

# **Бесконтактный считыватель карт доступа Dahua DHI-ASR1200E/DHI-ASR1200E-D**

## **Руководство пользователя**



версия 1.1.4

# Содержание

|                                                 |   |
|-------------------------------------------------|---|
| 1 Обзор.....                                    | 1 |
| 1.1 Внешний вид.....                            | 1 |
| 1.2 Схема сетевого подключения.....             | 2 |
| 2 Требования к подключению проводов.....        | 3 |
| 3 Установка.....                                | 4 |
| Приложение 1. Рекомендации по безопасности..... | 5 |

# 1 Обзор

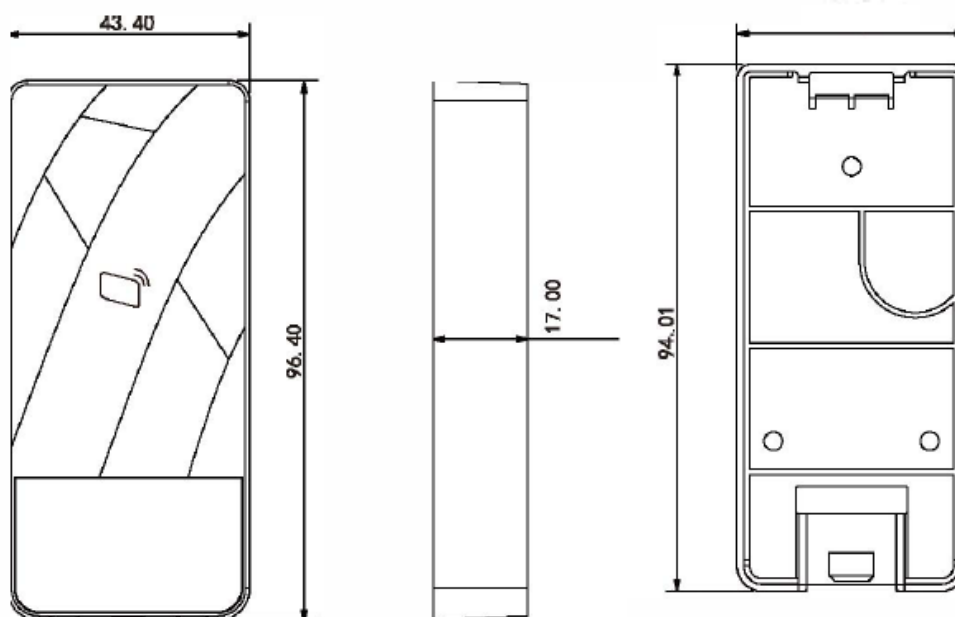
В большинстве систем контроля доступа считыватель карт доступа — это система безопасности, требующая проведения идентификационной карты для проверки того, что входящий в помещение/зону человек имеет разрешение на доступ. Он подходит для самых различных объектов, таких как офисные здания, школы, жилые комплексы, микрорайоны, заводы, общественные места, бизнес-центры и административные здания.

Основные функции:

- **Бесконтактный считыватель (только чтение)** — дальность считывания 2,5–5,5 см, время отклика < 0,3 с.
- **Поддерживает протоколы Wiegand и RS-485.** Скорость передачи данных RS-485 — 9600 бит/с.
- **Поддержка функции Watchdog** (сторожевого таймера).
- Все порты имеют **защиту от перегрузки** по току и **перенапряжения**.
- **Степень защиты:** IP67. Подходит для уличной установки. Рабочая температура: от –30 °С до +60 °С, рабочая влажность: ≤95 %.
- Поддержка **звукового сигнала** (зуммера) и **светодиодной индикации**.

## 1.1 Внешний вид

Рисунок 1–1 Габаритные размеры (мм)



## 1.2 Схема сетевого подключения

Схема сетевого подключения приведена только для справки.

Рисунок 1–2 Схема сетевого подключения



## 2 Требования к подключению проводов

- Подключайте считыватель карт к портам Wiegand или RS-485 в зависимости от типа считывателя.
- Выбирайте провода в соответствии с требованиями к кабелям.

