Терминалы доступа Dahua DHI-ASI2212H/ Dahua DHI-ASI2201H

Краткое руководство по началу работы

версия 1.0.1

Содержание

1 Устройство

Рисунок 1–1 Габаритные размеры (1) (мм [дюймы])

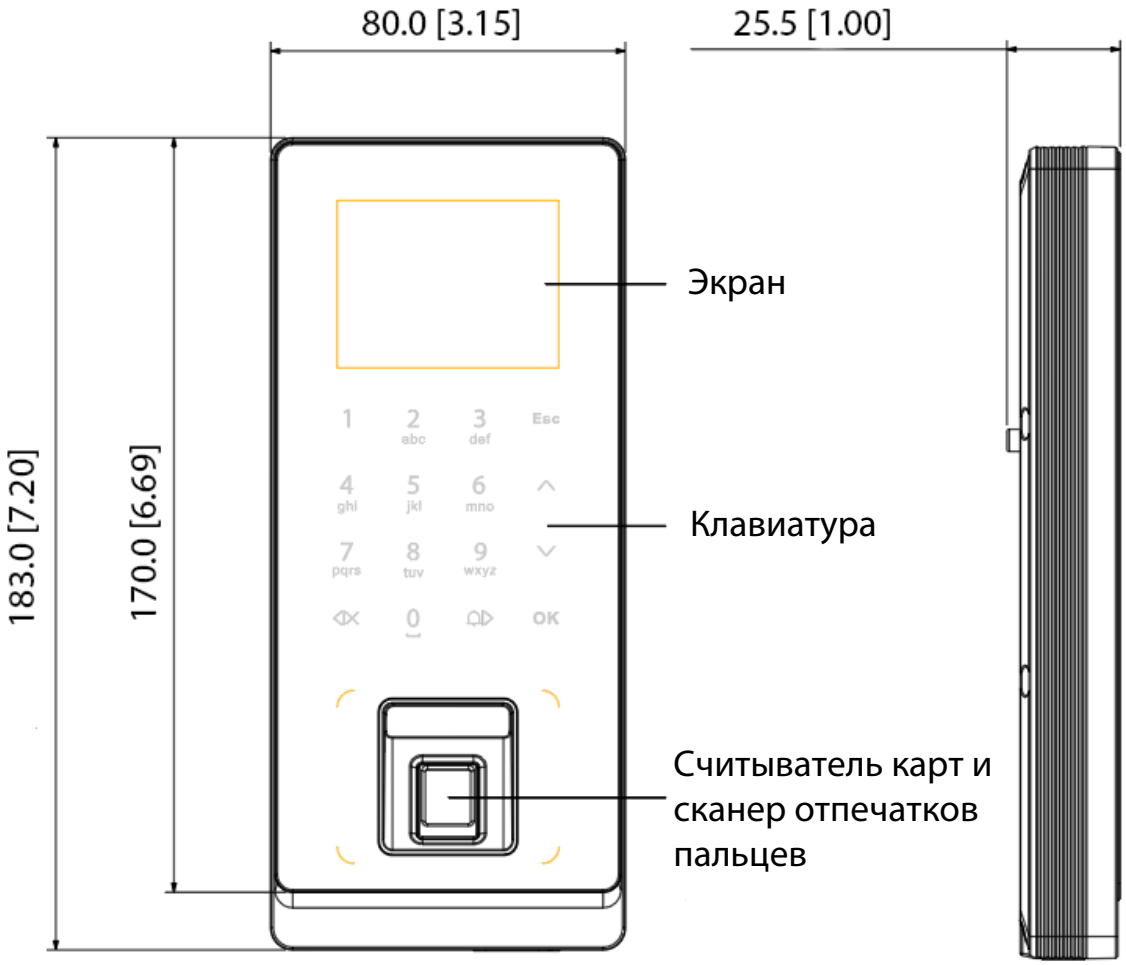
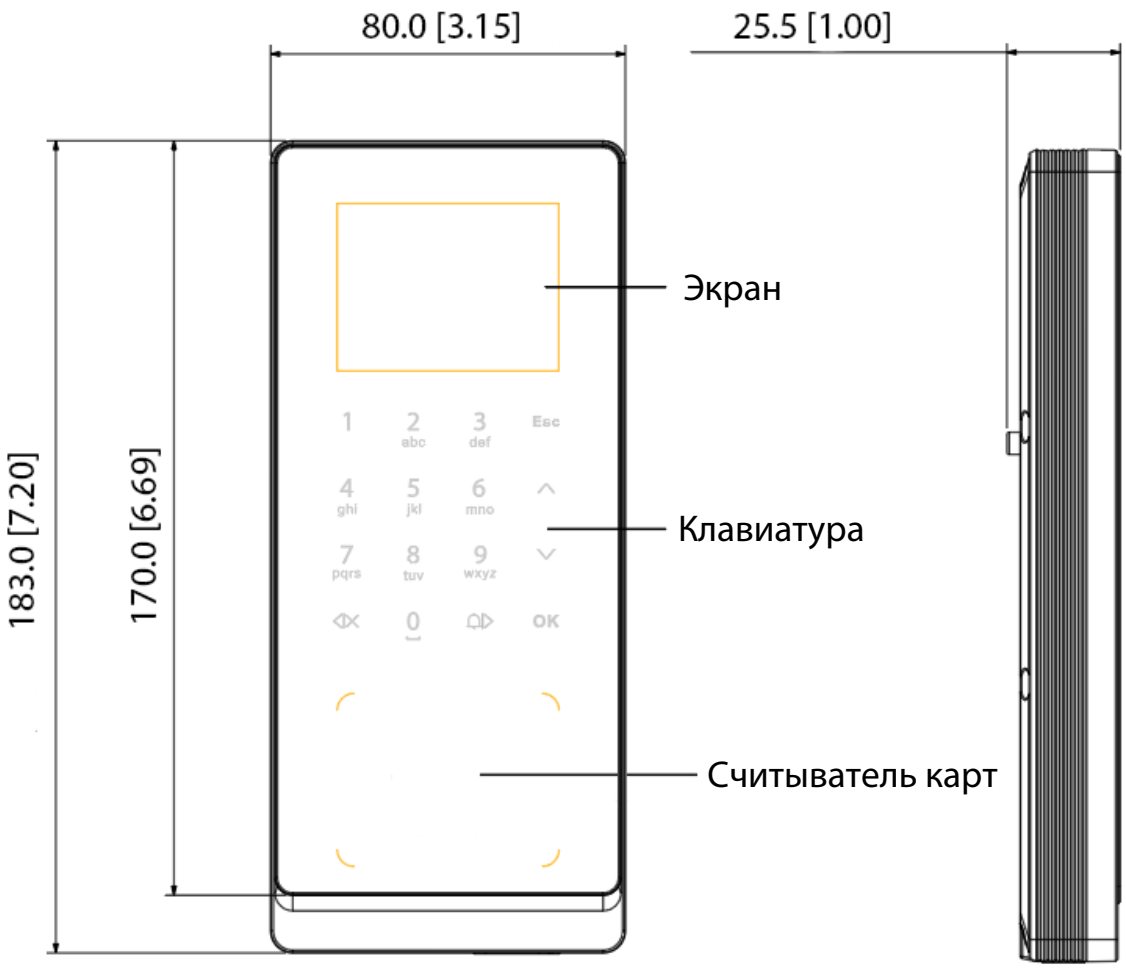


