

Серия ASI3204E / ASI3203E

Краткое руководство пользователя



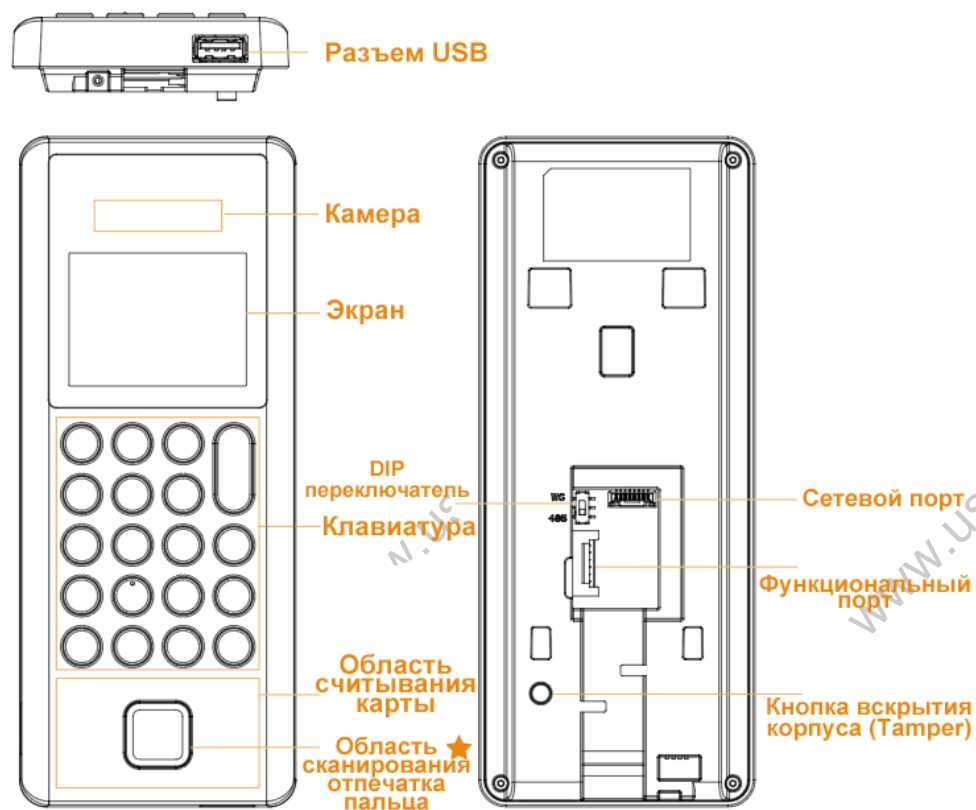
СОДЕРЖАНИЕ

1 Конструкция.....	1
2 Подключение и установка.....	2
2.1 Требования к установке.....	2
2.2 Подключение проводов.....	4
2.3 Порядок установки.....	6
3 Локальная конфигурация.....	8
3.1 Инициализация.....	8
3.2 Вход в систему.....	8
3.3 Добавление пользователей.....	9
4 Вход в веб-интерфейс.....	12
Приложение 1. Ключевые моменты регистрации лица.....	13
Приложение 2. Ключевые моменты инструкции по регистрации отпечатков пальцев.....	16
Приложение 3. Рекомендации по безопасности.....	18

1 КОНСТРУКЦИЯ

★ Указание означает, что функция доступна только в отдельных моделях.

Рис. 1-1 Конструкция



2. ПОДКЛЮЧЕНИЕ И УСТАНОВКА

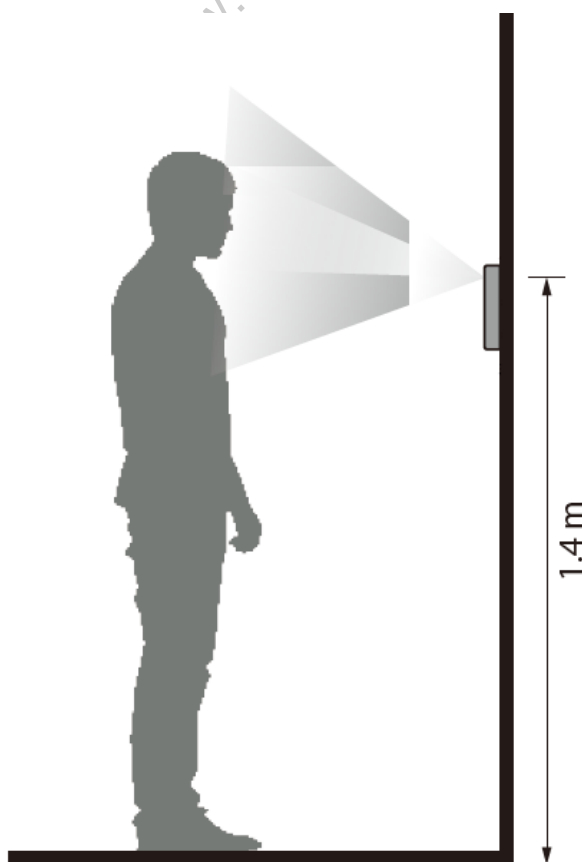
2.1 Требования к установке



- Рекомендуемая высота установки (от объектива до земли) — 1,4 м.
- Освещенность на расстоянии 0,5 метра от контроллера доступа должна быть не менее 100 Люкс.
- Рекомендуется устанавливать контроллер доступа внутри помещений, на расстоянии не менее 3 метров от окон и дверей и не менее 2 метров от источника света.
- Следует избегать условий контрового света, прямых солнечных лучей, близко расположенных и боковых источников света.

