



Сетевой видеорегистратор

Руководство пользователя

Правовая информация


Информация о документе

- Руководство содержит инструкции для использования и управления продуктом. Изображения, графики и вся другая информация предназначены только для ознакомления.
- Этот документ может быть изменен без уведомления, в связи с обновлением прошивки и по другим причинам. Актуальную версию настоящего документа можно найти на веб-сайте (<https://iflow-tech.ru>).
- При использовании данного документа обращайтесь за помощью к профессионалам, обученным работе с продуктом.

О продукте

- Послепродажное обслуживание данного продукта возможно только в той стране или регионе, где была совершена покупка.

Признание прав интеллектуальной собственности

-  Термины HDMI и HDMI High-Definition Multimedia Interface, а также логотип HDMI являются товарными знаками или зарегистрированными товарными знаками HDMI Licensing Administrator, Inc. в США и других странах.

ПРАВОВАЯ ИНФОРМАЦИЯ

- ДО МАКСИМАЛЬНО ДОПУСТИМОЙ СТЕПЕНИ, РАЗРЕШЕННОЙ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ДАННОЕ РУКОВОДСТВО, ПРОДУКТ, АППАРАТУРА, ПРОГРАММНОЕ И АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ», СО ВСЕМИ ОШИБКАМИ И НЕТОЧНОСТЯМИ. iFLOW НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, КАСАТЕЛЬНО УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ СООТВЕТСТВИЯ УКАЗАННЫМ ЦЕЛЯМ. ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА НЕСЕТ ПОЛЬЗОВАТЕЛЬ. КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ПЕРЕД ПОТРЕБИТЕЛЕМ ЗА КАКОЙ-ЛИБО СЛУЧАЙНЫЙ ИЛИ КОСВЕННЫЙ УЩЕРБ, ВКЛЮЧАЯ УБЫТКИ ИЗ-ЗА ПОТЕРИ ПРИБЫЛИ, ПЕРЕРЫВА В ДЕЯТЕЛЬНОСТИ ИЛИ ПОТЕРИ ДАННЫХ ИЛИ ДОКУМЕНТАЦИИ, ПО ПРИЧИНЕ НАРУШЕНИЯ УСЛОВИЙ КОНТРАКТА, ТРЕБОВАНИЙ (ВКЛЮЧАЯ ХАЛАТНОСТЬ), УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ ИНОГО, В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ КОМПАНИИ БЫЛО ИЗВЕСТНО О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.
- ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА С ДОСТУПОМ В ИНТЕРНЕТ НЕСЕТ ПОЛЬЗОВАТЕЛЬ; КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА НЕНОРМАЛЬНУЮ РАБОТУ ОБОРУДОВАНИЯ, ПОТЕРЮ ИНФОРМАЦИИ И ДРУГИЕ ПОСЛЕДСТВИЯ, ВЫЗВАННЫЕ КИБЕР АТАКАМИ, ВИРУСАМИ ИЛИ ДРУГИМИ ИНТЕРНЕТ РИСКАМИ; ОДНАКО, КОМПАНИЯ ОБЕСПЕЧИВАЕТ СВОЕВРЕМЕННУЮ ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ, ЕСЛИ ЭТО НЕОБХОДИМО.
- ВЫ СОГЛАШАЕТЕСЬ ИСПОЛЬЗОВАТЬ ДАННЫЙ ПРОДУКТ В СООТВЕТСТВИИ СО ВСЕМИ ПРИМЕНИМЫМИ ЗАКОНАМИ, И ВЫ НЕСЕТЕ ЕДИНОЛИЧНУЮ ОТВЕТСТВЕННОСТЬ ЗА ОБЕСПЕЧЕНИЕ ТОГО, ЧТОБЫ ВАШЕ ИСПОЛЬЗОВАНИЕ СООТВЕТСТВОВАЛО ПРИМЕНИМЫМ ЗАКОНАМ. В ЧАСТНОСТИ, ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ДАННОГО ПРОДУКТА ТАКИМ ОБРАЗОМ, КОТОРЫЙ НЕ НАРУШАЕТ ПРАВА ТРЕТЬИХ ЛИЦ, ВКЛЮЧАЯ, БЕЗ ОГРАНИЧЕНИЙ, ПРАВА НА ПУБЛИЧНОСТЬ, ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ ИЛИ ПРАВА НА ЗАЩИТУ ДАННЫХ И ДРУГИЕ ПРАВА НА КОНФИДЕНЦИАЛЬНОСТЬ. ВЫ ОБЯЗУЕТЕСЬ НЕ ИСПОЛЬЗОВАТЬ ЭТОТ ПРОДУКТ В ЗАПРЕЩЕННЫХ ЦЕЛЯХ, ВКЛЮЧАЯ РАЗРАБОТКУ ИЛИ ПРОИЗВОДСТВО ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ, РАЗРАБОТКУ ИЛИ ПРОИЗВОДСТВО ХИМИЧЕСКОГО ИЛИ БИОЛОГИЧЕСКОГО ОРУЖИЯ, ЛЮБУЮ ДЕЯТЕЛЬНОСТЬ, СВЯЗАННУЮ С ЯДЕРНЫМИ ВЗРЫВЧАТЫМИ ВЕЩЕСТВАМИ, НЕБЕЗОПАСНЫМ ЯДЕРНЫМ ТОПЛИВНЫМ ЦИКЛОМ ИЛИ НАРУШАЮЩУЮ ПРАВА ЧЕЛОВЕКА.
- В СЛУЧАЕ КАКИХ-ЛИБО КОНФЛИКТОВ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ И ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПОСЛЕДНЕЕ ПРЕВАЛИРУЕТ.

Модель

Данное руководство применимо к следующим моделям, однако не все функции, описанные в этом руководстве, поддерживаются каждой из них.


Модели
F-NR-416X/4(AI-Seek)
F-NR-432X/4(AI-Seek)
F-NR-432X/8(Ai-Seek)
F-NR-464X/8(Ai-Seek)
F-NR-464X/16(Ai-Seek)
F-NR-208/2(AI-Seek)
F-NR-216/2(AI-Seek)
F-NR-232/2(AI-Seek)



Инструкция по технике безопасности

- Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.
- Использование продукта должно строго соответствовать нормам электробезопасности страны и региона.
- Убедитесь, что штепсель плотно соединен с разъемом питания. Не подключайте несколько устройств к одному блоку питания. Перед подключением и отключением аксессуаров и периферийных устройств необходимо отключить питание устройства.
- Опасность поражения током! Перед обслуживанием отключите все источники питания.
- Оборудование должно быть подключено к розетке с заземлением.
- Розетка должна располагаться рядом с устройством, необходимо обеспечить легкий доступ к розетке.
- ⚡ указывает на наличие опасного напряжения. Внешняя проводка должна быть установлена квалифицированным персоналом.
- Запрещено размещать устройство на неустойчивой поверхности. Падение устройства может привести к серьезным травмам или смерти.
- Входное напряжение должно соответствовать стандарту безопасного сверхнизкого напряжения (SELV) и ограниченному источнику питания согласно IEC62368.
- Высокое напряжение! Выполните заземление перед подключением к источнику питания.
- Если из устройства идет дым или доносится шум – отключите питание, извлеките кабель и свяжитесь с сервисным центром.
- Если позволяют условия, рекомендуется использовать устройство в комбинации с ИБП.
- Данное оборудование не подходит для использования в местах, где могут присутствовать дети.
- При замене батареи батареей несоответствующего типа, существует риск взрыва.
- Не проглатывайте батарейку. Опасность химического ожога!
- Данное устройство оснащено батареей таблеточного типа. Проглатывание батареи таблеточного типа может вызвать серьезные внутренние ожоги всего за 2 часа и привести к смерти.
- Замена батареи на батарею несоответствующего типа может привести к нарушению мер предосторожности (например, в случае некоторых типов литиевых батарей).
- Запрещено помещать батарею в огонь или работающий духовой шкаф, разбивать и или резать батарею, так как это может привести к взрыву.
- Запрещено оставлять батарею в окружающей среде при очень высоких температурах, так как это может привести к взрыву или утечке горючей жидкости или газа.
- Запрещено подвергать батарею воздействию крайне низкого давления воздуха, так как это может привести к взрыву или утечке горючей жидкости или газа.
- Использованные батареи необходимо утилизировать в соответствии с инструкциями.
- Не прикасайтесь к лопастям вентилятора и двигателей. Во время обслуживания отключите источник питания.
- Не прикасайтесь к двигателю. Во время обслуживания отключите источник питания.
- Используйте только блоки питания, идентичные оригинальной модели, или блоки питания с ограниченным питанием (LPS) с тем же напряжением и током.

Профилактические меры и предостерегающие рекомендации

Перед подключением и эксплуатацией устройства, обратите внимание на следующие моменты:

- Устройство предназначено для использования исключительно в помещении. Установите устройство в хорошо проветриваемом, непыльном помещении.
- Убедитесь, что устройство надежно закреплено на стойке или полке. Сильные удары или толчки устройства, полученные в результате падения, могут привести к повреждению чувствительной электроники устройства.
- На устройство не должны попадать капли или брызги. Запрещено ставить на него предметы, наполненные жидкостью, например, вазы.
- Запрещается ставить на устройство источники открытого огня, например, зажженные свечи.
- Вентиляционные отверстия не должны быть закрыты такими предметами, как газеты, скатерти, занавески. Никогда не следует закрывать отверстия, кладя устройство на кровать, диван, ковер или другую подобную поверхность.
- Убедитесь, что клеммы у некоторых моделей правильно подключены к сети переменного тока.
- Оборудование некоторых моделей было специально разработано для ситуации, когда необходимо подключиться к ИТ-системе распределения питания.
-  определяет держатель батареи и положение элемента (элементов) внутри держателя батареи.
- ● + определяет положительный полюс оборудования, с которым используется или генерируется постоянный ток. - определяет отрицательный полюс устройства, которое использует или генерирует постоянный ток.
- Если устройство было выключено или долгое время находилось в нерабочем состоянии, его батарея таблеточного типа может разрядиться.
- Когда батарея таблеточного типа разрядится, системное время будет неверным, обратитесь в службу послепродажного обслуживания для замены батареи.
- Сохраняйте минимальное расстояние 200 мм (7,87") вокруг оборудования для обеспечения достаточной вентиляции.
- Убедитесь, что клеммы у некоторых моделей правильно подключены к сети переменного тока.
- Не прикасайтесь к острым краям и углам.
- Когда устройство работает при температуре выше 45 ° С или температура жесткого диска в S.M.A.R.T. превышает указанное значение, убедитесь, что устройство работает в прохладной среде, или замените жесткий диск (и), чтобы температура жесткого диска не превышала заявленного значения.
- При эксплуатации оборудования в нестандартных условиях, таких как горы, вышки, леса, необходимо установить ограничитель перенапряжения.

- Не прикасайтесь к оголенным компонентам (например, к металлическим контактам входных отверстий), после выключения устройства подождите не менее 5 минут, поскольку может оставаться напряжение.
- USB-порт оборудования используется только для подключения мыши, клавиатуры, USB-накопителя или адаптера для доступа к интернету по Wi-Fi. Ток для подключенного устройства не должен превышать 0.1 А.
- Серийный интерфейс устройства используется только для отладки.
- Если выходной порт питания устройства не соответствует ограниченному источнику питания, подключенное устройство, питаемое от этого порта, должно быть оснащено противопожарным кожухом.
- Если в комплект поставки устройства входит адаптер питания, используйте только прилагаемый адаптер.
- Для устройства с наклейкой  или  обратите внимание на следующие меры предосторожности: ПРЕДОСТЕРЕЖЕНИЕ. Нагрев деталей! Не прикасайтесь! При работе с такими деталями возможен ожог пальцев. После выключения необходимо подождать полчаса, прежде чем работать с деталями.
- Если устройство необходимо установить на стене или потолке, установите устройство в соответствии с инструкциями в данном руководстве.
- Во избежание травм это устройство должно быть надежно прикреплено к поверхности установки в соответствии с инструкциями по установке.
- При высокой рабочей температуре (от плюс 40 до плюс 55 °С) мощность некоторых адаптеров питания может снизиться.
- Прежде чем подключать, устанавливать или разбирать устройство, убедитесь, что питание отключено.
- Если подключение устройства необходимо выполнить самостоятельно, выберите провод для подачи питания в соответствии с электрическими параметрами, указанными на устройстве. Снимите изоляцию с провода в соответствующем месте с помощью инструмента для зачистки проводов. Во избежание серьезных последствий необходимо соблюдать требования к длине зачищенного провода, при этом проводники не должны быть оголены.
- Если из устройства идет дым или доносится шум – отключите питание, извлеките кабель и свяжитесь с сервисным центром.




Информация о тексте

Ознакомьтесь со следующими условными обозначениями, которые используются в документе.

- Для описания видеореги­стратора используются следующие названия: регистратор или устройство.
- IP-устройством является сетевая камера (IP-камера), купольная IP-камера (скоростная купольная камера), DVS (цифровой видеосервер) или NVS (сетевой видеосервер).
- Канал относится к видеоканалу в видеореги­страторе.

Условные обозначения

В настоящем документе используются следующие символы.




Символ	Описание
 Предупреждения	Указывает на опасную ситуацию, которая, если не удастся ее избежать, может привести к летальному исходу или серьезным травмам.
 Предостережение	Указывает на потенциально опасную ситуацию, которая может привести к повреждению оборудования, потере данных, ухудшению рабочих характеристик, либо к получению незапланированных результатов.
 Примечание	Дополнительная информация для дополнения важных моментов основного текста.

Описание индикаторов и интерфейсов

Описание индикаторов на передней панели

Индикаторы на передней панели указывают на различные рабочие состояния устройства.

Описание общих индикаторов


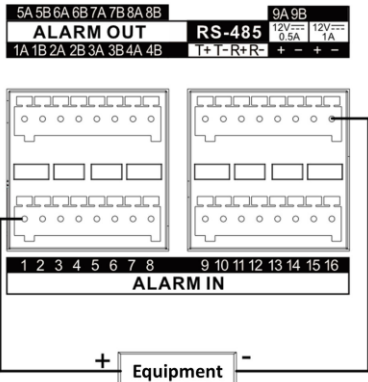
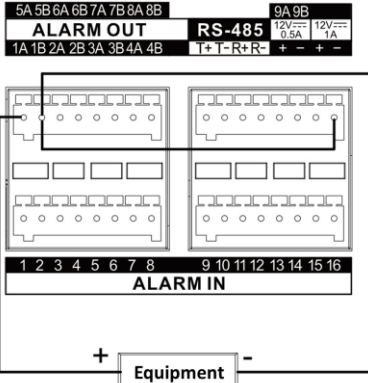
Индикатор	Описание
	Индикатор включается при включении питания устройства.
	Индикатор мигает, когда данные считываются с жесткого диска или записываются на него.
	Индикатор мигает, когда сетевое соединение работает в стандартном режиме.

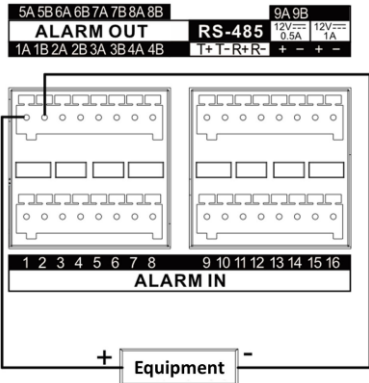
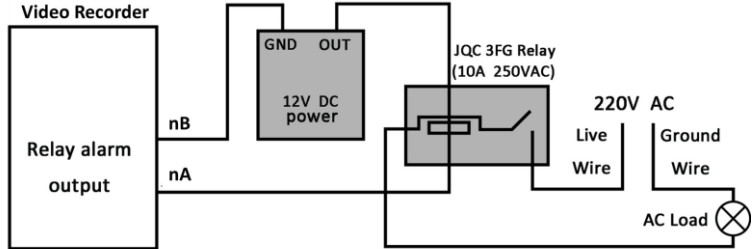
Описание интерфейсов

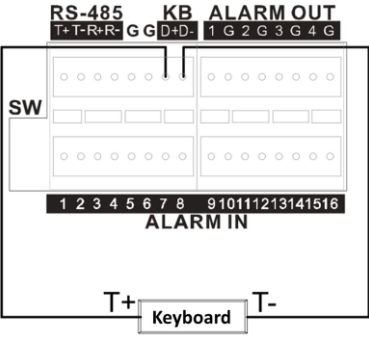
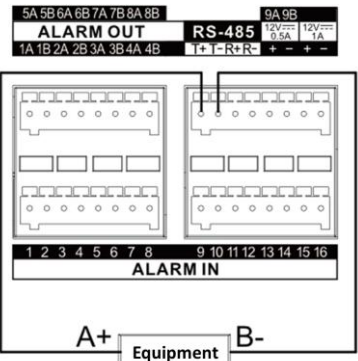
Интерфейсы различаются в зависимости от модели. В представленной ниже таблице отображено описание общих интерфейсов.

Описание индикаторов

Элемент	Описание
VIDEO IN	BNC-интерфейс для Turbo HD и аналоговый видеовход.
VIDEO OUT	BNC-разъем для видеовыхода.
AUDIO IN	RCA-разъем для аудиовхода.
AUDIO OUT	RCA-разъем для аудиовыхода.
LINE IN	RCA-разъем для двусторонней аудиосвязи.
USB	Разъем универсальной последовательной шины (USB) для дополнительных устройств.
VGA	Разъем DB15 для локального видеовыхода и отображения меню.
HDMI	HDMI-интерфейс для вывода видеосигнала.
RS-485	Серийный интерфейс RS-485 для PTZ-камер, скоростных купольных камер и т.д.
RS-232	Интерфейс RS-232 для настройки параметров или прозрачный канал.
LAN	Auto Ethernet-интерфейс RJ-45
eSATA	Интерфейс хранения и расширения для записи или резервного копирования.
GND	Заземление.

Элемент	Описание
Power Switch	Включение / выключение устройства.
Power Supply	Питание AC от 100 до 240 В, DC 48 В или DC 12 В.
USIM Card	Слот для UIM- / SIM-карты.
	Интерфейс антенны SMA.
ALARM IN	<p>Тревожный вход получает входной сигнал тревоги. Положительная клемма оборудования (+) должна быть подключена к соответствующему номеру, а отрицательная клемма оборудования (-) должна быть подключена к «-» или «G».</p> <p>Используйте следующую схему в качестве примера подключения для тревожного входа.</p> 
ALARM OUT	<p>Тревожный выход отправляет сигнал тревоги.</p> <p>Если оборудование использует источник питания постоянного тока, его положительная клемма (+) должна быть подключена к «А», а отрицательная клемма (-) - к «В», а затем подключена к «-» или «G». Используйте следующую схему в качестве примера подключения тревожного выхода для оборудования с постоянным током.</p> 

Элемент	Описание
	<p>Если оборудование использует источник питания переменного тока, его положительная клемма (+) должна быть подключена к «А», а отрицательная клемма (-) - к «В».</p> <p>Используйте следующую схему в качестве примера подключения тревожного выхода для оборудования с переменным током.</p>  <p>Примечание</p> <p>Поскольку напряжение нагрузки переменного тока может быть высоким, используйте внешнее реле для безопасности.</p> <p>Используйте следующую схему для справки.</p>  <p>Note: n represents a number in nA or nB, n can be 1 to 9.</p>
KB	<p>KB – клавиатура. Подключите «D+» и «D-» к «T+» и «T-» соответственно. Используйте следующую схему для справки.</p>

Элемент	Описание
	
<p>RS-485</p>	<p>RS-485 – это электрическая спецификация двухпроводного, полудуплексного, многоточечного последовательного соединения. Подключите «Т+» и «Т-» к «А+» и «В-» соответственно. Используйте следующую схему для справки.</p> 
<p>Управляемый выход питания DC 12 В / $\frac{12V}{0.5A}$</p>	<p>Управляемый выход питания 12 В постоянного тока и 0.5 / 1 А для внешнего тревожного устройства. Питание будет включено при срабатывании соответствующего тревожного выхода. Используйте следующую схему для справки.</p>

Установка жесткого диска (HDD)

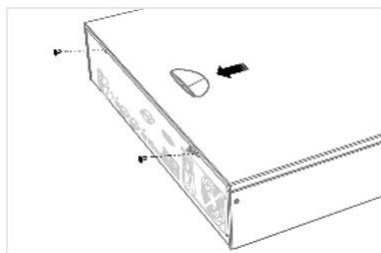
Если устройство не поддерживает замену HDD без выключения, отключите питание от устройства перед установкой HDD. Необходимо устанавливать рекомендованный производителем жесткий диск.

Установка на кронштейн

Установка кронштейна применима, когда необходимо снять крышку устройства и установить жесткий диск на внутренний кронштейн.

Шаги

1. Открутите винты на задней панели и сдвиньте крышку назад, чтобы снять ее.

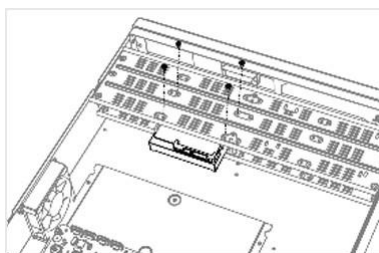


Снятие крышки

2. Закрепите жесткий диск на кронштейн винтами.

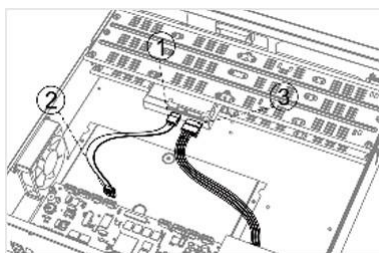
Примечание

Прежде чем устанавливать HDD на кронштейн нижнего уровня, снимите кронштейн верхнего уровня.



Фиксация жесткого диска

3. Подключите кабель передачи данных и кабель питания.



Подключение кабелей

Примечание

Для установки других жестких дисков необходимо повторить шаги установки, описанные выше.

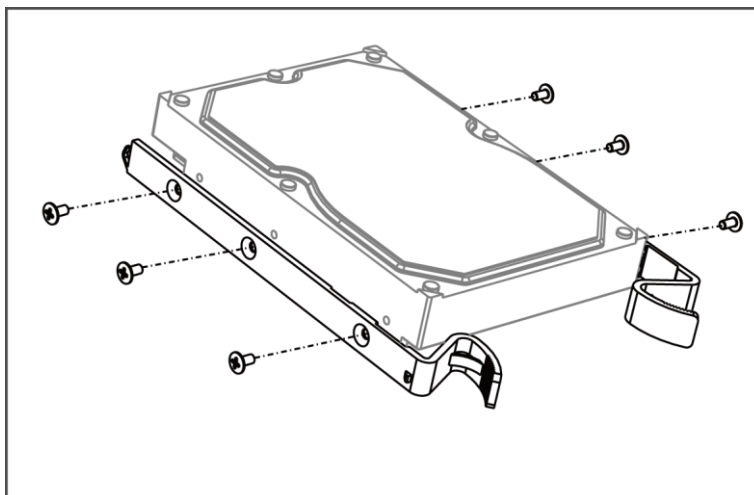
4. Установите на место крышку устройства и закрепите винтами.

Установка через переднюю панель

Установка через переднюю панель применима, когда вам необходимо открыть переднюю панель ключом и установить жесткий диск.

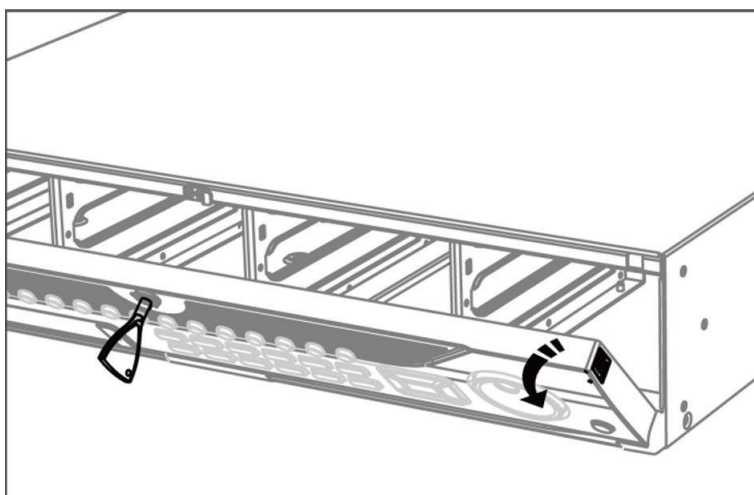
Шаги

1. Закрепите монтажные проушины на жестком диске винтами.



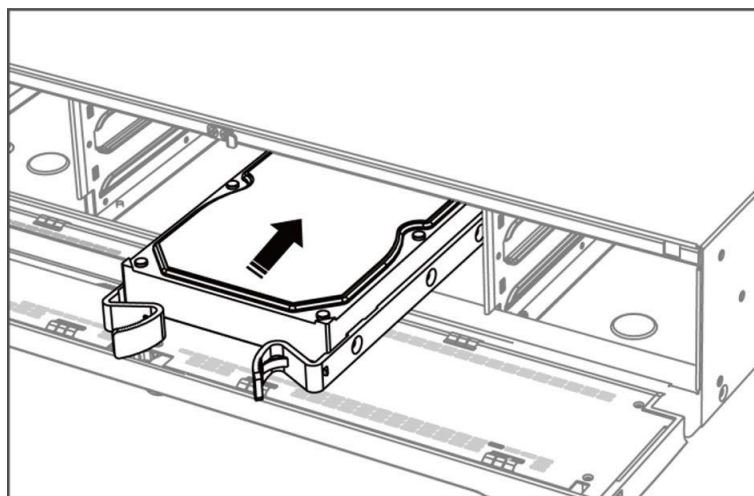
Фиксация монтажных проушин на HDD

2. Откройте переднюю панель прилагаемым ключом и нажмите кнопки на обеих сторонах передней панели, чтобы открыть ее.



Открытие передней панели

3. Вставьте и зафиксируйте жесткий диск.



Вставка жесткого диска

4. **Опционально.** Для установки других жестких дисков необходимо повторить шаги установки, описанные выше.
5. Закройте переднюю панель ключом.

Установка корпуса для жесткого диска

Жесткий диск сначала устанавливается в корпус, корпус вставляется в соответствующий слот.

Шаги

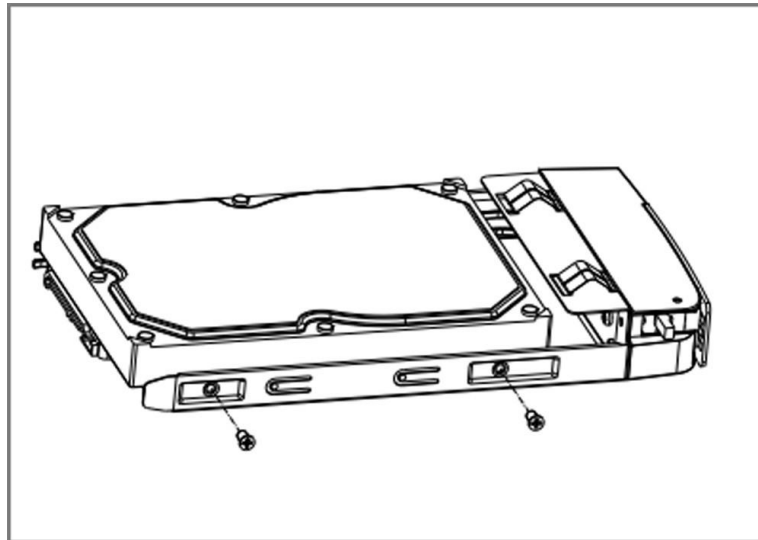
1. Разблокируйте переднюю панель с помощью ключа панели.
2. Аккуратно вытяните крышку из устройства и переведите ее в положение немного выше левой ручки.



Примечание

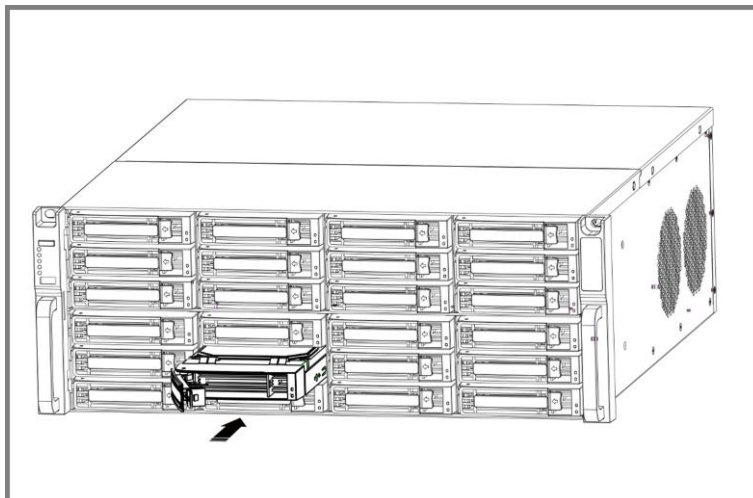
Угол между передней панелью и устройством должен быть в пределах 10°.

3. Нажмите синюю кнопку, чтобы поднять ручку, затем, удерживая ручку, вытащите корпус жесткого диска из слота.
4. Установите жесткий диск в корпус HDD.
 - 1) Установите жесткий диск в корпус. Интерфейс SATA должен быть обращен к нижней части корпуса.
 - 2) Отрегулируйте положение жесткого диска. Убедитесь, что задняя часть жесткого диска совпадает с нижней частью жесткого диска.
 - 3) С помощью отвертки закрепите четыре винта в отверстиях для винтов с обеих сторон.



Фиксация жесткого диска

5. Вставьте корпус жесткого диска обратно в слот.



Вставка корпуса жесткого диска в слот

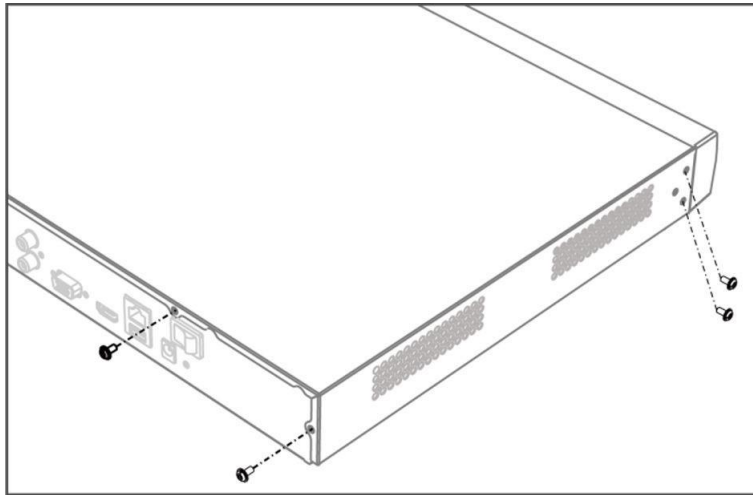
6. Нажмите на рукоятку до щелчка. Таким образом зафиксируется корпус жесткого диска. Повторите описанные выше шаги для установки остальных жестких дисков.
7. Закройте переднюю панель ключом.

Установка на нижней панели

Установка на нижней панели применима, когда вам необходимо установить и закрепить жесткий диск на нижней панели устройства.

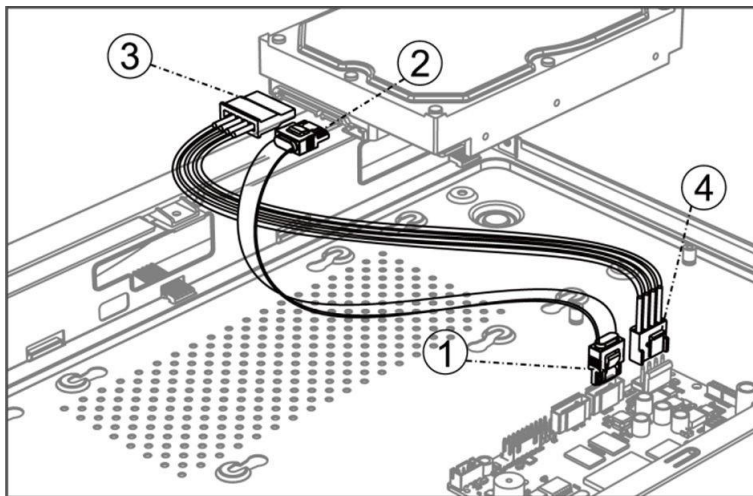
Шаги

1. Снимите крышку с устройства, открутив винты с панелей.



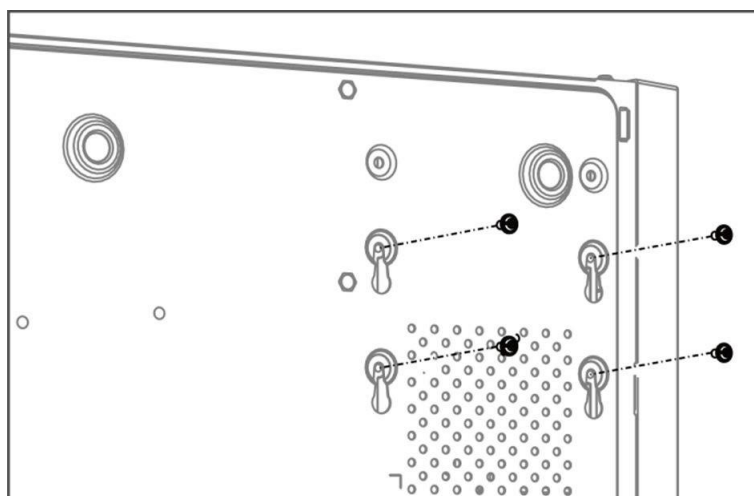
Снятие крышки

2. Подключите кабель передачи данных и кабель питания.
 - 1) Подключите один конец кабеля передачи данных к материнской плате устройства.
 - 2) Подключите второй конец кабеля передачи данных к жесткому диску.
 - 3) Подключите один конец кабеля питания к жесткому диску.
 - 4) Подключите второй конец кабеля питания к материнской плате устройства.



Подключение кабелей

3. Установите устройство, совместите винты для фиксации жесткого диска с соответствующими отверстиями в нижней части устройства и закрепите жесткий диск винтами.



Фиксация жесткого диска на нижней панели устройства

- 4. Опционально.** Для установки других жестких дисков необходимо повторить шаги установки, описанные выше.
- 5.** Установите на место крышку устройства и закрепите винтами.

Замена батареи таблеточного типа

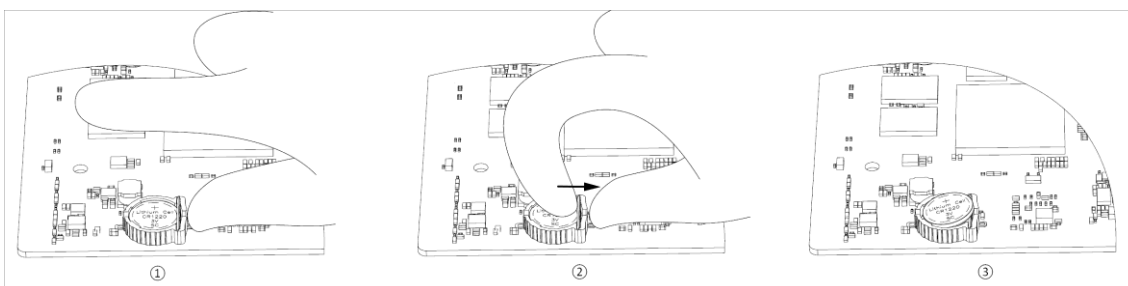
Батарею таблеточного типа следует заменить, если устройство было выключено или находилось в помещении в течение длительного времени, а системное время указано неверно.

Перед началом

Отключите устройство от питания.

Шаги

1. Снимите крышку корпуса устройства.
2. Найдите батарею таблеточного типа на материнской плате.
3. Поместите большой палец за пределы батарейного отсека, а указательным пальцем осторожно надавите на пружину положительного контакта наружу. Батарея автоматически выскочит.

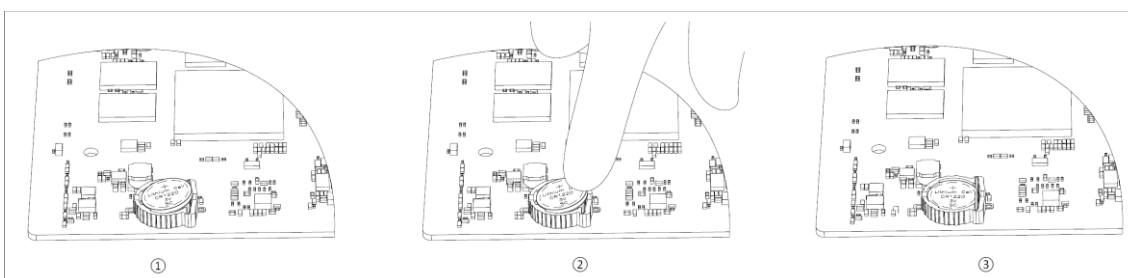


Извлечение батареи

Примечание

- При извлечении батареи используйте антистатические перчатки.
- Если пружина деформировалась из-за чрезмерного усилия при выдвигании, ее необходимо вернуть в исходное положение перед установкой батареи.

4. Вставьте батарею по диагонали в сторону, где пластиковый фиксатор находится в батарейном отсеке, а затем нажмите на батарею рядом с пружиной положительного контакта, чтобы защелкнуть ее под пружиной.



Замена батареи



Примечание

При замене батареи используйте антистатические перчатки.

5. Установите заново крышку корпуса устройства.

Дальнейшие шаги

Если системное время неверно, перейдите к настройке времени.

