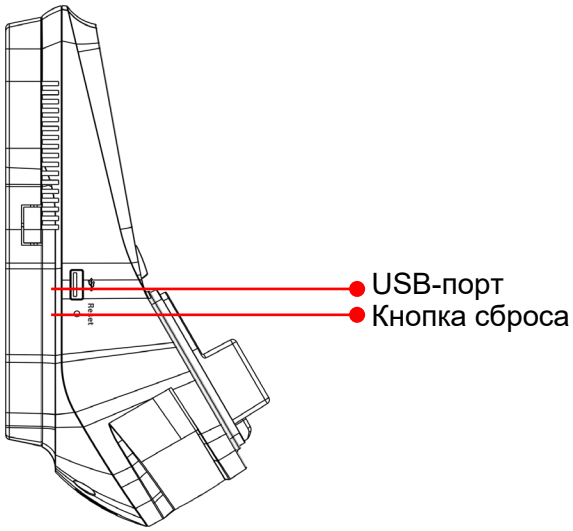
1.6.1 Внешний вид устройства

- Передний вид устройства вен и отпечатков пальца

Передний вид устройства вен пальца

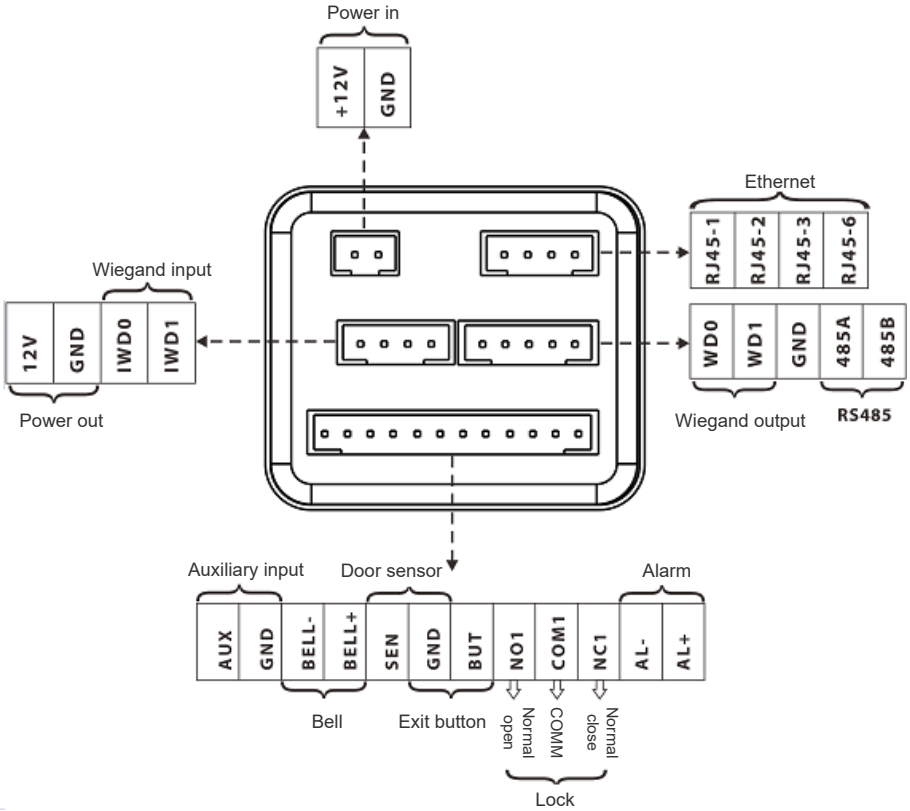


- **Вид сбоку**



Кнопка сброса: после того, как устройство будет включено в течение 30 секунд, нажмите эту кнопку с помощью острого инструмента диаметром менее 2 мм для сброса устройства.

1.6.2 Клеммные колодки

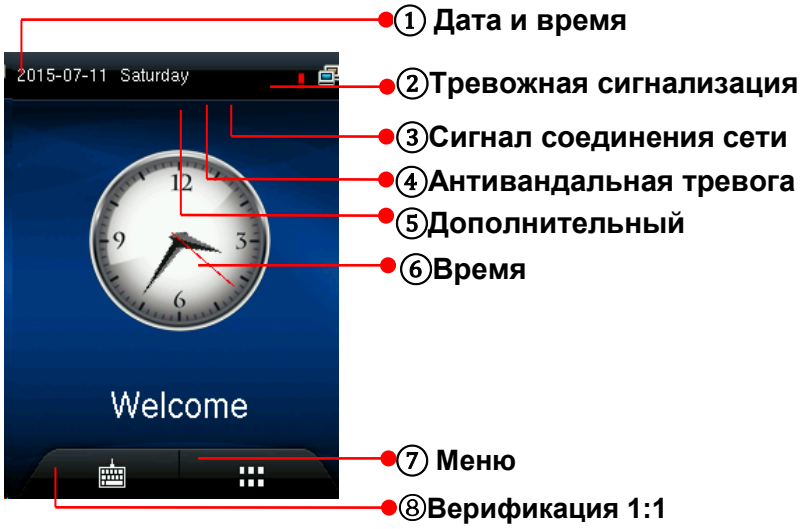


Входная мощность: используйте прилагаемый стандартный адаптер питания. Напряжение питания составляет 12 В постоянного тока, а ток не ниже 3А. Не используйте другой источник питания, чтобы не повредить устройство.

Порт Ethernet: сетевой интерфейс, через который устройство может быть подключено к сетевому оборудованию, такому как коммутатор, маршрутизатор или концентратор.

Вспомогательный входной порт: подключен к дымовой сигнализации для приема сигналов тревоги.

1.7 Начальный интерфейс



① **Дата:** Текущая дата устройства отображается..

②**Тревожная сигнализация:** если отображается этот значок, для устройства устанавливается сигнал тревоги.

③ **Сигнал соединения сети**: отображается состояние сетевого подключения устройства.

④ **Антивандальная тревога:** кнопка тревожной сигнализации о демонтаже активна, если отображается этот значок, а возможной причиной является «неправильная установка» или «неправильный демонтаж».

⑤ **Дополнительный вход:** этот значок отображается, когда клемма вспомогательного входа устройства подключена к вспомогательному устройству и срабатывает условие вспомогательного входа.

⑥**Время:** отображается текущее время устройства. Поддерживаются 12-часовая и 24-часовая системы. Пользователи могут настроить стиль основного интерфейса. Для получения подробной информации смотрите персональные настройки.

⑦**Меню:** нажмите этот значок, чтобы войти в главное меню. Если для устройства установлены администраторы, вы должны пройти проверку администратором, прежде чем получить доступ к главному меню.

⑧**Верификация 1:1 (виртуальная клавиатура):** нажмите клавишу, чтобы войти в интерфейс для ввода идентификатора пользователя в режиме верификации 1:1. После ввода идентификатора пользователя нажмите кнопку ОК и выполните верификацию 1:1 в соответствии с запросами интерфейса.

2. Главное меню

На начальном интерфейсе нажмите , чтобы войти в **Главное меню** (см. **Рис. 2**). Нажмите , чтобы прокрутить экран вниз (см. **Рис. 3**), чтобы отобразить больше содержания. (Примечание: вы можете нажать снова для прокрутки экрана).



В главном меню есть 12 субменю.

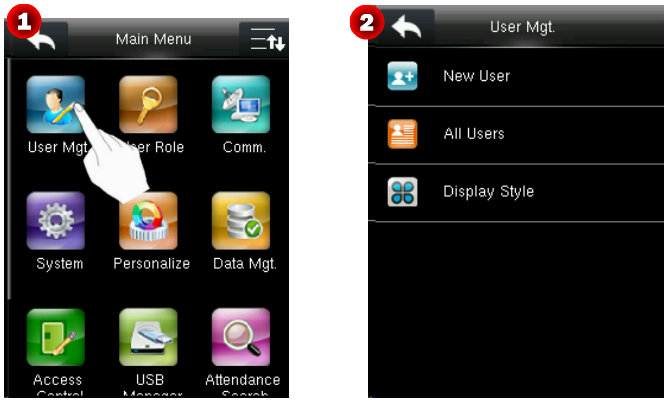
Управление пользователями	Чтобы добавлять пользователей и управлять ими, просматривайте информацию о пользователях (включая идентификаторы пользователей, имена, роли пользователей, отображения вен пальцев, отпечатки пальцев, номера карт★, пароли и уровень контроля доступа) и добавляйте, запрашивайте, изменяйте или удаляйте такую информацию.
Роль пользователя	Установка пользовательских ролей для доступа к меню и изменения настроек.
Связь	Для установки соответствующих параметров связи между устройством и ПК, включая параметры Ethernet, такие как IP-адрес и т. д., последовательную связь, соединение с ПК и настройки Wiegand.

Система	Для установки параметров системы и обновления прошивки, включая время, записи контроля доступа, параметры вен и отпечатков пальцев, а также восстановление заводских настроек, чтобы устройство максимально соответствовало требованиям пользователя в отношении функций и отображения.
Персонализация	Включает в себя отображение интерфейса, голос, звонок, режим клавиши состояния сканирования и настройки сочетаний клавиш быстрого вызова.
Управление данными	Для удаления данных учета рабочего времени, всех данных, роли супер-администратора или заставки и т. д.
Контроль доступа	Для настройки параметров управления замками и настройки параметров устройств контроля доступа, в том числе параметров контроля доступа, правил времени, праздников, комбинированной разблокировки и запрета двойного прохода.
Менеджер USB	Для передачи данных, таких как пользовательские данные и журналы событий с USB-диска на вспомогательное программное обеспечение или другие устройства.
Поиск событий учета рабочего времени	Для запроса записей, сохраненных в устройстве после успешной верификации.
Автоматическое тестирование	Для автоматического тестирования различных функций модуля, включая ЖК-дисплей, голос, клавиатуру, датчик отпечатков пальцев, камеру ★ и проверку часов RTC.
Информация о системе	Для проверки емкости устройства, информации об устройстве и прошивке.

Когда администратор не установлен, любой может получить доступ к главному меню, нажав  . После того, как администратор установлен, пользователь должен пройти верификацию личности администратором перед входом в меню. В целях безопасности рекомендуется зарегистрировать администратора при первом использовании устройства.

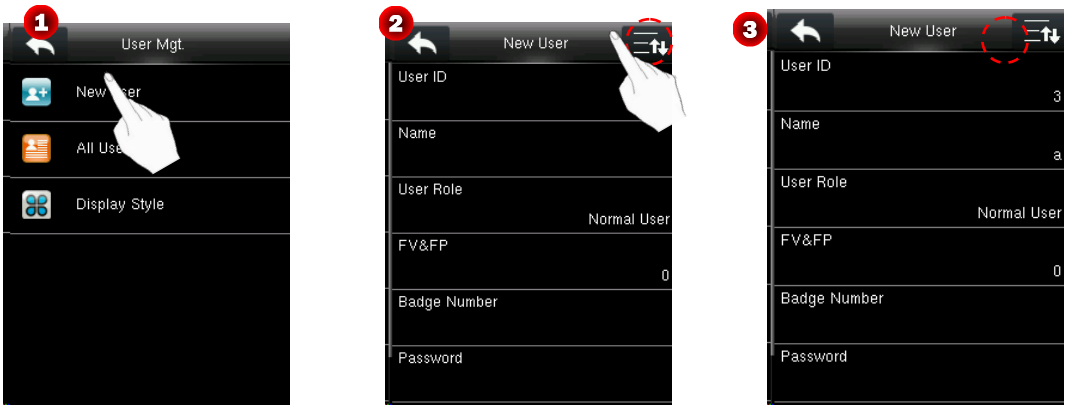
3. Управление пользователями

Основная информация о пользователях, зарегистрированная на устройстве, включает в себя идентификаторы пользователей, имена, роли пользователей, отображения вен и отпечатков пальцев★, пароли, номера карт★ и уровень контроля доступа. Такая информация может быть изменена в связи с кадровыми изменениями, поэтому устройство поддерживает операции добавления, удаления, запроса и изменения.



3.1 Добавление пользователей

На интерфейсе **Управ. польз.** нажмите **Новый пользователь**, чтобы войти в интерфейс «Новый пользователь», и нажмите , чтобы прокрутить экран вниз, чтобы отобразить больше содержания. (Примечание. Вы можете нажать еще раз, чтобы прокрутить экран вверх).



Идентификатор пользователя: Введите идентификатор пользователя. По умолчанию поддерживаются цифры 1-9.

Имя: введите имя пользователя. По умолчанию поддерживаются 1-24 символа. Один китайский иероглиф занимает два символа.

Роль пользователя: установить роль пользователя. Значением по умолчанию является **Обычный пользователь**. Вы можете выбрать **Суперадминистратора**. Обычный пользователь может только использовать верификацию по венам пальцев, отпечаткам пальцев★, карте★ или паролю, пока администратор обладает всеми функциями нормального пользователя и доступ в главное меню.

Регистрация по венам и отпечаткам пальца★: Зарегистрировать вены и отпечатки пальца. Указательный и средний пальцы рекомендуются.

Пароль: Зарегистрировать пароль. По умолчанию поддерживаются цифры 1-8.

Номер карты★: Зарегистрировать номер карты.

Уровень контроля доступа: Установить уровень контроля доступа пользователя.

3.1.1 Ввод идентификатора пользователя

Устройство автоматически присваивает идентификаторы пользователей пользователям, начиная с 1. Если вы используете назначенный устройству номер, пропустите этот шаг.

1. В интерфейсе **Новый пользователь** нажмите **Идентификатор пользователей**.



😐 **Совет: Зарегистрированный идентификатор пользователя не может быть изменен.**

2. На отображаемом интерфейсе введите идентификатор пользователя, который нужно зарегистрировать, и нажмите кнопку «ОК», чтобы сохранить настройку и вернуться в интерфейс **Новый пользователь**. Если отображается «Идентификатор пользователя существует!», это означает, что идентификатор пользователя был использован. Пожалуйста, введите другой идентификатор.

😐**Совет: по умолчанию поддерживаются идентификаторы пользователей от 1 до 9 цифр. Чтобы увеличить число цифр, проконсультируйтесь с нашими представителями бизнеса или предпродажной службой технической поддержки.**

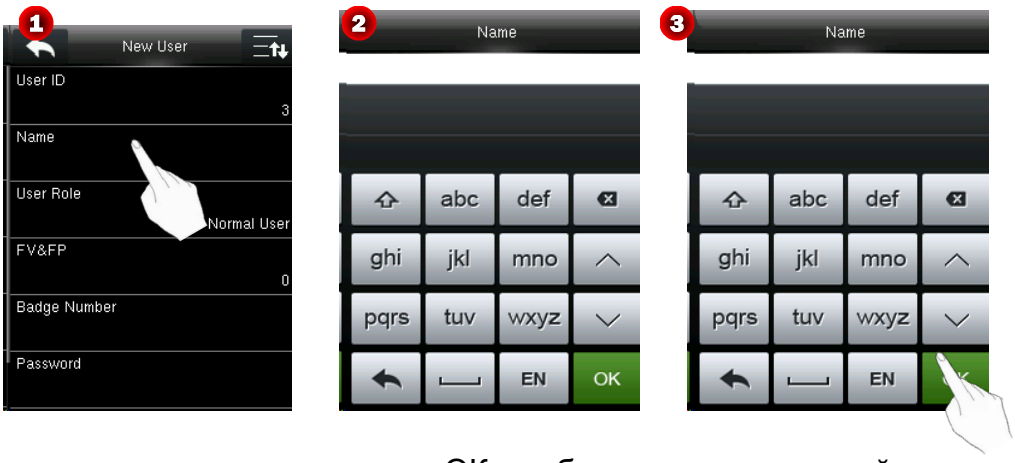
3.1.2 Ввод имени

Ввести имя пользователя с использованием способа ввода T9 через клавиатуру.

1. В интерфейсе нового пользователя нажмите «Имя».

2. В отображаемом интерфейсе введите имя пользователя для регистрации. Нажмите слова, чтобы выбрать их.

Для операций с интерфейсом клавиатуры см. Приложение 1 Инструкции по вводу текста.



3. После ввода имени нажмите кнопку OK, чтобы сохранить настройку и вернуться в интерфейс Новый пользователь. Если вы нажмете , устройство вернется к интерфейсу верхнего уровня без сохранения информации.

Советы: по умолчанию поддерживаются имена из 1-24 символов. Один китайский иероглиф занимает два символа.

3.1.3 Роль пользователя

Устройство поддерживает две роли пользователя: **Обычный пользователь** и **Суперадминистратор**.

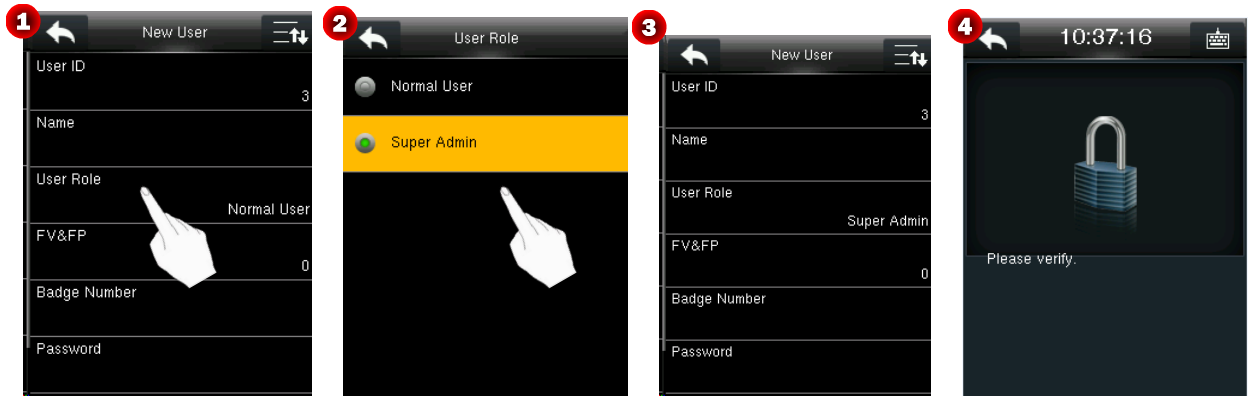
Суперадминистратор: Суперадминистратор может выполнять операции со всеми меню.

Обычный пользователь: если установлен администратор, обычный пользователь может использовать только вену пальца (отпечатки пальцев★), пароли или карты★ для верификации. Когда администратор не установлен, обычному пользователю разрешено выполнять операции со всеми меню.

Прописываемая роль пользователя: после того, как суперадминистратор установлен, вы можете прописать роли в **Роли пользователя** и прописать права на операции в меню для ролей. Прописываемые роли пользователей обладают всеми правами обычного пользователя, то есть верификацией по венам пальца (отпечаткам пальца★), паролем и картой.

указывает, что текущий пользователь является администратором.

1. На интерфейсе **Новый пользователь** нажмите **Роль пользователя**.



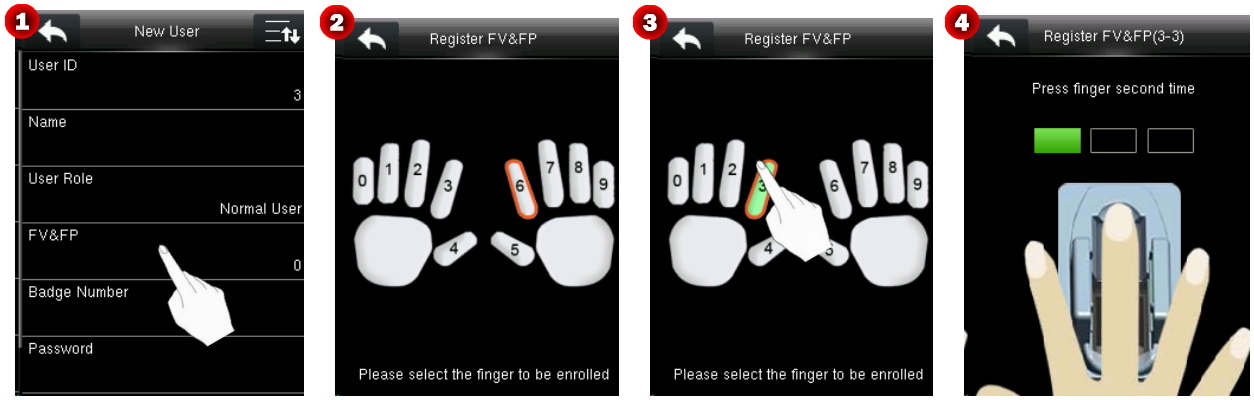
2. Выберите роль по мере необходимости. Затем устройство возвращается к интерфейсу **Новый пользователь**.

✍**Примечание**: после добавления суперадминистратора вам необходимо пройти верификацию суперадминистрирования, прежде чем получить доступ к главному меню.

3.1.4 Регистрация вены и отпечатка пальца

✍ Примечание: при регистрации вены пальца устройство также регистрирует отпечаток пальца выбранного пальца.

