



Беспроводной модуль дополнительного входа

Руководство пользователя



Введение

Общая информация






В настоящем руководстве пользователя описаны функции и работа беспроводного модуля дополнительного входа (далее "устройство"). Внимательно ознакомьтесь с этим руководством перед использованием устройства. Сохраните настоящее руководство, чтобы при необходимости обращаться к нему в будущем.

Модель

DHI-ARM320-W2; DHI-ARM320-W2(868)

Инструкции по технике безопасности

В руководстве могут встречаться следующие сигнальные слова.

Сигнальные слова	Значение
 DANGER	Указывает на высокую потенциальную опасность, которая, если ее не предотвратить, может привести к гибели или к серьезным травмам.
 WARNING	Указывает на среднюю или низкую потенциальную опасность, которая, если ее не предотвратить, может привести к травмам легкой или средней степени тяжести.
 CAUTION	Указывает на потенциальную опасность, которая, если ее не предотвратить, может привести к причинению ущерба имуществу, потере данных, ухудшению рабочих характеристик или иным непредсказуемым результатам.
 TIPS	Приводятся рекомендации, помогающие пользователю решить проблему или сэкономить время.
 NOTE	Приводится дополнительная информация в качестве пояснения и добавления к тексту.

Информация об изменениях в документе

Версия	История изменений	Дата публикации
Версия 1.0.0	Первая редакция	Апрель 2023 года

Уведомление о защите конфиденциальности

В качестве пользователя устройства или контролера данных вы можете собирать персональные данные других людей, в частности, изображения лиц, отпечатки пальцев и автомобильные номера. Вы обязаны соблюдать требования соответствующих местных законов и нормативных актов о защите конфиденциальности для обеспечения законных прав и интересов других людей путем принятия мер, включающих, помимо прочего, следующее: использование четких и хорошо заметных обозначений зоны видеонаблюдения для информирования людей о ее существовании, а также предоставление необходимой контактной информации.

О настоящем руководстве

- Настоящее руководство носит исключительно справочный характер. Указанные в руководстве параметры могут незначительно отличаться от реальных параметров продукта.
- Мы не несем ответственности за убытки, возникшие в результате эксплуатации продукта способами, которые не отвечают требованиям настоящего руководства.
- Руководство будет обновляться на основании законов и нормативных актов соответствующих юрисдикций. Для получения более подробной информации обратитесь к печатной версии руководства по эксплуатации или к версии на CD-ROM, либо отсканируйте QR-код или посетите наш официальный сайт. Настоящее руководство носит исключительно справочный характер. Между электронной и печатной версиями могут иметь место незначительные расхождения.
- Любые конструктивные элементы и программное обеспечение могут быть изменены без предварительного письменного уведомления. Обновления продукта могут стать причиной некоторых расхождений между параметрами реального продукта и информацией, изложенной в руководстве. Последнюю версию программного обеспечения и дополнительную документацию можно получить в службе поддержки клиентов.
- Существует вероятность ошибок печати или отклонений в описании функций, операций и технических данных. При возникновении каких-либо сомнений или разногласий мы оставляем за собой право окончательной трактовки.
- Если руководство (в формате PDF) не открывается, обновите установленное программное обеспечение для чтения файлов или попробуйте другое общедоступное программное обеспечение.
- Все товарные знаки, зарегистрированные товарные знаки и названия компаний в настоящем руководстве являются собственностью соответствующих владельцев.
- В случае появления любых проблем при использовании устройства посетите наш веб-сайт или обратитесь к поставщику или в службу поддержки.
- В случае каких-либо сомнений или противоречий мы оставляем за собой право окончательной трактовки.

Важные меры предосторожности и предупреждения

В настоящем разделе описываются правила надлежащего обращения с устройством и меры по предотвращению опасностей, включая опасность причинения ущерба имуществу.

Внимательно ознакомьтесь с содержимым данного раздела перед использованием устройства и соблюдайте указанные требования при работе с ним.

Требования к эксплуатации



- Перед использованием убедитесь, что источник питания устройства работает должным образом.
- Запрещается отсоединять шнур питания от устройства при включенном питании.
- Параметры электропитания устройства должны находиться в рекомендованном диапазоне.
- Транспортируйте, используйте и храните устройство при допустимых условиях влажности и температуры.
- Не допускайте попадания брызг или капель жидкости на устройство. Убедитесь, что на устройстве нет никаких предметов, наполненных жидкостью, которая может попасть внутрь устройства.
- Не разбирайте устройство.

Требования к установке



WARNING

- Перед подачей питания сначала подключите блок питания к устройству.
- Строго соблюдайте местные стандарты электробезопасности и убедитесь, что напряжение в месте установки стабильно и соответствует требованиям к питанию устройства.
- Не подключайте устройство более чем к одному источнику питания. В противном случае устройство может быть повреждено.