Содержание

Раздел 1 Активация через локальное меню	1
Раздел 2 Вход в устройство	3
Раздел 3 Пользовательский интерфейс	4
Раздел 4 Настройка параметров сети	6
4.1 Настройка параметров сети	6
4.1.1 Настройка TCP/IP	6
4.1.2 Конфигурация DDNS	7
4.1.3 Настройка параметров PPPoE	8
4.1.4 Настройка многоадресной передачи	9
4.2 Настройка параметров платформы доступа	9
4.2.1 Настройка Hik-Connect	9
4.2.2 Настройка ONVIF	11
4.2.3 Настройка ISUP.....	12
4.2.4 Настройка службы SDK.....	13
4.2.5 Включение ISAPI.....	14
4.2.6 Конфигурация ONVIF	14
4.2.7 Настройка сервера журналов.....	15
4.3 Настройки сетевых служб	16
4.3.1 Конфигурация HTTP(S).....	16
4.3.2 Конфигурация RTSP	17
4.3.3 Настройка WebSocket(s).....	18
4.3.4 Настройка проброса портов (NAT)	18
4.3.5 Конфигурация IoT	20
Раздел 5 Управление пользователями	21
Раздел 6 Доступ к устройству	22
6.1 Доступ к видеоустройству.....	22
6.1.1 Добавление сетевой камеры с автоматическим поиском в режиме онлайн	22
6.1.2 Добавление IP-камеры вручную	23

6.1.3	Добавление сетевой камеры через PoE.....	24
6.1.4	Добавление камеры с питанием от солнечной батареи через протокол ONVIF	24
6.1.5	Добавление IP-камеры по индивидуальному протоколу	25
6.1.6	Добавление IP-камеры через файл конфигурации камеры.....	27
6.2	Добавление устройств контроля доступа	27
6.3	Добавление охранной панели	27
6.4	Добавление аудиоустройства	28
6.5	Добавление POS-устройства.....	28
6.6	Управление каналами.....	30
Раздел 7 Группировка устройства		31
Раздел 8 Настройки видео- или аудиоустройств.....		32
8.1	Включение доступа к потоку H.265.....	32
8.2	Настройка параметров отображения	32
8.3	Настройка параметров видео	33
8.4	Настройка маскирования.....	34
8.5	Конфигурация защиты конфиденциальных данных.....	35
8.6	Настройка параметров аудио.....	36
8.7	Настройка службы ONVIF	36
8.8	Настройка в пакетном режиме	37
8.9	Настройка PoE-интерфейса.....	38
Раздел 9 Управление хранением.....		40
9.1	Управление HDD	40
9.2	Настройка RAID	41
9.2.1	Создание массива дисков.....	42
9.2.2	Восстановление массива	44
9.2.3	Удаление массива	44
9.2.4	Просмотр информации о прошивке	45
9.3	Настройка режима хранения	45
9.4	Конфигурация других параметров хранения.....	46
9.5	Управление USB-накопителем	46

Раздел 10 Конфигурация расписания	47
10.1 Настройка шаблона расписания	47
10.2 Настройка расписания записи	49
10.3 Настройка расписания захвата изображений.....	50
10.4 Конфигурация записи аудио.....	52
Раздел 11 Просмотр в режиме реального времени	54
11.1 Настройка просмотра в режиме реального времени.....	54
11.2 Графический интерфейс	54
11.3 Управление PTZ.....	56
Раздел 12 Воспроизведение	57
12.1 Графический интерфейс	57
12.2 Обычный режим воспроизведения.....	58
12.3 Воспроизведение по событию	60
12.4 Воспроизведение фрагмента	60
12.5 Воспроизведение дополнительных периодов.....	61
Раздел 13 Центр событий.....	62
13.1 Настройки событий	62
13.1.1 Базовое / общее событие	62
13.1.2 Защита периметра.....	64
13.1.3 Событие отклонений в поведении	78
13.1.4 Целевое событие	81
13.1.5 Обнаружение тепловизионной камеры.....	83
13.1.6 Событие тревожного входа	85
13.1.7 Событие аудиоанализа	87
13.2 Настройка привязки	89
13.3 Конфигурация снятия с охраны	91
13.4 Настройка в пакетном режиме	92
13.5 Поиск событий	93
13.6 Просмотр тревог	94
Раздел 14 Поиск и резервное копирование	95
Раздел 15 AI-Seek	97

Раздел 16 AcuSearch	100
Раздел 17 Интеллектуальные настройки	102
17.1 Управление алгоритмами	102
17.2 Состояние алгоритма	102
17.3 Управление планированием задач	102
17.4 Управление библиотекой списков	103
17.4.1 Добавление библиотеки списков	103
17.4.2 Загрузка изображений лиц в библиотеку	103
17.5 Настройки автоматического обучения	104
17.5.1 Управление задачей автоматического обучения	105
17.5.2 Управление моделью	106
17.5.3 Интеллектуальное состояние	106
Раздел 18 Центр приложений	107
18.1 Детекция целей «Человек» и «ТС»	107
18.2 Регистрация сотрудника / посетителя	107
18.2.1 Добавление задачи регистрации	108
18.2.2 Поиск записей регистрации	109
18.3 Статистический отчет	110
Раздел 19 Настройки системных параметров	111
Раздел 20 Резервное копирование устройства горячего резервирования	113
20.1 Настройка параметров рабочего устройства	113
20.2 Настройка устройств горячего резервирования	114
Раздел 21 Конфигурация события исключения	115
Раздел 22 Просмотр информации о системе	117
Раздел 23 Обслуживание системы	118
23.1 Перезагрузка по расписанию	118
23.2 Обновление устройства	118
23.3 Резервное копирование и восстановление	118
23.4 Информация о журнале	119
23.5 Настройка сервера журналов	119
23.6 Инструменты для ТО	119

23.7 Конфигурация функции плавного отключения питания.....	120
Раздел 24 Управление безопасностью	122
24.1 Фильтрация IP-адресов	122
24.2 Шифрование потока.....	122
24.3 Выбор версии TLS	123
Раздел 25 Приложение	124
25.1 Список совместимых адаптеров питания	124
25.2 Список терминов и сокращений	125
25.3 Часто задаваемые вопросы	126
25.3.1 Почему на некоторых каналах отображается сообщение No Resource («Ресурсы отсутствуют») или экран становится черным при просмотре в режиме реального времени на нескольких экранах? .	126
25.3.2 Почему при добавлении IP-камеры видеореги­стратор сообщает о ненадежности пароля?	127
25.3.3 Почему не поддерживается уведомление о типе потока с видеореги­стратора?	127
25.3.4 Как подтвердить, что видеореги­стратор использует H.265 для записи видео?	128
25.3.5 Почему видеореги­стратор сообщает о конфликте IP-адресов?	128
25.3.6 Почему изображение зависает при воспроизведении одноканальной или многоканальной камерой?	128
25.3.7 Почему устройство не может управлять PTZ-камерой через протокол Coaxitron?	128
25.3.8 Почему PTZ-камера не реагирует на команды через RS-485?	129
25.3.9 Почему качество звука видео плохое?	129
25.4 Уведомление о наличии агрессивного газа.....	129

Раздел 1 Активация через локальное меню

При первом подключении необходимо активировать устройство, установив пароль администратора. До активации выполнение каких-либо операций невозможно. Также устройство можно активировать через веб-интерфейс, SADP или клиентское программное обеспечение.

Перед началом

Убедитесь, что устройство подключено к монитору и мыши.

Шаги

1. Включите устройство.
2. Установите параметры региона или летнего времени (DST).
3. Выберите язык системы.
4. Введите пароль администратора дважды.



Предостережение

РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ – настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопаснее.

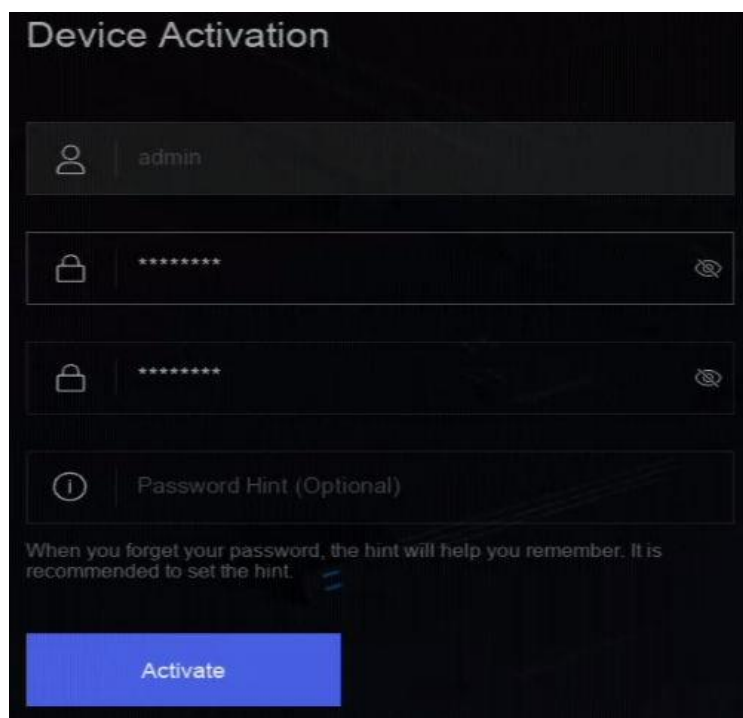


Рисунок 1-1 Активация через локальное меню

5. Опционально. Введите подсказку для пароля. Это поможет вспомнить пароль, если забудете его.

6. Нажмите **Activate** («Активировать»).

 **Примечание**

После активации устройства необходимо правильно сохранить пароль.

7. Опционально. Нарисуйте графический ключ.

8. Настройте как минимум один метод восстановления пароля.

Дальнейшие шаги

Следуйте инструкциям по настройке параметров.

Раздел 2 Вход в устройство

Необходимо войти в устройство перед использованием меню и других функций.

Перед началом

Убедитесь, что устройство активировано.

Шаги

1. Включите устройство.
2. Нажмите правой кнопкой мыши, чтобы отобразить контекстное меню.
3. Выберите нужный элемент. Например, выберите **Exit Full Screen** («Выйти из полноэкранного режима»), чтобы автоматически войти в интерфейс входа.

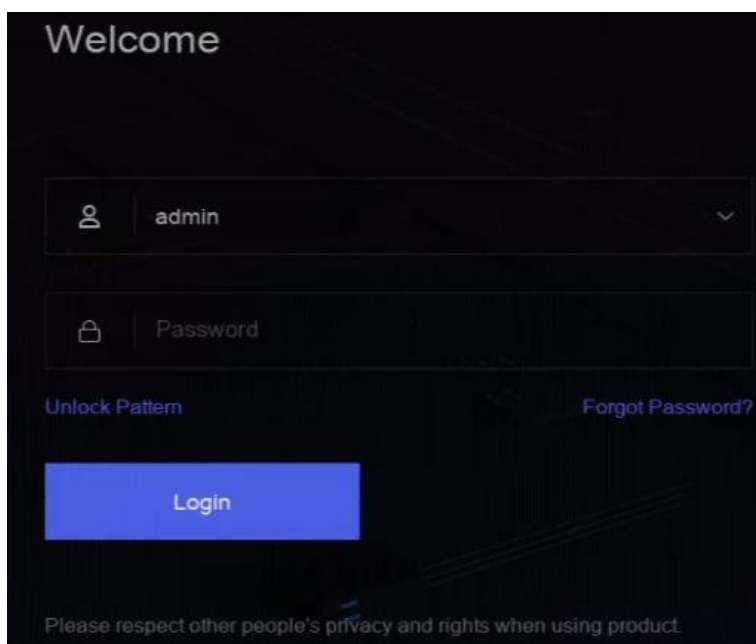


Рисунок 2-1 Вход в систему

4. Используйте графический ключ для входа или нажмите **Password Login** («Вход по паролю»), чтобы войти в систему с помощью имени пользователя и пароля.

Примечание

- Графический ключ разблокировки доступен только администратору.
 - Если забыли графический ключ или пароль для входа, нажмите **Forget Password** («Забыли пароль») в интерфейсе входа с паролем, чтобы сбросить пароль, или используйте подсказку по паролю, чтобы вспомнить.
-

Раздел 3 Пользовательский интерфейс

Устройство перейдет в интерфейс просмотра в режиме реального времени после включения. Нажмите правой кнопкой мыши и выберите **Exit Full Screen** («Выйти из полноэкранного режима») в контекстном меню.

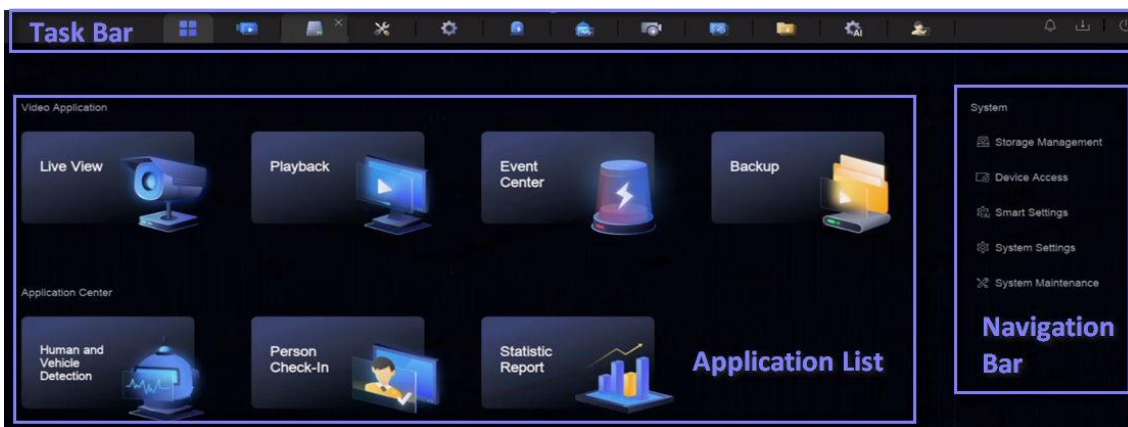


Рисунок 3-1 Страница с основными функциями

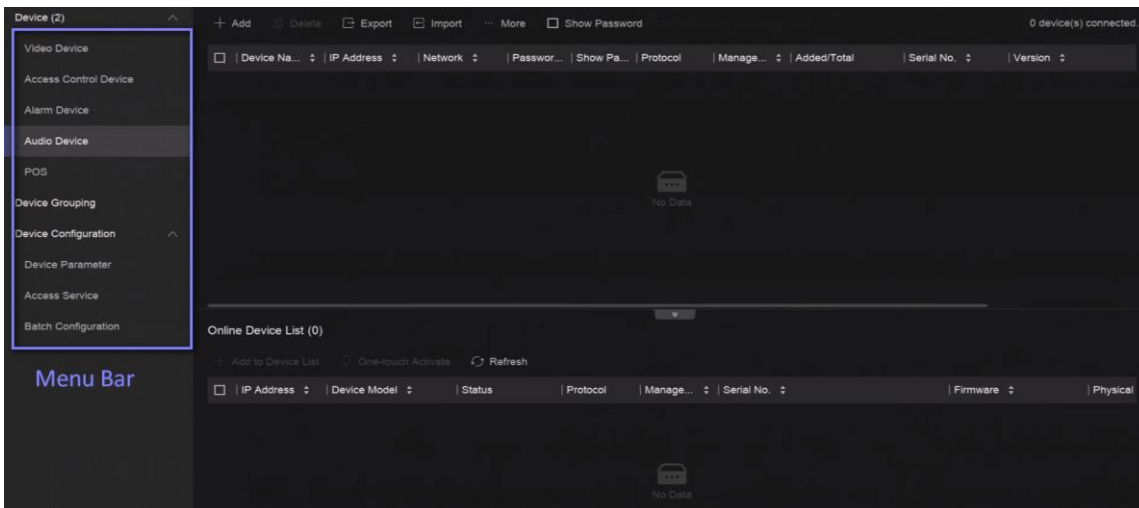


Рисунок 3-2 Пример панели меню

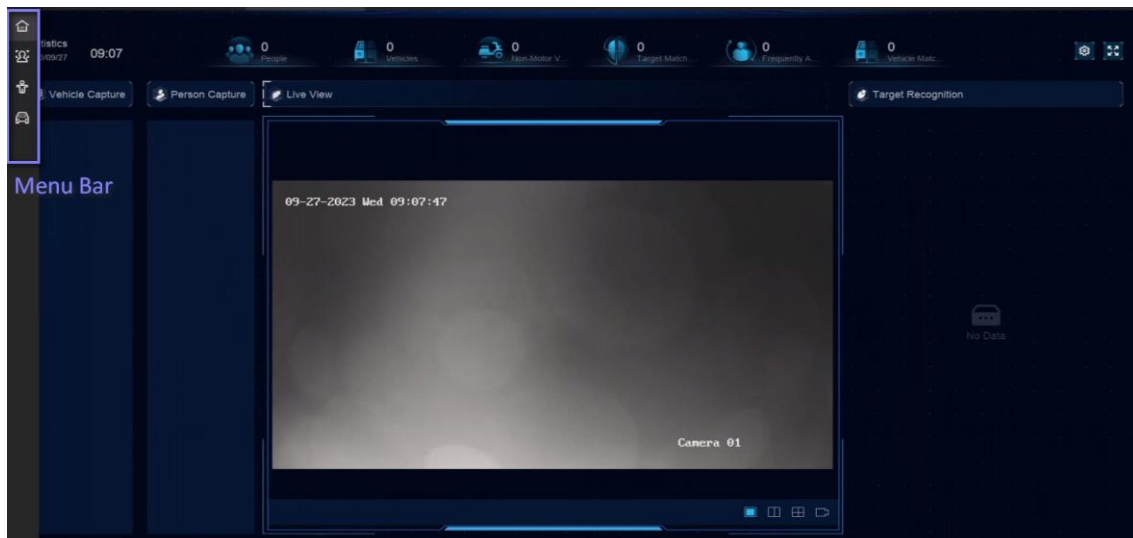








Рисунок 3-3 Пример детекции целей «Человек» и «ТС» в центре приложений

Таблица 3-1 Интерфейсы

Название интерфейса	Общая информация
Панель задач	<p>На панели задач отображаются открытые приложения. Можно перемещать и закрывать каждую вкладку приложения.</p> <p>Описание значков.</p> <ul style="list-style-type: none"> •  : главное меню •  : центр событий. Поиск и просмотр оповещений о событиях. •  : отображение процесса загрузки каждой задачи. •  : выключение, выход из системы или перезагрузка устройства.
Список приложений	Здесь отображаются все приложения. Можно нажать на один из них, чтобы настроить его.
Строка навигации	Нажмите, чтобы настроить каждую функцию системы.
Панель меню	<p>Здесь перечислены настраиваемые элементы каждого приложения.</p> <p> Примечание</p> <p>Нажмите  или правой кнопкой мыши, чтобы отобразить строку меню для приложений в центре приложений.</p>

Раздел 4 Настройка параметров сети

Параметры сети, параметры доступа к платформе и сетевые службы можно настраивать.

4.1 Настройка параметров сети

Перед использованием функций, требующих сетевого доступа, необходимо настроить сетевые параметры.

4.1.1 Настройка TCP/IP

TCP / IP необходимо правильно настроить перед использованием видеореги­стратора по сети или доступом к сетевым устройствам.

Шаги

1. Перейдите в меню **System** → **System Settings** → **Network** → **Network** → **TCP/IP** («Система → Настройки системы → Сеть → Сеть → TCP / IP»).

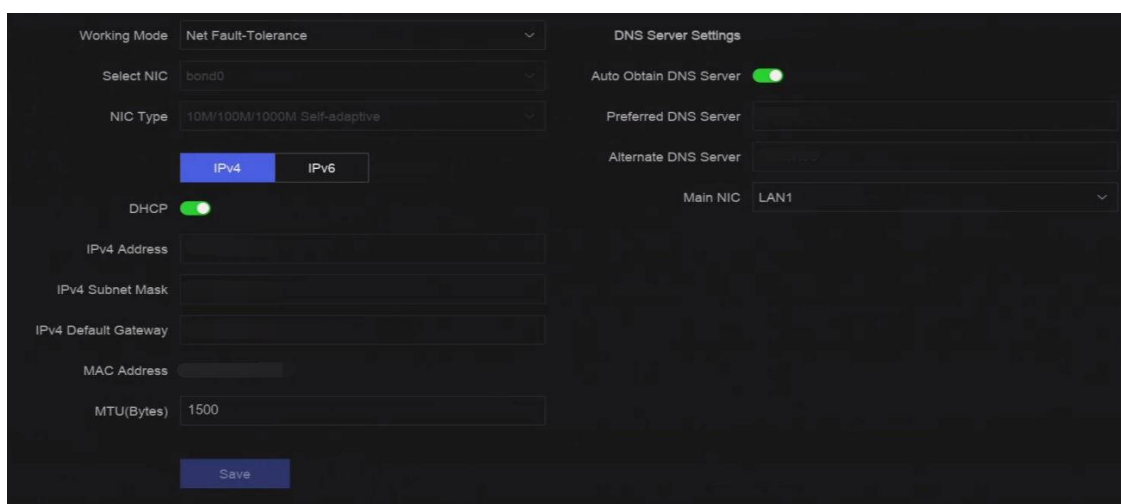


Рисунок 4-1 Настройка параметров TCP/IP

2. Настройте **Working Mode** («Рабочий режим») и выберите **NIC. Многоадресн.**

Параметры двух сетевых интерфейсных плат можно настраивать независимо. В поле типа NIC можно выбрать **LAN1** или **LAN2**. Вы можете выбрать одну NIC в качестве маршрута по умолчанию. Затем система подключается к внешней сети, и данные будут пересылаться по маршруту по умолчанию.

Режим отказоустойчивости сети

Две NIC используют один и тот же IP-адрес, и можно выбрать **Main NIC** («Основную NIC») для **LAN1** или **LAN2**. Таким образом, в случае отказа одной NIC видеореги­стратор автоматически включит другую резервную NIC, чтобы обеспечить нормальную работу всей системы.

 **Примечание**

Рабочий режим реализован только у определенных моделей.

3. Настройте параметры сети.

- IPv4 DHCP

Если DHCP-сервер доступен, включите **DHCP** для автоматического получения IP-адреса и других сетевых настроек.

MTU

Максимальный размер передаваемого блока данных (MTU) — это размер самого большого блока данных протокола, который может быть передан в ходе одной транзакции сетевого уровня.

Автоматическое получение DNS-сервера

Если **DHCP** включен. Выберите **Auto Obtain DNS Server** («Автоматическое получение DNS-сервера»), чтобы получить **Preferred DNS Server** («Предпочитаемый DNS-сервер») и **Alternate DNS server** («Альтернативный DNS-сервер»).

- IPv6

Сообщение маршрутизатора

Если маршрутизатор в сети поддерживает IPv6, рекомендуется использовать этот режим по умолчанию.

Автоматически

Если в сети есть устройство DHCPv6, рекомендуется использовать этот режим

Конфигурация вручную

Необходимо использовать этот режим, если собираетесь вручную вводить параметры IPv6.

4. Нажмите **Save («Сохранить»).**

4.1.2 Конфигурация DDNS

Сервер динамических доменных имен (DDNS) сопоставляет динамические IP-адреса пользователей с фиксированным сервером доменных имен.

Перед началом

Убедитесь, что службы DynDNS, PeanutHull и NO-IP зарегистрированы у интернет-провайдера.

Шаги

1. Перейдите в **System → System Settings → Network → Network → DDNS** («Система → Настройки системы → Сеть → Сеть → DDNS»).

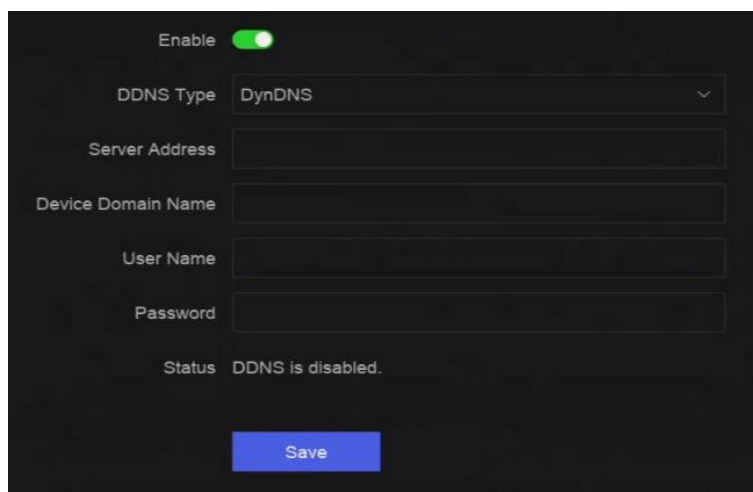


Рисунок 4-2 Летнее время

2. Нажмите **Enable** («Включить»).
3. Выберите **DDNS Type** («Тип DDNS»).
4. Настройте параметры, включая адрес службы, доменное имя и т. д.
5. Нажмите **Save** («Сохранить»).

4.1.3 Настройка параметров PPPoE

Если устройство подключено к сети Интернет через PPPoE, необходимо настроить имя пользователя и пароль соответственно. Обратитесь к своему интернет-провайдеру для получения подробной информации о PPPoE.

Шаги

1. Перейдите в **System** → **System Settings** → **Network** → **Network** → **PPPoE** («Система → Настройки системы → Сеть → Сеть → PPPoE»).

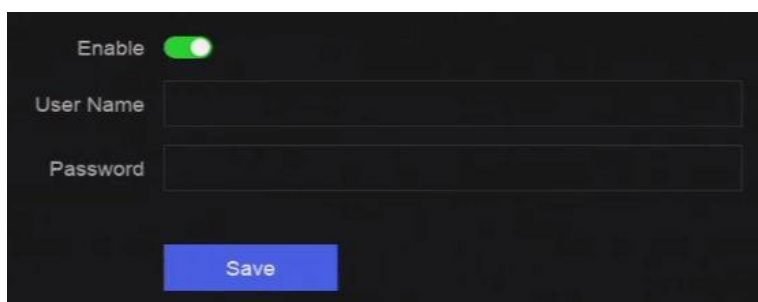


Рисунок 4-3 PPPoE

2. Нажмите **Enable** («Включить»).
3. Введите имя пользователя и пароль.
4. Нажмите **Save** («Сохранить»).

Дальнейшие шаги

Перейдите в меню **System → System Maintenance → Running Info → Network Status** («Система → Обслуживание системы → Информация о запуске → Состояние сети»), чтобы просмотреть состояние PPPoE.

4.1.4 Настройка многоадресной передачи

Многоадресную рассылку можно настроить для включения просмотра в режиме реального времени для камер, количество которых превышает максимально допустимое для сети.

Шаги

1. Перейдите в **System → System Settings → Network → Network → Other** («Система → Настройки системы → Сеть → Сеть → Другое»).
2. Настройте параметры **Multicast** («Многоадресная передача»).



Примечание

- При добавлении устройства через сетевой клиент видеобезопасности IP-адрес группы многоадресной передачи должен совпадать с IP-адресом многоадресной передачи устройства.
- IP-адрес многоадресной рассылки охватывает IP-адрес класса D в диапазоне от 224.0.0.0 до 239.255.255.255, и рекомендуется использовать IP-адрес в диапазоне от 239.252.0.0 до 239.255.255.255. При добавлении устройства в программное обеспечение CMS адрес многоадресной рассылки должен быть таким же, как и у устройства.

-
3. Нажмите **Save** («Сохранить»).

4.2 Настройка параметров платформы доступа

4.2.1 Настройка Hik-Connect

Hik-Connect объединяет в себе приложение для мобильных телефонов и служб платформы для доступа и управления видеореги­стратором, что позволяет легко получить удаленный доступ к системе видеомониторинга.

Шаги

1. Перейдите в **System → System Settings → Network → Hik-Connect** («Система → Настройки системы → Сеть → Hik-Connect»).

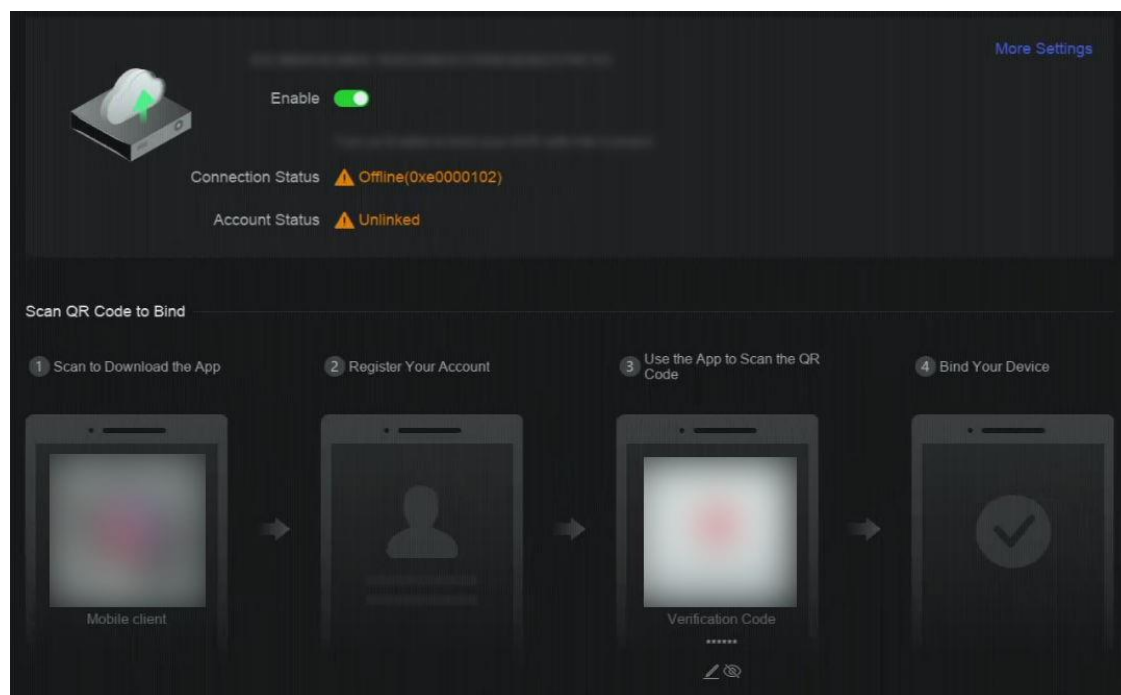


Рисунок 4-4 Hik-Connect

2. Нажмите **Enable** («Включить»), и появятся условия обслуживания.
3. Примите условия обслуживания.
4. Загрузите приложение Hik-Connect.
 - Используйте смартфон для сканирования QR-кода и загрузите приложение Hik-Connect.
 - Загрузите приложение по адресу <https://appstore.hikvision.com>.



Рисунок 4-5 Загрузка Hik-Connect

5. Зарегистрируйте учетную запись в приложении.
6. **Опционально.** Нажмите **More Settings** («Дополнительные настройки»), чтобы включить **Stream Encryption** («Шифрование потока»), **Platform Time Sync** («Синхронизация времени на платформе»), **Adaptive Bitrate Streaming** («Адаптивная потоковая передача битрейта») или изменить **Server IP Address** («IP-адрес сервера»).

Шифрование потока

После включения этой функции требуется ввести проверочный код в режиме просмотра в реальном времени и удаленного доступа.

Синхронизация времени платформы


Устройство будет синхронизировать время с Hik-Connect вместо NTP-сервера.

Адаптивная потоковая передача битрейта

При минимальных параметрах сетевой среды устройство автоматически регулирует битрейт видео для обеспечения плавности воспроизведения.

IP-адрес сервера

IP-адрес сервера Hik-Connect.

7. Нажмите , чтобы установить проверочный код.
8. Используйте приложение Hik-Connect для сканирования QR-кода устройства и привяжите устройство к своей учетной записи Hik-Connect.



Примечание

Если устройство уже привязано к учетной записи, вы можете нажать **Unbind** («Отменить привязку»), чтобы отменить привязку к текущей учетной записи.

Результат

- Если устройство подключено к Hik-Connect, **Connection Status** («Состояние подключения») будет **Online** («Подключено»).
- Если устройство привязано к учетной записи Hik-Connect, **Account Status** («Состояние учетной записи») будет **Linked** («Привязано»).

Дальнейшие шаги

Доступ к видеореги­стратору можно получить через Hik-Connect.

4.2.2 Настройка OTAP

OTAP – это единый интегрированный стандарт и режим push-pull протокола Hikvision в публичной и частной сети. После включения OTAP другие приложения могут удаленно просматривать видео через этот протокол.

Перед началом

Убедитесь, что сеть устройства доступна через OTAP.

Шаги

1. Перейдите в **System** → **System Settings** → **Network** → **Platform Access** → **OTAP** («Система → Настройки системы → Сеть → Доступ к платформе → OTAP»).

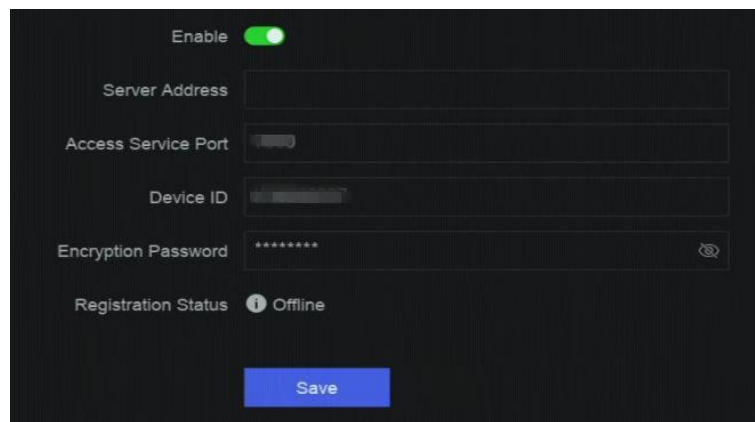


Рисунок 4-6 OTAP

2. Включите **OTAP**.
3. Настройте параметры.
4. Нажмите **Save** («Сохранить»).

4.2.3 Настройка ISUP

ISUP (протокол интеллектуальной безопасности восходящей связи) предоставляет API, файлы библиотеки и команды для сторонней платформы для доступа к таким устройствам, как NVR, скоростные купольные камеры, DVR, сетевые камеры, мобильные NVR, мобильные устройства, устройства декодирования и т. д. С помощью этого протокола сторонняя платформа может реализовывать такие функции, как просмотр в режиме реального времени, воспроизведение, двусторонняя аудиосвязь, управление PTZ и т. д.

Шаги

1. Перейдите в **System → CX → System Settings → Network → Platform Access → ISUP** («Система → CX → Настройки системы → Сеть → Доступ к платформе → ISUP»).

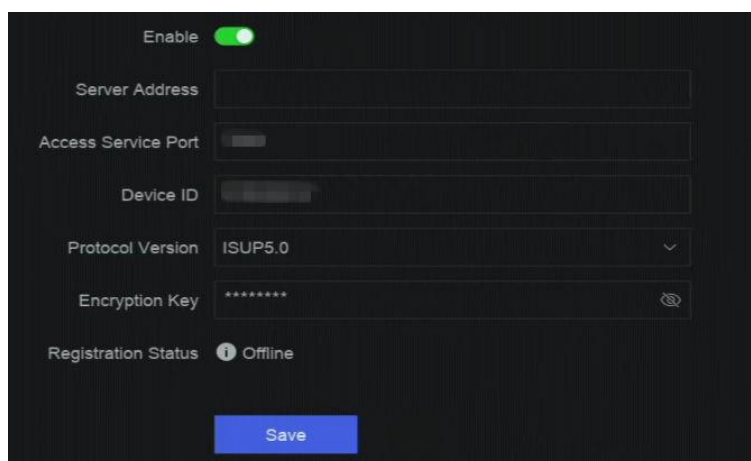


Рисунок 4-7 ISUP

2. Нажмите **Enable** («Включить»).

Примечание

Если ISUP включен, доступ Hik-Connect будет автоматически отключен.

3. Настройте соответствующие параметры.

Адрес сервера

Означает IP-адрес сервера платформы.

Порт сервера доступа

Порт сервера платформы: от 1024 до 65535. Фактический порт должен быть предоставлен платформой.

ID устройства

Идентификатор устройства предоставляется платформой.

Версия протокола

Версия протокола ISUP, доступен только ISUP 5.0.

Ключ шифрования

При использовании версии ISUP V5.0 требуется пароль шифрования, он обеспечивает более безопасную связь между устройством и платформой. Введите его для проверки после регистрации устройства на платформе ISUP. Не допускается оставлять пароль пустым или «ABCDEF».

4. Нажмите **Save** («Сохранить»).

Вы можете увидеть состояние (в сети или не в сети) после перезапуска устройства.

4.2.4 Настройка службы SDK

Служба SDK (комплект разработки ПО) используется сторонними партнерами для интеграции различных функций. Расширенная служба SDK использует протокол TLS, что обеспечивает более безопасную передачу данных.

Шаги

1. Перейдите в **System → System Settings → Network → Platform Access → SDK** («Система → Настройки системы → Сеть → Доступ к платформе → SDK»).

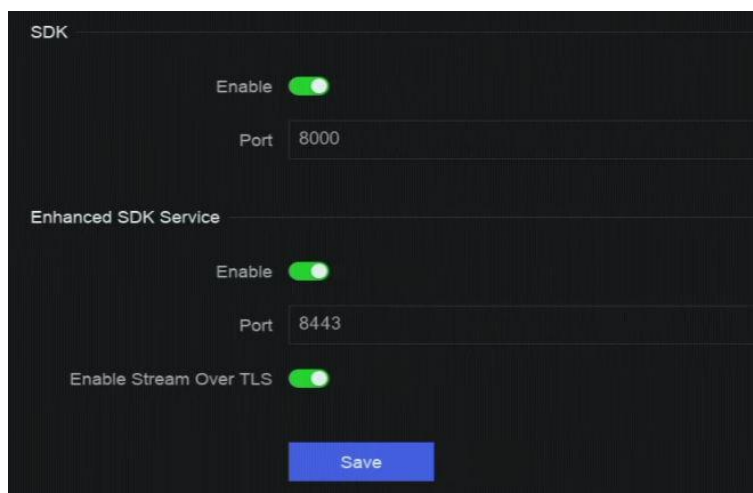


Рисунок 4-8 Служба SDK

2. Настройте **SDK** и **Enhanced SDK Service** («Расширенная служба SDK») в соответствии с требованиями.

 **Примечание**

Порт для **Enhanced SDK Service** («Расширенная служба SDK») по умолчанию – 8443.

3. **Опционально.** Включите **Stream Over TLS** («Потоковая передача по TLS»). Технология шифрования потока по TLS обеспечивает более безопасную передачу потока.

4. Нажмите **Save** («Сохранить»).

4.2.5 Включение ISAPI

ISAPI — это открытый протокол, основанный на HTTP, который может обеспечивать связь между системными устройствами (например, сетевой камерой, NVR и т. д.).

Перейдите в **System** → **System Settings** → **Network** → **Platform Access** → **ISAPI** («Система → Настройки системы → Сеть → Доступ к платформе → ISAPI»).

4.2.6 Конфигурация ONVIF

Протокол ONVIF позволяет подключаться к камерам сторонних производителей. У добавленных учетных записей пользователей должно быть разрешение на подключение других устройств по протоколу ONVIF.

Шаги

1. Перейдите в **System** → **CX** → **System Settings** → **Network** → **Platform Access** → **ONVIF** («Система → CX → Настройки системы → Сеть → Доступ к платформе → ONVIF»).

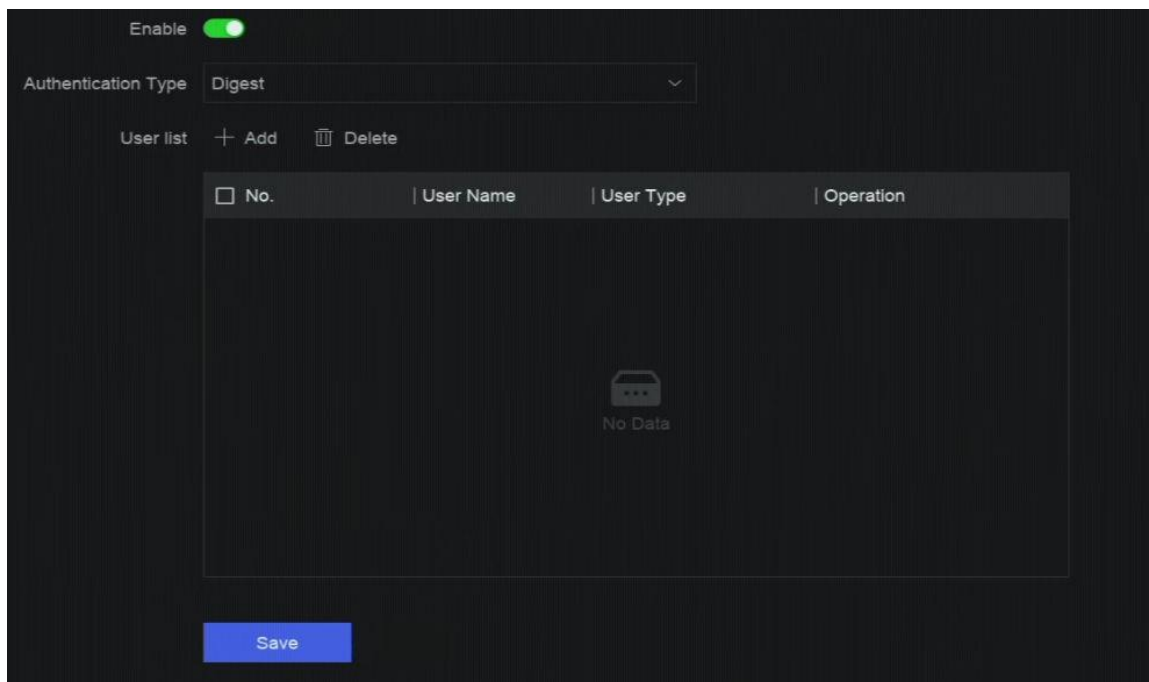


Рисунок 4-9 ONVIF

2. Нажмите **Enable** («Включить»).
3. Выберите тип аутентификации.
4. Нажмите **Add** («Добавить»), чтобы добавить пользователя.
5. Установите имя пользователя и пароль.



Предостережение

РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ – Настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

-
6. Нажмите **Save** («Сохранить»).

4.2.7 Настройка сервера журналов

Журналы можно загружать на сервер журналов для резервного копирования.

Шаги

1. Перейдите в **System → System Settings → Network → Platform Access → Log Server** («Система → Настройки системы → Сеть → Доступ к платформе → Сервер журналов»).