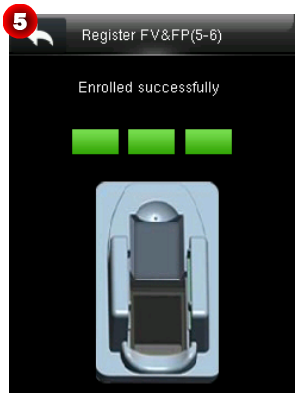
1. В интерфейсе **Новый пользователь** нажмите **FV & FP**, чтобы войти в интерфейс **Зарегистрировать FV & FP** (см. Рис. 2).

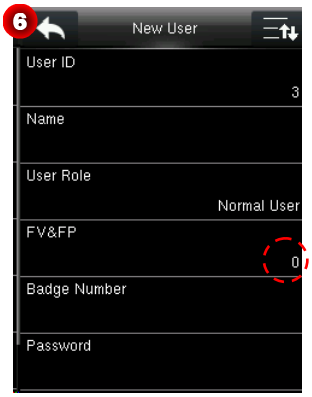


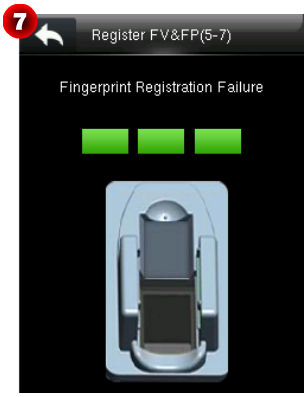
2. На отображаемом интерфейсе прижмите палец, чтобы зарегистрировать вену и отпечаток пальца (см. Рис. 3).

3. Правильно прижмите один и тот же палец к коллектору три раза подряд в соответствии с инструкциями на устройстве (см. Рис. 4). Подробнее см. 1.2 «Режимы регистрации и проверки вен пальцев».

После того, как вены и отпечаток пальца были успешно зафиксированы три раза, на экране отображается «Зарегистрировано успешно» (см. Рис. 5), и устройство возвращается в интерфейс нового пользователя, отображающий количество зарегистрированных вен и отпечатков пальцев (см. Рис. 6). Если регистрация не удается, на экране отображается «Ошибка регистрации отпечатка пальца» (см. Рис. 7). Чтобы продолжить регистрацию, повторите шаги 2 и 3.







✍**Примечания:**

(1) Во время регистрации вен и отпечатка пальца звук «Бип», генерируемый коллектором, указывает на то, что единственная регистрация прошла успешно.

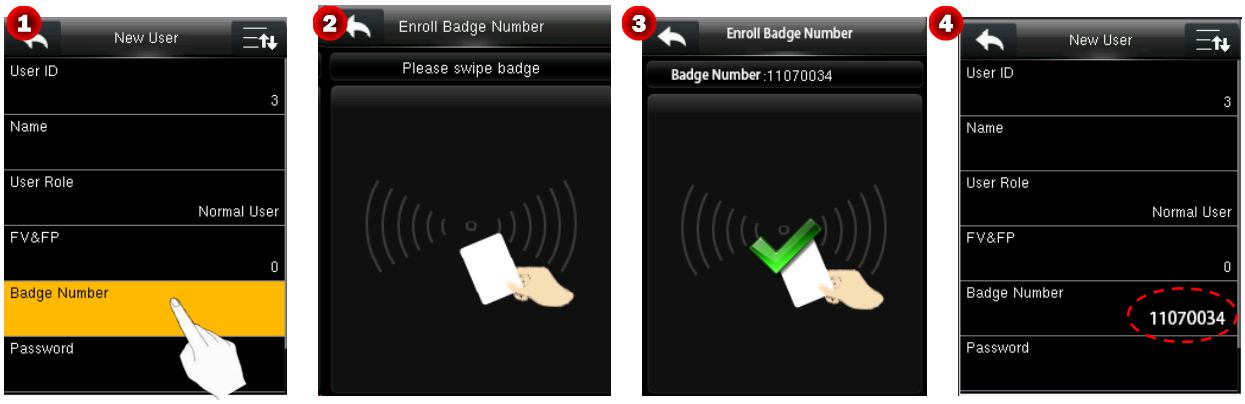
(2) Для лучшей фиксации вен и отпечатков пальцев, убирайте палец после успешной регистрации каждый раз (после генерации звука «Бип») и продолжайте регистрацию, снова нажимая палец в соответствии с инструкциями.

3.1.5 Регистрация номера карты★

1. В интерфейсе **Новый пользователь** нажмите **Номер карты**, чтобы войти в интерфейс **Зарегистрировать номер карты** (см. **Рис. 2**).

2. Просканируйте карту в зоне сканирования. Подробнее о зоне сканирования карт см. отметку в разделе 1.6.1 «Внешний вид устройства».

3. После успешного считывания карты отображается номер карты (см. **Рис. 3**), и устройство возвращается в интерфейс **Новый пользователь** (см. **Рис. 4**).



☺**Примечание**: некоторые устройства поддерживают карты Mifare в качестве идентификационных карт.

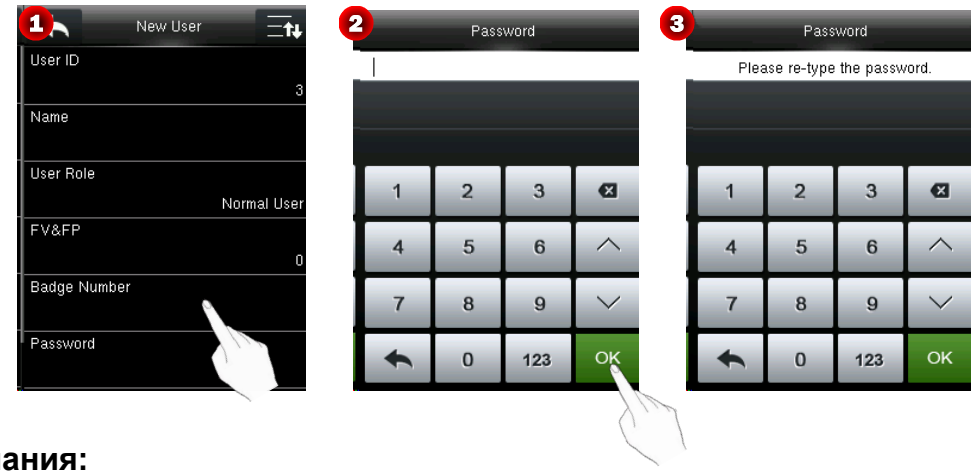
3.1.6 Регистрация пароля

1. На интерфейсе **Новый пользователь** нажмите **Пароль**.

2. На отображаемой клавиатуре интерфейса введите пароль и нажмите **OK** (см. **Рис. 2**).

😐**Совет**: По умолчанию поддерживаются 1-8 цифр.

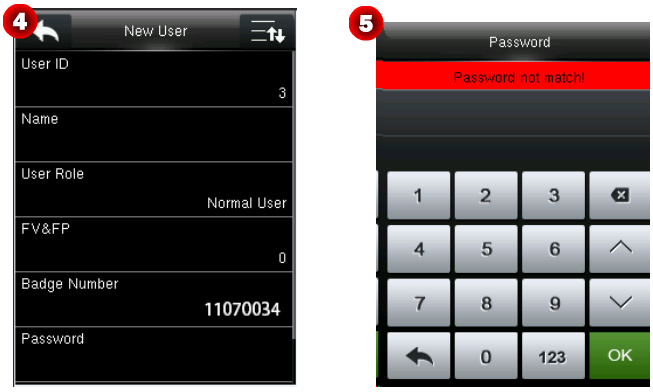
3. Повторно введите пароль в соответствии с инструкциями и нажмите **OK**, чтобы сохранить пароль (см. **Рис. 3**). После успешного сохранения пароля устройство возвращается в интерфейс нового пользователя (см. **Рис. 4**).



✍**Примечания:**

(1) Пароли, введенные в шагах 2 и 3, должны быть одинаковыми. В противном случае отображается окно подсказки (см. **Рис. 5**).

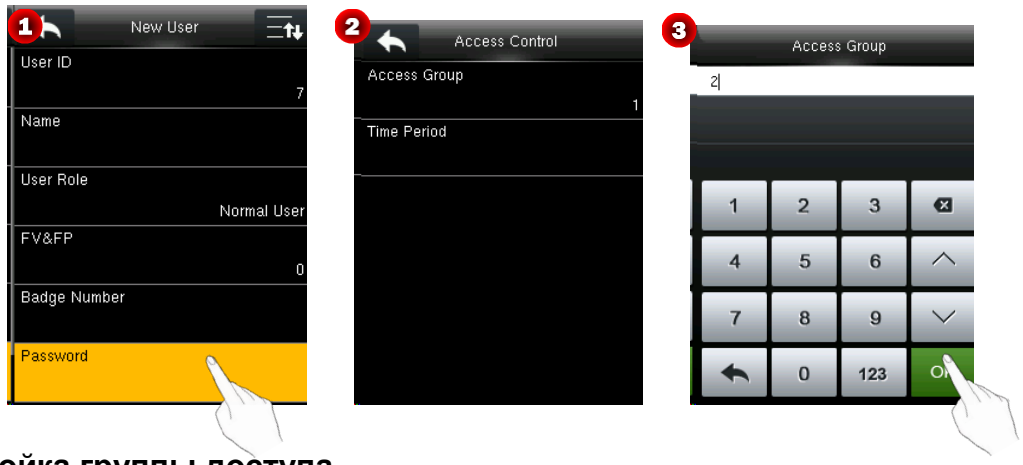
(2) Если вы введете неодинаковый пароль, вам нужно вернуться к шагу 2 и ввести его снова.



3.1.7 Настойка уровня контроля доступа

На интерфейсе **Новый пользователь** нажмите **Контроль доступа**, чтобы войти в интерфейс **Контроль доступа** (см. **Рис. 2**).

Уровень контроля доступа используется для установки уровня открытия двери для каждого пользователя, включая группу доступа и правила периода времени действия.



- **Настройка группы доступа**

Установите группу доступа, к которой относится пользователь, для обеспечения настроек комбинации разблокировки. Допустимый номер группы варьируется от 0 до 99999999.

(1) В интерфейсе **Контроль доступа** нажмите **Группа доступа**.

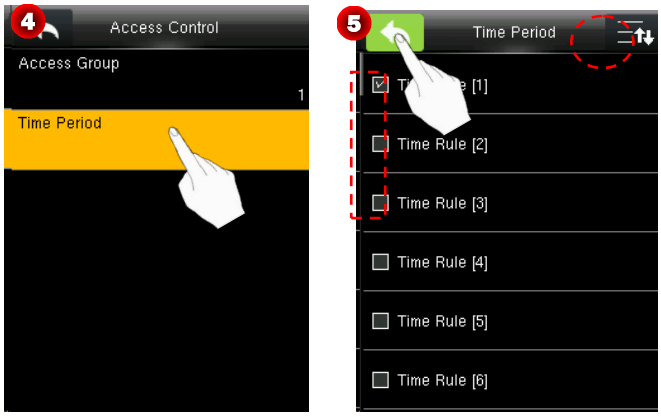
(2) Введите номер группы, к которой относится пользователь, и нажмите кнопку **ОК** (см. **Рис. 3**), чтобы сохранить настройки и вернуться в интерфейс **Контроль доступа**.

- **Установка периода времени действия**

Выберите правила времени действия для пользователя. Правила времени устанавливаются в меню «Контроль доступа» и поддерживаются не более 50 правил времени. Период времени действия открытия двери пользователя представляет собой сумму выбранных правил времени.

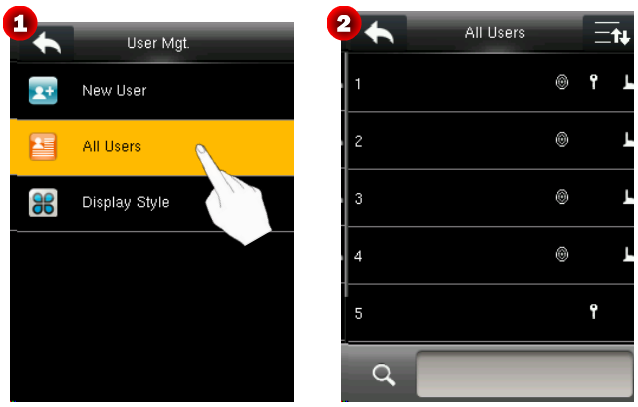
(1) В интерфейсе **Контроль доступа** нажмите **Период времени**, чтобы войти в интерфейс **Период времени** (см. **Рис. 4**). Нажмите , чтобы прокрутить экран вверх или вниз, чтобы отобразить больше содержания.

(2) В списке правил времени нажмите и выберите правило времени (допускается несколько вариантов выбора, а символ ☑ указывает, что выбрано правило времени), и нажмите (см. **Рис. 5**), чтобы сохранить настройки и вернуться к предыдущему интерфейсу.



3.2 Все пользователи

На интерфейсе **Управ. пользователями** нажмите **Все пользователи**, чтобы войти в интерфейс **Все пользователи** (см. **Рис. 2**). Администратор может запрашивать, редактировать или удалять пользователей.



: указывает, что текущий пользователь является суперадминистратором.

: указывает, что отпечаток пальца пользователя зарегистрирован ★.

: указывает, что номер карты пользователя зарегистрирован ★.

: указывает, что пароль пользователя зарегистрирован.

: указывает, что вена пальца пользователя зарегистрирована.

Совет: информация всех зарегистрированных пользователей отображается в соответствии с предустановленным стилем отображения. Подробнее о стиле отображения см. 3.3 «Стиль отображения».

3.2.1 Запрос пользователя

Вы можете запрашивать пользователей по имени или идентификатору пользователя. Подробная операция выглядит следующим образом:

1. Нажмите по полю запроса (см. **Рис. 1**), чтобы войти в интерфейс, показанный на **Рис. 2**.

2. Введите условие запроса, нажмите OK (см. **Рис. 3**), чтобы вернуться к интерфейсу **Все пользователи**. Информация о соответствующем пользователе отображается в соответствии с условием запроса (см. **Рис. 4**).

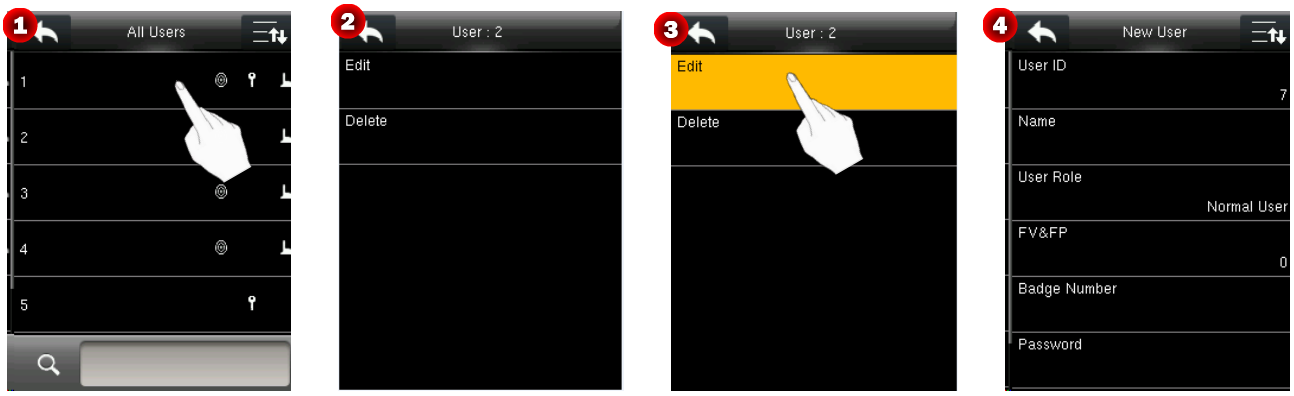


3.2.2 Редактирование / удаление пользователя

В интерфейсе **Все пользователи** нажмите пользователя (см. **Рис. 1**), чтобы войти в интерфейс, показанный на Рис. 2.

- **Редактирование пользователя**

Нажмите **Редактировать** (см. Рис. 3), чтобы войти в интерфейс **Новый пользователь** (см. Рис. 4).



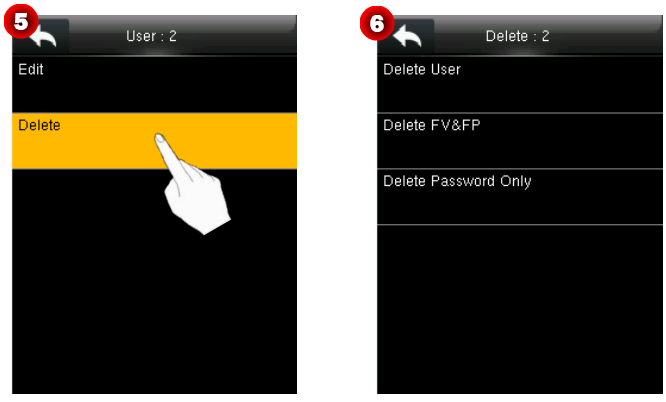
2. Измените информацию о пользователе и нажмите , чтобы сохранить настройки и вернуться к предыдущему интерфейсу.

Примечание. Метод редактирования пользователя такой же, как и при добавлении пользователя, и здесь он не описан.

- **Удаление пользователя**

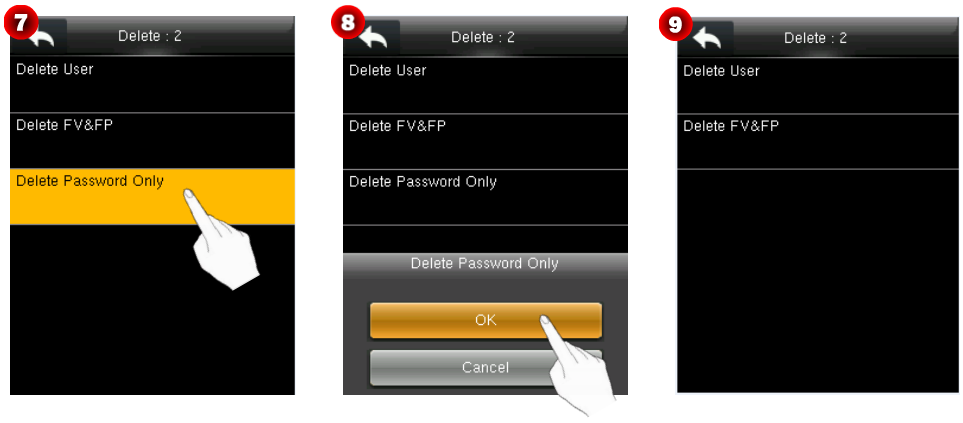
1. Нажмите **Удалить** (**Рис. 5**), чтобы войти в интерфейс, показанный на **Рис. 6**. Элементы операций отображаются в соответствии с зарегистрированной информацией.

Пример: если пароль пользователя не зарегистрирован, пункт **Удалить только пароль** не отображается.



Далее в качестве примера используется **Удалить только пароль**. Операция описана ниже.

2. Нажмите **Удалить только пароль** (см. **Рис. 7**), и появится диалоговое окно (см. **Рис. 8**).



3. Нажмите **OK**, чтобы удалить все **Пароли**, или нажмите **Отменить**, чтобы отменить операцию.

✍ **Примечание**:

(1) При удалении пользователя устройство удаляет всю информацию о пользователе, включая вену пальца, отпечаток пальца ★, пароль и номер карты ★.

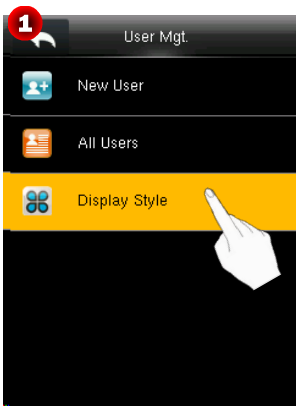
(2) При удалении только роли пользователя устройство меняет роль пользователя на **Обычного пользователя**.

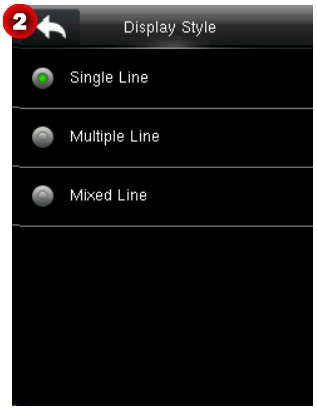
(3) После удаления роли последнего суперадминистратора все пользовательские роли становятся недоступными.

3.3 Стиль отображения

1. На интерфейсе **Управ. пользователями** нажмите **Стиль отображения**, чтобы войти в интерфейс **Стиль отображения,** показанный на **Рис. 2**.

😐**Совет**: стиль отображения по умолчанию - **Однострочный**.

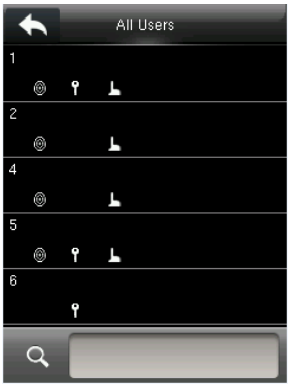




2. В интерфейсе **Стиль отображения** вы можете выбрать **Однострочный**, **Многострочный** или **Смешанная линия** ряд для отображения информации о пользователе.