- Соблюдайте все меры безопасности и используйте все необходимые при высотных работах средства защиты.
- Не подвергайте устройство воздействию прямого солнечного света или излучению источников тепла.
- Не устанавливайте устройство во влажных, пыльных или задымленных местах.
- Устанавливайте устройство в хорошо проветриваемом месте и не закрывайте вентиляционные отверстия устройства.
- Используйте только сетевой адаптер или блок питания, поставленный производителем устройства.
- Блок питания устройства должен соответствовать классу ES1 по стандарту IEC 62368-1 и иметь мощность не более чем для класса PS2. Рекомендованные параметры электропитания указываются на этикетке данного устройства.
- Электроприборы класса I следует подключать в розетки с защитным заземлением.

Содержание

Введение	I
Важные меры предосторожности и предупреждения.....	III
1 Вступление	1
1.1 Обзор	1
1.2 Технические характеристики	1
2 Комплектация.....	3
3 Конструкция	4
3.1 Внешний вид устройства	4
3.2 Размеры	5
4 Добавление модуля на контроллер.....	6
5 Установка	7
6 Настройка.....	9
6.1 Просмотр состояния.....	9
6.2 Настройка модуля.....	10
Приложение 1 Рекомендации по обеспечению кибербезопасности	15

1 Вступление

1.1 Обзор

Беспроводной модуль дополнительного входа представляет собой преобразователь беспроводного интерфейса в проводной интерфейс (тревожные входы), к которым подключается сторонний проводной извещатель для пересылки его сигналов тревоги на контроллер охранной сигнализации Dahua. При получении тревоги от проводного извещателя, подключенного к беспроводному модулю входа, этот модуль отправляет сигнал тревоги на контроллер по радиочастотному каналу, а затем контроллер сообщает об этом программным платформам. С помощью приложения DMSS можно сконфигурировать различные типы тревог в зависимости от типа подключенных извещателей. Модуль оснащен трехосевым акселерометром для обнаружения несанкционированного перемещения устройства. Один из входов используется для подключения противокражной сигнализации внешних извещателей сторонних производителей. Модуль получает питание от трех батарей и может подавать питание на подключенные к нему извещатели.

1.2 Технические характеристики

В этом разделе приведены технические характеристики устройства. Пожалуйста, выберите те, которые соответствуют вашей модели.

Таблица 1-1 Технические характеристики

Тип	Параметр	Описание
Порты	Тревожный вход	2 (1 для тревоги и 1 для противокражной сигнализации)
	Вспомогательный выход питания	3.3 В, до 10 мА
	Кнопки	1 кнопка питания
	Удаленное обновление	Облачное обновление
	Уровень сигнала	Определение уровня сигнала
	Диапазон измерения (температура)	От -10°C до +55°C
Технические характеристики	Датчик	Трехосевой акселерометр
	Светодиодный индикатор	1 зеленый индикатор тревоги
	Применение	В помещении
	Рабочий ток	45 мкА (с интервалом опроса 1 минута, нормально открытый режим, питание для других устройств отсутствует, а обнаружение перемещения устройства не включено)

Тип	Параметр	Описание
	Ток тревоги	50 мА
Беспроводное подключение	Несущая частота	<ul style="list-style-type: none"> ARM320-W2(868): 868 МГц ~ 868.6 МГц ARM320-W2: 433.1 МГц ~ 434.6 МГц
	Мощность передачи	<ul style="list-style-type: none"> ARM320-W2(868): 14 дБм ARM320-W2: 9 дБм
	Тип связи	Двухсторонний
	Дальность передачи сигнала	<ul style="list-style-type: none"> ARM320-W2(868): До 1200 м на открытом пространстве ARM320-W2: До 800 м на открытом пространстве
	Шифрование	AES128
	Псевдослучайная перестройка рабочей частоты	Есть
	Питание	3 батареи CR123A
	Тип аккумулятора	CR123A
	Срок службы батареи	5 лет (питание для других устройств отсутствует)
	Потребляемая мощность	≤150мВт (питание для других устройств отсутствует)
	Рабочая температура	От -10°C до +55°C
	Рабочая влажность	10% ~ 90% (относительная)
	Размеры продукта	102 мм × 39 мм × 21.5 мм
	Масса нетто	77 г
	Масса брутто	135 г
	Монтаж	Накладной или в корпус стороннего устройства
	Внешний цвет	<ul style="list-style-type: none"> ARM320-W2(868): Нет ARM320-W2: Черный
	Сертификаты	CE
Защита от коррозии	Базовая защита	
Размеры в упаковке	95 мм × 43 мм × 139 мм	