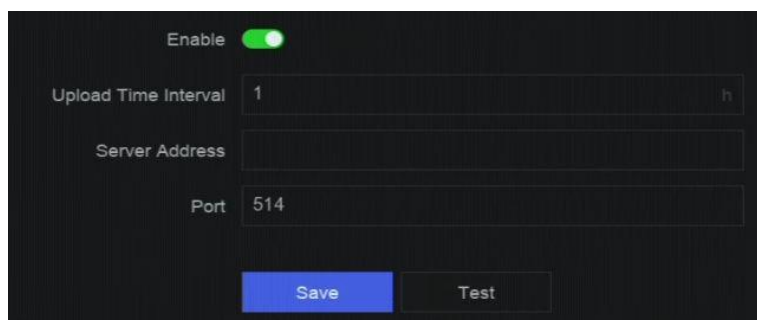


Рисунок 4-10 Сервер журналов

2. Нажмите **Enable** («Включить»).
3. Настройте **Upload Time Interval** («Интервал времени загрузки»), **Server IP Address** («IP-адрес сервера») и **Port** («Порт»).
4. **Опционально.** Нажмите **Test** («Проверить»), чтобы проверить правильность параметров.
5. Нажмите **Save** («Сохранить»).

4.3 Настройки сетевых служб

4.3.1 Конфигурация HTTP(S)

Для удаленного доступа через веб-интерфейс используются порты HTTP и HTTPS. Протокол HTTPS обеспечивает зашифрованную передачу и аутентификацию, что повышает безопасность удаленного доступа.

Шаги

1. Перейдите в **System** → **System Settings** → **Network** → **Network Service** → **HTTP(S)** («Система → Настройки системы → Сеть → Сетевая служба → HTTP(S)»).

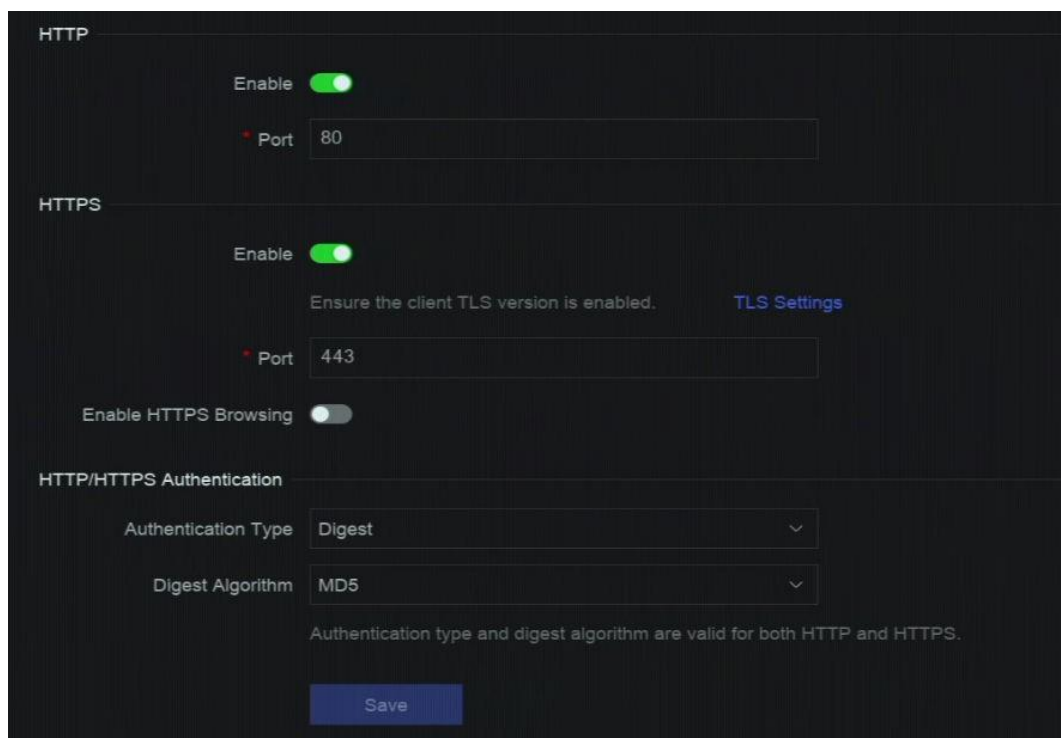


Рисунок 4-11 HTTP(S)

2. **Опционально.** Включите HTTP или HTTPS.
3. Просмотрите или измените **Port** («Порт») HTTP или HTTPS.
4. Настройте **HTTP/HTTPS Authentication** («Аутентификация HTTP / HTTPS»).

Тип аутентификации

По соображениям безопасности рекомендуется выбрать **Digest** («Дайджест») в качестве типа аутентификации.

Алгоритм дайджест-аутентификации

Алгоритмы дайджеста основаны на HTTP / HTTPS и в основном используются для дайджест-аутентификации при аутентификации пользователей.

5. Нажмите **Save** («Сохранить»).

4.3.2 Конфигурация RTSP

RTSP (поточный протокол реального времени) - это протокол управления сетью, предназначенный для управления серверами потоковых мультимедийных данных. При просмотре в режиме реального времени можно обезопасить поток данных, установив аутентификацию RTSP.

Шаги

1. Перейдите в **System** → **System Settings** → **Network** → **Network Service** → **RTSP** («Система → Настройки системы → Сеть → Сетевая служба → RTSP»).

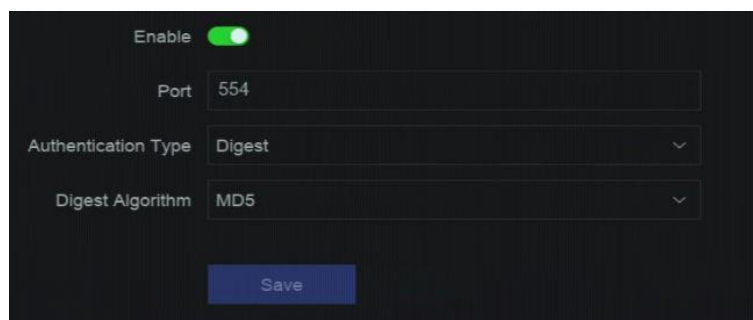


Рисунок 4-12 RTSP

2. Настройте параметры.

Порт

Порт 554 по умолчанию.

Тип аутентификации

Можно выбрать два типа аутентификации: если вы выберете **Digest** («Дайджест»), то получить доступ к видеопотоку по RTSP через IP-адрес можно только по запросу с дайджест-аутентификацией. По соображениям безопасности рекомендуется выбрать **Digest** («Дайджест») в качестве типа аутентификации.

Алгоритм дайджест-аутентификации по протоколу RTSP

Алгоритм дайджест-аутентификации по протоколу RTSP – это алгоритм для дайджест-аутентификации пользователя.

3. Нажмите **Save** («Сохранить»).

4.3.3 Настройка WebSocket(s)

Протокол WebSocket, основанный на TCP, направлен на обеспечение полнодуплексной связи между веб-интерфейсами и серверами. Позволяет открыть двусторонний интерактивный сеанс связи.

Шаги

1. Перейдите в **System** → **System Settings** → **Network** → **Network Service** → **WebSocket(s)** («Система → Настройки системы → Сеть → Сетевая служба → WebSocket(s)').
2. Нажмите **Enable** («Включить»).
3. Установите **Port** («Порт»).
4. Нажмите **Save** («Сохранить»).

4.3.4 Настройка проброса портов (NAT)

При сопоставлении портов для реализации удаленного доступа через межсегментную сеть предусмотрено два способа: UPnP™ (Universal Plug and Play) и ручное сопоставление. Функция UPnP™ позволяет устройству беспрепятственно обнаруживать присутствие других сетевых устройств в сети и создавать функциональные сетевые службы для обмена данными, сообщениями и т. д. Функция UPnP™ обеспечивает быстрое подключение устройства к глобальной сети через маршрутизатор без перенаправления портов.

Перед началом

Если необходимо включить функцию UPnP™ устройства, включите функцию UPnP™ маршрутизатора, к которому подклю­чено устройство. Когда установлен многоадресный режим, маршрут по умолчанию устройства должен находиться в том же сегменте сети, что и IP-адрес LAN маршрутизатора.

Шаги

1. Перейдите в **System** → **System Settings** → **Network** → **Network Service** → **NAT** («Система → Настройки системы → Сеть → Сетевая служба → NAT»).

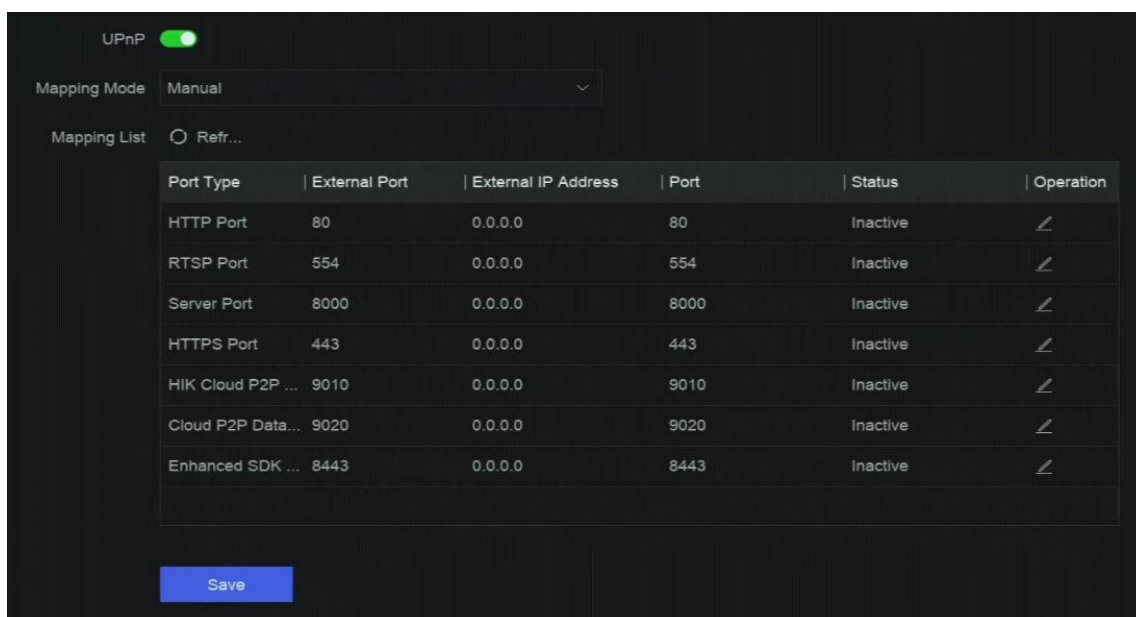


Рисунок 4-13 Перенаправление портов (NAT)


2. Нажмите **Enable** («Включить»).

3. Установите **Mapping Mode** («Режим перенаправления»). **Автоматически**

Элементы сопоставления портов доступны только для чтения, а внешние порты устанавливаются маршрутизатором автоматически.

Вручную

Можно вручную отредактировать внешний порт.

4. Если **Mapping Mode** («Режим перенаправления») выбран как ручной, нажмите , чтобы



Примечание

изменить соответствующие порты.

- Значение номера порта RTSP должно быть 554 или от 1024 до 65535, тогда как значение других портов должно быть от 1 до 65535, и значения должны отличаться друг от друга. Если несколько устройств настроены для настроек UPnP™ под одним и тем же маршрутизатором, значение номера порта для каждого устройства должно быть уникальным.
- **External Port** («Внешний порт») указывает внутренний номер порта для перенаправления портов в маршрутизаторе.

5. Нажмите **Save** («Сохранить»).

Дальнейшие шаги

Войдите на страницу настроек виртуального сервера маршрутизатора, затем заполните пробел внутреннего / внешнего исходного порта значением внутреннего / внешнего порта и другим необходимым содержимым.

4.3.5 Конфигурация IoT

Можно настроить сетевой порт, через который видеореги­стратор будет получать тревоги с охранной панели.

Перейдите в **System** → **System Settings** → **Network** → **Network Service** → **IoT** («Система → Настройки системы → Сеть → Сетевая служба → IoT»), чтобы включить эту функцию и настроить номер порта.



Примечание

Номер порта, который настроен, должен совпадать с портом отправки тревог на охранной панели.

Раздел 5 Управление пользователями

Для администратора есть учетная запись по умолчанию. Имя пользователя администратора — **Admin** («Администратор»). Администратор имеет право добавлять, удалять и редактировать параметры пользователя. Гости и операторы имеют только ограниченные права.

Перейдите в **System → System Settings → User Management** («Система → Настройки системы → Управление пользователями»).

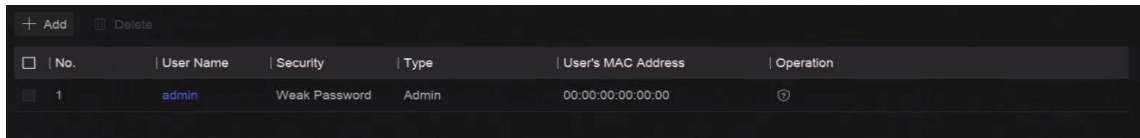


Рисунок 5-1 Управление пользователями

Таблица 5-1 Описание значков / кнопок

Значок / кнопка	Описание
ⓘ	Установите безопасность учетной записи.
+	Добавление
⊗	Удалите выбранного пользователя.

Примечание

Перед началом работы необходимо подтвердить пароль администратора.

Раздел 6 Доступ к устройству

Видеореги­стратор может иметь доступ к нескольким типам устройств, таким как IP-камера, устройство контроля доступа и тревожное устройство. Ознакомьтесь с фактическим устройством для получения информации о возможностях доступа видеореги­стратора.

6.1 Доступ к видеоустройству

Существует несколько способов доступа к видеоустройству.

6.1.1 Добавление сетевой камеры с автоматическим поиском в режиме онлайн

IP-камеры в одном сегменте сети могут быть автоматически найдены и добавлены на устройство.

Шаги

1. Перейдите в **System** → **Device Access** → **Device** → **Video Device** → **Online Device List** («Система → Доступ к устройству → Устройство → Видеоустройство → Список онлайн устройств»).
2. Выберите устройство из списка.

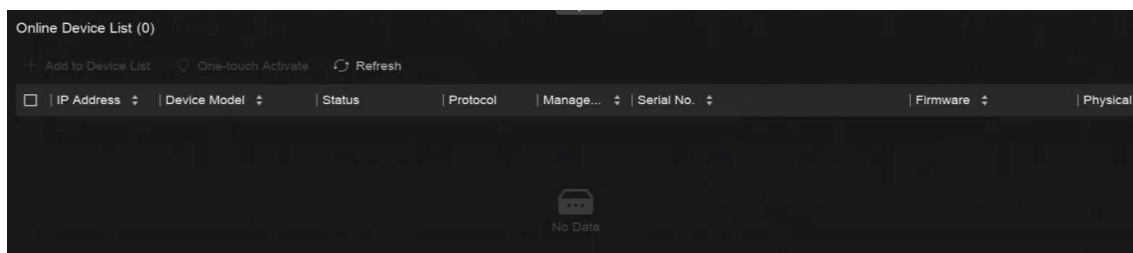


Рисунок 6-1 Добавление IP-камеры посредством автоматического поиска

3. Нажмите **Add to Device List** («Добавление в список устройств»).

Примечание

- Устройство будет использовать пароль по умолчанию для добавления IP-камер. Убедитесь, что пароль камеры совпадает с паролем по умолчанию. Пароль по умолчанию можно настроить в разделе **More** → **Default Password Settings** («Дополнительно → Настройки пароля по умолчанию»).
- Если найденные IP-камеры не активированы, устройство будет использовать пароль по умолчанию для активации и добавления неактивных IP-камер. Пароль по умолчанию можно настроить в разделе **More** → **Default Password Settings** («Дополнительно → Настройки пароля по умолчанию»).

- После успешного добавления IP-камеры ее состояние будет **Online** («Онлайн»).
- Нажмите на название устройства, чтобы добавить его параметры.

6.1.2 Добавление IP-камеры вручную

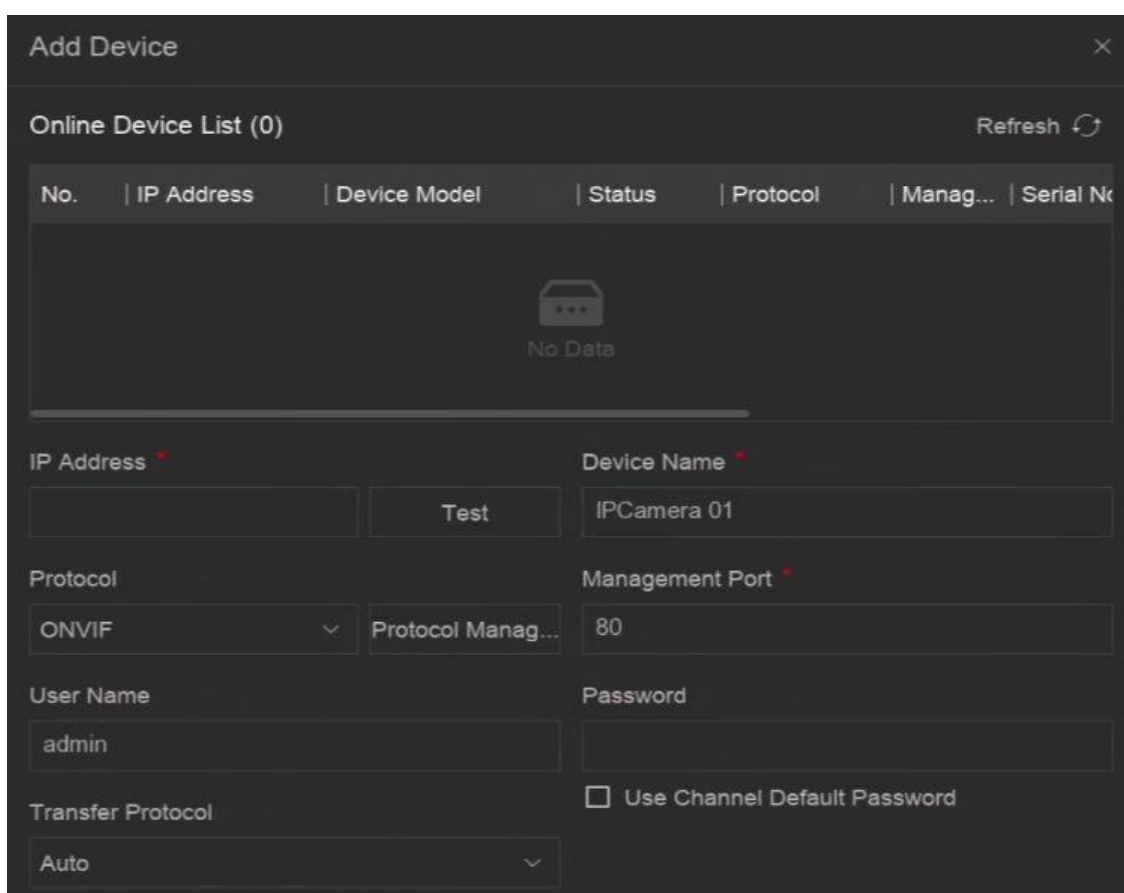
Вручную добавьте IP-камеры к видеореги­стратору.

Перед началом

- Убедитесь, что IP-камера находится в том же сегменте сети, что и видеореги­стратор.
- Убедитесь в правильности сетевого подключения.
- Убедитесь, что IP-камера активирована.

Шаги

1. Перейдите в **System → Device Access → Device → Video Device** («Система → Доступ к устройству → Устройство → Видеоустройство»).



The screenshot shows the 'Add Device' window. At the top, there's a title bar with 'Add Device' and a close button. Below it is a section for 'Online Device List (0)' with a 'Refresh' button. A table with columns 'No.', 'IP Address', 'Device Model', 'Status', 'Protocol', 'Manag...', and 'Serial N' is shown, but it contains 'No Data'. Below the table are several input fields: 'IP Address' with a 'Test' button, 'Device Name' (filled with 'IPCamera 01'), 'Protocol' (dropdown menu showing 'ONVIF'), 'Management Port' (filled with '80'), 'User Name' (filled with 'admin'), 'Password' (empty), and 'Transfer Protocol' (dropdown menu showing 'Auto'). There is also a checkbox labeled 'Use Channel Default Password'.

Рисунок 6-2 Добавление IP-камеры вручную

2. Нажмите **Add** («Добавить»).
3. Введите параметры сетевой камеры.

Использование пароля по умолчанию для канала

Если параметр включен, видеореги­стратор добавит камеру с помощью установленного пароля канала по умолчанию.

Дополнительные настройки

Можно включить **Verify Certificate** («Проверить сертификат»), чтобы проверить камеру с сертификатом. Сертификат - это форма идентификации камеры, обеспечивающая более безопасную аутентификацию камеры. При использовании этой функции необходимо сначала импортировать сертификат IP-камеры на устройство.

4. **Опционально.** Нажмите **Continue to Add** («Продолжить добавление»), чтобы добавить еще одну камеру.

5. Нажмите **Add** («Добавить»).

6.1.3 Добавление сетевой камеры через PoE

IP-камеру с питанием по сети Ethernet можно напрямую подключить к устройству через интерфейс PoE на задней панели.

После подключения IP-камеры с питанием по сети Ethernet к устройству с помощью сетевого кабеля необходимо настроить соответствующий интерфейс PoE. Подробная информация представлена в разделе **Настройка интерфейса PoE (питание по сети Ethernet)**.

6.1.4 Добавление камеры с питанием от солнечной батареи через протокол ONVIF

Камеры с питанием от солнечной батареи можно добавлять на устройство через протокол ONVIF.

Перед началом

Убедитесь, что сеть между устройством и камерой с питанием от солнечной батареи доступна через протокол ONVIF.

Введите содержание задачи (необязательно).

Шаги

1. Перейдите в **System** → **Device Access** → **Device Configuration** → **Access Service** → **ONVIF Service** («Система → Доступ к устройству → Конфигурация устройства → Служба доступа → Служба ONVIF»).
2. Нажмите **Enable** («Включить»).
3. Задайте **Server Port** («Порт сервера») ONVIF и **Encryption Key** («Ключ шифрования»).
4. **Опционально.** Включите **Auto Add IP Camera** («Автоматическое добавление IP-камеры»). После настройки параметров ONVIF устройства новые зарегистрированные IP-камеры (через протокол ONVIF) могут быть автоматически добавлены на устройство.
5. Настройте параметры протокола ONVIF камеры с питанием от солнечной батареи через веб-интерфейс. Подробная информация представлена в руководстве пользователя камеры.



Примечание

Параметры протокола ONVIF камеры с питанием от солнечной батареи должны быть такими же, как у устройства.

-
6. Добавьте камеру с питанием от солнечной батареи на устройство.

- Если включить **Auto Add IP Camera** («Автоматическое добавление IP-камеры»), новые зарегистрированные IP-камеры (через протокол ONVIF) будут автоматически добавлены на устройство.
 - Выберите камеру с питанием от солнечной батареи из **Online Device List** («Список онлайн устройства») и нажмите **Quick Add** («Быстрое добавление»).
7. Нажмите **Add** («Добавить») в меню **System → Device Access → Device → Video Device** («Система → Доступ к устройству → Устройство → Видеоустройство»), выберите **ONVIF** для **Protocol** («Протокол») и нажмите **Add** («Добавить»).

Дальнейшие шаги

- После добавления камеры с питанием от солнечной батареи на устройство можно включить ее, посмотреть заряд батареи, посмотреть видео в режиме реального времени, настроить ее параметры через веб-интерфейс и т. д.
- Настройте ANR (автоматическую детекцию сетевого статуса) для камеры. Подробная информация представлена в разделе [Настройка расписания записи](#).

6.1.5 Добавление IP-камеры по индивидуальному протоколу

Для IP-камер, не поддерживающих стандартные протоколы, можно настроить индивидуальные протоколы. Система предоставляет 8 настраиваемых протоколов.

Перед началом

- Убедитесь, что IP-камера поддерживает потоковую передачу RTSP.
- Подготовьте URL для получения основного или дополнительного потока IP-камер.

Шаги

1. Перейдите в **System → Device Access → Device → Video Device** («Система → Доступ к устройству → Устройство → Видеоустройство»).
2. Перейдите **More → Custom Protocol Management** («Дополнительно → Управление настраиваемым протоколом») или **Add → Protocol Management** («Добавить → Управление протоколом»).

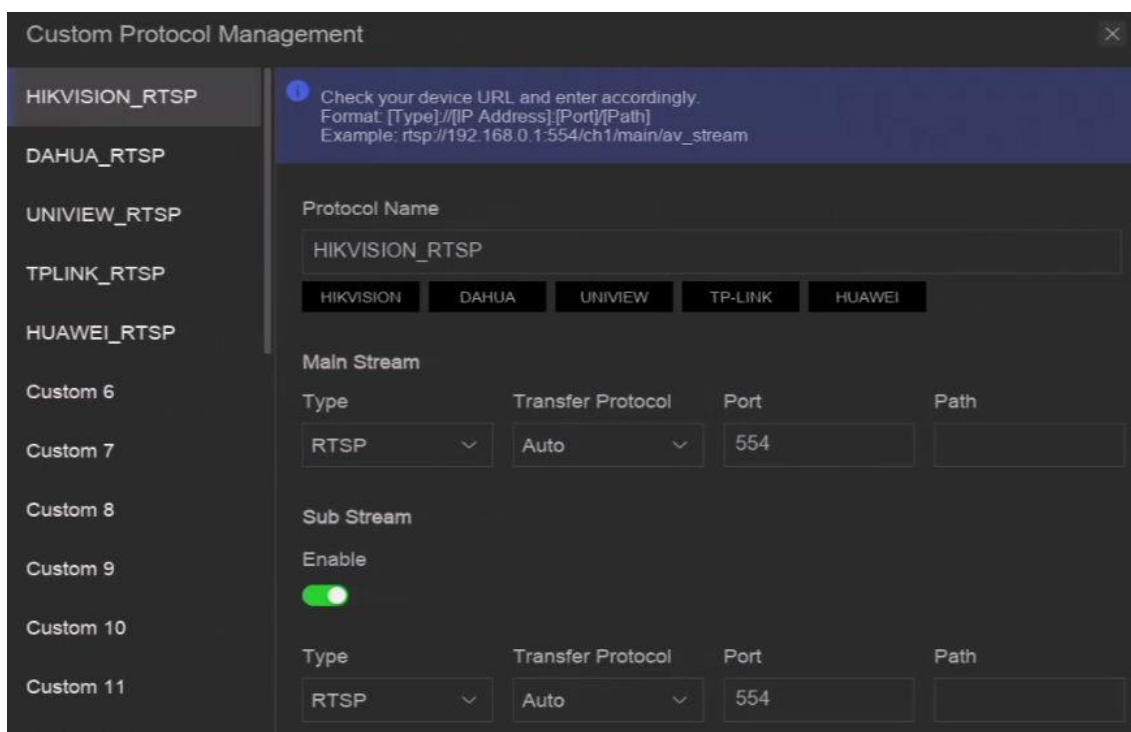


Рисунок 6-3 Добавление IP-камеры по индивидуальному протоколу

3. Выберите тип протокола слева.
4. Настройте параметры протокола.

Тип

IP-камера, использующая индивидуальный протокол, должна поддерживать получение потока через стандартный RTSP.

Протокол передачи

Доступно 3 типа: **Auto** («Автоматический режим»), **UDP** и **RTP Over RTSP** («RTP через RTSP»).

Порт

Значение порта для потоковой передачи данных по RTSP по умолчанию – 554.

Путь

Обратитесь к производителю IP-камеры для получения URL-адреса основного и дополнительного потока. Общий формат: *[Тип]://[IP-адрес]:[Порт]/[Путь к источнику]*. Например, *rtsp://192.168.0.1:554/ch1/main/av_stream*.



Примечание

- **Protocol Name** («Название протокола») и **Path** («Путь») могут быть автоматически сгенерированы, если нажать на название бренда под **Protocol Name** («Название протокола»).
- Можно отключить дополнительный поток, если камера не поддерживает дополнительный поток или не должна использовать дополнительный поток.

5. Нажмите **OK**.

6. Нажмите **Add** («Добавить») в меню **System → Device Access → Device → Video Device** («Система → Доступ к устройству → Устройство → Видеоустройство»), чтобы вручную добавить IP-камеру.

6.1.6 Добавление IP-камеры через файл конфигурации камеры

Информацию о добавленных IP-камерах можно экспортировать, включая IP-адрес, порт, пароль администратора и т. д. Содержимое экспортированного файла конфигурации камеры можно редактировать на компьютере. После редактирования файл также можно импортировать на другие устройства, чтобы добавить камеры в файл.

Перед началом

Подключите видеореги­стратор к USB-накопителю, содержащему файл конфигурации камеры.

Шаги


1. Перейдите в **System → Device Access → Device → Video Device** («Система → Доступ к устройству → Устройство → Видеоустройство»).
2. Нажмите **Import** («Импорт»), чтобы импортировать файл конфигурации на USB-накопитель.
3. Укажите путь к папке.
4. Нажмите **Confirm** («Подтвердить»).

6.2 Добавление устройств контроля доступа

Устройства контроля доступа можно добавлять к видеореги­стратору. Процесс добавления аналогичен процессу, описанному в разделе [Доступ к видеоустройству](#).

6.3 Добавление охранной панели

Шаги

1. Перейдите в **System → Device Access → Device → Security Control Panel** («Система → Доступ к устройству → Устройство → Охранная панель»).
2. Нажмите **Add** («Добавить»).
3. **Опционально.** Выберите протокол.
4. Введите IP-адрес устройства, имя и порт службы IoT.
5. **Опционально.** Если выбран **OPTEX** в качестве типа протокола, выберите протокол передачи.
6. **Опционально.** Нажмите  в столбце **Operation** («Операции»), чтобы задать параметры экранного меню, включая кодировку символов, режим наложения, размер шрифта и т. д.



Примечание

Привязанный канал нельзя редактировать. Перейдите **Event Center → Event Configuration → Event Configuration → Security Control Panel Event** («Центр событий → Конфигурация событий → Конфигурация событий → Событие охранной панели»), чтобы отредактировать привязанный канал.

Настроенная OSD-информация будет отображаться на видеоизображении.

6.4 Добавление аудиоустройства

К видеореги­стратору можно добавлять аудиоустройства, например, IP-динамики и микрофоны.

Процесс добавления аналогичен процессу, описанному в разделе [Доступ к видеоустройству](#). Если привязать видеоканалы к IP-динамике, то IP-динамик можно использовать для голосового вещания. Если привязать видеоканалы к микрофону, то микрофон будет использоваться в качестве аудиовхода привязанных видеоканалов при записи видео.

6.5 Добавление POS-устройства

POS-терминал / сервер могут быть подключены к определенным моделям устройств. Устройство может получать сообщения о транзакциях от POS-терминала / сервера, накладывать сообщения о транзакциях на видеоизображение и запускать тревоги POS-событий.

Шаги

1. Перейдите в **System** → **Device Access** → **Device** → **POS** («Система → Доступ к устройству → Устройство → POS»).
2. Нажмите **Add** («Добавить»), чтобы добавить POS-устройство.

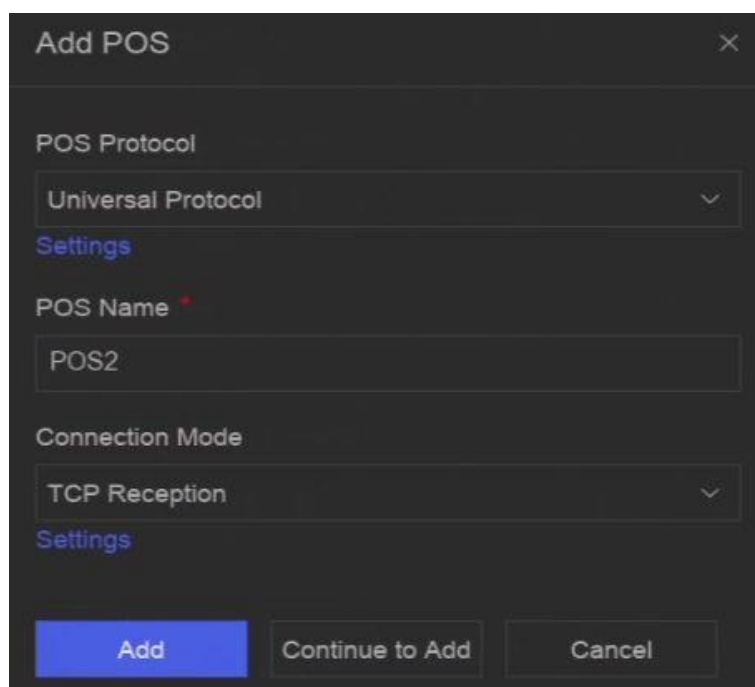


Рисунок 6-4 Добавление POS-устройства

3. Настройте параметры POS-устройства.

Протокол POS

Универсальный протокол

Установите идентификатор начальной строки, тег разрыва строки и тег конечной строки для символов наложения POS-информации, а также свойство символов с учетом регистра. Также можно дополнительно проверить идентификатор фильтрации и протокол XML.

EPSON

Фиксированные теги начальной и конечной строки используются для протокола EPSON.

AVE

Фиксированные теги начальной и конечной строки используются для протокола AVE. Поддерживаются следующие типы подключения: серийный интерфейс и виртуальный последовательный порт.

NUCLEUS

Фиксированные теги начальной и конечной строки используются для протокола AVE. Поддерживаются следующие типы подключения: серийный интерфейс и виртуальный последовательный порт. Протокол NUCLEUS должен использоваться при соединении RS-232.

Режим подключения

TCP-соединение

При использовании TCP-соединения порт должен быть установлен в значении от 1 до 65535, и порт для каждого POS-терминала должен быть уникальным.

UDP-соединение

При использовании UDP-соединения порт должен быть установлен в значении от 1 до 65535, и порт для каждого POS-терминала должен быть уникальным.

Подключение-RS-232 через USB

Настройте параметры порта преобразователя USB в RS-232, включая номер серийного интерфейса, скорость передачи данных, бит данных, стоповый бит и четность.

RS-232-соединение

Подключите устройство к POS-терминалу через RS-232.

Многоадресное соединение

При подключении устройства и POS-терминала по протоколу многоадресной передачи установите адрес и порт многоадресной передачи.


Соединение через сниффер

Подключите устройство к POS-терминалу через сниффер. Настройте параметры адреса источника и адреса назначения.

4. Нажмите Add («Добавить»).



Примечание

После добавления POS-устройства можно нажать  в разделе **Operation** («Операция»), чтобы настроить наложение POS-текста.

6.6 Управление каналами

После добавления видеоустройства можно посмотреть его номер канала и название канала, а также управлять его параметрами. Эта функция в основном используется для видеоустройства, которое содержит более одного канала.

Перейдите в **System** → **Device Access** → **Channel** («Система → Доступ к устройству → Канал») для управления каналами видеоустройств.

Раздел 7 Группировка устройства

Добавленные устройства можно классифицировать по различным настраиваемым группам.

Шаги

1. Перейдите в **System** → **Device Access** → **Device Grouping** («Система → Доступ к устройству → Группировка устройств»).

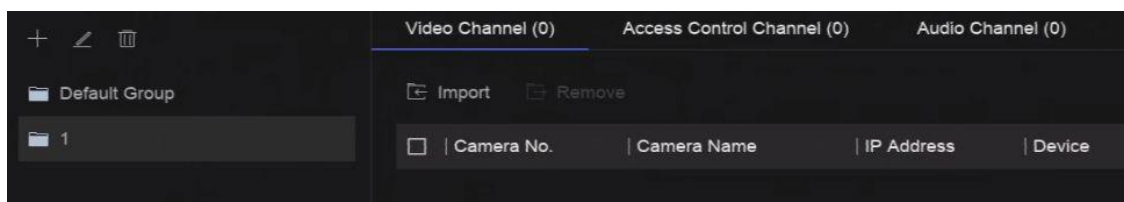


Рисунок 7-1 Группировка устройств

2. Нажмите **+**, чтобы добавить группу.

Примечание

После добавления группы можно нажать  / , чтобы изменить / удалить ее.

3. Нажмите **Import** («Импорт»), чтобы добавить каналы в выбранную группу.

Раздел 8 Настройки видео- или аудиоустройств

Можно настроить маскирование области, параметры изображения и др. для добавленного видео- или аудиоустройства.

8.1 Включение доступа к потоку H.265

Устройство может автоматически переключаться на поток H.265 IP-камеры (которая поддерживает видеоформат H.265) для начального доступа.

Шаги

1. Перейдите в **System → Device Access → Device → Video Device** («Система → Доступ к устройству → Устройство → Видеоустройство»).
2. Перейдите **More → Auto Switch to H.265** («Дополнительно → Автоматическое переключение на H.265»).
3. Включите эту функцию.
4. Нажмите **Save** («Сохранить»).

8.2 Настройка параметров отображения

Настройка экранного меню (OSD), настройка изображения, настройка экспозиции, настройка переключения режима «день/ночь» и т. д.

Перейдите в **System → Device Access → Device Configuration → Device Parameter → Video Device → Display Settings** («Система → Доступ к устройству → Конфигурация устройства → Параметры устройства → Видеоустройство → Настройки отображения»). Выберите камеру и настройте необходимые параметры.

Настройка параметров OSD

Настройте экранное меню (OSD) для камеры, включая дату / время, имя камеры и т. д.

Настройки изображения

Настройте параметры изображения, включая яркость, контрастность и насыщенность для просмотра в режиме реального времени и эффекта записи.

Время экспозиции

Установите время экспозиции камеры (от 1/10000 до 1 секунды). Чем больше значение экспозиции, тем ярче изображение.

Переключение режима «День / ночь»

В камере можно установить дневной, ночной или автоматический режим переключения в зависимости от условий окружающего освещения.

Контрольная засветка

Установите широкий динамический диапазон камеры (от 0 до 100). Если окружающее освещение и объект сильно различаются по яркости, следует установить значение WDR.

Улучшение изображения

Для оптимизированного повышения контрастности изображения.

8.3 Настройка параметров видео

Параметры видео повлияют на изображение в режиме времени и файл записи.

Перейдите в **System → Device Access → Device Configuration → Device Parameter → Video Device → Video Parameters** («Система → Доступ к устройству → Конфигурация устройства → Параметры устройства → Видеоустройство → Параметры видео»). Выберите камеру и настройте необходимые параметры.

Основной поток

Основной поток влияет на данные, записываемые на жесткий диск, и напрямую определяет качество видео и размер изображения. По сравнению с дополнительным потоком основной поток обеспечивает более высокое качество видео с более высоким разрешением и частотой кадров.

Дополнительный поток

Дополнительный поток — это второй кодек, который работает вместе с основным потоком. Это позволяет уменьшить исходящую пропускную способность интернета без ущерба для качества прямой записи. Дополнительный поток часто используется приложениями для смартфонов исключительно для просмотра видео в режиме реального времени. Данная настройка может принести наибольшую пользу пользователям с ограниченной скоростью интернета.

Разрешение

Разрешение изображения - это мера того, сколько деталей может содержать цифровое изображение: чем больше разрешение, тем выше уровень детализации. Чем выше разрешение, тем выше уровень детализации. Разрешение может быть указано как количество столбцов пикселей (ширина) по количеству строк пикселей (высота), например, например, 1024 × 768.

Тип битрейта

Скорость передачи данных (в Кбит/с или Мбит/с) часто называют скоростью, но на самом деле она определяет количество бит / единицу времени, а не расстояние / единицу времени. Доступны два типа: переменный и постоянный.

Частота кадров

Частота кадров означает, сколько кадров захватывается за секунду. Более высокая частота кадров предпочтительна для съемки движущихся объектов, так как при этом сохраняется высокое качество видео.

Интервал I-кадра

I-кадр также называют внутренним изображением. I-кадр – это первый кадр каждого GOP (технология сжатия видео в MPEG). Его можно просматривать как изображения после сжатия. Интервал I-кадра – это количество кадров между двумя непрерывными I-кадрами.

