

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

ProCapture-WP

Версия: 1.0

Дата: январь, 2019

Green
Label

Обзор Руководства

- Данное руководство знакомит с работой пользовательских интерфейсов и функций меню терминала контроля доступа ProCapture-WP.
- Изображения в этом руководстве могут не полностью соответствовать изображению вашего устройства; фактическое отображение устройства имеет преимущественную силу.
- Не все устройства имеют функцию ★, реальное устройство имеет преимущественную силу.

Содержание

1 Инструкция по применению	6
1.1 Способ размещения пальцев.....	6
1.2 Режимы верификации	7
1.2.1 Верификация отпечатков пальцев 1:N	7
1.2.2 Верификация отпечатков пальцев 1:1	7
1.2.3 Верификация паролем	8
1.2.4 Верификация карты.....	9
1.3 Начальный интерфейс	9
2 Главное меню	10
3 Настройки даты / времени	12
3.1 DST	12
4 Управление пользователями	15
4.1 Добавить пользователя.....	15
4.2 Настройка контроля доступа.....	16
4.3 Поиск пользователя	17
4.4 Редактировать пользователя.....	17
4.5 Удаление пользователя	18
4.6 Стиль отображения пользователя.....	18
5 Роль пользователя	19
5.1 Прописывание роли пользователя.....	19
5.2 Назначение прав.....	20
6 Настройка связи.....	21
6.1 Настройки Ethernet	21
6.2 Настройки последовательной связи	21
6.3 Подключение ПК	22
6.4 ADMS.....	23
6.5 Установка Wiegand	24
6.5.1 Вход Wiegand	24
6.5.2 Выход Wiegand	27
6.5.3 Формат карты определяется автоматически	28

7	Системные настройки.....	30
7.1	Настройки журналов доступа.....	30
7.2	Параметры отпечатков пальцев.....	31
7.3	Сброс до заводских настроек.....	32
8	Персонализация настройки.....	34
8.1	Настройки пользовательского интерфейса.....	34
8.2	Голосовые настройки.....	35
8.3	Настройки звонки.....	36
8.3.1	Добавить новый звонок.....	36
8.3.2	Редактировать звонок.....	37
8.3.3	Удалить звонок.....	37
9	Управление данными.....	38
9.1	Удаление данных.....	38
9.2	Резервное копирование данных.....	38
9.3	Восстановление данных.....	40
10	Контроль доступа.....	41
10.1	Настройки параметров контроля доступа.....	42
10.2	Настройки временных правил.....	44
10.3	Настройки праздников.....	45
10.3.1	Добавление праздника.....	46
10.3.2	Все праздники.....	47
10.4	Настройки комбинированной верификации.....	48
10.5	Настройки запрета двойного прохода.....	50
11	Интеллектуальная карта★.....	52
11.1	Зарегистрировать в качестве идентификационной карты.....	52
11.2	Зарегистрировать в качестве Карты отпечатков пальцев.....	53
11.3	Очистить данные карты.....	54
11.4	Копировать данные карты.....	55
11.5	Параметры Интеллектуальных карт.....	56
12	Поиск записей.....	58
13	Автоматическое тестирование.....	59

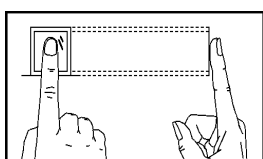
14	Информация о системе	61
15	Устранение неполадок.....	62
16	Приложения.....	63
16.1	Обзор Wiegand.....	63
16.1.1	Обзор Wiegand 26	64
16.1.2	Обзор Wiegand 34	65
16.2	Правило загрузки изображения.....	67
16.3	Настройки запрета двойного прохода.....	67
16.4	Заявление о правах человека и конфиденциальности.....	70
16.5	Описание экологичного использования.....	72

1 Инструкция по применению

1.1 Способ размещения пальцев

Рекомендуется использовать указательный, средний или безымянный; большой и мизинец использовать не рекомендуется.

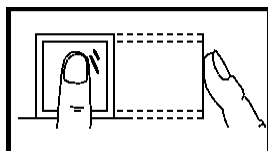
1. Правильное расположение пальцев:



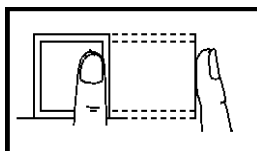
Прижмите палец горизонтально к датчику отпечатка пальца; центр отпечатка пальца должен быть помещен в центр датчика.

2. Неправильное расположение пальцев:

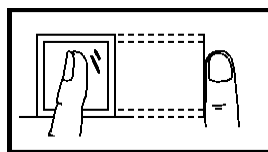
Вертикальное



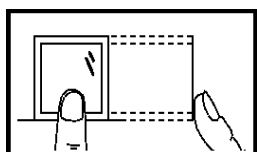
Боковой стороной



Под углом



Не по центру



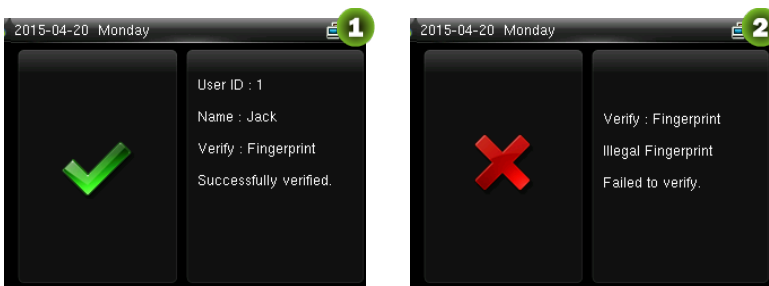
Пожалуйста, используйте правильный метод нажатия отпечатков пальцев для регистрации и верификации. Наша компания не несет ответственности за снижение эффективности верификации, вызванное неправильной работой пользователя. Права на окончательное толкование и изменение защищены.

1.2 Режимы верификации

1.2.1 Верификация отпечатков пальцев 1:N

В соответствии с методом верификации отпечатков пальцев отпечаток пальца, собранный датчиком, проходит верификацию со всеми отпечатками пальцев, хранящимися на устройстве.

Пожалуйста, используйте правильный способ прижима отпечатков пальца к датчику отпечатка пальца (для получения подробных инструкций см. 1.1 Способ прижима отпечатка пальца).

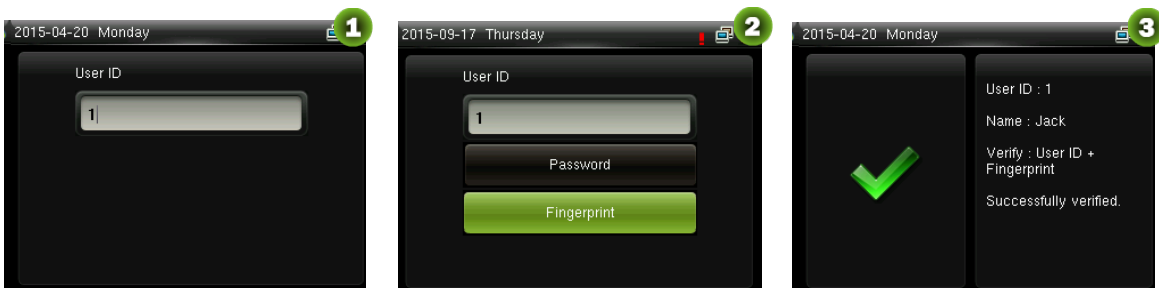


Верификация прошла успешно

Верификация не удалась

1.2.2 Верификация отпечатков пальцев 1:1

В соответствии со способом верификации отпечатка пальца отпечаток пальца, собранный датчиком, проходит верификацию по отпечатку пальца, соответствующему введенному идентификатору пользователя. Пожалуйста, используйте этот способ, когда возникают трудности при верификации отпечатков пальцев 1:N.



Введите идентификатор пользователя и нажмите ➤

Нажмите кнопку V, чтобы выбрать «Отпечаток пальца» и нажмите ➤. После этого прижмите палец к датчику

Верификация прошла успешно



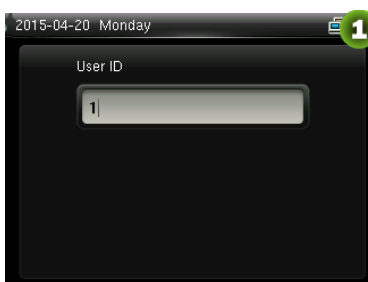
Верификация не удалась

☺ Примечания:

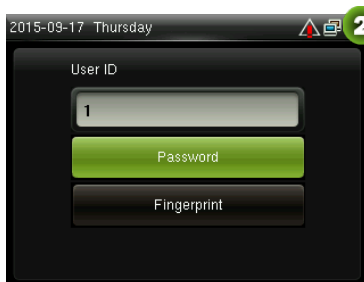
1. Введите идентификатор пользователя в начальный интерфейс и нажмите кнопку ➔. Если отображается «Неверный идентификатор пользователя!», Это означает, что идентификатор пользователя не существует.
2. Когда на устройстве отобразится сообщение «Пожалуйста, нажмите еще раз», снова прижмите палец к датчику отпечатков пальцев. Если после 2 попыток верификация по-прежнему не удалась, она вернется к начальному интерфейсу.

1.2.3 Верификация паролем

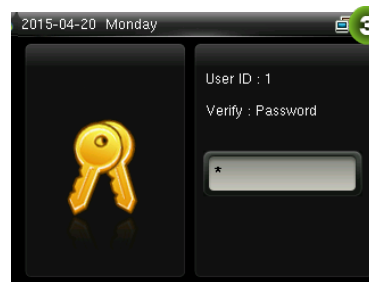
При таком способе верификации введенный пароль проверяется паролем введенного идентификатора пользователя.



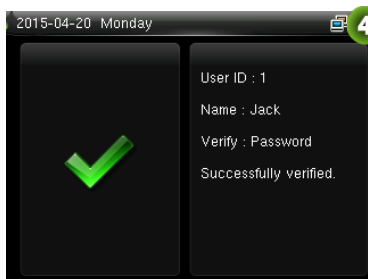
Введите идентификатор пользователя и нажмите ➔



Выберите «Пароль» и нажмите ➔



Введите пароль



Верификация прошла успешно

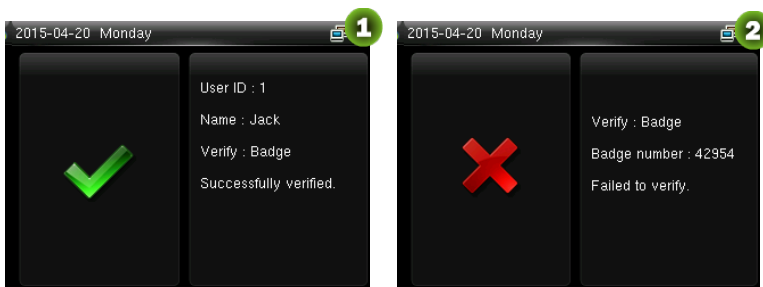


Верификация не удалась

☺ **Примечания:** If “Incorrect password” is displayed, please enter the password again. If verification still fails after 2 attempts, it will exit to the initial interface.

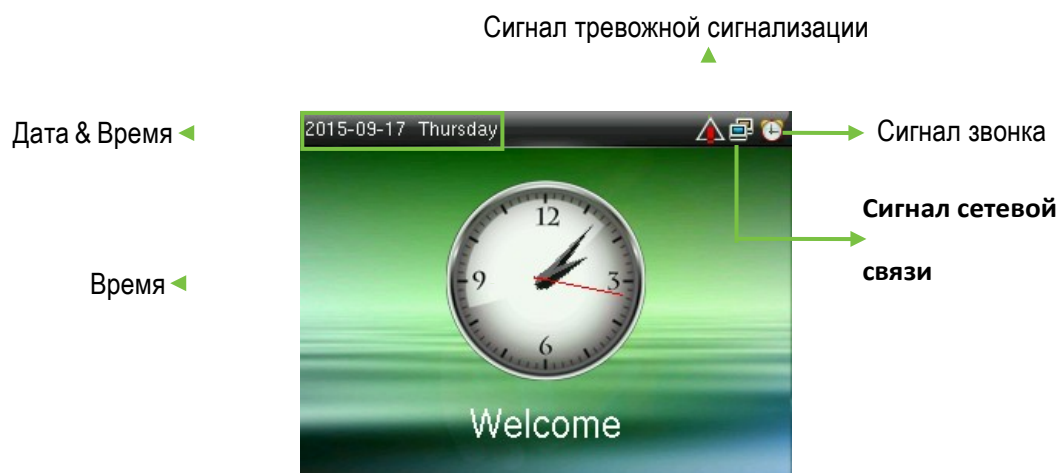
1.2.4 Верификация карты

1. Просканируйте карту (карта должна быть зарегистрирована в первую очередь).
2. Верификация прошла успешно
3. Верификация не удалась




1.3 Начальный интерфейс

Когда устройство включено, начальный интерфейс отображается, как показано ниже:



2 Главное меню

Когда устройство находится в режиме ожидания, нажмите , чтобы войти в Главное меню.



Управление пользователями: основная информация о зарегистрированных пользователях, включая идентификатор пользователя, роль пользователя, отпечаток пальца, карту, пароль и роль контроля доступа.

Роль пользователя: установка пользовательских ролей для доступа в меню и изменения настроек.

Связь: для настройки соответствующих параметров связи между устройством и ПК, включая параметры Ethernet, такие как IP-адрес и т. д., последовательный порт, соединение с ПК, настройки ADMS и Wiegand.

Система: для установки соответствующих параметров системы, включая настройку даты и времени, журналов доступа, параметров отпечатков пальцев и восстановления заводских настроек.

Персонализация: включает отображение интерфейса, настройки голоса и звонка.

Управление данными: удаление записей доступа, удаление всех данных, удаление роли администратора, удаление экранных заставок и резервного копирования, восстановление данных.

Контроль доступа: для настройки параметров блокировки управления и устройств контроля доступа, в том числе параметров контроля доступа, правил времени, выходных, комбинированной разблокировки и запрета двойного прохода.

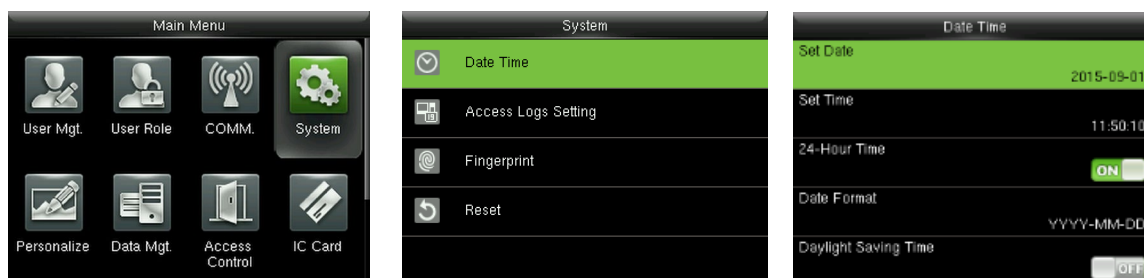
Интеллектуальная карта ★: это меню поддерживает интеграцию учета рабочего времени по отпечаткам пальцев и идентификационной карты с другими системами или устройствами с помощью зарегистрированной карты Mifare, а также поддерживает режим многократной верификации для удовлетворения потребностей разных людей.


Поиск учета рабочего времени: поиск записей, сохраненных на устройстве, после успешной верификации.

Автоматическое тестирование: для автоматического тестирования различных функций модуля, включая ЖК-дисплей, голос, клавиатуру, датчик отпечатков пальцев и проверку часов RTC.

Информация о системе: для проверки емкости устройства, информации об устройстве и прошивке.

3 Настройки даты / времени



В начальном интерфейсе нажмите  > Система > Дата Время, чтобы войти в интерфейс настройки даты / времени. Он включает в себя настройку даты, времени, 24-часовых часов, формата даты и летнего времени.

При восстановлении к заводским настройкам формат даты может быть восстановлен (ГГГГ-ММ-ДД).



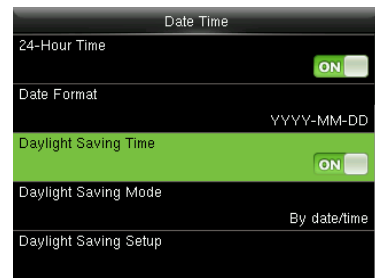
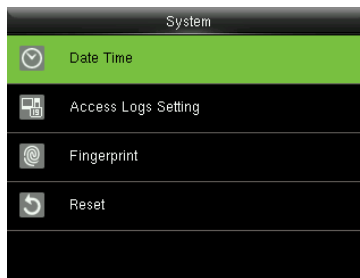
Примечания: При сбросе к заводским настройкам дата / время устройства не будут восстановлены

(если дата / время установлены на 18:30 1 января 2020 года, после сброса настроек дата / время останутся равными 18:30 на 1 января 2020 г.

