

Бесконтактный считыватель карт доступа Dahua DHI-ASR2100H/DHI-ASR2100H-D

Руководство пользователя



версия 1.0.0

Содержание

1 Описание устройства.....	1
1.1 Введение.....	1
1.2 Габаритные размеры.....	1
2 Схема подключения и монтаж.....	2
2.1 Обзор портов.....	2
2.2 Требования к подключению проводов.....	2
2.3 Подключение проводов.....	3
2.4 Процедура установки.....	4
3 Способы открытия двери.....	7
4 Световые и звуковые сигналы (индикация).....	8
5 Обновление системы.....	9
5.1 Обновление через SmartPSS Lite.....	9
5.2 Обновление через Config Tool.....	9
Приложение 1. Рекомендации по кибербезопасности.....	10

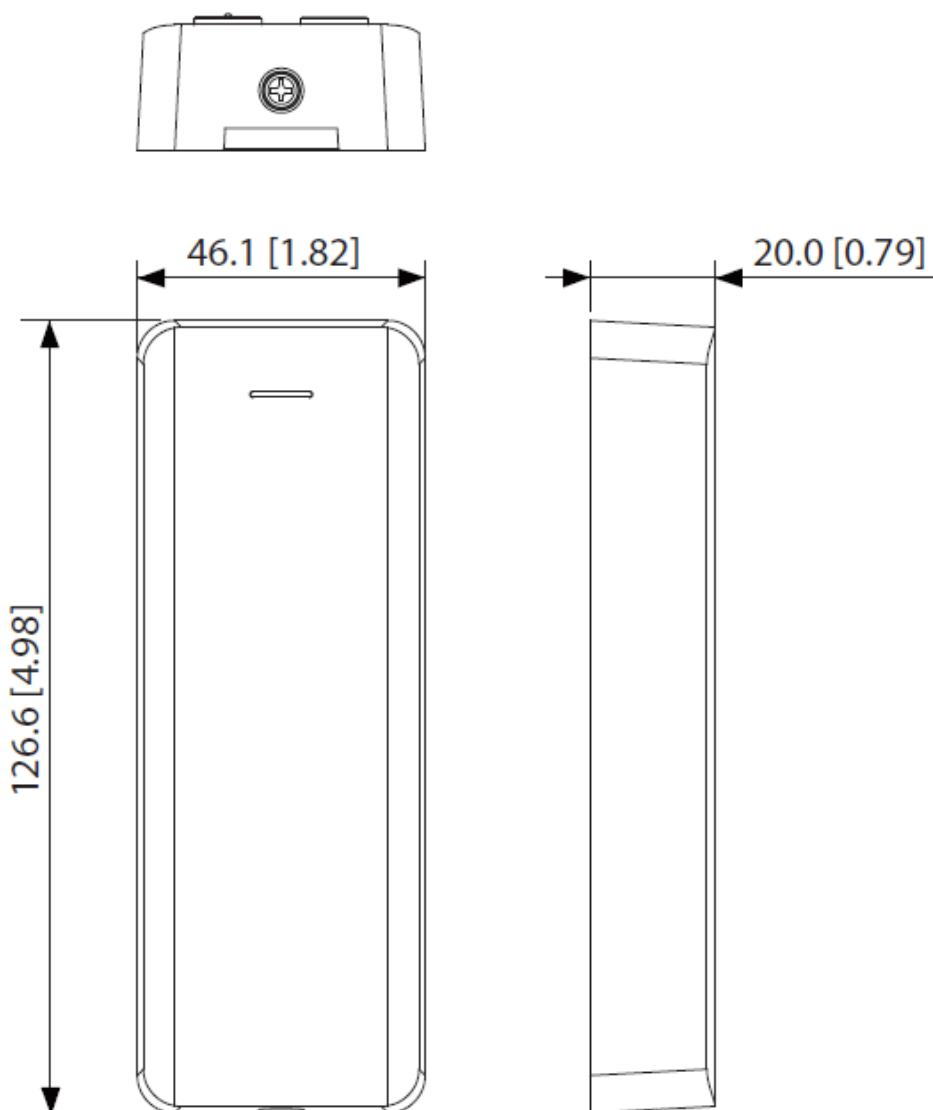
1 Описание устройства

1.1 Введение

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

1.2 Габаритные размеры

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



2 Схема подключения и монтаж

2.1 Обзор портов

Таблица 2–1 Описание портов

Цвет	Порт	Описание
Красный	RD+	PWR (12 VDC)
Черный	RD–	GND
Синий	CASE	Сигнал защиты от вскрытия
Белый	D1	Сигнал передачи Wiegand (еактивен только при использовании протокола Wiegand)
Зеленый	D0	
Коричневый	LED	Ответный сигнал Wiegand (активен только при использовании протокола Wiegand)
Желтый	RS–485_B	
Фиолетовый	RS–485_A	