Таблица 2–1 Описание подключения проводов

| Цвет       | Порт   | Описание                                                                                                                                                                                                                        |
|------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Красный    | 12 V   | Питание (12 В пост. тока)                                                                                                                                                                                                       |
| Черный     | GND    | Провод заземления                                                                                                                                                                                                               |
| Синий      | CASE   | Сигнал тревоги при вскрытии<br><br>Данная функция в настоящее время недоступна.                                                                |
| Белый      | D1     | Передающий сигнал Wiegand (активен только при использовании протокола Wiegand)                                                                                                                                                  |
| Зеленый    | D0     |                                                                                                                                                                                                                                 |
| Коричневый | LED    | Ответный сигнал Wiegand (активен только при использовании протокола Wiegand)                                                                                                                                                    |
| Желтый     | RS485- | Отрицательный провод RS-485 (активен только при использовании протокола RS-485)<br><br>Обновление устройства через RS-485 не поддерживается. |
| Фиолетовый | RS485+ | Положительный провод RS-485 (активен только при использовании протокола RS-485)<br><br>Обновление устройства через RS-485 не поддерживается. |

Таблица 2–2 Требования к подключению считывателя карт

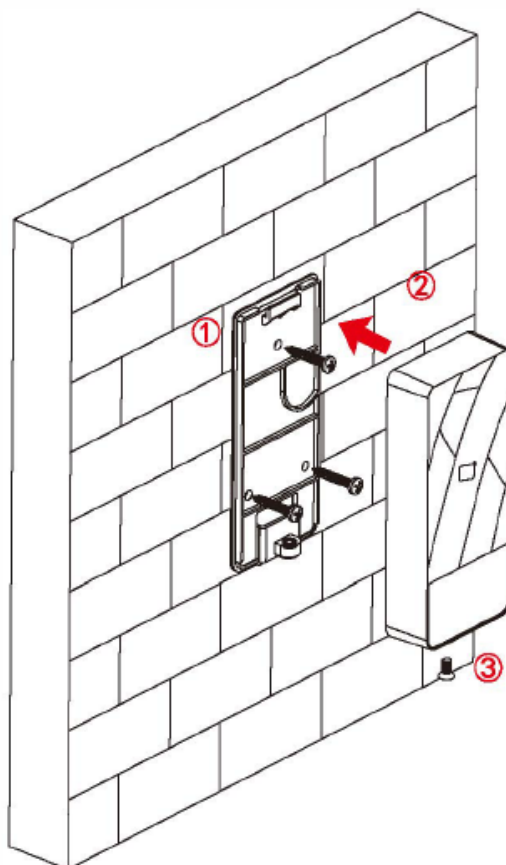
| Тип                 | Требования к сопротивлению                                     | Требования к длине                                                   |
|---------------------|----------------------------------------------------------------|----------------------------------------------------------------------|
| Считыватель RS-485  | Сопротивление каждого провода RS-485 должно быть $\leq 10$ Ом. | $\leq 100$ м.<br>Рекомендуется экранированный кабель UL1061, 24 AWG. |
| Считыватель Wiegand | Сопротивление каждого провода Wiegand должно быть $\leq 2$ Ом. | $\leq 80$ м.<br>Рекомендуется экранированный кабель UL1061, 18 AWG.  |

## 3 Установка

### Порядок действий

**Шаг 1.** Закрепите заднюю крышку на стене с помощью саморезов.

Рисунок 3–1 Установка



**Шаг 2.** Установите переднюю крышку на крючок в верхней части задней крышки.

**Шаг 3.** Вкрутите один винт в нижней части считывателя карт.

# Приложение 1. Рекомендации по безопасности

## Управление учётными записями

### 1. Используйте сложные пароли

При установке паролей следуйте приведённым ниже рекомендациям:

- Длина пароля должна быть не менее 8 символов;
- Пароль должен включать как минимум два типа символов: заглавные и строчные буквы, цифры и специальные знаки;
- Не используйте имя учётной записи или его обратное написание;
- Не используйте последовательные символы (например, 123, abc и т. п.);
- Не используйте повторяющиеся символы (например, 111, aaa и т. п.).

### 2. Регулярно меняйте пароли

Рекомендуется периодически менять пароль устройства для снижения риска его подбора или взлома.

### 3. Разумно назначайте учётные записи и права доступа

В соответствии с бизнес-требованиями и требованиями управления разумно добавляйте пользователей и назначайте им минимально необходимый набор прав.