Высота установки

Рисунок 2-1 Требования к высоте установки



Требования к освещению

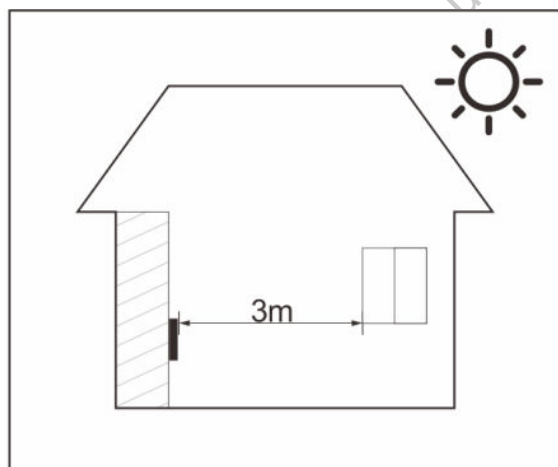
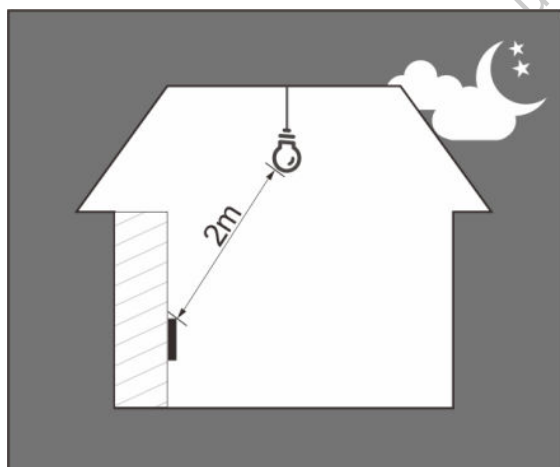
Рисунок 2-2 Требования к освещению



Свеча: 10 люкс Лампа накаливания: 100-850 люкс Солнечный свет: ≥ 1200 люкс

Рекомендуемое место установки

Рисунок 2-3 Рекомендуемое место установки



Нерекомендуемое место установки

Рисунок 2-4 Нерекомендуемое место установки



2.2 Подключение проводов

Комплектация портами может отличаться в зависимости от модели изделия.

- Провода **RS485A** и **WG_D0** объединены. Провода **RS485B** и **WG_D1** объединены.
- Когда DIP-переключатель установлен в положение **WG**, объединенные провода могут быть подключены к устройству с протоколом **Wiegand**. Когда DIP-переключатель установлен в положение **485**, объединенные провода могут быть подключены к устройству с протоколом **RS-485**.
- Если вы выбираете «**Door Control Module**» (Модуль управления дверью) через «**Communication Settings**» (Настройки связи) > «**RS-485 Config**» (Конфигурация RS-485), модуль безопасности управления дверью необходимо приобрести отдельно. Модуль безопасности требует отдельного источника питания.
- Когда функция модуля безопасности активирована, кнопка выхода, управление замком и тревожная сигнализация становятся неактивными.

