

Руководство пользователя



**Цифровая
IP-видеокамера**

Руководство пользователя

- **Об этом руководстве**

Данное руководство относится к цифровым IP-видеокамерам и содержит инструкции по их использованию и управлению ими. Все изображения, графики и иная информация приведены только для ознакомления и разъяснения функций. Информация, содержащаяся в руководстве, может быть изменена без предварительного оповещения в связи с обновлением программного обеспечения или по другим причинам. Пожалуйста, скачайте последнюю версию руководства на нашем сайте. Данное руководство предназначено для использования квалифицированными специалистами. В руководстве под термином «камера» подразумевается «цифровая IP-видеокамера».

- **Информация по сервисному обслуживанию**

При покупке изделия требуйте его полной проверки и заполнения гарантийного талона. Отсутствие правильно и полностью заполненного гарантийного талона является основанием для отказа в гарантийном обслуживании.

1. Гарантия не осуществляется в следующих случаях:

- наличие видимых механических и электрических (термических) повреждений, возникших в результате нарушения правил эксплуатации или транспортировки изделия, следов самостоятельного ремонта или ремонта в неуполномоченном сервисном центре;
- нарушение оригинальных пломб производителя, маркировки или невозможность считывания изделия;
- повреждений, вызванных стихийными бедствиями, пожаром, неблагоприятными бытовыми факторами;
- повреждений, вызванных использованием нестандартных материалов и запчастей;
- повреждения, вызванные несоответствием Госстандарту параметров питающих, телекоммуникационных, кабельных сетей и др. подобных внешних факторов;
- повреждения, связанные с попаданием на информационные и питающие соединения напряжения с непредусмотренными значениями и (или) полярностью.

Не допускается приложение усилий по вытаскиванию провода из корпуса, которые могут привести к механическим повреждениям внутри камеры, либо отсутствию/ухудшению контакта внутренних частей камеры.

2. Гарантия не распространяется:

- на расходные материалы (батареи и т. п.), в том числе и находящиеся в готовом изделии;
- на ущерб, причиненный другому оборудованию, работающему в сопряжении с данным изделием.

- **Соответствие нормативам**



Данное изделие соответствует требованиям нормативных документов ТР ТС: 020/2011 «Электромагнитная совместимость технических средств» Декларация о соответствии ТС № RU Д-RU.OM02.B.05240.

- **Инструкции по безопасности**

Приведенные ниже инструкции призваны помочь избежать неправильного использования оборудования, которое может привести к возникновению чрезвычайных ситуаций.

- Используйте блоки питания с выходным напряжением, соответствующим требуемому для конкретной модели оборудования (12В DC или 24В AC).
- Для исключения риска поражения электрическим током или возгорания не подвергайте оборудование воздействию влаги.
- Установка оборудования должна осуществляться квалифицированным сервисным персоналом.
- Для предотвращения перебоев в работе оборудования из-за отключения электричества используйте источники резервного питания.
- Удостоверьтесь, что потолочная конструкция может выдержать нагрузку в 50Н (ньютон), если камера будет установлена на потолке.
- Если оборудование не работает должным образом, пожалуйста, обратитесь в службу технической поддержки или в авторизованный сервисный центр. Никогда не предпринимайте попыток самостоятельно разобрать камеру. Наша компания не несет ответственности за любые проблемы, вызванные попытками ремонта вне авторизованного сервисного центра.
- Перед использованием камеры удостоверьтесь, что напряжение источника питания соответствует напряжению, требуемому для камеры.
- Не бросайте камеру и не подвергайте ее сильному механическому воздействию.
- Не касайтесь пальцами объектива камеры, если он не закрыт корпусным стеклом. Если требуется его очистка, воспользуйтесь чистым отрезком ткани и небольшим количеством этилового спирта. Если камера не будет использоваться в течение продолжительного времени, наденьте на объектив защитный колпачок для предотвращения его загрязнения.
- Не направляйте объектив камеры в сторону мощных источников света, таких как солнце или лампы накаливания. Это может привести к выходу из строя сенсора камеры.
- Сенсор камеры может выйти из строя из-за воздействия лазерного луча. Поэтому при использовании любого лазерного оборудования удостоверьтесь, что лазерный луч не направляется в сторону объектива камеры.
- Не используйте камеру в местах, где возможны экстремально низкие или высокие температуры (рабочий диапазон температур может быть различным для разных моделей камер и всегда указан в паспорте камеры). Не используйте камеру в сильно запыленных помещениях или при высокой влажности, а также не подвергайте камеру воздействию электромагнитного излучения.
- Удостоверьтесь, что в месте установки камеры имеется эффективный отвод тепла, то есть помещение вентилируется.
- Избегайте воздействия на внутреннюю камеру воды и других жидкостей.
- Для транспортировки камеры используйте ее заводскую упаковку.
- Замена заводских элементов питания (батарей) на иные, несовместимые с оборудованием, может привести к выходу оборудования из строя и возникновению возгорания. Пожалуйста, используйте батареи, рекомендованные производителем.

При использовании камер, оснащенных инфракрасной (ИК) подсветкой, обратите внимание на следующие пункты:

- Пыль и жирный налет на купольной камере приводят к проблемам с переотражением ИК-подсветки. Пожалуйста, не удаляйте защитную плёнку с купола камеры до окончания процесса установки. Для удаления загрязнений с купола используйте отрезок чистой мягкой ткани.
- Удостоверьтесь, что в непосредственной близости от места установки камеры нет предметов с отражающими поверхностями. Свет от ИК-подсветки будет отражаться от них и попадать в объектив камеры, вызывая засветку.

- Пластиковое кольцо вокруг объектива должно плотно прилегать к внутренней поверхности купола камеры чтобы изолировать объектив от переотраженного света ИК-подсветки. Закрепите купол на основании камеры таким образом, чтобы пластиковое кольцо и купол были соприкасались без просветов.

Оглавление

1.	Системные требования программного обеспечения	9
2.	Подключение в сеть	9
2.1.	Настройка IP-видеокамеры для работы через LAN	9
2.1.1.	Кабельное соединение	9
2.1.2.	Активация камеры	10
2.2.	Настройка IP-видеокамеры для работы через WAN.....	14
2.2.1.	Статический внешний IP-адрес	14
2.2.2.	Динамический внешний IP-адрес	15
3.	Доступ к IP-видеокамере.....	17
3.1.	Доступ через веб-браузер	17
3.2.	Доступ через программу-клиент.....	18
4.	Настройка Wi-Fi.....	19
4.1.	Настройка соединения Wi-Fi для обычного режима и режима точки доступа.....	19
4.1.1.	Беспроводное соединение в обычном режиме (Manage Mode).....	19
4.1.2.	Беспроводное соединение в режиме точки доступа (Ad-hoc Mode).....	20
4.1.3.	Описание режимов безопасности.....	20
4.2.	Соединение Wi-Fi с использованием WPS	22
4.3.	Сетевые настройки для беспроводного соединения.....	23
5.	Просмотр видеопотока	25
5.1.	Интерфейс просмотра видеопотока (Live View).....	25
5.2.	Запуск видеопотока.....	26
5.3.	Ручной захват скриншотов и запись видеопотока	26
5.4.	Управление PTZ	26
5.4.1.	Использование панели управления PTZ.....	27
5.4.2.	Сохранение и запуск пресета (предустановки).....	28
5.4.3.	Сохранение и вызов тура.....	28
6.	Настройки IP-видеокамеры (Settings)	30
6.1.	Настройка локальных параметров (Local settings).....	30
6.2.	Изменение системных настроек (System Settings)	31
6.2.1.	Основная информация (Basic Information)	31
6.2.2.	Настройки времени (Time Settings).....	32
6.2.3.	Настройка RS232 (RS232 Settings)	33
6.2.4.	Настройка RS485 (RS485 Settings)	34
6.2.5.	Настройка DST (DST Settings).....	34
6.2.6.	Настройка внешних устройств (External Devices Settings)	35

6.2.7.	Настройка VCA (VCA Settings)	35
6.3.	Обслуживание (Maintenance)	35
6.3.1.	Обновление и настройки (Upgrade & Maintenance).....	35
6.3.2.	Лог (Log)	36
6.3.3.	Системные службы (System Service).....	36
6.4.	Настройки безопасности (Security Settings).....	37
6.4.1.	Авторизация (Authentication)	37
6.4.2.	Фильтр IP-адресов (IP Address Filter).....	37
6.4.3.	Службы безопасности (Security Service).....	38
6.5.	Управление аккаунтом (User Management).....	39
6.5.1.	Управление аккаунтом (User Management)	39
6.5.2.	Пользователи онлайн (Online Users)	41
7.	Сеть (Network).....	42
7.1.	Базовые настройки (Basic Settings).....	42
7.1.1.	Настройка TCP/IP (TCP/IP Settings)	42
7.1.2.	Настройка DDNS (DDNS Settings)	43
7.1.3.	Настройка PPPoE (PPPoE Settings).....	44
7.1.4.	Настройки портов (Port Settings)	45
7.1.5.	Настройка NAT / UPnP (NAT Settings)	45
7.2.	Дополнительные настройки (Advanced Settings)	46
7.2.1.	Настройка SNMP (SNMP Settings)	46
7.2.2.	Настройка FTP (FTP Settings)	47
7.2.3.	Настройка Email (Email Settings).....	49
7.2.4.	Доступ через облачную платформу (Platform Access)	50
7.2.5.	Мобильная связь (Wireless Dial).....	50
7.2.6.	Настройка HTTPS (HTTPS Settings).....	51
7.2.7.	Настройка QoS (QoS Settings).....	53
7.2.8.	Настройка 802.1x (802.1x Settings)	53
8.	Настройки видео/аудио (Video/Audio Settings).....	55
8.1.	Настройка видео (Video Settings).....	55
8.2.	Настройка аудио (Audio Settings)	57
8.3.	Настройка ROI (ROI Settings).....	57
8.4.	Отображение информации (Display Info. on Stream)	59
8.5.	Вырезка области (Target Cropping).....	59
9.	Настройки изображения (Image Settings)	60
9.1.	Параметры изображения (Display Settings).....	60
9.1.1.	Переключение «День/ночь» (Day/Night Auto-Switch).....	60
9.1.2.	Переключение День/Ночь (Day/Night Scheduled-Switch)	63

9.2.	Настройка OSD (OSD Settings)	64
9.3.	Настройка маски приватности (Privacy Mask)	65
9.4.	Настройка наложения изображения («Picture Overlay»)	65
10.	Настройки событий (Event Settings).....	67
10.1.	Базовые события (Basic Events).....	67
10.1.1.	Настройка детекции движения (Motion Detection)	67
10.1.2.	Настройка тревоги по саботажу (Video Tampering Alarm)	72
10.1.3.	Настройка тревожных входов (Alarm Input).....	72
10.1.4.	Настройка тревожных выходов (Alarm Output)	73
10.1.5.	Предупреждения (Handling Exception).....	74
10.1.6.	Настройка других тревог (Other Alarm)	74
10.2.	Интеллектуальная аналитика (Smart Events)	76
10.2.1.	Настройка детекции звука (Audio Exception Detection).....	76
10.2.2.	Настройка детекции потери фокусировки (Defocus Detection)	76
10.2.3.	Настройка детекции изменения сцены (Scene Change Detection).....	77
10.2.4.	Настройка детекции лиц (Face Detection)	77
10.2.5.	Настройка детекции вторжения (Intrusion Detection)	78
10.2.6.	Настройка детекции пересечения линии (Line Crossing Detection).....	79
10.2.7.	Настройка детекции входа в область (Region Entrance Detection)	80
10.2.8.	Настройка детекции выхода из области (Region Exiting Detection).....	81
10.2.9.	Настройка детекции оставленных вещей (Unattended Baggage Detection).....	81
10.2.10.	Настройка детекции кражи (Object Removal Detection)	82
10.3.	Настройка VCA (VCA Configuration)	83
10.3.1.	Анализ поведения (Behavior Analysis)	83
10.3.2.	Снимок лица (Face Capture).....	86
10.3.3.	Подсчет людей (People Counting)	88
10.3.4.	Подсчет (Counting)	90
10.3.5.	Тепловая карта (Heat Map)	90
10.3.6.	Дорожный трафик (Road Traffic)	91
11.	Настройки хранения	93
11.1.	Настройка расписания записи	93
11.2.	Настройка расписания захвата скриншотов (Capture Schedule)	94
11.3.	Настройка сетевого хранилища (Net HDD)	96
11.4.	Поиск карты памяти (Memory Card Detection)	97
11.5.	Настройка облегченного хранилища (Lite Storage).....	98
12.	Архив (Playback)	99
13.	Скриншоты (Snapshots)	101
14.	Приложения (Application)	102

14.1.	Статистика обнаружения лиц (Face Capture Statistics).....	102
14.2.	Статистика подсчета людей (People Counting Statistics).....	102
14.3.	Статистика тепловой карты (Heat Map Statistics)	103
14.4.	Статистика подсчета.....	103
15.	Дополнительная информация	104
15.1.	Программное обеспечение iRUS Configurator	104
15.2.	Проброс портов.....	106

1. Системные требования программного обеспечения

- Операционная система: Microsoft Windows XP SP1 или выше
- Частота CPU: 2 ГГц или выше
- Объем оперативной памяти: 1 Гб или больше
- Разрешение дисплея: 1024 x 768 или выше
- Веб-браузер: Internet Explorer 8.0 или выше, Apple Safari 5.0.2 или выше, Mozilla Firefox 5.0 или выше, Google Chrome 18 или выше.

2. Подключение в сеть

Примечания:

- Обратите внимание, что при настройке доступа к оборудованию через интернет данное оборудование подвергается риску сетевой атаки. Для избегания сетевых атак и потери данных используйте системы защиты и устанавливайте оборудование за сетевым экраном. Если оборудование в результате атаки перестало работать должным образом, обратитесь в службу технической поддержки или в авторизованный сервисный центр.
- Для обеспечения сетевой безопасности рекомендуется периодически производить подключение к оборудованию и его проверку. Кроме того, рекомендуется периодически менять пароль доступа к оборудованию.

Прежде, чем начать:

- Если требуется настроить камеру для работы внутри локальной сети, обратитесь к разделу 2.1 – Настройка IP-видеокамеры для работы через LAN (локальную сеть).
- Если требуется настроить камеру для работы через интернет, обратитесь к разделу 2.1 – Настройка IP-видеокамеры для работы через WAN (интернет).

2.1. Настройка IP-видеокамеры для работы через LAN

Для просмотра видеопотока и конфигурирования камеры через локальную сеть (LAN) требуется, чтобы камера и компьютер находились в одной подсети. Требуется установить программное обеспечение **iRUS Configurator** для поиска камер и назначения IP-адресов.

Примечание: более детальная информация касательно настройки **iRUS Configurator** находится в главе «Дополнительная информация» в конце руководства.

2.1.1. Кабельное соединение

На приведенных ниже рисунках показаны два возможных способа подключения камеры к компьютеру через кабель.

- Для тестового подключения вы можете соединить камеру непосредственно с сетевой картой компьютера, как показано на рисунке 2.1.



Рисунок 2.1 – Подключение камеры к компьютеру напрямую

- На рисунке 2.2 показано подключение с использованием коммутатора.



Рисунок 2.2 – Подключение камеры к компьютеру через коммутатор

2.1.2. Активация камеры

Перед началом использования камеры ее необходимо активировать, установив надежный пароль. Возможна активация через программное обеспечение **iRUS Configurator**, через веб-браузер, через клиентское ПО.

- **Активация через веб-браузер.**

1. Подключите камеру к источнику питания, соедините камеру с сетью.
2. Введите IP-адрес камеры в адресную строку веб-браузера, затем нажмите «Вход» для входа в интерфейс активации. *Примечания:*
 - IP-адрес камеры по умолчанию – **192.168.1.64**.
 - Для камер с включенным по умолчанию режимом DHCP IP-адрес выдается автоматически. В этом случае удобнее всего активировать камеру через программное обеспечение **iRUS Configurator**.

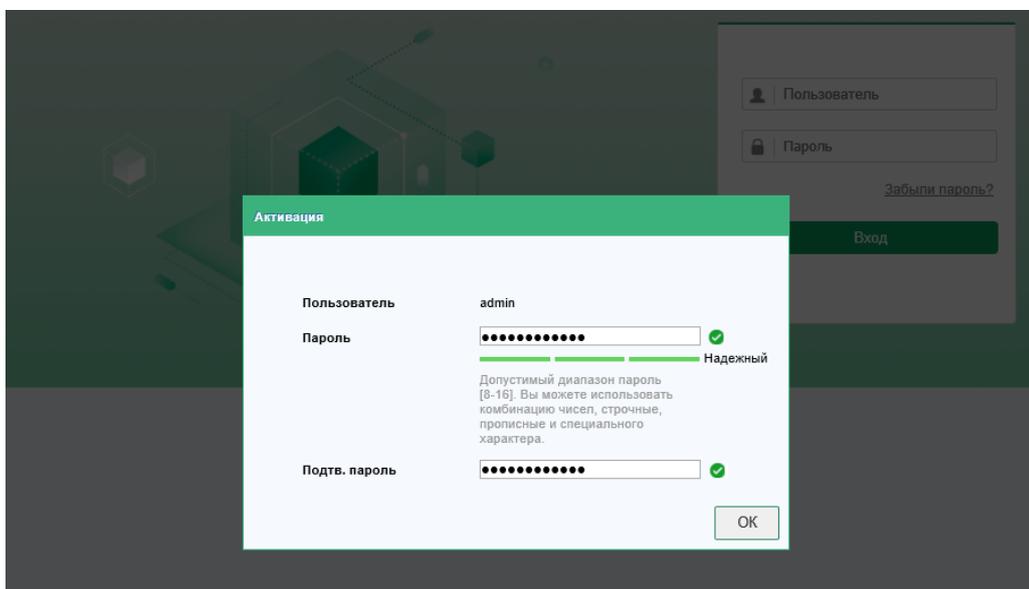


Рисунок 2.3 – Активация через веб-браузер

3. Придумайте надежный пароль и введите его в соответствующее поле. *Примечание:* Настоятельно рекомендуется установить сложный пароль, состоящий из более чем 8 символов, отвечающий как минимум трем из следующих критериев: содержит заглавные буквы, содержит строчные буквы, содержит цифры, содержит специальные символы. Также рекомендуется регулярно изменять пароль.
4. Подтвердите пароль, введя его снова в соответствующее поле.
5. Нажмите ОК для сохранения пароля и входа в веб-интерфейс камеры.

- **Активация через программное обеспечение iRUS Configurator**

ПО **iRUS Configurator** может быть использовано для поиска подключенных устройств, активации камер и сброса паролей. ПО **iRUS Configurator** можно скачать с нашего сайта. Для установки следуйте инструкциям программы-инсталлятора. Активация камеры:

1. Запустите ПО **iRUS Configurator** для поиска подключенных устройств.
2. В столбце «Status» («Статус») приводится статус активации. Выберите устройство без активации («Inactive»).

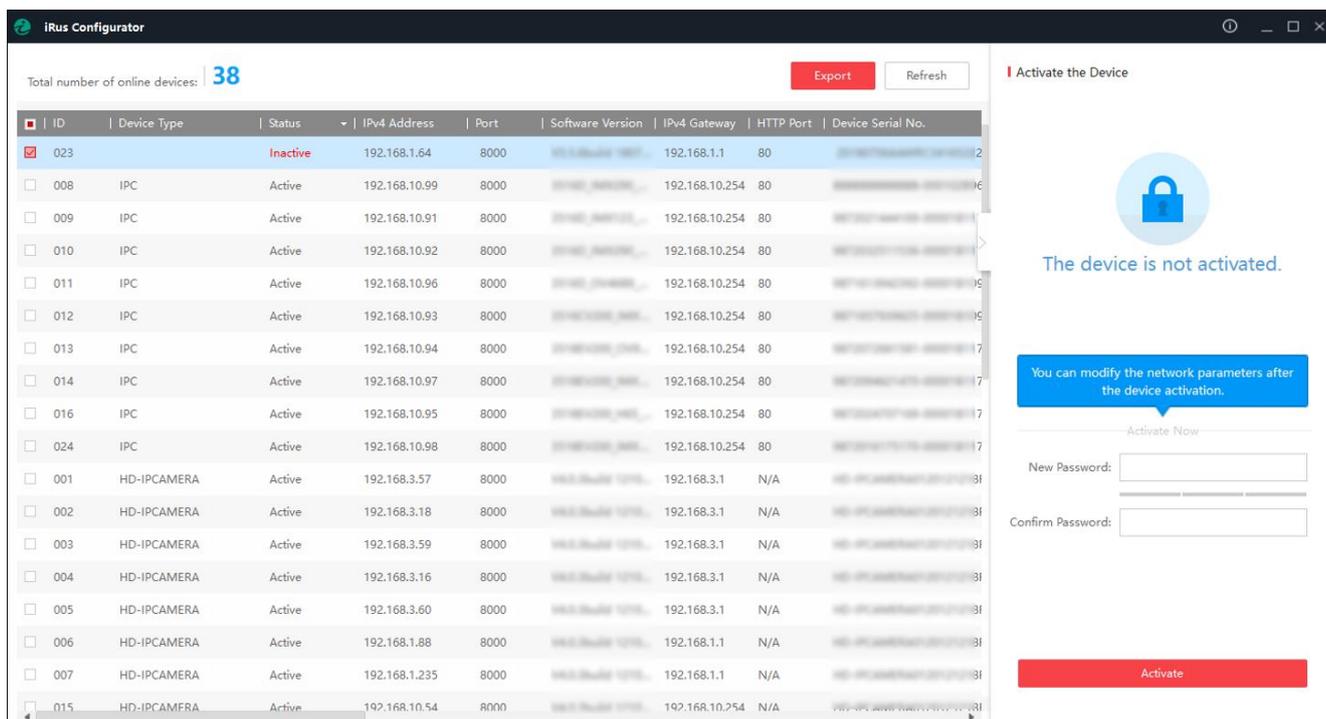


Рисунок 2.4 – Интерфейс ПО **iRUS Configurator**

3. Придумайте надежный пароль и введите его в соответствующее поле, затем подтвердите пароль.

Примечание: Настоятельно рекомендуется установить сложный пароль, состоящий из более чем 8 символов, отвечающий как минимум трем из следующих критериев: содержит заглавные буквы, содержит строчные буквы, содержит цифры, содержит специальные символы. Также рекомендуется регулярно изменять пароль.

4. Нажмите ОК для сохранения пароля.
Узнать о том, успешно ли прошла активация, можно по записи в окне, появившемся после нажатия ОК. Если произошел сбой активации, проверьте, отвечает ли пароль всем требованиям и попробуйте снова.
5. Измените IP-адрес камеры на соответствующий подсети вашего компьютера. Сделать это можно либо путем ручной установки IP-адреса, либо путем установки галочки «Enable DHCP» («Вкл. DHCP»).
6. Введите пароль и нажмите «Save» («Сохранить») для применения сетевых настроек.

Modify Network Parameters

Enable DHCP
 Enable Hik-Connect

Device Serial No.:

IP Address:

Port:

Subnet Mask:

Gateway:

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length:

HTTP Port:

Security Verification

Admin Password:

Modify

[Forgot Password](#)

Рисунок 2.5 – Изменение IP-адреса камеры

- **Активация через клиентское ПО iRUS**

Программа-клиент – это универсальное средство управления для различных типов устройств. Вы можете скачать программу-клиент с нашего сайта. Установите клиент, следуя инструкциям программы-установщика. Активация камеры:

1. Запустите программу-клиент, после чего появится панель управления программой, как показано на рисунке ниже.

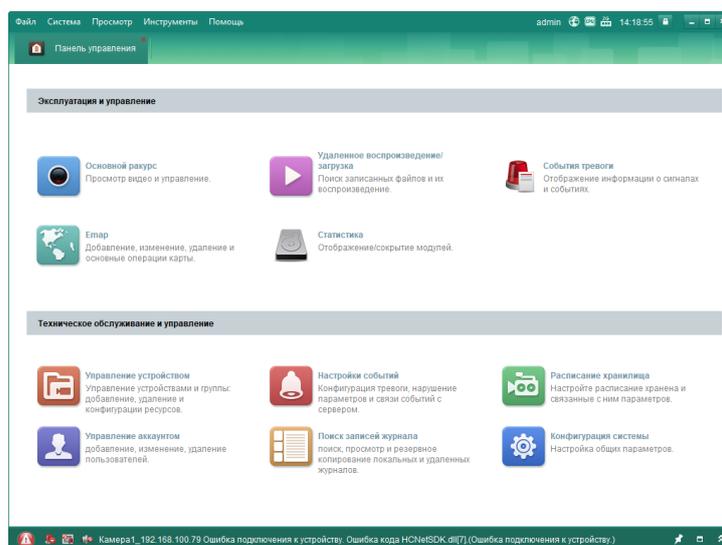


Рисунок 2.6 – Панель управления

- Нажмите на «Device Management» («Управление устройствами») для входа в соответствующий интерфейс, как показано на следующем рисунке.

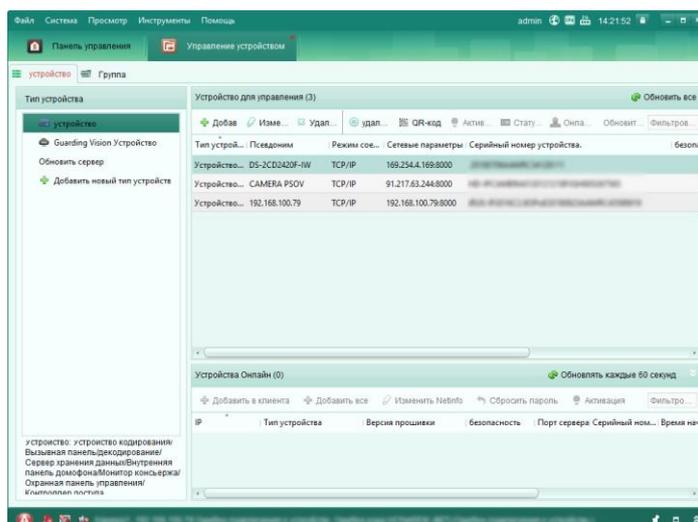


Рисунок 2.7 – Интерфейс «Управление устройствами»

- Проверьте статус устройств в списке и выберите устройство без активации («Inactive»).
- Нажмите на «Activate» («Активировать») для входа в интерфейс активации.
- Придумайте надежный пароль и введите его в соответствующее поле, затем подтвердите пароль.

Примечание: Настоятельно рекомендуется установить сложный пароль, состоящий из более чем 8 символов, отвечающий как минимум трем из следующих критериев: содержит заглавные буквы, содержит строчные буквы, содержит цифры, содержит специальные символы. Также рекомендуется регулярно изменять пароль.



Рисунок 2.8 – Интерфейс активации в программе-клиенте

- Нажмите ОК для начала активации.
- Нажмите на «Modify Net Info» («Изменить сетевые параметры») для входа в интерфейс изменения сетевых настроек устройства, как показано на рисунке ниже.

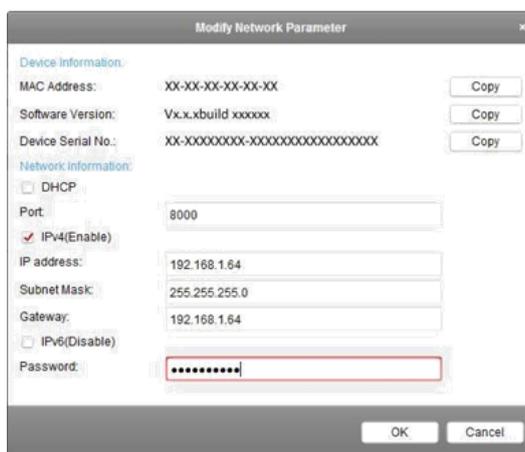


Рисунок 2.9 – Изменение сетевых настроек в программе-клиенте

8. Измените IP-адрес камеры на соответствующий подсети вашего компьютера. Сделать это можно либо путем ручной установки IP-адреса, либо путем установки галочки «Enable DHCP» («Вкл. DHCP»).
9. Введите пароль для применения сетевых настроек.

2.2. Настройка IP-видеокамеры для работы через WAN

В этом разделе приводятся разъяснения по настройкам доступа к камере через статический и динамический внешний IP-адрес.

2.2.1. Статический внешний IP-адрес

Прежде, чем начать:

Пожалуйста, получите статический IP-адрес от своего Интернет-провайдера. Со статическим IP-адресом можно подключить камеру как через маршрутизатор, так и непосредственно к кабелю от провайдера.

- **Подключение камеры через маршрутизатор**

1. Подключите камеру к маршрутизатору через сетевой кабель.
2. Присвойте камере локальный IP-адрес, маску подсети и адрес шлюза. Обратитесь к разделу 2.1.2 для более полной информации по изменению сетевых настроек камеры.
3. Примените статический IP-адрес в маршрутизаторе. В большинстве случаев достаточно задать на интерфейсе WAN режим DHCP и IP-адрес будет автоматически получен от провайдера.
4. Настройте проброс портов 80, 8000 и 554 (переадресацию портов, перенаправление портов, Portforwarding, Virtual Servers, Port Mapping – возможные названия функции в зависимости от модели маршрутизатора). Последовательность действий для настройки проброса портов варьируется в зависимости от производителя маршрутизатора. Пожалуйста, свяжитесь с поставщиком маршрутизатора для более подробной информации или обратитесь к руководству пользователя от маршрутизатора.

Примечание: Обратитесь к главе «Дополнительная информация» в конце руководства для получения дополнительной информации о пробросе портов.

5. Подключитесь к камере через веб-браузер или программу-клиент через интернет.



Рисунок 2.10 – Доступ к камере через статический IP-адрес

- **Подключение камеры непосредственно к кабелю от провайдера**

Имеется возможность задать статический внешний адрес на самой камере и подключить ее непосредственно к кабелю от провайдера не используя маршрутизатор. Обратитесь к разделу 2.1.2 для более полной информации по изменению сетевых настроек камеры.



Рисунок 2.11 – Доступ к камере через статический IP-адрес напрямую

2.2.2. Динамический внешний IP-адрес

Прежде, чем начать:

Пожалуйста, получите динамический IP-адрес от своего Интернет-провайдера. С динамическим IP-адресом можно подключить камеру как через маршрутизатор, так и через модем.

- **Подключение камеры через маршрутизатор**

1. Подключите камеру к маршрутизатору через сетевой кабель.
2. Присвойте камере локальный IP-адрес, маску подсети и адрес шлюза. Обратитесь к разделу 2.1.2 для более полной информации по изменению сетевых настроек камеры.
3. В настройках маршрутизатора установите PPPoE имя, пароль и подтверждение пароля.
4. Настройте проброс портов 80, 8000 и 554 (переадресацию портов, перенаправление портов, Portforwarding, Virtual Servers, Port Mapping – возможные названия функции в зависимости от модели маршрутизатора). Последовательность действий для настройки проброса портов варьируется в зависимости от производителя маршрутизатора. Пожалуйста, свяжитесь с поставщиком маршрутизатора для более подробной информации или обратитесь к руководству пользователя от маршрутизатора.
Примечание: Обратитесь к главе «Дополнительная информация» в конце руководства для получения дополнительной информации о пробросе портов.
5. Примените доменное имя от провайдера доменных имен.
6. Настройте DDNS на маршрутизаторе (зависит от конкретной модели маршрутизатора, смотрите руководство от вашей модели).
7. Подключитесь к камере, используя полученное доменное имя.

