

# Контроллер доступа с функцией распознавания лиц

Краткое руководство пользователя


**V1.0.0**

## Общие сведения

В данном руководстве описаны процедуры установки и основные операции с контроллером доступа с функцией распознавания лиц (далее – «контроллер доступа»).

## Инструкции по технике безопасности

В руководстве могут встречаться следующие разделенные на категории условные обозначения с определенным значением.

Условное обозначение	Значение
 <b>ПРИМЕЧАНИЕ</b>	Дополнительная информация, служащая для акцентирования внимания на тексте.

## История редакций

Версия	Содержание редакции	Дата выпуска
V1.0.0	Первый выпуск	Август 2019 года

## О руководстве

- Данное руководство используется только для ознакомления. В случае несоответствия между руководством и фактическим продуктом, последний имеет решающее значение.
- Мы не несем ответственности за какие-либо убытки, вызванные действиями, несоответствующими руководству.
- Руководство обновляется в соответствии с актуальным законодательством в соответствующих регионах. Более подробную информацию см. в бумажном руководстве пользователя, на компакт-диске, на нашем официальном вебсайте или с помощью QR-кода. При наличии несоответствий между руководством пользователя в бумажном формате и электронной версией, электронная версия имеет решающее значение.
- Любой дизайн и программное обеспечение могут быть изменены без предварительного письменного уведомления. Обновления продукта могут вызвать некоторые различия между фактическим продуктом и руководством. Чтобы получить последнее программное обеспечение или дополнительную документацию, свяжитесь со службой поддержки.
- Возможны отклонения в отношении технических данных, функций и описании операций, а также опечатки. При наличии каких-либо сомнений или разногласий, обратитесь к нам за окончательным разъяснением.
- Обновите программное обеспечение для чтения или используйте другое общедоступное программное обеспечение, если руководство (в формате PDF) невозможно открыть.
- Все торговые знаки и зарегистрированные торговые марки, упоминаемые в данном документе, являются собственностью соответствующих правообладателей.
- При возникновении каких-либо проблем в процессе эксплуатации устройства, посетите наш вебсайт, свяжитесь с поставщиком или службой поддержки.
- При наличии каких-либо сомнений или разногласий, обратитесь к нам за окончательным разъяснением.

# Важные меры предосторожности и предупреждения

Данная глава охватывает правильное обращение с контроллером доступа, информация о предотвращении опасности и порчи имущества. Перед тем, как приступить к эксплуатации контроллера доступа, внимательно изучите данные указания, следуйте им при работе и сохраните их, чтобы можно было обратиться к ним в будущем.

## Требования к эксплуатации

- Не размещайте и не устанавливайте контроллер доступа в местах, подверженных воздействию прямых солнечных лучей или вблизи отопительных приборов.
- Не устанавливайте контроллер доступа на влажном, пыльном, или покрытом копотью месте.
- Удерживайте контроллер доступа в горизонтальном положении на устойчивой поверхности, чтобы избежать его падения.
- Не подвергайте контроллер доступа воздействию каким-либо жидкостей; не ставьте на него какие-либо предметы, наполненные жидкостью, чтобы предотвратить попадание жидкости внутрь контроллера доступа.
- Устанавливайте контроллер доступа в местах с хорошей вентиляцией; не перекрывайте вентиляционные отверстия.
- Используйте контроллер доступа только в пределах номинального диапазона входа и выхода питания.
- Не разбирайте контроллер доступа.
- Транспортировка, эксплуатация и хранение контроллера доступа должны осуществляться при допустимой влажности и температуре.

## Требования к электропитанию

- Неправильное обращение с аккумулятором может привести к возгоранию или взрыву.
- При замене используйте аккумуляторы одного типа.
- Используйте рекомендуемые для вашего региона кабели питания, соответствующие номинальным спецификациям.
- Используйте адаптер питания, идущий в комплекте с контроллером доступа; в противном случае возможно травмирование и повреждение устройства.
- Источник питания должен соответствовать требованиям стандарта безопасного сверхнизкого напряжения (SELV) и должен иметь номинальное напряжение, соответствующее требованиям к ограниченным источникам питания по IEC60950-1. Обратите внимание на то, что требования к электропитанию указываются в маркировке устройства.
- Подключайте устройство (с категорией конструкции I) к сетевым розеткам с защитным заземлением.
- Приборный соединитель является разъединяющим устройством. При обычной эксплуатации используйте угол, облегчающий работу.

# Содержание

<b>Введение .....</b>	<b>I</b>
<b>Важные меры предосторожности и предупреждения .....</b>	<b>II</b>
<b>1 Размеры и компоненты .....</b>	<b>1</b>
<b>2 Установка .....</b>	<b>5</b>
2.1 Примечания по установке.....	5
2.2 Подключение кабелей.....	7
2.3 Установка .....	7
<b>3 Работа в системе .....</b>	<b>9</b>
3.1 Инициализация.....	9
3.2 Добавление новых пользователей .....	9
<b>4 Работа с веб интерфейсом .....</b>	<b>12</b>
<b>Приложение 1 Примечания по записи изображений лиц.....</b>	<b>13</b>
<b>Приложение 2 Инструкции по записи отпечатков пальцев.....</b>	<b>17</b>
<b>Приложение 3 Рекомендации по кибербезопасности .....</b>	<b>19</b>

# 1 Размеры и компоненты

Существует два типа контроллеров доступа: 7-дюймовые и 10-дюймовые. См. рисунок 1-1 и рисунок 1-2.