Рисунок 2-5 Схема подключения

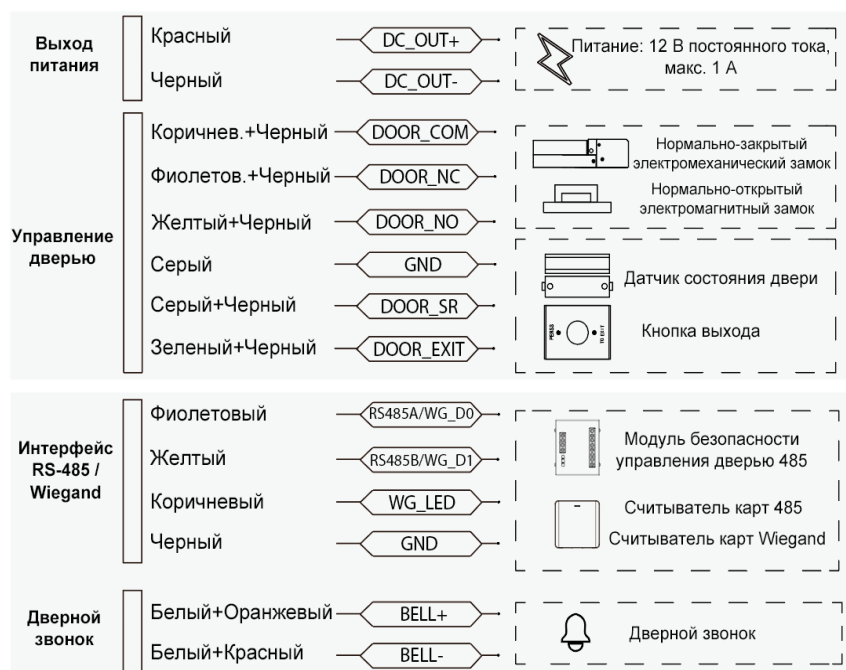


Рисунок 2-6 Схема подключения для стандартного устройства

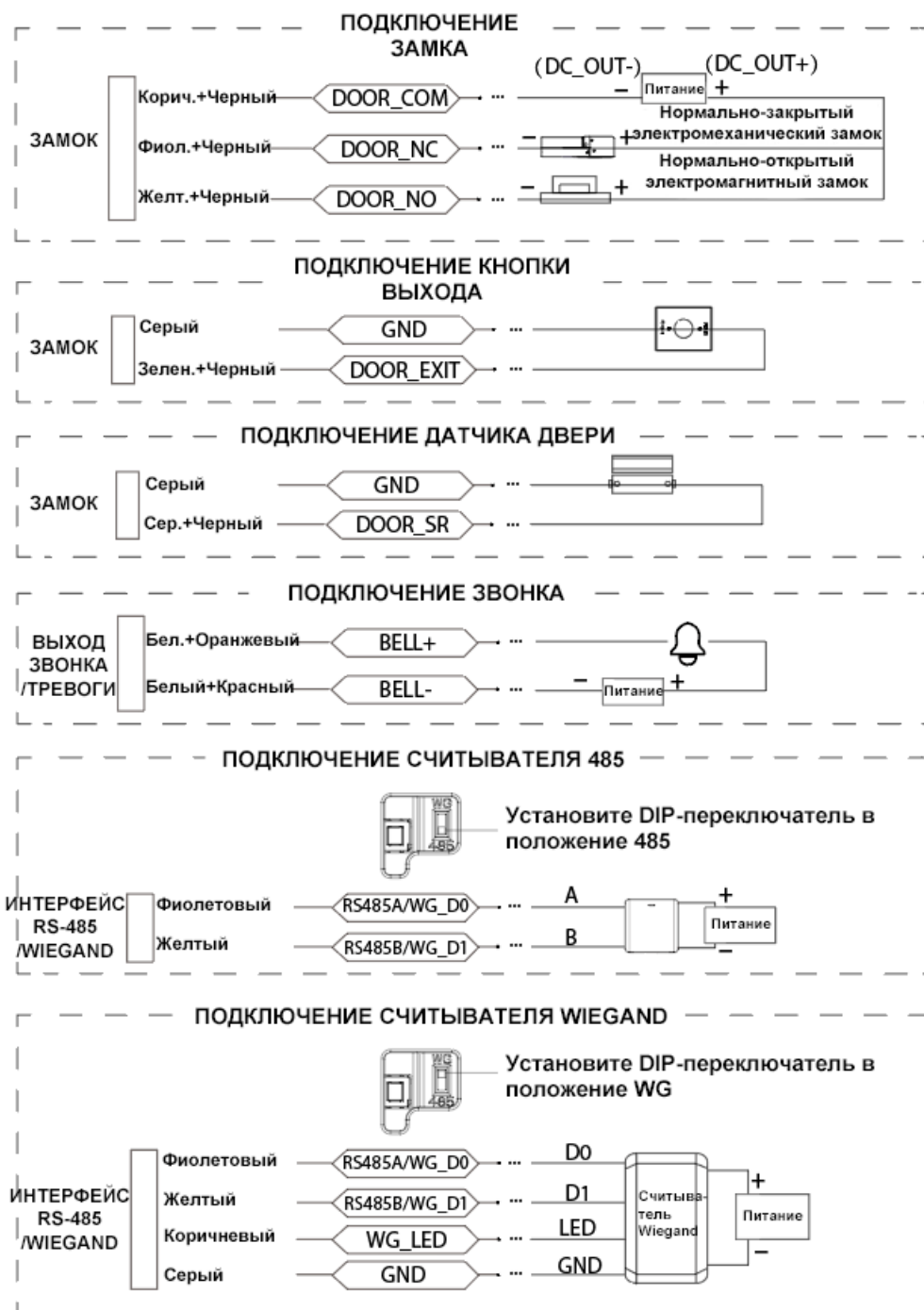
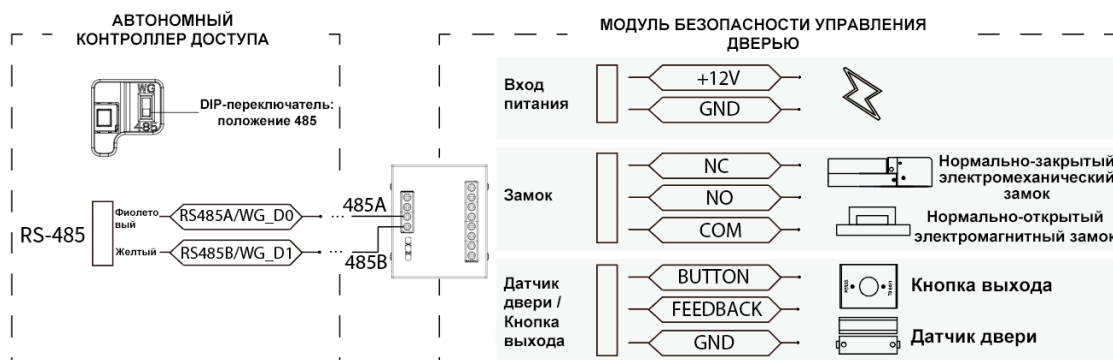


Рисунок 2-7 Схема подключения модуля безопасности управления дверью



2.3 Порядок установки

Устройство поддерживает настенный монтаж и предусматривает два способа прокладки проводов: внешний и скрытый (в стене).

Порядок монтажа

Шаг 1. По разметке монтажного кронштейна просверлите 6 отверстий и 1 канал для кабеля в стене.



Примечание: Канал в стене не требуется для наружной прокладки кабеля.

Шаг 2. Вставьте дюбели в отверстия и закрепите кронштейн на стене.

Шаг 3. Подключите кабели устройства. Подробности см. в разделе «2.2 Подключение».

- При скрытой прокладке пропустите кабель через заднюю панель и канал в стене.
- При наружной прокладке прокладка кабеля через заднюю панель не требуется.

Шаг 4. Установите устройство на кронштейн задней панели.

Шаг 5. Заверните винт в нижней части устройства.

Рисунок 2-8 Скрытая проводка



3 Локальная конфигурация

Процедура локальной настройки может отличаться в зависимости от модели контроллера доступа.

