

Терминал доступа

Dahua DHI-ASI2212J

Краткое руководство по началу работы



версия 1.0.4

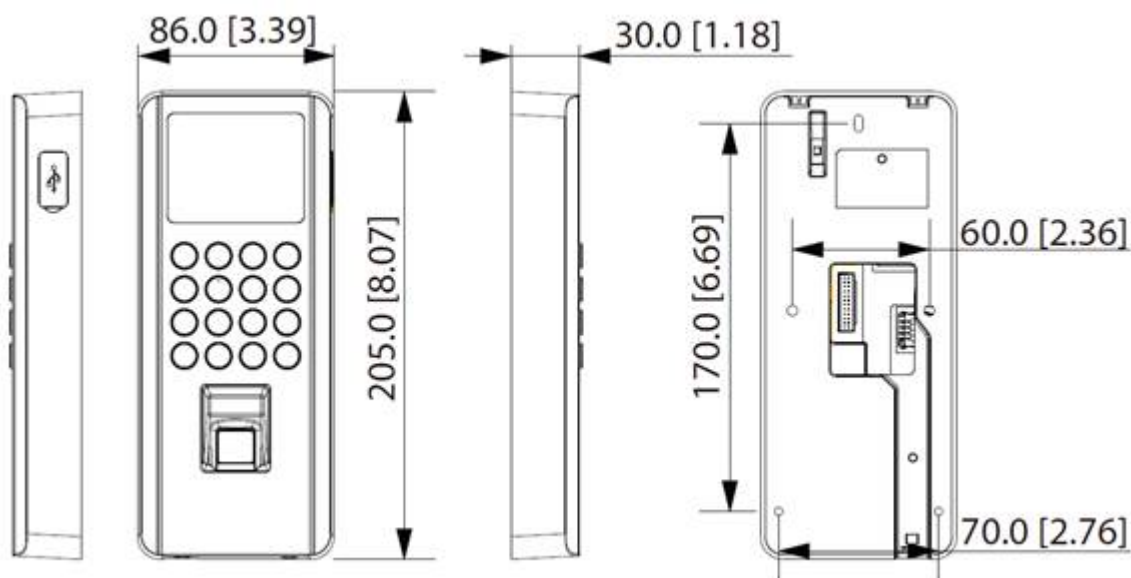
Содержание

1 Устройство.....	1
2 Подключение проводов и монтаж.	2
2.1 Подключение проводов.....	2
2.2 Условия монтажа.....	3
2.3 Процесс установки.....	5
2.3.1 Настенный монтаж.....	5
2.3.2 Установка на монтажную коробку 86 (подрозетник).....	6
3 Локальные настройки.....	8
3.1 Инициализация.....	8
3.2 Добавление пользователей.....	8
4 Веб-настройки.....	11
4.1 Инициализация.....	11
4.2 Вход в систему..	13
Приложение 1. Основные правила при добавлении отпечатков пальцев.....	14
Приложение 2. Рекомендации по кибербезопасности.....	16

1 Устройство

Внешний вид передней панели может отличаться в зависимости от модели контроллера доступа. В данном примере используется модель с датчиком отпечатков пальцев.

Рисунок 1–1 Конструкция автономного контроллера доступа (модель с отпечатком пальца)
(Размеры: мм [дюймы])



2 Подключение проводов и монтаж

2.1 Подключение проводов

Рисунок 2-1 Схема подключения автономного контроллера доступа (ASI22XXJ)