2 Комплектация

Рисунок 2-1 Комплектация

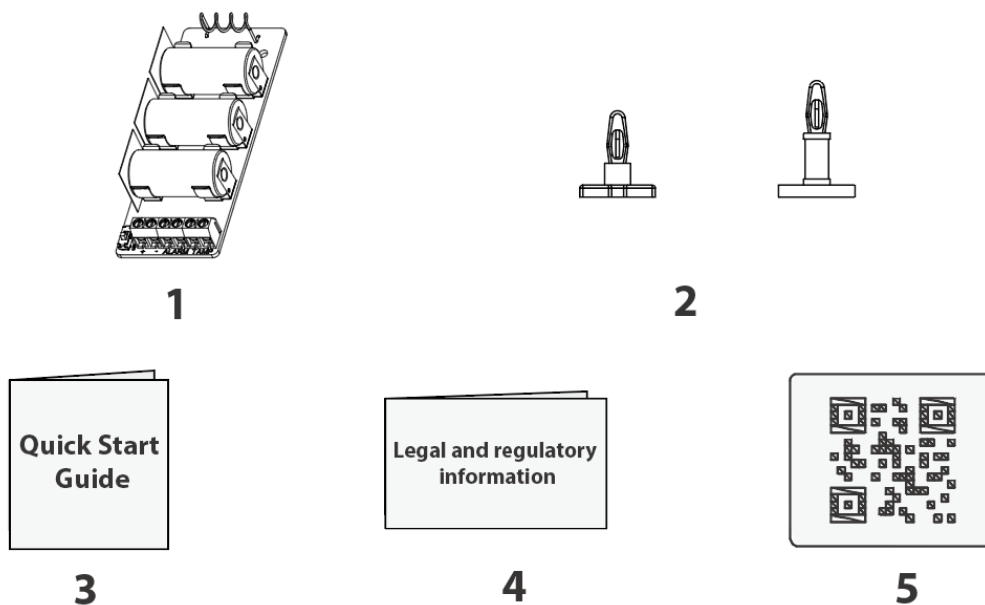


Таблица 2-1 Комплектация

№	Наименование	Количество	№	Наименование	Количество
1	Беспроводной модуль дополнительного входа	1	4	Юридическая и нормативная информация	1
2	Держатель	8	5	QR-код	1
3	Краткое руководство пользователя	1	–	–	–

3 Конструкция

3.1 Внешний вид устройства

Рисунок 3-1 Внешний вид устройства

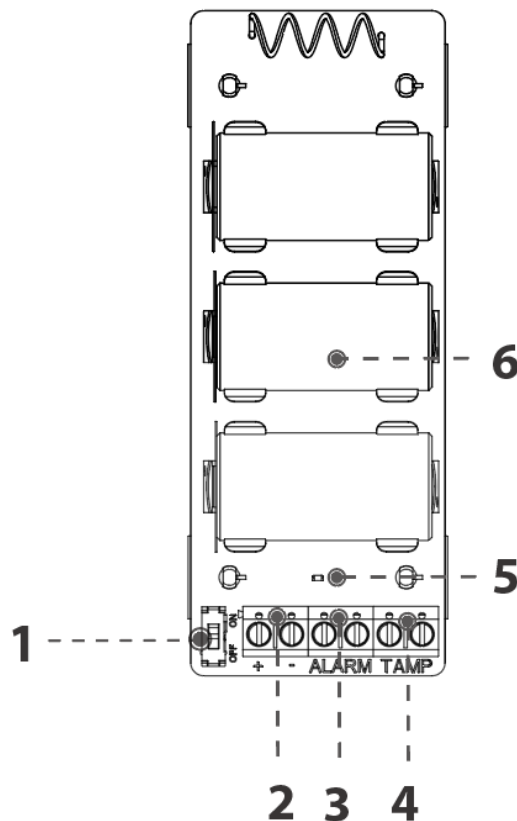
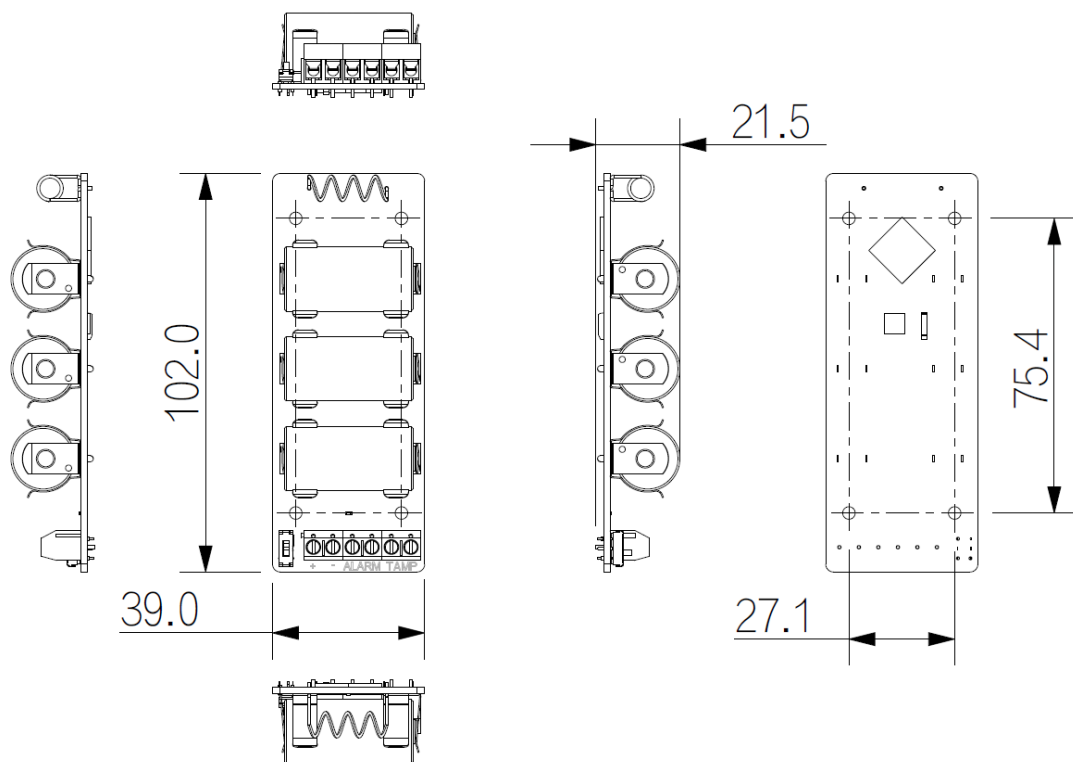


