Руководство пользователя

Устройство контроля доступа серии RFID

Версия 1.1.

Дата: январь 2020

Введение:

Этот документ представляет пользовательский интерфейс и операции с меню. Кроме того, может быть в комплекте Access3.5 Security System для совместного использования. Для установки, обращайтесь к руководству по установке.

Важное заявление

Прежде всего, спасибо за покупку этого гибридного терминала для лица и отпечатков пальцев. Перед использованием внимательно прочитайте данное руководство, чтобы избежать ненужных повреждений! Компания напоминает вам, что ответственный пользователь улучшит эффект использования и скорость аутентификации.

Никакое письменное согласие нашей компании, какого-либо подразделения или физического лица не допускается для выдержки, частичного или полного копирования содержания данного руководства, а также распространения в любой форме.

Продукт, описанный в руководстве, может включать программное обеспечение, авторские права которого передаются лицензиарам, включая нашу компанию. За исключением разрешения соответствующего владельца, никакое лицо не может копировать, распространять, редактировать, изменять, извлекать, декомпилировать, разбирать, дешифровать, предпринимать обратный инжиниринг, лизинг, передачу, сублицензирование программного обеспечения, и другие акты нарушения авторских прав, но ограничения, налагаемые на закон, исключаются.

Мы не можем ни обещать, что информация соответствует фактическому устройству из-за постоянно обновления устройства, ни принять любой спор, связанный с фактическими техническими параметрами и соответствующей этой информации. Любые изменения проводятся без предварительного уведомления.

Содержание

1. Примечания при использовании

Не используйте устройство под прямыми солнечными лучами и избегайте использования на открытом воздухе летом. Рабочая температура колеблется от 0 до 40 градусов по Цельсию. Тепло, рассеиваемое во время длительной работы, может легко привести к замедлению отклика и снижению скорости прохождения проверки. Рекомендуется использовать навесы и радиаторы для устройства при использовании снаружи.

1.1 Обзор руководства

- Фотография в этом руководстве может отличаться от реальной фотографии. Фактический продукт имеет преимущественную силу.

- Характеристика (аспекты логики приложения прошивки):

(1) Функция RFID
Поддерживает интеллектуальную и идентификационную карты.

(2) Параметры доступа пользователя

В основном имеют следующие расширенные функции контроля доступа:

1. Дата вступления пользователя в силу

2. Срок действия пользователя

3. Режим множественной верификации пользователя

4. Действующая зона времени разрешенного доступа для двери

5. Функция времени открытия двери

6. Период праздничных дней

7. Нормально-открытый режим для первой карты

8. Записи контроля доступа контроллера

9. Функция связи

10. Контроль прохода в обоих направлениях на вход и выход

11. Функция Wiegand для главного и вспомогательного устройств

12. Контроль прохода в обоих направлениях для зоны времени разрешенного доступа

Вышеуказанные расширенные функции контроля доступа должны поставляться в комплекте с Access3.5 Security System. Для получения подробной информации смотрите Руководство пользователя программного обеспечения Access3.5.

(3) Функция U-диска

Поддержка загрузки U-диска и загрузки пользовательских данных, не поддерживает загрузку U-диска к записям контроля доступа.

(4) Поддержка сетевой связи

Через интернет со связью программного обеспечения Access Control 3.5.

(5) Функция учета рабочего времени

Нажмите  чальном интерфейсе, соответствующие клавиши состояния и функциональные клавиши отображаются в правом углу интерфейса для использования. Включая регистрацию входа, регистрацию выхода, уход на перерыв, приход с перерыва, приход на сверхурочные и т. д.

1.2 Использование сенсорного экрана

Прикоснитесь к экрану кончиками пальцев или краем ногтя, как показано на рисунке ниже. Широкая точка контакта может привести к неточному наведению.

Когда сенсорный экран менее чувствителен к касанию, вы можете выполнить калибровку экрана с помощью следующих операций меню. Нажмите ***[Меню]*** > ***[Автоматическое тестирование]*** > ***[Калибровкаа]*** на экране, и появится значок креста. После того, как вы правильно дотронетесь до центра крестика в пяти точках на экране, система автоматически вернется в меню [***Автоматическое тестирование***]. Нажмите [***Выход***], чтобы вернуться к интерфейсу [***Меню***]. Подробнее см. Описание в разделе 9. Автоматическое тестирование.

Мазок или пыль на сенсорном экране могут повлиять на производительность сенсорного экрана. Поэтому старайтесь держать экран чистым и без пыли.

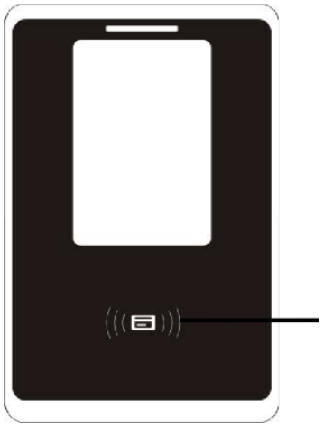
1.3 Операции на сенсорном экране

1. Введите цифры: нажмите клавишу [***Идентификатор пользователя***]. Система автоматически отобразит интерфейс ввода номера. После ввода идентификатора пользователя нажмите [***OK***] для сохранения или нажмите [***X***] для отмены и возврата к предыдущему интерфейсу.

2. Введите текст: нажмите клавишу [***Имя***]. Система автоматически отобразит интерфейс ввода текста. После вводаимя пользователя, нажмите [***X***], чтобы закрыть текстовые интерфейсы, а затем нажмите [***сохранить***] и вернитесь к предыдущему интерфейсу.

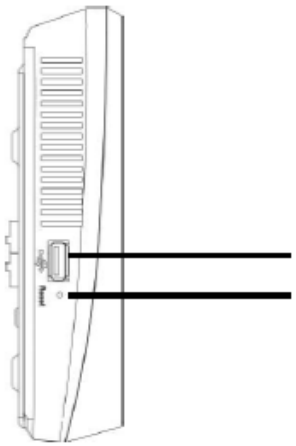
1.4 Внешний вид устройства

(1) Вид спереди



Зона сканирования карты

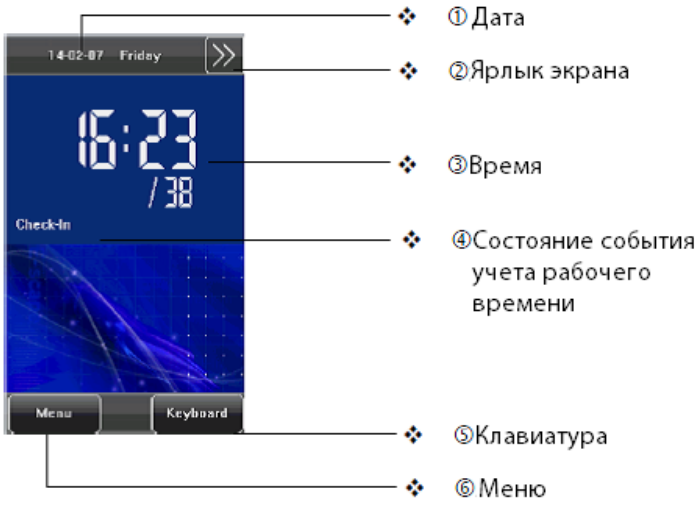
(2) Вид сбоку



USB-порт

Кнопка сброса

1.5Главный интерфейс



❖ ①Дата

❖ ②Ярлык экрана

❖ ③Время

❖ ④Состояние события учета рабочего времени

❖ ⑤Клавиатура

❖ ⑥Меню

① ***Дата:*** отображается текущая дата.

② ***Ярлык экрана:*** нажмите эти сочетания клавиш для отображения состояния событий учета рабочего времени.

③ ***Время:*** отображается текущее время. Поддерживаются как 12-часовые, так и 24-часовые системы времени.

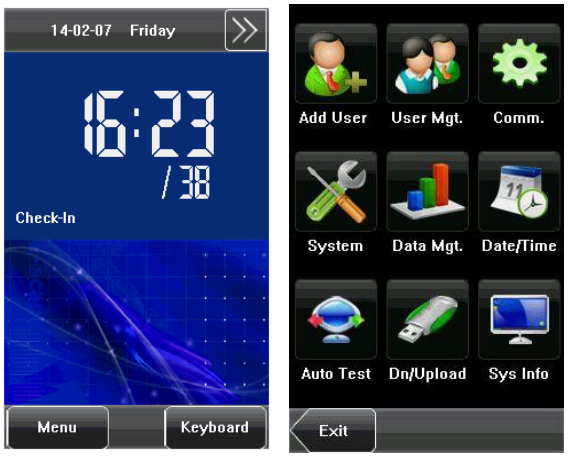
④ ***Состояние событий учета рабочего времени:*** отображается текущее состояние событий учета рабочего времени.