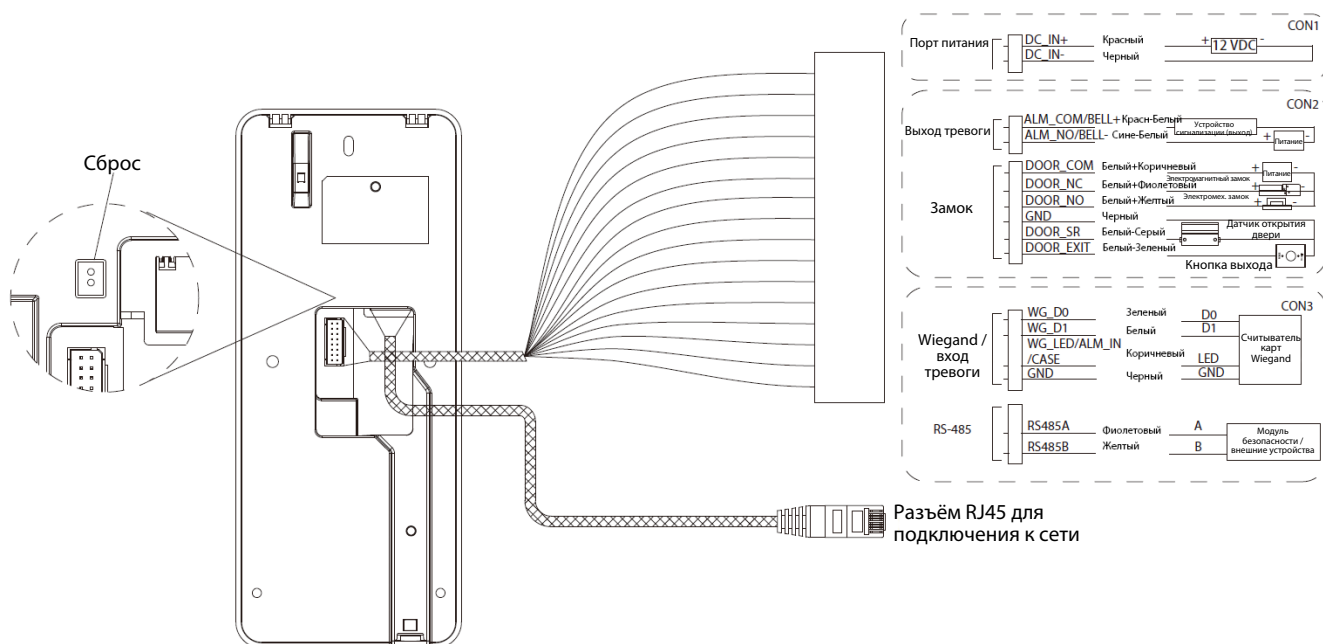
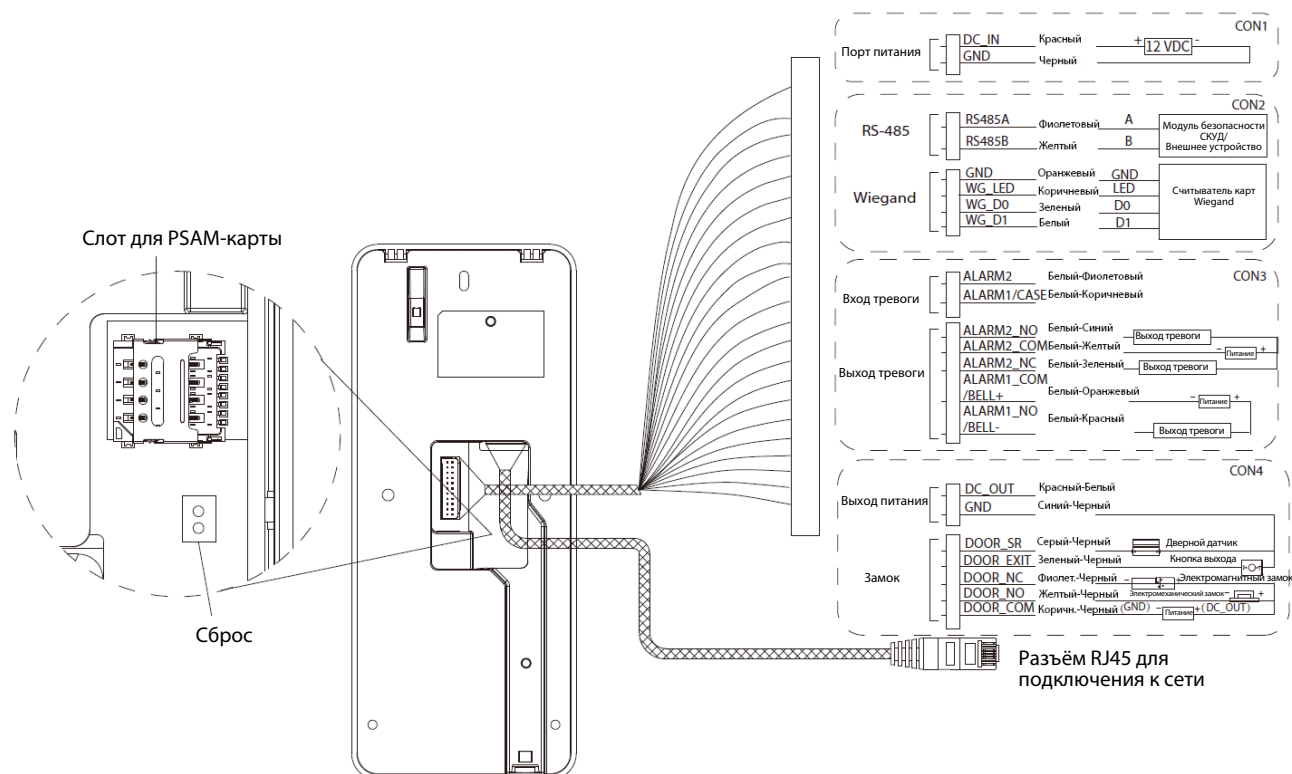


Рисунок 2-2 Схема подключения автономного контроллера доступа (ASI22XXJ-(D)PW)



- Автономный контроллер доступа с портом PoE поддерживает питание устройства через PoE. Контроллер также может подавать питание на считыватель карт (12 В / не более 200 мА) и электромагнитный замок (12 В / не более 500 мА). Расстояние передачи питания — не более 100 м. Рекомендуемое сечение кабеля питания — 20 AWG – 24 AWG; сопротивление — менее 1 Ом.
Сброс: с помощью пинцета замкните контакты сброса на 5 секунд.

- Для выхода тревоги подключайте устройство выхода тревоги к клеммам **ALARM2_NC** или **ALARM2_NO** в зависимости от типа устройства выхода тревоги.
- Для дверного замка подключайте замок к клеммам **DOOR_NC** или **DOOR_NO** в зависимости от типа замка.
- Некоторые провода могут использоваться для разных целей. На веб-странице автономного контроллера доступа выберите **Config Mgmt** (Управление конфигурацией) > **Interface Config** (Настройка интерфейсов) и задайте функцию портов.