Таблица 3-1 Описание портов

№	Наименование	Описание
1	Выключатель	<ul style="list-style-type: none"> • Верхнее положение: Включение. • Нижнее положение: Выключение.
2	Разъем питания	<ul style="list-style-type: none"> • +: Положительный полюс. • -: Отрицательный полюс.
3	Тревожный вход	Тревожный вход для подключения устройств охранной сигнализации
4	Вход противокражной сигнализации	Сигнал тревоги при демонтаже устройства.
5	Индикатор	–
6	Батарея	–

3.2 Размеры

Рисунок 3-2 Размеры, мм



4 Добавление модуля на контроллер

Справочная информация

Перед подключением устройства к контроллеру установите на своем смартфоне приложение DMSS. В настоящем руководстве в качестве примера приведено описание мобильного приложения под iOS.



- Эта функция доступна только в приложении версии 1.99.420 или более новой при работе с контроллером с прошивкой версии V1.001.0000006.0.R.230404 или более новой.
- У вас уже должен быть создан аккаунт DMSS и в нем добавлен контроллер.
- Контроллер должен иметь стабильное подключение к Интернету.
- Контроллер должен быть снят с охраны.

Порядок действий

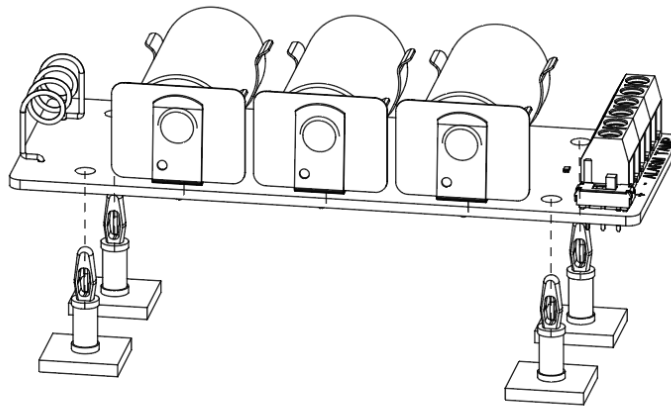
- Шаг 1 Перейдите на страницу контроллера, а затем нажмите **Периферийное устройство (Peripheral)**, чтобы добавить модуль.
- Шаг 2 Нажмите + для сканирования QR-кода на дне модуля, а затем нажмите **Далее (Next)**.
- Шаг 3 Нажмите **Далее (Next)**, после того как модуль будет найден.
- Шаг 4 Следуйте инструкциям на странице и включите модуль, а затем нажмите **Далее (Next)**.
- Шаг 5 Дождитесь сопряжения.
- Шаг 6 Измените имя модуля и выберите зону, а затем нажмите **Готово (Completed)**.

5 Установка

Порядок действий

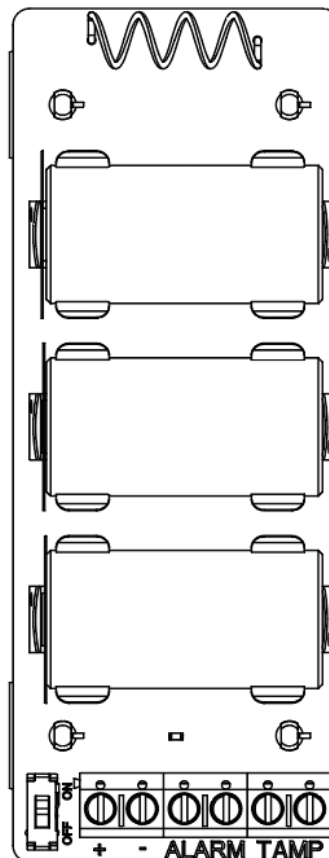
Шаг 1 Установите 4 держателя в плату модуля.

Рисунок 5-1 Держатели



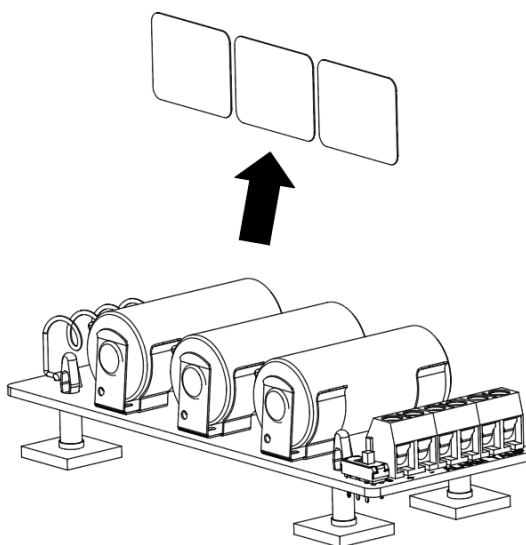
Шаг 2 Закрепите устройство на плоской поверхности.