3.1 Инициализация

Справочная информация

При первом использовании или после сброса к заводским настройкам необходимо выбрать язык на контроллере доступа, а затем установить пароль и адрес электронной почты для учетной записи администратора. Учетная запись администратора предоставляет доступ к главному меню контроллера доступа и его веб-интерфейсу.

Порядок действий

Шаг 1. Выберите язык и нажмите клавишу **OK**.

Шаг 2. Нажмите  для выбора пункта **Enter Password** (Ввод пароля), затем нажмите **OK**.

Шаг 3. Задайте пароль и нажмите **OK**.

- Метод ввода по умолчанию - буквенный. Нажмите  чтобы переключиться на цифровой метод.
- Ввод букв: Нажмите клавишу с соответствующей буквой, а затем цифру для выбора нужной буквы. Например, чтобы ввести букву "а", необходимо нажать клавишу 2, а затем клавишу 1.



- Если вы забыли пароль администратора, отправьте запрос на сброс на свой зарегистрированный адрес электронной почты.
- Пароль должен состоять из 8–32 символов (не включая пробелы) и содержать как минимум два типа символов: заглавные буквы, строчные буквы, цифры и специальные символы (кроме ' " ; : &).

Шаг 4. Нажмите  для выбора пункта **Confirm Password** (Подтвердить пароль), затем нажмите **OK**.

Шаг 5. Повторите Шаг 3, введите тот же пароль и нажмите **OK**.

Шаг 6. Введите адрес электронной почты и выберите часовой пояс.

Шаг 7. Нажмите  для выбора , а затем нажмите **OK**.

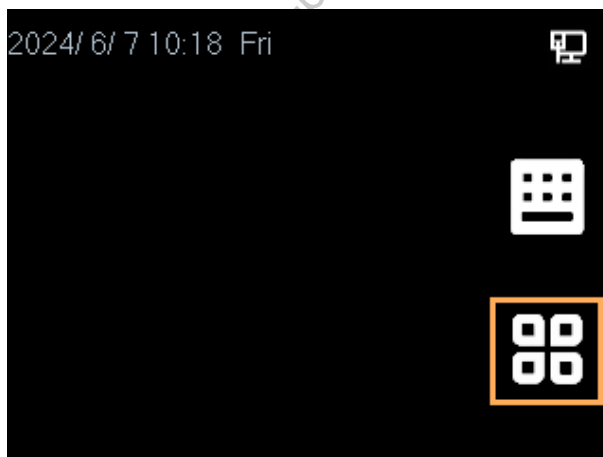
3.2 Вход в систему

Для настройки контроллера доступа выполните вход в главное меню. При первом использовании используйте учетную запись администратора для доступа к экрану главного меню, после чего вы сможете создать другие учетные записи администраторов.

Порядок действий

Шаг 1. Нажмите  или  для выбора , а затем нажмите **OK**.

Рисунок 3-1 Главный экран



Шаг 2. Нажмите , , или для выбора учетной записи "**Admin**", затем нажмите **OK**.

Шаг 3. Нажмите **OK**, а затем введите пароль, заданный во время первоначальной настройки.

Шаг 4. Нажмите или для выбора "**OK**", затем нажмите **OK**.

3.3 Добавление пользователей

Порядок действий

Шаг 1. В **Main Menu** (Главное меню), выбрать **Users** (Пользователи) > **Create User** (Создать пользователя).

Шаг 2. Настройте параметры в интерфейсе.

Рисунок 3-2 Добавление пользователя

Create User(1/3)		Create User(2/3)		Create User(3/3)	
No.	3	Password		User Type	General User >
Name		User Permission	User >	Department	1-Default
Fingerprint	0	Period	255-Default	Schedule Mode	apartment Schedule
Face	0	Holiday Plan	255-Default		
Card	0	Validity Period	2037-12-31		

Таблица 3-1 Описание параметров

Параметр	Описание
No. (номер)	Номер (например, табельный номер) может состоять из цифр, букв и их комбинаций. Максимальная длина номера — 32 символа.
Name (имя)	Имя может содержать до 30 символов (включая цифры, символы и буквы).

Параметр	Описание
Fingerprint (Отпечаток пальца)	Регистрация отпечатка пальцев. Пользователь может зарегистрировать до 3 отпечатков, один из которых можно установить как "тревожный". При использовании "тревожного" отпечатка для разблокировки двери будет активирована сигнализация.  ● Функция распознавания отпечатков пальцев доступна только в отдельных моделях. ● Не рекомендуется устанавливать первый отпечаток в качестве "тревожного". ● Один пользователь - один "тревожный" отпечаток. ● Функция доступна, если контроллер поддерживает модуль для считывания отпечатков пальцев.
Face (Лицо)	Расположите лицо в пределах рамки, и изображение будет захвачено автоматически. Если результат вас не устраивает, вы можете пройти регистрацию повторно.
Card (Карта)	Один пользователь может зарегистрировать не более 5 карт. Введите номер карты или проведите картой, после чего контроллер доступа считывает информацию с карты. Вы можете активировать функцию Duress Card (Тревожная карта). При использовании тревожной карты для разблокировки двери будет активирована сигнализация.  Один пользователь - только одна тревожная карта.
Password (Пароль)	Введите пароль пользователя. Максимальная длина пароля — 8 цифр. "Тревожный" пароль формируется как пароль для разблокировки + 1. Например, если пароль пользователя — 12345, то "тревожный" пароль будет 12346. При использовании "тревожного" пароля для разблокировки двери будет активирована сигнализация.
User Permission (Права доступа пользователя)	● Пользователь: Пользователи имеют только разрешения на доступ через дверь или учет рабочего времени. ● Администратор: Админы могут настраивать контроллер доступа, помимо разрешений на доступ через дверь и учет рабочего времени.
Period (Период)	Люди могут открывать дверь или отмечать посещаемость в течение заданного периода.
Holiday Plan (План праздников)	Люди могут открывать дверь или отмечать посещаемость в течение заданного праздничного дня.
Validity Period (Срок действия)	Установите дату, по истечении которой права доступа и учета посещаемости для человека будут аннулированы.

