

FOCUS

IP-камеры

**Руководство
пользователя**

Введение

Благодарим Вас за приобретение устройства нашей компании. В случае возникновения каких-либо вопросов или пожеланий убедительно просим Вас обращаться к нашему представителю / дилеру.

Данное Руководство относится к IP-камерам и служит справочным пособием для Вашей операционной системы. В этом руководстве Вы сможете найти информацию о применении функций устройства, а также подробное описание меню. Все фотографии, рисунки, значки и другие данные, приведенные в Руководстве, носят только информационный характер. Они могут отличаться от используемых в конкретных продуктах – ориентируйтесь на Интерфейс управления Вашей камеры. Тщательно ознакомьтесь с информацией, содержащейся в данном руководстве, перед установкой и использованием системы.

Руководство может содержать технические неточности или опечатки, а его содержимое может быть изменено без предварительного уведомления. Все обновления будут добавляться в новые версии данного Руководства. Мы с готовностью улучшим или обновим продукты или процедуры, описанные в Руководстве.

Перед использованием устройства

Для получения инструкций, прикладных инструментов и другой информации посетите наш Веб-сайт (www.focus-cctv.ru).

Проверьте оборудование перед использованием. Подробная информация о способах щадящей настройки приведена в разделе 8.2.1 «Настройка системы» ② «Настройки времени».

Ограничение правовой ответственности

- Компания не несет ответственности за причинение вреда здоровью Вашим сотрудникам или третьим лицам, а также за потерю имущества в случае, если устройство будет повреждено или перестанет работать по какой-либо из указанных ниже причин: ① Установка и использование устройства не в строгом соответствии с инструкциями; ② В целях поддержания государственного порядка или в общественных интересах; ③ В силу обстоятельств непреодолимой силы (форс-мажор); ④ Ваши личные или сторонние причины (включая, но не ограничиваясь, использованием продуктов, программного обеспечения или компонентов производства сторонних производителей).
- Наша компания никогда не давала гарантий на использование продукции в ненадлежащих или незаконных целях. Данное устройство не может использоваться в качестве медицинского оборудования, средств безопасности или в других целях, где оборудование может представлять опасность или привести к травмам. Убытки или ответственность, вызванные вышеуказанным использованием, Вы должны компенсировать самостоятельно.
- При корректной установке и использовании данное устройство может обнаруживать незаконное проникновение, но не может предотвратить несчастные случаи, травмы персонала или материальный ущерб, вызванные этими ситуациями. Будьте внимательны в повседневной жизни, повышайте свою осведомленность о безопасности.
- Наша компания не несет ответственности за любые косвенные, случайные, специальные или штрафные убытки, иски, материальный ущерб или любую потерю данных или файлов. В максимально допустимых законом пределах компенсация нашей компании не превышает суммы, потраченной Вами на приобретение данного устройства.

Инструкции по технике безопасности

Данное Руководство предназначено для того, чтобы пользователь мог надлежащим образом использовать устройства без опасности для себя или риска потери имущества. Внимательно ознакомьтесь с Руководством, а также приложите все усилия для получения дополнительной

информации по этим вопросам. Как указано ниже, меры безопасности подразделяются на предупреждения и предостережения.

Предупреждения («ПРЕДУПРЕЖДЕНИЕ!»): Несоблюдение любого из этих предупреждений может повлечь за собой смерть или серьезный вред здоровью.

Предостережения («ОСТОРОЖНО»): Несоблюдение любого из этих предостережений может повлечь за собой ущерб здоровью или повреждение оборудования.

	ПРЕДУПРЕЖДЕНИЕ! Соблюдайте эти меры предосторожности, чтобы избежать смерти или серьезных травм.		ОСТОРОЖНО! Соблюдайте эти меры, чтобы предотвратить возможные травмы или потерю имущества.
---	--	---	--



ПРЕДУПРЕЖДЕНИЕ!

- При монтаже и использовании устройств необходимо строго соблюдать правила электробезопасности, действующие в стране и регионе.
- Используйте подходящий адаптер питания от надежного производителя.
- Не подключайте несколько IP-камер к одному адаптеру питания (перегрузка адаптера может привести к перегреву или пожару).
- Отключайте питание при проведении подключения или демонтажа устройства. Не работайте при включенном питании.
- В случае монтажа устройства на стене или под потолком оно должно быть надежно закреплено.
- При появлении дыма, неприятного запаха или шума, исходящих от IP-камеры, немедленно отключите питание и отсоедините сетевой кабель, а затем обратитесь к дилеру или в сервисный центр.
- Если IP-камера работает некорректно, обратитесь к локальному дилеру оборудования или в сервисный центр. Не пытайтесь самостоятельно разбирать или модифицировать устройство (наша компания не несет ответственности за проблемы, вызванные несанкционированным ремонтом или техническим обслуживанием устройства).



ОСТОРОЖНО!

- Перед использованием камеры убедитесь в наличии корректного напряжения питания.
- Не роняйте на устройство посторонние предметы и не подвергайте его сильной вибрации, а также не храните устройство в местах наличия магнитных помех. Избегайте установки камер в таких местах, где поверхность выбириует или подвергается ударам (игнорирование этого может привести к повреждению устройства).
- Не направляйте объектив фотокамеры на источники яркого света, такие как солнце или лампы накаливания. Попадание яркого света на объектив может привести к безвозвратному повреждению камеры.
- Не подвергайте предназначенные для использования внутри помещений IP-камеры воздействию дождя или высокой влажности.
- Храните устройства в сухом месте, без угрозы возникновения коррозии, вдали от прямых солнечных лучей, в хорошо проветриваемых помещениях и вдали от источников тепла, таких как обогреватели или калориферы (игнорирование этого требования может привести к пожару).
- Во избежание повреждения IP-камер не устанавливайте их в местах, где присутствуют сажа или же водяные пары, в условиях слишком высоких температур или высокой запыленности.

- Чтобы избежать ожогов, не прикасайтесь непосредственно к теплоотводному радиатору устройства.
- При очистке камеры от загрязнений протирайте её корпус мягкой тканью. При очистке используйте сухую ткань. В случае если грязь удалить сложно, устройство можно протереть нейтральным моющим средством. Не используйте для мытья щелочные чистящие средства. Если на линзе объектива скопилась пыль, протрите ее специальной бумагой для протирки оптических стёкол.
- Устройства, подключаемые к сети Интернет, могут сталкиваться с проблемами сетевой безопасности. Усильте защиту личной информации и данных. Если Вы обнаружите, что устройство может подвергаться угрозам сетевой безопасности, своевременно свяжитесь с нашими специалистами.
- Помните, что Вы несете ответственность за корректную настройку всех паролей и других связанных с ними параметров безопасности устройства, а также за хранение Вашего имени пользователя и пароля в надежном месте.
- Храните оригинальную упаковку устройства надлежащим образом, чтобы в случае возникновения проблем использовать её для упаковки устройства и отправки его нашему представителю.

ПРИМЕЧАНИЕ: Полное наименование устройства «IP-камера» для краткости иногда заменяется на «IPC».

Оглавление

Глава 1. Описание устройства	7
1.1. Руководство по эксплуатации устройства	7
1.2. Характеристики устройства	7
Глава 2. Инструкции по эксплуатации	9
2.1. Подключение к сети	9
2.1.1. Доступ в Интернет по проводным сетям	9
2.1.2. Беспроводной доступ в Интернет	9
2.2. Определение и изменение IP-адреса.....	10
2.3. Настройка IP-камеры по ГВС.....	11
2.3.1. Подключение с использованием статического IP-адреса.....	11
2.3.2. Подключение с использованием динамического IP-адреса	12
Глава 3. Доступ к IP-камере с помощью клиентского программного обеспечения	14
Глава 4. Доступ к IP-камере с помощью веб-клиента	15
4.1. Подготовка перед установкой плагина	15
4.2. Вход в систему и выход из нее	15
4.2.1. Вход в систему.....	15
4.2.2. Изменение пароля.....	16
4.2.3. Если Вы забыли пароль	18
4.2.4. Выход из системы	21
4.3. Установка элементов управления IP-камерой LsIPCPlugin	21
4.4. Описание главного окна	25
Глава 5. Просмотр видео в реальном времени.....	27
5.1. Просмотр видео в реальном времени	27
Глава 6. Воспроизведение изображения.....	29
Глава 7. Получение снимков	32
Глава 8. Настройка	33
8.1. Локальная настройка	33
8.2. Система.....	34
8.2.1. Настройка системы	34
8.2.2. Безопасность	35
8.3. Сеть	38

8.1.3.	Основные настройки	38
8.2.3.	P2P	45
8.3.3.	Настройка передачи сообщений по электронной почте	48
8.4.	Видео	50
8.4.1.	Видео.....	50
8.4.2.	Звук.....	51
8.5.	Изображение	52
8.5.1.	Изображение.....	52
8.5.2.	Экранное OSD-меню	57
8.6.	События	58
8.6.1.	Обычные события	58
8.6.2.	Интеллектуальные события	72
8.7.	Хранение данных.....	85
8.7.1.	Настройка расписания	85
8.7.2.	Управление хранением данных	90
Глава 9.	Обслуживание устройства.....	93
9.1.	Информация об устройстве	93
9.2.	Обновление оборудования	93
9.3.	Возврат параметров устройства к заводским настройкам.....	94
9.4.	Автоматическое обслуживание	94
9.5.	Импорт и экспорт.....	95
9.6.	Ведение журналов.....	95
Глава 10.	Часто задаваемые вопросы	97

Глава 1. Описание устройства

1.1. Руководство по эксплуатации устройства

IP-камера - это интегрированное устройство сбора видео- и звуковых данных, интеллектуального кодирования и передачи их по сети, включает в себя также другие функции устройств цифрового мониторинга. В ней используется встроенная операционная система и высокопроизводительная аппаратная платформа обработки данных с высокой стабильностью и надежностью, предназначенные для удовлетворения разнообразных потребностей отрасли.

IP-камера, разработанная с возможностью управления через сеть Ethernet и сжатия изображения, позволяет передавать его по сети различным пользователям.

Для управления IP-камерой Вы можете использовать браузер или клиентское ПО, через браузер – задавать параметры IP-камеры, такие как настройки системных параметров, экранного меню и другие параметры. С помощью браузера или клиентского программного обеспечения можно также запускать такие функции как обнаружение движения, нештатных ситуаций обнаружение и другие интеллектуальные функции, для которых имеются собственные специфичные параметры (учтывайте при этом особенности конкретного устройства).

1.2. Характеристики устройства

В этом разделе представлен список функций веб-камер, который позволит Вам лучше ознакомиться с этими устройствами.

■ Системные функции

- Функции записи видео и захвата снимков**

IP-камера поддерживает функцию записи видео и захвата снимков. Чтобы настроить расписание ведения записи и захвата снимков с целью достижения необходимых результатов, Вы также можете установить карту памяти или настроить сетевой диск хранения данных.

- Управление правами пользователей**

Через профиль системного администратора («admin») и Вы можете управлять несколькими разными пользователями и настраивать разные права для каждого из них.

- Воспроизведение видеозаписи**

Для воспроизведения видео, обработки запросов и хранения данных используются TF-карты или SD-карты.

■ Функция обнаружения событий

IP-камера поддерживает обработку обычных и интеллектуальных событий.

- Обычные события**

Обычные события включают: обнаружение движения, настройку зон конфиденциальности, обнаружение закрытия объектива, обнаружение нештатных ситуаций, ввод / вывод тревог, вывод звукового сигнала тревоги и настройку зон интереса.

- Интеллектуальные события**

Интеллектуальные события включают: обнаружение вторжения, обнаружение пересечения линии, обнаружение подозрительного поведения и скопления людей.

■ **Интернет-функции**

IP-камера поддерживает TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, RTP, RTSP, NTP, SMTP, UDP, TCP, DNS, DDNS и другие сетевые коммуникационные протоколы; поддерживает ONVIF2.4, CGI, соглашения основных производителей и другие интернет-протоколы.

■ **Дополнительные функции**

- **Функция Wi-Fi**

С помощью камеры с функцией Wi-Fi можно реализовывать беспроводное подключение к точке доступа маршрутизатора Wi-Fi или беспроводное подключение к сетевому видеорегистратору NVR. С помощью камеры с функцией Wi-Fi поддерживающей точки Wi-Fi доступа к мобильному телефону, можно просматривать видео с IP-камеры в режиме реального времени.

- **Функция облачного хранения**

IP-камера поддерживает функцию облачного хранения, которая позволяет сохранять на облачном сервере записи устройства за весь день и информацию о сигналах тревоги при обнаружении движения.



ПРИМЕЧАНИЕ:

- Указанные выше характеристики IP-камер зависят от конкретной модели, ознакомьтесь с фактическими техническими особенностями Вашего устройства.

Глава 2. Инструкции по эксплуатации

2.1. Подключение к сети



ОСТОРОЖНО!

Если Вы осуществляете доступ в сеть Интернет на свой страх и риск, включая, но не ограничиваясь тем, что устройство может быть подвержено сетевым атакам, хакерским атакам, заражению вирусами, наша компания не гарантирует отсутствия сбоев в работе устройства, раскрытия информации и других проблем, но мы своевременно предоставим Вам информацию по технической поддержке устройства.

После установки IP-камеры Вы сможете просмотреть и настроить соответствующие функциональные параметры через браузер.

2.1.1. Доступ в Интернет по проводным сетям

Перед настройкой IP-камеры убедитесь в том, что она подключена к компьютеру и что Вы можете получить доступ к IP-камере, которую хотите настроить. Существует два типа проводных подключений. Вы можете напрямую подключить IP-камеру к компьютеру с помощью сетевого кабеля, как показано на рисунке 2-1.



Рисунок 2-1

Или же Вы можете подключить IP-камеру к локальной сети через коммутатор или маршрутизатор, как показано на рисунке 2-2.



Рисунок 2-2

2.1.2. Беспроводной доступ в Интернет

Некоторые IP-камеры поддерживают передачу данных по беспроводной сети. Подключение IP-камеры к компьютеру по беспроводной сети показано на рисунке 2-3.



Рисунок 2-3

2.2. Определение и изменение IP-адреса

Чтобы получить доступ к IP-адресу IP-камеры, выполните следующие действия.

Шаг 1: Найдите IP-адрес IP-камеры.

- Используя «Search tool (Инструмент поиска)», Вы сможете выполнить поиск по всем онлайн-камерам в локальной сети и отобразить их IP-адрес, MAC-адрес, версию, порт и другую информацию о камерах, как показано на рисунке 2-4.

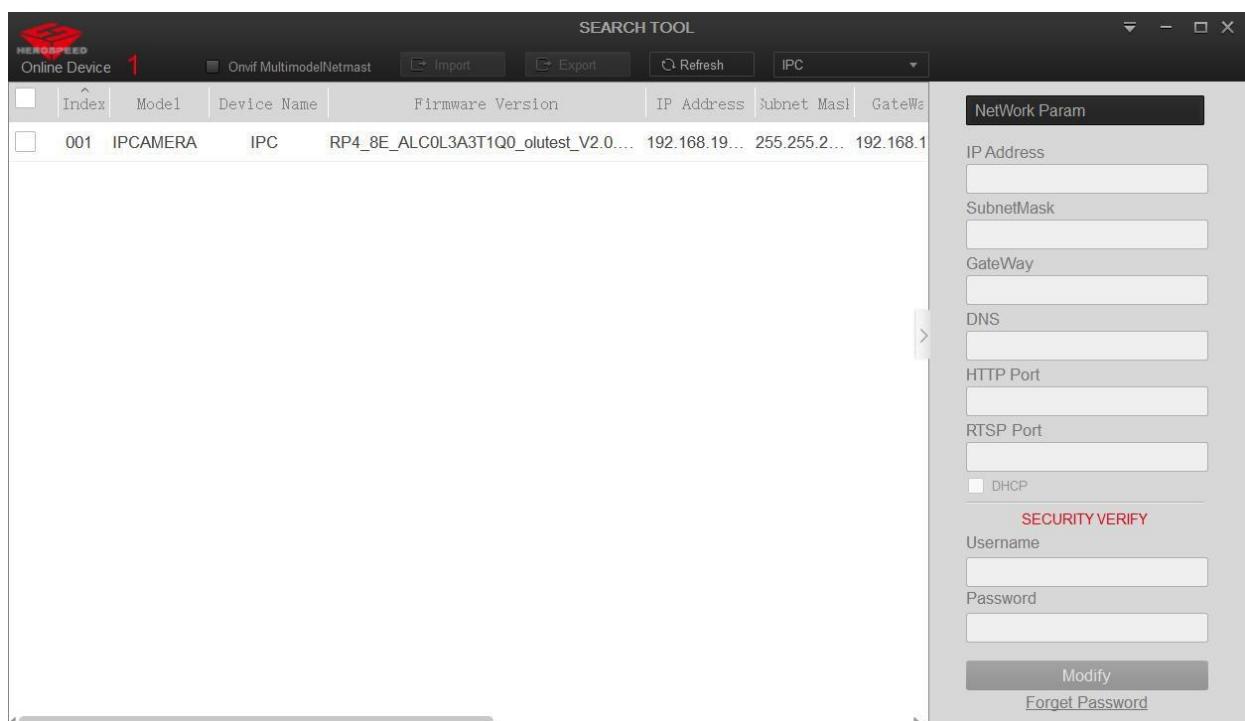


Рисунок 2-4

- Используйте клиентское программное обеспечение iVMS320 для поиска подключенных к сети устройств. Более подробную информацию смотрите в Руководстве пользователя для iVMS320.

Шаг 2: Измените IP-адрес IP-камеры и подключите компьютер к тому же сегменту сети.

- В Инструменте поиска выберите устройство для изменения IP-адреса, в правой части окна непосредственно измените IP-адрес и шлюз, введите пароль и нажмите на «Modify (Изменить)».

Шаг 3: Откройте браузер, чтобы ввести IP-адрес камеры, перейдите в окно входа в систему (login).



ПРИМЕЧАНИЕ:

- При настройке IP-адреса IP-камеры, сохраняйте IP-адрес устройства и IP-адрес компьютера в одном сегменте локальной сети.
- По умолчанию: IP-адрес - 192.168.1.168, номер порта - 80. Имя пользователя администратора по умолчанию - «admin», а пароль - «admin». Настоятельно рекомендуется изменить первоначальный пароль после первого входа в систему.
- Чтобы получить доступ к IP-камерам в различных подсетях, установите шлюз IP-камеры после входа в систему. Дополнительная информация приведена в разделе 8.3.1 «Основные настройки» → «Настройка протокола TCP/IP».

2.3. Настройка IP-камеры по ГВС

В этом разделе даны указания о том, как подключить IP-камеру к глобальной сети со статическим или динамическим IP-адресом.

2.3.1. Подключение с использованием статического IP-адреса

Перед тем как начать

Укажите статический IP-адрес от интернет-провайдера (Internet Service Provider). Используя статический IP-адрес, Вы можете подключить IP-камеру через маршрутизатор или напрямую к глобальной сети.

➤ Подключение маршрутизатора к IP-камере показано на рисунке 2-5.

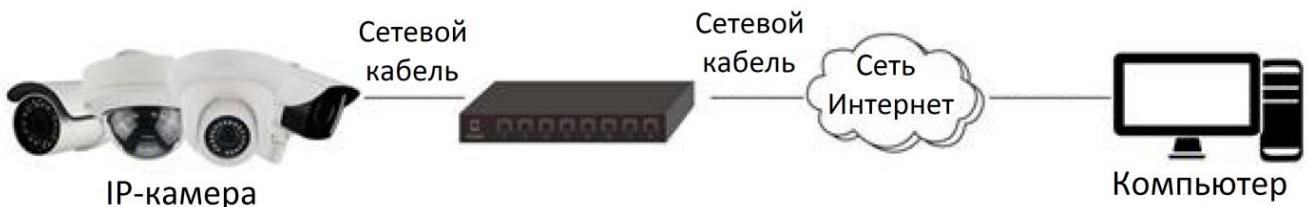


Рисунок 2-5

Выполните следующие действия:

Шаг 1: Подключите IP-камеру к маршрутизатору.

Шаг 2: Задайте IP-адрес локальной сети, маску подсети и шлюз. Подробная информация приведена в разделе 8.3.1.

Шаг 3: Сохраните статический IP-адрес в маршрутизаторе.

Шаг 4: Выполните назначение портов, например, порты 80, 8000 и 554. Шаги по назначению портов различаются в зависимости от конкретного роутера. При назначении портов обращайтесь к производителю маршрутизатора за помощью.

Шаг 5: Подключитесь к IP-камере по сети Интернет через веб-браузер или клиентское программное обеспечение.

- Непосредственное подключение к IP-камере через статическое IP-соединение показано на рисунке 2-6.

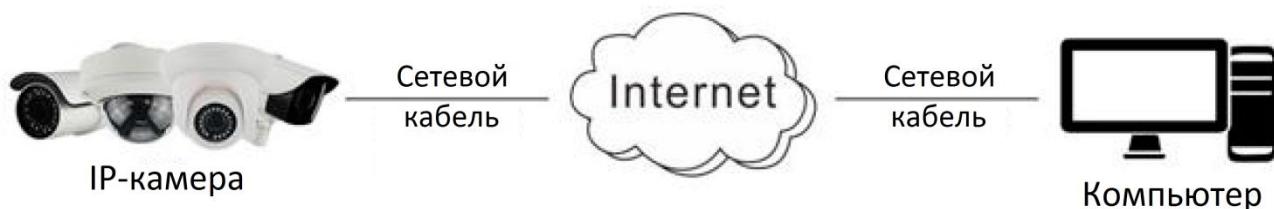


Рисунок 2-6

Вы также можете сохранить статический IP-адрес в камере и напрямую подключить ее к сети Интернет без использования маршрутизатора. Подробная информация приведена в разделе 8.3.1.

2.3.2. Подключение с использованием динамического IP-адреса

Перед тем как начать

Получите динамический IP-адрес от интернет-провайдера. Используя динамический IP-адрес, Вы можете подключить IP-камеру к модему или маршрутизатору.

- Подключение маршрутизатора к IP-камере.

Выполните следующие действия:

Шаг 1: Подключите IP-камеру к маршрутизатору.

Шаг 2: Задайте IP-адрес локальной сети, маску подсети и шлюз. Подробная информация приведена в разделе 8.3.1.

Шаг 3: В роутере задайте имя пользователя PPPoE, введите пароль и подтвердите его.

Шаг 4: Выполните назначение портов, например, порты 80, 8000 и 554. Шаги по назначению портов различаются в зависимости от конкретного роутера. При назначении портов обращайтесь к производителю маршрутизатора за помощью.

Шаг 5: Получите доменное имя у поставщика доменных имен.

Шаг 6: Настройте параметры DDNS в окне настройки маршрутизатора.

Шаг 7: Подключитесь к камере, используя выбранное доменное имя.



ПРИМЕЧАНИЕ:

- Полученный IP-адрес присваивается динамически с помощью PPPoE, поэтому после перезагрузки камеры IP-адрес всегда меняется. Чтобы устранить неудобства, связанные с динамическим IP, Вам необходимо получить доменное имя у провайдера DDNS (например, DynDns.com). Чтобы решить эту проблему, выполните следующие действия по назначению обычных и частных доменных имен.

➤ Процесс назначения обычных доменных имен показан на рисунке 2-7.

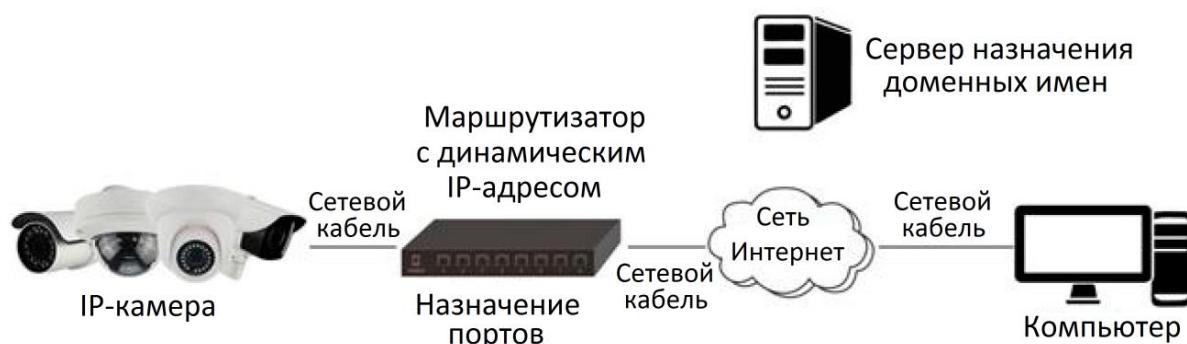


Рисунок 2-7

Выполните следующие действия:

Шаг 1: Получите доменное имя у поставщика доменных имен.

Шаг 2: Настройте параметры DDNS в окне настроек DDNS IP-камеры. Подробная информация приведена в разделе 8.3.2.

Шаг 3: Подключитесь к камере, используя выбранное доменное имя.

➤ Процесс назначения частных доменных имен показан на рисунке 2-8.

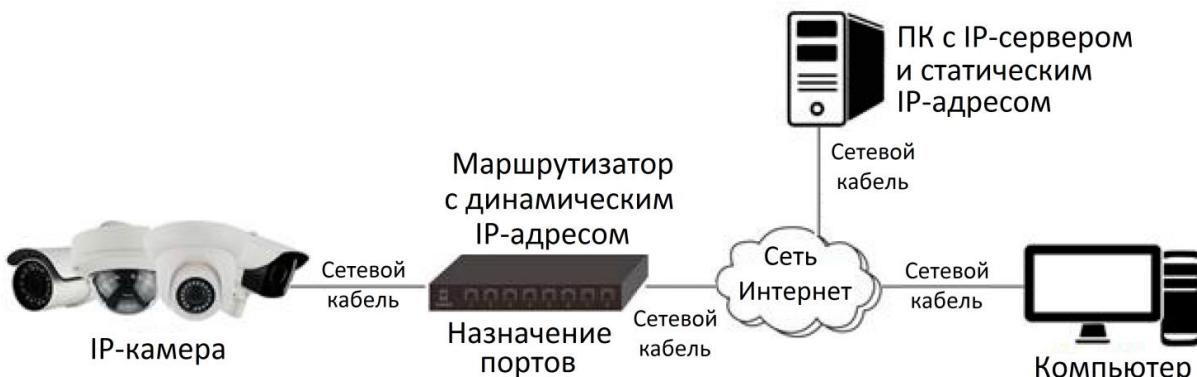


Рисунок 2-8

Выполните следующие действия:

Шаг 1: Установите и запустите программное обеспечение IP-сервера на компьютере со статическим IP-адресом.

Шаг 2: Получите доступ к IP-камере через локальную сеть с помощью веб-браузера или клиентского программного обеспечения.

Шаг 3: Включите DDNS и выберите в качестве типа протокола «IP Server (IP-сервер)». Подробная информация приведена в разделе 8.3.2.

Глава 3. Доступ к IP-камере с помощью клиентского программного обеспечения

Клиентское ПО iVMS320 доступно на веб-сайте компании (www.focus-cctv.ru). Вы можете использовать это программное обеспечение для просмотра видео в реальном времени и управления IP-камерой. Чтобы установить программное обеспечение, следуйте инструкциям по установке. Панель управления и окно просмотра в режиме реального времени клиентского ПО iVMS320 показаны на рисунке 3-1.

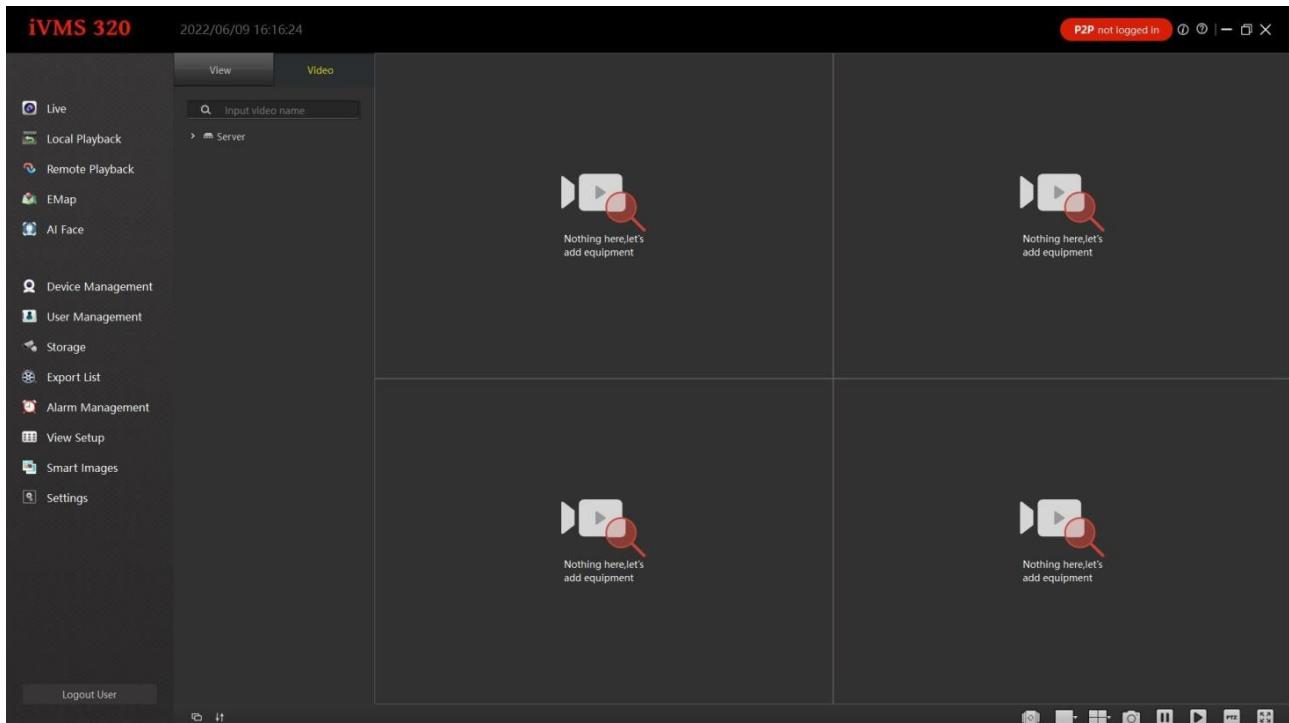


Рисунок 3-1



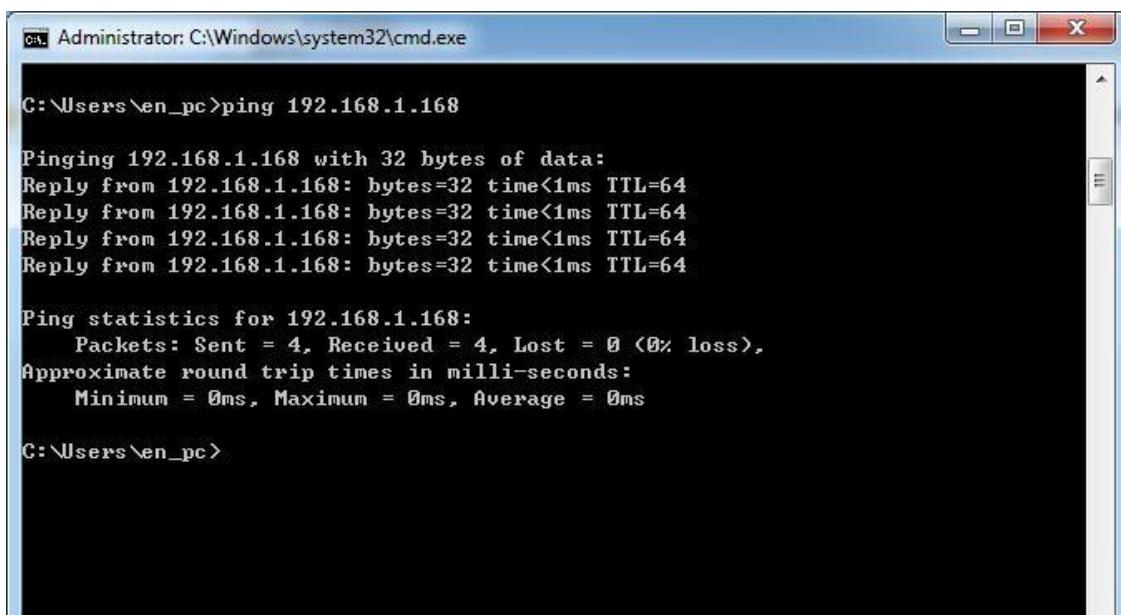
ПРИМЕЧАНИЕ:

- Для получения подробной информации о программном обеспечении, обратитесь к руководству пользователя клиентского программного обеспечения iVMS320.

Глава 4. Доступ к IP-камере с помощью веб-клиента

4.1. Подготовка перед установкой плагина

Для обеспечения нормальной работы IP-камеры и компьютера текущего пользователя – после завершения всех аппаратных подключений и подключения питания оборудования – включите компьютер и запустите проверку IP-адреса IP-камеры. (ПРИМЕЧАНИЕ: IP-адрес IP-камеры в локальной сети должен быть уникальным). Например, если IP-адрес IP-камеры – 192.168.1.168, запустите для проверки 192.168.1.168. Если сетевая IP-камера отвечает так, как показано на рисунке 4-1, это означает, что сетевое подключение в норме, и Вы можете открыть браузер для входа на веб-страницу веб-камеры.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\en_pc>ping 192.168.1.168