Рисунок 5-2 Плоская поверхность



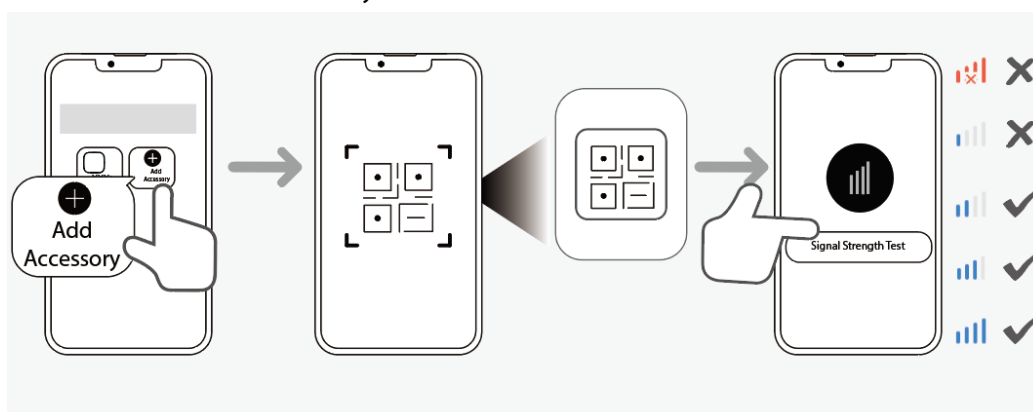
Шаг 3 Уберите лавсановую пленку.

Рисунок 5-3 Удаление лавсановой пленки



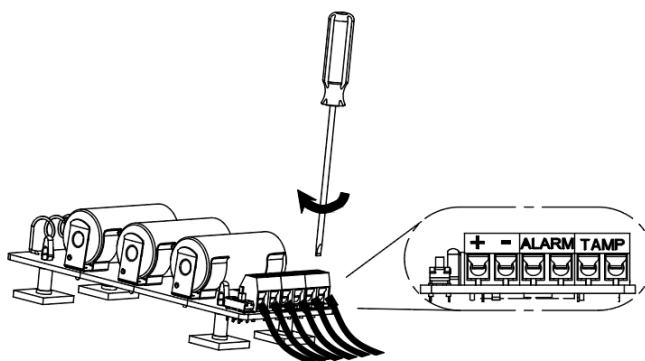
Шаг 4 Подключите беспроводной модуль дополнительного входа к контроллеру и проверьте уровень сигнала в месте установки.

Рисунок 5-4 Тест сигнала



Шаг 5 Подключите провода к 6 контактам. После подключения включите / выключите переключатель, чтобы проверить, работает ли устройство.

Рисунок 5-5 Подключение



























6 Настройка

6.1 Просмотр состояния

На странице контроллера выберите из списка периферийных устройств модуль дополнительного входа, и вы сможете просмотреть состояние модуля.

Таблица 6-1 Состояние

Параметр	Значение
Временно отключить (Temporary Deactivate)	<p>Показывает состояние работы устройства.</p> <ul style="list-style-type: none">  : Включено.  : Выключено. <p></p> <p>Эта функция доступна только в приложении версии 1.99.420 или более новой при работе с контроллером с прошивкой версии V1.001.0000006.0.R.230404 или новее.</p>
Температура (Temperature)	Температура окружающей среды.
Уровень сигнала (Signal Strength)	<p>Уровень сигнала показывает устойчивость связи между контроллером и модулем.</p> <ul style="list-style-type: none">  : Низкий.  : Слабый.  : Хороший.  : Отличный.  : Нет.
Уровень заряда батареи (Battery Level)	<p>Уровень заряда батареи модуля.</p> <ul style="list-style-type: none">  : Полный заряд.  : Достаточный заряд.  : Средний заряд.  : Низкий заряд.  : Низкий.
Состояние противокражной сигнализации внешнего устройства (External Device Tamper Status)	Отображает Включено (On) или Выключено (Off) .

Параметр	Значение
Состояние сетевого подключения (Online Status)	Состояние сетевого подключения модуля <ul style="list-style-type: none"> : В сети. : Не в сети.
Длительность задержки при входе (Entering Delay Time)	Задержка при входе.
Длительность задержки при выходе (Exiting Delay Time)	Время задержки при выходе.
Режим зоны круглосуточной охраны (24 H Protection Zone Status)	Активный режим зоны круглосуточной охраны. <ul style="list-style-type: none"> : Включено. : Выключено.
Передача через ретранслятор (Transmit through Repeater)	Состояние ретрансляции показывает пересылает ли модуль служебные сообщения на контроллер через ретранслятор.  Эта функция доступна только в приложении версии 1.99.420 или более новой при работе с контроллером с прошивкой версии V1.001.0000006.0.R.230404 или новее.
Состояние дверного звонка (Doorbell Status)	Открытое или замкнутое состояние контактов дверного звонка. <ul style="list-style-type: none"> : Открытое. : Замкнутое.
Внешний вход (External Input)	Показывает работоспособность внешнего входа модуля. <ul style="list-style-type: none"> : Нормально. : Неисправность.
Тревога движения (Movement Alarm)	<ul style="list-style-type: none"> : Тревога движения отключена. : Тревога движения включена.
Версия прошивки (Program Version)	Версия прошивки устройства.