Рисунок 1–2 Габаритные размеры (2) (мм [дюймы])



2 Подключение проводов и монтаж

2.1 Требования к условиям эксплуатации

- Уровень освещённости в 0,5 м от прибора должен составлять не менее 100 лк

Рисунок 2–1 Условия установки

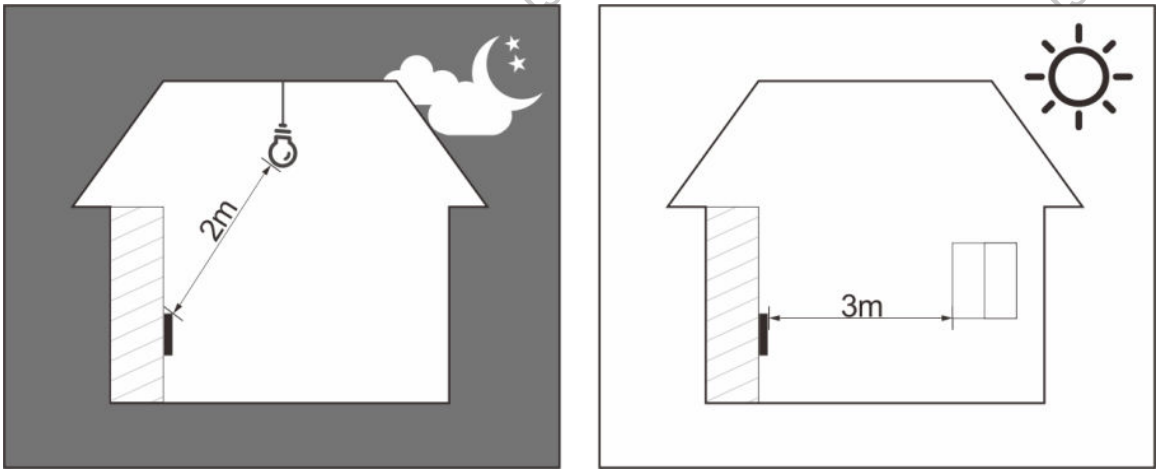
Свеча: 10 люкс

Лампа накаливания: 100–850 люкс

Солнечный свет: ≥1200 люкс

- Рекомендуется устанавливать устройство в помещении, на расстоянии 3 м от окон или дверей и 2 м от любых источников света.

