Беспроводной брелок

Руководство пользователя

ZHEJIANG DAHUA VISION TECHNOLOGY CO.LTD.

Версия 1.1.1

Введение

Общая информация

В настоящем руководстве пользователя описаны функции и работа беспроводного брелока (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 1.1.1	Исправлено время автономной работы.	Июнь 2023 года
Версия 1.1.0	• Добавлены технические характеристики. • Обновлены описания параметров. • Обновлены изображения.	Январь 2022 года
Версия 1.0.0	Первая редакция	Октябрь 2021 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

- 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

1 Вступление

1.1 Обзор

Беспроводной брелок – это миниатюрный пульт дистанционного управления, который подключается к контроллеру и управляет системой сигнализации в вашем доме. Он выполняет отправку беспроводных сигналов в систему сигнализации, которая распознает сигнал и затем выполняет функцию, назначенную данной зоне.

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	Световой индикатор	1 двухцветный индикатор состояния (зеленый: нормальный, красный: неисправность)	
	Кнопки	4 (В присутствии (Home), В отсутствие (Away), Снятие с охраны (Disarm) и SOS)	
Функции	Удаленное обновление	Облачное обновление	
	Сигнализация разрядки батареи	Есть	
Беспроводное подключение	Несущая частота	DHI-ARA24-W2(868): 868 МГц ~ 868.6 МГц	DHI-ARA24-W2: 433.1 МГц ~ 434.6 МГц
	Дальность передачи сигнала	DHI-ARA24-W2(868): до 900 м на открытом пространстве	DHI-ARA24-W2: до 500 м на открытом пространстве
	Тип связи	Двухсторонний	
	Шифрование	AES128	
	Псевдослучайная перестройка рабочей частоты	Есть	
Общие	Питание	Батарея CR2032	
	Напряжение батареи	3 В (DC)	
	Минимальное напряжение	1.8 В (DC)	
	Порог низкого заряда	2.6 В (DC)	

Тип	Параметр	Описание	
	Порог восстановления батареи	2.65 В (DC)	
	Энергопотребление	Ток в покое 3 мкА Максимальный ток 50 мА	
	Тип источника питания	TYPE C	
	Срок службы батареи	3 года	
	Потребляемая мощность	DHI-ARA24-W2(868): ≤100 мВт	DHI-ARA24-W2: ≤85 мВт
	Рабочая среда	В помещении: от -10°C до +55°C Сертифицированная температура: от -10°C до +40°C	
	Рабочая влажность	10% ~ 90% (относительная)	
	Размеры продукта	60 мм × 39.5 мм × 14.2 мм	
	Размеры в упаковке	135 мм × 98.5 мм × 27.8 мм	
	Масса нетто	20 г	
	Масса брутто	65 г	
	Корпус	Поликарбонат, АБС-пластик	
	Тип ACE	Тип B	
Сертификаты	DHI-ARA24-W2(868): EN 50131-1:2006 + A1: 2009 + A2:2017 + A3:2020 EN 50131-5-3:2017 EN 50131-6:2017 EN 50131-3:2009 Класс безопасности 2 Класс условий эксплуатации II CE		DHI-ARA24-W2: CE FCC

2 Комплектация

Проверьте содержимое упаковки в соответствии со следующим списком. Если вы обнаружите повреждение или неполную комплектацию, свяжитесь с поставщиком.