- **Подключение камеры через модем**

У камеры имеется поддержка PPPoE. Камера получает внешний IP-адрес через ADSL-соединение при подключении ее к модему. Требуется настроить параметры PPPoE на камере. Обратитесь к разделу 7.1.3 – «Настройка параметров PPPoE» для более детальной информации.



Рисунок 2.12 – Подключение к камере через динамический IP-адрес

Примечание: Полученный IP-адрес динамически назначается через PPPoE, т.е. адрес постоянно меняется, в том числе при перезагрузке камеры. Чтобы исправить неудобство использования динамического IP-адреса, следует воспользоваться услугами какого-либо сервиса DDNS (например, dyndns.com). Ниже приведены инструкции для публичного и частного DDNS-серверов.

- Публичный DDNS-сервер
 1. Получите доменное имя от DDNS-сервиса.
 2. Настройте DDNS в соответствующем разделе настроек камеры. Обратитесь к разделу 7.1.2 «Настройка DDNS» для более детальной информации.
 3. Подключитесь к камере через доменное имя.

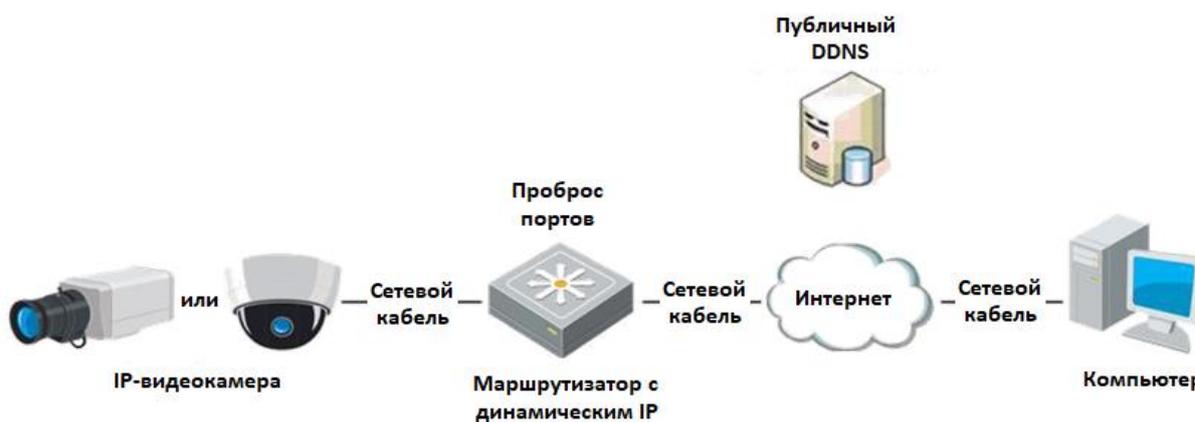


Рисунок 2.13 – Схема для случая использования публичного DDNS

- Частный DDNS-сервер
 1. Установите и запустите серверное программное обеспечение (DNS) на компьютере со статическим внешним IP-адресом.
 2. Подключитесь к камере через веб-браузер или через программу-клиент.
 3. Включите DDNS и выберите в качестве протокола «IP Server» («IP Сервер»). Обратитесь к разделу 7.1.2 для более детальной информации.

3. Доступ к IP-видеокамере

3.1. Доступ через веб-браузер

Последовательность действий для подключения через веб-браузер:

1. Откройте веб-браузер.
2. В адресной строке веб-браузера введите IP-адрес камеры и нажмите Enter для входа в интерфейс ввода логина и пароля.



Рисунок 3.1 – Интерфейс входа

3. Произведите активацию камеры, если она используется впервые (подробнее в разделе 2.1.2).

Примечания:

- Стандартный IP-адрес камеры – 192.168.1.64 (на некоторых моделях по умолчанию может быть включен DHCP – смотрите паспорт устройства).
- Если камера не активирована, пожалуйста, проделайте действия, описанные в разделе 2.1.2.

4. В правой верхней части окна выберите в качестве языка интерфейса «Русский» или «English».

5. Введите имя пользователя и пароль и нажмите «Login» («Вход»).

Примечания:

- Пользователь-администратор (admin) должен при необходимости правильно настроить учетные записи пользователей/операторов, а также их полномочия. Рекомендуется удалять не использующиеся учетные записи, а также необязательные полномочия учетных записей.
- При неправильном вводе пароля администратора (admin) 7 раз подряд камера будет заблокирована для IP-адреса, с которого производились попытки (для других учетных записей ограничение составляет 5 попыток).

6. Перед просмотром видеопотока и конфигурированием камеры требуется установить плагин для веб-браузера. Следуйте инструкциям программы-установщика.

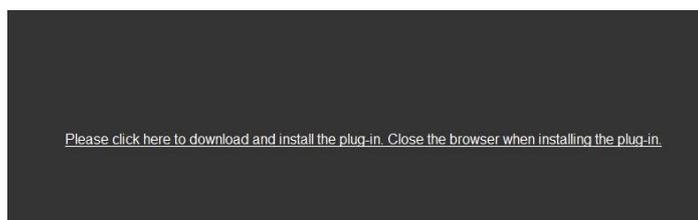


Рисунок 3.2 – Скачивание плагина для веб-браузера

Примечание: может потребоваться закрытие веб-браузера для установки плагина. Пожалуйста, откройте веб-браузер и введите учетные данные заново после установки плагина.

3.2. Доступ через программу-клиент

Программа-клиент iRus позволяет просматривать видеопотоки камер и производить их настройку. Следуйте инструкциям программы-установщика для правильной установки ПО iRus. Панель управления ПО iRus и меню просмотра видеопотока представлены на рисунках ниже.

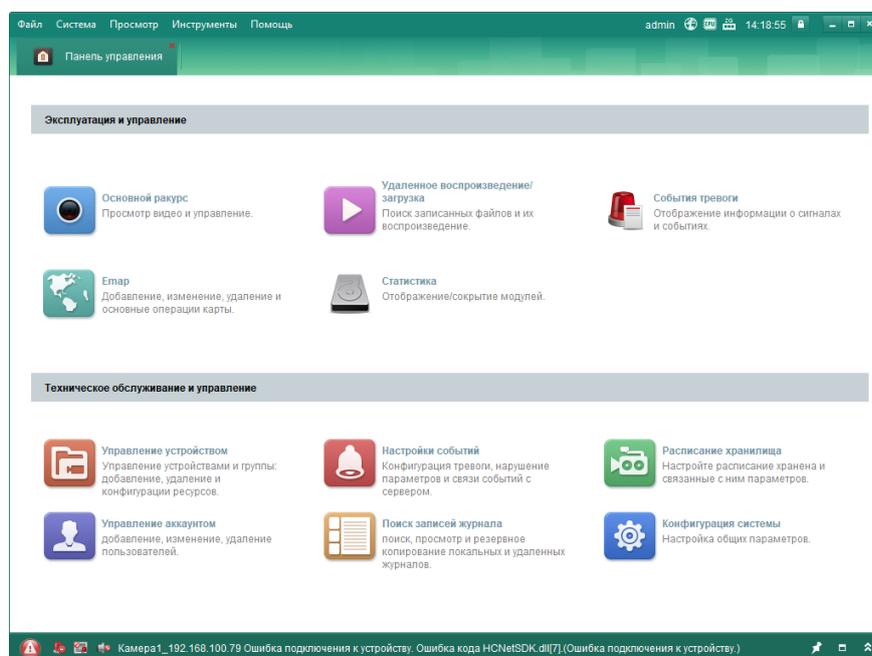


Рисунок 3.3 – Интерфейс панели управления (Control Panel) программы iRus

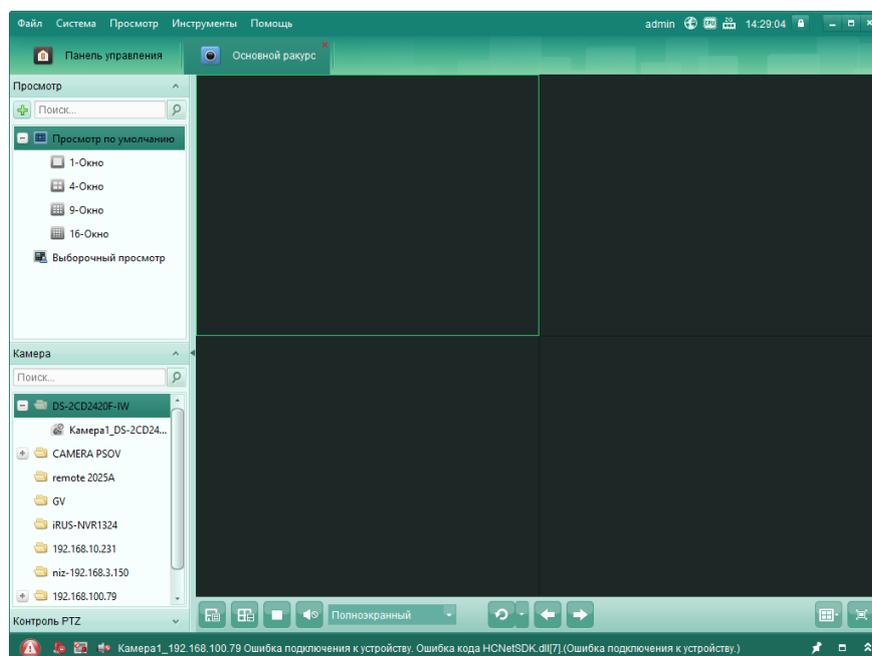


Рисунок 3.4 – Меню просмотра видеопотока программы iRus

4. Настройка Wi-Fi

При подключении через беспроводную сеть пропадает необходимость прокладки сетевого кабеля, что достаточно удобно для решения ряда задач охранного видеонаблюдения. Информация из данной главы относится только к камерам, оснащенным модулем Wi-Fi.

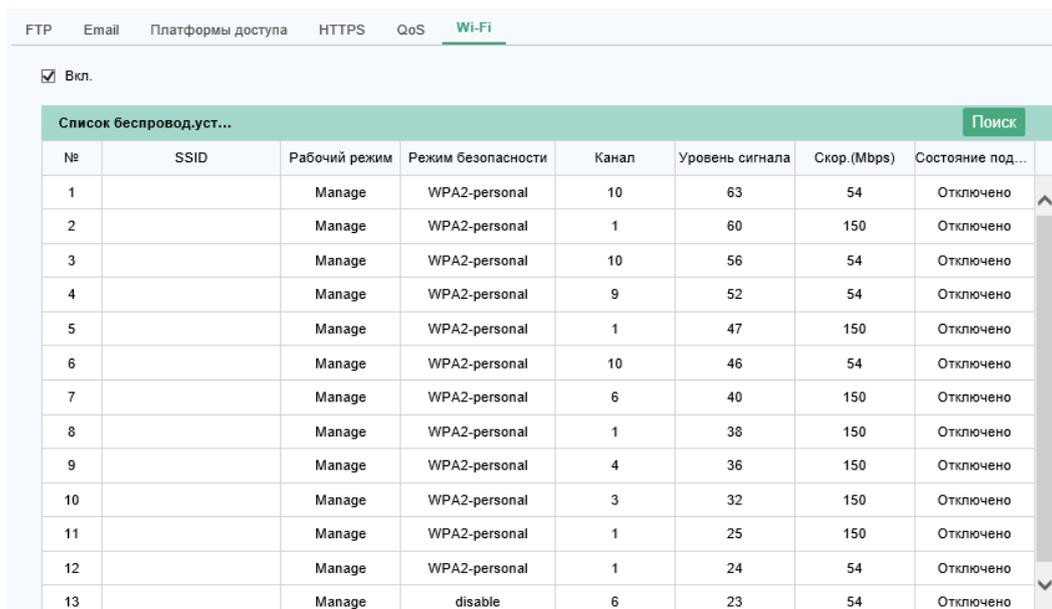
4.1. Настройка соединения Wi-Fi для обычного режима и режима точки доступа

Поддерживаются два режима подключения. Выберите требующийся режим и следуйте инструкциям, приведенным ниже, для настройки.

4.1.1. Беспроводное соединение в обычном режиме (Manage Mode)

Последовательность действий:

1. Зайдите в интерфейс настройки Wi-Fi: Configuration («Настройки») – Network («Сеть») - Advanced Settings («Доп. настройки») - Wi-Fi.
2. Нажмите «Search» («Поиск») для поиска работающих Wi-Fi сетей.



The screenshot shows the 'Wi-Fi' configuration page with a search bar and a table of detected networks. The table has columns for '№', 'SSID', 'Рабочий режим', 'Режим безопасности', 'Канал', 'Уровень сигнала', 'Скор.(Mbps)', and 'Состояние под...'. There are 13 rows of data, with the last row having a 'disable' security mode.

№	SSID	Рабочий режим	Режим безопасности	Канал	Уровень сигнала	Скор.(Mbps)	Состояние под...
1		Manage	WPA2-personal	10	63	54	Отключено
2		Manage	WPA2-personal	1	60	150	Отключено
3		Manage	WPA2-personal	10	56	54	Отключено
4		Manage	WPA2-personal	9	52	54	Отключено
5		Manage	WPA2-personal	1	47	150	Отключено
6		Manage	WPA2-personal	10	46	54	Отключено
7		Manage	WPA2-personal	6	40	150	Отключено
8		Manage	WPA2-personal	1	38	150	Отключено
9		Manage	WPA2-personal	4	36	150	Отключено
10		Manage	WPA2-personal	3	32	150	Отключено
11		Manage	WPA2-personal	1	25	150	Отключено
12		Manage	WPA2-personal	1	24	54	Отключено
13		Manage	disable	6	23	54	Отключено

Рисунок 4.1 – Список сетей Wi-Fi

3. Щелчком мыши выберите нужную сеть из списка.
4. В строке «Network Mode» («Тип сети») выберите пункт «Manage» («Управление»), а в строках «Security Mode» («Режим безопасности») и «Encryption Type» («Тип кодирования») должен автоматически выставиться нужный режим, соответствующий вашей сети. Пожалуйста, не меняйте его вручную без необходимости.
Примечание: Данные параметры полностью идентичны тем, что выставлены на маршрутизаторе (точке доступа).
5. Введите ключ (пароль) от сети.

4.1.2. Беспроводное соединение в режиме точки доступа (Ad-hoc Mode)

При выборе режима точки доступа не требуется подключать камеру к маршрутизатору (точке доступа). Принцип подключения такой же, как при прямом подключении камеры кабелем к компьютеру. В этом случае камера сама выступает точкой доступа. Последовательность действий для настройки:

1. Выберите режим «Ad-hoc» («Точка доступа»).

Рисунок 4.2 – Настройки Wi-Fi в режиме Ad-hoc

2. Введите SSID (идентификатор, т.е. имя беспроводной сети) камеры.
3. Выберите режим безопасности и тип кодирования («Security Mode» и «Encryption Type»).
4. Включите Wi-Fi на компьютере.
5. В списке найденных сетей на компьютере выберите то название, что ввели в поле SSID (пункт 2).
6. Введите пароль и подключитесь к сети.

4.1.3. Описание режимов безопасности

Рисунок 4.3 – Режимы безопасности

Имеется возможность выбрать следующие режимы безопасности («Security Modes»): без шифрования (not-encrypted), WEP, WPA-personal, WPA-enterprise, WPA2-personal, WPA2-enterprise.

- **Режим WEP**

Рисунок 4.4 – Режим WEP

«Авторизация» («Authentication») – выберите «Открытый» («Open») или «Общий» («Shared») тип ключа шифрования, в зависимости от того, какой метод используется на точке доступа. Не на всех точках доступа имеется данная опция, в этом случае лучше попробовать использовать режим «Открытый» («Open»).

«Длина ключа» («Key Length») – здесь задается длина ключа, используемого для шифрования. На выбор варианты 64 и 128 бит.

«Тип ключа» («Key Type») – доступны различные типы ключа, в зависимости от используемой точки доступа:

- HEX – позволяет вручную ввести HEX-ключ
- ASCII – в этом случае ключ должен состоять конкретно из 5 символов для WEP 64-бит или 13 символов для WEP 128-бит.

• Режимы WPA-personal и WPA2-personal

Выберите тип шифрования (изначально выбран автоматически по настройкам самой точки доступа, в большинстве случаев лучше не менять) и введите ключ от точки доступа:

Рисунок 4.5 – Настройки для WPA-personal

• Режимы WPA-enterprise и WPA2-enterprise

Выберите тип клиент-серверной аутентификации, использующийся на точке доступа: EAP-TLS или EAP-PEAP.

1. EAP-TLS:

Рисунок 4.6 – EAP-TLS

«Пользователь» («Identity») – введите User ID для представления в сети.

«Пароль» («Private key password») – введите пароль для данного User ID.

«Версия EAPOL» («EAPOL version») – выберите версию, использующуюся на точке доступа.

«CA сертификат» («CA Certificates») – загрузите сертификат для представления точке доступа для аутентификации.

2. EAP-PEAP:

«Пользователь» («User Name») – введите имя пользователя для представления в сети.

«Пароль» («Password») – введите пароль.

«Версия PEAP» («PEAP Version») – выберите версию PEAP, использующуюся на точке доступа.

«Метка» («Label») – выберите метку, использующуюся на точке доступа.

«Версия EAPOL» («EAPOL Version») – выберите версию EAPOL, использующуюся на точке доступа.

«CA сертификат» («CA Certificates») – загрузите сертификат для представления точке доступа для аутентификации.

Примечание:

В целях сохранения приватности и защиты данных настоятельно рекомендуется использовать надежные пароли для всех имеющихся сетей и устройств. Рекомендуется выбирать пароль, состоящий из более чем 8 символов, отвечающий как минимум трем из следующих критериев: содержит заглавные буквы, содержит строчные буквы, содержит цифры, содержит специальные символы. Также рекомендуется регулярно изменять пароль.

Менеджмент учетных записей и паролей целиком и полностью является зоной ответственности инсталлятора или конечного пользователя.

4.2. Соединение Wi-Fi с использованием WPS

Настройка сети Wi-Fi и впоследствии соединения с камерой в некоторых случаях является весьма нетривиальной задачей. Для упрощения процесса настройки можно воспользоваться функцией WPS.

WPS (Wi-Fi Protected Setup) по сути является простым способом настройки прямого подключения к точке доступа. WPS позволяет легко добавлять в беспроводную сеть новые устройства без долгого ввода паролей. Существуют два режима WPS-соединения: PBC и PIN.

Примечание: При включении функции WPS не требуется настраивать такие параметры как тип шифрования и не требуется знать ключ беспроводной сети.

Рисунок 4.7 – Настройки WPS

- **Режим PBC**

В режиме PBC (Push-Button-Configuration) пользователю требуется лишь нажать на кнопку, физическую или программную (кнопка «Подключение» / «Connect» в веб-интерфейсе) на точке доступа и на регистрируемом устройстве.

1. Установите галочку на «Enable WPS» («Включить WPS»).
2. В качестве режима соединения выберите «PBC».

Примечание: Необходимо, чтобы данный режим поддерживался как точкой доступа, так и всеми подключаемыми устройствами.

3. Проверьте, есть ли на маршрутизаторе кнопка подключения по WPS. Если есть – нажмите на кнопку; в результате должен сработать индикатор, что будет означать включение режима WPS.

Для более точного описания процесса включения WPS на маршрутизаторе обратитесь к руководству от вашей модели маршрутизатора.

4. Нажмите кнопку WPS на камере. Если физической кнопки нет, требуется нажать соответствующую кнопку в веб-интерфейсе.
5. Нажмите на кнопку «Подключение» («Connect»).
Когда режим PBC будет включен одновременно и на камере, и на точке доступа, камера автоматически подключится к беспроводной сети.

- **Режим PIN**

Данный режим предполагает использование PIN-кода (Personal Identification Number), который может быть указан на беспроводном устройстве. Данный PIN-код в дальнейшем используется для подключения к сети.

Рисунок 4.8 – Использование PIN-кода для WPS-подключения

1. Выберите беспроводное соединение, WPS.
2. Выберите режим «User router PIN code» («Использовать PIN-код роутера»).
3. Если PIN-код генерируется на стороне маршрутизатора, то требуется ввести данный код в поле «Router PIN code» («PIN-код роутера»).

Также можно сгенерировать PIN-код на стороне камеры. Время существования PIN-кода составляет 120 секунд.

1. Нажмите на «Generate» («Генерировать»).
2. Введите сгенерированный код на маршрутизаторе в соответствующем пункте его веб-интерфейса.

4.3. Сетевые настройки для беспроводного соединения

Беспроводной сетевой интерфейс имеет IP-адрес по умолчанию 192.168.1.64. При подключении к беспроводной сети адрес может быть изменен.

1. Войдите в интерфейс настройки TCP/IP: Configuration («Настройки») – Network («Сеть») – Basic Settings («Базовые настройки») – TCP/IP
2. Выберите вкладку «Wlan».
3. Измените адрес IPv4, маску подсети и сетевой шлюз, если это необходимо.
Процедура изменения настроек аналогична таковой для проводного соединения.
Для автоматического получения IP-адреса от маршрутизатора установите галочку на пункте «DHCP».

TCP/IP DDNS Порт NAT

Lan **Wlan**

DHCP

IPv4 Адрес

IPv4 Маска подсети

IPv4 Шлюз

MAC адрес

Адрес мультикаста

Активировать рассылку мультикаст

DNS сервер

Предпочт DNS сервер

Альтернат DNS сервер

Рисунок 4.9 – Настройка параметров Wlan

5. Просмотр видеопотока

5.1. Интерфейс просмотра видеопотока (Live View)

Интерфейс просмотра видеопотока предназначен для отображения видео с камеры в реальном времени, захвата скриншотов, управления камерой по PTZ, установки/вызова пресетов и изменения некоторых параметров изображения.

Войдите в веб-интерфейс камеры чтобы получить доступ к данному интерфейсу.

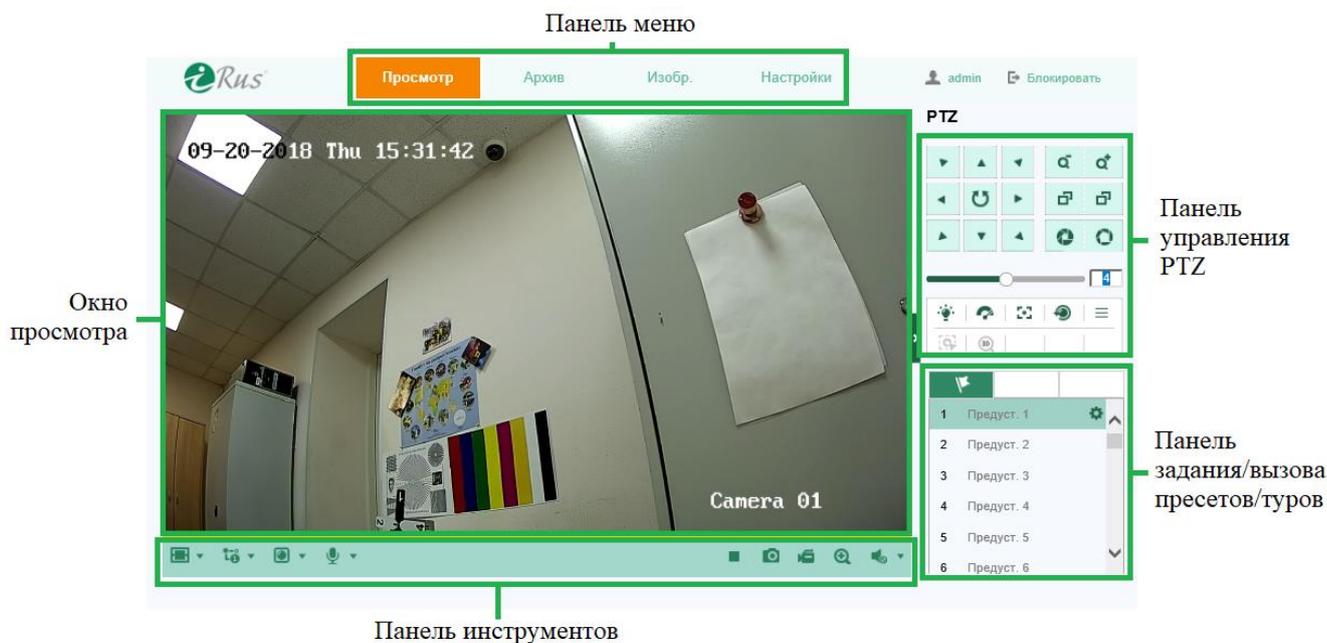


Рисунок 5.1 – Интерфейс просмотра видеопотока

- **Панель меню:**

Содержит кнопки перехода в разделы веб-интерфейса «Live View» («Просмотр»), «Playback» («Архив»), «Picture» («Изображение»), «Application» («Приложения» – не на всех моделях), «Configuration» («Настройка»).

- **Окно просмотра:**

Здесь отображается видеопоток с камеры.

- **Панель инструментов:**

Данная панель позволяет изменять размер окна просмотра, изменять тип потока. Кроме того, с помощью данной панели можно останавливать и запускать просмотр, захватывать скриншоты, записывать видео, включать и отключать звук, запускать двустороннюю аудиосвязь, управлять цифровым приближением и др.

- **Панель управления PTZ:**

Позволяет осуществлять управление поворотными камерами.

- **Панель задания/вызова пресетов/туров:**

Позволяет сохранять, вызывать, удалять пресеты и туры для поворотных камер.

5.2. Запуск видеопотока

Как показано на рисунке 5.2, для запуска видеопотока следует нажать на кнопку ▶.



Рисунок 5.2 – Панель инструментов

Таблица 5.1. Описание функций панели инструментов.

Иконка	Описание
▶ / ■	Запуск / остановка видеопотока
4:3	Установка соотношения сторон окна 4:3
16:9	Установка соотношения сторон окна 16:9
⊠	Исходный размер окна
⊞	Подстроить размер окна
📹	Просмотр первого потока
📹	Просмотр второго потока
📹	Просмотр третьего потока
📷	Выбор стороннего плагина
📷	Захват скриншота
📹 / 📹	Запуск / остановка записи видеопотока
🔊 / 🔊	Включение / отключение звука
🎤 / 🎤	Включение / отключение микрофона
🔍 / 🔍	Включение / отключение цифрового приближения

Примечание: вид иконок может быть иным в зависимости от модели камеры и прошивки.

5.3. Ручной захват скриншотов и запись видеопотока

Нажмите на кнопку 📷 для захвата скриншота или нажмите на 📹 для осуществления записи видеопотока. Пути сохранения скриншотов и видеозаписей могут быть настроены в разделе веб-интерфейса «Configuration» («Настройки») – «Local» («Локальные»). Настройка записи по расписанию описана в разделе 6.1.

Примечание: Скриншоты сохраняются на компьютере в формате JPEG или BMP.

5.4. Управление PTZ

В режиме просмотра видеопотока имеется возможность управления поворотными камерами.

Примечание: Для реализации всех функций PTZ подключенная камера должна иметь поддержку соответствующих функций. Пожалуйста, правильно установите все параметры в настройках PTZ камеры (раздел данного руководства 6.2.4).

5.4.1. Использование панели управления PTZ

Нажмите на кнопку  для открытия панели управления PTZ. Для скрытия панели нажмите на кнопку . Нажмите на кнопки направлений для перемещения направления обзора камеры.

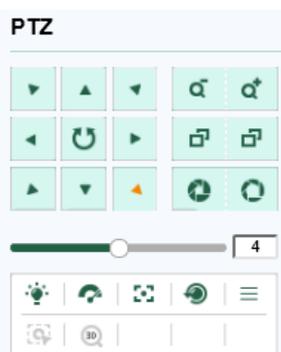


Рисунок 5.3 – Панель управления PTZ

Нажмите на кнопки изменения зума, фокуса, диафрагмы для управления объективом.

Примечания:

- Имеются всего восемь кнопок направления.
- Для камер, у которых реализовано только управление объективом, кнопки направления недоступны.

Таблица 5.2. Описание функций панели управления PTZ.

Иконка	Описание
	Управление оптическим зумом
	Управление фокусом
	Управление диафрагмой
	Скорость управления PTZ
	Включить / выключить подсветку
	Включить / выключить очиститель
	Дополнительный объектив
	Инициализация объектива
	Калибровка скорости наклона / поворота
	Запустить ручной трекинг
	Запустить 3D-зум

5.4.2. Сохранение и запуск пресета (предустановки)

- **Сохранение пресета:**

1. В панели управления PTZ выберите номер пресета из списка.



Рисунок 5.4 – Сохранение пресета

2. Используйте кнопки управления PTZ для перемещения обзора камеры в нужную позицию:
 - Поверните камеру под нужным углом
 - Наклоните камеру под нужным углом
 - Выставьте необходимое приближение (зум)
 - Сфокусируйте объектив (при необходимости)
3. Нажмите на кнопку ⚙ для сохранения текущей позиции камеры в пресет.
4. Для удаления пресета нажмите на кнопку ✕.

- **Вызов пресета:**

Эта функция предназначена для перевода обзора камеры в заранее сохраненную позицию (пресет). Выберите нужный пресет на панели управления PTZ и нажмите на кнопку 📄 для его вызова.

Также можно щелкнуть мышью на поле ввода номера пресета, ввести нужный номер и вызвать его.

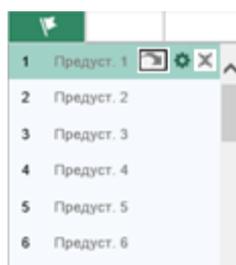


Рисунок 5.5 – Вызов пресета

5.4.3. Сохранение и вызов тура

Примечание: перед сохранением тура необходимо сохранить как минимум два пресета.

Последовательность действий:

1. Нажмите на кнопку ⚙ для входа в интерфейс настройки туров.
2. Выберите номер тура, затем нажмите на кнопку ➕ для добавления заранее сохраненных пресетов.

3. Выберите пресет, введите значение скорости перехода на пресет от 1 до 10 (Speed) и времени остановки на данном пресете (Time) в секундах.
4. Нажмите на ОК для сохранения первого пресета.
5. Повторите вышеперечисленные шаги для добавления других пресетов.

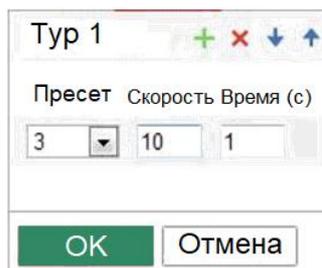


Рисунок 5.6 – Добавление пресета в тур

6. Нажмите ОК для сохранения тура.
7. Нажмите ► для запуска тура или ■ для его остановки.
8. (Опционально) Нажмите ✕ для удаления тура.