8.4 Настройка маскирования

Маскирование области способствует защите конфиденциальной информации, скрывая части изображения от просмотра в режиме реального времени или записи области маскирования.

Шаги

1. Перейдите в **System → Device Access → Device Configuration → Device Parameter → Video Device → Privacy Mask** («Система → Доступ к устройству → Конфигурация устройства → Параметры устройства → Видеоустройство → Маскирование области»).

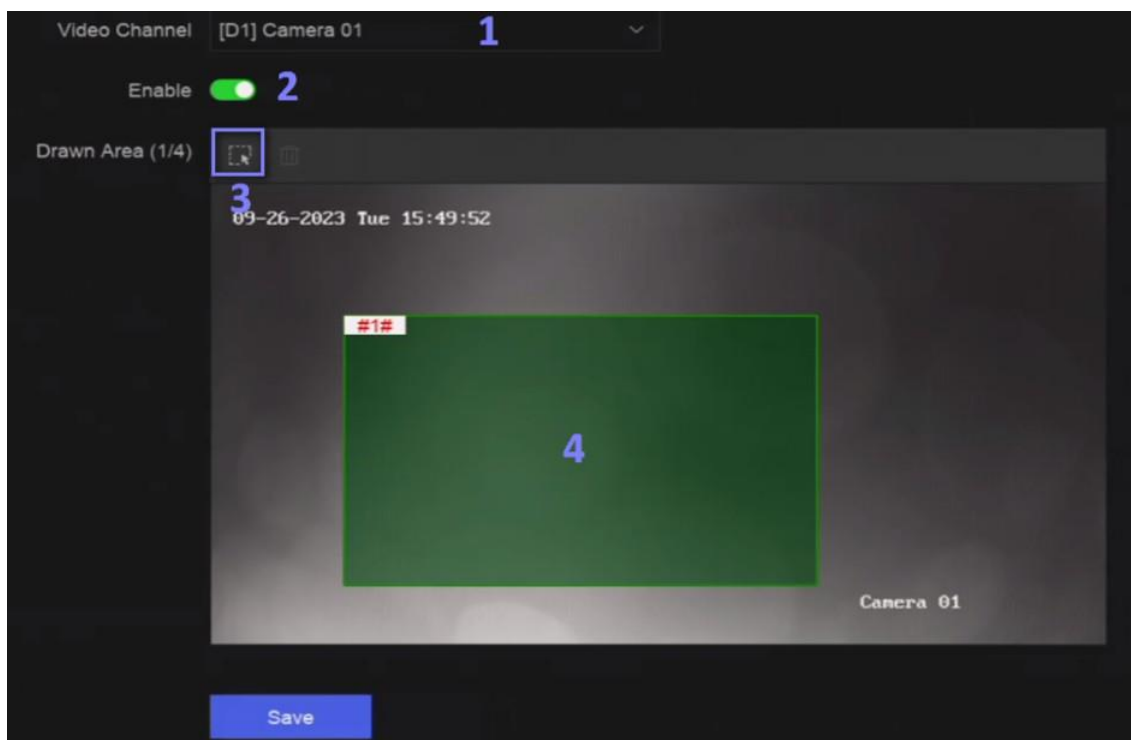


Рисунок 8-1 Маскирование области

2. Выберите камеру.
3. Нажмите **Enable** («Включить»).
4. Нарисуйте маски области в окне предварительного просмотра. Области будут отмечены



Примечание

рамками разных цветов.

Можно настроить до 4 масок области и отрегулировать размер каждой области.

5. Нажмите **Save** («Сохранить»).

8.5 Конфигурация защиты конфиденциальных данных

Эта функция позволяет автоматически затемнять или размывать определенные области (включая лицо, фигуру человека и ТС) на видеозаписи для защиты личной информации или конфиденциальных данных.

Перед началом

Камера должна поддерживать данную функцию.

Шаги

1. Перейдите в **System** → **Device Access** → **Device Configuration** → **Device Parameter** → **Video Device** → **Privacy Protection** («Система → Доступ к устройству → Конфигурация устройства → Параметры устройства → Видеоустройство → Защита конфиденциальных данных»).

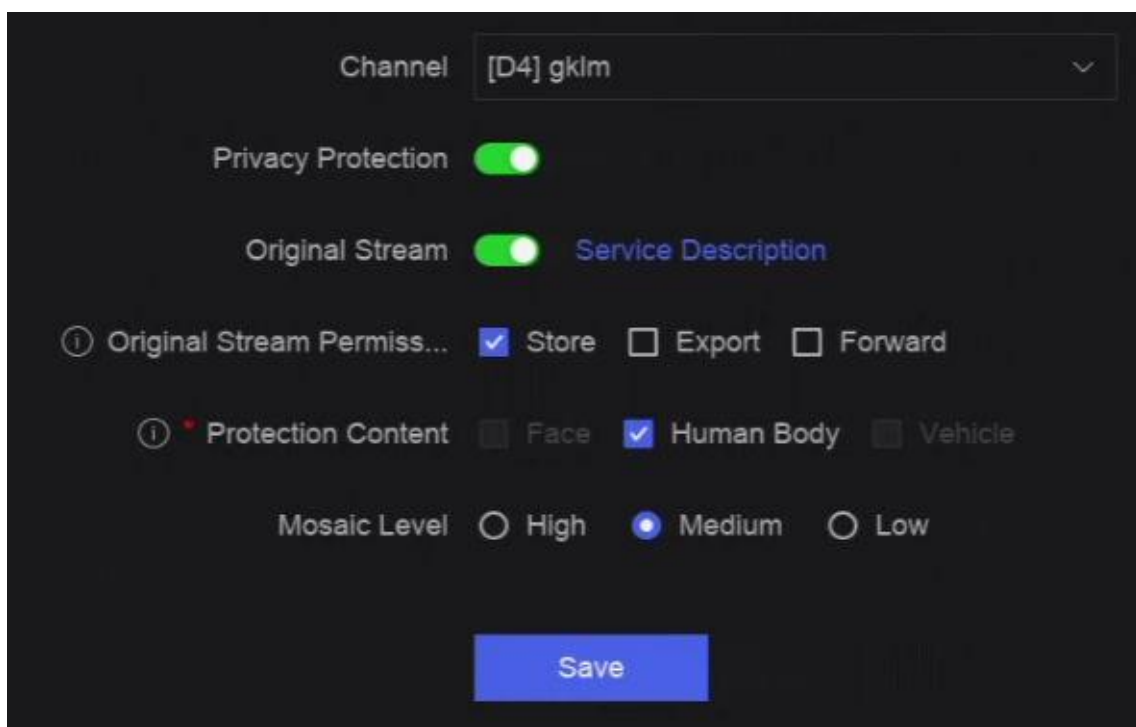


Рисунок 8-2 Защита конфиденциальных данных

2. Выберите камеру.
3. Включите **Privacy Protection** («Защита конфиденциальных данных»).
4. **Опционально.** Включите **Original Stream** («Исходный поток») и настройте разрешение

Примечание

потока.

Исходный поток означает видеопоток без маскирования

Сохранение

Исходный поток можно сохранить. Сохранение исходного потока приведет к увеличению объема памяти или уменьшению срока хранения записи канала. Битрейт исходного потока совпадает с битрейтом камеры, который не настраивается.

Экспорт

Исходный поток канала может быть экспортирован.

Переадресация

Исходный поток может быть переадресован.



Примечание

Необходимо проверить разрешение на сохранение, прежде чем проверять разрешения на экспорт и переадресацию.

5. Установите **Protection Content** («Защищенный контент»). Выбранный защищенный контент будет размыт при просмотре в режиме реального времени и воспроизведении.
6. Установите **Mosaic Level** («Уровень маскирования»). Чем выше уровень, тем более размытым будет целевое изображение.
7. Нажмите **Save** («Сохранить»).

8.6 Настройка параметров аудио

После добавления аудиоустройства можно настроить его параметры в **System → Device Access → Device Configuration → Device Parameter → Audio Device** («Система → Доступ к устройству → Конфигурация устройства → Параметры устройства → Аудиоустройство»). Например, если добавлен IP-динамик, можно настроить его название, громкость аудиовыхода и качество звука.

8.7 Настройка службы OTAP

OTAP – это единый интегрированный стандарт и режим push-pull протокола Hikvision в публичной и частной сети. После включения OTAP другие приложения могут удаленно просматривать видео через этот протокол.

Перед началом

Убедитесь, что сеть устройства доступна через протокол OTAP.

Шаги

1. Перейдите в **System → Device Access → Device Configuration → Access Service → OTAP Service** («Система → Доступ к устройству → Конфигурация устройства → Служба доступа → Служба OTAP»).

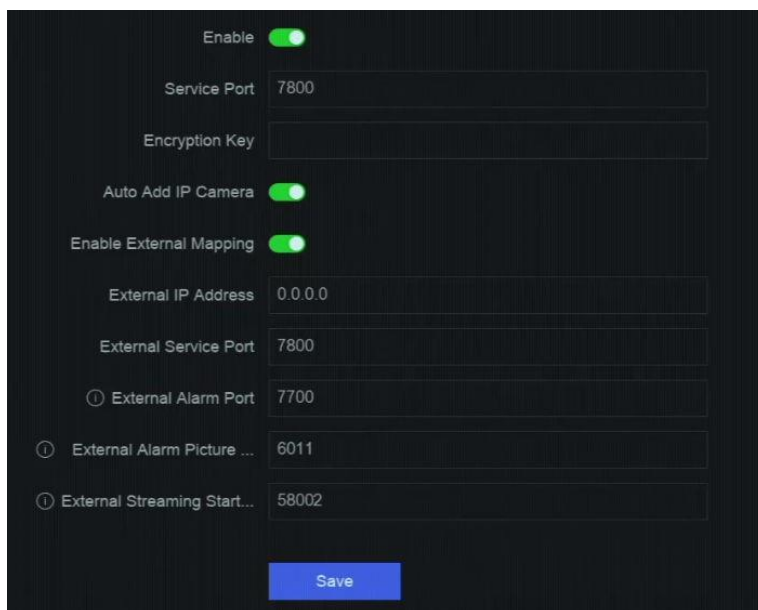


Рисунок 8-3 Настройка службы ONVIF

2. Нажмите **Enable** («Включить»).
3. Настройте параметры.
4. Нажмите **Save** («Сохранить»).

8.8 Настройка в пакетном режиме

Подключенные устройства можно настроить в пакетном режиме.

Шаги

1. Перейдите в **System** → **Device Access** → **Device Configuration** → **Batch Configuration** («Система → Доступ к устройству → Конфигурация устройства → Конфигурация в пакетном режиме»).

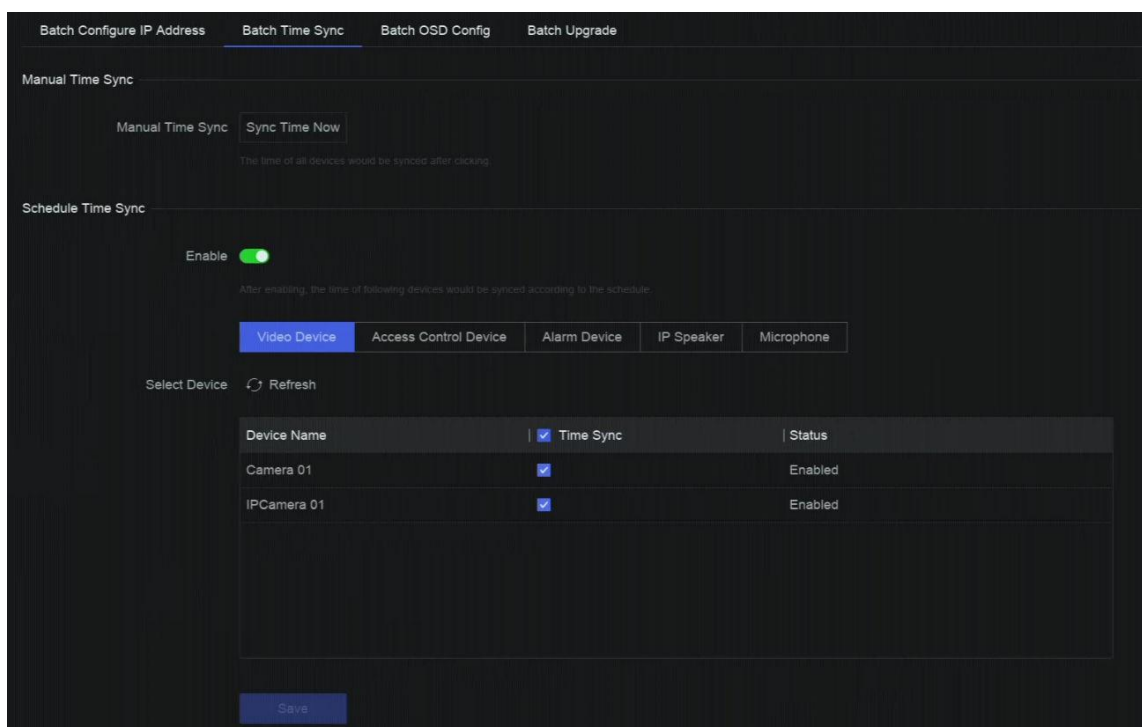


Рисунок 8-4 Конфигурация в пакетном режиме

2. Настройте IP-адрес, синхронизацию времени, OSD или обновите прошивку.

Синхронизация времени вручную

Нажмите **Sync Time Now** («Синхронизировать время сейчас»), чтобы вручную синхронизировать время всех подключенных устройств. Эта операция выполняется только один раз.

Синхронизация времени по расписанию

Регистратор будет синхронизировать время выбранных устройств по фиксированному графику.

3. Для настройки IP-адреса и синхронизации времени нажмите **Save** («Сохранить»).

8.9 Настройка PoE-интерфейса

PoE-интерфейсы позволяют устройству передавать электроэнергию и данные на подключенные устройства с поддержкой PoE. PoE-интерфейс поддерживает функцию Plug-and-Play. Количество подключаемых устройств с поддержкой PoE зависит от моделей устройства. Если отключить PoE-интерфейс, его также можно использовать для подключения к устройству в режиме онлайн.

Перед началом

Убедитесь, что NVR поддерживает функцию PoE.

Шаги

1. Перейдите в **System → Device Access → Device Configuration → PoE** («Система → Доступ к устройству → Конфигурация устройства → PoE»).

2. Включите функцию **Plug-and-Play** PoE-интерфейсов, если необходимо.
3. Выберите тип устройства: **IP Speaker** («IP-динамик») или **Camera** («Камера»).
4. Если PoE-интерфейс используется для подключения камеры с поддержкой PoE, выберите расстояние подключения сетевого кабеля.

Большая дальность

Передача по сети на большие расстояния (от 100 до 300 метров) через интерфейс PoE.

Малая дальность

Передача по сети на короткие расстояния (< 100 метров) через интерфейс PoE.



Примечание

- PoE-интерфейсы по умолчанию включены в режиме малой дальности.
 - Пропускная способность IP-камеры, подключенной к PoE через длинный сетевой кабель (от 100 до 300 м), не может превышать 6 Мбит/с.
 - Допустимая максимальная длина сетевого кабеля может составлять не более 300 метров в зависимости от различных моделей IP-камер и материалов кабелей.
 - Когда расстояние передачи достигает от 100 до 250 метров, необходимо использовать сетевой кабель Cat5e или Cat6 для подключения к интерфейсу PoE.
 - Когда расстояние передачи достигает 250–300 метров, вы должны использовать сетевой кабель CAT6 для подключения к интерфейсу PoE.
-

5. Нажмите **Save** («Сохранить»).

Дальнейшие шаги

Когда подключены устройства с поддержкой PoE, можно просматривать состояние и питание каждого PoE-интерфейса.

Раздел 9 Управление хранением

9.1 Управление HDD

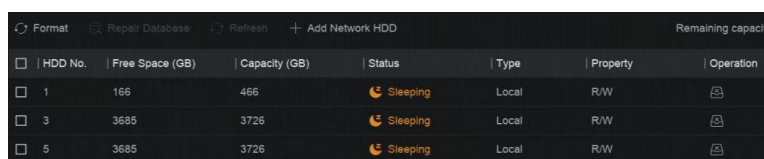
Перед использованием новый жесткий диск (HDD) необходимо инициализировать. Можно отформатировать HDD, восстановить базу данных и просмотреть состояние HDD через интерфейс управления HDD.

Перед началом

Убедитесь, что HDD правильно установлен.

Шаги

1. Перейдите в **System** → **Storage Management** → **Storage HDD** → **Storage HDD** («Система → Управление хранением → Хранение на HDD → Хранение на HDD»).



HDD No.	Free Space (GB)	Capacity (GB)	Status	Type	Property	Operation
1	166	466	Sleeping	Local	R/W	[Icon]
3	3685	3726	Sleeping	Local	R/W	[Icon]
5	3685	3726	Sleeping	Local	R/W	[Icon]

Рисунок 9-1 Управление HDD

2. **Опционально.** Выполните следующие необходимые операции.

Добавление сетевого HDD Добавление NAS или IP SAN.

Формат

Форматирование выбранного HDD.

Восстановление базы данных

Функция восстановления базы данных восстанавливает все базы данных. Это может помочь повысить скорость работы системы после обновления.

 **Примечание**

- Функция восстановления базы данных восстанавливает все базы данных. Существующие данные не будут затронуты, но функции локального поиска и воспроизведения будут недоступны во время процесса, при этом вы по-прежнему можете выполнять функции поиска и воспроизведения удаленно через веб-интерфейс, клиентское ПО и т. д.
- Не вынимайте накопитель и не выключайте устройство во время процесса.

 /  Извлечение / загрузка жесткого диска.

9.2 Настройка RAID

Массив дисков - это технология виртуализации хранилища данных, которая объединяет несколько физических дисков в одну логическую единицу. Также известный как «RAID», массив хранит данные на нескольких жестких дисках, чтобы обеспечить резервное копирование для восстановления данных в случае отказа одного из дисков. Данные распределяются по дискам одним из нескольких способов, называемых «уровнями RAID», в зависимости от требований к резервному копированию и производительности.

 **Предостережение**

RAID требует HDD корпоративного уровня.

Функции данного раздела представлены не во всех моделях. Рекомендуется использовать HDD той же модели и емкости.

Существует два способа создания RAID. Для быстрой настройки тип RAID по умолчанию – RAID5. Для настройки вручную доступно: RAID0, RAID1, RAID5, RAID6 и RAID10.

Таблица 9-1 Требования к HDD для каждого типа RAID

Тип RAID	Требуемое количество HDD
RAID0	≥ 2
RAID1	2
RAID5	≥ 3
RAID6	≥ 4
RAID10	4 или 8

Примечание

- Данная функция представлена не во всех моделях.
- При возникновении события исключения массива соответствующие действия по привязке можно настроить в **System → System Settings → Exception** («Система → Параметры системы → Исключение»).

9.2.1 Создание массива дисков

Массив дисков можно создать после включения режима массива.

Перед началом

- **Storage Mode** («Режим хранения») установлен на **Quota** («Квота») в **System → Storage Management → Storage Mode** («Система → Управление хранением → Режим хранения»).
- Убедитесь, что на устройстве правильно установлено достаточное количество HDD. Для создания массива необходимо использовать HDD уровня ИИ или корпоративного уровня.

Шаги

1. Перейдите в **System → Storage Management → Storage HDD → Array Management** («Система → Управление хранением → Хранение на HDD → Управление массивом»).
2. Нажмите **Enable Array Mode** («Включить режим массива») или включите **Array Mode** («Режим массива»).

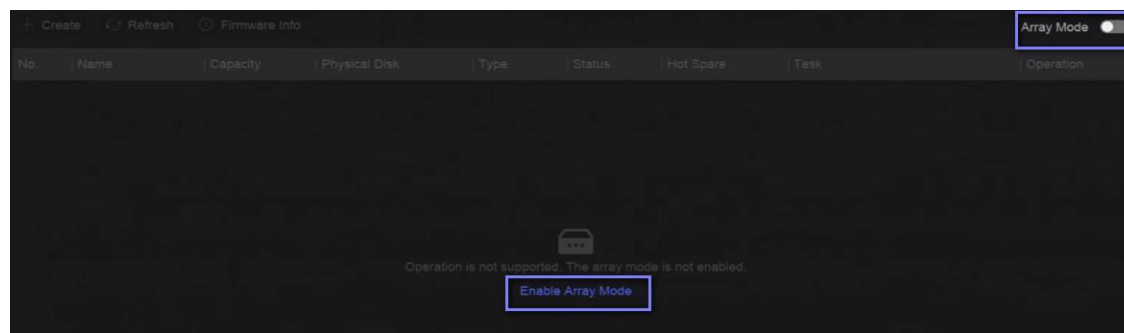


Рисунок 9-2 Включение RAID

3. Дождитесь перезагрузки устройства.
4. Снова перейдите в **System → Storage Management → Storage HDD → Array Management** («Система → Управление хранением → Хранение на HDD → Управление массивом»).

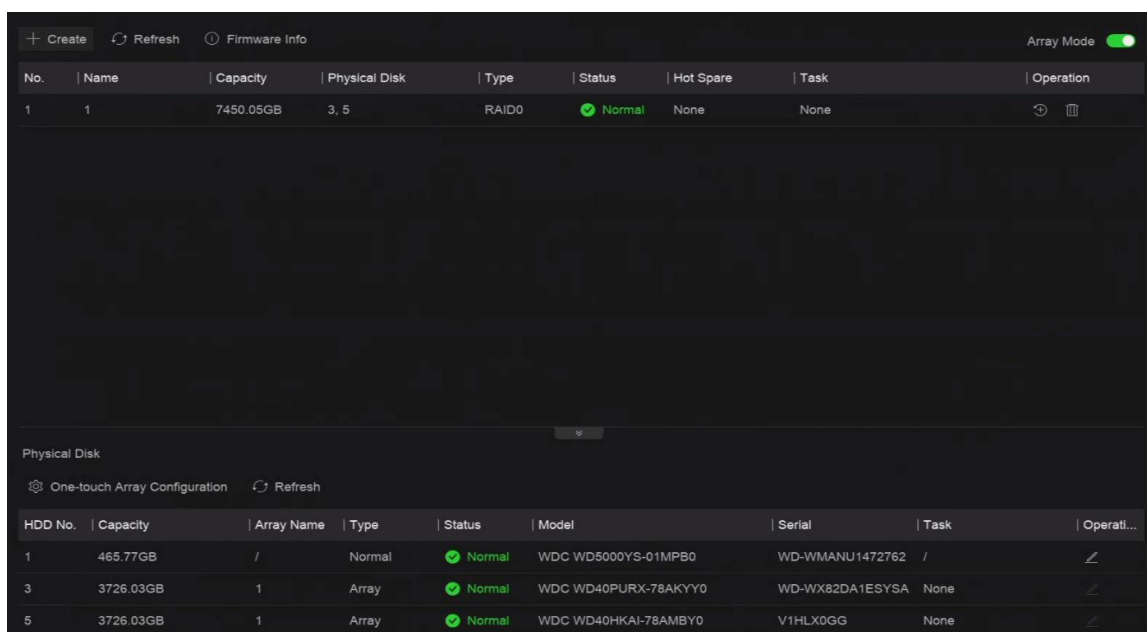


Рисунок 9-3 Управление массивом

5. Создайте массив.

Способ создания

Быстрая конфигурация массива

Описание

Нажмите **One-touch Array Configuration** («Быстрая конфигурация массива»).

Примечание

По умолчанию при настройке в одно касание создается массив типа RAID 5.

Создание вручную

Нажмите **Create** («Создать»), чтобы вручную создать массив RAID 0, RAID 1, RAID 5, RAID 6 или RAID 10.



9.2.2 Восстановление массива

Массив может иметь один из следующих состояний: **Functional** («Функциональный»), **Degraded** («Поврежденный») и **Offline** («Не в сети»). Чтобы обеспечить высокую безопасность и надежность данных, хранящихся в массиве, необходимо обеспечить своевременное обслуживание массивов в соответствии с их статусом.


Шаги

1. Перейдите в **System → Storage Management → Storage HDD → Array Management** («Система → Управление хранением → Хранение на HDD → Управление массивом»).
2. Восстановите массив.

Таблица 9-2 Способ восстановления

Способ восстановления	Описание
Автоматическое восстановление	<p>В массиве должен быть диск горячего резервирования с емкостью не меньше, чем у диска с минимальной емкостью в массиве. Нажмите  в столбце Operation («Операции») под Physical Disk («Физический диск»), чтобы установить диск горячего резервирования.</p> <p>Если жесткий диск в массиве не работает, будет активирован диск горячего резервирования, и массив будет автоматически перестроен.</p> <p> Примечание</p> <p>После завершения автоматического восстановления рекомендуется установить другой жесткий диск и настроить его как диск горячего резервирования.</p>
Восстановление вручную	<p>Если в массиве нет дисков горячего резервирования, необходимо вручную перестроить массив.</p> <p>Перейдите в System → Storage Management → Storage HDD → Array Management («Система → Управление хранением → Хранение на HDD → Управление массивом») и выберите в списке резервный диск для восстановления.</p>

9.2.3 Удаление массива

Перейдите в **System → Storage Management → Storage HDD** («Система → Управление хранением → Хранение на HDD»), нажмите на , чтобы удалить выбранный массив.

9.2.4 Просмотр информации о прошивке

Можно просмотреть информацию о прошивке массива и задать скорость фоновой задачи.

Перед началом

Убедитесь, что массив дисков включен.

Шаги

1. Перейдите в **System → Storage Management → Storage HDD → Array Management** («Система → Управление хранением → Хранение на HDD → Управление массивом»).
2. Нажмите **Firmware Info** («Информация о прошивке»).
3. **Опционально.** Настройте **Back Ground Task Speed** («Скорость фоновой задачи»).

9.3 Настройка режима хранения

Шаги

1. Перейдите в **System → Storage Management → Storage Mode** («Система → Управление хранением → Режим хранения»).

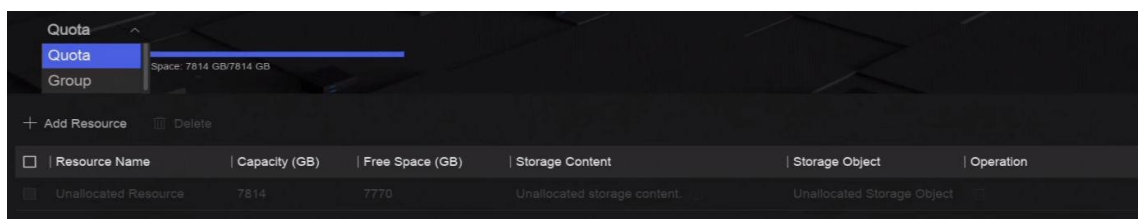


Рисунок 9-4 Режим хранения

2. Выберите **Quota** («Квота») или **Group** («Группа»). **Quota** («Квота»)

Каждая камера или аудиоустройство могут быть настроены с выделенной квотой для хранения видео, изображений или аудио.

Группа




Можно управлять несколькими жесткими дисками в группах. Видео с указанных каналов может быть записано на определенную группу жестких дисков через настройки жесткого диска.

3. Настройте соответствующие параметры.
 - **Quota** («Квота»): Выделите место для объектов хранения.
 - **Group** («Группа»). Привязка каналов к группам HDD.

9.4 Конфигурация других параметров хранения


Перейдите в **System** → **Storage Management** → **Advanced Settings** («Система → Управление хранением → Расширенные настройки»).

Таблица 9-3 Описание параметров

Имя параметра	Описание
Включение спящего режима HDD	Выберите режим для HDD. Доступно: Performance Mode («Режим максимальной производительности»), Balanced Mode («Сбалансированный режим») и Energy Saving Mode («Режим энергосбережения»).
Перезапись	Когда жесткий диск заполнен, видеореги­стратор продолжит запись новых файлов, удаляя самые старые файлы.
Сохранение VCA данных камеры	Данные VCA с камеры будут доступны для поиска в центре событий после сохранения на устройстве.
Макс. длина видеозаписи	Продолжительность каждого видеофайла при экспорте видео с устройства.
Запись видео с тегами	После добавления тега к видео, установите время, после которого начнется запись.  Примечание <ul style="list-style-type: none"> Можно нажать  во время просмотра в режиме реального времени или воспроизведения, чтобы добавить тег. Для поиска видео с тегами перейдите в  → Backup → By Tag («Резервное копирование → По тегам»).
eSATA	Для устройств с интерфейсом eSATA на задней панели.
Применение	Установите использование eSATA.

9.5 Управление USB-накопителем

После установки USB-накопителя в устройство можно просматривать его оставшуюся емкость, управлять его содержимым или форматировать его.

При первом подключении USB-накопителя к устройству можно выполнять обновление устройства и резервное копирование. В правом верхнем углу будет отображаться новый значок .

Раздел 10 Конфигурация расписания

Устройство будет следовать расписанию для сохранения файлов на диск.

10.1 Настройка шаблона расписания

Настройте шаблон расписания, чтобы использовать его в качестве расписания записи.

Шаги

1. Перейдите в **System** → **System Settings** → **Template Configuration** → **Holiday Schedule** («Система → Настройки системы → Конфигурация шаблона → Расписание выходных дней»).
2. Нажмите **Add** («Добавить»).

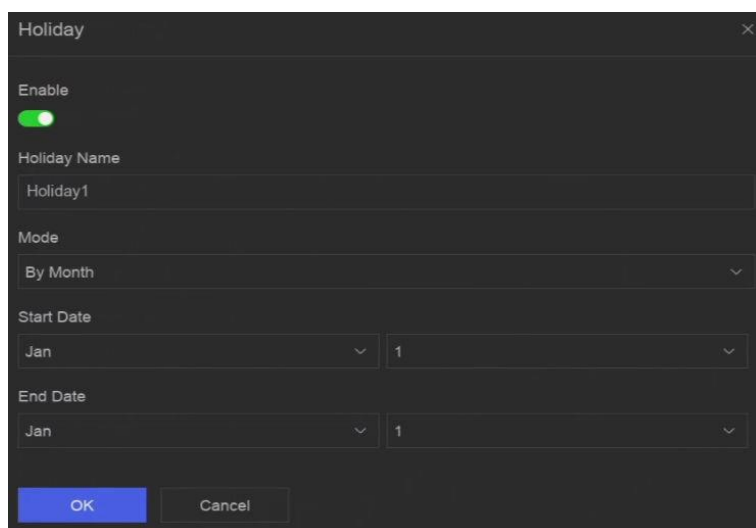


Рисунок 10-1 Добавление выходного дня

3. Нажмите **Enable** («Включить»).
4. Настройте выходной день.

Примечание

Сначала настройте выходные дни, затем можно самостоятельно настраивать расписание выходных дней. Расписание выходных дней имеет более высокий приоритет, чем обычное расписание (с понедельника по воскресенье).

-
5. Настройте **Storage Schedule** («Расписание хранения»).
 - 1) Нажмите **Storage Schedule** («Расписание хранения»).
 - 2) Выберите название шаблона.

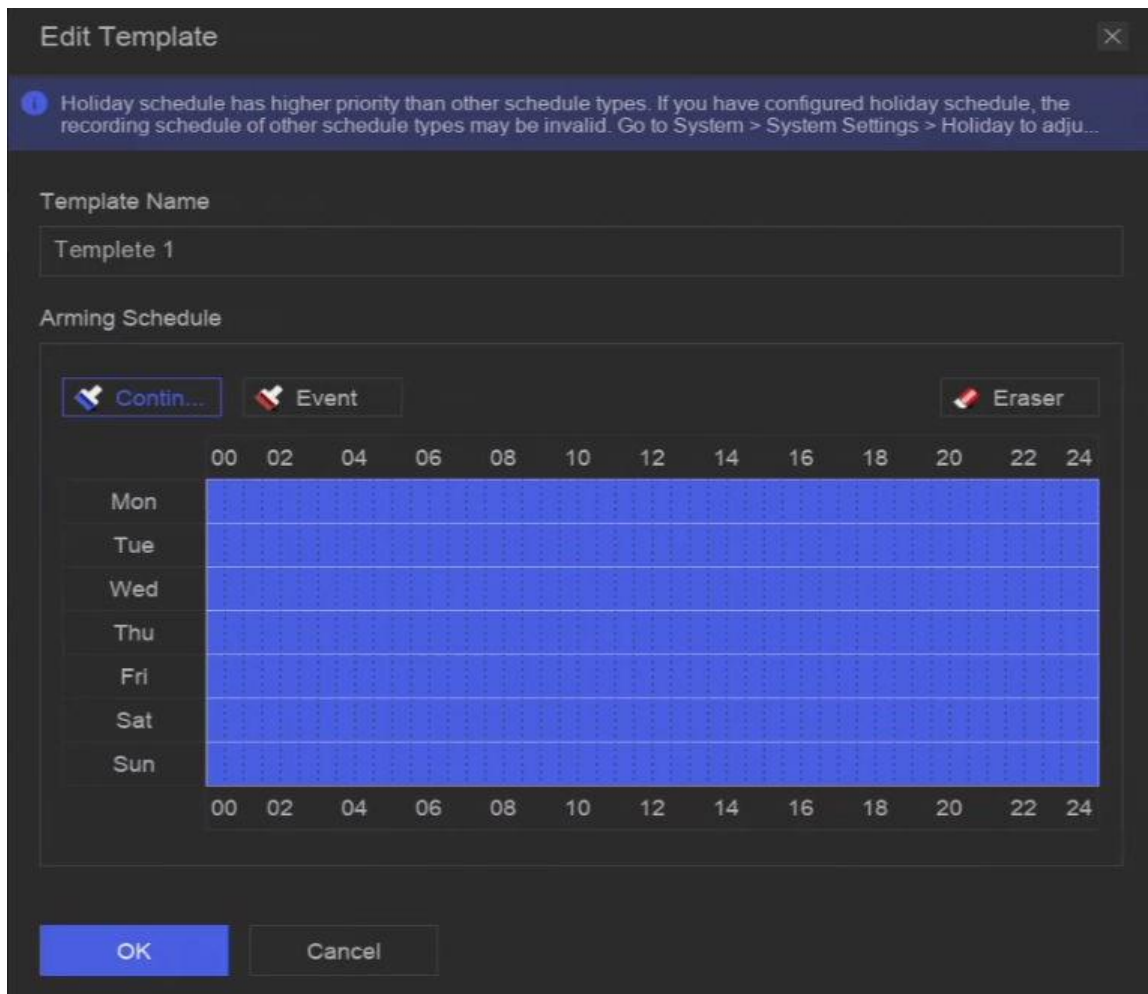



Рисунок 10-2 Изменение шаблона

- 3) Выберите тип записи. Например, **Event** («Событие»).
- 4) Перетащите курсор на временную шкалу, чтобы настроить расписание.

 **Примечание**

- После перемещения курсора на временную шкалу также можно нажать  **00:00-24:00**, чтобы установить указанное расписание.
- Можно нажать **Eraser** («Очистить»), чтобы очистить расписание.

 **Примечание**

Также можно нажать **Configure Template** («Настроить шаблон»), чтобы настроить шаблон в **System → Storage Management → Storage Schedule → Video Recording / Picture Capture / Audio Recording** («Система → Управление хранением → Расписание хранения → Видеозапись / Захват изображений / Аудиозапись»).

6. Нажмите **OK**.

10.2 Настройка расписания записи

Видеореги­стратор автоматически начнет/остановит запись в соответствии с настроенным расписанием записи.

Шаги

1. Перейдите в **System** → **Storage Management** → **Storage Schedule** → **Video Recording** («Система → Управление хранением → Расписание хранения → Видеозапись»).

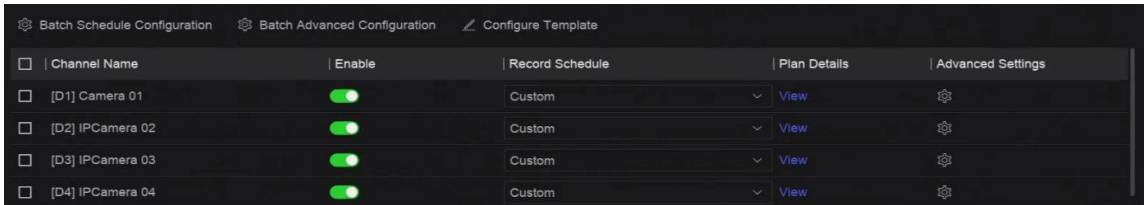


Рисунок 10-3 Конфигурация видеозаписи

2. Нажмите **Enable** («Включить») для камеры.
3. Выберите тип расписания.



Примечание

Если для **Record Schedule** («Расписание записи») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание записи, или переместить курсор на временную шкалу и нажать **00:00-24:00** ⌚, чтобы задать указанное расписание времени.

4. Нажмите **View** («Просмотр»), чтобы просмотреть расписание.

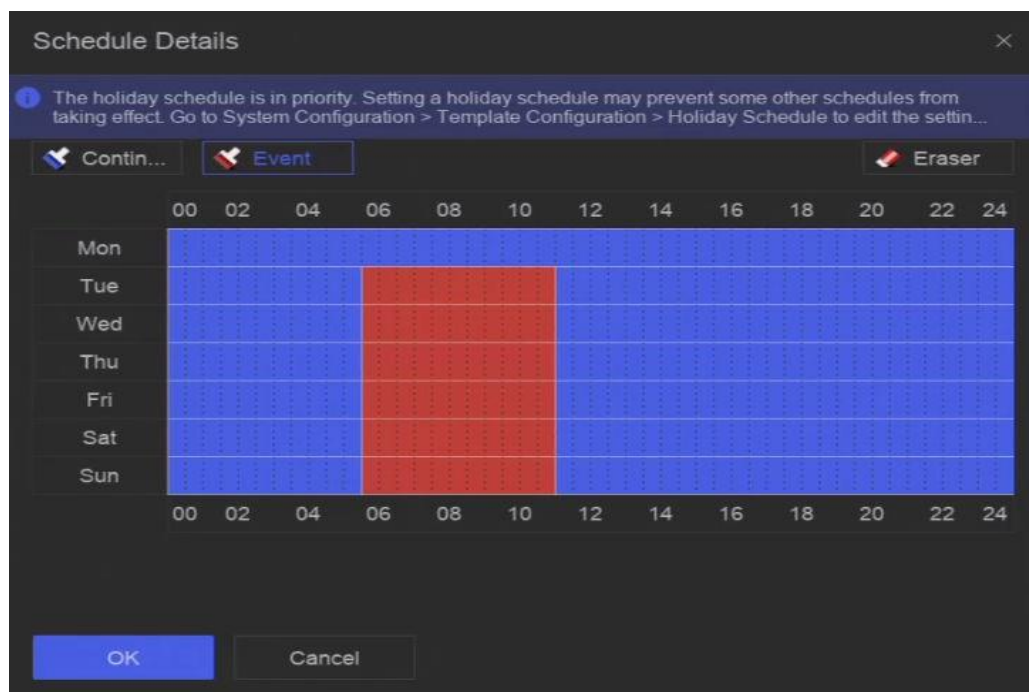


Рисунок 10-4 Расписание просмотра



5. **Опционально.** Нажмите  под **Advanced Settings** («Расширенные настройки»), чтобы задать другие дополнительные параметры.

Таблица 10-1 Описание дополнительных параметров

Параметр	Описание
Запись аудио	Включение / выключение функции аудиозаписи.  Примечание Канал должен поддерживать функцию аудио или к нему должно быть подключено аудиоустройство.
ANR	ANR (автоматическое пополнение сети) может автоматически включать SD-карту IP-камеры для сохранения видео без подключения к сети и синхронизировать данные после восстановления сети.
Предзапись	Время, установленное для записи до запланированного времени или события. Например, тревога запускает запись в 10:00. Если вы установите время предварительной записи как 5 секунд, камера начнет записывать в 9:59:55.
Постзапись	Время, установленное для записи после запланированного времени или события. Например, запись по тревоге заканчивается в 11:00. Если вы установите время постзаписи на 5 секунд, запись будет продолжаться до 11:00:05.
Тип потока	В режиме основного потока используется высокое разрешение. В режиме дополнительного потока можно записывать в течение длительного времени с тем же объемом памяти, но разрешение будет низким. В режиме двух потоков устройство будет записывать как основной поток, так и дополнительный поток.
Срок хранения видео / изображения	Срок хранения – это период, в течение которого файл хранится на HDD. По истечении крайнего срока файл будет удален. Если вы установите значение срока хранения на 0, файл не будет удален. Фактическое время хранения файла должно определяться емкостью жесткого диска.