Однострочный



Многострочный



Смешанная линия

4. Роль пользователя

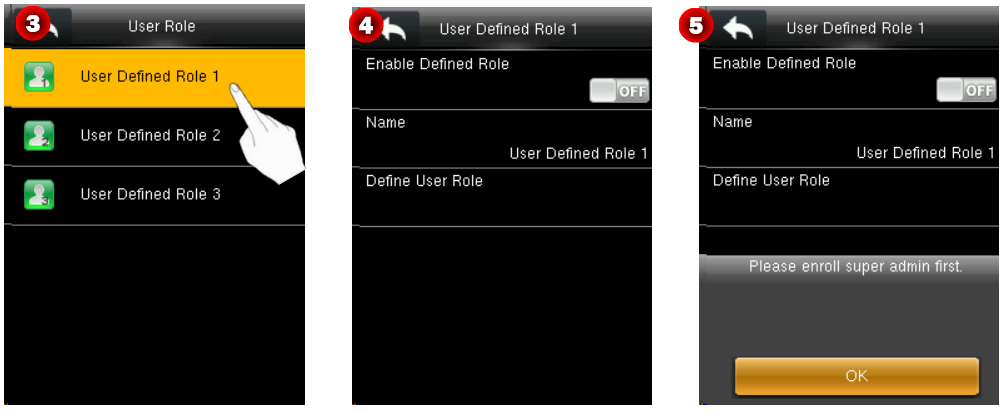
Вы можете установить пользовательские роли и прописывать уровни операций для ролей в Роли пользователя.



Прописываемая пользователю роль устанавливаются следующим образом:

В списке **Роль пользователя** выберите роль, которую нужно отредактировать (см. **Рис. 3**), чтобы войти в интерфейс **Прописываемая пользователю роль** (см. **Рис. 4**).

✍ **Примечание**: Пользовательские роли могут быть установлены только после добавления суперадминистратора. В противном случае отображается диалоговое окно, показанное на **Рис. 5**.



- **Включить прописываемую роль**

Значение по умолчанию - OFF, что означает роль отключена. Нажмите и перетащите значок для переключения между ON и OFF. Значок ON означает, что роль включена.

- **Имя**

Установите имя для роли. Нажмите **Имя**, чтобы войти в интерфейс **Имя** (см. **Рис**. **7**). Введите имя, используя метод ввода T9, и нажмите **OK** (см. **Рис**. **8**), чтобы сохранить настройки и вернуться к предыдущему интерфейсу (см. **Рис**. **9**).

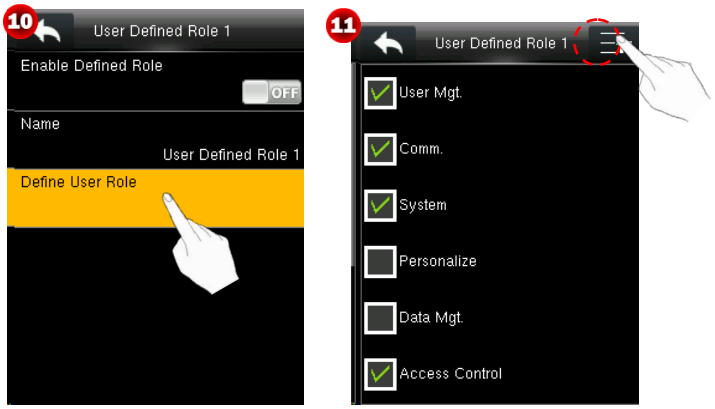
Для получения подробной информации о том, как ввести имя, см. Приложение 1 Инструкции по вводу текста.



- **Прописать роль пользователя**

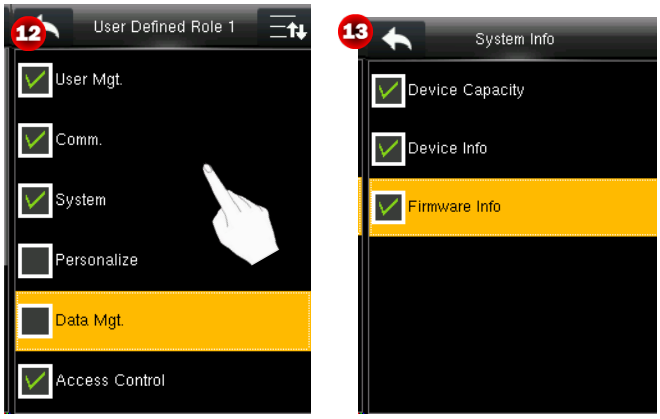
Чтобы прописать уровень операции для роли, выполните следующие действия:

1. Нажмите **Прописать роль пользователя**, чтобы войти в интерфейс, показанный на **Рис. 11**, и нажмите , чтобы прокрутить экран вниз, чтобы отобразить больше содержания.



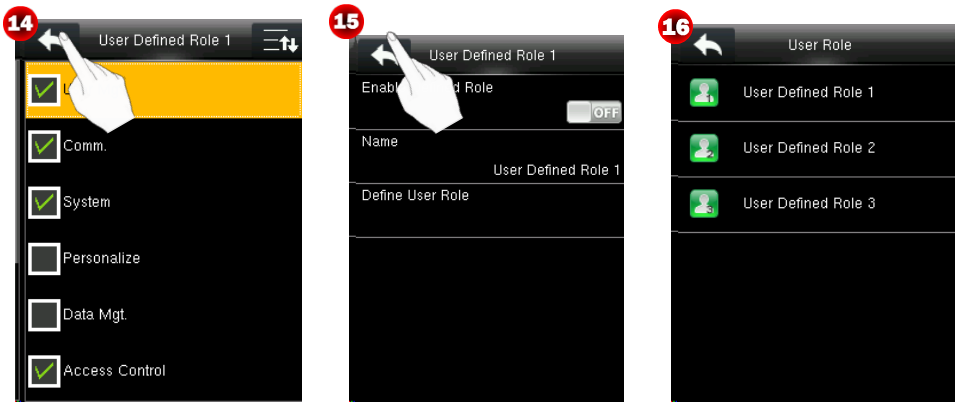
2. Пропишите операционные уровни для роли (символ ☑ указывает, что элемент выбран).

😐Советы: нажмите на родительском уровне (см. **Рис. 12**), чтобы войти в интерфейс выбора дочернего уровня (см. **Рис. 13**).



3. После настройки нажмите (см. **Рис. 14**), чтобы сохранить настройки и вернуться к интерфейсу **Прописанная пользователю роль**.

4. На интерфейсе **Прописанная пользователю роль** нажмите (см. **Рис. 15**) чтобы сохранить настройки и вернуться к интерфейсу **Роль пользователя**.



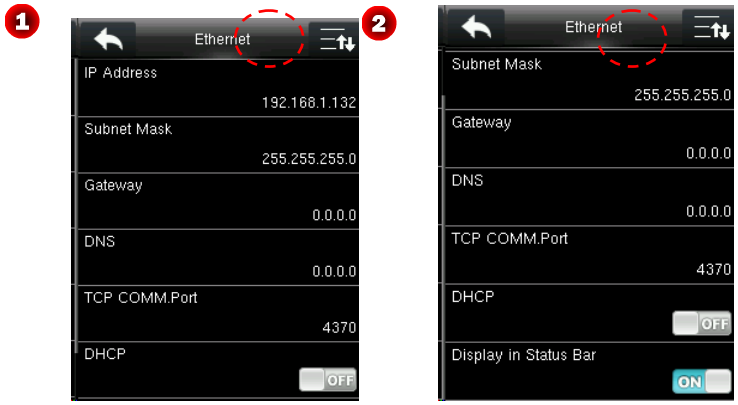
5. Настройки связи



Установите параметры для связи устройства и ПК, включая IP-адрес, шлюз, маску подсети, скорость передачи, номер устройства и пароль подключения

5.1 Настройки Ethernet

На интерфейсе **Связь**, нажмите **Ethernet**, чтобы войти в интерфейс **Ethernet**, и нажмите  , чтобы прокрутить экран вниз, чтобы отобразить больше содержания. (Примечание. Вы можете нажать  еще раз, чтобы прокрутить экран вверх).



Приведенные ниже параметры являются заводскими значениями по умолчанию, пожалуйста, отрегулируйте их в соответствии с реальной ситуацией в сети.

IP-адрес: 192.168.1.201

Маска подсети: 255.255.255.0

Шлюз: 0.0.0.0

DNS: 0.0.0.0

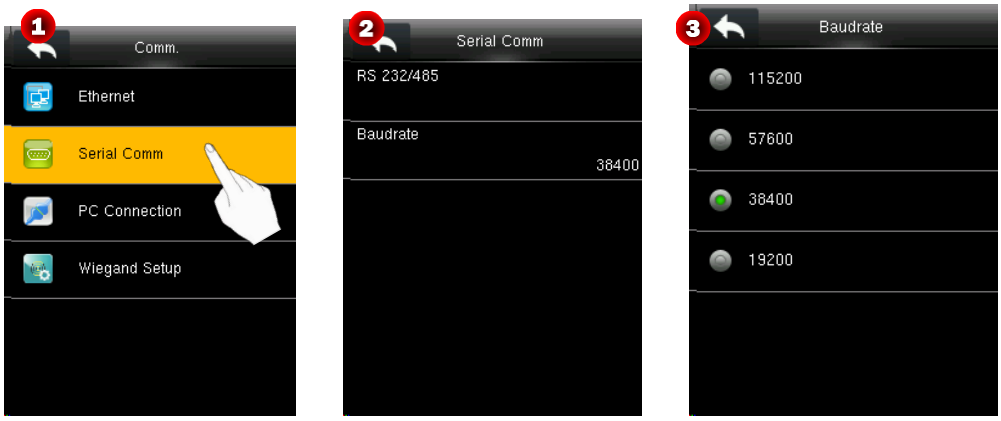
TCP COMM. Порт: 4370

DHCP: протокол динамической конфигурации хоста, который предназначен для динамического распределения IP-адресов для клиентов через сервер.

Отображать в строке состояния: установить, отображать ли значок сети в строке состояния.

5.2 Настройки последовательной связи

Нажмите **Последовательная связь**, чтобы войти в интерфейс **Последовательная связь**.



Когда устройство обменивается данными с ПК в последовательном режиме, проверьте следующие параметры.

RS232 / 485: активировать ли RS485 для связи. Значением по умолчанию является ON. Вы можете нажать **RS485** для переключения между OFF и ON.

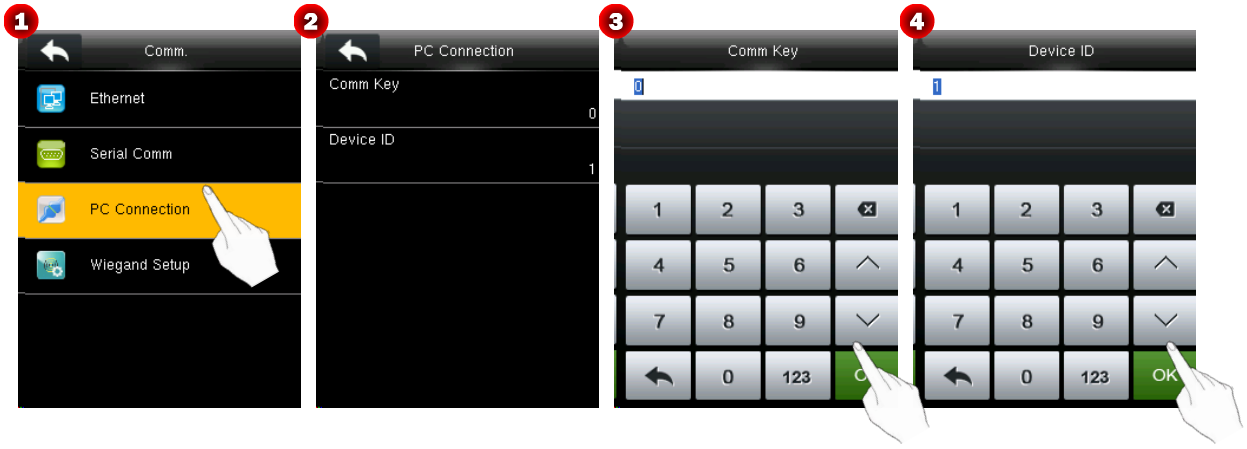
Скорость передачи данных: скорость связи с ПК; Существует 5 вариантов скорости передачи: 115200 (по умолчанию), 57600, 38400 и 19200. Чем выше скорость передачи, тем выше скорость связи, но при этом она менее надежна. Как правило, более высокая скорость передачи может использоваться, когда расстояние связи

короткое; когда расстояние связи большое, выбор более низкой скорости передачи данных будет более надежным.

5.3 Подключение ПК

Для повышения безопасности данных необходимо установить Ключ связи для связи между устройством и ПК.

Если в устройстве установлен Ключ связи, необходимо ввести правильный пароль подключения, когда устройство подключено к программному обеспечению ПК, чтобы устройство и программное обеспечение могли обмениваться данными.



- **Настройки Ключа связи**

Ключ связи: Пароль по умолчанию - 0 (отсутствие пароля). Войдите в интерфейс **Ключ связи**, введите пароль, нажмите **OK** (**Рис. 3**), чтобы сохранить настройки и вернуться в интерфейс **Подключения ПК**.

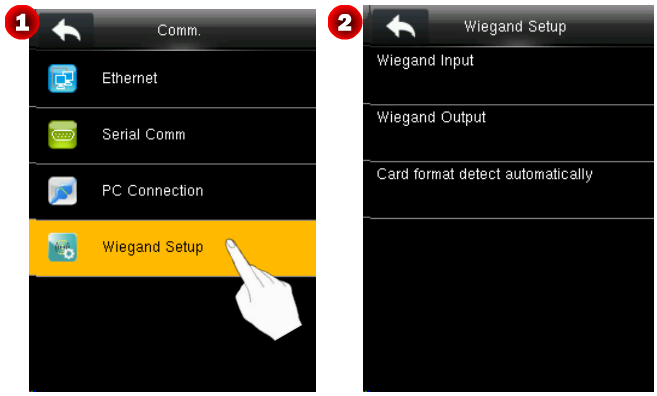
✍ Примечание: **Ключ связи** может состоять из 1-6 цифр и находится в диапазоне 0-999999.

- **Настройки идентификатора устройства**

Установите идентификатор устройства. Значение по умолчанию - 1. Нажмите **Идентификатор устройства**, чтобы войти в интерфейс **Идентификатор устройства**, введите идентификатор и нажмите **OK** (см. **Рис. 4**), чтобы сохранить настройки и вернуться к интерфейсу подключения ПК.

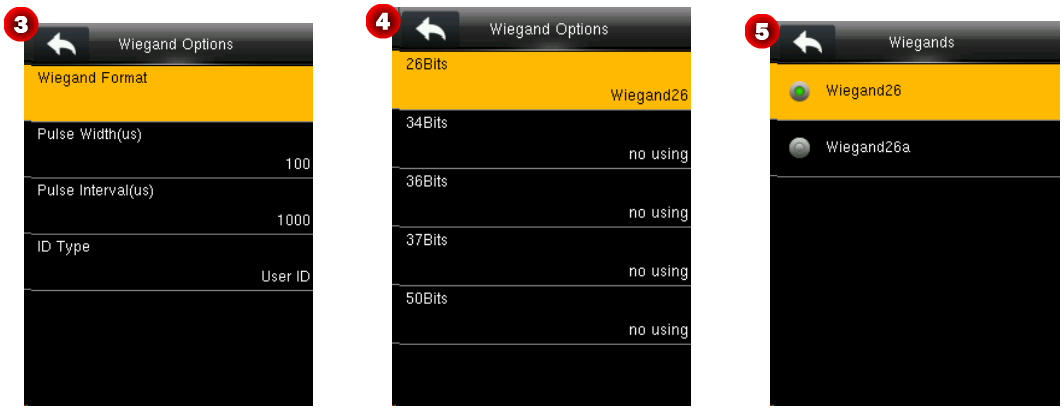
✍ **Примечание**: Идентификационный номер устройства варьируется от 1 до 254. Для последовательной связи RS235 идентификационный номер устройства необходимо ввести в программном интерфейсе связи.

5.4 Установка Wiegand



5.4.1 Вход Wiegand

Установите формат Wiegand внешнего считывателя.



Формат Wiegand: Пользователь может выбрать один из следующих встроенных форматов Wiegand: Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a, и Wiegand 50.

Отсутствие использования. Значение отсутствие использования означает, что формат с этим битовым номером не используется. В следующей таблице описаны все форматы.

Ширина импульса (мкс): ширина импульса, посылаемая Wiegand. Значение по умолчанию составляет 100 микросекунд, которые можно регулировать в диапазоне от 20 до 100 микросекунд.

Импульсный интервал (мкс): значение по умолчанию составляет 1000 микросекунд, которые можно регулировать в диапазоне от 200 до 20000 микросекунд.

Тип идентификатора: входной контент, включенный во входной сигнал Wiegand. Могут быть выбраны **Идентификатор пользователя** или **Номер карты**.

Определение форматов Wiegand:

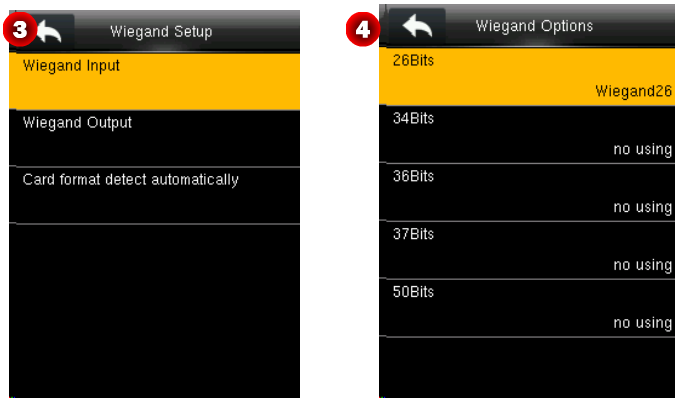
Формат Wiegand	**Определение**
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCC Состоит из 26 бит двоичных чисел, причем 1-й бит является битом четной проверки четности для 2-13-го битов, а бит 26 является битом нечетной проверки четности для 14-25-го битов, а 2-15-й биты являются номером карты.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCC Состоит из 26 бит двоичных чисел, причем 1-й бит является битом четной проверки четности для 2-13-го битов, бит 26 является битом нечетной проверки четности для 14-25-гой битов, 2-9-й биты являются кодом зоны и 10-15 -й биты являются номером карты.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC Состоит из 34 бит двоичных чисел, причем 1-й бит является битом проверки четности для 2-17-го битов, а 34-й бит является битом проверки нечетности для 18-33-го битов, а 2-15-й биты являются номером карты.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCC Состоит из 34 бит двоичных чисел, причем 1-й бит является битом четной проверки четности для 2-17-го битов, 34-й бит является битом

Формат Wiegand	Определение
	нечетной проверки четности для 18-33-го битов, 2-9-го битов являются кодом зоны, а 10-15-й биты являются номером карты.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Состоит из 36 бит двоичных кодов. 1-й бит является битом нечетной проверки четности от 2-го до 18-го битов, а 36-й бит является битом четной проверки четности от 19-го до 35-го битов. 2–17-й бит - это код устройства, 18–33-й - номер карты, а 34–35-й - код производителя.
Wiegand36a	EFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Состоит из 36 бит двоичного кода. 1-й бит является битом четной проверки четности от 2-го до 18-го битов, а 36-й бит является битом нечетной проверки четности от 19-го до 35-го битов. 2–19-й бит - это код устройства, а 20–35-й - номер карты.
Wiegand37	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE Состоит из 37 бит двоичного кода. 1-й бит является битом нечетной проверки четности со 2-го по 18-й биты, а 37-й бит является битом четной проверки четности с 19-го по 36-й биты. 2-4-й биты - это код производителя, 5-16-й биты - код сайта, а 21-16-й биты - номер карты.
Wiegand37a	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Состоит из 37 бит двоичного кода. 1-й бит является битом четной проверки четности от 2-го до 18-го битов, а 37-й бит является битом нечетной проверки четности от 19-го до 35-го битов. 2-4-й биты - это код производителя, 5-14-й биты - код устройства, 15-20-й биты - код сайта, а 21-16-й биты - номер карты.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO

Формат Wiegand	Определение
	Состоит из 50 бит двоичного кода. 1-й бит - это битом четной проверки четности со 2-го по 25-й бит, а 50-й бит - это битом нечетной проверки четности от 26-го до 49-го бита. 2–17-й биты - это код сайта, а 18–49-й биты - номер карты.

✍**Примечание: C** обозначает номер карты, **E** обозначает бит четной проверки четности, **O** обозначает бит нечетной проверки четности, **F** обозначает код устройства, **M** обозначает код производителя, **P** обозначает бит четности и **S** обозначает код сайта.