Рисунок 2-1 Комплектация

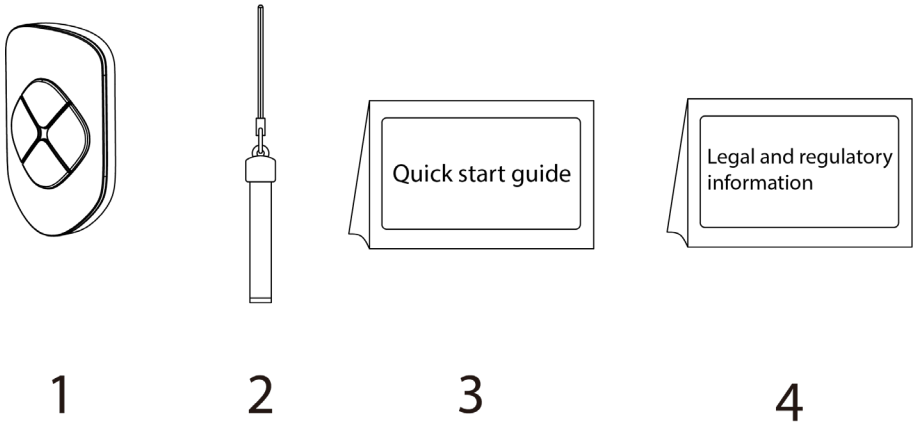


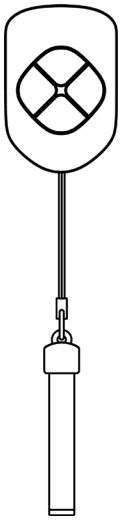
Таблица 2-1 Комплектация

№	Наименование	Количество
1	Беспроводной брелок	1
2	Шнурок	1
3	Краткое руководство пользователя	1
4	Юридическая и нормативная информация	1

3 Конструкция

3.1 Внешний вид устройства

Рисунок 3-1 Внешний вид устройства



3.2 Функциональные кнопки

Рисунок 3-2 Функциональные кнопки

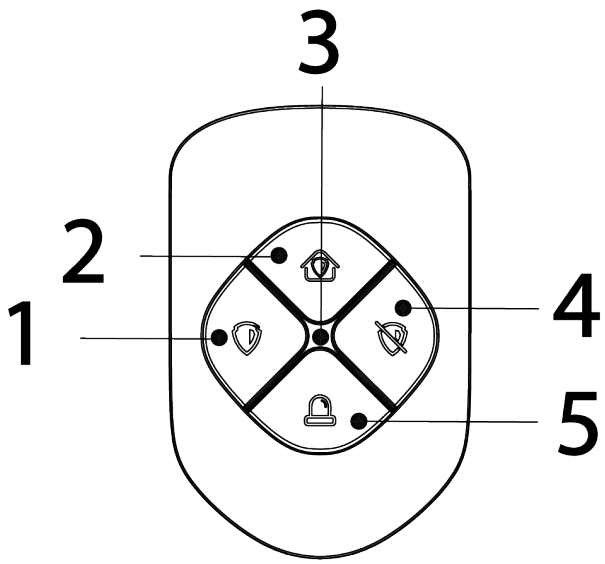


Таблица 3-1 Описание кнопок

№	Наименование	Описание
1	Кнопка постановки на охрану	Нажмите кнопку один раз, чтобы поставить на охрану систему. После нажатия кнопки постановки на охрану, если система не выполнила постановку на охрану, вы можете нажать кнопку еще раз в течение 10 секунд, чтобы отменить предупреждения, которые привели к предыдущему сбою постановки на охрану, и успешно поставить на охрану.  • Существует множество причин сбоя постановки на охрану, включая обнаружение злоумышленников другими извещателями, неисправности извещателей, срабатывание противокражной сигнализации и другие ситуации, которые могут прервать процесс постановки на охрану. • Если вы поставите систему на охрану во время процесса задержки при выходе, система немедленно начнет постановку на охрану. Если вы снимете с охраны во время этого процесса, система прекратит процес постановки на охрану. • Сбои, возникающие во время процесса задержки при выходе, функционируют иначе, чем при типичном процессе постановки на охрану, описанном выше.