3.1 DST

DST, также называемое летним временем, представляет собой систему, регулирующую местное время для экономии энергии. Время, принятое в установленные даты, называется «летнее время». Обычно время будет на один час вперед летом. Это позволяет пользователям спать или вставать раньше, а также уменьшать освещение устройства для экономии энергии. Осенью проходи переход на стандартное время. Правила разные в разных странах. В настоящее время почти 110 стран принимают DST.

Чтобы удовлетворить спрос DST, может быть настроен специальный параметр. Переведите время на час вперед в XX (час) XX (день) XX (месяц), и переведите время на час назад в XX (час) XX (день) XX (месяц).



Нажмите > Система > Дата Время > Летнее время, затем нажмите , чтобы включить Летнее время.

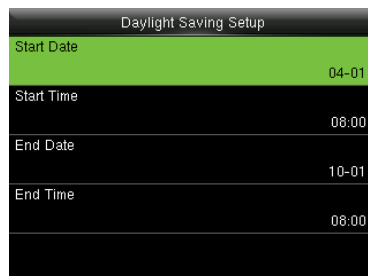
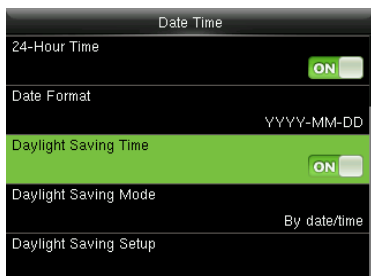
Режим летнего времени: режим летнего времени, режим даты / времени и режим недели / дня для выбора.

Настройка перехода на летнее время: установите дату / время или неделю / день для летнего времени в соответствии с выбором в режиме перехода на летнее время.

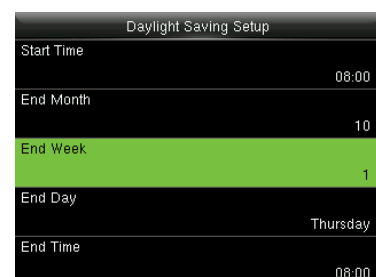
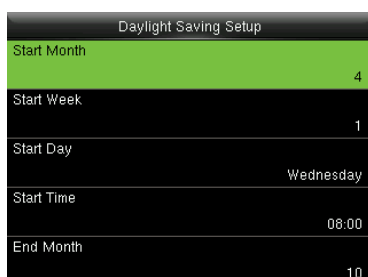
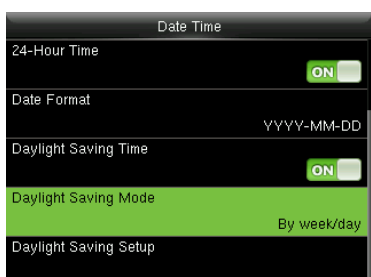
Как установить летнее время?

Например, настройте часы вперед на один час в 08:00 часов 1 апреля и назад на один час в 08:00 часов 1 октября (система возвращается к исходному времени).

- Режим настройки по дате / времени:



- Режим настройки по неделе / дате:



Примечания:

1. Если месяц, когда начинается летнее время, позже месяца, когда заканчивается летнее время, летнее время охватывает два разных года. Например, время начала летнего времени - 2014-9-1 4:00, а время окончания летнего времени - 2015-4-1 4:00.

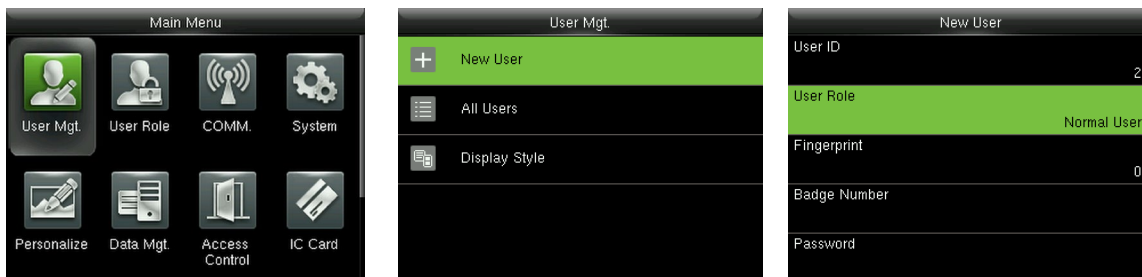
2. Предположим, что режим недели / дня выбран в [**Режим летнего времени**], и летнее время начинается с воскресенья шестой недели сентября 2013 года. Согласно календарю, сентябрь 2014 года не имеет шести недель, но имеет пять недель. В этом случае, в 2014 году, летнее время начинается в соответствующий момент последнего воскресенья сентября.


Предположим, что летнее время начинается с понедельника первой недели сентября 2014 года. Согласно календарю, первая неделя сентября 2015 года не имеет понедельника. В этом случае летнее время начинается с первого понедельника сентября 2015 года.

4 Управление пользователями

4.1 Добавить пользователя

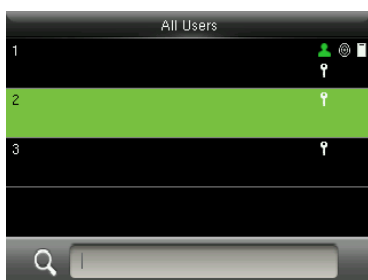
Включая добавление супер администратора и обычного пользователя.



В начальном интерфейсе нажмите  > Управление пользователями > Новый пользователь, чтобы войти в интерфейс настройки нового пользователя. Настройки включают ввод идентификатора пользователя, выбор роли пользователя (обычный пользователь / супер-администратор), регистрацию отпечатка пальца и номер карты, установку пароля и настройку роли контроля доступа.

Добавить Super Admin: выберите «Super Admin» в [Роль пользователя], которому разрешено управлять всеми функциями в меню.

Как показано ниже, пользователь с идентификатором пользователя 1 является супер-администратором



Добавить обычного пользователя: выберите «Обычный пользователь» в [Роль пользователя].

Когда установлен Суперадминистратор, обычные пользователи могут использовать только отпечаток пальца, пароль или карту для верификации; когда Суперадминистратор еще не установлен, обычные пользователи могут управлять всеми функциями в меню.

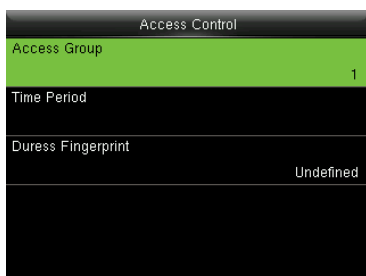
Пароль: от 1 до 8 цифр пароля.

Примечания:

1. Устройство автоматически распределяет идентификатор пользователя по порядку, но пользователь также может установить его вручную.
2. Устройство поддерживает идентификатор пользователя в диапазоне от 1 до 9 цифр.

4.2 Настройка контроля доступа

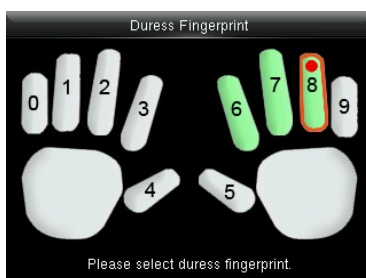
Параметр контроля доступа пользователя заключается в настройке ориентированного на всех доступа для открытия двери, включая настройку группы доступа, использование периода времени, управление отпечатками пальцев принуждения.



Группа доступа: для распределения пользователей по разным группам контроля доступа для управления. В настройках по умолчанию новые пользователи принадлежат группе 1, которую можно перераспределить в другие группы. Допустимый номер группы варьируется от 1 до 99.

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

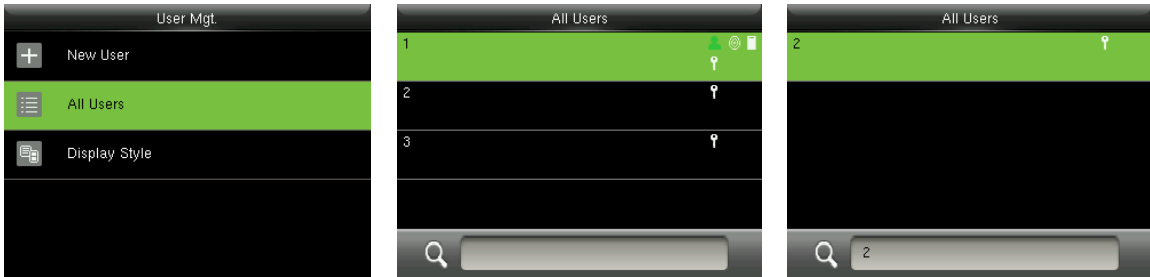
Отпечаток пальца принуждения: Пользователь может выбрать один или несколько зарегистрированных отпечатков пальцев в качестве отпечатка пальца принуждения. Если произойдет верификация этого отпечатка, сработает сигнализация принуждения.





Пример: Среди этих зарегистрированных отпечатков пальцев (6, 7, 8) выберите восьмой отпечаток пальца как отпечаток принуждения.

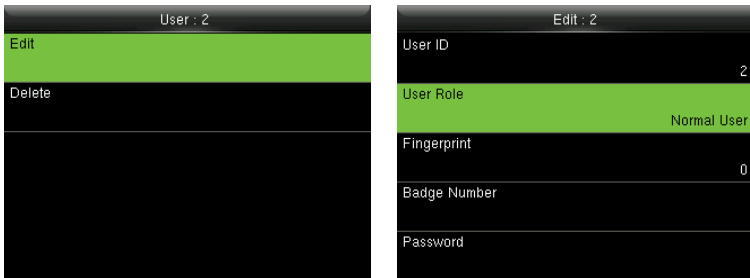
4.3 Поиск пользователя


Введите идентификатор пользователя в списке [Все пользователи] поиска пользователя.





В начальном интерфейсе нажмите  > **Управление пользователями** > **Все пользователи**, чтобы войти в интерфейс Все пользователи. Введите «Идентификатор пользователя» в , и соответствующий пользователь будет показан. Как показано на приведенном выше рисунке, выполните поиск пользователя с идентификатором пользователя «2».

4.4 Редактировать пользователя

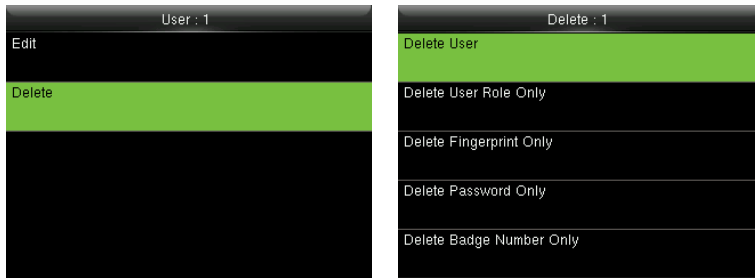



После выбора пользователя с помощью раздела 4.3 Поиск пользователя нажмите  и выберите [Изменить], чтобы войти в интерфейс редактирования пользователя.



Или в начальном интерфейсе нажмите  > **Управление пользователями** > **Все пользователи** > **Поиск пользователя** > Нажмите  > **Изменить**, чтобы войти в интерфейс редактирования пользователя.


Способ редактирования пользователя такой же, как и при добавлении пользователя, но идентификатор пользователя редактировать нельзя.

4.5 Удаление пользователя

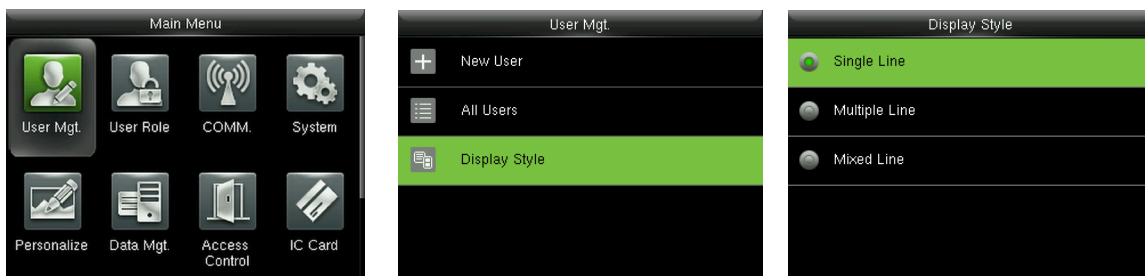



После выбора пользователя с помощью раздела 4.3 Поиск пользователя нажмите  и выберите [Удалить], чтобы ввести интерфейс удаление пользователя.

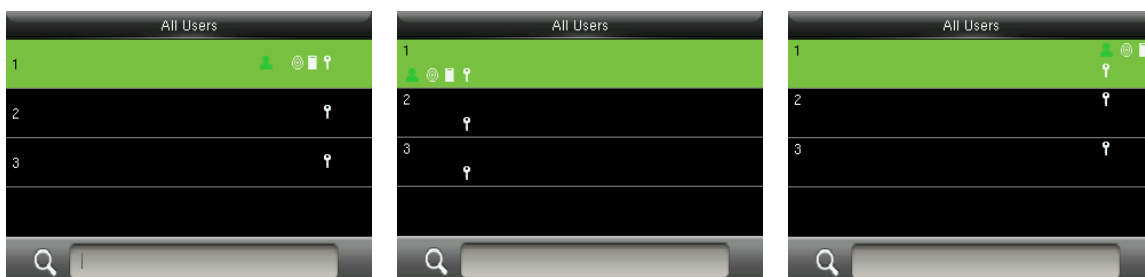
Или в начальном интерфейсе нажмите  > Управление пользователями > Все пользователи > Поиск пользователя > Нажмите  > Удалить, чтобы войти в интерфейс удаления пользователя. Выберите информацию пользователя для удаления или удалите всего пользователя.

 **Примечание:** соответствующий элемент, подлежащий удалению, будет отображаться, только если пользователь зарегистрировал отпечаток пальца, пароль и карту.

4.6 Стиль отображения пользователя



В начальном интерфейсе нажмите  > Управление пользователями > Стиль отображения, чтобы войти в интерфейс настройки стиля отображения. Несколько стилей отображения показаны ниже:



Стиль одной линии

Множественная линия

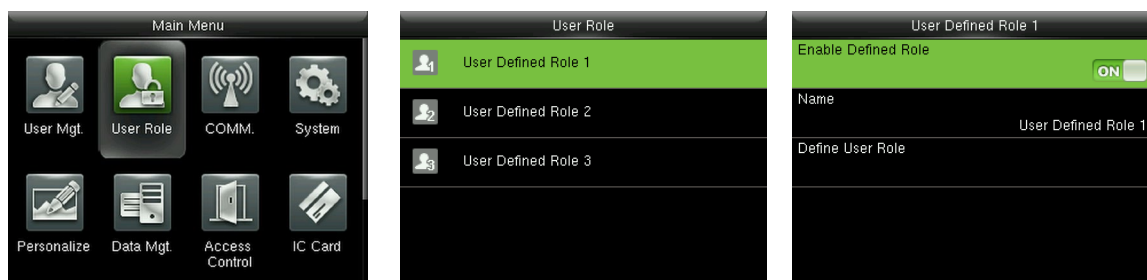
Смешанная линия


5 Роль пользователя

Настройка прав пользователя на управление меню (можно установить максимум 3 роли). Когда роль пользователя включена, в меню [Управление пользователями]> [Новый пользователь]> [Роль пользователя] вы можете назначить подходящую роль для каждого пользователя.

Роль: Суперпользователь должен предоставить новые права новым пользователям. Чтобы избежать настройки прав для каждого пользователя персонально, вы можете установить роли пользователей, чтобы классифицировать различные уровни прав доступа в управлении пользователями.

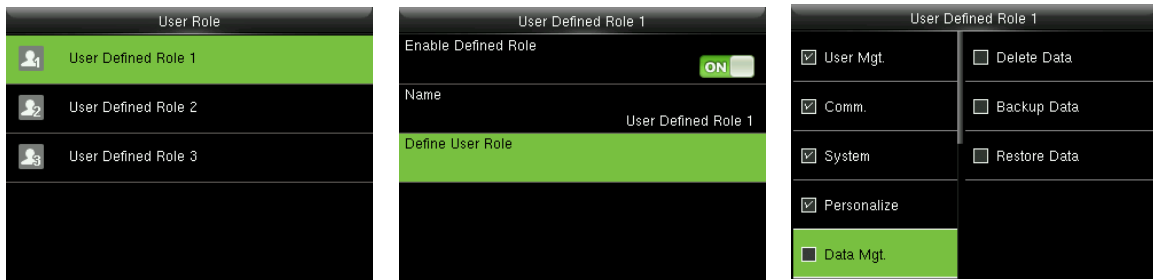
5.1 Прописывание роли пользователя



В начальном интерфейсе нажмите  > Роль пользователя > Определенная роль пользователя 1 (2/3)
> Включить определенную роль. Нажмите, чтобы включить определенную роль.

После включения определенных ролей вы можете проверить включенные роли пользователя в [Управление пользователями]> [Новый пользователь]> [Роль пользователя].