## 7-дюймовый контроллер доступа

Рисунок 1-1 Размеры и компоненты (1) (мм [дюймы])

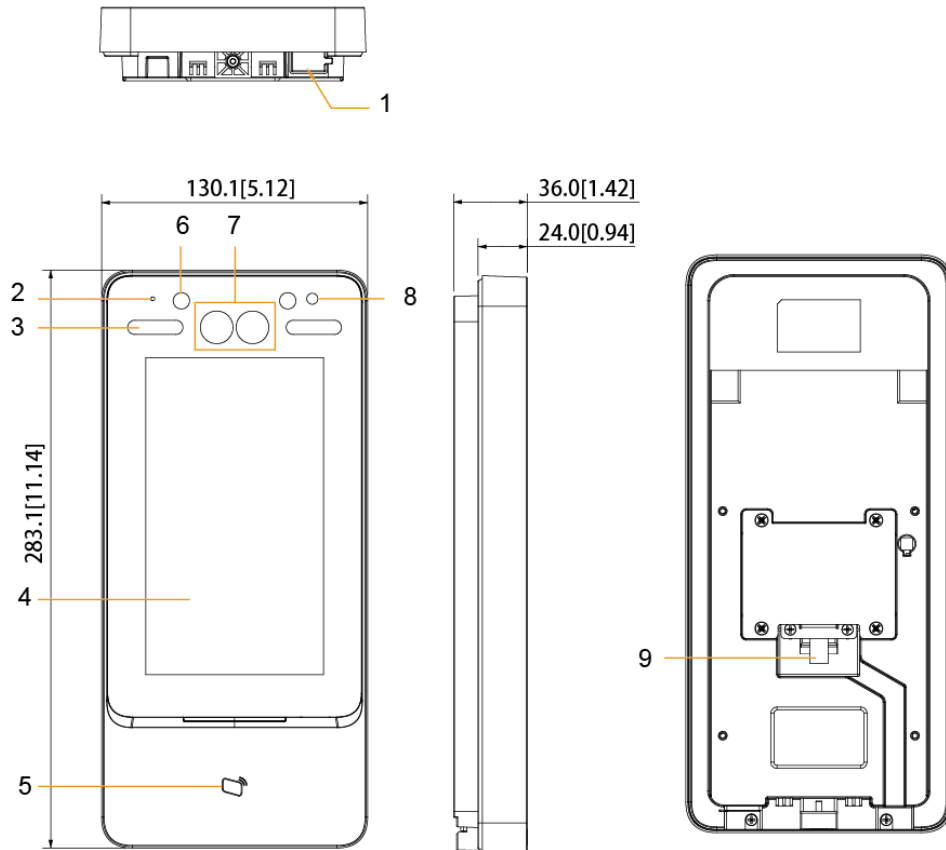


Таблица 1-1 Описание компонентов (1)

№	Название	№	Название
1	USB-порт	6	ИК-светодиод
2	Микрофон	7	Двойная камера
3	Источник белого света	8	Фототранзистор
4	Дисплей	9	Вход кабеля
5	Место сканирования карт	10	–

Рисунок 1-2 Размеры и компоненты (2) (мм [дюймы])

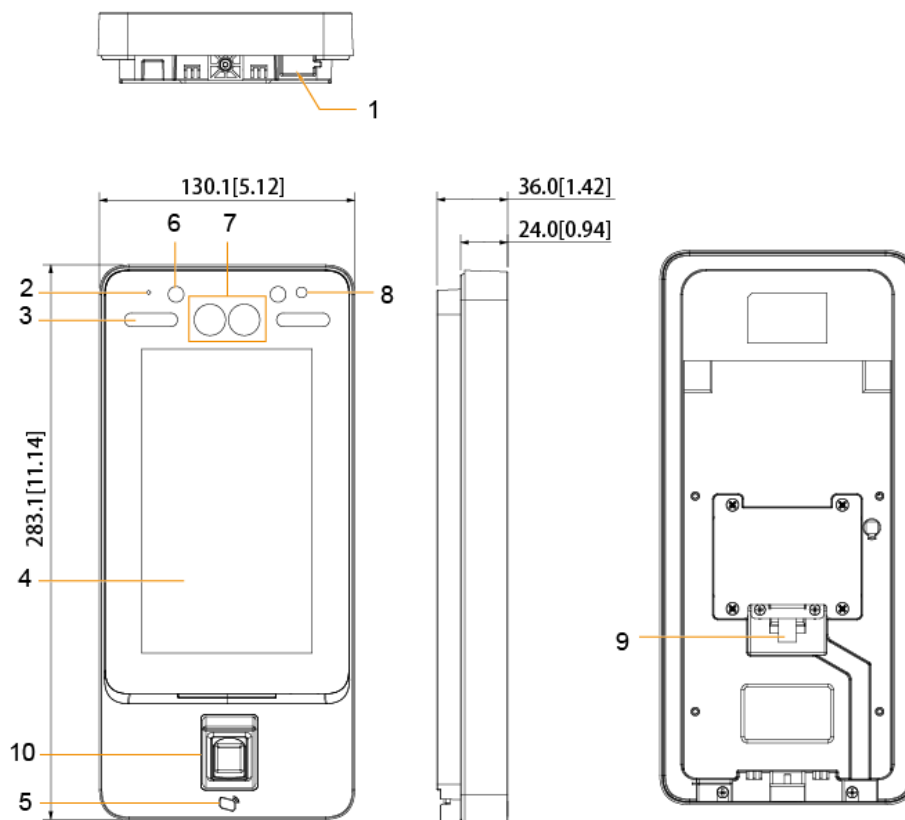


Таблица 1-2 Описание компонентов (2)

№	Название	№	Название
1	USB-порт	6	ИК-светодиод
2	Микрофон	7	Двойная камера
3	Источник белого света	8	Фототранзистор
4	Дисплей	9	Вход кабеля
5	Место сканирования карт	10	Сенсор отпечатков пальцев

10-дюймовый контроллер доступа

Рисунок 1-3 Размеры и компоненты (3) (мм [дюймы])