№	Наименование	Описание
2	В присутствии (Home Mode)	Нажмите кнопку В присутствии (Home mode), после чего выбранные периферийные устройства, настроенные для этого режима, будут переключены в режим охраны В присутствии. После нажатия кнопки В присутствии (Home Mode), если система не включается, вы можете нажать кнопку еще раз в течение 10 секунд, чтобы отменить предупреждения, которые привели к предыдущему сбою постановки на охрану, и успешно поставить на охрану.  • Существует множество причин сбоя постановки на охрану, включая обнаружение злоумышленников другими извещателями, неисправности извещателей, срабатывание противокражной сигнализации и другие ситуации, которые могут прервать процесс постановки на охрану. • Если вы поставите охрану во время процесса задержки при выходе, система немедленно начнет постановку на охрану; если вы снимете с охраны во время такого процесса, система отменит постановку на охрану. • Сбои, возникающие во время процесса задержки при выходе, функционируют иначе, чем при типичном процессе постановки на охрану, описанном выше.

№	Наименование	Описание
3	Индикатор	• Постоянно светится зеленым цветом 2 секунды: Включение. • Быстро мигает зеленым цветом: Режим сопряжения. • Постоянно светится зеленым цветом 2 секунды: Сопряжение прошло успешно. • Мигает зеленым цветом 3 раза: Сопряжение не удалось. • Медленно мигает зеленым цветом: Задержка при выходе. • Мигает зеленым цветом один раз: Команда была успешно отправлена. • Мигает красным цветом один раз: Не удалось отправить команду. • Мигает зеленым цветом один раз после успешной отправки команды: Команда была успешно выполнена. • Мигает красным цветом один раз после успешной отправки команды: Задержка с ответом на команду. • Мигает красным цветом два раза после успешной отправки команды: Не удалось выполнить команду. • Мигает красным цветом, а затем выключается: Низкий заряд батареи.
4	Кнопка снятия с охраны	Нажмите кнопку один раз, чтобы снять с охраны.
5	SOS	Нажмите тревожную кнопку, и затем брелок отправит сигнал тревоги в систему охранной сигнализации.

4 Добавление брелока на контроллер

Подготовка

Конфигурация устройства выполняется в приложении DMSS. Перед подключением брелока к контроллеру, у вас уже должен быть создан аккаунт DMSS и в нем добавлен контроллер. Подробная информация о добавлении контроллера приведена в соответствующем руководстве пользователя устройства.

- Контроллер должен иметь стабильное подключение к Интернету.
- Контроллер должен быть снят с охраны.

Справочная информация

Вы можете подключить брелок к контроллеру. В этом руководстве пользователя в качестве примера описан порядок действий для пользователей iOS.

Порядок действий

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

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

Шаг 3 Нажмите **Далее (Next)**, после того как брелок будет найден.

Шаг 4 Следуйте инструкциям на экране и нажмите и одновременно, а затем нажмите **Далее (Next)**.

Шаг 5 Дождитесь сопряжения.

Шаг 6 Измените имя брелока, а затем нажмите **Готово (Completed)**.

5 Настройка брелока

Вы можете просматривать и редактировать общую информацию брелока.

5.1 Просмотр состояния

На странице контроллера выберите брелок из списка периферийных устройств, и вы сможете просмотреть его состояние.

Таблица 5-1 Состояние

Параметр	Описание
Временно отключить (Temporary Deactivate)	Показывает состояние работы устройства. ● : Включено. ● : Отключена только противокражная сигнализация. ● : Выключено. Эта функция доступна только в приложении DMSS версии 1.96 или более новой для контроллера с прошивкой версии V1.001.0000000.6.R.211215 или более новой и брелока с прошивкой V1.000.0000001.0.R.20211203 или более новой.
Уровень заряда батареи (Battery Level)	Уровень заряда батареи брелока. ● : Полный заряд. ● : Достаточный заряд. ● : Средний заряд. ● : Низкий заряд.
Состояние SOS (SOS Status)	Состояние сигнала SOS.
Состояние ретрансляции (Relay Status)	Состояние ретрансляции показывает пересылает ли брелок дополнительные сообщения на контроллер через ретранслятор. Эта функция доступна только в приложении DMSS версии 1.96 или более новой для контроллера с прошивкой версии V1.001.0000000.6.R.211215 или более новой и брелока с прошивкой V1.000.0000001.0.R.20211203 или более новой.
Версия прошивки (Program Version)	Версия прошивки устройства.