6.2 Настройка модуля











На странице контроллера выберите из списка периферийных устройств модуль дополнительного входа, и затем нажмите  чтобы настроить его параметры.

Таблица 6-2 Описание параметров

Параметр	Описание
Конфигурация устройства (Device Configuration)	<ul style="list-style-type: none"> Просмотр имени, типа, серийного номера и модели устройства. Измените имя модуля, а затем нажмите Сохранить (Save), чтобы сохранить настройки.
Зона (Area)	Выбор зоны для данного устройства.
Зональный номер (Zone No.)	Номер, назначенный устройству в данной зоне, который невозможно изменить.
Временно отключить (Temporary Deactivate)	<ul style="list-style-type: none"> Нажмите Включить (Enable), после чего функция устройства будет включена, и информация будет отправляться на контроллер охранной сигнализации. Включить (Enable) по умолчанию. Нажмите Отключить (Disable), после чего функция устройства будет отключена, и информация не будет отправляться на контроллер охранной сигнализации.
Светодиодный индикатор (LED Indicator)	<p>Светодиодный индикатор (LED Indicator) включен по умолчанию.</p>  <ul style="list-style-type: none"> Если Светодиодный индикатор (LED Indicator) отключен, он будет оставаться выключенным независимо от того, нормально ли работает извещатель или нет. Эта функция доступна только в приложении версии 1.99.420 или более новой при работе с контроллером с прошивкой версии V1.001.0000006.0.R.230404 или более новой.
Зона круглосуточной охраны (24 H Protection Zone)	<ul style="list-style-type: none"> Если включена Зона круглосуточной охраны (24 H Protection Zone), даже если система снята с охраны, модуль расширения будет поставлен на охрану. Если выключена Зона круглосуточной охраны (24 H Protection Zone), только когда система поставлена на охрану, модуль расширения может быть поставлен на охрану. Модуль расширения не будет поставлен на охрану немедленно; он включится по истечению интервала опроса контроллера (по умолчанию 60 секунд). <p> Вы можете перейти на страницу контроллера, чтобы настроить интервал опроса контроллера. Подробная информация приведена в руководстве пользователя контроллера.</p>

Параметр	Описание
Режим В присутствии (Home Mode):	Включите режим В присутствии, и тогда выбранные периферийные устройства контроллера будут включены.
Режим задержки в режиме В присутствии (Delay Mode under Home Mode)	<p>Включите Режим задержки в режиме В присутствии (Delay Mode under Home Mode), выбранное периферийное устройство контроллера будет включено, и сигнал тревоги не будет обрабатываться до истечения заданного времени задержки.</p>  <p>Только сначала включите режим В присутствии (Home Mode), чтобы Режим задержки в режиме Дома (Delay Mode under Home Mode) вступил в силу.</p>
Длительность задержки (Delay Time)	<ul style="list-style-type: none"> ● Система предоставляет вам время покинуть или войти в охранную зону без тревоги. <ul style="list-style-type: none"> ◇ Время задержки постановки на охрану (Delay Time for Entering Arming Mode): При входе в зону сработает сигнализация, если система не будет снята с охраны до окончания времени задержки.  <p>Убедитесь, что время задержки входа в режим охраны не превышает 45 секунд для соответствия требованиям стандарта EN 50131-1.</p> ◇ Время задержки для выхода из режима постановки на охрану (Delay Time for Exiting Arming Mode): При нахождении в зоне и постановке системы на охрану сработает сигнализация, если не покинуть зону до окончания времени задержки. <ul style="list-style-type: none"> ● Выберите от 0 с до 120 с.  <p>Режим постановки на охрану вступит в силу по истечении времени задержки.</p>
Связывание с сиреной (Siren Linkage)	При срабатывании сигнализации устройство отправляет тревожное сообщение на контроллер с одновременным оповещением сиреной.
Связывание с тревожным видео (Alarm-video Linkage)	При срабатывании сигнализации устройство отправляет тревожное сообщение на контроллер со связанным видео.
Видеоканал (Video Channel)	Выберите нужный видеоканал.

