

Руководство по монтажу

www.beward.ru

Сменные IP-камеры BFM2530-LP, BFM2530-LPE



Детекция автомобильных номеров
Питание по Passive PoE
Быстрый монтаж, замена без инструмента
Управление через мобильное приложение

Оглавление

ГЛАВА 1. МЕРЫ ПРЕДОСТОРОЖНОСТИ	3
ГЛАВА 2. ОБЩИЕ СВЕДЕНИЯ	5
2.1. Особенности IP-видеокамер	5
2.2. Основные характеристики	6
2.3. Комплект поставки	6
2.4. Установки по умолчанию	6
ГЛАВА 3. РАЗМЕРЫ И ОСНОВНЫЕ ЭЛЕМЕНТЫ УСТРОЙСТВА.....	7
ГЛАВА 4. УСТАНОВКА И ПОДКЛЮЧЕНИЕ IP-КАМЕРЫ.....	8
4.1. Рекомендации по установке	8
4.2. Монтаж IP камер	9
4.3. Замена карты памяти	10
4.4. Варианты использования ПО видеокамеры	11
4.5. Сброс настроек видеокамеры	12
ГЛАВА 5. НАСТРОЙКА ПРОВОДНОГО СОЕДИНЕНИЯ	13
5.1. ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ ПРОВОДНОЙ ЛОКАЛЬНОЙ СЕТИ	13
5.1.1. <i>Определение параметров сети при динамическом IP-адресе</i>	17
5.2. ИЗМЕНЕНИЕ ПАРАМЕТРОВ ЛОКАЛЬНОЙ СЕТИ ДЛЯ ПОДКЛЮЧЕНИЯ К IP-КАМЕРЕ.....	20
5.3. ПОЛУЧЕНИЕ ДОСТУПА К IP-КАМЕРЕ С ПОМОЩЬЮ БРАУЗЕРА	23
5.4. ПОЛУЧЕНИЕ ДОСТУПА К ВЕБ-ИНТЕРФЕЙСУ IP-КАМЕРЫ.....	24
5.5. ИЗМЕНЕНИЕ НАСТРОЕК ПОДКЛЮЧЕНИЯ IP-КАМЕРЫ ЧЕРЕЗ ВЕБ-ИНТЕРФЕЙС	25
5.6. ВОЗВРАТ НАСТРОЕК ПОДКЛЮЧЕНИЯ ПК В ПЕРВОНАЧАЛЬНЫЕ ЗНАЧЕНИЯ.....	27
5.7. ПРОВЕРКА ПРАВИЛЬНОСТИ НАСТРОЕК ПОДКЛЮЧЕНИЯ IP-КАМЕРЫ К ЛОКАЛЬНОЙ СЕТИ	30
ПРИЛОЖЕНИЯ	32
Приложение А. ЗАВОДСКИЕ УСТАНОВКИ.....	32
Приложение В. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА	33
Приложение С. ПРАВА И ПОДДЕРЖКА.....	36
Приложение D. ГЛОССАРИЙ.....	38

Глава 1. Меры предосторожности

Перед использованием необходимо помнить нижеследующее.

Данный продукт удовлетворяет всем требованиям безопасности. Однако, как и любой электроприбор, в случае неправильного использования он может стать причиной пожара, что, в свою очередь, может повлечь за собой серьезные последствия. **Во избежание несчастных случаев обязательно изучите инструкцию!**

ВНИМАНИЕ!

Используйте только совместимые устройства. Эксплуатация устройств, не одобренных производителем, недопустима.

Соблюдайте инструкцию по эксплуатации!

Избегайте длительного использования или хранения камеры в неблагоприятных условиях:

- При слишком высоких или низких температурах (рабочая температура устройства от -40 до +40 °C).
- Избегайте попадания прямых солнечных лучей в течение длительного времени, а также нахождения поблизости отопительных и обогревательных приборов.
- Избегайте близости с водой или источниками влажности.
- Избегайте близости с устройствами, обладающими большим электромагнитным эффектом.
- Недопустима установка камеры в местах с сильной вибрацией.

ВНИМАНИЕ!

В случае неисправности камеры свяжитесь с сервисным центром ООО «НПП «Бевард».