2.2 Требования к подключению проводов

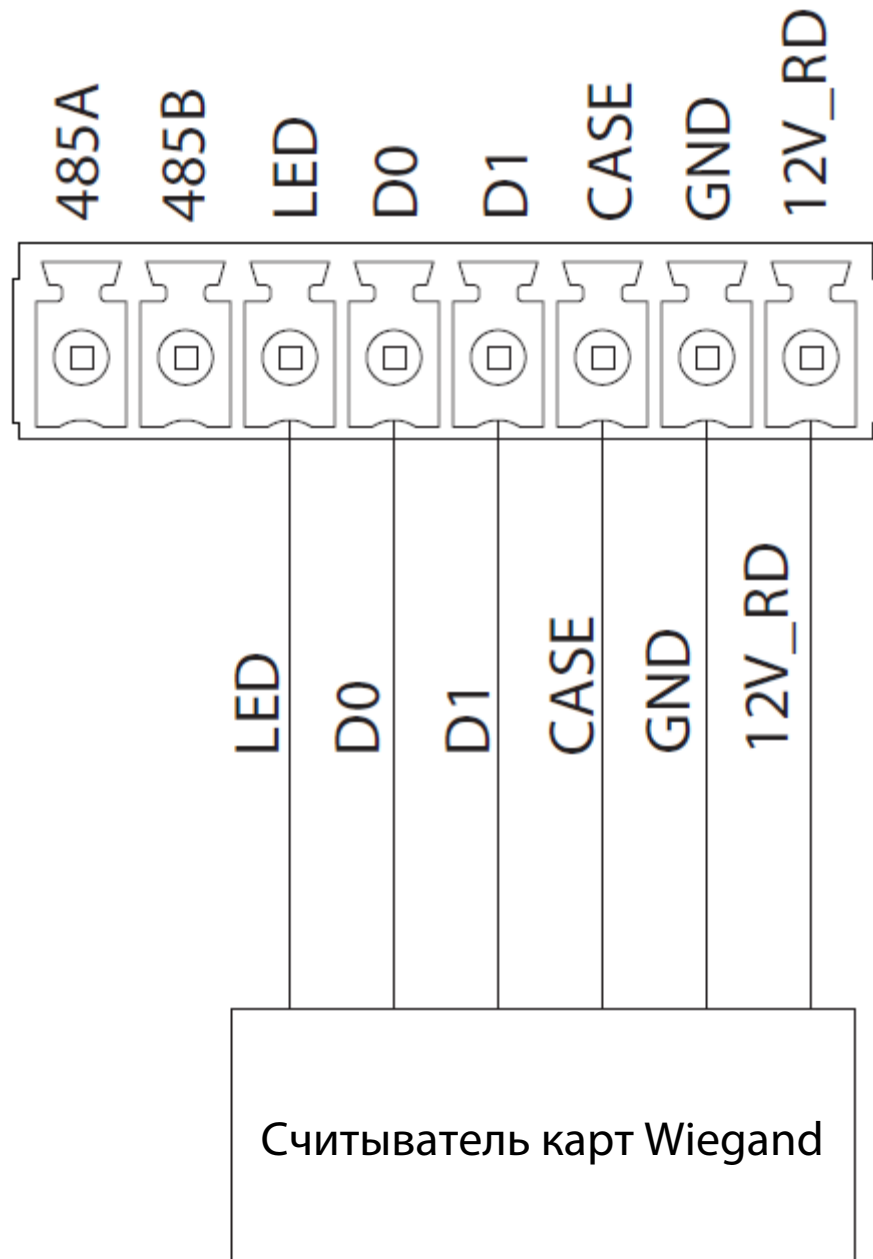
- Подключайте считыватель карт к портам Wiegand или RS-485 в зависимости от типа считывателя.
- Выбирайте провода в соответствии с требованиями к кабелям.