6. **Опционально.** Выберите каналы в списке и используйте **Batch Schedule Configuration** («Конфигурация расписания в пакетном режиме») и **Batch Advanced Settings** («Расширенные настройки в пакетном режиме») для настройки в пакетном режиме.

7. Нажмите **Save** («Сохранить»).

10.3 Настройка расписания захвата изображений

Устройство будет автоматически захватывать изображения в режиме реального времени в соответствии с расписанием.

Шаги

1. Перейдите в **System → Storage Management → Storage Schedule → Picture Capture** («Система → Управление хранением → Расписание хранения → Захват изображения»).

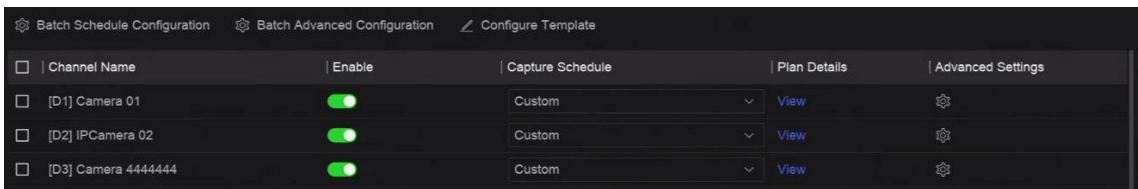


Рисунок 10-5 Настройка захвата изображения

2. Нажмите **Enable** («Включить») для камеры.
3. Выберите тип расписания.

Примечание

Если для **Capture Schedule** («Расписание захвата») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание захвата, или переместить курсор на временную шкалу и нажать **00:00-24:00** , чтобы задать указанное расписание времени.

4. Нажмите **View** («Просмотр»), чтобы просмотреть расписание.



Рисунок 10-6 Расписание просмотра

5. Нажмите в разделе **Advanced Settings** («Расширенные настройки»), чтобы задать дополнительные параметры изображения.

Таблица 10-2 Описание дополнительных параметров

Параметр	Описание
Задержка захвата	Длительность захвата изображения.
Разрешение	Настройте разрешение для захваченных изображений.
Качество изображения	Установите качество изображения: низкое, среднее или высокое. Высокое качество изображения требует больше места для хранения.
Интервал	Интервал времени захвата каждого изображения в режиме реального времени.

6. **Опционально.** Выберите каналы в списке и используйте **Batch Schedule Configuration** («Конфигурация расписания в пакетном режиме») и **Batch Advanced Settings** («Расширенные настройки в пакетном режиме») для настройки в пакетном режиме.

7. Нажмите **Save** («Сохранить»).

10.4 Конфигурация записи аудио


Устройство будет автоматически записывать аудио в соответствии с настроенным расписанием записи.

Шаги

1. Перейдите в **System** → **Storage Management** → **Storage Schedule** → **Audio Recording** («Система → Управление хранением → Расписание хранения → Аудиозапись»).
2. Нажмите **Enable** («Включить») для канала.
3. Выберите тип расписания.



Примечание

Если для **Record Schedule** («Расписание записи») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание записи, или переместить курсор на временную шкалу и нажать **00:00-24:00** , чтобы задать указанное расписание времени.

4. Нажмите **View** («Просмотр»), чтобы просмотреть расписание.
5. **Опционально.** Нажмите под **Advanced Settings** («Расширенные настройки»), чтобы задать другие дополнительные параметры.

Таблица 10-3 Описание дополнительных параметров

Параметр	Описание
Предзапись	Время, установленное для записи до запланированного времени или события. Например, тревога запускает запись в 10:00. Если вы установите время предварительной записи как 5 секунд, канал начнет записывать в 9:59:55.
Постзапись	Время, установленное для записи после запланированного времени или события. Например, запись по тревоге заканчивается в 11:00. Если вы установите время постзаписи на 5 секунд, запись будет продолжаться до 11:00:05.

6. Опционально. Выберите каналы в списке и используйте **Batch Schedule Configuration** («Конфигурация расписания в пакетном режиме») и **Batch Advanced Settings** («Расширенные настройки в пакетном режиме») для настройки в пакетном режиме.




7. Нажмите **Save** («Сохранить»).

Раздел 11 Просмотр в режиме реального времени

11.1 Настройка просмотра в режиме реального времени

В режиме реального времени отображается видеоизображение, получаемое с камеры.

Шаги

1. Перейдите к просмотру в режиме реального времени.
2. Нажмите  в правом нижнем углу.
3. Выберите тип разделения окна или нажмите **Custom** («Пользовательский»), чтобы настроить новый тип.
4. Переместите курсор на **Default View** («Вид по умолчанию») в разделе **View** («Вид»).
5. Нажмите  в правой части **View** («Вид»).
6. Следуйте инструкциям по настройке интерфейса вывода изображения в режиме реального времени. Помимо двух способов, указанных в пользовательском интерфейсе, можно перемещать канал из одного окна в другое.
7. Нажмите .

11.2 Графический интерфейс

Можно просматривать изображение в режиме реального времени, воспроизводить звук в режиме реального времени, захватывать изображения, выполнять мгновенное воспроизведение и т. д.



Рисунок 11-1 Просмотр в режиме реального времени (тип 1)

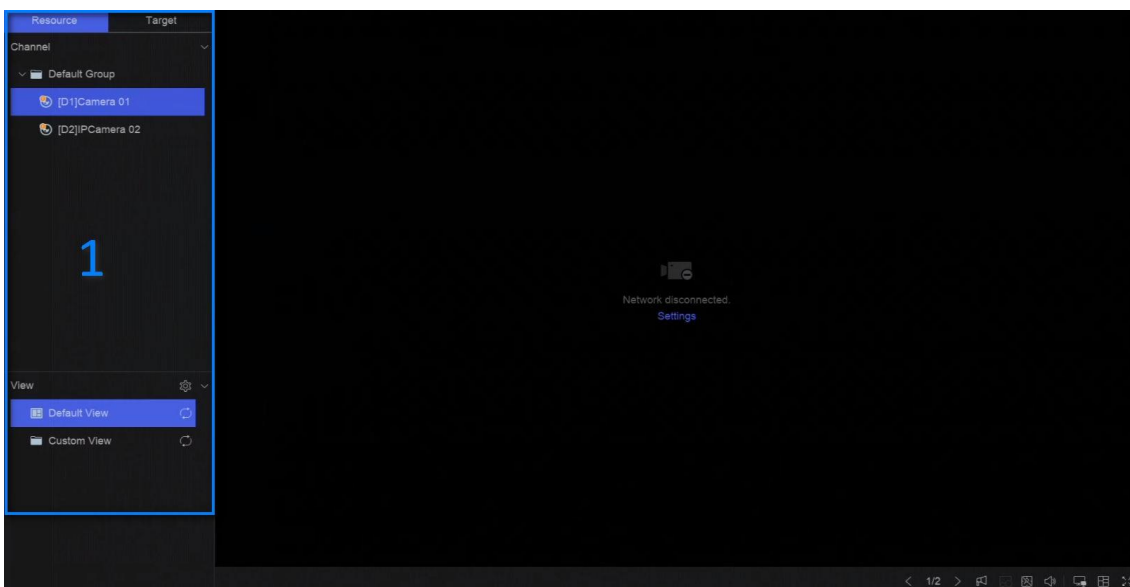






Рисунок 11-2 Просмотр в режиме реального времени (тип 2)

Таблица 11-1 Описание интерфейсов

№	Описание
1	Список каналов, панель управления PTZ и список обнаружения целей. Если выбрать канал из списка каналов, устройство перенаправит в соответствующее окно. Если нажать Target («Цель»), можно просмотреть результаты обнаружения цели в реальном времени в списке и нажать  для настройки соответствующих параметров.
2	Меню быстрого доступа правой кнопкой мыши. Появляется после нажатия правой кнопкой мыши по области изображения.
3	Панель инструментов канала. <ul style="list-style-type: none"> • Нажмите , чтобы добавить тег к каналу. После добавления перейдите в  → Backup → By Tag («Резервное копирование → По тегам»), чтобы выполнить поиск видео по тегам. • Можно выбрать  → Show VCA Info («Показать информацию VCA») для отображения рамок правил.
4	Панель инструментов просмотра в режиме реального времени. Выполняются следующие функции: Voice Broadcast («Голосовая трансляция»), Display VCA Info («Отображение информации VCA») и Switch Output («Переключение выхода»).

 **Примечание**







- Можно прокручивать мышью вверх / вниз, чтобы перейти к предыдущему / следующему экрану.
- Если возникнет исключение отображения изображения канала, в соответствующем окне появится сообщение об ошибке, и можно напрямую нажать на текст (синего цвета), чтобы изменить настройки устройства.

11.3 Управление PTZ


PTZ – это аббревиатура для **Pan / Tilt / Zoom** («Поворот, наклон, масштабирование»). После добавления PTZ-камеры на устройство, устройству будет разрешено поворачивать влево и вправо, наклонять вверх и вниз, а также увеличивать и уменьшать масштаб.

Выберите PTZ-камеру и разверните меню управления PTZ в нижнем левом углу.

Таблица 11-2 PTZ-управление

Задача	Описание	Операция
Предустановка	Предустановки записывают положение PTZ-камеры, состояние масштабирования, фокуса, диафрагмы и т. д. Можно вызвать предустановку, чтобы быстро переместить камеру в предварительно определенное положение.	Настройка предустановки 1. Выберите предустановку. 2. Для настройки изображения используйте кнопки со стрелками. 3. Нажмите  .
		Вызов предустановки. Нажмите  .
Патруль	Можно настроить патрулирование так, чтобы PTZ-камера перемещалась в ключевые точки и оставалась там в течение установленного времени, прежде чем перейти к следующей ключевой точке. Ключевая точка соответствует предустановке.	Настройка патруля 1. Выберите патруль. 2. Нажмите  .
		3. Добавьте предустановки для патруля. 4. Нажмите ОК . Вызов патруля. Нажмите  .
Шаблон	Для записи движения PTZ-камеры можно настроить шаблон. Вызовите шаблон, чтобы PTZ-камера двигалась в соответствии с заранее определенным маршрутом.	Настройка шаблона 1. Нажмите  .
		2. Используйте кнопки со стрелками для настройки изображения, устройство запишет движение. 3. Остановите запись. Вызов шаблона. Нажмите  .

 **Примечание**

Если нельзя использовать панель PTZ, нажмите , чтобы проверить настройки.

Раздел 12 Воспроизведение

12.1 Графический интерфейс

Можно воспроизводить видео- или аудио­файлы.

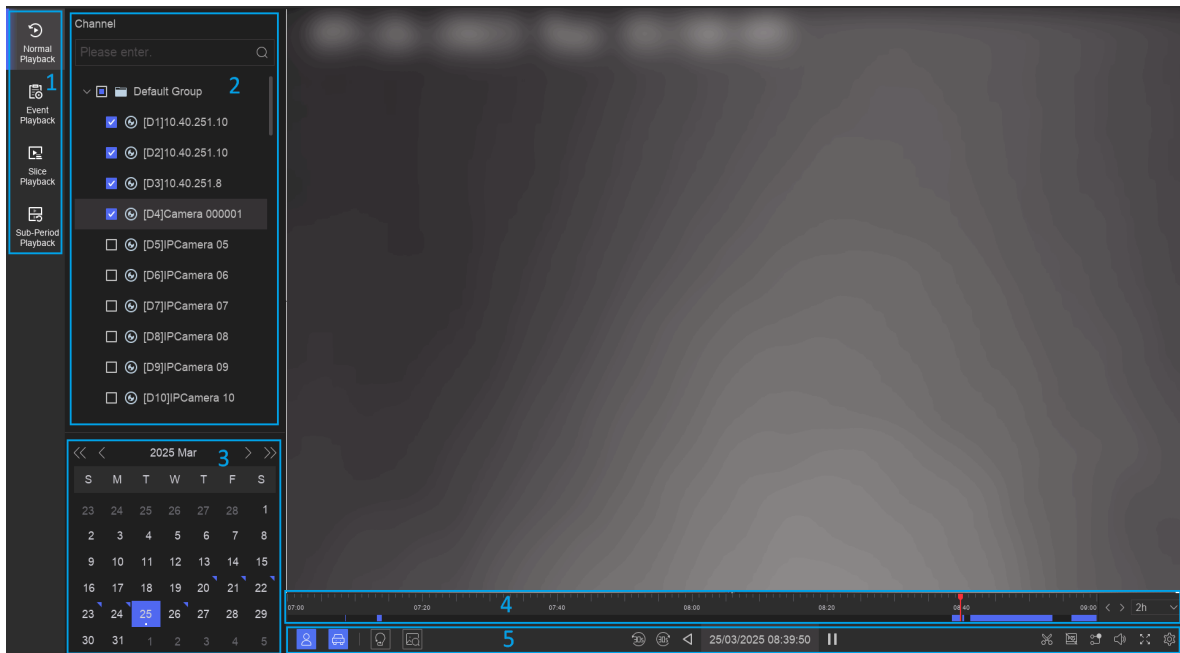









Рисунок 12-1 Воспроизведение

Таблица 12-1 Описание интерфейсов


№	Описание
1	Область выбора типа воспроизведения.
2	Список каналов.
3	Календарь для выбора времени.
4	Временная шкала воспроизведения. <ul style="list-style-type: none"> • Поместите курсор на шкалу времени, перетащите шкалу времени, чтобы установить определенное время. • Период, отмеченный синей полосой, содержит видео. Красная полоса указывает, что видео в периоде содержит событие. • Прокрутите вверх / вниз, чтобы уменьшить / увеличить шкалу времени.

№	Описание
5	<p>Панель инструментов воспроизведения.</p> <ul style="list-style-type: none"> Нажмите  (Интеллектуальный поиск), затем следуйте всплывающим подсказкам, чтобы нарисовать правило события и найти видео, которые могут вызвать соответствующее правило события. Аналогичные действия выполняются и с функцией Dual-VCA. Нажмите , чтобы выполнить функцию AcuSearch. Подробная информация представлена в разделе <u>AcuSearch</u>. Нажмите  / , чтобы показать видео с целями «Человек» / «ТС». <p> Примечание</p> <p>Чтобы использовать эту функцию, убедитесь, что для определенных типов событий в поле Detection Target («Цель обнаружения») выбрано Human («Человек») или Vehicle («ТС»).</p> <ul style="list-style-type: none"> Нажмите , выберите каналы и установите время начала и окончания воспроизведения видео в выбранных каналах в течение определенного периода времени. Нажмите , чтобы задать стратегию воспроизведения обычного и интеллектуального видео (видео с интеллектуальными данными).

12.2 Обычный режим воспроизведения

Воспроизведение видео для канала. На некоторых устройствах синхронное воспроизведение может быть разрешено для нескольких каналов.

Шаги

1. Перейдите **Playback** («Воспроизведение») → .
2. Выберите канал в списке слева.

Примечание


Групповое воспроизведение: выберите группу в списке, и каналы в группе можно будет воспроизвести.


3. Выберите дату в календаре.



Примечание


Синий треугольник в углу календарной даты указывает на наличие доступных видео.


4. **Опционально.** Выполняйте другие операции.

Захват Нажмите , чтобы выполнить захват изображения во время воспроизведения.


Цифровой зум Нажмите , чтобы увеличить определенную часть видеоизображения.

Нажмите , чтобы добавить тег к каналу. После добавления перейдите в  → **Backup** → **By Tag** («Резервное копирование → По тегам»), чтобы выполнить поиск видео по тегам.

Нажмите , чтобы заблокировать видео. После блокировки видео не будет перезаписано.

После блокировки перейдите в  → **Backup** → **By Tag** («Резервное копирование → По тегам»), чтобы выполнить поиск видео по блокировке.

Dual-VCA


Выберите  → **Dual-VCA** для поиска видео, которые могут запустить соответствующее правило события. Подробная информация о каждом типе события представлена в шагах настройки событий.




Примечание

Чтобы использовать эту функцию, перейдите в **Configuration** → **Device Access** → **Device Configuration** → **Device Parameter** → **Display Info. on Stream** («Конфигурация → Доступ к устройству → Конфигурация устройства → Параметры устройства → Отображение информации на потоке») и включите Dual-VCA через веб-интерфейс. Перейдите в **System** → **Storage Management** → **Advanced Settings** («Система → Управление хранением → Дополнительные настройки»), чтобы включить **Save Camera VCA Data** («Сохранение данных VCA с камеры») через локальный графический интерфейс.

Показать информацию VCA

Можно выбрать  → **Show VCA Info** («Показать информацию VCA») для отображения рамок правил.

Отключить защиту конфиденциальных данных

Если защита конфиденциальности включена, области на изображении могут быть скрыты маскированием. Можно выбрать  → **Display Privacy Protection** («Отображение защиты конфиденциальных данных»), чтобы отобразить исходное видео (без маскирования), если также включено разрешение на хранение в разделе защиты конфиденциальных данных. Подробная информация о функции защиты конфиденциальных данных представлена в разделе **Конфигурация защиты конфиденциальных данных**.


12.3 Воспроизведение по событию

Когда вы выбираете режим воспроизведения событий, система будет анализировать и отмечать видео, которые содержат информацию об обнаружении движения, пересечении линии или обнаружении вторжения.

Перед началом

- Убедитесь, что в камере включена функция Dual-VCA. Вы можете включить эту функцию через веб-интерфейс камеры в **Configuration → Video/Audio → Display Info. on Stream** («Настройки → Видео / Аудио → Отображение информации в потоке»).
- Убедитесь, что на видеореги­страторе включена функция **Save Camera VCA Data** («Сохранение данных VCA с камеры») в разделе **Storage management → Advanced Settings** («Управление хранением → Дополнительные настройки»).


Шаги

1. Выберите **Playback** («Воспроизведение») → .
2. Выберите дату в календаре.




Примечание

Синий треугольник в углу календарной даты указывает на наличие доступных видео.

3. Нажмите  → **Dual-VCA** в правом нижнем углу изображения воспроизведения, чтобы выбрать тип события. Подробная информация о каждом типе события представлена в шагах настройки событий.
4. Нажмите **Search** («Поиск»).

Видео, отвечающие требованиям правила обнаружения, будут отмечены красным.

5. Нажмите , чтобы задать стратегию воспроизведения обычного и интеллектуального видео (видео с интеллектуальными данными).




Примечание

Если функция **Dual-VCA** не используется, красные сегменты на индикаторе выполнения означают, что интеллектуальные видео созданы на основе исходного события.


12.4 Воспроизведение фрагмента

Разделите видео на фрагменты и воспроизведите их.

Шаги

1. Перейдите **Playback** («Воспроизведение») → .
2. Выберите камеру из списка камер.
3. Выберите дату в календаре.
4. Нажмите **Search** («Поиск»).


Извлеченное видео будет разделено на одночасовые фрагменты для воспроизведения.

5. **Опционально.** Выберите часовой фрагмент и нажмите , чтобы разделить его на минутные фрагменты для воспроизведения.

12.5 Воспроизведение дополнительных периодов

Видео файлы можно воспроизводить на экране одновременно в нескольких дополнительных периодах.

Шаги

1. Перейдите **Playback** («Воспроизведение») → .
2. Выберите камеру.
3. Установите **Start Time** («Время начала») и **End Time** («Время окончания»).
4. Нажмите **Search** («Поиск»).

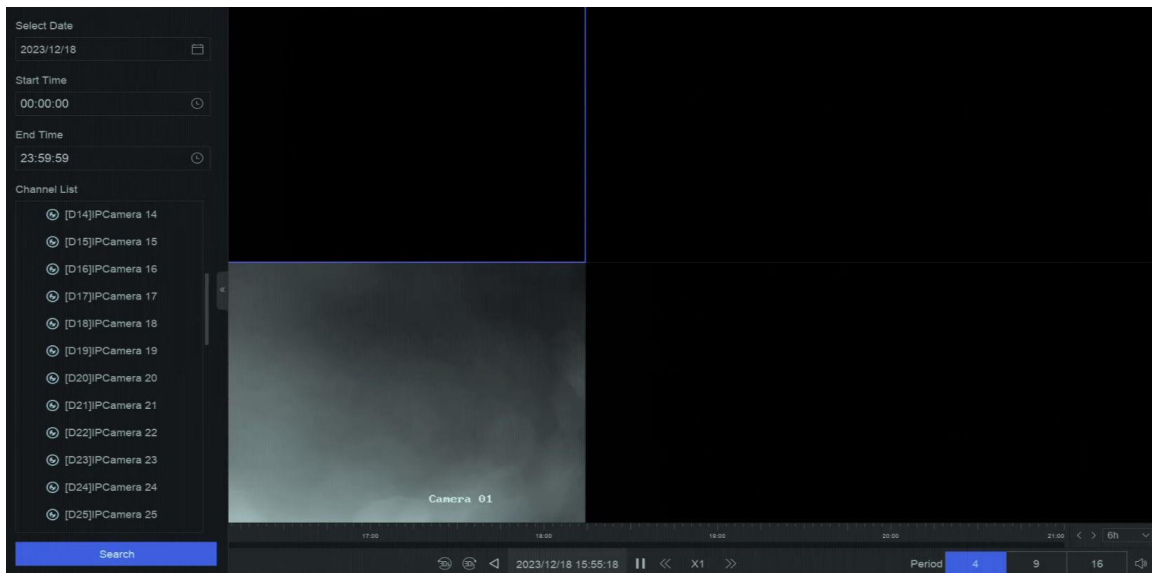


Рисунок 12-2 Воспроизведение дополнительных периодов

5. Выберите период в правом нижнем углу, например, 4.

Примечание

В соответствии с фактическим количеством разделенных экранов, видеофайлы на выбранную дату могут быть разделены на средние сегменты для воспроизведения. Например, при наличии видеофайлов между 16:00 и 22:00 и при режиме отображения с 6 экранами, видеофайлы могут воспроизводиться в течение 1 часа одновременно на каждом экране.

Раздел 13 Центр событий

13.1 Настройки событий

13.1.1 Базовое / общее событие

Шаги


1. Перейдите **Event Center** («Центр событий») →  → **Event Configuration** → **Basic Event / Generic Event** («Конфигурация событий → Базовое событие / общее событие»).
2. Выберите канал.
3. Выберите тип события.
4. Нажмите **Enable** («Включить»).
5. Нажмите **Rule Settings** («Настройки правила»), чтобы задать правило.

Таблица 13-1 Обычное событие


Имя события	Описание события	Настройка правила
Обнаружение движения	Функция обнаруживает движущиеся объекты в области мониторинга.	Используйте панель инструментов в верхней части изображения, чтобы нарисовать область обнаружения. <ul style="list-style-type: none"> • ИИ в NVR. Событие обнаружения движения будет проанализировано NVR. Устройство может анализировать видео с целями «Человек» / «ТС». Только цель выбранного типа («Человек» / «ТС») будет вызывать тревогу, что позволяет отфильтровать ложные тревоги. • ИИ с помощью камеры. Событие обнаружения движения будет проанализировано камерой. • Цели: можно выбрать цель Human («Человек») или Vehicle («ТС»). <p>Кроме ложных тревог, только выбранная цель может вызвать тревогу.</p>

Имя события	Описание события	Настройка правила
Детекция саботажа видео	Данная функция запускает тревогу в случае закрытия объектива камеры и вызывает соответствующие действия по тревоге.	Используйте панель инструментов в верхней части изображения, чтобы нарисовать область обнаружения.
Детекция потери видео	Данная функция позволяет обнаруживать потерю видеосигнала в канале и выдает соответствующую тревогу.	
Детекция звуковых событий	Функция детекции звуковых событий позволяет обнаружить звуковые отклонения в сцене, такие как резкий рост / спад интенсивности звука.	
Обнаружение расфокусировки	Обнаружение размытого изображения, вызванного расфокусировкой объектива.	
Обнаружение изменения сцены	Данная функция позволяет обнаружить изменение среды наблюдения, на которую влияют внешние факторы, такие как преднамеренное вращение камеры.	

6. Нажмите **Arming Schedule** («Расписание постановки на охрану»), чтобы выбрать тип расписания постановки на охрану.




Примечание

Если для **Arming Schedule** («Расписание постановки на охрану») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание постановки на охрану, или переместить курсор на временную шкалу и нажать **00:00-24:00** , чтобы задать указанное расписание времени.

7. Нажмите **Linkage Method** («Метод привязки») для настройки методов привязки.

Таблица 13-2 Описание метода привязки

Метод привязки	Описание
Уведомление центра мониторинга	Видеореги­стратор может направить исключение или тревогу на удаленный тревожный хост, когда происходит событие. Тревожный хост относится к ПК, на котором установлено клиентское программное обеспечение (например, iVMS-4200, iVMS-5200).
Всплывающее окно тревоги	При срабатывании тревоги на локальном мониторе отображается всплывающее окно тревоги.
Бипер	При обнаружении тревоги бипер издаст звуковой сигнал.
Отправка Email	Видеореги­стратор может отправлять электронное письмо с информацией о тревоге пользователю или пользователям.
Тревожный выход	Срабатывание тревожного выхода может быть вызвано обнаружением движения, детектором саботажа, детекцией лиц, обнаружением пересечения линии и любыми другими событиями.
Запись	<p>При обнаружении тревоги выбранный канал будет записывать видео.</p> <p> Примечание</p> <p>Для канала должно быть включено расписание видеозаписи, в противном случае данная привязка будет недействительной. Перейдите в System → Storage Management → Storage Schedule → Video Recording («Система → Управление хранением → Расписание хранения → Видеозапись») для настройки расписания записи видео.</p>

8. Нажмите **Save** («Сохранить»).

13.1.2 Защита периметра

События защиты периметра включают обнаружение пересечения линии, обнаружение вторжения, обнаружение входа в область и обнаружение выхода из области.


Настройка обнаружения пересечения линии

Функция обнаружения пересечения линии обнаруживает людей, транспортные средства или другие объекты, которые пересекают заранее заданную виртуальную линию. Направление пересечения линии могут быть различными: в обе стороны, слева направо или справа налево.

Шаги

Примечание

Часть следующих шагов доступна только для определенных моделей NVR или камер.

1. Перейдите **Event Center** («Центр событий») →  → **Event Configuration** → **Perimeter Protection** («Конфигурация событий → Защита периметра»).
2. Выберите камеру.
3. **Опционально.** Включите **Secondary Analysis** («Повторный анализ»). Соответствующий процессор повторно проанализирует это событие, чтобы уменьшить количество ложных тревог.

 **Примечание**

Алгоритм **Secondary Analysis for Perimeter Protection** («Повторный анализ для защиты периметра») должен быть запущен по крайней мере на одном устройстве. Справа нажмите **Allocate Engine** («Назначить процессор») для быстрого назначения или перейдите в **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** («Система → Интеллектуальные настройки → Конфигурация алгоритма → Управление алгоритмом»), чтобы включить **Secondary Analysis for Perimeter Protection** («Повторный анализ для защиты периметра»).

-
4. **Опционально.** Включите **AI by NVR** («ИИ с помощью NVR»). Устройство будет анализировать видео, а камеры только передавать видеопоток.

 **Примечание**

Алгоритм **Perimeter Protection** («Защита периметра») должен быть запущен по крайней мере на одном устройстве. Справа нажмите **Allocate Engine** («Назначить процессор») для быстрого назначения или перейдите в **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** («Система → Интеллектуальные настройки → Конфигурация алгоритма → Управление алгоритмом»), чтобы включить **Perimeter Protection** («Защита периметра»).

-
5. Выберите **Line Crossing** («Пересечение линии»).
 6. Нажмите **Enable** («Включить»).

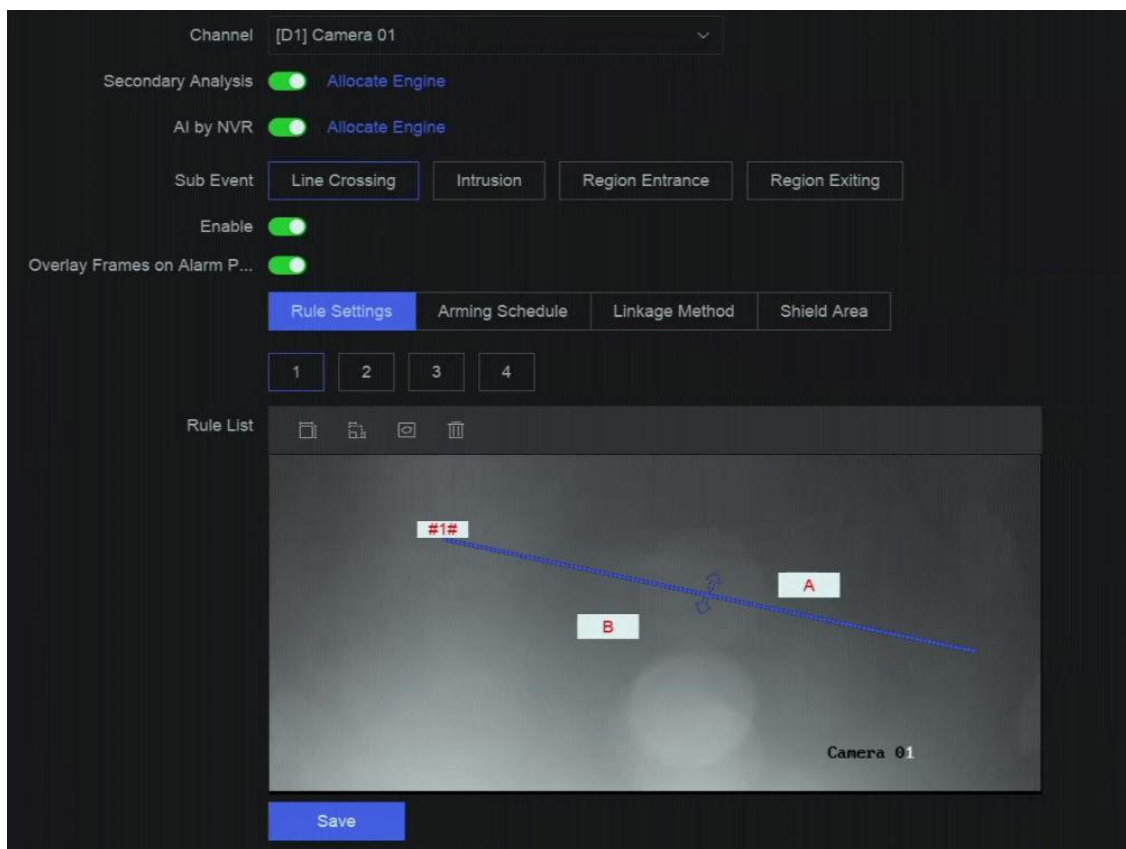



Рисунок 13-1 Обнаружение пересечения линии

7. Нажмите **Rule Settings** («Настройки правила»), чтобы настроить правила обнаружения.

1) Выберите номер правила. Например, выберите **1**.

2) Нажмите на  и дважды щелкните по изображению, чтобы нарисовать начальную и конечную точку линии обнаружения.

3) Настройте **Direction** («Направление»), **Sensitivity** («Чувствительность»), **Detection Target** («Обнаружение цели») и **Target Confidence** («Достоверность обнаружения цели»). **A->B**

Стрелка отображается только на стороне B. Тревога срабатывает при пересечении объектом заданной линии в обоих направлениях.

A->B

Обнаружение объекта при движении из стороны A на сторону B.

B->A

Обнаружение объекта при движении из стороны B на сторону A.

Чувствительность



Чем выше значение, тем больше вероятность срабатывания тревоги обнаружения движения.

Обнаружение цели

Выбрано **Target Detection** («Обнаружение цели») на значение **Human** («Человек») или **Vehicle** («Транспортное средство»), чтобы отключить тревогу при обнаружении человека или транспортного средства. Функция **Detection Target** («Обнаружение цели») представлена не во всех моделях.

Достоверность обнаружения цели

Используется для обозначения уровня достоверности или надежности обнаружения событий пересечения линии. Установка более высоких уровней достоверности гарантирует, что события будут запускаться только при наличии высокой надежности обнаружения, что снижает количество ложных тревог.

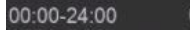

4) **Опционально.** Нажмите  / , чтобы нарисовать **Max. Size** («Макс. размер») и **Min. Size** («Мин. размер»). Тревогу могут запустить только те цели, которые соответствуют требованиям по размеру.

5) **Опционально.** Повторите шаги выше, чтобы нарисовать больше правил. Поддерживается до 4 правил.

8. Нажмите **Arming Schedule** («Расписание постановки на охрану»), чтобы выбрать тип расписания постановки на охрану.




Примечание

Если для **Arming Schedule** («Расписание постановки на охрану») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание постановки на охрану, или переместить курсор на временную шкалу и нажать  , чтобы задать указанное расписание времени.

9. Нажмите **Linkage Method** («Метод привязки») для настройки методов привязки.

Таблица 13-3 Описание метода привязки

Метод привязки	Описание
Уведомление центра мониторинга	Видеореги­стратор может направить исключение или тревогу на удаленный тревожный хост, когда происходит событие. Тревожный хост относится к ПК, на котором установлено клиентское программное обеспечение (например, iVMS-4200, iVMS-5200).
Всплывающее окно тревоги	При срабатывании тревоги на локальном мониторе отображается всплывающее окно тревоги.
Бипер	При обнаружении тревоги бипер издаст звуковой сигнал.
Отправка Email	Видеореги­стратор может отправлять электронное письмо с информацией о тревоге пользователю или пользователям.
Тревожный выход	Срабатывание тревожного выхода может быть вызвано обнаружением движения, детектором саботажа, детекцией лиц, обнаружением пересечения линии и любыми другими событиями.

Метод привязки	Описание
Запись	<p>При обнаружении тревоги выбранный канал будет записывать видео.</p> <p> Примечание</p> <p>Для канала должно быть включено расписание видеозаписи, в противном случае данная привязка будет недействительной. Перейдите в System → Storage Management → Storage Schedule → Video Recording («Система → Управление хранением → Расписание хранения → Видеозапись») для настройки расписания записи видео.</p>

10. Опционально. Настройте параметры **Shield Area** («Защищенная область»), если установлен флажок **AI by NVR** («ИИ с помощью NVR»). После установки зоны защиты устройство не будет анализировать поведение цели в этой зоне, поэтому события защиты периметра не будут срабатывать в пределах этой зоны.

11. Нажмите **Save** («Сохранить»).

Дальнейшие шаги

Перейдите в **Live View** («Просмотр в режиме реального времени») и нажмите **Target** («Цель»), чтобы просмотреть тревоги в режиме реального времени.


Настройка обнаружения вторжения

Функция обнаружения вторжения обнаруживает людей, транспортные средства или другие объекты, которые оказываются в заранее заданной области. При срабатывании сигнала тревоги могут быть предприняты определенные действия.

Шаги

Примечание

Часть следующих шагов доступна только для определенных моделей NVR или камер.

1. Перейдите **Event Center** («Центр событий») →  → **Event Configuration → Perimeter Protection** («Конфигурация событий → Защита периметра»).
2. Выберите камеру.
3. **Опционально.** Включите **Secondary Analysis** («Повторный анализ»). Соответствующий процессор повторно проанализирует это событие, чтобы уменьшить количество ложных тревог.

Примечание

Алгоритм **Secondary Analysis for Perimeter Protection** («Повторный анализ для защиты периметра») должен быть запущен по крайней мере на одном устройстве. Справа нажмите **Allocate Engine** («Назначить процессор») для быстрого назначения или перейдите в **System → Smart Settings → Algorithm Configuration → Algorithm Management** («Система →

Интеллектуальные настройки → Конфигурация алгоритма → Управление алгоритмом», чтобы включить **Secondary Analysis for Perimeter Protection** («Повторный анализ для защиты периметра»).

4. Опционально. Включите **AI by NVR** («ИИ с помощью NVR»). Устройство будет анализировать видео, а камеры только передавать видеопоток.

 **Примечание**

Алгоритм **Perimeter Protection** («Защита периметра») должен быть запущен по крайней мере на одном устройстве. Справа нажмите **Allocate Engine** («Назначить процессор») для быстрого назначения или перейдите в **System → Smart Settings → Algorithm Configuration → Algorithm Management** («Система → Интеллектуальные настройки → Конфигурация алгоритма → Управление алгоритмом»), чтобы включить **Perimeter Protection** («Защита периметра»).

5. Выберите **Intrusion** («Вторжение»).

6. Нажмите **Enable** («Включить»).

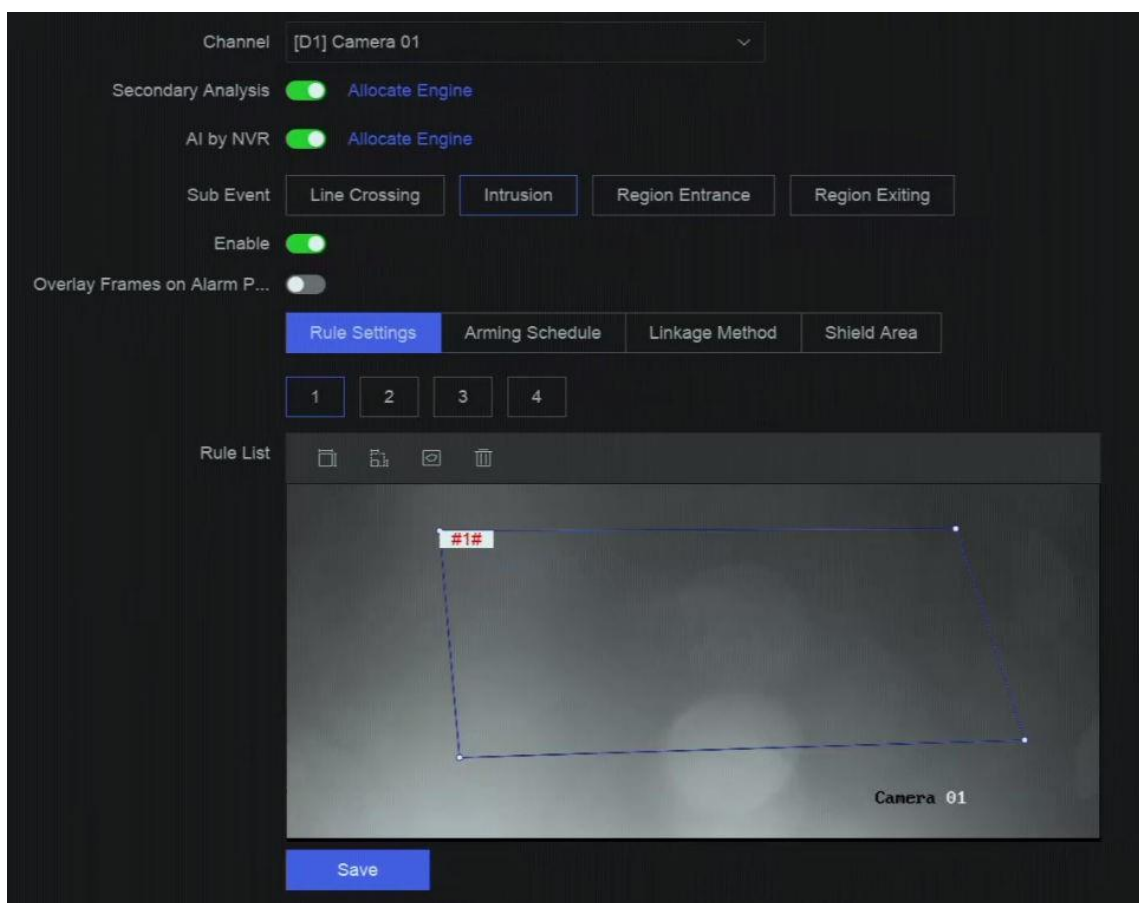



Рисунок 13-2 Обнаружение вторжения

7. Нажмите **Rule Settings** («Настройки правила»), чтобы настроить правила обнаружения.

