



HIKVISION

Терминал контроля доступа

Краткое руководство пользователя
V1.0.0

UD01883B-B

Краткое руководство пользователя

©2016 Hangzhou Hikvision Digital Technology Co., Ltd.

Руководство содержит инструкции по использованию продукта. Программное обеспечение, используемое в продукте, регулируется лицензионным соглашением пользователя, охватывающим этот продукт.

О руководстве

Вся информация, включая текст, изображения и графики является интеллектуальной собственностью Hikvision Digital Technology Co., Ltd. или ее дочерних компаний (далее Hikvision). Данное руководство пользователя (далее «Руководство») не подлежит воспроизведению, изменению, переводу или распространению, частично или целиком, без предварительного разрешения Hikvision.

Торговая марка

HIKVISION и другие торговые марки Hikvision и логотипы являются интеллектуальной собственностью Hikvision в различных юрисдикциях. Другие торговые марки и логотипы, содержащиеся в руководстве, являются собственностью их владельцев.

Правовая информация

ДО МАКСИМАЛЬНО ДОПУСТИМОЙ СТЕПЕНИ, РАЗРЕШЕННОЙ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПРОДУКТ, АППАРАТУРА, ПРОГРАММНОЕ И АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ», СО ВСЕМИ ОШИБКАМИ И НЕТОЧНОСТЯМИ, HIKVISION НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, КАСАТЕЛЬНО УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА, СООТВЕТСТВИЯ УКАЗАННЫМ ЦЕЛЯМ И ОТСУТСТВИЯ НАРУШЕНИЙ СО СТОРОНЫ ТРЕТЬИХ ЛИЦ. НИ HIKVISION, НИ ЕГО ДИРЕКТОРА, НИ СОТРУДНИКИ ИЛИ ПРЕДСТАВИТЕЛИ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ПЕРЕД ПОТРЕБИТЕЛЕМ ЗА КАКОЙ-ЛИБО СЛУЧАЙНЫЙ ИЛИ КОСВЕННЫЙ УЩЕРБ, ВКЛЮЧАЯ УБЫТКИ ИЗ-ЗА ПОТЕРИ ПРИБЫЛИ, ПЕРЕРЫВА В ДЕЯТЕЛЬНОСТИ ИЛИ ПОТЕРИ ДАННЫХ ИЛИ ДОКУМЕНТАЦИИ, В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ HIKVISION БЫЛО ИЗВЕСТНО О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.

ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА С ДОСТУПОМ В ИНТЕРНЕТ НЕСЕТ ПОЛЬЗОВАТЕЛЬ; НАША КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА НЕНОРМАЛЬНУЮ РАБОТУ ОБОРУДОВАНИЯ, ПОТЕРЮ ИНФОРМАЦИИ И ДРУГИЕ ПОСЛЕДСТВИЯ, ВЫЗВАННЫЕ КИБЕР АТАКАМИ, ВИРУСАМИ ИЛИ ДРУГИМИ ИНТЕРНЕТ РИСКАМИ; ОДНАКО, НАША КОМПАНИЯ ОБЕСПЕЧИВАЕТ СВОЕВРЕМЕННУЮ ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ, ЕСЛИ ЭТО НЕОБХОДИМО.

ЗАКОНЫ, РЕГУЛИРУЮЩИЕ ВИДЕОНАБЛЮДЕНИЕ, ВАРЬИРУЮТСЯ В ЗАВИСИМОСТИ ОТ СТРАНЫ. ПОЖАЛУЙСТА, ПРОВЕРЬТЕ ВСЕ СООТВЕТСТВУЮЩИЕ ЗАКОНЫ ВАШЕЙ СТРАНЫ ПЕРЕД ИСПОЛЬЗОВАНИЕМ ОБОРУДОВАНИЯ. НАША КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ИСПОЛЬЗОВАНИЕ ОБОРУДОВАНИЯ В НЕЗАКОННЫХ ЦЕЛЯХ.

В СЛУЧАЕ КОНФИЛИКТОВ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ И ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПОСЛЕДНЕЕ ПРЕВАЛИРУЕТ.

Поддержка

Если у вас есть какие-либо вопросы, пожалуйста, не стесняйтесь обращаться к местному дилеру.

Профилактические и предостерегающие советы

Перед подключением и эксплуатацией устройства, пожалуйста, обратите внимание на следующие советы:

- Убедитесь, что устройство установлено в хорошо проветриваемой, защищённой от пыли окружающей среде.
- Держите все жидкости подальше от устройства.
- Убедитесь, что условия окружающей среды соответствуют заводским спецификациям.
- Убедитесь, что устройство правильно закреплено на стойке или полке. Сильные удары или толчки устройства в результате его падения могут привести к повреждению чувствительной электроники, находящейся внутри.
- Используйте устройство в сочетании с ИБП, если это возможно.
- Выключайте питание устройства перед подключением и отключением аксессуаров и периферийных устройств.
- Используйте рекомендованные производителем HDD для данного устройства.
- Неправильное использование или замена батареи может привести к опасности взрыва. Производите замену только на такие же батареи или батареи аналогичного типа. Утилизируйте использованные батареи в соответствии с инструкциями, предоставленными изготовителем батареи.