В случае некорректной работы камеры:

- При обнаружении дыма или необычного запаха.
- При попадании воды или других инородных объектов внутрь.
- При падении камеры или повреждении корпуса:

Выполните следующие действия:

1. Отключите камеру от источника питания и отсоедините все остальные провода.
2. Свяжитесь с сервисным центром ООО «НПП «Бевард». Контактные данные Вы можете найти на сайте <http://www.beward.ru/>.

Транспортировка

При транспортировке камеры положите ее в упаковку производителя или любой другой материал соответствующего качества и ударопрочности.

Вентиляция

Во избежание перегрева, ни в коем случае не блокируйте циркуляцию воздуха вокруг камеры.

Чистка

Используйте мягкую сухую ткань для протирания внешних поверхностей. Для трудновыводимых пятен используйте небольшое количество чистящего средства, после чего насухо вытрите поверхность.

Не используйте летучие растворители, такие как спиртосодержащие средства или бензин, так как они могут повредить корпус камеры.

Глава 2. Общие сведения

Сменные видеокамеры BFM2530-LP и BFM2530-LPE для комплектов BEWARD BIN-LPF, BIN-LPH и BIN-LPS предназначены для интеграции в шлагбаумы Barrier-PRO и Barrier-PRO-RPD. Сменные видеокамеры оснащены современным алгоритмом детектирования (для BFM2530-LPE) или распознавания (для BFM2350-LP) номеров, который задействует ресурсы нейросетевого ускорителя видеокамеры. Такие технологии, как режим «День/Ночь», расширенный динамический диапазон (2xWDR), система шумоподавления (2D/3DNR), а также электромеханический ИК-фильтр, выгодно отличают данные модели, позволяя им соответствовать высоким требованиям, предъявляемым к современным системам видеонаблюдения.



Рис. 2.1

Камеры способны передавать видеопоток в форматах сжатия H.264/H.265 и MJPEG. Камеры подключаются к сети при помощи проводного интерфейса 10/100BASE-TX Ethernet. Камеры могут быть настроены через веб интерфейс, либо через P2P сервис мобильного приложения DoorHan. Добавление камер в аккаунт пользователя в мобильном приложении происходит с помощью чтения камерами QR-кода, генерируемого в приложении. При этом отсутствует необходимость настройки IP адресов и знания сетевых технологий. Сервера DoorHan находятся в России, благодаря чему облачный сервис работает стабильно в отличие от зарубежных аналогов.

2.1. Особенности IP-видеокамер

- 2Мп 1/2.8" КМОП-сенсор SONY Starvis с прогрессивным сканированием
- Одновременное кодирование: H.265/H.264/MJPEG
- Революционный кодек H.265: до 50% прироста эффективности сжатия
- Расширенный динамический диапазон 2xWDR до 120 дБ
- Мощная ИК-подсветка до 10 м
- Уличное исполнение, от -40 до +40°C, IP66

- ИК-светодиоды III поколения, угол подсветки до 90°
- Фиксированный объектив 3.6 мм
- До 25 к/с при любом разрешении
- Поддержка 2xWDR до 120 дБ, 2D/3DNR, запись на microSDHC
- Питание по Passive PoE
- Быстрый монтаж, замена без инструмента

2.2. Основные характеристики

- Допустимое отклонение от оси объектива для распознавания – до 50 градусов
- Поддержка стандартных прямоугольных и “квадратных” автономеров (Тип 1 и 1A)
- Поддержка автономеров такси и спецслужб: тип 1Б, группа 2, 3 и 5.
- Управление через веб интерфейс или мобильное приложение по P2P

2.3. Комплект поставки

- IP камера (для BFM2530-LP - с установленной картой памяти microSDHC 4 ГБ)
- Упаковочная тара

ВНИМАНИЕ!

BEWARD оставляет за собой право на изменение комплектации оборудования и его любых характеристик без предварительного уведомления.

