Комплект дистанционного управления по радиоканалу

Руководство пользователя

Оглавление

1 Обзор

1.1 Введение

Радиоприёмник и пульт дистанционного управления используется для обеспечения беспроводного контроля прохода через турникеты в общественных местах, таких как жилые комплексы, учебные заведения, государственные учреждения, заводы и офисные здания, что обеспечивает общее сдерживающее управление доступом для общественных проходов.

1.2 Внешний вид

Рисунок 1-1 Внешний вид

Пульт дистанционного управления

Радиоприёмник

Таблица 1-1 Компоненты

Компоненты	Описание
Пульт ДУ	Сопоставляет коды с приемником для дистанционного управления проходом.
Радиоприёмник	Подключается к основной плате управления турникета для дистанционного управления проходом.

1.3 Функции

- Надежное шифрование.
- Дистанционное управление.
- Несколько методов открытия прохода.
- Сопоставление кодов через радиоприёмник. Один приемник может сопоставить коды для 32 пультов ДУ.

- Сопоставление кодов через пульт ДУ. Один пульт может сопоставить коды до 32 приёмников.
- Два режима сопряжения.

◇ Нажмите кнопку  и кнопку A (открытие на вход) одновременно, чтобы начать сопряжение.

◇ Нажмите кнопку  и кнопку B (открытие на выход) одновременно, чтобы отменить сопряжение.

2 Подключение

2.1 Описание портов радиоприёмника

Установите приемник под платой считывания карт, под верхней крышкой турникета или рядом с основной платой управления внутри турникета.