6. Настройки IP-видеокамеры (Settings)

6.1. Настройка локальных параметров (Local settings)

Локальные параметры – это параметры просмотра видеопотока в веб-интерфейсе, записи и захвата скриншотов. Кроме того, здесь задаются пути сохранения скриншотов и записей для компьютера, на котором в данный момент запущен веб-интерфейс камеры.

1. Зайдите в интерфейс локальной конфигурации: Configuration («Настройки») – Local («Локальные»).

The screenshot shows the 'Local Settings' interface with the following sections and options:

- Параметры отображения (Display Parameters):**
 - Протокол (Protocol): TCP, UDP, MULTICAST, HTTP
 - Включить Производительность (Enable Performance): Кратчайшее время (Shortest Delay), Авто (Auto)
 - Правила (Rules): Вкл. (On), Выкл. (Off)
 - Формат изображения (Image Format): JPEG, BMP
- Настройки файла записи (File Recording Settings):**
 - Размер файла записи (Recording File Size): 256M, 512M, 1G
 - Сохранять видео в папку (Save video to folder): [text input]
 - Сохранять загр. файлы (Save uploaded files): [text input]
- Настройки картинки и клипа (Picture and Clip Settings):**
 - Сохранять снимки в папку (Save snapshots to folder): [text input]
 - Сохранять снимки из архива (Save snapshots from archive): [text input]
 - Сохранять видео из архива (Save video from archive): [text input]

At the bottom, there is a green button labeled 'Сохранить' (Save).

Рисунок 6.1 – Интерфейс локальных параметров

2. Настройте следующие параметры:

- **Live View Parameters** («Параметры отображения»): выберите транспортный протокол и установите параметры производительности передачи потока.
 - **Protocol Type** («Протокол»): TCP, UDP, Multicast, HTTP.
 - **TCP**: Обеспечивает доставку пакетов с данными без потерь ценой увеличения задержки видео.
 - **UDP**: Обеспечивает передачу видеопотока без задержек.
 - **HTTP**: Обеспечивает такое же качество изображения, как при TCP без необходимости открытия доступа до каких-либо портов кроме HTTP.
 - **Multicast**: Рекомендуется использовать только при использовании функционала Multicast. Более подробная информация о Multicast приведена в разделе 7.1.1.
 - **Play Performance** («Производительность»): возможность установить на значение Shortest Delay («Кратчайшее время») или Auto («Авто»).
 - **Rules** («Правила»): при включении данного параметра возможно отображение прямоугольных рамок вокруг детектируемых объектов (например, лиц людей) при наличии данного функционала на камере.
 - **Image Format** («Формат изображения»): выберите формат файлов скриншотов.
- **Record File Settings** («Настройки файлов записи»): различные настройки записи через веб-интерфейс.

- **Record File Size** («Размер файла»): выберите предельный размер файла записываемого в веб-интерфейсе видео.
- **Save record files to** («Сохранять видео в папку»): выберите путь для сохранения файлов записанного через веб-интерфейс видео.
- **Save downloaded files to** («Сохранять загр. файлы»): выберите путь для сохранения файлов, скачанных из архива на устройстве.
- **Picture and Clip Settings** («Настройки картинки и клипа»): различные настройки скриншотов, захватываемых через веб-интерфейс.
 - **Save snapshots in live view to** («Сохранять снимки в папку»): выберите путь для сохранения скриншотов, захваченных из меню просмотра видеопотока в реальном времени.
 - **Save snapshots when playback to** («Сохранять снимки из архива»): выберите путь для сохранения скриншотов из меню воспроизведения устройства.
 - **Save clips to** («Сохранять видео из архива»): выберите путь сохранения фрагментов, вырезанных в меню просмотра архива устройства.

Примечание: Нажав **Browse** («Выбор»), можно выбрать пути через проводник.

3. Нажмите **Save** («Сохранить») для применения настроек.

6.2. Изменение системных настроек (System Settings)

6.2.1. Основная информация (Basic Information)

Зайдите в меню основной информации об устройстве: Configuration («Настройки») – System («Система») - System Settings («Настройки системы») - Basic Information («Основная информация»).

В интерфейсе «Basic Information» («Основная информация») имеется возможность редактирования имени устройства («Device name») и номера устройства («Device No.»). Остальная информация недоступна для редактирования: модель, версия прошивки, серийный номер и т.д.

Осн. информация	Настройки времени	DST	RS232	Сведения
Имя устройства	<input type="text" value="IP CAMERA"/>			
Номер устройства	<input type="text" value="88"/>			
Модель	<input type="text"/>			
Серийный №	<input type="text"/>			
Версия прошивки	<input type="text" value="V5.4.81 build 180717"/>			
Версия кодир.	<input type="text" value="V1.0 build 180110"/>			
Интернет версия	<input type="text" value="V4.0.51 build 180710"/>			
Версия плагина	<input type="text" value="V3.0.6.1"/>			
Количество каналов	<input type="text" value="1"/>			
Количество жестких дис...	<input type="text" value="0"/>			
Кол-во трев. вх.	<input type="text" value="1"/>			
Кол-во трев. вых.	<input type="text" value="1"/>			
<input type="button" value="Сохранить"/>				

Рисунок 6.2 – Основная информация

• Обновление онлайн

Для некоторых моделей камер доступно онлайн-обновление. При нажатии на кнопку «Update» («Обновить») камера опросит сервер на наличие более новой версии прошивки. Если новая версия доступна, то номер версии будет отображен в поле «New Version» («Новая версия»). При нажатии на кнопку «Upgrade» («Прошить») будет установлена данная новая версия прошивки.

Firmware Version	VX.X.X build XXXXXX	Update
New Version	VX.X.X build XXXXXX	Upgrade

Рисунок 6.3 – Обновление онлайн

Примечание: Не отключайте питание камеры во время процесса обновления. Во время обновления камера может быть недоступна. Требуется от 1 до 2 минут для осуществления процесса обновления.

6.2.2. Настройки времени (Time Settings)

В данном разделе руководства приведены инструкции по настройке времени и синхронизации.

1. Зайдите в раздел настроек времени: Configuration («Настройки») – System («Система») – System Settings («Настройки системы») – Time Settings («Настройки времени»).

Рисунок 6.4 – Настройки времени

2. Выберите часовой пояс («Time Zone»), соответствующий вашему местоположению.
3. Установите настройки NTP.
 - а) Установите флажок напротив NTP для включения данной функции.
 - б) Настройте следующие параметры:
 - **Server Address** («Адрес сервера»): IP-адрес сервера NTP.
 - **NTP Port** («Порт»): порт NTP-сервера.
 - **Interval** («Интервал»): Интервал в минутах между двумя запросами синхронизации.
 - в) (*Опционально*) Нажатие кнопки «Test» («Тест») позволяет проверить возможность синхронизации времени при текущих настройках.

Рисунок 6.5 – Синхронизация времени с NTP-сервером

Примечание: Если камера подключена к интернету, возможно использовать различные публичные NTP-серверы, например, time.windows.com, ntp1.vniiftri.ru, ntp2.vniiftri.ru, ntp21.vniiftri.ru. Если камера работает внутри локальной сети, то можно использовать любой локальный сервер с настроенным программным обеспечением NTP.

- **Настройка времени вручную**

1. Установите флажок напротив «Manual Time Sync.» («Ручная синхронизация времени») для включения соответствующей функции.
2. Нажмите на значок 📅 для выбора даты и времени из календаря.
3. (Опционально) При установке галочки на «Sync. with computer time» («Синхронизировать со временем ПК») время камеры будет синхронизировано с временем на компьютере, с которого производится настройка.

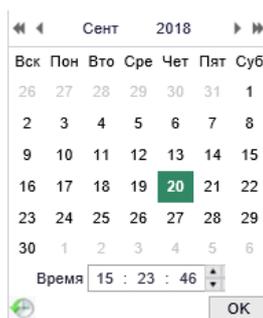


Рисунок 6.6 – Ручная настройка времени

4. Нажмите «Save» («Сохранить») для применения настроек.

6.2.3. Настройка RS232 (RS232 Settings)

Порт RS232 может быть использован в двух назначениях:

- Конфигурирование параметров камеры. При подключении камеры к последовательному порту компьютера и использовании соответствующего ПО, например, HyperTerminal, могут быть изменены некоторые параметры камеры. При этом параметры последовательного порта компьютера должны совпадать с таковыми у камеры.
- Сквозной канал. Подключение устройства с последовательным портом непосредственно к камере. Этим устройством впоследствии можно управлять удаленно, подключаясь к камере через сеть.

Осн. информация	Настройки времени	DST	RS232	Сведения
Скорость, бод	115200			
Биты данных	8			
Стоповый бит	1			
Соответствие	Нет			
Потоковый контроль	Нет			
Использование	Панель упр-я			



Рисунок 6.7 – Настройка RS232

Последовательность действий для настройки:

1. Зайдите в раздел настроек RS232: Configuration («Настройки») – System («Система») – System Settings («Настройки системы») – RS232.
2. Установите параметры «Baud Rate» («Скорость, бод»), «Data Bit» («Биты данных»), «Stop Bit» («Стоповый бит»), «Parity» («Четность»), «Flow Control» («Потоковый контроль»), «Usage» («Использование»).

Примечание: При подключении камеры по порту RS232 к любому другому устройству его параметры должны в точности совпадать с выставленными в данном меню.

3. Нажмите «Save» («Сохранить») для применения настроек.

6.2.4. Настройка RS485 (RS485 Settings)

Порт RS485 используется для управления поворотными камерами. Последовательность действий для настройки:

1. Зайдите в раздел настроек RS485: Configuration («Настройки») – System («Система») – System Settings («Настройки системы») – RS485.
2. Введите параметры интерфейса RS485 и нажмите «Save» («Сохранить») для применения настроек. По умолчанию «Baud Rate» («Скорость») – 9600, «Data Bit» («Биты данных») – 8, «Stop Bit» («Стоп-бит») – 1, «Parity» («Четность») и «Flow Control» («Управление потоком») – отключены.

Примечание: «Baud Rate» («Скорость»), «PTZ Protocol» («протокол PTZ») и «PTZ Address» («адрес PTZ») должны в точности совпадать с параметрами поворотной камеры.

6.2.5. Настройка DST (DST Settings)

DST (Daylight Saving Time) – автоматический перевод часов на летнее время. В настоящий момент (2018 год) в России отменен перевод на летнее время.

При необходимости настройки последовательность действий следующая:

1. Зайдите в раздел настроек DST: Configuration («Настройки») – System («Система») – System Settings («Настройки системы») – DST.
2. Выберите время перевода на летнее время и на зимнее.
3. Выберите значение смещения времени («DST Bias»).
4. Нажмите «Save» («Сохранить») для применения настроек.

6.2.6. Настройка внешних устройств (External Devices Settings)

Существует возможность управления внешними устройствами, подключенными к камере, такими как стеклоочиститель или ИК-подсветка. Для разных моделей камер могут поддерживаться разные внешние устройства.

1. Зайдите в раздел настроек внешних устройств: Configuration («Настройки») – System («Система») – System Settings («Настройки системы») – External Devices («Внешние устройства»).
2. Установите галочку «Enable Supplement Light» («Вкл. дополнительную подсветку») для активации внешней подсветки.
3. Настройте ползунки для установки нужного уровня яркости.
4. Выберите режим работы подсветки: «Timing» («Расписание») или «Auto» («Авто»).
 - **Расписание:** подсветка будет включена по настроенному расписанию. Требуется настроить время начала и время окончания.
 - **Авто:** Подсветка будет включена автоматически в соответствии с внешним освещением.
5. Нажмите «Save» («Сохранить») для применения настроек.

6.2.7. Настройка VCA (VCA Settings)

Раздел настроек VCA предназначен для включения некоторых функций, таких как детектор лиц и тепловая карта. Те или иные функции могут быть доступны в зависимости от модели камеры.

1. Зайдите в раздел настроек VCA: Configuration («Настройки») – System («Система») – System Settings («Настройки системы») – VCA Resource («Ресурсы VCA»).
2. Выберите требующуюся комбинацию функций.
3. Нажмите «Save» («Сохранить») для применения настроек. Для сохранения настроек потребуется перезагрузка камеры.

Примечания:

- Функции, представленные в разделе VCA могут варьироваться в зависимости от модели камеры.
- Детектор лиц (Face Detection) и тепловая карта (Heat Map) являются взаимоисключающими функциями.
- Этот раздел может быть недоступен на некоторых моделях камер.

6.3. Обслуживание (Maintenance)

6.3.1. Обновление и настройки (Upgrade & Maintenance)

Интерфейсе обновления и обслуживания позволяет осуществлять такие операции, как перезагрузка устройства, сброс к заводским настройкам, экспорт и импорт файлов конфигурации, обновление прошивки.

Для входа в данный раздел настроек перейдите в Configuration («Настройки») – System («Система») – Maintenance («Обслуживание») – Upgrade & Maintenance («Обновление и настройки»).

- **Reboot** («Перезапуск»): перезапуск устройства.
- **Restore** («Возобновить»): сброс к заводским установкам всех параметров, кроме сетевых настроек и учетных записей пользователей.
- **Default** («По умолчанию»): сброс к заводским установкам всех параметров без исключения.

Примечание: Обратите внимание, что при выборе данного пункта IP-адрес устройства также будет сброшен на заводский.

- **Export/Import Config. File** («Экспорт/Импорт»): экспорт (выгрузка) и импорт (загрузка) файла конфигурации, который используется для хранения всех настроек камеры. Это может быть полезно для настройки большого количества камер.
- **Upgrade** («Обновление»): обновление прошивки устройства.

Примечание: обновление прошивки устройства может занимать от 1 до 10 минут. Пожалуйста, не отключайте камеру во время процесса обновления. После завершения обновления камера перезагрузится автоматически.

6.3.2. Лог (Log)

Информация о действиях, ошибках, тревогах может быть записана в журнал (лог). Имеется возможность экспортировать файл журнала при необходимости.

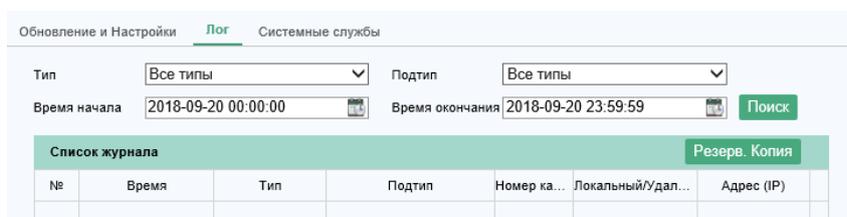


Рисунок 6.8 – Интерфейс поиска записей журнала

Прежде, чем начать:

Подготовьте сетевое хранилище или SD-карту для экспорта файла журнала.

1. Зайдите в интерфейс поиска записей журнала: Configuration («Настройки») – System («Система») – Maintenance («Обслуживание») – Log («Лог»).
2. Выберите условия поиска: «Major Type» («Тип»), «Minor Type» («Подтип»), «Start Time» («Время начала») и «End Time» («Время окончания»).
3. Нажмите на «Search» («Поиск»), чтобы найти файлы журнала. Найденные файлы будут отображены в списке.
4. Нажмите на «Export» («Экспорт») для сохранения (выгрузки) файлов журнала.

6.3.3. Системные службы (System Service)

Данный раздел настроек содержит различные программные и аппаратные службы, поддерживаемые камерой. Список служб может быть различным для разных моделей камер. Для камер, поддерживающих функции IR LED, ABF (Auto Back Focus), Auto Defog (анти-туман), Status LED (индикатор-светодиод) имеется возможность их включения и отключения.

- **ABF:** когда функция включена, появляется возможность управления вспомогательной фокусировкой в панели управления PTZ.
- **Third Stream** («Третий поток»): для некоторых моделей камер имеется возможность включения третьего потока; после его включения потребуются перезагрузка камеры.

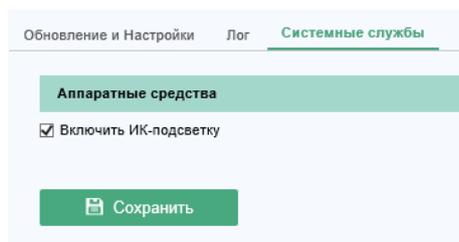


Рисунок 6.9 – Включение ИК-подсветки

6.4. Настройки безопасности (Security Settings)

Данный раздел содержит различные настройки, связанные с авторизацией, фильтрами IP-адресов и т.п.

6.4.1. Авторизация (Authentication)

Имеется возможность включить Авторизацию для доступа к RTSP-потoku с камеры.

1. Зайдите в интерфейс настроек аутентификации: Configuration («Настройки») – System («Система») – Security («Безопасность») – Авторизация («Аутентификация»).

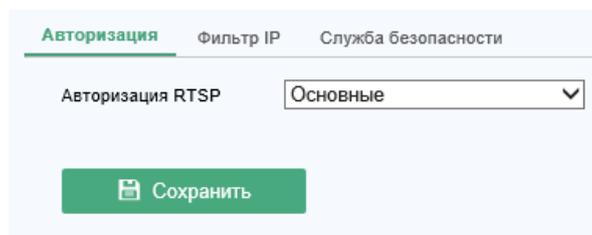


Рисунок 6.10 – Аутентификация для RTSP-потока

2. Выберите в качестве типа авторизации «basic» («основной») или «disable» («выкл.»).

Примечание: При выборе опции «отключен» появится возможность получить видеопоток с камеры, не зная пароля.

3. Нажмите «Save» («Сохранить») для применения настроек.

6.4.2. Фильтр IP-адресов (IP Address Filter)

Данная функция позволяет настроить систему контроля доступа по IP-адресам.

1. Зайдите в интерфейс настроек фильтров IP: Configuration («Настройки») – System («Система») – Security («Безопасность») – IP Address Filter («Фильтр IP»).

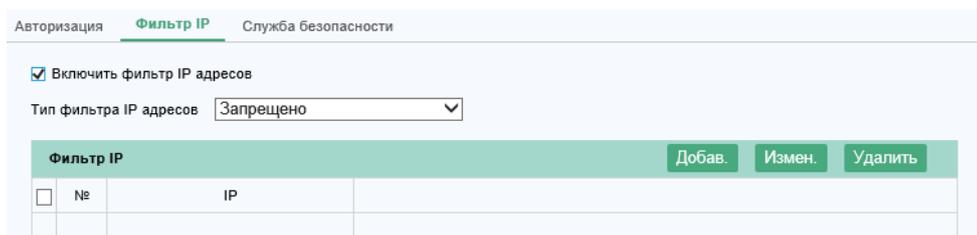


Рисунок 6.11 – Интерфейс настройки IP-фильтров

2. Поставьте галочку на «Enable IP Address Filter» («Вкл. фильтр IP-адресов»).
3. Выберите тип фильтра в выпадающем меню: «Forbidden» («Запрещено») или «Allowed» («Разрешено»).
4. Настройте список IP-адресов.
 - a. Для добавления IP-адреса:

Рисунок 6.12 – Добавление IP-адреса в список

- Нажмите на «Add» («Добавить») чтобы добавить IP;
 - Введите IP-Адрес;
 - Нажмите на ОК для добавления.
- b. Для изменения IP-адреса:

Рисунок 6.13 – Изменение IP-адреса в списке

- Нажмите левой кнопкой мыши по IP-адресу из списка и выберите «Modify» («Изменить»).
 - Измените IP-адрес в соответствующем поле.
 - Нажмите ОК для применения изменений.
- c. Для удаления IP-адреса из списка выберите адрес и нажмите «Delete» («Удалить»).
5. Нажмите «Save» («Сохранить») для применения настроек.

6.4.3. Службы безопасности (Security Service)

В данном разделе осуществляется включение и отключение различных вспомогательных служб, связанных с безопасностью.

1. Зайдите в интерфейс настройки служб безопасности: Configuration («Настройки») – System («Система») – Security («Безопасность») – Security Service («Служба безопасности»).

Рисунок 6.14 – Службы безопасности

2. Установите галочку на «Enable SSH» («Включить SSH») для включения соответствующей службы при необходимости.

- Установите галочку на «Enable Illegal Login Lock» («Включить блокировку несанкционированного доступа») для включения соответствующей службы при необходимости. При включении данной функции IP-адреса, с которых вводится неправильный пароль от учетной записи admin 7 раз подряд или от любой другой учетной записи 5 раз подряд, будут временно попадать в черный список.

Примечание: После блокировки IP-адреса повторно можно пробовать вводить пароль спустя 30 минут.

- Нажмите «Save» («Сохранить») для применения настроек.

6.5. Управление аккаунтом (User Management)

6.5.1. Управление аккаунтом (User Management)

Пользователь-администратор (admin) имеет возможность добавлять, изменять и удалять учетные записи пользователей, а также предоставлять им различные полномочия. Настоятельно рекомендуется ответственно и внимательно относиться к настройке учетных записей и их полномочий.

Зайдите в интерфейс настройки пользователей: Configuration («Настройки») – System («Система») – User Management («Управление аккаунтом»).

Управление аккаунтом			Пользователи онлайн		
Список польз.			Добав.	Измен.	Удалить
№	Пользователь	Права			
1	admin	Администратор			

Рисунок 6.15 – Интерфейс настроек пользователей

- **Добавление пользователя**

Пользователь admin имеет все полномочия по умолчанию и может добавлять, изменять и удалять другие учетные записи. Данный пользователь не может быть удален. Можно лишь изменить его пароль.

- Нажмите «Add» («Добавить»).
- Введите имя пользователя, выберите уровень («Level») и введите пароль («Password»)

Примечания:

- Может быть создано до 31 учетной записи.
 - Пользователи с разными уровнями имеют разные стандартные наборы полномочий.
 - Настоятельно рекомендуется установить сложный пароль, состоящий из более чем 8 символов, отвечающий как минимум трем из следующих критериев: содержит заглавные буквы, содержит строчные буквы, содержит цифры, содержит специальные символы. Также рекомендуется регулярно изменять пароль.
- Установите или снимите галочки на полномочиях, если это требуется.
 - Нажмите ОК для окончания процесса создания пользователя.

Рисунок 6.16 – Добавление пользователя

- **Изменение пользователя**

1. Нажмите левой кнопкой мыши по пользователю в списке и выберите «Modify» («Изменить»).
2. Измените имя пользователя, уровень и пароль.
3. Установите или снимите галочки на полномочиях, если это требуется.
4. Нажмите ОК для применения изменений.

Рисунок 6.17 – Изменение пользователя

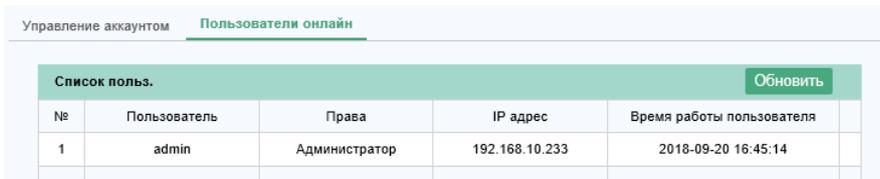
- Удаление пользователя

1. Выберите пользователя и нажмите «Delete» («Удалить»).
2. Нажмите ОК для завершения процесса удаления пользователя.

6.5.2. Пользователи онлайн (Online Users)

В данном разделе можно увидеть список пользователей, в настоящий момент подключенных к устройству. В списке приведена такая информация, как имя пользователя («User Name»), уровень полномочий («Level»), IP-адрес («IP Address») и продолжительность сеанса («User Operation Time»).

Нажмите на «Refresh» («Обновить») для обновления списка.



Управление аккаунтом Пользователи онлайн				
Список польз.				Обновить
№	Пользователь	Права	IP адрес	Время работы пользователя
1	admin	Администратор	192.168.10.233	2018-09-20 16:45:14

Рисунок 6.18 – Просмотр пользователей Online

7. Сеть (Network)

Следуйте инструкциям из этой главы для конфигурирования основных параметров, связанных с сетью.

7.1. Базовые настройки (Basic Settings)

Имеется возможность настройки таких параметров, как TCP/IP, DDNS, PPPoE, Port, NAT.

7.1.1. Настройка TCP/IP (TCP/IP Settings)

Раздел настроек TCP/IP должен быть сконфигурирован для возможности работы камеры по сети. Камера поддерживает как протокол IPv4, так и IPv6. Обе версии протокола могут быть настроены для одновременной бесконфликтной работы, и как минимум одна из версий должна быть настроена в обязательном порядке. Последовательность действий для настройки:

1. Зайдите в интерфейс настройки TCP/IP: Configuration («Настройки») – Network («Сеть») – Basic Settings («Базовые настройки») – TCP/IP.

The screenshot displays the TCP/IP configuration page. At the top, there are tabs for 'TCP/IP', 'DDNS', 'Port', and 'NAT'. Below these, there are sub-tabs for 'Lan' and 'Wlan'. The main configuration area includes:

- Тип NIC:** 10M/100M/1000M Auto
- Дhcp:**
- IPv4 Адрес:** 192.168.10.236 (with a 'Тест' button)
- IPv4 Маска подсети:** 255.255.255.0
- IPv4 Шлюз:** 192.168.10.254
- Режим IPv6:** Объявление маршрута (with a 'Просмотреть объявление маршрута' button)
- IPv6 Адрес:** (empty)
- Маска подсети IPv6:** (empty)
- Шлюз IPv6:** ::
- MAC адрес:** 94:e1:ac:f7:4a:be
- MTU:** 1500
- Адрес мультикаста:** (empty)
- Активировать рассылку мультикаст:**

Below this section is a 'DNS сервер' section with:

- Предпочт DNS сервер:** 8.8.8.8
- Альтернат DNS сервер:** 8.8.4.4

A 'Сохранить' button is located at the bottom of the form.

Рисунок 7.1 – Настройки TCP/IP

2. Установите основные сетевые настройки, включая тип NIC («NIC Type»), адрес IPv4 или IPv6 («IPv4 Address» и «IPv6 Address»), маску подсети IPv4 или IPv6 («IPv4 Subnet Mask» или «IPv6 Subnet Mask»), шлюз по умолчанию IPv4 или IPv6 («IPv4 Default Gateway» или «IPv6 Default Gateway»), значение MTU и адрес Multicast («Multicast Address»).
3. (Опционально) Установите галочку «Enable Multicast Discovery» чтобы камера могла быть найдена внутри локальной сети при помощи клиентского ПО через широковещательный запрос.
4. Установите адреса DNS-серверов – основного и вспомогательного.

5. Нажмите «Save» («Сохранить») для применения настроек.

Примечания:

- Диапазон возможных значений MTU – от 1280 до 1500.
- При задании адреса Multicast поток данных будет отправлен на данный адрес Multicast-группы, что позволит получать поток одновременно нескольким клиентам, путем запроса копии данных от адреса Multicast-группы. Перед использованием этой функции убедитесь, что ваш маршрутизатор поддерживает Multicast.
- Для применения настроек требуется перезагрузка.

7.1.2. Настройка DDNS (DDNS Settings)

Если на камере в качестве основного типа подключения настроено PPPoE, имеется возможность использовать DDNS для доступа к ней.

Прежде, чем начать:

Перед настройкой DDNS на камере требуется регистрация на каком-либо сервисе DDNS.

1. Зайдите в интерфейс настройки DDNS: Configuration («Настройки») – Network («Сеть») – Basic Settings («Базовые настройки») – DDNS.

The screenshot shows the DDNS configuration page. At the top, there are tabs for 'TCP/IP', 'DDNS', 'Port', and 'NAT'. The 'DDNS' tab is active. Below the tabs, there is a checkbox labeled 'DDNS' which is checked. Underneath, there are several input fields: 'DDNS provider' is a dropdown menu showing 'DynDNS'; 'Address of server' is a text box containing 'members.dyndns.org'; 'Domain' is an empty text box; 'Username' is an empty text box; 'Port' is a text box containing '0'; 'Password' is an empty text box; and 'Confirm password' is an empty text box. At the bottom of the form is a green button with a floppy disk icon and the text 'Сохранить' (Save).

Рисунок 7.2 – Настройки DDNS с типом «DynDNS»

2. Установите галочку на «Enable DDNS» («DDNS») для включения данной функции.
 3. Выберите тип DDNS («DDNS Type»). Следующие два типа доступны для выбора: DynDNS и NO-IP.
- **DynDNS:**
 - a. Введите адрес сервера DynDNS в поле «Server Address» (например, members.dyndns.org).
 - b. В поле «Domain» («Домен») введите доменное имя, полученное от сервиса.
 - c. Введите имя пользователя от учетной записи на сервисе в поля «User Name» и «Password» соответственно.
 - d. Нажмите «Save» («Сохранить») для применения настроек.
 - **NO-IP:**
 - a. Выберите тип «NO-IP».
 - b. Введите адрес сервера («Server Address»): www.noip.com

- c. Введите доменное имя, полученное от сервиса, в поле «Domain Name».
- d. Введите имя пользователя от учетной записи на сервисе в поля «User Name» и «Password» соответственно.
- e. Нажмите «Save» («Сохранить») для применения настроек.

Рисунок 7.3 - Настройки DDNS с типом «NO-IP»

Примечание: для сохранения настроек требуется перезагрузка.

7.1.3. Настройка PPPoE (PPPoE Settings)

1. Зайдите в интерфейс настройки PPPoE: Configuration («Настройки») – Network («Сеть») – Basic Settings («Базовые настройки») – PPPoE.

Рисунок 7.4 – Настройки PPPoE

2. Установите галочку на «Enable PPPoE» («PPPoE») для включения данной функции.
3. Введите имя пользователя, пароль и подтверждение пароля для доступа через PPPoE в поля «Пользователь» («User Name»), «Пароль» («Password») и «Подтв. пароль» («Confirm») соответственно.

Примечания:

- Имя пользователя и пароль должны быть выданы вашим провайдером.
- Настоятельно рекомендуется установить сложный пароль, состоящий из более чем 8 символов, отвечающий как минимум трем из следующих критериев: содержит заглавные буквы, содержит строчные буквы, содержит цифры, содержит специальные символы. Также рекомендуется регулярно изменять пароль.
- Менеджмент учетных записей и паролей целиком и полностью является зоной ответственности инсталлятора или конечного пользователя.

4. Нажмите «Save» («Сохранить») для применения настроек.

Примечание: для сохранения настроек требуется перезагрузка.

7.1.4. Настройки портов (Port Settings)

В этом разделе настроек имеется возможность изменять номера портов для различных служб камеры, таких как HTTP, RTSP, HTTPS.

1. Зайдите в интерфейс настройки портов: Configuration («Настройки») – Network («Сеть») – Basic Settings («Базовые настройки») – Port («Порт»).
2. Выставьте номера портов HTTP, RTSP, HTTPS и номер порта для нативного протокола камеры («Server Port»).
 - a. **HTTP Port:** по умолчанию номер 80.
 - b. **RTSP Port:** по умолчанию номер 554.
 - c. **HTTPS Port:** по умолчанию порт 443.
 - d. **Server Port:** по умолчанию 8000.

