



Беспроводной релейный модуль

Руководство пользователя








Введение

Общая информация

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

Инструкции по технике безопасности

В руководстве могут встречаться следующие сигнальные слова.

Сигнальные слова	Значение
 ОПАСНО!	Указывает на высокую потенциальную опасность, которая, если ее не предотвратить, может привести к гибели или к серьезным травмам.
 ОСТОРОЖНО!	Указывает на среднюю или низкую потенциальную опасность, которая, если ее не предотвратить, может привести к травмам легкой или средней степени тяжести.
 ВНИМАНИЕ!	Указывает на потенциальную опасность, которая, если ее не предотвратить, может привести к причинению ущерба имуществу, потере данных, ухудшению рабочих характеристик или иным непредсказуемым результатам.
 СОВЕТ	Приводятся рекомендации, помогающие пользователю решить проблему или сэкономить время.
 ПРИМЕЧАНИЕ	Приводится дополнительная информация в качестве дополнения к тексту.

Информация об изменениях в документе

Версия	История изменений	Дата публикации
Версия 1.0.0	Первая редакция	Ноябрь 2022 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 Внешний вид устройства	4
4 Добавление беспроводного релейного модуля на контроллер	5
5 Установка	6
5.1 Подключение	6
5.2 Установка беспроводного релейного модуля	6
6 Настройка	7
6.1 Просмотр состояния	7
6.2 Настройка релейного модуля	7
Приложение 1 Рекомендации по обеспечению кибербезопасности	10

1 Вступление

1.1 Обзор

Беспроводной релейный модуль – это устройство с выходом типа «сухой контакт» для коммутации напряжения 0 В ~ 36 В (DC). Такой тип выхода релейного модуля гальванически изолирован от его цепи питания. Релейный модуль можно использовать для управления подачей низковольтного питания на другие устройства. Устройство оснащено защитой от перенапряжения и защитой от перегрева.

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	
Функции	Световой индикатор	1 для нескольких состояний (сопряжение, питание, тревога)	
	Кнопки	1	
	Удаленное обновление	Облачное обновление	
	Уровень сигнала	Определение уровня сигнала	
Беспроводное подключение	Несущая частота	DHI-ARM7011-W2(868): 868 МГц ~ 868.6 МГц	DHI-ARM7011-W2: 433.1 МГц ~ 434.6 МГц
	Дальность передачи сигнала	DHI-ARM7011-W2(868): до 1200 м на открытом пространстве	DHI-ARM7011-W2: до 800 м на открытом пространстве
	Мощность передачи	DHI-ARM7011-W2(868): ограничение 25 мВт	DHI-ARM7011-W2: ограничение 15.8 мВт
	Тип связи	Двухсторонний	
	Шифрование	AES128	
	Псевдослучайная перестройка рабочей частоты	Есть	
Общие	Рабочая температура	От -10°C до +55°C	
	Температура хранения	От -10°C до +55°C	
	Рабочая влажность	10% ~ 90% (относительная)	

Тип	Параметр	Описание	
	Влажность хранения	10% ~ 90% (относительная)	
	Питание	DHI-ARM7011-W2(868) и DHI-ARM7011-W2: 7 ~ 24 В (DC)	
	Размеры продукта	39 мм × 33 мм × 19 мм	
	Размеры в упаковке	95 мм × 59.5 мм × 30.5 мм	
	Монтаж	Монтаж на стену	
	Масса нетто	45 г	
	Масса брутто	60 г	
	Сертификаты	DHI-ARM7011-W2(868): CE	DHI-ARM7011-W2: CE, FCC
	Материал корпуса	Поликарбонат, АБС-пластик	
Технические характеристики	Тестовый режим	Есть	
Порты	Тревожный вход	1 для противокражной сигнализации, НО/НЗ	
	Релейный выход	1, НО/НЗ (0 ~ 36 В (DC), до 5 А)	

2 Комплектация

Рисунок 2-1 Комплектация

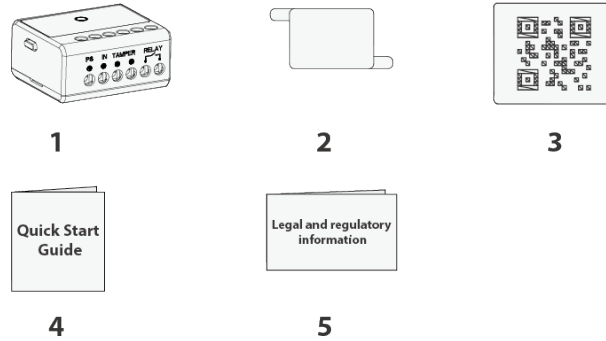


Таблица 2-1 Комплектация

№	Наименование	Количество	№	Наименование	Количество
1	Релейный модуль	1	4	Краткое руководство пользователя	1
2	Двухсторонняя клейкая лента	1	5	Юридическая и нормативная информация	1
3	QR-код	1	–	–	–