5.4.2 Выход Wiegand



Формат Wiegand: Пользователи могут выбирать стандартные форматы Wiegand, встроенные в систему. См. определения всех типов общих форматов Wiegand в 5.4.1 «Вход Wiegand». Поддерживается несколько вариантов, но фактический формат определяется Выходными битами Wiegand.

Выходные биты Wiegand: количество бит данных Wiegand. После выбора [**Выходные биты Wiegand**] устройство будет использовать заданное количество бит, чтобы найти подходящий формат Wiegand в [**Формат Wiegand**].

Например, если выбраны 26-битный Wiegand26, 34-битный Wiegand34a, 36-битный Wiegand36, 37-битный Wiegand37a и 50-битный Wiegand50, а выходные биты Wiegand установлены на 36, принимается 36-битный формат Wiegand36.

Неудавшийся идентификатор: определяется как выходное значение неудавшейся верификации пользователя. Формат вывода зависит от настройки [**Формат Wiegand**]. Значение по умолчанию варьируется от 0 до 65535.

Код сайта: аналогичен идентификатору устройства, за исключением того, что его можно установить вручную и повторить на разных устройствах. Значение по умолчанию составляет от 0 до 256.

Ширина импульса (мкс): ширина импульса, посылаемая Wiegand. Значение по умолчанию составляет 100 микросекунд, которые можно регулировать в диапазоне от 20 до 100 микросекунд.

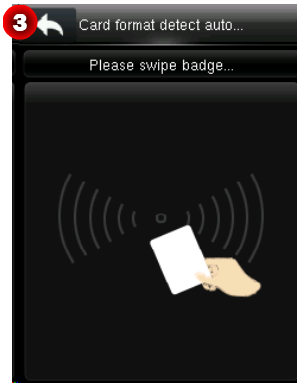
Импульсный интервал (**мкс**): значение по умолчанию составляет 1000 микросекунд, которые можно регулировать в диапазоне от 200 до 20000 микросекунд.

Тип идентификатора: вывод содержимого после успешной проверки. Идентификатор пользователя или номер карты могут быть выбраны.

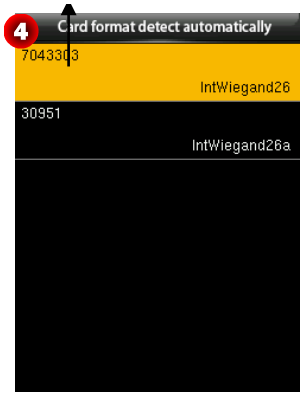
5.4.3 Формат карты определяется автоматически

[**Формат карты определяется автоматически**] помогает пользователю быстро определить тип карты и соответствующий ей формат. В устройстве предустановлены различные форматы карт. После считывания карты система будет определять его как разные номера карт в соответствии с каждым форматом; пользователю требуется только выбрать элемент, эквивалентный фактическому номеру карты, и установить формат в качестве формата Wiegand для устройства. Эта функция также применима к функции чтения карт и вспомогательному считывателю Wiegand.

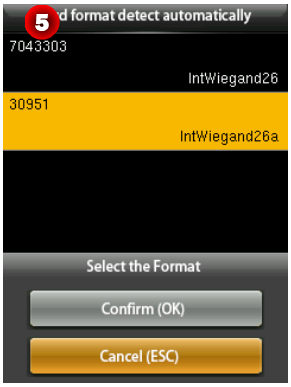
Номер карты, полученный на основе анализа формата IntWiegnad26



После ввода автоматического определения просканируйте карту в зоне считывания карт (на этом устройстве или считывателе).



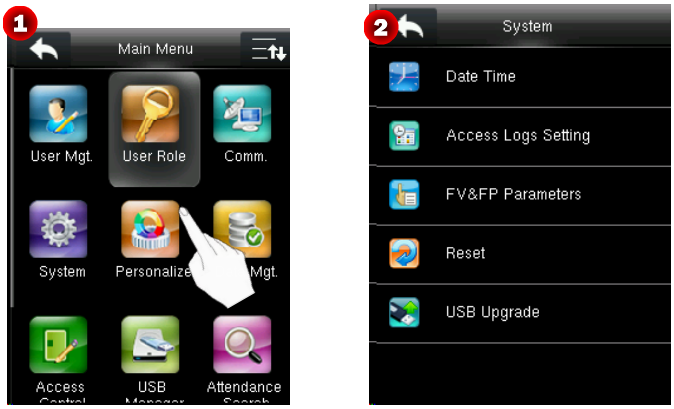
Формат Wiegand и проанализированный номер карты определяются автоматически.



Выберите номер, соответствующий фактическому номеру карты, и соответствующий формат - это формат Wiegand, который должен быть выбран для чтения этого типа карты.

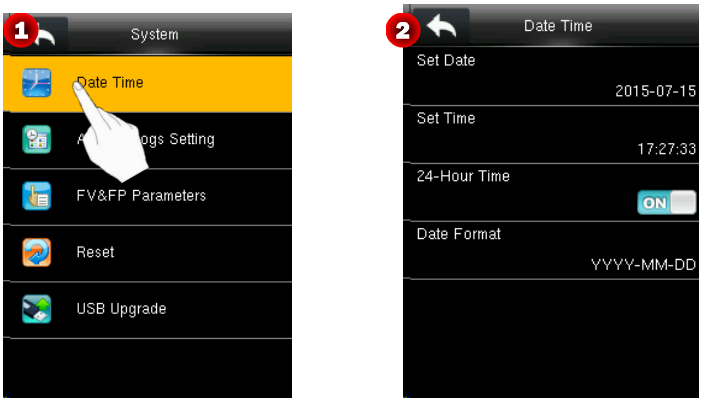
6. Системные настройки

Установите системные параметры, включая дату и время, журналы доступа★, параметры вены пальцев, восстановление заводских настроек и обновление USB-диска, чтобы устройство максимально соответствовало требованиям пользователя в отношении функций и отображения.



6.1 Настройки даты / времени

Установить дату и время устройства.

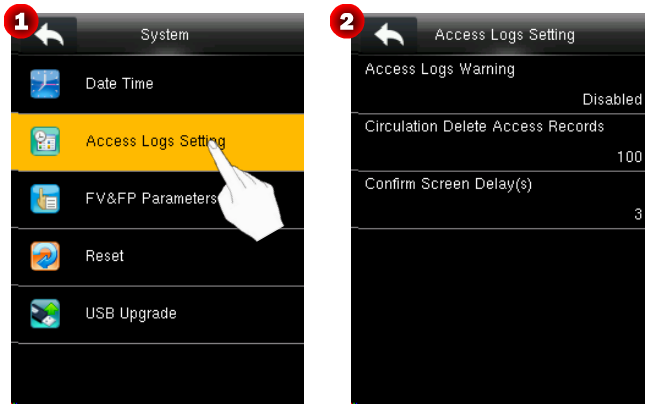


Дата и время: установите дату и время устройства.

24-часовое время: установите формат отображения времени на главном интерфейсе. Выберите ВКЛ., чтобы время отображалось в 24-часовой системе, или выберите ВЫКЛ., чтобы время отображалось в 12-часовой системе.

Формат даты: установите формат времени, отображаемый на всех интерфейсах устройства.

6.2 Настройка журналов доступа★

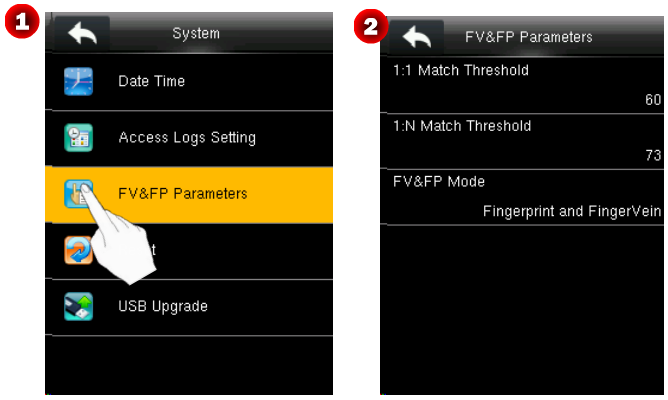


Предупреждение журналов доступа. Если остаточная емкость записи меньше, чем заданное значение, устройство автоматически генерирует сообщение с указанием остаточной емкости записи. Вы можете установить его на **Отключено** или установить значение в диапазоне от 1 до 9999.

Цикличное удаление записей доступа: установите количество записей журнала, которые могут быть удалены в тот момент, когда существующие записи достигают максимально допустимой емкости журнала. Значение по умолчанию - **Отключено**. Вы можете установить его в диапазоне от 1 до 999.

Подтвердить время ожидания экрана (сек): установите длительность отображения сообщений о результатах верификации. Диапазон допустимых значений: 1-9.

6.3 Настройка параметров вен и отпечатков пальцев★



Пороговое значение 1:1: установите сходство между отображением вен на пальцах, полученным в настоящее время, и зарегистрированными отображениями на устройстве в режиме верификации 1:1. Значение по умолчанию - 60, и вы можете установить его в диапазоне от 55 до 75. Когда сходство достигает заданного уровня верификация считается успешной. Чем выше пороговое значение, тем ниже процент ошибочных оценок и выше уровень ложного отклонения, и наоборот.

Пороговое значение 1:N: установите сходство между изображением вены пальца, полученным в настоящее время, и зарегистрированными изображениями на устройстве в режиме верификации 1:N. Значение по умолчанию - 70, и вы можете установить его в диапазоне от 65 до 85. Когда сходство достигает заданного уровня верификация считается успешной. Чем выше пороговое значение, тем ниже процент неправильных оценок и выше уровень ложных отклонений, и наоборот.

Рекомендуемые пороговые значения сравнения:

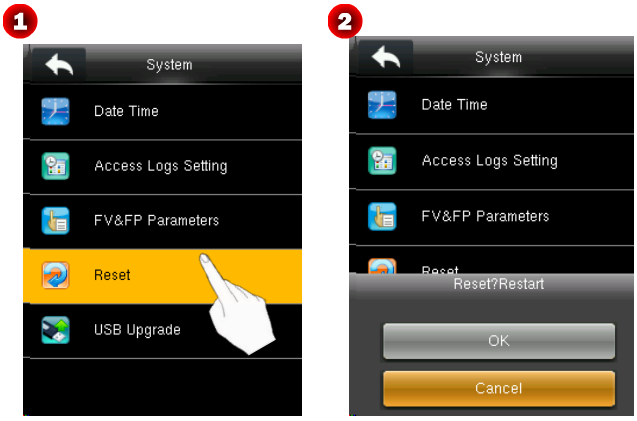
Процент ошибочного отказа в доступе	Процент неправильной оценки	Пороговое значение сравнения	
		1:N	1:1
высокий	низкий	85	75

средний	средний	70	60
низкий	высокий	65	55

Режим вен и отпечатков пальцев: Верификация считается успешной, когда пройдена успешно как верификация по венам пальцев, так и верификация по отпечаткам пальцев.

6.4 Сброс до заводских настроек

Сбросить такие данные, как настройки связи и системных настроек до заводских настроек.

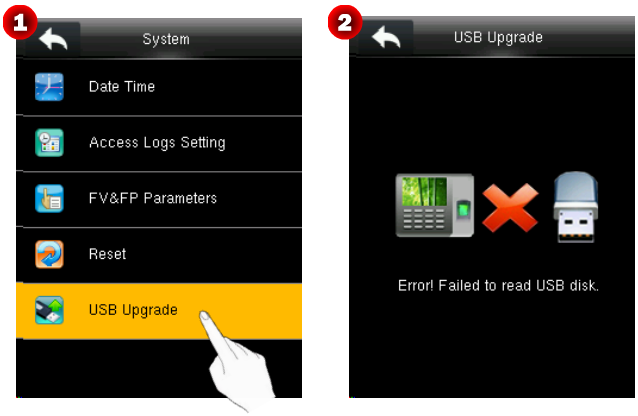


✍**Примечание**: после сброса пользовательская информация в устройстве и настройки в интерфейсе контроля доступа не удаляются.

6.5 Обновить USB

Эта функция позволяет обновить прошивку устройства с помощью файла обновления на USB-диске.

Вставьте USB-диск в порт USB и нажмите **Обновить USB** для обновления прошивки.

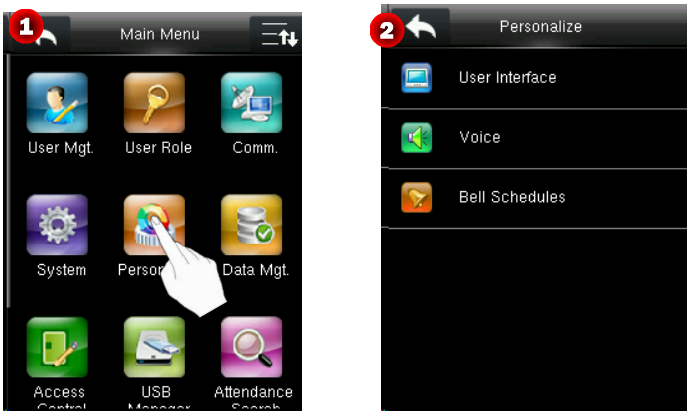


✍**Примечание:**

(1) Если USB-диск не вставлен, на **Рис. 2** отображается сообщение.

(2) Если необходимо обновление файлов, пожалуйста обратитесь к службе техподдержки. В обычных обстоятельствах обновление прошивки не рекомендуется.

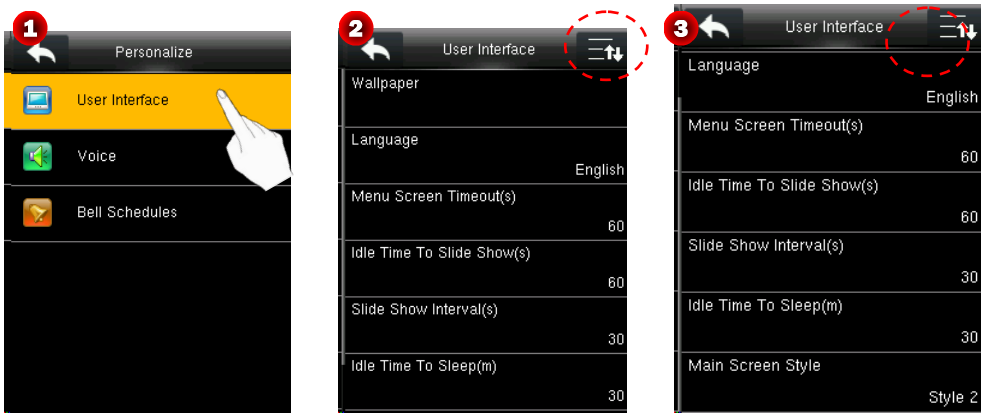
7. Настройки персонализации



7.1 Настройки пользовательского интерфейса

Вы можете настроить стиль отображения домашнего интерфейса.

В интерфейсе **Персонализации** нажмите **Интерфейс пользователя**, чтобы войти в интерфейс, и нажмите , чтобы прокрутить экран вниз, чтобы отобразить больше содержимого. (Примечание. Вы можете нажать еще раз, чтобы прокрутить экран вверх).



- **Обои**

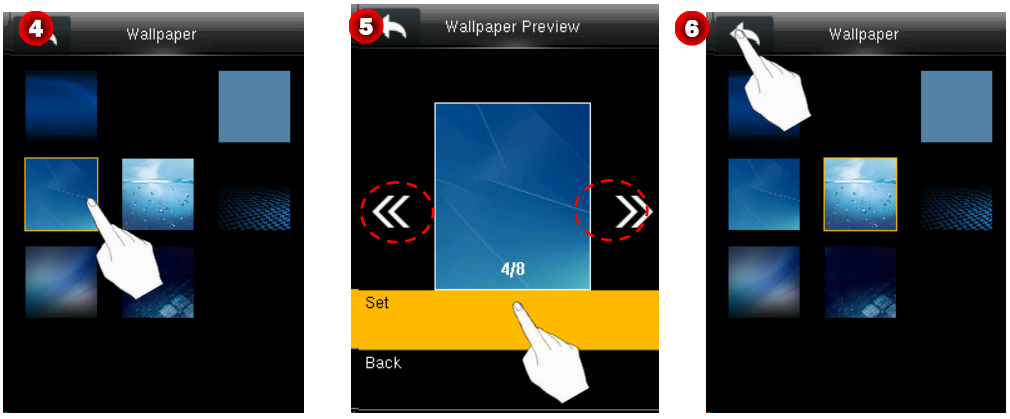
Выберите обои главного экрана по мере необходимости, вы можете найти обои различных стилей в устройстве. Подробная операция заключается в следующем:

1. Нажмите **Обои**.

2. Нажмите на изображение (**Рис. 4**), чтобы войти в интерфейс **Предварительного просмотра обоев**.

3. Восемь обоев хранятся в устройстве. Чтобы выбрать один, нажмите  , а затем нажмите **Установить** (**Рис. 5**). После настройки устройство вернется в интерфейс обоев.

Нажмите  (**Рис. 6**), чтобы сохранить настройку и вернуться к интерфейсу **Интерфейс пользователя**.



- **Язык**: выберите необходимый язык устройства.

- **Время ожидания меню экрана (сек)**

Если в интерфейсе меню не происходит никаких операций, а время превышает установленное значение, устройство автоматически вернется к начальному интерфейсу. Вы можете отключить его или установить значение 60 ~ 99999 секунд.

- **Время бездействия до появления слайд-шоу (сек)**

Если в начальном интерфейсе не происходит никаких операций, а время превышает установленное значение, будет показано слайд-шоу. Его можно отключить (установить на Отсутствует) или установить на 3 ~ 999 секунд.

- **Интервалы слайд-шоу (сек)**

Это относится к интервалу между отображением различных изображений слайд-шоу. Его можно отключить или установить на 3 ~ 999 с.

- **Время бездействия до перехода в спящий режим (мин)**

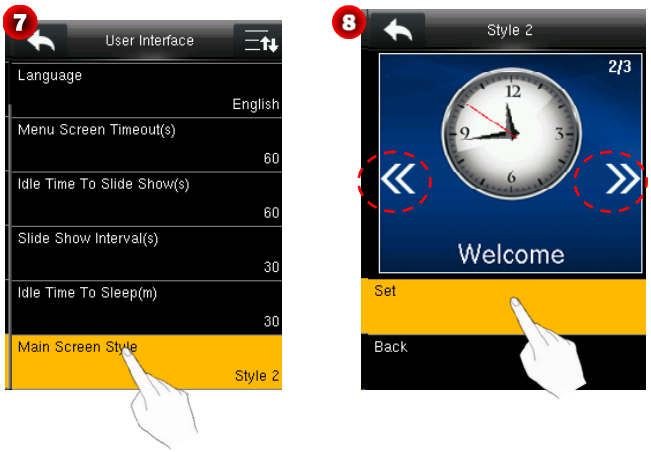
Если на устройстве не выполняется никаких операций и установлено Время ожидания, устройство переходит в режим ожидания. Нажмите любую клавишу, чтобы отменить режим ожидания. Вы можете отключить эту функцию или установить значение от 1 до 999 минут. Если для этой функции установлено значение [Отключено], устройство не перейдет в режим ожидания.

- **Стиль главного экрана**

Подробная операция выглядит следующим образом:

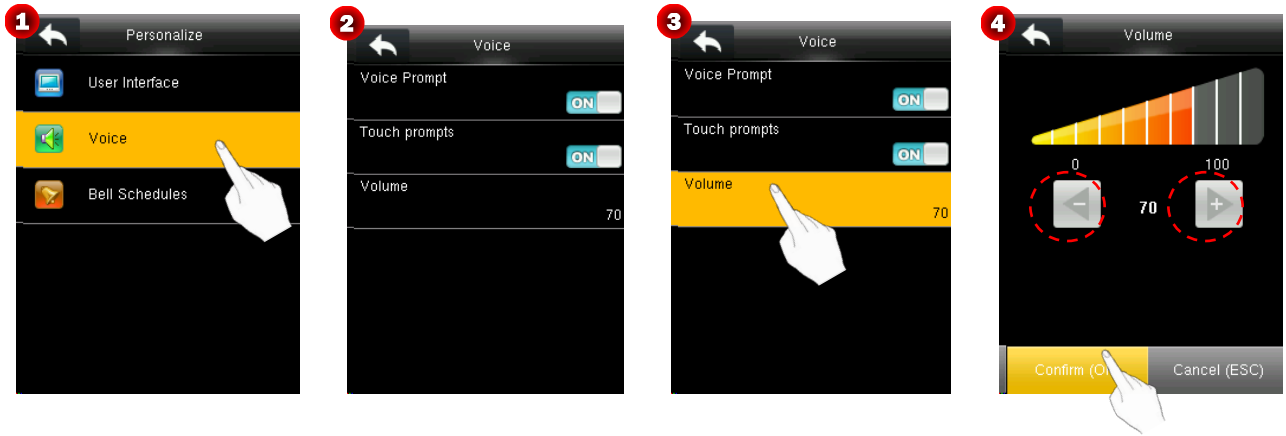
1. Нажмите **Стиль главного экрана**, чтобы войти в интерфейс настроек.