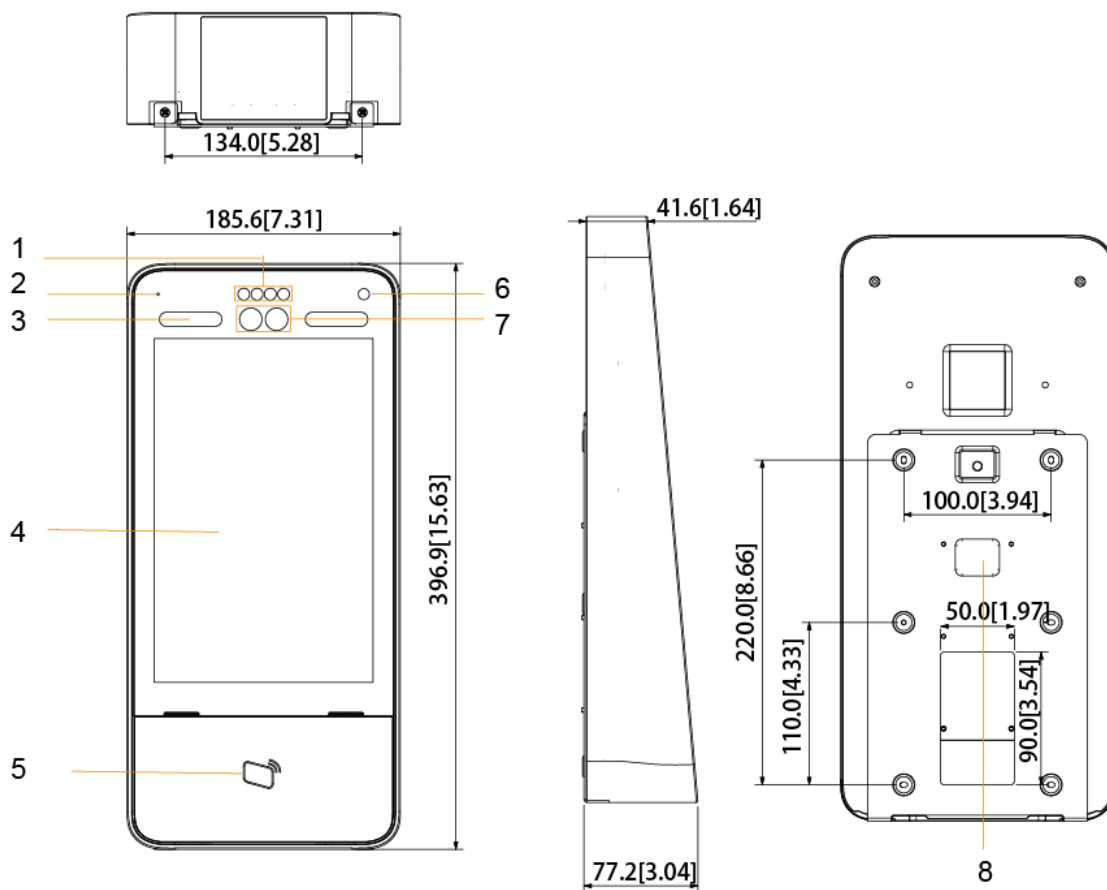


Таблица 1-3 Описание компонентов (3)

№	Название	№	Название
1	ИК-светодиод	6	Фототранзистор
2	Микрофон	7	Двойная камера
3	Источник белого света	8	Вход кабеля
4	Дисплей	9	–
5	Место сканирования карт	10	–

Рисунок 1-4 Размеры и компоненты (4) (мм [дюймы])

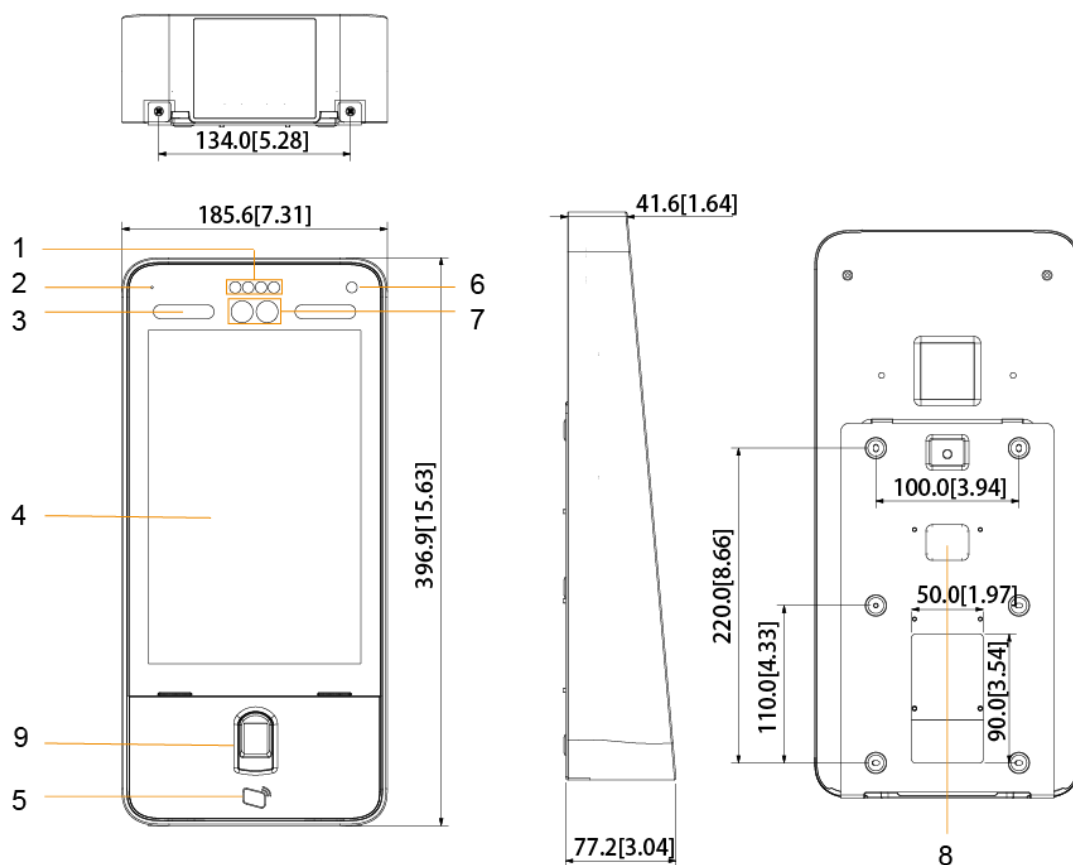


Таблица 1-4 Описание компонентов (4)

№	Название	№	Название
1	ИК-светодиод	6	Фототранзистор
2	Микрофон	7	Двойная камера
3	Источник белого света	8	Вход кабеля
4	Дисплей	9	Сенсор отпечатков пальцев
5	Место сканирования карт	10	–



# 2 Установка

## 2.1 Примечания по установке



- Если на расстоянии 0,5 метров от устройства находится источник освещения, 0,5 минимальная чувствительность должна быть не менее 100 люкс.
- Рекомендуется устанавливать устройство в помещении, на расстоянии минимум 3 метра от окон и дверей, и 2 метра – от источников освещения.
- Избегайте воздействия задней подсветки и прямых солнечных лучей.