Рисунок 2-1 Порты приемника

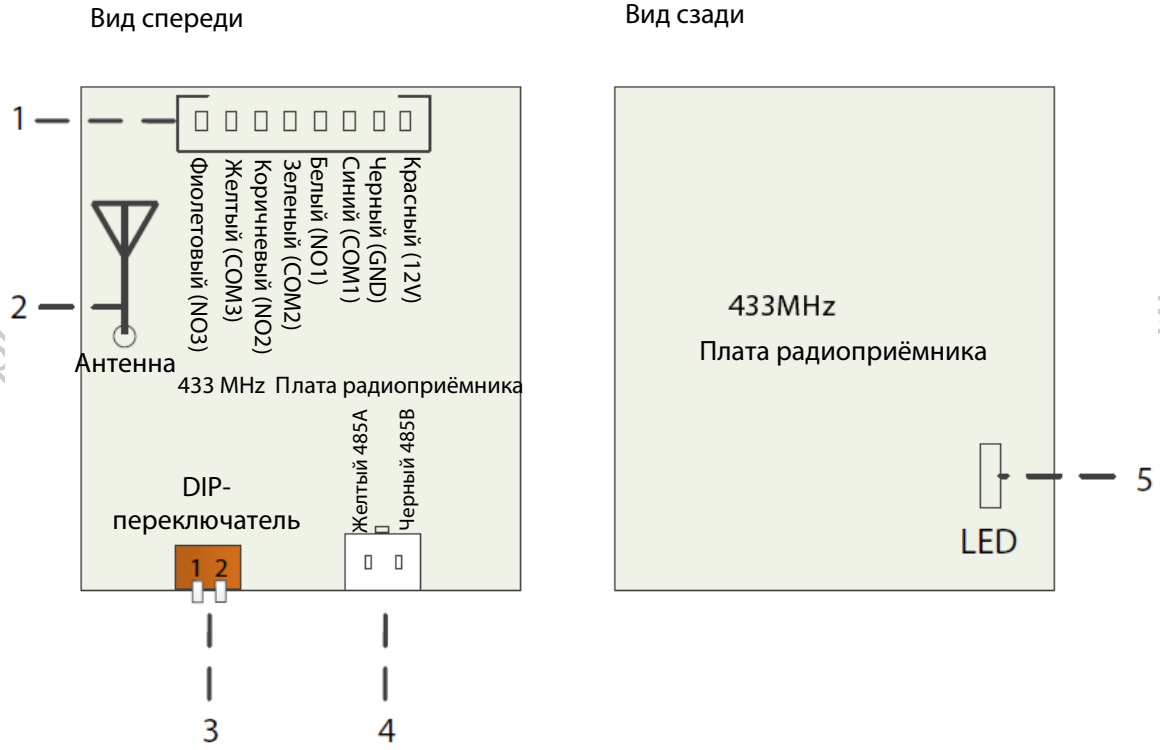


Таблица 2-1 Описание портов приемника

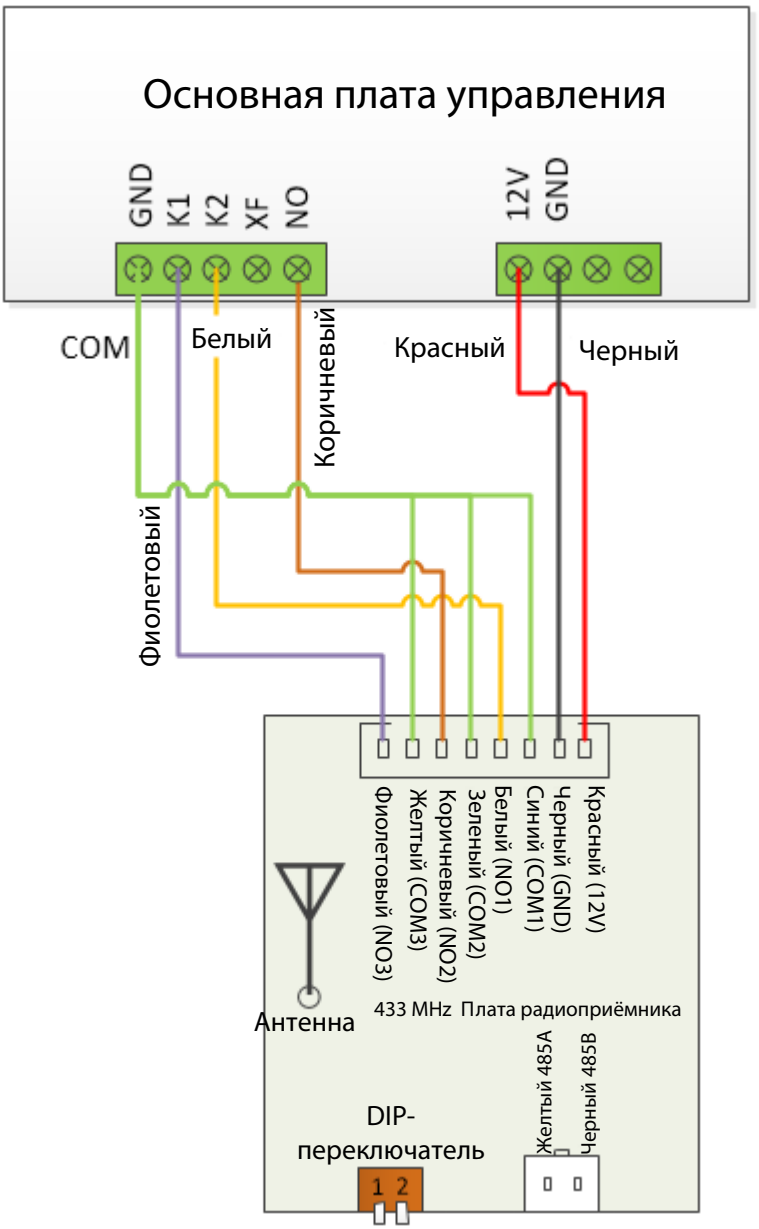
No.	Описание
1	8-контактный разъем: один канал для питания 12 В и три канала для выхода «сухой контакт». ● Красный (12V) и черный (GND): Подают питание 12 В. ● Белый (NO1): Подключается к контакту K2 основной платы управления турникета. ● Коричневый (NO2): Подключается к контакту NO основной платы управления турникета. ● Фиолетовый (NO3): Подключается к контакту K1 основной платы управления турникета. ● Синий (COM1), зеленый (COM2) и желтый (COM3): Подключаются к контакту GND основной платы управления турникета.
2	Антенна.
3	● **Включить DIP-переключатель 1:** Приемник начинает сопряжение. ● **Включить DIP-переключатель 2:** Приемник отменяет сопряжение. ● **Включить оба DIP-переключателя 1 и 2:** Доступно для турникетов без сигналов NO/ восстановления (например, маятниковые турникеты W-типа).