Инструкции по технике безопасности

Обозначение	Описание
 Предупреждение	Следуйте данным правилам для предотвращения серьезных травм и смертельных случаев.
 Примечание	Следуйте мерам предосторожности, чтобы предотвратить возможные повреждения или материальный ущерб.
 Совет	Дополнительная информация.



Предупреждения:

- Пожалуйста, используйте заводской адаптер питания, который соответствует стандарту безопасности сверхнизкого напряжения (SELV).
- Пожалуйста, убедитесь, что питание отключено перед подключением, установкой или демонтажем устройства.

- Чтобы снизить риск возгорания или поражения электрическим током, не подвергайте продукт воздействию дождя или влаги.
- Установка должна выполняться квалифицированным специалистом и должна соответствовать всем региональным стандартам.
- Если продукт не работает должным образом, обратитесь к дилеру или в ближайший сервисный центр. Не пытайтесь самостоятельно разобрать устройство. (Мы не несем ответственность за проблемы, вызванные несанкционированным ремонтом или техническим обслуживанием.)



Примечания:

- Не бросайте устройство и не подвергайте его ударам, воздействию сильных электромагнитных излучений. Избегайте установки на поверхности, подверженные вибрациям и встряскам.
- Не устанавливайте устройство в условиях экстремальных температур (выше 65°C или ниже -20°C)
- Обеспечьте хорошую вентиляцию.
- Не используйте во влажной среде.
- Не используйте во взрывоопасной среде.
- Держите устройство в чистоте и сухости.
- Избегайте оголенных электрических проводов.

Содержание

1 Обзор	5
1.1 Описание	5
1.2 Основные особенности	5
2 Внешний вид	6
2.1 Внешний вид модели DS-K1T500SF	6
2.2 Внешний вид модели DS-K1T500S	7
2.2.1 Описание компонентов	7
2.3 Разъемы терминала контроля доступа	8
2.4 Описание DIP-переключателя	8
3 Установка	10
4 Подключение терминала	11
4.1 Описание терминала	11
5 Описание подключения	13
5.1 Обзор подключения внешних устройств	13
5.2 Подключение внешнего считывателя карт	13
5.2.1 Подключение внешнего RS-485 считывателя карт	13
5.3 Подключение считывателя карт	14
5.3.1 Подключение Wiegand	14
5.3.2 Подключение RS-485 выхода	15
6 Активация терминала контроля доступа	16
6.1 Активация при помощи SADP	16
6.2 Активация через клиентское ПО	17
Приложение: Советы по сканированию отпечатков пальцев	19

1 Обзор

1.1 Описание

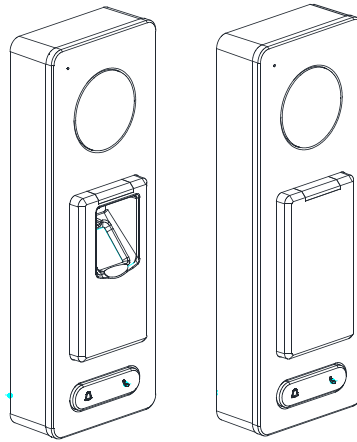


Рисунок 1-1 Серии DS-K1T500S/SF терминалов контроля доступа – Передняя панель

DS-K1T500S/SF – это серии видео терминалов контроля доступа с несколькими передовыми технологиями, включая распознавание отпечатков пальцев, распознавание лиц, Wi-Fi, распознавание смарт-карт и HD камеру (2 МП опционально). Оснащен оптическим модулем распознавания отпечатков пальцев (поддерживает режимы 1:1 и 1:N), поддерживает оффлайн операции.

1.2 Основные особенности

- Настройка мелодии звонка
- Автономная настройка терминала
- Проводные режимы передачи (TCP/TP) и Wi-Fi
- Функции обнаружения лиц и захвата изображений, осуществляемые встроенной камерой (2Мп опционально)
- Поддержка RS-485 соединения для подключения внешних считывателей карт
- Поддержка работы в качестве считывателя карт и подключение через интерфейсы Wiegand и RS-485 к контроллеру
- Хранение в памяти до 50000 карт, 200000 событий и 3000 отпечатков пальцев (поддерживается только DS-K1T500SF)
- Встроенный модуль считывания отпечатков пальцев, поддерживающий режимы 1:N (отпечаток пальца, карта + отпечаток пальца) и 1:1 (карта + отпечаток пальца)
- Поддержка нескольких режимов аутентификации: карта, отпечаток пальца, карта + отпечаток пальца, карта + пароль, отпечаток пальца + пароль, карта + отпечаток пальца + пароль и т.д. (аутентификация по отпечатку пальца поддерживается только DS-K1T500SF)
- Поддержка чтения Mifare карт/серийного номера CPU
- Тревога тампера, тревога удержания двери, тревога повторных проводок карты и тревога карты по принуждению и т.п.
- Поддержка подключения модуля безопасности
- Уровень защиты: IP65
- Данные могут быть сохранены после отключения питания

2 Внешний вид

2.1 Внешний вид модели DS-K1T500SF

Более подробную информацию о серии DS-K1T500SF смотрите в данном разделе.