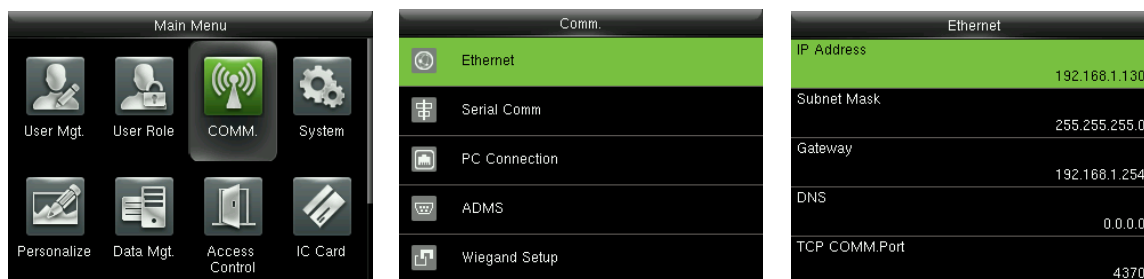
5.2 Назначение прав



В начальном интерфейсе нажмите > Роль пользователя > Определенная роль пользователя 1 (2/3) > Включить определенную роль, чтобы войти в меню **Определенная роль пользователя 1 (2/3)** интерфейса назначения прав. Нажмите , чтобы выбрать или отменить право на каждое меню для Определенной роли пользователя 1 (2/3). После выбора нажмите , чтобы вернуться к Определенной роли пользователя 1 (2/3) интерфейса редактирования.

6 Настройка связи

6.1 Настройки Ethernet



В начальном интерфейсе, нажмите > Связь > Ethernet, чтобы войти в меню настройки Ethernet.

Приведенные ниже параметры являются заводскими значениями по умолчанию, пожалуйста, настройте 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. Если DHCP включен, IP не может быть установлен вручную.

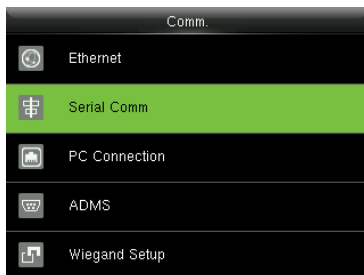
Отображать в строке состояния: установить, отображать ли значок в строке состояния.

6.2 Настройки последовательной связи

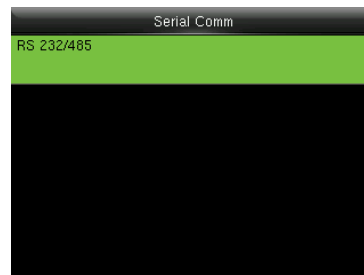
- Включение / выключение функции RS485



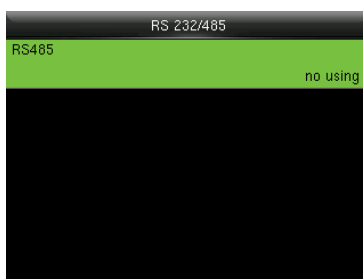
В начальном интерфейсе, нажмите \Rightarrow , чтобы войти в главное меню и нажмите $>$, чтобы выбрать Связь.



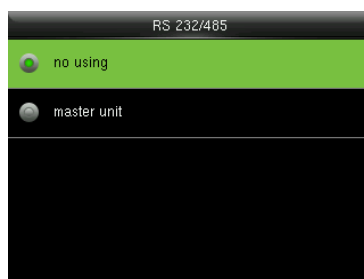
Нажмите клавишу \vee , чтобы выбрать Последовательная связь и нажмите \Rightarrow , чтобы войти.



Выберите **RS232/485** и нажмите \Rightarrow , чтобы войти.



Выберите RS485 и нажмите \Rightarrow , чтобы войти



Нажмите клавишу \vee , чтобы выбрать RS485 как функцию «Главный модуль» или выбрать отключить RS485

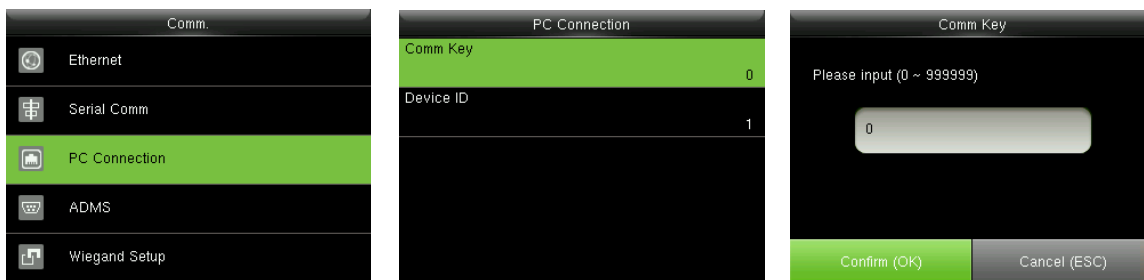
☺ Примечание:

Когда RS485 используется как функция «Главного модуля», устройство будет работать как «Главный модуль», и его можно подключить к считывателю отпечатков пальцев RS485.

6.3 Подключение ПК

- Настройки клавиши связи

Для повышения безопасности данных необходимо установить Клавишу связи для связи между устройством и ПК. Если в устройстве установлена Клавиша связи, необходимо ввести правильный пароль подключения, когда устройство подключено к программному обеспечению ПК, чтобы устройство и программное обеспечение могли обмениваться данными.

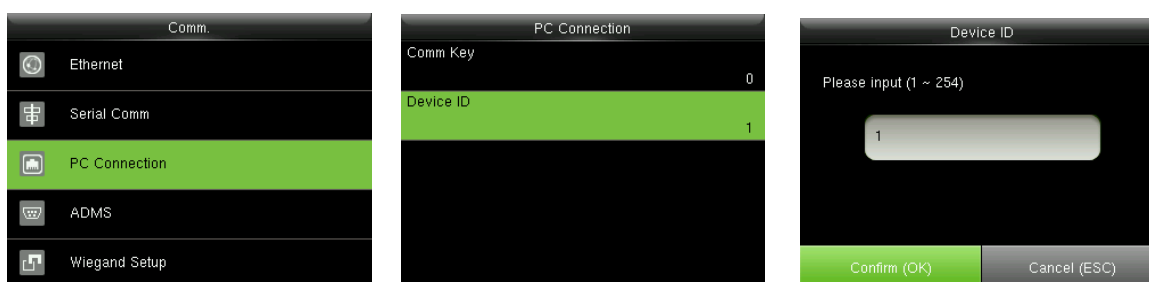


В начальном интерфейсе нажмите > Связь > Подключение к ПК > Клавиша связи для ввода интерфейса настройки Клавиши связи.

Клавиша связи: пароль по умолчанию - 0 (без пароля). Клавиша связи может содержать от 1 до 6 цифр и находится в диапазоне от 0 до 999999.

- Настройки идентификатора устройства

Если используется метод связи RS232 / RS485, необходимо ввести этот идентификатор устройства в программный интерфейс связи.

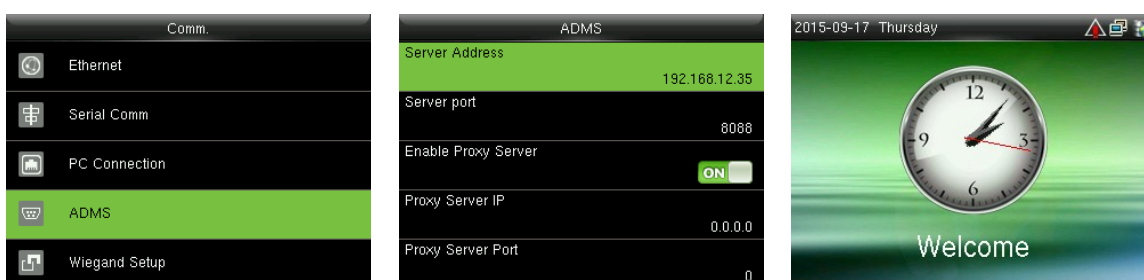




В начальном интерфейсе нажмите > Связь > Подключение ПК > Идентификатор устройства, чтобы войти в интерфейс настроек идентификатора устройства.

Идентификатор устройства: идентификационный номер устройства, который находится в диапазоне от 1 до 254.

6.4 ADMS

Параметры, используемые для подключения к серверу ADMS, такие как IP-адрес и настройки порта, а также необходимость включения прокси-сервера и т. д.



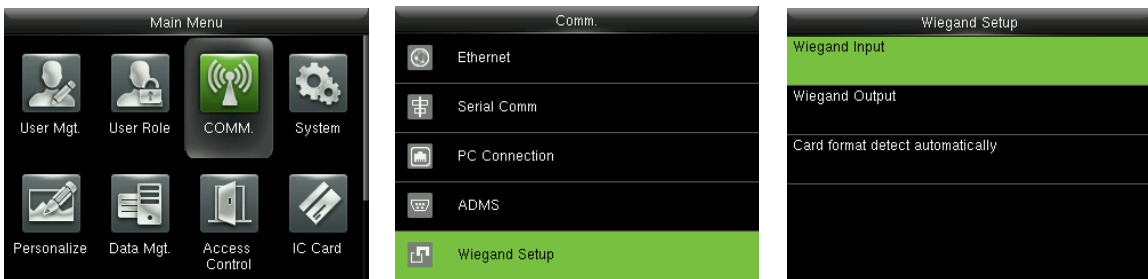
В начальном интерфейсе нажмите  > **Связь** > **ADMS**, чтобы войти в интерфейс настройки сервера ADMS. Когда веб-сервер подключен успешно, основной интерфейс будет отображать логотип .


Адрес сервера: введите IP-адрес сервера ADMS (а именно, IP-адрес сервера, на котором установлено программное обеспечение).

Порт сервера: введите номер порта, используемый сервером ADMS.

Включить прокси-сервер: метод включения прокси. Чтобы включить прокси, пожалуйста, установите IP-адрес и номер порта прокси-сервера. Ввод IP прокси и адреса сервера будет одинаковым.

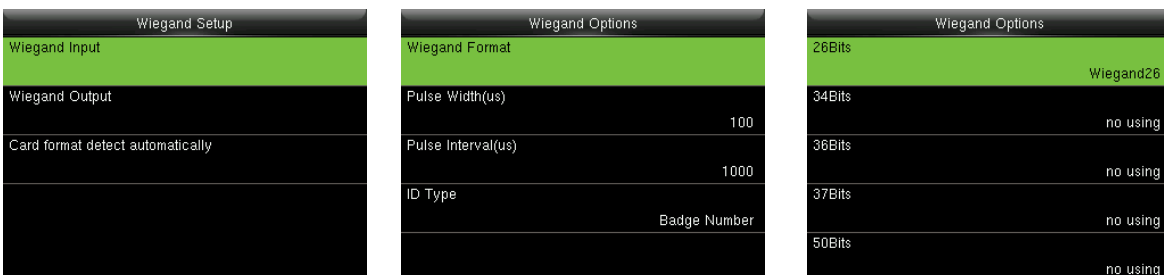
6.5 Установка Wiegand




В начальном интерфейсе нажмите  > **Связь** > **Установка Wiegand**, чтобы войти в интерфейс настроек Установка Wiegand.

6.5.1 Вход Wiegand

Разъем вход Wiegand поддерживает устройство чтения карт или подключает устройство как главный модуль к другому модулю (подчиненный модуль), образуя главную / подчиненную систему.



Выбрать “Вход Wiegand” и нажмите , чтобы войти

Установите параметры в интерфейсе “Вход Wiegand”

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.

Ширина импульса (мкс): ширина импульса, посылаемая устройством считывания карт 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. **Идентификатор пользователя** или **Номер карты** могут быть выбраны.

Определения формата Wiegand:

Формат Wiegand	Определение
Wiegand26	<p>ECCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>Состоит из 26 бит двоичного кода. 1-й бит является четным битом четности от 2-го до 13-го битов, а 26-й бит является нечетным битом четности от 14-го до 25-го битов. 2-25 биты - это номер карты.</p>
Wiegand26a	<p>ESSSSSSSCCCCCCCCCCCCCCCCCO</p> <p>Состоит из 26 бит двоичного кода. 1-й бит является четным битом четности от 2-го до 13-го битов, а 26-й бит является нечетным битом четности от 14-го до 25-го битов. 2-9-й бит - это код сайта, а 10-25-й - номер карты.</p>
Wiegand34	<p>ECCCCCCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>Состоит из 34 бит двоичного кода. 1-й бит является четным битом четности от 2-го до 17-го битов, а 34-й бит является нечетным битом четности от 18-го до 33-го битов. 2-25 биты - это номер карты.</p>
Wiegand34a	<p>ESSSSSSSCCCCCCCCCCCCCCCCCCCCCO</p> <p>Состоит из 34 бит двоичного кода. 1-й бит является четным битом четности от 2-го до 17-го битов, а 34-й бит является нечетным битом четности от 18-го до 33-го битов. 2-9-й бит - это код сайта, а 10-25-й - номер карты.</p>


Wiegand36	<p>OFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME</p> <p>Состоит из 36 бит двоичного кода. 1-й бит является нечетным битом четности от 2-го до 18-го битов, а 36-й бит является четным битом четности от 19-го до 35-го битов. Биты со 2-го по 17-й - это код устройства, биты с 18-го по 33-й - это номер карты, а биты с 34-го по 35-й - это код производителя.</p>
Wiegand36a	<p>FFFFFFFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCO</p> <p>Состоит из 36 бит двоичного кода. 1-й бит является четным битом четности от 2-го до 18-го битов, а 36-й бит является нечетным битом четности от 19-го до 35-го битов. 2–19-й бит - это код устройства, а 20–35-й - номер карты.</p>
Wiegand37	<p>OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE</p> <p>Состоит из 37 бит двоичного кода. 1-й бит является нечетным битом четности со 2-го по 18-й биты, а 37-й бит является четным битом четности с 19-го по 36-й биты. 2–4-й бит - это код производителя, 5–16-й бит - это код сайта, а 21–36-й - номер карты</p>
Wiegand37a	<p>EMMMFFFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCO</p> <p>Состоит из 37 бит двоичного кода. 1-й бит является четным битом четности от 2-го до 18-го битов, а 37-й бит является нечетным битом четности от 19-го до 35-го битов. 2–4-й бит - это код производителя, 5–14-й бит - код устройства, 15–20-й бит - код сайта, а 21–36-й бит - номер карты.</p>
Wiegand50	<p>ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCO</p> <p>Состоит из 50 бит двоичного кода. 1-й бит - это четный бит четности со 2-го по 25-й бит, а 50-й бит - это нечетный бит четности от 26-го до 49-го бита. Биты со 2-го по 17-й - это код сайта, а с 18-го по 49-й - номер карты.</p>

 **Примечание:** **C** обозначает номер карты, **E** обозначает четный бит четности, **O** обозначает нечетный бит четности, **F** обозначает код устройства, **M** обозначает код производителя, **P** обозначает бит четности и **S** обозначает код сайта.

6.5.2 Выход Wiegand

Разъем выхода Wiegand поддерживает SRB, или подключает устройство как подчиненный модуль к другому модулю (главный модуль), образуя главную / подчиненную систему.



Выбрать “Выход Wiegand” и нажмите , чтобы войти

Установите параметры в интерфейсе “Выход Wiegand”

SRB: выберите [ВКЛ], чтобы включить функцию SRB, а при выборе [ВЫКЛ] можно отключить эту функцию.

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. Доступны несколько вариантов выбора, но фактический формат Wiegand будет зависеть от параметра в [Выходные биты Wiegand].

Например: если 26-битный Wiegand26, 34-битный Wiegand34a, 36-битный Wiegand36, 37-битный Wiegand37a и 50-битный Wiegand50 выбран в [Формат Wiegand], но 36 бит выбрано в [Выходные биты Wiegand], то фактический формат Wiegand для использования будет 36-битный Wiegand36.

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 26-битный Wiegand26, 34-битный Wiegand34a, 36-битный Wiegand36, 37-битный Wiegand37a и 50-битный Wiegand50 выбран в [Формат Wiegand], но 36 бит выбрано в [Выходные биты Wiegand], то фактический формат Wiegand для использования будет 36-битный Wiegand36.

Неудавшийся идентификатор: определяется как выходное значение неудачной верификации пользователя. Формат выхода зависит от Настройка [Формат Wiegand]. Значение по умолчанию составляет от 0 до 65535.

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

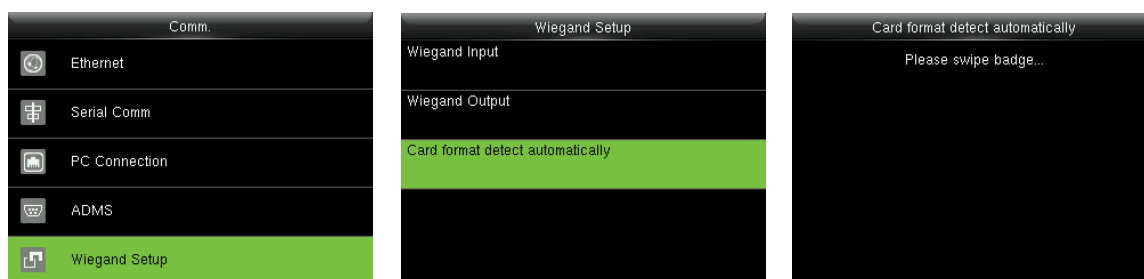
Ширина импульса (мкс): ширина импульса, посылаемая устройством считывания карт Wiegand. Значение по умолчанию составляет 100 микросекунд, которые можно регулировать в диапазоне от 20 до 100 микросекунд.