No.	Описание
4	Порт RS-485. Обеспечивает связь с основной платой управления турникета.
5	Индикатор. ● Синий: Рабочий режим. ● Зеленый: Сопряжение. ● Красный: Отмена сопряжения. ● Желтый: Доступно для турникетов без сигналов нормально замкнутого/восстановления (например, маятниковый турникет W-типа).

2.2 Подключение к основной плате управления (с поддержкой порта NO)

Управляющий сигнал от приемника подключается к сигналам K1, K2 и NO основной платы управления.

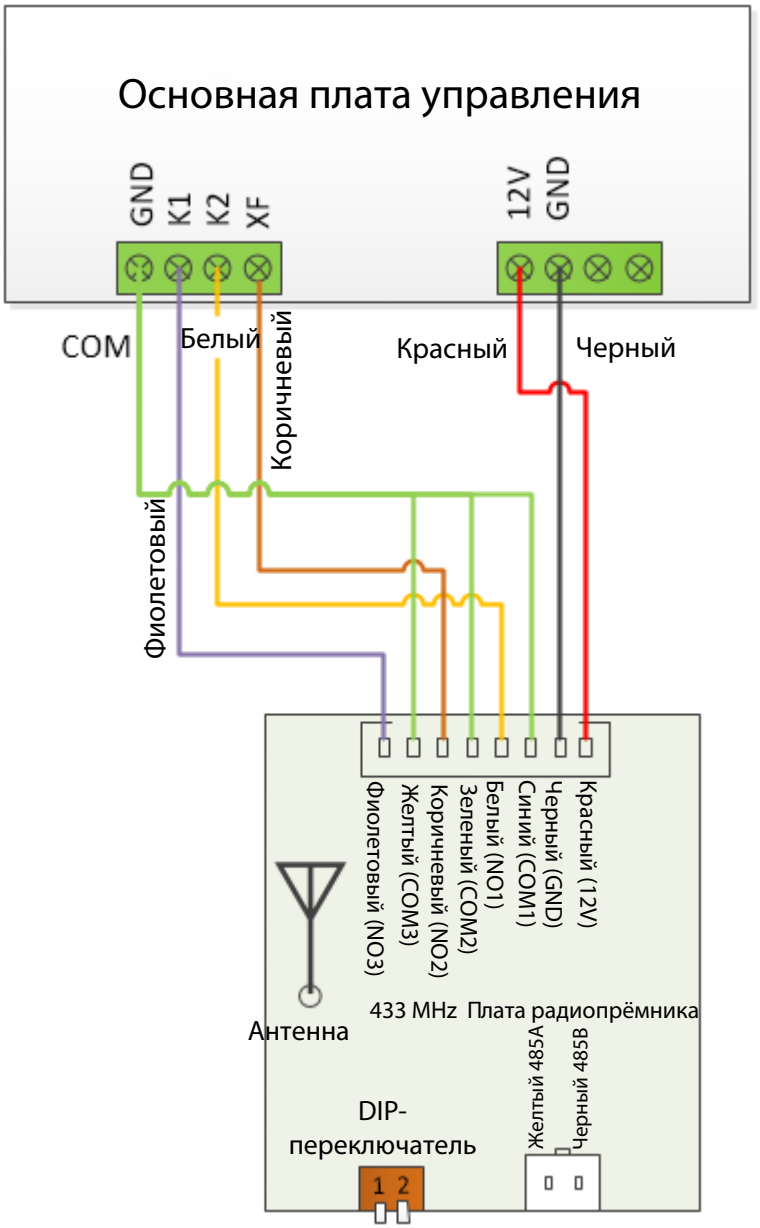
Рисунок 2-2 Подключение проводов



2.3 Подключение к основной плате управления (без поддержки порта NO)

Приемник подключается к основной плате управления. Управляющий сигнал может контролироваться через сигналы K1 и K2.