Pinging 192.168.1.168 with 32 bytes of data:
Reply from 192.168.1.168: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.168:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\en_pc>
```

Рисунок 4-1

4.2. Вход в систему и выход из нее

4.2.1. Вход в систему

Чтобы вызвать окно входа в систему, как показано на рисунке 4-2, откройте браузер на Вашем компьютере и введите IP-адрес IP-камеры в строке веб-адреса (адрес по умолчанию, используемый в первый раз: <http://192.168.1.168>).

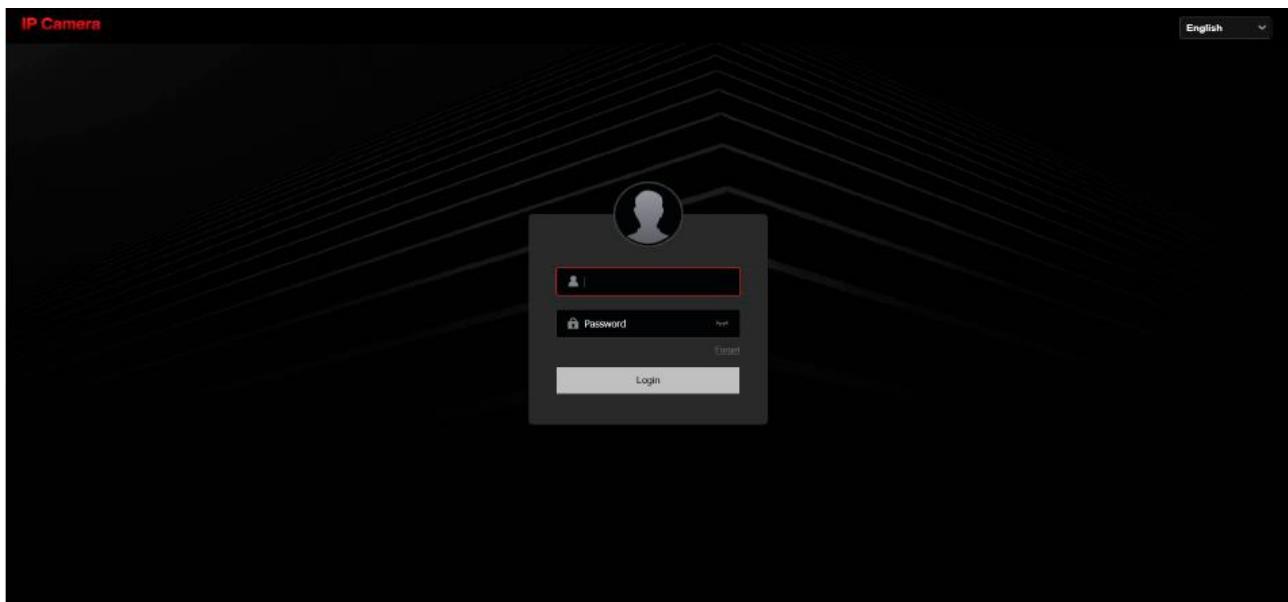


Рисунок 4-2

Выберите системный язык: (поддерживаются следующие языки: Simplified Chinese (Упрощенный китайский), Traditional Chinese (Традиционный китайский), English (Английский), Russian (Русский), Korean (Корейский), Polish (Польский), French (Французский), Japanese (Японский), Spanish (Испанский), Portuguese (Португальский), Italian (Итальянский), Hebrew (Иврит), Turkish (Турецкий), Bulgarian (Болгарский), Arabic (Арабский), German (Немецкий), Dutch (Голландский), Czech (Чешский), Vietnamese (Вьетнамский)). Введите имя пользователя (по умолчанию «admin») и пароль (по умолчанию «admin»). Нажмите на «Login (Войти)».



ПРИМЕЧАНИЕ:

- Если Вы изменили IP-адрес IP-камеры, войдите в систему с новым заданным Вами IP-адресом.

4.2.2. Изменение пароля

После успешного входа в систему появится окно-приглашение изменить пароль (см. рисунок 4-3).

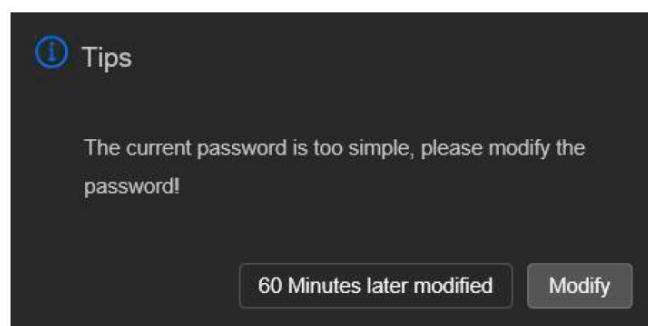


Рисунок 4-3

Чтобы ознакомиться с рекомендациями по безопасности учетной записи, нажмите на «Modify (Изменить)» и войдите в пользовательский интерфейс изменения пароля, как показано на рисунке 4-4.

Users to edit

Old Password	
User Name	admin
User Type	Admin
Password	

Confirm Password	
The length of the password is 8 to 31 digits, and only two or more combinations of numbers, lowercase letters, uppercase letters, and special characters (~!@#\$%^&*-+=;.,/?) can be used	
<input checked="" type="checkbox"/> Do you want to set a new security question	
Security issue1	
Answer1	
Security issue2	
Answer2	
Security issue3	
Answer3	
key export	
OK	

Рисунок 4-4

Чтобы изменить свой пароль, выполните следующие действия.

Шаг 1: Введите старый и задайте новый пароль в полях «Old Password (Старый пароль)» - «Confirm Password (Подтвердите пароль)».

Шаг 2: Настройте секретные вопросы 1, 2 и 3 и введите релевантные ответы на них.

Шаг 3: Чтобы сохранить файл ключа на Вашем компьютере, нажмите на «Key export (Экспорт ключа)».

Шаг 4: Чтобы завершить процесс смены пароля, нажмите на «Save (Сохранить)».



ПРИМЕЧАНИЕ:

- Для успешной установки нового пароля необходимо ввести не менее 8 символов, которые должны содержать как буквы, так и цифры.

- Если исходным паролем IP-камеры является пароль «admin», то при каждом новом входе в систему Вам будет предлагаться изменить его. Вы можете выбрать опцию «After 60 Minutes later modified (Изменить пароль через 60 минут)». Через 60 минут в окне автоматически появится всплывающее окно изменения пароля.

4.2.3. Если Вы забыли пароль

Если Вы забыли свой пароль, Вы можете сбросить его двумя способами: с помощью секретного вопроса или же ключа безопасности.

Проверка с помощью секретного вопроса

Шаг 1: В окне входа в систему нажмите на «Forget (Забыт)».

Шаг 2: Выберите метод проверки «Security question validation (Проверка с помощью секретного вопроса)» (как показано на рисунке 4-5 ①), введите ответы на секретные вопросы 1, 2 и 3, нажмите на «Next (Далее)».

Рисунок 4-5 ①

Шаг 3: Введите новый пароль и подтвердите его (как показано на рисунке 4-5 ②), затем нажмите на «Next (Далее)».

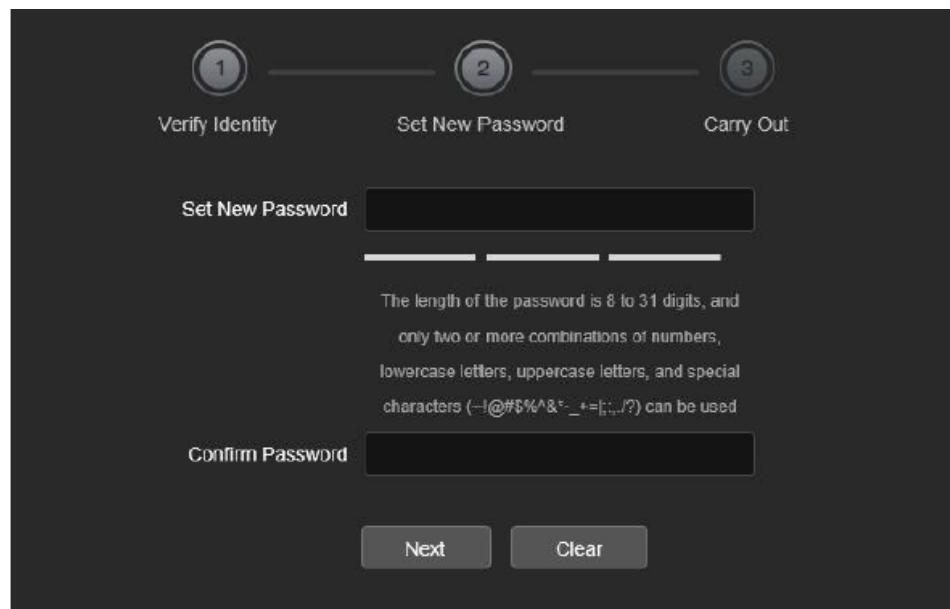


Рисунок 4-5 (2)

Шаг 4: Нажмите на «Re-login (Повторно войти)», чтобы вернуться в окно входа в систему (как показано на рисунке 4-5 (3)).

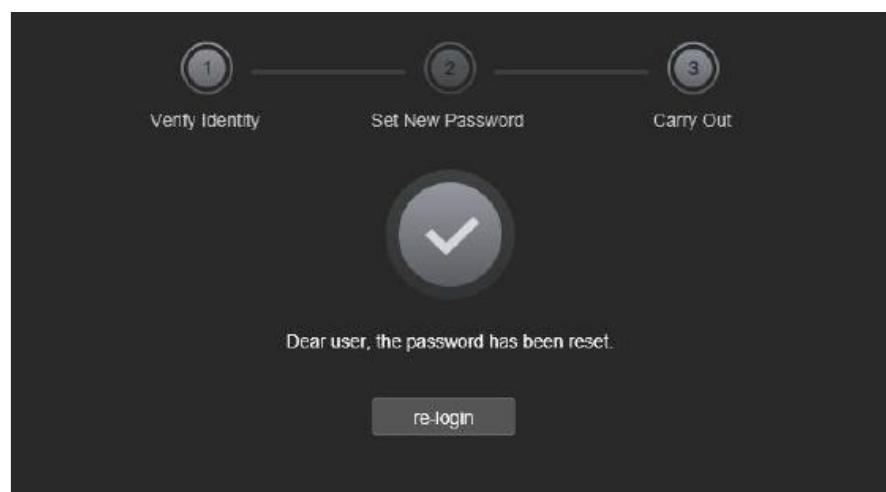


Рисунок 4-5 (3)

Проверка с помощью ключа безопасности

Шаг 1: В окне входа в систему нажмите на «Forget (Забыт)».

Шаг 2: Выберите метод проверки «Security Key Verification» (Проверка с помощью ключа безопасности) (как показано на рисунке 4-6 (1)), и нажмите «Import (Импортировать)» чтобы импортировать файл ключа, экспортенный при изменении пароля.

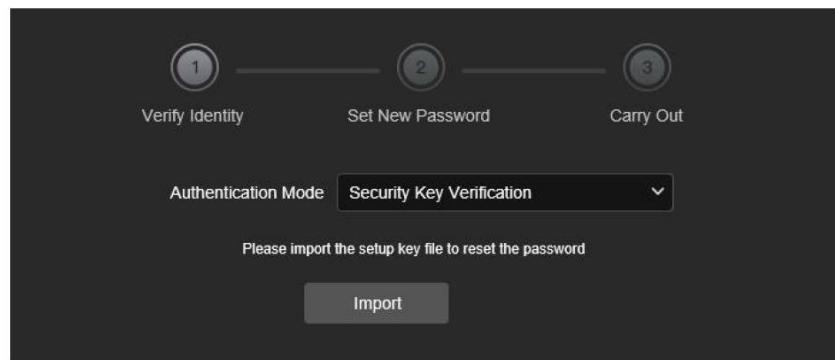


Рисунок 4-6 (1)

Шаг 3: Введите новый пароль и подтвердите его (как показано на рисунке 4-6 (2)), затем нажмите на «Next (Далее)».

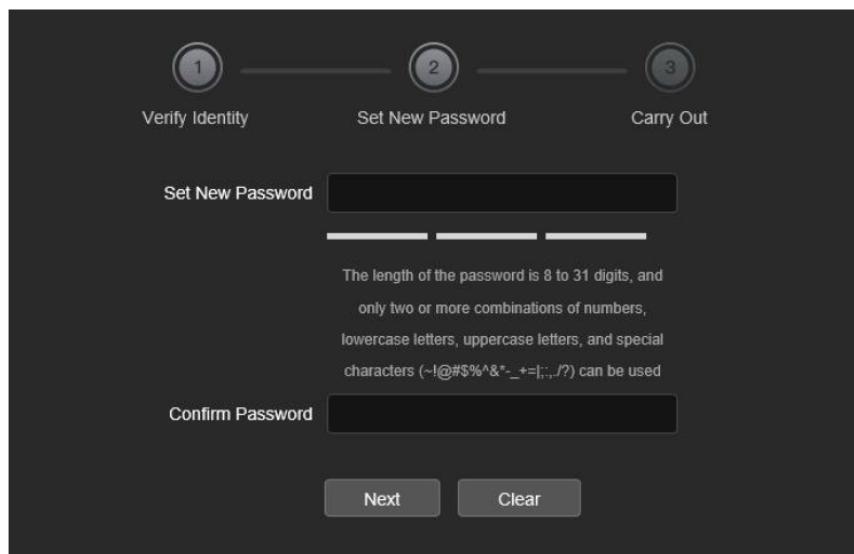


Рисунок 4-6 (2)

Шаг 4: Нажмите на «Re-login (Повторно войти)», чтобы вернуться в окно входа в систему (как показано на рисунке 4-6 (3)).

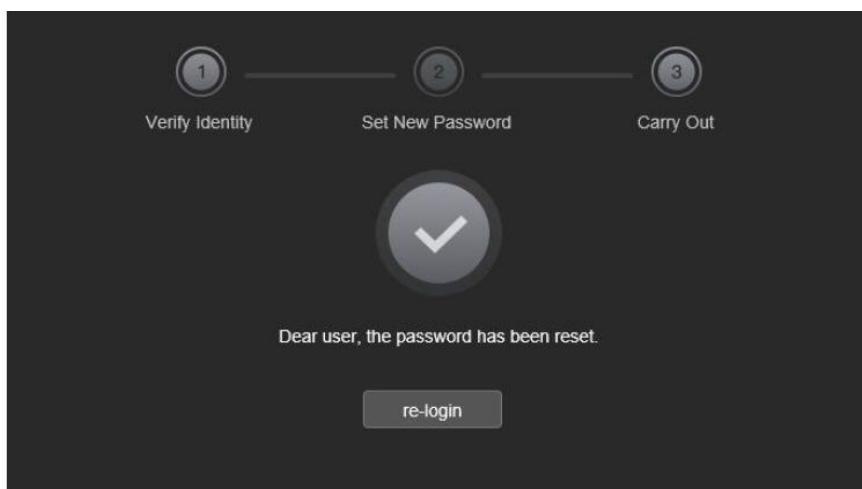


Рисунок 4-6 (3)



ПРИМЕЧАНИЕ:

- Выбрав опцию «Security question validation (Проверка с помощью секретного вопроса)», введите правильные ответы на 2 вопроса, чтобы перейти в окно «Set New Password» (Установить новый пароль) и далее – к следующему шагу.
- Для успешной установки нового пароля необходимо ввести не менее 8 символов, которые должны содержать как буквы, так и цифры.
- Если Вы забудете пароль, файл ключа безопасности IP-камеры можно использовать для сброса пароля несколько раз.

4.2.4. Выход из системы

При входе в главное окно IP-камеры Вы можете щелкнуть в правом верхнем углу иконку безопасного выхода из системы («»).

4.3. Установка элементов управления IP-камерой LsIPCPlugin



ПРИМЕЧАНИЕ:

- Если Вы используете браузеры Internet Explorer или 360, после входа в систему Вам необходимо будет загрузить и установить элементы управления.
- Плагин для интеллектуальной IP-камеры называется «LsIPCPlugin».

Откройте Internet Explorer и войдите в окно предварительного просмотра IP-камеры, как показано на рисунке 4-7.

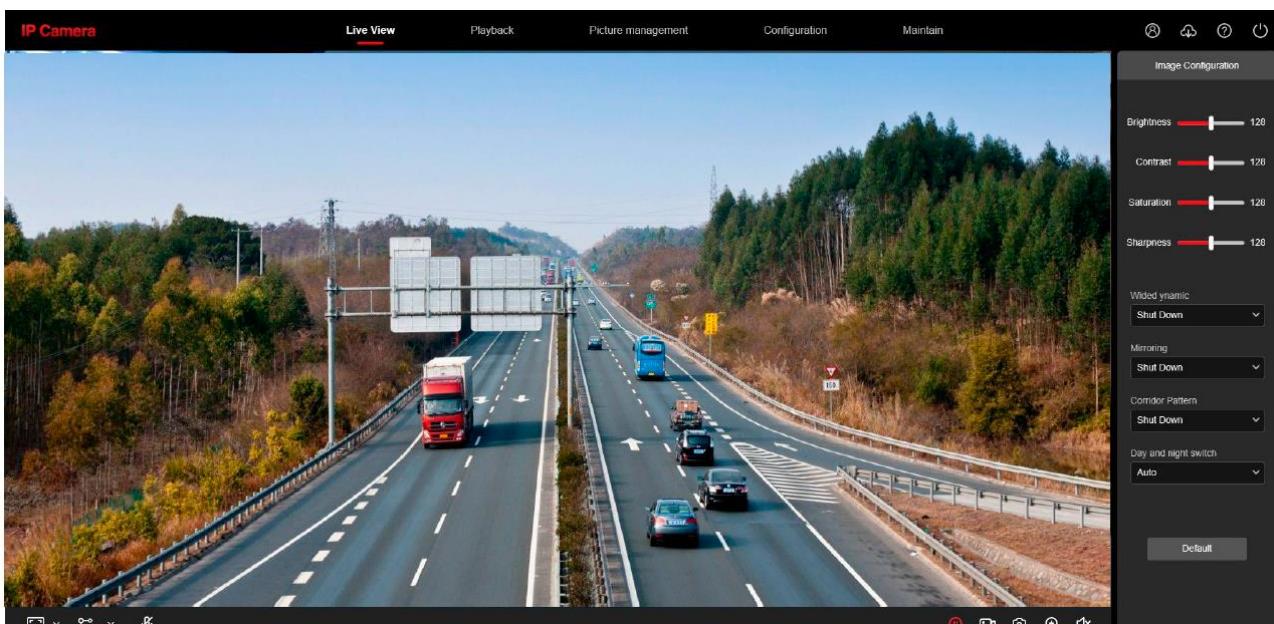


Рисунок 4-7

Нажмите кнопку «Download plugin (Скачать плагин)» в правом верхнем углу, выберите путь сохранения элемента управления, нажмите на «Download (Скачать)», закройте браузер Internet Explorer, нажмите кнопку «Open (Открыть)», выберите язык «English (Английский)» → «OK» → «Next (Далее)» → «Next (Далее)» → «Next (Далее)» → «Install (Установить)» → «Finish (Готово)» – см. рисунки 4-8 (①, ②, ③, ④, ⑤, ⑥), чтобы завершить процесс установки.

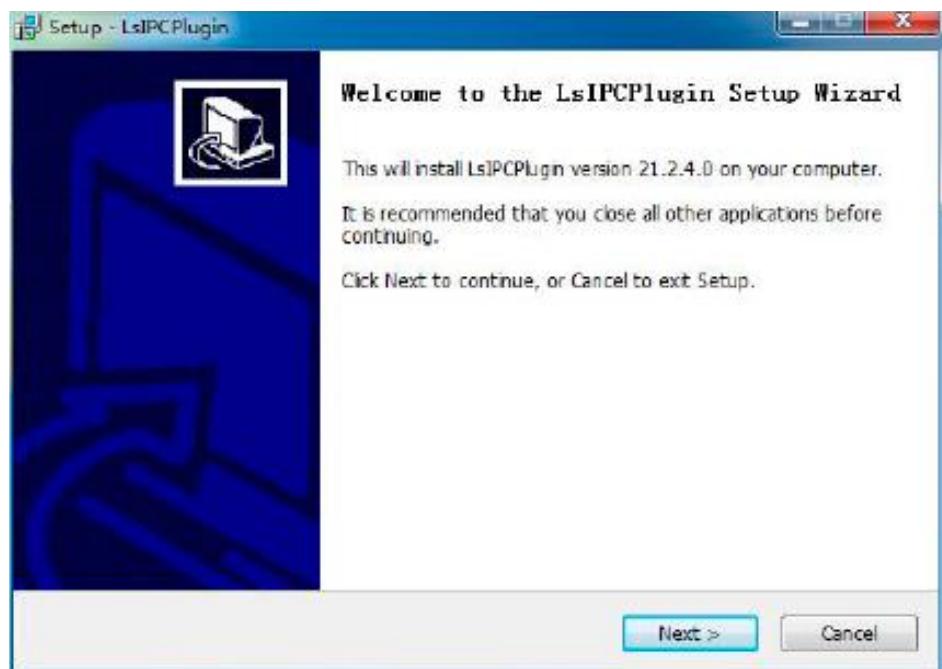


Рисунок 4-8 ①

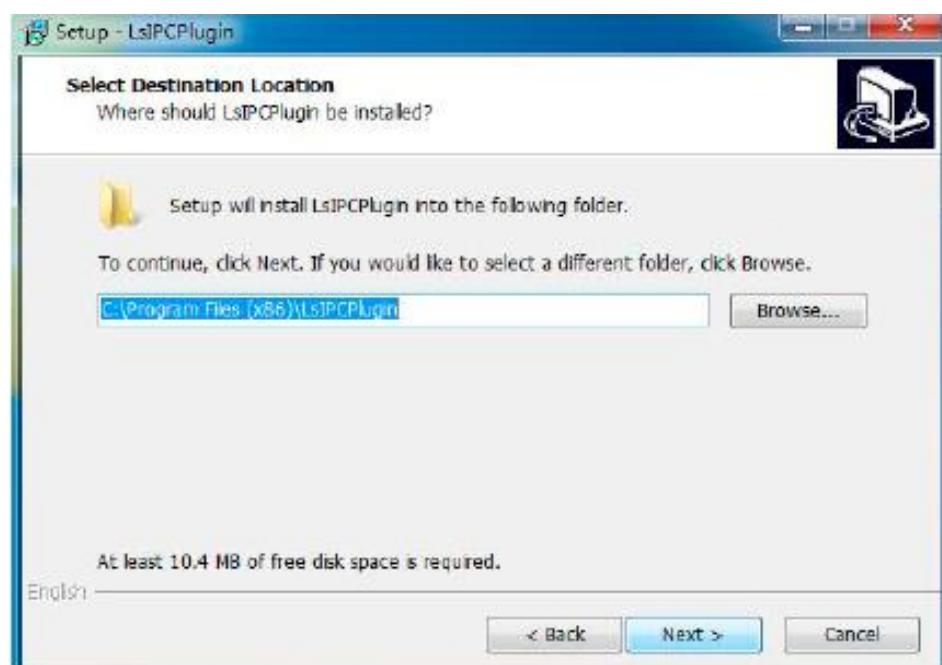


Рисунок 4-8 ②



Рисунок 4-8 (3)

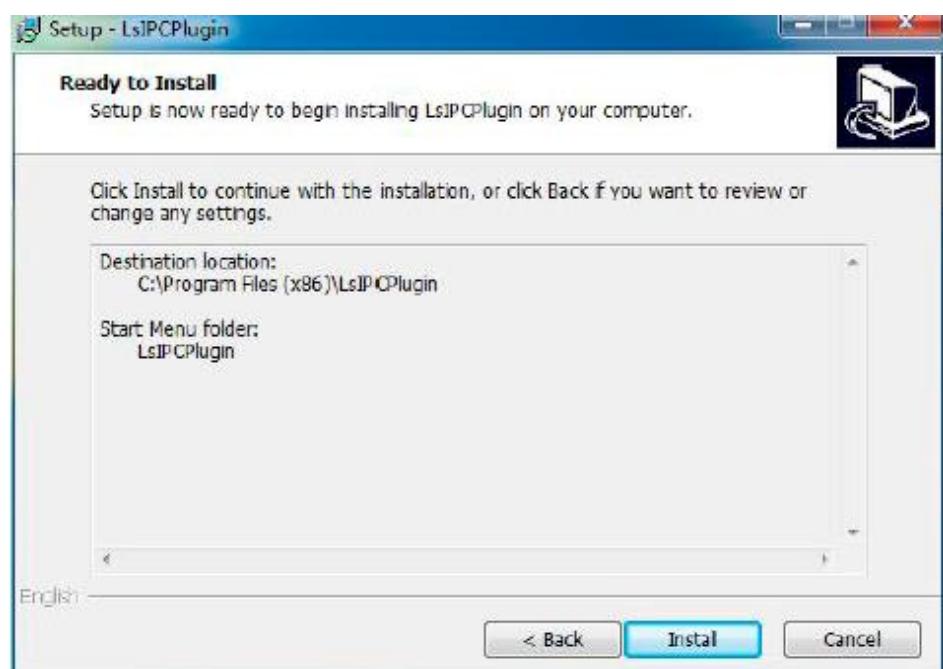


Рисунок 4-8 (4)

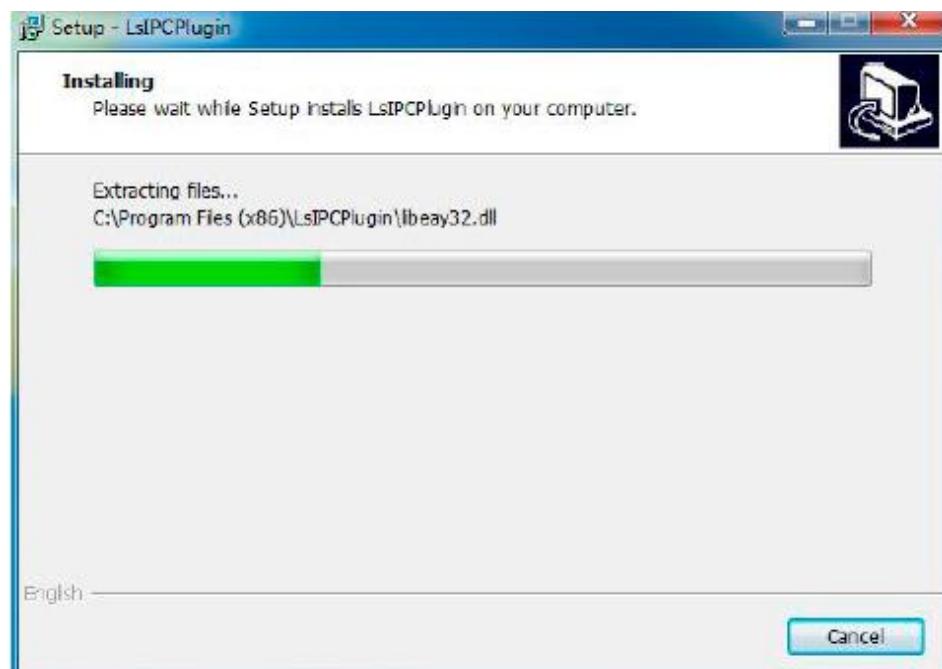


Рисунок 4-8 (5)

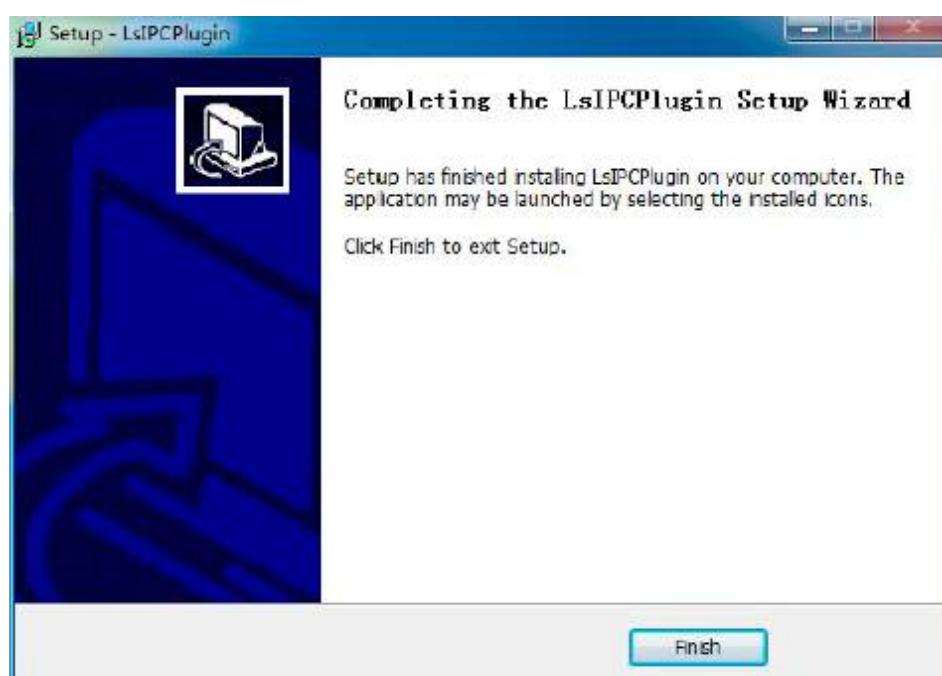


Рисунок 4-8 (6)



Уведомление

Если система выдаст сообщение «Installation failure (Ошибка установки)», снимите флажок «Cancel protection mode (Отменить режим защиты)» в настройках безопасности в «Internet options (Свойства обозревателя)» и введите «Custom level (Пользовательский уровень)» в настройках управления ActiveX как показано на рисунке 4-4, затем переустановите LsIPCPlugin после сохранения настроек.

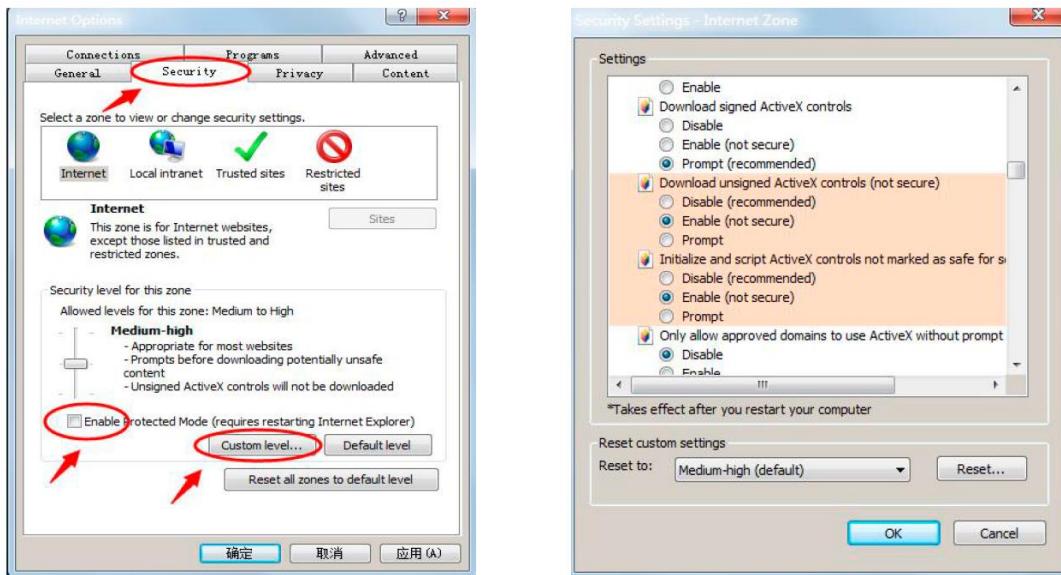


Рисунок 4-9

4.4. Описание главного окна

В главном окне IP-камеры Вы можете просматривать видео в реальном времени, воспроизводить, настраивать его, выполнять сервисные и другие функции. Это окно показано на рисунке 4-10.

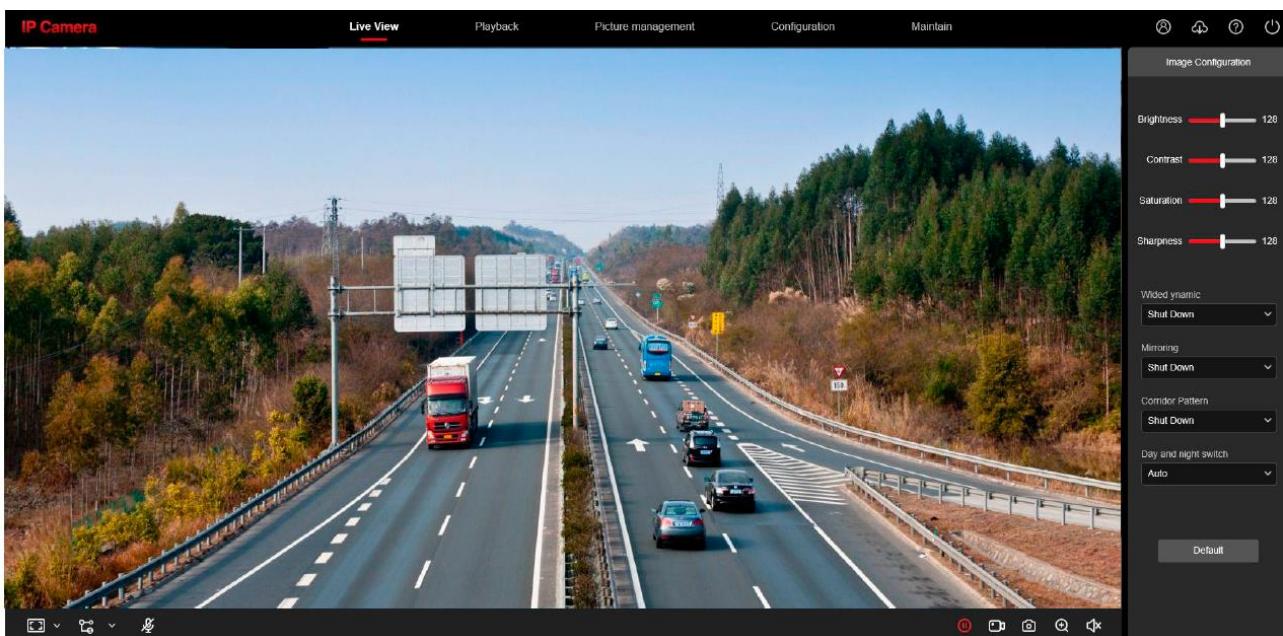


Рисунок 4-10

[Live View (Просмотр изображений в реальном времени)]: Для предварительного просмотра экрана мониторинга IP-камеры Вы можете переключать режим просмотра потока, а также можно выполнять просмотр архивного видео, снимков, использовать электронный зум и другие функции.

[Playback (Воспроизведение)]: Для поиска данных на SD-карте устройства и запуска процесса воспроизведения выберите время или тип видео.

[Picture (Снимок)]: Используется для запроса, просмотра и загрузки файлов изображений, хранящихся на карте памяти EMMC/TF IP-камеры.

[Configuration (Настройка)]: Для ввода настроек системы и функций перейдите в окно настройки IP-камеры.

[Maintain (Обслуживание)]: Используется для просмотра информации об устройстве, обновления, восстановления параметров по умолчанию, обслуживания, импорта и экспорта параметров, запроса журналов.

[Image Configuration (Настройка изображения)]: Используется для настройки параметров изображения, WDR, зеркального отображения, коридорного режима, переключения режимов День / Ночь.



ПРИМЕЧАНИЕ:

- Информацию о внешнем виде главного окна IP-камеры и его функциях смотрите в документации к конкретному устройству.

Глава 5. Просмотр видео в реальном времени

5.1. Просмотр видео в реальном времени

Live View

Нажмите на «Live View», чтобы войти в окно просмотра видео IP-камеры, как показано на рисунке 5-1.

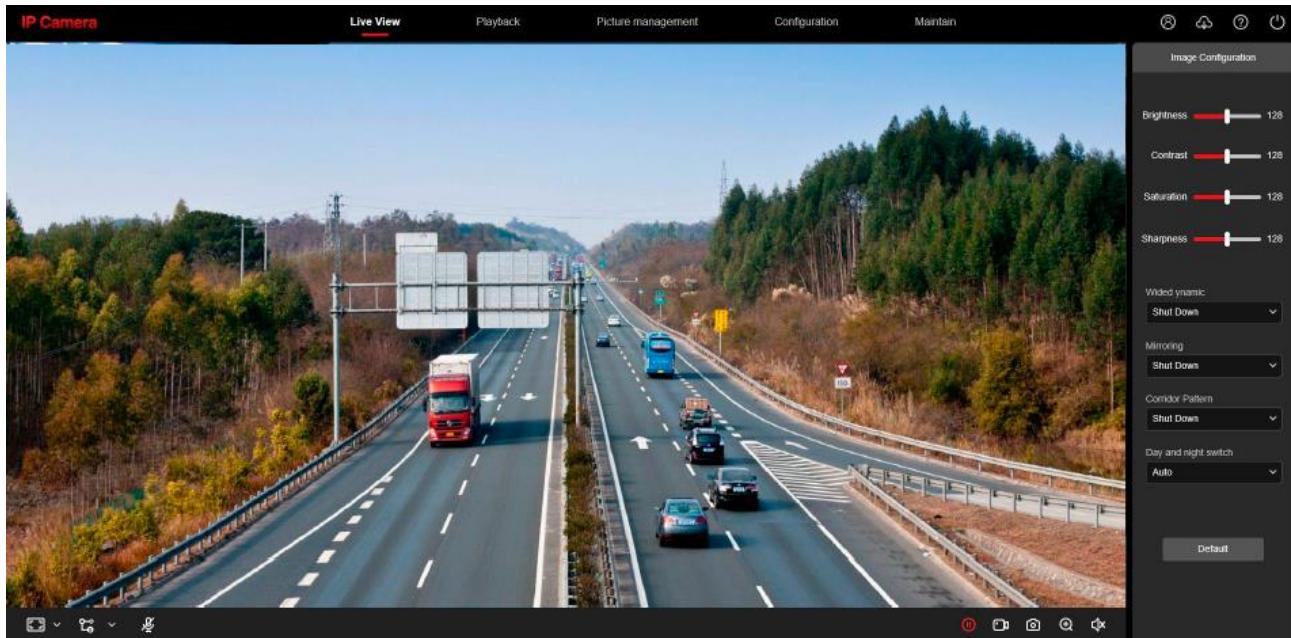


Рисунок 5-1

[Switching window size (Изменение размера окна)]: В окне просмотра видео в режиме реального времени в левом нижнем углу имеются опции масштаба окна просмотра, выберите желаемую: «4:3», «16:9», «1:1», «Full screen (Полноэкранный режим)».

[Switching option (Опции переключения)]: Выберите в левом нижнем углу окна поток для просмотра в режиме реального времени.

Кнопки управления окном просмотра показаны в таблице 5-1.

Иконка	Описание
	Размер окна 4:3.
	Исходный размер окна просмотра.
	Размер окна 16:9.
	Самонастраивающийся размер окна.
	Выбор потока просмотра в реальном времени.
	Запуск / остановка просмотра в реальном времени
	Запуск / остановка записи вручную.

	Захват снимка вручную.
	Включение / выключение электронного масштабирования. Включите функцию электронного масштабирования. В окне предварительного просмотра, удерживая нажатой левую кнопку мыши, выберите область электронного масштабирования, в окне отобразится область для увеличения изображения.
	Включение / выключение звука.
	Включение / выключение переговорного устройства.

Таблица 5-1

Глава 6. Воспроизведение изображения

Playback

В главном окне нажмите кнопку «  », чтобы перейти в окно воспроизведения видео. Окно воспроизведения можно сохранить на EMMC/TF-карте камеры внутри видеофайла для целей выполнения запросов, воспроизведения и загрузки, как показано на рисунке 6-1.

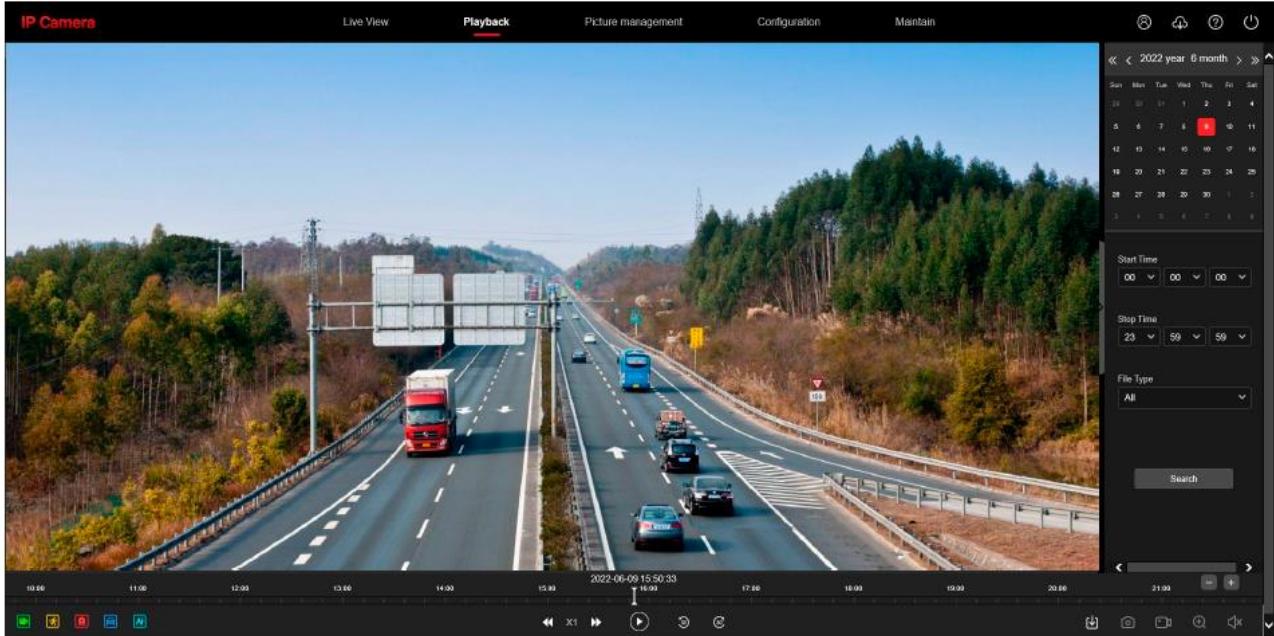
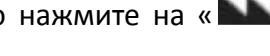


Рисунок 6-1

Здесь по типу видео (обычное видео, видео тревог) и времени его записи Вы можете запросить с EMMC/TF-карты воспроизведение видеофайла, скриншоты, клипы и загрузки.

[Video search (Поиск видеозаписей)]: Выберите время начала и окончания записи, тип файла (All video, Normal Record, Motion Detection, External Alarm, Vehicle Detection, Area Intrusion, Line Cross Detection, Loiter Detection, Personnel Gathering (Все видео, Обычная запись, Обнаружение движения, Внешняя тревога, Обнаружение транспортного средства, Вторжение в зону, Пересечение линии, Обнаружение подозрительного поведения, Обнаружение скопления людей)), нажмите на «  » для выполнения поиска. Соответствующий условиям поиска файл появится в правой части окна календаря. Здесь можно выбрать отмеченную красным дату (красная дата обозначает день выхода видео) и время начала видео, отображаемое на временной шкале.

[Play / Stop (Воспроизведение / Пауза)]: После поиска видео нажмите на «  », чтобы начать воспроизведение видео. После этого кнопка станет выглядеть таким образом: «  ». Если Вы хотите остановить воспроизведение видео, нажмите её.

[Slow Play / Fast Forward (Замедленное воспроизведение / быстрая перемотка вперед)]: При воспроизведении видео нажмите на «  », чтобы замедлить скорость воспроизведения видео, или на «  » – чтобы увеличить скорость воспроизведения, фактическая скорость воспроизведения будет отображаться в правом верхнем углу окна.

[Drag and drop (Перетаскивание)]: При воспроизведении видео, щелкнув левой кнопкой мыши можно определить нужную точку воспроизведения на оси времени, точку можно пе-

ретащить влево или вправо. Перетаскивание в середину желтой точки времени приведет к воспроизведению видео канала в указанный момент времени.

[Electronic zoom (Электронное масштабирование)]: Во время воспроизведения видео нажмите на «» и выделите при помощи мыши область для увеличения , отпустите кнопку мыши. Изображение в данной области будет увеличено. Чтобы восстановить масштаб, нажмите правую кнопку мыши, далее кнопка приобретет такой вид: «». Нажмите её, если хотите восстановить прежний масштаб.

[Capture (Захват снимка)]: Во время воспроизведения видео нажмите на «», чтобы захватить текущее изображение на экране воспроизведения, при этом появится всплывающее окно выбора пути сохранения, где Вы сможете сохранить только что сделанный снимок.

[Audio (Звук)]: Если видеофайл содержит звук, во время воспроизведения нажмите кнопку «», чтобы включать / выключать воспроизведение записанного файла. Вы также можете регулировать громкость, перетаскивая её регулятор.

[Timeline magnification (Увеличение временной шкалы)]: Щелкните мышью в правой части окна справа от кнопки «», окно под временной осью будет увеличено – максимально до сетки в 5 минут.

[The timeline is reduced (Уменьшение временной шкалы)]: Если масштаб временной шкалы был увеличен, нажмите кнопку «», чтобы вернуться к её исходному масштабу.

[Video File Query and Download (Выбор и скачивание видеофайлов)]: Выберите дату, период времени и тип видео в календаре. Нажмите «» в правой части окна, чтобы открыть всплывающее окно скачивания видео. В этом окне осуществляется автоматический поиск всех видеофайлов, соответствующий указанному временному диапазону и типу видеофайлов (см. рисунок 6.2).

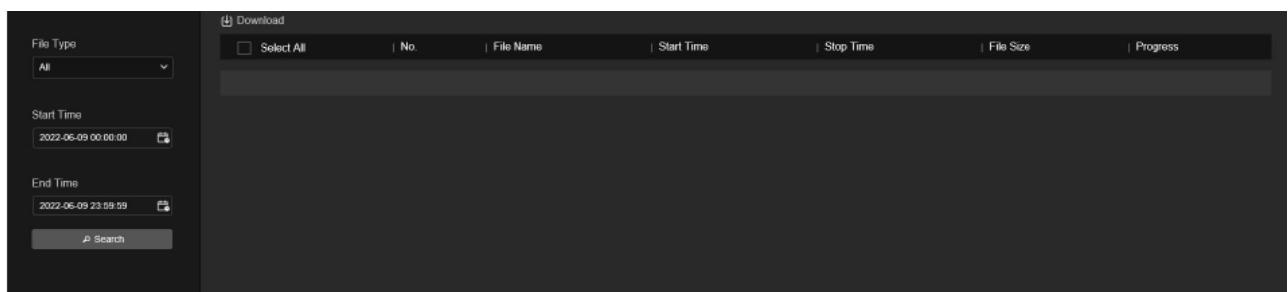


Рисунок 6-2

[Prev Page (Предыдущая страница)]: Функция перелистывания назад, нажмите для перехода на предыдущую страницу.

[Next Page (Следующая страница)]: Функция перелистывания вперед, нажмите для перехода на следующую страницу.

[Download (Скачать)]: Поставьте флажок «» напротив имени скачиваемого файла, нажмите «Download (Скачать)»  «Save (Сохранить)», укажите путь сохранения скачиваемого файла, далее начнется выгрузка файла, дождитесь её завершения.



ПРИМЕЧАНИЕ:

- Видеокамеры, в которых не предусмотрено наличие карт памяти EMMC/TF, не располагают интерфейсом настроек воспроизведения видео, учитывайте особенности Вашего конкретного устройства.
- Для хранения данных на карте EMMC требуется, чтобы камера поддерживала аппаратное обеспечение EMMC. Для получения подробной информации по данному вопросу, обратитесь к описанию имеющегося у Вас устройства.
- Перед запросом видео, убедитесь в том, что состояние карты памяти EMMC/TF в устройстве обозначено как «In use (Используется)» и были заданы соответствующие настройки записи в разделе 8.7.2 «Хранение данных на карте памяти».
- Ознакомьтесь с информацией о настройках сохранения видео и снимков в окне воспроизведения в разделе 8.1 «Локальная настройка».
- Чтобы приостановить воспроизведение, нажмите на «Download (Загрузить)».

Глава 7. Получение снимков

Picture Management

Нажмите « Picture Management » в главном окне, чтобы перейти к управлению снимками. Файлы снимков, хранящиеся на EMMC/TF-карте камеры, можно найти и скачать (см. рисунок 7-1).

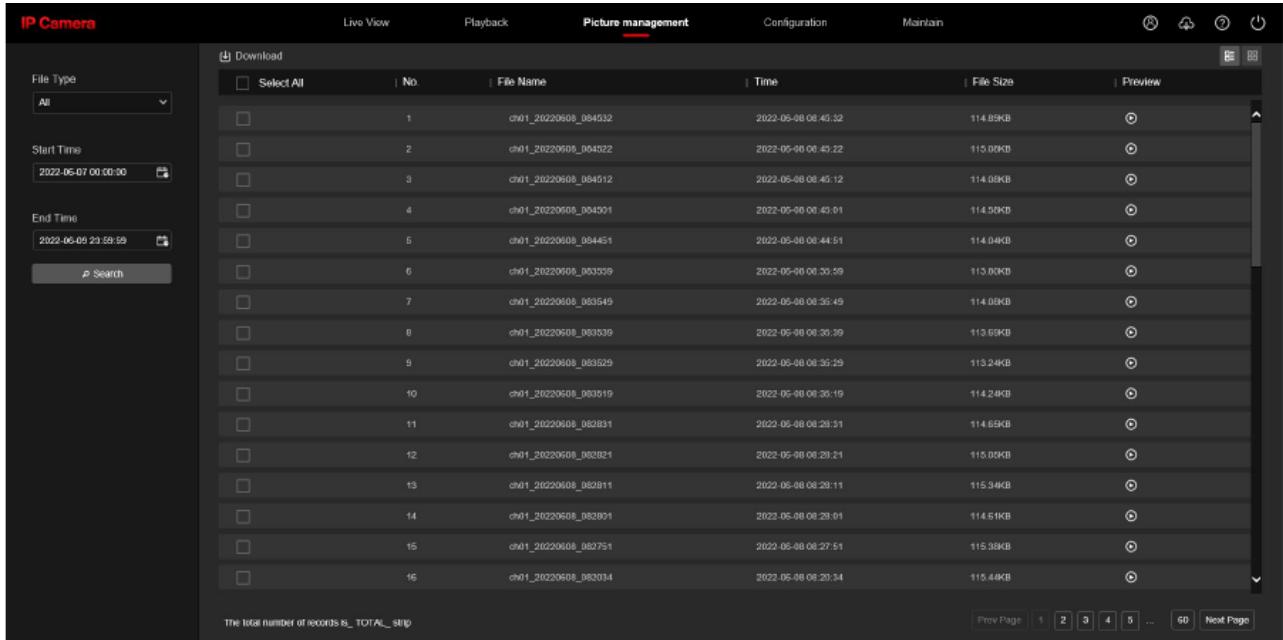


Рисунок 7-1

[Search (Поиск)]: Выберите тип файла в левой части окна, задайте время выполнения поиска и нажмите « », чтобы отобразить справа информацию о нужных Вам снимках.

[Preview (Предварительный просмотр)]: В правой части списка файлов дважды щелкните « », чтобы просмотреть изображение.

[Download (Скачать)]: Выберите снимок, который хотите просмотреть, и нажмите на «Download (Скачать)», чтобы сохранить его на Вашем локальном ПК. Поддерживается одновременная загрузка нескольких снимков.



[View (Просмотр)]: Нажмите « » в правом верхнем углу окна, чтобы отобразить файл в режиме просмотра.



ПРИМЕЧАНИЕ:

- Изображение сохраняется на карте памяти EMMC/TF устройства.
- Для хранения данных на карте EMMC требуется, чтобы камера поддерживала аппаратное обеспечение EMMC. Для получения подробной информации по данному вопросу, обратитесь к описанию имеющегося у Вас устройства.

Глава 8. Настройка

Configuration

Нажмите «**Configuration**» в главном окне, чтобы перейти в окно локальной настройки устройства. Здесь Вы можете настроить систему устройства, задать сетевые настройки, настройки видео, снимков, событий и другие параметры.

8.1. Локальная настройка

Чтобы перейти в окно локальной настройки, в главном окне выберите меню «**Configuration (Настройка)**» → «**Local Configuration (Локальная настройка)**». Здесь Вы сможете задать путь сохранения для «**Record File Settings (Настройки записи файлов)**», «**Picture and Clip Settings (Настройки снимков и клипов)**». Задать путь можно выбрав «**Browse (Обзор)**», как показано на рисунке 8-1.

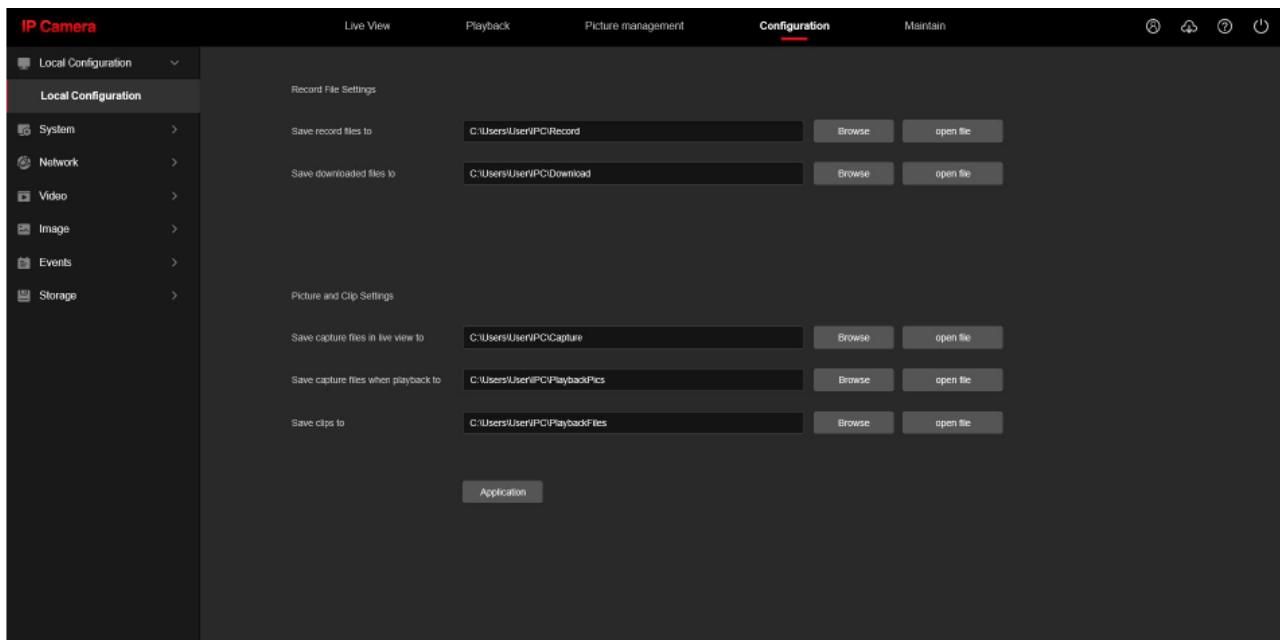


Рисунок 8-1

[Record File Settings (Настройки записи файлов)]: Задайте путь сохранения записанных видеофайлов. Эти настройки касаются файлов, которые Вы записали с помощью веб-браузера.

[Record Path of Live View (Путь сохранения записей просмотра в реальном времени)]: Задайте путь сохранения видеофайлов, записанных вручную.

[Download Path of Playback (Путь сохранения файлов воспроизведения)]: Путь сохранения выгружаемых файлов.