3 Внешний вид устройства

Рисунок 3-1 Внешний вид устройства

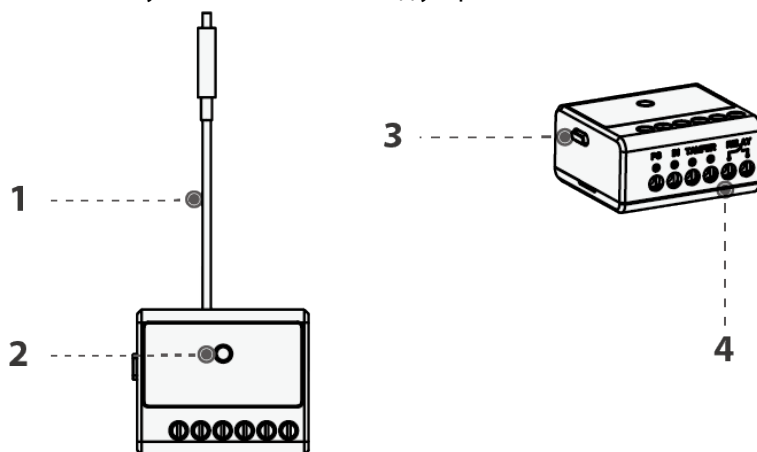


Таблица 3-1 Конструкция

№	Наименование	Описание
1	Антенна	Посылает и принимает сигналы.
2	Индикатор	<ul style="list-style-type: none"> ● Нажмите и удерживайте кнопку в течение 2 секунд, чтобы система вошла в режим сопряжения. <ul style="list-style-type: none"> ◇ Постоянно загорается на 1 секунду, затем выключается на 0.5 секунды, а затем постоянно включается: Сопряжение прошло успешно. ◇ Медленно мигает 3 секунды, а затем выключается: Сопряжение не удалось. ● После включения питания нажмите и удерживайте кнопку в течение 2 секунд, а затем устройство выключится.
3	Кнопка питания	
4	Подключение клемм	Реле может быть подключено к источнику питания 6.5 ~ 36.5 В (DC). <ul style="list-style-type: none"> ● PS IN: Клемма питания. Для прямого подключения кабеля питания ● RAMPER: Клемма для внешнего устройства. Подключается к внешнему устройству для срабатывания противокражной сигнализации. ● RELAY: Соединение между выходной клеммой и клеммой питания, которое контролируется посредством размыкания и замыкания встроенного реле.

4 Добавление беспроводного релейного модуля на контроллер

Перед подключением реле 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 DMSS версии 1.99.200 или более новой при работе с контроллером с прошивкой версии V1.001.0000004.0.R.221104 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.

Шаг 1 Перейдите на страницу контроллера, а затем нажмите **Периферийное устройство (Peripheral)**, чтобы добавить реле.

Шаг 2 Нажмите + для сканирования QR-кода на дне релейного модуля, а затем нажмите **Далее (Next)**.

Шаг 3 Нажмите **Далее (Next)**, после того как релейный 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)**.

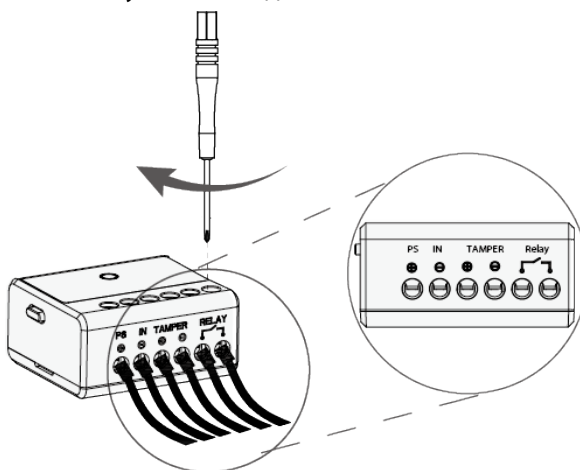
5 Установка

Перед установкой подключите релейный модуль к контроллеру и проверьте уровень сигнала в месте установки. Мы рекомендуем устанавливать модуль в местах с уровнем сигнала не менее 2 делений.

5.1 Подключение

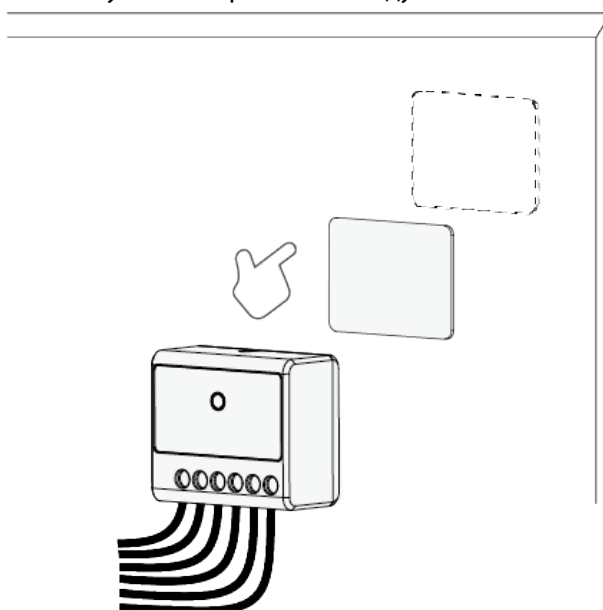
- Реле может быть подключено к источнику питания 6.5 ~ 36.5 В (DC).
- Исходя из его размеров, вы можете установить реле в глубокую монтажную коробку, внутри корпуса электроприбора или в распределительный щит.