⑤ ***Клавиатура:*** нажав эту клавишу, вы можете войти в интерфейс цифрового ввода.

⑥ ***Меню:*** вы можете войти в главное меню, нажав эту клавишу.

2. Главное меню

Нажмите [***Меню***] в начальном интерфейсе для доступа к главному меню, как показано на рисунке ниже:



Главное меню включает в себя девять подменю:

Добавить пользователя: с помощью этого подменю можно добавить нового пользователя и ввести информацию об устройстве, включая идентификатор пользователя, имя, карту, пароль, роль (авторизации).

Управление пользователем: с помощью этого подменю можно просматривать информацию о пользователе, хранящуюся на устройстве, включая идентификатор пользователя, имя, карту, пароль, роль. Здесь вы также можете добавить, изменить, запросить или удалить информацию о пользователе.

Связь: с помощью этого подменю можно установить соответствующие параметры для связи между устройством и ПК, включая IP-адрес, маску подсети, шлюз, идентификатор устройства и ключ связи.

Система: с помощью этого подменю можно установить системные параметры, включая общие, отображение, ярлык по умолчанию, параметры контроля доступ и обновление.

Управление данными: с помощью этого подменю можно выполнять управление данными, хранящимися на устройстве, например, удаление всех данных, очистка администратора, восстановление заводских настроек.

Дата / Время: в этом подменю можно установить дату, время, формат даты и 24-часовой формат времени.

Автоматическое тестирование: это подменю позволяет системе автоматически проверять, являются ли функции различных модулей нормальными, включая экран, голос, время и калибровку экрана.

Загрузить / выгрузить: с помощью этого подменю можно загружать информацию о пользователе и данные о событиях учета рабочего времени, хранящиеся на устройстве, через USB-диск и загружать информацию о пользователе на устройство.

Информация о системе: в этом подменю можно просматривать записи емкости Контроль доступа (100 000), Пользователи (30 000) и информацию об устройстве.

Любой пользователь может получить доступ к главному меню, нажав клавишу [***Меню***], если в системе нет администратора. Если у вас есть администратор, устройство должно проверить личность администраторов, прежде чем предоставить им доступ к главному меню. Для обеспечения безопасности устройства рекомендуется установить администратора при первоначальном использовании терминала.

3. Добавить пользователя

Нажмите [***Добавить пользователя***] в интерфейсе главного меню, чтобы отобразить интерфейс [***Добавить пользователя***], как показано ниже:

Этапы добавления пользователя: введите Идентификатор пользователя> введите имя> зарегистрируйте идентификационную карту> введите пароль> установите роль.

Идентификатор пользователя: введите идентификатор пользователя. Идентификаторы пользователя от 1 до 9 цифр поддерживаются по умолчанию.

Имя: введите имя пользователя. 24 символов имени пользователя поддерживаются по умолчанию.

Карта: нажмите на идентификационную карту, чтобы зарегистрировать нового пользователя.

Пароль: введите пароль пользователя. Устройство поддерживает пароли из 1-8 цифр по умолчанию.

Роль: установите права пользователя. Пользователь по умолчанию настроен на ***обычного пользователя***, а также на ***администратора***.

Рекомендация: когда новый пользователь регистрируется на устройстве, он одновременно устанавливает функцию контроля доступа по умолчанию. Другие сложные расширенные функции контроля доступа для настройки требуют программного обеспечения Access3.5.

3.1 Ввод идентификатора пользователя

Устройство автоматически назначает идентификатор, начиная с 1, для каждого пользователя в последовательности. Если вы используете идентификатор, присвоенный устройству, вы можете пропустить этот раздел.

1. Нажмите [***Идентификатор пользователя***] на интерфейсе [***Добавить пользователя***], чтобы отобразить интерфейс управления Идентификатором пользователя.

Рекомендация: Совет: идентификатор пользователя может быть изменен во время начальной регистрации, но после регистрации он не может быть изменен.

2. В отображаемом интерфейсе клавиатуры введите идентификатор пользователя и нажмите [***OK***]. Если сообщение «Идентификатор пользователя существует!», введите идентификатор еще раз.

Рекомендация: По умолчанию устройство поддерживает от 1 до 9 цифр. Если вам нужно увеличить длину идентификационных номеров текущих пользователей, проконсультируйтесь с нашими коммерческими представителями или службой технической предпродажи.

3. После ввода идентификатора пользователя нажмите [***Сохранить***], чтобы сохранить текущую информацию и вернуться к предыдущему интерфейсу. Нажмите [***Выход***], чтобы вернуться к предыдущему интерфейсу без сохранения текущей информации.

3.2 Ввод имени

Используйте метод ввода T9, чтобы ввести имя пользователя через клавиатуру.

1. Нажмите [***Имя***] в интерфейсе [***Добавить пользователя***], чтобы отобразить интерфейс ввода имени.

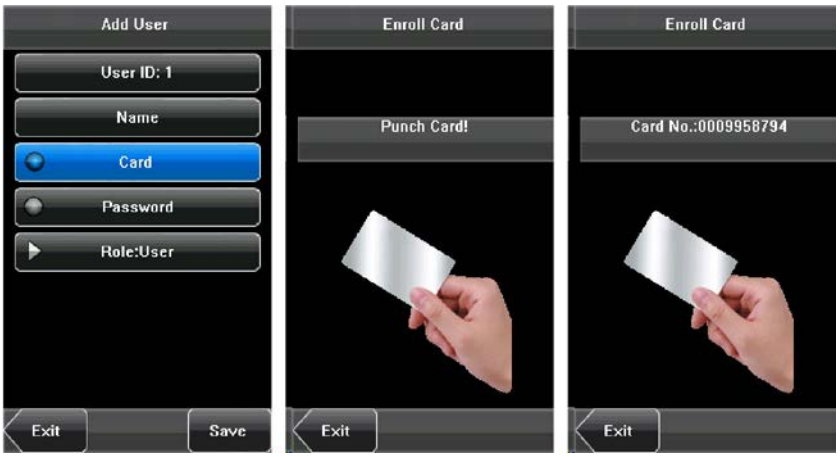
2. В отображаемом интерфейсе клавиатуры введите имя пользователя и нажмите [***Вход***], а затем нажмите [***X***]. Подробнее об операциях с интерфейсом клавиатуры смотрите раздел 12.1 Инструкция по вводу T9.

3. После ввода имени пользователя нажмите [***Сохранить***], чтобы сохранить текущую информацию и вернуться к предыдущему интерфейсу. Нажмите [***Выход***], чтобы вернуться к предыдущему интерфейсу без сохранения текущей информации.

Рекомендация: имя по умолчанию для устройства поддерживает от 1 до 24 цифр (содержит пробелы).

3.3 Регистрация идентификационной карты

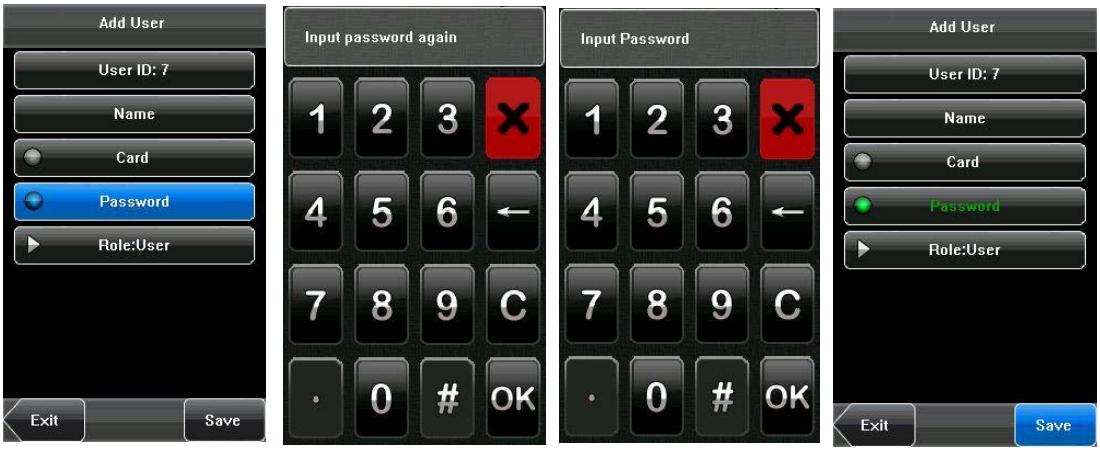
1. Нажмите [***Карта***] в интерфейсе [***Добавить пользователя***], чтобы отобразить интерфейс [***Зарегистрировать карту***].
2. Откроется интерфейс [***Сканировать карту***], как показано ниже. Проведите пальцем по вашей идентификационной карточке в области сканирования. Подробности см. В разделе «Внешний вид устройства».
3. Нажмите [***Сохранить***], чтобы сохранить текущую информацию и вернуться к предыдущему интерфейсу. Нажмите [***Выход***], чтобы вернуться к предыдущему интерфейсу без сохранения текущей информации.