Примечание: все номера могут быть при необходимости изменены на любые другие не занятые значения от 1 до 65535 (не рекомендуется задействовать номера до 1000).

3. Нажмите «Save» («Сохранить») для применения настроек.

Примечание: для сохранения настроек требуется перезагрузка.

7.1.5. Настройка NAT / UPnP (NAT Settings)

Данный раздел настроек позволяет выставить параметры протокола UPnP. UPnP (Universal Plug and Play) – сетевая архитектура, обеспечивающая совместимость различного сетевого оборудования, программного обеспечения и других устройств. Данный протокол позволяет избежать необходимости проброса портов для доступа к камере из внешней сети (из-за сетевого шлюза).

1. Зайдите в интерфейс настройки NAT: Configuration («Настройки») – Network («Сеть») – Basic Settings («Базовые настройки») – NAT.

Включить UPnP™
 Псевдоним:

Способ проброса порт... Авто

Тип порта	Внешний порт	Внешний IP-адрес	Внутренний порт	Статус
HTTP	80	0.0.0.0	80	не действительный
RTSP	554	0.0.0.0	554	не действительный
Порт сервера	8000	0.0.0.0	8000	не действительный

Рисунок 7.5 – Настройки NAT

2. Установите галочку на «Enable UPnP» («Включить UPnP») для включения данной функции.
3. Выберите произвольное имя камеры («Псевдоним» / «Nickname») или используйте стандартное.

4. Выберите способ проброса портов («Port Mapping Mode»). Доступны для выбора способы вручную («Manual») и авто («Auto»). В ручном режиме имеется возможность менять номера внешних портов в правилах проброса.
5. Нажмите «Save» («Сохранить») для применения настроек.

7.2. Дополнительные настройки (Advanced Settings)

В данном разделе имеется возможность настроить такие службы, как SNMP, FTP, E-Mail, HTTPS, QoS, 802.1x и другие.

7.2.1. Настройка SNMP (SNMP Settings)

Служба SNMP может быть использована для получения информации о камере, ее параметрах и о тревогах, а также для удаленного управления камерой.

Прежде, чем начать:

Перед использованием функционала SNMP на камере необходимо скачать и установить какое-либо программное обеспечение, позволяющее принимать данные с SNMP-порта камеры.

The screenshot displays the SNMP configuration page, organized into three main sections:

- SNMP v1/v2:** Includes checkboxes for 'Активация SNMP v1' and 'Активация SNMP v2c'. Below are input fields for 'Читатель SNMP общ.' (public), 'Писатель SNMP общ.' (private), 'Trap Address', 'Trap Port' (162), and 'Trap сообщество' (public).
- SNMP v3:** Contains two identical sets of configuration options. Each set includes a checkbox for 'Активация SNMPv3', a 'Чтен имен польз' field, a 'Уровень безопасности' dropdown (set to 'no auth, no priv'), radio buttons for 'Алгоритм авторизации' (MD5 selected), a 'Пароль авторизации' field, radio buttons for 'Алгоритм частного ключа' (DES selected), and a 'Пароль частного ключа' field.
- Другие параметры SNMP:** Features a 'Порт SNMP' field set to 161.

A green 'Сохранить' button is located at the bottom of the form.

Рисунок 7.6 – Настройки SNMP

Примечания:

- Версия SNMP в камере должна быть выставлена такой же, как на программном обеспечении, получающем данные от камеры. Рекомендуется использовать версию SNMP в соответствии с требованиями безопасности объекта. Версия SNMP v1 не обеспечивает никакой защиты данных. Версия SNMP v2 обеспечивает защиту паролем. Версия SNMP v3 обеспечивает шифрование данных (требуется HTTPS).
- Настоятельно рекомендуется установить сложный пароль, состоящий из более чем 8 символов, отвечающий как минимум трем из следующих критериев: содержит заглавные буквы, содержит строчные буквы, содержит цифры, содержит специальные символы. Также рекомендуется регулярно изменять пароль.
- Менеджмент учетных записей и паролей целиком и полностью является зоной ответственности инсталлятора или конечного пользователя.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки SNMP: Configuration («Настройки») – Network («Сеть») – Advanced Settings («Дополнительные настройки») – SNMP.
2. Установите галочку на «Активация SNMP v1» («Enable SNMP v1»), «Активация SNMP v2» («Enable SNMP v2») или «Активация SNMP v3» («Enable SNMP v3») для включения SNMP нужной версии.
3. Выставьте требуемые настройки SNMP.

Примечание: Настройки в программном обеспечении SNMP должны быть идентичными выставленным здесь.

4. Нажмите «Save» («Сохранить») для применения настроек.

Примечания:

- Для сохранения настроек требуется перезагрузка.
- Чтобы избежать риска кражи данных рекомендуется использовать SNMP v3 вместо SNMP v1 и SNMP v2.

7.2.2. Настройка FTP (FTP Settings)

В данном разделе может быть настроены данные для подключения к FTP-серверу для загрузки на него захваченных скриншотов. Скриншоты могут быть захвачены по различным событиям либо по расписанию.

1. Зайдите в интерфейс настройки FTP: Configuration («Настройки») – Network («Сеть») – Advanced Settings («Дополнительные настройки») – FTP.

Рисунок 7.7 – Настройки FTP

- Введите адрес и порт сервера FTP в поля «Адрес сервера» («Server Address») и «Порт» («Port») соответственно.
- Выставьте остальные настройки: для авторизации на FTP-сервере требуются имя пользователя («User Name») и пароль («Password»).

Примечания:

- Настоятельно рекомендуется установить сложный пароль, состоящий из более чем 8 символов, отвечающий как минимум трем из следующих критериев: содержит заглавные буквы, содержит строчные буквы, содержит цифры, содержит специальные символы. Также рекомендуется регулярно изменять пароль.
 - Менеджмент учетных записей и паролей целиком и полностью является зоной ответственности инсталлятора или конечного пользователя.
- Задайте папку, куда будут сохраняться скриншоты («Структура каталога» / «Directory Structure») и интервал сохранения скриншотов в одну и ту же папку («Интервал отправки изображений» / «Filing Interval»).
- Структура каталога / Directory Structure:** в этом поле можно выбрать опции «Root Directory», «Parent Directory» и «Child Directory». При выборе опции «Parent Directory» имеется возможность использовать имя устройства («Device Name»), номер устройства («Device Number») или IP-адрес устройства («Device IP») в качестве имени папки. При выборе опции «Child Directory» имеется возможность использовать имя камеры («Camera Name») или номер камеры («Camera No.») в качестве имени папки.
 - Интервал отправки изображений / Picture Filing Interval:** для удобства организации скриншотов имеется возможность задать период от 1 до 30 дней, в течение которых все скриншоты будут сохраняться в одну и ту же папку. Спустя это время будет создана новая папка с другим названием, содержащим время ее создания, куда будут сохраняться новые скриншоты и т.д.
 - Название изображения / Picture Name:** В этом параметре задаются правила формирования имени файла скриншота. Имеется возможность использовать стандартное имя или сформировать свое правило из доступных префиксов.
- Установите галочку на пункте «Загрузка изображения» («Upload Picture») для включения данной функции – загрузки скриншотов на FTP-сервер.

Примечание: Для анонимного доступа к FTP-серверу следует установить галочку на пункте «Anonymous» напротив поля ввода пароля. Данная функция должна при этом поддерживаться на самом сервере.

6. Нажмите «Save» («Сохранить») для применения настроек.

7.2.3. Настройка Email (Email Settings)

Устройство может быть настроено на отправку сообщений по Email о различных тревожных событиях, таких как детекция движения, потеря видео и т.п.

Прежде, чем начать:

Пожалуйста, задайте корректный адрес DNS-сервера в настройках TCP/IP, прежде чем приступать к настройке службы Email.

1. Зайдите в интерфейс настройки TCP/IP: Configuration («Настройки») – Network («Сеть») – Basic Settings («Базовые настройки») – TCP/IP. Задайте корректные настройки для камеры (подробнее в разделе 7.1.1).
2. Зайдите в интерфейс настройки Email: Configuration («Настройки») – Network («Сеть») – Advanced Settings («Дополнительные настройки») – Email.

The screenshot shows the 'Email' configuration page. At the top, there are tabs for 'SNMP', 'FTP', 'Email' (active), 'Платформы доступа', 'HTTPS', 'QoS', '802.1x', and 'Протокол интеграции'. The main content area includes the following fields:

- Имя отпр.: test (with a green checkmark)
- От Email адреса: test@gmail.com (with a green checkmark)
- SMTP Сервер: [empty field]
- Порт SMTP: 25
- Шифрование почты: Нет (dropdown menu)
- Вложенное изображение
- Интервал: 2 (dropdown menu) с
- Авторизация
- Пользователь: [empty field]
- Пароль: [empty field]
- Подтв. пароль: [empty field]

Below the fields is a section titled 'Имя получ.' containing a table:

№	Имя получ.	Для адреса Email	Тест
1			Тест
2			
3			

At the bottom of the page is a green button labeled 'Сохранить'.

Рисунок 7.8 – Настройки Email

3. Настройте следующие параметры:
 - **Имя отправителя / Sender:** имя ящика-отправителя.
 - **От Email адреса / Senders Address:** Email адрес отправителя.
 - **SMTP Сервер / SMTP Server:** IP-адрес или доменное имя сервера SMTP.
 - **Порт SMTP / SMTP Port:** порт SMTP, по умолчанию 25 (без шифрования). Для SMTP с SSL – по умолчанию 465.

- **Шифрование почты / Email Encryption:** доступны на выбор без шифрования, SSL и TLS.
Примечание: убедитесь, что выбранный метод шифрования поддерживается SMTP-сервером.
- **Вложенное изображение / Attached Image:** установите галочку, чтобы при тревожных событиях вместе с текстовым сообщением был отправлен скриншот.
- **Интервал / Interval:** минимальный интервал в секундах между двумя отправками сообщений с вложениями.
- **Авторизация / Authentication:** (*Опционально*) если сервер требует авторизации для отправки писем, то нужно установить галочку напротив данного пункта и ввести логин и пароль (с подтверждением) для входа в учетную запись почты ниже.

Примечания:

- Настоятельно рекомендуется установить сложный пароль, состоящий из более чем 8 символов, отвечающий как минимум трем из следующих критериев: содержит заглавные буквы, содержит строчные буквы, содержит цифры, содержит специальные символы. Также рекомендуется регулярно изменять пароль.
 - Менеджмент учетных записей и паролей целиком и полностью является зоной ответственности инсталлятора или конечного пользователя.
 - Таблица **Имя получателя / Reciever:** таблица содержит список адресатов (получателей писем). Возможно ввести до трех адресов-получателей.
 - **Receiver:** имя получателя.
 - **Receivers Address:** адрес получателя.
4. Нажмите «Save» («Сохранить») для применения настроек.

7.2.4. Доступ через облачную платформу (Platform Access)

Данный раздел настроек позволяет осуществлять управление устройствами через облачную платформу.

1. Зайдите в интерфейс настройки облачной платформы: Configuration («Настройки») – Network («Сеть») – Advanced Settings («Дополнительные настройки») – Platform Access («Платформы доступа»).
2. Установите галочку на «Enable» («Вкл.») для включения данной функции.
3. Выберите «Режим» («Platform Access Mode»).
4. Можно использовать как IP-адрес сервера по умолчанию, так и ввести другие IP-адреса.
5. Нажмите «Save» («Сохранить») для применения настроек.

7.2.5. Мобильная связь (Wireless Dial)

В данном разделе настраивается подключение к мобильным сетям 3G/4G.

Примечание: данная функция может не поддерживаться некоторыми моделями камер.

1. Зайдите в интерфейс настройки мобильной связи: Configuration («Настройки») – Network («Сеть») – Advanced Settings («Дополнительные настройки») – Wireless Dial («Мобильная связь»).
2. Установите галочку на «Enable» («Вкл.») для включения данной функции.
3. Настройте параметры мобильной связи.
 - a. Выберите режим подключения («Dial Mode») из выпадающего списка. На выбор имеются варианты «Auto» («Авто») и «Manual» («Вручную»). «Авто» – настройка

- расписания для подключения к сети; «Вручную» – выставляется время нахождения в режиме offline (без подключения) и параметры подключения.
- b. Введите номер дозвона, имя пользователя, пароль, APN (имя точки доступа) и значение MTU в соответствующие поля. Имеется возможность оставить данные поля пустыми, в этом случае устройство осуществит попытку подключения с параметрами по умолчанию.
 - c. Выберите режим сети («Network Mode») из выпадающего списка. На выбор доступны 3G и 4G. Если выбран пункт «Auto», то режим сети будет выбран автоматически с приоритетом на 4G.
 - d. Введите время в режиме offline («Offline Time»), если был выбран режим подключения «Manual» («Вручную»).
 - e. Введите номер телефона в поле «UIM Number».
 - f. Нажмите на кнопку «Edit» («Редактировать») для изменения расписания подключений, если был выбран режим подключения «Auto» («Авто»).
 - g. Нажмите «Save» («Сохранить») для применения настроек.
4. Проверка статуса подключения:
- a. Нажмите на «Refresh» («Обновить») для просмотра статуса подключения, статуса UIM, уровня сигнала и т.п.
 - b. Если выбран режим подключения «Manual» («Вручную»), имеется возможность вручную подключаться и отключаться от мобильной сети.
5. Настройка белого списка: номер телефона, указанный в белом списке, может получать тревожные сообщения от устройства и отправлять его в перезагрузку по SMS-сообщению.
- a. Установите галочку напротив «Enable SMS Alarm» для включения данной функции.
 - b. Выберите строку в белом списке и нажмите на «Edit» («Редактировать»).
 - c. Введите номер сотового телефона для белого списка, поставьте галочку на «Reboot via SMS» («Перезагружать по SMS»), выберите типы тревог для отправки SMS и нажмите ОК.

Примечание: для перезагрузки устройства отправьте на номер телефона, привязанный к сим-карте в устройстве, сообщение «reboot». Устройство должно будет ответить сообщением «reboot success».

- d. (Опционально) При нажатии на кнопку «Send Test SMS» («Послать тестовое SMS») будет отправлено специальное SMS-сообщение для проверки связи.
- e. Нажмите «Save» («Сохранить») для применения настроек.

7.2.6. Настройка HTTPS (HTTPS Settings)

Протокол HTTPS обеспечивает аутентификацию на веб-сайтах и соответствующих веб-серверах, которая обеспечивает защиту против т.н. «атак посредника». Следуйте инструкциям ниже для настройки данной службы.

Примечание: для подключения через веб-браузер по HTTPS требуется добавить номер порта после адреса, например, по умолчанию: <https://192.168.1.64:443>

1. Зайдите в интерфейс настройки HTTPS: Configuration («Настройки») – Network («Сеть») – Advanced Settings («Дополнительные настройки») – HTTPS.
2. Установите галочку на «Enable» («Вкл.») для включения данной функции.

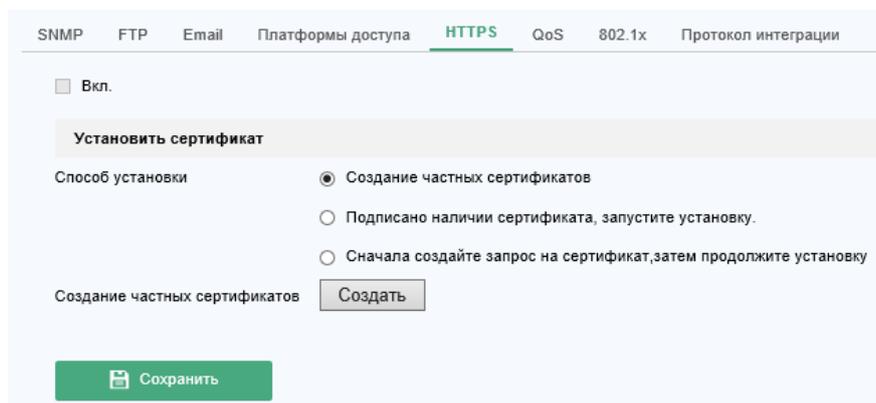


Рисунок 7.9 – Настройки HTTPS

3. Создайте частный (Self-signed) или авторизованный (Authorized) сертификат.
 - o Создание частного сертификата:
 - a. Выберите «Create Self-signed Certificate» («Создание частных сертификатов») в качестве способа установки («Installation Method»).
 - b. Нажмите на «Create» («Создать») для входа в интерфейс создания.

Рисунок 7.10 – Создание самоподписанного сертификата

- c. Введите название страны, доменное имя или IP-адрес и другую информацию в соответствующие поля.
 - d. Нажмите ОК для сохранения настроек.

Примечание: если сертификат уже создавался, данная опция будет недоступна.

- o Создание авторизованного сертификата:
 - a. Выберите «Сначала создайте запрос на сертификат, затем продолжите установку» («Create the certificate request first and continue the installation») в качестве метода установки («Installation Method»).
 - b. Нажмите на «Create» («Создать») для входа в интерфейс создания.
 - c. Скачайте созданный запрос и предоставьте его сертифицирующей службе для подписи.
 - d. После получения подписанного сертификата импортируйте его на устройство.
4. После успешного создания сертификата будет выведена сертификационная информация.

5. Нажмите «Save» («Сохранить») для применения настроек.

7.2.7. Настройка QoS (QoS Settings)

Служба QoS (Quality of Service, качество обслуживания) позволяет решить проблему задержек и перегруженности сети за счет приоритизации сетевого трафика.

1. Зайдите в интерфейс настройки QoS: Configuration («Настройки») – Network («Сеть») – Advanced Settings («Дополнительные настройки») – QoS.

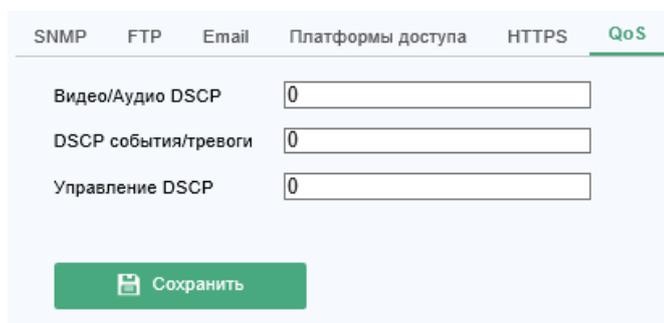


Рисунок 7.11 – Настройки QoS

2. Выставьте настройки QoS: «Видео/Аудио DSCP» («Video/Audio DSCP»), «DSCP события/тревоги» («Event/Alarm DSCP») и «Управление DSCP» («Management DSCP»). Диапазон допустимых значений в данных полях – от 0 до 63. Чем выше значение в поле, тем выше приоритет соответствующих данных (видео/аудио, тревоги и управление соответственно).

Примечание: значение DSCP (Differentiated Service Code Point) используется в заголовке IP-пакетов для обозначения приоритета данных.

3. Нажмите «Save» («Сохранить») для применения настроек.

Примечание: для сохранения настроек потребуется перезагрузка устройства.

7.2.8. Настройка 802.1x (802.1x Settings)

Стандарт IEEE 802.1x поддерживается камерами, и при его активации данные, передаваемые камерой, становятся защищены, и для их получения требуется авторизация при работе в сети, использующей IEEE 802.1x

Прежде, чем начать:

Вначале должен быть настроен сервер аутентификации. Пожалуйста, задайте имя пользователя и пароль для 802.1x на сервере.

SNMP FTP Email Платформы доступа HTTPS QoS **802.1x**

Включить IEEE 802.1X

Протокол EAP-MD5

версия EAPOL 1

Пользователь

Пароль

Подтв. пароль

Сохранить

Рисунок 7.12 – Настройки 802.1x

Примечания:

- Настоятельно рекомендуется установить сложный пароль, состоящий из более чем 8 символов, отвечающий как минимум трем из следующих критериев: содержит заглавные буквы, содержит строчные буквы, содержит цифры, содержит специальные символы. Также рекомендуется регулярно изменять пароль.
- Менеджмент учетных записей и паролей целиком и полностью является зоной ответственности инсталлятора или конечного пользователя.

Последовательность настройки:

1. Зайдите в интерфейс настройки 802.1x: Configuration («Настройки») – Network («Сеть») – Advanced Settings («Дополнительные настройки») – 802.1x.
2. Установите галочку на «Enable IEEE 802.1x» («Вкл. IEEE 802.1x») для включения данной функции.
3. Введите настройки 802.1x, включающие протокол («Protocol»), версию EAPOL («EAPOL Version»), имя пользователя («User Name») и пароль («Password»), а также подтверждение пароля («Confirm»).

Примечание: Версии EAPOL должны быть идентичны на устройстве и на маршрутизаторе.

4. Введите имя пользователя и пароль для доступа к серверу.
5. Нажмите «Save» («Сохранить») для применения настроек.

Примечание: для сохранения настроек потребуется перезагрузка устройства.

8. Настройки видео/аудио (Video/Audio Settings)

Следуйте инструкциям из этой части для настройки параметров компрессии видео, аудио, RoI, информации на экране и т.п.

8.1. Настройка видео (Video Settings)

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки видео: Configuration («Настройки») – Video/Audio («Видео и Аудио») – Video («Видео»).

The screenshot shows the 'Video' settings tab in a configuration interface. It contains the following settings:

Параметр	Значение
Тип потока	Осн. поток (норм. реж.)
Тип видео	Поток видео
Разрешение	1920*1080P
Тип скорости данных	Переменный
Качество	Среднее
Частота кадров	25 fps
Максимальный битрейт	4096 Kbps
Кодирование видео	H.264
H.264+	OFF
Профиль	Основной профиль
Интервал I кадра	50
Сглаженный поток	50 [Чёткий<->Сглаженное]

At the bottom of the settings panel is a green button labeled 'Сохранить' (Save).

Рисунок 8.1 – Настройки видео

2. Выберите тип потока камеры для настройки – «Main Stream» («Основной поток»), «Sub-Stream» («Вторичный поток») или «Third Stream» («Третий поток»).

Примечания:

- В некоторых моделях для включения третьего потока требуется зайти в меню камеры System («Система») – Maintenance («Обслуживание») – System Service («Системные службы») – Software («ПО») и установить галочку на пункте «Enable Third Stream» («Включить третий поток»).
 - Основной поток обычно используется для записи и для просмотра в реальном времени при хорошей пропускной способности сети; дополнительный поток может быть использован для просмотра в реальном времени, когда пропускная способность ограничена.
3. Имеется возможность настройки следующих параметров выбранного потока:
 - **Тип потока / Video Type:** выберите вариант передачи только видео или комбинированного потока видео + аудио. Звук будет добавляться в поток только в том случае, если в этом пункте выбрано «Видео и аудио» («Video & Audio»).
 - **Разрешение / Resolution:** выберите разрешение потока.

- **Тип скорости данных / Bitrate Type:** выберите постоянный («Constant») или переменный («Variable») битрейт.
- **Качество / Video Quality:** при выборе переменного типа битрейта имеются на выбор шесть уровней качества видео.
- **Частота кадров / Frame Rate:** задайте число кадров в секунду. Чем выше данное значение, тем более плавным будет изображение.
- **Максимальный битрейт / Max Bitrate:** выберите максимальное значение битрейта в пределах от 32 кбит/с до 16384 кбит/с. Чем выше данное значение, тем выше качество видеопотока, при этом требуется большая пропускная способность сети.
- **Кодирование видео / Video Encoding:** если для настройки выбран основной поток, то доступны для выбора могут быть кодеки H.264 и H.265; если выбран дополнительный или третий поток, то доступны могут быть H.264, MJPEG и H.265. H.265 – это новый кодек, обеспечивающий лучшее сжатие видеопотока в сравнении с H.264 при сохранении качества изображения.

Примечание: список доступных для выбора кодеков может быть различным для разных моделей камер.

- **H.264+ и H.265+:**
 - **H.264+:** при выборе в качестве кодека H.264 становится доступной опция H.264+, включающая улучшенный алгоритм сжатия видео, основанный на H.264. По сравнению с базовым H.264, H.264+ обеспечивает выигрыш до 50% по требуемому дисковому пространству для хранения одинакового времени записи.
 - **H.265+:** при выборе в качестве кодека H.265 становится доступной опция H.265+, включающая улучшенный алгоритм сжатия видео, основанный на H.265. По сравнению с базовым H.265, H.265+ обеспечивает выигрыш до 50% по требуемому дисковому пространству для хранения одинакового времени записи.

При включении или отключении опций H.264+ или H.265+ потребуется перезагрузка камеры. При переходе от H.264+ к H.265+ и наоборот перезагрузка не требуется.

Примечания:

- Обновите ваш видеопроигрыватель до последней версии, если выгруженное видео не воспроизводится.
- Для возможности использования H.264+ или H.265+ тип битрейта должен быть переменным.
- С включенным H.264+ или H.265+ такие параметры, как «Profile» («Профиль»), «I Frame Interval» («Интервал I кадра»), «Video Quality» («Качество») и «SVC» становятся недоступными для изменения.
- При включенном H.264+ или H.265+ битрейт может постоянно подстраиваться под текущую сцену, доходя до предельно допустимого (максимального, выставленного в настройках). Для калибровки под конкретную сцену камере может потребоваться до 3 дней.
- **Макс. средний битрейт / Max. Average Bitrate:** при установке конкретного значения максимального битрейта в данной строке будет отображено оценочное значение максимального среднего битрейта; также имеется возможность задать его вручную от 32 кбит/с до значения максимального битрейта.
- **Профиль / Profile:** профили кодека «Базовый» («Basic»), «Основной» («Main») и «Высокий» («High Profile») доступны для выбора.

- **Интервал I кадра / I Frame Interval:** интервал между опорными кадрами, задается в кадрах от 1 до 400.
 - **SVC:** Scalable Video Coding – расширение стандарта H.264/AVC.
 - **Сглаженный поток / Smoothing:** при высоких значениях видеопоток будет более плавным ценой некоторого снижения качества изображения.
4. Нажмите «Save» («Сохранить») для применения настроек.

Примечание: настройки видео могут отличаться для разных моделей камер.

8.2. Настройка аудио (Audio Settings)

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки аудио: Configuration («Настройки») – Video/Audio («Видео и Аудио») – Audio («Аудио»).

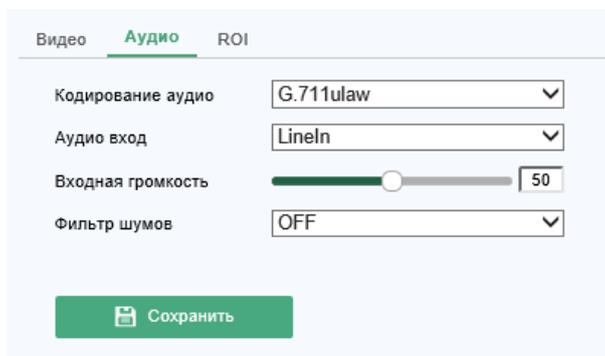


Рисунок 8.2 – Настройки аудио

2. Для настройки доступны следующие параметры:

Примечание: доступные параметры могут отличаться в зависимости от модели камеры.

- **Кодирование аудио / Audio Encoding:** доступны для выбора кодеки G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2 и PCM. При выборе MP2L2 параметры «Частота выборки» («Sampling Rate») и «Битрейт аудио потока» («Audio Stream Bitrate») становятся доступными для изменения. При выборе PCM может быть изменено значение «Частота выборки» («Sampling Rate»).
- **Аудиовход / Audio Input:** доступны для выбора вход микрофона («MicIn») и линейный вход («LineIn»).
- **Входная громкость / Input Volume:** доступны значения громкости от 0 до 100.
- **Фильтр шумов / Environmental Noise Filter:** подавление шума окружения.

3. Нажмите «Save» («Сохранить») для применения настроек.

8.3. Настройка ROI (ROI Settings)

Функция ROI (Region of Interest, зона интереса) позволяет распределить ресурсы для компрессии видеопотока таким образом, что некая выбранная зона (Region of Interest) кодируется с более высоким битрейтом, что повышает качество изображения в этой зоне и улучшает возможности

распознавания объектов. Остальная часть изображения помимо выбранной кодируется с меньшим битрейтом.

Примечание: наличие данной функции зависит от модели камеры.

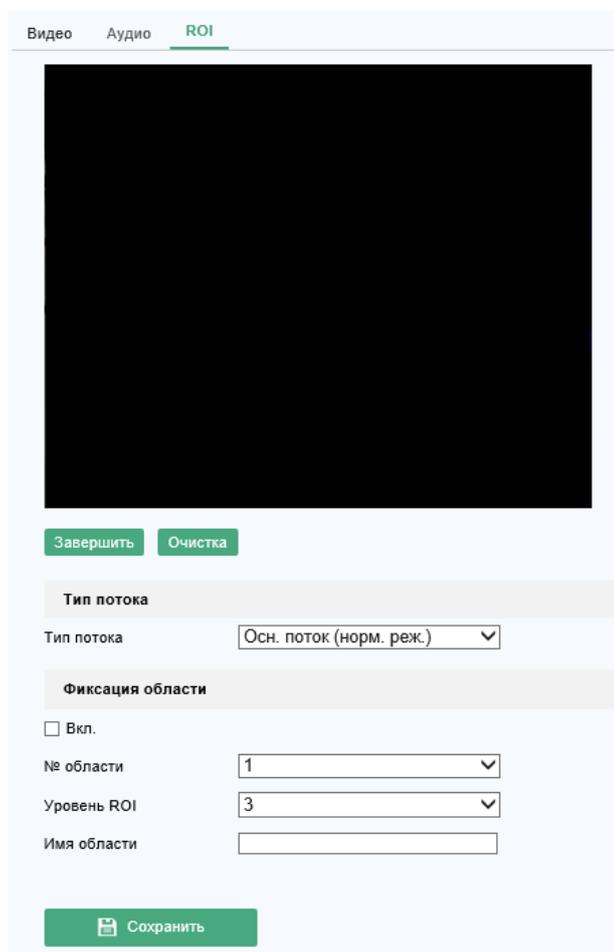


Рисунок 8.3 – Настройки ROI

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки ROI: Configuration («Настройки») – Video/Audio («Видео/Аудио») – ROI.
2. Выберите тип потока для активации в нем ROI.
3. Установите галочку на «Enable» («Вкл.») для активации функции.
4. Задайте область, в которой будет работать функция:
 - a. Выберите номер области («Region No.») из выпадающего списка.
 - b. Установите галочку на «Enable» («Вкл.»).
 - c. Нажмите на «Drawing» («Создание зоны»). Выделите мышью интересующую область, обведя ее красным прямоугольником. Для отмены выбора следует нажать на «Clear» («Очистка»). Нажмите на «Stop Drawing» («Завершить») по окончании.
 - d. Выберите уровень ROI («ROI Level»).
 - e. Введите произвольное имя области («Region Name»).
 - f. Нажмите «Save» («Сохранить») для применения настроек ROI к выбранной области.
 - g. Повторите шаги a – f для настройки других областей.
5. Настройка динамической области («Dynamic Region»):
 - a. Установите галочку на «Face Tracking» («Отслеживание лиц»).