[Picture and Clip Settings (Настройки снимков и клипов)]: Задайте пути сохранения для захваченных снимков и разбитых на клипы видеофайлов. Эти настройки касаются снимков, которые Вы получили с помощью веб-браузера.

[Snapshot Path of Live View (Путь сохранения снимков просмотра в реальном времени)]: Путь сохранения для снимков, снятых вручную, в режиме реального времени.

[Snapshot Path of Playback (Путь сохранения снимков воспроизведения)]: Путь сохранения для снимков, отснятых вручную, в режиме воспроизведения.

[Record Path of Playback (Путь сохранения видеозаписей воспроизведения)]: Путь сохранения разбитых на клипы видеофайлов в режиме воспроизведения.



ПРИМЕЧАНИЕ:

- Для локальной настройки необходимо установить промежуточное программное обеспечение, в противном случае настройка выполнена быть не может.
- Браузер Safari не поддерживает опцию локальной настройки.

8.2. Система

Чтобы перейти в окно настройки системы, выберите в главном окне меню «Configuration (Настройка)» → «System (Система)». Модуль настройки системы состоит из настройки самой системы и выбора настроек безопасности.

8.2.1. Настройка системы

Чтобы перейти в окно системных настроек, выберите в главном окне меню «Configuration (Настройка)» → «System (Система)» → «System Configuration (Настройка системы)».

① Настройки времени

В окне «System Configuration (Настройка системы)» нажмите на «Time Settings (Настройки времени)», чтобы перейти в окно настройки, где Вы сможете задать время устройства, как показано на рисунке 8.2.

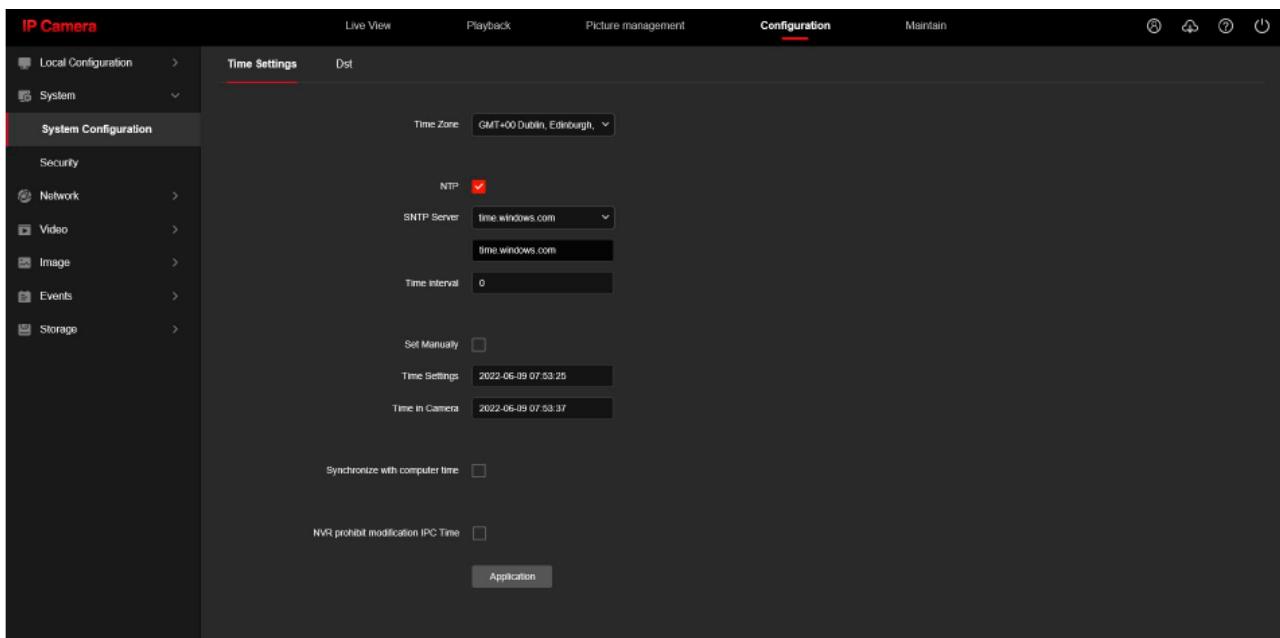


Рисунок 8-2

[Time Zone (Часовой пояс)]: Отображает текущий часовой пояс выбранного устройства.

[Time in Camera (Время камеры)]: Отображает текущее время устройства.

[NTP]: Время IP-камеры синхронизируется с сетевым, и Вы можете изменять часовые пояса (для этой функции требуется, чтобы сетевая среда IP-камеры могла иметь доступ к сети Интернет). После завершения настроек нажмите на «Application (Применить)».

[SNTP Server (SNTP-сервер)]: Адрес SNTP-сервера, включая опции: «time.windows.com», «time.nist», «gov», «time-nw.nist.gov», «time-a.nist.gov», «time-b.nist.gov». По желанию Вы также можете ввести свой адрес SNTP-сервера через «Customize (Настроить)».

[Time Interval (Временной интервал)]: По умолчанию интервал времени между IP-камерой и SNTP-сервером составляет 1 минуту. Вы можете установить значения от 1 до 10080.

[Set Manually (Задать вручную)]: Настройка даты и времени IP-камеры вручную. После завершения настроек нажмите на «Application (Применить)».

[Synchronize with computer time (Синхронизировать со временем ПК)]: IP-камера будет синхронизироваться со временем и датой того ПК, к которому Вы подключили ее в данный момент. После завершения настроек нажмите на «Application (Применить)».

[NVR prohibit modification IPC time (Запрет для NVR на изменение времени в IP-камере)]: После установки этого параметра внутренние устройства хранения данных (такие как NVR, XVR и т.д.) не будут влиять на время IP-камеры. Время IP-камеры будет отображаться в соответствии с настройками пользователя.

② Переход на летнее время

Летнее время (DST) - это система искусственного установления местного времени в целях экономии энергии. Единое время, используемое при внедрении этой системы, называется «DST (Daylight Saving Time)». В окне настройки системы нажмите на «Dst (Переход на летнее время)», чтобы перейти в окно настройки перехода на летнее время. Здесь Вы сможете включить переход на летнее время, установить время перехода на летнее время и окончания перехода на летнее время (возврата к исходному времени), как показано на рисунке 8-3.

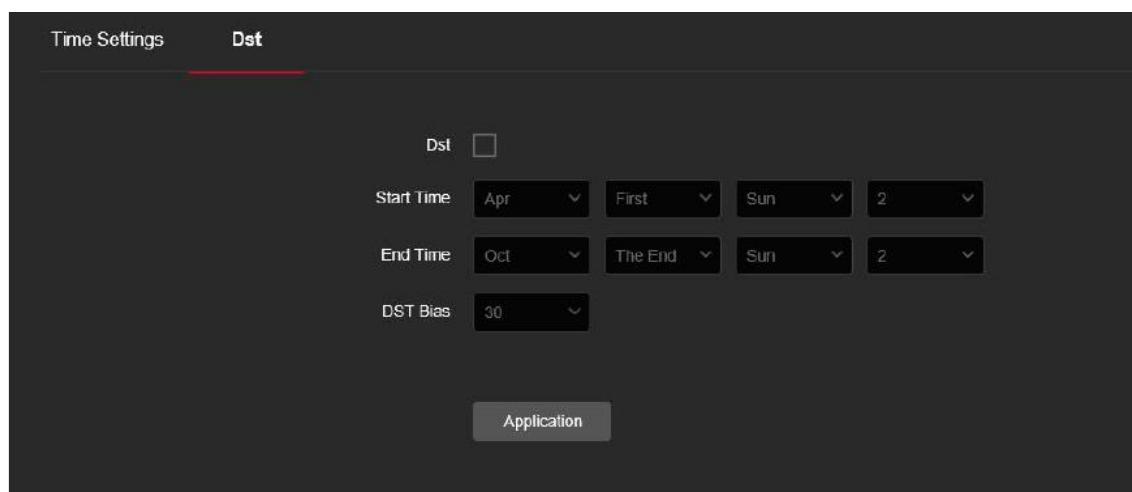


Рисунок 8-3

8.2.2. Безопасность

В главном окне выберите «Configuration (Настройка)» → «System (Система)» → «Security (Безопасность)», чтобы перейти в окно настроек прав пользователей, где Вы можете добавлять, редактировать, удалять пользователей, а также запрашивать текущую информацию о пользователе. Текущий пользователь – администратор («admin»), для работы ему может понадобиться добавить других пользователей. Вы можете добавить до 10 пользователей, как показано на рисунке 8-4.

① Добавление пользователя

User Management			
online user			
Add User			
No.	User Name	Competence	operate
1	admin	Admin	Edit

Рисунок 8-4

Шаг 1: Чтобы добавить пользователя, нажмите «Add User (Добавить пользователя)».

Шаг 2: Введите «User Name (Имя пользователя)», выберите «User Type (Тип пользователя)» и задайте для него «Password (Пароль)».

Шаг 3: Чтобы завершить процедуру добавления пользователя, нажмите «OK».

Процедура добавления пользователя представлена на рисунке 8-5.

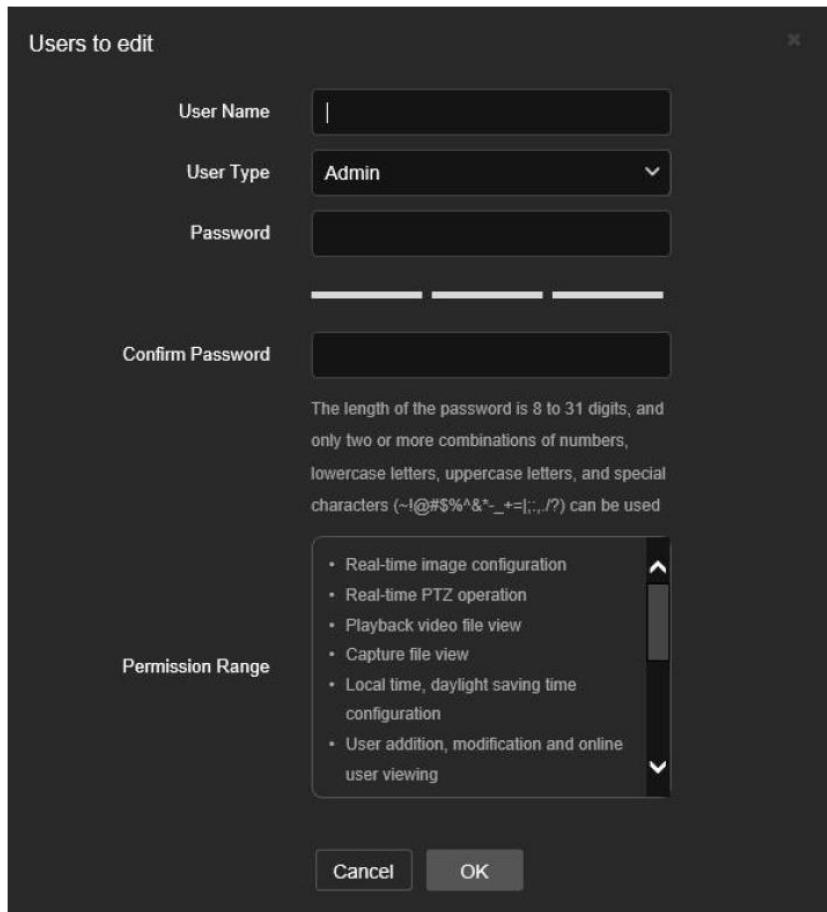


Рисунок 8-5



ОСТОРОЖНО!

- Для повышения сетевой безопасности устройства, регулярно меняйте пароль пользователя. Рекомендуется проводить обслуживание каждые 3 месяца. Если IP-камера используется в условиях повышенного риска безопасности, рекомендуется обновлять ее данные безопасности раз в месяц или каждую неделю.
- Системному администратору рекомендуется эффективно управлять правами пользователей, удалять посторонних пользователей и отключать неиспользуемые сетевые порты.



ПРИМЕЧАНИЕ:

- Пользователя «admin» удалить нельзя, Вы можете только изменить пароль администратора.
- Описание прав пользователей:
 - Администратор – все права доступа.
 - Оператор – Все разрешения (кроме настройки параметров безопасности системы).

- Наблюдающий – разрешен только просмотр данных.
- При выборе пароля для IP-камеры его длина должна составлять от 8 до 31 символа, пароль должен состоять из цифр и букв.

Ниже приведены правила поддержания надежности пароля:

- Надежный пароль содержит три или более типов символов (цифры, строчные буквы, заглавные буквы, специальные символы).
- Если в качестве пароля задана комбинация цифр и специальных символов, то в пароле используются строчные буквы и специальные комбинации символов, заглавные буквы и специальные символы, строчные буквы и прописные буквы.
- Если в качестве пароля задана комбинация цифр и строчных букв, то сочетания только цифр и заглавных букв являются слабозащищенными паролями.
- Длина пароля составляет 8 символов. Если пароль содержит только один тип символов, пароль и имя пользователя или только пароль – это имя самого пользователя — все указанные выше типы паролей являются рискованными, задавать их не рекомендуется.

Чтобы усилить защиту данных и повысить безопасность устройства, рекомендуем Вам для защиты от рисков заменить пароль на надежный.

(2) Первое изменение пароля (для пользователя-администратора («admin»))

Шаг 1: В списке пользователей нажмите кнопку «Edit (Изменить)» рядом с именем пользователя «admin», чтобы войти в окно настроек пользователя.

Шаг 2: Введите старый пароль (пароль по умолчанию – «admin») и задайте новый пароль в полях «Password (Пароль)» и «Confirm Password (Подтверждение пароля)».

Шаг 3: Выберите секретные вопросы 1, 2, 3 и задайте соответствующие им корректные ответы, затем нажмите на «Key export (Экспорт ключа)», чтобы экспортировать файл ключа на свой компьютер.

Шаг 4: Чтобы завершить процедуру смены пароля, нажмите «OK».

(3) Повторное изменение пароля (для пользователя-администратора («admin»))

Шаг 1: В списке пользователей нажмите кнопку «Edit (Изменить)» рядом с именем пользователя «admin», чтобы войти в окно настроек пользователя.

Шаг 2: Введите старый пароль и задайте новый пароль в полях «Password (Пароль)» и «Confirm Password (Подтверждение пароля)».

Шаг 3: Чтобы завершить процедуру смены пароля, нажмите «OK».



ПРИМЕЧАНИЕ:

- Если исходным паролем IP-камеры является пароль «admin», то при каждом новом входе в систему Вам будет предлагаться изменить его. Вы можете выбрать опцию «Modify after 60 mins (Изменить через 60 минут)». Через 60 минут в окне автоматически появится всплывающее окно изменения пароля.
- При изменении пароля администратора, после задания секретного вопроса, нажмите на «Browse (Обзор)» и выберите путь. Далее нажмите на «Export (Экспортировать)», чтобы экспортировать файл ключа (тогда пароль можно будет сбросить в случае, если он будет забыт).
- После изменения пароля администратора (когда компьютер и устройство будут подключены к одному сегменту локальной сети) нажмите на «Forget (Забыт)», чтобы сбросить пароль, ответив на секретный вопрос или же импортировав ключ.
- При повторном изменении пароля Вам не нужно задавать новый секретный вопрос. Если Вы забудете свой пароль, Вы сможете сбросить его с помощью последнего заданного Вами секретного вопроса.

④ Изменение профиля пользователя (добавление нового пользователя)

Шаг 1: В списке пользователей выберите запись того пользователя, профиль которого нужно изменить, и нажмите на «Edit (Изменить)», чтобы перейти в окно редактирования пользователя.

Шаг 2: Измените тип пользователя или пароль, введите пароль для подтверждения.

Шаг 3: Чтобы завершить редактирование пользователя, нажмите на «OK».



ПРИМЕЧАНИЕ:

- Правила выбора пароля те же, что и при добавлении пользователя.

⑤ Удаление пользователей

Шаг 1: Выберите пользователя, которого Вы хотите удалить, и нажмите на «Delete (Удалить)».

Шаг 2: Нажмите во всплывающем диалоговом окне на «OK», чтобы завершить процедуру удаления пользователя.

8.3. Сеть

8.1.3. Основные настройки

① Настройка протокола TCP/IP

Окно TCP/IP используется для просмотра и настройки сетевых параметров, таких как IP-адрес камеры. Вы можете включить DHCP или вручную изменить сетевые параметры IP-камеры.

Включение DHCP:

Подключите IP-камеру к маршрутизатору с включенным DHCP, включите функцию DHCP, после чего IP-камера получит соответствующий IP-адрес, маску подсети, шлюз по умолчанию и информацию о предпочтительном DNS-сервере.

Шаги изменения сетевых параметров вручную приведены ниже:

Шаг 1: Чтобы вызвать окно настройки TCP/IP, в главном окне выберите «Configuration (Настройка)» → «Network (Сеть)» → «Basic Setup (Основные настройки)» → «TCP/IP», см. рисунок 8-6 ①.

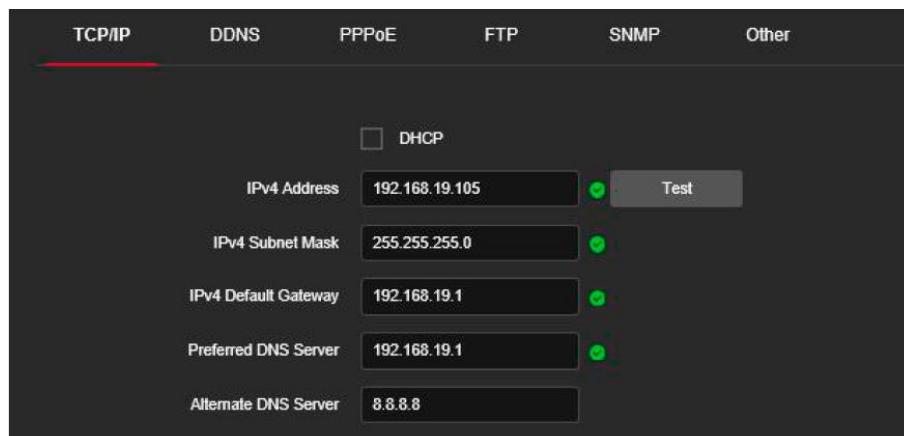


Рисунок 8-6 ①

Шаг 2: Задайте IP-адрес, маску подсети, шлюз и DNS.

Шаг 3: Нажмите на «Test (Проверить)», чтобы убедиться, что измененный IP-адрес доступен в локальной сети.

Шаг 4: Нажмите на «Application (Применить)», чтобы сохранить конфигурацию.

Порт

В главном окне выберите «Configuration (Настройка)» → «Network (Сеть)» → «Basic Setup (Основные настройки)» → «TCP/IP», чтобы перейти в окно настройки параметров TCP/IP, где Вы можете установить сетевой порт IP-камер и порт протокола. Сетевой порт имеет порт HTTP (по умолчанию 80), порт RTSP (по умолчанию 554), порт HTTPS (по умолчанию - 443), порт BITVISION (по умолчанию - 6000), порт протокола имеет порт ONVIF (по умолчанию - 8999) (см. рисунок 8-6 ②).

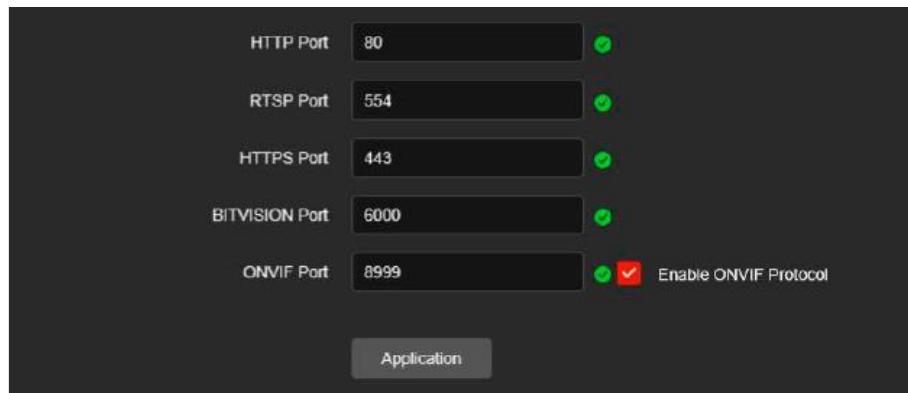


Рисунок 8-6 ②

[BITVISION Port (Порт BITVISION)]: Когда приложение BitVision напрямую подключено к устройству, в поле **[BITVISION Port (Порт BITVISION)]** вводится параметр «Private port (Частный порт)».

[ONVIF Port (Порт ONVIF)]: Если нужно, чтобы IP-камера осуществляла доступ к серверному оборудованию в рамках стандарта ONVIF, протокол ONVIF следует включить (выставить флагок «Enable ONVIF Protocol (Включить протокол ONVIF)»).



ПРИМЕЧАНИЕ:

Не изменяйте параметры порта произвольно; если возникнет необходимость в изменении номера порта из-за конфликта портов, измените следующую информацию.

- Порт HTTP и HTTPS: чтобы добавить адрес после номера порта, используйте логин браузера. Если Вы восстанавливаете HTTP-порт с номером 8555, при входе в систему браузера Вам необходимо ввести логин браузера.
- Порт RTSP: порт протокола передачи данных в реальном времени, чтобы убедиться, что измененный порт доступен.
- Устройства на платформе AL не поддерживают порт BITVISION.

② DDNS

После установки параметра DDNS (Сервер динамических доменных имен), когда IP-адрес IP-камеры часто меняется, система может динамически обновлять взаимосвязь между доменным именем и IP-адресом на DNS-сервере. Вы можете использовать доменное имя для прямого доступа к IP-камере, не записывая постоянно меняющийся IP-адрес.

Важно!

Перед настройкой DDNS убедитесь в том, что устройство поддерживает тип сервера назначения доменных имен, и зайдите на веб-сайт поставщика услуг DDNS, чтобы зарегистрировать имя пользователя, пароль, доменное имя и другую информацию о ПК в ГВС.

Выполните следующие действия:

Шаг 1: Чтобы вызвать окно настройки функции DDNS, в главном окне выберите «Configuration (Настройка)» → «Network (Сеть)» → «Basic configuration (Основные настройки)» → «DDNS», см. рисунок 8-7.

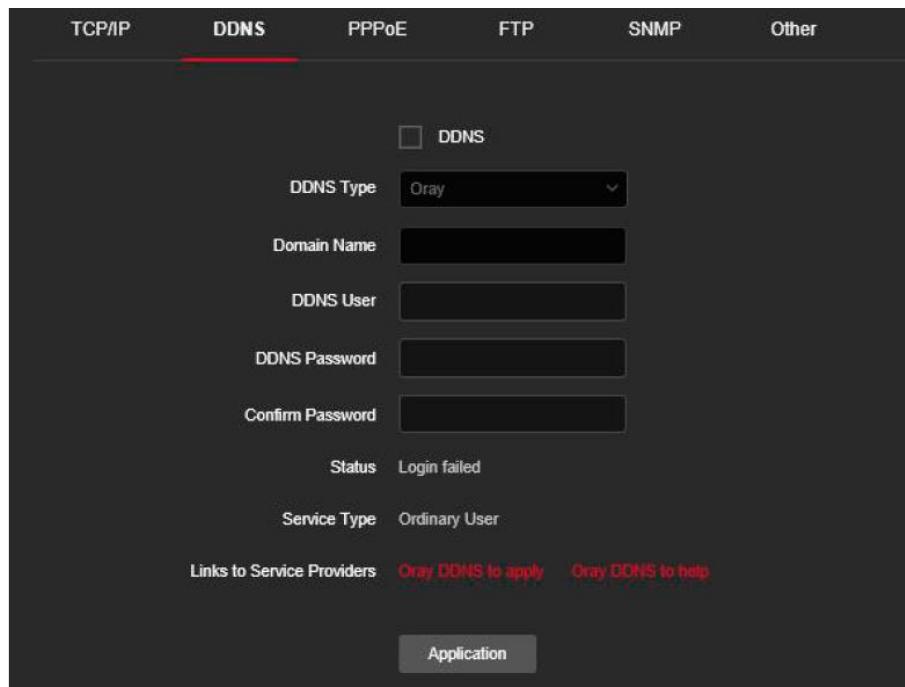


Рисунок 8-7

Шаг 2: Включите DDNS (опция «Enable»), выберите тип DDNS и введите имя пользователя, пароль и название сайта.

Шаг 3: Нажмите на «Application (Применить)», чтобы сохранить конфигурацию.

Шаг 4: Введите доменное имя в веб-браузере ПК и нажмите на «Enter». Если Вы сможете отобразить веб-интерфейс устройства, настройка выполнена успешно. Если он не отображается, настройка выполнена некорректно.

[DDNS]: Включение / отключение функции DDNS.

[DDNS Type (Тип DDNS)]: Выберите из пяти типов: Oray, NO-IP, Dyn, Planet Dynamic DNS и Planet Easy DDNS.

[Site Name (Имя сайта)]: Доменное имя согласно выбранному типу DDNS.

[DDNS User (Пользователь DDNS)]: Зарегистрированная учетная запись согласно выбранному типу DDNS.

[DDNS Password (Пароль DDNS)]: Пароль при регистрации согласно выбранному типу DDNS.

[Confirm Password (Подтверждение пароля)]: Повторно введите этот пароль и пароль DDNS.

[Status (Состояние)]: Показывает, успешно ли настроено текущее устройство DDNS.

[Service Type (Тип обслуживания)]: Отображает тип имени пользователя.

[Links to service providers (Ссылки на поставщиков услуг)]: Отображает информацию о поставщике услуг.



ПРИМЕЧАНИЕ:

- Для доступа через домен DDNS требуется, чтобы к IP-камере можно было осуществлять доступ через сеть Интернет.

(3) PPPoE

Протокол PPPoE (Point-to-Point Protocol over Ethernet) – один из способов, с помощью которого IP-камеры получают доступ к сети. После получения имени пользователя и пароля PPPoE, предоставляемых интернет-провайдером, Вы можете устанавливать сетевое подключение через удаленный доступ по протоколу PPPoE. После успешного подключения IP-камера автоматически получает динамический IP-адрес в глобальной сети.

Выполните следующие действия:

Шаг 1: Чтобы вызвать окно настройки функции PPPoE, в главном окне выберите «Configuration (Настройка)» → «Network (Сеть)» → «Basic configuration (Основные настройки)» → «PPPoE», см. рисунок 8-8.

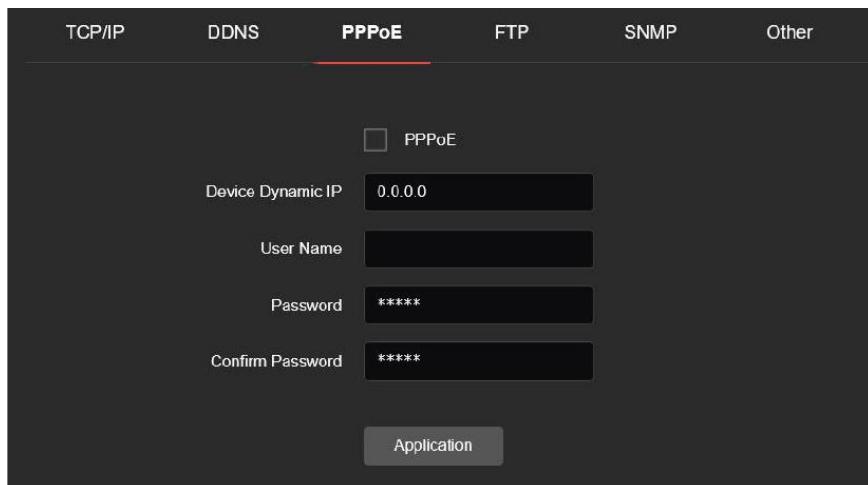


Рисунок 8-8

Шаг 2: Нажмите на , чтобы открыть окно настройки PPPoE, введите имя пользователя с динамическим IP-адресом устройства и пароль для PPPoE.

Шаг 3: Нажмите на «Apply (Применить)», чтобы сохранить конфигурацию.

[PPPoE]: Включение / выключение функции PPPoE устройства.

[User Name (Имя пользователя)]: Имя пользователя PPPoE, предоставленное провайдером интернет-услуг.

[Password (Пароль)]: Пароль, соответствующий имени пользователя.



ПРИМЕЧАНИЕ:

После завершения настройки устройство автоматически выполнит подключение (после перезагрузки). После успешного подключения информация о сети может быть отображена в статусе сети, и пользователи смогут получить доступ к устройству по IP-адресу.

④ FTP

Настроив обмен с сервером FTP, Вы сможете сохранять изображения, выполненные в случае тревог, на FTP-сервере.

Важно!

Вам необходимо приобрести или скачать Инструмент обслуживания FTP и установить программное обеспечение на свой компьютер.



ПРИМЕЧАНИЕ:

- Чтобы создать пользователя FTP, Вам необходимо установить разрешение на запись в папку FTP, в противном случае изображения не будут успешно загружаться.

Для настройки обмена с FTP выполните следующие действия:

Шаг 1: Чтобы вызвать окно настройки обмена с FTP, в главном окне выберите «Configuration (Настройка)» → «Network (Сеть)» → «Basic configuration (Основные настройки)» → «FTP», см. рисунок 8-9.

The screenshot shows the 'Basic configuration' screen with the 'FTP' tab active. The configuration fields include:

- FTP Server: 192.168.1.1
- Port: 21
- User Name: admin
- Password: *****
- Confirm Password: *****
- Storage First Level Directory: Use IP address (192.168.19.112)
- Storage Secondary Directory: Chinese
- AutoCover: Unchecked
- Image Format: JPEG

A note in red text states: "Select the language used to create the secondary directory for Chinese. The FTP server is required to support setting UTF-8 encoding."

Рисунок 8-9

Шаг 2: Задайте следующие параметры: «FTP Server (Адрес FTP-сервера)», «Port (Порт)», «User Name (Имя пользователя)», «Password (Пароль)» (подтвердите пароль - «Confirm Password»)/ Выберите папку хранения первого уровня («Storage First Level Directory»), дополнительную папку хранения («Storage Secondary Directory»)/ Установите флагок «Auto Cover (Автоматическое закрытие)» и выберите формат JPEG для загружаемых на FTP-сервер снимков.