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

Тип идентификатора: содержимое выход после успешной верификации. **Идентификатор пользователя** или **Номер карты** могут быть выбраны.

6.5.3 Формат карты определяется автоматически

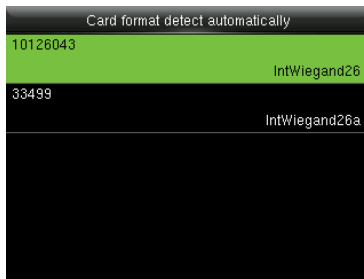
[Формат карты определяется автоматически] помогает пользователю быстро определить тип карты и соответствующий ей формат. В устройстве предустановлены различные форматы карт. После считывания карты система будет определять его как разные номера карт в соответствии с каждым форматом; пользователю требуется 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.



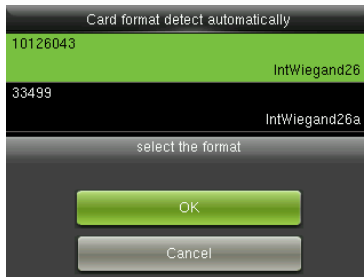
В начальном интерфейсе нажмите  > **Связь** > **Установка Wiegand** > **Формат карты определяется автоматически**, чтобы войти в интерфейс **Формат карты определяется автоматически**.

Процедура операции:

1. После входа в интерфейс [Формат карты определяется автоматически] устройства идентификации, просканируйте идентификационную карту (на локальном устройстве или вспомогательном устройстве чтения карт), интерфейс покажет автоматически обнаруженные форматы Wiegand и проанализированные номера карт.



2. Выберите элемент, соответствующий фактическому номеру карты, в качестве [Формат Wiegand] устройства, которое является форматом Wiegand для чтения карт этого типа.

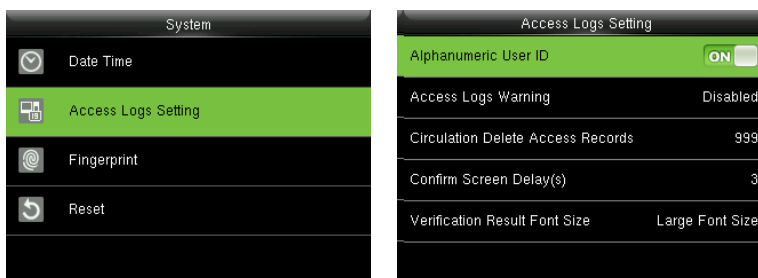



 **Примечание:** в интерфейсе **[Формат карты определяется автоматически]** устройства с

идентификационной картой устройство не может определить номер карты или формат Wiegand, только проводя идентификационную карту. Для определения формата Wiegand идентификационной карты, необходимо подключить устройство чтения идентификационных карт к устройству и провести идентификационную карту над вспомогательным устройством чтения карт, чтобы устройство показывало номер карты и формат Wiegand.

7 Системные настройки

7.1 Настройки журналов доступа



В начальном интерфейсе нажмите  > **Система** > **Настройка журналов доступа**, чтобы войти в интерфейс Настройки журналов доступа.

Буквенно-цифровой идентификатор пользователя: если включен [Буквенно-цифровой идентификатор пользователя], вы можете использовать буквенно-цифровой идентификатор пользователя.

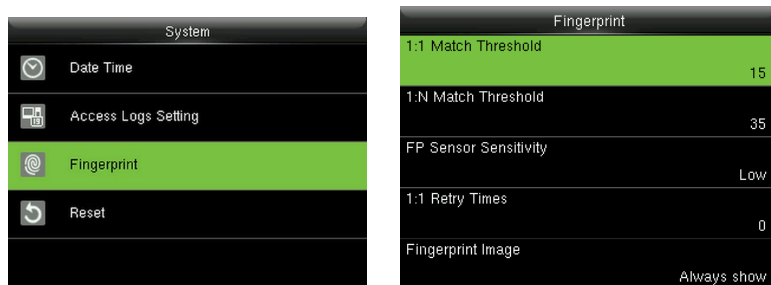
Предупреждение журналов доступа. Если остаточная емкость записи доступа меньше предварительно установленного значения, устройство автоматически генерирует сообщение, указывающее остаточную емкость записи. Вы можете установить его на **Отключено** или установить значение в диапазоне от 1 до 9999.

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

Подтвердите задержку экрана (сек): установите длительность отображения сообщений о результатах верификации. Диапазон допустимых значений составляет 1-9 секунд.

Размер шрифта результата верификации: вы можете выбрать обычный шрифт, крупный или крупный шрифт в качестве размера шрифта результата верификации.

7.2 Параметры отпечатков пальцев



В начальном интерфейсе нажмите > Система > Отпечаток пальца, чтобы войти в интерфейс настройки Отпечатка пальца.

Пороговые значения сравнения 1:1: при способе верификации 1:1 верификация может быть успешной, только если совпадение между проверяющим отпечатком и зарегистрированным отпечатком пользователя превышает это значение.

Пороговые значения сравнения 1:N: при способе верификации 1: N верификация может быть успешной, только если совпадение между проверяющим отпечатком и зарегистрированным отпечатком пользователя превышает это значение.

Рекомендуемые пороговые значения сравнения:

		Пороговые значения сравнения	
FRR	FAR	1: N	1:1
Высокий	Низкий	45	25
Средн.	Средн.	35	15
Низкий	Высокий	25	10

Чувствительность датчика устройства: настройка чувствительности сбора отпечатков пальцев.

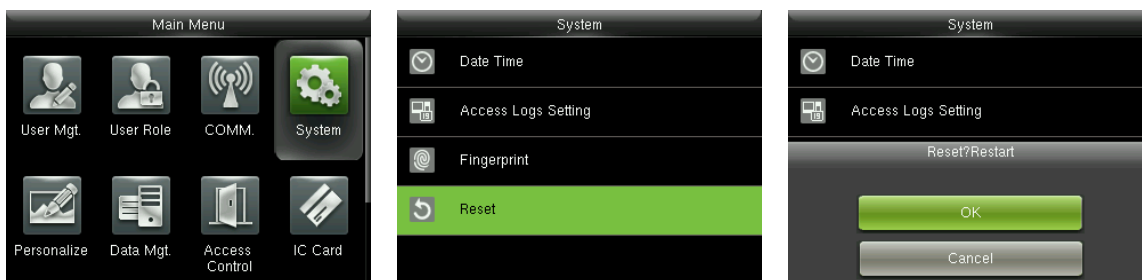
Рекомендуется использовать уровень по умолчанию «Средний». Когда среда сухая, что приводит к медленному обнаружению отпечатков пальцев, вы можете установить уровень «Высокий», чтобы повысить чувствительность; когда среда влажная, что затрудняет идентификацию отпечатка пальца, вы можете установить уровень «Низкий».

Время повтора способа 1:1. При верификации способом 1:1 или верификации пароля пользователи могут забыть зарегистрированный отпечаток пальца или пароль или неправильно прижать палец. Чтобы сократить процесс повторного ввода идентификатора пользователя, повтор разрешен; количество повторных попыток может быть в пределах 1 ~ 9.

Изображение отпечатка пальца: настройка отображения изображения отпечатка пальца на экране при регистрации или верификации. Доступны четыре варианта: Показать для регистрации, Показать для сравнения, Всегда показывать, Не показывать.

7.3 Сброс до заводских настроек

Сброс таких данных, как настройки связи и настройки системы до заводских настроек.




В исходном интерфейсе нажмите \Rightarrow > **Система** > Сброс> ОК, чтобы завершить настройку сброса.

Параметры сброса включают в себя параметры контроля доступа, настройку защиты от переадресации, настройку связи (а именно, настройку Ethernet, последовательную связь, соединение с ПК и настройку Wiegand), персонализацию (такую как голосовая подсказка, клавиатурная подсказка, громкость и время простоя до сна) так далее.

Параметры	Заводские настройки по умолчанию
Параметры контроля доступа	Задержка блокировки двери: 5 сек Задержка датчика двери: 10 секунд Тип датчика двери: нормально открытый (NO) Режим верификации: пароль / отпечаток пальца / дверная карта доступный период времени : 1 Временной период режима Нормально открытый : Нет Использовать как главный модуль : Вход Вспомогатель. Выход / время разблокировки замка : 255 сек Настройка типа вспомогательного выхода:

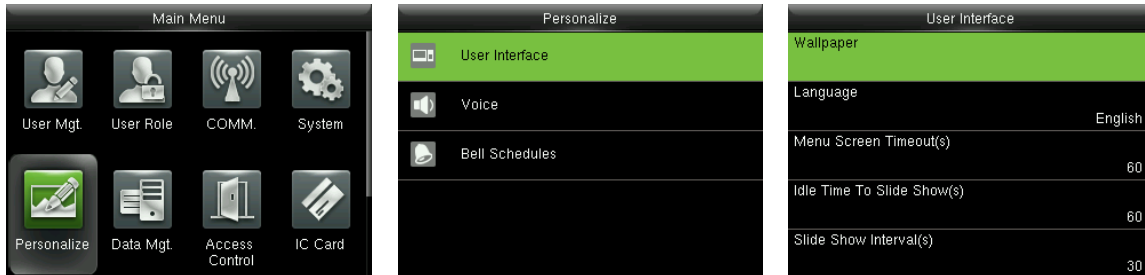
	триггерная дверь открыта
Направление запрета двойного прохода	Нет запрета двойного прохода
Ethernet	IP-адрес: 192.168.1.201 Маска подсети : 255.255.255.0 Шлюз : 0.0.0.0
Подключение ПК	Клавиша связи : 0 Идентификатор устройства : 1
Установка Wiegand	Wiegand тип ввода / вывода ID: идентификатор пользователя Ширина импульса: 100 мкс Интервал импульса: 1000 мкс
Время ожидания до появления слайд-шоу	60 сек
Время ожидания до режима сна	30 мин
Время истечения ожидания экрана меню	60 сек
Подсказка клавиатуры	ВКЛ
Голосовая подсказка	ВКЛ


 **Примечания:** При сбросе к заводским настройкам дата и время не будут затронуты.

Например, если 1 января 2020 года дата и время устройства установлены на 18:30, дата и время останутся неизменными после сброса к заводским настройкам.

8 Персонализация настройки

8.1 Настройки пользовательского интерфейса




В начальном интерфейсе нажмите  > **Персонализация** > **Пользовательский интерфейс**, чтобы установить Пользовательский интерфейс.

Обои: при необходимости выберите обои главного экрана, в устройстве можно найти обои разных стилей.

Язык: выберите необходимый язык устройства.


Время истечения ожидания экрана меню: если в интерфейсе меню не выполняется никаких операций, а время превышает установленное значение, устройство автоматически выйдет на начальный интерфейс. Вы можете отключить его или установить значение 60 ~ 99999 секунд.

 **Примечания:** Если выбрано [Отключено], система не выйдет из интерфейса меню, даже если не будет выполнено никаких действий. Отключение этой функции не рекомендуется из-за большой потребляемой мощности и небезопасности.

Время ожидания до появления слайд-шоу: если в начальном интерфейсе нет операций, а время превышает установленное значение появится слайд-шоу. Его можно отключить (установить на «Нет») или установить на 3 ~ 999 секунд.

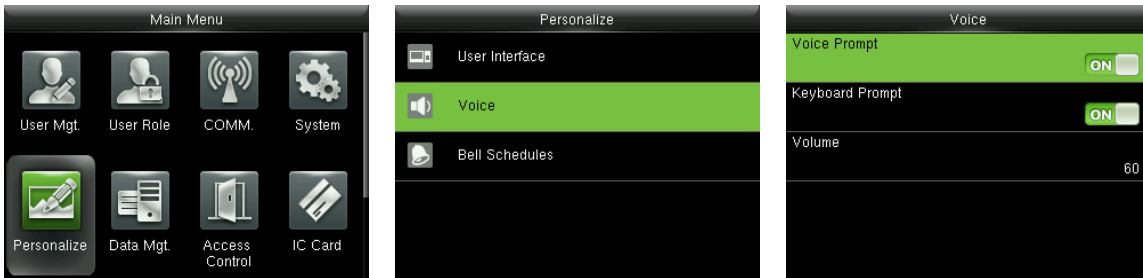
Интервал слайд-шоу: относится к интервалу между показом изображений слайд-шоу. Его можно отключить или установить на 3 ~ 999 с.


Время ожидания до режима сна: когда на устройстве не выполняется никаких операций и достигается установленное время ожидания, устройство переходит в режим ожидания. Нажмите любую клавишу или палец, 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.


 **Примечания:** отключение этой функции не рекомендуется из-за большой потребляемой мощности.


Стиль основного экрана: выбор положения и пути часов и клавиши состояния.



8.2 Голосовые настройки



В начальном интерфейсе нажмите  > **Персонализация** > **Голос**, чтобы войти в интерфейс настроек **Голоса**.

Голосовая подсказка: выберите, нужно ли включать голосовые подсказки во время работы. Значением по умолчанию является [ВКЛ], означающее, что голосовая подсказка включена. Вы можете нажать  для переключения между [ВКЛ] и [ВЫКЛ]. Значок [ВЫКЛ] указывает, что голосовая подсказка отключена.

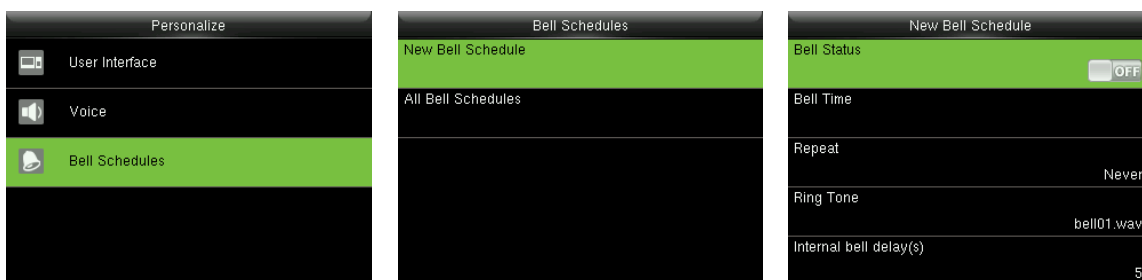
Подсказка клавиатуры: выберите, следует ли включить голос при касании клавиатуры. Значением по умолчанию является [ВКЛ], что указывает на то, что подсказка клавиатуры включена. Вы можете нажать  для переключения между [ВКЛ] и [ВЫКЛ]. Значок [ВЫКЛ], указывающий, что подсказка клавиатуры отключена.


Громкость: установите громкость устройства. Значение по умолчанию - 70. Нажмите клавишу , чтобы увеличить громкость, нажмите клавишу , чтобы уменьшить громкость.

8.3 Настройки звонки

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

8.3.1 Добавить новый звонок



В начальном интерфейсе нажмите  > Персонализация > Расписание звонков > Новое расписание звонков, чтобы войти в интерфейс добавления Расписания нового звонка.

Состояние звонка: [ВКЛ] - для включения звонка, а [ВЫКЛ] - для его отключения.

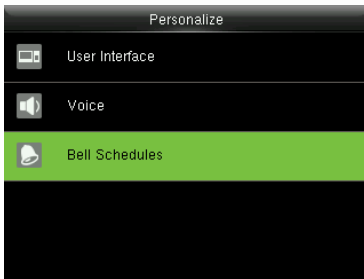
Время звонка: звонок звонит автоматически при достижении указанного времени.

Повторить: установить, повторять ли звонок с понедельника по воскресенье.

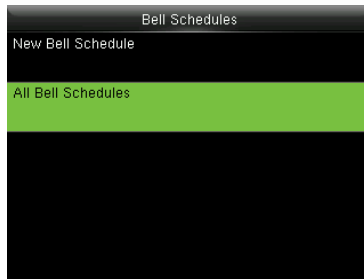
Рингтон: рингтон для звонка.

Интервальная задержка звонка: для установки продолжительности звонка. Значение колеблется от 1 до 999 секунд.