Примечание: для активации отслеживания лиц на камере должна поддерживаться и быть активирована функция детекции лиц.

- b. Выберите уровень ROI («ROI Level»).
6. Нажмите «Save» («Сохранить») для применения настроек.

Примечание: Уровень ROI определяет степень улучшения изображения в выбранной области. Чем выше данное значение, тем выше будет качество изображения.

8.4. Отображение информации (Display Info. on Stream)

Установите галочку для выделения в видеопотоке различных объектов (людей, машин и т.п.). Имеется возможность задания различных правил для сторонних подключенных устройств для детектирования разного рода событий.

8.5. Вырезка области (Target Cropping)

Имеется возможность выбора некоторой области, которая в дальнейшем может передаваться отдельным третьим потоком в определенном разрешении.

Примечание: наличие данной функции зависит от модели камеры.

Последовательность действий для настройки:

1. Войдите в интерфейс вырезки области («Target Cropping»).
2. Установите галочку «Enable Target Cropping» («Вкл. вырезку области») для активации данной функции.
3. Выберите третий поток.
4. Выберите область путем обведения ее красным прямоугольником.
5. Нажмите «Save» («Сохранить») для применения настроек.

9. Настройки изображения (Image Settings)

Следуйте инструкциям из этой части для настройки параметров изображения, таких как OSD, маски приватности, оверлей и др.

9.1. Параметры изображения (Display Settings)

Имеется возможность изменения экспозиции, режима «день/ночь», компенсации засветки, баланса белого, улучшений изображения и других параметров.

Примечание: набор параметров может быть различным для разных моделей камер.

9.1.1. Переключение «День/ночь» (Day/Night Auto-Switch)

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки параметров изображения: Configuration («Настройки») – Image («Изображение») – Display Settings («Настройки дисплея»).

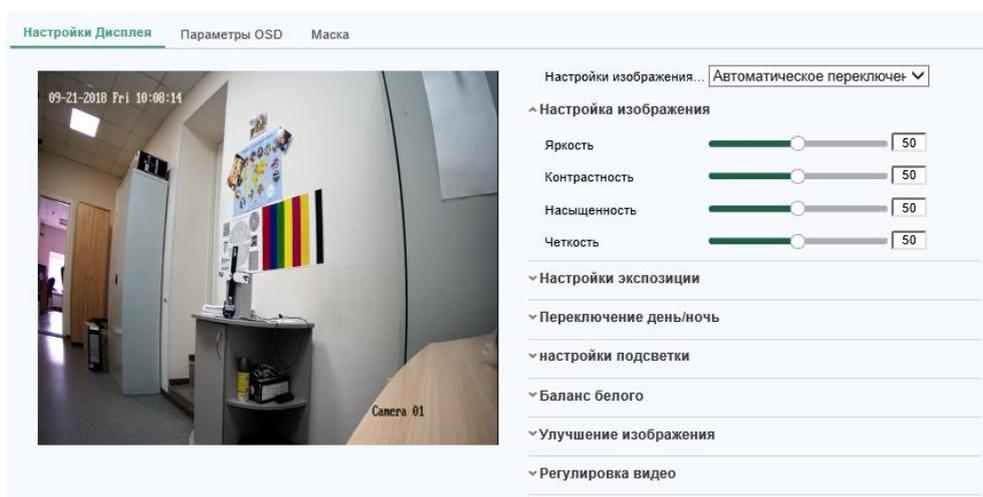


Рисунок 9.1 – Параметры изображения

2. Для настройки доступны следующие параметры изображения:

Примечание: для обеспечения качества изображения в разных условиях освещения имеются два набора параметров, доступные для сохранения.

- **Настройка изображения / Image Adjustment:**
 - **Яркость / Brightness:** регулировка яркости в пределах от 1 до 100.
 - **Контрастность / Contrast:** регулировка контраста в пределах от 1 до 100.
 - **Насыщенность / Saturation:** регулировка цветовой насыщенности в пределах от 1 до 100.
 - **Четкость / Sharpness:** регулировка резкости изображения в пределах от 1 до 100.
- **Настройки экспозиции / Exposure Settings:** если на камере установлен фиксированный объектив без АРД, в качестве «Iris Mode» («Режим экспозиции») можно выставить только «Manual» («Вручную»), то есть настраивать работу диафрагмы нельзя. Если регулировка диафрагмы доступна («Auto»), то имеется возможность выставить ее значение в пределах от 0 до 100. Параметр «Exposure Time» («Время экспозиции») определяет время

электронного затвора, которое варьируется от 1 до 1/100000 секунды. Чем больше данное значение (1 – максимальное), тем светлее и ярче будет изображение, при этом также увеличится и уровень шумов.

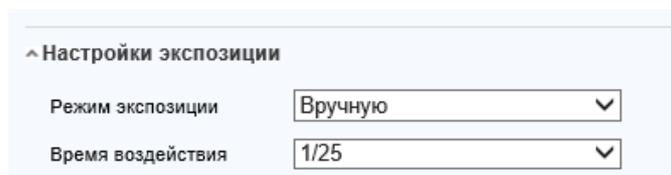


Рисунок 9.2 – Настройки экспозиции

- **Переключение день/ночь / Day/Night Switch.**

Выберите режим день/ночь в соответствии с требованиями проектируемой системы видеонаблюдения. Доступны варианты «Day» («День»), «Night» («Ночь»), «Auto» («Авто»), «Scheduled-Switch» («Переключение по расписанию») и «Triggered by Alarm Input» («По входной тревоге»).

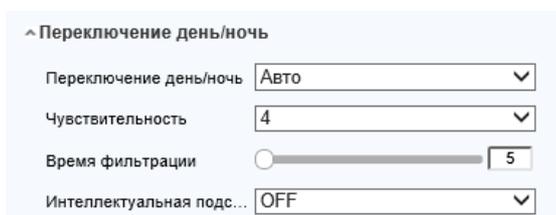


Рисунок 9.3 – Настройки день/ночь

- **День / Day:** камера будет постоянно работать в дневном режиме (цветном).
- **Ночь / Night:** камера будет постоянно работать в ночном режиме (ч/б).
- **Авто / Auto:** камера будет переключаться между режимами в соответствии с текущей освещенностью. Чувствительность («Sensitivity») варьируется от 0 до 7, чем выше значение, тем при менее слабом изменении освещенности происходит переход. Параметр «Filtering Time» («Время фильтрации») определяет минимальный интервал между двумя переключениями, он может быть выставлен в пределах от 5 до 120 секунд.
- **Переключение по расписанию / Scheduled-Switch:** возможность установить расписание для перехода в режим «Ночь» и обратно.
- **По входной тревоге / Triggered by alarm input:** переключение происходит при сработке тревожного входа.
- **Умная подсветка / Smart Supplement Light:** при включении данной функции доступны режимы «Auto» («Авто») и «Manual» («Вручную») для режима работы подсветки.

При выборе «Auto» подсветка будет включаться в соответствии с освещенностью на объекте наблюдения. Если текущая сцена достаточно яркая, подсветка будет отключаться или ее мощность будет снижена, а если сцена недостаточно яркая – мощность подсветки будет увеличена.

При выборе «Manual» имеется возможность настроить подсветку на сработку по приближению или удалению объекта от камеры. Если объект находится рядом с камерой, подсветка мощность подсветки будет снижена, а при удалении объекта подсветка будет работать с максимальной мощностью.

- **Backlight Settings** («Компенсация засветки»):

- **Зона BLC / BLC Area:** если наблюдаемый объект находится перед мощным источником света, данный объект становится слишком затемнен для опознания. Функция BLC компенсирует засветку, чтобы решить данную проблему. Имеется возможность выбрать «Off» («Выкл.»), «Up» («Вверху»), «Down» («Внизу»), «Left» («Слева»), «Right» («Справа»), «Center» («По центру»), «Auto» («Авто») и «Custom» («Настроить») для выбора области изображения, где требуется скомпенсировать засветку.

Примечание: При выборе «Custom» появляется возможность обвести на изображении интересующую зону красным прямоугольником; в этой зоне будет работать функция BLC.

- **WDR:** Wide Dynamic Range, расширенный динамический диапазон – позволяет уравнивать освещенность темных и светлых участков изображения.
- **HLC:** High Light Compensation, компенсация встречной засветки – компенсирует свет от мощных источников света в обзоре камеры.
- **White Balance** («Баланс белого»): функция позволяет выбрать цветовую температуру изображения в зависимости от окружения.

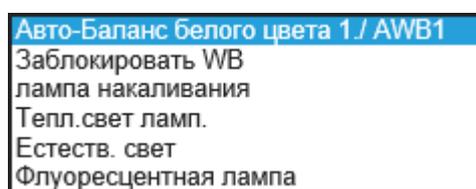


Рисунок 9.4 – Баланс белого

- **Улучшение изображения / Image Enhancement:**
 - **Цифровое шумоподавление / Digital Noise Reduction:** подавляет шумы на изображении. Доступны для выбора варианты «Off» («Выкл.»), «Normal» («Нормальный») и «Expert» («Эксперт»). В режиме «Normal» возможно изменение уровня шумоподавления («DNR Level») в пределах от 0 до 100. В режиме «Expert» возможно изменения как уровня пространственного шумоподавления («Space DNR Level»), так и уровня временного шумоподавления («Time DNR Level») в пределах от 0 до 100.
 - **Антитуман / Defog Mode:** функция позволяет очистить изображение от тумана.
 - **Электронная стабилизация / EIS, Electrical Image Stabilizer:** функция позволяет скомпенсировать дрожание картинки из-за вибрации.
 - **Оттенки серого / Grey Scale:** имеется возможность выбрать диапазон оттенков серого: [0-255] или [16-235].
- **Регулировка видео / Video Adjustment:**
 - **Зеркало / Mirror:** отражает изображение по вертикали или по горизонтали.
 - **Поворот / Rotate:** имеется возможность повернуть изображение на 90° при настройке камеры на наблюдение объекта, растянутого по вертикали, например, коридора. Соотношение сторон в этом случае становится 9:16.
 - **Режим сцены / Scene Mode:** имеется возможность выбрать режим сцены «Indoor» («Внутренний») или «Outdoor» («Наружный»).
 - **Стандарт видео / Video Standard:** имеется возможность выбрать 50 Гц (PAL) или 60 Гц (NTSC).
 - **Режим захвата / Capture Mode:** Создание зоны из поля зрения камеры, которая будет в дальнейшем обрабатываться и передаваться в видеопотоке.
 - **Коррекция искажения / Lens Distortion Correction:** функция позволяет произвести цифровую коррекцию изображения, скомпенсировав искажения, создаваемые объективом.

- **Другое / Others:** в некоторых моделях камер могут поддерживаться выходы CVBS, SDI или HDMI; выберите «On» («Вкл.») или «Off» («Выкл.») для требуемого видеовыхода.

9.1.2. Переключение День/Ночь (Day/Night Scheduled-Switch)

Данный раздел настроек позволяет установить параметры камеры отдельно для дневного и ночного режимов, обеспечивая высокое качество изображения в различных условиях освещения.

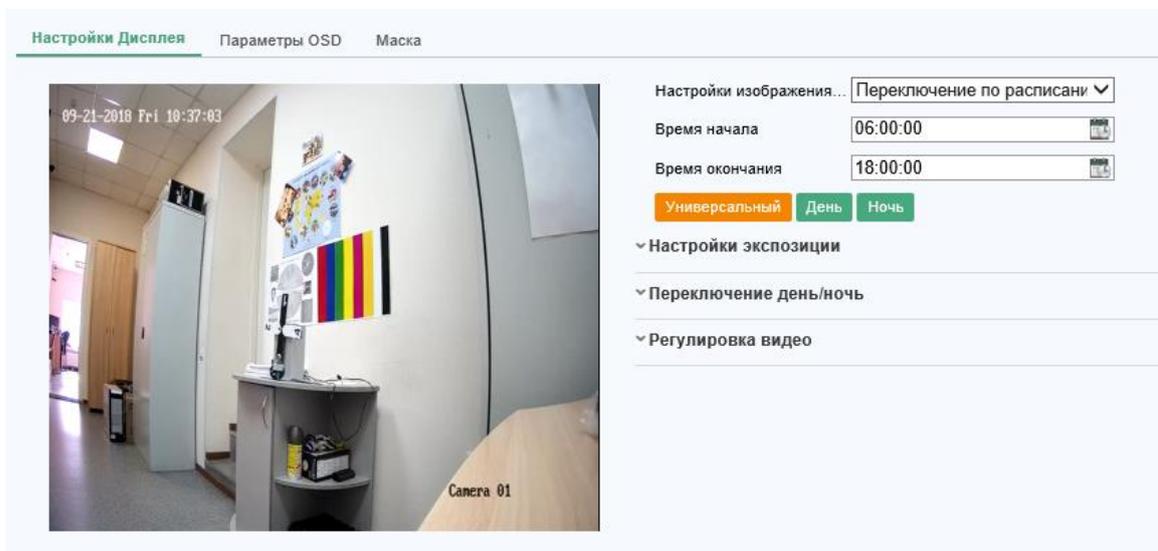


Рисунок 9.5 – Настройка переключения День/Ночь

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки параметров изображения: Configuration («Настройки») – Image («Изображение») – Display Settings («Настройки дисплея»).
2. Нажмите на иконку календаря, чтобы выбрать начальное и конечное время переключения

Примечания:

- Начальное и конечное время относится к дневному режиму (т.е. вход в дневной режим и выход из него).
 - Период времени может включать в себя два идущих подряд дня. Например, при установке начального времени на 10:00 и конечного времени на 1:00, дневной режим будет включен в 10 часов утра первых суток и отключен в час ночи вторых суток.
3. Выберите вкладку «Common» («Общие») для настройки параметров, относящихся к дневному и ночному режимам.

Примечание: настройка данных параметров подробно описана в разделе 9.1.1.

4. Выберите вкладку «Day» («День») для настройки параметров, относящихся к дневному режиму.
5. Выберите вкладку «Night» («Ночь») для настройки параметров, относящихся к ночному режиму.

Примечание: При смене любого параметра настройки будут сохранены автоматически.

9.2. Настройка OSD (OSD Settings)

В данном разделе имеется возможность настроить отображаемое имя камеры, формат времени и даты, режим отображения, размер OSD.

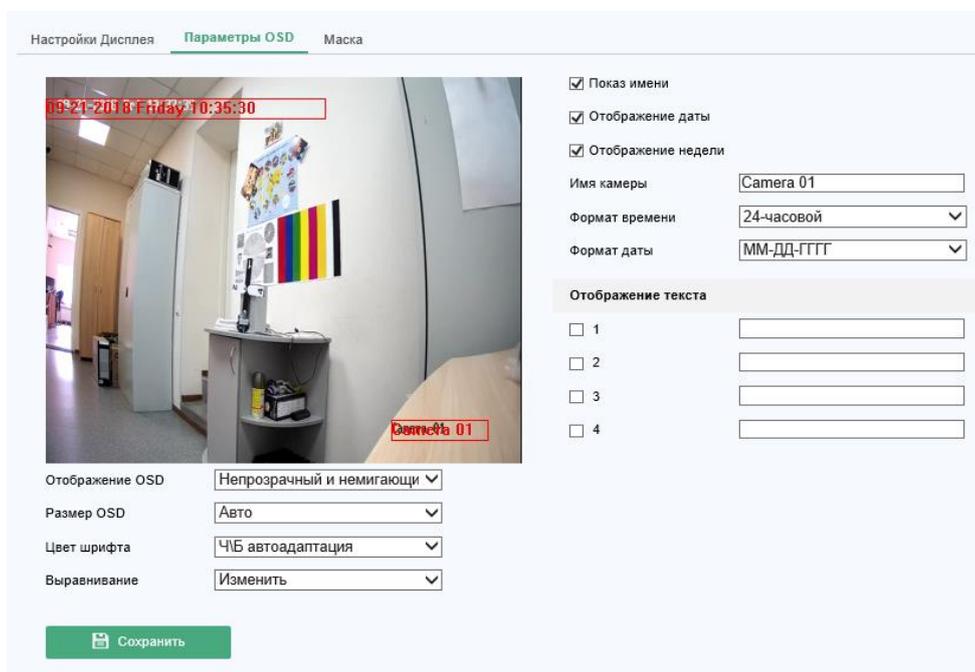


Рисунок 9.6 – Параметры OSD

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки OSD: Configuration («Настройки») – Image («Изображение») – OSD Settings («Параметры OSD»).
2. Выставьте галочки на «Display Name» («Показ имени»), «Display Date» («Отображение даты»), «Display Week» («Отображение недели») для включения отображения соответствующего элемента, если это требуется.
3. Выставьте имя камеры в поле «Camera Name» («Имя камеры»).
4. Выберите формат даты из выпадающего меню «Date Format» («Формат даты / времени»).
5. Выберите режим отображения «Отображение OSD» («Display Mode»), «Размер OSD» («OSD Size») и «Цвет шрифта» («Font Color») в соответствующих выпадающих меню.
6. Настройте текстовый оверлей (вставку текста поверх изображения):
 - a. Установите галочку напротив текстового поля для активации экранного оверлея.
 - b. Введите текст в поле.

Примечание: имеется возможность создания до 8 текстовых оверлеев.

7. Установите требуемый режим выравнивания («Alignment») для элементов OSD. Доступны выравнивания по левому краю («Left»), по правому краю («Right») и настраиваемое выравнивание («Custom»). При выборе «Custom» появляется возможность при помощи мыши переносить текстовые блоки на изображении для подстройки их позиции.

Примечание: доступно только выравнивание текстовых оверлеев.

8. Нажмите «Save» («Сохранить») для применения настроек.

9.3. Настройка маски приватности (Privacy Mask)

Маска приватности позволяет скрыть определенные области изображения для предотвращения отображения в реальном времени и записи каких-либо конкретных сегментов наблюдаемой зоны.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки масок приватности: Configuration («Настройки») – Image («Изображение») – Privacy Mask («Маска»).
2. Установите галочку на «Enable Privacy Mask» («Активирование видео маски») для активации данной функции.
3. Нажмите на «Draw Area» («Создание зоны»).

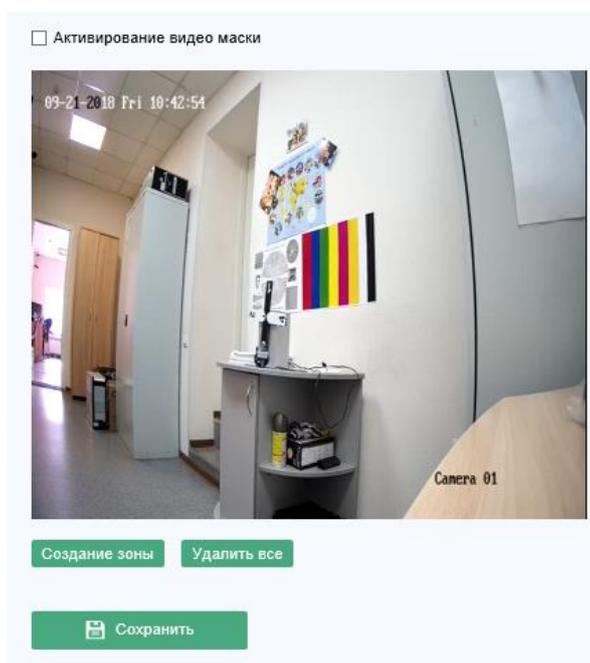


Рисунок 9.7 – Настройки маски приватности

4. При помощи мыши выделите зоны, которые требуется закрыть масками приватности.

Примечание: имеется возможность выбрать до 4 зон.

5. По окончании нажмите на «Stop Drawing» («Завершить») или «Clear All» («Удалить все»).
6. Нажмите «Save» («Сохранить») для применения настроек.

9.4. Настройка наложения изображения («Picture Overlay»)

В данном разделе имеется возможность наложить на видеопоток изображение, например, логотип.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки наложения изображения: Configuration («Настройки») – Image («Изображение») – Picture Overlay («Наложение изображения»).
2. Нажмите на «Browse» («Обзор») для выбора изображения.

3. Нажмите на «Upload» («Загрузить») для загрузки изображения на камеру.
4. Установите галочку на «Enable Picture Overlay» («Включить наложение изображения») для активации данной функции.
5. Введите значения координат X и Y для выравнивания положения изображения на видео. При помощи параметров «Picture Width» («Ширина изображения») и «Picture Height» («Высота изображения») можно настроить размер изображения на видео.
6. Нажмите «Save» («Сохранить») для применения настроек.

Примечание: Формат изображения должен быть BMP (цветность RGB24), максимальный размер изображения – 128 * 128.

10. Настройки событий (Event Settings)

В этой секции руководства приводятся инструкции по настройке поведения камеры при возникновении тревожных событий.

Обратите внимание, что настройки, рассматриваемы в данном разделе, могут отсутствовать на тех или иных моделях камер.

10.1. Базовые события (Basic Events)

Базовые события включают в себя детекцию движения, подделку видео, сработку тревожного входа, ошибки и т.п. Данные события могут запустить различные привязанные к ним действия, например, оповещение наблюдательного центра, отправку сообщения по электронной почте, сработку тревожного выхода и т.п.

10.1.1. Настройка детекции движения (Motion Detection)

Детекция движения позволяет обнаружить движущийся в поле зрения камеры объект, после чего могут быть предприняты различные автоматические действия. Для настройки детекции движения доступны два режима – «Обычный» («Normal Configuration») и «Эксперт» («Expert Configuration»).

I. Normal Configuration («Обычный»):

В данном режиме производится одинаковая настройка параметров детекции движения для дневного и ночного режимов.

Задача 1. Настройка зоны детекции движения.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки детекции движения: Configuration («Настройки») – Event («По событию») – Basic Event («По событию») – Motion Detection («Детектор движения»).
2. Поставьте галочку на «Enable Motion Detection» («Вкл. детекцию движения»).
3. Установите галочку на «Enable Dynamic Analysis for Motion» («Включить метаданные ActiveSearch») для обведения на видео движущихся объектов зелеными прямоугольниками.

Примечание: для обведения прямоугольниками движущихся объектов также должна быть включена функция «Rules» («Правила») в разделе настроек Configuration («Настройки») – Local Configuration («Локальные») – Live View Parameters («Параметры просмотра видеопотока») – Rules («Правила»).

4. Нажмите на «Draw Area» («Создание зоны»). При помощи мыши выберите зону для детекции движения. По окончании нажмите на «Stop Drawing» («Завершить»).
5. (Опционально) Нажмите на «Clear All» («Удалить все») для снятия выбора со всех зон.
6. (Опционально) Выставьте нужную чувствительность детекции движения.

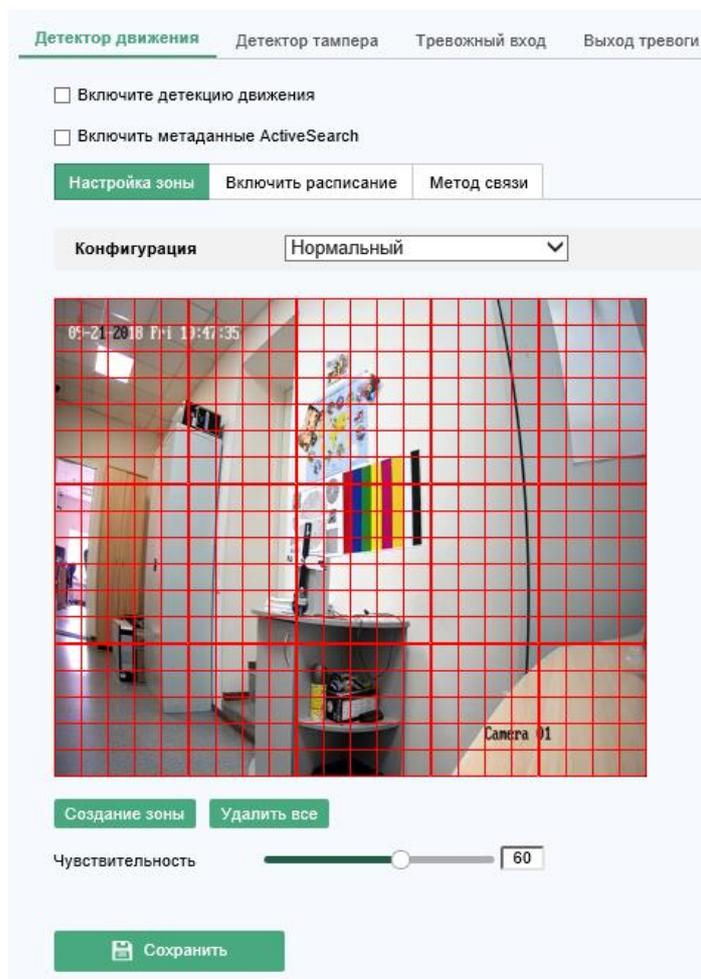


Рисунок 10.1 – Включение детекции движения

Задача 2. Настройка расписания работы детекции движения.

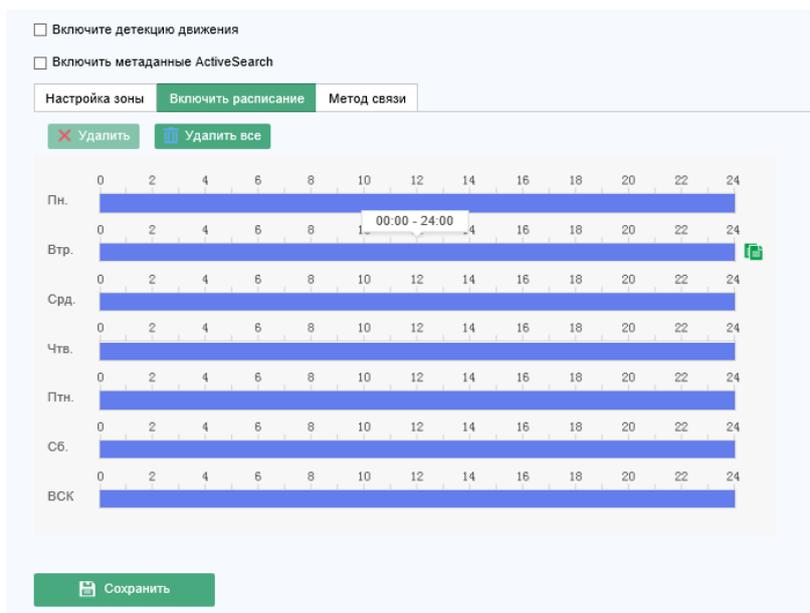


Рисунок 10.2 – Настройка расписания работы детекции движения

Последовательность действий для настройки:

1. Нажмите на «Arming Schedule» («Включить расписание») для редактирования расписания.
2. При помощи мыши выберите нужные периоды времени на днях недели, когда детекция движения должна работать.

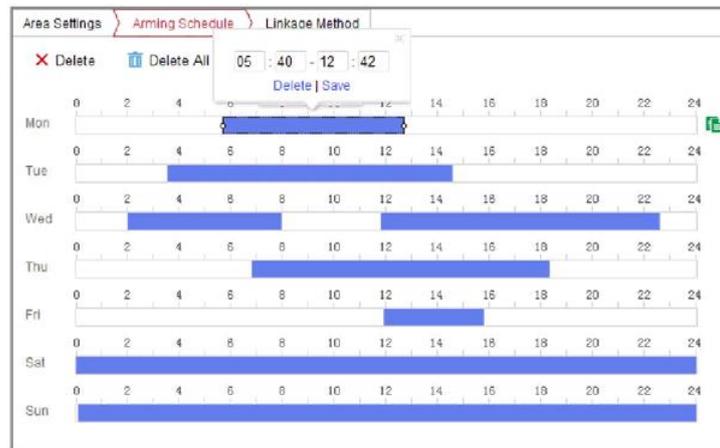


Рисунок 10.3 – Редактирование расписания

Примечание: Нажмите на какой-либо период для отображения полей ввода времени начала и времени окончания данного периода.

3. (Опционально) Нажмите на «Delete» («Удалить») для удаления текущего расписания или «Save» («Сохранить») для его сохранения.
4. При наведении указателя мыши на окончание любого из дней появится иконка копирования, с помощью которой можно скопировать расписание для данного дня на другие дни.
5. Нажмите «Save» («Сохранить») для применения настроек.

Примечание: Периоды не могут накладываться друг на друга. Всего можно создать до 8 периодов работы детекции движения для каждого дня.

Задача 3. Привязка действий к детекции движения («Метод связи»).

Установите галочки для выбора требуемых действий. Доступны следующие действия: «Audible Warning» («Звуковое предупреждение»), «Send Email» («Отправка Email»), «Notify Surveillance Center» («Предупредить центр наблюдения»), «Upload to FTP/Memory Card/NAS» («Загрузить на FTP/Карту памяти/NAS»), «Trigger Channel» («Запись по пусковому событию») и «Trigger Alarm Output» («Срабат. тревож. выхода»).

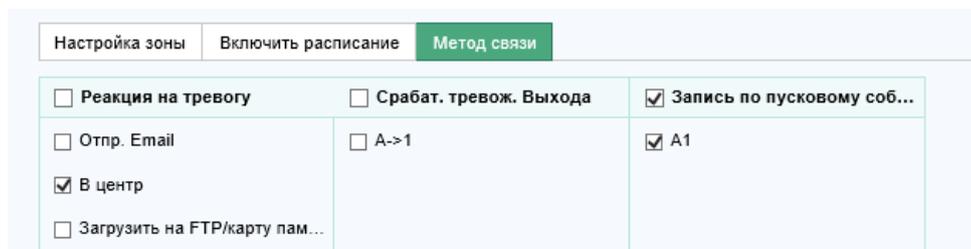


Рисунок 10.4 – Привязка действий

Примечание: доступные действия могут различаться для разных моделей камер.

- **Звуковое оповещение / Audible Warning:** поддерживается устройствами с аудиовыходом.
- **Предупредить центр наблюдения / Notify Surveillance Center:** отправка сигнала о тревоге или об ошибке для ПО удаленного наблюдения.
- **Отправка Email / Send Email:** отправка сообщения о тревоге или об ошибке по Email.

Примечание: информация о настройке отправки сообщений по Email приведена в разделе 7.2.3.

- **Загрузить на FTP/Карту памяти/NAS / Upload to FTP/Memory Card/NAS:** захват скриншота в момент срабатывания тревоги и отправка его на соответствующее хранилище.