Параметр	Описание
User Type (Тип пользователя)	● Обычный пользователь: Может открывать дверь. ● Пользователь в черном списке: При попытке открыть дверь пользователем из черного списка активируется соответствующая сигнализация. ● Гостевой пользователь: Может открывать дверь в течение заданного периода или ограниченное количество раз. По истечении срока или исчерпания попыток доступ блокируется. ● Патрульный пользователь: Может отмечать посещаемость на контроллере, но не имеет права открывать дверь. ● VIP-пользователь: При открытии двери VIP-пользователем обслуживающий персонал получает уведомление. ● Другой пользователь: При открытии двери этим типом пользователя дверь остается разблокированной на 5 секунд дольше.s.  Задержка по времени не применяется при использовании методов удаленной верификации. ● Пользователь 1/Пользователь 2 (настраиваемые): Аналогичны обычным пользователям.
Department (Подразделение)	Выберите подразделения. Это полезно при настройке графиков подразделений.  Данная функция доступна только в отдельных моделях.
Schedule Mode (Режим графика)	● График подразделения: Применить к пользователю графики, установленные для его подразделения. ● Личный график: Применить к пользователю индивидуально настроенные графики.  ◇ Данная функция доступна только в отдельных моделях. ◇ Если вы установите здесь режим графика как «График подразделения», то личный график, настроенный для этого пользователя в Attendance (Учет времени) > Schedule Config (Настройка графиков) > Personal Schedule (Личный график) станет недействительным.

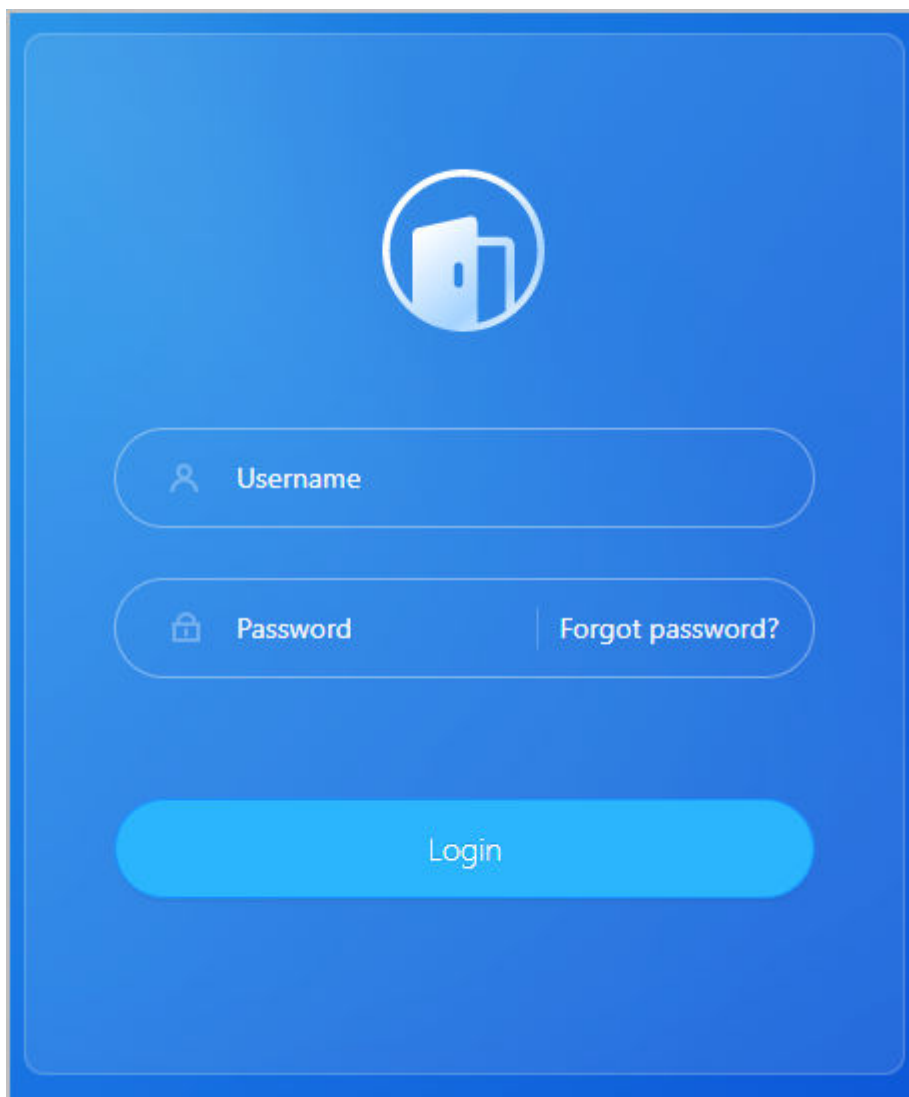
Шаг 3. Нажмите клавишу **Esc**, а затем нажмите **OK** для сохранения настроек.

4 Вход в веб-интерфейс

Порядок действий

Шаг 1. Откройте браузер, введите IP-адрес контроллера доступа в **Address** (адресную строку) и нажмите клавишу Enter.