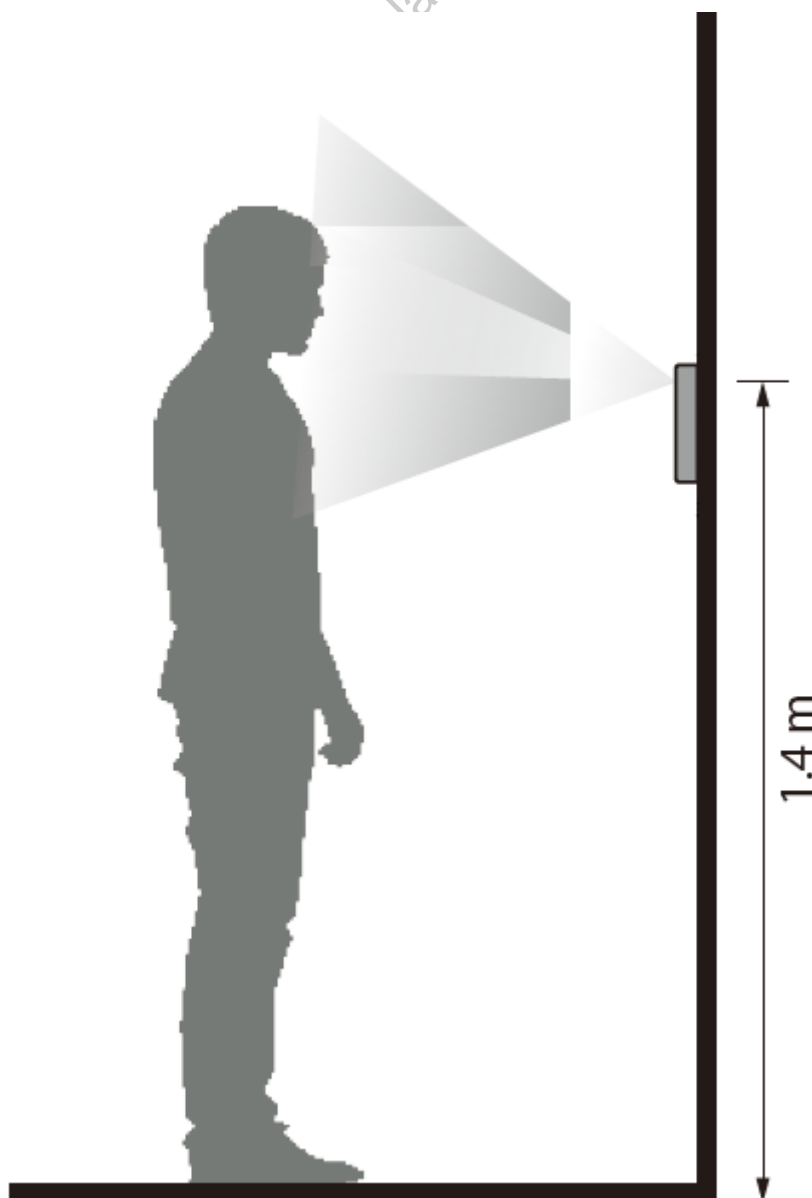
2.2 Условия монтажа



- Освещённость на расстоянии 0,5 м от автономного контроллера доступа должна быть не менее 100 люкс.
- Рекомендуется устанавливать автономный контроллер доступа в помещении, на расстоянии не менее 3 м от окон и дверей и 2 м от источников света.
- Избегайте контрового света, прямых солнечных лучей, близкого расположения источников света и косого освещения.

Высота установки

Рисунок 2–3 Требования к высоте установки



Требования к уровню освещённости окружающей среды

Рисунок 2–4 Требования к освещённости окружающей среды



Свеча: 10 люкс



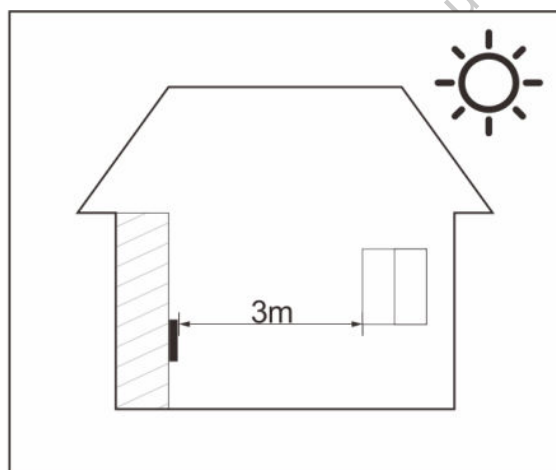
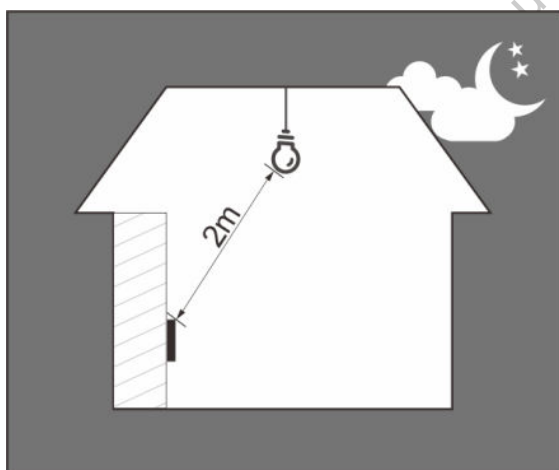
Лампа накаливания:
100–850 люкс



Солнечный свет:
 ≥ 1200 люкс

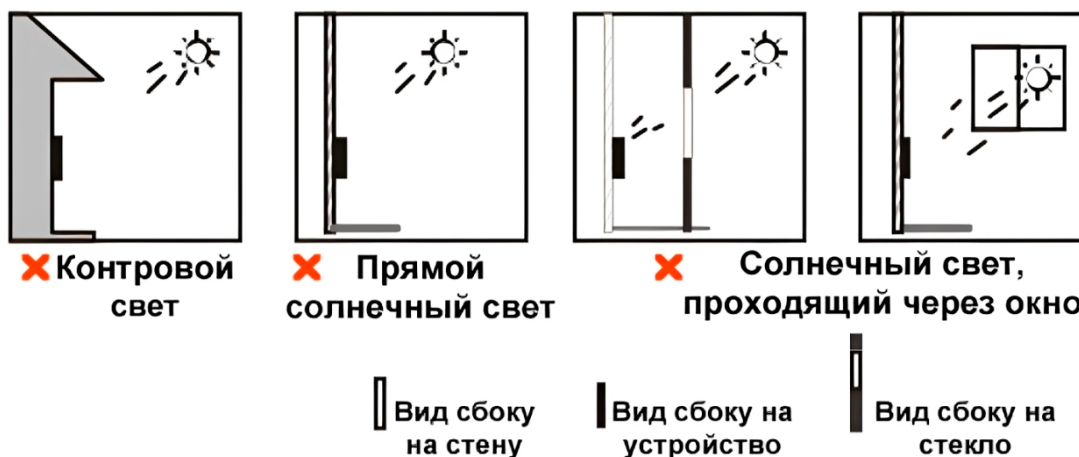
Рекомендуемые места установки

Рисунок 2–5 Рекомендуемые места установки



Места, не рекомендуемые для установки

Рисунок 2–6 Места, не рекомендуемые для установки



2.3 Процесс установки

Автономный контроллер доступа поддерживает два способа установки: настенный монтаж и установка на монтажную коробку 86 (подрозетник). Рекомендуемая высота установки — 1,2–1,6 м.