Примечания:

- Настройка FTP рассмотрена в разделе 7.2.2.
- Настройка захвата скриншотов осуществляется через раздел настроек Configuration («Настройки») – Storage («Хранение») – Schedule Settings («Параметры расписания») – Capture Parameters («Сохранение»).
- Захваченный скриншот может быть загружен на SD-карту, если она имеется, или на сетевой диск.
- **Запись по пусковому событию / Trigger Channel:** при срабатывании детекции движения начнется запись видео. Для этого нужно настроить соответствующим образом расписание записи. Пожалуйста, обратитесь для этого к секции 11.1 данного руководства.
- **Срабат. тревож. выхода / Trigger Alarm Output:** активировать один или несколько тревожных выходов при срабатывании детекции движения.

Примечание: информация о настройке тревожных выходов приведена в разделе 10.1.4.

II. Expert Configuration («Эксперт»)

Данный режим в основном предназначен для настройки чувствительности и размера отслеживаемых объектов для ночных и дневных условий.

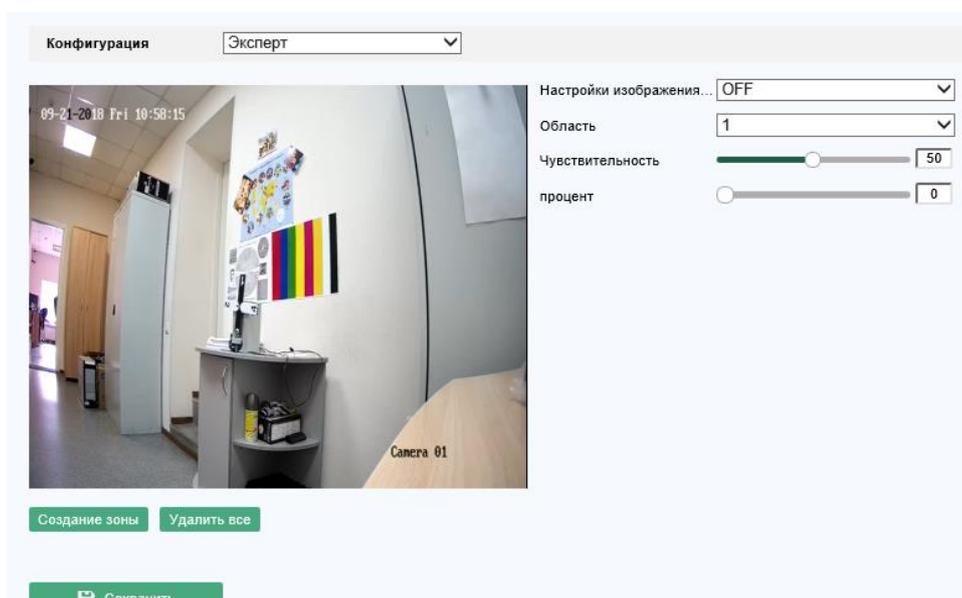


Рисунок 10.5 – Настройка детекции движения в режиме «Эксперт»

- **Переключение день/ночь отключено**

Последовательность действий для настройки:

1. Выделите мышью зону детекции движения, как в обычном режиме настройки. Имеется возможность выбрать до 8 зон.
2. Выберите «Off» («Выкл.») для параметра «Switch Day and Night Settings» («Настройки изображения по расписанию»).
3. Выберите зону из выпадающего меню «Area» («Область»).
4. Выставьте нужные «Чувствительность» («Sensitivity») и размеры объекта относительно кадра «Процент» («Percentage») для выбранной зоны.
5. Настройте расписание и привязку действий как в обычном режиме.
6. Нажмите «Save» («Сохранить») для применения настроек.

- **Переключение день/ночь включено (авто)**

Последовательность действий для настройки:

1. Выделите мышью зону детекции движения, как в обычном режиме настройки. Имеется возможность выбрать до 8 зон.
2. Выберите «Auto-Switch» («Авто переключение») для параметра «Switch Day and Night Settings» («Настройки изображения по расписанию»).
3. Выберите зону из выпадающего меню «Area» («Область»).
4. Выставьте нужные чувствительность («Sensitivity») и размеры объекта относительно кадра («Percentage») для выбранной зоны и дневного времени.
5. Выставьте нужные чувствительность («Sensitivity») и размеры объекта относительно кадра («Percentage») для выбранной зоны и ночного времени.
6. Настройте расписание и привязку действий как в обычном режиме.
7. Нажмите «Save» («Сохранить») для применения настроек.

- **Переключение день/ночь включено (расписание)**

Последовательность действий для настройки:

1. Выделите мышью зону детекции движения, как в обычном режиме настройки. Имеется возможность выбрать до 8 зон.
2. Выберите «Scheduled-Switch» («По расписанию») для параметра «Switch Day and Night Settings» («Настройки изображения по расписанию»).

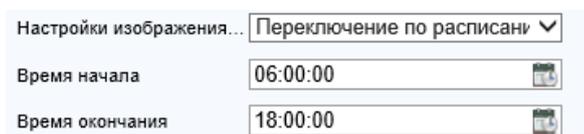


Рисунок 10.6 – Переключение день/ночь по расписанию (детекция движения)

3. Выберите время начала и окончания («Start Time» и «End Time» соответственно) работы дневного режима.
4. Выберите зону из выпадающего меню «Area» («Область»).
5. Выставьте нужные чувствительность («Sensitivity») и размеры объекта относительно кадра («Percentage») для выбранной зоны и дневного времени.
6. Выставьте нужные чувствительность («Sensitivity») и размеры объекта относительно кадра («Percentage») для выбранной зоны и ночного времени.

7. Настройте расписание и привязку действий как в обычном режиме.
8. Нажмите «Save» («Сохранить») для применения настроек.

10.1.2. Настройка тревоги по саботажу (Video Tampering Alarm)

В данном разделе можно настроить действия камеры при закрытии объектива.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки обнаружения саботажа: Configuration («Настройки») – Event («По событию») – Basic Event («По событию») – Video Tampering («Детектор тампера»).

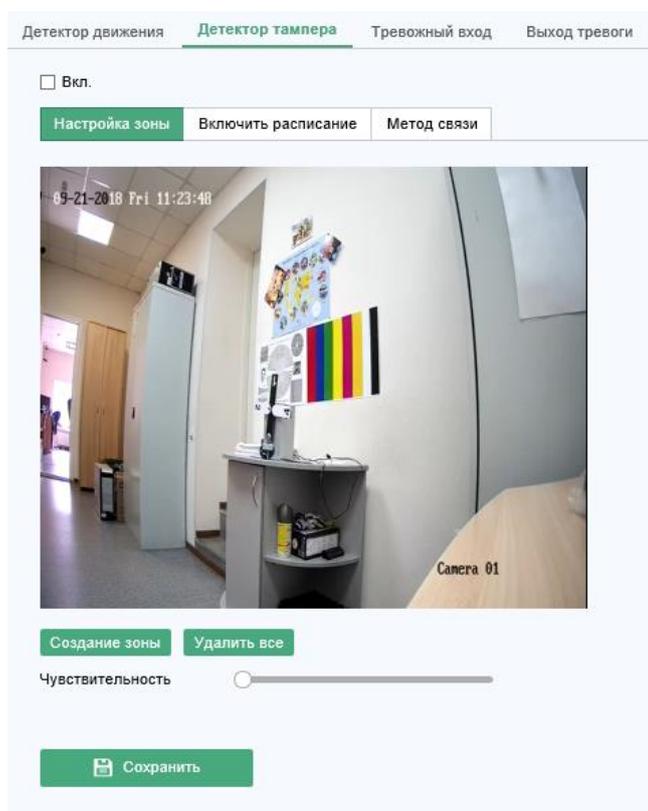


Рисунок 10.7 – Настройки тревоги «Саботаж»

2. Установите галочку «Enable Video Tampering» («Вкл.») для активации данной функции.
3. Выберите зону для обнаружения саботажа. Обратитесь к разделу 10.1.1, задача 1 – для более полной информации по выбору областей.
4. Нажмите на «Edit» («Включить расписание») для настройки расписания работы функции. Настройка осуществляется так же, как в разделе 10.1.1, задача 2.
5. Установите галочки для привязки действий по данной тревоге. Сделать это можно так же, как в разделе 10.1.1, задача 3.
6. Нажмите «Save» («Сохранить») для применения настроек.

10.1.3. Настройка тревожных входов (Alarm Input)

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки тревожных входов: Configuration («Настройки») – Event («По событию») – Basic Event («По событию») – Alarm Input («Тревожный вход»).
2. Выберите номер тревожного входа («Alarm Input No.») и тип тревоги («Alarm Type»): нормально открыт («NO») или нормально замкнут («NC»). *Опционально* – задайте произвольное имя тревожного входа в поле «Alarm Name».

Рисунок 10.8 – Настройки тревожных входов

3. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы тревожного входа. Обратитесь к разделу 10.1.1, задача 2 – для более детальной информации.
4. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях при срабатывании тревожного входа. Обратитесь к разделу 10.1.1, задача 3 – для более детальной информации.
5. Имеется возможность скопировать настройки в другие тревожные входы.
6. Нажмите «Save» («Сохранить») для применения настроек.

10.1.4. Настройка тревожных выходов (Alarm Output)

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки тревожных выходов: Configuration («Настройки») – Event («По событию») – Basic Event («По событию») – Alarm Output («Выход тревоги»).
2. Выберите один из тревожных выходов в выпадающем списке «Alarm Output». *Опционально* – имеется возможность задать произвольное имя тревожного выхода.
3. Параметр «Delay Time» («Задержка») может быть выставлено на значения 5 сек, 10 сек, 30 сек, 1 мин, 2 мин, 5 мин, 10 мин или «Manual» («Вручную»). Время задержки определяет временной промежуток, в течение которого тревожных выход будет активирован при срабатывании тревожного события.
4. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы тревожного входа. Обратитесь к разделу 10.1.1, задача 2 – для более детальной информации.

5. Имеется возможность скопировать настройки в другие тревожные входы.
6. Нажмите «Save» («Сохранить») для применения настроек.

Рисунок 10.9 – Настройки тревожных выходов

10.1.5. Предупреждения (Handling Exception)

Возможные ошибки – заполнение жесткого диска, ошибка жесткого диска, отключение сети, конфликт IP-адресов, несанкционированный доступ к камере. В данном разделе можно настроить автоматические действия при возникновении данных ошибок.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки ошибок: Configuration («Настройки») – Event («По событию») – Basic Event («По событию») – Exception («Предупреждения»).
2. Установите галочки на ошибках, которые нужно отслеживать и выберите соответствующие им действия. Обратитесь к разделу 10.1.1, задача 3 – для более детальной информации.

Рисунок 10.10 – Настройка обработки ошибок

3. Нажмите «Save» («Сохранить») для применения настроек.

10.1.6. Настройка других тревог (Other Alarm)

Примечание: Некоторые модели камер могут поддерживать беспроводные датчики, пассивные инфракрасные датчики и т.п.

- **Беспроводные датчики / Wireless Alarm:** при получении камерой сигнала с беспроводного датчика, такого как магнитный датчик открывания двери, могут быть предприняты настроенные заранее автоматические действия.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки беспроводных датчиков: Configuration («Настройки») – Event («По событию») – Basic Event («События») – Wireless Alarm («Беспроводные датчики»).
 2. Выберите номер беспроводного датчика («Select Wireless»). Имеется возможность добавить до 8 беспроводных датчиков.
 3. Установите галочку на «Enable Wireless Alarm» («Вкл. беспроводной датчик») для активации функции.
 4. Введите произвольное имя датчика в поле «Alarm Name».
 5. Выберите привязку действий по сработке датчика.
 6. Нажмите «Save» («Сохранить») для применения настроек.
 7. Расположите беспроводной датчик за камерой и перейдите в раздел настроек Configuration («Настройки») – System («Система») – System Settings («Настройки системы») – Remote Control («Удаленный контроль»), чтобы запомнить («Study») новый датчик.
- **Пассивные инфракрасные датчики / PIR Alarm:** пассивные инфракрасные датчики срабатывают при пересечении нарушителем его поля зрения. Может быть зафиксирована тепловая энергия, излучаемая любыми теплокровными существами.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки инфракрасных датчиков: Configuration («Настройки») – Event («По событию») – Basic Event («События») – PIR Alarm («Инфракрасные датчики»).
 2. Установите галочку на «Enable» («Вкл.») для активации данной функции.
 3. Введите произвольное имя датчика в поле «Alarm Name».
 4. Выберите привязку действий по сработке датчика.
 5. Нажмите «Edit» («Изменить») для редактирования расписания работы датчика.
 6. Нажмите «Save» («Сохранить») для применения настроек.
 7. Расположите беспроводной датчик за камерой и перейдите в раздел настроек Configuration («Настройки») – System («Система») – System Settings («Настройки системы») – Remote Control («Удаленный контроль»), чтобы запомнить («Study») новый датчик.
- **Тревожная кнопка / Emergency Alarm:** при нажатии на подключенную к камере тревожную кнопку происходит срабатывание тревоги, по которой могут быть произведены автоматические действия.

Примечание: для работы данной функции требуется включить функцию «Удаленный контроль» в разделе настроек Configuration («Настройки») – System («Система») – System Settings («Настройки системы») – Remote Control («Удаленный контроль») и подключить через данное меню кнопку.

1. Зайдите в интерфейс настройки тревожной кнопки: Configuration («Настройки») – Event («По событию») – Basic Event («События») – Emergency Alarm («Тревожная кнопка»).
2. Выберите привязку действий по сработке датчика.
3. Нажмите «Save» («Сохранить») для применения настроек.

10.2. Интеллектуальная аналитика (Smart Events)

Имеется возможность настройки аналитики, включая детекцию звука, детекцию потери фокусировки, детекцию изменения сцены, детекцию вторжения, детекцию пересечения линии. По этим событиям может быть настроен автоматический запуск различных действий.

10.2.1. Настройка детекции звука (Audio Exception Detection)

Данная функция позволяет обнаружить аномальные звуки в зоне наблюдения, такие как резкое увеличение или уменьшение громкости. По этому событию могут быть настроены различные автоматические действия.

Примечание: данная функция имеется не на всех моделях камер.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки детекции звука: Configuration («Настройки») – Event («По событию») – Smart Event («Событие SMART») – Audio Exception Detection («Детекция звука»).
2. Установите галочку на «Audio Loss Exception» для активации детектора потери звука.
3. Установите галочку на «Sudden Increase of Sound Intensity Detection» для активации детектора резкого увеличения громкости звука. Имеется возможность выставить чувствительность («Sensitivity») и пороговое значение («Threshold»).
4. Установите галочку на «Sudden Decrease of Sound Intensity Detection» для активации детектора резкого снижения громкости звука. Имеется возможность выставить чувствительность («Sensitivity») и пороговое значение («Threshold»).

Примечания:

- Чувствительность: от 1 до 100, чем ниже значение, тем большие изменения в звуке должны произойти для срабатывания тревоги.
 - Пороговое значение: от 1 до 100, позволяет отфильтровать звуки окружающей среды; чем громче фоновые звуки, тем выше должно быть значение. Выставьте значение в соответствии с условиями, в которых работает камера.
 - В интерфейсе есть возможность наблюдать текущий уровень звука.
5. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы функций. Обратитесь к разделу 10.1.1, задача 2 – для более детальной информации.
 6. Нажмите на «Linkage Method» («Метод связи») и выберите действия, которые нужно предпринять при срабатывании тревоги. Доступны следующие действия: «Audible Warning» («Звуковое предупреждение»), «Send Email» («Отправка сообщения эл. почты»), «Notify Surveillance Center» («Предупредить центр наблюдения»), «Upload to FTP/Memory Card/NAS» («Загрузить на FTP/Карту памяти/NAS»), «Trigger Channel» («Запись канала») и «Trigger Alarm Output» («Запуск тревожного выхода»).
 7. Нажмите «Save» («Сохранить») для применения настроек.

10.2.2. Настройка детекции потери фокусировки (Defocus Detection)

С помощью данной функции можно детектировать потерю фокуса из-за расстройки объектива. По данному тревожному событию могут быть настроены различные автоматические действия.

Примечание: данная функция имеется не на всех моделях камер.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки детекции потери фокусировки: Configuration («Настройки») – Event («По событию») – Smart Event («Событие SMART») – Defocus Detection («Потеря фокуса»).
2. Установите галочку на «Enable» («Вкл.») для активации данной функции.
3. Перетащите ползунок для настройки чувствительности. Чем выше данное значение, тем более слабая потеря фокуса сможет активировать тревогу.
4. Выберите привязку действий при срабатывании тревоги.
5. Нажмите «Save» («Сохранить») для применения настроек.

10.2.3. Настройка детекции изменения сцены (Scene Change Detection)

Данная функция позволяет обнаружить изменения в сцене, вызванные резким сдвигом или вращением камеры. По данному тревожному событию могут быть настроены различные автоматические действия.

Примечание: данная функция имеется не на всех моделях камер.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки детекции изменения сцены: Configuration («Настройки») – Event («По событию») – Smart Event («Событие SMART») – Scene Change Detection («Изменение сцены»).
2. Установите галочку на «Enable» («Вкл.») для активации данной функции.
3. Перетащите ползунок для настройки чувствительности. Чем выше данное значение, тем более слабое изменение сцены сможет активировать тревогу.
4. Настройте расписание работы функции («Arming Schedule»). Обратитесь к разделу 10.1.1, задача 2 – для более детальной информации.
5. Выберите привязку действий при срабатывании тревоги.
6. Нажмите «Save» («Сохранить») для применения настроек.

10.2.4. Настройка детекции лиц (Face Detection)

Детекция лиц позволяет обнаружить лица в кадре. По данному событию могут быть настроены различные автоматические действия.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки детекции лиц: Configuration («Настройки») – Event («По событию») – Smart Event («Событие SMART») – Face Detection («Детекция лиц»).
2. Установите галочку на «Enable Face Detection» («Вкл. детекцию лиц») для активации данной функции.
3. Установите галочку «Enable Dynamic Analysis» («Вкл. динамический анализ») для отображения зеленых прямоугольников вокруг замеченных лиц.

Примечание: для обведения прямоугольниками движущихся объектов также должна быть включена функция «Rules» («Правила») в разделе настроек Configuration («Настройки») – Local Configuration («Локальные») – Live View Parameters («Параметры просмотра видеопотока») – Rules («Правила»).

4. Установите ползунок на нужное значение чувствительности. Чем выше данное значение, тем выше вероятность обнаружения лица.
5. Настройте расписание работы функции («Arming Schedule»). Обратитесь к разделу 10.1.1, задача 2 – для более детальной информации.
6. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях при срабатывании детекции лиц. Обратитесь к разделу 10.1.1, задача 3 – для более детальной информации.
7. Нажмите «Save» («Сохранить») для применения настроек.

10.2.5. Настройка детекции вторжения (Intrusion Detection)

Детекция вторжения позволяет обнаружить объекты, входящие в заранее очерченную зону на изображении. По данному событию могут быть настроены различные автоматические действия.

Примечание: данная функция имеется не на всех моделях камер.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки детекции вторжения: Configuration («Настройки») – Event («По событию») – Smart Event («Событие SMART») – Intrusion Detection («Обнаружение вторжения»).

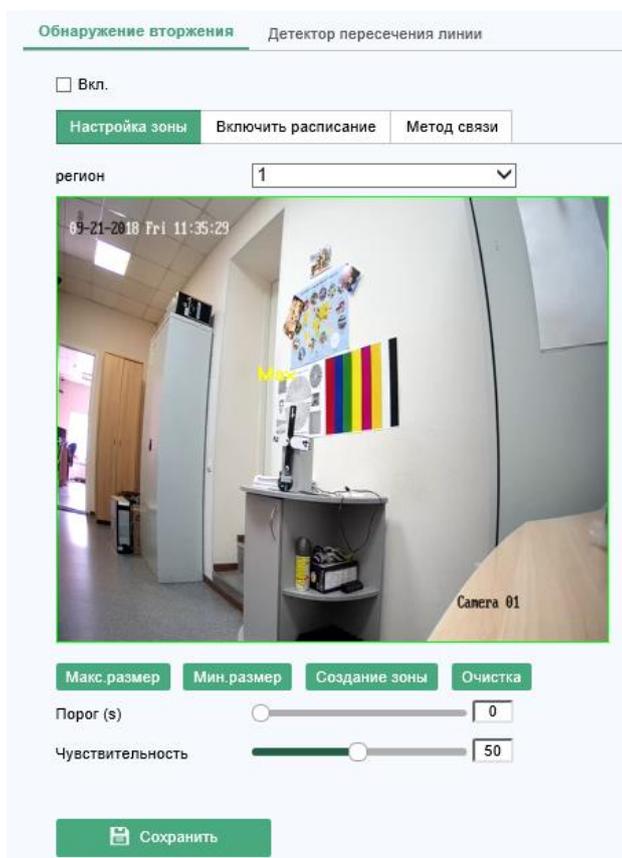


Рисунок 10.11 – Настройка детекции вторжения

2. Установите галочку на «Enable Intrusion Detection» («Вкл.») для активации данной функции.
3. Выберите область из выпадающего меню для изменения ее настроек.

4. Нажмите на вкладку «Area Settings» («Настройки зоны») и затем нажмите на «Draw Area» («Создание зоны») для входа в режим рисования области.
5. С помощью мыши нарисуйте область на изображении и нажмите правой кнопкой мыши для завершения.
6. Выберите порог в секундах («Threshold»), чувствительность («Sensitivity»), размер объекта относительно кадра («Percentage»).
 - **Порог / Threshold:** от 0 до 10 секунд; временной порог, в течение которого должен находиться объект внутри области, для срабатывания тревоги. При установке значения «0» тревога сработает сразу после пересечения объектом любой из границ области.
 - **Чувствительность / Sensitivity:** от 1 до 100; определяет чувствительность детекции, чем выше значение, тем чувствительнее.
 - **Размер / Percentage:** от 1 до 100; определяет отношение размера объекта, который может вызвать срабатывание тревоги, к полному размеру области (в процентах). Например, если выставленное значение равно 50, тревога сработает только в случае появления в области объекта, занявшего как минимум половину ее площади.
7. Повторите приведенные выше шаги для других областей. Всего может быть настроено до 4 областей. Кнопка «Clear» («Очистка») стирает все настроенные области.
8. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы функции.
9. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях при срабатывании детекции вторжения.
10. Нажмите «Save» («Сохранить») для применения настроек.

10.2.6. Настройка детекции пересечения линии (Line Crossing Detection)

Детекция пересечения линии позволяет обнаружить объекты, пересекающие заранее очерченную линию на изображении. По данному событию могут быть настроены различные автоматические действия.

Примечание: данная функция имеется не на всех моделях камер.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки детекции пересечения линии: Configuration («Настройки») – Event («По событию») – Smart Event («Событие SMART») – Line Crossing Detection («Детектор пересечения линии»).
2. Установите галочку на «Enable Line Crossing Detection» («Вкл. детекцию пересечения линии») для активации данной функции.
3. Выберите линию из выпадающего меню.
4. Нажмите на вкладку «Area Settings» («Настройки зоны») и затем нажмите на «Draw Area» («Создание зоны») для входа в режим рисования линии.
5. С помощью мыши нарисуйте линию на изображении и нажмите правой кнопкой мыши для завершения.
6. Выберите направление движения, которое будет детектироваться: можно выбрать из A<->B, A->B, B->A.

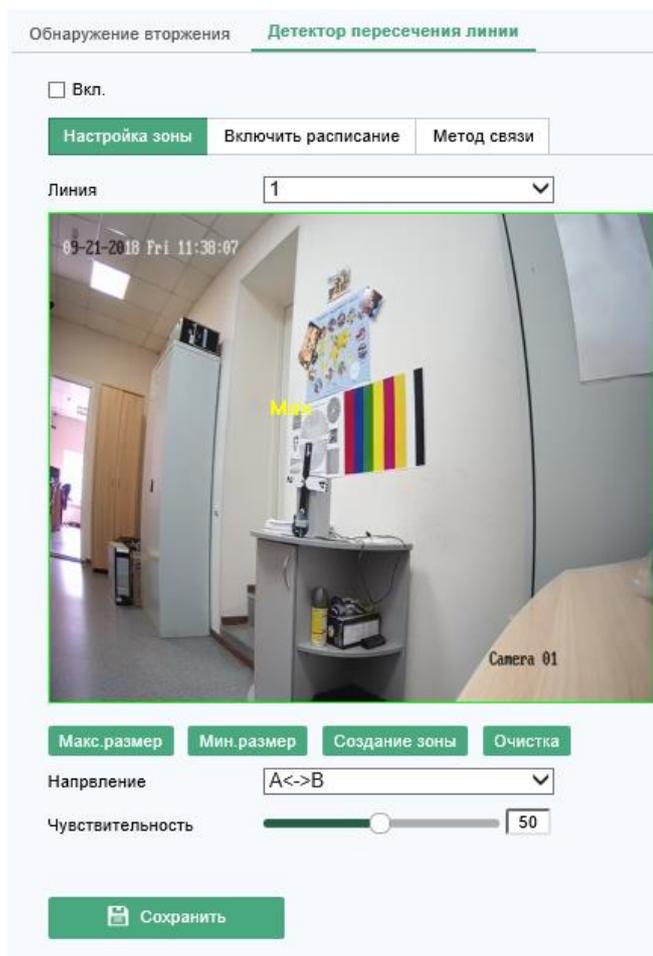


Рисунок 10.12 – Настройка детекции пересечения линии

7. При помощи ползунка «Чувствительность» («Sensitivity») выставьте нужную чувствительность.
8. Повторите приведенные выше шаги для настройки других линий. Всего может быть добавлено до 4 линий. Кнопка «Clear» («Очистка») стирает все настроенные линии.
9. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы функции.
10. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях при срабатывании детекции пересечения линии.
11. Нажмите «Save» («Сохранить») для применения настроек.

10.2.7. Настройка детекции входа в область (Region Entrance Detection)

Детекция входа в область позволяет обнаружить людей, транспортные средства или другие объекты, входящие в заранее созданную область. По данному событию могут быть настроены различные автоматические действия.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки детекции входа в область: Configuration («Настройки») – Event («По событию») – Smart Event («Событие SMART») – Region Entrance Detection («Детекция входа в область»).
2. Установите галочку на «Enable» («Вкл.») для активации данной функции.
3. Выберите область из выпадающего меню «Region» («Область») для ее настройки.

4. Нажмите на вкладку «Area Settings» («Настройки зоны») и затем нажмите на «Draw Area» («Создание зоны») для входа в режим рисования область.
5. С помощью мыши нарисуйте область на изображении и нажмите правой кнопкой мыши для завершения.
6. Установите ползунок «Sensitivity» на нужное значение чувствительности. Чувствительность может быть установлена на значение от 1 до 100, чем выше значение, тем меньший объект сможет вызвать срабатывание тревоги.
7. Повторите приведенные выше шаги для настройки других областей. Всего может быть добавлено до 4 областей. Кнопка «Clear» («Очистка») стирает все настроенные области.
8. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы функции.
9. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях при срабатывании детекции пересечения линии.
10. Нажмите «Save» («Сохранить») для применения настроек.

10.2.8. Настройка детекции выхода из области (Region Exiting Detection)

Детекция выхода из области позволяет обнаружить людей, транспортные средства или другие объекты, выходящие из заранее созданной области. По данному событию могут быть настроены различные автоматические действия.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки детекции выхода из области: Configuration («Настройки») – Event («По событию») – Smart Event («Событие SMART») – Region Exiting Detection («Детекция выхода из области»).
2. Установите галочку на «Enable» («Вкл.») для активации данной функции.
3. Выберите область из выпадающего меню «Region» («Область») для ее настройки.
4. Нажмите на вкладку «Area Settings» («Настройки зоны») и затем нажмите на «Draw Area» («Создание зоны») для входа в режим рисования область.
5. С помощью мыши нарисуйте область на изображении и нажмите правой кнопкой мыши для завершения.
6. Установите ползунок «Sensitivity» на нужное значение чувствительности. Чувствительность может быть установлена на значение от 1 до 100, чем выше значение, тем меньший объект сможет вызвать срабатывание тревоги.
7. Повторите приведенные выше шаги для настройки других областей. Всего может быть добавлено до 4 областей. Кнопка «Clear» («Очистка») стирает все настроенные области.
8. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы функции.
9. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях при срабатывании детекции пересечения линии.
10. Нажмите «Save» («Сохранить») для применения настроек.

10.2.9. Настройка детекции оставленных вещей (Unattended Baggage Detection)

Детекция оставленных вещей позволяет обнаружить предметы, оставленные без присмотра в заранее заданной области. По данному событию могут быть настроены различные автоматические действия.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки детекции оставленных вещей: Configuration («Настройки») – Event («По событию») – Smart Event («Событие SMART») – Unattended Baggage Detection («Детекция оставленных вещей»).
2. Установите галочку на «Enable» («Вкл.») для активации данной функции.
3. Выберите область из выпадающего меню «Region» («Область») для ее настройки.
4. Нажмите на вкладку «Area Settings» («Настройки зоны») и затем нажмите на «Draw Area» («Создание зоны») для входа в режим рисования область.
5. С помощью мыши нарисуйте область на изображении и нажмите правой кнопкой мыши для завершения.
6. Установите ползунок «Sensitivity» на нужное значение чувствительности. Чувствительность может быть установлена на значение от 1 до 100, чем выше значение, тем меньший объект сможет вызвать срабатывание тревоги. Установите ползунок «Threshold» на нужное значение временного порога нахождения в области оставленного предмета. Например, при установке значения 10 секунд тревога сработает спустя 10 секунд после оставления предмета в области.
7. Повторите приведенные выше шаги для настройки других областей. Всего может быть добавлено до 4 областей. Кнопка «Clear» («Очистка») стирает все настроенные области.
8. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы функции.
9. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях при срабатывании детекции пересечения линии.
10. Нажмите «Save» («Сохранить») для применения настроек.

10.2.10. Настройка детекции кражи (Object Removal Detection)

Детекция кражи позволяет обнаружить похищение предметов из заранее заданной области. По данному событию могут быть настроены различные автоматические действия.

Последовательность действий для настройки:

1. Зайдите в интерфейс настройки детекции кражи: Configuration («Настройки») – Event («По событию») – Smart Event («Событие SMART») – Object Removal Detection («Детекция кражи»).
2. Установите галочку на «Enable» («Вкл.») для активации данной функции.
3. Выберите область из выпадающего меню «Region» («Область») для ее настройки.
4. Нажмите на вкладку «Area Settings» («Настройки зоны») и затем нажмите на «Draw Area» («Создание зоны») для входа в режим рисования область.
5. С помощью мыши нарисуйте область на изображении и нажмите правой кнопкой мыши для завершения.
6. Установите ползунок «Sensitivity» на нужное значение чувствительности. Чувствительность может быть установлена на значение от 1 до 100, чем выше значение, тем меньший объект сможет вызвать срабатывание тревоги. Установите ползунок «Threshold» на нужное значение временного порога отсутствия в области оставленного предмета. Например, при установке значения 10 секунд тревога сработает спустя 10 секунд после пропадания предмета из области.
7. Повторите приведенные выше шаги для настройки других областей. Всего может быть добавлено до 4 областей. Кнопка «Clear» («Очистка») стирает все настроенные области.
8. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы функции.
9. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях при срабатывании детекции пересечения линии.
10. Нажмите «Save» («Сохранить») для применения настроек.