Шаг 3: Нажмите на «Application (Применить)», чтобы сохранить конфигурацию.

Шаг 4: Чтобы подтвердить правильность сетевого подключения и настройки обмена с FTP, нажмите на «Test (Проверка)».



ПРИМЕЧАНИЕ:

- Если проверка завершилась отказом, перепроверьте настройки сети или FTP-сервера.

[FTP Server (FTP-сервер)]: Введите адрес FTP-сервера.

[Test (Проверка)]: Введите информацию об FTP-сервере и нажмите на «Test (Проверка)», чтобы подтвердить правильность всей введенной информации и проверить, корректно ли подключены устройство и сервер.

[Port (Порт)]: Введите номер порта FTP-сервера.

[User Name (Имя пользователя)]: Введите имя пользователя FTP-сервера.

[Password (Пароль)]: Введите пароль FTP-сервера.

[Confirm Password (Подтверждение пароля)]: **[Password (Пароль)]**: Введите пароль FTP-сервера.

[Storage first level directory (Папка хранения первого уровня)]: Автоматически создайте папку первого уровня в зависимости от пути к хранилищу FTP.

[Storage secondary directory (Дополнительная папка хранения)]: Создайте дополнительную папку в зависимости от папки хранения первого уровня.

⑤ SNMP

Прежде чем задать параметры SNMP, пользователь должен определить SNMP-сервер и убедиться в том, что SNMP-сервер имеет корректные настройки и может правильно работать. IP-камера поддерживает три простые версии протокола сетевого управления: V1, V2 и V3. Протокол сетевого управления выбирается в соответствии с версией серверного протокола SNMP. Настроив протокол SNMP, можно получить параметры устройства и информацию о тревогах при нештатных ситуациях на устройстве.

После включения функции SNMP на устройстве, задайте параметры «Read community name (Имя сообщества чтения)» и «Write community name (Имя сообщества записи)». Затем введите «Trap address (Адрес ловушки)», тогда устройство сможет отправлять информацию о тревогах и нештатных ситуациях на станцию управления. Чтобы иметь возможность получить информацию об устройстве, задайте параметр «Trap port (Порт ловушки)».

Выполните следующие действия:

Чтобы вызвать окно настройки SNMP, в главном окне выберите «Configuration (Настройка)» → «Network (Сеть)» → «Basic configuration (Основные настройки)» → «SNMP», см. рисунок 8-10. После выставления флагка «SNMP» (включение функции SNMP устройства) выберите версию SNMP, например V3. Далее Вы сможете задать информацию о параметрах SNMP версии V3 («SNMP Port (SNMP-порт)», «Read community name (Имя сообщества чтения)», «Write community name (Имя сообщества записи)», «Trap address (Адрес ловушки)» и т.д.). Тогда устройство сможет отправлять информацию о тревогах и нештатных ситуациях на станцию управления и можно будет получать информацию об устройстве (при условии настройки параметра «Trap port (Порт ловушки)»). После ввода всех параметров нажмите на «Application (Применить)».

TCP/IP	DDNS	PPPoE	FTP	SNMP	Other
<p><input checked="" type="checkbox"/> SNMP</p> <p>SNMP Version <input type="button" value="V3"/></p> <p>SNMP Port <input type="text" value="161"/></p> <p>Read Community Name <input type="text" value="public"/></p> <p>Write Community Name <input type="text" value="private"/></p> <p>Trap Address <input type="text"/></p> <p>Trap Port <input type="text" value="162"/></p> <p>Read Security Name <input type="text"/></p> <p>Authentication Algorithm <input checked="" type="checkbox"/> MD5 <input type="checkbox"/> SHA</p> <p>Authentication Password <input type="text" value="*****"/></p> <p>Secret Key Algorithm <input checked="" type="checkbox"/> DES <input type="checkbox"/> AES</p> <p>Secret Key Password <input type="text" value="*****"/></p> <p><input type="button" value="Application"/></p>					

Рисунок 8-10

⑥ Дополнительно

Чтобы вызвать окно настройки защиты видео паролем, в главном окне выберите «Configuration (Настройка)» → «Network (Сеть)» → «Basic configuration (Основные настройки)» → «Other (Дополнительно)», как показано на рисунке 8-11.

TCP/IP	DDNS	PPPoE	FTP	SNMP	Other
<p><input checked="" type="checkbox"/> Video Password Authentication</p> <p><input type="checkbox"/> Enable RTSP Encryption</p> <p><input type="checkbox"/> Enable BITVISION Encryption</p> <p><input type="button" value="Application"/></p>					

Рисунок 8-11

[Video Password Authentication (Защита видео паролем)]: После выбора этой опции видео с камеры будет зашифровано для всех устройств и платформ, подключенных к камере. Доступ к видео с IP-камеры будет возможен только после ввода корректных имени пользователя и пароля.

[Enable RTSP Encryption (Включить шифрование RTSP)]: При выборе этой опции шифруется поток RTSP с камеры.

[Enable BITVISION Encryption (Включить шифрование BITVISION)]: Если выбрана эта опция, то шифруется поток данных между камерой и приложением BitVision.



ПРИМЕЧАНИЕ:

- Устройства на платформе AL не поддерживают шифрование BITVISION.

8.2.3. P2P

① P2P

P2P - это технология проникновения в частную сеть. Для этого не требуется подавать заявку на динамическое доменное имя, выполнять назначение портов или развертывать транзитный сервер. Вы можете непосредственно отсканировать QR-код, чтобы загрузить мобильный клиент. После регистрации учетной записи Вы сможете одновременно добавлять несколько устройств (IP-камер , NVR, XVR) и управлять ими в мобильном клиенте.

Для управления несколькими устройствами Вы можете добавить их двумя следующими способами.

1) Отсканируйте QR-код для мобильного телефона, загрузите приложение и зарегистрируйте учетную запись. Более подробную информацию смотрите в Руководстве пользователя приложения на веб-сайте.

2) Войдите на платформу P2P, зарегистрируйте учетную запись и добавьте устройство с помощью серийного номера.



ПРИМЕЧАНИЕ:

- Функция P2P устройства включена по умолчанию. Для использования этой функции устройство должно быть подключено к внешней сети, а статус подключения должен отображаться как «P2P connection successful (P2P-соединение установлено успешно)». В противном случае оно не будет работать корректно.

Выполните следующие действия:

Шаг 1: Чтобы вызвать окно настройки P2P, в главном окне выберите «Configuration (Настройка)» → «Network (Сеть)» → «P2P», как показано на рисунке 8-12.

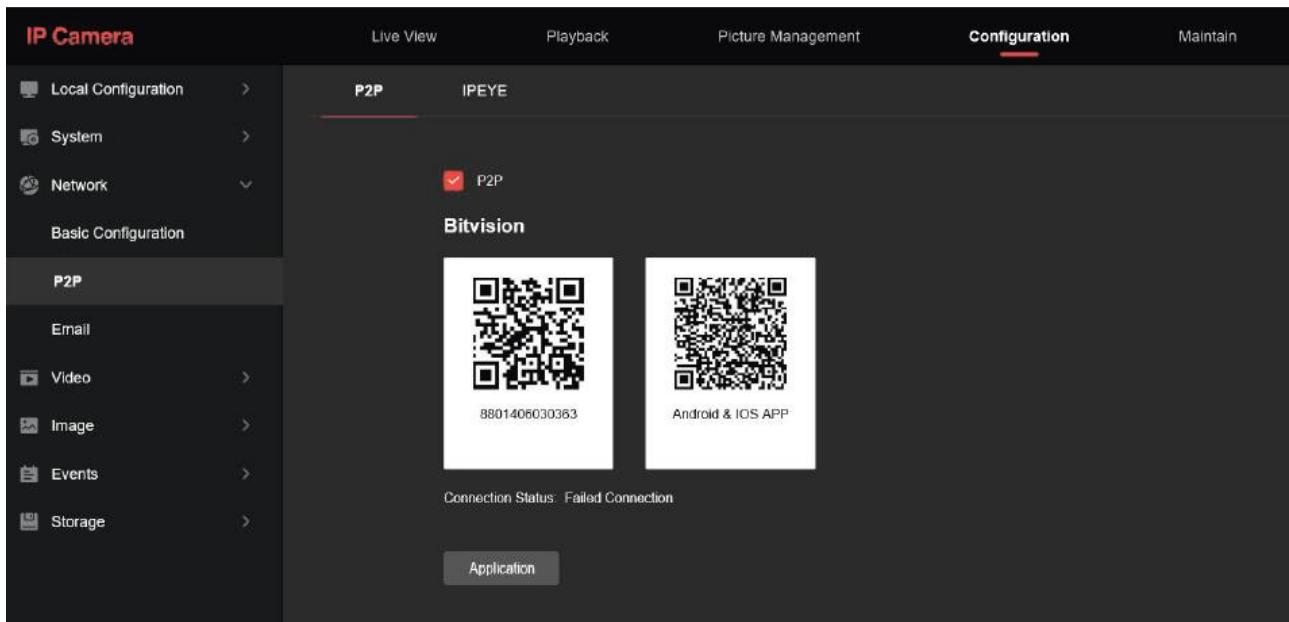


Рисунок 8-12

Шаг 2: Убедитесь в том, что IP-камера имеет доступ к внешней сети, далее, чтобы открыть P2P, и нажмите на «», .

Шаг 3: Нажмите на «Application (Применить)», чтобы сохранить конфигурацию.

Шаг 4: Обновите страницу, на ней появится статус «Connection successful (Подключение выполнено успешно)». Это означает, что P2P включен и может использоваться в обычном режиме.

Пример работы клиента приложения

Приведенный ниже материал представлен на примере работы клиента для мобильных телефонов (приложения BitVision) исключительно в ознакомительных целях. Шаги выполнения следующие:

Шаг 1: С помощью телефона Android или iOS отсканируйте соответствующий QR-код, чтобы загрузить и установить приложение BitVision.

Шаг 2: Запустите клиент и войдите в учетную запись (при первичной регистрации учетная запись не требуется).

Шаг 3: Добавьте устройства в мобильный клиент.

После входа в систему нажмите на «Device manage (Управление устройством)», «» и «»

Add device (Добавить устройство), выберите «SN Add (Добавить SN)», введите имя пользователя устройства, пароль и проверочный код после сканирования QR-кода (проверочный код напечатан на этикетке). Нажмите на «Add (Добавить)», чтобы настроить устройство и группу, после успешного добавления нажмите на «Done (Готово)».

Шаг 4: Просмотр в реальном времени.

Выберите опцию «Real time (В реальном времени)» и нажмите на «», чтобы войти в список устройств в главном окне, выберите сенсорное перо и канал для предварительного

просмотра в группе, после нажатия кнопки «Done (Готово)» Вы увидите видео в реальном времени.

② IPEYE

Чтобы вызвать окно настройки функции облачного хранения IPEYE, в главном окне выберите «Configuration (Настройка)» → «Network (Сеть)» → «P2P» → «IPEYE». После включения IPEYE Вы сможете добавить устройство в учетную запись IPEYE по адресу //www.ipeye.ru/. Пример просмотра аудио / видео с IP-камеры в режиме реального времени приведен на рисунке 8-13 ①.

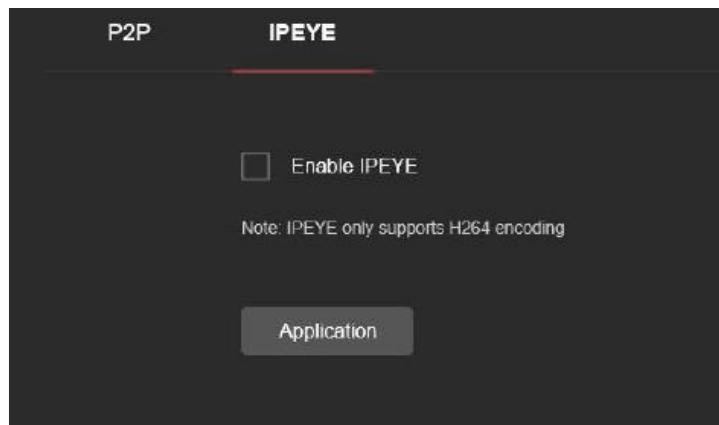


Рисунок 8-13 ①

Чтобы отслеживать аудио- и видеосигнал в режиме реального времени по адресу <https://www.ipeye.ru/>, выполните следующие действия.

Шаг 1: Войдите в окно настройки IPEYE, включите функцию IPEYE, обновите окно, и в нем отобразится адрес клиента IPEYE (IPEYE Client address), как показано на рисунке 8-13 ②.

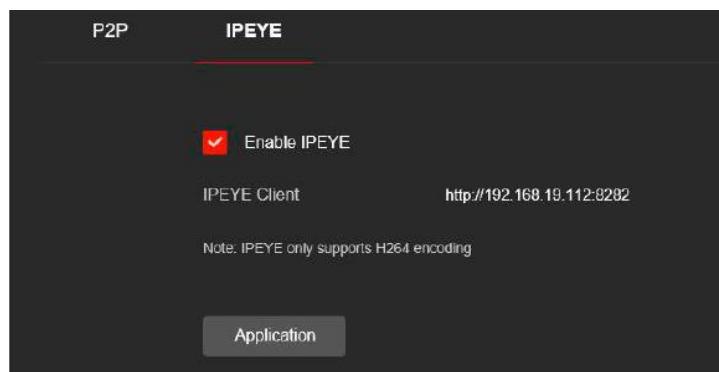


Рисунок 8-13 ②

Шаг 2: Войдите в клиент IPEYE (IPEYE Client) «<http://192.168.19.112:8282>», введите учетную запись и пароль для входа в IPEYE, имя пользователя и пароль IP-камеры, нажмите на «Confirm (Подтвердить)», чтобы добавить устройство, как показано на рисунке 8-14 ③.

Добавление камеры в облако

Логин от облака
Логин от облака
Для регистрации в облаке перейдите по ссылке <https://ipeye.ru>.

Пароль от облака
Пароль от облака

Логин от камеры
Логин от камеры

Пароль от камеры
Пароль от камеры

Добавить в Облако

© IPEYE Company, Inc.

Рисунок 8-13 ③

Шаг 3: Войдите в систему через «<https://www.ipeye.ru/>» и введите список устройств IPEYE, чтобы просмотреть имя недавно добавленного устройства (как «cloud_xxxxx»). Чтобы просмотреть видео мониторинга в режиме реального времени с устройства, нажмите на «Play (Воспроизвести)». Список устройств IPEYE показан на рисунке 8-13 ④.

Name	Group	Tariff	Bitrate	Viewers	Options	Action
106.205	No group	Бесплатный	0 Mbps	0		
cloud_100000	No group	Бесплатный	0 Mbps	0		
cloud_190.206	No group	Бесплатный	0 Mbps	0		
cloud_1056	No group	Бесплатный	0 Mbps	0		

Рисунок 8-13 ④

**ПРИМЕЧАНИЕ:**

- Некоторые камеры не поддерживают функцию IPEYE. Внешний вид окна данной функции зависит от конкретного устройства.

8.3.3. Настройка передачи сообщений по электронной почте

После настройки параметров электронной почты и включения функции отправки сообщений по электронной почте – при возникновении тревоги IP-камеры система будет отправлять электронное сообщение с этими данными на почтовый ящик пользователя.

Выполните следующие действия:

Шаг 1: Чтобы вызвать окно настройки передачи сообщений по электронной почте, в главном окне выберите «Configuration (Настройка)» → «Network (Сеть)» → «Email», как показано на рисунке 8-14.

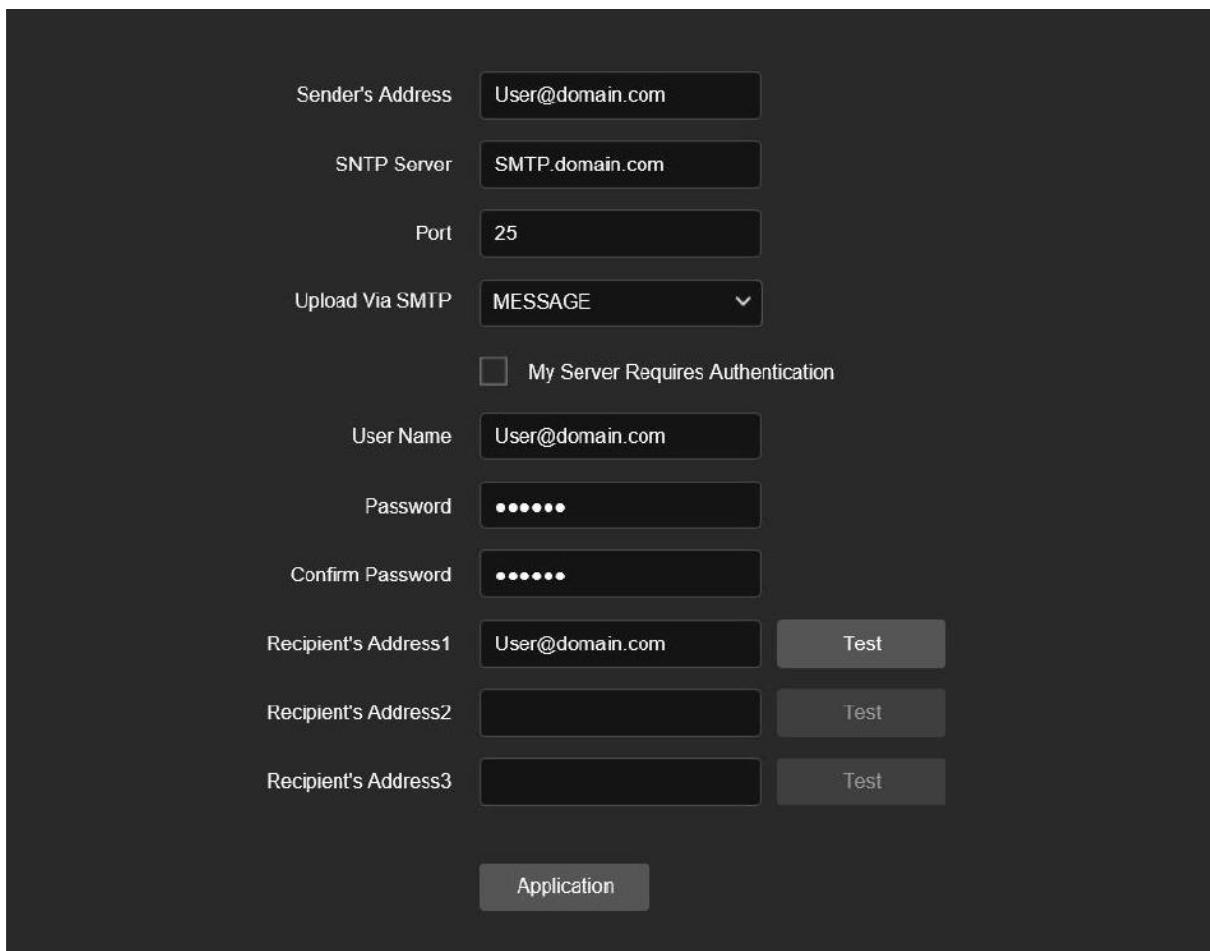


Рисунок 8-14

Шаг 2: Настройте параметры «Sender's Address (Адрес отправителя)», «SMTP Server (SMTP-сервер)», «Port (Порт)», «User Name (Имя пользователя)», «Password (Пароль)» адреса получателя («Recipient's Address 1-3»).

Шаг 3: Чтобы подтвердить правильность сетевого подключения и настройки SMTP, нажмите на «Test (Проверка)».

Шаг 4: Нажмите на «Application (Применить)», чтобы сохранить конфигурацию.



ПРИМЕЧАНИЕ:

Отправитель:

[Sender's Address (Адрес отправителя)]: Укажите полный адрес почтового ящика отправителя.

[SMTP Server (Сервер SMTP)]: Введите адрес Вашего сервера обработки электронной почты.

[Port (Порт)]: Введите порт Вашего сервера обработки электронной почты.

[Upload Via SMTP (Загрузить на SMTP)]: В выпадающем меню выберите формат файла SMTP, формат изображения - JPEG, формат видео - AVI и сообщение.

[My Server Requires Authentication (Мой сервер требует проверки подлинности)]: Если эта функция включена, сервер и пользователь проходят проверку подлинности, чтобы убедиться, что данные отправляются правильному клиенту и серверу.

[User Name (Имя пользователя)]: Введите имя почтового ящика отправки.

[Password (Пароль)]: Введите пароль почтового ящика отправки.

[Confirm Password (Подтверждение пароля)]: **[Password (Пароль)]**: Введите пароль почтового ящика отправки.

Получатель:

[Recipient's Address 1, 2, 3 (Адреса получателей)]: Введите полный адрес Вашего почтового ящика (максимум 3), для завершения процесса настройки нажмите на «Test (Проверка)», чтобы убедиться в правильности всей введенной информации и корректности сетевого подключения камеры.

8.4. Видео

Чтобы перейти в окно ввода настроек видео и звука, где Вы сможете настроить видео, звук и другие функции устройства, в главном окне выберите «Configuration (Настройка)» → «Video (Видео)».

8.4.1. Видео

В главном окне выберите «Configuration (Настройка)» → «Video (Видео)» → «Video (Видео)» и перейдите в окно настройки видео, где можно задать имя IP-камеры, тип потока, кодировку и другие параметры видео, как показано на рисунке 8-15.

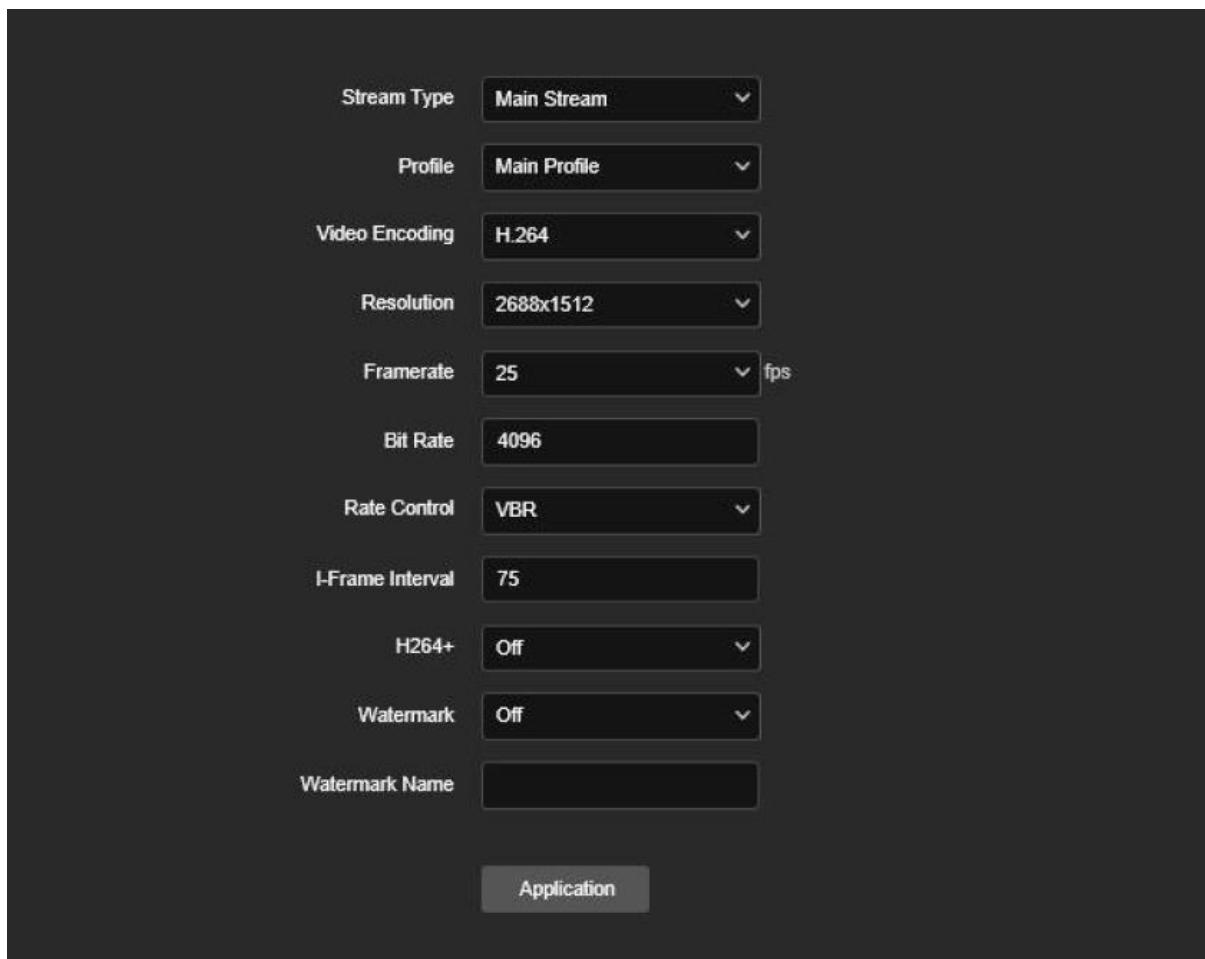


Рисунок 8-15

[Stream Type (Тип потока)]: По умолчанию используется «Main Stream (Основной поток)», Вы можете выбрать «Sub Stream (Дополнительный поток)» или «Tri-Stream (Поток мобильных данных)».

[Profile (Профиль)]: По умолчанию используется «Main Profile (Основной профиль)», Вы можете также выбрать «Basic Profile (Базовый профиль)» или «High Profile (Высокий профиль)».

[Video Encode (Кодировка видео)]: Выберите в выпадающем меню способ кодирования.

[Resolution (Разрешение)]: Выберите в выпадающем меню разрешение изображения на выходе.

[Framerate (Частота кадров)]: Задайте частоту кадров текущего видео на выходе устройства.

[Bit Rate (Скорость передачи данных)]: Поддерживается в диапазоне 64-12000 Кбит/с. Чем выше скорость передачи данных, тем лучше качество видео, но при этом оно требует большей полосы пропускания в сети и увеличивает нагрузку на передачу.

[Rate Control (Управление скоростью)]: Выберите метод управления скоростью в выпадающем меню: фиксированную и переменную скорость.

[I-Frame Interval (Интервал между I-кадрами)]: Интервал между ключевыми кадрами сбора данных IP-камерой может составлять от 1 до 5 секунд.

[H265+/H264+]: Включение / выключение в камере кодирования H265+/H264+.

[Watermark (Водяной знак)]: Включение / выключение функции добавления в изображение водяного знака. Это может предотвратить искажение видео после его включения. После настройки параметра «Watermark name (Содержание водяного знака)» воспользуйтесь нашим проигрывателем «HSPlayer», чтобы проверить, не было ли изменено видео и содержание водяного знака.

[Watermark name (Содержание водяного знака)]: Введите содержание водяного знака.



ПРИМЕЧАНИЕ:

- Параметры типа потока с устройства, кодировки, частоты кадров и другая информация в выпадающем меню различных IP-камер также отличаются друг от друга.
- Параметр «Profile (Профиль)» отображается в меню настройки видео только тех камер, которые поддерживают H264/H264+.
- Помните: если для параметра «Framerate (Частота кадров)» задано слишком низкое значение, это приведет к сбою видеосигнала.
- Чем выше значение параметра «Bit Rate (Скорость передачи данных)», тем большая пропускная способность сети потребуется для передачи данных и тем выше будет нагрузка на сеть.
- Параметр «H265+/H264+» отображается в меню настройки видео только тех камер, которые поддерживают H264/H264+.
- Процесс включения / выключения кодировки H265+/H264+ в камере занимает 30-60 секунд. Наберитесь терпения.

8.4.2. Звук

Чтобы перейти в окно ввода настроек звука, где Вы сможете настроить режим ввода звука в устройство, выбрать кодировку звука, установить громкость звука на входе, в главном окне выберите «Configuration (Настройка)» → «Video (Видео)» → «Audio (Звук)», как показано на рисунке 8-16.

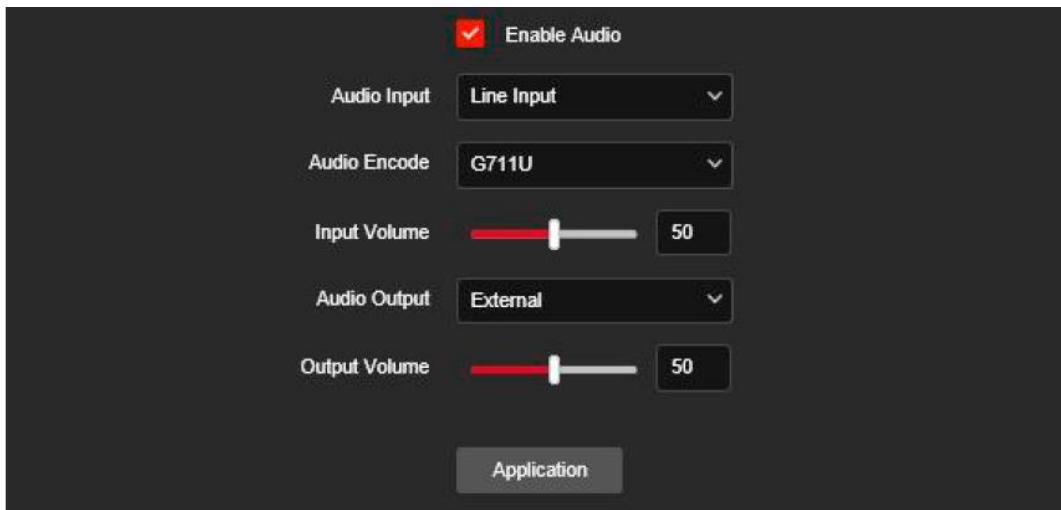


Рисунок 8-16

[Enable Audio (Включить звук)]: Включение / выключение аудиовхода устройства.

[Audio Input (Ввод звука)]: Выберите способ ввода звука.

[Audio Encoding (Кодировка звука)]: Выберите кодировку звука: G711U / G711A / AAC.

[Input Volume (Входная громкость)]: Задайте громкость на входе устройства, диапазон громкости составляет от 0 до 100.

[Audio Output (Выход звука)]: Выберите способ вывода звука.

[Output Volume (Выходная громкость)]: Задайте громкость на выходе устройства, диапазон громкости составляет от 0 до 100.

8.5. Изображение

В главном окне выберите меню «Configuration (Настройка)» → «Image (Изображение)» и перейдите в окно настройки изображения, здесь Вы можете настроить изображение устройства, выбрать текст экранного меню OSD и ввести другую информацию.

8.5.1. Изображение

В главном окне выберите меню «Configuration (Настройка)» → «Image (Изображение)» → «Image (Изображение)» и войдите в меню настройки параметров изображения. Здесь Вы сможете задать параметры изображения из разделов «Image adjustment (Настройки изображения)», «Exposure settings (Настройки экспозиции)», «Day and Night Switch (Переключение режимов День / Ночь)», «White Balance (Баланс белого)», «Video adjustment (Регулировка видео)», «Image enhancement (Улучшение качества изображения)» и «Back Light Settings (Настройки компенсации засветки)», см. рисунок 8-17.

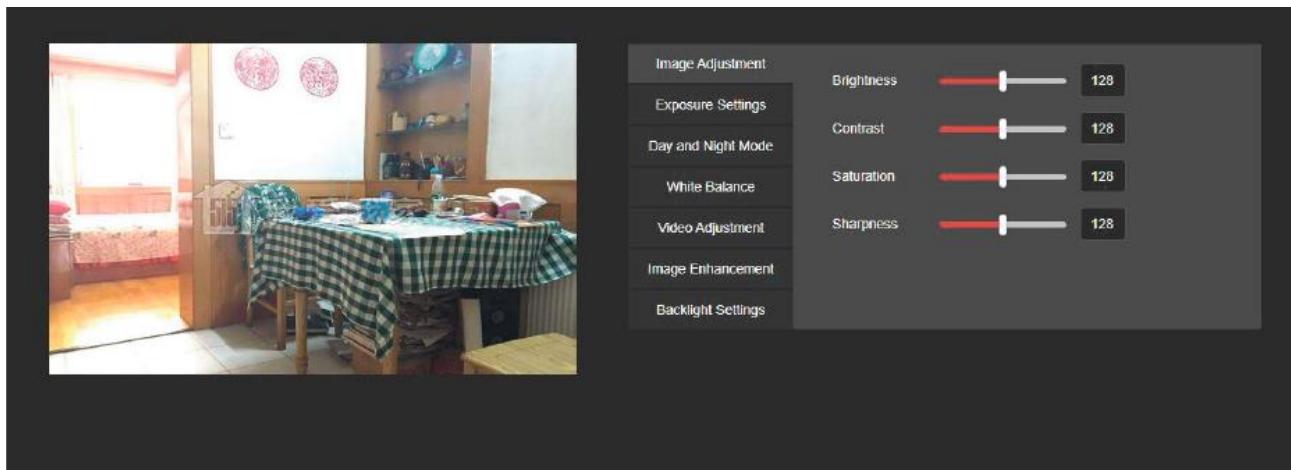


Рисунок 8-17

[Image adjustment (Настройки изображения)]: Здесь Вы можете ввести вручную следующие настройки изображения: «Brightness (Яркость)», «Contrast (Контрастность)», «Saturation (Насыщенность)» и «Sharpness (Резкость)». Эти параметры должны быть заданы согласно реальным условиям. Диапазон допустимых значений: от 0 до 255, для выбора Вы можете перетаскивать ползунок напротив нужного параметра; значение по умолчанию равно 128, как показано на рисунке 8-18.