2.3.1 Настенный монтаж

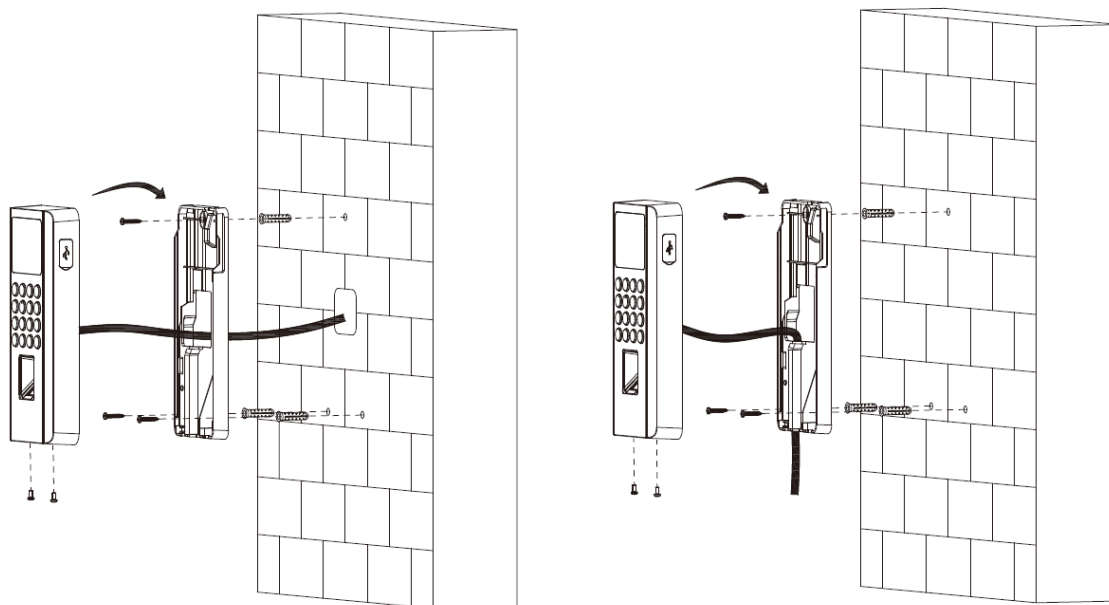
Порядок действий

- Шаг 1** Выкрутите два винта в нижней части автономного контроллера доступа, затем снимите задний кронштейн.
- Шаг 2** По отверстиям в заднем кронштейне разметьте и просверлите 3 отверстия, затем вставьте в них дюбели (анкерные болты).
- 
- Просверлите одно отверстие в стене для вывода кабеля, если используется скрытая проводка.
- Шаг 3** Закрепите кронштейн на стене с помощью трёх винтов.
- 
- При наружной прокладке кабеля сначала пропустите провода через задний кронштейн, а затем закрепите кронштейн на стене.
- Шаг 4** Выполните подключение проводов автономного контроллера доступа. Подробную информацию см. в разделе «2.1 Подключение проводов».
- Шаг 5** Установите автономный контроллер доступа на кронштейн.
- Шаг 6** Надёжно затяните два винта в нижней части автономного контроллера доступа.

Рисунок 2-7 Настенный монтаж

Скрытая проводка

Наружная (открытая) проводка

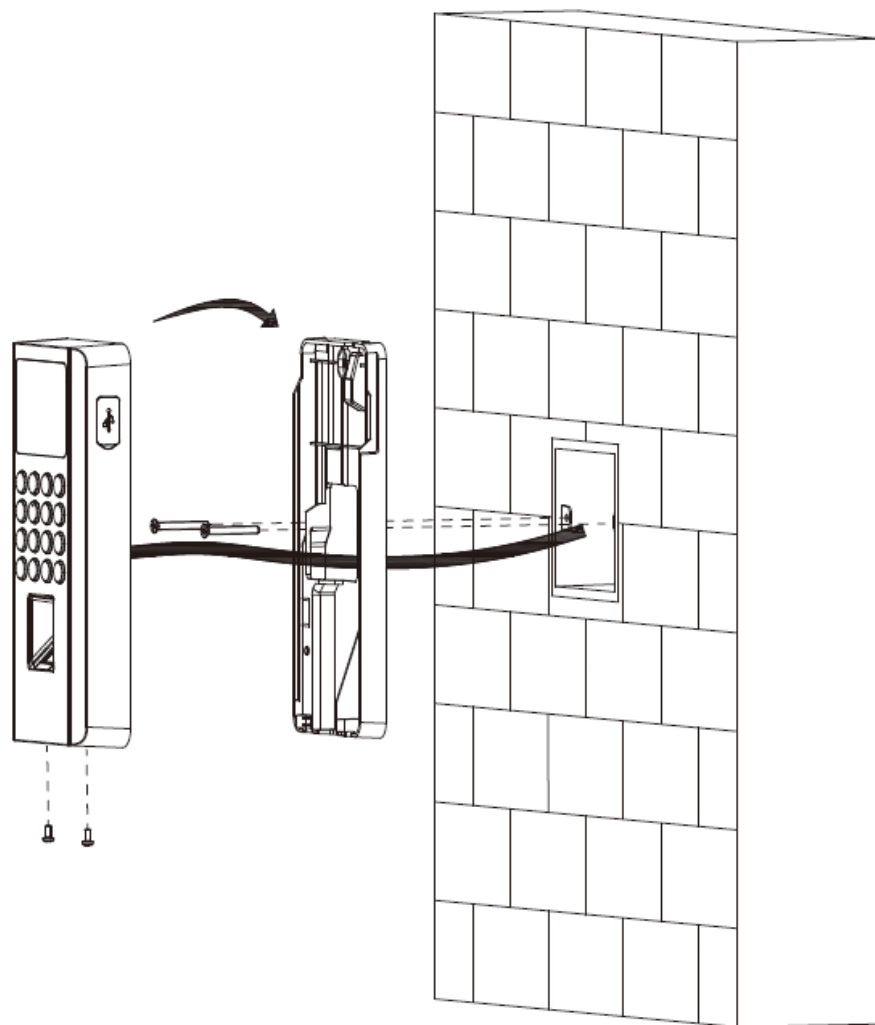


2.3.2 Установка на монтажную коробку 86 (подрозетник)