Рекомендация: по умолчанию используется бесконтактная карта 125 кГц, дополнительная карта Mifare 13,56 МГц.

3.4 Регистрация пароля

1. Нажмите [***Пароль***] в интерфейсе [***Добавить пользователя***], чтобы отобразить интерфейс управления паролями.
2. В отображаемом интерфейсе клавиатуры введите пароль и нажмите [***OK***]. Повторно введите пароль в соответствии с запросом системы, а затем нажмите [***OK***].
3. После ввода пароля отображается интерфейс, как показано ниже. Нажмите [***Сохранить***], чтобы сохранить текущую информацию и вернуться к предыдущему интерфейсу. Нажмите [Выход], чтобы вернуться к предыдущему интерфейсу без сохранения текущей информации.



3.5 Роль пользователя

Существует два типа авторизаций пользователей: ***пользователь*** и ***администратор***. Обычным пользователям предоставляются только права верификации пароля или карты. Администраторы получают доступ к главному меню для различных операций, помимо всех полномочий, предоставляемых обычным пользователям.

 Укажите, что пользователь является администратором.

1. В интерфейсе [***Добавить пользователя***] нажмите [***Роль: Пользователь***], чтобы изменить пользователя на администратора.

2. После внесения изменений интерфейс выглядит так, как показано ниже. Нажмите [***Сохранить***], чтобы сохранить текущую информацию и вернуться к предыдущему интерфейсу; нажмите [***Выход***], чтобы вернуться к предыдущему интерфейсу без сохранения текущей информации.

3.6 Верификация пользователя

После регистрации вы можете проверить действительность этой идентификационной карты или пароля в начальном интерфейсе. Верификация пользователя должна соответствовать типу верификации. Способ установки типа верификации, обратитесь к разделу 6.4.4 Тип верификации.

3.6.1 Верификация пароля

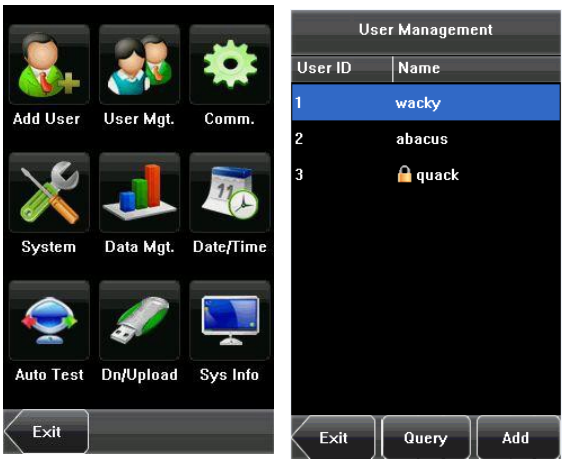
1. Нажмите [***Клавиатура***] на экране.
2. Введите идентификатор пользователя, а затем нажмите  , чтобы войти в режим верификации пароля. Если появится подсказка «Не зарегистрирован!», идентификатор не существует.
3. Введите пароль и нажмите [***OK***], чтобы начать сравнение пароля.
4. Если верификация прошла успешно, устройство выдаст запрос «Верификация прошла успешно», в противном случае устройство выдаст запрос «Верификация не удалась» и вернется к начальному интерфейсу.

3.6.2 Верификация идентификационной карты

1) Проведите свою идентификационную карту в области сканирования карты, выбирая правильный путь.
2) Если верификация выполнена успешно, устройство выдаст сообщение «Верификация прошла успешно».
3) Если верификация не удалась, устройство выдаст сообщение «Не зарегистрирован».

4. Управление пользователями

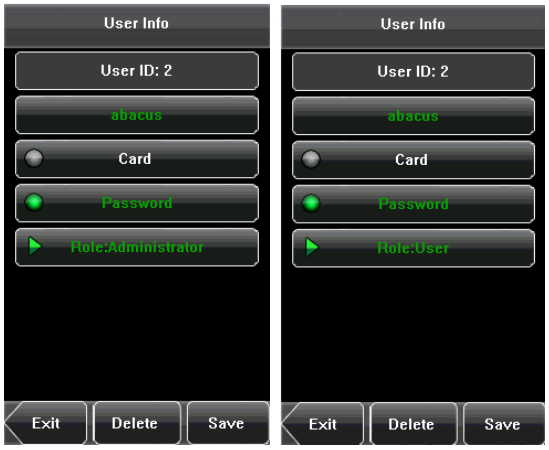
Управление пользователями: управление зарегистрированными пользователями. Просмотрите информацию о пользователе, включая идентификатор пользователя, имя, карту, пароль, роль (авторизация). С помощью этого интерфейса можно добавлять, запрашивать, редактировать или удалять основную информацию пользователей.
Нажмите [***Управление пользователями***] в интерфейсе главного меню, чтобы отобразить интерфейс управления пользователями.



Этот пользователь является администратором.

4.1 Редактирование пользователя

Нажмите имя пользователя из списка, чтобы войти в интерфейс [***Информация о пользователе***].
Идентификатор пользователя не может быть изменен, а другие операции аналогичны тем, которые выполняются при добавлении пользователя. Вы можете изменить имя пользователя, пароль и роль, повторно зарегистрировать идентификационную карту.
Например: измените права пользователя с администратора на обычного пользователя. Как показано ниже.



4.2 Удалить пользователя

В интерфейсе [***Информация о пользователе***] вы можете удалить всю или частичную информацию пользователя.

1. Нажмите [***Удалить***], чтобы удалить пользователя.
2. На отображаемом интерфейсе нажмите [***ДА***], чтобы удалить текущего пользователя, или [***НЕТ***], чтобы вернуться к предыдущему интерфейсу.
3. В интерфейсе [***Информация о пользователе***] нажмите [***Имя***] или [***Пароль***], чтобы удалить информацию о соответствующем пользователе и повторно зарегистрировать новую информацию, следуя подсказке устройства.

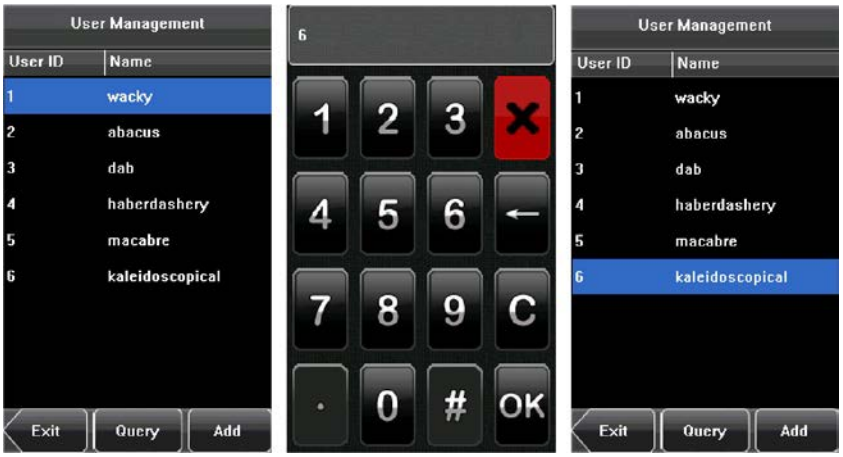
4.3 Запрос пользователя

Чтобы облегчить администраторам быстрый поиск пользователя среди большого количества зарегистрированных пользователей, устройство позволяет выполнять запросы по «Идентификатору пользователя».

Запрос идентификатора пользователя:

1. Нажмите [***Запрос***] в интерфейсе [***Управление пользователями***], чтобы отобразить интерфейс запроса идентификатора пользователя.

2. Введите идентификатор пользователя в отображаемом интерфейсе и нажмите [***OK***], чтобы навести курсор на нужного пользователя.