### Требования к окружающему освещению

Рисунок 2-1 Требования к окружающему освещению



Свеча: 10 лк



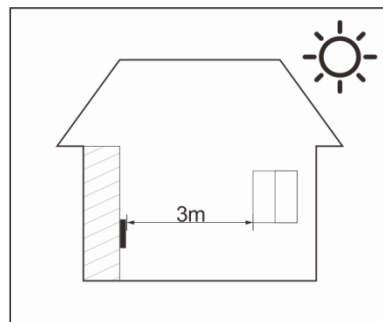
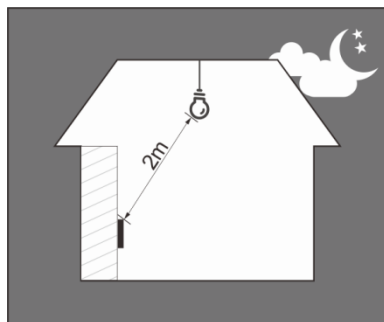
Лампочка: 100-850 лк



Солнечный свет: > 1200 лк

### Рекомендуемые места

Рисунок 2-2 Рекомендуемые места



### Не рекомендуемые места

Рисунок 2-3 Не рекомендуемые места



## 2.2 Подключение кабелей



- Проверьте, активирован ли что модуль безопасности контроля доступа в меню **Function > Security Module (Функции > Модуль безопасности)**. Если модуль безопасности активирован, вам необходимо отдельно приобрести модуль безопасности контроля доступа. Для модуля безопасности требуется отдельный источник питания.
- Если модуль безопасности активирован, кнопка выхода, управление блокировкой и функция отпечатков пальцев будут недоступны.

Рисунок 2-4 Подключение кабелей

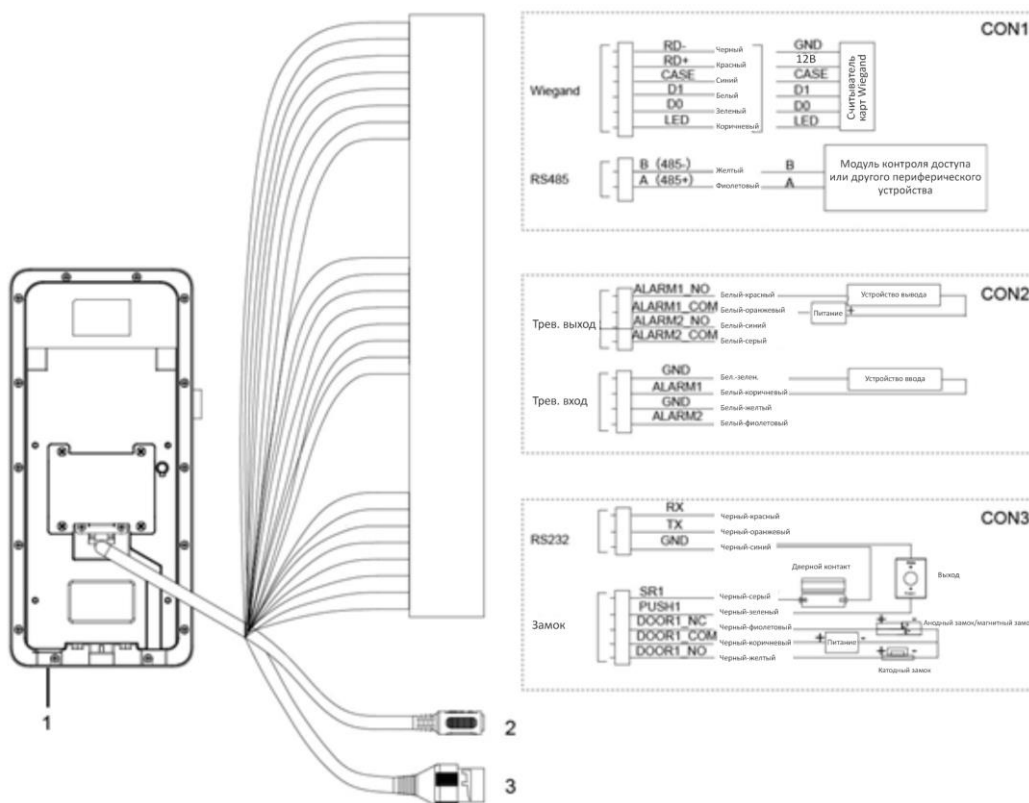


Таблица 2-1 Описание компонентов

№	Название
1	USB-порт
2	Порт питания
3	Ethernet-порт

## 2.3 Установка

Способы установки моделей A и B одинаковы. Убедитесь в том, что расстояние между объективом и землей составляет 1,4 метра. См. рисунок 2-5.

Рисунок 2-5 Высота установки

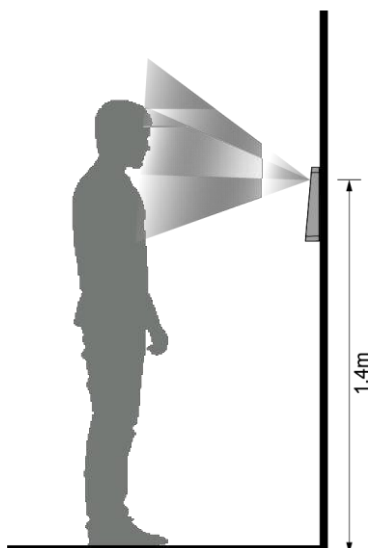
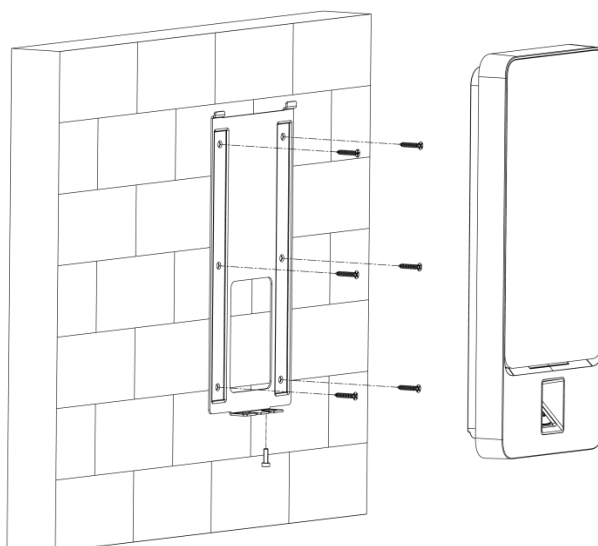