2.4. Установки по умолчанию

- DHCP: **включено**
- IP-адрес: **192.168.0.99**
- Маска подсети: **255.255.255.0**
- Сетевой шлюз: **192.168.0.1**
- Имя пользователя: **admin**
- Пароль: **admin**
- HTTP-порт: **80**
- RTSP-порт: **554**
- Порт данных: **5000**
- ONVIF-порт: **80**

Глава 3. Размеры и основные элементы устройства

Основные элементы IP-камер BEWARD BFM2530-LP(E) рассмотрены ниже (Рис 3.1):

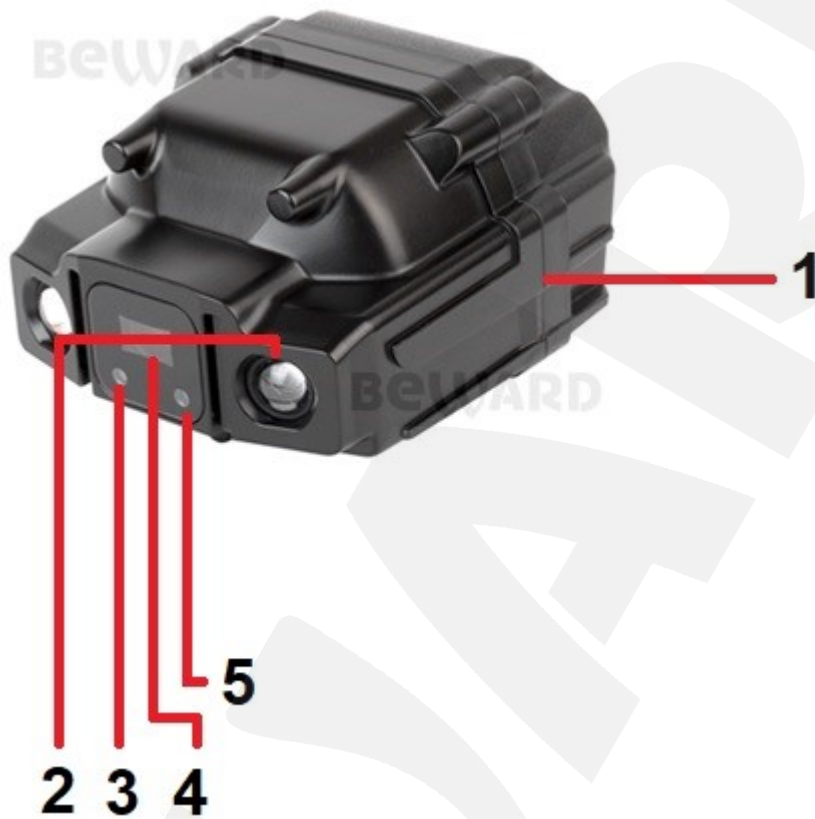


Рис. 3.1

Корпус камеры (1)

ИК-подсветка (2): в темное время суток, при недостаточной освещенности камера переходит в режим «Ночь» и включается ИК-подсветка, которая позволяет вести видеонаблюдение даже в полной темноте. ИК-подсветка является альтернативой стандартному освещению, но при этом она мало заметна окружающим.

Светодиодный индикатор (3) предназначен для отображения одного из трёх режимов работы видеокамеры при работе с облачным сервисом DoorHan:

1. **Мигает зеленый:** режим чтения QR кода
2. **Горит зеленый:** QR код прочитан, в ожидании подключения Wi-Fi и/или VPN
3. **Выключен:** режим распознавания номеров, VPN подключен

Объектив (4) предназначен для проецирования оптического изображения на матрицу видеокамеры.

Датчик света (5): фотоэлемент, предназначенный для автоматического перехода камеры из режима «День» в режим «Ночь» и обратно.

Глава 4. Установка и подключение IP-камеры

4.1. Рекомендации по установке

В данном разделе приведен список рекомендаций, которые необходимо учитывать при монтаже IP-камер BFM2530-LP(E).

IP-видеокамеры BFM2530-LP(E) устанавливаются внутрь вставки BIN-LPx, установленной в шлагбауме DoorHan Barrier-PRO или Barrier-PRO-RPD с помощью быстрозажимного шасси (см. пункт [4.2](#))

Описание граничных условий применения IP-камеры:

- Отклонение оси объектива видеокамеры от направления движения транспортного средства не должно превышать 50 градусов по горизонтальной оси (см. рисунок 4.1).
- Расстояние от камеры до области распознавания автономеров должно быть как можно меньше, и не должно превышать 5 метров (см. рисунок 4.1).



Рис. 4.1

- В частном случае, при виде повороте машины справа к шлагбауму, длина прямого участка дороги должна быть не менее 6 метров. При повороте машины слева полоса движения и поворот могут находиться на любой расстоянии от шлагбаума (см. рисунок 4.2).