5. Настройка связи

Вы можете установить соответствующие параметры для связи между устройством и ПК, включая ***IP-адрес, маску подсети, шлюз, идентификатор устройства, ключ связи, вход Wiegand*** и ***выход Wiegand.***

5.1 Настройка связи

***IP-адрес*:** IP-адрес по умолчанию 192.168.1.201 и может быть изменен при необходимости.

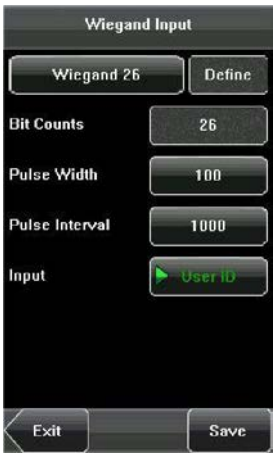
Маска подсети: Маска подсети по умолчанию 255.255.255.0 и может быть изменена при необходимости.

Шлюз: шлюз 0.0.0.0 по умолчанию и может быть изменен при необходимости.

Идентификатор устройства: этот параметр используется для установки идентификатора устройства от 1 до 254.

Ключ связи: для повышения безопасности данных о посещаемости вы можете установить пароль для соединения между устройством и ПК. После установки пароля вы можете подключить ПК к устройству для доступа к данным о посещаемости только после ввода правильного пароля. Пароль по умолчанию - 0 (то есть без пароля), поддерживаются пароли от 1 до 6 цифр.

5.2 Вход Wiegand



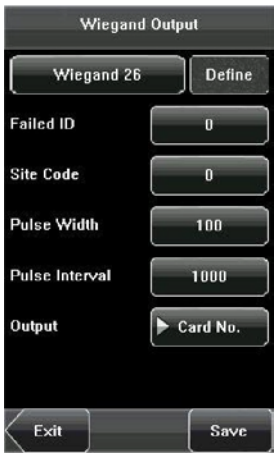
Число битов: длина цифры данных Wiegand.

Ширина импульса: ширина импульса по умолчанию составляет 100 микросекунд, который можно настроить в диапазоне от 1 до 1000. Интервал импульса: по умолчанию составляет 1000 микросекунд, который можно настроить в диапазоне от 1 до 10000. Вход: содержимое содержится во входном сигнале Wiegand, включая пользователя. ID или номер карты.

Рекомендация: Поддержка подключения к сторонней панели управления доступом с помощью интерфейса Wiegand.

Для получения подробной информации о Wiegand смотрите раздел 12.3 Введение в Wiegand.

5.3 Выход Wiegand



Формат Wiegand: система имеет два встроенных формата Wiegand 26-бит и Wiegand 34-бит, а также поддерживает функцию настройки формата для удовлетворения индивидуальных требований.

Неудавшийся идентификатор: Относится к значению, выводимому системой при сбое верификации. Выходной формат зависит от настройки формата Wiegand. Область значений по умолчанию для ***Неудавшегося идентификатора*** составляет 0-65535.

Код сайта: код сайта используется для настраиваемого формата Wiegand. ***Код сайта*** аналогичен идентификатору устройства, но ***Код сайта*** настраивается и может дублироваться на разных устройствах. Область значений по умолчанию для кода сайта составляет 0 ~ 255.

Ширина импульса: обозначает ширину импульса Wiegand в микросекундах. Диапазон значений по умолчанию для ширины импульса составляет 1 ~ 1000.

Интервал импульса: Относится к интервалу импульса Виганда в микросекундах. Диапазон значений по умолчанию для ширины импульса составляет 1 ~ 10000.

Выход: относится к выводу содержимого после успешной проверки. Вы можете выбрать ***Идентификатор пользователя*** или ***Номер карты*** в качестве выхода.

Подробнее о Wiegand смотрите раздел 12.3 Введение в Wiegand.

5.4 Индивидуальный формат

Помимо двух встроенных форматов ***Wiegand 26-bit*** и ***Wiegand 34-bit***, система также поддерживает функцию настройки формата для удовлетворения индивидуальных требований.

Настраиваемый формат состоит из двух строк символов: биты ***Формата карты*** и ***Битов формата четности***. Эти две строки символов должны быть определены отдельно.

Биты ***Формата карты*** определяют количество двоичных битов, выводимых Wiegand, а также значение каждого бита. Биты данных, выводимые Wiegand, могут представлять собой номер карты (C), код сайта (s), код объекта (f), код производителя (m) и биты четности (p).

Биты ***Формата четности*** определяют режим проверки каждого бита в формате карты и обеспечивают правильность формата карты при передаче через проверку четности. Биты четности могут быть установлены для проверки нечетности (o), проверки четности (e) и для обоих проверок нечетности и четности (b).

Существует взаимно-однозначное соответствие между битами данных и битами четности.

Например, Wiegand26 можно настроить следующим образом:

Определение битов формата карты: pssssssssccccccccccccccccp

Определение битов формата четности: eeeeeeeeeeeeeeoooooooooooooo

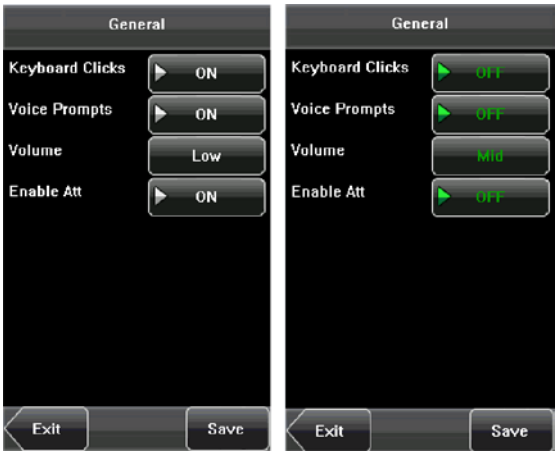
Рекомендация: Wiegand26 состоит из 26 бит. Первый бит - это четный бит четности от 2 до 13; 26-й бит является нечетным битом четности битов с 14 по 25; от 2-го до 9-го бита - код сайта; биты с 10-го по 25-й - это номер карты. Подробнее о Wiegand смотрите раздел 12.3 Введени в Wiegand.

6. Настройка системы

С помощью меню [***Система***] можно установить системные параметры, включая «Общие», «Дисплей», «Ярлык по умолчанию», «Параметры контроля доступа» и «Обновление прошивки».

6.1 Общий параметр

Общие настройки параметров включают щелчки клавиатуры, голосовые подсказки, громкость и включение учета рабочего времени.



6.1.1 Клавишные нажатия

Этот параметр используется, чтобы установить, генерировать ли звуковой сигнал в ответ на каждое касание клавиатуры. Выберите [***ВКЛ***], чтобы включить звуковой сигнал, и выберите [***ВЫКЛ***], чтобы отключить звук.

6.1.2 Голосовые подсказки

Этот параметр используется, чтобы указать, следует ли воспроизводить голосовые подсказки во время работы устройства. Выберите [***ВКЛ***] для включите голосовые подсказки и выберите [***ВЫКЛ***], чтобы отключить звук.

6.1.3 Громкость

Этот параметр используется для регулировки громкости голосовых подсказок.

6.1.4 Учет рабочего времени

Этот параметр используется для открытия функции учета рабочего времени, и в начальном интерфейсе отображается значок  .

6.2 Параметры дисплея

6.2.1 Язык

Этот параметр используется для отображения текущего языка, используемого устройством. С помощью этого параметра для многоязычных устройств можно переключаться на разные языки (английский, китайский и традиционный китайский). Затем вы должны перезагрузить устройство.

6.2.2 Панель инструментов

Этот параметр доступен для отображения состояния клавиш быстрого доступа в начальном интерфейсе, когда включена функция учета рабочего времени. Пользователь может нажать [***Скрыть автоматически***] или [***Отобразить на экране***].
Если функция учета рабочего времени отключена, эта функция параметра недействительна.

6.2.3 Время сна

Этот параметр используется для указания периода, после которого устройство переводится в спящий режим, если в течение этого периода не выполняются никакие операции. Вы можете вывести устройство из спящего режима, нажав любую клавишу или коснувшись экрана. Числовые диапазоны составляют 1 ~ 30 минут, 3 минуты по умолчанию.

6.3 Определение быстрого вызова

6.3.1 Использование сочетаний клавиш быстрого вызова

Нажмите  в начальном интерфейсе, и соответствующие клавиша состояния и функциональная клавиши отобразятся в правом углу интерфейса для использования.

6.3.2 Настройка определения быстрого вызова

Нажмите [***Меню***]> [***Система***]> [***Определение быстрого вызова***] в соответствии с необходимостью установки для пользователя клавиш быстрого вызова для клавиши состояния.