2. Нажмите ⟪/⟫, чтобы включить и выберите стиль, а затем нажмите **Установить** (**Рис. 8**). После настройки устройство возвращается в интерфейс **Обоев**.



7.2 Настройки голоса

Нажмите **Голос**, чтобы в интерфейс настроек.



Голосовая подсказка: выберите, нужно ли включать голосовые подсказки во время работы. Значение по умолчанию ON означает, что голосовая подсказка включена. Вы можете нажать на нее, чтобы переключаться между ON и OFF. Значок OFF указывает, что голосовая подсказка отключена.

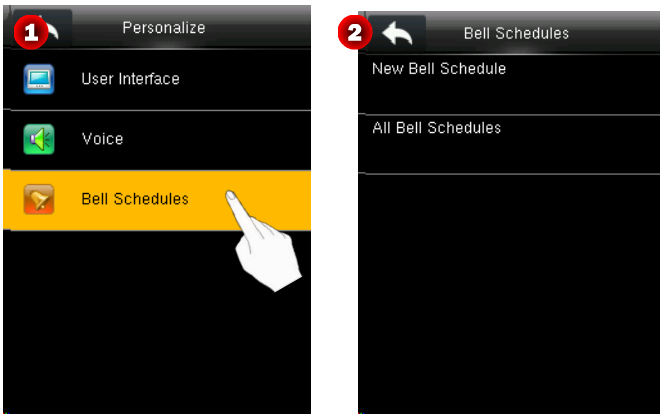
Подсказка клавиатуры: выберите, следует ли включать голос клавиатуры во время нажатия клавиатуры. Значением по умолчанию является то, что подсказка клавиатуры включена. Вы можете щелкнуть по нему, чтобы переключаться между ON и OFF. Значок OFF указывает на то, что подсказка клавиатуры отключена.

Громкость: установите громкость устройства. Значение по умолчанию - 70. Нажмите **Громкость**, чтобы войти в интерфейс настройки. Нажмите /, чтобы уменьшить / увеличить громкость, затем нажмите **Подтвердить (OK)** (см. **Рис. 4**), чтобы сохранить и вернуться к интерфейсу **Голос**.

7.3 Настройки звонков

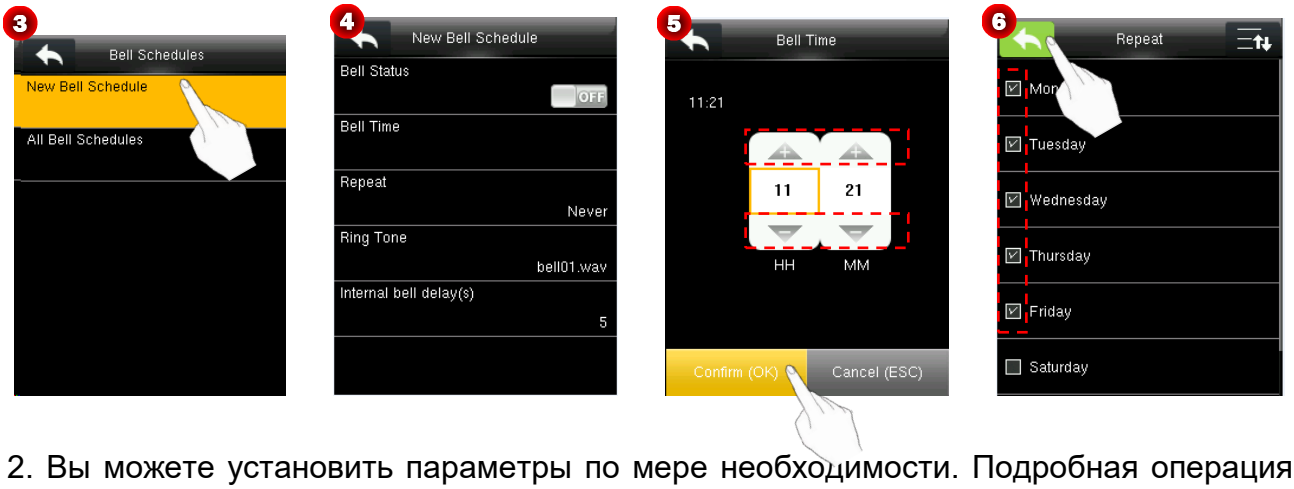
Многие компании предпочитают использовать звонки для обозначения рабочего и нерабочего времени. При достижении запланированного времени для звонка устройство будет автоматически воспроизводить выбранную мелодию звонка, пока не истечет продолжительность звонка.

Нажмите **Графики звонков**, чтобы войти в интерфейс **Графики звонков**.



7.3.1 Новый график звонков

1. Нажмите **Новый график звонков**, чтобы войти в интерфейс Новый график звонков (см. **Рис. 4**).



2. Вы можете установить параметры по мере необходимости. Подробная операция выглядит следующим образом:

- Статус звонка

Значением по умолчанию является OFF, которое означает, что статус звонка отключен. Нажмите, чтобы переключаться между ON и OFF. Значок указывает, что статус звонка включен.

Примечание: Расписание вступает в силу только после установки статуса звонка.

- Время звонка

Установите время начала звонка.

Нажмите **Время звонка**, чтобы войти в интерфейс **Время звонка**.

(2) Установите время звонка, нажимая ▲/▼ для увеличения / уменьшения номера, и нажмите **Подтвердить (OK)** (см. **Рис. 6**), чтобы сохранить и вернуться к интерфейсу **Новый график звонков**.

- **Повторить**

Значением по умолчанию является **Никогда**, которое используется для одноразового графика звонков.

Чтобы повторить использование графика звонков, нажмите **Повторить**, чтобы войти в интерфейс **Повторить**. Отметьте одну или несколько дат, требующих расписания звонков, и нажмите (см. **Рис. 6**), чтобы сохранить настройки и вернуться в интерфейс **Новый график звонков**. Когда наступают выбранные даты и время звонка, срабатывают сигналы реле и воспроизводится установленный звонок. Когда продолжительность звонка истекает, звонок останавливается автоматически.

- **Мелодия звонка**

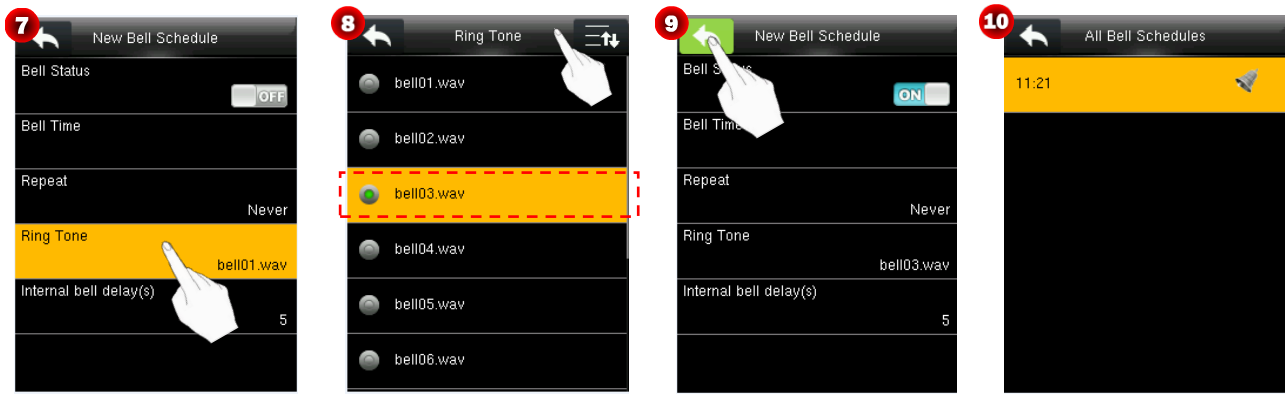
Установите мелодию звонка для графика звонков.

Нажмите **Мелодия звонка**, чтобы войти в интерфейс **Мелодия звонка**.

(2) В списке мелодий звонка нажмите мелодию звонка, чтобы выбрать ее, и нажмите (см. **Рис. 8**), чтобы сохранить настройки и вернуться к интерфейсу **Новый график звонков**.

- **Время ожидания внутреннего звонка (сек)**

Установите Время ожидания звонка. Значение по умолчанию составляет 5 секунд. Вы можете установить его в диапазоне от 1 до 999.



3. После настройки нажмите в интерфейсе Новый график звонков (**Рис. 9**), чтобы сохранить настройки и вернуться к начальному интерфейсу.

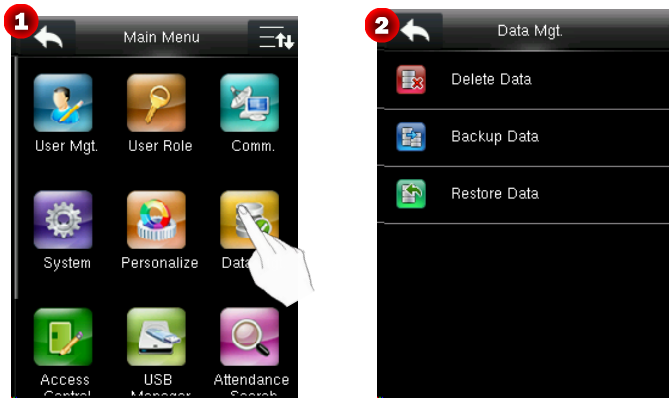
7.3.2 Все графики звонков

В интерфейсе **Графики звонков** нажмите **Все графики звонков**, чтобы войти в интерфейс, как показано на Рис. 10. Вы можете редактировать / удалять расписания звонков по мере необходимости.

✍ **Примечание**: метод редактирования / удаления графиков звонков такой же, как и при редактировании / удалении пользователей. Подробнее см. 3.2.2 Редактирование / удаление пользователя.

8. Управление данными

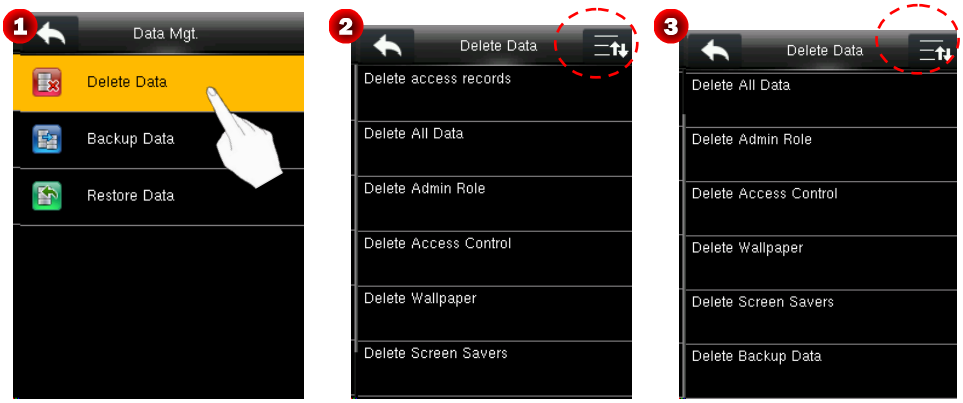
В интерфейсе **Главное меню** нажмите **Управление данными**, чтобы войти в интерфейс **Управление данными.**



8.1 Удалить данные

Управление данными на устройстве, включая удаление данных учета рабочего времени, удаление всех данных, удаление роли администратора, удаление заставок и т. д.

Нажмите **Удалить данные**, чтобы войти в интерфейс **Удалить данные** и нажмите , чтобы прокрутить экран вниз, чтобы отобразить больше содержания. (Примечание. Вы можете нажать еще раз, чтобы прокрутить экран вверх).



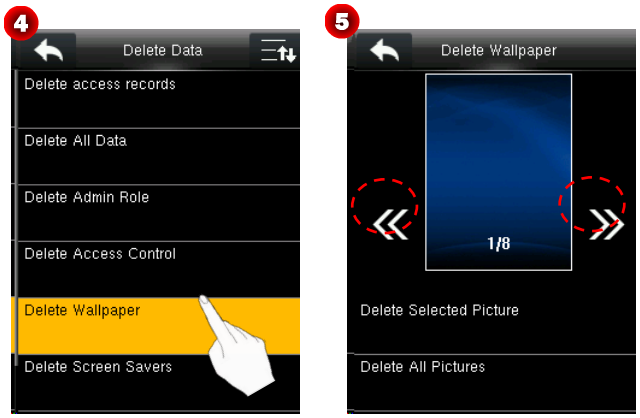
- **Удалить записи доступа★**: Удалить все записи доступа.

- **Удалить все данные:** удалить всю информацию о пользователях, информацию о венах пальцев, журналы событий учета рабочего времени и т. д.
- **Удалить роль администратора**: сделать всех администраторов обычными пользователями.
- **Удалить контроль доступа**: восстановление заводских настроек по умолчанию для таких настроек контроля доступа, как праздники, права пользователей на доступ, правила времени, группы пользователей. Записи доступа не будут удалены.
- **Удалить обои**:

  Удалить обои. Конкретные операции заключаются в следующем.

  1. Нажмите Удалить обои.

  2. Нажмите ⏮/⏭, чтобы переключаться и выбрать обои, а затем нажмите **Удалить выбранное изображение**, чтобы удалить выбранное изображение, или нажмите **Удалить все изображения**, чтобы удалить все изображения.

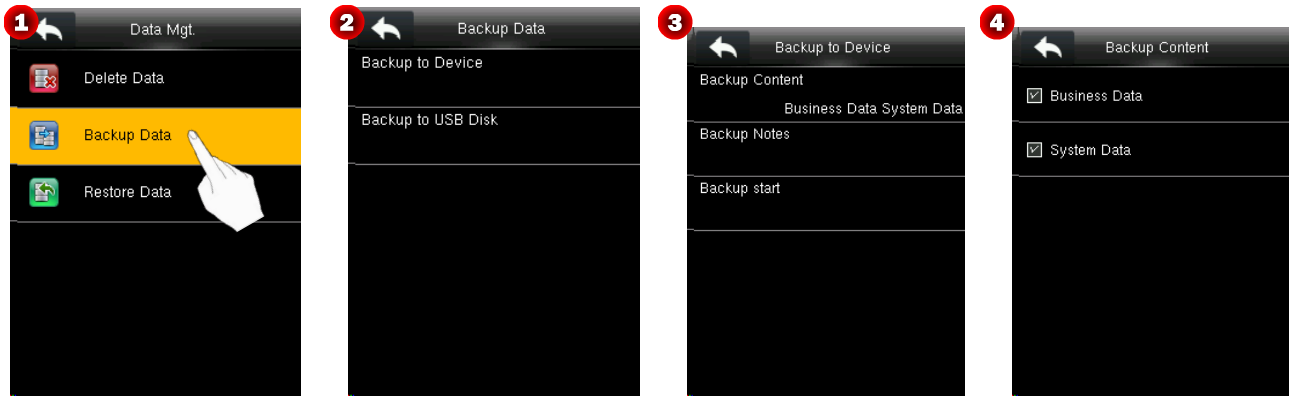


- **Удалить заставки экрана**

Метод удаления заставок такой же, как и для удаления обоев. (Подробнее о том, как загрузить заставки, см. 10.2 Загрузка с USB).

- Удалить данные резервной копии: удалить все данные резервной копии.

8.2 Данные резервной копии



- **Резервное копирование на устройство**

Вы можете выполнить резервное копирование бизнес-данных или данных конфигурации с устройства на локальный ПК.

1. Нажмите **Резервное копирование на устройство**, чтобы войти в интерфейс **Резервное копирование на устройство**.

2. Вы можете установить параметры по мере необходимости. Подробная операция выглядит следующим образом:

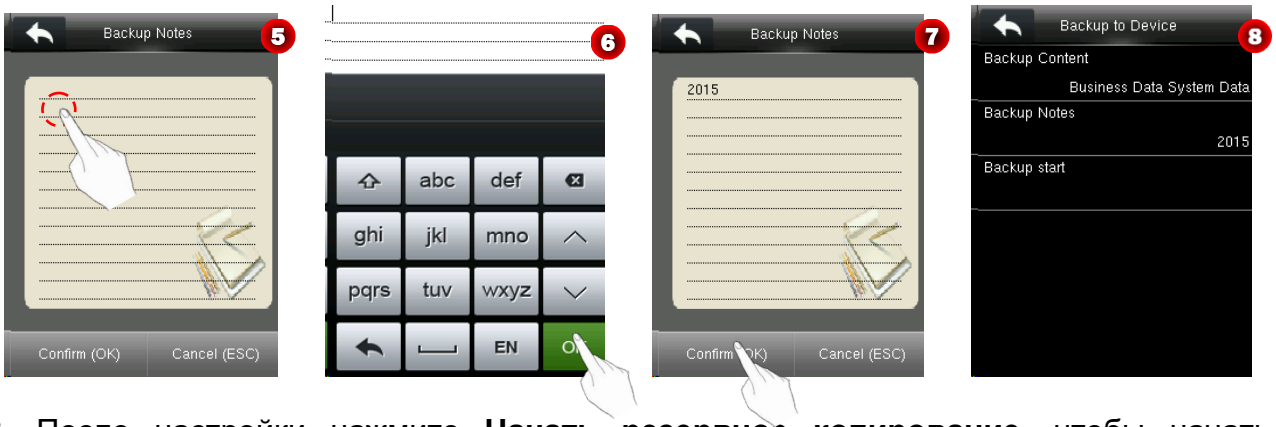
Содержимое резервной копии: нажмите **Содержимое резервной копии**, чтобы войти в интерфейс **Содержимое резервной копии**. Выберите содержимое для резервного копирования. (**Примечание**. Значок ☑ обозначает выбранный элемент).

Примечания по резервному копированию: введите содержимое резервной копии. Подробный метод заключается в следующем:

Нажмите **Примечания по резервному копированию**, чтобы войти в интерфейс **Примечания по резервному копированию** (см. **Рис. 5**).

② Нажмите на экран. Клавиатура предлагается. Введите примечание, используя метод ввода T9, и затем нажмите OK (см. **Рис. 6**), чтобы подтвердить и вернуться к интерфейсу **Примечания по резервному копированию**.

③ Нажмите **Подтвердить** (**OK**) (см. **Рис. 7**), чтобы сохранить настройки и вернуться к интерфейсу **Резервное копирование на устройство**.



3. После настройки нажмите **Начать резервное копирование**, чтобы начать резервное копирование содержимого на устройство.

- Резервное копирование на USB-диск

Резервное копирование бизнес-данных или данных конфигурации с устройства на USB-диск. Метод такой же, как и у **Резервного копирования на устройство**.

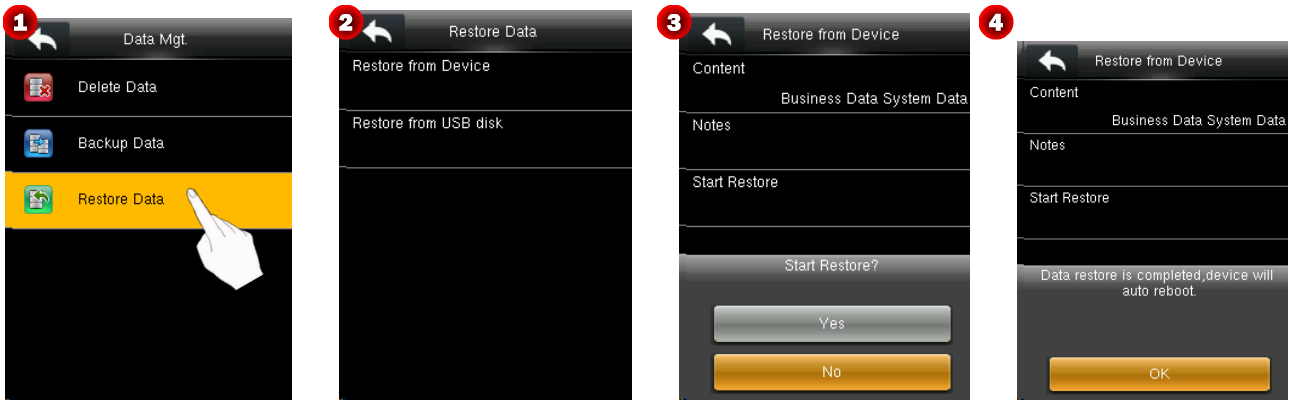
Примечания:

(1) Перед резервным копированием данных на USB-диск вставьте USB-диск в USB-порт устройства.

(2) Перед резервным копированием данных на локальный ПК система заменяет старые данные резервной копии на самые последние данные.

8.3 Восстановить данные

В интерфейсе **Управ. данными** нажмите **Восстановить данные**, чтобы войти в интерфейс **Восстановить данные**.



- **Восстановить на устройство**

Восстановить данные с ПК на устройство.

1. Нажмите **Восстановить на устройство**, чтобы войти в интерфейс **Восстановить на устройство**.