Порядок действий

- Шаг 1** Выкрутите два винта в нижней части автономного контроллера доступа, затем снимите задний кронштейн.
- Шаг 2** Установите в стену монтажную коробку 86 на подходящей высоте.
- Шаг 3** Закрепите кронштейн на коробке 86 с помощью двух винтов.
- Шаг 4** Подключите провода автономного контроллера доступа. Подробную информацию см. в разделе «2.1 Подключение проводов».
- Шаг 5** Установите автономный контроллер доступа на кронштейн.
- Шаг 6** Надёжно затяните два винта в нижней части автономного контроллера доступа.

Рисунок 2–8 Установка на монтажную коробку 86 (подрозетник)



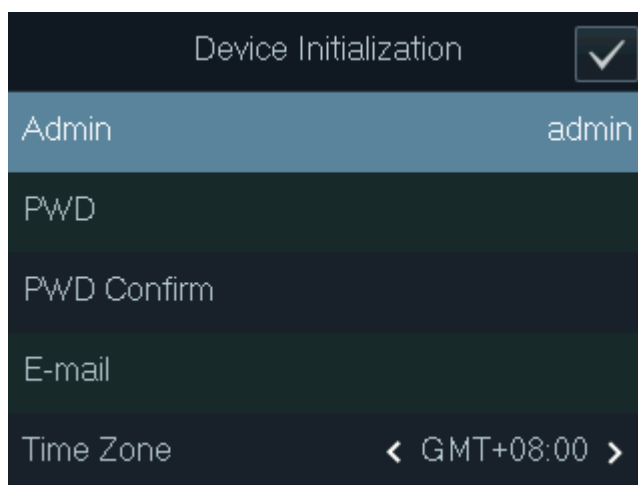
3 Локальные настройки

Локальные операции могут отличаться в зависимости от модели контроллера доступа.

3.1 Инициализация

При первом использовании или после восстановления заводских настроек необходимо задать пароль и адрес электронной почты для учётной записи администратора. Учётная запись администратора используется для входа в главное меню автономного контроллера доступа и его веб-страницу.

Рисунок 3–1 Инициализация



- Если вы забыли пароль администратора, отправьте запрос на сброс на связанный адрес электронной почты.
- Пароль должен содержать от 8 до 32 непробельных символов и включать как минимум два типа из следующих символов: прописные буквы, строчные буквы, цифры и специальные символы (за исключением ' " ; : &). Устанавливайте пароль с высокой степенью надёжности, следуя подсказкам по сложности пароля.

3.2 Добавление пользователей

Порядок действий

Шаг 1. На экране ожидания нажимайте $\wedge$ или $\vee$ для выбора , затем нажмите **ОК**.

Шаг 2. Войдите в систему с учётной записью администратора, затем выберите **Пользователи** (User) > **Новый пользователь** (New User).



Изображения экранов в данном руководстве приведены только для справки и могут отличаться от фактического вида продукта.

Рисунок 3–2 Добавление нового пользователя

New User(1/2)

User ID	1
Name	
FP	0
Card	0
PWD	

New User(2/2)

Permission	User >
Period	255-Default
Holiday Plan	255-Default
Valid Date	2037-12-31
User Type	General >

Шаг 3. Настройте параметры.

Таблица 3–1 Описание параметров пользователя

Параметр	Описание
ID (Идентификатор)	Каждый идентификатор пользователя уникален. Он может содержать до 18 символов, включая цифры, буквы или их комбинацию.
Name (Имя)	Укажите имя пользователя. Длина — не более 32 символов; допустимы цифры, буквы и специальные символы.
Fingerprint (Отпечаток пальца)	Каждый пользователь может добавить до 3 отпечатков пальцев. Следуйте инструкциям на экране и голосовым подсказкам для добавления отпечатков. Вы можете включить функцию тревожного отпечатка для каждого отпечатка. После включения функции тревожного отпечатка при открытии двери с помощью этого отпечатка будет инициирована тревога.  ● Не рекомендуется устанавливать первый отпечаток в качестве тревожного отпечатка. ● Функция отпечатка пальца поддерживается только моделями автономного контроллера доступа с биометрическим сканером (сенсором отпечатков).

Параметр	Описание
Card (Карта)	Вы можете зарегистрировать до 5 карт для каждого пользователя. На странице регистрации карт приложите карту к считывателю, и информация о карте будет считана устройством. На странице регистрации карт вы можете включить функцию тревожной карты. После включения функции тревожной карты при открытии двери с помощью этой карты будет инициирована тревога.
PWD (Пароль)	Введите пароль пользователя. Максимальная длина пароля — 8 цифр. Тревожный пароль формируется путём увеличения последней цифры пароля для разблокировки на 1. Например, если пароль пользователя — 12345, то тревожный пароль будет 12346; если пароль пользователя — 789, то тревожный пароль — 780. При использовании тревожного пароля для открытия двери будет инициирована тревога.
Permission (Права доступа)	Вы можете выбрать права доступа для нового пользователя. - Обычные пользователи имеют только разрешение на открытие двери. - Администраторы могут настраивать автономный контроллер доступа и открывать дверь.
Period (Временной интервал)	Права доступа пользователя действуют только в рамках заданного временного интервала. По умолчанию установлено значение 255 — период не задан (доступ разрешён всегда).
Holiday Plan (Расписание праздничных дней)	Доступ пользователя разрешён только в определённые праздничные дни согласно настроенному расписанию. По умолчанию установлено 255 — расписание праздничных дней не задано.
Valid Date (Срок действия)	Установите временной интервал действия прав доступа для данного пользователя.
User Type (Тип пользователя)	Обычный (General): Обычные пользователи могут открывать дверь в обычном режиме. Чёрный список (Block list): Когда пользователи из чёрного списка открывают дверь, обслуживающий персонал получает уведомление. Гость (Guest): Гости могут открывать дверь в течение определённого периода или ограниченное количество раз. После истечения срока действия или исчерпания количества открытий они не смогут открывать дверь. Патрульный (Patrol): Патрульные пользователи могут отслеживать свои отметки о присутствии, но не имеют разрешения на открытие двери. VIP: Когда VIP-пользователь открывает дверь, обслуживающий персонал получает уведомление. VIP-пользователь не ограничен режимами открытия, такими как «Несколько карт» или «Временные интервалы». Другие (Others): При открытии двери дверь остаётся открытой ещё на 5 секунд. Пользовательский 1/2 (Custom User 1/2): Аналогичны обычному пользователю (General).