(1) Нажмите [***Состояние***], войдите в экран редактирования клавиши состояния, как показано на рисунке 1 ниже; нажмите на поле «***Метка***», войдите в экран «***Метка***», как показано на рисунке 2 ниже; нажмите на строку метки (шесть вариантов состояний), чтобы изменить ее на соответствующую метку; пользователь может выбрать метку клавиши состояния в соответствии с практическими потребностями.

Рис. 1

Рис. 2

Рекомендация: ***Код*** не может быть изменен; он изменяется соответственно с выбранной меткой клавиши состояния.

(1) Выберите [***Вкл.***] в ***Автовыключателе***, затем нажмите [***Определить***], цифры соответствуют показанным на рисунке 1 и рисунке 2 ниже.

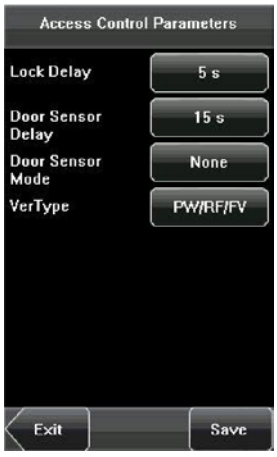
Рис. 1

Рис. 2

Рис. 3

(1) Нажмите поле времени после [***Воскресенье***], установите время, как показано на рисунке 3 выше. Нажмите [***OK***], чтобы сохранить и вернуться к экрану редактирования. Нажмите [**Сохранить**], чтобы сохранить настройку.

6.4 Параметры контроля доступа



Вы можете нажать [***Меню***]> [***Система***]> [***Параметры контроля доступа***], чтобы установить параметры задержки срабатывания замка, задержки датчика двери, режима датчика двери, типа верификации.

6.4.1 Задержка срабатывания замка

Время, в течение которого электромагнитный замок срабатывает от открытия до закрытия, когда верификация пользователя завершается успешно (в случае, если дверь закрыта).
«S (секунда)» выбрана в качестве единицы длительности срабатывания привода замка, и ее можно установить в пределах 1 ~ 10 сек.

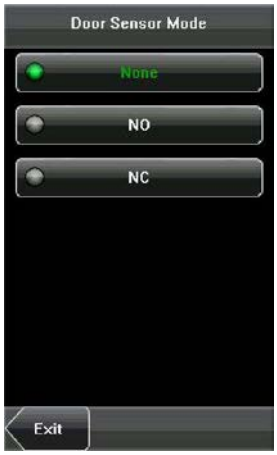
Если для длительности задано значение ***0***, значит параметр «Длительность срабатывания привода замка» отключен. Обычно мы не рекомендуем устанавливать его на ***0.***

6.4.2 Задержка датчика двери

Указывает на задержку проверки датчика двери после открытия двери. Если состояние датчика двери не соответствует нормальному состоянию, установленному переключателем датчика двери, срабатывает сигнал тревоги, и этот период времени считается ***Задержкой датчика двери***. (Диапазон значений в пределах 1 ~ 99 сек.)

6.4.3 Режим датчика двери

Включает режимы Отсутствует, Нормально-открытый (NO) и Нормально-закрытый (NC). ***Отсутствует*** указывает на то, что выключатель датчика двери не используется. ***NO*** означает, что датчик двери открыт в нормальном состоянии. ***NC*** указывает, что датчик двери закрыт в нормальном состоянии.



6.4.4 Тип верификации

Устройство поддерживает различные типы верификации: ***пароль или идентификационная карта (PW / RF), только пароль (PW), только карта (RF), пароль плюс идентификационная карта (PW & RF)***.
Пользователь может выбрать тип верификации, который ему нужен. Пути: [***Меню***]> [***Система***]> [***Параметры контроля доступа***]> [***Тип верификации***].

Рекомендация: Когда устройство подключено к считывателю, если тип верификации считывателя PW & RF, тогда тип верификации устройства должен быть PW & RF; если считыватель без клавиатуры, то есть тип верификации считывателя - только карта, тогда тип верификации устройства должен быть PW / RF или RF.

6.5 Обновление

С помощью этой функции вы можете обновить прошивку устройства, используя файл обновления на USB-диске.

Если вам нужен файл обновления прошивки, пожалуйста, свяжитесь с нашей службой технической поддержки. Обычно обновление прошивки не рекомендуется.

7. Управление данными

С помощью меню [***Управление данными***] можно выполнять управление данными, хранящимися на устройстве, например, удалять все данные, очищать администратора, восстанавливать заводские настройки устройства.

Удалить все данные: удалить всю информацию о зарегистрированных сотрудниках, включая их идентификационные карты и записи паролей.

Очистить администратора: поменяйте всех администраторов на обычных пользователей.

Восстановить заводские настройки: восстановить все параметры устройства до заводских настроек.

Рекомендация: записи с информацией о сотрудниках не будут удалены при восстановлении до заводских настроек.

8. Настройка даты / времени

Дата и время устройства должны быть установлены точно, чтобы обеспечить точное время события учета рабочего времени.

1. Нажмите [***Меню***] в начальном интерфейсе, чтобы отобразить интерфейс главного меню.

2. Нажмите [Дата / Время] в интерфейсе главного меню, чтобы отобразить интерфейс настройки времени.

3. Введите желаемую дату и время, нажав на параметр.

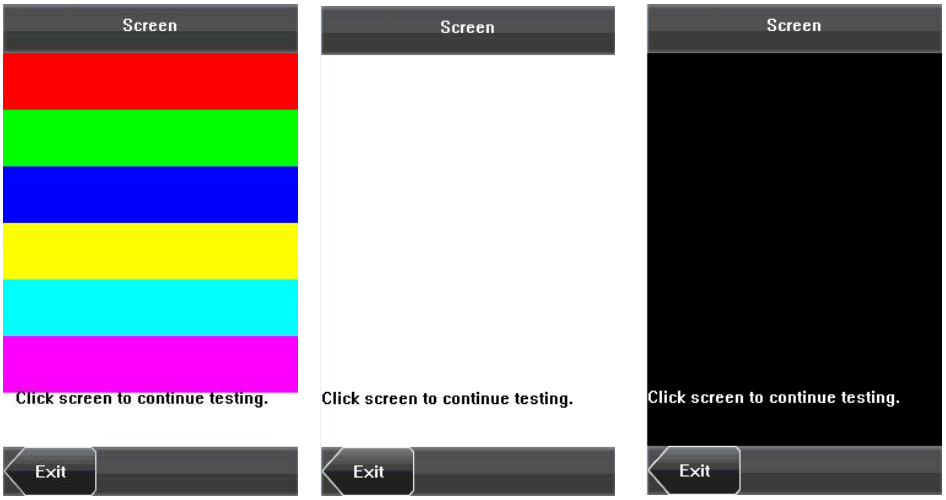
4. Нажмите [***Сохранить***], чтобы сохранить текущую информацию и вернуться к предыдущему интерфейсу. Нажмите [***Выход***], чтобы вернуться к предыдущему интерфейсу без сохранения текущей информации..

9. Автоматическое тестирование

Автоматическое тестирование позволяет системе автоматически проверять, являются ли функции различных модулей нормальными, включая тестирование экрана, голоса, времени и калибровки.

9.1 Тестирование экрана

Устройство автоматически проверяет эффект отображения цветного TFT-дисплея, отображая полноцветный, чисто белый и чисто черный цвета, и проверяет, правильно ли отображается экран. Вы можете продолжить тестированеи, коснувшись экрана или выйдя из него, нажав [***Выход***].



9.2 Тестированрие голоса

Устройство автоматически проверяет, являются ли голосовые файлы полными, и хорошее ли качество голоса, воспроизводя голосовые файлы, хранящиеся на устройстве. Вы можете продолжить тестирование, коснувшись экрана или выйдя из него, нажав ***[Выход***].

9.3 Время тестирования

Устройство проверяет, правильно ли работают его часы, проверяя секундомер часов. Коснитесь экрана, чтобы начать подсчет, и коснитесь его еще раз, чтобы остановить, чтобы проверить точность подсчета. Нажмите [***Выход***], чтобы выйти из тестирования.