Рисунок 4-1 Вход в систему



Шаг 2. Введите имя пользователя и пароль.



- Имя администратора по умолчанию — **admin**, а пароль — тот, который был установлен во время первоначальной настройки. Рекомендуется регулярно менять пароль администратора для повышения безопасности.
- Если вы забыли пароль администратора, нажмите **Forget password?** (Забыли пароль?) Подробности см. в соответствующем руководстве пользователя.

Шаг 3. Нажмите **Login** (Вход).

Приложение 1. Ключевые моменты регистрации лица

Перед регистрацией

- Очки, головные уборы и борода могут влиять на эффективность распознавания лиц.
- При ношении головного убора не закрывайте брови.
- Если вы используете устройство, не меняйте кардинально стиль бороды; в противном случае распознавание лица может оказаться неудачным.
- Следите за чистотой лица.
- Располагайте устройство на расстоянии не менее 2 метров от источника света и не менее 3 метров от окон или дверей; в противном случае контровой свет и прямые солнечные лучи могут повлиять на эффективность распознавания лиц контроллером доступа.

Во время регистрации

- Регистрацию лиц можно проводить через Устройство или через платформу. Инструкции по регистрации через платформу приведены в руководстве пользователя платформы.
- Расположите голову по центру рамки захвата изображения. Изображение лица будет захвачено автоматически.



- Не двигайте головой и не раскачивайтесь, иначе регистрация может завершиться неудачно.
- Не допускайте одновременного появления двух лиц в рамке захвата изображения.

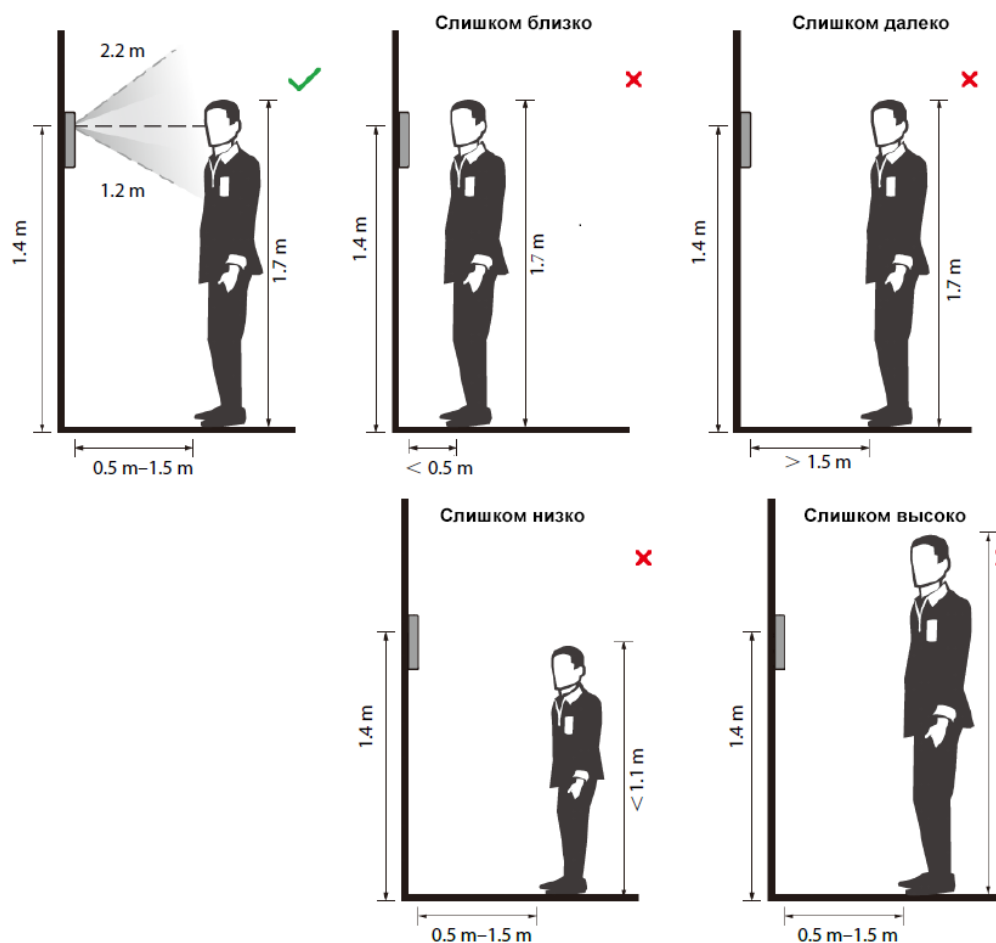
Положение лица

Если ваше лицо находится в неподходящем положении, точность распознавания может снизиться.



Положение лица, приведенное ниже, показано только для справки и может отличаться от реальной ситуации.

Рисунок Приложения 1-1 Правильное положение лица



Требования к изображениям лиц

- Убедитесь, что лицо чистое, а лоб не закрыт волосами.
- Не надевайте маски, очки, головные уборы, не отращивайте густую бороду и не используйте другие аксессуары, которые могут повлиять на запись изображения лица.
- Глаза должны быть открыты, сохраняйте нейтральное выражение лица и смотрите прямо в центр камеры.
- Во время записи лица или его распознавания не надевайте маску, не приближайте лицо слишком близко к камере и не отдаляйте его слишком далеко.