2. Нажмите **Начать восстановление**, и появится диалоговое окно (см. **Рис. 3**). Нажмите **Да**, чтобы начать.

✍ **Примечание**. После восстановления нажмите кнопку **ОК**, чтобы перезагрузить устройство.

- Восстановление с USB-диска

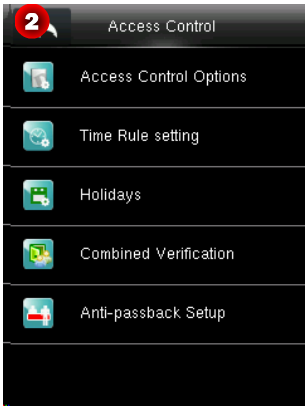
Восстановите данные на устройство с USB-диска. Подробная операция аналогична той, которая используется в **Восстановить на устройство**.

✍ **Примечание**. Перед восстановлением данных с USB-диска вставьте USB-диск с резервными данными в USB-порт устройства.

9. Контроль доступа

Настройки функции контроля доступа - для периодов доступа пользователей и параметров управления замком и связанного устройства.





Чтобы получить доступ зарегистрированный пользователь должен соответствовать следующим условиям:

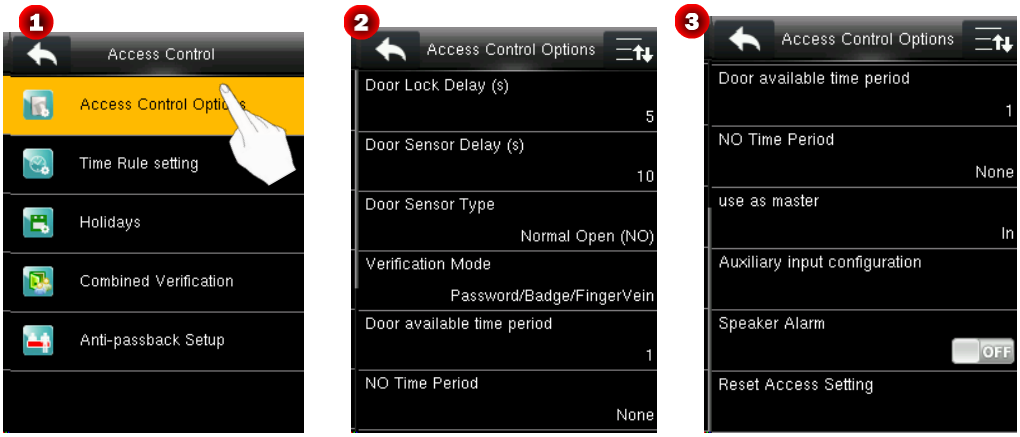
1. Время доступа пользователя относится либо к личному периоду доступа, либо к периоду доступа группы.

2. Группа пользователей должна находиться в комбинированном доступе (когда в том же комбинированном доступе находятся другие группы, верификация членов этих групп также необходима для открытия двери).

В настройках по умолчанию новые пользователи распределяются в первую группу с временем доступа группы по умолчанию и комбинированным доступом, обозначенную как группа «1» и устанавливаются в состояние разблокировки.

9.1 Настройки параметров контроля доступа

В интерфейсе контроля доступа нажмите **Параметры контроля доступа**, чтобы войти в интерфейс **Параметры контроля доступа** и нажмите , чтобы прокрутить экран вниз, чтобы отобразить больше содержимого. (**Примечание**: вы можете нажать еще раз, чтобы прокрутить вверх).



Set the parameters of the control lock and related devices.

Время ожидания дверного замка (сек): Период времени разблокировки (от открытия двери до автоматического закрытия) после того, как электронный замок получает сигнал открытия, отправленный с устройства (значение находится в диапазоне от 0 до 10 секунд).

Время ожидания датчика двери (сек): Когда дверь открыта, датчик двери будет проверен через некоторое время; если состояние датчика двери не совпадает с состоянием режима датчика двери, сработает сигнализация. Период времени - это **Время ожидания датчика двери** (значение колеблется от 1 до 255 секунд).

Тип датчика двери: включает в себя «Отсутствует», «Нормальное открытие» (NO) и «Нормальное закрытие» (NC). **Отсутствует** означает, что датчик двери не используется; **Нормальное открытие** означает, что дверь открыта, когда включено электричество; **Нормальное закрытие** означает, что дверь закрыта, когда включено электричество.

Режим верификации: вы можете выбрать **Пароль/Вена пальца**, **Толька карта**, **Пароль**, **Вена пальца, Пароль & Вена пальца**, **Карта/Отпечаток пальца★**, **Только отпечаток пальца★**, **Только карта★**, **Отпечаток пальца & Пароль★**, **Карта & Пароль★**, **Карта & Отпечаток пальца ★** или **Badge & Отпечаток пальца & Пароль★** по мере необходимости.

Период доступности двери: Установите периоды открытия двери для пользователей.

Использовать в качестве главного: при настройке главного и подчиненного блоков вы можете установить состояние главного в качестве **Выхода** или **Входа**.

Выход: запись верификации на главном блоке является записью регистрации выхода.

Вход: запись верификации на главном блоке является записью регистрации входа.

Конфигурация вспомогательного входа★: установка времени **Вспомогательного выхода / открытия замка** и **типа Вспомогательного выхода** для устройства со вспомогательным разъемом. **Тип вспомогательного выхода** включает **Отсутствует**, **триггер открытия двери, триггер тревожной сигнализации, триггер открытия двери** и **тревожной сигнализации**.

Тревожная сигнализация динамика: Когда [**Тревожная сигнализация динамика**] включена, динамик подаст сигнал тревоги при демонтаже устройства.

Сброс настроек доступа: для сброса параметров времени ожидания дверного замка, времени ожидания датчика двери, типа датчика двери, времени ожидания тревожной сигнализации двери, времени повторных попыток до срабатывания тревожной сигнализации, периода времени Нормально открытый, конфигурации вспомогательного входа, исключая данных доступа, которые должны быть удалены в [**Управ. данными**].

Параметры доступа	**Заводские настройки по умолчанию**
Время ожидания дверного замка	10 сек
Время ожидания датчика двери	10 сек
Режим датчика двери	Отсутствует
Время ожидания тревожной сигнализации двери	30 сек
Период доступа режима Нормально открытый	Отсутствует

Время доступа Вспомогательного выхода ★	255 сек

✍**Примечания:** после установки периода режима **Нормально закрытый**, пожалуйста хорошо заблокируйте дверь, иначе в течение периода режима Нормально закрытый может сработать тревожная сигнализация.

9.2 Настройки графиков

Временной график - минимальная единица времени настроек контроля доступа; Для системы может быть установлено не более 50 графиков. Каждый график состоит из 7 временных отрезков (неделя), и каждый временной отрезок является действительным временем в течение 24 часов.

Вы можете установить максимум 3 периода для каждого правила времени. Соотношение между этими периодами - «или». Когда время верификации приходится на любой из этих периодов, верификация действительна. Формат периода - ЧЧ:ММ-ЧЧ:ММ в 24-часовой системе с точностью до секунд.

В интерфейсе **Контроль доступа** щелкните **Настройка правила времени**, чтобы войти в интерфейс **Правило времени**, и нажмите  , чтобы прокрутить экран вниз, чтобы отобразить больше содержимого. (**Примечание**. Вы можете нажать  еще раз, чтобы прокрутить экран вверх).



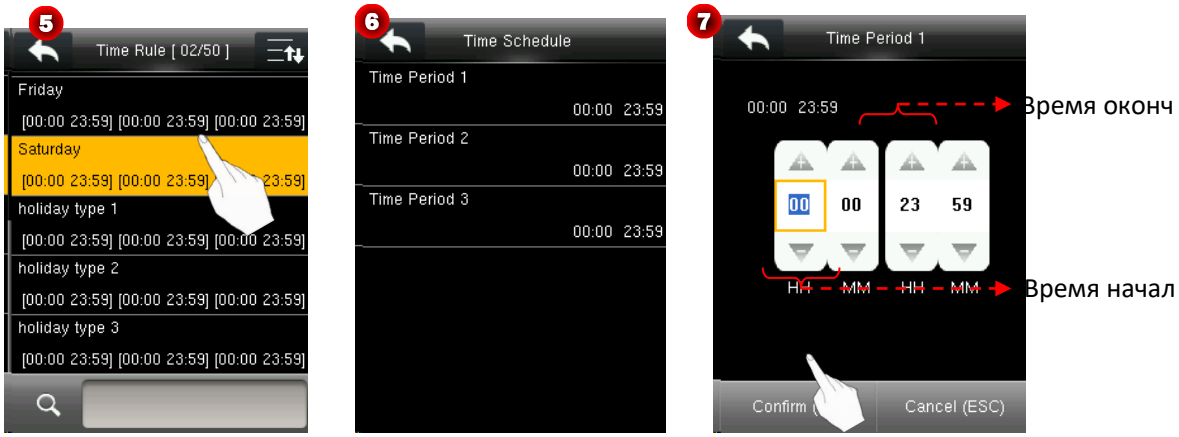
- **Редактирование правила времени**

Суперадминистратор может редактировать правила времени по мере необходимости. Подробная операция выглядит следующим образом:

1. Нажмите поле запроса (см. **Рис. 2**), чтобы войти в интерфейс **Правило поиска**.

2. Введите номер правила времени, нажмите **OK** (см. **Рис. 3**), чтобы войти в интерфейс **Правило времени** (см. **Рис. 4**).

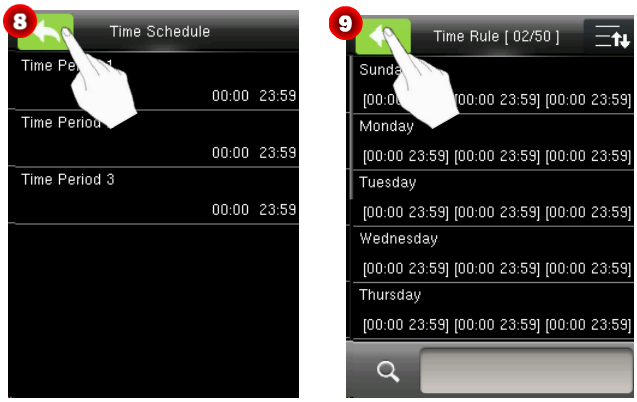
3. В списке периодов времени нажмите период, который нужно отредактировать (см. **Рис. 5**), чтобы войти в интерфейс **Временные графики** (см. **Рис. 6**).



4. В перечисленных графиках нажмите **Период времени 1/2/3**, чтобы войти в интерфейс настройки. При необходимости вы можете установить время начала и время окончания периода.

Рекомендации: нажмите значок /, чтобы увеличить / уменьшить число при настройке времени.

5. После настройки нажмите кнопку **Подтвердить** (**OK**) (см. **Рис. 7**), чтобы сохранить настройки и вернуться к интерфейсу **Временные графики**, и нажмите (см. **Рис. 8**), чтобы сохранить настройки и вернуться к интерфейсу **Правило времени**.



6. Установите другие периоды правила времени. Нажмите (см. **Рис. 9**) в интерфейсе **Правило времени**, чтобы сохранить настройки и вернуться к интерфейсу верхнего уровня.

Примечания:

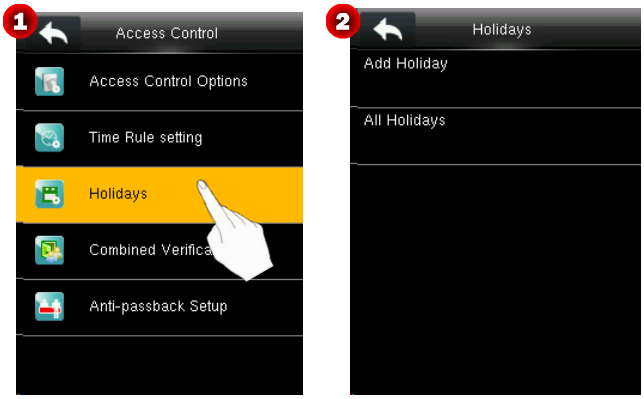
(1) Когда время окончания раньше времени начала (например, 23:57 - 23:56), это означает закрытие в течение всего дня. Когда время окончания позже времени начала (например, 00:00 - 23:59), это означает, что этот интервал действителен.

(2) **График действующего времени**: 00:00 - 23:59 (действителен весь день) или когда время окончания позже времени начала.

(3) По умолчанию правило времени с номером 1 указывает на открытие на весь день.

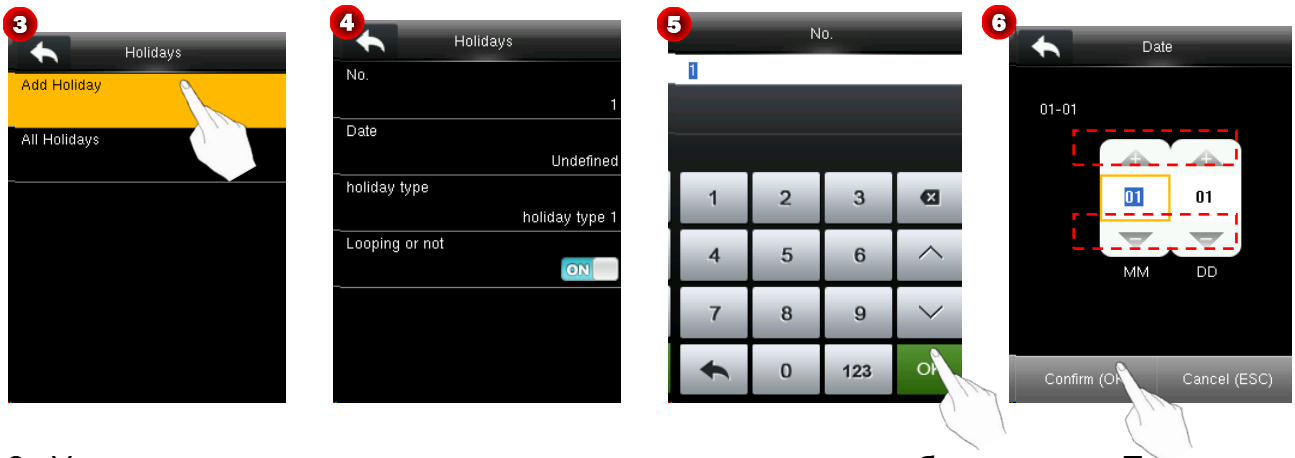
9.3 Настройки праздничных дней

Добавьте контроля доступа в праздничные дни для устройства и при необходимости установите периоды праздничных дней. Устройство управляет контролем доступа в праздничные дни в соответствии с настройками праздничных дней.



9.3.1 Добавить праздничные дни

1. Нажмите **Добавить праздничные дни**, чтобы войти в интерфейс **Праздничные дни** (см. **Рис. 4**).



2. Установите параметры праздничного дня по мере необходимости. Параметры устанавливаются следующим образом:

- **Номер**

Устройство автоматически присваивает номер праздничному дню. Нажмите **Номер**, чтобы войти в интерфейс **Номер**. При необходимости введите номер праздничного дня и нажмите **ОК** (см. **Рис. 5**), чтобы сохранить настройки и вернуться в интерфейс **Праздничные дни**.

Примечание: номер праздничного дня варьируется от 1 до 2000.

- Дата

Установите дату праздничного дня.

(1) Нажмите **Дата**, чтобы войти в интерфейс **Дата**.

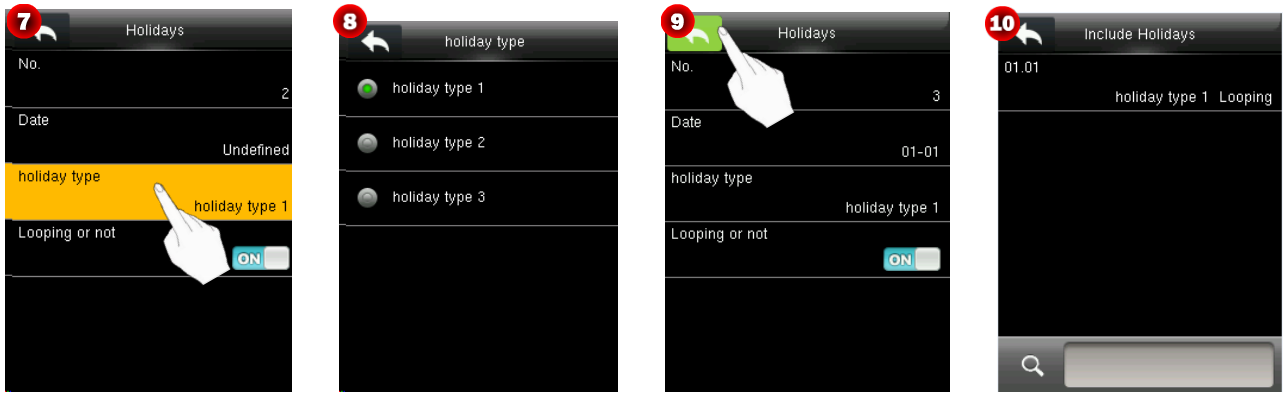
(2) Нажмите , чтобы увеличить число, или нажмите , чтобы уменьшить число для того, чтобы установить дату. Затем нажмите **Подтвердить** (**ОК**) (см. **Рис. 6**), чтобы сохранить настройки и вернуться в интерфейс **Праздничные дни**.

- тип праздничного дня

Установите тип праздничного дня.

(1) Нажмите **тип праздничного дня**, чтобы войти в интерфейс **тип праздничного дня.**

(2) Выберите тип праздничного дня и нажмите (см. **Рис**. **8**), чтобы сохранить настройки и вернуться в интерфейс **Праздничные дни**.



- **Цикличность или ее отсутствие**

Значением по умолчанию **Цикличность или ее отсутствие** является . Вы можете установить **Цикличность или ее отсутствие** переключением между и .

Например, для фиксированных праздничных дней каждый год Новый год - это 1 января, для них с помощью можно установить **Цикличность или ее отсутствие**. Например, для нефиксированных праздничных дней День матери каждый год - это второе воскресенье мая, конкретные даты являются

неопределенными, и для них с помощью  может быть установлена **Цикличность или ее отсутствие.**

Например, если для даты праздничного дня установлено 1 января 2010 г., а для **типа праздничного дня** установлено **тип праздничного дня 1** контроль доступа 1 января осуществляется в соответствии с настройками периода времени для типа праздничных дней 1, а не в соответствии с настройками периода времени Пятницы**.**

После настройки нажмите  в интерфейсе Праздничные дни (см. **Рис. 9**), чтобы сохранить настройки и вернуться к интерфейсу верхнего уровня**.**

9.3.2 Включить праздничные дни

В интерфейсе Праздничные дни, показанном на Рис. 3, нажмите **Все праздничные дни**, чтобы войти в интерфейс **Включить праздничные дни** (см. **Рис. 10**). Вы можете редактировать или удалять праздники по мере необходимости.

✍ **Примечание.** Методы редактирования или удаления праздничных дней те же, что и при редактировании или удалении пользователя, и здесь не описаны. Подробнее см. 3.2.2 Редактирование / удаление пользователя.

9.4 Настройки комбинированной верификации

✍ **Примечания:**

(1) Программное обеспечение Access3.5 не требуется, если устройство используется впервые. Вы можете установить комбинированную верификацию на устройстве напрямую.

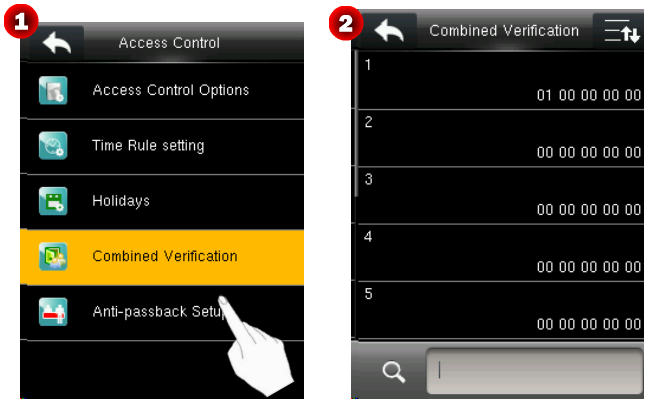
(2) После установки комбинированной верификации в программном обеспечении Access3.5 и установки настроек на устройство, устройство поддерживает только настройки комбинированной верификации, установленные из программного

обеспечения Access3.5, а комбинированная верификации не может быть установлена на устройстве.

Объедините двух или более участников, чтобы обеспечить многократную верификацию и повысить безопасность.

При комбинированной верификации диапазон номера пользователя составляет: 0 ≤ N ≤ 5; все пользователи могут принадлежать к одной группе или максимум к 5 различным группам.

В интерфейсе **Контроль доступа** нажмите **Комбинированная верификация**, чтобы войти в интерфейс **Комбинированная верификация**.