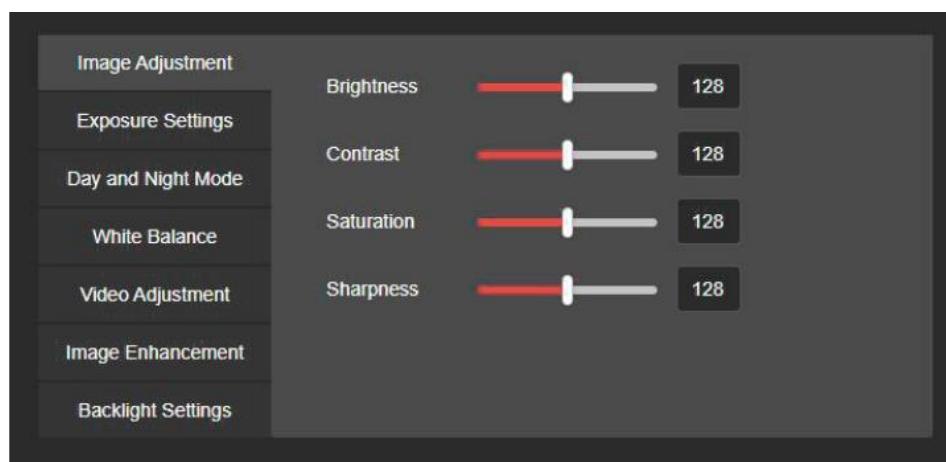


Рисунок 8-18

[Exposure settings (Настройки экспозиции)]: Здесь Вы можете просмотреть «Aperture Type (Тип диафрагмы)» камеры, задать «Exposure Time (Время экспозиции)» в соответствии с фактическими потребностями и автоматически сохранить значения после настройки (см. рисунок 8-19).

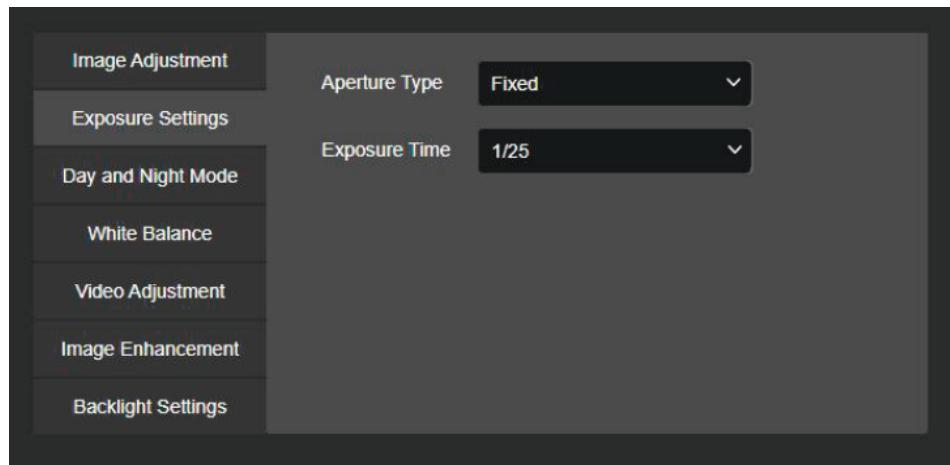


Рисунок 8-19

[Day and Night Switch (Переключение режимов День / Ночь)]: Настройки по умолчанию: «Fill Light Mode (Режим освещения изображения)» - «Auto (Автоматически)», «Sensitivity (Чувствительность)» - 3, «Filter Time (Время фильтрации)» - 3 секунды, «Light Mode (Режим подсветки)» - «Manual (Вручную)», «Brightness Adjustment (Регулировка яркости подсветки)» - 100, как показано на рисунке 8-20 ①. Если для параметра «Fill Light Mode (Режим освещения изображения)» выбран режим «Auto (Автоматически)», устройство включит режим освещения изображения в соответствии с фактическими условиями. Пользователь может переключать режим освещения изображения на «Daytime (Дневной)», «Night (Ночной)» и «Time (По времени)» в соответствии с фактическими условиями на объекте, а также изменять параметры «Sensitivity (Чувствительность)» и «Filter Time (Время фильтрации)» в соответствии с выбранным режимом освещения изображения.

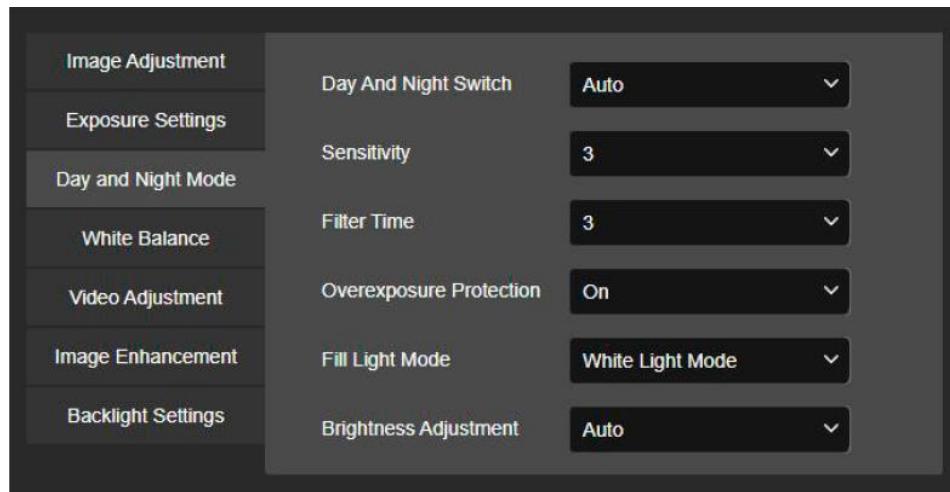


Рисунок 8-20 ①

- Если выбран режим «Time (По времени)», Вы можете задать «Dawn time (Время наступления рассвета)» и «Dark time (Время наступления заката)» (время начала и окончания освещения), а также «Light Brightness (Яркость подсветки)», как показано на рисунке 8-20 ②.

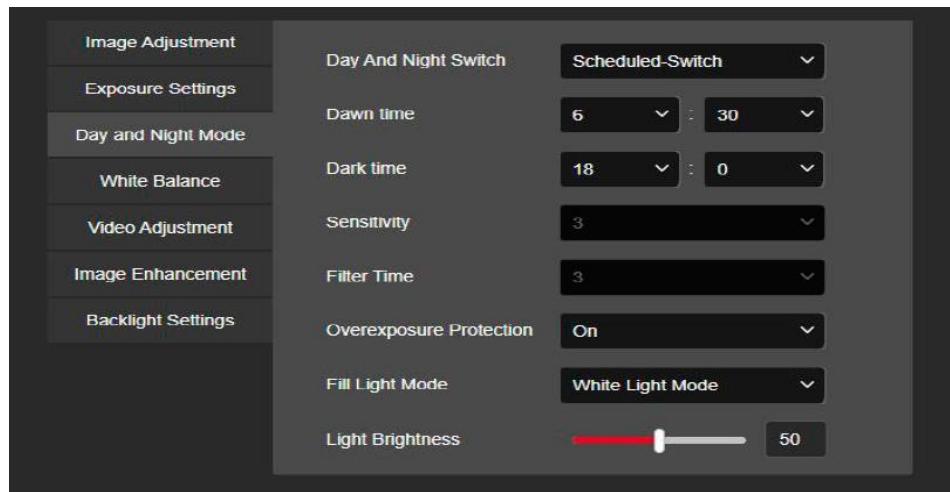


Рисунок 8-20 ②

- Если выбран режим «Daytime (Дневной)», подсветка всегда будет выключена, а камера будет работать в цветном режиме.
- Если выбран режим «Night (Ночной)», подсветка всегда будет включена.

Filter Time (Время фильтрации): Используется в тех случаях, когда при изменении освещенности подсветка часто включается и выключается, это может привести к ухудшению изображения, поэтому задается время фильтрации. В течение этого периода времени окружающий свет не мешает работе камеры.

Light brightness (Яркость подсветки): Используется для регулировки яркости подсветки, диапазон значений составляет 0-100.

[White Balance (Баланс белого):] Режим по умолчанию «Auto (Автоматически)», можно переключить на «Manual (Вручную)». Существует два типа автоматического баланса белого, которые могут удовлетворить потребности клиентов в различных сценариях (см. рисунок 8-21).

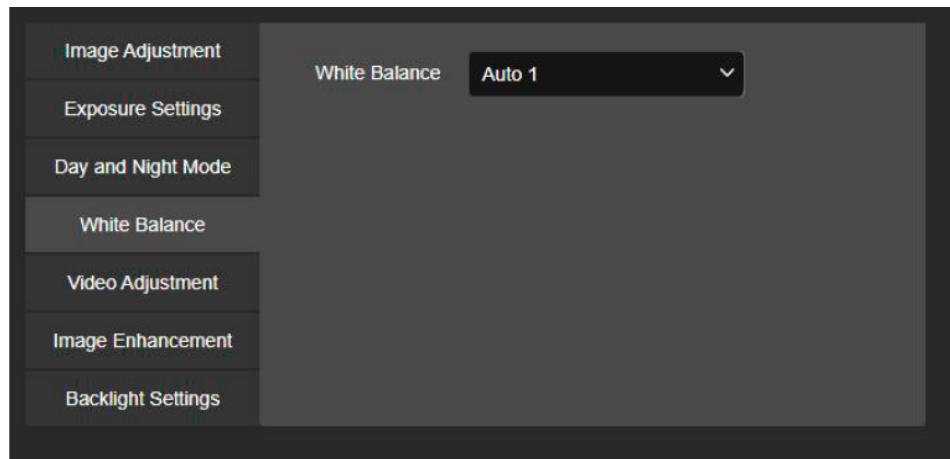


Рисунок 8-21

Manual white balance (Ручной баланс белого): Поддерживается настройка усиления красного и синего цветов, диапазон (0-255).

[Video adjustment (Регулировка видео):] Здесь Вы можете включить режимы «Mirroring (Зеркальное отображение)», «Corridor Mode (Коридорный режим)», а также задать «Video Format (Формат видео)», как показано на рисунке 8-22.

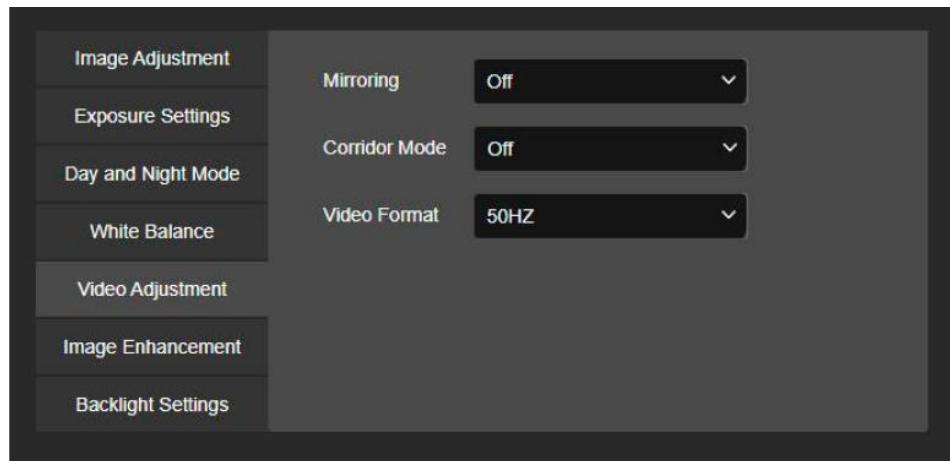


Рисунок 8-22

Mirroring (Зеркальное отображение): По умолчанию отключено (Off), в этом меню Вы можете выбрать режим отображения изображения – «Level (По горизонтали)», «Vertical (По вертикали)» или «Both (Оба)».

Corridor Mode (Коридорный режим): По умолчанию выключен (Off), включив коридорный режим, Вы можете настроить окно просмотра, повернув его 90 и 270 градусов.

Video Format (Формат видео): По умолчанию установлен PAL (50 Гц), в выпадающем меню Вы можете переключиться на NTSC (60 Гц). Для фактического изменения формата видео (чтобы оно вступило в силу) потребуется перезагрузка устройства.

[Image enhancement (Улучшение качества изображения)]: Здесь Вы можете настроить режимы WDR, DNR, режим устранения искажений, режим «антитуман» (см. рисунок 8-23).

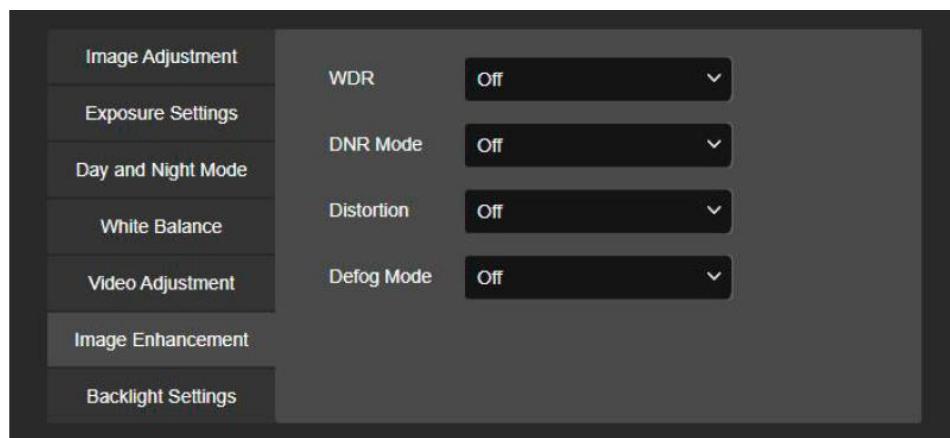


Рисунок 8-23

WDR: По умолчанию выключен («Off»), в выпадающем меню Вы можете переключиться на «Low (Низкий)», «Mid (Средний)» или «High (Высокий)» уровни.

DNR Mode (Режим шумоподавления): По умолчанию выключен («Off»), в выпадающем меню Вы можете переключиться на «Low (Низкий)», «Mid (Средний)» или «High (Высокий)» уровни.

Distortion (Устранение искажений): По умолчанию выключен («Off»), в выпадающем меню Вы можете включить его («On»).

Defog Mode (Режим «антитуман»): По умолчанию выключен («Off»), в выпадающем меню Вы можете переключиться на «Low (Низкий)», «Mid (Средний)» или «High (Высокий)» уровни.

[BackLight Settings (Настройки компенсации засветки)]: Используются для настройки «Backlight Compensation (Компенсация задней засветки изображения)» и «Strong Light Suppression (Подавление фронтальной засветки изображения)». По умолчанию выключены (Off), можно включить вручную, как показано на рисунке 8-24.

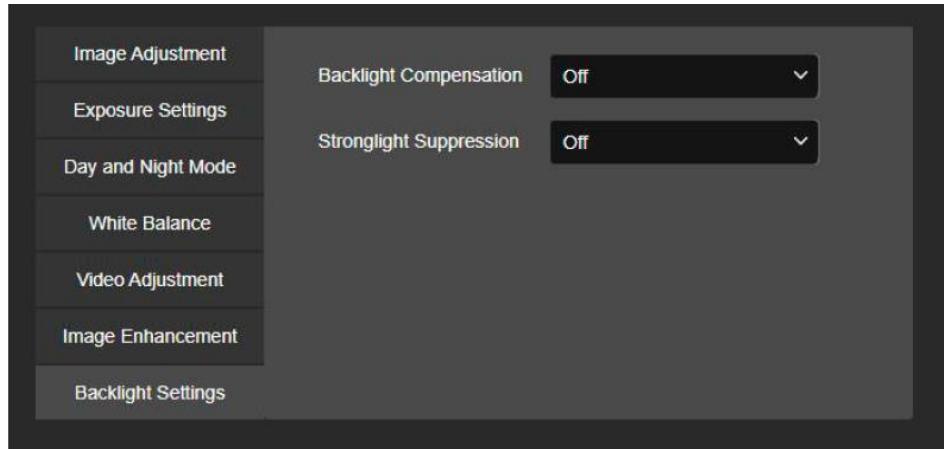


Рисунок 8-24



ПРИМЕЧАНИЕ:

- Окно настройки изображения камеры отображает только те функции, которые поддерживает устройство. Внешний вид окна данной функции зависит от конкретного устройства.
- Функции «WDR», «Backlight Compensation (Компенсация задней засветки изображения)» и «Strong Light Suppression (Подавление фронтальной засветки изображения)» являются взаимоисключающими. Включение одной из этих функций автоматически отключает две другие.

8.5.2. Экранное OSD-меню

Экранное OSD-меню – это информация, отображаемая на экране мониторинга в режиме реального времени. На экране IP-камеры могут быть отображены её имя, данные и дата.

Чтобы перейти в окно настройки экранного меню, выберите в главном окне меню «Configuration (Настройка)» → «Image (Изображение)» → «OSD». В этом окне Вы можете настроить отображение меню времени, текста экранного меню и другой информации в окне просмотра видео, как показано на рисунке 8-25.

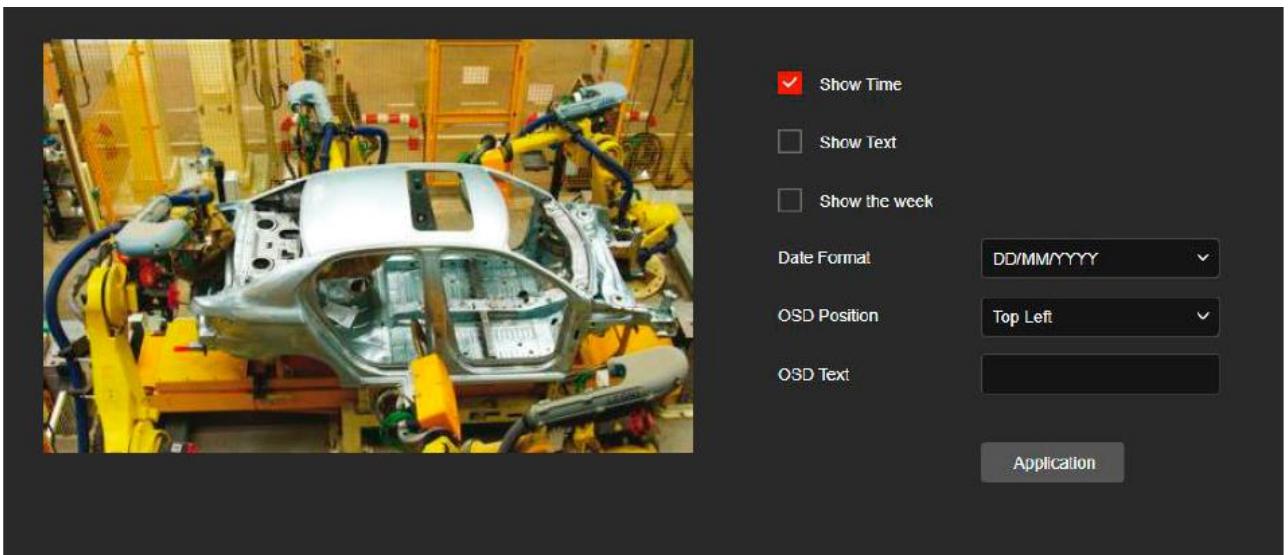


Рисунок 8-25

[Time (Время)]: Включение / выключение отображения времени в окне просмотра видео.

[Text (Текст)]: Включение / выключение отображения экранного текста в окне просмотра видео.

[Show the week (Отображать неделю)]: Включение / выключение отображения недели в окне просмотра видео Вы можете выбрать язык: «English (Английский)» или «Chinese (Китайский)».

[Date Format (Формат даты)]: Настройте формат отображения даты в окне просмотра видео: (ДД / ММ / ГГГГ) по умолчанию, опции: (ММ / ДД / ГГГГ) или (ГГГГ / ММ / ДД).

[OSD Position (Положение OSD-меню)]: Задайте положение OSD-меню в окне просмотра видео, по умолчанию – «Top_Left (Вверху_Слева)», опция - «Bottom_Left (Внизу_Слева)».

[OSD Text (Текст OSD-меню)]: Введите текст для отображение в окне просмотра видео, например, «Лифтовый холл», «У двери в холле» или другие сведения о местоположении оборудования.

8.6. События

В главном окне выберите путь «Configuration (Настройка)» → «Events (События)», чтобы перейти в окно настройки событий, обычных и интеллектуальных.

8.6.1. Обычные события

В окне настройки обычных событий Вы можете ввести настройки таких функций устройства как Обнаружение движения, Зоны конфиденциальности, Обнаружение закрытия объектива, Обнаружение нештатных ситуаций, Ввод / вывод тревог, Вывод звукового сигнала тревоги и Настройку зон интереса и другие события.

① Обнаружение движения

Функция обнаружения движения используется для определения наличия движущегося объекта в определенной области в течение определенного периода времени. При обнаружении движущегося объекта IP-камера подает сигнал тревоги в соответствии с её настройками.

Выполните следующие действия:

Шаг 1: Чтобы вызвать окно настроек функции обнаружения движения, выберите в главном окне следующий путь «Configuration (Настройка)» → «Events (События)»→ «Ordinary Events (Обычные события)» → «Motion Detection (Обнаружение движения)», как показано на рисунке 8-26.

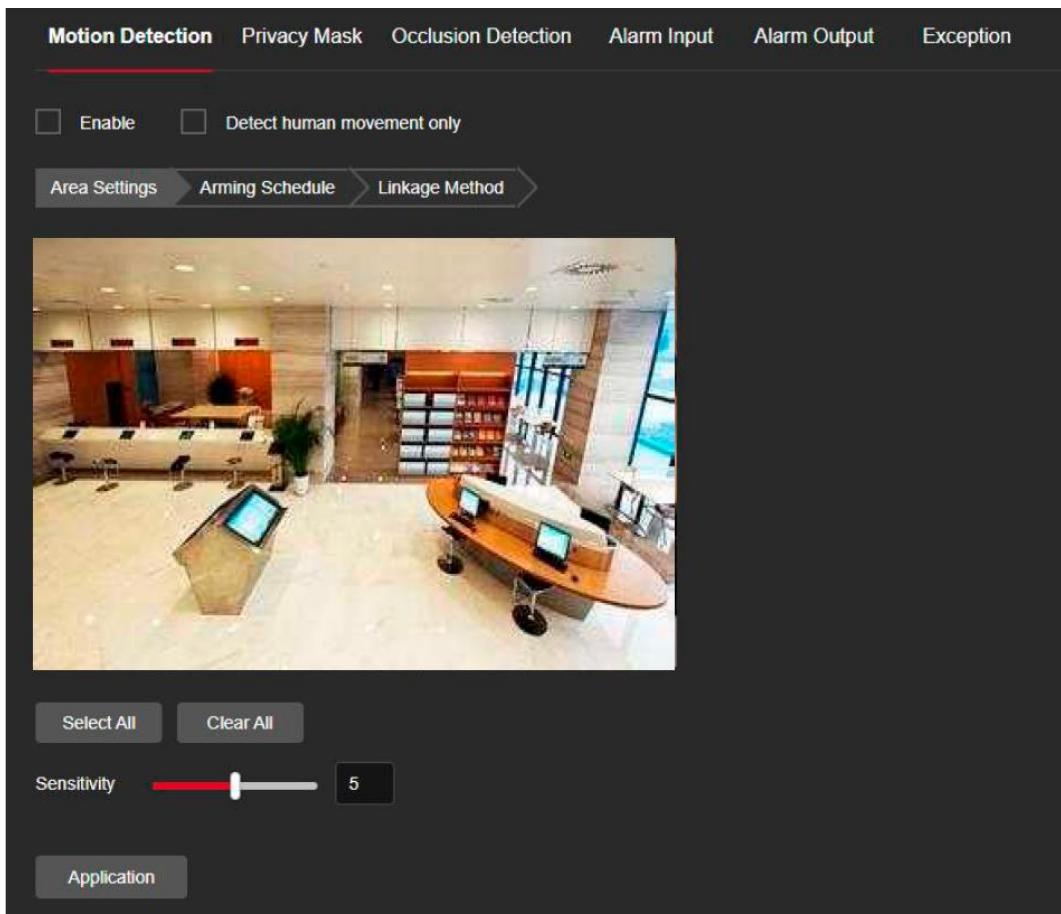


Рисунок 8-26

Шаг 2: Нажмите на «Enable (Включить)» или «Detect human movement only (Обнаруживать только движение человека)», чтобы включить сигнализацию обнаружения движения.

Шаг 3: Выберите область, чтобы настроить для неё чувствительность обнаружения движения, нажмите на «Application (Применить)».

[Select All (Выбрать всё)]: Диапазон обнаружения движения позволяет контролировать всю область, которая состоит из 396 (22*18) небольших квадратных фрагментов.

[Manually draw the alarm area (Нарисовать область сигнализации вручную)]: Наведите курсор мыши на экран просмотра, нажмите левую кнопку мыши и выделите область обнаружения движения, затем отпустите левую кнопку мыши, чтобы завершить выбор области. Камера позволяет одновременно настраивать несколько зон обнаружения движения.

[Clear All (Очистить всё)]: Очистка всей области обнаружения движения, выбранной в данный момент.

[Sensitivity (Чувствительность)]: Значение по умолчанию равно 5, диапазон возможных значений – от 0 до 10. Чем выше заданное здесь значение, тем легче устройство генерирует сигнал тревоги.

Шаг 4: Задайте расписание осуществления контроля.

Как показано на рисунке 8-27, Вы можете просматривать, редактировать и удалять время осуществления контроля функцией обнаружения движения. По умолчанию контроль включен 24 часа в сутки. Вы можете настроить время контроля следующим образом.

- Метод 1: Щелкните по шкале времени осуществления контроля, вручную введите для него время начала и окончания, для сохранения настроек нажмите на «Application (Применить)». Если Вам нужно удалить период осуществления контроля, нажмите кнопку «Delete (Удалить)», а затем сбросьте период времени.
- Метод 2: Щелкните по шкале времени осуществления контроля, на обоих концах периода времени отобразятся две стрелки. Переместите стрелку настройки влево или вправо, чтобы настроить время осуществления контроля.
- Вы можете настроить более одного периода времени, максимум их может быть 8.
- По окончании настройки времени выполнения на контроля для целого дня, если для другого дня необходимо установить такое же время контроля, нажмите в правой части временной шкалы кнопку копирования «», в окне «Copy to (Копировать в)» установите флажок «Select All (Выбрать все)» или «Day (День)», затем нажмите «OK».
- После выполнения настройки нажмите на «Application (Применить)», чтобы завершить процедуру настройки времени осуществления контроля.



Рисунок 8-27



ПРИМЕЧАНИЕ:

- При настройке времени осуществления контроля следите за тем, чтобы никакие два периода времени не совпадали.

Шаг 5: Настройте способ оповещения о тревоге.

Способы оповещения о тревоге включают в себя как обычные методы оповещения («Upload Via SMTP (Загрузить по SMTP)», «Upload Via FTP (Загрузить на FTP)», «Upload Via Cloud (Загрузить на облако)», «Flash Warning (Мигание подсветки)», «Sound Alarm (Звуковое оповещение о тревоге)»), так и вывод сигнала тревоги через выход тревог («IO Output (Выход тревог)»), как показано на рисунке 8-28.

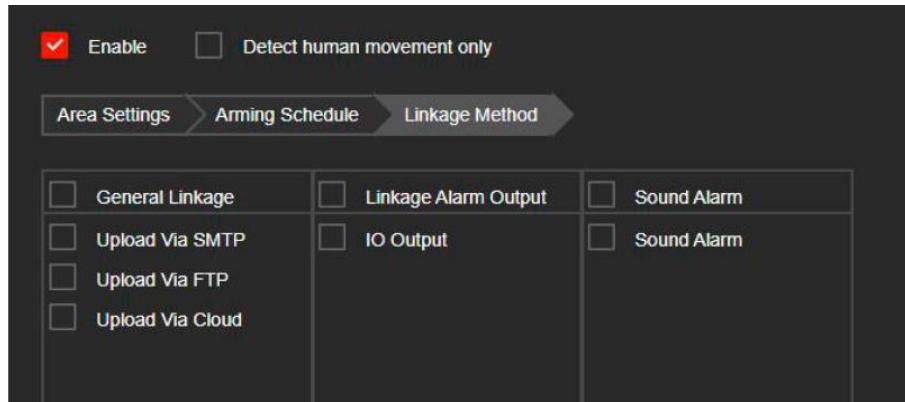


Рисунок 8-28

[Upload Via SMTP (Загрузить на SMTP): При выборе данной опции (если в системе настроен обмен по SMTP) информация о тревоге будет отправлена в почтовый ящик получателя SMTP.

[Upload Via FTP (Загрузить на FTP): При выборе данной опции (если в системе настроен обмен с FTP-сервером) информация о тревоге будет отправлена на FTP-сервер.

[Upload Via Cloud (Загрузить на облако): При выборе данной опции (если в системе настроен обмен с помощью облачного сервера) информация о тревоге будет отправлена в облачную учетную запись.

[Flash Warning (Мигание подсветки): При выборе этого метода сигнализации устройство будет сообщать о тревоге миганием лампы подсветки.

[IO Output (Выход тревог): При выборе данной опции убедитесь в том, что порт ввода-вывода сигналов подключен к устройству сигнализации. Во время тревоги камера передаст сигнал тревоги на это устройство.

[Sound Alarm (Звуковой сигнал тревоги): При выборе данной опции при тревоге устройство будет подавать звуковой сигнал.



ПРИМЕЧАНИЕ:

- Различные устройства поддерживают различные методы выдачи сигналов тревоги. Способ подачи сигнала тревоги зависит от конкретного устройства.

② Зоны конфиденциальности

Настройка зон конфиденциальности - это функция защиты конфиденциальности, которая блокирует просмотр и запись изображения определенных участков наблюдения.

Чтобы перейти к настройкам зон конфиденциальности, выберите в главном окне меню «Configuration (Настройка)» → «Event (События)» → «Ordinary Events (Обычные события)» → «Privacy Mask (Зоны конфиденциальности)», (см. рисунок 8-29).

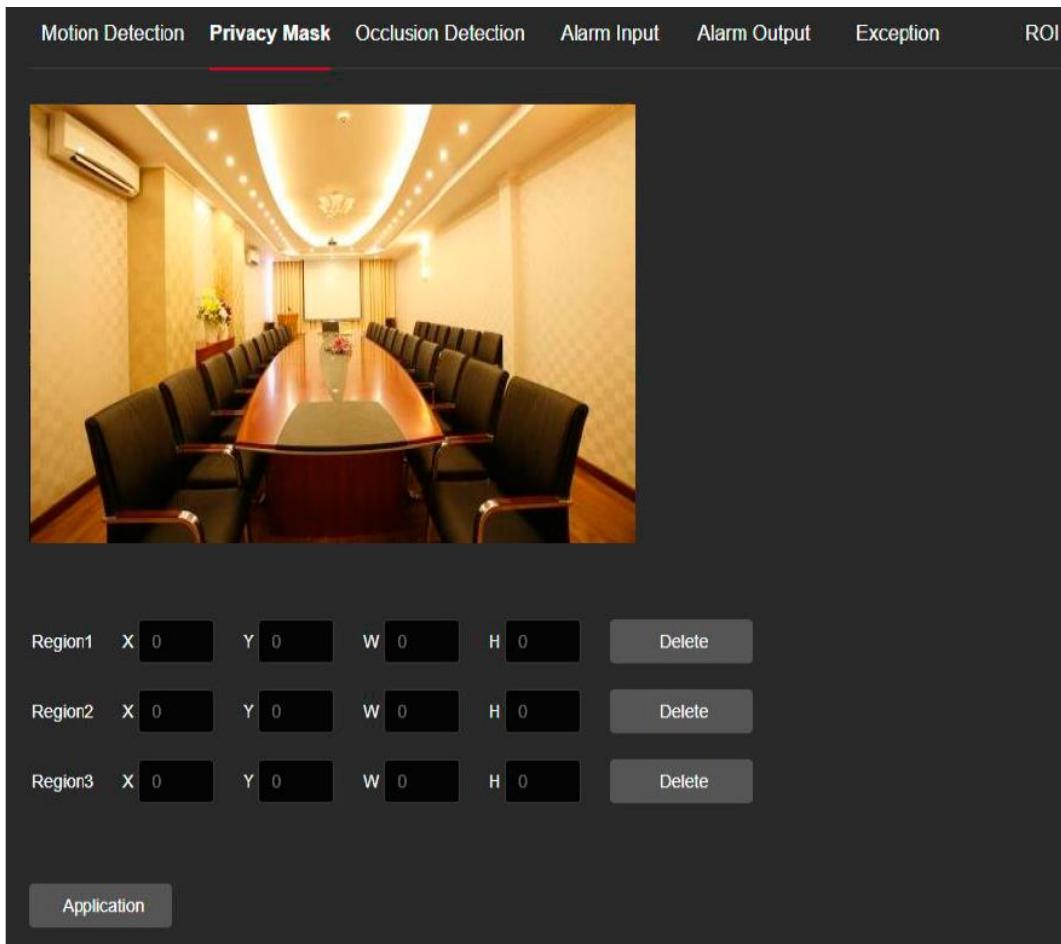


Рисунок 8-29

Здесь Вы можете выбрать до 3 зон конфиденциальности. Удерживая нажатой левую кнопку мыши, перетащите курсор мыши, чтобы выбрать нужную область в разделе «Area (Область)». «Region 1 (Область 1)», «Region 2 (Область 2)», «Region 3 (Область 3)» — рядом с ними будут показаны их соответствующие координаты, а также их ширина (W) и высота (H). Если Вы хотите удалить область, нажмите на соответствующую ей кнопку «Delete (Удалить)». После завершения настройки нажмите на «Application (Применить)».

③ Обнаружение закрытия объектива

Функция обнаружения закрытия объектива используется для определения того, заблокирована ли область мониторинга людьми или вследствие влияния других факторов в течение определенного периода времени. Если область мониторинга устройства заблокирована, IP-камера подает сигнал тревоги в соответствии со своими настройками. При появлении сигнала тревоги о закрытии объектива можно быстро устранить вызвавшую её причину и восстановить контроль в зоне мониторинга.

Выполните следующие действия:

Шаг 1: Чтобы вызвать окно настроек функции обнаружения закрытия объектива, выберите в главном окне следующий путь «Configuration (Настройка)» → «Events (События)»→ «Ordinary Events (Обычные события)» → «Occlusion Detection (Обнаружение закрытия объектива)», как показано на рисунке 8-30.

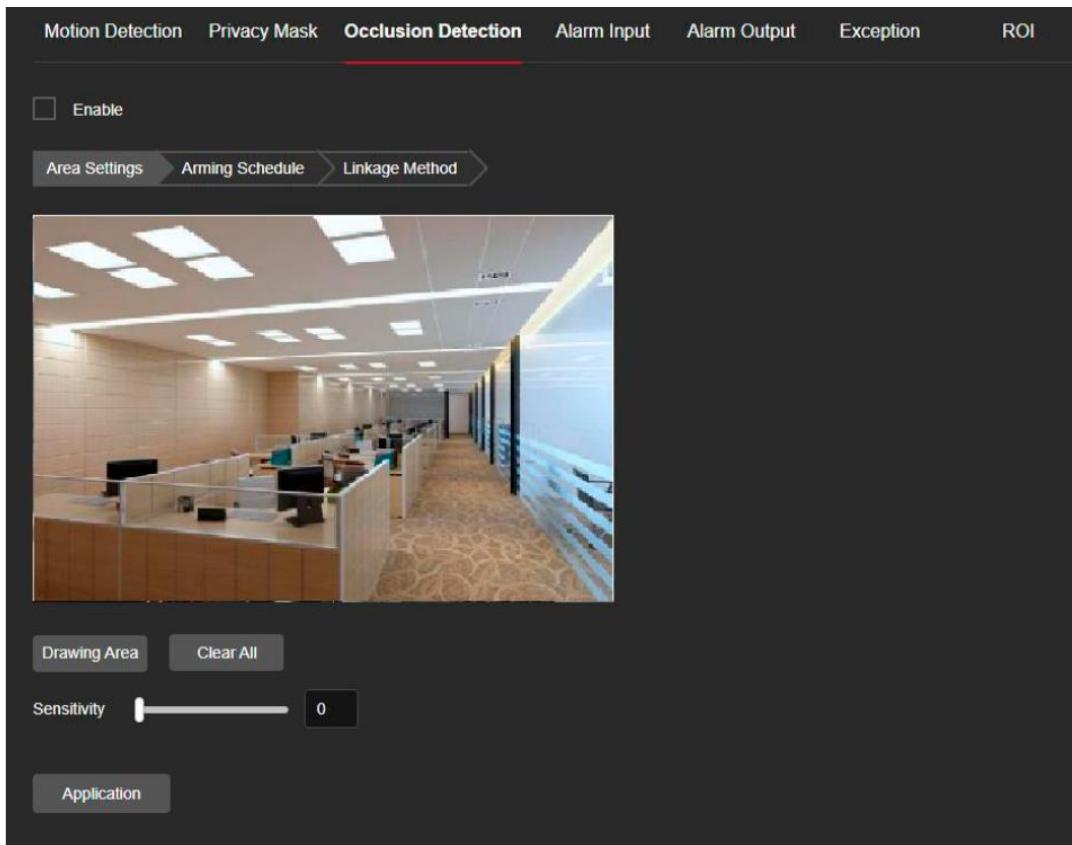


Рисунок 8-30

Шаг 2: Нажмите на «Enable (Включить)», чтобы включить сигнализацию о несанкционированном доступе к видео.

Шаг 3: Выберите область обнаружения закрытия объектива, чтобы настроить для неё чувствительность, нажмите на «Application (Применить)».

[Drawing Area (Область рисования): Наведите курсор мыши на экран просмотра, нажмите левую кнопку мыши и выделите область обнаружения, затем отпустите левую кнопку мыши, нажмите на «Stop Drawing (Остановить рисование)», чтобы завершить процесс выбора области обнаружения.

[Clear All (Очистить всё): Очистка всей области обнаружения закрытия объектива, выбранной в данный момент.

[Sensitivity (Чувствительность): Значение по умолчанию равно 0, можно выбрать значение в диапазоне от 0 до 2. Чем выше это значение, тем чувствительнее будет генерироваться оборудованием сигнал тревоги.

Шаг 4: Задайте расписание осуществления контроля.

Как показано на рисунке 8-31, Вы можете просматривать, редактировать и удалять время осуществления контроля функции обнаружения закрытия объектива. По умолчанию контроль включен 24 часа в сутки. Вы можете настроить время контроля следующим образом.

- Метод 1: Щелкните по шкале времени осуществления контроля, вручную введите для него время начала и окончания, для сохранения настроек нажмите на «Application (Применить)». Если Вам нужно удалить период осуществления контроля, нажмите кнопку «Delete (Удалить)», а затем сбросьте период времени.

- Метод 2: Щелкните по шкале времени осуществления контроля, на обоих концах периода времени отобразятся две стрелки. Переместите стрелку настройки влево или вправо, чтобы настроить время осуществления контроля.
- Вы можете настроить более одного периода времени, максимум их может быть 8.
- По окончании настройки времени выполнения на контроля для целого дня, если для другого дня необходимо установить такое же время контроля, нажмите в правой части временной шкалы кнопку копирования «», в окне «Copy to (Копировать в)» установите флажок «Select All (Выбрать все)» или «Day (День)», затем нажмите «OK».
- После выполнения настройки нажмите на «Application (Применить)», чтобы завершить процедуру настройки времени осуществления контроля.

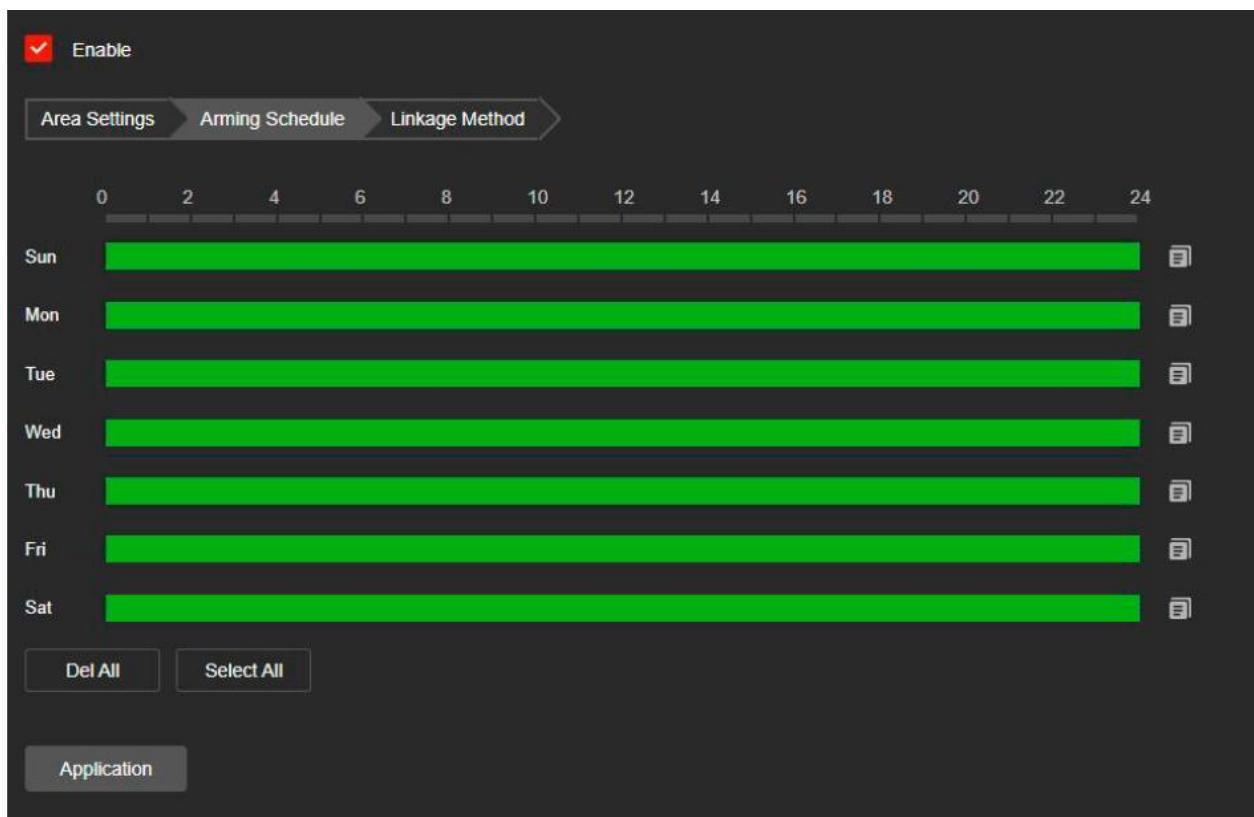


Рисунок 8-31



ПРИМЕЧАНИЕ:

- При настройке времени осуществления контроля следите за тем, чтобы никакие два периода времени не совпадали.

Шаг 5: Настройте способ оповещения о тревоге.

Способы оповещения о тревоге включают в себя как обычные методы оповещения («Upload Via SMTP (Загрузить по SMTP)», «Upload Via FTP (Загрузить на FTP)», «Upload Via Cloud (Загрузить на облако)», «Flash Warning (Мигание подсветки)», «Sound Alarm (Звуковое оповещение о тревоге)»), так и вывод сигнала тревоги через выход тревог («IO Output (Выход тревог)»), как показано на рисунке 8-32.

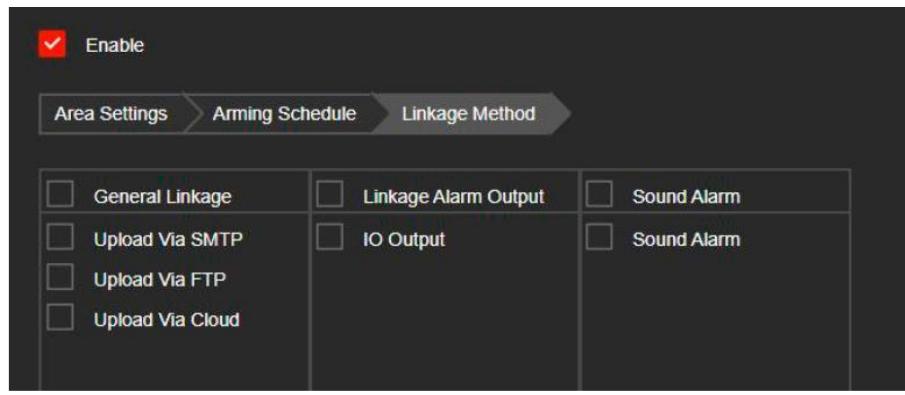


Рисунок 8-32

[Upload Via SMTP (Загрузить на SMTP): При выборе данной опции (если в системе настроен обмен по SMTP) информация о тревоге будет отправлена в почтовый ящик получателя SMTP.