Рис. 4.2

- Максимальная ширина проезда не должна превышать 6 метров.
- IP-камеры BEWARD BFM2530-LP(E) предназначены для осуществления видеонаблюдения с предельной температурой эксплуатации от -40 до +40 °С.

4.2. Монтаж IP камер

IP-видеокамеры BFM2530-LP(E) устанавливаются внутрь вставки BIN-LPx, предназначенной для установки в шлагбаумах DoorHan Barrier-PRO или Barrier-PRO-RPD, с помощью быстрозажимного шасси. Для установки выполните следующие действия:

Шаг 1: установите вставку BIN-LPx в шлагбаум (см. руководство по монтажу BIN-LPx)

Шаг 2: отключите питание шлагбаума 220В.

Шаг 3: снимите верхнюю крышку шлагбаума Barrier-PRO или Barrier-PRO-RPD с установленной вставкой BIN-LPx. Для этого необходимо с помощью специального ключа из комплекта поставки шлагбаума открыть его боковую крышку, отвернуть 3 винта крепления крышки шестигранным ключом на 3 и, потянув крышку на себя, отсоединить провод сигнальной лампы сверху крышки и снять саму крышку.

Шаг 4: установите видеокамеру внутрь вставки BIN-LPx с помощью быстрозажимного шасси. При демонтаже существующей камеры откройте крышку роутера STWD-210P, отключите кабель RJ-45 от камеры, ослабьте пластиковые направляющие быстрозажимного шасси и, раздвинув их рукой в стороны, потяните видеокамеру внутрь вставки.

Шаг 5: подключите кабель RJ-45 от видеокамеры в порт CAM1 или CAM2 роутера.

Шаг 6: зафиксируйте стяжками кабель от камеры так, чтобы он не соприкасался с подвижными частями механизма шлагбаума.

Шаг 7: закройте крышку роутера.

Шаг 8: включите питание шлагбаума питания 220В.

4.3. Замена карты памяти

ВНИМАНИЕ!

Перед установкой и извлечением карты памяти необходимо отключить питание видеокамеры и демонтировать её. Замена карты памяти должна осуществляться в сухом и теплом помещении. Горячая замена карты памяти не поддерживается видеокамерой и может привести к повреждению оборудования и потере данных.

Для установки/извлечения карты памяти выполните следующие действия:

Шаг 1: открутите 4 винта и снимите заднюю часть разъемного корпуса камеры (см. рисунок 4.3)



Рис. 4.3

Шаг 2: Слот карты памяти находится на шлейфе рядом с герметичным отверстием для ввода кабеля (см. рисунок 4.4). Для извлечения карты памяти нажмите на её торец до щелчка, и пружинный механизм вытолкнет карту из слота. Для установки карты памяти вставьте её в слот до щелчка.

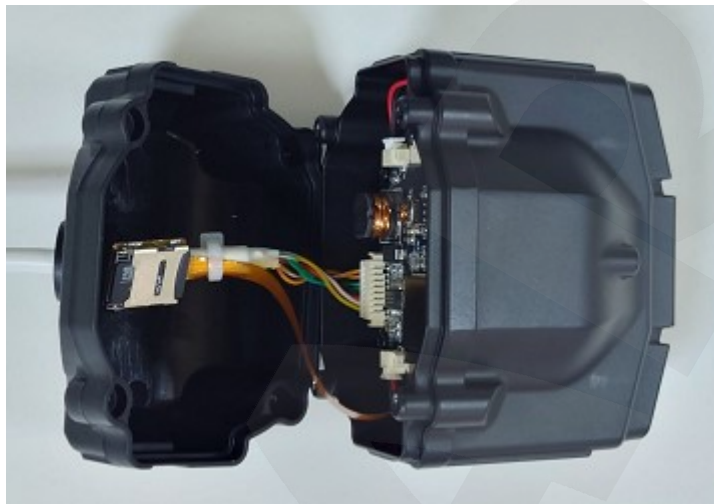


Рис. 4.4

Шаг 3: установите заднюю часть разъемного корпуса камеры на место и закрутите 4 винта.