Таблица 2–2 Требования к подключению считывателя карт

Тип	Требования к сопротивлению	Требования к длине
Считыватель карт RS-485	Подключение проводов RS-485: сопротивление каждого провода должно быть ≤ 10 Ом.	≤ 100 м. Рекомендуется использовать экранированные провода UL1061 сечением 24 AWG
Считыватель карт Wiegand	Подключение проводов Wiegand: сопротивление каждого провода должно быть ≤ 2 Ом.	≤ 80 м. Рекомендуется использовать экранированные провода UL1061 сечением 18 AWG.

2.3 Подключение проводов

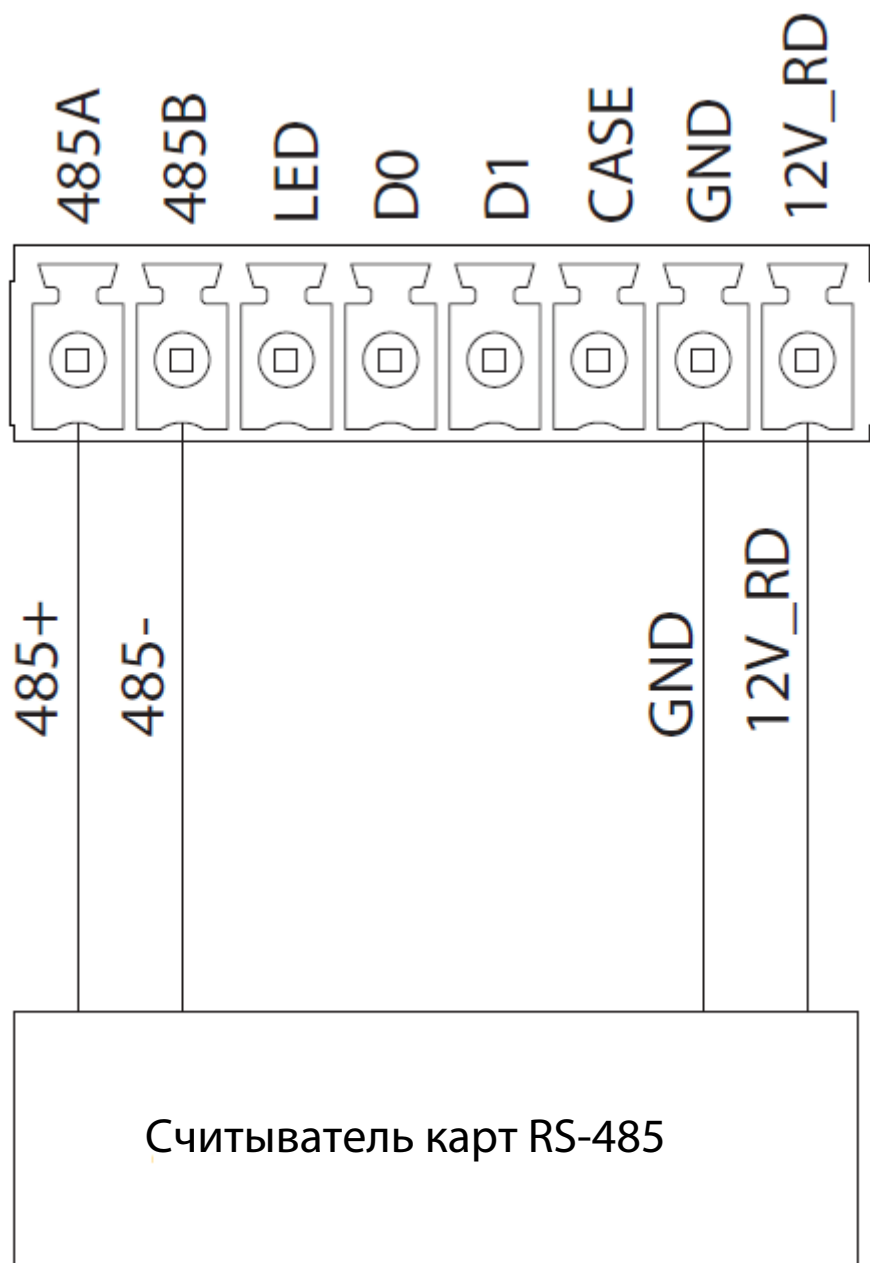
Рисунок 2–1 Схема подключения считывателя карт Wiegand





- Для считывателя карт Wiegand без клавиатуры по умолчанию поддерживается формат Wiegand 34, возможна настройка на Wiegand 26.
- Для считывателя карт Wiegand с клавиатурой нажмите 0034 для переключения на формат Wiegand 34 и 0026 для переключения на формат Wiegand 26.