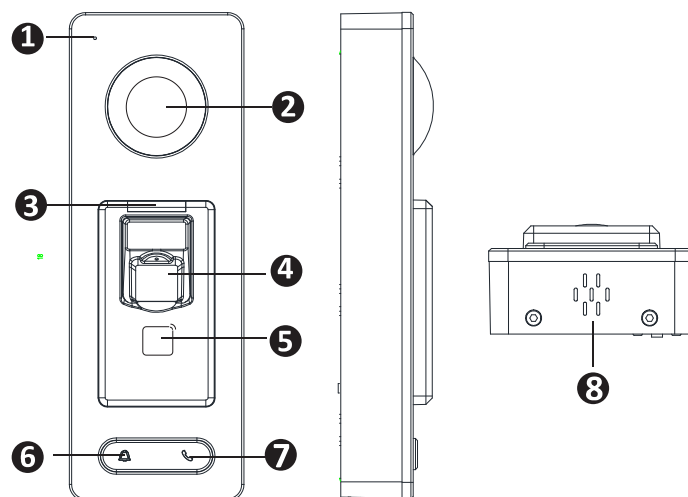


Рисунок 2-1 Внешний вид модели серии DS-K1T500SF

Таблица 2-1 Описание модели серии DS-K1T500SF

№	Описание
1	Микрофон
2	Камера
3	Светодиодный индикатор
4	Сканер отпечатков пальцев
5	Область считывания карт
6	Кнопка дверного звонка
7	Кнопка голосовой связи
8	Динамик

2.2 Внешний вид модели DS-K1T500S

Более подробную информацию о серии DS-K1T500S смотрите в данном разделе

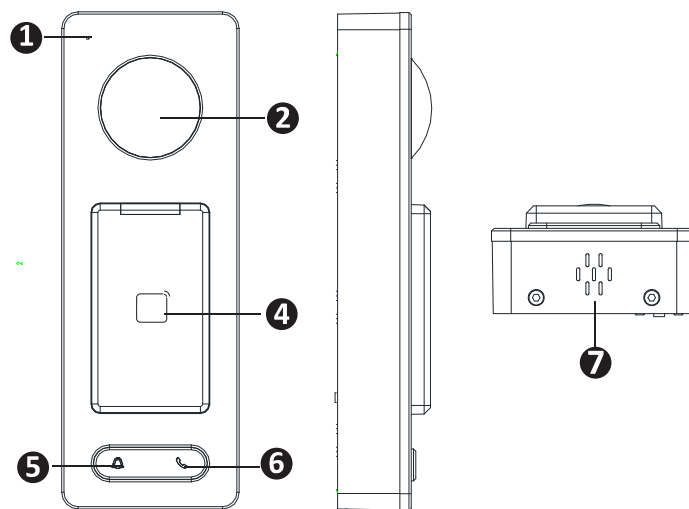


Рисунок 2-2 Внешний вид модели серии DS-K1T500S

2.2.1 Описание компонентов

Таблица 2-2 Описание компонентов модели серии DS-K1T500S

№	Описание
1	Микрофон
2	Камера
3	Светодиодный индикатор
4	Область считывания карт
5	Кнопка дверного звонка
6	Кнопка голосовой связи
7	Динамик



Совет

В интерфейсе событий в программном обеспечении клиента iVMS-4200 выберите тревожный выход звонка по событию. Вы можете подключить звонок к тревожному выходу. За более подробной информацией обратитесь к руководству пользователя клиентского ПО iVMS- 4200.