Шаг 4. После настройки всех параметров нажмите **Esc**.

Шаг 5. Нажмите **OK** для сохранения изменений.

4 Веб-настройки

4.1 Инициализация

Перед первым входом в веб-интерфейс необходимо задать пароль и привязать адрес электронной почты.

Порядок действий

Шаг 1. Введите IP-адрес устройства в браузере (по умолчанию — 192.168.1.108).



Убедитесь, что компьютер находится в одной локальной сети (LAN) с устройством.

Рисунок 4–1 Инициализация

Boot Wizard

1 Device Initialization 2 Auto Check

Username admin

New Password

Low Medium High

Confirm Password

Password shall be at least 8 digits, and shall at least include two types, including number, letter and common character

☐ Bind Email

(It will be used to reset password. Please fill in or complete it timely)

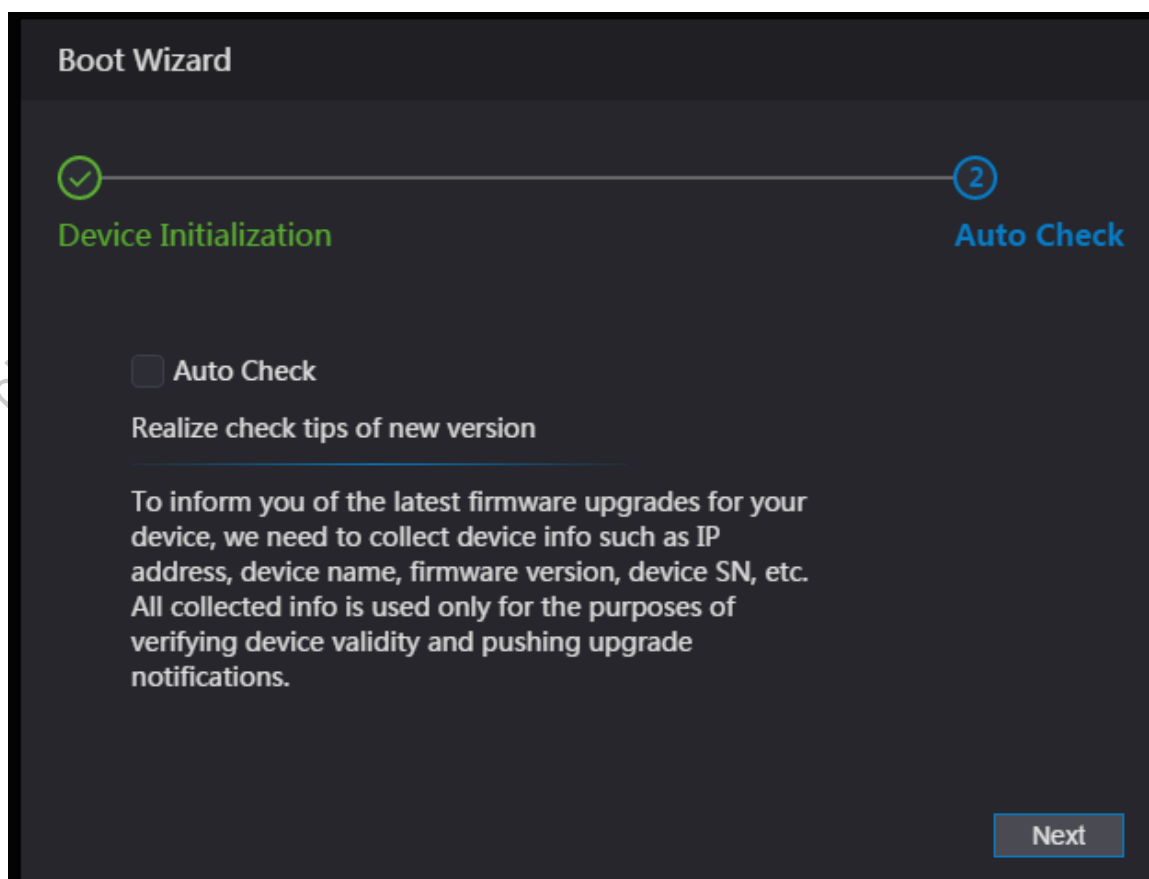
Next

Шаг 2. Введите новый пароль, подтвердите пароль, включите функцию **Привязать почту (Bind Email)**, укажите адрес электронной почты и нажмите **Далее (Next)**.



- Пароль должен содержать от 8 до 32 непробельных символов и включать как минимум два типа из следующих символов: прописные буквы, строчные буквы, цифры и специальные символы (за исключением ' " ; &). Устанавливайте пароль с высокой степенью надёжности, следуя подсказкам по сложности пароля.
- Сохраняйте пароль в надёжном месте после инициализации и регулярно меняйте его для повышения уровня безопасности.
- При необходимости сброса пароля администратора через сканирование QR-кода необходимо, чтобы на связанный адрес электронной почты был получен код подтверждения.

Рисунок 4–2 Автоматическая проверка



Шаг 3 Нажмите «Далее» (Next).

Шаг 4 (Опционально) Выберите «Автоматическая проверка» (Auto Check).