Рисунок 2–2 Схема подключения считывателя карт RS-485



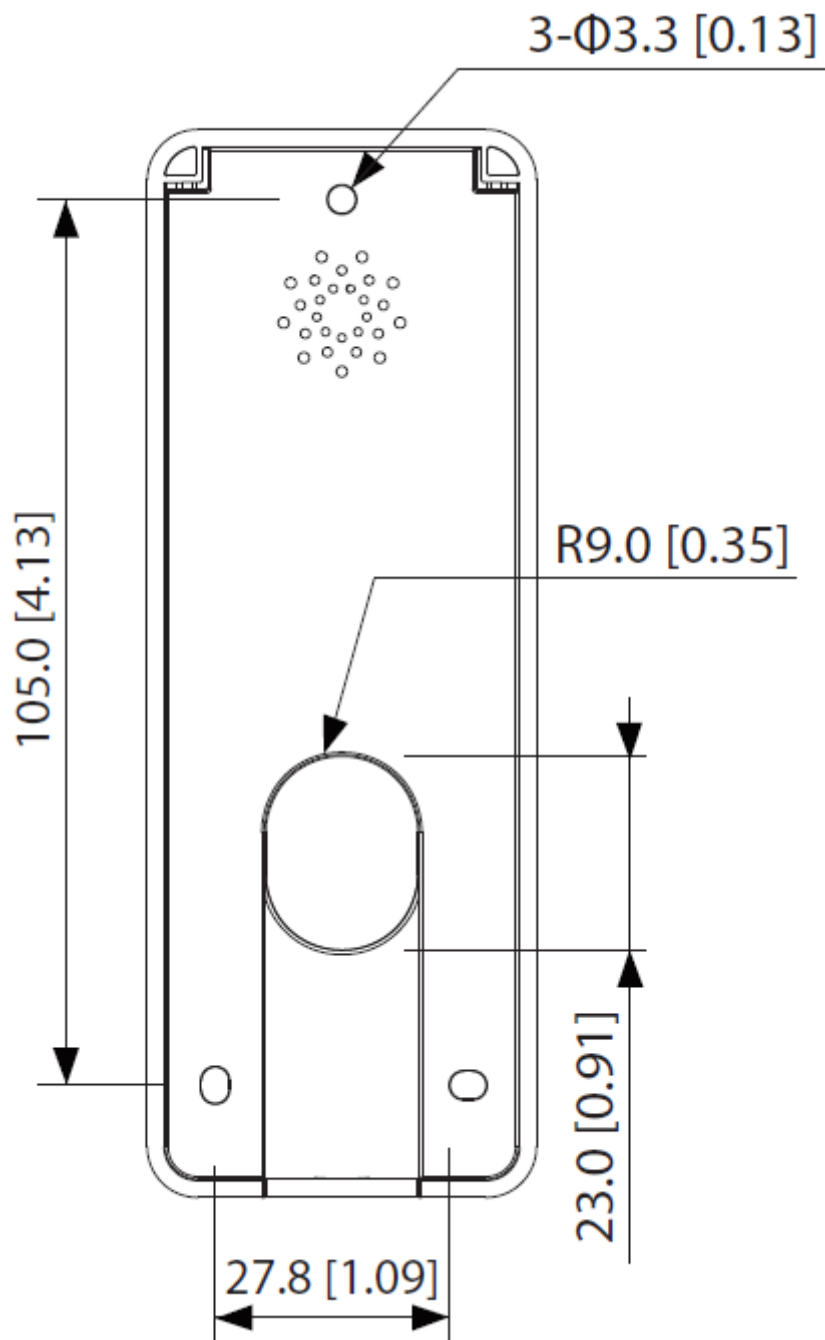
2.4 Процедура установки

Рекомендуемая высота установки — 1,3–1,5 м (от центра устройства до пола), но не более 2 м.