Рисунок 2-6 Схема установки



## Процедура установки

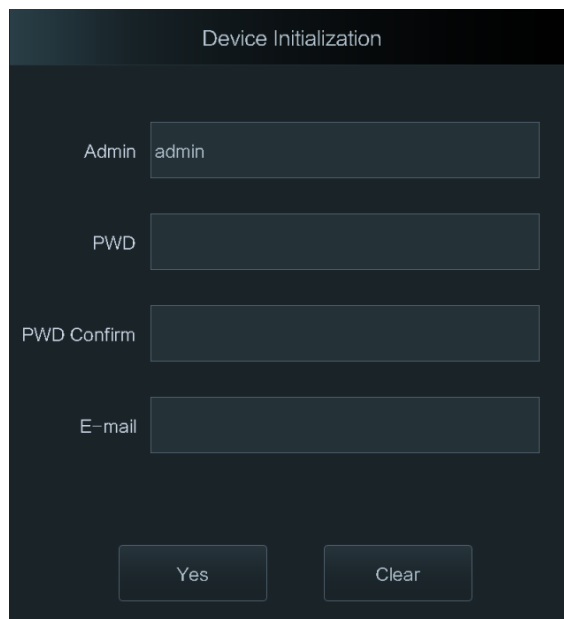
- Шаг 1** Просверлите семь отверстий (шесть для установки кронштейна и один для входа кабеля) в соответствии с отверстиями на кронштейне.
- Шаг 2** Зафиксируйте кронштейн на стене, вставив дюбели в шесть установочных отверстий кронштейна.
- Шаг 3** Подсоедините кабели контроллера доступа.  
См. Раздел 2.2 «Подключение кабелей».
- Шаг 4** Повесьте контроллер доступа на крючок кронштейна.
- Шаг 5** Закрутите шурупы в нижней части контроллера доступа.  
Теперь установка выполнена.

# 3 Работа в системе

## 3.1 Инициализация

При первом включении контроллера доступа необходимо настроить пароль администратора и email; в противном случае контроллер доступа не будет работать. См. рисунок 3-1.

Рисунок 3-1 Инициализация



- Если вы забыли пароль администратора, его можно переустановить с помощью указанного адреса электронной почты.
- Пароль должен состоять из от 8 до 32 символов без пробелов и как минимум два разных видов символов, включая верхний регистр, нижний регистр, цифры и специальные знаки (кроме ' " ; : &).
- Если контроллер доступа не имеет сенсорного экрана, инициализацию можно выполнить с помощью веб-интерфейса. Подробную информацию см. в руководстве пользователя.

## 3.2 Добавление новых пользователей

При добавлении новых пользователей вы можете вводить их ID, имена, импортировать их отпечатки пальцев, изображения лиц, пароли и выбирать их категорию.

Следующие изображения представлены только для ознакомления, и преимущественное значение имеет реальный интерфейс.

**Шаг 1** Выберите **User > New User (Пользователь > Новый пользователь)**.

Появится окно **New User (Новый пользователь)**. См. рисунок 3-2.




Следующее изображение представлено только для ознакомления, и преимущественное значение имеет реальный интерфейс.




Рисунок 3-2 Новый пользователь


Parameter	Value
User ID	1
Name	
FP	0
Face	0
Card	0
PWD	
User Level	User
Period	255-Default
Holiday Plan	255-Default
Valid Date	2037-12-31
User Level	General
Use Time	Unlimited

**Шаг 2** Выполните настройку параметров. См. таблицу 3-1.

Таблица 3-1 Описание параметров нового пользователя

Параметр	Описание
User ID	Вы можете вводить ID пользователей. ID состоит из 32 знаков (включая цифры и буквы), и каждый ID уникален.
Name (имя)	Вы можете вводить имена пользователей, состоящие максимум из 32 символов (включая цифры, знаки и буквы).
FP	<p>Можно записать максимум три отпечатка одного пользователя, и каждый отпечаток подтверждается трижды.</p> <p>Вы можете активировать функцию Duress FP для каждого отпечатка, и только один отпечаток будет использоваться для тревоги принуждения. Если такой отпечаток используется для открытия двери, срабатывает тревога.</p> <p></p> <ul style="list-style-type: none"> <li>Для тревоги принуждения не рекомендуется использовать отпечаток большого пальца.</li> <li>Разблокировка с помощью отпечатка пальца возможна для некоторых моделей.</li> </ul>
Face (лицо)	Убедитесь в том, что ваше лицо находится в центре рамки изображения. Снимок вашего лица будет сделан автоматически. Подробную информацию о записи изображений лиц см. в Приложении 1 «Примечания по записи изображений лиц».

Параметр	Описание
Card (карта)	<p>Для каждого пользователя можно зарегистрировать до пяти карт. Введите номер вашей карты в окне регистрации карты или отсканируйте карту, после чего контроллер доступа будет осуществлять считывание карты.</p> <p>В окне регистрации карты можно активировать функцию Duress Card. При попытке разблокировать дверь с помощью карты с настройкой тревоги принуждения, сработает сигнализация.</p>  <p>Если ваше устройство не имеет модуля считывания карт, вы можете подключить периферические считыватели.</p>
Password (пароль)	<p>Пароль для разблокировки двери. Максимальная длина – 8 знаков.</p>  <p>Если контроллер доступа не имеет сенсорного экрана, необходимо подключить к нему периферический считыватель карт. На считывателе карт имеются кнопки.</p>
Level (уровень)	<p>Вы можете выбрать уровень для нового пользователя. Возможны два варианта.</p> <ul style="list-style-type: none"> <li>● User (пользователь): Пользователь имеет полномочия только на открытие двери.</li> <li>● Admin (администратор): Администраторы могут не только разблокировать двери, но и настраивать параметры системы.</li> </ul>  <p>На случай того, что вы забудете пароль администратора, лучше создать более одного администратора.</p>
Period (период)	<p>Можно настраивать период, в течение которого пользователь может разблокировать дверь. Подробную информацию о настройках периодов см. в руководстве по конфигурации.</p>
Holiday Plan (план праздничных дней)	<p>Можно настраивать план праздничных дней, в течение которых пользователь может разблокировать дверь. Подробную информацию о настройках плана праздничных дней см. в руководстве по конфигурации.</p>
Valid Date (дата действия)	<p>Можно настраивать период, в течение которого информация о разблокировании пользователем будет действительной.</p>
User Level (категория пользователя)	<p>Существует шесть категорий:</p> <ul style="list-style-type: none"> <li>● General (общий): Общие пользователи могут открывать дверь в обычном режиме.</li> <li>● Blacklist (черный список): Если дверь открывает пользователь из черного списка, обслуживающий персонал получает уведомление.</li> <li>● Guest (гость): Гости могут открывать двери несколько раз в определенные периоды. После превышения максимального числа раз и истечения периода они не смогут открывать двери.</li> <li>● Patrol (патруль): Отслеживается посещаемость патрулирующих пользователей, и они не имеют полномочий на открывание дверей.</li> <li>● VIP: При открытии двери VIP-пользователем обслуживающий персонал получает уведомление.</li> <li>● Disable (лица с ограниченными возможностями): Если дверь открывается лицом с ограниченными возможностями, произойдет задержка в 5 секунд до закрытия двери.</li> </ul>
Use Time (время использования)	<p>Для пользователей категории <b>Guest</b> можно настроить максимальное число раз открытия двери.</p>