Рисунок 2-3 Подключение



3 Настройка и отладка

3.1 Кнопки и индикатор

Рисунок 3-1 Кнопки и индикатор

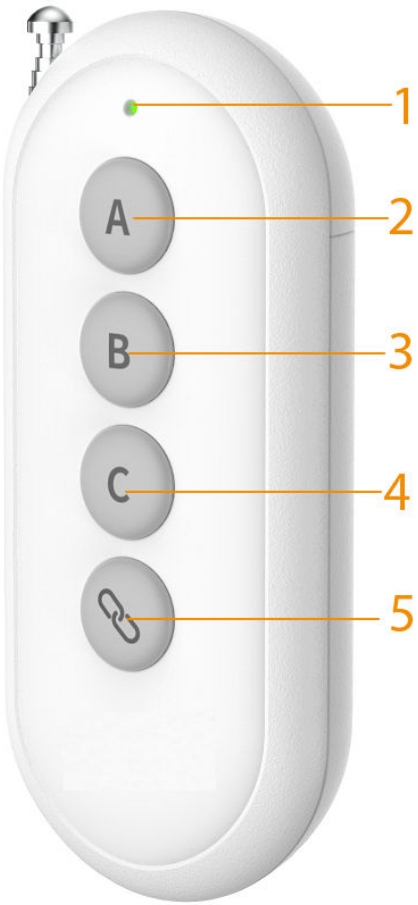


Таблица 3-1 Описание кнопок и индикатора

No.	Название	Описание
1	Индикатор	Отображает состояние и режим работы пульта ДУ. ● Однократное зеленое мигание: Успешная передача. ● Однократное красное мигание: Неудачная передача. ● Поочередное однократное мигание зеленым и красным: Низкий заряд батареи, но передача успешна.
2	A (открытие на вход)	Нажмите кнопку, чтобы открыть проход в направлении входа.
3	B (открытие на выход)	Нажмите кнопку, чтобы открыть проход в направлении выхода.

No.	Название	Описание
4	C (одноклавишное нормальное открытие/ восстановление)	Нажмите кнопку, чтобы удерживать турникет в открытом состоянии, затем нажмите ее снова, чтобы закрыть проход. Можно изменить режим энергопотребления при использовании вместе с кнопкой Подробности см. в разделе "3.3 Режим энергопотребления".
5	Сопряжение	Нажмите кнопку и кнопку A или B одновременно, чтобы настроить режим сопряжения. Подробности см. в разделе "3.2 Настройка режима сопряжения".

3.2 Настройка режима сопряжения

3.2.1 Запуск режима сопряжения

Порядок действий:

Шаг 1. Включите DIP-переключатель 1 на приемнике, после чего индикатор начнет мигать зеленым цветом.
Шаг 2. Одновременно нажмите кнопку и кнопку A на пульте ДУ, чтобы начать сопряжение.

- **Индикатор мигает зеленым:** приемник начал процесс сопряжения.
- **Индикатор мигает зеленым 3 секунды, а затем гаснет после короткого постоянного свечения зеленым:** сопряжение успешно завершено.
- **Индикатор мигает зеленым 10 секунд, а затем гаснет:** сопряжение не удалось.

Шаг 3. После завершения сопряжения выключите DIP-переключатель 1.

3.2.2 Отмена режима сопряжения

Порядок действий:

Шаг 1. Включите DIP-переключатель 2 на приемнике.
Шаг 2. Одновременно нажмите кнопку и кнопку B на передатчике, чтобы отменить сопряжение.