8.3.2 Редактировать звонок



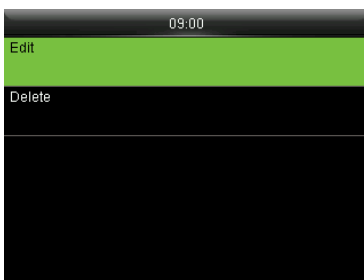
Нажмите **V**, чтобы выбрать «Расписания звонков» и нажмите **→**, чтобы войти



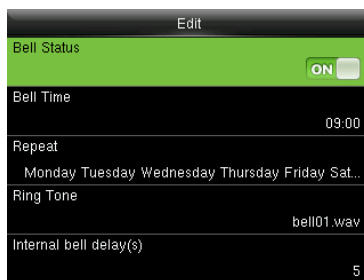
Нажмите **V**, чтобы выбрать «Расписания всех звонков» и нажмите **→** для входа



Выберите звонок для редактирования и нажмите **→**, чтобы войти

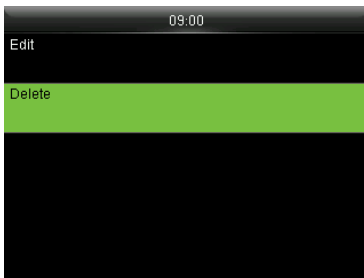


Выберите Редактировать» и нажмите **→**

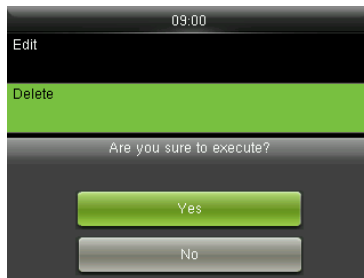


Измените параметры звонка

8.3.3 Удалить звонок



Нажмите **V**, чтобы выбрать «Удалить» и нажмите **→**, чтобы войти.

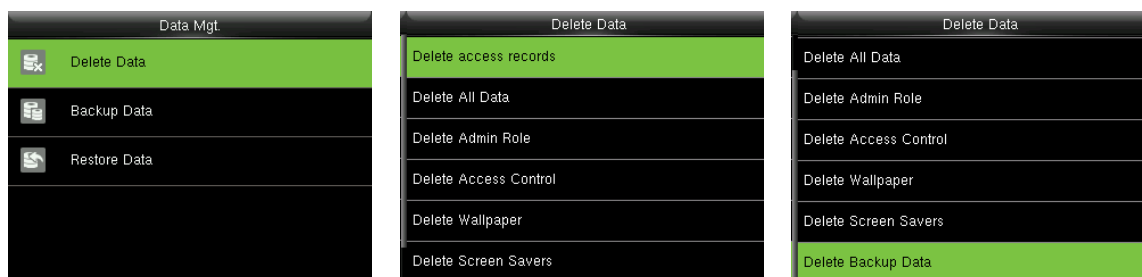



Нажмите **L**, чтобы выбрать «Да» и нажмите **→**, чтобы войти.

9 Управление данными

9.1 Удаление данных

Для управления данными на устройстве, включая удаление записей доступа, удаление всех данных, удаление роли администратора, удаление экранных заставок и т. д.



В начальном интерфейсе нажмите  > **Управ. данными** > **Удалить данные**, чтобы войти в интерфейс настроек удаления данных.

Удалить записи доступа: удалить все записи доступа, сохраненные на устройстве, или удалить записи доступа за указанный промежуток времени.

Удалить все данные: для удаления всей пользовательской информации, отпечатков пальцев, доступа к записям и т. д.

Удалить роль администратора: чтобы все администраторы стали обычными пользователями.

Удалить контроль доступа: удалить все данные доступа.

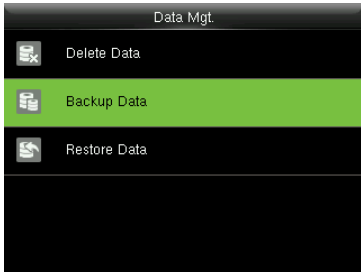
Удалить обои: чтобы удалить выбранные или все обои на устройстве.

Удалить заставки: удаление выбранных или всех заставок на устройстве. (Для получения дополнительной информации о загрузке заставок см. Правило загрузки изображений.)

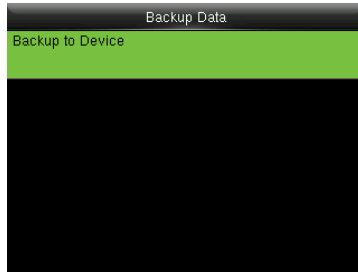
Удалить данные резервной копии: удалить все данные резервной копии.

9.2 Резервное копирование данных

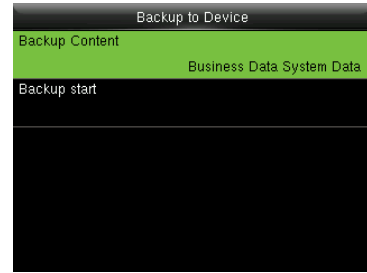
Резервное копирование бизнес-данных или данных конфигурации на устройство.



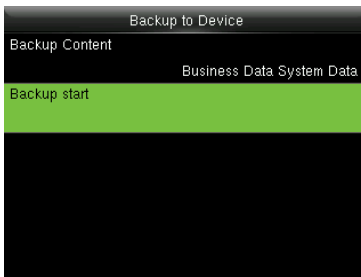
Нажмите \downarrow , чтобы выбрать «Резервное копирование данных» и нажмите \rightarrow , чтобы войти.



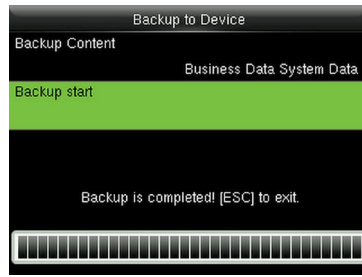
Выберите «Резервное копирование в устройство» и нажмите \rightarrow



Выберите «Содержание резервного копирования» и нажмите \rightarrow , чтобы войти и отметьте содержимое резервной копии.



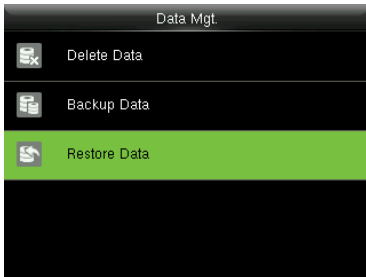
Нажмите \downarrow , чтобы выбрать «Запуск резервного копирования» и нажмите, чтобы начать



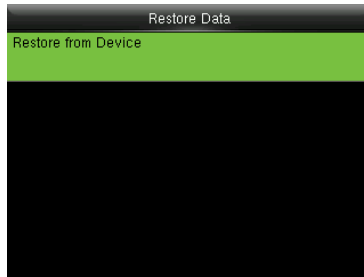
После резервного копирования нажмите \rightarrow для выхода

9.3 Восстановление данных

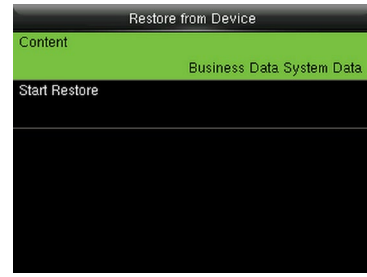
Чтобы восстановить данные, сохраненные в устройстве.



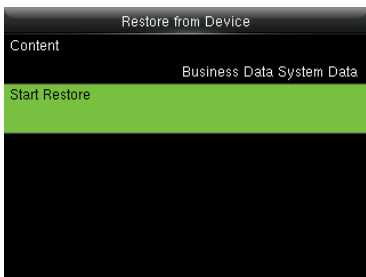
Нажмите \checkmark , чтобы выбрать «Восстановить данные» и нажмите \rightarrow



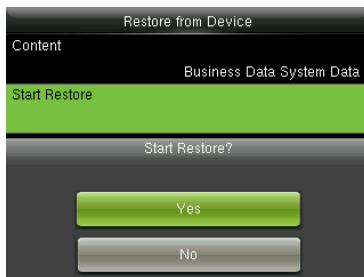
Выберите «Восстановить с устройства» и нажмите \rightarrow



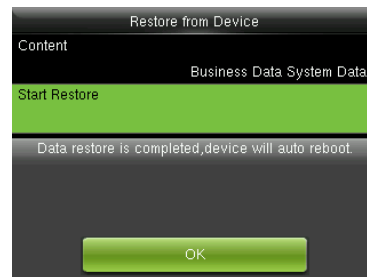
Выберите «Содержимое», нажмите для входа и отметьте, чтобы содержание было восстановлено.



Нажмите \checkmark , чтобы выбрать «Начать восстановление» и нажмите \rightarrow , чтобы начать.



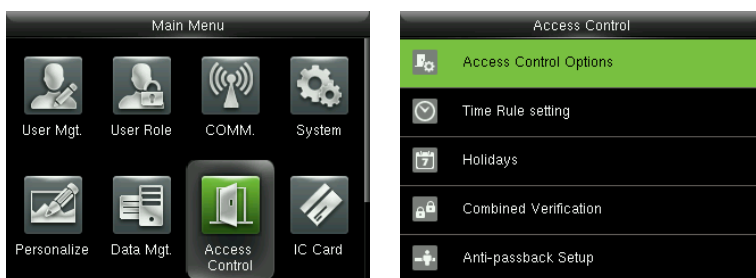
Нажмите \checkmark , чтобы выбрать «Да» и нажмите \rightarrow , чтобы подтвердить.




После восстановления нажмите \rightarrow , чтобы перезапустить устройство.

10 Контроль доступа

Параметр «Контроль доступа» используется для установки временных правил, выходных, комбинированной проверки и т. д., соответствующих параметров устройства для управления замками и другими модулями.



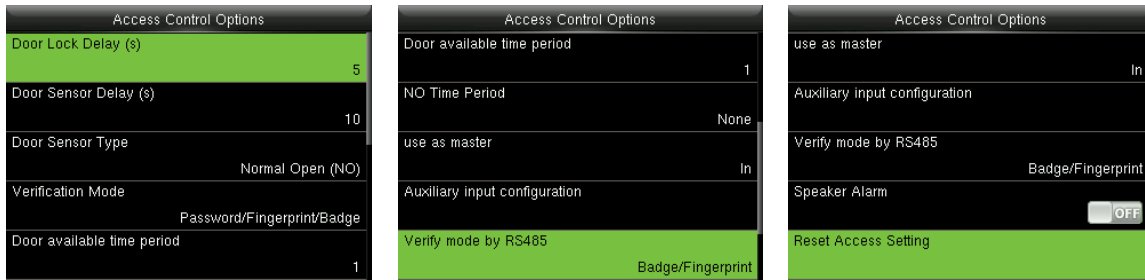
В начальном интерфейсе нажмите  > **Контроль доступа**, чтобы войти в интерфейс настроек Контроля доступа.

Чтобы получить доступ, зарегистрированный пользователь должен соответствовать следующим условиям:

1. Время доступа пользователя находится в пределах временного интервала личного доступа или временного интервала доступа группы.
2. Группа пользователей должна находиться в комбинированном доступе (когда в том же комбинированном доступе есть другие группы, верификация членов этих групп также необходима для открытия двери).

В настройках по умолчанию новые пользователи распределяются в первую группу доступа с правилом времени группы по умолчанию [1] и комбинированным доступом как «1» и устанавливаются в состояние разблокировки.

10.1 Настройки параметров контроля доступа



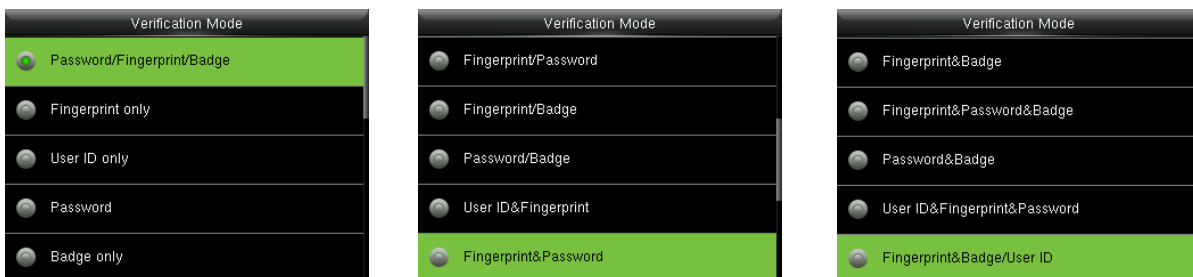
В начальном интерфейсе нажмите > **Контроль доступа** > **Параметры контроля доступа**, чтобы войти в интерфейс **Настройки параметров контроля доступа**.

Задержка блокировки двери: 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 1 до 10 секунд).

Задержка датчика двери: 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 задержка датчика двери (значение колеблется от 1 до 255 секунд).

Тип датчика двери: включает в себя «Отсутствует», «Нормально открытый» (NO) и «Нормально закрытый» (NC). **Отсутствует** означает дверной датчик не используется; **Нормально открытый** означает, что дверь открывается, когда включено электричество; **Нормально закрытый** означает, что дверь закрыта, когда включено электричество.

Режим верификации: выберите режим верификации, чтобы открыть дверь, включая пароль / отпечаток пальца / карту, только отпечаток пальца, только идентификатор пользователя, пароль, только карта, отпечаток пальца / пароль, отпечаток пальца / карта, пароль / карта, идентификатор пользователя и отпечаток пальца, отпечаток пальца и пароль, отпечаток пальца и карта, отпечаток пальца, пароль и карта, пароль и карта, идентификатор пользователя, отпечаток пальца и пароль, отпечаток пальца, карта и идентификатор пользователя.



 Примечание:

1. «/» означает «или». «&» Означает «и».
2. В комбинированном режиме верификации соответствующая информация верификации должна быть зарегистрирована в первую очередь. Например: если пользователь А регистрирует только **отпечаток пальца**, а [Режим верификации] установлен как «Пароль & карта», пользователь А не пройдет верификацию.

Временной период доступа двери: установить периоды для открытия двери для пользователей.

Временной период NO: установить период времени для режима Нормально открытый, чтобы дверь всегда была разблокирована в течение этого периода.

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

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

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

Конфигурация вспомогательного входа: установить **Вспомог. выход / время открытия замка** и тип **Вспомог. выхода** для устройства со вспомогательным разъемом. Тип **Вспомогательного выхода** включает **Отсутствие, триггер открытия двери, триггер тревожной сигнализации, триггер открытия двери и Тревожную сигнализацию**.

Режим верификации по RS485★: включить функцию считывателя RS485; это способ верификации, используется устройством, когда оно является главным / подчиненным устройством.

Динамик тревожной сигнализации: когда [Динамик тревожной сигнализации] включен, динамик подаст сигнал тревожной сигнализации при демонтаже устройства.

Сброс настроек доступа: для сброса параметров задержки блокировки двери, задержки датчика двери, типа датчика двери, режима верификации, периода времени доступа двери, периода времени NO, конфигурации вспомогательного входа, динамика тревожной сигнализации, направления запрета двойного прохода. Однако содержимое удаления данных доступа в [Управ. данными] Не будет затронуто.

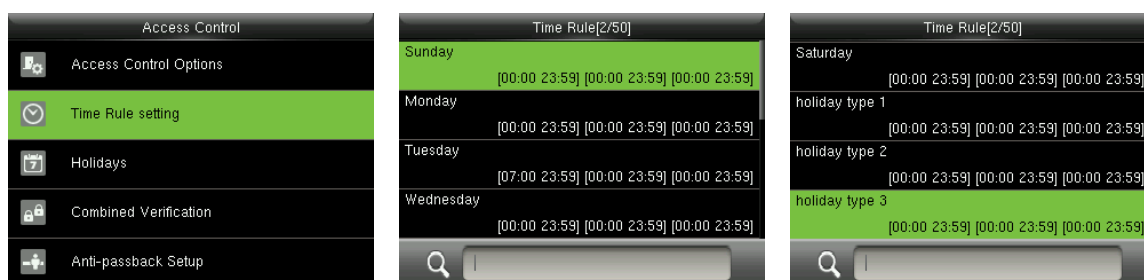
Параметры доступа	Заводские настройки
Задержка блокировки двери	5 сек
Задержка датчика двери	10 сек
Тип датчика двери	Нормальной открытый (NO)

Режим верификации	Пароль / Отпечаток пальца / Карта
Временной период доступа двери	1
Временной период NO	Отсутствует
Вспомог. выход / время открытия замка	255 сек
Настройка типа Вспомогательного выхода	триггер открытия двери
Динамик тревожной сигнализации	Откл.
Направление запрета двойного прохода	Нет запрета двойного прохода

10.2 Настройки временных правил

Временное правило - минимальная единица времени настроек контроля доступа; для системы может быть установлено не более 50 временных правил. Каждое **Правило времени** состоит из 7 графиков (в неделю) и 3 графика в праздничные дни, и каждый график является временем действия в течение 24 часов.