Порядок действий

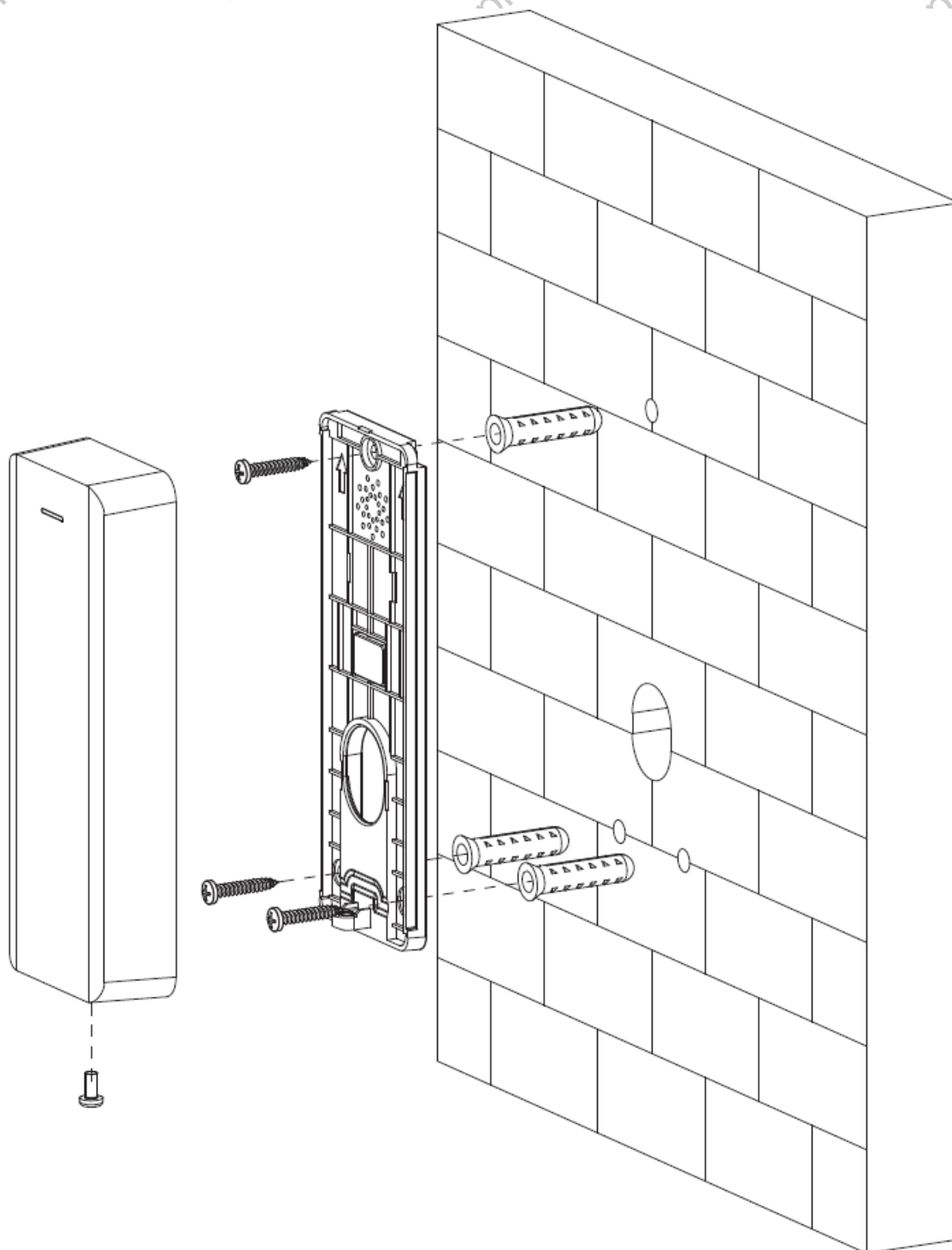
- Шаг 1** Просверлите в стене 3 монтажных отверстия в соответствии с отверстиями на кронштейне.
- Шаг 2** Вставьте в отверстия 3 анкерных болта.

Рисунок 2–3 Сверление отверстий (размеры в мм [дюймы])



- Шаг 3** Пропустите провода считывателя карт через прорезь в кронштейне.
- Шаг 4** Закрепите кронштейн на стене с помощью 3 винтов.
- Шаг 5** Установите считыватель карт на кронштейн снизу вверх.
- Шаг 6** Вкрутите 1 винт в нижней части для фиксации считывателя карт.