Рисунок 2–2 Место установки

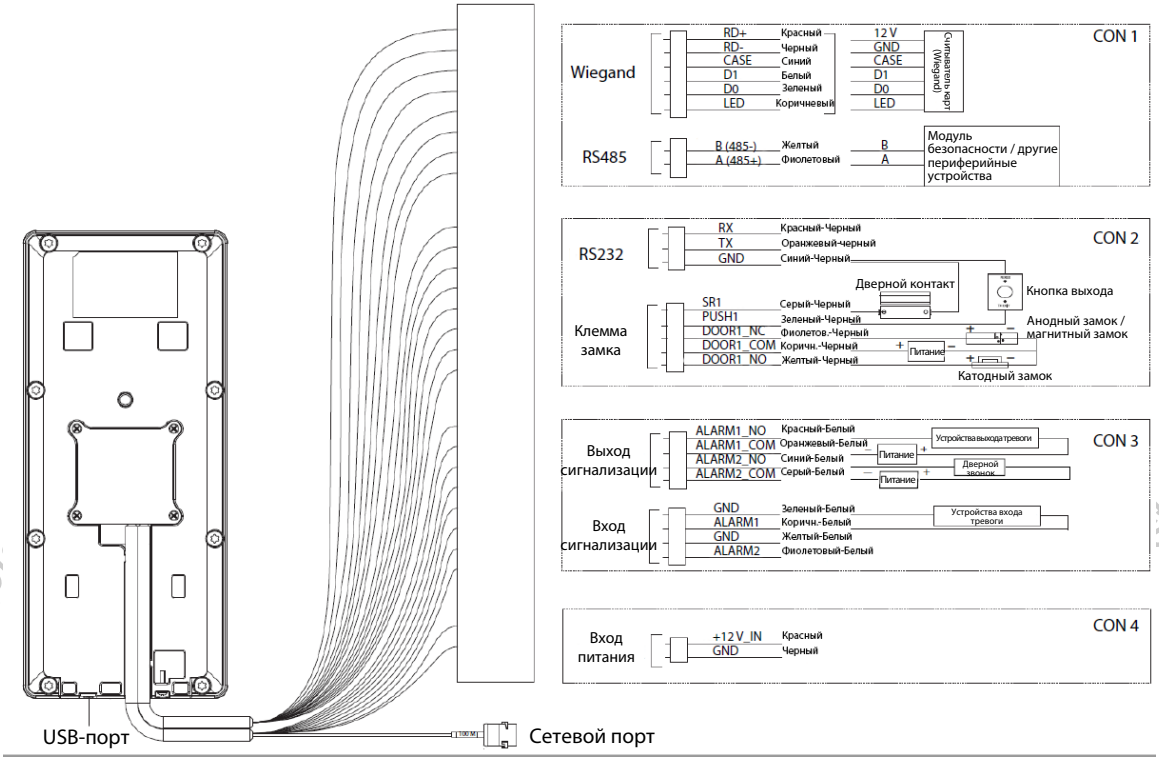


- Избегайте установки устройства при контровом освещении, под прямыми солнечными лучами или вблизи каких-либо источников света.

Рисунок 2–3 Места, не рекомендуемые для установки

2.2 Подключение проводов

Рисунок 2–4 Схема подключения



- На веб-портале выберите **Config Mgmt** (Управление конфигурацией) > **Features** (Функции), чтобы проверить, включён ли **Security Module** (Модуль безопасности). Если он включён, необходимо приобрести совместимый модуль безопасности, который требует отдельного питания.
- Когда модуль безопасности включён, кнопка выхода, замок и пожарная блокировка (пожарная сигнализация) становятся недействительными.