2.3 Разъемы терминала контроля доступа

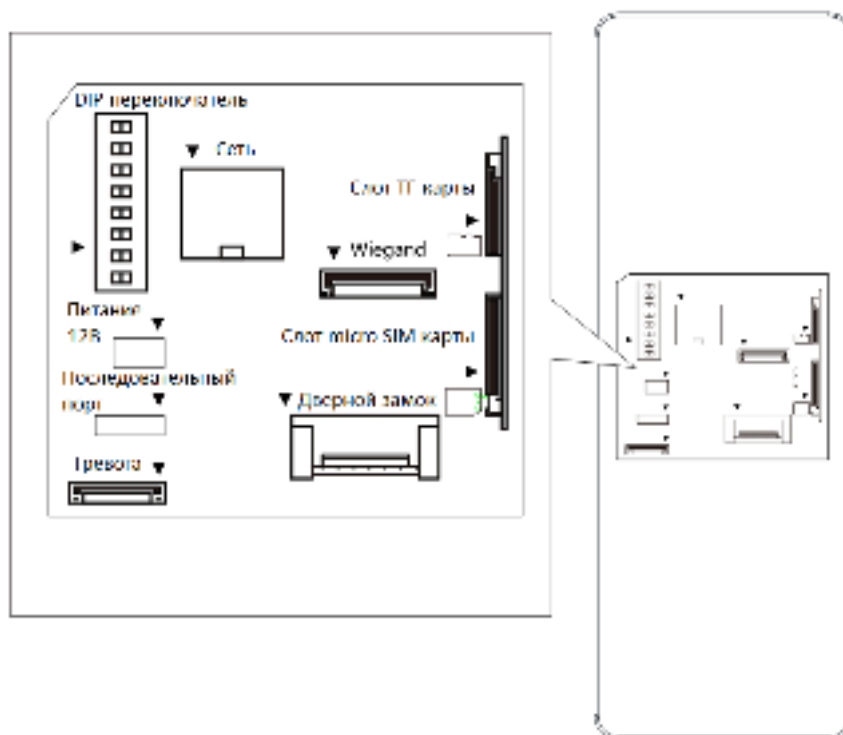


Рисунок 2-3 Описание разъемов терминала контроля доступа

2.4 Описание DIP-переключателя

Модуль DIP-переключателя показан ниже. Номера DIP-переключателей слева направо: 1 - 8.

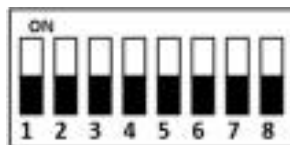


Рисунок 2-4 Модуль DIP-переключателя

Таблица 2-3 Описание DIP-переключателя

Иконка	Описание
	Представляет 1 в двоичном виде
	Представляет 0 в двоичном виде

Например, двоичное значение следующего состояния: 0000 1100.



Рисунок 2-5 Модуль DIP-переключателя

Таблица 2-4 Описание DIP-переключателя

№	Описание	Состояние переключателя	DIP-
1 ~ 4	Адрес RS-485	1: Модуль безопасности 0: Считыватель карт	
5	Направление RS-485 в режиме терминала	1: Восходящий; 0: Нисходящий	
6	Режим работы	1: Считыватель карт; 0: Терминал.	
7	Wiegand протокол (доступен, когда № 6 равен 1)	1: Протокол Wiegand 26-бит; 0: Протокол Wiegand 34-бита.	
8	Согласованное сопротивление (доступно для RS-485 протокола)	1: Включен; 0: Выключен.	

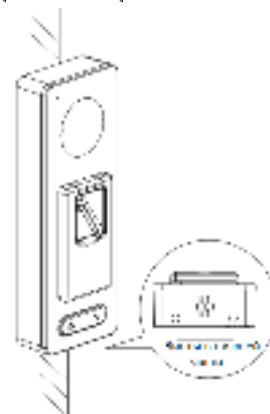
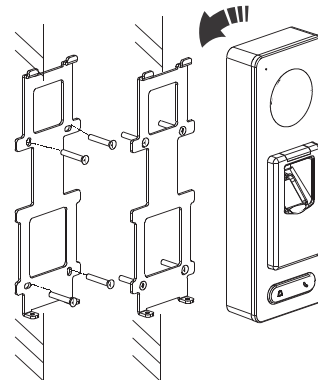
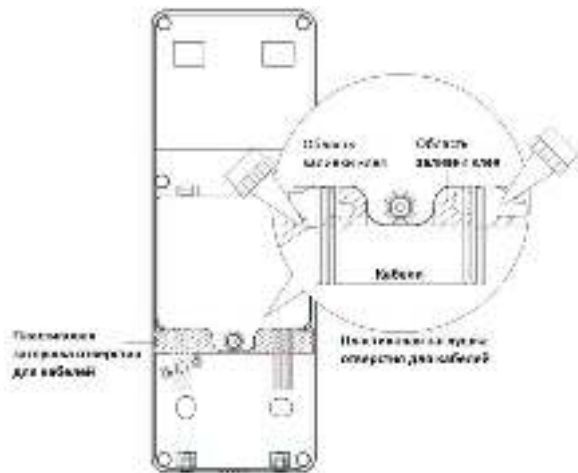
3 Установка

Перед началом:

- Убедитесь, что устройство в упаковке находится в должном состоянии, и все детали на месте.
- Убедитесь, что стена достаточно прочная, чтобы выдерживать вес в три раза больше веса терминала.
- Установите DIP-адрес перед установкой.

Шаги:

1. Подключите кабели к разъему на задней панели устройства. Проложите кабели через отверстие для кабелей монтажной пластины. Кабельные отверстия расположены с правой стороны, с левой стороны и с нижней стороны задней крышки. Если выбрано правое/левое отверстие для кабеля, снимите пластиковую заглушку с отверстия для кабеля.
2. После прокладки кабелей залейте клей (рекомендуемая модель: Devcon 24105) в область заливки клея.
3. Закрепите монтажную пластину на стене с помощью 4 прилагаемых винтов.
4. Подключите соответствующие кабели.
5. Вставьте терминал в монтажную пластину нажатием снизу вверх.
6. Затяните винты в нижней части терминала, чтобы зафиксировать терминал на монтажной пластине и завершить установку.