1) Выберите номер правила. Например, выберите **1**.

2) Нажмите на  и щелкните по изображению 4 раза, чтобы нарисовать каждую точку четырехугольной или десятиугольной области.

3) Настройте **Time Threshold** («Порог времени»), **Sensitivity** («Чувствительность»), **Detection Target** («Обнаружение цели») и **Target Confidence** («Достоверность обнаружения цели»).

Порог времени

Время, когда объект находится в пределах области. Когда продолжительность нахождения объекта в определенной области обнаружения превышает пороговое значение, устройство выдает тревогу.

Чувствительность



Чем выше значение, тем больше вероятность срабатывания тревоги обнаружения движения.

Обнаружение цели

Выбрано **Target Detection** («Обнаружение цели») на значение **Human** («Человек») или **Vehicle** («Транспортное средство»), чтобы отключить тревогу при обнаружении человека или транспортного средства. Функция **Detection Target** («Обнаружение цели») представлена не во всех моделях.

Достоверность обнаружения цели

Используется для обозначения уровня достоверности или надежности обнаружения вторжений. Установка более высоких уровней достоверности гарантирует, что события будут запускаться только при наличии высокой надежности обнаружения, что снижает количество ложных тревог.



4) **Опционально.** Нажмите  / , чтобы нарисовать **Max. Size** («Макс. размер») и **Min. Size** («Мин. размер»). Тревогу могут запустить только те цели, которые соответствуют требованиям по размеру.

5) **Опционально.** Повторите шаги выше, чтобы нарисовать больше правил. Поддерживается до 4 правил.

8. Нажмите **Arming Schedule** («Расписание постановки на охрану»), чтобы выбрать тип расписания постановки на охрану.




Примечание

Если для **Arming Schedule** («Расписание постановки на охрану») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание постановки на охрану, или переместить курсор на временную шкалу и нажать  , чтобы задать указанное расписание времени.

9. Нажмите **Linkage Method** («Метод привязки») для настройки методов привязки.

Таблица 13-4 Описание метода привязки

Метод привязки	Описание
Уведомление центра мониторинга	Видеореги­стратор может направить исключение или тревогу на удаленный тревожный хост, когда происходит событие. Тревожный хост относится к ПК, на котором установлено клиентское программное обеспечение (например, iVMS-4200, iVMS-5200).
Всплывающее окно тревоги	При срабатывании тревоги на локальном мониторе отображается всплывающее окно тревоги.
Бипер	При обнаружении тревоги бипер издаст звуковой сигнал.
Отправка Email	Видеореги­стратор может отправлять электронное письмо с информацией о тревоге пользователю или пользователям.
Тревожный выход	Срабатывание тревожного выхода может быть вызвано обнаружением движения, детектором саботажа, детекцией лиц, обнаружением пересечения линии и любыми другими событиями.
Запись	<p>При обнаружении тревоги выбранный канал будет записывать видео.</p> <p> Примечание</p> <p>Для канала должно быть включено расписание видеозаписи, в противном случае данная привязка будет недействительной. Перейдите в System → Storage Management → Storage Schedule → Video Recording («Система → Управление хранением → Расписание хранения → Видеозапись») для настройки расписания записи видео.</p>

10. Опционально. Настройте параметры **Shield Area** («Защищенная область»), если установлен флажок **AI by NVR** («ИИ с помощью NVR»). После установки зоны защиты устройство не будет анализировать поведение цели в этой зоне, поэтому события защиты периметра не будут срабатывать в пределах этой зоны.

11. Нажмите **Save** («Сохранить»).

Дальнейшие шаги

Перейдите в **Live View** («Просмотр в режиме реального времени») и нажмите **Target** («Цель»), чтобы просмотреть тревоги в режиме реального времени.


Настройка входа в область

Функция обнаружения входа в область обнаруживает объекты, которые входят в заранее заданную виртуальную область.

Шаги

Примечание

Часть следующих шагов доступна только для определенных моделей NVR или камер.

1. Перейдите **Event Center** («Центр событий») →  → **Event Configuration** → **Perimeter Protection** («Конфигурация событий → Защита периметра»).
 2. Выберите камеру.
 3. **Опционально.** Включите **Secondary Analysis** («Повторный анализ»). Соответствующий процессор повторно проанализирует это событие, чтобы уменьшить количество ложных тревог.
-

Примечание

Алгоритм **Secondary Analysis for Perimeter Protection** («Повторный анализ для защиты периметра») должен быть запущен по крайней мере на одном устройстве. Справа нажмите **Allocate Engine** («Назначить процессор») для быстрого назначения или перейдите в **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** («Система → Интеллектуальные настройки → Конфигурация алгоритма → Управление алгоритмом»), чтобы включить **Secondary Analysis for Perimeter Protection** («Повторный анализ для защиты периметра»).

4. **Опционально.** Включите **AI by NVR** («ИИ с помощью NVR»). Устройство будет анализировать видео, а камеры только передавать видеопоток.
-

Примечание

Алгоритм **Perimeter Protection** («Защита периметра») должен быть запущен по крайней мере на одном устройстве. Справа нажмите **Allocate Engine** («Назначить процессор») для быстрого назначения или перейдите в **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** («Система → Интеллектуальные настройки → Конфигурация алгоритма → Управление алгоритмом»), чтобы включить **Perimeter Protection** («Защита периметра»).

5. Выберите **Region Entrance** («Вход в область»).
6. Нажмите **Enable** («Включить»).

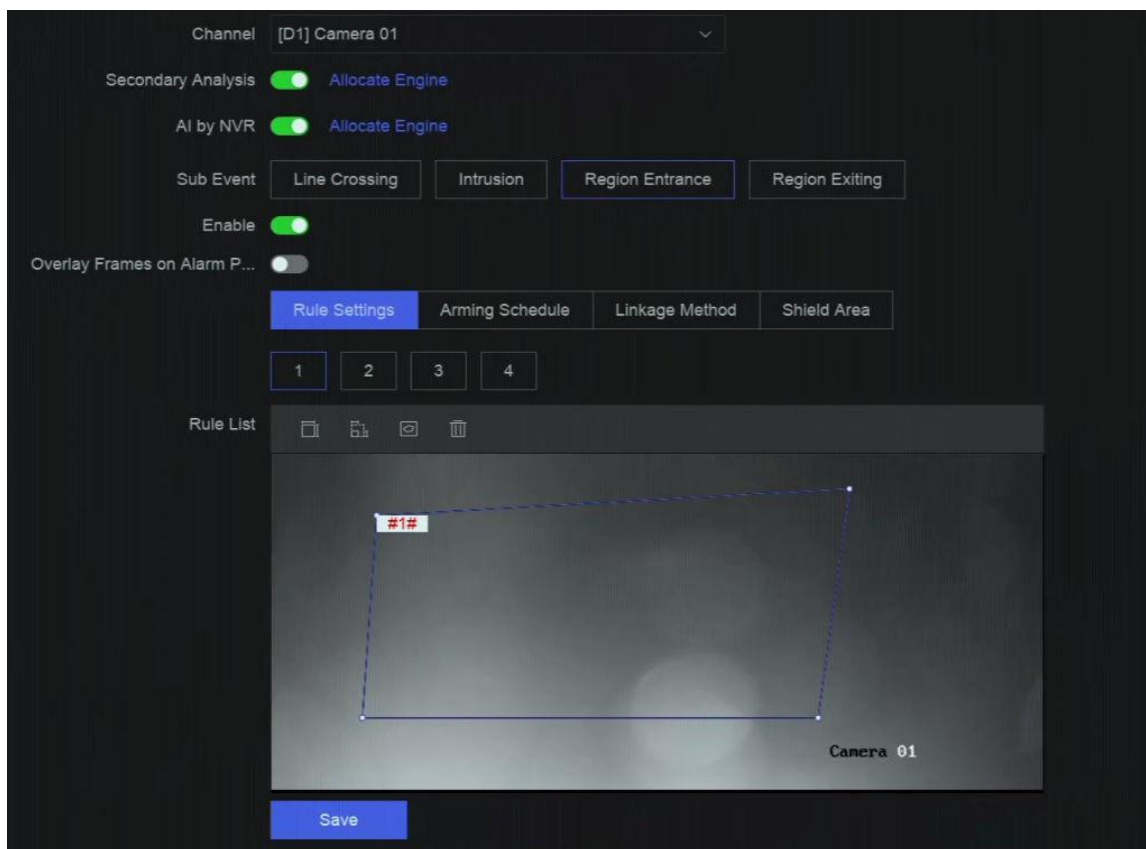



Рисунок 13-3 Обнаружения входа в область

7. Нажмите **Rule Settings** («Настройки правила»), чтобы настроить правила обнаружения.

1) Выберите номер правила. Например, выберите **1**.

2) Нажмите на  и щелкните по изображению 4 раза, чтобы нарисовать каждую точку четырехугольной или десятиугольной области.

3) Настройте **Sensitivity** («Чувствительность»), **Detection Target** («Обнаружение цели») и **Target Confidence** («Достоверность обнаружения цели»).

Чувствительность

Чем выше значение, тем больше вероятность срабатывания тревоги обнаружения движения.

Обнаружение цели

Выбрано **Target Detection** («Обнаружение цели») на значение **Human** («Человек») или **Vehicle** («Транспортное средство»), чтобы отключить тревогу при обнаружении человека или транспортного средства. Функция **Detection Target** («Обнаружение цели») представлена не во всех моделях.


Достоверность обнаружения цели

Используется для обозначения уровня достоверности или надежности обнаружения событий входа в область. Установка более высоких уровней достоверности гарантирует, что события будут запускаться только при наличии высокой надежности обнаружения, что снижает количество ложных тревог.

4) **Опционально.** Повторите шаги выше, чтобы нарисовать больше правил. Поддерживается до 4 правил.


8. Нажмите **Arming Schedule** («Расписание постановки на охрану»), чтобы выбрать тип расписания постановки на охрану.

 **Примечание**

Если для **Arming Schedule** («Расписание постановки на охрану») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание постановки на охрану, или переместить курсор на временную шкалу и нажать , чтобы задать указанное расписание времени.

9. Нажмите **Linkage Method** («Метод привязки») для настройки методов привязки.

Таблица 13-5 Описание метода привязки

Метод привязки	Описание
Уведомление центра мониторинга	Видеореги­стратор может направить исключение или тревогу на удаленный тревожный хост, когда происходит событие. Тревожный хост относится к ПК, на котором установлено клиентское программное обеспечение (например, iVMS-4200, iVMS-5200).
Всплывающее окно тревоги	При срабатывании тревоги на локальном мониторе отображается всплывающее окно тревоги.
Бипер	При обнаружении тревоги бипер издаст звуковой сигнал.
Отправка Email	Видеореги­стратор может отправлять электронное письмо с информацией о тревоге пользователю или пользователям.
Тревожный выход	Срабатывание тревожного выхода может быть вызвано обнаружением движения, детектором саботажа, детекцией лиц, обнаружением пересечения линии и любыми другими событиями.
Запись	При обнаружении тревоги выбранный канал будет записывать видео.  Примечание Для канала должно быть включено расписание видеозаписи, в противном случае данная привязка будет недействительной. Перейдите в System → Storage Management → Storage Schedule → Video Recording («Система → Управление хранением → Расписание хранения → Видеозапись») для настройки расписания записи видео.

10. **Опционально.** Настройте параметры **Shield Area** («Защищенная область»), если установлен флажок **AI by NVR** («ИИ с помощью NVR»). После установки зоны защиты устройство не будет анализировать поведение цели в этой зоне, поэтому события защиты периметра не будут срабатывать в пределах этой зоны.

11. Нажмите **Save** («Сохранить»).

Дальнейшие шаги

Перейдите в **Live View** («Просмотр в режиме реального времени») и нажмите **Target** («Цель»), чтобы просмотреть тревоги в режиме реального времени.


Настройка выхода из области

Функция обнаружения выхода из области обнаруживает объекты, которые перемещаются из заранее заданной виртуальной области.

Шаги

Примечание

Часть следующих шагов доступна только для определенных моделей NVR или камер.

1. Перейдите **Event Center** («Центр событий») →  → **Event Configuration** → **Perimeter Protection** («Конфигурация событий → Защита периметра»).
 2. Выберите камеру.
 3. **Опционально.** Включите **Secondary Analysis** («Повторный анализ»). Соответствующий процессор повторно проанализирует это событие, чтобы уменьшить количество ложных тревог.
-

Примечание

Алгоритм **Secondary Analysis for Perimeter Protection** («Повторный анализ для защиты периметра») должен быть запущен по крайней мере на одном устройстве. Справа нажмите **Allocate Engine** («Назначить процессор») для быстрого назначения или перейдите в **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** («Система → Интеллектуальные настройки → Конфигурация алгоритма → Управление алгоритмом»), чтобы включить **Secondary Analysis for Perimeter Protection** («Повторный анализ для защиты периметра»).

4. **Опционально.** Включите **AI by NVR** («ИИ с помощью NVR»). Устройство будет анализировать видео, а камеры только передавать видеопоток.
-

Примечание

Алгоритм **Perimeter Protection** («Защита периметра») должен быть запущен по крайней мере на одном устройстве. Справа нажмите **Allocate Engine** («Назначить процессор») для быстрого назначения или перейдите в **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** («Система → Интеллектуальные настройки → Конфигурация алгоритма → Управление алгоритмом»), чтобы включить **Perimeter Protection** («Защита периметра»).

5. Выберите **Region Exiting** («Выход из области»).
6. Нажмите **Enable** («Включить»).

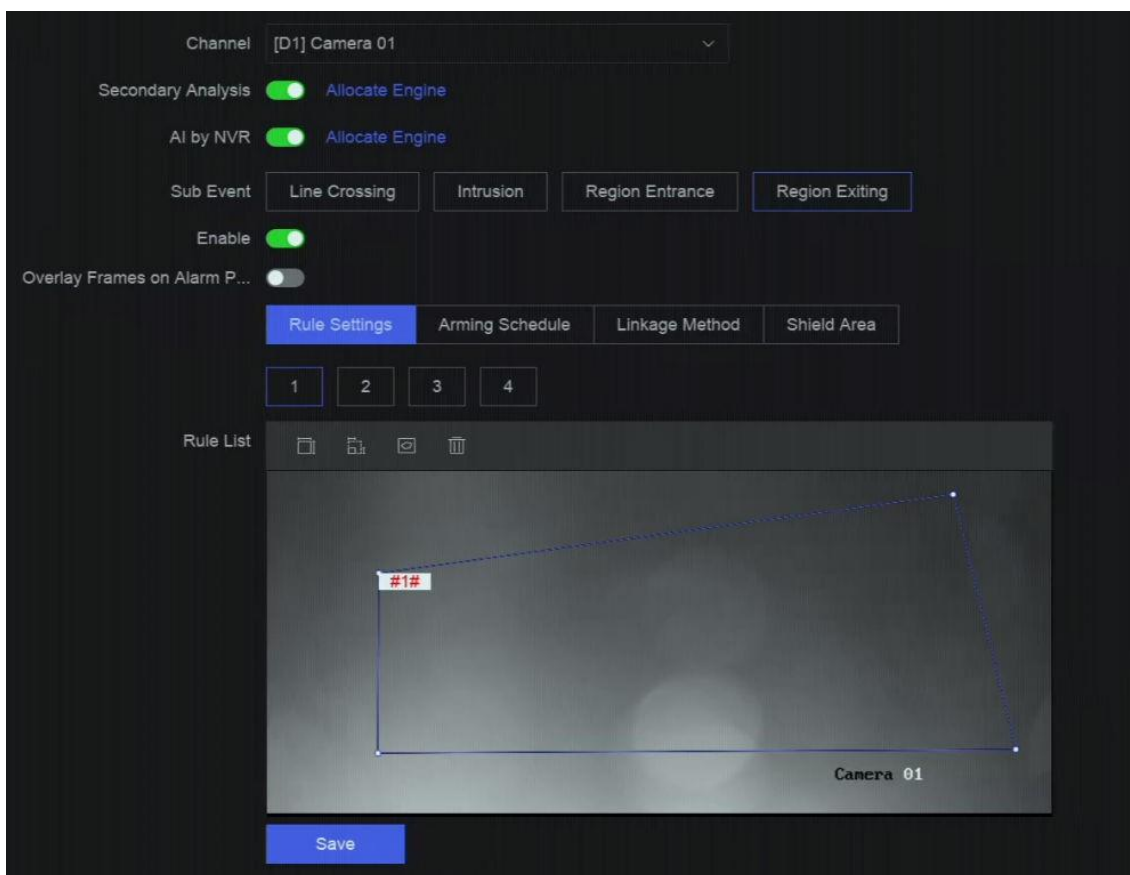



Рисунок 13-4 Выход из области

7. Нажмите **Rule Settings** («Настройки правила»), чтобы настроить правила обнаружения.

1) Выберите номер правила. Например, выберите **1**.

2) Нажмите на  и щелкните по изображению 4 раза, чтобы нарисовать каждую точку четырехугольной или десятиугольной области.

3) Настройте **Sensitivity** («Чувствительность»), **Detection Target** («Обнаружение цели») и **Target Confidence** («Достоверность обнаружения цели»). **Чувствительность**

Чем выше значение, тем больше вероятность срабатывания тревоги обнаружения движения.

Обнаружение цели

Выбрано **Target Detection** («Обнаружение цели») на значение **Human** («Человек») или **Vehicle** («Транспортное средство»), чтобы отключить тревогу при обнаружении человека или транспортного средства. Функция **Detection Target** («Обнаружение цели») представлена не во всех моделях.

Достоверность обнаружения цели


Используется для обозначения уровня достоверности или надежности обнаружения событий выхода из области. Установка более высоких уровней достоверности гарантирует, что события будут запускаться только при наличии высокой надежности обнаружения, что снижает количество ложных тревог.

4) **Опционально.** Повторите шаги выше, чтобы нарисовать больше правил. Поддерживается до 4 правил.

8. Нажмите **Arming Schedule** («Расписание постановки на охрану»), чтобы выбрать тип расписания постановки на охрану.




Примечание

Если для **Arming Schedule** («Расписание постановки на охрану») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание постановки на охрану, или переместить курсор на временную шкалу и нажать **00:00-24:00** , чтобы задать указанное расписание времени.

9. Нажмите **Linkage Method** («Метод привязки») для настройки методов привязки.

Таблица 13-6 Описание метода привязки

Метод привязки	Описание
Уведомление центра мониторинга	Видеореги­стратор может направить исключение или тревогу на удаленный тревожный хост, когда происходит событие. Тревожный хост относится к ПК, на котором установлено клиентское программное обеспечение (например, iVMS-4200, iVMS-5200).
Всплывающее окно тревоги	При срабатывании тревоги на локальном мониторе отображается всплывающее окно тревоги.
Бипер	При обнаружении тревоги бипер издаст звуковой сигнал.
Отправка Email	Видеореги­стратор может отправлять электронное письмо с информацией о тревоге пользователю или пользователям.
Тревожный выход	Срабатывание тревожного выхода может быть вызвано обнаружением движения, детектором саботажа, детекцией лиц, обнаружением пересечения линии и любыми другими событиями.
Запись	<p>При обнаружении тревоги выбранный канал будет записывать видео.</p> <p> Примечание</p> <p>Для канала должно быть включено расписание видеозаписи, в противном случае данная привязка будет недействительной. Перейдите в System → Storage Management → Storage Schedule → Video Recording («Система → Управление хранением → Расписание хранения → Видеозапись») для настройки расписания записи видео.</p>

10. **Опционально.** Настройте параметры **Shield Area** («Защищенная область»), если установлен флажок **AI by NVR** («ИИ с помощью NVR»). После установки зоны защиты устройство не будет анализировать поведение цели в этой зоне, поэтому события защиты периметра не будут срабатывать в пределах этой зоны.

11. Нажмите **Save** («Сохранить»).

Дальнейшие шаги

Перейдите в **Live View** («Просмотр в режиме реального времени») и нажмите **Target** («Цель»), чтобы просмотреть тревоги в режиме реального времени.

13.1.3 Событие отклонений в поведении

Перед началом

Убедитесь, что камера поддерживает эту функцию.

Шаги


1. Перейдите **Event Center** («Центр событий») →  → **Event Configuration** → **Abnormal Behavior Event** («Конфигурация событий → Событие отклонений в поведении»).
2. Выберите камеру
3. Выберите тип события.
4. Нажмите **Enable** («Включить»).
5. Нажмите **Rule Settings** («Настройки правила»), чтобы задать правило.

Таблица 13-7 События отклонений в поведении


Имя события	Описание события	Настройка правила
Детекция праздношата­ния	Функция обнаружения праздношатания используется для определения нахождения цели в указанной области дольше установленного времени, и срабатывания тревоги для связанных действий.	а. Выберите номер правила. б. Используйте панель инструментов в верхней части изображения, чтобы нарисовать линию обнаружения. с. Задайте Time Threshold («Порог времени») и Sensitivity («Чувствительность»). Порог времени
Детекция парковочного места	Обнаружение парковки используется для обнаружения нарушения парковки в зоне. Широко применяется на скоростной автомагистрали и улицах с односторонним движением.	Период времени, в течение которого объект остается в области. Если значение – 10, то тревога сработает тогда, когда объект остается в области в течение 10 секунд. Диапазон: [от 1 до 10].
Обнаружение оставленного багажа	Функция обнаружения оставленного багажа обнаруживает объекты (например, багаж, кошелек, опасные предметы), оставленные в предварительно заданной области. Устройство активирует определенные действия в ответ на срабатывание тревоги.	Чувствительность Сходство фонового изображения с объектом. Чем выше значение, тем больше вероятность срабатывания тревоги обнаружения движения. d. Опционально. Повторите указанные выше шаги, чтобы установить еще одно.
Обнаружение перемещения объекта	Функция обнаружения оставленного багажа обнаруживает объекты (например, экспонаты на выставке), которые были перемещены из области. Устройство активирует определенные действия в ответ на срабатывание тревоги.	
Детекция быстрого движения	Обнаружение быстрого движения используется для обнаружения подозрительного бега и преследования, превышения скорости и быстрого движения. Устройство вызовет тревогу при обнаружении быстрого движения, и отправит уведомление в хост постановки на охрану, чтобы позволит предпринять необходимые действия заранее.	

Имя события	Описание события	Настройка правила
Детекция скоплений людей	Функция детекции скоплений людей используется для определения того, превышает ли плотность скопления людей в указанной области установленное значение, и инициирует тревогу для связанных действий.	<p>a. Выберите номер правила.</p> <p>b. Используйте панель инструментов в верхней части изображения, чтобы нарисовать линию обнаружения.</p> <p>c. Настройте Percentage («Процент»). Процентное значение показывает уровень скопления людей в пределах области. Если оно превышает пороговое значение, устройство вызовет тревогу.</p> <p>d. Опционально. Повторите указанные выше шаги, чтобы установить еще одно.</p>

6. Нажмите **Arming Schedule** («Расписание постановки на охрану»), чтобы выбрать тип расписания постановки на охрану.




Примечание

Если для **Arming Schedule** («Расписание постановки на охрану») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание постановки на охрану, или переместить курсор на временную шкалу и нажать , чтобы задать указанное расписание времени.

7. Нажмите **Linkage Method** («Метод привязки») для настройки методов привязки.

Таблица 13-8 Описание метода привязки

Метод привязки	Описание
Уведомление центра мониторинга	Видеореги­стратор может направить исключение или тревогу на удаленный тревожный хост, когда происходит событие. Тревожный хост относится к ПК, на котором установлено клиентское программное обеспечение (например, iVMS-4200, iVMS-5200).
Всплывающее окно тревоги	При срабатывании тревоги на локальном мониторе отображается всплывающее окно тревоги.
Бипер	При обнаружении тревоги бипер издаст звуковой сигнал.
Отправка Email	Видеореги­стратор может отправлять электронное письмо с информацией о тревоге пользователю или пользователям.
Тревожный выход	Срабатывание тревожного выхода может быть вызвано обнаружением движения, детектором саботажа, детекцией лиц, обнаружением пересечения линии и любыми другими событиями.
Запись	При обнаружении тревоги выбранный канал будет записывать видео.

Метод привязки	Описание
	 Примечание Для канала должно быть включено расписание видеозаписи, в противном случае данная привязка будет недействительной. Перейдите в System → Storage Management → Storage Schedule → Video Recording («Система → Управление хранением → Расписание хранения → Видеозапись») для настройки расписания записи видео.


8. Нажмите **Save** («Сохранить»).

13.1.4 Целевое событие

Перед началом

Убедитесь, что подключенная камера поддерживает эту функцию, или что в настройках устройства включен алгоритм **Target Recognition** («Распознавание цели») или **Video Structuralization** («Структуризация видео») в **Event Center → Event Configuration → Smart Settings → Algorithm Configuration → Algorithm Management** («Центр событий → Конфигурация событий → Интеллектуальные настройки → Конфигурация алгоритма → Управление алгоритмом»).

Шаги


1. Перейдите **Event Center** («Центр событий») →  → **Event Configuration → Target Event** («Конфигурация событий → Целевое событие»).
2. Выберите камеру.
3. Выберите события.
4. Нажмите **Enable** («Включить»).
5. Установите правила событий.

Имя события	Описание события	Настройка правила
Захват лиц	Функция захвата лиц обнаруживает и фиксирует лица, появляющиеся в зоне. Связанные действия могут запускаться при обнаружении лиц.	-
Сравнение изображений лиц	Функция сравнивает обнаруженные изображения лиц с указанной библиотекой списков. При успешном сравнении срабатывает сигнал.	<ul style="list-style-type: none"> Поддержка настройки оценки цели. Сравнение изображений лиц начинается, когда оценка цели соответствует требованиям сравнения (расстояние между зрачками больше заданного порогового значения, а угол наклона и угол поворота меньше заданных пороговых значений). Поддержка настройки уведомлений об ошибке сравнения и об успешном сравнении.
Детекция неизвестных лиц	Лица, отсутствующие в библиотеке списков и появляющиеся на видео, будут идентифицированы как посторонние.	<ul style="list-style-type: none"> Поддержка настройки оценки цели. Сравнение изображений лиц начинается, когда оценка цели соответствует требованиям сравнения (расстояние между зрачками больше заданного порогового значения, а угол наклона и угол поворота меньше заданных пороговых значений). Поддерживается настройка уведомления при обнаружении посторонних лиц.
Детекция и анализ нескольких целей	Обнаружение нескольких целей позволяет устройству одновременно обнаруживать лица, фигуру человека и транспортные средства в сцене.	-

6. Нажмите **Arming Schedule** («Расписание постановки на охрану»), чтобы выбрать тип расписания постановки на охрану.




Примечание

Если для **Arming Schedule** («Расписание постановки на охрану») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание постановки на охрану, или переместить курсор на временную шкалу и нажать , чтобы задать указанное расписание времени.

7. Нажмите **Linkage Method** («Метод привязки») для настройки методов привязки.

Таблица 13-9 Описание метода привязки

Метод привязки	Описание
Уведомление центра мониторинга	Видеореги­стратор может направить исключение или тревогу на удаленный тревожный хост, когда происходит событие. Тревожный хост относится к ПК, на котором установлено клиентское программное обеспечение (например, iVMS-4200, iVMS-5200).
Всплывающее окно тревоги	При срабатывании тревоги на локальном мониторе отображается всплывающее окно тревоги.
Бипер	При обнаружении тревоги бипер издаст звуковой сигнал.
Отправка Email	Видеореги­стратор может отправлять электронное письмо с информацией о тревоге пользователю или пользователям.
Тревожный выход	Срабатывание тревожного выхода может быть вызвано обнаружением движения, детектором саботажа, детекцией лиц, обнаружением пересечения линии и любыми другими событиями.
Запись	При обнаружении тревоги выбранный канал будет записывать видео.
	 Примечание Для канала должно быть включено расписание видеозаписи, в противном случае данная привязка будет недействительной. Перейдите в System → Storage Management → Storage Schedule → Video Recording («Система → Управление хранением → Расписание хранения → Видеозапись») для настройки расписания записи видео.

8. Нажмите **Save** («Сохранить»).

13.1.5 Обнаружение тепловизионной камеры

Сетевой видеореги­стратор поддерживает режимы обнаружения событий тепловизионных IP-камер: обнаружение возгораний и дыма, определение температуры, определение разницы температур и т. д.

Перед началом

Добавьте тепловизионную IP-камеру к устройству и убедитесь, что камера активирована.

Шаги


1. Перейдите **Event Center** («Центр событий») →  → **Event Configuration → Thermal Event** («Конфигурация событий → Тепловизионное событие»).
2. Выберите камеру.
3. Выберите тип события.
4. Нажмите **Enable** («Включить»).
5. Нажмите **Rule Settings** («Настройки правила»), чтобы задать правило.


Таблица 13-10 Тепловизионное событие

Имя события	Описание события
Обнаружение возгораний	Тревога сработает при обнаружении пожара в зоне постановки на охрану.
Определение температуры тела	Тревога сработает, если температура превысит пороговое значение.
Защита периметра	События защиты периметра включают обнаружение пересечения линии, обнаружение вторжения, обнаружение входа в область и обнаружение выхода из области.

6. Нажмите **Arming Schedule** («Расписание постановки на охрану»), чтобы выбрать тип расписания постановки на охрану.



Примечание

Если для **Arming Schedule** («Расписание постановки на охрану») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание постановки на охрану, или переместить курсор на временную шкалу и нажать , чтобы задать указанное расписание времени.

7. Нажмите **Linkage Method** («Метод привязки») для настройки методов привязки.

Таблица 13-11 Описание метода привязки

Метод привязки	Описание
Уведомление центра мониторинга	Видеореги­стратор может направить исключение или тревогу на удаленный тревожный хост, когда происходит событие. Тревожный хост относится к ПК, на котором установлено клиентское программное обеспечение (например, iVMS-4200, iVMS-5200).
Всплывающее окно тревоги	При срабатывании тревоги на локальном мониторе отображается всплывающее окно тревоги.
Бипер	При обнаружении тревоги бипер издаст звуковой сигнал.
Отправка Email	Видеореги­стратор может отправлять электронное письмо с информацией о тревоге пользователю или пользователям.
Тревожный выход	Срабатывание тревожного выхода может быть вызвано обнаружением движения, детектором саботажа, детекцией лиц, обнаружением пересечения линии и любыми другими событиями.


Метод привязки	Описание
Запись	<p>При обнаружении тревоги выбранный канал будет записывать видео.</p> <p> Примечание</p> <p>Для канала должно быть включено расписание видеозаписи, в противном случае данная привязка будет недействительной. Перейдите в System → Storage Management → Storage Schedule → Video Recording («Система → Управление хранением → Расписание хранения → Видеозапись») для настройки расписания записи видео.</p>

8. Нажмите **Save** («Сохранить»).

13.1.6 Событие тревожного входа

Установите действие обработки сигнала тревоги охранного датчика.

Шаги

1. Перейдите **Event Center** («Центр событий») →  → **Event Configuration → Alarm Input Event** («Конфигурация событий → Событие тревожного входа»).
2. Выберите название тревожного входа.

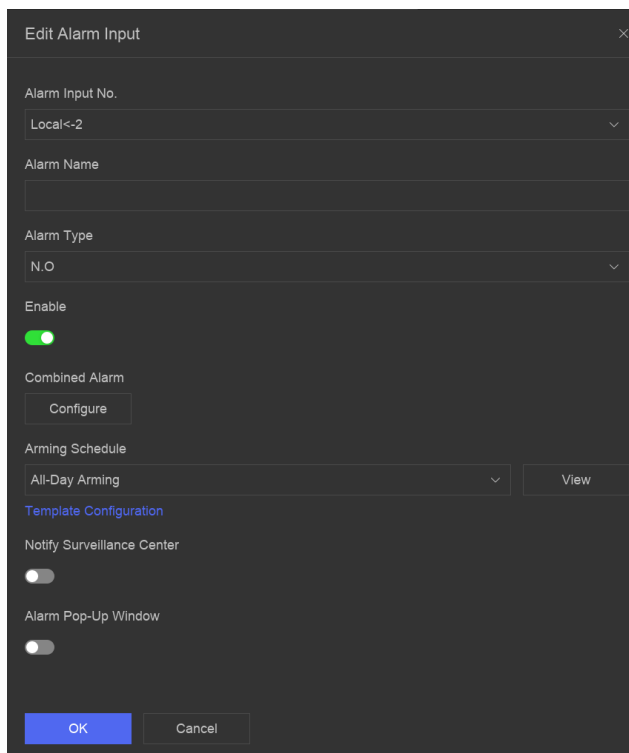


Рисунок 13-5 Настройка тревожного входа

 **Примечание**

Например, **Local<-1** означает, что номер тревожного входа на задней панели устройства равен 1.

3. Измените **Alarm Name** («Название тревоги»).

4. Настройте **Alarm Type** («Тип тревоги»). **N.O** («Нормально разомкнутый»)

Когда контакты находятся в естественном и выключенном состоянии, если два контакта выключены, их можно назвать нормально разомкнутыми.

N.O («Нормально разомкнутый»)

Когда контакты находятся в естественном и выключенном состоянии, если подключены два контакта, то их можно назвать нормально замкнутыми.

5. Нажмите **Enable** («Включить»).

6. **Опционально.** Если на шаге 2 выбрано значение **Local<-1**, выберите метод обработки.

- Выберите **Process Alarm Input** («Обработка тревожного входа»), после чего можно установить соответствующее расписание постановки на охрану, методы привязки и т. д.

 **Примечание**

Все описанные ниже операции доступны при выборе этого метода обработки.

- Выберите **Quick Disarming** («Быстрое снятие с охраны»), после чего методы привязки всех событий будут отключены.

7. Нажмите **Configure** («Настроить»), чтобы настроить комбинированную тревогу.

1) Выберите канал.


2) Выберите комбинированные события тревоги, такие как обнаружение движения и детекция саботажа видео.

3) Нажмите **OK**.

Комбинированные тревоги будут срабатывать при получении тревоги как от тревожного входа, так и от событий.


8. Нажмите **Arming Schedule** («Расписание постановки на охрану»), чтобы выбрать тип расписания постановки на охрану.

 **Примечание**

Если для **Arming Schedule** («Расписание постановки на охрану») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание постановки на охрану, или переместить курсор на временную шкалу и нажать **00:00-24:00** , чтобы задать указанное расписание времени.

9. Нажмите **Linkage Method** («Метод привязки») для настройки методов привязки.

Таблица 13-12 Описание метода привязки

Метод привязки	Описание
Уведомление центра мониторинга	Видеореги­стратор может направить исключение или тревогу на удаленный тревожный хост, когда происходит событие. Тревожный хост относится к ПК, на котором установлено клиентское программное обеспечение (например, iVMS-4200, iVMS-5200).
Всплывающее окно тревоги	При срабатывании тревоги на локальном мониторе отображается всплывающее окно тревоги.
Бипер	При обнаружении тревоги бипер издаст звуковой сигнал.
Отправка Email	Видеореги­стратор может отправлять электронное письмо с информацией о тревоге пользователю или пользователям.
Тревожный выход	Срабатывание тревожного выхода может быть вызвано обнаружением движения, детектором саботажа, детекцией лиц, обнаружением пересечения линии и любыми другими событиями.
Запись	<p>При обнаружении тревоги выбранный канал будет записывать видео.</p> <p> Примечание</p> <p>Для канала должно быть включено расписание видеозаписи, в противном случае данная привязка будет недействительной. Перейдите в System → Storage Management → Storage Schedule → Video Recording («Система → Управление хранением → Расписание хранения → Видеозапись») для настройки расписания записи видео.</p>

10. Нажмите **Save** («Сохранить»).

13.1.7 Событие аудиоанализа

Шаги


1. Перейдите **Event Center** («Центр событий») →  → **Event Configuration** → **Audio Analysis** («Конфигурация событий → Анализ аудио»).
2. Выберите канал.
3. Выберите тип события.
4. Нажмите **Enable** («Включить»).
5. Нажмите **Rule Settings** («Настройки правила»), чтобы задать правило.


Таблица 13-13 Событие аудиоанализа

Имя события	Описание события	Настройка правила
Детекция звуковых событий	Функция детекции звуковых событий позволяет обнаружить звуковые отклонения в сцене, такие как резкий рост / спад интенсивности звука.	<p>Детекция внезапного роста интенсивности звука Детекция резкого роста интенсивности звука в сцене.</p> <p>Детекция внезапного спада интенсивности звука Обнаружение внезапного спада интенсивности звука в области.</p> <p>Чувствительность Чем выше значение, тем больше вероятность срабатывания тревоги обнаружения движения.</p> <p>Sound Intensity Threshold («Пороговое значение интенсивности звука») Фильтрация звука в окружающей среде. Чем громче звук окружающей среды, тем выше должно быть значение интенсивности. Можно отрегулировать данный параметр в соответствии с условиями среды.</p>

6. Нажмите **Arming Schedule** («Расписание постановки на охрану»), чтобы выбрать тип расписания постановки на охрану.



Примечание

Если для **Arming Schedule** («Расписание постановки на охрану») выбрать **Custom** («Пользовательский»), то можно перетащить курсор на временную шкалу и задать настраиваемое расписание постановки на охрану, или переместить курсор на временную шкалу и нажать , чтобы задать указанное расписание времени.

7. Нажмите **Linkage Method** («Метод привязки») для настройки методов привязки.

Таблица 13-14 Описание метода привязки

Метод привязки	Описание
Уведомление центра мониторинга	Видеореги­стратор может направить исключение или тревогу на удаленный тревожный хост, когда происходит событие. Тревожный хост относится к ПК, на котором установлено клиентское программное обеспечение (например, iVMS-4200, iVMS-5200).
Всплывающее окно тревоги	При срабатывании тревоги на локальном мониторе отображается всплывающее окно тревоги.
Бипер	При обнаружении тревоги бипер издаст звуковой сигнал.
Отправка Email	Видеореги­стратор может отправлять электронное письмо с информацией о тревоге пользователю или пользователям.

Метод привязки	Описание
Тревожный выход	Срабатывание тревожного выхода может быть вызвано обнаружением движения, детектором саботажа, детекцией лиц, обнаружением пересечения линии и любыми другими событиями.
Запись	<p>При обнаружении тревоги выбранный канал будет записывать видео.</p> <p> Примечание</p> <p>Для канала должно быть включено расписание видеозаписи, в противном случае данная привязка будет недействительной. Перейдите в System → Storage Management → Storage Schedule → Video Recording («Система → Управление хранением → Расписание хранения → Видеозапись») для настройки расписания записи видео.</p>

8. Нажмите **Save** («Сохранить»).

13.2 Настройка привязки

Настройте параметры для привязки событий.

Шаги



1. Перейдите **Event Center** («Центр событий») →  → **Event Configuration → Linkage Configuration** («Конфигурация событий → Конфигурация привязки») или **System → Event Configuration →** («Система → Конфигурация событий»)  → **Event Configuration → Linkage Configuration** («Конфигурация событий → Конфигурация привязки»).
2. Нажмите **Email**, чтобы настроить параметры электронной почты.

Таблица 13-15 Привязка Email

Элемент	Описание
Серверная аутентификация	Включите эту функцию, если сервер SMTP требует аутентификации пользователя, и введите имя пользователя и пароль соответственно.
SMTP-сервер	IP-адрес или имя хоста (например, smtp.263xmail.com) SMTP-сервера.
SMTP-порт	SMTP-порт. По умолчанию, порт TCP/IP, используемый для SMTP – 25.
Активация SSL/TLS	Включите SSL / TLS, если необходимо для SMTP-сервера.
Отправитель	Имя отправителя.
Адрес отправителя	Введите e-mail адрес отправителя.
Выбор получателя	Выберите получателя. Можно настроить до 3 получателей.
Вложенное изображение	Отправка электронного письма с вложенными изображениями тревог.

Элемент	Описание
Прикрепление 3 изображений для функции защиты периметра	При срабатывании события защиты периметра устройство отправит электронное письмо с 3 прикрепленными изображениями тревоги.
Интервал	Временной интервал для захвата прикрепленных изображений.