Параметр	Описание
Внешний вход (External Input)	<ul style="list-style-type: none"> • Тип тревоги (Alarm Type): Выберите из списка тревог • Внешний вход (External Input): Выберите Нормально открытый (Normally Open), Нормально замкнутый (Normally Closed) или Импульсный (Pulse).
Внешняя противокражная сигнализация (External Tamper)	<ul style="list-style-type: none"> • Внешняя противокражная сигнализация (External Tamper): Нажмите для включения функции. • Проводной вход (Cable Connection): Выберите из Нормально открытый (Normally Open), Нормально замкнутый (Normally Closed).
Тревога перемещения (Movement Alarm)	<p>Модуль отслеживает перемещение каждые 5 секунд. Когда обнаруженное ускорение устройства достигнет определенного порога, сработает сигнализация о перемещении с миганием светодиодного индикатора.</p> <p>Нажмите <input type="checkbox"/> для включения функции Тревога перемещения (Movement Alarm), и нажмите <input type="checkbox"/> рядом для включения функции Связать тревогу перемещения со звуковым оповещателем (Link Movement Alarm to Siren).</p>
Выход внешнего питания (External Power Supply)	<ul style="list-style-type: none"> • Всегда открыт (Always Open): Модуль всегда будет обеспечивать внешним питанием другие устройства. • Отключен при снятии с охраны (Disabled while Disarmed): Когда модуль снят с охраны, выход внешнего питания отключен. • Всегда отключен (Always Disabled): Модуль никогда не будет обеспечивать внешним питанием другие устройства. <p></p> <ul style="list-style-type: none"> • Если выход внешнего питания модуля всегда открыт то срок службы батарей сократится. • Поддерживается подача питания с напряжением 3.3 В (DC).
Звонок (Chime)	<p>После включения, когда зона снята с охраны, при открытии магнитоконтактного извещателя сработает звуковой оповещатель для помещений.</p>
Температурная сигнализация (Over-temperature Alarm)	<p>Нажмите <input type="checkbox"/>, чтобы включить функцию Температурная сигнализация (Over-temperature Alarm), и тогда сигнализация сработает, когда температура в зоне, где установлен извещатель, будет выше или ниже заданной. Прокрутите шкалу температуры влево и вправо, чтобы установить самую низкую или самую высокую температуру, или нажмите + или -, чтобы установить диапазоны температур.</p>
Определение уровня сигнала (Signal Strength Detection)	<p>Проверка текущего значения уровня сигнала</p>

Параметр	Описание
Тест датчика (Detector Test)	<p>Нажмите Начать обнаружение (Start Detection), чтобы проверить состояние устройства.</p>  <ul style="list-style-type: none"> • Тест датчика не будет включен немедленно. он включится по истечении интервала опроса контроллера (по умолчанию 60 секунд). • Вы можете настроить интервал опроса на контроллере.
Мощность передатчика (Transmit Power)	<ul style="list-style-type: none"> • Можно выбрать следующие значения: высокая (high), низкая (low) и авто (automatic). • Чем выше мощность передачи, тем дальше может распространяться сигнал, но тем больше потребляемая мощность.  <ul style="list-style-type: none"> • Если вы выберете Низкая (Low), то устройство перейдет в режим пониженной чувствительности. • Мы рекомендуем вам выбрать Низкий (Low) при установке устройства, чтобы проверить уровень сигнала в месте установки, а затем установить Высокий (High) или Авто (Automatic). • Индикатор мигает при установке на Низкая (Low). • Эта функция доступна только в приложении версии 1.99.420 или более новой при работе с контроллером с прошивкой версии V1.001.0000006.0.R.230404 или более новой.
Облачное обновление (Cloud Update)	Обновление прошивки устройства по сети
Удалить (Delete)	<p>Удалить модуль</p>  <p>Перейдите на экран контроллера, выберите устройство из списка периферийных устройств и смахните его влево для удаления.</p>

Приложение 1 Рекомендации по обеспечению кибербезопасности

Кибербезопасность – это больше, чем просто популярное слово. Она в той или иной мере затрагивает любое устройство, подключенное к Интернету. IP-видеонаблюдение не застраховано от угроз кибербезопасности, но принятие основных мер по защите и укреплению безопасности сетей и сетевых устройств сделает их менее уязвимыми для атак. Ниже приведены несколько советов и рекомендаций от Dahua о том, как создать более защищенную систему безопасности.

Обязательные предосторожности для обеспечения базовой сетевой безопасности устройства:

1. Используйте надежные пароли

Обратите внимание на следующие рекомендации по установке паролей:

- Длина пароля должна составлять не менее 8 символов.
- Используйте по меньшей мере два типа символов, к которым относятся буквы верхнего и нижнего регистров, цифры и специальные символы.
- Не используйте имя аккаунта ни в прямом, ни в обратном порядке.
- Не используйте символы, идущие по порядку, например, «123», «abc» и т.д.
- Не используйте идущие подряд одинаковые символы, например, «111», «aaa» и т.д.

2. Своевременно обновляйте прошивку и клиентское программное обеспечение

- В соответствии со стандартной процедурой в индустрии высоких технологий мы рекомендуем обновлять прошивку вашего устройства (например, IP-видеорегистратора, цифрового видеорегистратора, IP-видеокамеры и т.д.), чтобы система была защищена последними обновлениями безопасности и исправлениями ошибок. Когда устройство подключено к общедоступной сети, рекомендуется включить функцию автоматической проверки обновлений, чтобы своевременно получать информацию об обновлениях прошивки, выпущенных производителем.
- Мы предлагаем вам загрузить и использовать последнюю версию клиентского программного обеспечения.

Желательные, но не обязательные рекомендации для повышения уровня сетевой безопасности вашего устройства:

1. Физическая защита

Мы предлагаем вам обеспечить физическую защиту устройства, особенно это касается устройств хранения. Например, установите устройство в специальное серверное помещение или шкаф для оборудования и организуйте продуманный контроль доступа и ключей, чтобы предотвратить физический доступ к устройству посторонних и повреждение оборудования, несанкционированное подключение съемного накопителя (например, USB-накопителя) или к последовательному порту) и т.д.