**Шаг 3** После того, как вы установите параметры, нажмите  чтобы сохранить настройки. Будет создан новый пользователь.



Если контроллер доступа не имеет сенсорного экрана, пользователей необходимо создавать с помощью платформ управления. Подробную информацию см. в руководстве пользователя.

# 4 Работа с веб-интерфейсом

Контроллер доступа можно настраивать и работать с ним в веб-интерфейсе. С помощью веб-интерфейса можно настраивать такие параметры как параметры сети, параметры видео и параметры контроля доступа; здесь также можно осуществлять обновление системы.

## Авторизация



Перед первой авторизацией в веб-интерфейсе необходимо настроить пароль и указать адрес электронной почты. Настраиваемый вами пароль используется для авторизации в веб-интерфейсе, а адрес электронной почты – для восстановления пароля.

**Шаг 1** Откройте браузер IE, введите IP-адрес (192.168.1.108 по умолчанию) контроллера доступа в адресной строке и нажмите Enter.

Рисунок 4-1 Авторизация

The image shows a login interface for a 'WEB SERVICE'. It features a dark background with white text. The title 'WEB SERVICE' is at the top. Below it are two input fields: 'Username:' and 'Password:'. A 'Forget Password?' link is positioned below the password field. At the bottom, there is a prominent blue button labeled 'Login'.

**Шаг 2** Введите имя пользователя и пароль.



- Имя администратора по умолчанию – admin, а пароль – это пароль входа после инициализации контроллера доступа. Регулярно меняйте пароль администратора и обеспечивайте его надежное хранение.
- Если вы забыли пароль администратора, вы можете нажать **Forget Password? (Забыли пароль?)**, чтобы переустановить пароль. См.

**Шаг 3** руководство пользователя.

Нажмите **Login (авторизация)**.

Откроется домашняя страница веб-интерфейса.



# Приложение 1 Примечания по записи изображений лиц

---

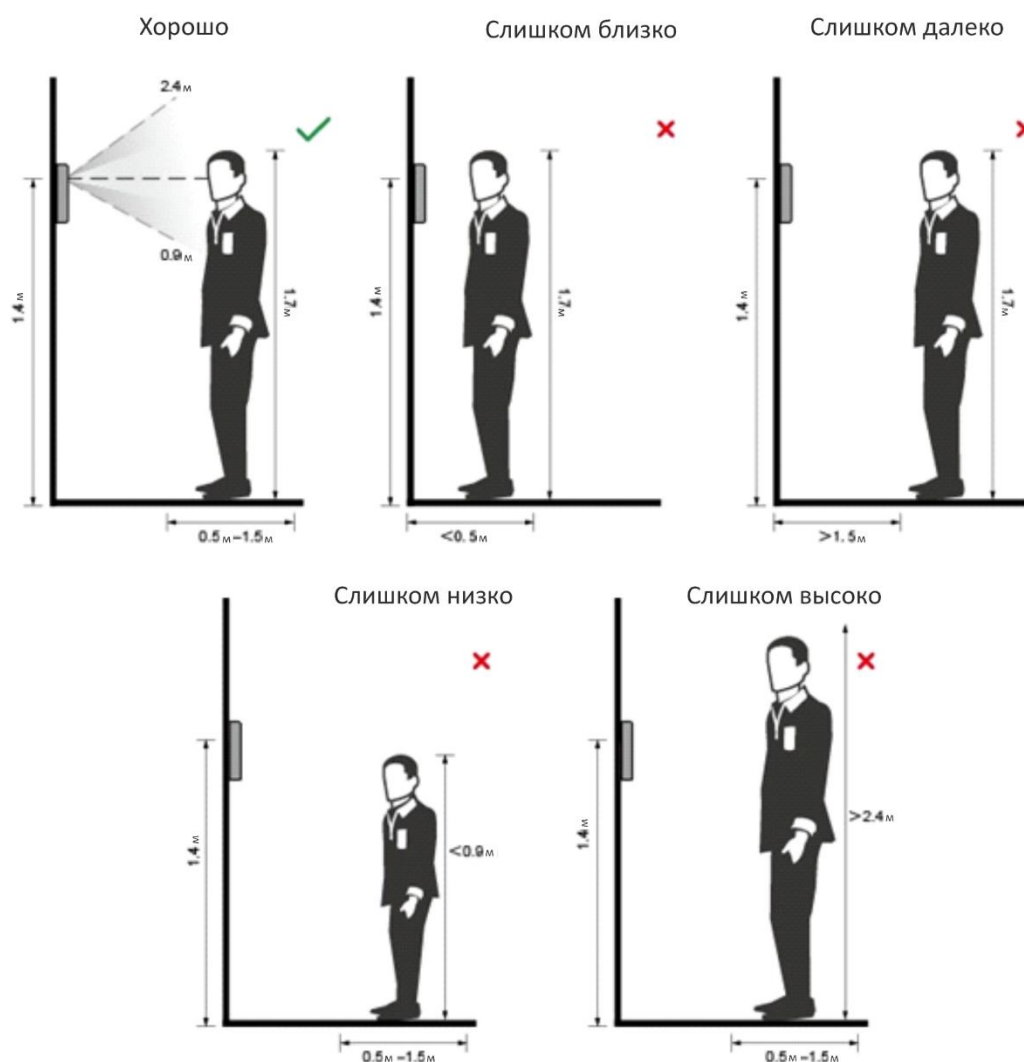
## Перед регистрацией

- На эффективность распознавания лиц может влиять наличие очков, головного убора и бороды.
- Не закрывайте брови, если на вас надет головной убор.
- Не меняйте стиль вашей бороды существенным образом, если вы используете устройство; в противном случае процесс распознавания может не происходить.
- Ваше лицо должно быть чистым.
- Держите устройство на расстоянии минимум два метра от источника освещения и минимум три метра от окон или дверей; в противном случае, задний свет или прямые солнечные лучи могут повлиять на эффективность распознавания лиц.