- **Индикатор мигает красным:** приемник начал процесс отмены сопряжения.
- **Индикатор мигает красным 3 секунды, а затем гаснет после короткого постоянного свечения красным:** отмена сопряжения успешно завершена.
- **Индикатор мигает красным 10 секунд, а затем гаснет:** отмена сопряжения не удалась.

Шаг 3. После отмены выключите DIP-переключатель 2.

3.3 Режим энергопотребления

Существует 2 режима энергопотребления. Одновременное нажатие кнопки и кнопки C изменяет режим.

- **Режим высокого энергопотребления:** Дальность дистанционного управления достигает 15 метров (индикатор светится желтым цветом).
- **Режим низкого энергопотребления:** Дальность дистанционного управления не достигает 15 метров (индикатор светится зеленым цветом).

Устройство по умолчанию находится в режиме низкого энергопотребления.

3.4 Подключение к турникету (модель 1W) без сигналов NO или Restore

Для подключения устройства к турникету без функций NO или Restore, например модели 1W, включите DIP-переключатели согласно инструкции.

Порядок действий:

Шаг 1. Сопрягите приемник (пульт ДУ) и передатчик. Подробности см. в разделе "3.2 Настройка режима сопряжения".
Шаг 2. Включите DIP-переключатели 1 и 2 на приемнике.

3.5 Включение питания

Порядок действий:

Шаг 1. Проверьте комплектность.

Устройство полностью проверяется перед отгрузкой с завода. Транспортировка и установка могут повлиять на его состояние.

Шаг 2. Проверьте, является ли соединение стабильным и нормальным.
Шаг 3. Включите питание пульта дистанционного управления. Если индикатор приемника горит постоянным синим цветом, приемник работает нормально.
Шаг 4. Сопоставьте коды между приемником и передатчиком.
Нажмите 3 кнопки, чтобы проверить, открывается ли турникет в том же направлении, что и направление кнопки. Если турникет открывается в неправильном направлении, следуйте инструкциям по подключению, чтобы изменить соединение.

4 Часто задаваемые вопросы

- Индикатор приемника не загорается при включении питания.

  Проверьте кабель питания приемника.

- Турникет не открывается при нажатии кнопки A.

  ◇ Проверьте, правильно ли подключено устройство.

  ◇ Проверьте заряд батареи пульта ДУ.

- Турникет открывается в направлении выхода при нажатии кнопки A.

  Проверьте, правильно ли подключено устройство.

Приложение 1 Рекомендации по безопасности

Управление учетными записями

1. **Используйте сложные пароли**

   При установке паролей следуйте следующим рекомендациям:

   - Длина пароля должна быть не менее 8 символов;
   - Пароль должен содержать как минимум два типа символов: заглавные и строчные буквы, цифры и специальные символы;
   - Пароль не должен содержать имя учетной записи или имя учетной записи в обратном порядке;
   - Не используйте последовательные символы, такие как 123, abc и т.д.;
   - Не используйте повторяющиеся символы, такие как 111, aaa и т.д.
2. **Регулярно меняйте пароли**
   Рекомендуется периодически менять пароль устройства, чтобы снизить риск его угадывания или взлома.
3. **Рационально распределяйте учетные записи и права доступа**
   Добавляйте пользователей в соответствии с требованиями обслуживания и управления, назначая им минимально необходимые наборы прав.
4. **Включите функцию блокировки учетной записи**
   Функция блокировки учетной записи включена по умолчанию. Рекомендуется оставить ее включенной для защиты безопасности учетной записи. После нескольких неудачных попыток ввода пароля соответствующая учетная запись и IP-адрес источника будут заблокированы.
5. **Своевременно настраивайте и обновляйте информацию для сброса пароля**
   Устройство поддерживает функцию сброса пароля. Чтобы снизить риск использования этой функции злоумышленниками, своевременно вносите изменения при любом обновлении информации. При настройке контрольных вопросов рекомендуется не использовать легко угадываемые ответы.