Примечание

Если вы используете учетную запись электронной почты Outlook, для параметра **Email Type** («Тип электронной почты») выберите значение **Outlook** и нажмите **Help** («Справка») справа, чтобы прочитать инструкции по настройке, затем следуйте инструкциям в интерфейсе для завершения настройки.

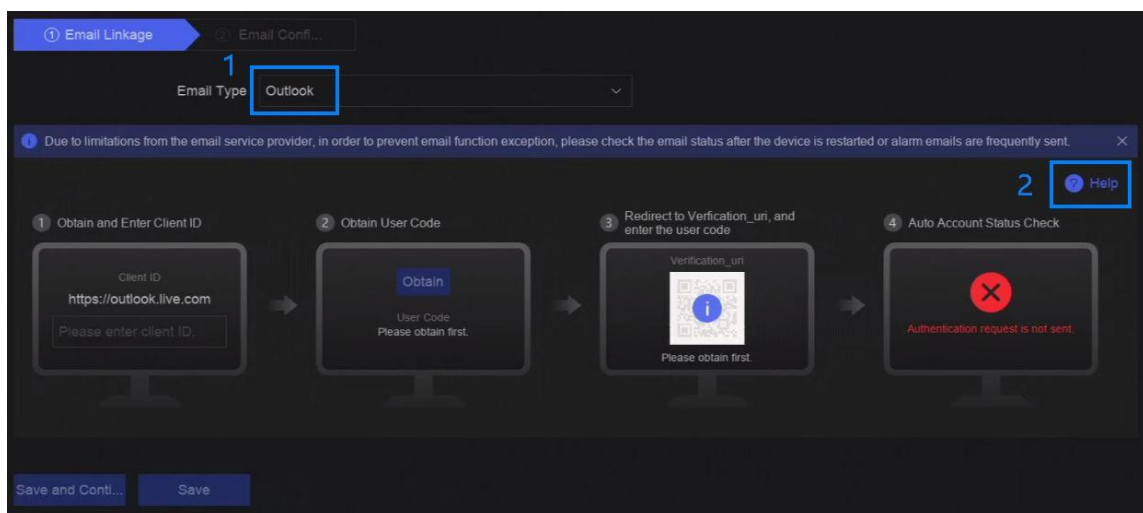


Рисунок 13-6 Настройка электронной почты Outlook

3. Нажмите **Audio Management** («Управление аудио»), чтобы управлять аудиофайлами для привязки к тревоге.

Примечание

В списке есть 3 аудиофайла по умолчанию, которые нельзя удалить. Можно импортировать аудиофайлы с USB-накопителя. Файлы должны быть в формате AAC или MP3, а размер каждого файла должен быть в пределах 1 Мб.

4. Если подключены IP-динамики, нажмите **IP Speaker** («IP-динамик»), чтобы импортировать аудиофайлы в выбранные IP-динамики для привязки к тревоге.

Примечание

- Это действие привязки доступно только для нескольких типов событий.
- Загруженный аудиофайл должен быть в формате MP3, WAV или ACC, а размер файла должен быть менее 1 Мб.

5. Нажмите **Alarm Output** («Тревожный выход»), чтобы задать параметры тревожного выхода.

Примечание

- Нажмите на название каждого тревожного выхода, чтобы изменить его.
 - Номер тревожного выхода такой же, как на задней панели устройства. Например, **Local->1** обозначает, что номер тревожного выхода на задней панели устройства равен 1.
-

Задержка

Длительность тревоги.

Состояние тревоги

Нажмите **Trigger** («Запуск»), чтобы переключить состояние.

6. Если подключена камера со стробоскопом и звуковым предупреждением, нажмите **Camera Audio and Light Configuration** («Конфигурация стробоскопа и динамика камеры»), чтобы настроить параметры стробоскопа и динамика камеры для привязки тревог.

Примечание



Это действие привязки доступно только для нескольких типов событий.

7. Если подключены охранные панели, нажмите **Security Control Panel** («Охранный панель»), чтобы настроить параметры, включая IP-адрес и номер порта.

13.3 Конфигурация снятия с охраны

После настройки шаблона снятия с охраны можно использовать шаблон для снятия каналов с охраны в пакетном режиме. Каналы, для которых включен параметр **Allow Disarming** («Разрешить снятие с охраны»), не будут активировать элементы привязки тревоги в соответствии с шаблоном снятия с охраны.

Шаги

1. Перейдите **Event Center** («Центр событий») →  → **Event Configuration** → **Linkage Configuration** («Конфигурация событий → Конфигурация привязки») или **System** → **Event Configuration** → («Система → Конфигурация событий»)  → **Event Configuration** → **Linkage Configuration** («Конфигурация событий → Конфигурация привязки»).

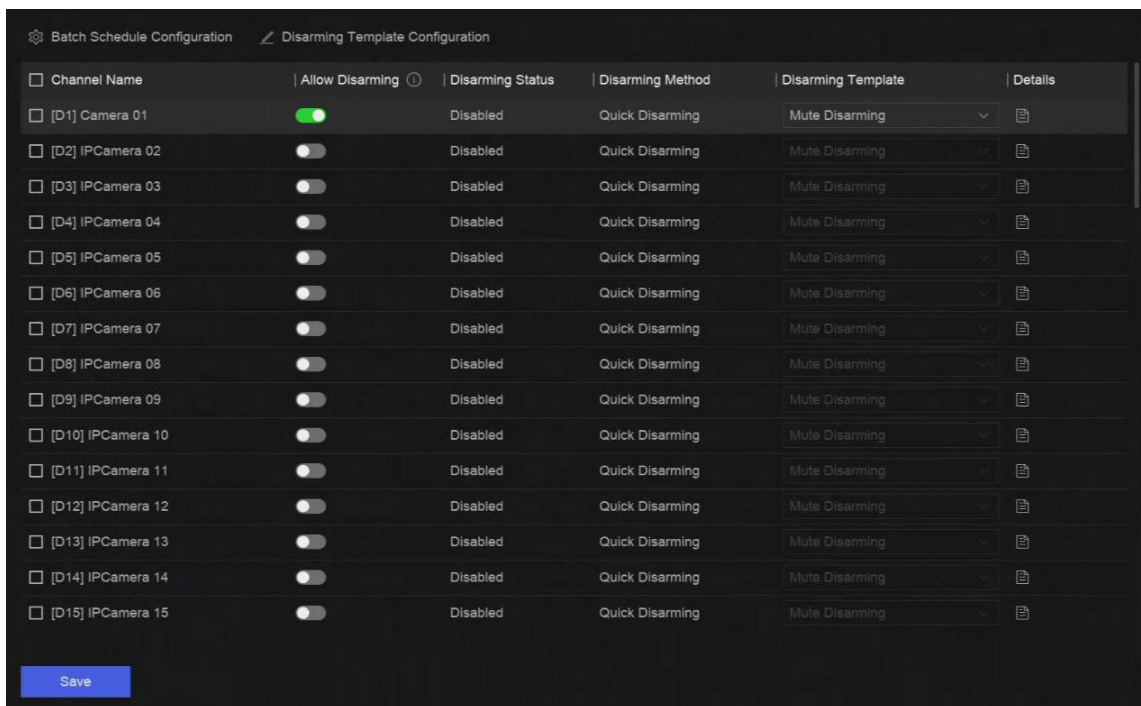


Рисунок 13-7 Конфигурация снятия с охраны

- Выберите каналы, которые разрешено снимать с охраны.
- Нажмите **Batch Schedule Configuration** («Конфигурация расписания в пакетном режиме»).
- Нажмите **Enable** («Включить»).
- Выберите **Disarming Template** («Шаблон снятия с охраны»). Доступно только два типа.



Примечание

В настоящее время доступны только два типа шаблонов, и параметры каждого шаблона не могут быть настроены.

- Нажмите **OK**.

13.4 Настройка в пакетном режиме

Перечисленные события и соответствующее действие привязки в **Notify Surveillance Center** («Уведомление центра мониторинга») можно включать или отключать в пакетном режиме через **Event Center** («Центр событий») → → **Event Configuration** → **Batch Configuration** («Конфигурация событий → Конфигурация в пакетном режиме») или **System** → **Event Configuration** («Система → Конфигурация событий») → → **Event Configuration** → **Batch Configuration** («Конфигурация событий → Конфигурация в пакетном режиме»). После включения события нажмите **Go to Event Configuration** («Перейти к конфигурации событий»), чтобы задать правила.

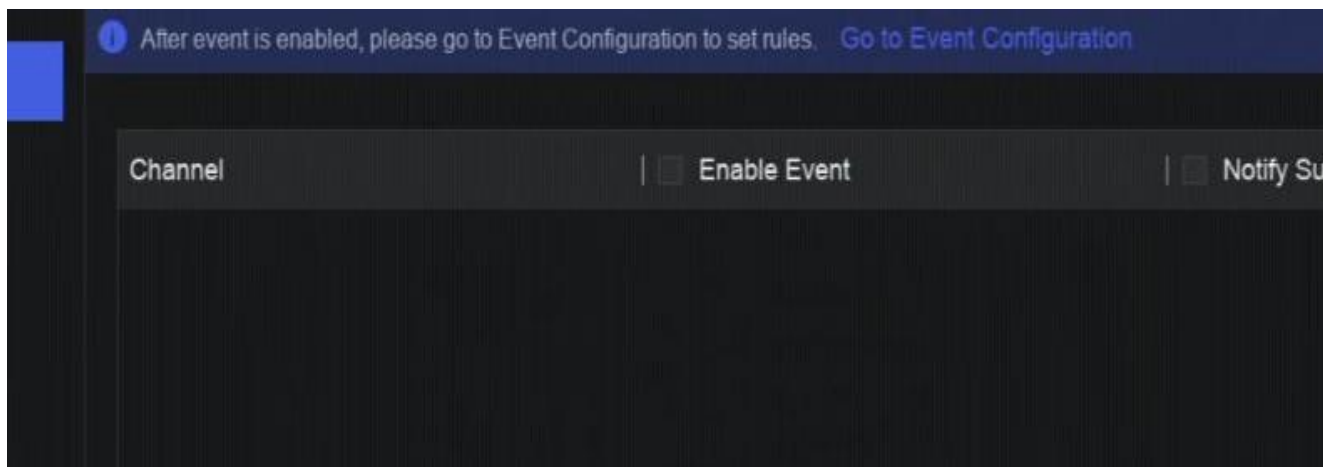


Рисунок 13-8 Конфигурация в пакетном режиме

13.5 Поиск событий

Можно искать файлы событий, такие как видео и изображения, в соответствии с условием поиска.

Шаги

1. Перейдите **Event Center** («Центр событий») → .

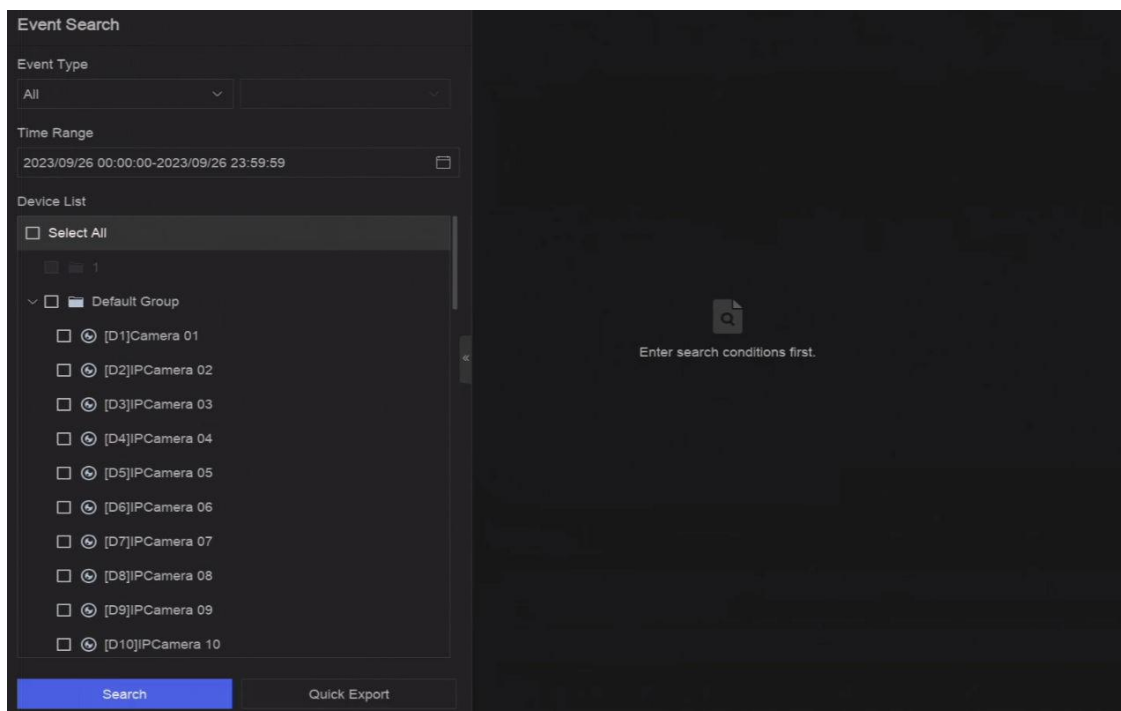


Рисунок 13-9 Поиск событий

2. Укажите подробные условия, включая тип события, время, канал и т. д.
3. Нажмите **Search** («Поиск»).

Устройство отобразит результаты поиска выбранных каналов.


Дальнейшие шаги

Выберите элементы из списка результатов и экспортируйте их для резервного копирования.

13.6 Просмотр тревог

Можно просматривать видео и изображения тревоги в режиме реального времени и воспроизводить их.

Шаги

1. Перейдите **Event Center** («Центр событий») → .
2. Нажмите **Real-Time Alarm** («Тревога в режиме реального времени»).
3. Выберите тревогу из списка.
Если тревог слишком много, нажмите **Filter** («Фильтр»), чтобы выполнить поиск и найти тревогу.
4. Нажмите **Playback** («Воспроизведение»), и видеозапись тревоги будет воспроизведена.
5. Просмотрите изображения тревоги справа. Будет указано количество доступных изображений.

Раздел 14 Поиск и резервное копирование

Можно искать файлы в соответствии с различными условиями поиска, включая тип файла, тип события, время, тег и т. д. Результаты поиска можно экспортировать на другое устройство, например, на USB-накопитель.

Перед началом

Убедитесь, что HDD правильно установлен и параметры записи настроены правильно.

Шаги

1. Перейдите в **Backup** («Резервное копирование»).

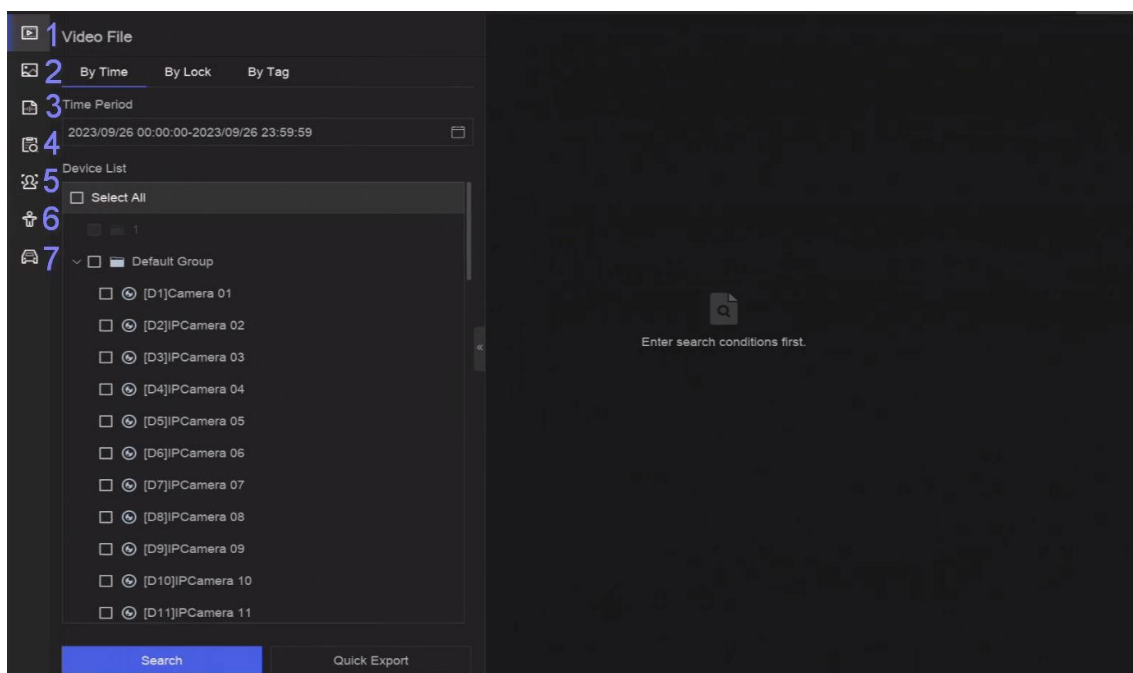


Рисунок 14-1 Поиск и резервное копирование

2. Выберите необходимый метод поиска слева, поддерживается 7 типов.

Примечание

Условия поиска будут различаться в зависимости от выбранного метода поиска.

3. Установите условия поиска.
4. Нажмите **Search** («Поиск»).

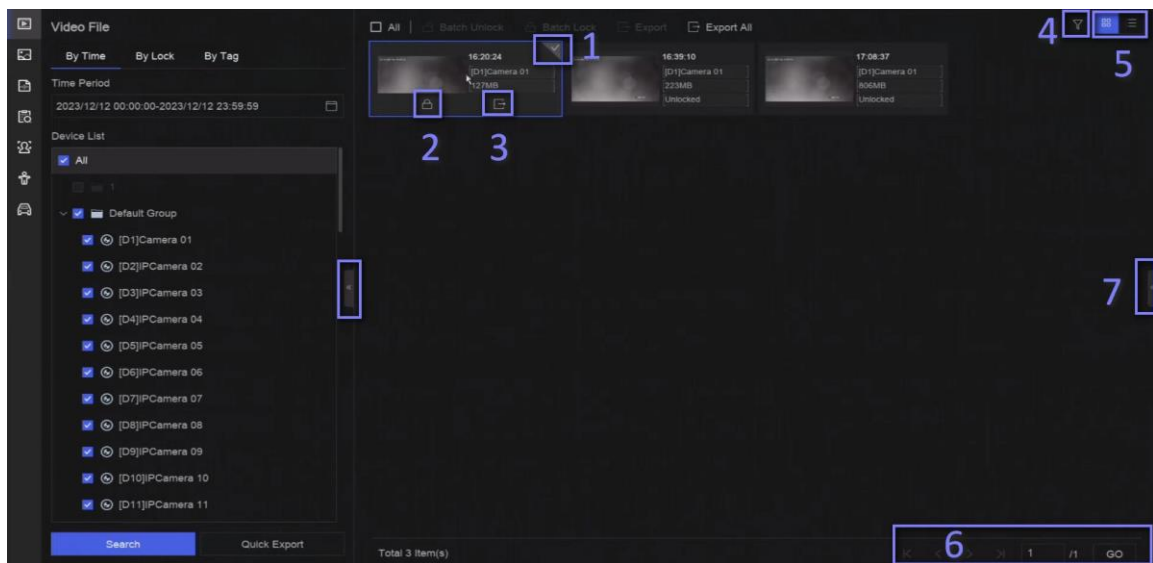


Рисунок 14-2 Результат поиска

5. **Опционально.** Выполните следующие операции.

- 1 Нажмите, чтобы выбрать файл.
 - 2 Нажмите, чтобы заблокировать файл. После блокировки файл не будет перезаписан.
 - 3 Нажмите, чтобы экспортировать файл.
 - 4 Используйте панель инструментов сверху, чтобы отфильтровать результаты по каналу.
 - 5 Используйте панель инструментов сверху, чтобы переключить эффект отображения.
 - 6 Переход на разные страницы результатов.
 - 7 Разверните или сверните интерфейс. Выбрав видео из списка результатов, можно быстро воспроизвести его.
6. Вставьте USB-накопитель в устройство для резервного копирования.
7. Экспортируйте файлы на USB-накопитель.
- Выберите файлы в списке результатов и нажмите **Export** («Экспорт»).
 - Нажмите **Export All** («Экспортировать все»), чтобы экспортировать все файлы.

Раздел 15 AI-Seek

AI-Seek обеспечивает эффективный и точный поиск нужных изображений и видео путем простого ввода соответствующих текстовых описаний.

Перед началом

- Убедитесь, что добавлена камера, поддерживающая AI-Seek, и настроено расписание записи для этой камеры.
- Убедитесь, что настроен поисковый алгоритм AcuSearch. Подробная информация представлена в разделе [AcuSearch](#).

Шаги

1. Перейдите **Event Center** → **Event Configuration** → **Smart Settings** → **Algorithm Management** → **Smart Search** («Центр событий → Конфигурация событий → Интеллектуальные настройки → Управление алгоритмом → Интеллектуальный поиск»), выберите **AI-Seek** и проверьте анализ цели для соответствующих каналов.

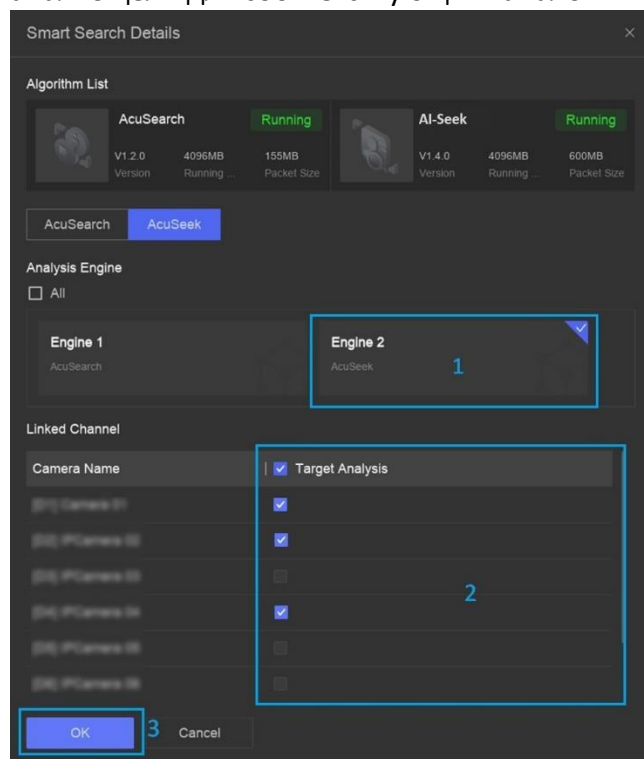


Рисунок 15-1 Конфигурация алгоритма AI-Seek

2. На главной странице графического интерфейса нажмите **AI-Seek** и задайте необходимые условия.

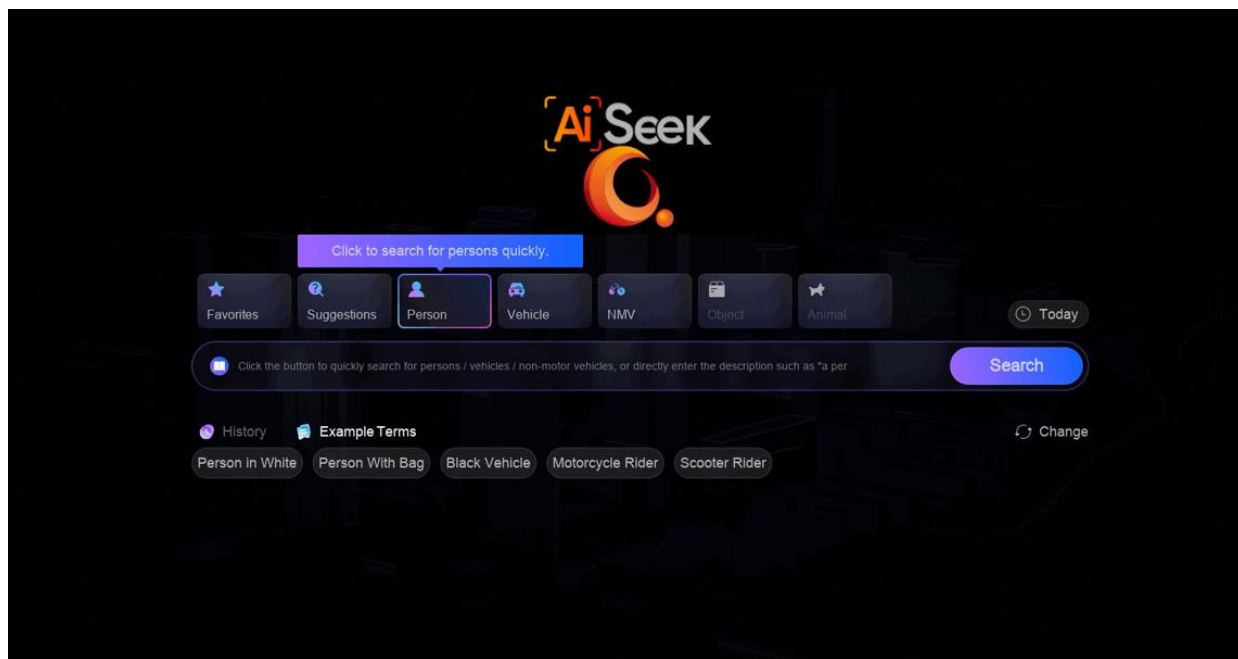



Рисунок 15-2 Настройка условий поиска

- (Рекомендуется) Нажмите **Suggestions** («Предложения»), **Person** («Человек»), **Vehicle** («ТС») или **NMV** и выберите из predetermined условий. При поиске людей и ТС можно выбрать условия по нескольким параметрам. Например, можно искать человека в желтой футболке, синих брюках и шляпе.
 - Введите условие в поле поиска.
 - Нажмите **Favorites** («Избранное»), чтобы выбрать условия из избранного. Можно нажать **Custom** («Пользовательский»), чтобы добавить примеры в избранное.
 - Нажмите **Today** («Сегодня») и укажите время (3 дня, 7 дней, пользовательская настройка) для поиска.
 - Нажмите на условие поиска в истории / пример под полем поиска. Нажмите  для добавления условия поиска в историю в избранное.
- 3.** Нажмите **Search** («Поиск»), чтобы просмотреть результаты поиска и выполнить дополнительные операции в соответствии с рисунком ниже.

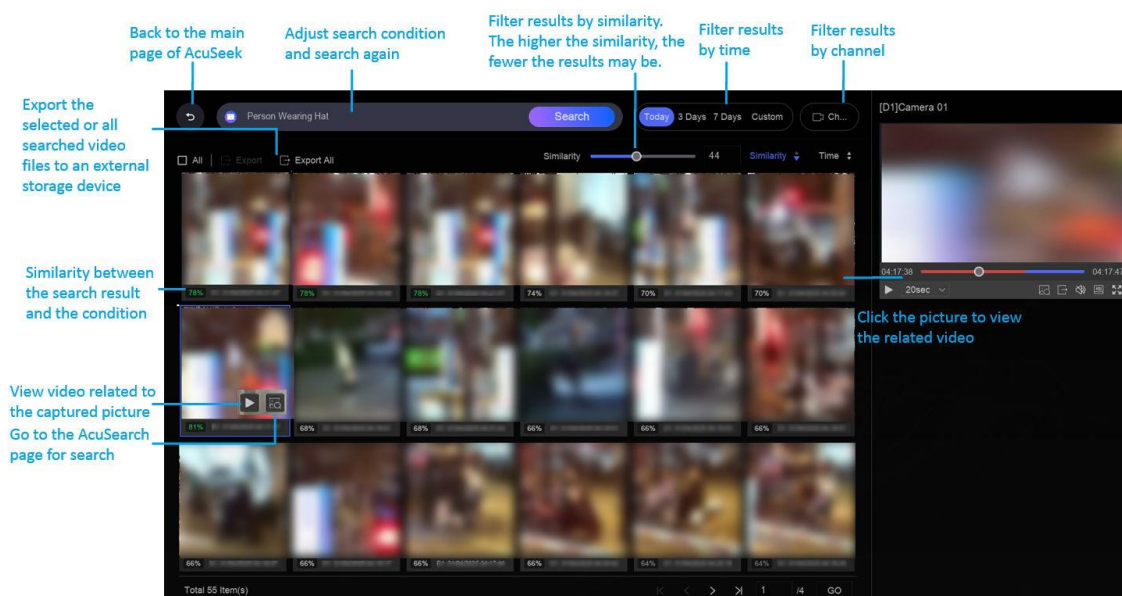


Рисунок 15-3 Результаты AI-Seek

Раздел 16 AcuSearch

Функция AcuSearch сначала извлекает изображения лица или фигуры из видеосцены во время просмотра в режиме реального времени или воспроизведения, затем сравнивает извлеченное изображение с записанными видео и в конечном итоге находит видео, содержащие цель.


Перед началом

Убедитесь, что устройство или камера поддерживают эту функцию.



Шаги

1. Перейдите в **System → Smart Settings → Algorithm Configuration → Algorithm Management** («Система → Интеллектуальные настройки → Конфигурация алгоритма → Управление алгоритмом») для включения алгоритма AcuSearch.

- **ИИ с помощью камеры.** камера выполнит анализ AcuSearch.
- **ИИ в NVR.** анализ AcuSearch будет выполняться устройством, но для этого потребуются ресурсы процессора.

2. Перейдите в режим просмотра в реальном времени или воспроизведения и нажмите на  в нижнем левом углу во время воспроизведения видео.

Примечание

- Если цели трудно найти во время воспроизведения, рекомендуется использовать **Smart Search** («Интеллектуальный поиск») () , чтобы найти сцены, содержащие цели.
- Лицо и фигура человека будут выделены разными цветами.
- После нажатия кнопки , также можно перетащить курсор на изображение, чтобы вручную кадрировать цель или вручную настроить область кадра.

3. Нажмите на  выбранной цели.

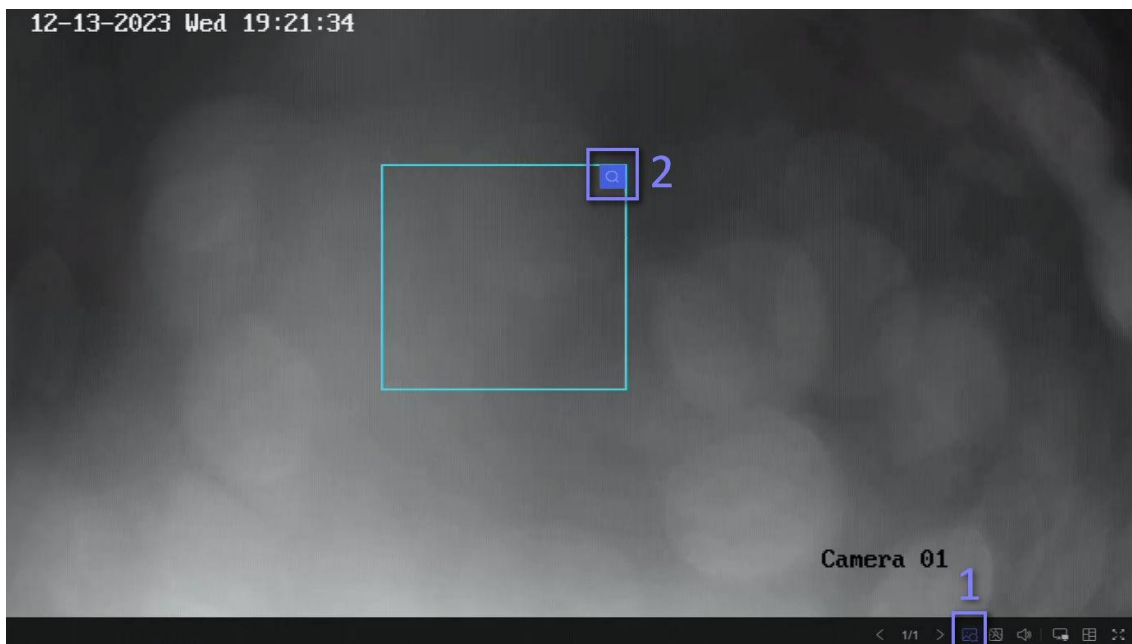


Рисунок 16-1 AcuSearch

Если будут найдены сравниваемые видео, устройство перенаправится в интерфейс AcuSearch.
4. Просмотрите результаты поиска.

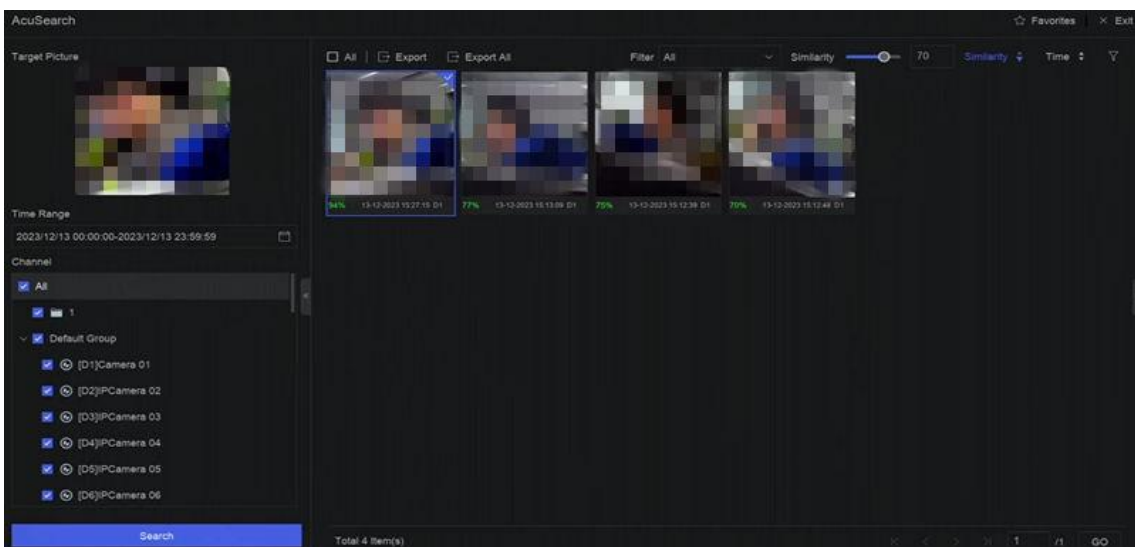


Рисунок 16-2 Результаты AcuSearch

5. **Опционально.** Если результаты не устраивают, можно настроить такие параметры, как **Time Range** («Диапазон времени»), **Channel** («Канал») или **Similarity** («Сходство»), чтобы выполнить поиск еще раз.
6. **Опционально.** Выберите элемент из списка результатов, и соответствующее ему видео будет воспроизведено справа и отмечено красным цветом. Можно нажать на значки на панели инструментов, чтобы выполнить функции.

Раздел 17 Интеллектуальные настройки

17.1 Управление алгоритмами

Алгоритмы используются для анализа различных интеллектуальных функций. Интеллектуальную функцию можно будет использовать после настройки соответствующего алгоритма для процессора.

Перейдите в **System → Event Configuration → Event Configuration → Smart Settings → Algorithm Management** («Система → Конфигурация события → Конфигурация события → Интеллектуальные настройки → Управление алгоритмом») или **Event Center → Event Configuration → Smart Settings → Algorithm Management** («Центр событий → Конфигурация события → Интеллектуальные настройки → Управление алгоритмом»). Доступные алгоритмы будут отображены в списке. Чтобы привязать процессор, нажмите на необходимый алгоритм. Чтобы запустить алгоритм AcuSearch на определенных моделях, которые поддерживают этот алгоритм, можно выбрать камеру (**AI by Camera** («ИИ с помощью камеры»)) или NVR (**AI by NVR** («ИИ с помощью NVR»)).

17.2 Состояние алгоритма

Можно просмотреть состояние устройства, включая состояние работы, температуру и название алгоритма.

Перейдите в **System → Event Configuration → Event Configuration → Smart Settings → Engine Status** («Система → Конфигурация события → Конфигурация события → Интеллектуальные настройки → Состояние алгоритма») или **Event Center → Event Configuration → Smart Settings → Engine Status** («Центр событий → Конфигурация события → Интеллектуальные настройки → Состояние алгоритма»). Подробная информация о переключении алгоритма представлена в разделе [Управление алгоритмом](#).

17.3 Управление планированием задач

Можно просмотреть прогресс выполняемой задачи в центре загрузок. Результаты интеллектуального анализа используются для фильтрации изображений при поиске интересующих изображений фигуры человека и ТС.

Перейдите в **System → Event Configuration → Event Configuration → Smart Settings → Task Plan Management** («Система → Конфигурация события → Конфигурация события → Интеллектуальные настройки → Управление планированием задач») или **Event Center → Event Configuration → Smart Settings → Task Plan Management** («Центр событий → Конфигурация события → Интеллектуальные настройки → Управление планированием задач»). Можно просматривать прогресс выполнения за каждый день для **Non-Real-Time Target Comparison** («Сравнение цели не в режиме реального времени»).

Состояние задачи в основном включает 3 типа: **Disabled** («Отключена»), **Waiting** («Приостановлена») и **Enabled** («Включена»).

Отключено

На камере не включена задача анализа.

Ожидание

Включена задача анализа. Устройство ожидает анализа данных.

Включено

Задача анализа камеры включена, устройство анализирует данные камеры.

17.4 Управление библиотекой списков

Библиотека списков в основном используется для хранения целевых изображений и сравнения целей. **Strangers library** («Библиотека неизвестных лиц») используется для хранения изображений посторонних лиц и не может быть удалена.

17.4.1 Добавление библиотеки списков

Шаги

1. Перейдите в **System** → **Event Configuration** → **Event Configuration** → **Data Archive** → **List Library** («Система → Конфигурация события → Конфигурация события → Архив данных → Библиотека списков») или **Event Center** → **Event Configuration** → **Data Archive** → **List Library** («Центр событий → Конфигурация события → Архив данных → Библиотека списков»).
2. Нажмите **Add** («Добавить»).
3. Введите название библиотеки.
4. Нажмите **Confirm** («Подтвердить»).



Примечание

- После списка библиотеки можно переместить курсор на библиотеку, чтобы отредактировать или удалить ее.
 - Можно нажать **Delete in Batch** («Удалить в пакетном режиме»), чтобы удалить выбранные библиотеки, или очистить все изображения в выбранных библиотеках.
-


17.4.2 Загрузка изображений лиц в библиотеку

Сравнение целевых изображений основано на целевых изображениях в библиотеке. Можно загрузить одно целевое изображение или импортировать несколько целевых изображений в библиотеку.

Перед началом

- Изображения должны быть сохранены в формате JPEG или JPG.
- Заранее импортируйте все изображения на устройство резервного копирования.


Шаги

1. Дважды нажмите на библиотеку списков.
2. **Опционально.** Нажмите **Custom Tag** («Пользовательский тег»), чтобы добавить теги к изображениям. Тег можно редактировать, включая, персональные данные, организацию, должность и т. д.
3. Нажмите **Add** («Добавить») или **Import** («Импортировать»).
4. Импортируйте изображения.
 - **Add** («Добавить»): нажмите , чтобы загрузить изображение. Если на изображении несколько целей, необходимо выбрать одну из них.
 - **Import** («Импортировать»): одновременно можно импортировать несколько изображений. Устройство будет использовать имя файла в качестве имени изображения, при этом остальные атрибуты оставит пустыми или импортирует файлы изображений в соответствии с указанными правилами. Если на изображении есть несколько целей, устройство по умолчанию выберет цель в центре.
5. **Опционально.** Выполните следующие операции.

Удаление изображений из библиотеки

- Выберите изображение и удалите его.
- Выберите изображения и нажмите **Delete in Batch** («Удалить в пакетном режиме»), чтобы удалить выбранные.

Поиск изображений в библиотеке

Нажмите  на панели инструментов, чтобы выполнить поиск изображений.

Копирование изображений в другую библиотеку

Выберите изображения и нажмите **Copy to** («Копировать в»), чтобы скопировать загруженные изображения из текущей библиотеки в другую библиотеку.

Редактировать изображение

Нажмите на название изображения и отредактируйте его атрибуты.