9.4 Калибровка экрана

Вы можете выполнять все операции с меню, касаясь экрана одним пальцем или ручкой. Когда сенсорный экран менее чувствителен к касанию, вы можете выполнить калибровку экрана с помощью операций меню.
Операция калибровки экрана:

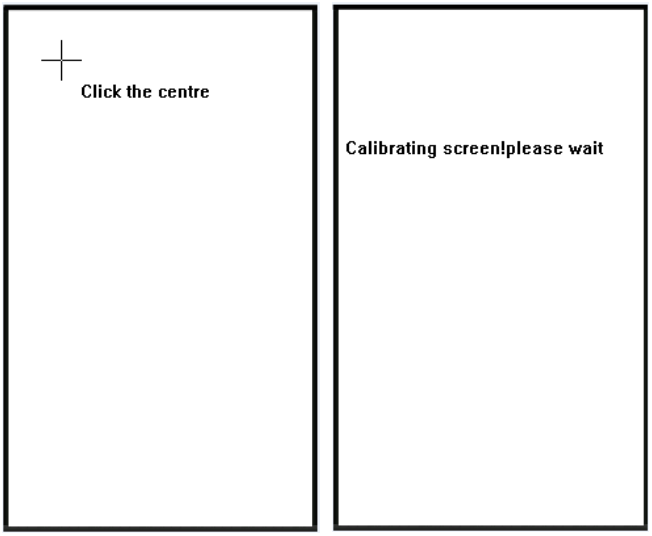
(1) Нажмите [***Меню***] в начальном интерфейсе, чтобы отобразить интерфейс главного меню.

(2) Нажмите [***Калибровка***] на интерфейсе [***Автоматическое тестирование***], чтобы отобразить интерфейс калибровки экрана.

(3) Коснитесь центра креста [**+**].

(4) Повторите шаг 3 после перемещения значка [**+**] в разные места на экране.

(5) Правильно коснитесь центра креста в пяти местах на экране. Когда на экране отображается сообщение «Экран калибровки, пожалуйста, подождите ...», калибровка завершается успешно, и система автоматически возвращается в главное меню. Если калибровка не удалась, перекалибровка системы начнется с шага 3.


Click the centre
Calibrating screen!please wait

10. Управление дисками USB

Через меню [***Загрузить / Выгрузить***] вы можете загрузить информацию о пользователях и данные о событиях учета рбочего времени, сохраненные на USB-диске, в соответствующее программное обеспечение.

Загрузка событий учета рабочего времени: загрузить данные о событиях учета рабочего времени с устройства в USB-диск.

Загрузка пользователя: загрузить всю пользовательскую информацию с устройства в USB-диск.

Выгрузить пользователя: выгрузить пользовательскую информацию, хранящуюся на USB-диске, в устройство.

11. Системная информация

Вы можете проверить состояние хранилища и информацию о версии устройства с помощью опции [***Системная информация***].

Записи: номера записей контроля доступа и зарегистрированных пользователей отображаются в интерфейсе [***Записи***]; общая емкость и занимаемая емкость отображаются графически.

Емкость карты: 30000

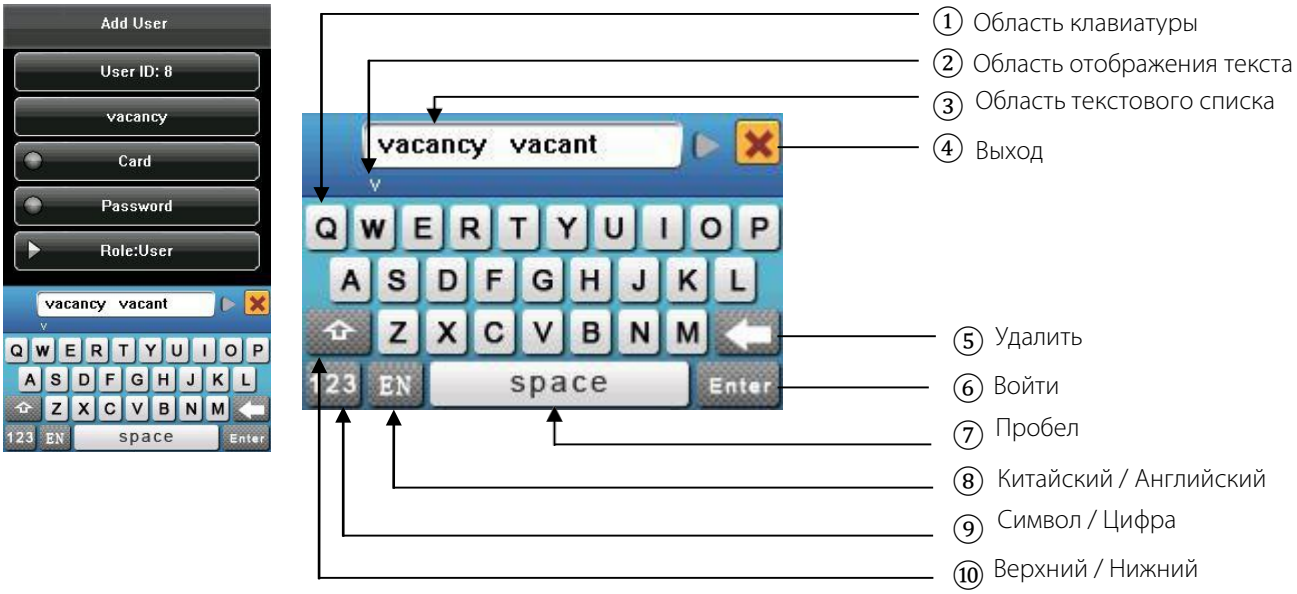
Объем записей: 100000

Устройство: имя устройства, серийный номер, MAC-адрес, поставщик, время изготовления и информация о версии прошивки отображаются в интерфейсе [***Устройство***].

12. Приложение

12.1 T9 Входной сигнал

Устройство поддерживает ввод английских букв, цифр и символов. Нажмите соответствующую кнопку, чтобы ввод текста. Например, нажмите [Имя], чтобы отобразить интерфейс ввода текста, как показано на рисунке:



Чтобы ввести имя, выполните следующие действия:

1. Нажмите [***Имя***] в интерфейсе [***Добавить пользователя***], как показано на рисунке ниже.

2. Введите буквенные символы, и в области отображения текста появится список символов, связанных с этой буквой.

3. Если нужный символ отображается в области отображения текста, нажмите этот символ или нажмите [***Войти***]. И этот символ в то же время отображается на кнопке [***Имя***]. Введите следующий символ, повторив шаг 2.

4. После завершения ввода имени нажмите [***X***], чтобы выйти из интерфейса клавиатуры и вернуться к предыдущему интерфейсу.

12.2 USB

1. USB-хост

Устройства могут использоваться в качестве USB-хоста для обмена данными с внешним U-диском. Скорость передачи данных является высокой, традиционное устройство поддерживает только способ Ethernet для передачи данных, когда в результате ограничения физического состояния количество данных велико, а передачи данных занимает довольно долгое время. Но передача данных через USB быстрее, чем в любом из предыдущих режимов передачи, может завершить загрузку данных на U-диск за короткий промежуток времени, а это значительно повышает эффективность.

2. USB-клиент

Устройство будет представлять собой съемные устройства хранения данных, данные на устройстве будут переданы на ПК через подключенный USB-кабель.
Когда устройство используется в качестве USB-клиента, в меню настроек связи устройства будут доступны параметры связи USB. За деталями обратитесь к разделу 5. Настройка связи.

12.3 Введение в Wiegand

Wiegand26 - это стандартный протокол контроля доступа, установленный подкомитетом контроля доступа, связанным с Ассоциацией индустрии безопасности (SIA). Это бесконтактный интерфейс считывателя карт IC и протокол вывода. Wiegand26 определяет интерфейс между устройством чтения карт и контроллером, используемым в области контроля доступа, безопасности и других смежных областях промышленности. Wiegand26 помогает стандартизировать работу дизайнеров кард-ридеров и производителей контроллеров. Продукты контроля доступа, произведенные нашей компанией, также разработаны согласно этому протоколу.

Цифровые сигналы

На рисунке ниже показана схема последовательности, на которой устройство считывания карт отправляет цифровые сигналы в битовом формате на контроллер доступа. На этой диаграмме последовательности Wiegand следует стандартному протоколу управления доступом SIA для 26-разрядного устройства считывания карт Wiegand (время одного импульса составляет от 20 до 100 мкс, а время скачка импульса - от 200 мс до 20 мс). Данные1 и Данные0 являются сигналами высокого уровня (больше, чем Vol), пока устройство чтения карт не подготовится к отправке потока данных. Асинхронный низкоуровневый импульс (меньше, чем Vol), генерируемый устройством считывания карт, отправляется на панель управления доступом (пилообразная волна, как показано на рисунке ниже) через данные 1 или данные 0. Импульсы Data1 и Data0 не будут перекрываться и генерироваться синхронно. В приведенной ниже таблице указаны максимальная и минимальная длительность импульса (последовательный импульс) и время перехода импульса (время между импульсами), допустимые для устройства контроля доступа к венам пальцев серии F.