[Upload Via FTP (Загрузить на FTP): При выборе данной опции (если в системе настроен обмен с FTP-сервером) информация о тревоге будет отправлена на FTP-сервер.

[Upload Via Cloud (Загрузить на облако): При выборе данной опции (если в системе настроен обмен с помощью облачного сервера) информация о тревоге будет отправлена в облачную учетную запись.

[Flash Warning (Мигание подсветки): При выборе этого метода сигнализации устройство будет сообщать о тревоге миганием лампы подсветки.

[IO Output (Выход тревог): При выборе данной опции убедитесь в том, что порт ввода-вывода сигналов подключен к устройству сигнализации. Во время тревоги камера передаст сигнал тревоги на это устройство.

[Sound Alarm (Звуковой сигнал тревоги): При выборе данной опции при тревоге устройство будет подавать звуковой сигнал.



ПРИМЕЧАНИЕ:

- Различные устройства поддерживают различные методы выдачи сигналов тревоги. Способ подачи сигнала тревоги зависит от конкретного устройства.

④ Ввод тревог

Важно!

Перед выполнением настройки камеры необходимо подключить к устройству ввода сигнала тревоги. Если в камере настроен ввод тревоги, то сигнал тревоги, полученный от устройства ввода тревоги, может быть передан в IP-камеру для дальнейшей обработки.

Выполните следующие действия:

Шаг 1: Чтобы перейти к настройкам входа тревог, выберите в главном меню «Configuration (Настройка)» → «Event (События)» → «Ordinary Events (Обычные события)» → «Alarm Input (Ввод тревог)».

Шаг 2: Выберите вход тревоги и его тип (NO (нормально-разомкнутый), NC (нормально-замкнутый)).

Шаг 3: Задайте расписание осуществления контроля.

Как показано на рисунке 8-33, Вы можете просматривать, редактировать и удалять время осуществления контроля ввода тревог. По умолчанию контроль включен 24 часа в сутки. Вы можете настроить время контроля следующим образом.

- Метод 1: Щелкните по шкале времени осуществления контроля, вручную введите для него время начала и окончания, для сохранения настроек нажмите на «Application (Применить)». Если Вам нужно удалить период осуществления контроля, нажмите кнопку «Delete (Удалить)», а затем сбросьте период времени.
- Метод 2: Щелкните по шкале времени осуществления контроля, на обоих концах периода времени отобразятся две стрелки. Переместите стрелку настройки влево или вправо, чтобы настроить время осуществления контроля.
- Вы можете настроить более одного периода времени, максимум их может быть 8.
- По окончании настройки времени выполнения на контроля для целого дня, если для другого дня необходимо установить такое же время контроля, нажмите в правой части временной шкалы кнопку копирования «», в окне «Copy to (Копировать в)» установите флажок «Select All (Выбрать все)» или «Day (День)», затем нажмите «OK».
- После выполнения настройки нажмите на «Application (Применить)», чтобы завершить процедуру настройки времени осуществления контроля.

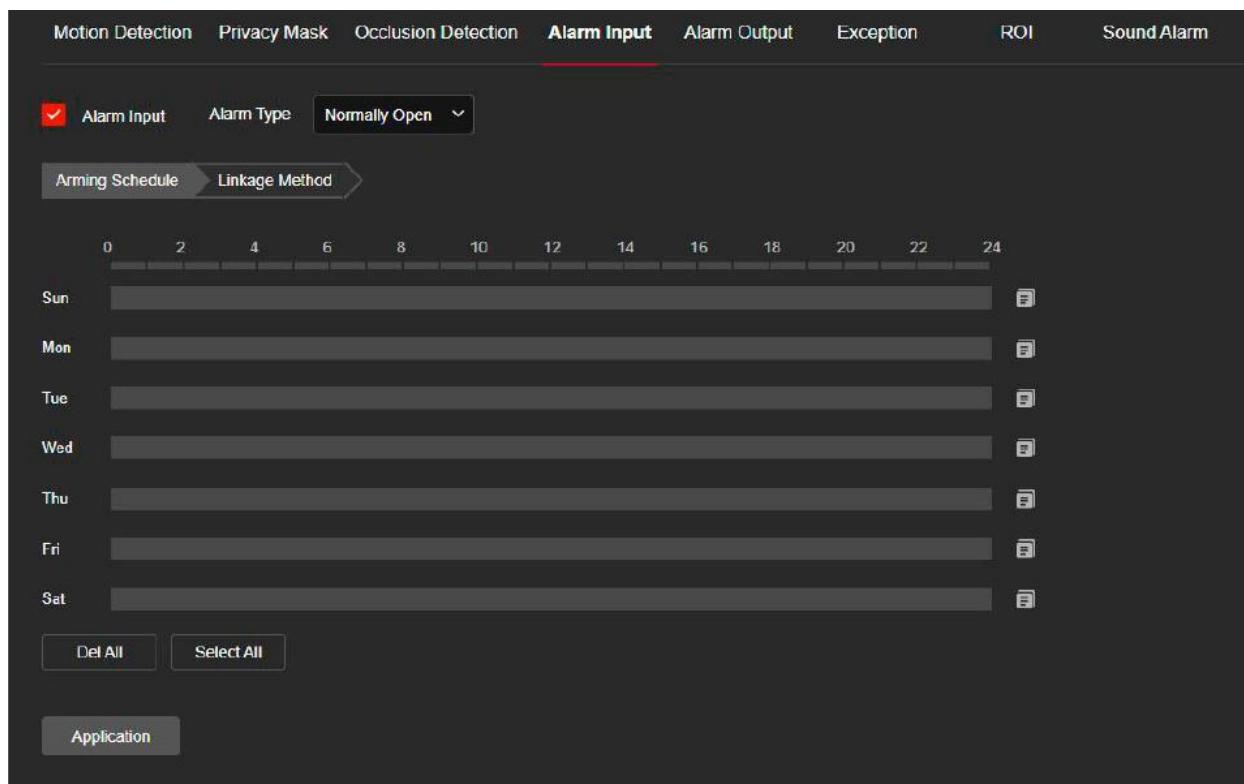


Рисунок 8-33

Шаг 4: Настройте способ оповещения о тревоге.

Способы оповещения о тревоге включают в себя как обычные методы оповещения («Upload Via SMTP (Загрузить по SMTP)», «Upload Via FTP (Загрузить на FTP)», «Upload Via Cloud (Загрузить на облако)», «Flash Warning (Мигание подсветки)», «Sound Alarm (Звуковое оповещение о тревоге)»), так и вывод сигнала тревоги через выход тревог («IO Output (Выход тревог)»), как показано на рисунке 8-34.

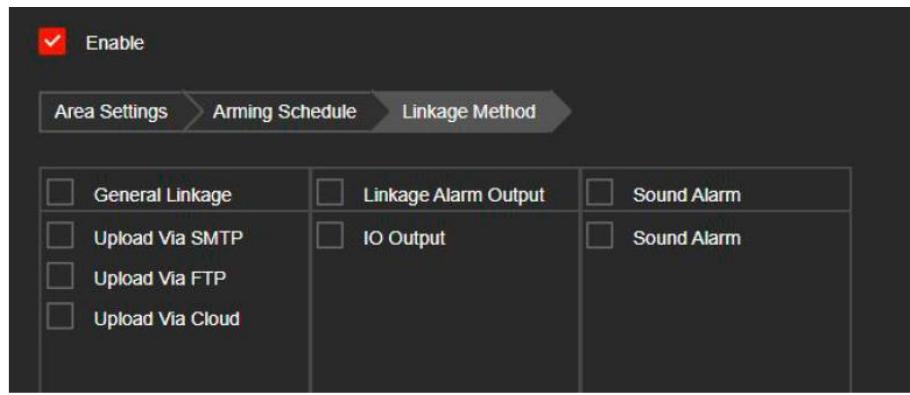


Рисунок 8-34

[Upload Via SMTP (Загрузить на SMTP):] При выборе данной опции (если в системе настроен обмен по SMTP) информация о тревоге будет отправлена в почтовый ящик получателя SMTP.

[Upload Via FTP (Загрузить на FTP):] При выборе данной опции (если в системе настроен обмен с FTP-сервером) информация о тревоге будет отправлена на FTP-сервер.

[Upload Via Cloud (Загрузить на облако):] При выборе данной опции (если в системе настроен обмен с помощью облачного сервера) информация о тревоге будет отправлена в облачную учетную запись.

[Flash Warning (Мигание подсветки):] При выборе этого метода сигнализации устройство будет сообщать о тревоге миганием лампы подсветки.

[IO Output (Выход тревог):] При выборе данной опции убедитесь в том, что порт ввода-вывода сигналов подключен к устройству сигнализации. Во время тревоги камера передаст сигнал тревоги на это устройство.

[Sound Alarm (Звуковой сигнал тревоги):] При выборе данной опции при тревоге устройство будет подавать звуковой сигнал.



ПРИМЕЧАНИЕ:

- Различные устройства поддерживают различные методы выдачи сигналов тревоги. Способ подачи сигнала тревоги зависит от конкретного устройства.

⑤ Вывод тревог

Важно!

Перед выполнением настройки камеры необходимо подключить к устройству вывода тревоги. Если в камере настроен вывод тревоги, то сигнал тревоги, полученный устройством ввода тревоги, может быть передан в IP-камеру для дальнейшей обработки.

Выполните следующие действия:

Шаг 1: Чтобы перейти к настройкам выхода тревог, выберите в главном окне меню «Configuration (Настройка)» → «Event (События)» → «Ordinary Events (Обычные события)» → «Alarm Output (Вывод тревог)»,

Шаг 2: Выберите значение для «Delay Time (Время задержки)».

Шаг 3: Задайте расписание осуществления контроля.

Как показано на рисунке 8-35, Вы можете просматривать, редактировать и удалять время осуществления контроля ввода тревог.

По умолчанию контроль включен 24 часа в сутки. Вы можете настроить время контроля следующим образом.

- Метод 1: Щелкните по шкале времени осуществления контроля, вручную введите для него время начала и окончания, для сохранения настроек нажмите на «Application (Применить)». Если Вам нужно удалить период осуществления контроля, нажмите кнопку «Delete (Удалить)», а затем сбросьте период времени.
- Метод 2: Щелкните по шкале времени осуществления контроля, на обоих концах периода времени отобразятся две стрелки. Переместите стрелку настройки влево или вправо, чтобы настроить время осуществления контроля.
- Вы можете настроить более одного периода времени, максимум их может быть 8.
- По окончании настройки времени выполнения на контроля для целого дня, если для другого дня необходимо установить такое же время контроля, нажмите в правой части временной шкалы кнопку копирования «», в окне «Copy to (Копировать в)» установите флажок «Select All (Выбрать все)» или «Day (День)», затем нажмите «OK».

Шаг 4: Нажмите на «Application (Применить)», чтобы завершить процедуру настройки времени осуществления контроля.

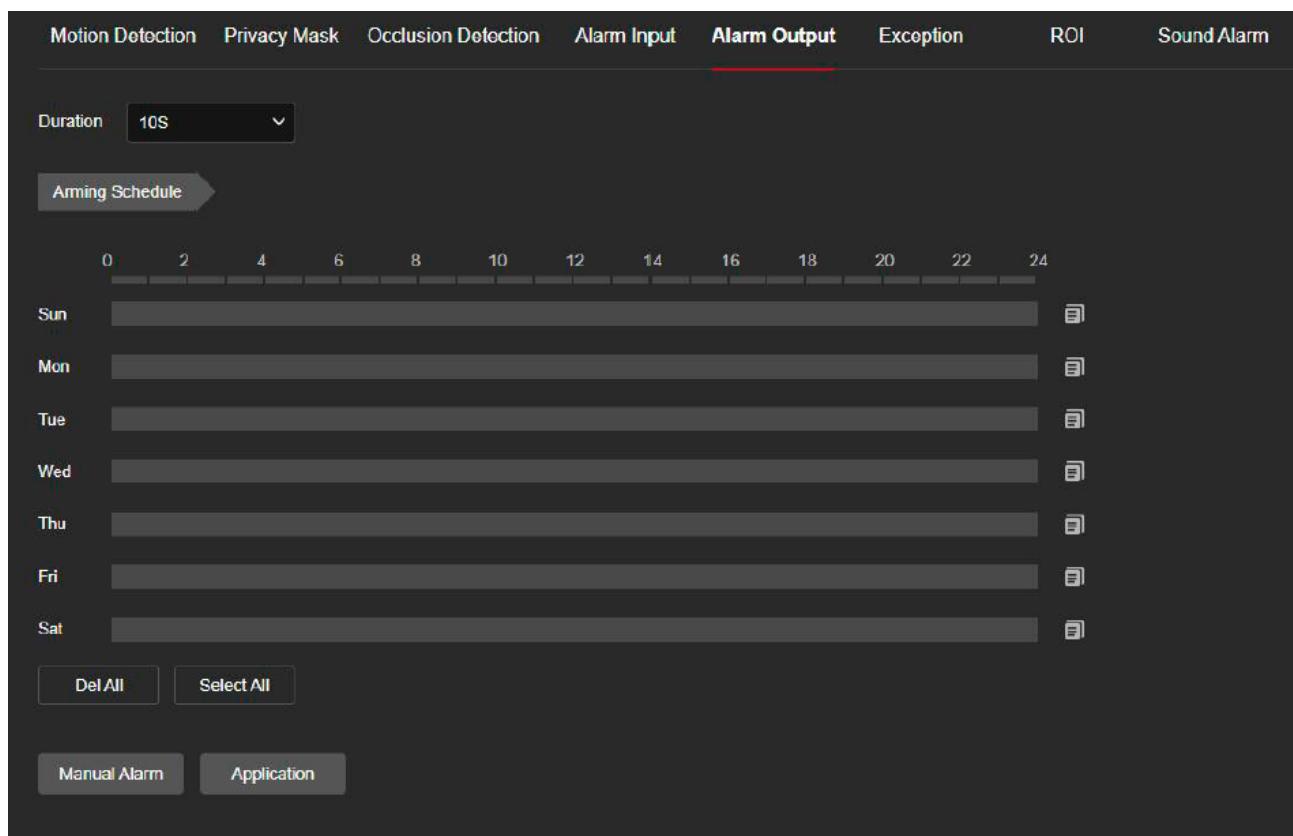


Рисунок 8-35

[Manual alarm (Отправка тревог вручную)]: Управление устройством вывода сигнала тревоги вручную – ручное подключение сигнала тревоги в окне вывода тревоги.

⑥ Обнаружение нештатных ситуаций

Настройте режим сигнализации о нештатных ситуациях. Когда во время работы IP-камеры происходит аномальное событие, система генерирует сигнал тревоги.

Выполните следующие действия:

Шаг 1: Чтобы перейти к настройкам обработки нештатных ситуаций, выберите в главном окне меню «Configuration (Настройка)» → «Event (События)» → «Ordinary Events (Обычные события)» → «Exception (Обнаружение нештатных ситуаций)», как показано на рисунке 8-36.

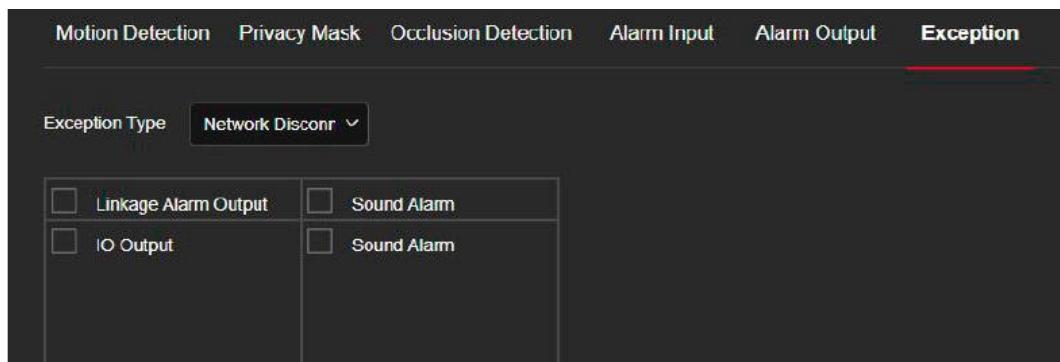


Рисунок 8-36

Шаг 2: Выберите тип нештатной ситуации и установите способ вывода сигнала тревоги.

Шаг 3: После завершения настроек нажмите на «Application (Применить)».

[IO Output (Выход тревог)]: При выборе данной опции убедитесь в том, что порт ввода-вывода сигналов подключен к устройству сигнализации. Во время тревоги камера передаст сигнал тревоги на это устройство.

[Sound Alarm (Звуковой сигнал тревоги)]: При выборе данной опции при тревоге устройство будет подавать звуковой сигнал.

⑦ Зоны интереса

Зоны интереса - это области интереса, с помощью этой функции пользователи могут настроить наблюдение наиболее интересующих областей на экране, IP-камера улучшит качество видеоизображения в соответствующей области при кодировании видео, снизит качество кодирования в других областях, чтобы подчеркнуть эффект изображения в выбранной области.

Выполните следующие действия:

Шаг 1: Чтобы вызвать окно настроек зон интереса, выберите в главном окне следующий путь «Configuration (Настройка)» → «Events (События)» → «Ordinary Events (Обычные события)» → «ROI (Зоны интереса)», как показано на рисунке 8-37.

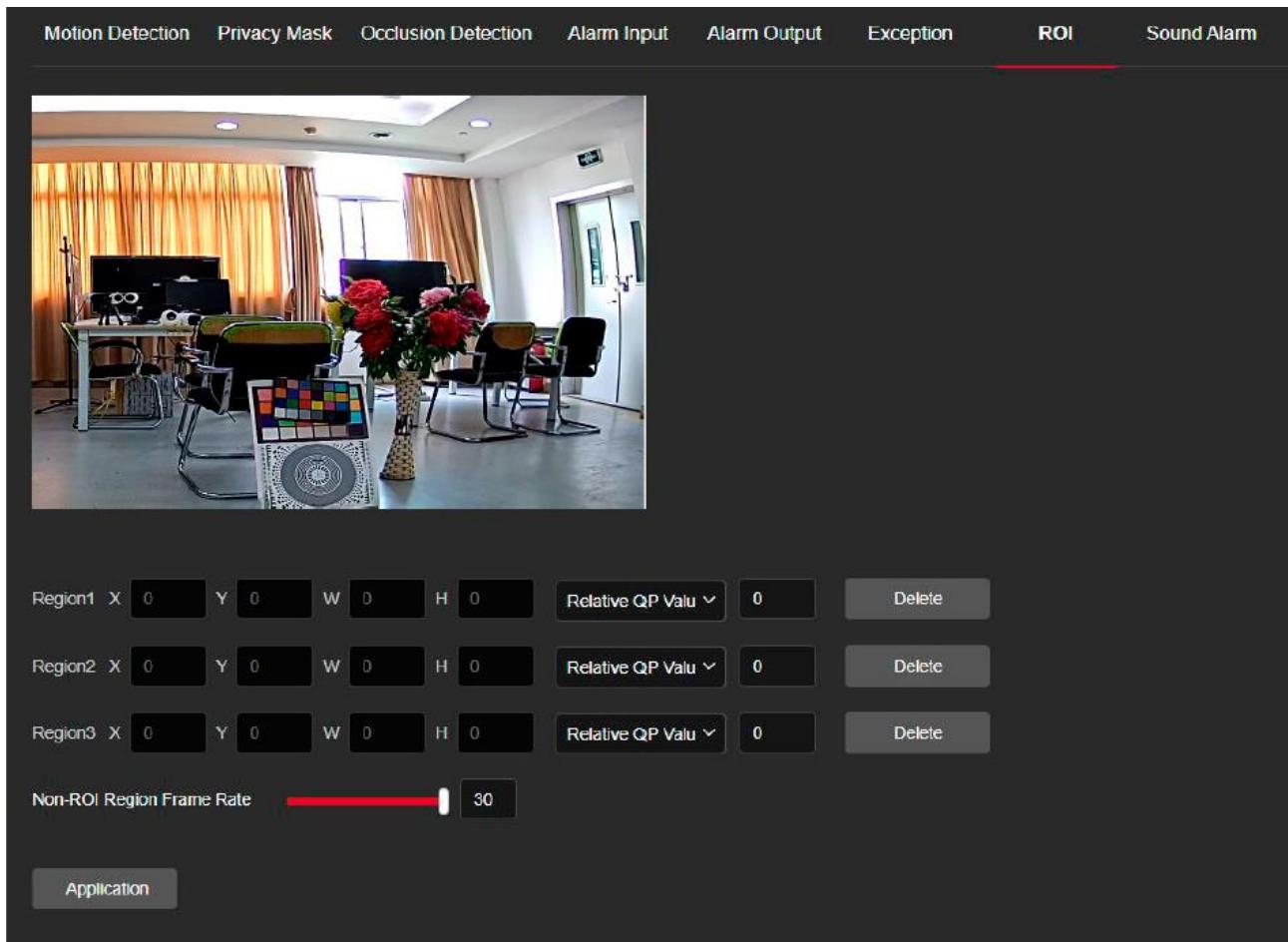


Рисунок 8-37

Шаг 2: [Region Settings (Настройка зон)]: Наведите курсор мыши на экран просмотра, нажмите левую кнопку мыши и выделите область зоны интереса, затем отпустите левую кнопку мыши, чтобы завершить выбор области. Вы также можете ввести соответствующие координаты X, Y, а также ширину (W) и высоту (H) соответствующей области, чтобы задать её.

Шаг 3: [Set «Relative QP value» or «Absolute QP value» (Задать «Относительное значение QP» или «Абсолютное значение QP»)]: Выберите «Относительное значение QP» или «Абсолютное значение QP» в соответствующей области и введите для них нужное значение.

Шаг 4: Сдвиньте полосу прокрутки так, чтобы установить частоту кадров для области, не относящейся к зонам интереса.

Шаг 5: Нажмите на «Application (Применить)», чтобы завершить настройку зон интереса.



ПРИМЕЧАНИЕ:

- Функция настройки зон интереса зависит от конкретной модели камеры, данная функция присутствует в моделях, в которых поддерживается кодировка H.264 или H.265. В настоящее время модели с другими типами кодирования видео не поддерживают функцию настройки зон интереса.
- Функция зон интереса более эффективна при использовании более низкой частоты кадров для зон, не являющихся зонами интереса.
- Чтобы удалить заданную Вами зону интереса, нажмите на «Delete (Удалить)»] в соответствующей области настроек.

⑧ Звуковое оповещение о тревоге

После настройки звукового оповещения о тревоге, при возникновении соответствующего события, динамик на устройстве может быть подключен к сигналу тревоги.

Выполните следующие действия:

Шаг 1: Чтобы вызвать окно настроек звукового оповещения о тревоге, выберите в главном окне следующий путь «Configuration (Настройка)» → «Events (События)»→ «Ordinary Events (Обычные события)» → «Sound Alarm (Звуковое оповещение о тревоге)», как показано на рисунке 8-38.

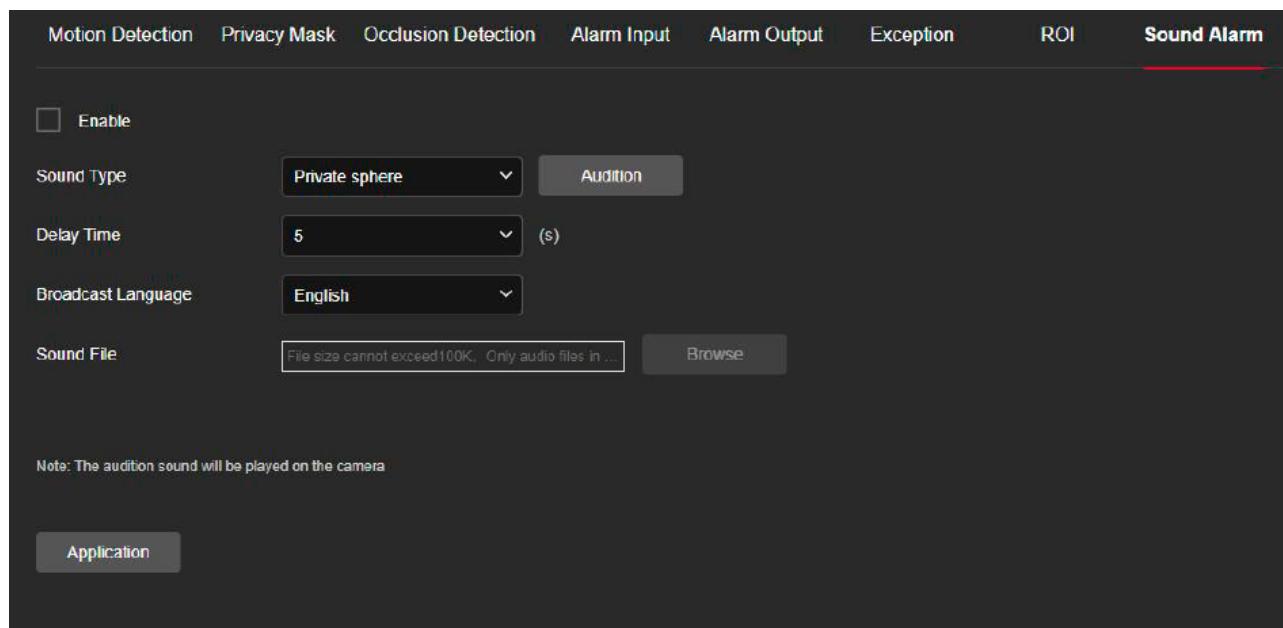


Рисунок 8-38

Шаг 2: Нажмите на «Enable (Включить)», чтобы включить звуковую сигнализацию о тревоге. Настройте тип звуковой сигнализации камеры, Вы можете выбрать из: «Private Area (Частная зона)», «Warning Area (Зона предупреждения)», «Surveillance Area (Зона наблюдения)», «Welcome (Приветствие)», «Deep Water Warning (Предупреждение о большой глубине)», «Dangerous Area (Опасная зона)», «Valuables (Ценные вещи)», «High Altitude Warning (Предупреждение о большой высоте)», «Custom (Пользовательский)».

Шаг 3: Задайте «Delay Time (Время задержки)»: по умолчанию оно рано 5 секунд, имеются опции 10, 20 и 30 секунд.

Шаг 4: Выберите язык оповещения – «Chinese (Китайский)» или «English (Английский)».

Шаг 5: Вы можете настроить загрузку звуковых файлов. Для этого Вам нужно выбрать опцию «Custom (Пользовательский)» в поле «Sound type (Тип звука)», а затем выбрать свой собственный звуковой файл для загрузки (поддерживается только один звуковой файл, его размер не может превышать 100 Кб, поддерживается только формат G711U).



ПРИМЕЧАНИЕ:

- Некоторые камеры не поддерживают звуковую сигнализацию. Внешний вид окна данной функции зависит от конкретного устройства.

8.6.2. Интеллектуальные события

① Обнаружение вторжения

Функция обнаружения вторжения используется для определения того, входит ли кто-либо в заданную зону в поле наблюдения камеры, сигнал тревоги включается в соответствии с результатом оценки.

Выполните следующие действия:

Шаг 1: Чтобы вызвать окно настроек функции обнаружения вторжения, выберите в главном окне следующий путь «Configuration (Настройка)» → «Events (События)»→ «Smart Event (Интеллектуальные события)» → «Intrusion Detection (Обнаружение вторжения)», как показано на рисунке 8-39.

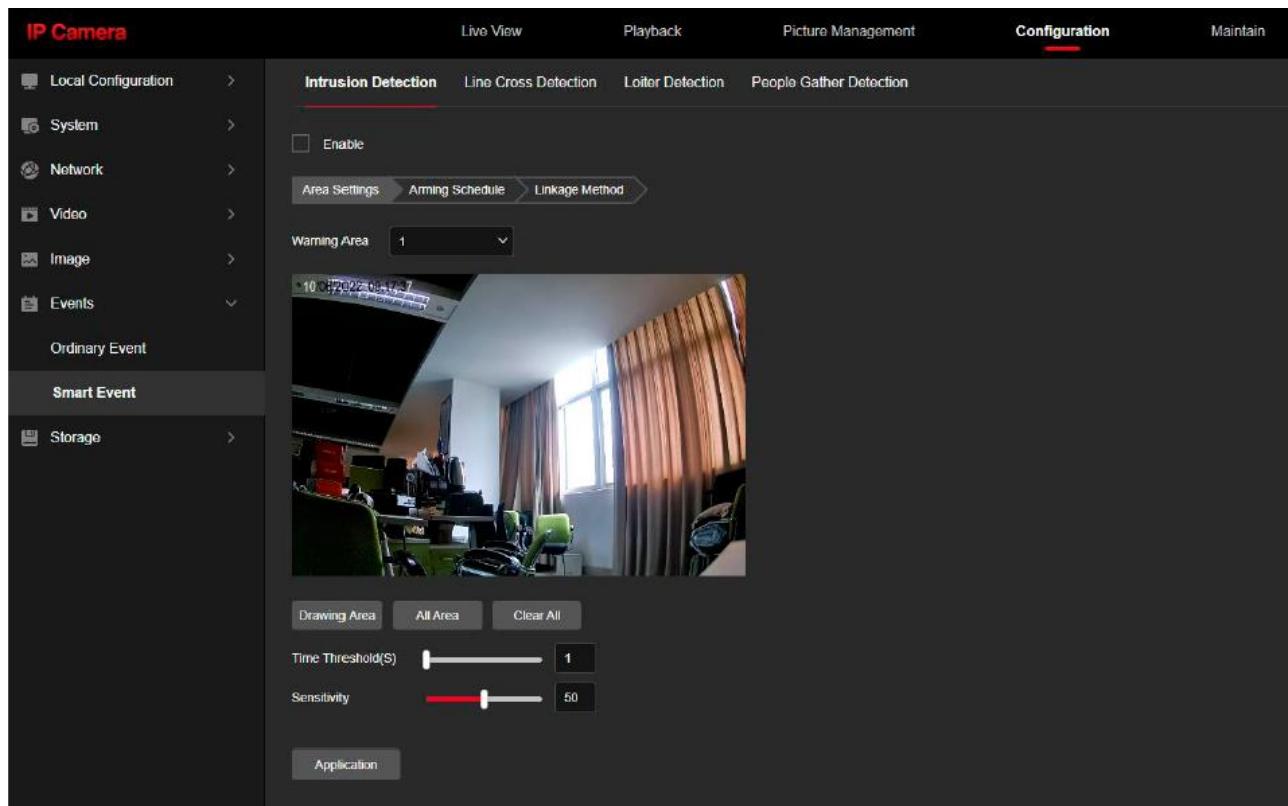


Рисунок 8-39

Шаг 2: Установите флажок «Enable (Включить)», чтобы включить функцию обнаружения вторжения.

Шаг 3: Выберите параметр «Warn Region (Область контроля)». Система поддерживает настройку до 4 областей контроля. После выбора областей контроля Вам необходимо выполнить следующие настройки. После ввода настройки нажмите на «Save (Сохранить)».

[Drawing Area (Область рисования)]: Нажмите на «Drawing Area Область рисования», наведите курсор мыши на экран просмотра, нажмите левую кнопку мыши, выделите четырехугольную область контроля, затем щелкните на окне просмотра, чтобы завершить рисование области.

[All Area (Вся область)]: Если требуется контролировать все области, нажмите на «All Area (Вся область)», чтобы автоматически выбрать все области.

[Clear All (Очистить всё)]: Используется для удаления выбранной области контроля.

[Time Threshold(s) (Временной порог (и))]: Для подачи сигнала тревоги необходимо, чтобы объект вошел в область контроля и оставался в ней в течение этого времени. Если установлено значение, равное 5 секундам, целевая область контроля запустит сигнал тревоги через 5 секунд.

[Sensitivity (Чувствительность]): Используется для настройки чувствительности обнаружения вторжения в области контроля. Значение по умолчанию равно 50. Перетащите индикатор или введите значение непосредственно в поле значения, чтобы изменить чувствительность. Чем выше это значение, тем выше чувствительность срабатывания сигнала тревоги.

Шаг 4: Если Вам нужно задать другую область контроля, повторите шаг 3 для завершения настройки.

Шаг 5: Задайте расписание осуществления контроля.

Как показано на рисунке 8-40, Вы можете просматривать, редактировать и удалять время осуществления контроля функции обнаружения вторжения. По умолчанию контроль включен 24 часа в сутки. Вы можете настроить время контроля следующим образом.

- Метод 1: Щелкните по шкале времени осуществления контроля, вручную введите для него время начала и окончания, для сохранения настроек нажмите на «Application (Применить)». Если Вам нужно удалить период осуществления контроля, нажмите кнопку «Delete (Удалить)», а затем сбросьте период времени.
- Метод 2: Щелкните по шкале времени осуществления контроля, период времени отобразится двумя кружками на обоих концах, курсор мыши переместится на кружок, передвигните стрелку настройки влево и вправо, чтобы задать время контроля.
- Вы можете настроить более одного периода времени, максимум их может быть 8.
- По окончании настройки времени выполнения на контроля для целого дня, если для другого дня необходимо установить такое же время контроля, нажмите в правой части временной шкалы кнопку копирования «», в окне «Copy to (Копировать в)» установите флажок «Select All (Выбрать все)» или «Day (День)», затем нажмите «OK».
- После выполнения настройки нажмите на «Application (Применить)», чтобы завершить процедуру настройки времени осуществления контроля.

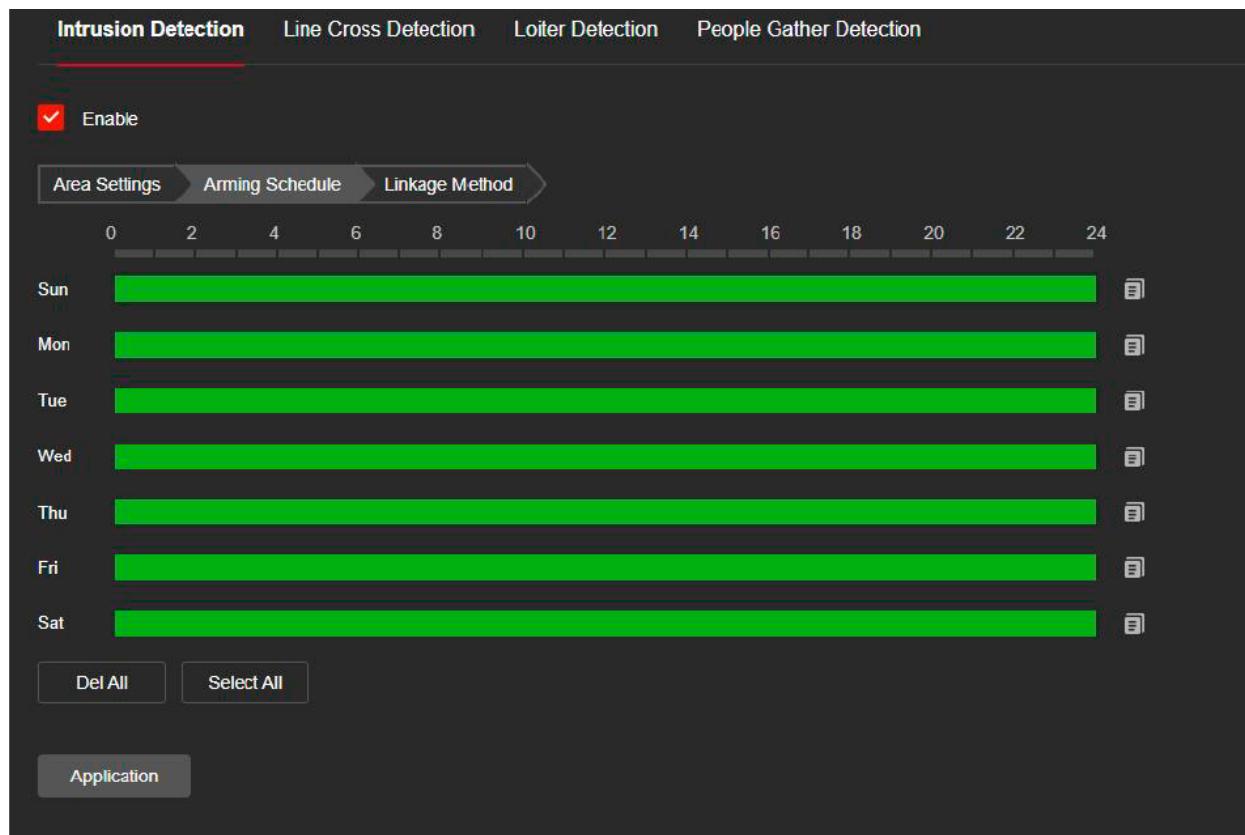


Рисунок 8-40



ПРИМЕЧАНИЕ:

- При настройке времени осуществления контроля следите за тем, чтобы никакие два периода времени не совпадали.

Шаг 6: Выберите нужный Вам метод выдачи сигналов тревоги.

Способы оповещения о тревоге включают в себя как обычные методы оповещения («Upload Via SMTP (Загрузить по SMTP)», «Upload Via FTP (Загрузить на FTP)», «Upload Via Cloud (Загрузить на облако)», «Flash Warning (Мигание подсветки)», «Sound Alarm (Звуковое оповещение о тревоге)»), так и вывод сигнала тревоги через выход тревог («IO Output (Выход тревог)»), как показано на рисунке 8-41.

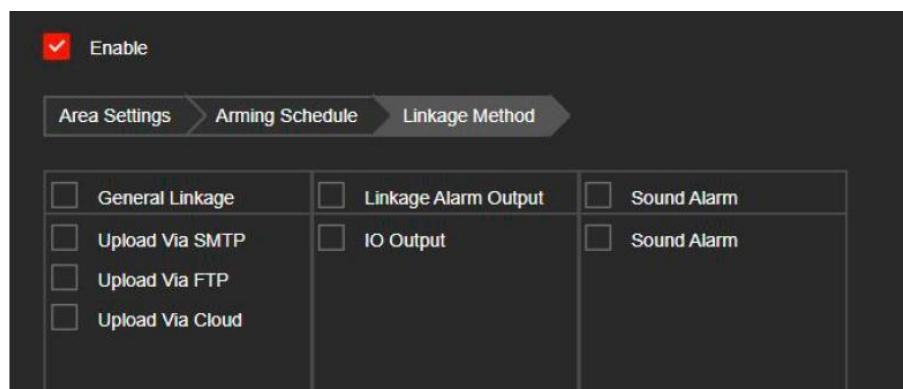


Рисунок 8-41

[Upload Via SMTP (Загрузить на SMTP): При выборе данной опции (если в системе настроен обмен по SMTP) информация о тревоге будет отправлена в почтовый ящик получателя SMTP.

[Upload Via FTP (Загрузить на FTP): При выборе данной опции (если в системе настроен обмен с FTP-сервером) информация о тревоге будет отправлена на FTP-сервер.

[Upload Via Cloud (Загрузить на облако): При выборе данной опции (если в системе настроен обмен с помощью облачного сервера) информация о тревоге будет отправлена в облачную учетную запись.

[Flash Warning (Мигание подсветки): При выборе этого метода сигнализации устройство будет сообщать о тревоге миганием лампы подсветки.

[IO Output (Выход тревог): При выборе данной опции убедитесь в том, что порт ввода-вывода сигналов подключен к устройству сигнализации. Во время тревоги камера передаст сигнал тревоги на это устройство.

[Sound Alarm (Звуковой сигнал тревоги): При выборе данной опции при тревоге устройство будет подавать звуковой сигнал.



ПРИМЕЧАНИЕ:

- Различные устройства поддерживают различные методы выдачи сигналов тревоги. Способ подачи сигнала тревоги зависит от конкретного устройства.

② Обнаружение пересечения линии

Функция обнаружения пересечения линии используется для определения того, присутствует ли на видео объект, пересекающий заданную линию контроля. В соответствии с результатом такой оценки включается оповещение о тревоге.