10.3. Настройка VCA (VCA Configuration)

10.3.1. Анализ поведения (Behavior Analysis)

Данная функция позволяет обнаружить различного рода подозрительное поведение. По данному событию могут быть настроены различные автоматические действия.

I. Оверлей и захват (Overlay & Capture)

Данный раздел включает в себя настройку отображения OSD на видео и на захваченных скриншотах.

- **Display VCA info on Stream** («Отображать VCA на видеопотоке»): зеленые фигуры, обозначающие обнаруженное подозрительное поведение, будут отображаться на видеопотоке в реальном времени и в записях.
- **Display Target info on Alarm Picture** («Отображать обнаружение на скриншоте»): зеленые фигуры, обозначающие обнаруженное подозрительное поведение, будут отображаться на захваченных скриншотах.
- **Display Rule info on Alarm Picture** («Отображать правила на скриншоте»): зеленые фигуры, обозначающие обнаруженное подозрительное поведение, а также области, в которых осуществляется анализ поведения, будут отображаться на захваченных скриншотах.

Примечание: убедитесь, что функция «Rules» («Правила») включена в локальных настройках: Configuration («Настройки») – Local Configuration («Локальные») – Rules («Правила»).

- **Snapshot Settings** («Настройки скриншотов»):
 - **Upload JPEG Image to Center** («Отправить JPEG на центр наблюдения»): установите галочку для отправки захваченных скриншотов на центр наблюдения, когда происходят срабатывания VCA.
 - **Picture Quality** («Качество изображения»): настройка качества изображения скриншота.
 - **Picture Resolution** («Разрешение изображения»): настройка разрешения скриншота: CIF, 4CIF (D1), 720p, 1080p.
- **Camera Calibration** («Калибровка камеры»): приведенные ниже инструкции помогут осуществить калибровку камеры в трех измерениях для возможности аналитики и вычисления размера объектов. Детекция VCA будет более точной, если камера будет должным образом откалибрована.

Последовательность действий для настройки:

1. Установите галочку «Camera Calibration» («Калибровка камеры») для активации данной функции.
2. Выберите режим калибровки – «Input Basic Data» («Ввести базисные данные») или «Draw on Live View Video» («Нарисовать на видео»):
 - a. **Input Basic Data** («Ввести базисные данные»): введите высоту установки камеры («Mounting Height»), угол обзора («Viewing Angle»), отношение горизонта («Horizon Ratio») вручную.
 - b. **Draw on Live Video** («Нарисовать на видео»): Нажмите на «Draw Verification Line (Horizontal)» («Нарисовать гориз. линию») и «Draw Verification Line (Vertical)»

(«Нарисовать верт. линию») для того чтобы нарисовать на видео горизонтальную и вертикальную линии и ввести их длины. На основании этих данных камера будет рассчитывать размеры всех объектов.

3. Нажмите на «Horizontal Verify» («Проверить горизонталь») / «Vertical Verify» («Проверить вертикаль») для того чтобы нарисовать горизонтальную / вертикальную линию, после чего камера вычислит ее длину. Сравните вычисленное значение с реальной длиной линии для проверки правильности калибровки камеры.

Примечание: калибровка не завершена, если отображение видеопотока останавливается.

4. Нажатие на удаляет нарисованные линии.
5. Нажмите «Save» («Сохранить») для применения настроек.

II. Защищенная область (Shield Region)

Данная функция позволяет задать область, в которой не будет работать анализ поведения. Всего может быть создано до 4 таких областей.

Последовательность действий для настройки:

1. Нажмите на «Shield Region» («Защищенная область») для входа в интерфейс настройки.
2. Нажмите на значок шестиугольника для того чтобы нарисовать область при помощи мыши в окне просмотра. Нажмите правой кнопкой мыши для сохранения области.

Примечания:

- Возможно создать область с количеством сторон до 10.
 - Нажатие на удаляет созданные области.
 - Если просмотр в реальном времени остановлен, возможности нарисовать область не будет.
3. Нажмите «Save» («Сохранить») для применения настроек.

III. Правило (Rule)

Функция анализа поведения позволяет обнаружить различные типы действий, например, пересечение линии, вторжение, вход в область, выход из области и т.п.

Примечание: пожалуйста, обратитесь к соответствующим разделам руководства для получения детальной информации по каждому из типов.

Последовательность действий для настройки:

1. Нажмите на вкладку «Rule» («Правило») для входа в интерфейс настройки.
2. Установите галочку на одно из правил для активации его отслеживания.
3. Выберите тип правила («Rule Type»), тип фильтрации («Filter Type») и затем нарисуйте линию или область на видео для данного правила.
 - a. **Filter Type** («Тип фильтрации»): на выбор имеются «Pixels» («Пиксели») и «Actual Size» («Реальный размер»). Если выбран тип «Pixels», то нужно нарисовать на видео область максимального и минимального размера для каждого правила. Если выбран тип «Actual Size», то нужно ввести максимальные и минимальные длину и ширину. Вызвать срабатывание тревоги сможет только объект, размер которого меньше максимального и больше минимального.

Примечание: убедитесь, что камера предварительно откалибрована для использования типа фильтрации «Actual Size».

- b. **Detection Target** («Цель»): выберите «Human» («Человек») или «Vehicle» («Автомобиль») в качестве цели обнаружения. Также можно выбрать «All» («Все») для обнаружения любых объектов.
- c. **Draw Line / Area** («Нарисовать линию / область»): для обнаружения пересечения линии требуется нарисовать линию и выбрать направление пересечения; для иных действий, таких как вторжение, вход в область, выход из области и т.п. следует нарисовать область.

Примечание: если просмотр в реальном времени остановлен, возможности нарисовать область или линию не будет.

4. Добавьте при помощи кнопки «+» новое правило и выберите его, после чего сконфигурируйте аналогичным образом.
5. Выберите два созданных правила и создайте комбинированное правило («Combine Rule»), введите минимальный и максимальный временной интервал совпадения двух правил.

Примечания:

- При выборе типа одного из правил внутри комбинированного как «None» анализ производится не будет.
 - Может быть создано до 8 одиночных и до 2 комбинированных правил. Для комбинированных правил поддерживаются: пересечение линии, вторжение, вход в область и выход из области.
6. Нажмите «Save» («Сохранить») для применения настроек.
 7. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы функции. Нажмите «Save» («Сохранить») для применения настроек.
 8. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях при срабатывании детекции пересечения линии. Нажмите «Save» («Сохранить») для применения настроек.

IV. Дополнительные настройки (Advanced Configuration)

В строке «Behavior Analysis Version» приводятся версии библиотек алгоритмов.

- **Parameter** («Параметры»):

Настройте следующие параметры для более тонкой настройки аналитики:

- **Detection Sensitivity** («Чувствительность») [0-4]: чувствительность детекции. Чем выше значение, тем выше шанс на обнаружение мелких объектов, в том числе шумов. Рекомендуется значение 3.
- **Background Update Rate** («Частота обновления») [0-4]: частота считывания данных. Рекомендуется значение 3.
- **Single Alarm** («Одиночная тревога»): если выбран этот пункт, то при обнаружении тревожного события тревога сработает только один раз. Если пункт не выбран, то тревога будет продолжаться, пока тревожное событие не пройдет (например, пока объект не выйдет из зоны и т.п.).

- Leave Interference Suppression («Компенсация движения растительности»): при выборе данного пункта в настраиваемых областях будет компенсироваться движение листы, которая может вызывать срабатывание тревоги.
 - Output Type («Тип выхода»): выберите местонахождение данных о тревогах на видеокадре – «Target Center» («На цели тревоги»), «Bottom Center» («Внизу по центру»), «Top Center» («Вверху по центру»).
 - Restore Default («По умолчанию»): возврат всех параметров на исходные значения.
 - Restart VCA («Перезапуск VCA»): перезапуск всех алгоритмов анализа поведения.
- **Global Size Filter** («Глобальный фильтр размера»): в отличие от параметра **Filter Type** в настройках каждого отдельного правила, данный параметр применяется ко всем параметрам сразу.

Последовательность действий для настройки:

1. Установите галочку на «Global Size Filter» («Глобальный фильтр размера») для активации данной функции.
2. На выбор имеются типы «Pixels» («Пиксели») и «Actual Size» («Реальный размер»). Если выбран тип «Pixels», то нужно нарисовать на видео область максимального и минимального размера для каждого правила. Если выбран тип «Actual Size», то нужно ввести максимальные и минимальные длину и ширину. Вызвать срабатывание тревоги сможет только объект, размер которого меньше максимального и больше минимального.
3. Нажмите «Save» («Сохранить») для применения настроек.

10.3.2. Снимок лица (Face Capture)

С помощью данной функции может быть осуществлен снимок скриншота, когда в кадре появляется лицо. Помимо изображения будут сохранены следующие данные: возраст, пол, наличие на лице очков.

I. Оверлей и захват (Overlay & Capture)

Данный раздел включает в себя настройку отображения OSD на видео и на захваченных скриншотах.

- **Display VCA info on Stream** («Отображать VCA на видеопотоке»): зеленые прямоугольники, обозначающие обнаруженные лица, будут отображаться на видеопотоке в реальном времени и в записях.
- **Display Target info on Alarm Picture** («Отображать обнаружение на скриншоте»): зеленые фигуры, обозначающие обнаруженное подозрительное поведение, будут отображаться на захваченных скриншотах.
- **Snapshot Settings** («Настройки скриншотов»):
 - **Upload JPEG Image to Center** («Отправить JPEG на центр наблюдения»): установите галочку для отправки захваченных скриншотов на центр наблюдения, когда происходят срабатывания VCA.
 - **Picture Quality** («Качество изображения»): настройка качества изображения скриншота.
 - **Picture Resolution** («Разрешение изображения»): настройка разрешения скриншота: CIF, 4CIF (D1), 720p, 1080p.
- **Background Upload** («Загрузка фона»): при включении опции также будет сохраняться и фон, не только изображение лица.

II. Защищенная область (Shield Region)

Данная функция позволяет задать область, в которой не будет работать обнаружение лиц. Всего может быть создано до 4 таких областей.

Последовательность действий для настройки:

1. Нажмите на «Shield Region» («Защищенная область») для входа в интерфейс настройки.
2. Нажмите на значок шестиугольника для того чтобы нарисовать область при помощи мыши в окне просмотра. Нажмите правой кнопкой мыши для сохранения области.

Примечания:

- Возможно создать область с количеством сторон до 10.
 - Нажатие на удаляет созданные области.
 - Если просмотр в реальном времени остановлен, возможности нарисовать область не будет.
3. Нажмите «Save» («Сохранить») для применения настроек.

III. Правила (Rule)

Последовательность действий для настройки:

1. Установите галочку на «Rule» («Правила») для включения правил захвата скриншотов с лицами.
2. Нажмите на значок для задания минимального расстояния между зрачками для фиксации лица.
3. Нажмите на значок для выделения области, в которой будет работать функция детекции лиц. Нарисуйте область при помощи мыши, нажмите правой кнопкой мыши для сохранения.

Примечания:

- Возможно создать область с количеством сторон до 10.
 - Если просмотр в реальном времени остановлен, возможности нарисовать область не будет.
4. Нажмите «Save» («Сохранить») для применения настроек.

IV. Дополнительные настройки (Advanced Configuration)

В строке «Face Capture Version» приводятся версии библиотек алгоритмов детекции лиц. Настройте приведенные ниже параметры в соответствии с задачей.

- **Detection Parameters** («Параметры детекции»):
 - Generation Speed («Скорость идентификации») [1-5]: скорость идентификации цели. Чем выше значение, тем быстрее будет происходить обнаружение. При установке низких значений неподвижные лица, находящиеся постоянно в кадре, не будут детектироваться. Это поможет избежать ситуаций детекции лиц на плакатах и т.п. Рекомендуется оставить стандартное значение – 3.

- Capture Times («Количество захватов») [1-10]: количество захватов скриншота при фиксации лица на изображении. Значение по умолчанию – 1.
- Sensitivity («Чувствительность») [1-5]: чем выше значение чувствительности, тем с большей вероятностью будет опознано лиц. Рекомендуется значение 3 для избегания ложных срабатываний.
- Capture Interval («Интервал захвата») [1-255]: интервал кадров между двумя захватами скриншота с зафиксированным лицом. При значении 1 (по умолчанию) будет фиксироваться каждый кадр, содержащий лицо.
- Capture Sensitivity («Чувствительность захвата») [0-20]: порог, при котором камера определяет цель как лицо. Только если внутреннее значение «Face Score», генерируемое алгоритмом, равно или выше установленного, камера будет опознавать объект как лицо. Рекомендуется значение по умолчанию – 2.
- **Face Capture Advanced Parameters** («Дополнительные параметры захвата»):
 - Face Exposure («Выдержка для лиц»): при включении опции будет задействована дополнительная выдержка/экспозиция для лиц (независимая от выдержки/экспозиции для обычного режима работы камеры).
 - Reference Brightness («Яркость») [0-100]: Яркость в режиме «Face Exposure». Если камерой обнаружено лицо, будет использовано значение яркости из этого параметра. Чем выше значение, тем ярче будет изображение с лицом.
 - Minimum Duration («Минимальная продолжительность») [1-60min]: минимальное время в минутах для использования дополнительной выдержки. Значение по умолчанию – 1 минута.

Примечание: если задействована функция дополнительной выдержки, пожалуйста, убедитесь, что функция WDR отключена, а также выбран режим ручного управления диафрагмой.

- Enable Face ROI («Включить ROI для лиц»): при фиксации лица область с лицом будет обработана как область интереса (ROI), что повысит качество изображения.
- Restore Default («По умолчанию»): нажмите для восстановления заводских установок.

10.3.3. Подсчет людей (People Counting)

Данная функция используется для подсчета числа людей, вошедших или вышедших из определенной заранее заданной области и может быть применима для подсчета посетителей.

Примечание: рекомендуется установить камеру непосредственно над проходом, в котором будет осуществляться подсчет посетителей, чтобы сам проход при этом был расположен горизонтально на изображении. Это значительно повысит точность подсчета.

Последовательность действий для настройки:

1. Зайдите настройки подсчета людей: Configuration («Настройки») – People Counting («Подсчет людей»)
2. Установите галочку на «Enable People Counting» («Вкл. подсчет людей») для активации данной функции.
3. Настройте линию детекции. Оранжевая линия, называемая линией детекции, может быть настроена на изображении. При пересечении этой линии в заданном направлении человеком он будет посчитан.
 - a. Нажмите на значок / в левом верхнем углу относительно изображения. Желтая линия появится на изображении.
 - b. Выставьте нужное положение линии с помощью мыши.

- c. Перенесите желтые точки по краям линии для настройки ее длины.

Примечания:

- Лучше всего настроить линию прямо под камерой, при этом линия должна перекрывать проход целиком.
 - Не рекомендуется устанавливать линию в тех местах, где люди могут подолгу задерживаться.
 - d. Нажатие на ✕ удаляет линию
 - e. Нажатие на ⇌ позволяет изменить направление, в котором будут проходить люди, которых следует подсчитать.
4. Установите галочку «Camera Calibration» («Калибровка камеры») для включения калибровки. На изображении появятся калибровочная линия (зеленая вертикальная) и несколько синих горизонтальных линий.
- **Camera Calibration** («Калибровка камеры»): имеется возможность задать размер, занимаемый человеком, для подсчета (обычно задается средняя ширина плеч). Правильно откалиброванная камера выдаст более точный результат при подсчете посетителей.
 - **Синие горизонтальные линии:** каждая синяя линия обозначает ширину плеч зафиксированного человека. Всего может быть отображено до восьми синих линий с каждой стороны линии детекции. Эти линии являются опорными значениями для калибровки.
 - **Зеленая вертикальная линия:** расстояние от левого края линии детекции до калибровочной зеленой линии обозначает настроенную ширину плеч человека. Имеется возможность перенести данную линию для подстройки в соответствии с синими линиями.
 - **Advanced** («Дополнительно»): имеется возможность точно задать местоположение линии детекции и калибровочной линии.
 - Координаты начальной и конечной точек линии детекции можно задать путем ввода значений вручную
 - Нажмите на значок ⚙ для установки калибровочной линии в оптимальное значение, высчитанное автоматически. Либо выставьте положение калибровочной линии при помощи соответствующего ползунка.
5. Настройка данных подсчета и отображения:
- a. Установите галочку «Enable OSD Overlay» («Вкл. OSD оверлей») и количество прошедших людей будет отображаться на видео.
 - b. Поле с количеством людей можно переносить по изображению при помощи мыши.
 - c. Установите галочку «Real-Time Upload Data» («Загрузить данные в реальном времени») для загрузки данных о подсчете в реальном времени.
 - d. Для установки периода подсчета выберите нужный временной период из выпадающего меню «Data Statistics Cycle» («Цикл сбора данных»).
 - e. Для сброса счетчика нажмите на кнопку 0 слева от окна с отображением видео.
6. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы функции. Обратитесь к разделу 10.1.1, задача 2 – для более детальной информации.
7. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях. Обратитесь к разделу 10.1.1, задача 3 – для более детальной информации.
8. Нажмите «Save» («Сохранить») для применения настроек.

Примечание: статистика подсчета людей будет собираться во вкладке «Application» («Приложения»).

10.3.4. Подсчет (Counting)

Данная функция используется для подсчета числа людей, вошедших или вышедших из определенной заранее заданной области и может быть применима для подсчета посетителей. В отличие от функции «Counting People» («Подсчет людей») для работы данной функции не требуется калибровка.

Примечание: рекомендуется установить камеру непосредственно над проходом, в котором будет осуществляться подсчет посетителей, чтобы сам проход при этом был расположен горизонтально на изображении. Это значительно повысит точность подсчета.

Последовательность действий для настройки:

1. Зайдите настройки подсчета: Configuration («Настройки») – Counting («Подсчет людей»)
2. Установите галочку на «Enable Counting» («Вкл. подсчет») для активации данной функции.
3. Установите галочку на «Enable OSD Overlay» («Вкл. OSD оверлей»)
4. Настройте линию детекции. Оранжевая линия, называемая линией детекции, может быть настроена на изображении. При пересечении этой линии в заданном направлении человеком он будет посчитан.
 - a. Нажмите на значок / в левом верхнем углу относительно изображения. Желтая линия появится на изображении.
 - b. Выставьте нужное положение линии с помощью мыши.
 - c. Перенесите желтые точки по краям линии для настройки ее длины.

Примечания:

- Лучше всего настроить линию прямо под камерой, при этом линия должна перекрывать проход целиком.
 - Не рекомендуется устанавливать линию в тех местах, где люди могут подолгу задерживаться.
 - d. Нажатие на ✕ удаляет линию
 - e. Нажатие на ⇌ позволяет изменить направление, в котором будут проходить люди, которых следует подсчитать.
5. Для сброса счетчика нажмите на кнопку 0 слева от окна с отображением видео.
 6. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы функции. Обратитесь к разделу 10.1.1, задача 2 – для более детальной информации.
 7. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях. Обратитесь к разделу 10.1.1, задача 3 – для более детальной информации.
 8. Нажмите «Save» («Сохранить») для применения настроек.

Примечание: статистика подсчета людей будет собираться во вкладке «Application» («Приложения»).

10.3.5. Тепловая карта (Heat Map)

Тепловая карта – это графическое отображение данных при помощи цветов. Тепловая карта используется для отображения данных о времени наибольшей посещаемости и ожидания клиентов в заданной области.

Последовательность действий для настройки:

1. Зайдите в настройки тепловой карты: Configuration («Настройки») – Heat Map («Тепловая карта»).
2. Установите галочку на «Enable Heat Map» для включения данной функции.
3. Перейдите в «Area Settings» («Настройки зоны»), чтобы нарисовать область, в которой будет работать функция. Нарисуйте область при помощи мыши, затем нажмите правой кнопкой мыши для сохранения. Всего может быть создано до 8 областей.

Примечание: При нажатии на «Select All» («Выбрать все») будет выбрана вся область изображения. При нажатии на «Delete» («Удалить») для удаления текущей области.

4. Настройте параметры для области:
 - Detection Sensitivity («Чувствительность детекции») [0-100]: рекомендованное значение – 50. Более высокие значения могут привести к ложным срабатываниям.
 - Background Update Rate («Частота обновления») [0-100]: частота обновления сцены. Рекомендованное значение – 50.
 - Scene Change Level («Уровень изменения сцены») [0-100]: уровень опознавания камерой меняющегося окружения, например, качающихся штор. Рекомендованное значение – 50.
 - Minimum Target Size («Минимальный размер объекта») [0-100]: размер объекта, опознаваемого камерой для учета в тепловой карте. Рекомендованное значение – 50.
 - Target Track («Слежение за объектом»): включение и выключение слежения за объектом.
5. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы функции. Обратитесь к разделу 10.1.1, задача 2 – для более детальной информации.
6. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях. Обратитесь к разделу 10.1.1, задача 3 – для более детальной информации.
7. Нажмите «Save» («Сохранить») для применения настроек.

10.3.6. Дорожный трафик (Road Traffic)

Из данного раздела доступны настройки «Vehicle Detection» («Детекция автомобилей») и «Mixed-Traffic Detection» («Детекция смешанного трафика»).

В случае «Vehicle Detection» может быть настроено срабатывание на проезжающие автомобили, в результате чего захватывается скриншот с регистрационным номером автомобиля, а также автоматически распознаются такие данные, как цвет автомобиля, марка автомобиля и т.п.

В случае «Mixed-Traffic Detection» может быть настроено срабатывание на проходящих пешеходов, проезжающие транспортные средства различных типов, в результате чего захватывается скриншот с изображением такого объекта.

Примечание: наличие данной функции зависит от модели камеры.

- **Detection Configuration** («Настройка детекции»)

Последовательность действий для настройки:

1. Выберите тип детекции из списка – «Vehicle Detection» («Детекция автомобилей») или «Mixed-Traffic Detection» («Детекция смешанного трафика»).

Примечание: для применения настроек при изменении типа детекции потребуется перезагрузка камеры.

2. Установите галочку на «Enable» («Вкл.») для активации данной функции.
3. Выберите номер полосы из выпадающего меню «Lane Number». Может быть выбрано до 4 полос.
4. При помощи мыши выделите полосу на дороге для отслеживания.
5. Настройте зум на камере таким образом, чтобы размер автомобиля на изображении был максимально близок к красному прямоугольнику на изображении.

Примечание: одновременно на каждой полосе может быть снят только один регистрационный номер.

6. Нажмите на «Arming Schedule» («Включить расписание») для настройки расписания работы функции. Обратитесь к разделу 10.1.1, задача 2 – для более детальной информации.
7. Нажмите на «Linkage Method» («Метод связи») и установите галочки на требуемых действиях. Обратитесь к разделу 10.1.1, задача 3 – для более детальной информации.
8. Нажмите «Save» («Сохранить») для применения настроек.

11. Настройки хранения

11.1. Настройка расписания записи

На камере есть два типа записи: ручную и по расписанию. Следуя инструкциям из этого раздела, вы можете настроить запись по расписанию. По умолчанию записанные файлы сохраняются на локальный жесткий диск или на сетевой диск.

Последовательность действий для настройки:

1. Зайдите в настройки расписания записи: Configuration («Настройки») – Storage («Хранение») – Schedule Settings («Параметры расписания») – Record Schedule («Расписание записи»).

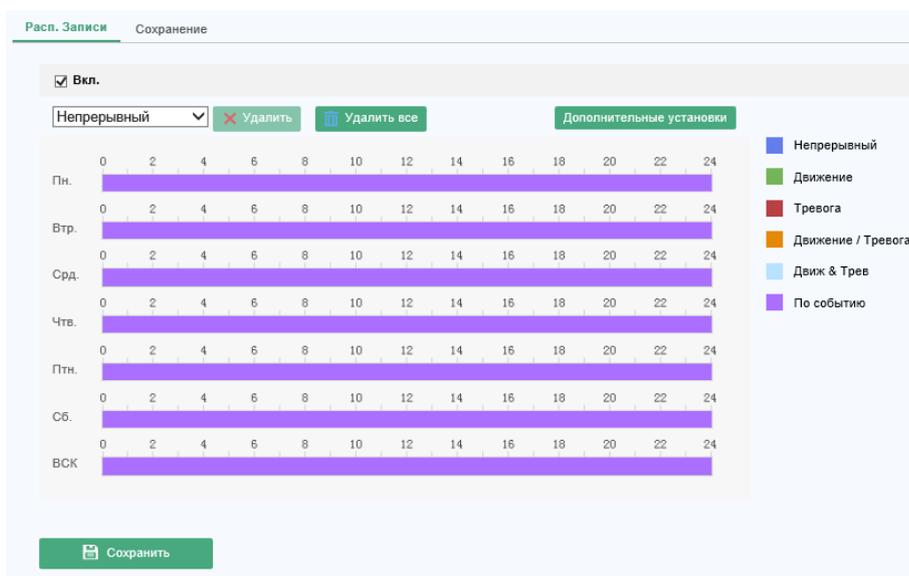


Рисунок 11.1 – Настройка расписания записи

2. Установите галочку на «Enable» («Вкл.») для активации записи по расписанию.
3. Нажмите на «Advanced» («Дополнительные установки») для настройки параметров записи.

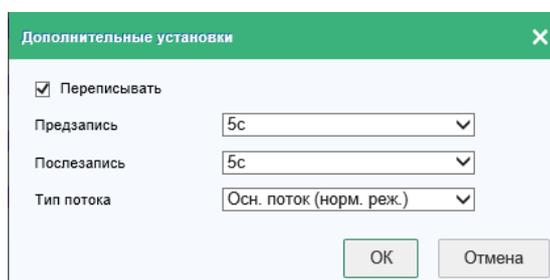


Рисунок 11.2 – Параметры записи

- **Переписывать / Overwrite:** включение перезаписи на носителе при окончании свободного места.
- **Предзапись / Pre-Record:** выставленное в секундах время будет добавлено перед записанным фрагментом. Например, если в 10:00 происходит срабатывание тревоги и начинается запись, а время предзаписи выставлено на значение 5 секунд, то к фрагменту записи будет добавлено время с 9:59:55.

- **Послезапись / Post-Record:** выставленное в секундах время будет добавлено после записанного фрагмента. Например, если в 11:00 завершается тревога, по которой началась запись, а время постзаписи выставлено на значение 5 секунд, то к фрагменту записи будет добавлено время до 11:00:05.
- **Тип потока / Stream Type:** выбор типа потока для записи.

Примечание: параметры записи могут быть различными на разных моделях камер.

4. Выберите тип записи («Record Type»). На выбор имеются варианты: «Continuous» («Непрерывная»), «Motion Detection» («Движение»), «Alarm» («Тревога»), «Motion | Alarm» («Движение / тревога»), «Motion & Alarm» («Движение и тревога»), «Event» («По событию»).
- **Непрерывная / Continuous:** видео записывается автоматически в соответствии с временем в расписании.
 - **Движение / Motion Detection:** видео записывается при срабатывании детекции движения. Помимо настройки расписания записи также требуется настроить детекцию движения и установить галочку на «Trigger Channel» («Запись канала») с номером нужного канала в разделе настроек детекции «Linkage Methods» («Привязка действий»). Более детальная информация приведена в главе 10.1.1., Задаче 1 данного руководства.
 - **Тревога / Alarm:** видео записывается при срабатывании тревожного события. Помимо настройки расписания записи также требуется настроить соответствующее тревожное событие и установить галочку на «Trigger Channel» («Запись канала») с номером нужного канала в разделе настроек тревожного события «Linkage Methods» («Привязка действий»). Более детальная информация приведена в главе 10.1.3 данного руководства.
 - **Движение и тревога / Motion & Alarm:** видео записывается при срабатывании одновременно детекции движения и тревожного события. Помимо настройки расписания записи также требуется настроить соответствующее тревожное событие и детекцию движения и установить галочку на «Trigger Channel» («Запись канала») с номером нужного канала в разделе настроек тревожного события и детекции движения «Linkage Methods» («Привязка действий»). Более детальная информация приведена в главах 10.1.1 и 10.1.3 данного руководства.
 - **Движение / тревога / Motion | Alarm:** видео записывается при срабатывании детекции движения или тревожного события, а также при их одновременном срабатывании. Помимо настройки расписания записи также требуется настроить соответствующее тревожное событие и детекцию движения и установить галочку на «Trigger Channel» («Запись канала») с номером нужного канала в разделе настроек тревожного события и детекции движения «Linkage Methods» («Привязка действий»). Более детальная информация приведена в главах 10.1.1 и 10.1.3 данного руководства.
 - **По событию / Event:** запись видео будет запускаться при срабатывании любых тревожных событий. Помимо настройки расписания записи также требуется настроить тревожные события.
5. Выберите тип записи и при помощи мыши настройте расписание.
 6. Нажмите «Save» («Сохранить») для применения настроек.

11.2. Настройка расписания захвата скриншотов (Capture Schedule)

Имеется возможность настройки расписания для захвата скриншотов по времени и по событиям. Захваченные скриншоты могут быть сохранены на локальном жестком диске или на сетевом хранилище.

Последовательность действий для настройки:

1. Зайдите в настройки расписания захвата скриншотов: Configuration («Настройки») – Storage («Хранение») – Schedule Settings («Параметры расписания») – Capture («Режим снимка»).

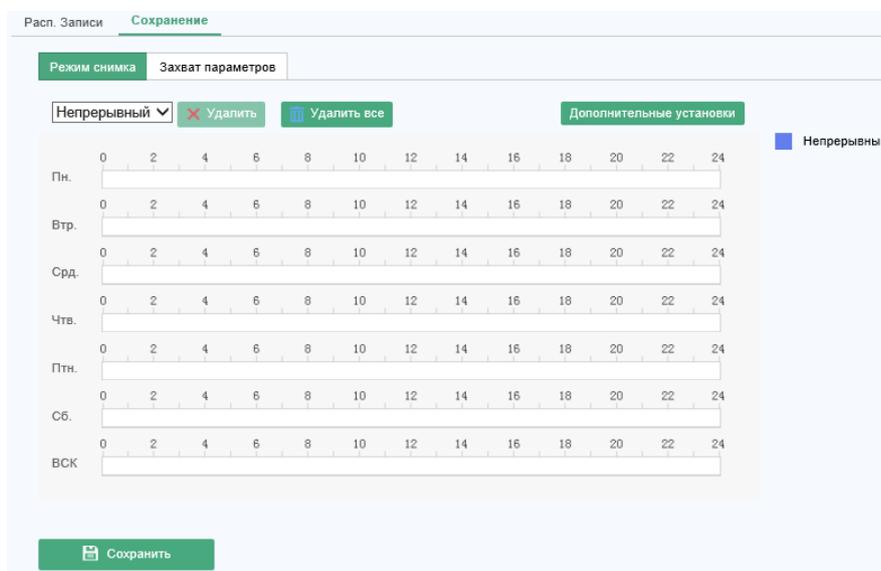


Рисунок 11.3 – Настройка расписания захвата скриншотов

2. Нажмите на вкладку «Capture Schedule» («Расписание захвата») для настройки расписания при помощи мыши. Имеется возможность скопировать настройки одного дня и перенести их на другие дни путем нажатия на зеленую кнопку, появляющуюся при наведении указателя мыши на правый край каждой из полос.
3. Нажмите на «Advanced» («Дополнительные установки») для выбора типа потока.