## Положение лица

На эффективности распознавания лица может сказываться его неправильное положение.

Рисунок 1-1 в приложении. Соответствующее положение лица



## Требования к лицам

- Лицо должно быть чистым, и волосы не должны закрывать лоб.
- Не надевайте очки, головной убор или какие-либо украшения для лица, которые могут влиять на изображение лиц.
- Глаза должны быть открыты, выражение лица должно быть нейтральным, и лицо должно быть направлено в центр камеры.
- При выполнении записи изображений лиц или в ходе распознавания лицо не должно находиться слишком близко или слишком далеко от камеры.

Рисунок 1-2 в приложении. Положение головы



Рисунок 1-3 в приложении. Расстояние до лица



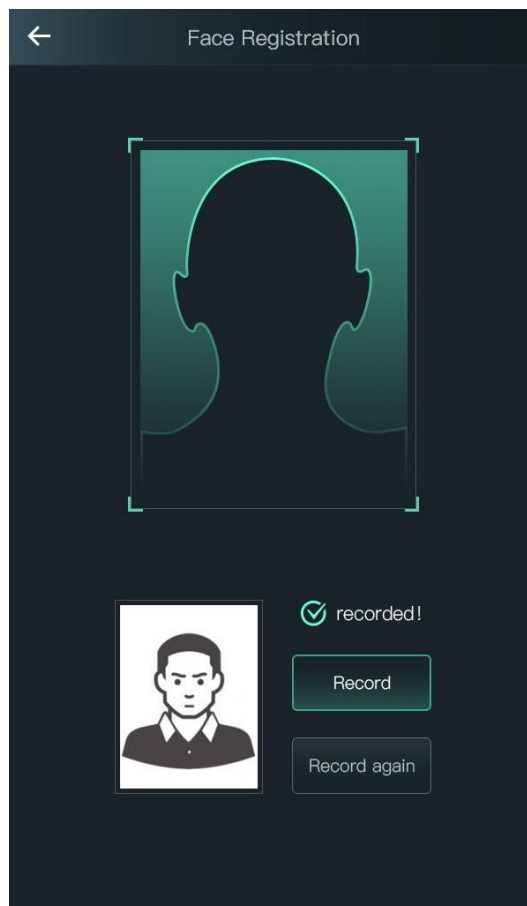
- При импорте изображений лиц с помощью платформы управления разрешение изображений должно быть в диапазоне 150×300–600×1200; количество пикселей больше 500×500; размер изображения меньше 75 Кб, а номер изображения и ID человека должны совпадать.
- Убедитесь в том, что лицо не занимает 2/3 всего изображения, а соотношение сторон не превышает 1:2.

## В ходе регистрации

Регистрацию лиц можно выполнять с помощью контроллера доступа или платформы. Если вы выполняете регистрацию с помощью платформы, см. руководство пользователя по платформе.

Голова должна находиться в центре кадра. Снимок изображения вашего лица будет сделан автоматически.

Рисунок 1-4 в приложении. Регистрация



- Не двигайтесь, или регистрация может не произойти.
- В окне не должно быть двух лиц одновременно.

## Приложение 2 Инструкции по записи отпечатков пальцев

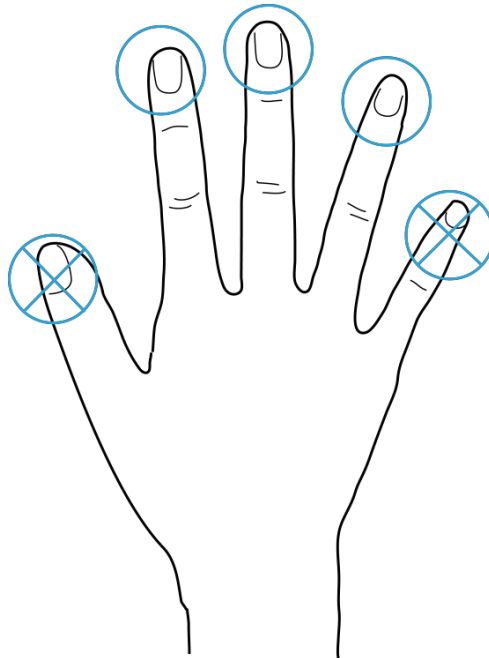
### Примечания

- Перед началом записи отпечатков пальцев убедитесь в том, что ваши руки чистые и сухие.
- Прижмите палец к месту сканирования; отпечаток пальца должен находиться в центре области записи.
- Не размещайте сенсор отпечатков пальцев в местах с интенсивным освещением, высокой температурой и влажностью.
- Если отпечатки пальцев людей повреждены нечетко регистрируются, следует использовать другой способ разблокировки.

### Рекомендуемые пальцы

Рекомендуется использовать указательный, средний или безымянный палец. Большой палец или мизинец сложно прикладывать в центре области записи.

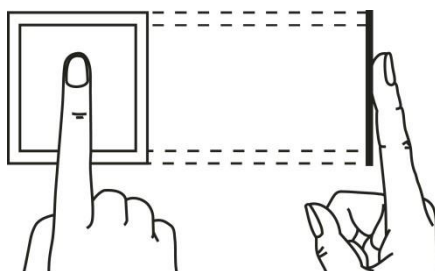
Рисунок 2-1 в приложении. Рекомендуемые пальцы



### Способ прикладывания пальца

- Правильный способ

Рисунок 2-2 в приложении. Правильный способ приложения пальца



- Неправильный способ

Рисунок 2-3 в приложении. Неправильный способ приложения пальца

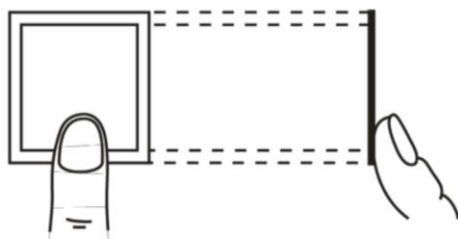
Палец перпендикулярно области записи



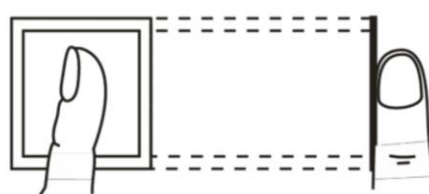
Палец перпендикулярно области записи



Палец не в центре области записи



Палец наклонен



# Приложение 3 Рекомендации по кибербезопасности

Кибербезопасность – это не просто модное слово: она относится к любому устройству, которое подключается к Интернету. IP-видеонаблюдение не может быть неуязвимым перед рисками кибератак, но базовые процедуры по обеспечению защиты, усиление сетей и сетевых устройств позволяет снизить такую уязвимость. Ниже представлено несколько советов о том, как создать более защищенную систему безопасности.