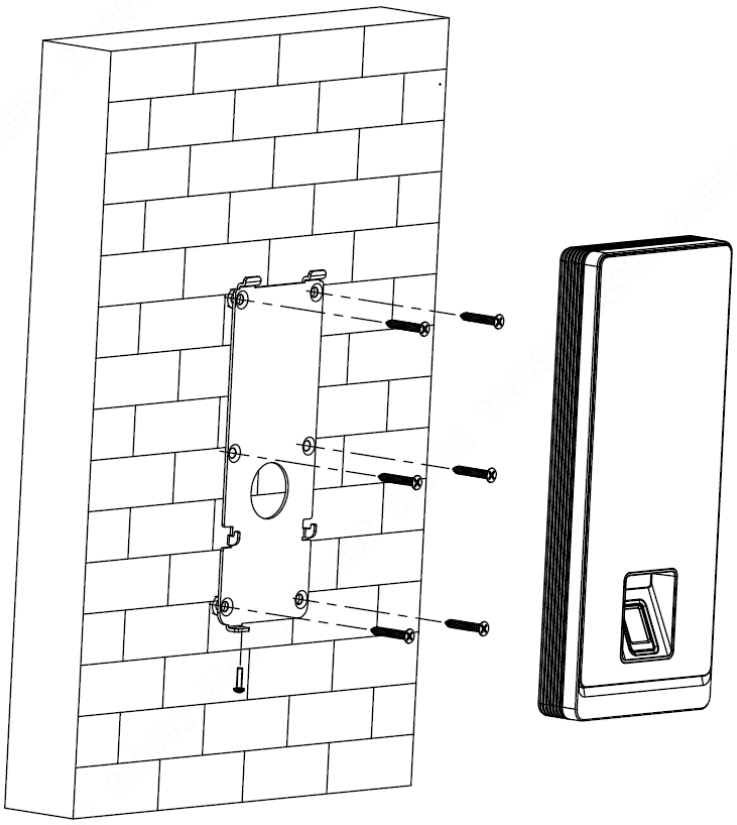
2.3 Установка

В данном разделе в качестве примера используется устройство с функцией отпечатка пальца. Рекомендуется устанавливать устройство на высоте 1,2–1,6 м от пола (от центра объектива до пола).

Порядок действий

Шаг 1 Разметьте отверстия на стене в соответствии с кронштейном. Просверлите в стене шесть отверстий под винты и одно отверстие для вывода кабеля. Вставьте в отверстия анкерные болты.

Рисунок 2–5 Установка устройства на стену



Шаг 2 Закрепите кронштейн на стене с помощью винтов.

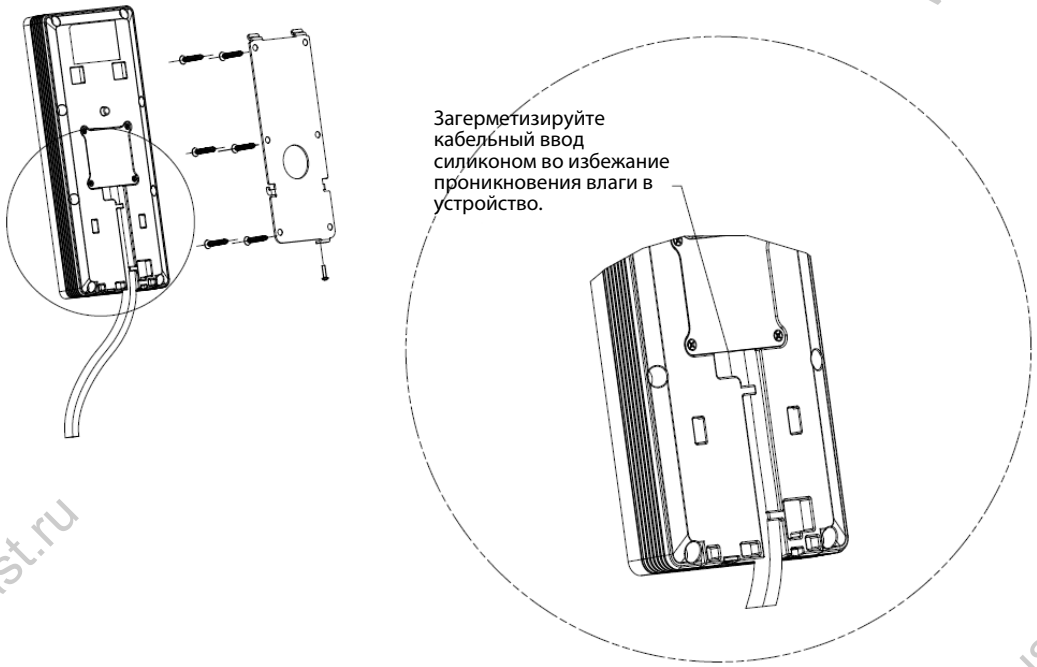
Шаг 3 Подключите провода устройства. Подробности см. в разделе «2.2 Подключение проводов».

Шаг 4 Установите устройство на крючки кронштейна.

Шаг 5 Затяните винт в нижней части устройства.

Шаг 6 (Опционально) Нанесите силиконовый герметик на отверстие для вывода кабеля.

Рисунок 2–6 Нанесение силиконового герметика



3 Локальные настройки

3.1 Первоначальная настройка

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

Рис. 3–1 Начальная настройка

- 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 Вход в систему

Выполните вход в главное меню для настройки автономного контроллера доступа. Только учётная запись администратора может входить в главное меню устройства. При первом использовании используйте учётную запись администратора для входа в главное меню, после чего вы сможете создавать другие учётные записи администраторов.

Общая информация

- **Учётная запись администратора (admin):** позволяет входить в главное меню автономного контроллера доступа, но не имеет разрешения на проход.
- **Учётная запись администратора (administrator):** позволяет входить в главное меню автономного контроллера доступа и имеет разрешение на проход.

Порядок действий

Шаг 1. На экране ожидания нажимайте ∧ и ∨ для выбора , затем нажмите **OK**.

Шаг 2. Выберите способ проверки подлинности для входа в главное меню.