Рисунок: Диаграмма последовательности

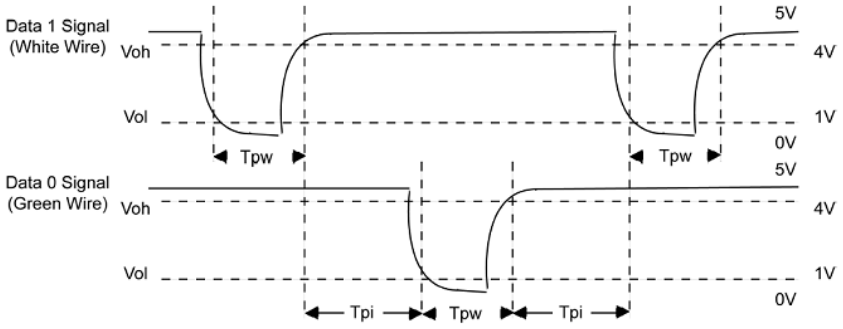


Таблица: Время пульса

Symbol	Definition	Typical Value of Reader
Tpw	Pulse Width	100 μs
Tpi	Pulse Interval	1 ms

12.3.1 Описание 26-битного выхода Wiegand

Система имеет встроенный 26-битный формат Wiegand.

Состав формата 26-битного формата Wiegand содержит 2 бита четности и 24 бита для выходного содержимого («Идентификатор пользователя» или «Номер карты»). 24-битный двоичный код представляет до 16777216 (0 - 16777215) различных значений.

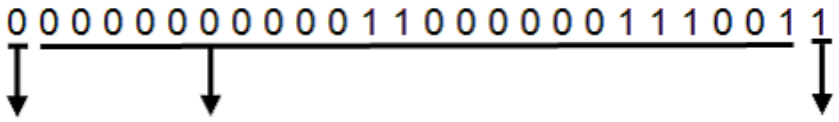
1	2	25	26
Бит четности	Идентификатор пользователя / Номер карты		Бит нечетности

Определение полей:

Поле	Описание
Бит четности	Оценивается от бита 2 до бита 13. ***Бит четности*** равен 0, если символ имеет четное число 1 бит; в противном случае бит четности равен 1.
Идентификатор пользователя / Номер карты (бит 2-бит 25)	Идентификатор пользователя / номер карты (код карты, 0-16777215). Бит 2 является наиболее значимым битом (MSB).
Бит нечетности	Оценивается от бита 14 до бита 25. ***Бит нечетности*** равен 1, если символ имеет четное число 1 бит; в противном случае бит нечетности равен 0.

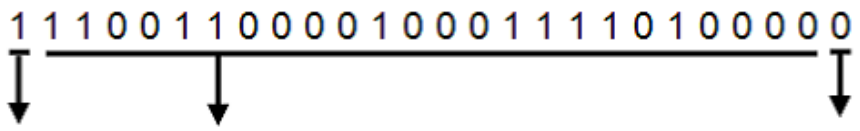
Например, для пользователя с идентификатором пользователя 12345 номер зарегистрированной карты равен 0013378512, а для идентификатора с ошибкой установлено значение 1.

1. Когда для выхода задано «ID пользователя», вывод Wiegand при успешной проверке выглядит следующим образом:



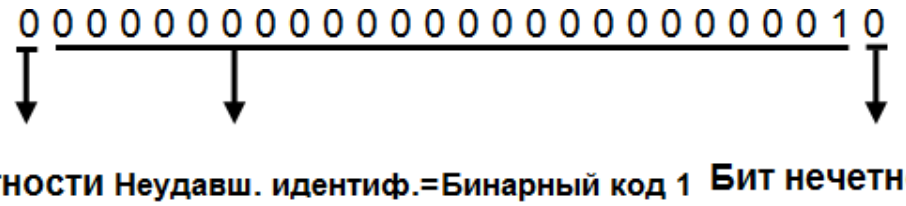
Бит четности Идентиф. польз. = Бинарный код 12345 Бит нечетности

2. Когда для выхода установлено значение «Номер карты», вывод Wiegand при успешной верификации выглядит следующим образом:



Бит четности Идентиф. польз. = Бинарный код 0013378512 Бит нечетности

3. Выход Wiegand выглядит следующим образом при сбое верификации:



Рекомендация: Если выходное содержимое превышает область, разрешенную для формата Wiegand, последние несколько бит будут приняты и 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, а первые 6 бит «110 100» автоматически отбрасываются.

12.3.2 Описание 34-битного выхода Wiegand

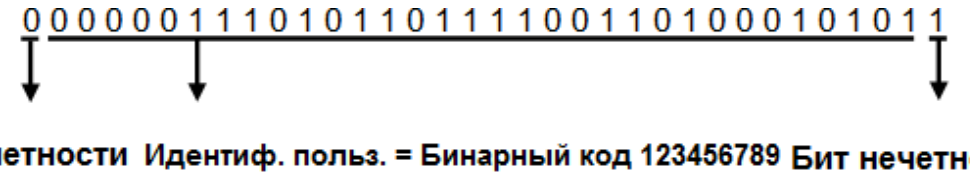
Система имеет встроенный 34-битный формат Wiegand. Нажмите [***Формат Wiegand***] и выберите «Стандартный 34-битный Wiegand». Состав формата 34-битного Wiegand состоит из 2 бит четности и 32 битов для выходного содержимого («Идентификатор пользователя» или «Номер карты»). Бинарный код из 32 битов представляет до 4 294 967 296 (0-4 294 967 295) разных значений.

1	2 33	34
Бит четности	Идентификатор пользователя / Номер карты	Бит нечетности

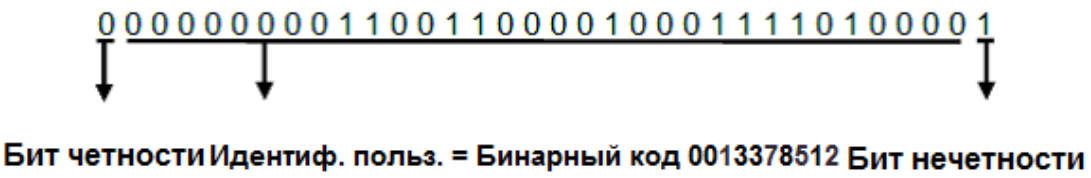
Таблица 2: Определение полей

Поле	Описание
Бит четности	Оценивается от бита 2 до бита 17. ***Бит четности*** равен 0, если символ имеет четное число 1 бит; в противном случае бит четности равен 1.
Идентификатор пользователя / Номер карты (бит 2-бит 25)	Идентификатор пользователя / номер карты (код карты, 0-4294967295). Бит 2 является наиболее значимым битом (MSB).
Бит нечетности	Оценивается от бита 18 до бита 33. ***Бит нечетности*** равен 1, если символ имеет четное число 1 бит; в противном случае бит нечетности равен 0.

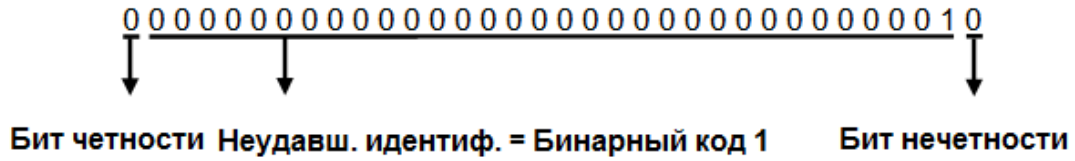
Например: для пользователя с идентификатором пользователя 123456789 зарегистрированный номер карты равен 0013378512, а неудавшийся идентификатор устанавливается равным 1.



2.Если для выхода установлено значение «Номер карты», следующим после успешной верификации выход Wiegand будет следующим образом:



3.Выход Wiegand выглядит следующим образом при сбое верификации:



12.3.3 Описание специального формата Wiegand

Чтобы настроить формат Wiegand, выполните следующие действия:

(1) Выберите [***Определить формат пользователя***], и клавиша [***Определить***] будет активирована.