Выполните следующие действия:

Шаг 1: Чтобы вызвать окно настроек функции обнаружения пересечения линии, выберите в главном окне следующий путь «Configuration (Настройка)» → «Events (События)»→ «Smart Event (Интеллектуальные события)» → «Line Cross Detection (Обнаружение пересечения линии)», как показано на рисунке 8-42.

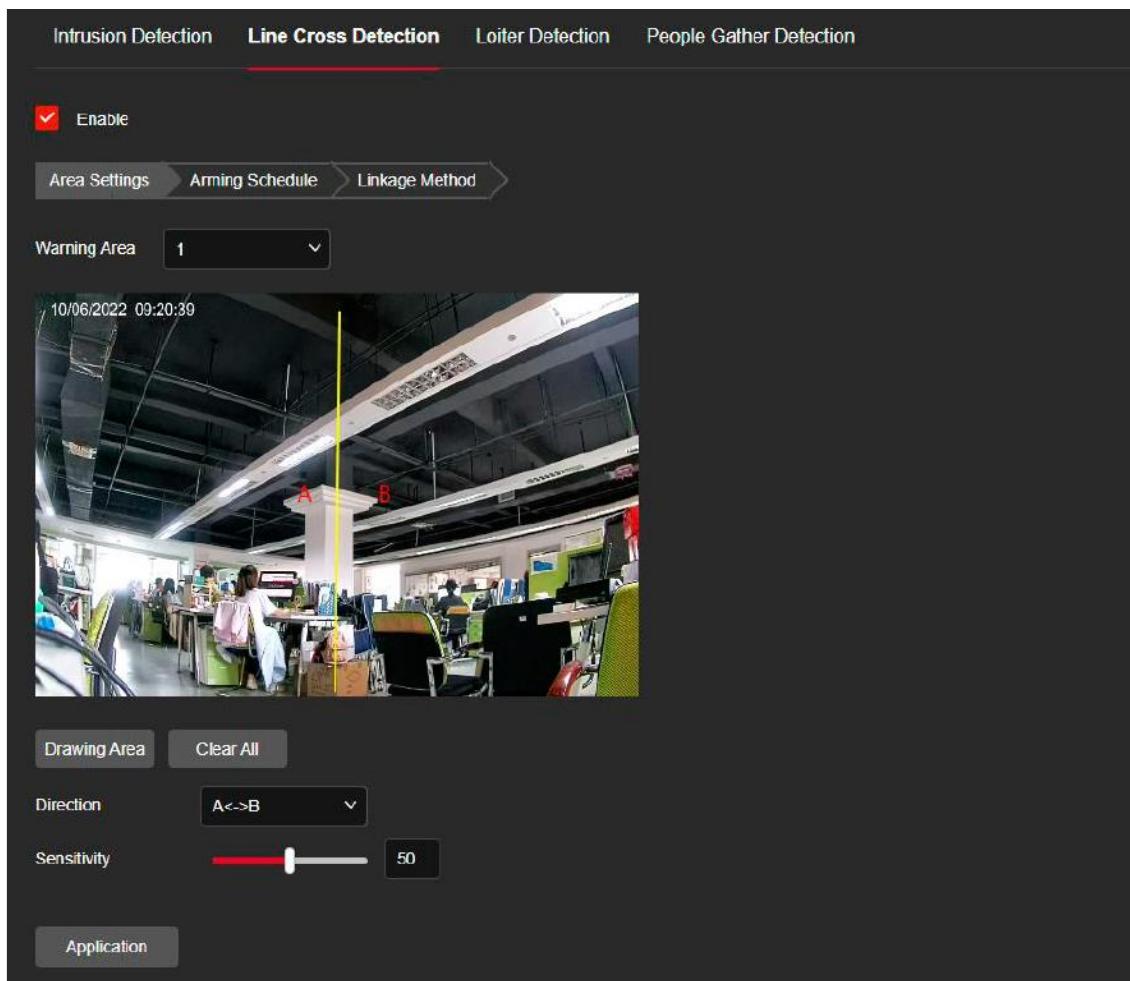


Рисунок 8-42

Шаг 2: Установите флажок «Enable (Включить)», чтобы включить функцию обнаружения пересечения линии.

Шаг 3: Выберите параметр «Warn Line (Линия контроля)». Система поддерживает настройку до 4 линий контроля. После выбора линий контроля Вам необходимо выполнить следующие настройки. После выполнения настройки нажмите на «Save (Сохранить)».

[Warn Line (Линия контроля)]: Нажмите на «Drawing Area (Область рисования)», и на экране появится отрезок линии со стрелкой. Щелкните на отрезке, затем щелкните и перетащите одну из конечных точек, чтобы изменить длину отрезка линии. Или же щелкните и перетащите отрезок линии со стрелкой на рисунке, чтобы завершить рисование линии контроля.

[Clear All (Очистить всё)]: Используется для удаления выбранной области контроля.

[Direction (Направление)]: Существует три опции: «A->B», «A->B» и «B->A». Эти настройки указывают направление, в котором объект должен пересечь линию контроля для того, чтобы вызвать сигнал тревоги. Настройка «A->B» означает, что сигнал тревоги сработает, когда объект перейдет из зоны A в зону B; «B->A» означает, что сигнал тревоги сработает, когда объект перейдет из зоны B в зону A; «A<->B» означает, что сигнализация срабатывает, если объект переходит из зоны A в зону B или из зоны B в зону A, то есть сигнализация срабатывает в обоих направлениях.

[Sensitivity (Чувствительность)]: Используется для настройки чувствительности обнаружения вторжения в области контроля. Значение по умолчанию равно 50. Перетащите индикатор или введите значение непосредственно в поле значения, чтобы изменить чувствительность. Чем выше это значение, тем выше чувствительность срабатывания сигнала тревоги.

Шаг 4: Если Вам нужно задать другую линию контроля «Warn Line (Линия контроля)», повторите шаг 3 для завершения настройки.

Шаг 5: Задайте расписание осуществления контроля.

Как показано на рисунке 8-43. Вы можете просматривать, редактировать и удалять время осуществления контроля функции обнаружения пересечения линии. По умолчанию контроль включен 24 часа в сутки. Вы можете настроить время контроля следующим образом.

- Метод 1: Щелкните по шкале времени осуществления контроля, вручную введите для него время начала и окончания, для сохранения настроек нажмите на «Application (Применить)». Если Вам нужно удалить период осуществления контроля, нажмите кнопку «Delete (Удалить)», а затем сбросьте период времени.
- Метод 2: Щелкните по шкале времени осуществления контроля, период времени отобразится двумя кружками на обоих концах, курсор мыши переместится на кружок, передвигните стрелку настройки влево и вправо, чтобы задать время контроля.
- Вы можете настроить более одного периода времени, максимум их может быть 8.
- По окончании настройки времени выполнения на контроля для целого дня, если для другого дня необходимо установить такое же время контроля, нажмите в правой части временной шкалы кнопку копирования «», в окне «Copy to (Копировать в)» установите флажок «Select All (Выбрать все)» или «Day (День)», затем нажмите «OK».
- После выполнения настройки нажмите на «Application (Применить)», чтобы завершить процедуру настройки времени осуществления контроля.

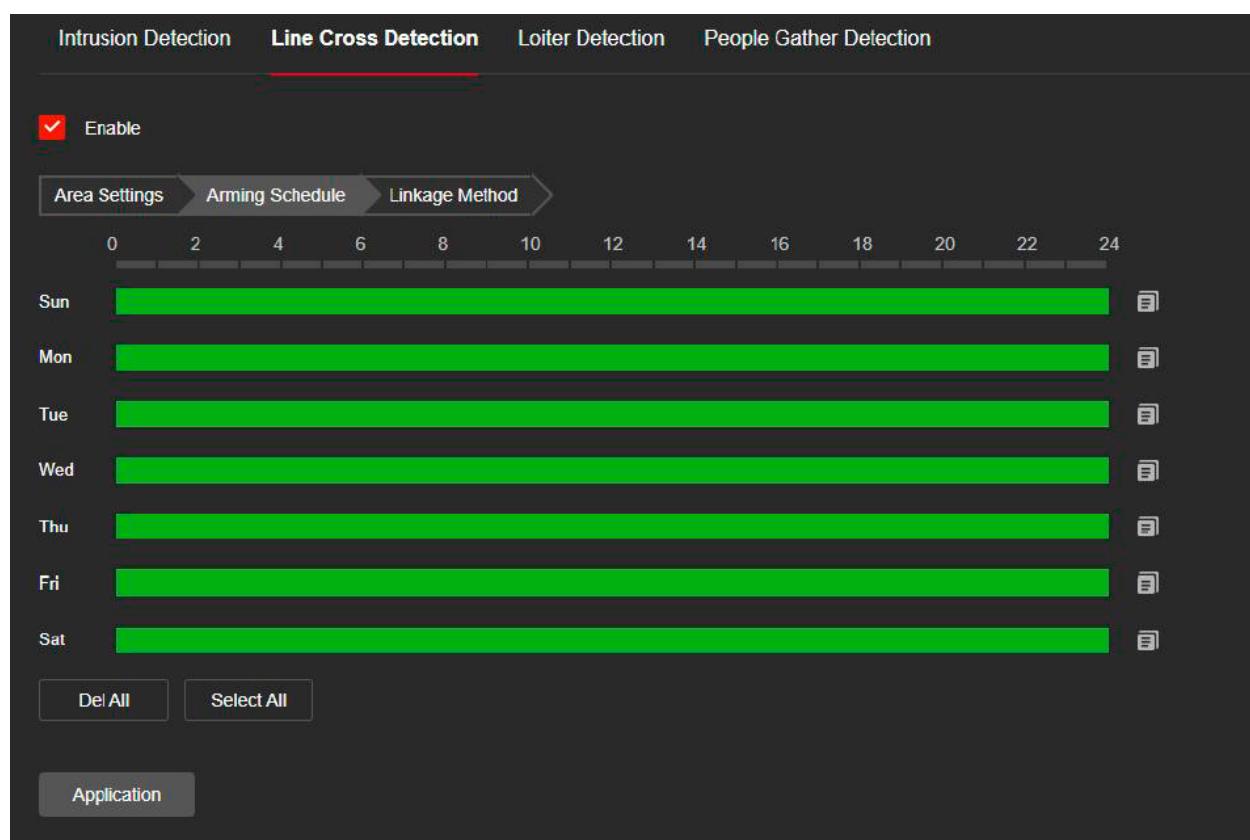


Рисунок 8-43



ПРИМЕЧАНИЕ:

- При настройке времени осуществления контроля следите за тем, чтобы никакие два периода времени не совпадали.

Шаг 6: Выберите нужный Вам метод выдачи сигналов тревоги.

Способы оповещения о тревоге включают в себя как обычные методы оповещения («Upload Via SMTP (Загрузить по SMTP)», «Upload Via FTP (Загрузить на FTP)», «Upload Via Cloud (Загрузить на облако)», «Flash Warning (Мигание подсветки)», «Sound Alarm (Звуковое оповещение о тревоге)»), так и вывод сигнала тревоги через выход тревог («IO Output (Выход тревог)»), как показано на рисунке 8-44.

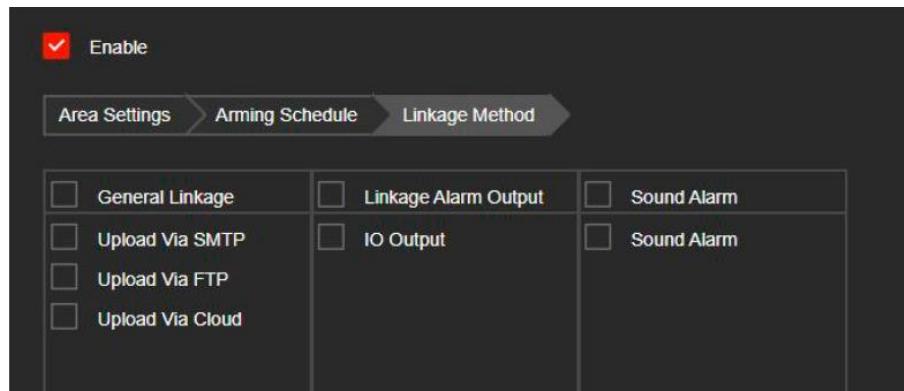


Рисунок 8-44

[Upload Via SMTP (Загрузить на SMTP): При выборе данной опции (если в системе настроен обмен по SMTP) информация о тревоге будет отправлена в почтовый ящик получателя SMTP.

[Upload Via FTP (Загрузить на FTP): При выборе данной опции (если в системе настроен обмен с FTP-сервером) информация о тревоге будет отправлена на FTP-сервер.

[Upload Via Cloud (Загрузить на облако): При выборе данной опции (если в системе настроен обмен с помощью облачного сервера) информация о тревоге будет отправлена в облачную учетную запись.

[Flash Warning (Мигание подсветки): При выборе этого метода сигнализации устройство будет сообщать о тревоге миганием лампы подсветки.

[IO Output (Выход тревог): При выборе данной опции убедитесь в том, что порт ввода-вывода сигналов подключен к устройству сигнализации. Во время тревоги камера передаст сигнал тревоги на это устройство.

[Sound Alarm (Звуковой сигнал тревоги): При выборе данной опции при тревоге устройство будет подавать звуковой сигнал.



ПРИМЕЧАНИЕ:

- Различные устройства поддерживают различные методы выдачи сигналов тревоги. Способ подачи сигнала тревоги зависит от конкретного устройства.

③ Обнаружение подозрительного поведения

Функция обнаружения подозрительного поведения предназначена для определения, остался ли объект в пределах заданной зоны дольше установленного порогового значения времени. Затем функция генерирует сигнал тревоги в соответствии с результатом оценки.

Выполните следующие действия:

Шаг 1: Чтобы перейти к настройкам обнаружения подозрительного поведения, выберите в главном окне меню «Configuration (Настройка)» → «Event (События)» → «Smart Event (Интеллектуальные события)» → «Loiter Detection (Обнаружение подозрительного поведения)», как показано на рисунке 8-45.

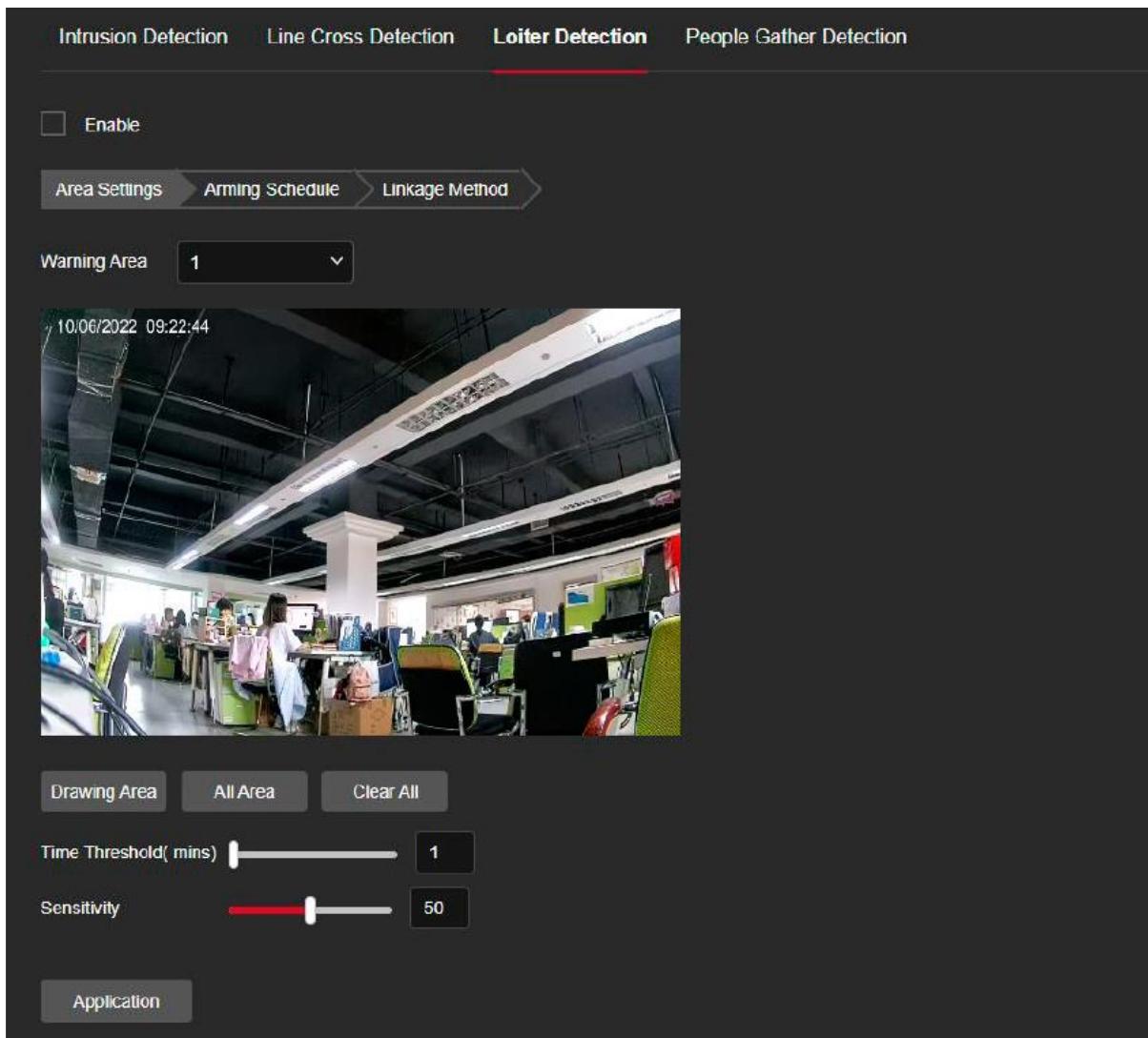


Рисунок 8-45

Шаг 2: Установите флажок «Enable (Включить)», чтобы включить функцию обнаружения подозрительного поведения.

Шаг 3: Выберите параметр «Warn Region (Область контроля)». Система поддерживает настройку до 4 областей контроля. После выбора областей контроля Вам необходимо выполнить следующие настройки. После выполнения настройки нажмите на «Save (Сохранить)».

[Drawing Area (Область рисования)]: Нажмите на «Drawing Area Область рисования», наведите курсор мыши на экран просмотра, нажмите левую кнопку мыши, выделите четырехугольную область контроля, затем щелкните на окне просмотра, чтобы завершить рисование области.

[All Area (Вся область)]: Если требуется контролировать все области, нажмите на «All Area (Вся область)», чтобы автоматически выбрать все области.

[Clear All (Очистить всё)]: Используется для удаления выбранной области контроля.

[Time Threshold (min) (Минимальный временной порог): После продолжительного перемещения объекта в области контроля по истечении данного периода времени генерируется сигнал тревоги. Чем выше значение временного порога, тем дольше объект сможет перемещаться в области контроля, не вызывая тревоги.

[Sensitivity (Чувствительность): Используется для настройки чувствительности обнаружения вторжения в области контроля. Значение по умолчанию равно 50. Перетащите индикатор или введите значение непосредственно в поле значения, чтобы изменить чувствительность. Чем выше это значение, тем выше чувствительность срабатывания сигнала тревоги.

Шаг 4: Если Вам нужно задать другую область контроля, повторите шаг 3 для завершения настройки.

Шаг 5: Задайте расписание осуществления контроля.

Как показано на рисунке 8-46. Вы можете просматривать, редактировать и удалять время осуществления контроля функции обнаружения подозрительного поведения. По умолчанию контроль включен 24 часа в сутки. Вы можете настроить время контроля следующим образом.

- Метод 1: Щелкните по шкале времени осуществления контроля, вручную введите для него время начала и окончания, для сохранения настроек нажмите на «Application (Применить)». Если Вам нужно удалить период осуществления контроля, нажмите кнопку «Delete (Удалить)», а затембросьте период времени.
- Метод 2: Щелкните по шкале времени осуществления контроля, период времени отобразится двумя кружками на обоих концах, курсор мыши переместится на кружок, передвигните стрелку настройки влево и вправо, чтобы задать время контроля.
- Вы можете настроить более одного периода времени, максимум их может быть 8.
- По окончании настройки времени выполнения на контроля для целого дня, если для другого дня необходимо установить такое же время контроля, нажмите в правой части временной шкалы кнопку копирования «», в окне «Copy to (Копировать в)» установите флажок «Select All (Выбрать все)» или «Day (День)», затем нажмите «OK».
- После выполнения настройки нажмите на «Application (Применить)», чтобы завершить процедуру настройки времени осуществления контроля.

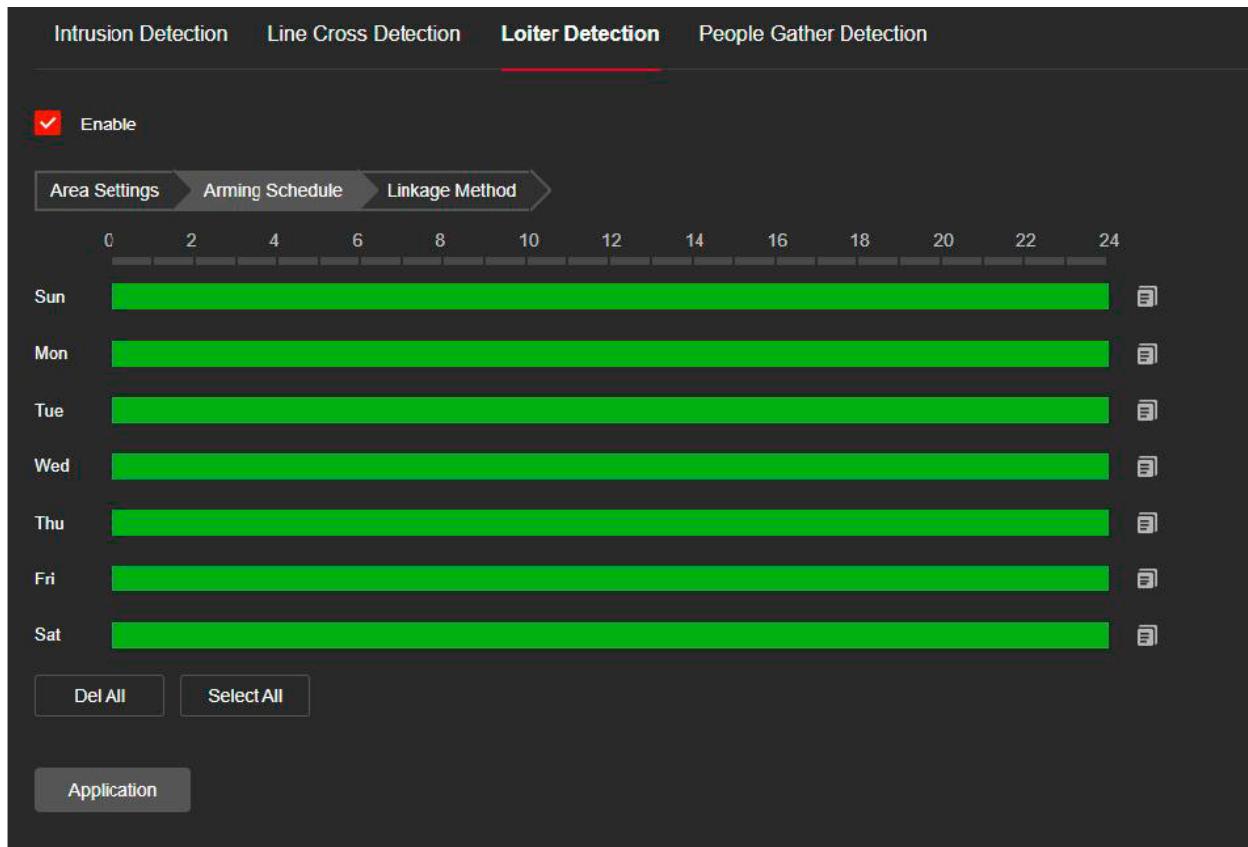


Рисунок 8-46



ПРИМЕЧАНИЕ:

- При настройке времени осуществления контроля следите за тем, чтобы никакие два периода времени не совпадали.

Шаг 6: Выберите нужный Вам метод выдачи сигналов тревоги.

Способы оповещения о тревоге включают в себя как обычные методы оповещения («Upload Via SMTP (Загрузить по SMTP)», «Upload Via FTP (Загрузить на FTP)», «Upload Via Cloud (Загрузить на облако)», «Flash Warning (Мигание подсветки)», «Sound Alarm (Звуковое оповещение о тревоге)»), так и вывод сигнала тревоги через выход тревог («IO Output (Выход тревог)»), как показано на рисунке 8-47.

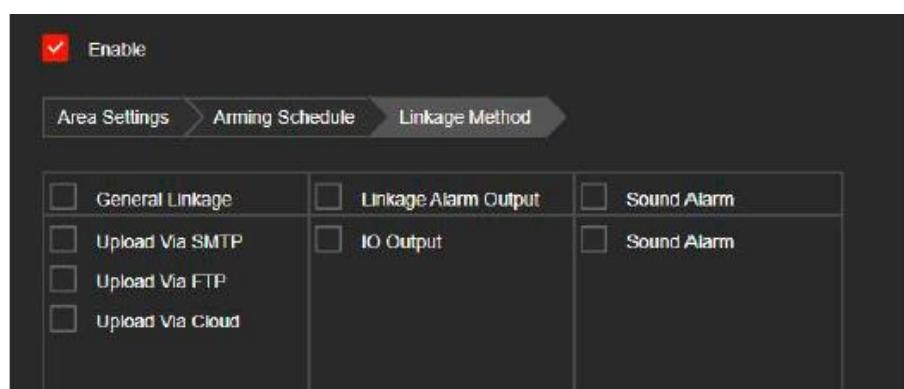


Рисунок 8-47

[Upload Via SMTP (Загрузить на SMTP): При выборе данной опции (если в системе настроен обмен по SMTP) информация о тревоге будет отправлена в почтовый ящик получателя SMTP.

[Upload Via FTP (Загрузить на FTP): При выборе данной опции (если в системе настроен обмен с FTP-сервером) информация о тревоге будет отправлена на FTP-сервер.

[Upload Via Cloud (Загрузить на облако): При выборе данной опции (если в системе настроен обмен с помощью облачного сервера) информация о тревоге будет отправлена в облачную учетную запись.

[Flash Warning (Мигание подсветки): При выборе этого метода сигнализации устройство будет сообщать о тревоге миганием лампы подсветки.

[IO Output (Выход тревог): При выборе данной опции убедитесь в том, что порт ввода-вывода сигналов подключен к устройству сигнализации. Во время тревоги камера передаст сигнал тревоги на это устройство.

[Sound Alarm (Звуковой сигнал тревоги): При выборе данной опции при тревоге устройство будет подавать звуковой сигнал.



ПРИМЕЧАНИЕ:

- Различные устройства поддерживают различные методы выдачи сигналов тревоги. Способ подачи сигнала тревоги зависит от конкретного устройства.

④ Обнаружение скопления людей

Функция обнаружения скопления людей используется для обнаружения, превышает ли плотность скопления людей в заданном районе установленное пороговое значение. В соответствии с результатом оценки подается сигнал тревоги.

Выполните следующие действия:

Шаг 1: Чтобы перейти к настройкам обнаружения скопления людей, выберите в главном окне меню «Configuration (Настройка)» → «Event (События)» → «Smart Event (Интеллектуальные события)» → «People Gather Detection (Обнаружение скопления людей)», как показано на рисунке 8-48.

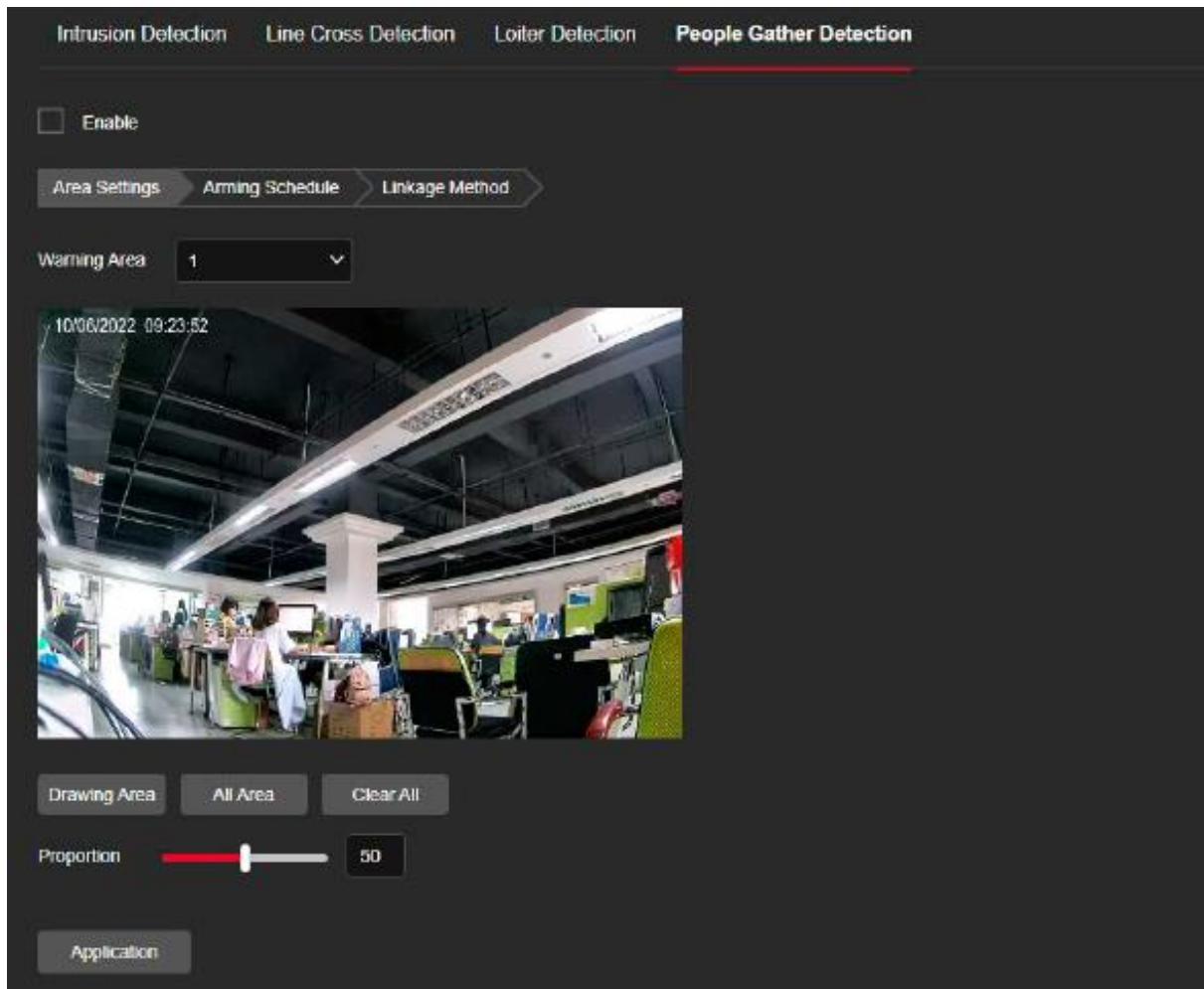


Рисунок 8-48

Шаг 2: Установите флажок «Enable (Включить)», чтобы включить функцию обнаружения скопления людей.

Шаг 3: Выберите параметр «Warn Region (Область контроля)». Система поддерживает настройку до 4 областей контроля. После выбора областей контроля Вам необходимо выполнить следующие настройки. После выполнения настройки нажмите на «Save (Сохранить)».

[Drawing Area (Область рисования)]: Нажмите на «Drawing Area Область рисования», наведите курсор мыши на экран просмотра, нажмите левую кнопку мыши, выделите четырехугольную область контроля, затем щелкните на окне просмотра, чтобы завершить рисование области.

[All Area (Вся область): Если требуется контролировать все области, нажмите на «All Area (Вся область)», чтобы автоматически выбрать все области.

[Clear All (Очистить всё)]: Используется для удаления выбранной области контроля.

[Proportion (Доля присутствия)]: Указывает долю присутствия во всей области контроля. Когда процент присутствия превысит установленное здесь значение (в процентах), система выдаст сигнал тревоги. По умолчанию это значение равно 50%. Чем выше это значение, тем больше людей может находиться в зоне оповещения и тем меньше вероятность срабатывания сигнализации.

Шаг 4: Если Вам нужно задать другую область контроля, повторите шаг 3 для завершения настройки.

Шаг 5: Задайте расписание осуществления контроля.

Как показано на рисунке 8-49. Вы можете просматривать, редактировать и удалять время осуществления контроля функции обнаружения скопления людей. По умолчанию контроль включен 24 часа в сутки. Вы можете настроить время контроля следующим образом.

- Метод 1: Щелкните по шкале времени осуществления контроля, вручную введите для него время начала и окончания, для сохранения настроек нажмите на «Application (Применить)». Если Вам нужно удалить период осуществления контроля, нажмите кнопку «Delete (Удалить)», а затем сбросьте период времени.
- Метод 2: Щелкните по шкале времени осуществления контроля, период времени отобразится двумя кружками на обоих концах, курсор мыши переместится на кружок и покажет направление стрелки настройки влево и вправо. Передвиньте стрелку настройки влево и вправо, чтобы задать время контроля.
- Вы можете настроить более одного периода времени, максимум их может быть 8.
- По окончании настройки времени выполнения на контроля для целого дня, если для другого дня необходимо установить такое же время контроля, нажмите в правой части временной шкалы кнопку копирования «», в окне «Copy to (Копировать в)» установите флажок «Select All (Выбрать все)» или «Day (День)», затем нажмите «OK».
- После выполнения настройки нажмите на «Application (Применить)», чтобы завершить процедуру настройки времени осуществления контроля.

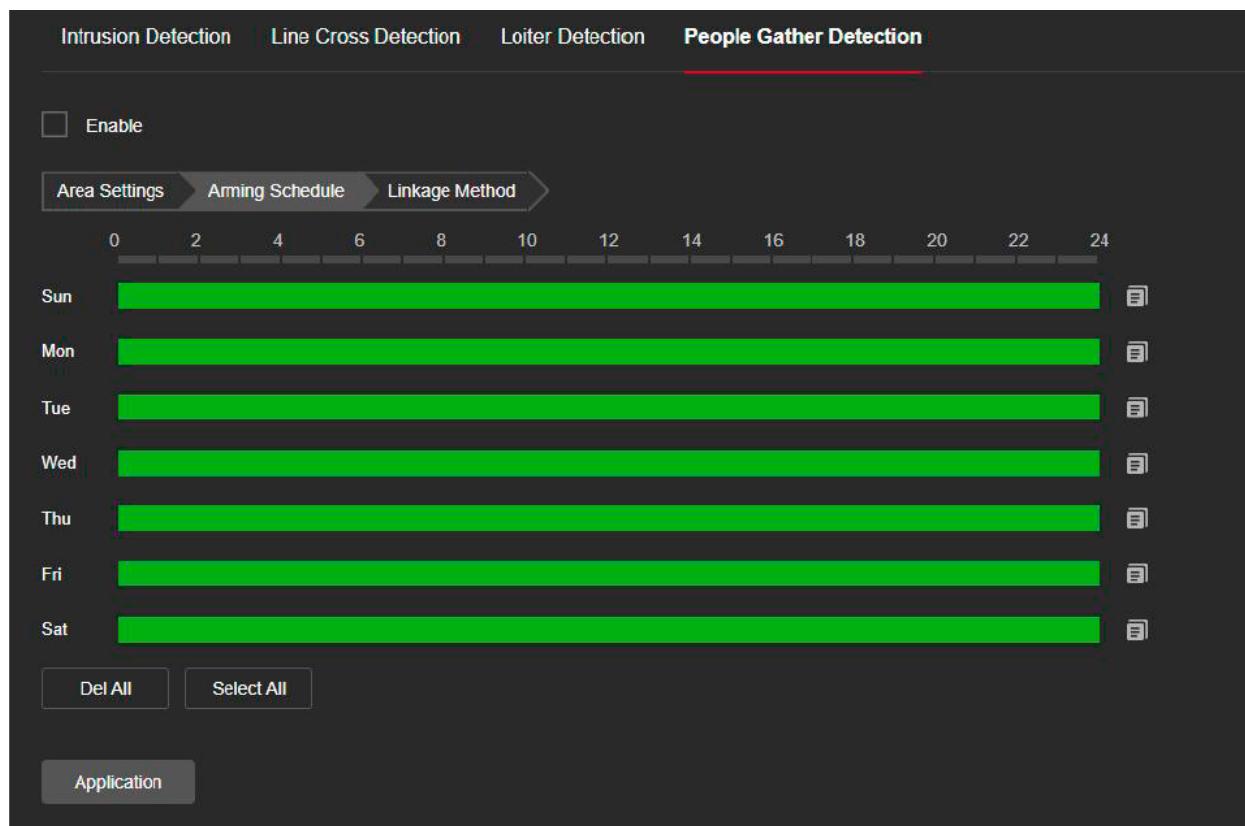


Рисунок 8-49



ПРИМЕЧАНИЕ:

- При настройке времени осуществления контроля следите за тем, чтобы никакие два периода времени не совпадали.

Шаг 6: Выберите нужный Вам метод выдачи сигналов тревоги.

Способы оповещения о тревоге включают в себя как обычные методы оповещения («Upload Via SMTP (Загрузить по SMTP)», «Upload Via FTP (Загрузить на FTP)», «Upload Via Cloud (Загрузить на облако)», «Flash Warning (Мигание подсветки)», «Sound Alarm (Звуковое оповещение о тревоге)»), так и вывод сигнала тревоги через выход тревог («IO Output (Выход тревог)»), как показано на рисунке 8-50.

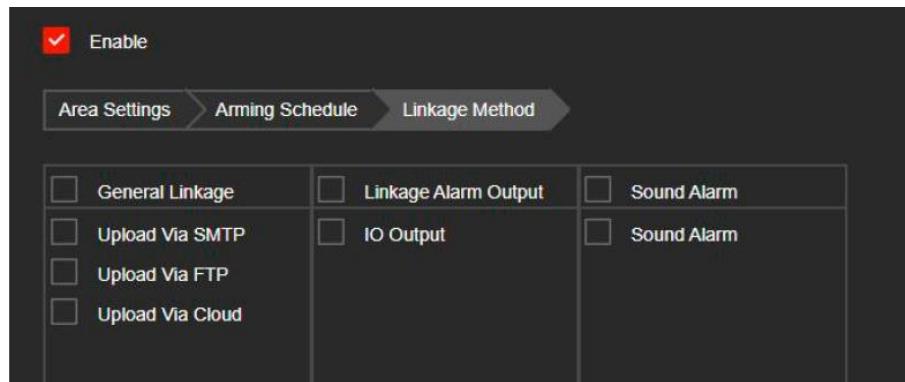


Рисунок 8-50

[Upload Via SMTP (Загрузить на SMTP): При выборе данной опции (если в системе настроен обмен по SMTP) информация о тревоге будет отправлена в почтовый ящик получателя SMTP.

[Upload Via FTP (Загрузить на FTP): При выборе данной опции (если в системе настроен обмен с FTP-сервером) информация о тревоге будет отправлена на FTP-сервер.

[Upload Via Cloud (Загрузить на облако): При выборе данной опции (если в системе настроен обмен с помощью облачного сервера) информация о тревоге будет отправлена в облачную учетную запись.

[Flash Warning (Мигание подсветки): При выборе этого метода сигнализации устройство будет сообщать о тревоге миганием лампы подсветки.

[IO Output (Выход тревог): При выборе данной опции убедитесь в том, что порт ввода-вывода сигналов подключен к устройству сигнализации. Во время тревоги камера передаст сигнал тревоги на это устройство.

[Sound Alarm (Звуковой сигнал тревоги): При выборе данной опции при тревоге устройство будет подавать звуковой сигнал.



ПРИМЕЧАНИЕ:

- Различные устройства поддерживают различные методы выдачи сигналов тревоги. Способ подачи сигнала тревоги зависит от конкретного устройства.

8.7. Хранение данных

8.7.1. Настройка расписания

① Расписание записи

Выполните следующие действия:

Шаг 1: Чтобы перейти к настройкам расписания ведения записи, выберите в главном окне меню «Configuration (Настройка)» → «Storage (Хранение данных)» → «Schedule Configuration (Настройка расписания)» → «Record Schedule (Расписание записи)», как показано на рисунке 8-51 ①.

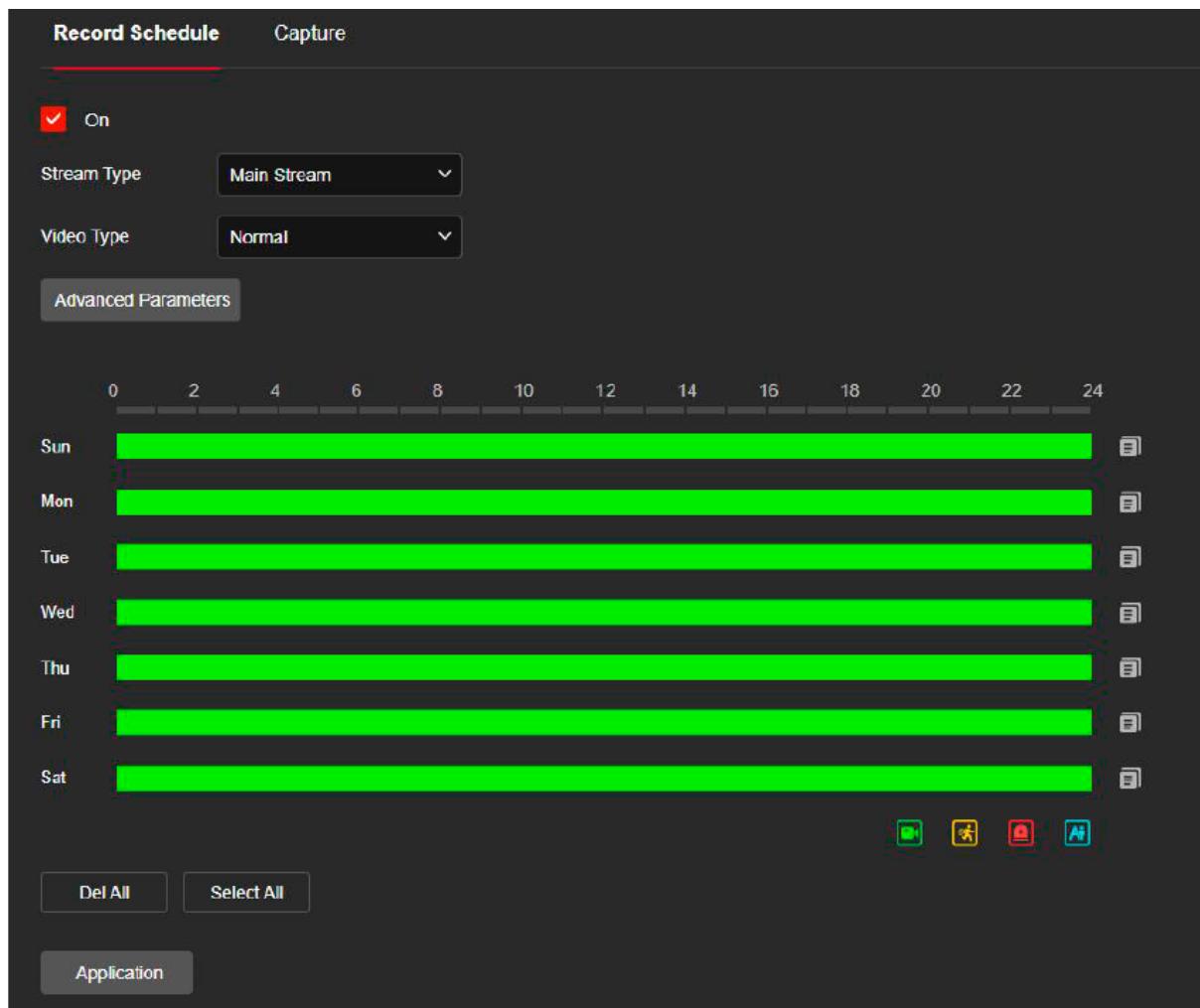


Рисунок 8-51 ①

Шаг 2: Чтобы включить запись, выберите настройку для параметра «Stream Type (Тип потока)» («Main Stream (Основной поток)», «Sub Stream (Дополнительный поток)» или «Tri-Stream (Поток мобильных данных)») и для параметра «Video type (Тип записи видео)» («Normal Record (Обычная запись)», «Motion Detection (При обнаружении движения)», «External Alarm (При внешней тревоге)», «Intelligent (При тревоге от интеллектуального события)»).