4 Подключение терминала

4.1 Описание терминала

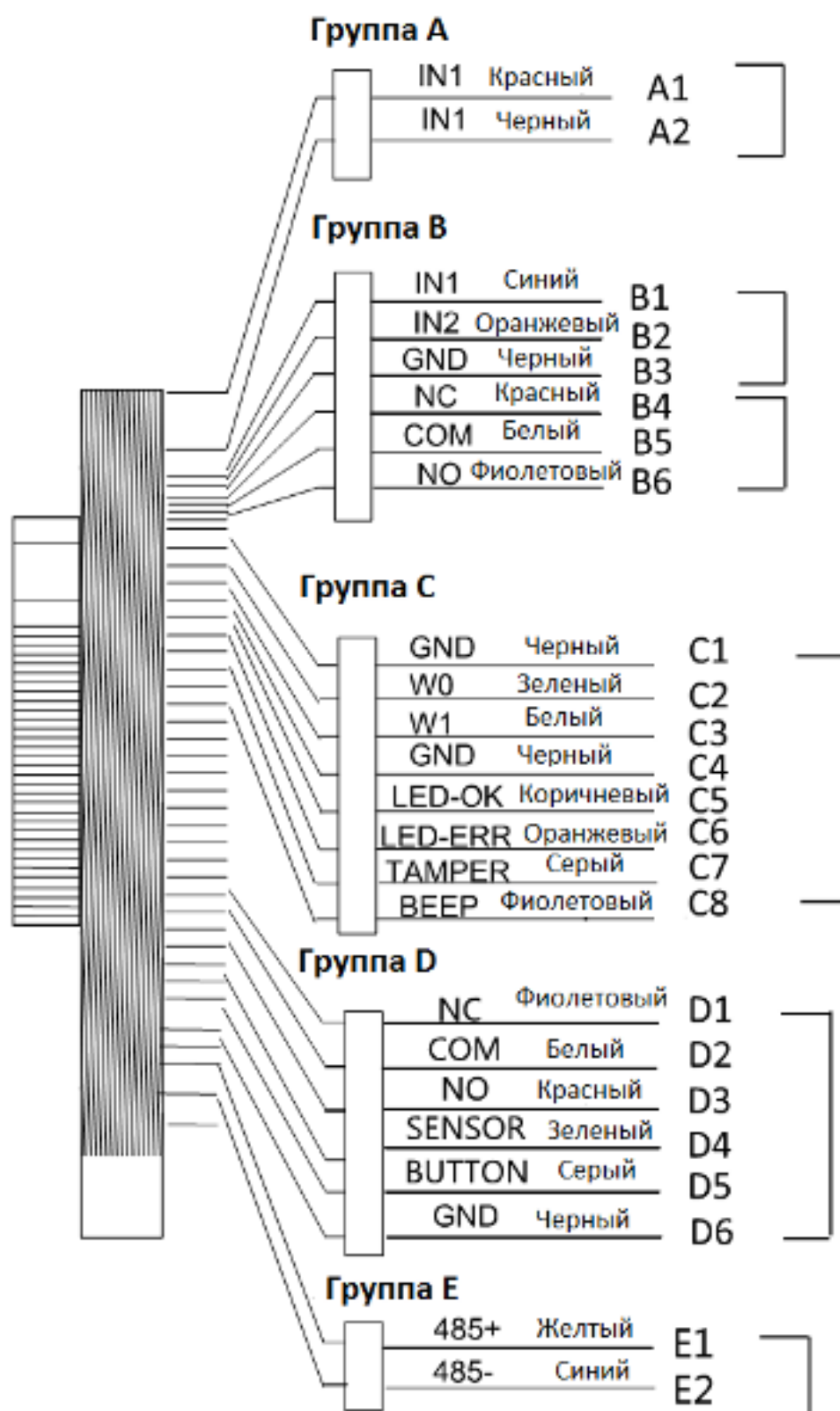


Рисунок 4-1 Схема клемм терминала контроля доступа

Таблица 4-1 Описание клемм

Группа	№	Функция	Цвет	Название клеммы	Описание
Группа А	A1	Вход питания	Красный	+12V	Питание 12В DC
	A2		Черный	GND	Общий
Группа В	B1	Тревожный вход	Желтый	IN1	Тревожный вход 1
	B2		Оранжевый	IN2	Тревожный вход 2
	B3		Черный	GND	Общий
	B4	Тревожный выход	Красный	NC	Подключение тревожного выхода
	B5		Белый	COM	
	B6		Фиолетовый	NO	
Группа С	C1	Wiegand	Черный	GND	Общий
	C2		Зеленый	W0	Подключение Wiegand 0
	C3		Белый	W1	Подключение Wiegand 1
	C4		Черный	GND	Общий
	C5		Коричневый	LED-OK	Успешная аутентификация Wiegand
	C6		Оранжевый	LED-ERR	Ошибка аутентификации Wiegand
	C7		Серый	TAMPER	Подключение тревоги тамперинга
	C7		Фиолетовый	BEEP	Подключение зуммера
Группа D	D1	Замок	Желтый	NC	Подключение замка
	D2		Белый	COM	
	D3		Красный	NO	
	D4		Зеленый	SENSOR	Сигнальный вход контакта двери
	D5		Серый	BUTTON	Подключение кнопки выхода
	D6		Черный	GND	Общий
Группа Е	E1	RS-485	Желтый	485 +	Подключение RS-485
	E2		Синий	485 -	