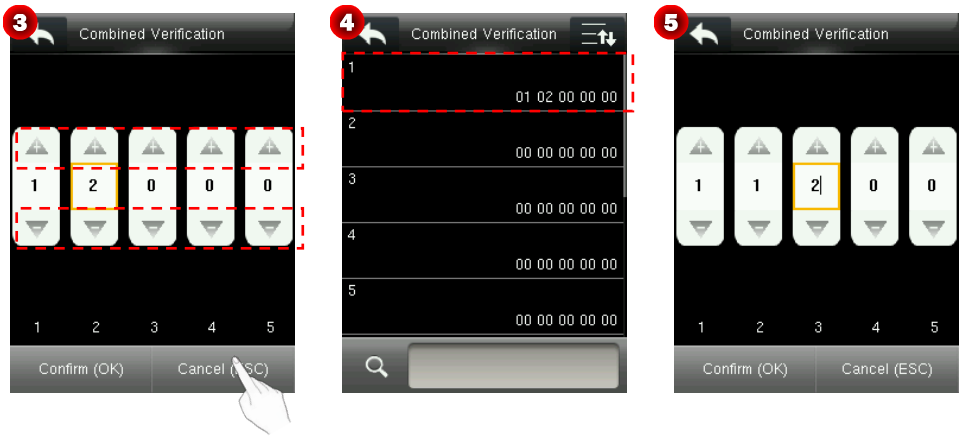


По умолчанию устройство поддерживает десять комбинаций разблокировки. Пользователи могут изменять параметры комбинированной верификации по мере необходимости. Конкретные операции заключаются в следующем:

Например, добавьте комбинацию разблокировки, требующую одновременной верификации группы пользователей 1 и группы пользователей 2.

1. В интерфейсе **Комбинированная верификация** нажмите комбинацию, которую нужно изменить, чтобы войти в интерфейс, показанный на **Рис. 3**.

2. Нажмите , чтобы увеличить число или нажмите , чтобы уменьшить число для того, чтобы установить идентификатор группы пользователей. Затем нажмите **Подтвердить** (**ОК**), чтобы сохранить настройки и вернуться в интерфейс **Комбинированная верификация**.



После успешной настройки дверь можно открыть только после того, как пользователь в группе пользователей 1 и пользователь в группе 2 пройдут верификацию.

✍ Примечания:

(1) Комбинация разблокировки поддерживает максимум пять групп пользователей. То есть в комбинации разблокировки дверь можно открыть только после того, как максимум пять пользователей пройдут верификацию.

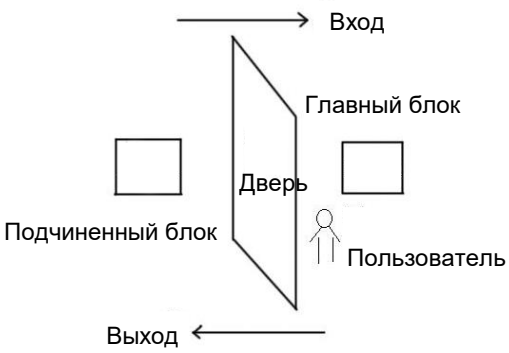
(2) После того, как установлена комбинация разблокировки, показанная на **Рис. 5**, дверь можно открыть только после того, как пользователь в группе пользователей 2 и два пользователя в группе пользователей 1 пройдут верификацию.

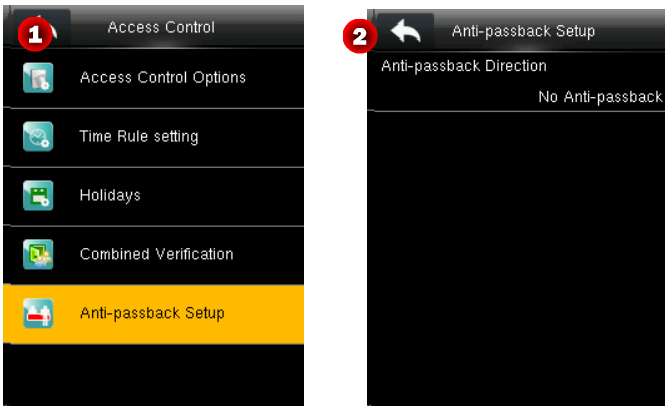
(3) Комбинация разблокировки очищается, когда все идентификаторы групп пользователей в комбинации разблокировки установлены на 0.

9.5 Настройки запрета двойного прохода

Чтобы некоторые люди, следующие непосредственно за пользователями, не входили в дверь без верификации, что приводит к проблемам с безопасностью, пользователи могут включить функцию запрета двойного прохода. Для того, чтобы открыть дверь запись регистрации входа должна совпадать с записью регистрации выхода.

Эта функция требует двух блоков для совместной работы: одно устанавливается внутри двери (главный блок), другое - снаружи двери (подчиненный блок). Два блока обмениваются данными через сигнал Wiegand. Формат Wiegand и тип вывода (идентификатор пользователя / номер карты), принятые главным и подчиненным блоками, должны быть согласованы.





Направление запрета двойного прохода

Отсутствие запрета двойного прохода: функция Запрета двойного прохода отключена, что означает то, что прохождение верификации на главном или подчиненном блоке может разблокировать дверь. Состояние учета рабочего времени не зарезервировано.

Запрет двойного прохода на выход: после того, как пользователь зарегистрировался на выход пользователь снова сможет зарегистрироваться на выход, только если последняя запись будет регистрацией на вход; в противном случае будет активирована тревожная сигнализация. Тем не менее, пользователь может свободно зарегистрироваться на вход.

Запрет двойного прохода на вход: после того, как пользователь зарегистрировался на вход пользователь снова сможет зарегистрироваться на вход, только если последняя запись будет регистрацией на выход; в противном случае будет активирована тревожная сигнализация. Тем не менее, пользователь может свободно зарегистрироваться на выход.

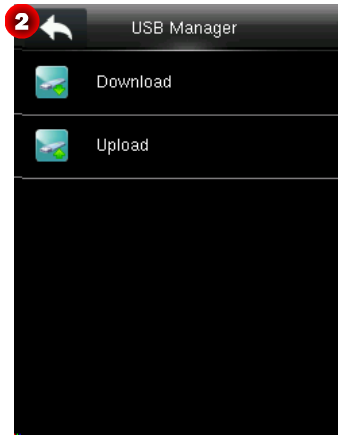
Запрет двойного прохода на вход / выход: после того, как пользователь зарегистрировался на вход/выход пользователь снова сможет зарегистрироваться на вход, только если последняя запись будет регистрацией на выход или пользователь снова сможет зарегистрироваться на выход, только если последняя запись будет регистрацией на вход; в противном случае будет активирована тревожная сигнализация.

10. Диспетчер USB

Информация о пользователе, шаблоны вен пальцев, шаблоны отпечатков пальцев, данные верификации и другие данные можно экспортировать в соответствующее программное обеспечение для обработки через USB-диск, а пользовательскую информацию, шаблоны вен пальцев и другие данные можно импортировать на устройство с помощью USB-диска.

✍Примечания. Перед загрузкой / выгрузкой данных с / на USB-диск сначала вставьте USB-диск в USB-слот.





10.1 Загрузить на USB

Загрузите записи контроля доступа★ и данные пользователя с устройства на USB-диск.

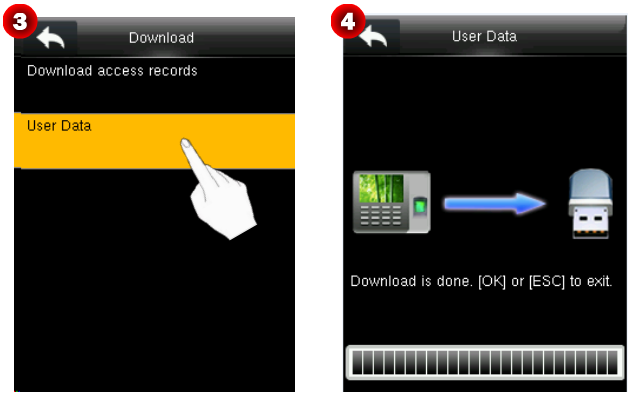
Загрузка записей доступа★: загрузите записи контроля доступа в указанном диапазоне дат с устройства на USB-диск.

Данные пользователя: загрузите всю информацию о пользователе и информацию о венах пальцев с устройства на USB-диск.

Далее в качестве примера используется операция загрузки пользовательских данных, чтобы описать, как загружать данные с использованием USB-диска.

1. Выберите **Загрузка** > **Данные пользователя**, чтобы начать загрузку данных пользователя на USB-диск. После успешной загрузки на экране отобразится **Загрузка завершена** (см. **Рис. 4**).

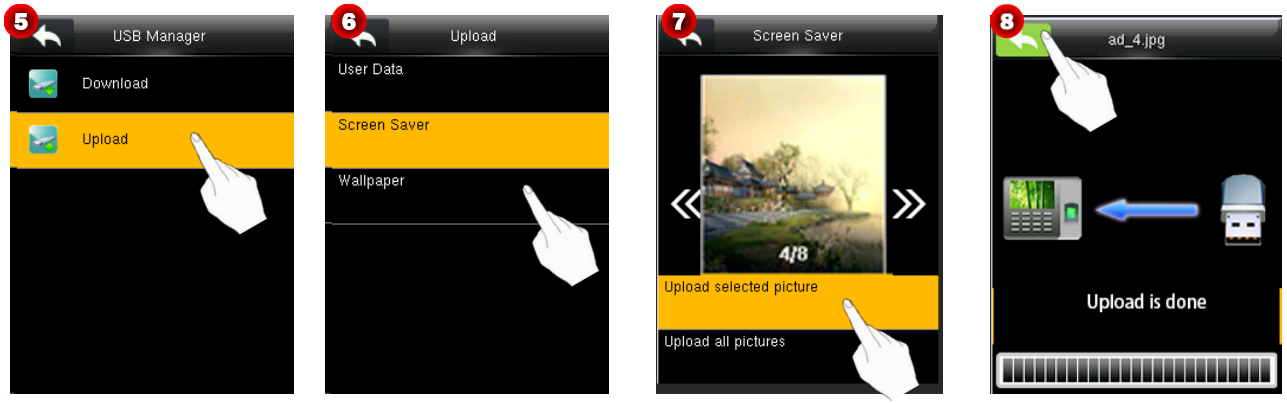
2. Извлеките USB-диск и нажмите , чтобы вернуться в интерфейс **Загрузка**.



10.2 Выгрузить с USB

Выгрузите данные об использовании, заставки и обои с USB-диска на устройство.

Нажмите **Выгрузить**, чтобы войти в интерфейс **Выгрузить**.



- **Данные о пользователе:** выгрузите всю информацию о пользователе с USB-диска на устройство.

- **Заставка экрана**

Загрузите изображения заставки с USB-диска на устройство. После того, как устройство переходит в режим ожидания, отображаются загруженные изображения заставки. Конкретная операция заключается в следующем:

1. Нажмите **Заставка экрана** (см. **Рис. 6**), чтобы войти в интерфейс **Заставка экрана**.

2. Нажмите  , чтобы переключиться, выберите изображение заставки экрана и нажмите **Выгрузить выбранное изображение**, чтобы загрузить выбранное изображение на устройство, или **Выгрузить все изображения**, чтобы выгрузить все изображения, которые соответствуют требованиям в папке рекламы, с USB-диск на устройство.

3. После успешной выгрузки на экране отобразится Выгрузка завершена. Нажмите  , чтобы вернуться к интерфейсу верхнего уровня.

- **Обои**

Выгрузить все обои с USB-диска на устройство. Конкретный метод работы такой же, как метод выгрузки изображений заставки, и здесь он не описан.

✍ **Примечания**:

(1) Перед загрузкой изображений заставки поместите изображения для загрузки в папку **рекламы** на USB-диске.

(2) Перед загрузкой обоев поместите загружаемые обои в папку **обоев** на USB-диске.

(3) Изображения и обои для заставки должны быть в формате PNG, JPG или BMP, размер которых не должен превышать 30 КБ.

(4) Названия заставок и обоев содержат не более 20 символов.

11. Поиск событий учета рабочего времени

Устройство автоматически сохраняет все записи верификации пользователей. С функцией поиска событий учета рабочего времени пользователи могут удобно запрашивать все записи.

1. Нажмите **Поиск событий учета рабочего времени** в главном меню**,** чтобы войти в интерфейс **Идентификатор пользователя** (см. **Рис. 2**).



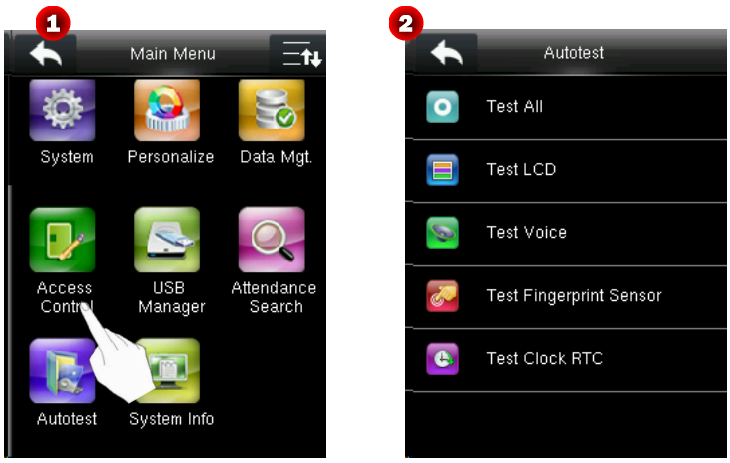
2. Введите Идентификатор пользователя и нажмите **OK**, чтобы войти в интерфейс **Временной диапазон** (см. **Рис. 3**).

3. Нажмите просматриваемый временной диапазон по мере необходимости, или нажмите **Определенный пользователь**, чтобы указать время начала и окончания записей в соответствии с запросом, а также просмотреть соответствующие записи.

✍ **Примечание**: Если вы нажмете **ОК** без ввода идентификатора пользователя, отобразятся записи верификации всех пользователей в выбранном диапазоне времени.

12. Автоматическое тестирование

Устройство автоматически проверяет все ли модули работают должным образом, включая ЖК-дисплей, голос, датчик отпечатков пальцев, датчик вены пальцев и часы реального времени (RTC).



Тестировать все: для тестирования ЖК, голоса, датчика отпечатков пальцев★ и часов реального времени. Во время тестирования нажмите на экран, чтобы продолжить следующее тестирование, или нажмите , чтобы выйти из тестирования.

Тестировать ЖК: проверьте эффект отображения на экране ЖК, отображая полный цвет, чистый белый и чистый черный, чтобы проверить, правильно ли отображаются цвета на экране. Во время тестирования нажмите на экран, чтобы продолжить следующее тестирование, или нажмите , чтобы выйти из тестирования.

Тестировать голос: проверьте заполнены ли голосовые файлы, хранящиеся на устройстве, и хорошее ли качество голоса. Во время тестирования нажмите на экран, чтобы продолжить следующее тестирование, или нажмите , чтобы выйти из тестирования.

Тестировать датчика отпечатков пальцев★: Проверьте правильно ли работает коллектор отпечатков пальцев. Во время тестирования пользователь прижимает

отпечаток пальца и проверяет является ли собранное изображение отпечатка пальца четким. При нажатии отпечатка пальца в окне коллектора полученное изображение отпечатка пальца отображается на экране в режиме реального времени. Нажмите , чтобы выйти из тестирования.

Проверка часов реального времени (RTC): проверка часов реального времени. Устройство проверяет, правильно ли работают часы, проверяя секундомер. Нажмите , чтобы выйти из теста.

13. Информация о системе

Функция информации о системе позволяет пользователям просматривать условия хранения на устройстве и версии устройства.

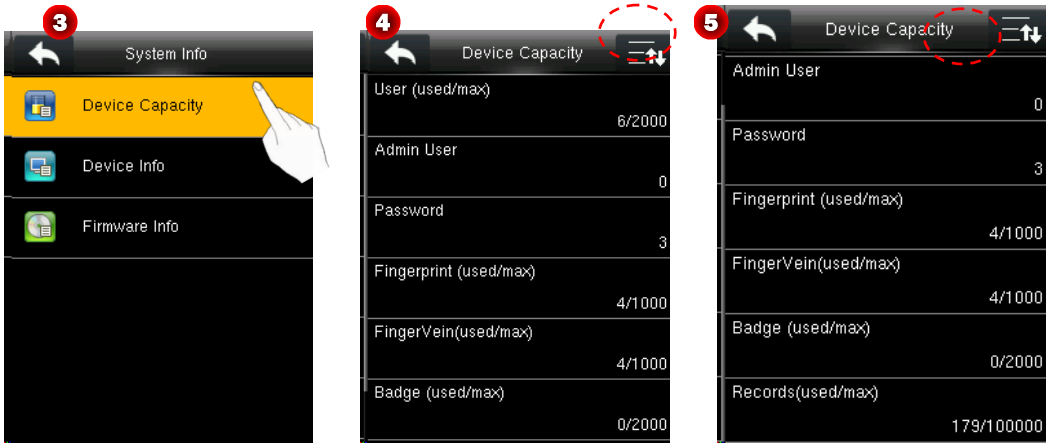
Нажмите **Информация о системе** в главном меню, чтобы войти в интерфейс **Информация о системе** (см. **Рис. 2**).



- **Емкость устройства**

Устройство отображает число зарегистрированных пользователей, количество администраторов, пароли, отпечатки пальцев, вены пальцев, количество зарегистрированных номеров значков★ и записи контроля доступа на устройстве.

Нажмите **Емкость устройства**, чтобы войти в интерфейс **Емкость устройства**. Нажмите , чтобы прокрутить экран вниз, чтобы отобразить больше контента. (Примечание. Вы можете нажать еще раз, чтобы прокрутить экран вверх).



- **Информация об устройстве**

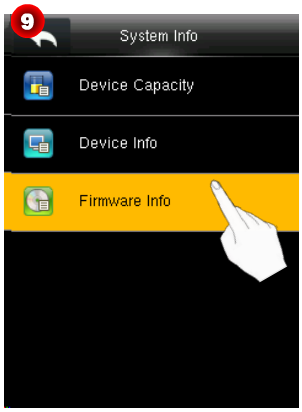
Информация об устройстве: отображает имя устройства, серийный номер, MAC-адрес, алгоритм вены пальца★, информацию о платформе, версии MCU★, производителе, дате производства.

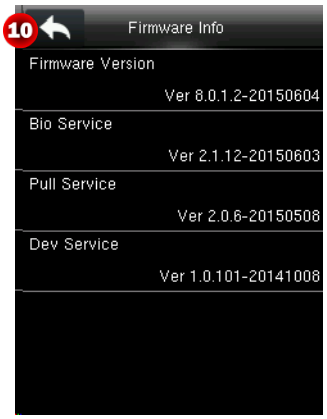
Нажмите **Информация об устройстве**, чтобы войти в интерфейс **Информация об устройстве**. Нажмите , чтобы прокрутить экран вниз, чтобы отобразить больше контента. (Примечание. Вы можете нажать еще раз, чтобы прокрутить экран вверх).



- **Информация о прошивке**

Отображение версии прошивки, службы Bio, службы Push, службы Pull и службы Dev. Нажмите **Информация о прошивке**, чтобы войти в интерфейс **Информация о прошивке**.

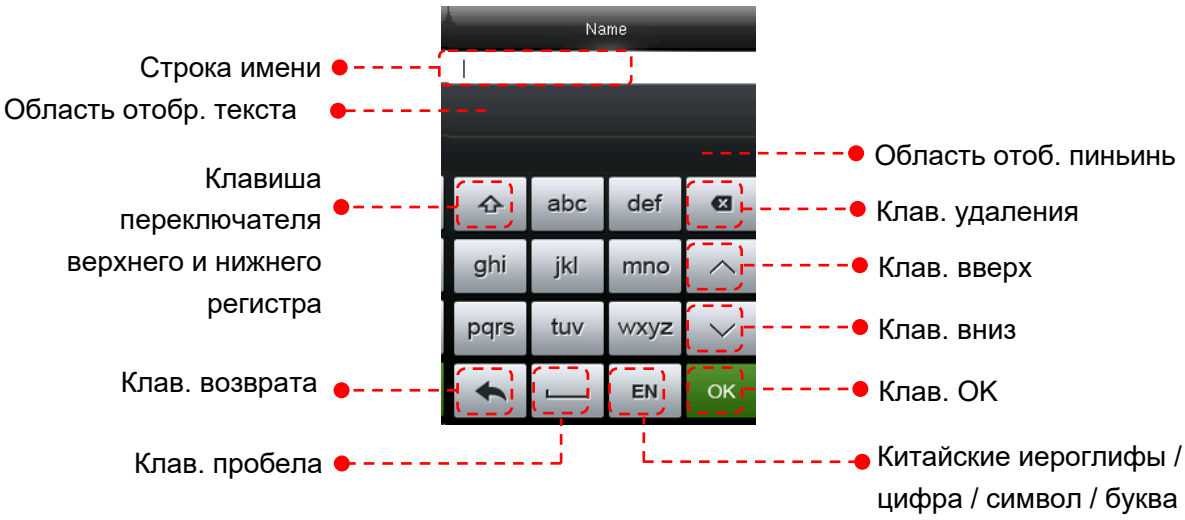

9
System Info
Device Capacity
Device Info
Firmware Info


10
Firmware Info
Firmware Version
Ver 8.0.1.2-20150604
Bio Service
Ver 2.1.12-20150603
Pull Service
Ver 2.0.6-20150508
Dev Service
Ver 1.0.101-20141008

14. Приложения

Приложение 1 Инструкции ввода текста

Устройство поддерживает китайский, английский, цифры и символы. Нажмите место, в которое необходимо ввести текст, чтобы войти в соответствующий интерфейс ввода. Например, нажмите **Имя**, чтобы войти в интерфейс **Имя**.