Экспорт изображений

Выберите изображения и нажмите **Export** («Экспорт»), чтобы экспортировать их на USB-накопитель.

17.5 Настройки автоматического обучения

Технология автоматического обучения оптимизирует точность алгоритма и требует минимального вмешательства со стороны пользователей. При включении функции автоматического обучения устройство будет автоматически собирать ложные тревоги и использовать их для постоянного обучения и оптимизации соответствующего алгоритма.

Перейдите в **System** → **Event Configuration** → **Event Configuration** → **Smart Settings** → **Algorithm Management** («Система → Конфигурация события → Конфигурация события → Интеллектуальные настройки → Управление алгоритмом») или **Event Center** → **Event Configuration** → **Smart Settings** → **Algorithm Management** («Центр событий → Конфигурация события → Интеллектуальные настройки → Управление алгоритмом»), чтобы включить

алгоритм автоматического обучения.



Примечание

- Данная функция реализована только у определенных моделей камер.
 - В настоящее время функция автоматического обучения может быть использована только для событий защиты периметра.
 - Если на устройстве установлен только один процессор, необходимо отключить функцию **AI by NVR** («ИИ с помощью NVR»), и анализ обнаруженных целей должен выполняться камерой. Если на устройстве установлено два процессора или больше, можно включить функцию **AI by NVR** («ИИ с помощью NVR») и использовать один из них для анализа обнаруженных целей, а другой использовать для запуска алгоритма автоматического обучения.
-

17.5.1 Управление задачей автоматического обучения

После запуска алгоритма автоматического обучения также должна быть включена задача автоматического обучения.

Перейдите в **System → Event Configuration → Event Configuration → Self-Learning → Task Management** («Система → Конфигурация события → Конфигурация события → Автоматическое обучение → Управление задачей») или **Event Center → Event Configuration → Self-Learning → Task Management** («Центр событий → Конфигурация события → Автоматическое обучение → Управление задачей»), чтобы включить задачу.

Доступная задача будет отображена в списке. Можно просмотреть состояние задачи и индикатор выполнения. Сбор данных займет много времени.

После завершения задачи алгоритм автоматического обучения будет автоматически обновлен.

Можно нажать **Auto Update Config** («Конфигурация автоматического обновления») для настройки **Update Time** («Время обновления»).



Примечание

- В процессе обновления алгоритм автоматического обучения будет недоступен для событий защиты периметра.
 - **Force Training** («Принудительное обучение») используется только для технической поддержки.
-

17.5.2 Управление моделью

Можно установить необходимую версию модели алгоритма автоматического обучения.

Перейдите в **System → Event Configuration → Event Configuration → Self-Learning → Task Management** («Система → Конфигурация события → Конфигурация события → Автоматическое обучение → Управление задачей») или **Event Center → Event Configuration → Self-Learning → Task Management** («Центр событий → Конфигурация события → Автоматическое обучение → Управление задачей»), чтобы включить задачу.

Восстановление предыдущей версии

Восстановление модели до версии, предшествующей этой.

Восстановление версии по умолчанию

Восстановление модели до заводской версии по умолчанию.

17.5.3 Интеллектуальное состояние

Можно просмотреть состояние производительности алгоритма автоматического обучения каждого канала в меню **System → Event Configuration → Event Configuration → Self-Learning → Smart Status** («Система → Конфигурация события → Конфигурация события → Автоматическое обучение → Интеллектуальное состояние») или **Event Center → Event Configuration → Self-Learning → Smart Status** («Центр событий → Конфигурация события → Автоматическое обучение → Интеллектуальное состояние»).

Раздел 18 Центр приложений

18.1 Детекция целей «Человек» и «ТС»

Информация о цели «Человек» / «ТС» будет отображаться для выбранного канала в режиме реального времени.


Обнаружение человека и транспортного средства должно быть настроено заранее. Перейдите **Event Center** («Центр событий») →  для настройки.



Рисунок 18-1 Обнаружение целей «Человек» / «ТС»

Таблица 18-1 Описание обнаружения цели «Человек» / «ТС»

№	Описание
1	Меню быстрого доступа правой кнопкой мыши.
2	Настройки обнаружения человека и ТС. Можно задать макет, подсказку об успешном сравнении и каналы ресурсов.
3	Вход / выход из полноэкранного режима.

18.2 Регистрация сотрудника / посетителя

После добавления задач регистрации можно просматривать информацию о регистрации в режиме реального времени и результаты поиска регистрации.


18.2.1 Добавление задачи регистрации

Перед началом регистрации соответствующая задача должна быть правильно настроена.

Перед началом

- Камера для регистрации подключена правильно.
- Перейдите в **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** («Система → Интеллектуальные настройки → Конфигурация алгоритма → Управление алгоритмом»). Запустите **Target Recognition** («Распознавание цели») как минимум на одном процессоре.
- Список библиотеки для сравнения регистрации настроен правильно. Подробная информация представлена в разделе [Добавление библиотеки списков](#).

Шаги

1. Нажмите **Person Check-In** («Регистрация сотрудника / посетителя»).
2. Нажмите правой кнопкой мыши, чтобы отобразить меню слева.
3. Нажмите .
4. Нажмите **Add** («Добавить»).

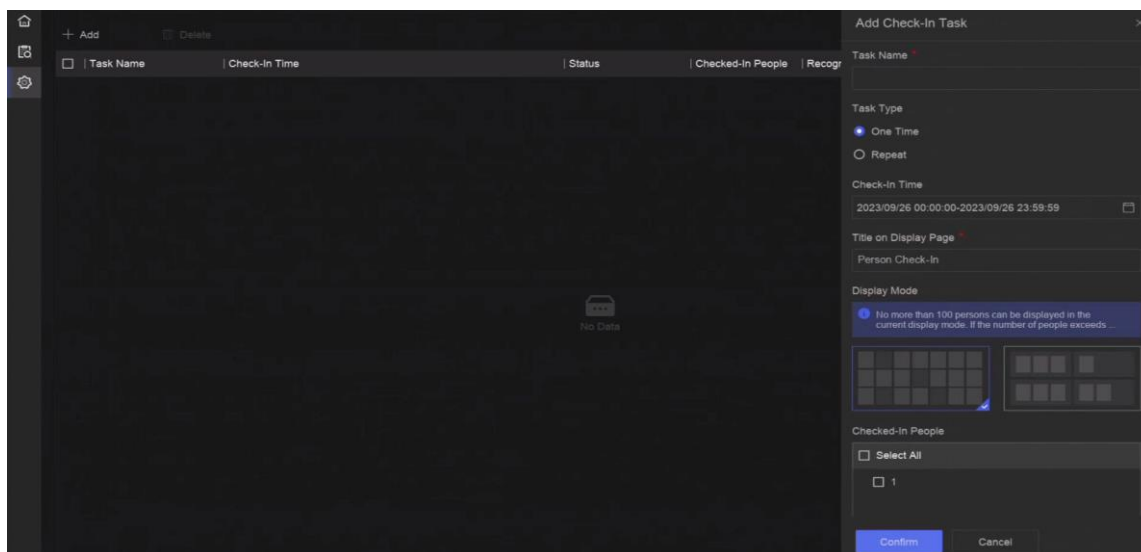


Рисунок 18-2 Добавление задачи регистрации

5. Настройте **Task** («Задача»). **Единоразово**

Задача будет использована один раз.

Повторное воспроизведение

Задача будет использована и повторена несколько раз.

6. Настройте другие параметры, включая **Task Name** («Название задачи»), **Check-In Time** («Время регистрации»), **Recognition Channel** («Канал распознавания») и т. д.
7. Нажмите **Confirm** («Подтвердить»).


18.2.2 Поиск записей регистрации

После настройки задач регистрации можно искать записи по дню или месяцу.

Перед началом

Убедитесь, что задачи регистрации настроены.

Шаги

1. Перейдите в **Person Check-In** («Регистрация сотрудника / посетителя»).
2. Нажмите правой кнопкой мыши, чтобы отобразить меню слева.
3. Нажмите .

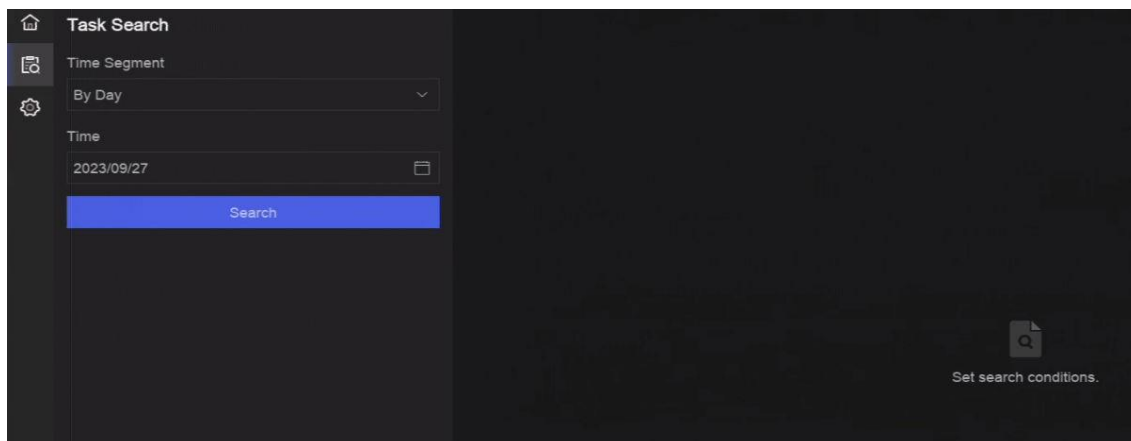




Рисунок 18-3 Поиск записей регистрации

4. Установите время.
5. Нажмите **Search** («Поиск»).

18.3 Статистический отчет

Можно просматривать отчеты о подсчете людей и тепловой карте.

Таблица 18-2 Статистический отчет

Наименование функции	Значок	Условие	Описание
Подсчет людей		<ul style="list-style-type: none"> Функция должна поддерживаться подключенной IP-камерой. Например, к устройству подключена камера с функцией подсчета людей. Статистические данные камеры могут быть сохранены на HDD устройства. 	Подсчет количества сотрудников / посетителей, вошедших, ушедших и прошедших через определенную настроенную область и получение ежедневных / еженедельных / ежемесячных / годовых отчетов для анализа.
Тепловая карта		<ul style="list-style-type: none"> Функция должна поддерживаться подключенной IP-камерой. Статистические данные камеры могут быть сохранены на HDD устройства. 	Тепловая карта представляет собой графическое представление данных, выделенных цветом. Функция тепловой карты используется для анализа количества текущих посетителей и общего количества посетителей в области.

Раздел 19 Настройки системных параметров

Параметры системы включают имя устройства, регион, время, время блокировки экрана, язык и т. д. Перейдите в **System** → **System Settings** → **System Configuration** («Система → Настройки системы → Конфигурация системы»), чтобы настроить параметры.

Таблица 19-1 Описание параметров

Тип	Имя параметра	Описание
Основная информация	Время блокировки экрана	Экран будет заблокирован, если курсор не перемещается в течение указанного времени.
	Разрешение на просмотр в режиме реального времени на экране блокировки	После блокировки экрана устройство будет воспроизводить изображение в режиме реального времени с камер, имеющих это разрешение.
Конфигурация времени и области	Блокировка часового пояса	Для этой операции требуется пароль администратора. После блокировки Time Zone («Часовой пояс») информацию о часовом поясе устройства нельзя изменить удаленно с других платформ или интерфейсов, например, через веб-интерфейс в веб-браузере. Блокировку или разблокировку Time Zone («Часовой пояс») можно осуществить только через локальный графический интерфейс пользователя.
	Режим синхронизации времени	<ul style="list-style-type: none"> • Синхронизация времени с NTP-сервером. Можно выбрать NTP Time Sync («Синхронизация времени с NTP-сервером») и настроить NTP Server («NTP-сервер»), NTP Server Port («Порт NTP-сервера»), NTP Client Port («Порт NTP-клиента») и Interval («Интервал»). Интервал – это интервал времени между двумя действиями синхронизации на сервере NTP. Если устройство подключено к общедоступной сети, следует использовать NTP-сервер с функцией синхронизации времени, например, перечисленные адреса серверов для выбора. Если устройство подключено только к локальной сети, можно использовать ПО NTP, чтобы установить NTP-сервер для синхронизации.

Тип	Имя параметра	Описание
Конфигурация времени и области	Режим синхронизации времени	<ul style="list-style-type: none"> • Синхронизация времени вручную. Вручную установите системное время. • Синхронизация времени с сервером Hik-Connect. Устройство будет синхронизировать время с Hik-Connect вместо NTP-сервера. • Синхронизация времени с сервером Guarding Vision: включите синхронизацию времени, устройство будет синхронизировать время с Guarding Vision вместо NTP-сервера.
	Переход на летнее время	<p>DST (переход на летнее время) относится к периоду, когда часы переводятся на один час вперед. В некоторых регионах мира это приводит к увеличению количества солнечных часов по вечерам в месяцы, когда погода самая теплая.</p> <p>Часы переводят вперед на определенный период (в зависимости от установленной погрешности DST) в начале DST и перемещают назад на тот же период при возвращении к стандартному времени (ST).</p>
Режим вывода меню	Автопереключение дополнительного порта	Когда к задней панели подключены два или более мониторов, один из них может стать вспомогательным выходом, через который невозможно войти в главное меню. Изображения в окнах вспомогательного выхода будут автоматически переключаться на следующие в соответствии с интервалом.
Нулевой канал	-	Нулевой канал, известный как виртуальный канал, может показывать изображения всех каналов устройства в режиме реального времени, что экономит полосу пропускания для передачи.
RS-232	Применение	<p>Консоль</p> <p>После подключения к ПК с помощью преобразователя ПК может устанавливать параметры устройства.</p> <p>Прозрачный канал</p> <p>Напрямую подключен к последовательному устройству. ПК может удаленно получать доступ к последовательному устройству через сеть.</p>

Раздел 20 Резервное копирование устройства горячего резервирования

Видеореги­страторы могут образовывать систему горячего резервирования N + M. Система состоит из нескольких работающих видеореги­страторов и как минимум одного видеореги­стратора горячего резервирования. При выходе из строя работающего видеореги­стратора включается видеореги­стратор горячего резервирования, что увеличивает надежность системы. Двухнаправленное соединение, показанное на рисунке ниже, необходимо установить между видеореги­стратором горячего резерва и работающими видеореги­страторами.



Рисунок 20-1 Создание системы горячего резервирования



Примечание

- Допускается использование до 32 рабочих устройств и 32 устройств горячего резервирования.
- Для целей совместимости рекомендуется использовать все устройства одной модели. Обратитесь к своему продавцу для получения информации о моделях, поддерживающих функцию горячего резервирования.
- Данная функция реализована только у определенных моделей камер.

20.1 Настройка параметров рабочего устройства

Шаги

1. Перейдите в **System** → **System Management** → **N+M Hot Spare** («Система → Управление системой → Горячее резервирование N + M»).
2. Установите режим работы устройства: **Normal Mode** («Обычный режим»).
3. Нажмите **Enable** («Включить»).
4. Нажмите **Save** («Сохранить»).
5. **Опционально.** Просмотрите **Hot Spare Device IP Address** («IP-адрес устройства горячего резервирования») и **Hot Spare Device Working Status** («Рабочее состояние устройства горячего резервирования»).

20.2 Настройка устройств горячего резервирования

Устройство горячего резервирования примет на себя задачи рабочего устройства при выходе из его из строя.

Шаги

1. Перейдите в **System → System Management → N+M Hot Spare** («Система → Управление системой → Горячее резервирование N + M»).
2. Установите режим работы: **Hot Spare Mode** («Режим горячего резервирования»).
3. Нажмите **Save** («Сохранить»). Устройство автоматически перезагрузится.



Примечание

- Соединение с камерой будет отключено, когда устройство работает в режиме горячего резервирования.
- Для корректной работы устройства настоятельно рекомендуется восстановить настройки устройства по умолчанию после переключения режима горячего резервирования в обычный режим.

-
4. Снова перейдите в **System → System Management → N+M Hot Spare** («Система → Управление системой → Горячее резервирование N + M»).
 5. Добавьте рабочие устройства в систему горячего резервирования.
 6. Добавьте устройства горячего резервирования в систему.
 7. Нажмите **Save** («Сохранить»).

Раздел 21 Конфигурация события исключения

События исключений можно настроить так, чтобы они принимали подсказку о событии в интерфейсе просмотра в режиме реального времени и запускали тревожный выход и действия привязки.

Шаги

1. Перейдите в **System** → **System Settings** → **Exception** («Система → Настройки системы → Исключение»).

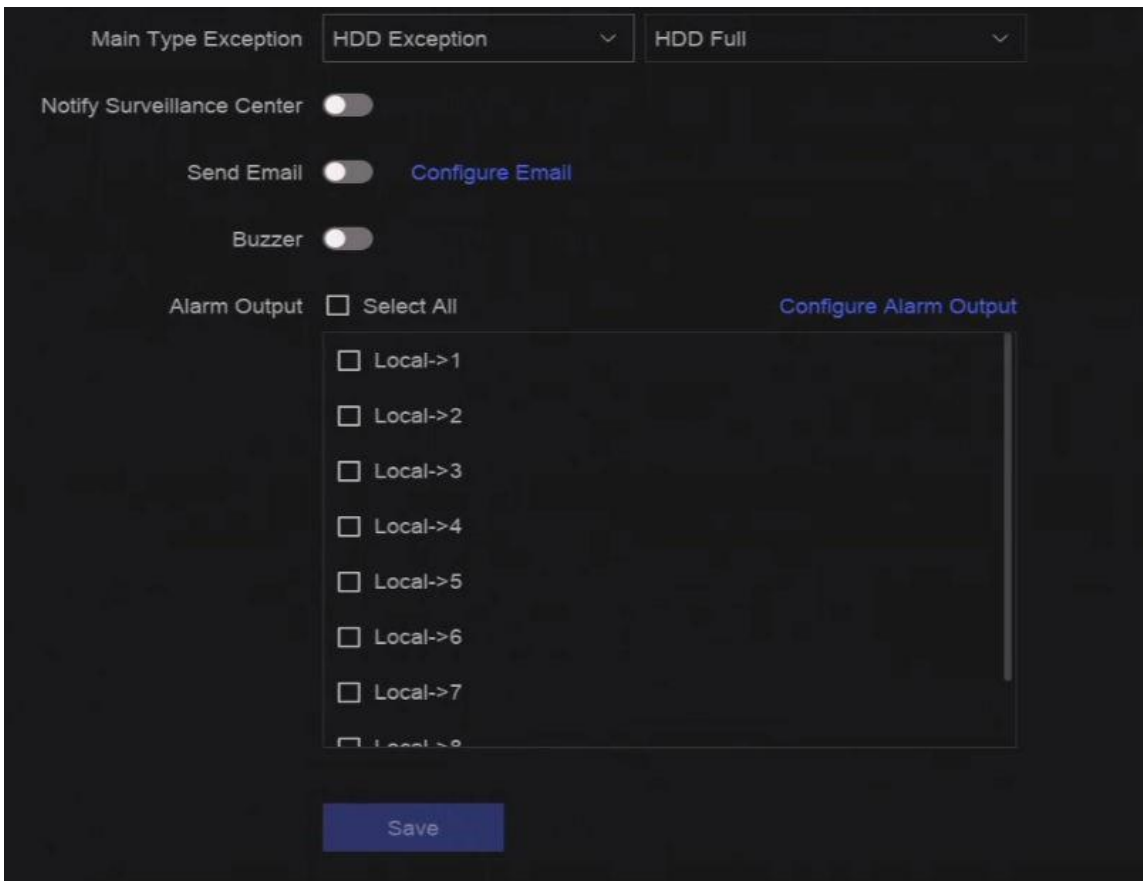




Рисунок 21-1 Конфигурация события исключения

2. Выберите тип исключения.
3. Настройте методы привязки.

Таблица 21-1 Описание привязки

Метод привязки	Описание
Уведомление центра мониторинга	Видеореги­стратор может направить исключение или тревогу на удаленный тревожный хост, когда происходит событие. Тревожный хост относится к ПК, на котором установлено клиентское программное обеспечение (например, iVMS-4200, iVMS-5200).
Бипер	При обнаружении тревоги бипер издаст звуковой сигнал.
Отправка Email	Видеореги­стратор может отправлять электронное письмо с информацией о тревоге пользователю или пользователям.
Тревожный выход	Срабатывание тревожного выхода может быть вызвано обнаружением движения, детектором саботажа, детекцией лиц, обнаружением пересечения линии и любыми другими событиями.

 **Примечание**

При возникновении событий исключения в правом верхнем углу появится уведомление , и можно нажать  для просмотра.

4. Нажмите **Save** («Сохранить»).

Раздел 22 Просмотр информации о системе

Перейдите в **System** → **System Maintenance** → **Running Info** → **System Info** («Система → Обслуживание системы → Информация о запуске → Информация о системе»), чтобы просмотреть системную информацию, включая информацию о записи видео, информацию об HDD, информацию о сети, информацию о потоке просмотра в режиме реального времени или воспроизведения видео, информацию о диагностике синхронизации времени и т. д.

Например, когда происходит исключение синхронизации времени и батарея RTC (таблеточного типа) разряжена, это может повлиять на запись или воспроизведение видео, поэтому необходимо устранить исключение как можно скорее.

Раздел 23 Обслуживание системы

Функции обслуживания системы включают поиск в журнале, запланированную перезагрузку, обновление и т. д.

23.1 Перезагрузка по расписанию

Устройство автоматически перезапустится по расписанию.

Перейдите в **System → System Maintenance → Maintenance → Schedule Reboot** («Система → Обслуживание системы → Обслуживание → Перезагрузку по расписанию»), чтобы включить функцию, и установите расписание перезагрузки.

23.2 Обновление устройства

Систему устройства можно обновить с помощью локального USB-накопителя, удаленного FTP-сервера и т. д.

Перейдите в **System → System Maintenance → Maintenance → Upgrade** («Система → Обслуживание системы → Обслуживание → Обновление»), чтобы обновить устройство.

23.3 Резервное копирование и восстановление

Перейдите в **System → System Maintenance → Maintenance → Backup and Restore** («Система → Обслуживание системы → Обслуживание → Резервное копирование и восстановление»), чтобы восстановить или создать резервную копию системных параметров.

Импорт / экспорт файла настройки

Файлы конфигурации устройства можно экспортировать на локальное устройство для резервного копирования. Файлы конфигурации одного устройства можно импортировать на несколько устройств, если для них настроены одинаковые параметры.

Простое восстановление

Восстановите все параметры, кроме сети, включая IP-адрес, маску подсети, шлюз, MTU, рабочий режим NIC, маршрут по умолчанию, порт сервера и т. д., и параметры учетной записи пользователя, до заводских настроек по умолчанию.

Заводские установки

Восстановление всех параметров до заводских настроек.

Восстановление устройства до неактивного состояния

Верните устройство в неактивное состояние и оставьте все настройки без изменений, кроме восстановления учетных записей пользователей.

23.4 Информация о журнале

Перейдите в **System → System Maintenance → Maintenance → Log** («Система → Обслуживание системы → Обслуживание → Журнал») для поиска и экспорта информации журнала.

Настройки времени окончания

Когда диск журнала заполнен, более старые журналы будут перезаписаны.

23.5 Настройка сервера журналов

При необходимости можно загрузить системные журналы на сервер для резервного копирования.

Шаги

1. Перейдите в **System → CX → System Settings → Network → Network → Log Server** («Система → CX → Настройки системы → Сеть → Сеть → Сервер журнала»).
2. Нажмите **Enable** («Включить»).
3. Настройте время загрузки, IP-адрес сервера и порт.
4. **Опционально.** Нажмите **Test** («Проверить»), чтобы проверить правильность параметров.
5. Нажмите **Save** («Сохранить»).

23.6 Инструменты для ТО

Для обслуживания системы предусмотрено множество инструментов, таких как S.M.A.R.T-обнаружение и функция обнаружения неисправного сектора.

Перед началом

Убедитесь, что жесткий диск установлен правильно.

Шаги

1. Перейдите в **System → System Maintenance → Maintenance → Maintenance Tools** («Система → Обслуживание системы → Обслуживание → Инструменты обслуживания»).
2. Выберите необходимые инструменты.

Таблица 23-1 Описание инструментов

Название инструмента	Описание
Мониторинг сетевых данных	Мониторинг сетевых данных — это процесс просмотра, анализа и управления сетевыми данными для любых отклонений или процессов, которые могут повлиять на производительность сети, доступность или безопасность.
Захват сетевых пакетов	Пинг Ping-тест используется для определения доступности IP-адреса назначения. Захват пакетов на уровне сетевого интерфейса После получения видеорегиcтpатором доступа к сети можно использовать USB-накопитель для захвата и экспорта сетевого пакета.
Определение состояния жесткого диска	Здесь можно просмотреть состояние Seagate HDD от 4 ТБ до 8 ТБ, созданного после 1 октября 2017 г. Используйте эту функцию для устранения сбоев HDD. Функция обнаружения статуса показывает более подробную информацию о статусе HDD, чем функция S.M.A.R.T.-обнаружения.
S.M.A.R.T.-обнаружение Детекция	S.M.A.R.T. (Технология самоконтроля, анализа и отчета) — это система мониторинга жесткого диска, позволяющая обнаруживать и сообщать о различных показателях надежности в целях предупреждения возникновения ошибок.
Обнаружение неисправного сектора	Если жесткий диск содержит слишком много поврежденных секторов, рекомендуется заменить жесткий диск, в противном случае файлы на жестком диске могут быть утеряны.
Клонирование HDD	Скопируйте данные с жесткого диска на другой через интерфейс eSATA.

**Примечание**

Рекомендуется использовать инструменты обслуживания с помощью технической поддержки.

23.7 Конфигурация функции плавного отключения питания

Функция плавного отключения питания доступна только для устройств с тревожными выходами POWER-AC (исключение питания переменного тока), POWER-UPS (исключение ИБП) и POWER-UPSL (низкая мощность ИБП) (на задней панели). Устройство может принимать и записывать эти тревоги. При срабатывании тревоги POWER-AC и POWER-UPSL устройство автоматически отключится в соответствии с заданным временем. Если тревога POWER-AC или POWER-UPSL не срабатывает, устройство автоматически включится.

Шаги

1. Перейдите в **System → System Maintenance → Maintenance → Soft Power Off Configuration** («Система → Обслуживание системы → Обслуживание → Конфигурация плавного отключения питания»).

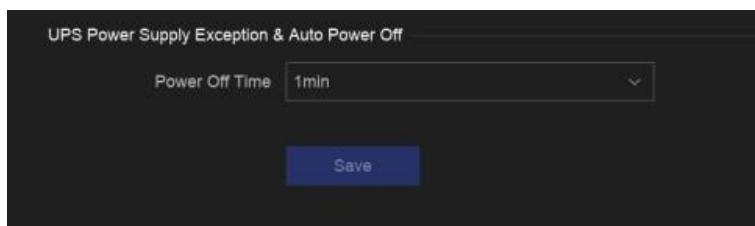


Рисунок 23-1 Конфигурация функции плавного отключения питания

2. Настройте **Power Off Time** («Время отключения питания»). Устройство автоматически отключится по истечении заданного времени при срабатывании соответствующих тревог.
3. Нажмите **Save** («Сохранить»).

Пример

Например, если **Power Off Time** («Время отключения питания») установлено на **1 минуту**, то при срабатывании тревог POWER-AC (исключение питания переменного тока) и POWER-UPS1 (низкая мощность ИБП) устройство автоматически выключится через 1 минуту.

Раздел 24 Управление безопасностью

24.1 Фильтрация IP-адресов

Фильтрация адресов позволяет разрешить или запретить доступ к устройству с определенного IP- / MAC-адреса.

Перед началом

Войдите в систему с учетной записью администратора.

Шаги

1. Перейдите в **System → System Maintenance → Security Management → Address Filter** («Система → Обслуживание системы → Управление безопасностью → Фильтр адресов»).
2. Нажмите **Enable** («Включить»).
3. Установите **Filtering Type** («Тип фильтрации»). Выберите фильтрацию по IP-адресу или MAC-адресу.
4. Установите **Restriction Type** («Тип ограничения»). Механизм устройства разрешит или запретит доступ к устройству с определенного IP- / MAC-адреса.
5. **Опционально.** Настройте **Restriction List** («Список ограничений»). Здесь можно добавлять, редактировать и удалять адреса.
6. Нажмите **Save** («Сохранить»).

24.2 Шифрование потока

После включения шифрования потока для удаленного просмотра в режиме реального времени, удаленного воспроизведения и загруженных видео потребуется ключ шифрования.

Шаги

1. Перейдите в **System → System Maintenance → Security Management → Stream Encryption** («Система → Обслуживание системы → Управление безопасностью → Шифрование потока»).
2. Нажмите **Enable** («Включить»).
3. Настройте **Encryption Key** («Ключ шифрования»).



Примечание

Ключ шифрования потока синхронизируется с проверочным кодом службы Hik-Connect. После активации кода шифрования поток Hik-Connect будет принудительно зашифрован.

4. Нажмите **Save** («Сохранить»).

24.3 Выбор версии TLS

Настройки TLS действуют для HTTP(S) и расширенной службы SDK. Это обеспечивает безопасность потоковой передачи. Перейдите в **System → System Maintenance → Security Management → TLS** («Система → Обслуживание системы → Управление безопасностью → TLS») для выбора версии TLS.

Раздел 25 Приложение

25.1 Список совместимых адаптеров питания

Используйте только те адаптеры питания, которые указаны в списке.

Модель адаптера питания	Спецификации	Производитель
ADS-26FSG-12 12024EPG	12 В, 2 А	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 В, 3.33 А	MOSO Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 В, 1.5 А	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, AC от 100 до 240 В, 12 В, 1.5 А, 18 Вт, $\Phi 5.5 \times 2.1 \times 10$	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 В, 1.5 А	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	AC от 100 до 240 В, 12 В, 1.5 А, 18 Вт, $\Phi 5.5 \times 2.1 \times 10$	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 В, 2 А	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, AC от 100 до 240 В, 12 В, 2 А, 24 Вт, $\Phi 2.1$	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 В, 2 А	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 В, 2 А	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 В, 3.33 А, 40 Вт	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 В, 3.33 А	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 В, 1.36 А	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 В, 1.04 А	0000203078 Channel Well Technology Co., Ltd.

25.2 Список терминов и сокращений

Двойной поток

Двойной поток — это технология, используемая для локальной записи видео высокого разрешения при передаче потока с более низким разрешением по сети. Два потока генерируются DVR, причем основной поток имеет максимальное разрешение 1080P, а дополнительный поток — максимальное разрешение CIF.

DVR

Акроним от **Digital Video Recorder** («Цифровой видеореги­стратор»). Цифровой видеореги­стратор — это устройство, которое может принимать видеосигналы от аналоговых камер, сжимать сигнал и сохранять его на своих жестких дисках.

HDD

Акроним от **Hard Disk Drive** («Жесткий диск»). Носитель данных, который хранит их в цифровом виде на пластинах с магнитными поверхностями.

DHCP

Протокол динамической настройки узла (DHCP) — это протокол сетевого приложения, используемый устройствами (клиентами DHCP) для получения информации о конфигурации для работы в IP-сети.

HTTP

Акроним от **Hypertext Transfer Protocol** («Протокол передачи гипертекста»). Протокол для передачи гипертекстовых запросов и информации между серверами и браузерами по сети.

PPPoE

Протокол PPPoE представляет собой сетевой протокол для инкапсуляции кадров PPP через Ethernet. Он используется в основном с услугами ADSL, когда отдельные пользователи подключаются к приемопередатчику ADSL (модему) через Ethernet и в простых сетях Metro Ethernet.

DDNS

Динамический DNS — это метод, протокол или сетевая служба, которые предоставляют возможность сетевому устройству, например, маршрутизатору или компьютерной системе, использующей Internet Protocol Suite, уведомлять сервер доменных имен об изменениях, предоставлять информацию в режиме реального времени об активных DNS-настройках имен хоста, адресов или другой информации, хранящейся в DNS.

Гибридный DVR

Гибридный DVR сочетает в себе функции DVR и NVR.

NTP

Акроним от **Network Time Protocol** («Протокол сетевого времени»). Протокол предназначен для синхронизации часов компьютеров по сети.

NTSC

Акроним от **National Television System Committee** («Национальный комитет по телевизионным системам»). NTSC — это стандарт аналогового телевидения, используемый в таких странах, как США и Япония. Каждый кадр сигнала NTSC состоит из 525 строк развертки при 60 Гц.

NVR

Акроним от **Network Video Recorder** («Сетевой видеореги­стратор»). Сетевым видеореги­стратором может быть ПК или встроенная система, используемая для централизованного управления и хранения IP-камер, купольных IP-камер и других цифровых видеореги­страторов.

PAL

Акроним от **Phase Alternating Line** («Построчное изменение фазы»). PAL также является еще одним видеостандартом, используемым в системах теле­вещания во многих частях мира. Сигнал PAL состоит из 625 строк развертки при 50 Гц.

PTZ

Акроним от **Pan, Tilt, Zoom** («Поворот, наклон, масштабирование»). PTZ-камеры — это моторизированные системы, которые позволяют камере поворачиваться влево и вправо, наклоняться вверх и вниз, а также увеличивать и уменьшать масштаб.

USB

Акроним от Universal Serial Bus («Универсальная последовательная шина»). USB — это стандарт последовательной шины с функцией plug-and-play для подключения устройств к главному компьютеру.

25.3 Часто задаваемые вопросы

25.3.1 Почему на некоторых каналах отображается сообщение No Resource («Ресурсы отсутствуют») или экран становится черным при просмотре в режиме реального времени на нескольких экранах?

Причина

1. Неверные настройки разрешения дополнительного потока или битрейта.
2. Ошибка подключения к дополнительному потоку.

Решение

1. Перейдите в меню **Camera → Video Parameters → Sub-Stream** («Камера → Параметры видео → Дополнительный поток»). Выберите канал и уменьшите разрешение и макс. битрейт (разрешение должно быть меньше 720р, макс. битрейт меньше 2048 Кбит/с).



Примечание

Если видеореги­стратор не поддерживает эту функцию, вы можете войти в систему и настроить параметры видео через веб-интерфейс.

2. Настройте разрешение дополнительного потока и макс. битрейт (разрешение должно быть меньше 720р, максимальный битрейт должен быть меньше 2048 Кбит/с), затем удалите канал и снова добавьте его.

25.3.2 Почему при добавлении IP-камеры видеореги­стратор сообщает о ненадежности пароля?

Причина

Пароль камеры слишком слабый.

Решение

Измените пароль камеры.



Предупреждение

РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ – Настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

25.3.3 Почему не поддерживается уведомление о типе потока с видеореги­стратора?

Причина

Формат кодирования камеры не соответствует формату видеореги­стратора.

Решение

Если камера использует H.265 / MJPEG для кодирования, но видеореги­стратор не поддерживает H.265 / MJPEG, измените формат кодирования камеры на подходящий для видеореги­стратора.

25.3.4 Как подтвердить, что видеореги­стратор использует H.265 для записи видео?

Решение

Убедитесь, что тип кодирования на панели инструментов просмотра в реальном времени — H.265.

25.3.5 Почему видеореги­стратор сообщает о конфликте IP-адресов?

Причина

Видеореги­стратор использует IP-адрес, который уже используется другими устройствами.

Решение

Измените IP-адрес видеореги­стратора. Убедитесь, что IP-адрес не используется другими устройствами.

25.3.6 Почему изображение зависает при воспроизведении одноканальной или многоканальной камерой?

Причина

Ошибка чтения / записи HDD.

Решение

Экспортируйте видео и воспроизводите его на других устройствах. Если на другом устройстве видео воспроизводится нормально, замените HDD и повторите попытку.

25.3.7 Почему устройство не может управлять PTZ-камерой через протокол Coaxitron?

Причина

1. Камера не поддерживает протокол Coaxitron.
2. Протокол Coaxitron работает неверно.
3. На сигнал влияет волоконно-оптический передатчик.

Решение

1. Убедитесь, что входной видеосигнал — HDTVl, а камера поддерживает протокол Coaxitron.
2. Убедитесь, что параметры протокола Coaxitron верны, например скорость передачи данных и адрес.
3. Отсоедините волоконно-оптический передатчик и повторите попытку.

25.3.8 Почему PTZ-камера не реагирует на команды через RS-485?

Причина

1. Кабель RS-485 подключен неправильно.
2. Интерфейс RS-485 неисправен.
3. Неправильный протокол управления.

Решение

1. Проверьте, правильно ли подключен кабель RS-485.
2. Измените интерфейс RS-485 и повторите попытку.
3. Убедитесь, что используется протокол управления Pelco.

25.3.9 Почему качество звука видео плохое?

Причина

1. Снижение качеств звука при передаче через микрофон.
2. Помехи при передаче.
3. Параметры аудио некорректны.

Решение

1. Проверьте работу микрофона. Замените микрофон и попробуйте еще раз.
2. Проверьте линию передачи звука. Убедитесь, что все линии надежно соединены или закреплены и отсутствуют электромагнитные помехи.
3. Отрегулируйте громкость звука в соответствии с окружающей средой и параметрами микрофона.

25.4 Уведомление о наличии агрессивного газа

В помещении, не являющемся центром обработки данных, рекомендуется соблюдать предельную концентрацию агрессивных газов в соответствии с требованиями стандарта IEC 60721-3-3:2002 по уровню химического активного вещества 3C2.

Таблица 25-1 Пределъная концентрация агрессивных газов

Категория агрессивных газов	Среднее значение (мг/м ³)	Максимальное значение (мг/м ³)
SO ₂ (диоксид серы)	0.3	1.0
H ₂ S (сероводород)	0.1	0.5
Cl ₂ (хлор)	0.1	0.3
HCl (хлороводород)	0.1	0.5
HF (фтороводород)	+0.01	0.03
NH ₃ (аммиак)	1.0	3.0
O ₃ (озон)	0.05	0.1
NO _x (оксиды азота)	0.5	1.0

 **Примечание**

- Средние значения, приведенные в таблице выше, являются типичными контрольными значениями для агрессивных газов в среде серверного помещения. Не рекомендуется, чтобы концентрация агрессивных газов превышала среднее значение.
- Максимальное значение относится к предельному или пиковому значению. Время, в течение которого концентрация агрессивных газов достигает максимального значения, не должно превышать 30 минут в день.

Таблица 25-2 Общие категории и источники агрессивных газов

Категория	Первоисточник
H ₂ S (сероводород)	Геотермальные выбросы, микробиологическая активность, производство нефти, коррозия древесины, очистка сточных вод и т. д.
SO ₂ (диоксид серы), SO ₃ (триоксид серы)	Сжигание угля, нефтепродуктов, автомобильных выхлопов, плавка руды, производство серной кислоты, сжигание табака и т. д.
S (сера)	Литейные цеха, производство серы и т. д.
HF (фтороводород)	Производство удобрений, производство алюминия, керамики, стали, электронного оборудования, сжигание полезных ископаемых и т. д.
NO _x (оксиды азота)	Автомобильные выхлопы, сжигание нефти, микробиологическая активность, химическая промышленность и т. д.
NH ₃ (аммиак)	Микробиологическая активность, сточные воды, производство удобрений, геотермальные выбросы и т. д.
CO (угарный газ)	Горение, автомобильные выхлопы, микробиологическая активность, гниение деревьев и т. д.
Cl ₂ (хлор), ClO ₂ (диоксид хлора)	Производство хлора, производство алюминия, производство цинка, разложение отходов и т. д.
HCl (хлороводород)	Автомобильные выхлопные газы, продукты сгорания, лесные пожары, сгорание полимерных отходов и т. д.
HBr (бромистоводородная кислота), HI (йодистоводородная кислота)	Автомобильные выхлопы и т. д.
O ₃ (озон)	Атмосферные оптические процессы (в основном включающие оксид азота и пероксид водорода) и т. д.
C _n H _n (алкан)	Автомобильные выхлопы, табачная гарь, отходы животноводства, сточные воды, гниение деревьев и т. д.