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

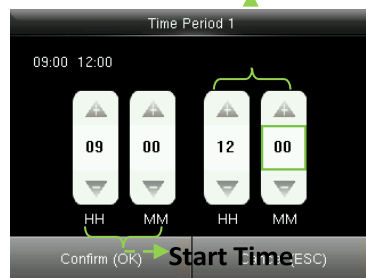
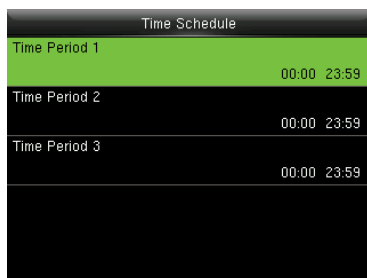
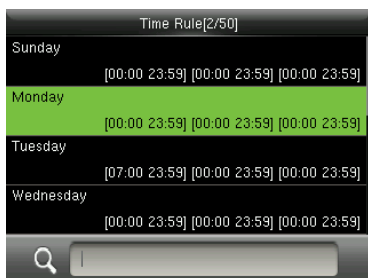


В начальном интерфейсе нажмите > **Контроль доступа > Настройка правила времени**, чтобы войти в интерфейс Настройки временных правил. Номер временного правила по умолчанию - 1 (действителен целый день), который можно редактировать.

- Редактирование временного правила

Супер администратор может редактировать временное правило по мере необходимости.

Подробная операция выглядит следующим образом:



Введите номер временного правила (например, «2»), временное правило (2) будет найдено автоматически, выберите график (например, «Понедельник») и нажмите \rightarrow

Выберите «Период времени 1/2/3» и нажмите \rightarrow , чтобы войти в интерфейс настройки временного периода

Установите «Время начала» и «Время окончания» как требуется, после настройки нажмите \rightarrow для сохранения и выхода

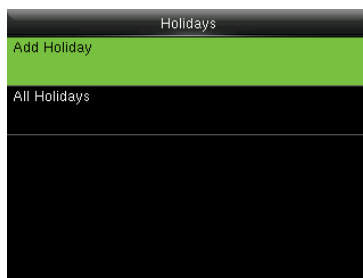
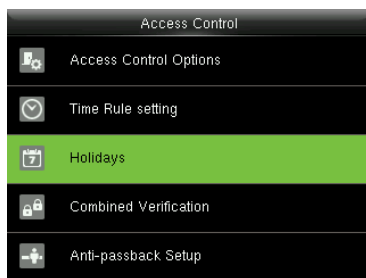
Подсказка: Вы можете установить «Время начала» и «Время окончания», нажав \wedge/\vee или введите непосредственно в цифровом виде, нажмите \langle/\rangle , чтобы переключить окно редактирования. Вы можете установить другие графики по мере необходимости после установки графика на понедельник, а затем нажмите \rightarrow , чтобы выйти.

 Примечание:

- (1) Если 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 период времени действителен.
- (2) Действительный период времени: 00:00 - 23:59 (действителен весь день) или когда время окончания позже времени начала (например, 08:00 - 23:59).
- (3) По умолчанию правило 01 времени указывает на открытие полного дня (00:00 - 23:59).

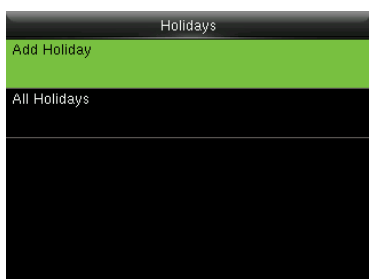
10.3 Настройки праздников

Добавьте в устройство контроль доступа на праздники и при необходимости установите периоды праздников. Устройство контролирует контроль доступа в праздничные дни в соответствии с настройками праздников.

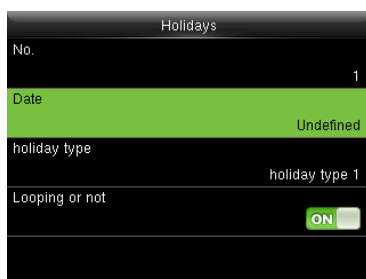


В начальном интерфейсе нажмите \Rightarrow > **Управление доступом** > **Праздники**, чтобы войти в интерфейс настройки **Праздников**.

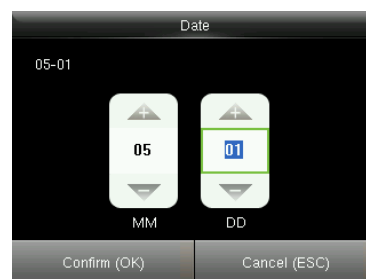
10.3.1 Добавление праздника



Выберите «Добавить праздник» и нажмите \Rightarrow , чтобы войти.




Выберите «Дату» и нажмите \Rightarrow , чтобы войти.



Установите дату для добавленного праздника и нажмите \Rightarrow , чтобы сохранить и выйти.

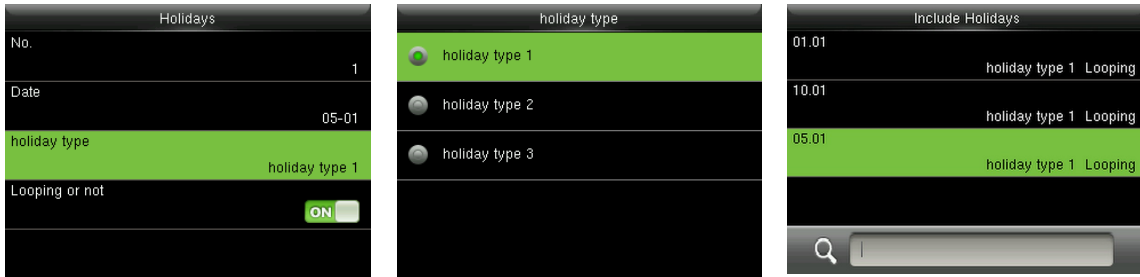
Параметры праздника устанавливаются следующим образом:

№: устройство автоматически присваивает номер празднику. Вы также можете выбрать [№] и нажать \Rightarrow , чтобы войти в интерфейс №. При необходимости введите номер праздника и нажмите \Rightarrow , чтобы сохранить настройки и вернуться в интерфейс **Праздники**.

 **Примечание:** номер отпуска варьируется от 1 до 24.

Дата: установите дату праздника. Нажмите \wedge/\vee или введите цифру напрямую, чтобы установить дату, нажмите $</>$ чтобы переключить окно редактирования. Затем нажмите \Rightarrow , чтобы сохранить настройки и вернуться в интерфейс **Праздников**.

Тип праздника: выберите график времени доступа для праздника. Период времени для типа отпуска 1/2/3 можно редактировать во временном правиле. Для получения подробной информации о методах редактирования, пожалуйста, обратитесь к 10.2 Настройки временных правил.

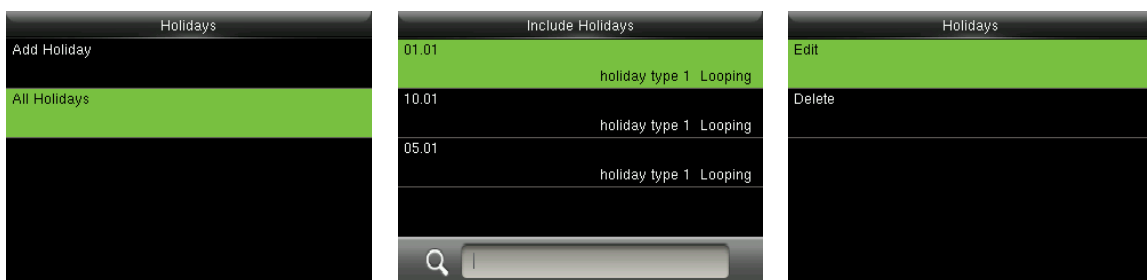


Установка цикла или его отсутствие: по умолчанию значение Установка цикла или его отсутствие - [ВКЛ]. Вы можете нажать для переключения между [ВКЛ] и [ВЫКЛ].

Для фиксированных праздников каждый год, например, Новый год - это 1 января, для них можно установить «Установка цикла или его отсутствие» на [ВКЛ]. Например, для нефиксированных праздников каждый год - День матери - это второе воскресенье мая, конкретные даты неопределенны, и для них можно установить «Установка цикла или его отсутствие» на [ВЫКЛ].

Например, когда дата праздника установлена на 1 января 2010 г., а тип праздника установлен на тип праздника 1, контроль доступа с 1 января проводится в соответствии с настройками временного периода типа праздника 1, а не настройками временного периода пятницы.

10.3.2 Все праздники



Нажмите \checkmark , чтобы выбрать «Все праздник» и нажмите \Rightarrow , чтобы войти.

Выберите праздник и нажмите \Rightarrow , чтобы войти.

Редактируйте или удалите праздник.

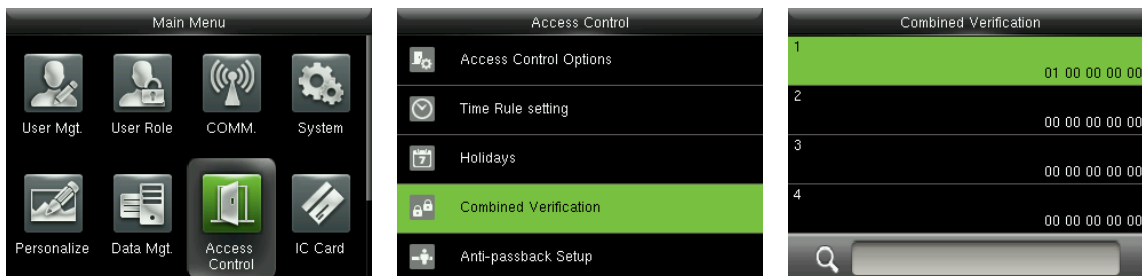
☺ Примечания: Способы редактирования или удаления праздника те же, что и при редактировании или удалении пользователя, и здесь не описаны. Для получения дополнительной информации см. 4.4 Редактирование пользователя и 4.5 Удаление пользователя.

10.4 Настройки комбинированной верификации

Объедините две или более группы доступа для обеспечения многократной верификации и повышения безопасности.

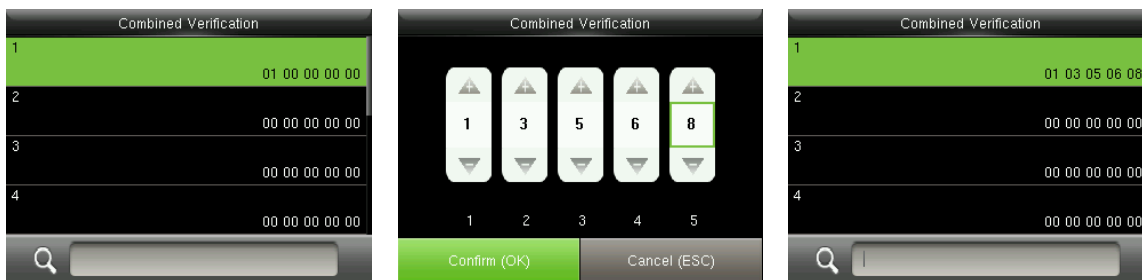
При комбинированной верификации диапазон номера пользователя составляет: $0 \leq N \leq 5$; все пользователи могут принадлежать к одной группе или максимум к 5 различным группам.

☺ Примечания: Группы доступа устанавливаются при добавлении пользователя (в начальном интерфейсе нажмите \Rightarrow > **Управление пользователем** > **Новый пользователь** > **Роль управления доступом** > **Группа доступа** (для установки номера группы доступа, к которой принадлежит добавленный пользователь), номер группы доступа варьируется от 1 до 99.

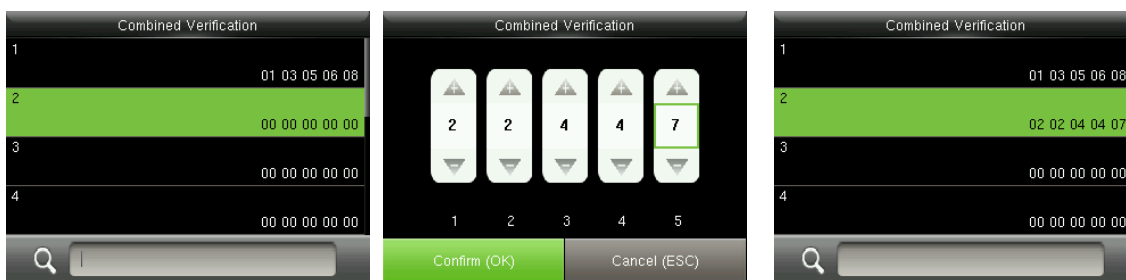


В начальном интерфейсе нажмите \Rightarrow > **Контроль доступа** > Комбинированная верификация, чтобы войти в интерфейс настройки Комбинированной верификации.

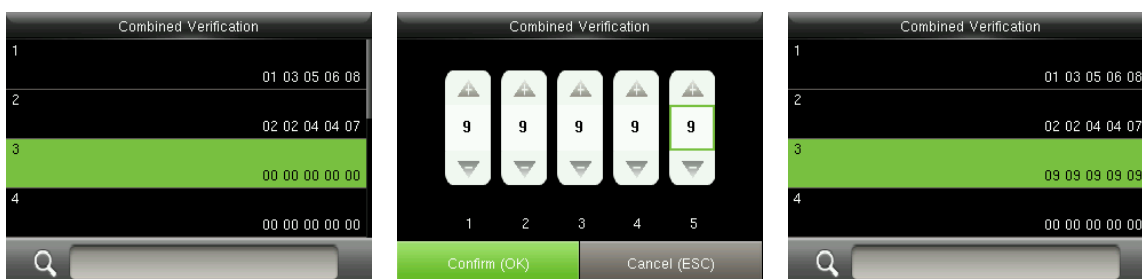
Например:



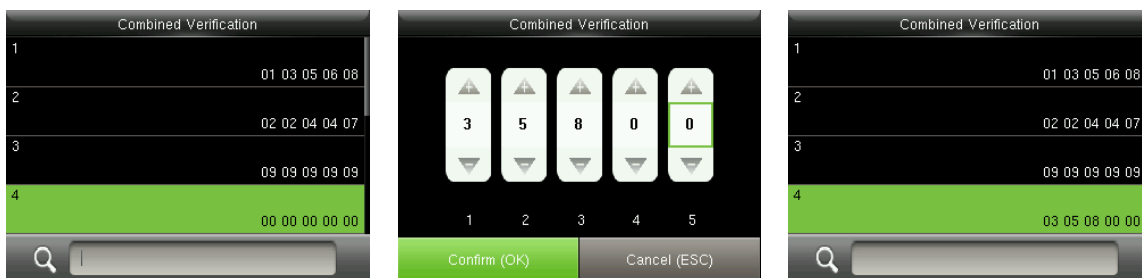
Как показано на рисунке выше, комбинированная верификация 1 состоит из пяти участников из пяти разных групп - группа доступа 1/3/5/6/8 соответственно.



Как показано на рисунке выше, комбинированная верификация 2 состоит из пяти участников из трех разных групп: двух членов из группы доступа 2, двух из группы доступа 4 и одного из группы доступа 7.



Как показано на рисунке выше, комбинированная верификация 3 состоит из пяти участников, и все они принадлежат группе доступа 9.

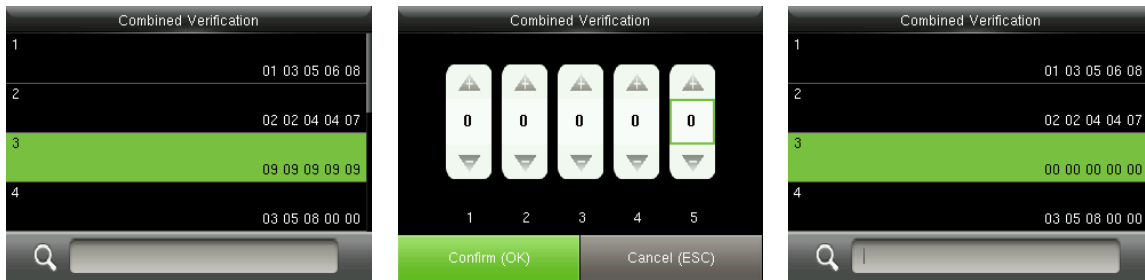


Как показано на рисунке выше, комбинированная верификация 4 состоит из трех участников из трех разных групп - группы доступа 3, 5, 8 соответственно.

Удаление комбинированной верификация

Чтобы удалить комбинированную верификацию, установите для всех номеров групп доступа значение 0.

Например, чтобы удалить Комбинированную верификацию 3, см. рисунки ниже:

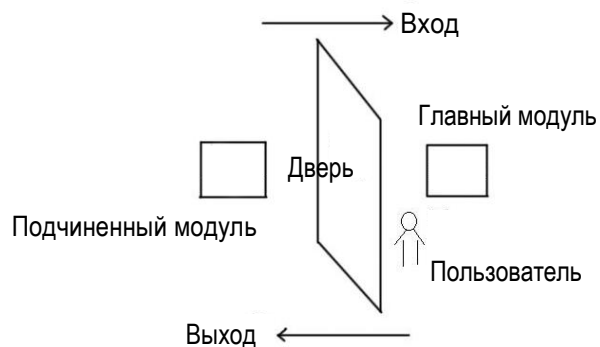


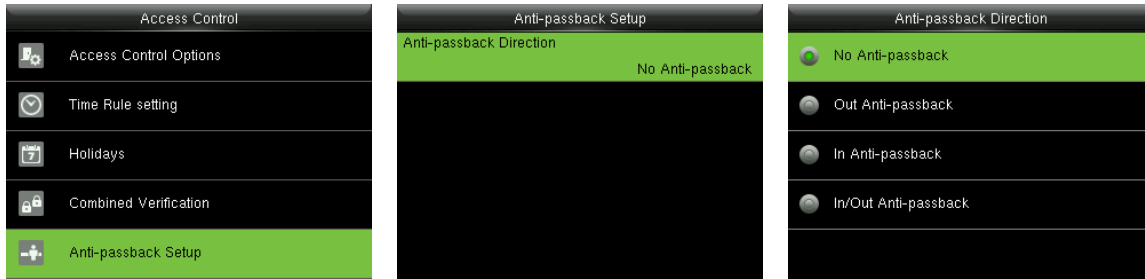
Если все номера групп доступа в Комбинированной верификации 3 установлены на 0, они будут удалены.