Рисунок Приложения 1-2 Положение головы



Рисунок Приложения 1-3 Расстояние до лица

Правильно



Слишком
близко



Слишком
далеко



- При импорте изображений лиц через платформу управления убедитесь, что разрешение изображения находится в диапазоне **от 150 × 300 пикселей до 600 × 1200 пикселей**. Рекомендуется, чтобы разрешение было **не менее 500 × 500 пикселей**, размер файла — **менее 100 КБ**, а имя файла изображения совпадало с идентификатором человека.
- Убедитесь, что лицо занимает **более 1/3, но не более 2/3** общей площади изображения, а соотношение сторон не превышает **1:2**.

Приложение 2. Ключевые моменты инструкции по регистрации отпечатков пальцев

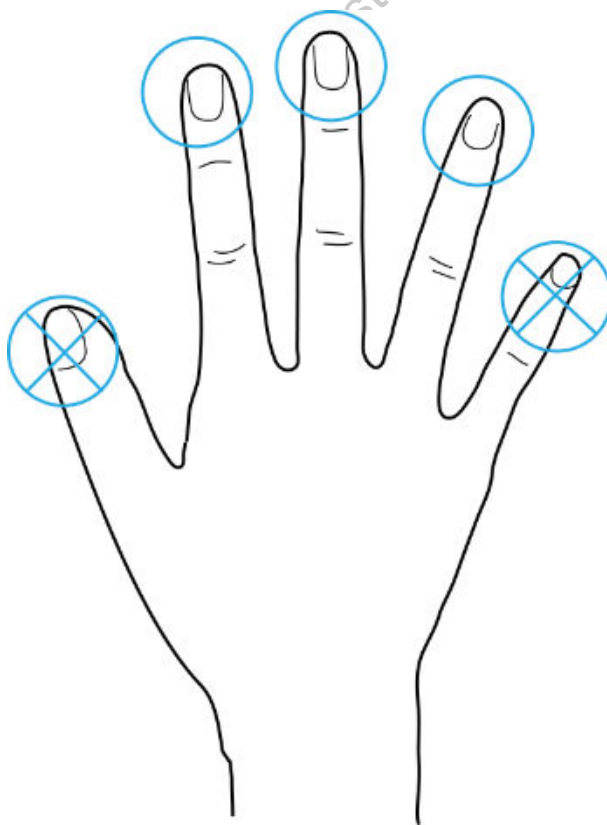
При регистрации отпечатка пальца обратите внимание на следующие моменты:

- Убедитесь, что ваши пальцы и поверхность сканера чистые и сухие.
- Прикладывайте палец к центру сканера отпечатков пальцев.
- Не размещайте датчик отпечатков пальцев в местах с интенсивным освещением, высокой температурой и влажностью.
- Если ваши отпечатки пальцев нечеткие, используйте другие методы разблокировки.

Рекомендуемые пальцы

Рекомендуется использовать указательные, средние и безымянные пальцы. Большие пальцы и мизинцы сложно правильно разместить в центре зоны сканирования.

Рисунок Приложения 2-1 Рекомендуемые пальцы



Как правильно прикладывать палец к сканеру

Рисунок Приложения 2-2 Правильное расположение

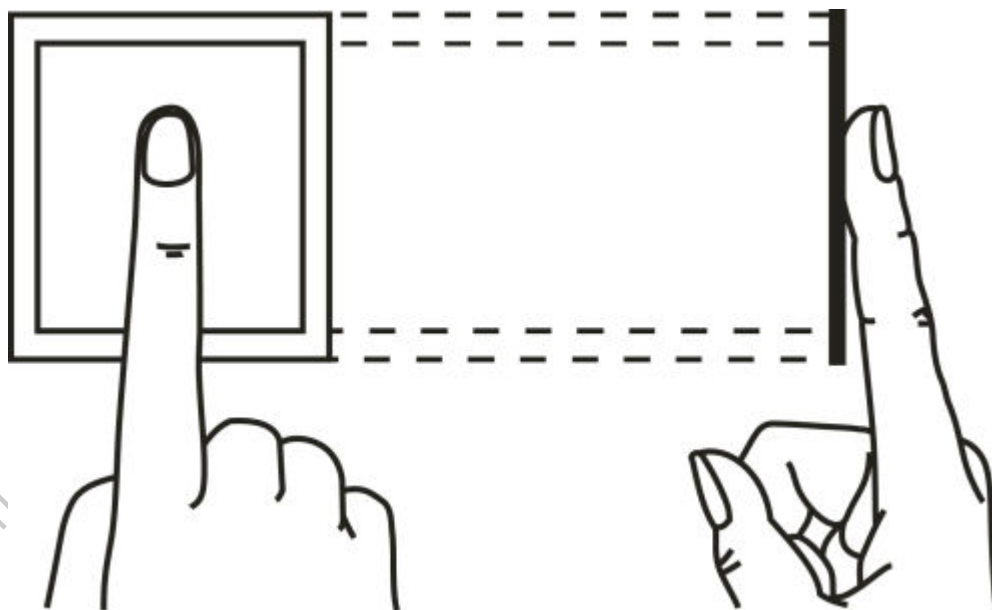
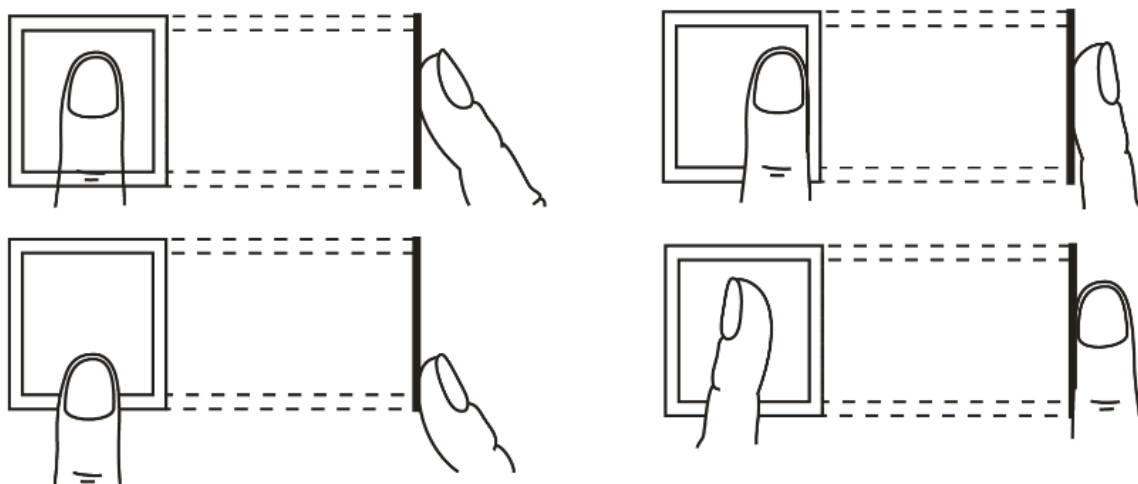