Способы верификации могут различаться в зависимости от модели автономного контроллера доступа.

- **Card (Карта)**: вход в главное меню осуществляется по карте.

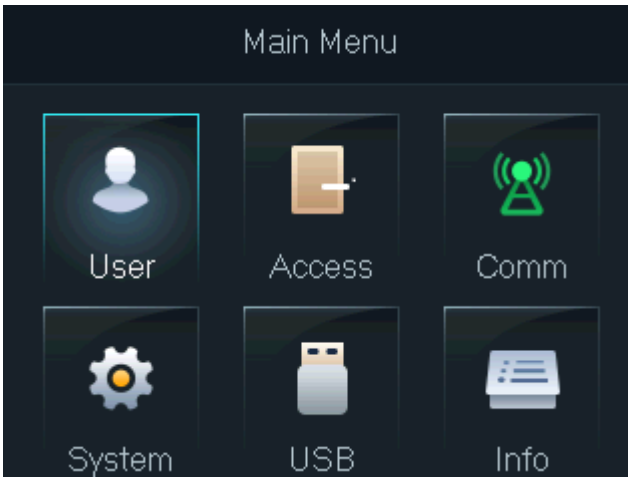
- **FP (отпечаток пальца)**: вход в главное меню осуществляется по отпечатку пальца.
- **PWD (пароль):** введите идентификатор пользователя и пароль учётной записи администратора.
- **Admin (администратор)**: введите пароль администратора для входа в главное меню.

Шаг 3. В главном меню нажимайте ∧ или ∨ для навигации по пунктам меню, затем нажмите **OK** для настройки параметров.

Используйте сочетания клавиш для выбора меню, просто нажимая кнопки 1–6.

- Для настройки управления пользователями нажмите **1.**
- Для настройки контроля доступа нажмите **2.**
- Для настройки связи нажмите **3.**
- Для настройки системы нажмите **4.**
- Для настройки USB нажмите **5.**
- Для просмотра информации о системе нажмите **6**.

Рисунок 3–2 Главное меню



User - Пользователи
Access - Доступ
Comm - Связь
System - Система
USB
Info - Информация

3.3 Добавление пользователей

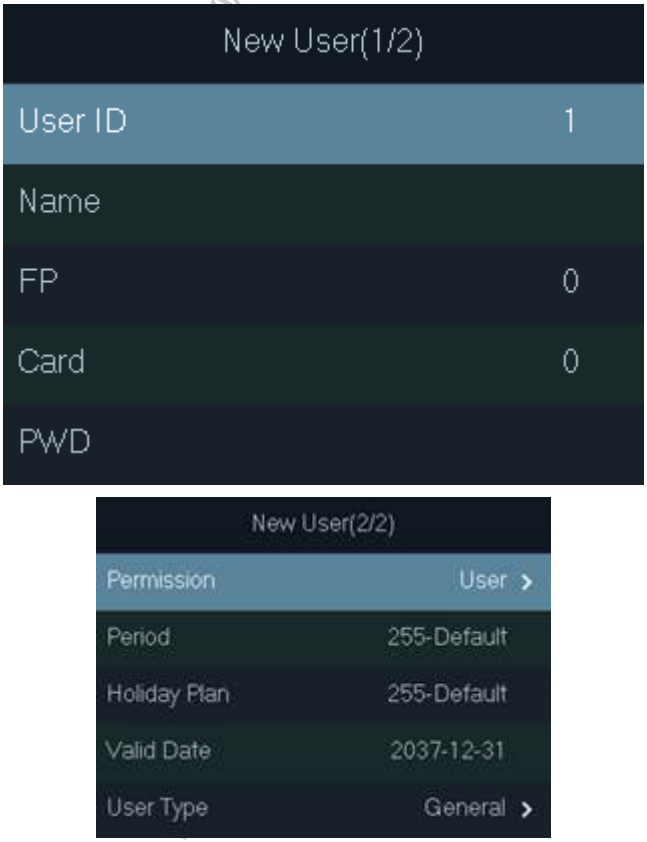
Порядок действий

Шаг 1. На экране ожидания нажимайте ∧ или ∨ для выбора , затем нажмите **OK**.

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 3–3 Добавление нового пользователя