10.5 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 защиты от двойного прохода. Запись регистрации входа должна совпадать с записью регистрации выхода, чтобы открыть дверь.

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





В начальном интерфейсе нажмите  >, **Контроль доступа > Установка запрета двойного прохода**, чтобы войти в интерфейс **Установка запрета двойного прохода**. Выберите направление запрета двойного прохода.

- **Направление запрета двойного прохода**

Отсутствие запрета двойного прохода: запрет двойного прохода отключен, что означает, что при прохождении верификации главный модуль или подчиненный модуль могут открыть дверь. Записи доступа не зарезервированы.

Запрет двойного прохода на выход: после того, как пользователь прошел выход пользователь может пройти выход снова, только если последняя запись является записью о регистрации входа; в противном случае тревожная сигнализация будет активирована. Тем не менее, пользователь может свободно зарегистрировать вход.

Запрет двойного прохода на вход: после того, как пользователь прошел вход, пользователь может пройти вход снова, только если последняя запись является записью о регистрации выхода; в противном случае тревожная сигнализация будет активирована. Тем не менее, пользователь может свободно зарегистрировать выход.

Запрет двойного прохода на вход/выход: после того, как пользователь прошел вход/выход, пользователь может пройти вход снова, только если последняя запись является записью о регистрации выхода, или пользователь может пройти выход снова, только если последняя запись является записью о регистрации входа; в противном случае тревожная сигнализация будет активирована.

11 Интеллектуальная карта★

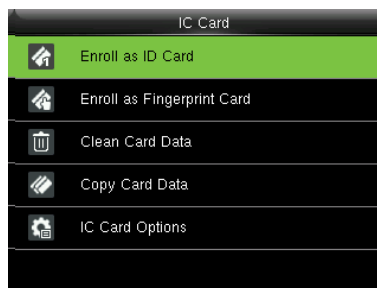
Чтобы зарегистрировать карту Mifare в качестве идентификационной карты или карты отпечатков пальцев. Это меню поддерживает интеграцию учета рабочего времени по отпечаткам пальцев и идентификационной карте с другими системами или устройствами с помощью зарегистрированной карты Mifare, а также поддерживает режим множественной верификации для удовлетворения потребностей разных людей. Он также поддерживает чистое копирование данных карты, зарегистрированных на карте Mifare.

11.1 Зарегистрировать в качестве идентификационной карты

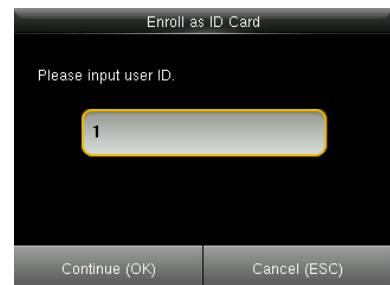
Зарегистрируйте карту Mifare в качестве идентификационной карты. Для регистрации требуется только номер идентификационной карты (а именно, идентификационный номер пользователя). Перфорирование зарегистрированной карты Mifare на устройстве эквивалентно перфокарте ID-



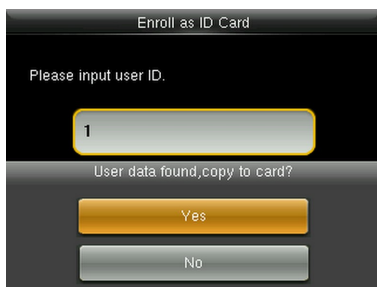
В начальном интерфейсе нажмите \Rightarrow для входа в главное меню, затем нажмите $>$ для выбора **Интеллектуальной карты** и нажмите \Rightarrow , чтобы войти.




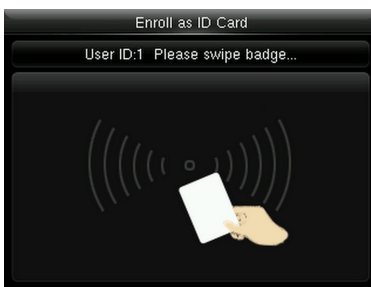
Выберите **«Зарегистрировать в качестве идентификационной карты»** и нажмите \Rightarrow , чтобы войти.



Введите идентификатор пользователя для регистрации и нажмите \Rightarrow .



Если идентификатор пользователя уже зарегистрирован устройство предложит вам скопировать информацию на карту, а затем нажмите , чтобы войти.



Сканируйте карту в области сканирования карты, пока операция не будет успешной.



- **Верификация**

Просканируйте зарегистрированную карту Mifare в области карты. После того, как устройство идентифицирует карту уберите карту.

После того, как верификация прошла успешно, устройство предложит номер карты.



Примечание: Измените режим верификации на режимы, связанные с картами в роли

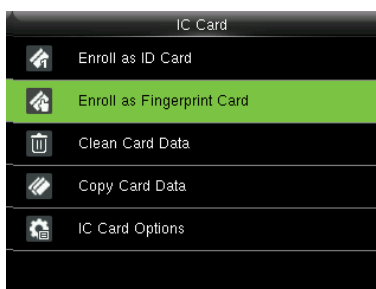
контроля доступа пользователя (В начальном интерфейсе нажмите  > **Управление пользователем** > **Все пользователи** > выберите пользователя > нажмите  > **Редактировать** > **Роль контроля доступа** > **Режим верификации**), или верификация не будет успешной.

11.2 Зарегистрировать в качестве Карты отпечатков пальцев

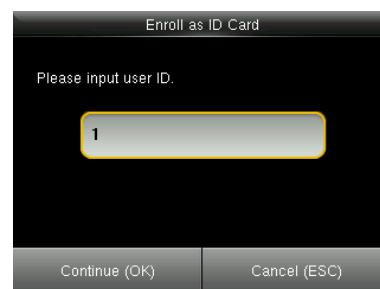
Зарегистрируйте отпечаток пальца и запишите данные отпечатка пальца на зарегистрированную карту Mifare.



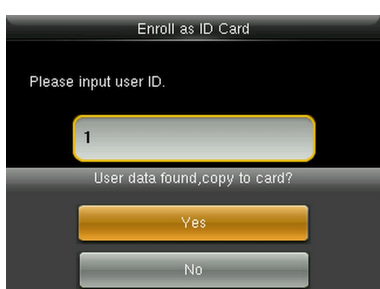
В начальном интерфейсе нажмите \Rightarrow для входа в главное меню, затем нажмите \Rightarrow для выбора **Интеллектуальной карты** и нажмите \Rightarrow , чтобы войти.



Нажмите \checkmark , чтобы выбрать «Зарегистрировать в качестве **Карты отпечатков пальцев**» и нажмите \Rightarrow , чтобы войти.



Введите идентификатор пользователя и нажмите \Rightarrow .



Если идентификатор пользователя уже зарегистрирован устройство предложит вам скопировать информацию на карту, а затем нажмите \Rightarrow .



Выберите палец и нажмите \Rightarrow , затем трижды прижмите палец к датчику отпечатков пальцев.



Поместите карту Mifare в область карты, ожидая, что устройство просканирует данные отпечатка пальца на карту, пока регистрация не будет успешной.

- **Верификация**

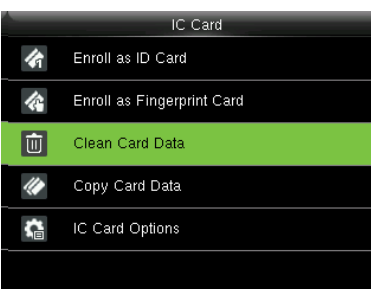
Просканируйте зарегистрированную карту Mifare в области карты. После того, как устройство идентифицирует карту уберите карту. Затем, пожалуйста, прижмите палец, появится отображение окна запроса, прижмите отпечаток пальца, зарегистрированный на карте Mifare, чтобы завершить верификацию. Если прижатый отпечаток пальца отличается от того, который хранится на карте Mifare, верификация выполнена не будет.

11.3 Очистить данные карты

Удалите всю информацию, сохраненную на карте Mifare, которая используется в настоящее время.



В начальном интерфейсе нажмите \Rightarrow для входа в главное меню, затем нажмите $>$ для выбора **Интеллектуальной карты** и нажмите \Rightarrow , чтобы войти.



Нажмите \checkmark , чтобы выбрать «Очистить данные карты» и нажмите \Rightarrow , чтобы войти.



Просканируйте картой Mifare в области карт, ожидая, пока устройство не удалит всю информацию на карточке.

Примечание: Если данные карты были сохранены в устройстве (в исходном интерфейсе нажмите \Rightarrow)>

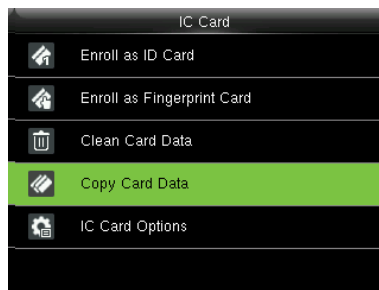
Интеллектуальная карта > Параметры интеллектуальной карты > Режим хранения данных карты > выберите режим «**Сохранить данные пользователя на устройстве**» или «**Сохранить пользователя и отпечатки пальцев на устройстве**», устройство напомнит вам, следует ли удалять информацию, сохраненную в устройстве или нет. [Да] - удалить информацию пользователя, сохраненную на устройстве. [Нет], чтобы сохранить информацию в устройстве.

11.4 Копировать данные карты

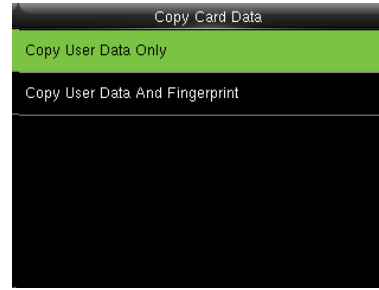
Скопируйте информацию о карте Mifare на устройство (после копирования пользовательские данные и отпечаток пальца все еще сохраняются на карте Mifare), затем нажмите отпечаток пальца для непосредственного присутствия на устройстве, не ударяя карту Mifare.



В начальном интерфейсе нажмите \Rightarrow для входа в главное меню, затем нажмите $>$ для выбора **Интеллектуальной карты** и нажмите \Rightarrow , чтобы войти.



Нажмите \checkmark , чтобы выбрать «Копировать данные карты» и нажмите \Rightarrow .



Выберите «**Копировать только данные пользователя**» или «**Копировать данные пользователя и отпечаток пальца**» и нажмите \Rightarrow .



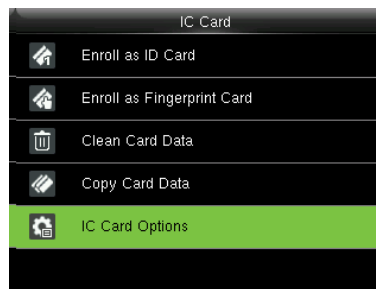
Поместите карту Mifare в область карты, ожидая, пока устройство не скопирует пользовательскую информацию (только пользовательские данные или пользовательские данные и отпечаток пальца) на устройство.

11.5 Параметры Интеллектуальных карт

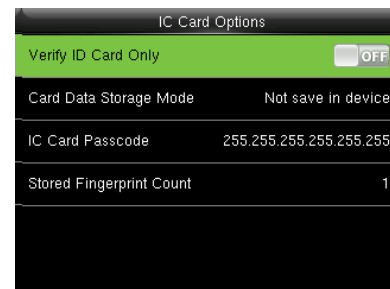
При необходимости настройте параметры Интеллектуальных карты, например, верифицировать ли только идентификационную карту, режим хранения данных карты, пароль интеллектуальной карты и количество сохраненных отпечатков пальцев.




В начальном интерфейсе нажмите \Rightarrow для входа в > главное меню, затем нажмите для выбора **Интеллектуальной карты** и нажмите \Rightarrow , чтобы войти.



Нажмите \surd , чтобы выбрать «**Параметры интеллектуальной карты**» и нажмите \Rightarrow .



Установите параметры интеллектуальной карты, как требуется.

Верифицировать только идентификационную карту: чтобы установить следует ли верифицировать только идентификационную карту, нажмите , чтобы включить функцию. После включения все зарегистрированные карты отпечатков пальцев не могут быть верифицированы на этом устройстве, только номер зарегистрированной идентификационной карты может быть успешно верифицирован. О том, как зарегистрировать карту Mifare в качестве идентификационной карты или карты отпечатков пальцев см. 11.1 Регистрация в качестве идентификационной карты или 11.2 Регистрация в качестве карты отпечатков пальцев для получения подробной информации.

Режим хранения данных на карте: установка режима хранения данных, зарегистрированных на карте Mifare, который включает следующие режимы:

1. **Не сохранять на устройстве:** все зарегистрированные данные будут сохранены только на карте Mifare, они не будут сохранены на устройстве.
2. **Сохраните пользовательские данные на устройстве:** за исключением пользовательских данных, другие зарегистрированные данные (например, отпечатки пальцев) не будут сохранены на устройстве.
3. **Сохранение пользователя и отпечатка пальца на устройстве:** все зарегистрированные пользовательские данные и отпечаток пальца будут сохранены на устройстве и карте Mifare синхронно.

Код доступа интеллектуальной карты: при необходимости установите код доступа интеллектуальной карты, который находится в диапазоне от 0 до 255. После того, как код доступа установлен, устройство запишет код доступа на зарегистрированную карту Mifare. Карту Mifare можно использовать только на этом устройстве.

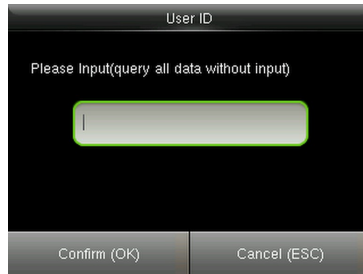
Количество сохраненных отпечатков пальцев: укажите количество отпечатков пальцев, хранящихся на карте.

12 Поиск записей

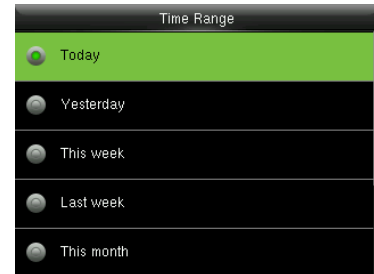
Когда пользователи успешно пройдут верификацию, записи будут сохранены на устройстве. Эта функция позволяет пользователям проверять записи доступа.



В начальном интерфейсе нажмите \rightarrow для входа в > главное меню, затем нажмите для выбора **Поиск учета рабочего времени** и нажмите \rightarrow .



Введите идентификатор пользователя (запросите все данные без ввода) и нажмите, чтобы ввести \rightarrow .



Выберите диапазон времени для поиска и нажмите для входа \rightarrow .

Personal Record Search		
Date	User ID	Access records
09-17		Number of Records:24
	0	17:05 17:05 14:40 14:40 14:24 14:24 13:32 10:29 10:29 10:29 10:29 10:29 10:29 10:29 08:59
	1	13:33 13:32 10:30 10:30 10:05 10:04 10:04 10:04

Prev : Left key Next : Right key Details : OK

Общее количество записей доступа за указанный промежуток времени отобразится на экране и нажмите \rightarrow .

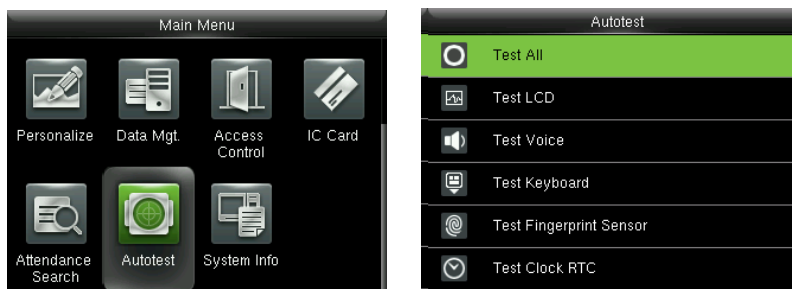
Personal Record Search				
User ID	Name	Access reco	Mode	Sta
1		09-17 13:33	255	0
1		09-17 13:32	0	0
1		09-17 10:30	0	0
1		09-17 10:30	0	0
1		09-17 10:05	0	0
1		09-17 10:04	0	0
1		09-17 10:04	255	0
1		09-17 10:04	0	0


Verify By : 0 Status : In



Подробные записи доступа каждого пользователя будут отображаться.