(2) Нажмите [***Определить***], чтобы отобразить интерфейс [***Определить формат пользователя***], как показано на следующем рисунке:

(3) Нажмите поле ввода ниже «Формат карты», чтобы отобразить следующий интерфейс:

Символы, используемые для определения битов формата карты и их значения:

c: указывает номер карты, то есть содержимое выхода, для него можно установить идентификатор пользователя / номер карты с помощью операций меню.
f: указывает код объекта, который по умолчанию равен 0. Это не настраивается. Чтобы изменить его свяжитесь с поставщиком оборудования.
m: указывает код производителя, который по умолчанию равен 0. Это не настраивается. Чтобы изменить его свяжитесь с поставщиком оборудования.
p: указывает положение четности.
s: Указывает код сайта, который по умолчанию можно установить от 0 до 255.
(4) Щелкните поле ввода ниже «Формат четности», чтобы отобразить следующий интерфейс:

Символы, используемые для определения битов формата четности и их значения:

o: обозначает нечетную проверку, то есть в последовательности битов есть нечетное число единиц (включая один бит четности). Например, для 1000110 (0) бит четности равен 0, и уже есть три единицы. После того, как 0 добавляется к 1000110 остается нечетное число единиц.
e: обозначает четную проверку, то есть четное число единиц в битовой последовательности (включая один бит четности). Например, для 1000110 (1) бит четности равен 1, и уже есть три единицы. После того, как 1 добавляется к 1000110 появляется четное число единиц.

b: Обозначает нечетную и четную проверку.

Обозначает нечетную и четную проверку.

Например, определения нескольких универсальных форматов Wiegand.

Wiegand34

Биты формата карты:

pccccccccccccccccccccccccccccccp

Биты формата четности:

eeeeeeeeeeeeeeeeoooooooooooooooo

Рекомендация: Wiegand34 состоит из 34 бит. Первый бит - это четный бит четности от битов 2 до 17; 34-й бит - это нечетный бит четности от битов 18 до 33; вторые-девятые биты - код сайта; с 10-го по 25-й биты - номер карты.

Wiegand37a

Биты формата карты: pmmmmsssssssssssscccccccccccccccccp

Биты формата четности: oeobeobeobeobeobeobeobeobeobeobeoe

Рекомендация: Wiegand37a состоит из 37 бит. Первый бит является нечетным битом четности битов 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 18, 19, 21, 22, 24, 25, 27, 28, 30, 31, 33, 34 и 36; 37-й бит является нечетным битом четности битов 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, 28, 29, 31, 32, 34 и 35; биты 4, 7, 10, 13, 16, 19, 22, 25, 28, 31 и 34 участвуют как в проверке четности, так и в четности. Биты со 2 по 5 являются кодом производителя; биты с 6 по 17 - это код сайта; биты с 18 по 36 являются номером карты.

Wiegand37

Биты формата карты:

pmmmfffffffffssssscccccccccccccccp

Биты формата четности:

eeeeeeeeeeeeeeeeeoooooooooooooooooo

Рекомендация: Wiegand37 состоит из 37 бит. Первый бит - это четный бит четности от битов 2 до 18; 34-й бит является нечетным битом четности битов с 19 по 36; биты со второго по четвертый являются кодом производителя; с 5-го по 14-й биты являются упрощенным кодом; 15-20 биты - это код сайта; 21-й по 36-й биты - номер карты.

Wiegand 50

Биты формата карты:

psssssssssssssssccccccccccccccccccccccccccccccp

Биты формата четности:

eeeeeeeeeeeeeeeeeeeeeeeeooooooooooooooooooooooooo

Рекомендация: Wiegand50 состоит из 50 бит. Первый бит - это четный бит четности от битов 2 до 25; 50-й бит - это нечетный бит четности от битов 26 до 49; вторые-шестнадцатые биты - это код сайта; с 17-го по 49-й биты - номер карты.

12.4 Контроль прохода в двух направлениях

[**Обзор**]

Иногда некоторые лица, не имеющие доступ, следуют непосредственно за лицом, имеющим доступ, через барьер турникета, что вызывает проблемы с безопасностью. Чтобы предотвратить такие риски, эта функция включена. Входная запись должна соответствовать выходной записи, иначе барьер не откроется.

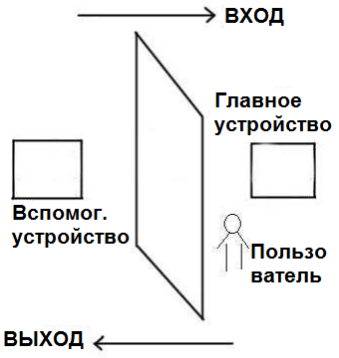
Для этой функции нужны два устройства или устройство со считывателем для совместной работы.

Контроль прохода в двух направлениях между двумя устройствами:

Одно из них установлено внутри двери (в дальнейшем Главное устройство), другое - снаружи двери (далее – Вспомогательное устройство). Сигнал связи Wiegand принимается между двумя устройствами.

Контроль прохода в двух направлениях между устройством и считывателем:

Устройство установлено внутри двери (далее - Главное устройство), считыватель установлен снаружи двери (далее - Вспомогательное устройство). Сигнал связи Wiegand принимается между устройством и считывателем.



[***Рабочий принцип***]

У главного устройства есть функция Вход Wiegand, а у вспомогательного устройства есть функция Выход Wiegand. Подключите Выход Wiegand от вспомогательного устройства к Вход Wiegand главного устройства. Выход Wiegand от вспомогательного устройства не должен иметь идентификатор устройства. Номер, отправленный на главное устройство от вспомогательного устройства, должен находится в главном устройстве.

[***Функция***]

Оцените, является ли это контролем прохода в двух направлениях в соответствии с последней записью пользователя. Записим входа и выхода должны совпадать. Это устройство поддерживает контроль прохода в двух направлениях на вход, выход или выход-вход.

Если в главном устройстве установлена функция «контроль прохода в двух направлениях на выход». Если пользователь хочет войти и выйти нормально, его последняя запись должна быть «вход», иначе он не сможет выйти. Любая попытка «выхода» будет отклонена функцией «контроль прохода в двух направлениях». Например, последняя запись пользователя «вход», его вторая запись может быть «выход» или «вход». Его третья запись основана на его второй записи. Запись выхода и запись входа должны совпадать. (Примечание: если клиент не имеет ранней записи, тогда он

сможет войти, но не сможет выйти).

Если в главном устройстве установлена функция «контроль прохода в двух направлениях на вход». Если пользователь хочет войти и выйти нормально, его последняя запись должна быть «выход», иначе он не сможет выйти. Любая запись на выход будет отклонена системой контроля прохода в двух направлениях. (Примечание: если у клиента нет прежней записи, он сможет выйти, но не сможет войти).
Когда в главном устройстве установлена функция «контроль прохода в двух направлениях на выход-вход», если пользователь хочет войти и выйти нормально, если его недавняя запись «выход» и «вход», тогда его следующая запись должна быть «вход» и «выход».

[***Работа***]

1. Выберите модель

Главное устройство: устройство с функцией Вход Wiegand, кроме считывателя F10.
Вспомогательное устройство: устройство с функцией Выход Wiegand.

2. Настройка меню

Контроль прохода в двух направлениях

Есть четыре варианта: контроль прохода в двух направлениях на вход / выход, контроль прохода в двух направлениях на выход, контроль прохода в двух направлениях на вход и отсутсвует.

Контроль прохода в двух направлениях на выход: дверь может быть открыта, только если последняя запись пользователя была записью на вход.

Контроль прохода в двух направлениях на вход: дверь может быть открыта, только если последняя запись пользователя была записью на выход.

Состояние устройства: существует три параметра: вход, выход и отсутствует.

Контроль входа: когда он установлен, записи верификации на устройстве являются записями входа.

Контроль выхода: когда он установлен, записи верификации на устройстве являются записями выхода.

Отсутствует: когда он установлен, функция контроля прохода в двух направлениях устройства отключена.

3. Измените формат выхода Wiegand устройства.

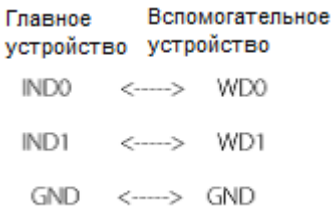
Когда два устройства обмениваются данными, принимаются только сигналы ***Wiegand*** без идентификатора устройства. Войдите в меню устройства> параметр связи> параметр Wiegand или введите программное обеспечение> базовые настройки> управление устройством> Wiegand, чтобы изменить «определенный формат» как «wiegand26 без идентификатора устройства».

4. Зарегистрировать пользователя

Пользователь должен одновременно находиться на главном и вспомогательном устройствах, а ПИН-код пользователя должен совпадать. Следовательно, необходимо зарегистрировать пользователя на главном устройстве и на вспомогательном устройстве одновременно.

5. Инструкция по подключению

Связь Wiegand принята для главного и на вспомогательного устройств. Обратитесь к следующему для подключения:



: Indicates that this toxic or hazardous substance contained in all of the h

×: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this

Tip: 80% of the parts in this product are manufactured with non-hazardous environment-friendly materials. The hazardous substances or elements contained cannot be replaced with environment-friendly materials at present due to technical or economical constraints.