## **Обязательные действия, обеспечивающие базовую сетевую безопасность оборудования:**

### **1. Использование надежных паролей**

Соблюдайте следующие указания по установке паролей:

- Длина должна быть не меньше 8 символов.
- Используйте как минимум два вида символов; к видам символов относятся буквы в верхнем и нижнем регистре, цифры и знаки.
- Не используйте название учетной записи или его же 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. Своевременно обновляйте программное обеспечение**

- Как принято в технической индустрии, мы рекомендуем постоянно обновлять программное обеспечения вашего оборудования (например, NVR, DVR, IP-камер и т.д.), чтобы обеспечить самые последние патчи для устранения уязвимостей системы. Если оборудование подключается к публичной сети, рекомендуется включать «автоматический поиск обновлений», чтобы получать актуальную информацию об обновлениях программного обеспечения, выпущенных производителем.
- Мы рекомендуем скачивать и использовать последние версии клиентского программного обеспечения.

## **Необязательные рекомендации по повышению сетевой безопасности:**

### **1. Физическая защита**

Мы рекомендуем обеспечивать физическую защиту оборудования, особенно устройств для хранения данных. Например, размещать оборудование в специальных помещениях для ЭВМ и шкафах, а также обеспечивать надлежащий контроль доступа и распределение ключей, чтобы избежать физического контакта неуполномоченного персонала с оборудованием, например, повреждение оборудования, несанкционированное подключение съемных устройств (таких как USB-накопители, серийные порты) и т.д.

### **2. Регулярно меняйте пароли**

Мы рекомендуем регулярно менять пароли, чтобы избежать доступа неуполномоченных пользователей или взлома.

### **3. Своевременно настраивайте и обновляйте информацию о смене паролей**

Оборудование поддерживает функцию смены паролей. Своевременно настраивайте информацию, необходимую для смены паролей, включая электронную почту конечного пользователя и контрольные вопросы. Если информация изменилась, своевременно заменяйте ее. При настройке контрольных вопросов не рекомендуется использовать простые вопросы.

### **4. Активируйте блокировку учетной записи**

Функция блокировки учетной записи установлена по умолчанию, и мы рекомендуем использовать ее, чтобы обеспечить безопасность учетной записи. Если злоумышленник попытается войти в систему, используя неправильный пароль несколько раз, соответствующая учетная запись и IP-адрес источника будут заблокированы.

## **5. Меняйте HTTP и другие сервисные порты по умолчанию**

Мы рекомендуем менять HTTP и другие сервисные порты по умолчанию, используя любой набор цифр между 1024~65535. Это позволяет снизить риск того, что посторонние смогут догадаться, какие порты вы используете.

## **6. Активируйте HTTPS**

Мы рекомендуем активировать HTTPS, чтобы вы получали доступ к веб-сервису через защищенный канал связи.

## **7. Активируйте «белый список»**

Мы рекомендуем использовать функцию «белого списка», чтобы вход в систему был возможен только с указанных IP-адресов. При этом, убедитесь в том, что IP-адрес вашего ПК и IP-адреса прочего оборудования были добавлены в «белый список».

## **8. Привязка по MAC-адресу**

Мы рекомендуем связывать IP- и MAC-адрес шлюза оборудования, чтобы снизить риск сетевой атаки с помощью протокола ARP.

## **9. Предоставляйте учетные записи и привилегии рациональным образом**

Добавляйте пользователей и назначайте минимальный набор разрешений для них в соответствии с целями бизнеса и управления.

## **10. Отключайте ненужные сервисы и выбирайте безопасные режимы**

Чтобы снизить возможные риски, рекомендуется отключать сервисы SNMP, SMTP, UPnP и т.д., если они не нужны.

Если такие сервисы нужны, настоятельно рекомендуется использовать безопасные режимы, включая следующие сервисы, но не ограничиваясь ими:

- SNMP: Выберите SNMP v3 и установите надежные пароли шифрования и авторизации.
- SMTP: выберите TLS для доступа к серверу электронной почты.
- FTP: выберите SFTP и установите надежные пароли.
- Точка доступа AP: Выберите режим шифрования WPA2-PSK и установите надежные пароли.

## **11. Передача аудио и видеоданных с шифрованием**

Если ваши аудио и видеоданные очень важны или являются конфиденциальными, мы рекомендуем использовать функцию передачи с шифрованием, чтобы снизить риск перехвата аудио и видео при передаче

## **12. Контроль безопасности**

- Проверка онлайн-пользователей: мы рекомендуем регулярно проверять онлайн-пользователей, чтобы видеть, если в систему вошли несанкционированные пользователи.
- Проверка журналов оборудования: Просматривая журналы, вы можете узнать IP-адреса, используемые для авторизации и выполненные ключевые операции.

## **13. Сетевой журнал**

Поскольку место для хранения данных в устройствах ограничено, также ограничены и сохраняемые журналы. Если вам необходимо хранить журнал в течение продолжительного времени, рекомендуется активировать функцию сетевого журнала, чтобы обеспечить синхронизацию критических журналов с сервером сетевого журнала для отслеживания.

## **14. Создание безопасной сетевой среды**

Чтобы обеспечить более надежную защиту оборудования и снизить возможные риски для кибербезопасности, мы рекомендуем:

- Отключать функцию распределения портов для роутера, чтобы избежать прямого доступа к устройствам интрасети из внешней сети.



- Сеть должна быть разделена и изолирована в соответствии с реальными нуждами. Если какие-либо требования к связи между двумя подсетями отсутствуют, рекомендуется использовать VLAN, сетевой GAP и другие технологии для разделения сети, чтобы обеспечить изолирование сети.
- Используйте систему доступа 802.1x, чтобы снизить риск доступа неуполномоченных пользователей к частным сетям.