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

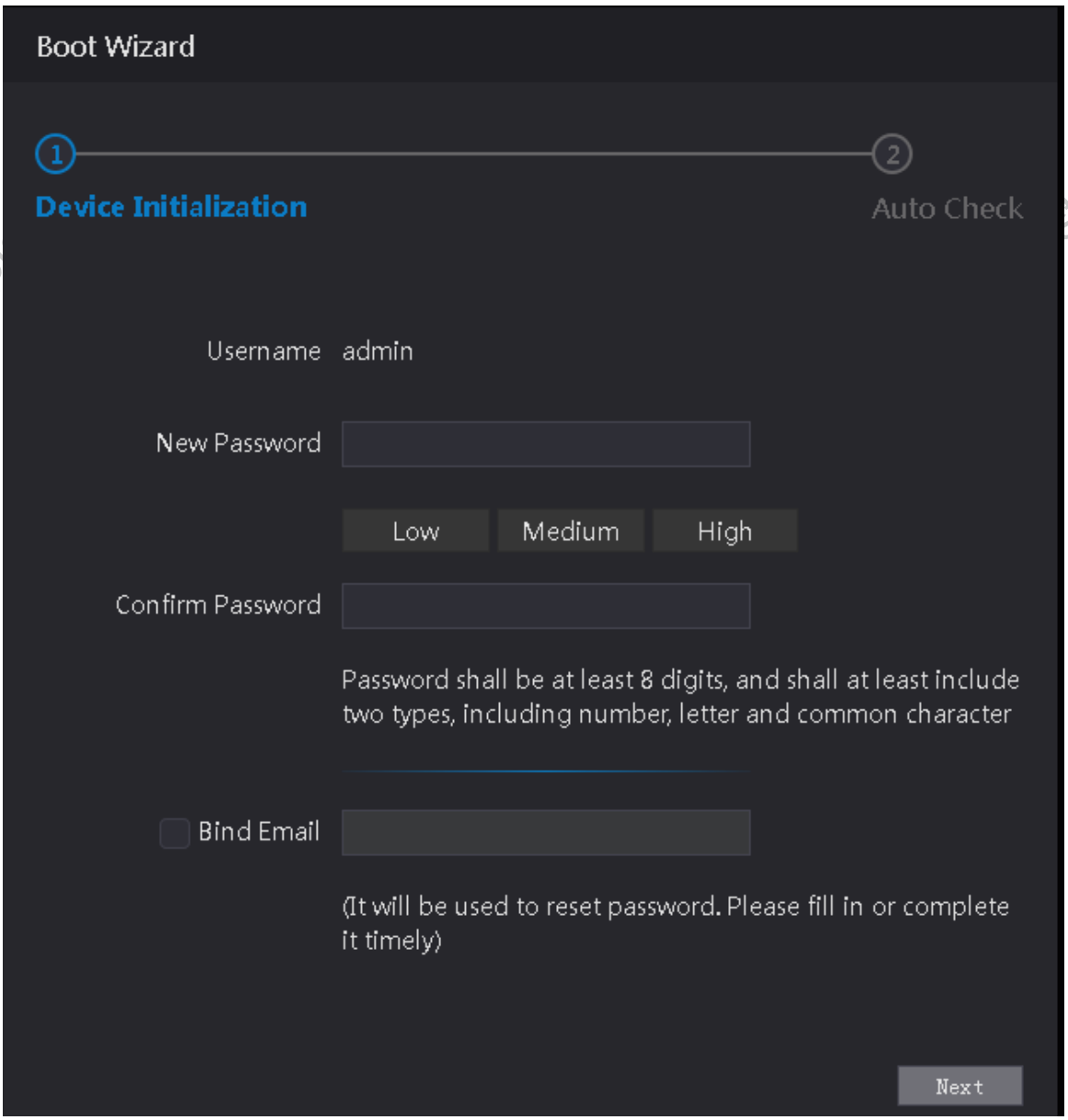
Перед первым входом в веб-интерфейс необходимо задать пароль и привязать адрес электронной почты.

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.