Рисунок 2-4 Сверление отверстий (размеры в мм [дюймы])



3 Способы открытия двери

Приложите карту к считывателю, чтобы открыть дверь. Для считывателя с клавиатурой также можно открыть дверь, введя пароль.

- **Открытие двери по общему паролю:** Введите общий пароль, затем нажмите #.
- **Открытие двери по пользовательскому паролю:** Введите идентификатор пользователя и нажмите #, затем введите пользовательский пароль и нажмите #.
- **Открытие двери по карте + пароль:** Приложите карту, введите пароль, затем нажмите #. Если пароль правильный, индикатор загорается зелёным, и зуммер издаёт один звуковой сигнал. Если пароль неверный, индикатор загорается красным, и зуммер издаёт 4 звуковых сигнала (при связи RS-485) или 3 звуковых сигнала (при связи Wiegand или если сигнальная линия не подключена).**

4 Световые и звуковые сигналы (индикация)

После включения питания считывателя карт он издаёт звуковой сигнал, и светодиод горит постоянным синим светом, что означает успешный запуск.



Прикладывайте только одну карту за раз. Не прикладывайте несколько карт одновременно.

Таблица 4–1 Световые и звуковые сигналы (индикация)

Функция	Сигналы (индикация)
Считыватель карт включён	Издаётся один звуковой сигнал, индикатор горит постоянным синим светом.
Антивандальная защита	Один звуковой сигнал продолжительностью 15 секунд.
Звук нажатия клавиши	Один звуковой сигнал.
Тревога	Один звуковой сигнал продолжительностью 15 секунд.
Прикладывание авторизованной карты (связь RS-485)	Один звуковой сигнал, индикатор загорается зелёным.
Прикладывание неавторизованной карты (связь RS-485)	4 звуковых сигнала, индикатор загорается красным.
Ошибка связи RS-485 и прикладывание авторизованной/неавторизованной карты	3 звуковых сигнала, индикатор загорается красным.
Прикладывание авторизованной карты (связь Wiegand)	Один звуковой сигнал, индикатор загорается зелёным.
Прикладывание неавторизованной карты (связь Wiegand)	Один звуковой сигнал, индикатор загорается красным.
Обновление основной программы или состояние BOOT при обновлении	Индикатор мигает синим до завершения обновления.

5 Обновление системы

5.1 Обновление через SmartPSS Lite

Предварительные требования

- Считыватель карт подключён к контроллеру доступа через провода RS-485.
- Контроллер доступа и считыватель карт включены (питание подано).

Порядок действий

Шаг 1 Установите **SmartPSS Lite** и войдите в систему, затем выберите «**Диспетчер устройств**» (Device Manager).

Шаг 2 Нажмите 

Рисунок 5–1 Выбор контроллера доступа

No.	Name	IP	Device Type	Device Model	Port	Channel Number	Online Status	SN	Operation
1	Device01	172.17.0.100	Access Controller	ASC2208C-S	37777	0/0/8/8	Online	6H029E1YAJ5FD7D	  

Шаг 3 Нажмите  и  для выбора файла обновления.

Шаг 4 Нажмите «**Обновить**» (Upgrade).

Индикатор считывателя карт мигает синим до завершения обновления, затем считыватель автоматически перезагружается.

5.2 Обновление через Config Tool

Предварительные требования

- Считыватель карт подключён к контроллеру доступа через провода RS-485.
- Контроллер доступа и считыватель карт включены (питание подано).

Порядок действий

Шаг 1 Установите и откройте **ConfigTool**, затем выберите «**Обновление устройства**» (Device upgrade).

Шаг 2 Нажмите  у контроллера доступа, затем нажмите 

Шаг 3 Нажмите «**Обновить**» (Upgrade).

Индикатор считывателя карт мигает синим до завершения обновления, затем считыватель автоматически перезагружается.

Приложение 1. Рекомендации по кибербезопасности

Обязательные меры по обеспечению базовой сетевой безопасности оборудования:

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 оборудования (например, NVR, DVR, IP-камеры и т. д.) в актуальном состоянии, чтобы система имела последние обновления безопасности и исправления. При подключении оборудования 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 оборудования:

1. Физическая защита

Рекомендуется обеспечить физическую защиту оборудования, особенно накопителей данных. Например, разместите оборудование 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 оборудованию, что позволит снизить риск подмены ARP (ARP-спуфинга).

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 оборудования:** 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 оборудования 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 оборудования 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.