5 Описание подключения

5.1 Обзор подключения внешних устройств

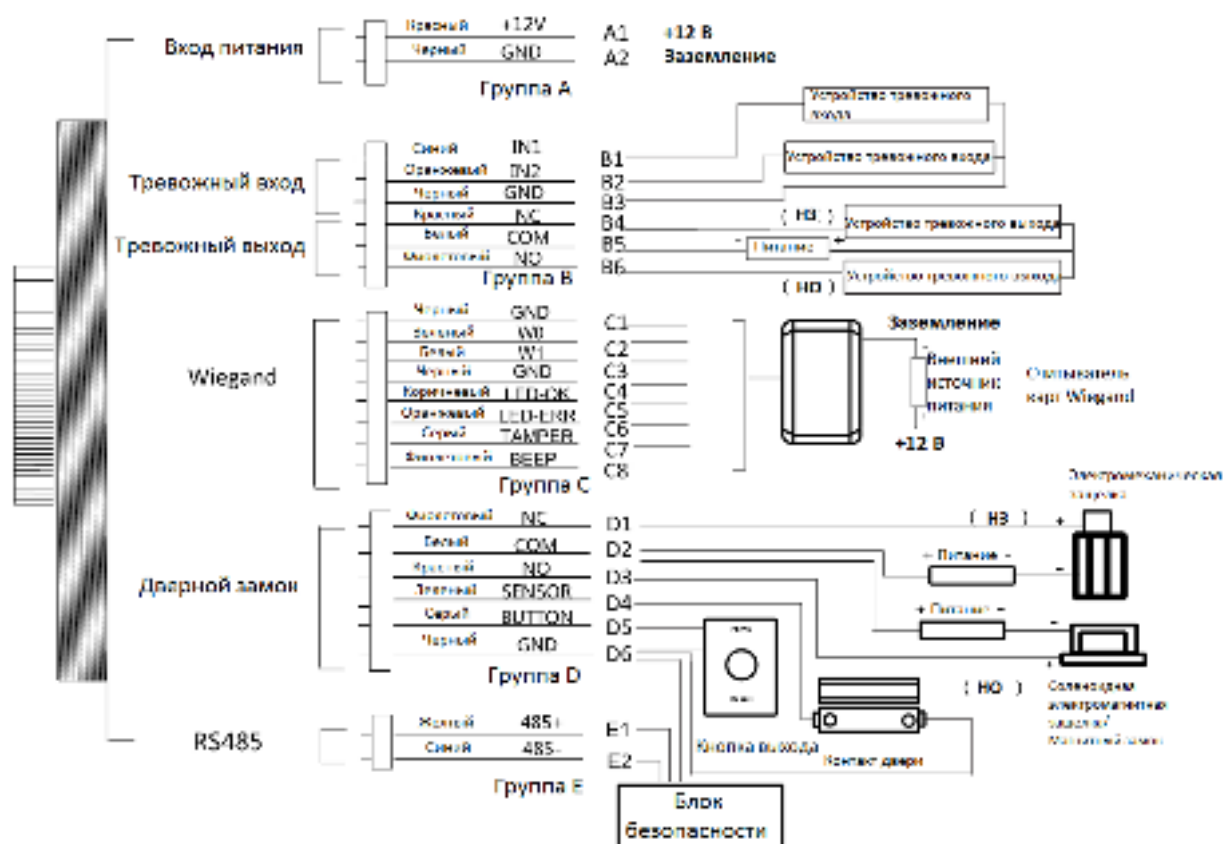


Рисунок 5-1 Схема подключения внешних устройств

5.2 Подключение внешнего считывателя карт

5.2.1 Подключение внешнего RS-485 считывателя карт

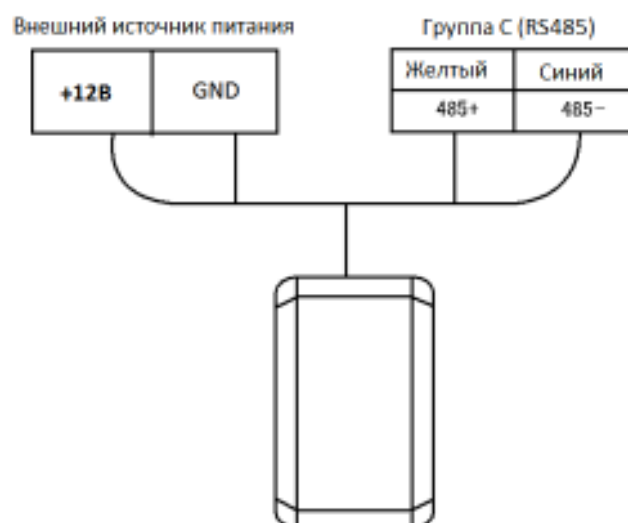


Рисунок 5-2 Схема подключения внешнего RS-485 считывателя карт

5.3 Подключение считывателя карт

Терминал контроля доступа может быть переключен в режим считывателя карт. Он может иметь доступ к контроллеру доступа в качестве устройства считывания карт и поддерживать порт связи Wiegand и порт связи RS-485.