Следующий шаг 1 использует ввод китайского иероглифа чжун в качестве примера.

1. Нажмите на клавиатуру, чтобы ввести китайский пиньинь **чжун**. Устройство отображает соответствующий китайский пиньинь в соответствии с введенными буквами в области отображения китайского пиньинь (см. **Рис. 1**).

2. Нажмите и выберите китайский пиньинь, соответствующий вводимому китайскому символу. Устройство отображает соответствующий китайский символ в области отображения текста в соответствии с выбранным пиньинь (см. **Рис. 2**).

Примечание: Вы можете нажать или для перемещения вперед или назад, чтобы отобразить больше текстов.



3. Нажмите и выберите требуемый китайский символ в области отображения текста (см. **Рис. 4**). Выбранный символ отображается в поле **Имя** (см. **Рис. 5**).



4. Для ввода других текстов повторите шаги 1-3. После ввода необходимой информации нажмите кнопку ОК, чтобы сохранить настройки и вернуться к интерфейсу верхнего уровня.

Приложение 2 USB

Устройство служит USB-хостом, который можно подключить к USB-диску для обмена данными.

Традиционные устройства для измерения пальцев пальцев поддерживают передачу данных через RS485 или Ethernet. Когда объем данных большой, передача данных занимает очень много времени из-за ограничений физических условий. Скорость передачи данных по USB намного выше, чем у любых традиционных режимов передачи. При загрузке данных с помощью USB-диска вставьте USB-диск в устройство для загрузки данных, а затем вставьте его в ПК для импорта данных на

ПК. Кроме того, устройство поддерживает взаимную передачу пользовательской информации и данных о венах пальцев между двумя устройствами, тем самым устраняя утомительное кабельное соединение для передачи данных между традиционными устройствами и ПК.

Приложение 3 Введение в Wiegand

Протокол Wiegand26 - это стандартный протокол контроля доступа, разработанный Подкомитетом контроля доступа, входящим в Ассоциацию индустрии безопасности (SIA). Это протокол, используемый для порта и выхода бесконтактного считывателя интеллектуальных карт.

Протокол определяет порт между устройством считывания карт и контроллером, которые широко используются в управлении доступом, безопасности и других смежных отраслях. Это стандартизировало работу дизайнеров кард-ридеров и производителей контроллеров. Устройства контроля доступа, производимые нашей компанией, также применяют этот протокол.

Цифровой сигнал

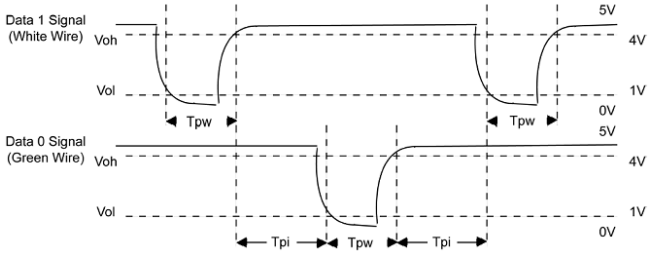
На Рис. 1 показана диаграмма последовательности устройства чтения карт, отправляющего цифровой сигнал в битах на контроллер доступа. Wiegand на этой диаграмме следует стандартному протоколу управления доступом SIA, который нацелен на 26-разрядное устройство считывания карт Wiegand (с временем импульса в пределах от 20 до 100 мкс и временем переключения импульсов в пределах от 200 мс до 20 мс). Сигналы Data1 и Data0 имеют высокий уровень (больше, чем Voh), пока устройство чтения карт не будет готово к отправке потока данных. Считыватель карт посылает асинхронный импульс низкого уровня (меньше чем Voh), передавая поток данных через кабель Data1 или Data0 на блок управления доступом (как пилообразная волна на **Рис. 1**). Импульсы Data1 и Data0 не перекрываются и не синхронизируются. На **Рис. 1** показана максимальная и минимальная ширина импульса (последовательные импульсы) и время

скачкообразного изменения импульсов (время между двумя импульсами), допустимое для терминалов контроля доступа по отпечаткам пальцев серии F.

Таблица 1: Длительность импульса

Знак	Определение	Типичное значение считывателя карт
Tpw	Ширина импульса	100 мкс
Tpi	Интервал импульса	1 мс

Figure1: Диаграмма последовательности



Приложение 3.1 Введение в Wiegand 26

Система является встроенным Wiegand 26-битным форматом.

Состав 26-битного формата Wiegand - это 2-битные биты проверки четности и 24-битный выходной контент (идентификатор пользователя или номер карты). 24-битный двоичный код может указывать 16 777 216 (0-16 777 215) различных значений.

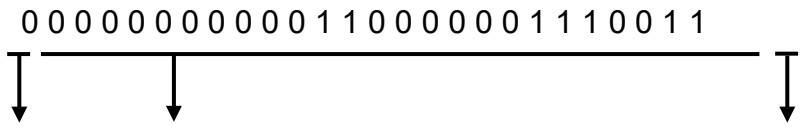
1	**2** ... **25**	**26**
Четный бит проверки четности	Идентификатор пользователя / Номер карты	Нечетный бит проверки четности

В таблице ниже описаны поля.

Поле	Описание
Четный бит проверки четности	Четный бит проверки четности определяется битами 2-13. Если имеется четное число единиц, четный бит проверки четности равен 0. Если существует нечетное число единиц, четный бит проверки четности равен 1.
Идентификатор пользователя / Номер карты (от бита 2 до бита 25)	Идентификатор пользователя / Номер карты (код карты, 0-16777215) и бит 2 указывает на самый значимый бит (MSB).
Нечетный бит проверки четности	Нечетный бит проверки нечетности определяется битами 14-25. Если есть четное число единиц, нечетный бит проверки нечетности равен 1. Если есть нечетное число единиц, нечетный бит проверки нечетности равен 0.

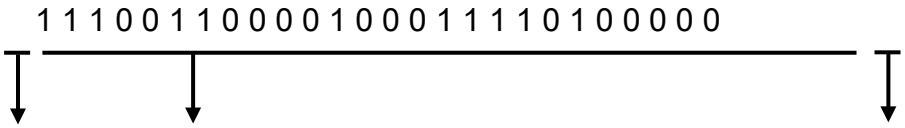
Пример: пользователь с идентификатором пользователя 12345 имеет номер карты 0013378512, а для идентификатора ошибки установлено значение 1.

1. Когда для выходного содержимого задан идентификатор пользователя и после того, как пользователь пройдет верификацию выход системы Wiegand будет выглядеть, как показано ниже.



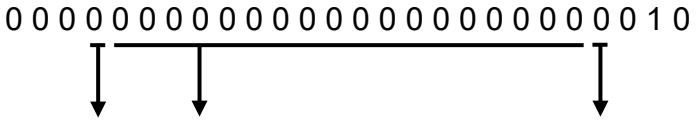
Четный бит проверки четности ID пользов. = двоич. код 12345 Нечетный бит проверки четности

2. Если для выходного содержимого задан номер карты и после того, как пользователь пройдет верификацию выход системы по Wiegand будет выглядеть, как показано ниже:



Четный бит проверки четности ID пользов. = двоич. код 0013378512 Нечетный бит проверки четности

3. При неудавшейся верификации выход системы по Wiegand будет выглядеть, как показано ниже:



Четный бит проверки четности Сбой ID = двоич. код 1 Нечетный бит проверки четности

☺**Примечание: если содержимое выхода превышает область, разрешенную для формата Wiegand, последние несколько бит будут приняты, а первые несколько бит будут автоматически отброшены. Например, идентификатор пользователя 888 888 888 равен 110 100 111 110 110 101 111 000 111 000 в двоичном формате. Wiegand26 поддерживает только 24 бита, то есть он выводит только последние 24 бита, и первые 6 бит «110 100» автоматически отбрасываются.**

Приложение 3.2 Введение в Wiegand 34

Система является встроенным Wiegand 34-битным форматом.

Состав 34-битного формата Wiegand - это 2-битные биты проверки четности и 32-битный выходной контент (идентификатор пользователя или номер карты). 32-битный двоичный код может указывать 4 294 967 296 (0-4 294 967 295) различных значений.

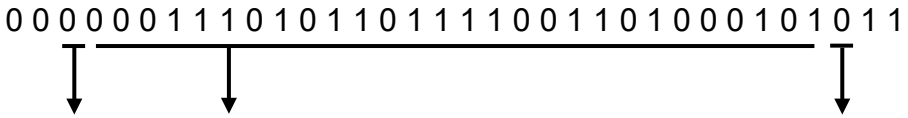
1	**2**	**33**	**34**
Четный бит проверки четности	Идентификатор пользователя / Номер карты		Нечетный бит проверки четности

В таблице ниже описаны поля.

Поле	Описание
Четный бит проверки четности	Четный бит проверки четности определяется битами 2-17. Если имеется четное число единиц, четный бит проверки четности равен 0. Если существует нечетное число единиц, четный бит проверки четности равен 1.
Идентификатор пользователя / Номер карты (от бита 2 до бита 25)	Идентификатор пользователя / Номер карты (код карты, 0-4 294 967 295) и бит 2 указывает на самый значимый бит (MSB).
Нечетный бит проверки четности	Нечетный бит проверки нечетности определяется битами 18-33. Если есть четное число единиц, нечетный бит проверки нечетности равен 1. Если есть нечетное число единиц, нечетный бит проверки нечетности равен 0.

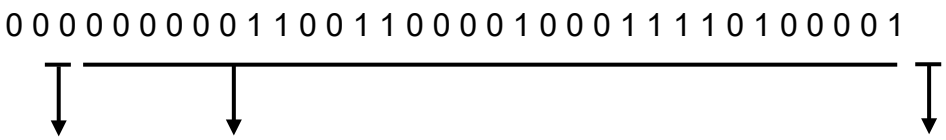
Пример: пользователь с идентификатором пользователя 123456789 имеет номер карты 0013378512, а для идентификатора ошибки установлено значение 1.

1. Когда для выходного содержимого задан идентификатор пользователя и после того, как пользователь пройдет верификацию выход системы Wiegand будет выглядеть, как показано ниже.



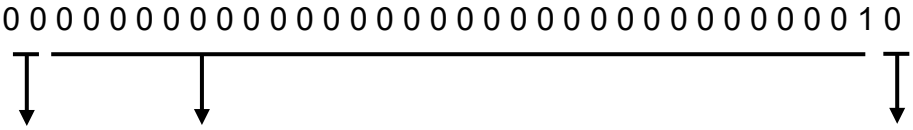
Четный бит проверки четности ID пользов. = двоич. код 123456789 Нечетный бит проверки четности

2. Если для выходного содержимого задан номер карты и после того, как пользователь пройдет верификацию выход системы по Wiegand будет выглядеть, как показано ниже.



Четный бит проверки четности ID пользов. = двоич. код 0013378512 Нечетный бит проверки четности

3. При неудавшейся верификации выход системы по Wiegand будет выглядеть, как показано ниже:

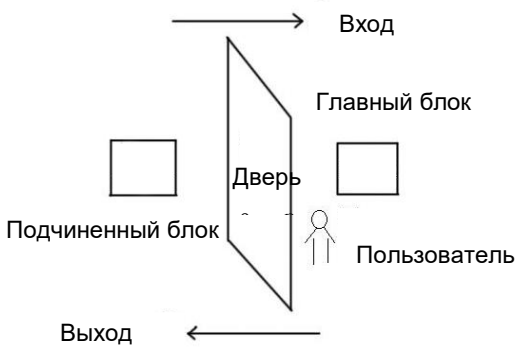


Четный бит проверки четности Сбой ID = двоич. код 1 Нечетный бит проверки четности

Приложение 4 Настройки запрета двойного прохода

Чтобы некоторые люди, следующие за пользователями, не входили в дверь без верификации, что приводило бы к проблемам с безопасностью, пользователи могут включить функцию запрета двойного прохода. Запись регистрации входа должна совпадать с записью регистрации выхода, чтобы открыть дверь.

Эта функция требует двух блоков для совместной работы: одно устанавливается внутри двери (главный блок), другое - снаружи двери (подчиненный блок). Два блока обмениваются данными с помощью сигнала Wiegand. Формат Wiegand и тип выхода (идентификатор пользователя / номер карты), принятые главным и подчиненным блоками, должны быть согласованы.



[Принцип работы]

Главный модуль поддерживает функцию Вход Wiegand, а подчиненный модуль поддерживает функцию Выход Wiegand. После того, как выходной порт Wigand подчиненного модуля подключен к входному порту Wiegand главный модуля, сигналы Wiegand, идущие из подчиненного модуля, не могут содержать идентификатор устройства, и числа, отправленные с подчиненного модуля на главный модуль, должны присутствовать на главном модуле. То есть пользовательская информация на подчиненном модуле, поддерживающем функцию запрета двойного прохода, должна отображаться в пользовательскую информацию на главном модуле, поддерживающем функцию запрета двойного прохода.

[Описание функции]

Устройство обнаруживает запрет двойного прохода на основании последней записи пользователей о регистрации входа / выхода. Запись регистрации входа должна соответствовать записи регистрации выхода. Устройство поддерживает запрет двойного прохода на выход, запрет двойного прохода на вход и запрет двойного прохода на вход / выход.

Когда для пользователя на главном блоке установлен параметр **Запрет двойного прохода на выход**, если пользователю необходимо свободно выполнить вход / выход, последняя запись пользователя должна быть записью регистрации входа. В противном случае пользователь не сможет выполнить регистрацию выхода, и запрос на выход пользователя отклоняется из-за запрета двойного прохода. Например, если последняя первая запись пользователя является записью регистрации входа, вторая запись пользователя может быть или записью регистрации входа, или записью регистрации выхода, но третья запись должна основываться на второй записи, гарантируя, что запись регистрации входа соответствует записи регистрации выхода. Примечание. Если у пользователя нет записи, он может зарегистрироваться только на вход.

Если для пользователя на главном модуле установлен параметр **Запрет двойного прохода на вход**, если пользователю необходимо свободно выполнить вход / выход, последняя запись пользователя должна быть записью регистрации выхода. В противном случае пользователь не сможет выполнить регистрацию входа, и запрос на вход пользователя отклоняется из-за запрета двойного прохода. Примечание. Если у пользователя нет записи, он может зарегистрироваться только на выход.

Если для пользователя на главном блоке установлен параметр **Запрет двойного прохода на вход / выход**, если пользователю необходимо свободно выполнить вход / выход, последняя запись пользователя должна быть записью регистрации входа или выхода. То есть, запись регистрации входа должна соответствовать записи регистрации выхода.

[Описание работы]

(1) Выбор модели

Главный блок: устройства, поддерживающие функцию Вход Wiegand, кроме считывателя F10.

Подчиненный блок: устройства, поддерживающие функцию Выход Wiegand

(2) Настройки меню

- Направление запрета двойного прохода

Параметры **Направление запрета двойного прохода** включают **Запрет двойного прохода на вход / выход, Запрет двойного прохода на выход, Запрет двойного прохода на вход** и **Отсутствие запрета двойного прохода**.

Запрет двойного прохода на выход: после того, как пользователь зарегистрировался на выход, пользователь может зарегистрироваться на выход снова, только если последняя запись является регистрацией входа.

Запрет двойного прохода на вход: после того, как пользователь зарегистрировался на вход, пользователь может зарегистрироваться на вход снова, только если последняя запись является регистрацией выхода.

- **Состояние устройства**

Параметры состояния устройства включают **Отсутствует, Выход** и **Вход**.

Отсутствует: отключить функцию Запрета двойного прохода.

Выход: все записи на устройстве являются записями регистрации выхода.

Вход: Все записи на устройстве являются записями регистрации входа.

(3) Изменение формата выхода Wiegand для устройства

Когда два устройства обмениваются данными друг с другом, принимаются только сигналы Wiegand, которые не содержат идентификатор устройства. Вы можете выбрать **Связь > Установка Wiegand** в главном меню или откройте программное обеспечение и выберите **Основная настройка > Управление устройством > Wiegand** и установите **Определенный формат** для **Wiegand26-bits** или **Wiegand26 без идентификатора устройств**.

(4) Регистрация пользователя

Идентификаторы пользователя должны существовать как на главном, так и на подчиненном блоках, и идентификаторы пользователя должны быть согласованными. Следовательно, пользователи должны быть зарегистрированы как на главном, так и на подчиненном блоках.

(5) Описание проводки

Главный и подчиненный блоки обмениваются данными друг с другом по Wiegand, а схема подключения следующая:

Главный блок		Починенный блок
IND0	<----->	WD0
IND1	<----->	WD1
GND	<----->	GND

Заявление о правах человека и конфиденциальности

Уважаемые клиенты:

Благодарим Вас за выбор гибридных биометрических продуктов, разработанных и изготовленных нами. Как всемирно известный поставщик биометрических технологий и услуг, мы уделяем большое внимание соблюдению законов, касающихся прав человека и неприкосновенности частной жизни в каждой стране, постоянно проводя исследования и разработки.

Настоящим мы делаем следующие заявления:

1. Все наши устройства распознавания отпечатков пальцев для гражданского использования собирают только характерные точки отпечатков пальцев, а не изображения отпечатков пальцев, и, следовательно, никаких проблем конфиденциальности.
2. Характерные точки отпечатков пальцев, собранные нашими продуктами, не могут быть использованы для восстановления оригинальных изображений отпечатков пальцев, и, следовательно, никаких проблем конфиденциальности.
3. Мы, как поставщик оборудования, не несем юридической, прямой или косвенной ответственности за какие-либо последствия, возникшие в результате использования наших продуктов.
4. По любым спорам, связанным с правами человека или неприкосновенностью частной жизни при использовании наших продуктов, обращайтесь напрямую к своему работодателю.

Наше другое полицейское оборудование или средства разработки отпечатков пальцев обеспечат функцию сбора исходного отпечатка пальца граждан. Что касается того, является ли такой тип сбора отпечатков пальцев нарушением вашей конфиденциальности, пожалуйста, свяжитесь с правительством или конечным поставщиком оборудования. Мы, как производитель оригинального оборудования, не несем юридической ответственности за любые нарушения, возникающие в связи с этим.

Закон Китайской Народной Республики содержит следующие положения, касающиеся свободы личности:

1. Незаконный арест, задержание или обыск граждан Китайской Народной Республики запрещены; Нарушение частной жизни запрещено.
2. Личное достоинство граждан Китайской Народной Республики не прикосновенно.
3. Дом граждан Китайской Народной Республики не прикосновенен.
4. Свобода и тайна переписки граждан Китайской Народной Республики охраняются законом.

Наконец, мы еще раз подчеркиваем, что биометрия, как передовая технология распознавания, будет применяться во многих секторах, включая электронную коммерцию, банковское дело, страхование и юридические вопросы. Каждый год люди во всем мире страдают от огромных потерь из-за ненадежности паролей. Распознавание отпечатков пальцев на самом деле обеспечивает адекватную защиту вашей личности в условиях высокой безопасности.

Описание экологичного использования



Период экологичного использования (EFUP), обозначенный на этом продукте, относится к периоду безопасности, в течение которого продукт используется в условиях, указанных в инструкциях по продукту, без утечки вредных и вредных веществ.
EFUP этого продукта не распространяется на расходные материалы, которые необходимо регулярно заменять, такие как батареи и т. д. ЭФУП батарей 5 лет.

Названия и концентрация токсичных и опасных веществ или элементов						
Название частей	Наименование частей Токсичные и опасные вещества или элементы					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Чип резистор	×	○	○	○	○	○
Чип конденсатор	×	○	○	○	○	○
Чип индуктор	×	○	○	○	○	○
Чип диод	×	○	○	○	○	○

Компоненты ESD	×	○	○	○	○	○
Зуммер	×	○	○	○	○	○
адаптер	×	○	○	○	○	○
Винты	○	○	○	×	○	○

○: Указывает, что это токсичное или опасное вещество, содержащееся во всех однородных материалах для этой части, ниже предельного требования в SJ / T11363-2006.

×: Указывает, что это токсичное или опасное вещество, содержащееся по крайней мере в одном из однородных материалов для этой части, превышает предельное требование в SJ / T11363-2006.

Примечание: 80% деталей в этом продукте изготовлены из неопасных для окружающей среды материалов. Содержащиеся в них опасные вещества или элементы в настоящее время не могут быть заменены экологически чистыми материалами из-за технических или экономических ограничений.