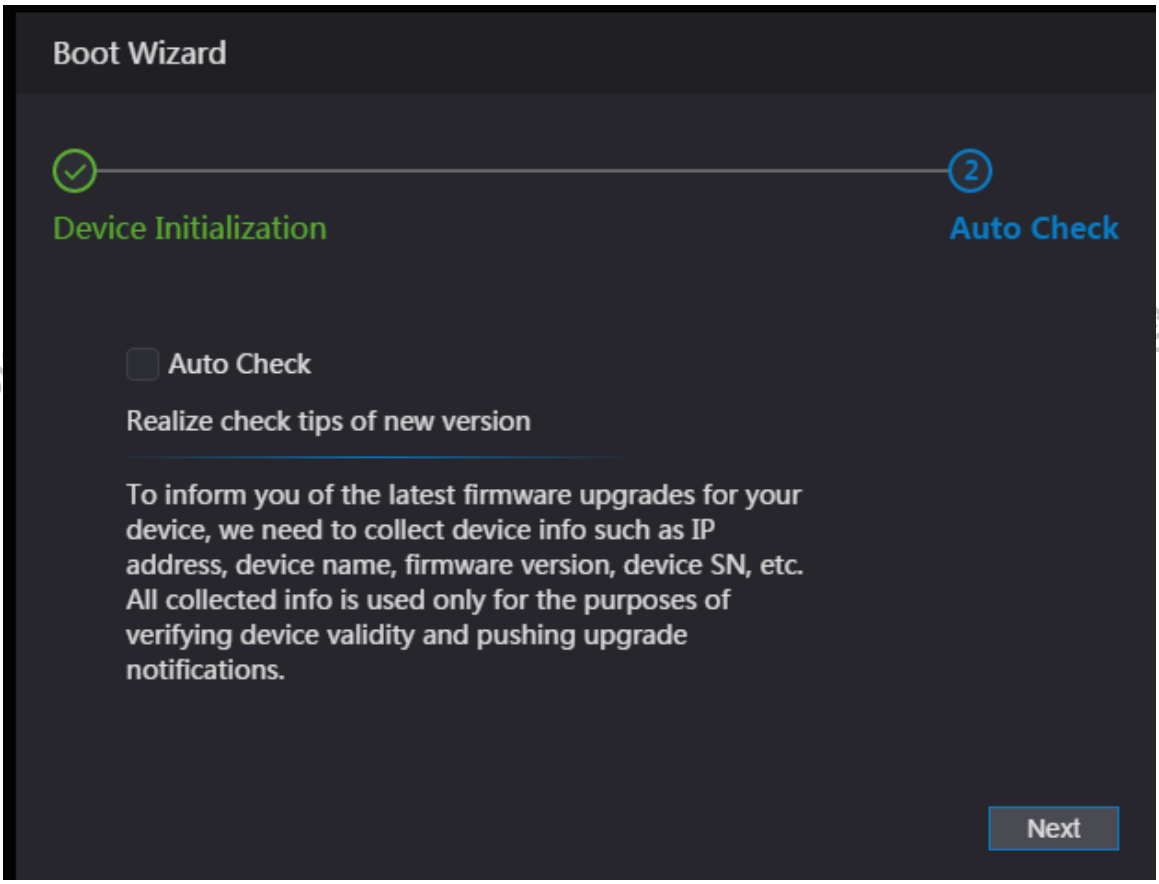
Рисунок 4–1 Инициализация



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).**

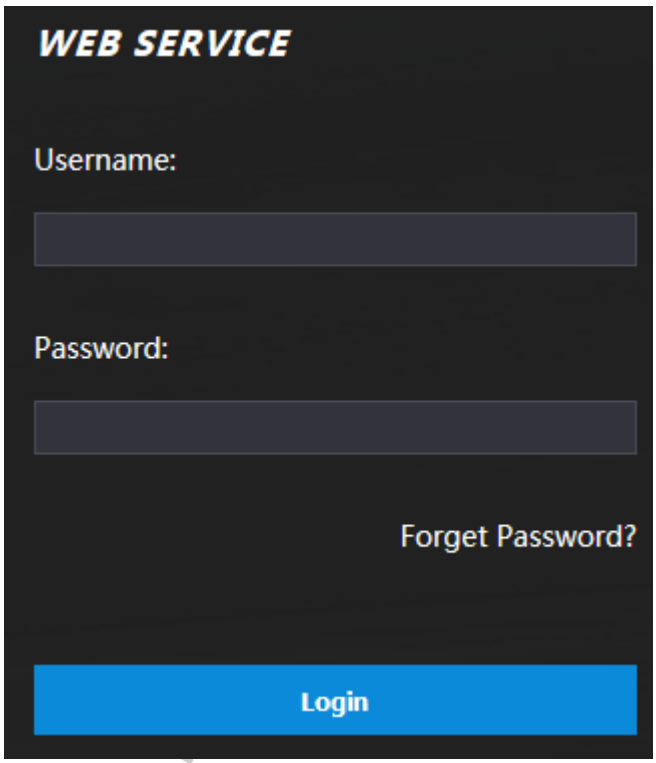
4.2 Вход в систему

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



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

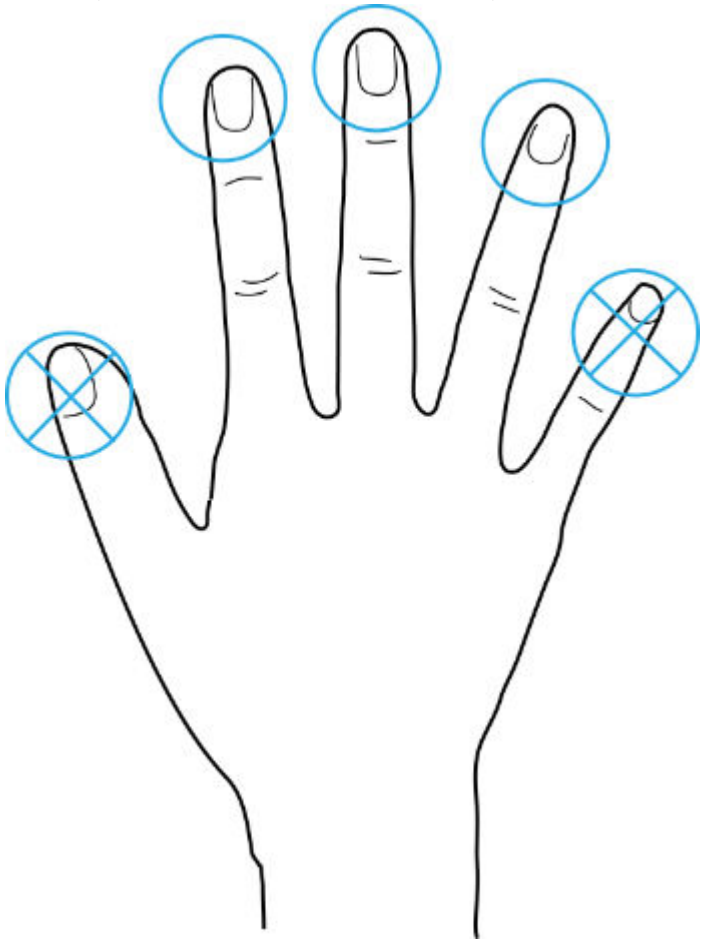
При регистрации отпечатка пальца обратите внимание на следующее:

- 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

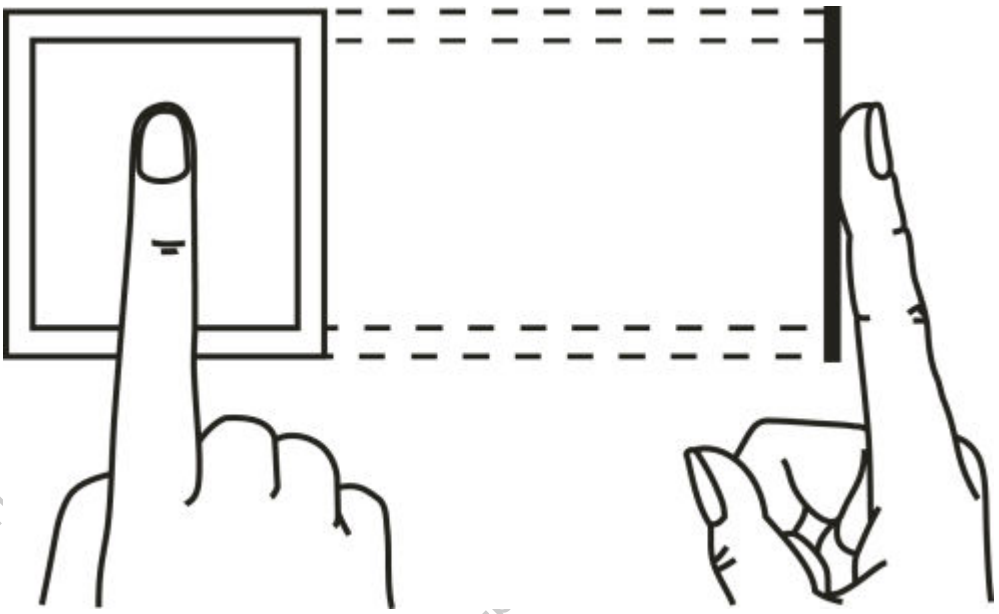
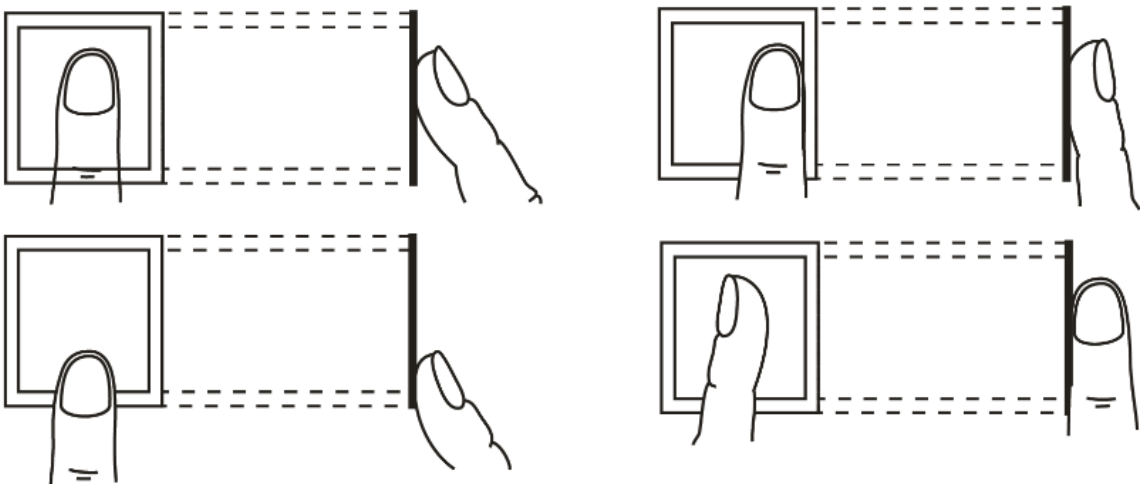


Рисунок Приложения 1–3 Неправильное расположение



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.