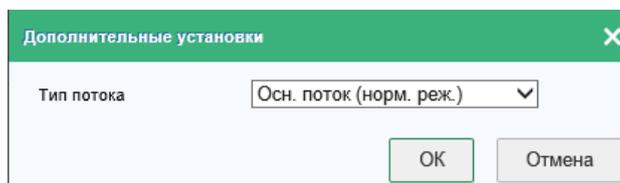


Рисунок 11.4 – Дополнительные настройки захвата скриншотов

4. Нажмите «Save» («Сохранить») для применения настроек.
5. Нажмите на вкладку «Capture Parameters» («Параметры захвата») для настройки различных параметров захвата скриншотов.
 - a. Установите галочку на «Активация захвата изображения по времени» («Enable Timing Snapshot») для включения режима непрерывного захвата скриншотов по расписанию.
 - b. Выберите формат изображения («Format»), разрешение («Resolution»), качество («Quality») и интервал захвата («Capture Interval»).
 - c. Установите галочку на «Активация захвата изображения по событию» («Enable Event-Triggered Snapshot») для включения захвата скриншотов по событиям.
 - d. Выберите формат изображения («Format»), разрешение («Resolution»), качество («Quality»), интервал захвата («Capture Interval») и номер («Number»).
6. Выберите интервал в миллисекундах между двумя скриншотами («Interval»).
7. Нажмите «Save» («Сохранить») для применения настроек.

Рисунок 11.5 – Настройка параметров скриншотов

11.3. Настройка сетевого хранилища (Net HDD)

Прежде, чем начать:

Сетевой диск должен быть доступен из сети и должным образом настроен для возможности сохранения на него записанных файлов, данных журнала, изображений и т.п.

Последовательность действий для настройки:

1. Добавьте сетевое хранилище:
 - а. Зайдите в настройки сетевого хранилища: Configuration («Настройки») – Storage («Хранение») – Storage Management («Управление хранением») – Net HDD («Сетевой HDD»).

№ HDD	Адрес сервера	Путь к файлу	Тип	Удалить
1			NAS	✖
Тип установки: NFS Пользователь: <input type="text"/> Пароль: <input type="text"/> Тест				
2			NAS	✖

Рисунок 11.6 – Добавление сетевого хранилища

- б. Введите IP-адрес сетевого диска («Server Address») и путь к папке для сохранения файлов («File Path»).
- с. Выберите тип устройства («Mounting Type»). Поддерживаются NFS и SMB/CIFS. Введите имя пользователя («User Name») и пароль («Password»), если выбран тип устройства SMB/CIFS.

Примечания:

- Пожалуйста, обратитесь к руководству пользователя сетевого хранилища для создания папки, в которой будут храниться данные.
 - Настоятельно рекомендуется установить сложный пароль, состоящий из более чем 8 символов, отвечающий как минимум трем из следующих критериев: содержит заглавные буквы, содержит строчные буквы, содержит цифры, содержит специальные символы. Также рекомендуется регулярно изменять пароль.
 - Менеджмент учетных записей и паролей целиком и полностью является зоной ответственности инсталлятора или конечного пользователя.
- d. Нажмите «Save» («Сохранить») для применения настроек.
2. Инициализация добавленного сетевого диска:
 - a. Зайдите в интерфейс настройки жестких дисков: Configuration («Настройки») – Storage («Хранение») – Storage Management («Управление хранилищами») – HDD Management («Управление HDD»). В этом меню имеется возможность просмотреть емкость («Capacity»), свободное пространство («Free Space»), состояние («Status»), тип («Type») и назначение («Property») жесткого диска.
 - b. Если состояние диска «Uninitialized» («Не инициализирован»), установите соответствующую галочку напротив диска и нажмите на кнопку «Format» («Форматировать») для начала инициализации. После окончания инициализации состояние диска перейдет на значение «Normal» («Нормальный»).
 3. Задайте пространство, отведенное для видеозаписей и для скриншотов:
 - a. Введите значения в процентах долей объема диска, занимаемых скриншотами («Percentage of Picture») и видеозаписями («Percentage of Record»).
 - b. Нажмите «Save» («Сохранить») для применения настроек.

Примечание: всего может быть добавлено до 8 дисков NAS (сетевых хранилищ).

11.4. Поиск карты памяти (Memory Card Detection)

С помощью данного раздела настроек имеется возможность просматривать состояние карты памяти, осуществить блокировку карты памяти, настроить получение уведомлений при возникновении ошибок в работе карты памяти.

Примечание: данная функция поддерживается только определенными типами карт памяти и моделями камер. Если данного раздела настроек нет в камере, то либо сама камера не поддерживает SD-карты, либо SD-карта не поддерживается данной функцией.

Последовательность действий для настройки:

1. Зайдите в интерфейс поиска карты памяти: Configuration («Настройки») – Storage («Хранение») – Storage Management («Управление хранением») – Memory Card Detection («Поиск карты памяти»).
2. Просмотрите состояние карты памяти во вкладке «Status Detection» («Состояние карты»).
 - **Оставшееся время работы / Remaining Lifespan:** отображается оценка оставшегося времени работы карты в процентах. На продолжительность жизни карты влияют ее объем и битрейт записываемой информации. Если данный параметр значительно снизился, рекомендуется заменить карту памяти.
 - **Здоровье карты / Health Status:** показывает текущее состояние карты. Всего существует три характеристики состояния карты – обычное («good»), плохое («bad») и поврежденное («damaged»). При должной настройке расписания («Arming Schedule») и привязки

действий («Linkage Methods») вы получите уведомление в случае изменения состояния карты на любое помимо нормального.

Примечание: в этом случае рекомендуется сменить карту памяти.

3. Нажмите на вкладку «R/W Lock» («Блокировка») для блокировки чтения и записи.
 - Добавление блокировки:
 - a. Выберите в строке «Lock Switch» значение «ON» («Вкл.»).
 - b. Введите пароль в поле «Password Settings».
 - c. Нажмите «Save» («Сохранить») для применения настроек.
 - Снятие блокировки:
 - a. Если карта памяти используется на том же самом устройстве, на котором настроена блокировка, процедура разблокировки не требуется, т.е. чтение и запись будут работать.
 - b. Если же данная заблокированная карта памяти будет использоваться на другой камере, то следует перейти в интерфейс «HDD Management» («Управление HDD») для разблокировки. Выберите карту памяти и нажмите на кнопку «Unlock» («Разблокировать») рядом с кнопкой «Format» («Форматировать»). Затем введите пароль для разблокировки.

Примечания:

- Данные с карты памяти могут быть считаны и записаны только если она разблокирована.
 - Если камера, на которой настраивалась блокировка, была сброшена к заводским настройкам, то следует перейти в интерфейс «HDD Management» и разблокировать карту, введя пароль от нее.
 - Удаление блокировки:
 - a. Выберите в строке «Lock Switch» значение «OFF» («Выкл.»).
 - b. Введите пароль от карты памяти.
 - c. Нажмите «Save» («Сохранить») для применения настроек.
4. Настройте расписание («Arming Schedule») и привязку действий («Linkage Methods»), если требуется получать уведомления об изменении состояния карты памяти. Более детальная информация приведена в главах 10.1.1 и 10.1.3 данного руководства.
 5. Нажмите «Save» («Сохранить») для применения настроек.

11.5. Настройка облегченного хранилища (Lite Storage)

В случае, если в поле зрения камеры отсутствуют движущиеся объекты, число кадров в секунду и битрейт видеопотока могут быть снижены для увеличения глубины архива.

Примечания:

- Данная функция может отсутствовать на некоторых моделях камер.
 - Видеофайлы, записанные в данном режиме, будут проигрываться с обычной частотой кадров (25 или 30 в секунду), из-за этого скорость воспроизведения будет увеличена.
1. Зайдите в интерфейс облегченного хранилища: Configuration («Настройки») – Storage («Хранение») – Storage Management («Управление хранилищами») – Lite Storage («Облегченное хранилище»).
 2. Установите галочку на «Enable» («Вкл.») для активации данной функции.
 3. Введите глубину архива в поле «Storage Time».
 4. Нажмите «Save» («Сохранить») для применения настроек.

12. Архив (Playback)

В этой главе руководства приведены инструкции по использованию интерфейса воспроизведения записанных файлов, которые хранятся на сетевых жестких дисках или картах памяти.

Последовательность действий:

1. Нажмите на «Playback» («Архив») на панели меню веб-интерфейса для входа в интерфейс воспроизведения.

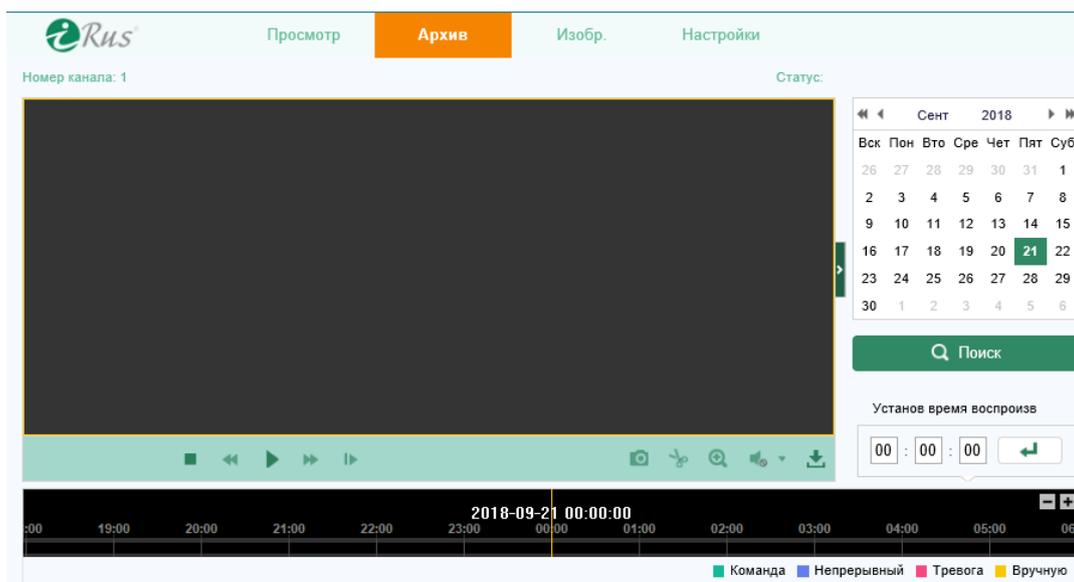


Рисунок 12.1 – Интерфейс воспроизведения записей

2. Выберите дату и нажмите на кнопку «Search» («Поиск»).

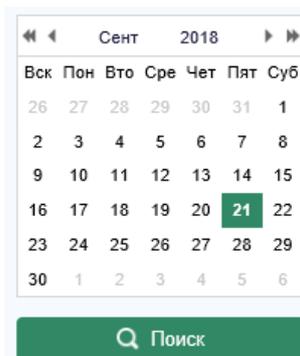


Рисунок 12.2 – Осуществление поиска видеозаписей

3. Нажмите на кнопку ► для воспроизведения видеозаписей за выбранную дату. Панель инструментов в нижней части интерфейса воспроизведения используется для управления воспроизведением.



Рисунок 12.3 – Панель инструментов воспроизведения

Примечание: выбрать пути сохранения скачиваемых фрагментов видео и скриншотов можно в меню «Local Configuration» («Локальные конфигурации»).

Таблица 5.1. Описание функций панели инструментов.

Иконка	Описание
▶	Воспроизведение
⏸	Пауза
■	Стоп
⏮	Замедление
⏭	Ускорение
🔍 / 🔍	Включение / отключение цифрового приближения
📷	Захват скриншота
✂ / ✂	Начать / завершить вырезку фрагмента видео для сохранения
🔊 / 🔊	Включение / отключение звука
⬇	Скачивание
▶	Покадровое воспроизведение

Также имеется возможность ввести точное значение времени в поле «Установ. время воспроизведения» («Set Playback Time») и нажать на  для перехода в заданное время. Для изменения масштаба временной шкалы используются кнопки  .

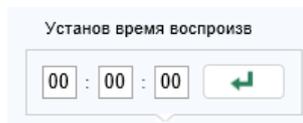


Рисунок 12.4 – Переход на определенное время при воспроизведении

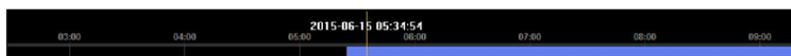


Рисунок 12.5 – Временная шкала

Разные цвета на временной шкале обозначают разные типы записи: «Command» («Команда»), «Continuous» («Непрерывный»), «Alarm» («Тревога») и «Manual» («Вручную»).



Рисунок 12.6 – Типы записей по цветам

13. Скриншоты (Snapshots)

Нажмите на кнопку «Picture» («Изобр.») для входа в интерфейс поиска сохраненных скриншотов. Имеется возможность искать, просматривать и скачивать скриншоты, хранящиеся на сетевом хранилище или на карте памяти камеры.

Примечания:

- Убедитесь, что локальное или сетевое хранилище должным образом настроено для хранения скриншотов.
- Убедитесь, что настроено расписание захвата скриншотов: Configuration («Настройки») – Storage («Хранение») – Schedule Settings («Настройки расписания») – Capture («Сохранение»).

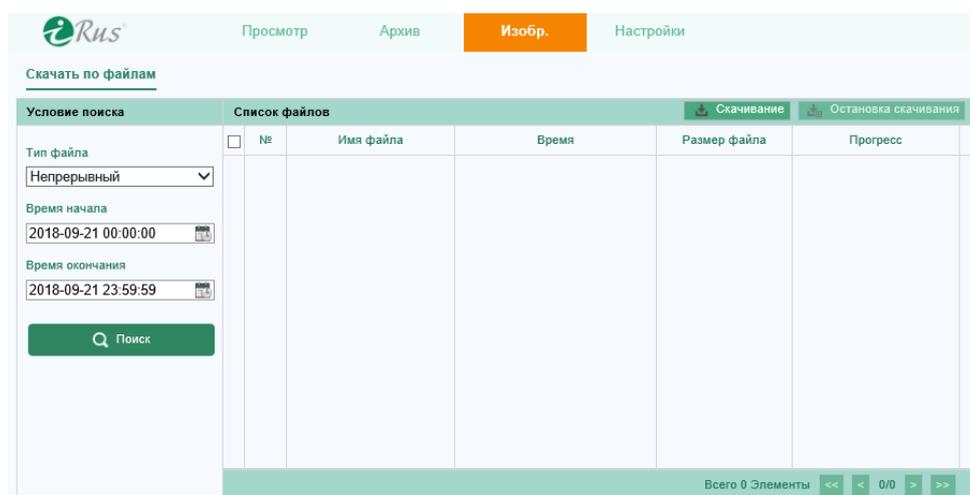


Рисунок 13.1 – Интерфейс поиска скриншотов

Последовательность действий:

1. Выберите тип файлов из выпадающего списка «File Type»: «Continuous» («Непрерывный»), «Motion» («Движение»), «Alarm» («Тревога»), «Motion | Alarm» («По движению или тревоге»), «Motion & Alarm» («По движению и тревоге»), «Line Crossing» («По пересечению линии»), «Intrusion Detection» («По вторжению»), «Scene Change Detection» («По изменению сцены»).
2. Выберите время начала («Start Time») и время окончания («End Time»).
3. Нажмите на «Search» («Поиск») для поиска результатов, отвечающих заданным критериям.
4. Установите галочку напротив нужных скриншотов и нажмите на «Download» («Скачивание») для скачивания выбранных файлов.

Примечание: единовременно может быть отображено не более 4000 скриншотов.

14. Приложения (Application)

Нажмите на «Application» («Приложения») для входа в интерфейс просмотра статистики. Имеется возможность искать, просматривать и скачивать данные статистики, хранящиеся на сетевом хранилище или на карте памяти камеры.

Обратите внимание, что функции в данном разделе могут различаться в зависимости от модели камеры.

14.1. Статистика обнаружения лиц (Face Capture Statistics)

После включения функции обнаружения лиц на камере появляется возможность просматривать и скачивать данные об обнаружении лиц через данный интерфейс. Для удобства отображения имеется возможность выводить данные в разных представлениях.

Последовательность действий:

1. Выберите тип отчета из выпадающего списка «Report Type»: «Daily Report» («За день»), «Weekly Report» («За неделю»), «Monthly Report» («За месяц») и «Annual Report» («За год»).
2. Выберите тип статистики из выпадающего списка «Statistics Type».
3. Выберите время начала («Start Time») и нажмите на «Counting» («Подсчитать»). Результаты подсчета будут отображены в поле «Statistics Result» («Результаты статистики»). Выберите вкладку «Table» («Таблица») или «Pie Chart» («Круговая диаграмма») для выбора соответствующего представления данных.

Примечание: при просмотре результатов в виде таблицы имеется возможность экспортировать («Export») данные в файл excel.

14.2. Статистика подсчета людей (People Counting Statistics)

После включения функции подсчета людей на камере появляется возможность просматривать и скачивать данные соответствующей статистики через данный интерфейс. Для удобства отображения имеется возможность выводить данные в разных представлениях.

Последовательность действий:

1. Выберите тип отчета из выпадающего списка «Report Type»: «Daily Report» («За день»), «Weekly Report» («За неделю»), «Monthly Report» («За месяц») и «Annual Report» («За год»).
2. Выберите тип статистики из выпадающего списка «Statistics Type»: «People Entered» («Вошедшие люди») или «People Exited» («Вышедшие люди»).
3. Выберите время начала («Start Time») и нажмите на «Counting» («Подсчитать»). Результаты подсчета будут отображены в поле «Statistics Result» («Результаты статистики»). Выберите вкладку «Table» («Таблица»), «Bar Chart» («Ступенчатая диаграмма») или «Line Chart» («Линейная диаграмма») для выбора соответствующего представления данных.

Примечание: при просмотре результатов в виде таблицы имеется возможность экспортировать («Export») данные в файл excel.

14.3. Статистика тепловой карты (Heat Map Statistics)

После включения функции тепловой карты на камере появляется возможность просматривать и скачивать данные соответствующей статистики через данный интерфейс. Для удобства отображения имеется возможность выводить данные в разных представлениях.

Последовательность действий:

1. Выберите тип отчета из выпадающего списка «Report Type»: «Daily Report» («За день»), «Weekly Report» («За неделю»), «Monthly Report» («За месяц») и «Annual Report» («За год»).
2. Выберите время начала («Start Time») и нажмите на «Counting» («Подсчитать»). Результаты подсчета будут отображены в поле «Statistics Result» («Результаты статистики»). Выберите вкладку «Space Heat Map» («Пространственная тепловая карта») или «Time Heat Map» («Временная тепловая карта») для выбора соответствующего представления данных.

Примечание: при просмотре результатов в виде временной тепловой карты имеется возможность экспортировать («Export») данные в файл excel.

14.4. Статистика подсчета

После включения функции подсчета на камере появляется возможность просматривать и скачивать данные соответствующей статистики через данный интерфейс. Для удобства отображения имеется возможность выводить данные в разных представлениях.

Последовательность действий:

1. Выберите тип отчета из выпадающего списка «Report Type»: «Daily Report» («За день»), «Weekly Report» («За неделю»), «Monthly Report» («За месяц») и «Annual Report» («За год»).
2. Выберите тип статистики из выпадающего списка «Statistics Type»: «People Entered» («Вошедшие люди») или «People Exited» («Вышедшие люди»).
3. Выберите время начала («Start Time») и нажмите на «Counting» («Подсчитать»). Результаты подсчета будут отображены в поле «Statistics Result» («Результаты статистики»). Выберите вкладку «Table» («Таблица»), «Bar Chart» («Ступенчатая диаграмма») или «Line Chart» («Линейная диаграмма») для выбора соответствующего представления данных.

Примечание: при просмотре результатов в виде таблицы имеется возможность экспортировать («Export») данные в файл excel.

15. Дополнительная информация

15.1. Программное обеспечение iRUS Configurator

- Описание ПО iRUS Configurator

iRUS Configurator – бесплатная программа для поиска устройств с удобным и понятным интерфейсом. При помощи данного ПО можно найти работающие устройства в сети и просмотреть информацию о них. Также имеется возможность изменения основных сетевых настроек устройства.

- Поиск подключенных устройств

- Автоматический поиск

После запуска ПО **iRUS Configurator** автоматически запускается поиск устройств, находящихся в одной подсети с компьютером, повторяющийся каждые 15 секунд. В интерфейсе «Online Devices» («Устройства онлайн») отображается список найденных устройств с информацией о них: тип устройства, IP-адрес, номер порта и т.п.

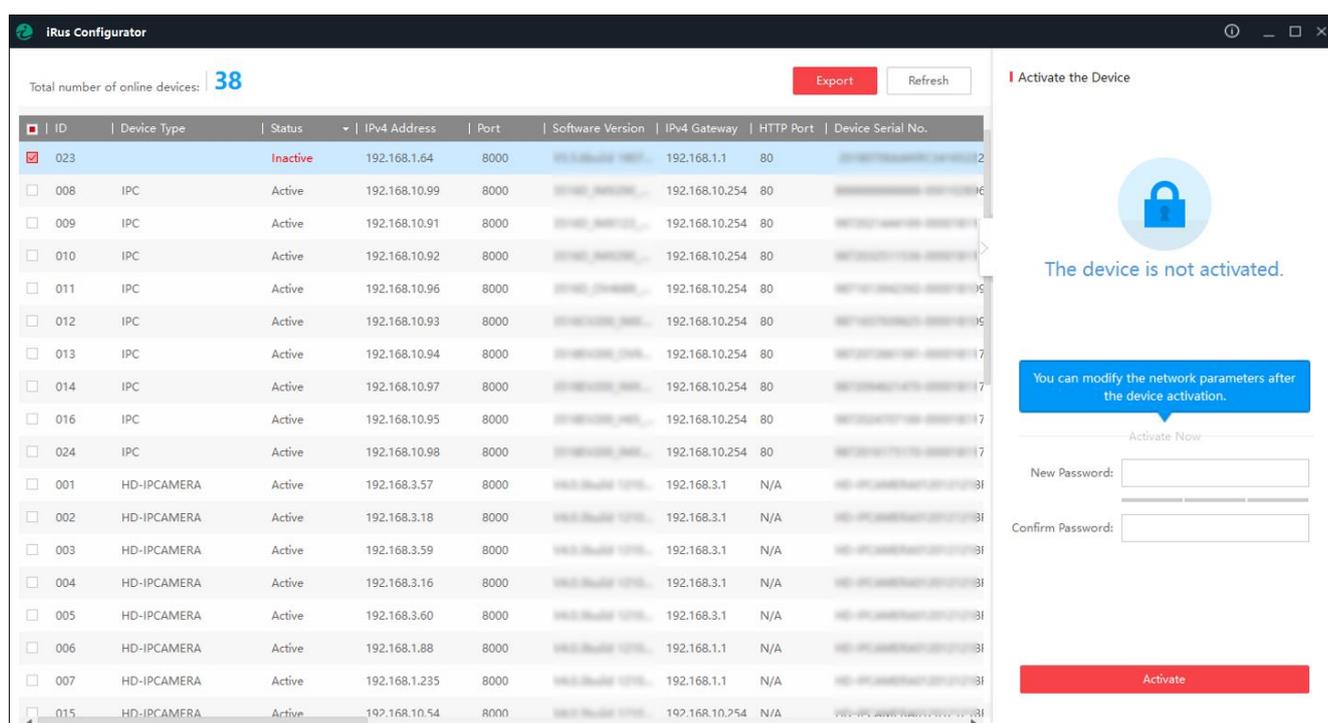


Рисунок 15.1 – Поиск подключенных устройств

Примечание: после включения устройство появляется в списке спустя 15 секунд; после отключения устройство пропадает из списка спустя 45 секунд.

- Поиск устройств вручную

При нажатии на кнопку «Обновить» («Refresh») осуществляется поиск устройств в ручном режиме. Найденные новые устройства будут добавлены в список.

Примечание: для упорядочивания списка нажмите на кнопки ▲ или ▼ на заголовках столбцов; для скрытия панели изменения сетевых параметров нажмите на кнопку ►.

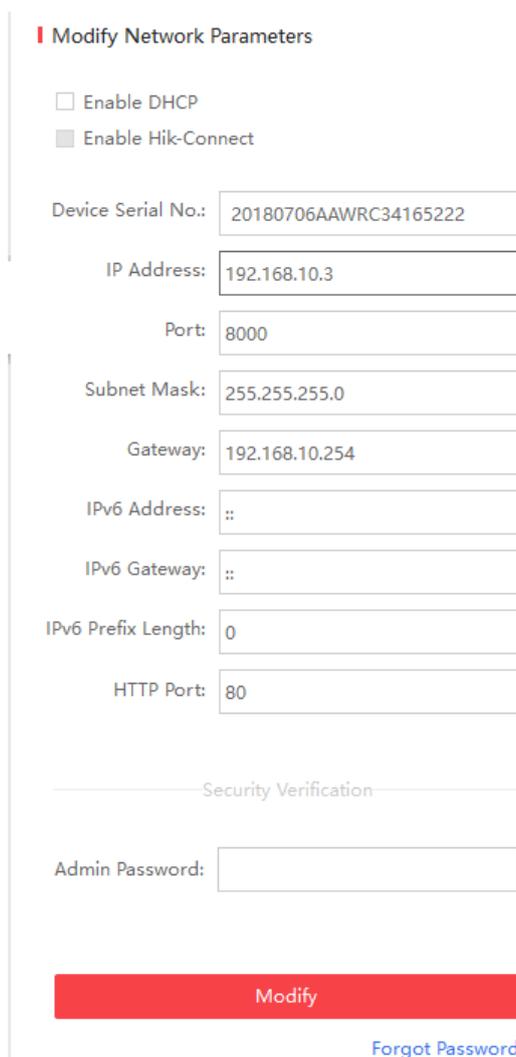
- **Изменение сетевых настроек**

Последовательность действий для настройки:

1. Выберите устройство, настройки которого требуется изменить, из списка. Его сетевые параметры будут отображены на панели «Modify Network Parameters» («Изменить сетевые параметры») в правой части окна программы.
2. Измените сетевые параметры на нужные (IP-адрес, номер порта и т.д.).
3. Введите пароль от учетной записи «admin» и нажмите на кнопку  для применения настроек.

Примечания:

- Настоятельно рекомендуется установить сложный пароль, состоящий из более чем 8 символов, отвечающий как минимум трем из следующих критериев: содержит заглавные буквы, содержит строчные буквы, содержит цифры, содержит специальные символы. Также рекомендуется регулярно изменять пароль.
- Менеджмент учетных записей и паролей целиком и полностью является зоной ответственности инсталлятора или конечного пользователя.



Modify Network Parameters

Enable DHCP

Enable Hik-Connect

Device Serial No.: 20180706AAWRC34165222

IP Address: 192.168.10.3

Port: 8000

Subnet Mask: 255.255.255.0

Gateway: 192.168.10.254

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Security Verification

Admin Password:

[Modify](#)

[Forgot Password](#)

Рисунок 15.2 – Изменение сетевых настроек устройства

15.2. Проброс портов

Ниже приведен пример настройки проброса портов для маршрутизатора TP-Link TL-WR641G. Настройки могут отличаться в зависимости от модели маршрутизатора. Настоятельно рекомендуем ознакомиться с документацией по конкретной используемой модели маршрутизатора для правильной настройки проброса портов.

Последовательность действий для настройки:

1. Выберите тип подключения WAN:



Рисунок 15.3 – Выбор типа подключения WAN

2. Установите параметры LAN маршрутизатора как на приведенном ниже рисунке, включая IP-адрес и маску подсети:

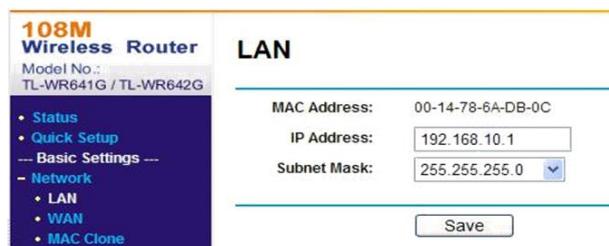


Рисунок 15.4 – Установка параметров LAN

3. Настройте проброс портов в разделе «Forwarding». По умолчанию камера использует порты 80, 8000 и 554. Эти значения могут быть изменены через веб-интерфейс или ПО SAPD.

Пример:

При подключении двух камер к одному и тому же маршрутизатору и при необходимости проброса портов до каждой из них можно поменять номера портов одной из камер. Например, первая камера с IP-адресом 192.168.1.23 и портами 80, 8000, 554 и 8200. Вторая камера с IP-адресом 192.168.1.24 и портами 81, 8001, 555 и 8201.

Последовательность действий для проброса портов до каждой из камер:

1. Создайте правила для портов 80, 8000, 554 и 8200 для IP-адреса 192.168.1.23.
2. Создайте правила для портов 81, 8001, 555 и 8201 для IP-адреса 192.168.1.24.
3. В качестве протокола выберите «ALL» или «TCP».
4. Установите галочки на «Enable» напротив каждого правила и нажмите «Save» для применения настроек.

108M
Wireless Router
Model No.:
TL-WR641G / TL-WR642G

- Status
- Quick Setup
- Basic Settings ---
- Network
- Wireless
- Advanced Settings ---
- DHCP
- Forwarding
 - Virtual Servers
 - Port Triggering
 - DMZ
 - UPnP
- Security
- Static Routing
- Dynamic DNS
- Maintenance ---
- System Tools

Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	<input checked="" type="checkbox"/>
2	8000	192.168.10.23	ALL	<input checked="" type="checkbox"/>
3	554	192.168.10.23	ALL	<input checked="" type="checkbox"/>
4	8200	192.168.10.23	ALL	<input checked="" type="checkbox"/>
5	81	192.168.10.24	ALL	<input checked="" type="checkbox"/>
6	8001	192.168.10.24	ALL	<input checked="" type="checkbox"/>
7	555	192.168.10.24	ALL	<input checked="" type="checkbox"/>
8	8201	192.168.10.24	ALL	<input checked="" type="checkbox"/>

Common Service Port: DNS(53) Copy to ID 1

Previous Next Clear All Save

Рисунок 15.5 – Проброс портов

Примечание: порт камеры не должен конфликтовать с другими портами. Например, если роутером используется порт 80 для доступа к его веб-интерфейсу извне, следует изменить веб-порт камеры на другой (например, 81 или 8080).