Конфигурация служб

1. **Включите HTTPS**

   Рекомендуется включить HTTPS для доступа к веб-службам по защищенному каналу.
2. **Шифрование передачи аудио и видео**
   Если содержимое ваших аудио- и видеоданных является очень важным или конфиденциальным, рекомендуется использовать функцию шифрования передачи, чтобы снизить риск перехвата данных во время передачи.
3. **Отключение необязательных служб и использование безопасных режимов**
   Если в них нет необходимости, рекомендуется отключить некоторые службы, такие как SSH, SNMP, SMTP, UPnP, точка доступа AP и т.д., чтобы уменьшить поверхность атаки.
   При необходимости настоятельно рекомендуется выбирать безопасные режимы, включая, но не ограничиваясь следующими службами:
   - SNMP: Выберите SNMP v3 и настройте надежное шифрование и пароли аутентификации.
   - SMTP: Выберите TLS для доступа к почтовому серверу.
   - FTP: Выберите SFTP и настройте сложные пароли.
   - Точка доступа AP: Выберите режим шифрования WPA2-PSK и настройте сложные пароли.
4. **Изменение портов HTTP и других служб по умолчанию**
   Рекомендуется изменить порт по умолчанию для HTTP и других служб на любой порт в диапазоне от 1024 до 65535, чтобы снизить риск их угадывания злоумышленниками.

Конфигурация сети

1. **Включите разрешающий список (Allow list)**
   Рекомендуется включить функцию разрешающего списка и разрешить доступ к устройству только IP-адресам из этого списка. Поэтому обязательно добавьте в разрешающий список IP-адрес своего компьютера и IP-адреса поддерживающих устройств.
2. **Привязка MAC-адреса**
   Рекомендуется привязать IP-адрес шлюза к MAC-адресу на устройстве, чтобы снизить риск ARP-спуфинга.
3. **Создайте безопасную сетевую среду**
   Для лучшего обеспечения безопасности устройств и снижения потенциальных сетевых рисков рекомендуется следующее:
   - Отключите функцию перенаправления портов (port mapping) на маршрутизаторе, чтобы избежать прямого доступа к устройствам внутренней сети из внешней сети.
   - В соответствии с фактическими потребностями сети сегментируйте ее: если между двумя подсетями нет необходимости в обмене данными, рекомендуется использовать VLAN, шлюзы и другие методы для разделения сети и достижения сетевой изоляции.
   - Установите систему контроля доступа 802.1x, чтобы снизить риск несанкционированного доступа терминалов к частной сети.

Аудит безопасности

1. **Проверяйте пользователей в сети**
   Рекомендуется регулярно проверять пользователей в сети, чтобы выявлять несанкционированных пользователей.
2. **Проверяйте журнал устройства**
   Просматривая журналы, можно получить информацию об IP-адресах, с которых осуществлялись попытки входа на устройство, а также о ключевых операциях, выполненных вошедшими пользователями.
3. **Настройте сетевой журнал (лог)**
   Из-за ограниченного объема памяти устройства сохраняемый журнал ограничен. Если требуется длительное хранение журналов, рекомендуется включить функцию сетевого журнала, чтобы обеспечить синхронизацию критически важных записей на сетевой сервер журналов для последующего анализа.

Безопасность программного обеспечения

1. **Своевременно обновляйте микропрограмму (прошивку)**
   В соответствии с отраслевыми стандартами эксплуатации микропрограмма устройств должна своевременно обновляться до последней версии, чтобы обеспечить наличие у устройства новейших функций и безопасности. Если устройство подключено к публичной сети, рекомендуется включить функцию автоматического обнаружения онлайн-обновлений для своевременного получения информации об обновлениях прошивки, выпускаемых производителем.
2. **Своевременно обновляйте клиентское программное обеспечение**
   Рекомендуется загружать и использовать последние версии клиентского программного обеспечения.

Физическая защита

Рекомендуется обеспечить физическую защиту устройств (особенно устройств хранения данных), например, размещать устройства в выделенных серверных комнатах и стойках, а также внедрять контроль доступа и управление ключами, чтобы предотвратить повреждение оборудования и периферийных устройств (например, USB-накопителей, последовательных портов) несанкционированным персоналом.