Рекомендуется включить «Автоматическую проверку», чтобы своевременно получать информацию о последней версии.

Шаг 5 Нажмите «Далее» (Next).

Шаг 6 Нажмите «Готово» (Complete).

4.2 Вход в систему

Порядок действий

Шаг 1 Введите IP-адрес автономного контроллера доступа в браузере (по умолчанию — **192.168.1.108**) и нажмите клавишу **Enter**.



Убедитесь, что компьютер находится в одной локальной сети (LAN) с автономным контроллером доступа.

Рисунок 4–3 Вход в систему

WEB SERVICE

Username:

Password:

Forget Password?

Login

Шаг 2. Введите **имя пользователя (user name)** и **пароль (password)**.



- Имя администратора по умолчанию — **admin**, пароль — тот, который вы задали при инициализации. Рекомендуется регулярно менять пароль администратора для повышения безопасности.
- Если вы забыли пароль администратора, нажмите «**Забыли пароль?**» (**Forget Password?**) для его сброса.

Шаг 3. Нажмите «**Войти**» (**Login**).

Приложение 1. Основные правила при добавлении отпечатков пальцев

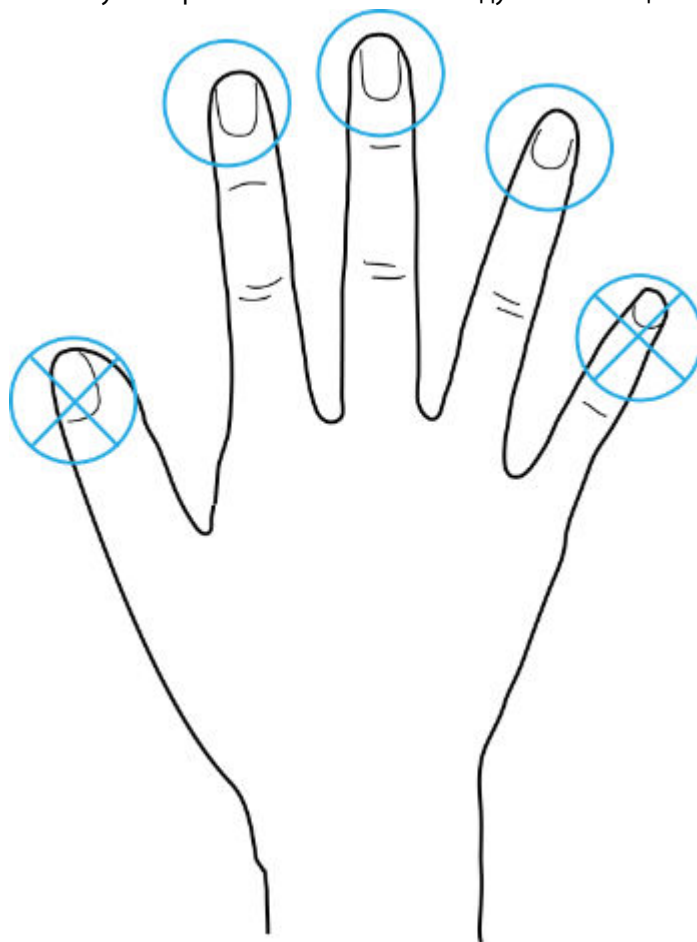
При регистрации отпечатка пальца обратите внимание на следующее:

- Убедитесь, что пальцы и поверхность сканера чистые и сухие.
- Прижимайте палец к центру сканера отпечатков пальцев.
- Не размещайте сканер отпечатков в местах с интенсивным освещением, высокой температурой и повышенной влажностью.
- Если ваши отпечатки пальцев нечёткие, используйте другие способы разблокировки.

Рекомендуемые пальцы

Рекомендуется использовать указательные, средние и безымянные пальцы. Большие пальцы и мизинцы сложнее правильно расположить в центре сканера при записи.

Рисунок Приложения 1–1 Рекомендуемые пальцы



Как правильно прикладывать палец к сканеру

Рисунок Приложения 1-2 Правильное расположение

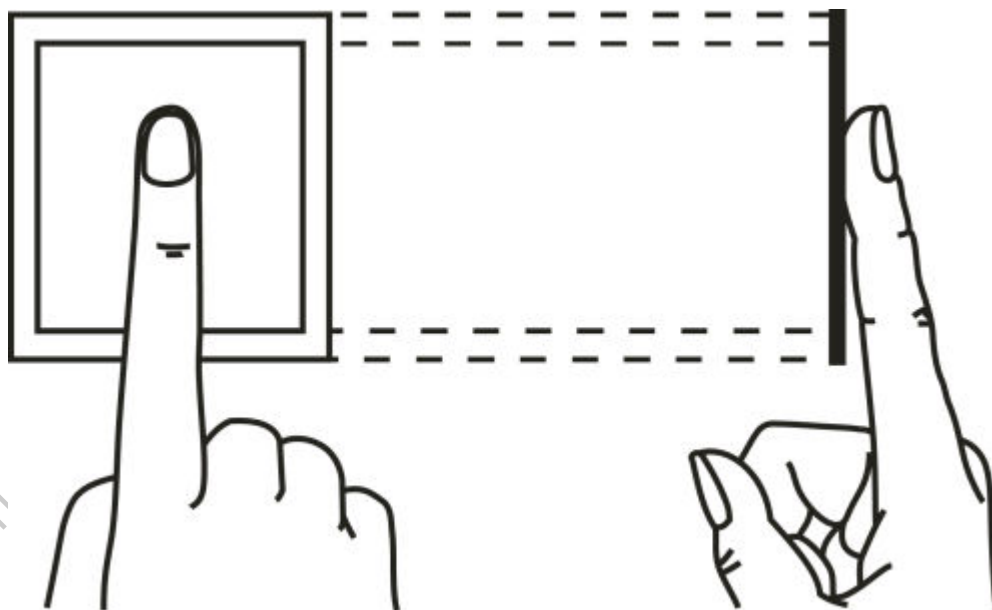
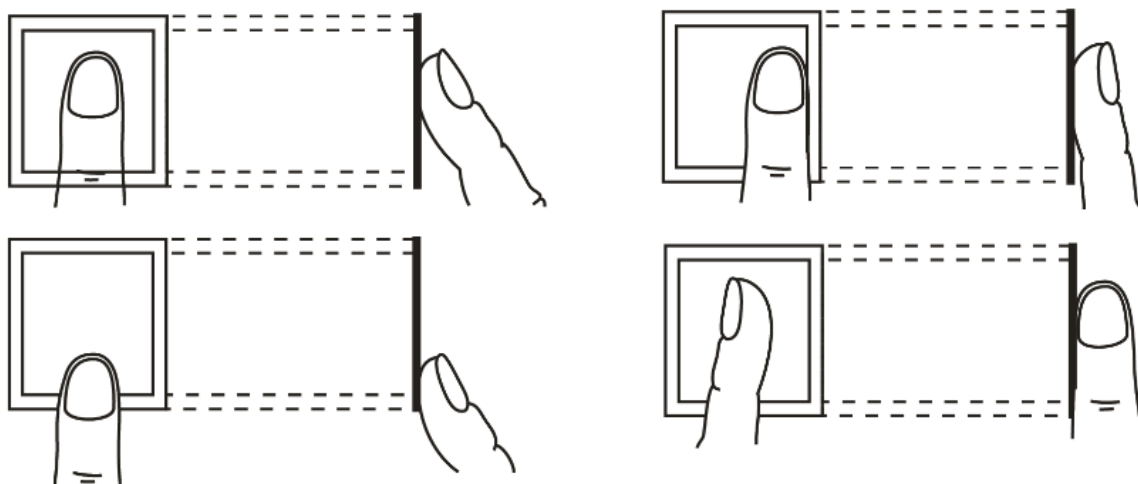