Совет

Когда терминал контроля доступа работает в качестве считывателя карт, он поддерживает подключение только к контроллеру, и не поддерживает тревожные входы и выходы, или подключение к внешним устройствам.

5.3.1 Подключение Wiegand

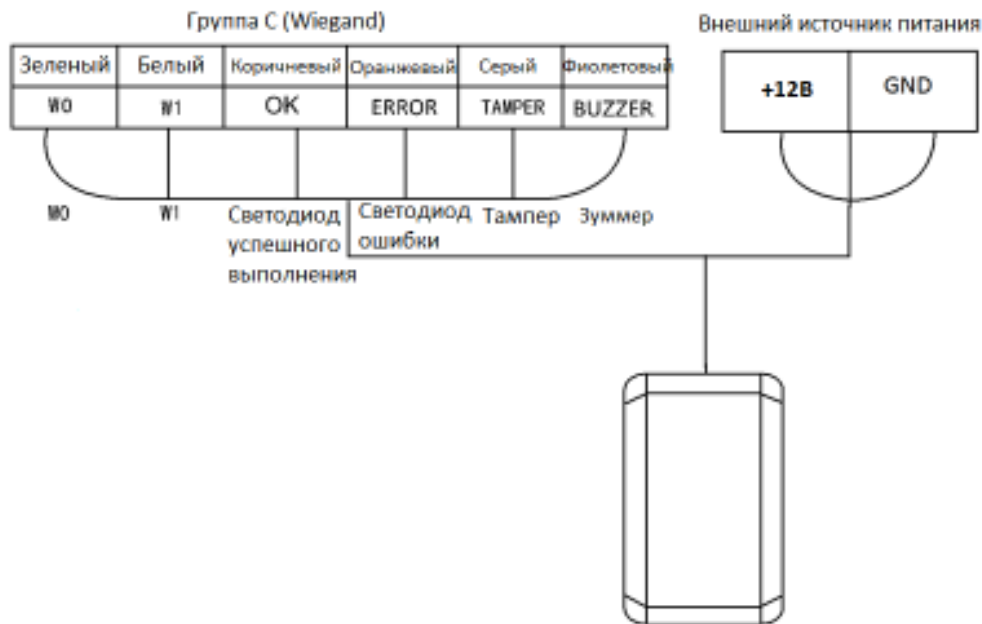


Рисунок 5-3 Схема подключения Wiegand



Совет

- Когда терминал контроля доступа работает в качестве считывателя карт, вы должны подключить интерфейсы **WG_ERR**, **BUZZER** и **WG_OK**, если вы хотите управлять светодиодом и зуммером Wiegand считывателя карт.
- Установите в качестве рабочего режима терминала значение «считыватель карт», если терминал требует работы в качестве считывателя карт. Режим считывателя карт поддерживает связь по Wiegand или RS-485.
- Расстояние Wiegand-подключения должно быть не более 80 м.
- Внешний источник питания и терминал контроля доступа должны использовать один и тот же кабель заземления.

5.3.2 Подключение RS-485 выхода

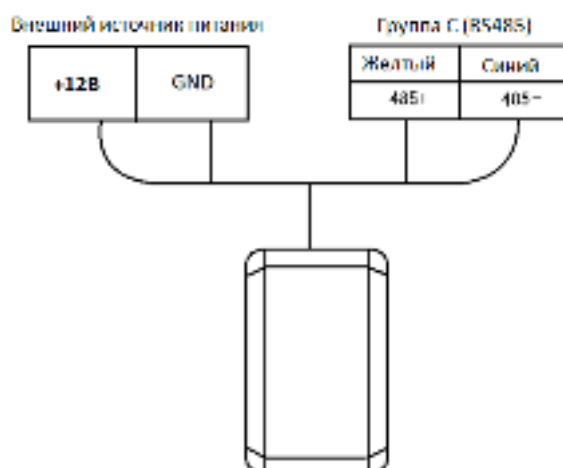


Рисунок 5-4 Схема подключения RS-485



Совет

- Установите в качестве рабочего режима терминала значение «считыватель карт», если терминал требует работы в качестве считывателя карт.
- Когда терминал контроля доступа работает как RS-485 считыватель карт, по умолчанию RS-485 адрес - 1.
- Внешний источник питания и терминал контроля доступа должны использовать один и тот же кабель заземления.

6 Активация терминала контроля доступа

Цель:

Вам необходимо активировать терминал перед его использованием.

Поддерживается активация через SADP и при помощи клиентского ПО.

Значения по умолчанию для терминала.

- IP-адрес по умолчанию: 192.0.0.64.
- № порта по умолчанию: 8000.
- Имя пользователя по умолчанию: admin.

6.1 Активация при помощи SADP

Программное обеспечение SADP используется для обнаружения онлайн-устройств, активации устройств и сброса пароля. Получите программное обеспечение SADP с прилагаемого диска или официального сайта и установите SADP в соответствии с подсказками. Выполните следующие шаги для активации панели управления.

Шаги:

1. Запустите ПО SADP для поиска онлайн-устройств.
2. Проверьте статус устройства в списке устройств и выберите неактивное устройство.