### 4. Включите блокировку учётной записи

Функция блокировки учётной записи включена по умолчанию. Рекомендуется оставить её включённой для обеспечения безопасности учётной записи. После нескольких неудачных попыток ввода пароля соответствующая учётная 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, при изменении информации обновите её. При настройке контрольных вопросов рекомендуется не использовать вопросы, ответы на которые легко угадать.

## Настройка служб

### 1. Включите HTTPS

Рекомендуется включить HTTPS для доступа к веб-службам через защищённые каналы.

### 2. Шифрованная передача аудио и видео

Если содержимое ваших аудио- и видеоданных является важным или чувствительным, рекомендуется использовать функцию шифрованной передачи, чтобы снизить риск перехвата аудио- и видеоданных во время передачи.

### 3. Отключите неиспользуемые службы и используйте безопасный режим

Если они не нужны, рекомендуется отключить некоторые службы, такие как SSH, SNMP, SMTP, UPnP, точка доступа (AP hotspot) и другие, чтобы уменьшить количество векторов атак.

При необходимости настоятельно рекомендуется выбирать безопасные режимы, включая, помимо прочего, следующие службы:

- **SNMP:** Выберите SNMP v3 и установите надёжные пароли шифрования и аутентификации.
- **SMTP:** Выберите TLS для доступа к почтовому серверу.
- **FTP:** Выберите SFTP и установите сложные пароли.
- **Точка доступа (AP hotspot):** Выберите режим шифрования WPA2-PSK и установите сложный пароль.

### 4. Измените HTTP и другие порты служб по умолчанию

Рекомендуется изменить стандартные порты HTTP и других служб на любой порт в диапазоне от 1024 до 65535, чтобы снизить риск их угадывания злоумышленниками.

## Настройки сети

### 1. Включите «Белый список» (Allow list)

Рекомендуется включить функцию «Белый список» и разрешить доступ к устройству только IP-адресам, внесённым в этот список. Убедитесь, что вы добавили в него IP-адрес вашего компьютера и IP-адреса вспомогательных устройств.

### 2. Привязка MAC-адреса

Рекомендуется привязать IP-адрес шлюза к MAC-адресу на устройстве, чтобы снизить риск подмены ARP (ARP-спуфинга).

### 3. Создание безопасной сетевой среды

Для лучшего обеспечения безопасности устройств и снижения потенциальных киберрисков рекомендуется:

- Отключить функцию проброса портов на маршрутизаторе, чтобы избежать прямого доступа к устройствам внутренней сети из внешней сети;
- В соответствии с реальными сетевыми потребностями выполнить сегментацию сети: если между двумя подсетями нет необходимости в обмене данными, рекомендуется использовать VLAN, шлюз и другие методы для разделения сети с целью достижения изоляции;
- Внедрить систему аутентификации доступа 802.1x для снижения риска несанкционированного подключения неавторизованных терминалов к частной сети.

## Безопасный аудит

### 1. Проверка онлайн-пользователей

Рекомендуется регулярно проверять список подключённых пользователей для выявления неавторизованных (нелегальных) пользователей.

### 2. Проверка журнала устройства

Просматривая логи, вы можете узнать IP-адреса, с которых выполнялись попытки входа в устройство, а также ключевые операции авторизованных пользователей.

### 3. Настройка сетевого журнала (логирования)

В связи с ограниченным объёмом встроенной памяти устройства хранимые логи ограничены. Если требуется длительное хранение логов, рекомендуется включить функцию сетевого логирования, чтобы критически важные записи синхронизировались с сервером сетевых журналов для последующего анализа.

## Безопасность программного обеспечения

### 1. Своевременно обновляйте встроенное ПО

Согласно отраслевым стандартам эксплуатации, прошивка устройств должна своевременно обновляться до последней версии, чтобы устройство имело последние функции и обновления безопасности. Если устройство подключено к публичной сети, рекомендуется включить функцию автоматического обнаружения обновлений, чтобы своевременно получать информацию о новых версиях прошивки от производителя.

### 2. Своевременно обновляйте клиентское программное обеспечение

Рекомендуется загружать и использовать последнюю версию клиентского программного обеспечения.

## Физическая защита

Рекомендуется обеспечить физическую защиту устройств (особенно накопителей данных), например, разместить оборудование в специальном серверном помещении и стойке, а также организовать контроль доступа и управление ключами, чтобы предотвратить несанкционированный доступ персонала и физическое воздействие на аппаратное обеспечение и другое периферийное оборудование (например, USB-флешки, последовательные порты).