Рисунок Приложения 1-3 Неправильное расположение



Приложение 2. Рекомендации по кибербезопасности

Обязательные меры по обеспечению базовой сетевой безопасности устройства:

1. Используйте надёжные 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. Своевременно обновляйте встроенное ПО и клиентское программное обеспечение

- Согласно стандартной практике в индустрии, рекомендуется поддерживать прошивку вашего устройства (например, NVR, DVR, IP-камеры и т. д.) в актуальном состоянии, чтобы система имела последние обновления безопасности и исправления. При подключении устройства к публичной сети рекомендуется включить функцию «автоматической проверки обновлений» для своевременного получения информации о новых версиях прошивки от производителя.
- Рекомендуется загружать и использовать последнюю версию клиентского программного обеспечения.

Дополнительные рекомендации по повышению сетевой безопасности устройства:

1. Физическая защита

Рекомендуется обеспечить физическую защиту устройства, особенно накопителей данных. Например, разместите устройство в специальном серверном помещении и стойке, внедрите надёжный контроль доступа и управление ключами, чтобы предотвратить несанкционированный физический доступ (повреждение оборудования, подключение внешних устройств, таких как USB-флешки, последовательные порты и т. п.).

2. Регулярно меняйте пароли

Рекомендуется регулярно менять пароли для снижения риска их подбора или взлома.

3. Своевременно настраивайте и обновляйте информацию для сброса пароля

Устройство поддерживает функцию сброса пароля. Пожалуйста, своевременно настройте соответствующую информацию для сброса пароля, включая почтовый ящик конечного пользователя и контрольные вопросы. При изменении информации обновите её. При настройке контрольных вопросов рекомендуется не использовать вопросы, ответы на которые легко угадать.

4. Включите блокировку учётной записи

Функция блокировки учётной записи включена по умолчанию; рекомендуется оставить её включённой для обеспечения безопасности учётной записи. Если злоумышленник несколько раз пытается войти с неверным паролем, соответствующая учётная запись и IP-адрес источника будут заблокированы.

5. Измените порты HTTP и других служб по умолчанию

Рекомендуется изменить стандартные порты HTTP и других служб на любые числа в диапазоне 1024–65535, чтобы снизить риск угадывания используемых портов посторонними.

6. Включите HTTPS

Рекомендуется включить HTTPS, чтобы доступ к веб-сервису осуществлялся через защищённый канал связи.

7. Привязка MAC-адреса

Рекомендуется привязать IP- и MAC-адрес шлюза к устройству, чтобы снизить риск подмены ARP.

8. 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.

9. **Отключите неиспользуемые службы и выбирайте безопасные режимы**

Если они не нужны, рекомендуется отключить некоторые службы, такие как SNMP, SMTP, UPnP и другие, чтобы снизить риски.

При необходимости настоятельно рекомендуется использовать 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 надёжные пароли.
- **Точка доступа (AP hotspot):** Выберите режим шифрования WPA2-PSK и установите надёжный пароль.

10. **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.

Напоминание: шифрованная передача приводит к некоторой потере эффективности передачи.

11. **Безопасный аудит**

- **Проверка онлайн-пользователей:** рекомендуется регулярно проверять список подключённых пользователей, чтобы убедиться, что устройство не используется несанкционированно.
- **Проверка журнала устройства:** просматривая логи, вы можете узнать IP-адреса, с которых выполнялся вход в устройство, и ключевые операции.

12. **Сетевой журнал (логирование)**

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.

13. **Создание безопасной сетевой среды**

Для лучшего обеспечения безопасности устройства и снижения потенциальных киберрисков рекомендуется:

- Отключить функцию проброса портов на маршрутизаторе, чтобы избежать прямого доступа к устройствам внутренней сети из внешней сети.
- Выполнять сегментацию и изоляцию сети в соответствии с фактическими потребностями. Если между двумя подсетями нет необходимости в обмене данными, рекомендуется использовать VLAN, сетевые разрывы (GAP) и другие технологии для разделения сети с целью достижения изоляции.
- Внедрить систему аутентификации доступа 802.1x для снижения риска несанкционированного подключения к частным сетям.
- Включить фильтрацию IP/MAC-адресов для ограничения круга хостов, которым разрешён доступ к устройству.