13 Автоматическое тестирование



Для автоматической проверки правильности работы всех модулей устройства, включая ЖК-дисплей, голос, клавиатуру, датчик отпечатков пальцев, камеру и часы реального времени (RTC).







В начальном интерфейсе нажмите  > Автоматическое тестирование, чтобы войти в интерфейс **Автоматическое тестирование**.





Тестирование всего: для тестирования ЖК-дисплея, голоса, клавиатуры, датчика отпечатков пальцев и RTC. Во время тестирования нажмите , чтобы перейти к следующему тестированию, а затем нажмите , чтобы выйти из тестирования.

Тестирование ЖК-дисплея: для тестирования эффекта отображения на ЖК-экране путем отображения полноцветного, чисто белого и чисто черного цветов, чтобы проверить правильность отображения цветов на экране. Во время тестирования нажмите , чтобы перейти к следующему тестированию, а затем нажмите , чтобы выйти из тестирования.

Тестирование голоса: устройство автоматически тестирует, заполнены ли голосовые файлы, хранящиеся на устройстве, и хорошее ли качество голоса. Во время тестирования нажмите , чтобы перейти к следующему тестированию, а затем нажмите , чтобы выйти из тестирования.

Тестирование клавиатуры: тестировать все клавиши, чтобы увидеть, работает ли каждая клавиша должным образом. Нажмите любую клавишу в интерфейсе тестирования клавиатуры; если нажатая клавиша соответствует значку клавиши, отображаемому на экране, то эта клавиша функционирует должным образом. Нажмите  или , чтобы выйти из тестирования.

Тестирование датчика отпечатка пальца: чтобы протестировать датчик отпечатка пальца, нажмите отпечаток пальца, чтобы проверить, четкое ли полученное изображение отпечатка пальца. При прижатии отпечатка пальца к датчику изображение будет отображаться на экране. Нажмите  или , чтобы выйти из тестирования.

Тестирование часов RTC: для тестирования часов реального времени. Устройство тестирует, правильно и точно ли работают часы, сверяясь с секундомером. Нажмите , чтобы начать отсчет времени, и нажмите  еще раз для прекращения отсчета, чтобы увидеть, точно ли секундомер отсчитывает время. Нажмите  или , чтобы выйти из тестирования.

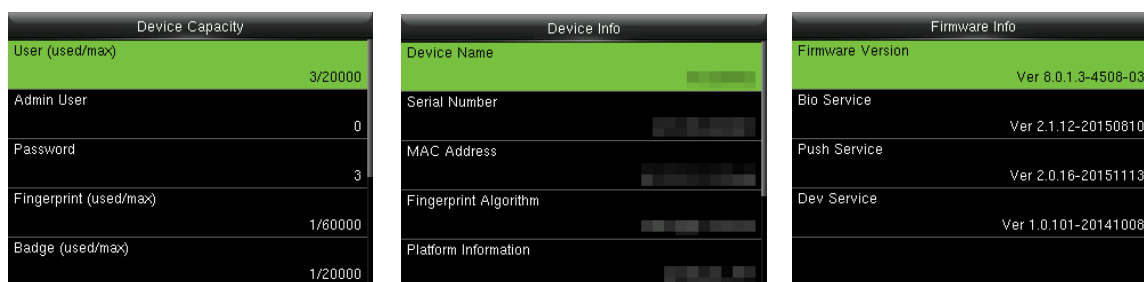
14 Информация о системе

Проверьте емкость данных, информацию об устройстве и прошивке.



В начальном интерфейсе нажмите  > **Информация о системе**, чтобы войти в интерфейс

Информация о системе.



Емкость устройства


Информация об устройстве

Информация об прошивке


Емкость устройства: для отображения количества зарегистрированных пользователей, администраторов, паролей, отпечатков пальцев, карт и записей, а также для проверки общего хранилища пользователей, отпечатков пальцев, карт и записей.

Информация об устройстве: для отображения имени устройства, серийного номера, MAC-адреса, алгоритма отпечатка пальца, информации о платформе, версии MCU, производителя и даты производителя.

Информация о прошивке: для отображения версии прошивки, службы Bio, службы Push и службы Dev.

 **Примечания:** отображение емкости устройства, информации об устройстве и информации о программном обеспечении на системном информационном интерфейсе разных продуктов может отличаться; фактический продукт имеет преимущественную силу.

15 Устранение неполадок

- Датчик отпечатков пальцев не может эффективно считывать и верифицировать отпечатки пальцев.
 - Проверьте не мокрый ли палец или не загрязнен ли датчик отпечатков пальцев.
 - Очистите палец и датчик отпечатков пальцев и попробуйте снова.
 - Если палец слишком сухой, подуйте на него и попробуйте снова.
- После верификации отображается «Неверный часовой пояс».
 - Обратитесь к администратору, чтобы проверить, имеет ли пользователь право на получение доступа в течение этого времени.
- Верификация прошла успешно, но пользователь не может открыть дверь.
 - Проверьте, правильно ли установлена пользовательская привилегия.
 - Проверьте правильность проводки замка.
- Тревожная сигнализация антивандального датчика сработала.
 - Проверьте, закреплены ли устройство и задняя панель вместе; если нет, антивандальный датчик сработает и поднимет тревогу, значок  будет отображаться в правом верхнем углу интерфейса. Только когда для параметра **[Тревожная сигнализация динамика] (Контроль доступа > Параметры контроля доступа > Тревожная сигнализация динамика)** установлено значение [ВКЛ], динамик подаст сигнал тревоги.

16 Приложения

16.1 Обзор Wiegand

Протокол Wiegand26 - это стандартный протокол контроля доступа, разработанный Подкомитетом стандартов 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

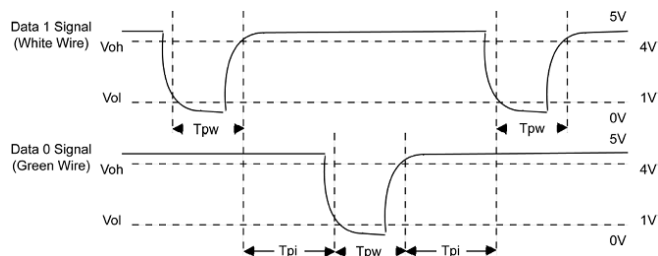
На рис.1 показана диаграмма последовательности устройства чтения карт, отправляющего цифровой сигнал в битах на контроллер доступа. Wiegand на этой диаграмме соответствует стандартному протоколу управления доступом SIA, который предназначен для 26-разрядного устройства считывания карт Wiegand (с временем 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 V_{oh}), пока устройство чтения карт не будет готово к отправке потока данных. Считыватель карт посылает асинхронный импульс низкого уровня (меньше чем V_{oh}), передавая поток данных через кабель Data1 или Data0 на блок управления доступом (как пилообразная волна на рисунке 1). Импульсы Data1 и Data0 не перекрываются и не синхронизируются. На рис.1 показана максимальная и минимальная длительность импульса (последовательные импульсы) и время скачкообразного изменения импульсов (время между двумя импульсами), допустимое для терминалов контроля доступа по отпечаткам пальцев серии F.

Таблица 1: Время пульса

Знак	Определение	Типичное значение считывателя карт
Тpw	Ширина импульса	100 μ s

T _{pi}	Интервал пульса	1 ms
-----------------	--------------------	------

Рис. 1: Схема последовательности



16.1.1 Обзор Wiegand 26

26-битные и 34-битные форматы Wiegand описываются следующим образом.

Композиция формата Wiegand 26 бит содержит 2 бита четности и 24 бита для выходного содержимого («Идентификатор пользователя» или «Номер карты»). 24-битный двоичный код представляет до 16 777 216 (0–16 777 215) различных значений.

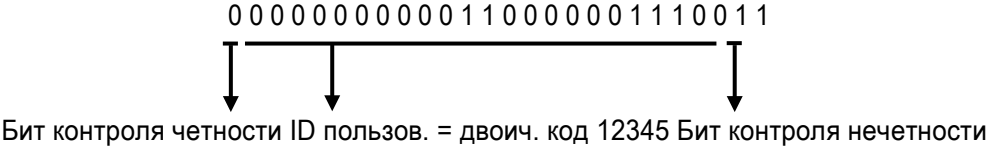
1	2	25	26
Бит контроля четности	Идентификатор пользователя / номер карты	Бит контроля нечетности	

В следующей таблице описаны поля.

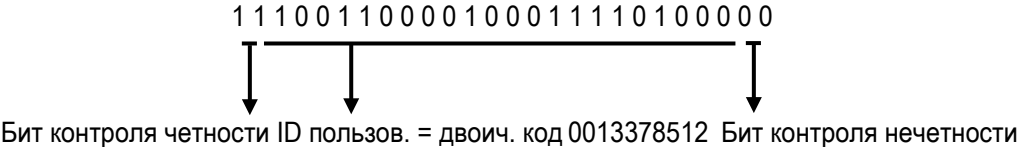
Поле	Описание
Бит контроля четности	Бит контроля четности определяется битами 2-13. Если есть четное число 1, бит контроля четности равен 0. Если есть нечетное число 1, бит контроля четности равен 1.
Идентификатор пользователя / номер карты (бит 2-бит25)	Идентификатор пользователя / номер карты (код карты, 0–16777215) Бит 2 является наиболее значимым битом (MSB).
Бит контроля нечетности	Бит контроля нечетности определяется битами 14-25. Если есть четное число единиц, бит контроля нечетности равен 1. Если есть нечетное число 1, бит контроля четности равен 0.

Например: для пользователя с идентификатором пользователя 12345 номер зарегистрированной карты равен 0013378512, а для идентификатора с ошибкой установлено значение 1.

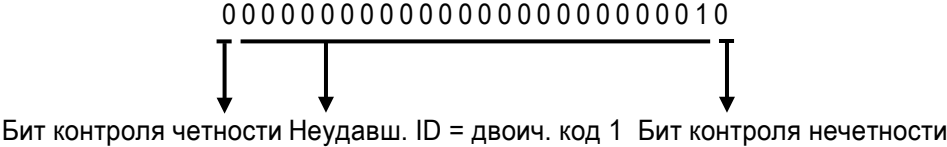
1. Когда для выхода задано «ID пользователя», выход Wiegand при успешной верификации выглядит следующим образом.



2. Когда для выхода задано «Номер карты», выход Wiegand будет следующим после успешной верификации.



3. Выход Wiegand выглядит следующим образом при сбое верификации:



Примечание: если выходное содержимое 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.

16.1.2 Обзор Wiegand 34

Система имеет встроенный Wiegand 34-битный формат. Композиция формата Wiegand 34-bit содержит 2 бита четности и 32 бита для выходного содержимого («Идентификатор пользователя» или «Номер карты»). 32-разрядный двоичный код представляет до 4 294 967 296 (0–4 294 967 295) различных значений.

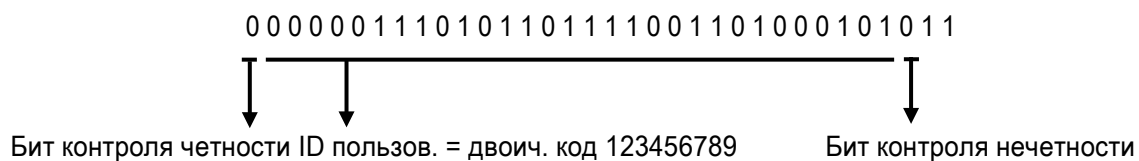
1	2	33	34
Бит контроля четности	Идентификатор пользователя / номер карты	Бит контроля нечетности	

В следующей таблице описаны поля.

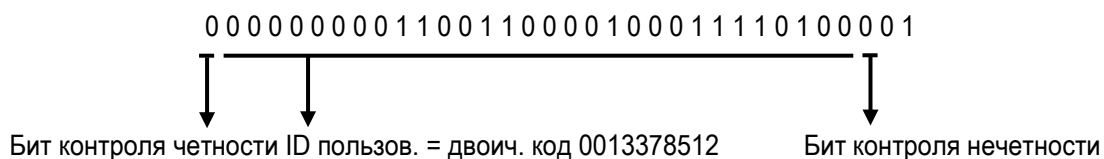
Поле	Описание
Бит контроля четности	Бит контроля четности определяется битами 2-17. Если есть четное число 1, бит контроля четности равен 0. Если есть нечетное число 1, бит контроля четности равен 1.
Идентификатор пользователя / номер карты (бит 2-бит25)	Идентификатор пользователя / номер карты (код карты, 0-4 294 967 295) Бит 2 является наиболее значимым битом (MSB).
Бит контроля нечетности	Бит контроля нечетности определяется битами 18-33. Если есть четное число единиц, бит контроля нечетности равен 1. Если есть нечетное число 1, бит контроля четности равен 0.

Например: для пользователя с идентификатором пользователя 123456789 номер зарегистрированной карты равен 0013378512, а для неудавшегося идентификатора установлено значение 1.

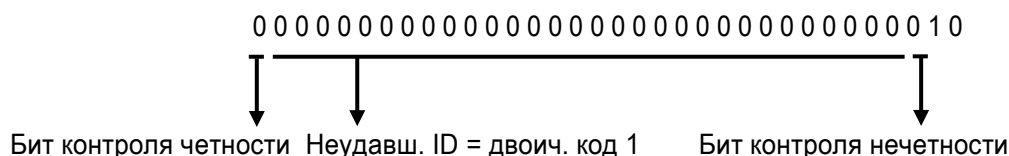
1. Когда для выхода задано «ID пользователя», выход Wiegand при успешной верификации выглядит следующим образом.



2. Когда для выхода задано «Номер карты», после прохождения пользователем успешной верификации выход Wiegand будет следующим.



3. При сбое верификации выход Wiegand выглядит следующим образом:



16.2 Правило загрузки изображения

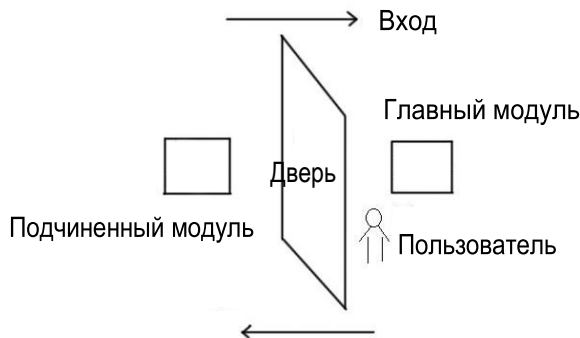
1. Рекламное изображение: необходимо создать файл с именем «advertise» в файле USB-диска и поместить в него рекламные изображения. Емкость составляет 20 изображений, каждое из которых не превышает 30к. Имя и формат изображения не ограничены.

2. Обои: необходимо создать файл с именем «wallpaper» в файле USB-диска и поместить обои в файл. Емкость составляет 20 изображений, каждое из которых не превышает 30к. Имя и формат изображения не ограничены.

16.3 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 устройств для совместной работы: одно устанавливается внутри двери (главный модуль), другое - снаружи двери (подчиненный модуль). Два модуля обмениваются данными с помощью сигнала Wiegand. Формат Wiegand и тип выхода (идентификатор пользователя / номер карты), принятые главным модулем и подчиненным модулем, должны быть согласованы.



[Принцип работы]

Главный модуль поддерживает функцию Вход Wiegand, а подчиненный модуль поддерживает функцию Выход Wiegand. После того, как выходной порт Wiegand подчиненного модуля подключен к входному порту Wiegand главного 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.

Если для пользователя на главном модуле 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 регистрации 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 регистрации 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 модуле 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 модуль: устройства, поддерживающие функцию Вход Wiegand, кроме ведомого устройства считывателя F10.

Подчиненный модуль: 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.

(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 **«Основные настройки» > «Управление устройством» > «Wiegand»** и установите **«Определенного формат»** для Wiegand26-bits или **Wiegand26 без идентификатора**

устройств.

(4) Регистрация пользователя

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

(5) Описание проводки

Ведущее и ведомое устройства обмениваются данными друг с другом по Wiegand, а схема подключения следующая :

Главный модуль		Подчинен. модуль
IWD0	<----->	WD0
IWD1	<----->	WD1
GND	<----->	GND

16.4 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.

16.5 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 опасных 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	x	○	○	○	○	○
Чип конденсатор	x	○	○	○	○	○
Чип индуктор	x	○	○	○	○	○
Чип диод	x	○	○	○	○	○
Компоненты ESD	x	○	○	○	○	○
Зуммер	x	○	○	○	○	○
адаптер	x	○	○	○	○	○
Винты	○	○	○	x	○	○

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

x: 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.

Green Label

ZK Building, Wuhe Road, Gangtou, Bantian, Buji Town,
Longgang District, Shenzhen China 518129

Tel: +86 755-89602345

Fax: +86 755-89602394

www.zkteco.com