Рисунок Приложения 2-3 Неправильное расположение



Приложение 3. Рекомендации по безопасности

Управление учетными записями

1. Используйте сложные пароли

При установке пароля рекомендуется следовать следующим правилам:

- 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 его запись 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 изменять пароль устройства, чтобы снизить риск его угадывания или взлома.

3. Рационально распределяйте учетные записи и права доступа

Добавляйте пользователей в соответствии с операционными и управленческими потребностями и назначайте им минимально необходимые наборы прав.

4. Активируйте функцию блокировки учетной записи

Функция блокировки учетной записи включена по умолчанию. Рекомендуется сохранить её 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, при любом изменении информации своевременно её обновляйте. При настройке контрольных вопросов рекомендуется не использовать ответы, которые легко угадать.

Конфигурация служб

1. Активация HTTPS

Рекомендуется включить протокол HTTPS для доступа к веб-сервисам через безопасное соединение.

2. Шифрование передачи аудио и видео

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

3. Отключение неиспользуемых служб и использование безопасных режимов

Если некоторые службы (такие как SSH, SNMP, SMTP, UPnP, точка доступа AP и др.) не требуются, рекомендуется их отключить, чтобы сократить поверхность атаки.

4. При необходимости настоятельно рекомендуется выбирать безопасные режимы, включая, но не ограничиваясь следующими службами:

- **SNMP:** Выбирайте версию SNMP v3 и настраивайте надежные пароли шифрования и аутентификации.
- **SMTP:** Используйте TLS для подключения к почтовому серверу.
- **FTP:** Выбирайте SFTP и устанавливайте сложные пароли.
- **Точка доступа AP:** Выбирайте режим шифрования WPA2-PSK и настраивайте сложные пароли.

5. Изменение портов HTTP и других служб по умолчанию

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

Сетевая настройка

1. Активация белого списка

Рекомендуется включить функцию белого списка и разрешить доступ к устройству только IP-адресам, внесенным в этот список. Обязательно добавьте в белый список IP-адрес вашего компьютера и поддерживаемых устройств.

2. Привязка MAC-адресов

Рекомендуется выполнить привязку IP-адреса шлюза к его MAC-адресу на устройстве, чтобы снизить риск ARP-спуфинга.

3. Создание безопасной сетевой среды

Для обеспечения повышенной безопасности устройств и снижения потенциальных сетевых рисков рекомендуется:

- Отключить функцию проброса портов (port mapping) на маршрутизаторе, чтобы исключить прямой доступ к устройствам внутренней сети из внешней сети;
- В соответствии с фактическими сетевыми потребностями сегментировать сеть: если между двумя подсетями не требуется обмен данными, рекомендуется использовать VLAN, шлюзы и другие методы для разделения сети и обеспечения её изоляции;
- Настроить систему контроля доступа 802.1x для снижения риска несанкционированного доступа терминалов в частную сеть.

Аудит безопасности

1. Проверка пользователей в сети

Рекомендуется регулярно проверять список активных пользователей для выявления несанкционированных подключений.

2. Просмотр журналов устройства

Анализ журналов позволяет отслеживать IP-адреса, с которых выполнялись попытки входа на устройство, а также ключевые действия авторизованных пользователей.

3. Настройка сетевого журналирования

Из-за ограниченного объема памяти устройства количество хранимых локально журналов ограничено. При необходимости длительного сохранения логов рекомендуется активировать функцию отправки журналов на сетевой сервер. Это обеспечит синхронизацию критически важных записей для последующего анализа и отслеживания событий.

Безопасность программного обеспечения

1. Своевременное обновление прошивки

В соответствии с отраслевыми стандартами эксплуатации прошивку устройств необходимо своевременно обновлять до последней версии, чтобы обеспечить наличие новейших функций и исправлений уязвимостей. Если устройство подключено к публичной сети, рекомендуется включить функцию автоматической проверки онлайн-обновлений для своевременного получения информации о выходящих обновлениях прошивки от производителя.

2. Своевременное обновление клиентского программного обеспечения

It is recommended to download and use the latest client software.

Физическая защита

Рекомендуется обеспечить физическую защиту устройств (особенно устройств хранения данных). Например, размещайте оборудование в специальных серверных комнатах и стойках, организуйте контроль доступа и управление ключами, чтобы предотвратить повреждение оборудования и периферийных устройств (таких как USB-накопители, последовательные порты) несанкционированным персоналом.