2. Регулярно меняйте пароли

Мы рекомендуем регулярно менять пароли, чтобы уменьшить риск угадывания или взлома.

3. Своевременно введите и обновляйте информацию для сброса пароля

Устройство поддерживает функцию сброса пароля. Своевременно введите

соответствующую информацию для сброса пароля, включая адрес e-mail конечного пользователя и контрольные вопросы для сброса пароля. Своевременно обновляйте эту информацию в случае ее изменения. При вводе контрольных вопросов для сброса пароля рекомендуется избегать таких, которые можно легко угадать.

4. Пользуйтесь функцией блокировки аккаунта

Функция блокировки аккаунта включена по умолчанию, и мы рекомендуем вам оставить ее включенной, чтобы гарантировать безопасность аккаунта. Если злоумышленник несколько раз попытается войти в систему с неправильным паролем, соответствующий аккаунт и исходящий IP-адрес будут заблокированы.

5. Измените порт HTTP по умолчанию и другие служебные порты

Мы предлагаем вам изменить порты HTTP и других служб по умолчанию на любое значение в диапазоне от 1024 до 65535, чтобы снизить риск того, что посторонние смогут угадать, какие порты вы используете.

6. Включите протокол HTTPS

Мы предлагаем вам включить протокол HTTPS, чтобы вы подключались к веб-интерфейсу по защищенному каналу связи.

7. Привязка MAC-адреса

Мы рекомендуем вам привязать IP-адрес и MAC-адрес шлюза к устройству, что снизит риск атаки типа ARP-spoofing.

8. Назначайте аккаунты и права доступа разумно

В соответствии с потребностями вашей деятельности и администрирования разумно добавляйте пользователей и назначайте им минимально необходимый набор прав доступа.

9. Отключите ненужные службы и используйте безопасные протоколы

Для снижения рисков рекомендуется отключать такие службы, как SNMP, SMTP, UPnP и т.д., если они не используются.

Настоятельно рекомендуется использовать безопасные реализации протоколов, включая, помимо прочего, следующие:

- SNMP: выберите протокол SNMP v3 и настройте надежные пароли шифрования и пароли аутентификации.
- SMTP: выберите протокол TLS для доступа к почтовому серверу.
- FTP: выберите протокол SFTP и установите надежные пароли.
- Точка доступа Wi-Fi: выберите режим шифрования WPA2-PSK и установите надежные пароли.

10. Шифрование аудио и видео

Если содержимое ваших аудио- и видеоданных очень важно или конфиденциально, мы рекомендуем вам использовать функцию шифрования, чтобы снизить риск похищения аудио- и видеоданных во время передачи.

Внимание: функция шифрования при передаче данных требует вычислительных ресурсов и приведет к некоторому снижению эффективности передачи данных.

11. Аудит безопасности

- Проверяйте пользователей, выполнивших вход на устройство: мы предлагаем вам регулярно проверять пользователей, выполнивших вход на устройство, чтобы отслеживать несанкционированный доступ.
- Проверяйте журналы устройства: просматривая журналы, вы можете узнать IP-адреса, которые использовались для входа на ваши устройства, и отслеживать основные

действия пользователей.

12. Сетевой журнал

Из-за ограниченного объема памяти устройства количество записей в журналах ограничено. Если вам необходимо сохранять записи журнала за длительный период времени, рекомендуется включить функцию сетевого журнала, чтобы обеспечить синхронизацию важных журналов с сервером сетевых журналов для отслеживания.

13. Создайте безопасную сетевую среду

Чтобы эффективнее обеспечить безопасность устройства и снизить потенциальные риски кибербезопасности, мы рекомендуем следующее:

- Отключите функцию преобразования портов на маршрутизаторе, чтобы исключить прямой доступа к устройствам локальной сети из внешней сети.
- Сеть должна быть сегментирована и изолирована в соответствии с фактическими потребностями обмена данными в ней. Если нет требований к организации связи между двумя подсетями, предлагается использовать VLAN и другие технологии для сегментирования сети, чтобы добиться изоляции сетей.
- Используйте протокол контроля доступа и аутентификации 802.1X, чтобы снизить риск несанкционированного доступа в локальных сетях.
- Включите функцию фильтрации IP-адресов и MAC-адресов, чтобы ограничить диапазон адресов, с которых разрешен доступ к устройству.

Дополнительная информация

Посетите Центр реагирования на чрезвычайные ситуации на официальном веб-сайте Dahua, чтобы ознакомиться с уведомлениями о безопасности и последними рекомендациями по безопасности.

БЕЗОПАСНЕЕ ОБЩЕСТВО, КАЧЕСТВЕННЕЕ ЖИЗНЬ

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Адрес: №1399, улица Биньянь, район Биньцзян, Ханчжоу, Китай | Веб-сайт: www.dahuasecurity.com | Почтовый индекс: 310053

E-mail: dhoverseas@dhvisiontech.com | Телефон: +86-571-87688888 28933188