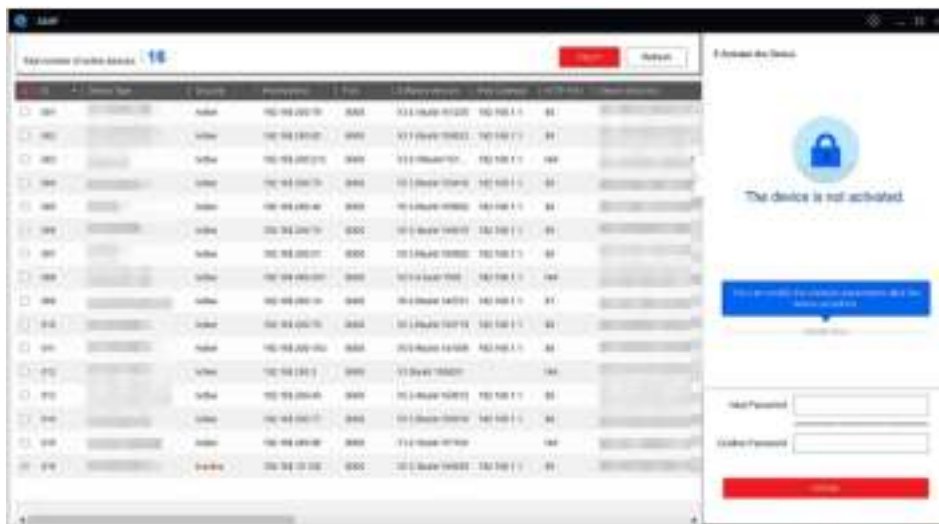


Рисунок 6-1 Интерфейс SADP

3. Создайте пароль, введите его в поле **new password** («Новый пароль») и подтвердите пароль в поле **confirm password** («Подтверждение пароля»).



РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ — Настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

4. Нажмите **Activate** («Активировать») для активации устройства.
5. Вы можете проверить, завершена ли активация во всплывающем окне.
6. Если произошла ошибка активации, пожалуйста, убедитесь, что пароль отвечает требованиям и повторите попытку.
7. Измените IP-адрес устройства так, чтобы он находился в той же подсети, к которой

подключен Ваш компьютер, вручную или, поставив галочку Enable DHCP («Включить DHCP»).



Рисунок 6-2 Меню изменения сетевых параметров

8. Введите пароль и нажмите кнопку Modify («Изменить») для того, чтобы изменить IP-адрес.

6.2 Активация через клиентское ПО

Клиентское программное обеспечение является универсальным программным обеспечением для управления видеонаблюдением для нескольких видов устройств.

Получите клиентское программное обеспечение с прилагаемого диска или на официальном сайте и установите программное обеспечение в соответствии с подсказками. Выполните следующие действия для активации панели управления.

Шаги:

1. Запустите клиентское программное обеспечение, появится панель управления программным обеспечением, как показано на рисунке ниже.
2. Нажмите иконку  вверху в левой стороне интерфейса, выберите **Access Control** («Контроль доступа») для входа в панель управления.



Рисунок 6-3 Панель управления

3. Нажмите иконку **Controller Management** («Управление контроллером») для входа в меню управления терминалом контроля доступа как показано на рисунке ниже.



Рисунок 6-4 Список устройств

4. Проверьте статус устройства в списке устройств и выберите неактивное устройство.
5. Нажмите на кнопку **Activate** («Активация») для вызова интерфейса активации.



Рисунок 6-5 Меню списка выбора

6. Создайте пароль, введите его в поле **password** («пароль») и подтвердите пароль в поле **confirm** («подтверждение»).



РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ – Настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.



7. Нажмите **OK** для начала активации.
8. Нажмите кнопку **Edit Network...** («Изменить сетевые параметры») для появления всплывающего меню изменения сетевых параметров.
9. Измените IP-адрес устройства так, чтобы он был в той же подсети, к которой подключен Ваш компьютер, вручную или, поставив галочку **Enable DHCP** («Включить DHCP»).
10. Введите пароль для сохранения изменений.

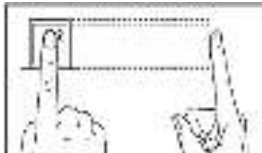
Приложение: Советы по сканированию отпечатков пальцев

Рекомендуемый палец

Указательный палец или средний палец.

Правильное сканирование

Показанный ниже рисунок - это правильный способ сканирования пальца:



Вы должны прижать палец к сканеру горизонтально. Центр сканируемого пальца должен совпадать с центром сканера.

Неправильное сканирование

Приведенные ниже рисунки показывают неверные способы сканирования отпечатков пальцев:



Окружающая среда

Сканер должен избегать прямых лучей света, высоких температур, влажных условий и дождя.

Когда палец замерзший, сканер может не распознать ваш отпечаток. Вы можете подуть на палец и снова приложить его к сканеру.

Другое

Если ваш отпечаток неглубокий или трудно отсканировать отпечаток пальца, мы рекомендуем использовать другие методы аутентификации.

Если у вас есть травмы на сканируемом пальце, сканер может его не распознать. Вы можете изменить палец и повторить попытку снова.

0101001060602