Шаг 3: Задайте период времени ведения записи по расписанию.

- Метод 1: Щелкните по шкале времени осуществления контроля, вручную введите для него время начала и окончания, для сохранения настроек нажмите на «Application (Применить)». Если Вам нужно удалить период времени контроля, нажмите кнопку «Del All (Удалить все)», а затем сбросьте период времени.
- Метод 2: Щелкните по шкале времени осуществления контроля, на обоих концах периода времени отобразятся две стрелки. Переместите стрелку настройки влево или вправо, чтобы настроить время осуществления контроля.

Шаг 4: Чтобы настроить параметры «Pre-recorded time (Время предварительной записи)» и «Video delay time (Время задержки видео)», щелкните по «Advance parameters (Дополнительно)». Для времени предварительной записи имеются следующие опции: Unlimited (Без ограничений), 10s (10 сек), 15s (15 сек), 20s (20 сек), 25s (25 сек), 30s (30 сек), для времени задержки видео: 5s (5 сек), 10s (10 сек), 30s (30 сек), 1min (1 мин), 2min (2 мин), 5min (5 мин), 10min (10 мин) (см. рисунок 8-51 ②).

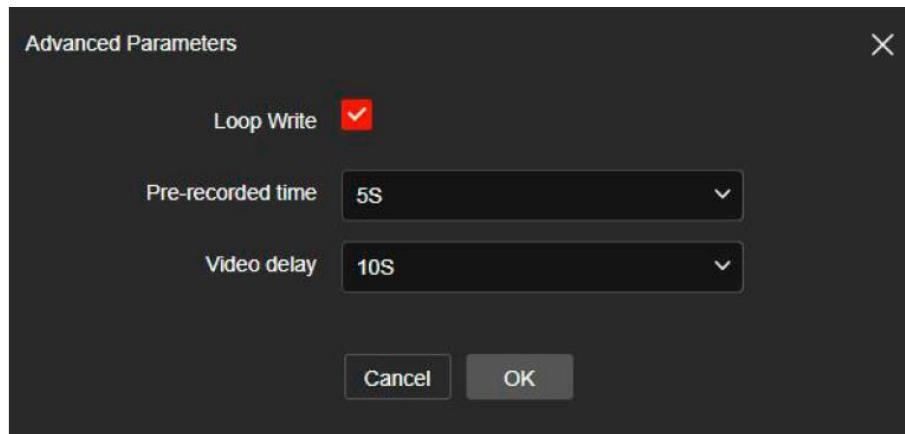


Рисунок 8-51 ②

Шаг 5: Нажмите на «Application (Применить)», чтобы завершить процедуру настройки времени осуществления контроля.



ПРИМЕЧАНИЕ:

- Вы можете настроить более одного периода времени, максимум их может быть 8.
- Завершив настройку времени осуществления контроля для целого дня, если для другого дня необходимо установить такое же время контроля, нажмите в правой части временной шкалы кнопку копирования «», в окне «Copy to (Копировать в)» установите флажок «Select All (Выбрать все)» или «Day (День)», затем нажмите «OK».
- Если Вы хотите вести запись в режиме 24/7, установите флажок «Select All (Выбрать все)».
- Если в камере отсутствует функция записи видео на EMMC/TF-карту, у камеры будет отсутствовать окно управления EMMC/TF-картой. Учитывайте фактические свойства и особенности Вашего устройства.
- Для хранения данных на карте EMMC требуется, чтобы камера поддерживала аппаратное обеспечение EMMC. Для получения подробной информации по данному вопросу, обратитесь к описанию имеющегося у Вас устройства.
- Если в качестве типа видео («Video type») выбрано «Motion Detection (При обнаружении движения)» и «External Alarm (При внешней тревоге)», устройство также выполнит запись данного типа видео по расписанию.
- Параметры «Pre-recorded time (Время предварительной записи)» и «Video delay time (Время задержки видео)» могут использоваться для записи видео при обнаружении движения и при внешней по тревоге.

② Моментальный снимок

Функция захвата снимка используется при настройке плана съемки камеры и параметров захвата изображения. После выполнения данной настройки IP-камера будет захватывать снимки автоматически. Если выбран параметр «Enable timed capture (Включить захват по времени)», то в окне настройки параметров захвата снимка для камеры можно настроить расписание создания снимков так, как это необходимо.

Выполните следующие действия:

Шаг 1: Чтобы перейти к настройкам захвата снимков, выберите в главном окне меню «Configuration (Настройка)» → «Storage (Хранение данных)» → «Schedule Configuration (Настройка расписания)» → «Capture (Захват снимков)», как показано на рисунке 8-52 ①.



Рисунок 8-52 ①

Шаг 2: Настройте расписание захвата снимков.

- Метод 1: Щелкните по расписанию, вручную введите время начала и окончания, для сохранения настроек нажмите на «Application (Применить)». Если Вам нужно удалить период времени контроля, нажмите кнопку «Del All (Удалить все)», а затем сбросьте период времени.
- Метод 2: Щелкните по расписанию, на обоих концах периода времени отобразятся две стрелки. Переместите стрелку настройки влево или вправо, чтобы настроить время осуществления контроля.

Шаг 3: Повторите шаг 2, чтобы настроить расписание записи полностью.

Шаг 4: Нажмите на «Application (Применить)», чтобы завершить процедуру настройки времени осуществления контроля.

Шаг 5: Щелкните по «Capture Parameters (Параметры захвата снимков)», чтобы перейти в окно настройки параметров захвата, как показано на рисунке 8-52 ②.

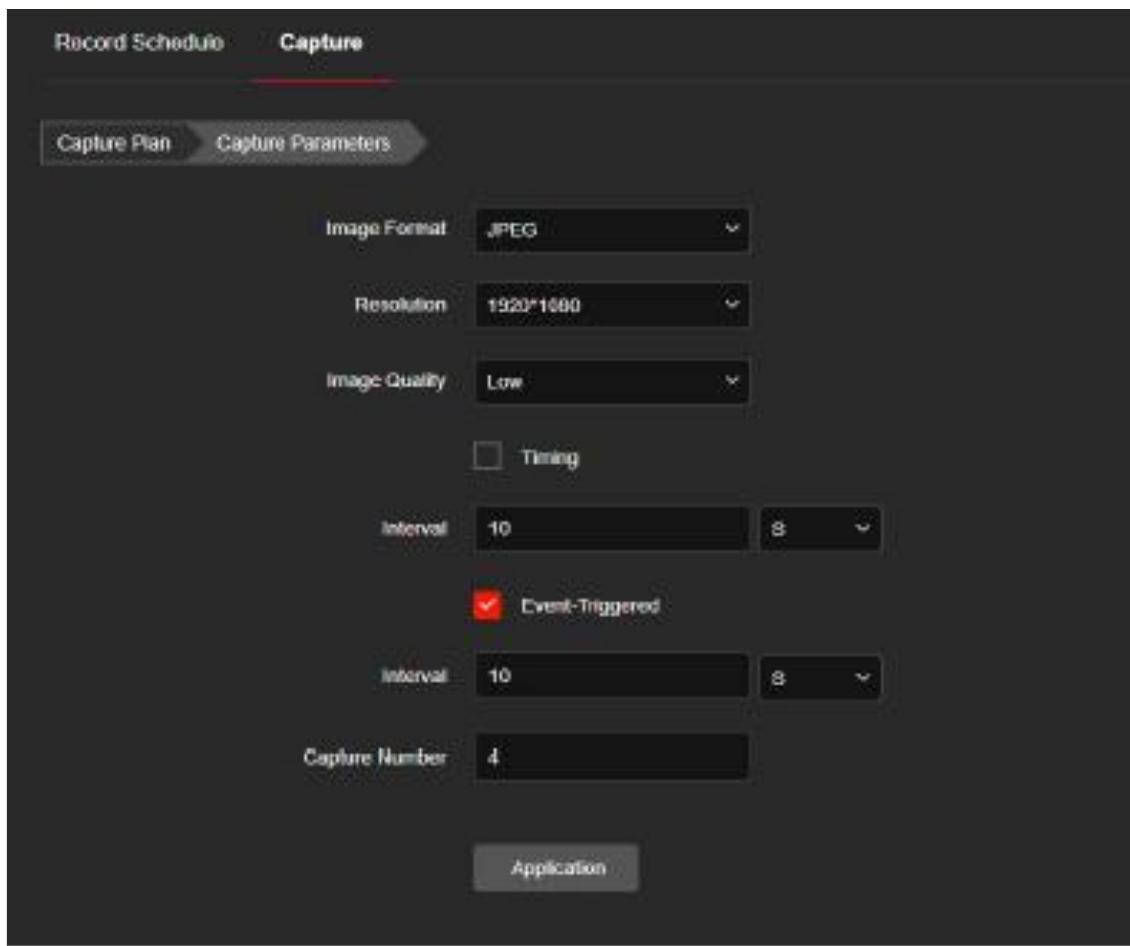


Рисунок 8-52 ②

Шаг 6: Выберите необходимые параметры, такие как формат изображения (JPEG), разрешение и качество изображения, и настройте процедуру захвата снимков по времени и по событиям.

[Image Format (Формат изображения)]: Поддерживается формат JPEG.

[Resolution (Разрешение)]: Разрешение полученного изображения.

[Image Quality (Качество изображения)]: Можно выбрать три уровня: «Low (Низкое)», «Middle (Среднее)» и «High (Высокое)».

[Timed capture (Захват по времени)]: В течение заданного здесь периода времени будут выполняться снимки в соответствии с заданным интервалом времени.

[Interval time (Интервал времени)]: Задайте временной интервал захвата снимков согласно Вашим потребностям.

[Capture Number (Количество снимков)]: Для событий, запускающих захват снимков, Вы можете задать количество снимков, получаемых при возникновении события.

Шаг 7: Нажмите на «Application (Применить)», чтобы завершить процедуру настройки.



ПРИМЕЧАНИЕ:

- Вы можете настроить более одного периода времени, максимум их может быть 8.
- По окончании настройки времени выполнения на контроля для целого дня, если для другого дня необходимо установить такое же время контроля, нажмите в правой части вре-



менной шкалы кнопку копирования «», в окне «Copy to (Копировать в)» установите флажок «Select All (Выбрать все)» или «Day (День)», затем нажмите «OK».

- Если Вы хотите вести запись в режиме 24/7, установите флажок «Select All (Выбрать все)».
- Если в камере отсутствует функция записи видео на EMMC/TF-карту, у камеры будет отсутствовать окно управления EMMC/TF-картой. Учитывайте фактические свойства и особенности Вашего устройства.
- Для хранения данных на карте EMMC требуется, чтобы камера поддерживала аппаратное обеспечение EMMC. Для получения подробной информации по данному вопросу, обратитесь к описанию имеющегося у Вас устройства.
- Время выполнения захвата снимков необходимо настраивать индивидуально для каждого события.

8.7.2. Управление хранением данных

① Хранение данных на карте памяти

В главном окне выберите путь «Configuration (Настройка)» → «Storage (Хранение данных)» → «Storage Management (Управление хранением данных)» → «Storage (Хранение данных на карте памяти)», чтобы перейти в окно настройки управления хранением данных на карте памяти. Здесь Вы можете просмотреть объем и состояние карты памяти и выполнить такие операции, как форматирование и настройка карты, как показано на рисунке 8-53 ниже.

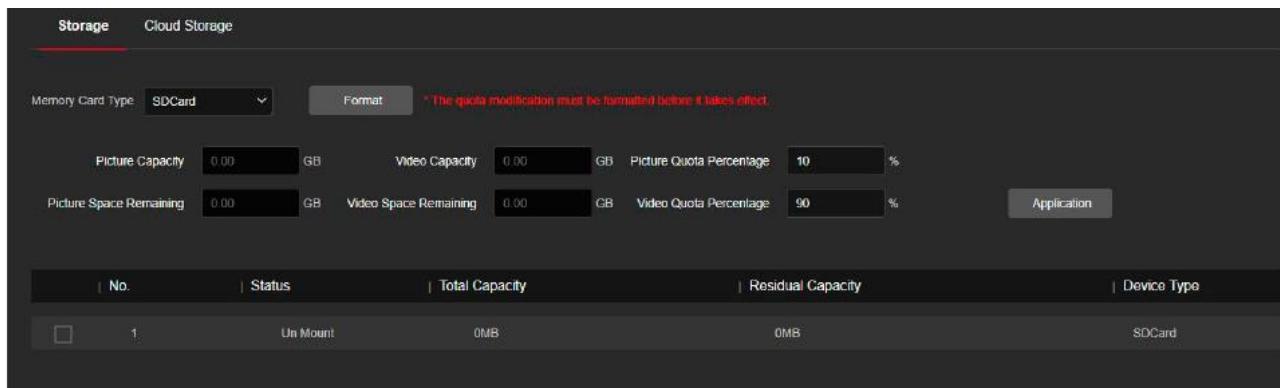


Рисунок 8-53

Форматирование карты памяти EMMC/SD выполняется следующим образом.

Шаг 1: Выберите карту для форматирования, нажмите на «Format (Форматировать)».

Шаг 2: Нажмите на «OK».

Шаг 3: Дождитесь завершения процесса форматирования, индикатор выполнения покажет, что форматирование завершено, проверьте информацию о карте памяти, если ее общая емкость равна объему свободного места на ней, то форматирование прошло успешно.

Для настройки ограничения выделенного дискового пространства (дисковой квоты) выполните следующие действия.

Шаг 1: Выберите карту памяти.

Шаг 2: Задайте ограничения пространства, включая такие параметры, как объем для снимков и видео.

Шаг 3: Нажмите на «Save (Сохранить)».

Шаг 4: Нажмите на «Format (Форматировать)» → «OK», чтобы завершить настройку ограничения дискового пространства после форматирования.



ПРИМЕЧАНИЕ:

- Хранение на карте EMMC не поддерживает запись по времени.
- Для хранения данных на карте EMMC требуется, чтобы камера поддерживала аппаратное обеспечение EMMC. Для получения подробной информации по данному вопросу, обратитесь к описанию имеющегося у Вас устройства.

② Хранение данных на облаке

▪ Облачное хранение

Настройка хранения данных на облаке. Когда устройство подает сигнал тревоги, Вы можете сохранить снимок, сделанный устройством, на облачном сервере.

Важно!

1) У Вас должна быть учетная запись на облачном сервере Google.

2) Чтобы использовать эту функцию, устройство должно быть подключено к внешней сети, в противном случае оно не будет работать корректно.

Выполните следующие действия:

Шаг 1: Чтобы перейти в окно настройки хранения данных на облаке, выберите в главном окне меню «Configuration (Настройка)» → «Storage (Хранение данных)» → «Storage Management (Управление хранением данных)» → «Cloud Storage (Хранение данных на облаке)», как показано на рисунке 8-54.

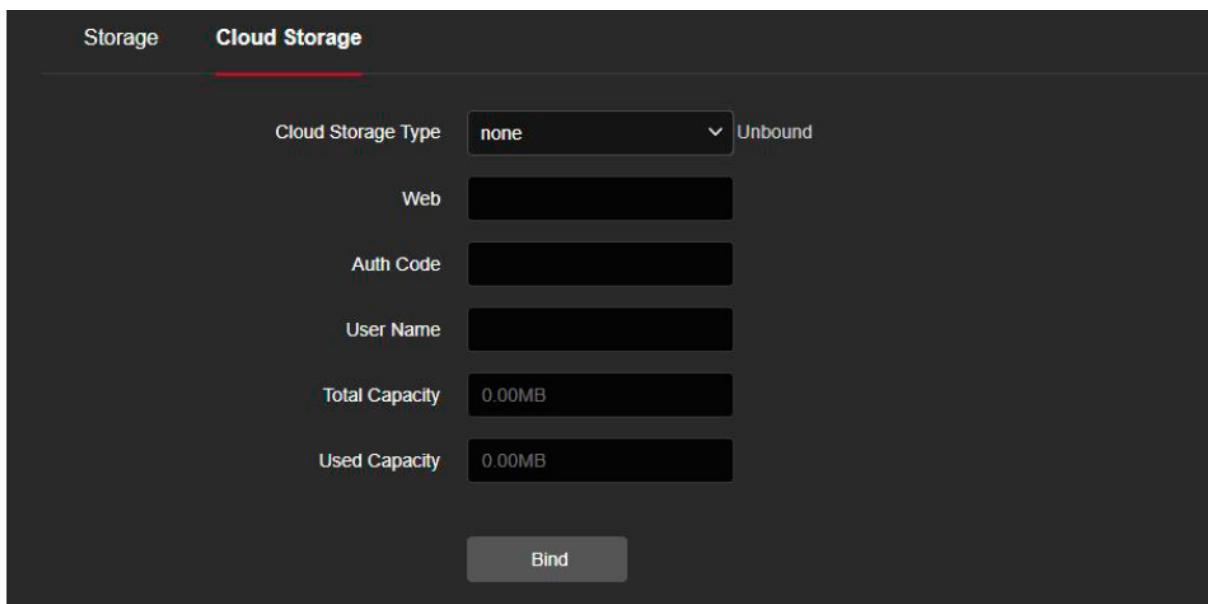


Рисунок 8-54

Шаг 2: Выберите тип облачного хранилища, например «Google».

Шаг 3: Чтобы войти на веб-сайт с помощью браузера на компьютере и получить «Verification Code (Проверочный код)», следуйте инструкциям.

Шаг 4: Введите проверочный код в поле «Auth code (Код аутентификации)» настройки хранения данных на облаке.

Шаг 5: Нажмите на «Bind (Привязать)».



ПРИМЕЧАНИЕ:

- Поддерживается только облачное хранение Google.
- «Total capacity (Общая емкость) – это общая емкость облачного диска, принадлежащего текущей учетной записи. Если Вам необходимо увеличить емкость, Вы можете зайти на соответствующий веб-сайт облачного хранения, чтобы увеличить или приобрести емкость.

Глава 9. Обслуживание устройства

9.1. Информация об устройстве

В окне настройки системы (System Configuration interface) нажмите на «Device Information (Информация об устройстве)», чтобы перейти в окно настройки информации об устройстве, где Вы можете просмотреть основную информацию о текущем устройстве, как показано на рисунке 9-1.



Рисунок 9-1

[Device Name (Имя устройства)]: Имя текущей IP-камеры.

[Firmware Version (Версия устройства)]: Текущая версия IP-камеры.

[Software Version (Версия ПО)]: Текущая версия LsIPCPlugin IP-камеры.

[WEB Version (Веб-версия)]: Текущая версия веб-страницы IP-камеры.

9.2. Обновление оборудования

Чтобы перейти в окно обновления устройства, где Вы сможете выполнить обновление вручную или онлайн-обновление, в окне обслуживания нажмите на «Equipment Upgrade (Обновление оборудования)», как показано на рисунке 9-2.

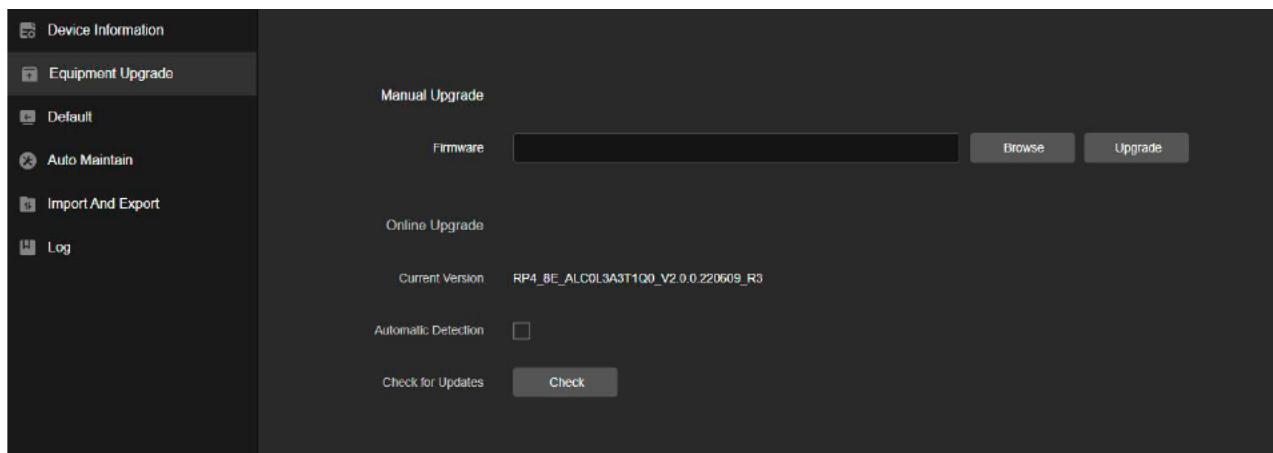


Рисунок 9-2

[Upgrade (Обновить)]: Чтобы добавить пакет файлов обновления, нажмите на «Browse (Обзор)» и обновите программу IP-камеры (соблюдайте осторожность – ошибка в файле обновления приведет к некорректной работе системы оборудования).

[Online Upgrade (Онлайн-обновление)]: Чтобы обнаружить подключенное к сети устройство, проверьте номер текущей версии, нажмите на кнопку «Check (Проверить)», появится всплывающая подсказка с последней версией обновления и местом скачивания. Нажмите «OK». Устройство начнет загрузку обновления версии до полного автоматического обновления. Чтобы отменить обновление, нажмите на «Cancel (Отмена)».

[Automatic Detection (Автоматическое обнаружение)]: Чтобы обнаружить подключенное к сети устройство, устройство начнет автоматически определять, имеется ли последняя версия обновления, появятся всплывающие подсказки с последней версией обновления и местом скачивания. Нажмите на «OK». Устройство начнет загрузку обновления версии до полного автоматического обновления. Чтобы отменить обновление, нажмите на «Cancel (Отмена)».

9.3. Возврат параметров устройства к заводским настройкам

Чтобы перейти в окно восстановления настроек устройства по умолчанию, в окне обслуживания нажмите на «Default (Возврат до заводских настроек)». Здесь Вы можете сбросить параметры устройства и восстановить все параметры до заводских настроек, как показано на рисунке 9.3.

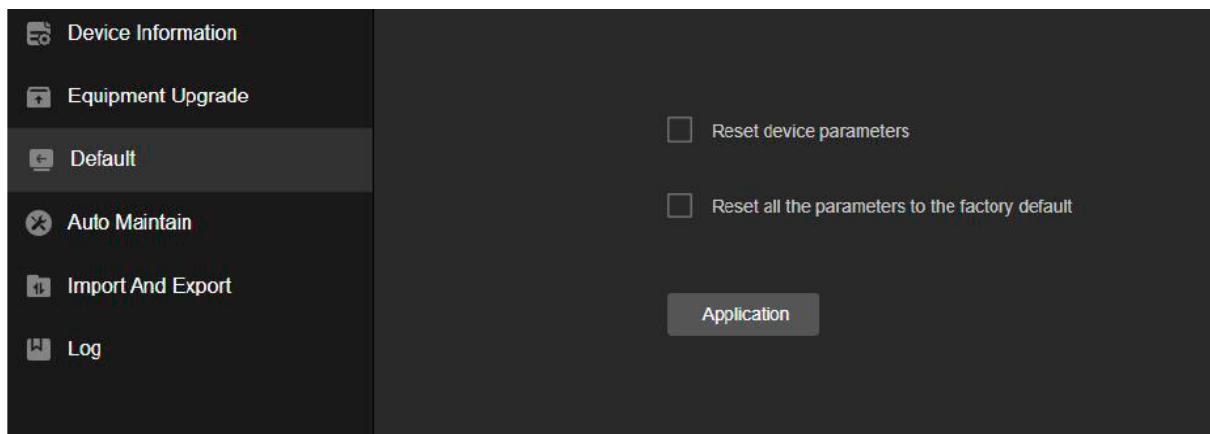


Рисунок 9-3

[Reset device parameters (Сбросить параметры устройства)]: IP-камера автоматически восстановит заводские параметры, за исключением параметров сети.

[Reset all the parameters to the factory default (Сбросить все параметры до заводских настроек по умолчанию)]: Все настройки IP-камеры будут автоматически сброшены до заводских настроек (используйте эту функцию с осторожностью).

9.4. Автоматическое обслуживание

В окне обслуживания выберите опцию «Auto Maintain (Автоматическое обслуживание)», чтобы перейти в окно настроек расписания перезагрузки камеры. Здесь Вы можете задавать время перезагрузки устройства, выбрать в выпадающем меню цикл перезагрузки, например, задать для перезагрузки «3:03 3-го числа каждого месяца». Нажмите на «Application (Применить)». Теперь IP-камера будет перезагружаться в 3 часа 30 минут 3-го числа каждого месяца (см. рисунок 9-4).

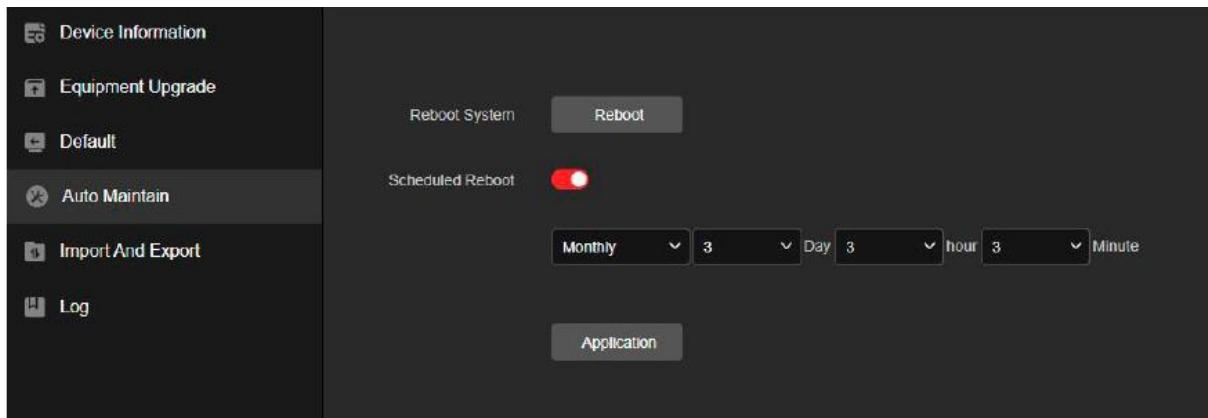


Рисунок 9-4



ПРИМЕЧАНИЕ:

- Если для перезапуска устройства используется конфигурация по умолчанию, то из-за большого количества одновременных перезапусков устройств может произойти перегрузка сервера. Чтобы избежать этого, следует выполнять перезапуск устройства случайным образом в течение 1 часа.

9.5. Импорт и экспорт

В окне обслуживания нажмите на «Import And Export (Импорт и экспорт)», чтобы перейти в окно импортирования и экспортации параметров устройства. Здесь Вы сможете экспортировать параметры устройства или импортировать файл параметров в IP-камеру, как показано на рисунке 9-5.

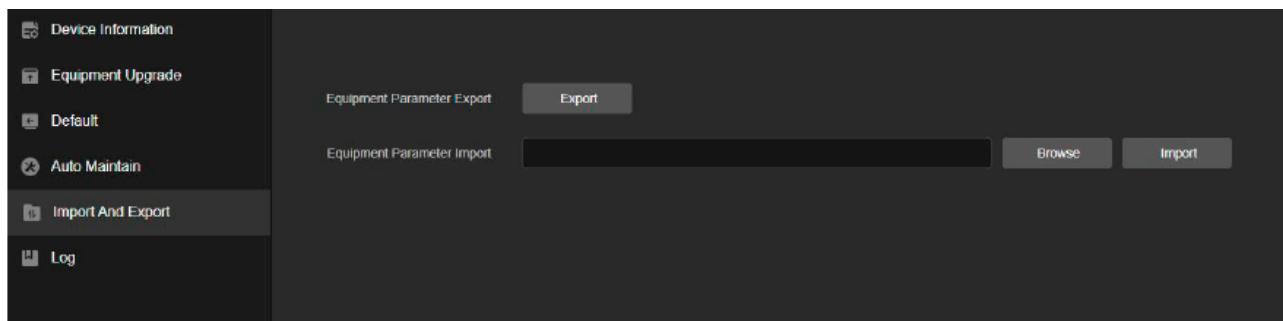


Рисунок 9-5

9.6. Ведение журналов

В окне обслуживания нажмите на кнопку «Log (Журналы)», чтобы перейти в окно поиска журнала, где Вы сможете запросить данные о тревогах устройства и другую соответствующую информацию (см. рисунок 9-6).

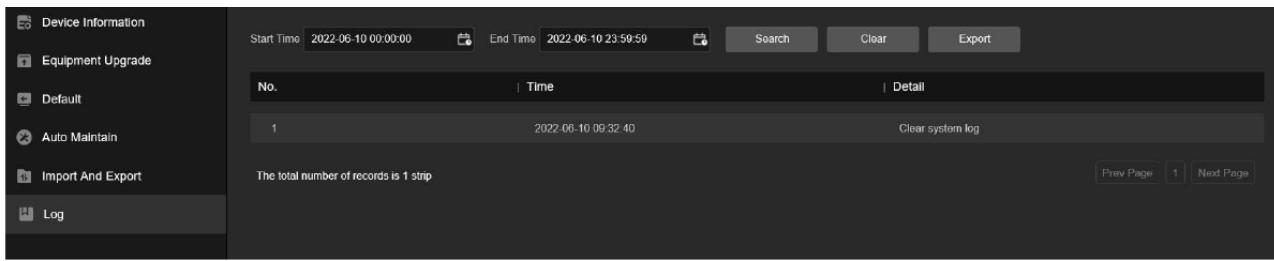


Рисунок 9-6

[Search (Поиск)]: Задайте дату и время начала поиска данных в журнале, нажмите на «Search (Поиск)», в списке отобразятся записи о работе IP-камеры согласно выбранным условиям.

[Clear (Очистить): Если Вы хотите очистить все записи в журнале, нажмите кнопку «Очистить».

[Export (Экспортировать): Сохранение содержимого текущего журнала в указанном Вами месте в формате txt.

Глава 10. Часто задаваемые вопросы

1. Не удается получить доступ к камере с помощью Internet Explorer.

Ответ: Возможные причины:

- a. Неисправность сети.

Решение: Сначала Вы можете подключиться к сети с помощью ПК и проверить, исправен ли сетевой кабель. Проверьте также, исправно ли сетевое соединение между камерой и ПК.

- b. IP-адрес камеры занят другим устройством или ПК.

Решение: Вы можете подключить камеру непосредственно к компьютеру и изменить IP-адрес или воспользоваться инструментом поиска IP-адресов.

- c. Возможно, камера находится в другом сегменте сети.

Решение: Проверьте IP-адрес и маску сети.

2. Не удается получить доступ к камере после установки обновления.

Ответ: Очистите кэш Вашего браузера.

Выполните следующие шаги: Откройте Internet Explorer, нажмите на «Tools (Инструменты)» и выберите «Internet Options (Свойства обозревателя)». Далее Вы сможете увидеть разделы «Temporary Internet files (Временные Интернет-файлы)». Нажмите на «Delete Files (Удалить файлы)», , откроется диалоговое окно, в котором Вам нужно установить флажок «Delete all offline content (Удалить все оффлайн-данные)» и нажать на «OK».

Также Вы можете нажать на «Start (Пуск)» и выбрать опцию «Run (Выполнить)», затем ввести «arp -d» в окне командной строки». Повторите попытку осуществить доступ к камере.

3. Не удается отобразить весь интерфейс.

Ответ: Закройте некоторые опции браузера Internet Explorer.

Выполните следующие шаги: Откройте Internet Explorer, нажмите на «View (Просмотр)», выберите «Tools (Инструменты)», закройте «Favorites bar (Избранное)», «Status bar (Строка состояния)» и «Command bar (Панель команд)».

4. Не работает POE-подключение IP-камеры к коммутатору POE.

Ответ: Возможные причины:

- d. Убедитесь в том, что IP-камера поддерживает функцию POE. Если это невозможно подтвердить, проверьте это свойство камеры через идентификационный номер или разобрав устройство.
- e. Используйте 8-жильный сетевой кабель, не используйте 4-жильный сетевой кабель.
- f. Проверьте корректность работы коммутатора POE.
- g. Протокол питания IP-камер по технологии POE несовместим с протоколом питания коммутатора, можно поменять коммутатор.
- h. POE-модуль IP-камеры поврежден, замените этот модуль.

5. Не работает подключение IP-камеры к сетевому видеорегистратору NVR.

Ответ: Возможные причины:

- a. Сегменты сети IP-камеры и NVR различны.

Решение: Измените значения первых трех групп IP-адреса IP-камеры так, чтобы они совпадали со значениями первых трех групп IP-адреса сетевого видеорегистратора, измените последнюю группу цифр на другие значения.

- b. Пароль IP-камеры был изменен.

Решение: Найдите соответствующее устройство в интерфейсе сетевого видеорегистратора, нажмите кнопку «Edit (Изменить)», затем введите для IP-камеры корректный пароль.

6. После форматирования SD-карты в IP-камере не отображается ее паспортная ёмкость.

Ответ: Возможные причины:

- a. Проблема с SD-картой.

Решение: Используйте другую SD-карту или SD-карту другой емкости.

- b. SD-карта содержит несколько разделов, поэтому IP-камера не может корректно считывать данные.

Решение: Удалите разделы SD-карты на компьютере.