5.2 Настройка брелока

На странице контроллера выберите из списка периферийных устройств брелок, и затем

нажмите , чтобы настроить его параметры.

Таблица 5-2 Описание параметров брелока

Параметр	Описание
Конфигурация устройства (Device Configuration)	• Просмотр имени, типа, серийного номера и модели устройства. • Измените имя устройства, а затем нажмите **Сохранить (Save)**, чтобы сохранить настройки.
Зона (Area)	• Просмотр существующей зоны. • Добавьте зону, которую вы хотите поставить на охрану, а затем нажмите **Сохранить (Save)**, чтобы сохранить конфигурацию.
Временно отключить (Temporary Deactivate)	• Нажмите **Включено (Enable)**, после чего функция сирены будет включена. **Включено (Enable)** по умолчанию. • Нажмите **Отключена только противокражная сигнализация (Only Disable Tamper Alarm)**, и тогда система будет игнорировать только тревожные сообщения о противокражной сигнализации. • Нажмите **Отключено (Disable)**, после чего функция будет выключена.
Светодиодный индикатор (LED Indicator)	**Светодиодный индикатор (LED Indicator)** включен по умолчанию в мобильном приложении. Вам также необходимо нажать любую кнопку на брелоке, чтобы включить эту функцию. Подробнее о светодиодной индикации см. в разделе "3.2 Функциональные кнопки". • Если **Светодиодный индикатор (LED Indicator)** отключен, он будет оставаться выключенным независимо от того, нормально ли работает брелок или нет. • Эта функция доступна только в приложении DMSS версии 1.96 или более новой для контроллера с прошивкой версии V1.001.0000000.4.R.211014 или более новой и брелока с прошивкой V1.000.0000001.0.R.20210818 или более новой.
Назначение прав доступа (Control Permissions)	Выберите зону для управления брелоком.
Сигнал тревоги SOS (SOS Alarm)	Если включено, сигналы тревоги SOS будут отправляться при обнаружении тревожного события.
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.

Параметр	Описание
Видеоканал (Video Channel)	Выберите нужный видеоканал.
Облачное обновление (Cloud Update)	Обновление прошивки устройства по сети Если обнаружена последняя версия, вам нужно нажать **Обновить (Update)** в приложении, а затем нажать любую кнопку на брелоке, чтобы обновить прошивку брелока.
Удалить (Delete)	Удалите периферийное устройство в сети.  Перейдите на экран контроллера, выберите устройство из списка периферийных устройств и смахните его влево для удаления.

6 Использование брелока

Максимальное расстояние подключения между брелоком и контроллером составляет 900 метров. Это расстояние уменьшается за счет стен, полов и любых предметов, препятствующих передаче сигнала.

После добавления периферийных устройств на контроллер вы можете управлять ими с помощью брелока.

- Одновременно нажмите и один раз для подключения к контроллеру.
- Нажмите один раз, чтобы включить режим В отсутствие (Away Mode), после чего все периферийные устройства в этой зоне будут поставлены на охрану.

  Нажмите дважды, если функция **Диагностика системы (System Integrity Check)** включена на контроллере.
- Нажмите один раз, чтобы включить режим В присутствии (Home Mode), после чего все периферийные устройства в этой зоне будут сняты с охраны.
- Нажмите один раз, чтобы включить режим снятия с охраны, после чего все периферийные устройства в этой зоне будут сняты с охраны.
- Нажмите один раз, чтобы включить сигнал тревоги SOS.

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 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 Биньань, район Биньцзян, Ханчжоу, Китай | Веб-сайт: www.dahuasecurity.com | Почтовый индекс: 310053
E-mail: dhoverseas@dhvisiontech.com | Телефон: +86-571-87688888 28933188