Рисунок 5-1 Подключение



5.2 Установка беспроводного релейного модуля

Рисунок 5-2 Крепление модуля












6 Настройка

Вы можете просматривать и редактировать общую информацию релейного модуля.

6.1 Просмотр состояния

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

Таблица 6-1 Состояние контроллера

Параметр	Преимущества
Временно отключить (Temporary Deactivate)	Показывает состояние работы устройства. <ul style="list-style-type: none"> ●  : Включено. ●  : Выключено.
Уровень сигнала (Signal Strength)	Уровень сигнала показывает устойчивость связи между контроллером и устройством. <ul style="list-style-type: none"> ●  : Низкий. ●  : Слабый. ●  : Хороший. ●  : Отличный. ●  : Нет.
Входное напряжение (Input Voltage)	Значение напряжения на входе питания.
Состояние на выходе (Output Status)	Состояние выходного реле
Состояние сетевого подключения (Online Status)	Состояние сетевого подключения модуля <ul style="list-style-type: none"> ●  : В сети. ●  : Не в сети.
Передача через ретранслятор (Transmit through Repeater)	Состояние ретрансляции показывает пересылает ли модуль служебные сообщения на контроллер через ретранслятор.
Версия прошивки (Program Version)	Версия прошивки устройства.

6.2 Настройка релейного модуля





На странице контроллера выберите из списка периферийных устройств релейный модуль, 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.
Временно отключить (Temporary Deactivate)	<p>Следует ли отправлять информацию с датчиков на контроллер охранной сигнализации.</p> <ul style="list-style-type: none"> Нажмите Включено (Enable), и тогда модуль будет отправлять тревожные сообщения на контроллер. Включено (Enable) по умолчанию. Нажмите Отключено (Disable), и тогда модуль не будет отправлять тревожные сообщения на контроллер.
Тип выхода (Output Type)	Выберите Нормально открытый (Normally Open) , Нормально замкнутый (Normally Closed) . Нормально замкнутый (Normally Closed) установлен по умолчанию.
Режим выхода (Output Mode)	<p>Выберите Бистабильный режим (Steady State) или Импульсный режим (Pulse). Импульсный режим (Pulse) установлен по умолчанию.</p> <p>При выборе Импульсный режим (Pulse) вы можете установить длительность импульса.</p>
Светодиодный индикатор (LED Indicator)	<p>Светодиодный индикатор включен по умолчанию.</p>  <p>Если Светодиодный индикатор (LED Indicator) отключен, он будет оставаться выключенным независимо от того, нормально ли работает модуль или нет.</p>

Параметр	Описание
Настройка сценариев (Scenario Setting)	Настройте сценарии модуля для выполнения соответствующего действия Нажмите Создать сценарий (Create Scenario) , вы можете выбрать Сценарий с постановкой или снятием с охраны (Arming/Disarming Linkage Scenario) , Сценарий с тревогой (Alarm Linkage Scenario) или Сценарий с расписанием (Scheduled Linkage Scenario) . <ul style="list-style-type: none"> ● Сценарий с постановкой или снятием с охраны (Arming/Disarming Linkage Scenario): После настройки названия сценария и выбора зоны привязки вы можете включить или отключить Активация выхода при постановке на охрану (Arming Linkage Output Module), Активация выхода при снятии с охраны (Disarming Linkage Output Module), или Активация выхода при включении режима В присутствии (Home Mode Linkage Output Module). ● Сценарий с тревогой (Alarm Linkage Scenario) ● Сценарий с расписанием (Scheduled Linkage Scenario): После настройки имени сценария и включения Сценарий с расписанием (Scheduled Linkage Scenario), вы можете настроить время и периоды расписания.
Внешняя противокражная сигнализация (External Tamper)	После включения Внешняя противокражная сигнализация (External Tamper) сработает противокражная сигнализация.
Определение уровня сигнала (Signal Strength Detection)	Проверка текущего значения уровня сигнала.
Мощность передатчика (Transmit Power)	<ul style="list-style-type: none"> ● Можно выбрать следующие значения: высокая (high), низкая (low) и авто (automatic). ● Чем выше уровень мощности передачи, тем дальше может передаваться сигнал, но при этом увеличивается энергопотребление.  <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).
Удалить (Delete)	Удаление модуля.  Перейдите на экран контроллера, выберите модуль из списка устройств и смахните его влево для удаления.

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-видеорегастратора, цифрового видеорегастратора, 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