4.4. Варианты использования ПО видеонаблюдения

Камеры распознавания номеров BFM2530-LP(E) возможно использовать с одним из нескольких видео программного обеспечения:

- 1) Настройка и администрирование через облачный сервис мобильного приложения DoorHan. Камеры по-умолчанию находятся в режиме чтения QR-кодов. Добавление камер в аккаунт пользователя в мобильном приложении происходит с помощью чтения камерами QR-кода, генерируемого в приложении. После этого камеры переходят в режим распознавания (детектирования) номеров. **В этом способе отсутствует необходимость настройки IP адресов, знания сетевых технологий и использования компьютера.** При этом, для первоначальной настройки, редактирования белого списка номеров и получения информации с камер, например, журнал проезда, на камерах требуется наличие интернета. Скачивайте приложение DoorHan из Google Play или AppStore и смотрите пошаговые инструкции по настройке и использованию камеры в самом приложении.
- 2) Настройка и администрирование через веб интерфейс. Данный способ не требует наличия интернета для камер, но требуется наличия компьютера и знания основ сетевых технологий. Настройка и эксплуатация через веб-интерфейс описаны в руководстве по эксплуатации на данную камеру.

ВНИМАНИЕ!

При эксплуатации камеры через веб интерфейс требуется отключить облачный сервис DoorHan в настройках камеры, иначе распознавание номеров не будет работать.

- 3) Дополнительно, камеру BFM2530-LP после выполнения первоначальной настройки через веб интерфейс возможно подключить к облачному серверу мобильного приложения BEWARD Intercom для администрирования базы номеров с мобильного телефона. Скачивайте приложение BEWARD Intercom из Google Play или AppStore или с [сайта BEWARD](#). Там же вы найдете инструкции к данному приложению.

ВНИМАНИЕ!

Для обеспечения возможности работы камеры через приложение BEWARD Intercom требуется выбрать облачный сервис = Cloud P2P в настройках камеры, иначе распознавание номеров не будет работать.

4.5. Сброс настроек видеокамеры

Для сброса настроек камеры в заводские установки необходимо в течение десяти секунд зажать кнопку, расположенную на кабеле IP-камеры.

ВНИМАНИЕ!

После сброса настроек камера перейдёт в режим чтения QR-кодов приложения DoorHan и будет удалена из аккаунта в мобильном приложении.

Глава 5. Настройка проводного соединения

При использовании видеокamеры через веб-интерфейс для того, чтобы IP-камера BFM2530-LP(E) работала в вашей локальной сети совместно с другим оборудованием, необходимо выполнить ее подключение в соответствии с текущими настройками данной сети, для чего, в свою очередь, необходимо определить эти настройки.

ПРИМЕЧАНИЕ!

Описание установки и настройки соединения для Windows 7 выполнено на примере Windows 7 Максимальная. Вследствие этого, названия некоторых пунктов меню и функций могут отличаться от Вашей версии Windows, однако алгоритм приведенных действий является универсальным.

5.1. Определение параметров проводной локальной сети

В случае подключения по кабелю Ethernet необходимо определить текущие настройки проводной сети.

Для доступа к текущим настройкам проводной локальной сети используйте компьютер, подключенный к этой сети. Нажмите **Пуск – Панель управления** (Рис. 5.1).

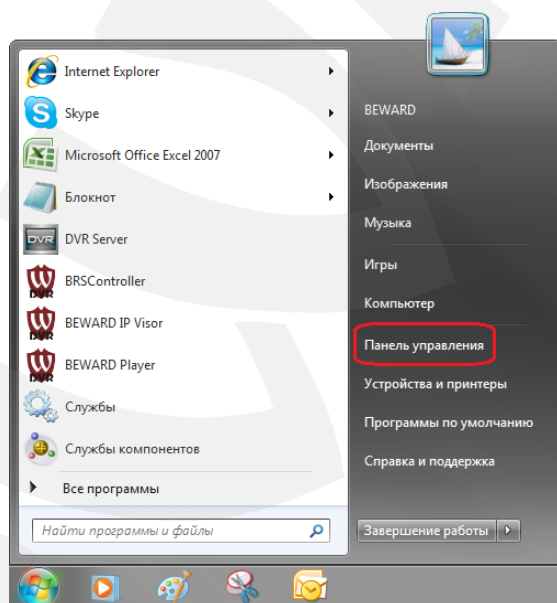


Рис. 5.1

В открывшемся диалоговом окне выберите пункт **[Просмотр состояния сети и задач]** в разделе **[Сеть и Интернет]** (Рис. 5.2).

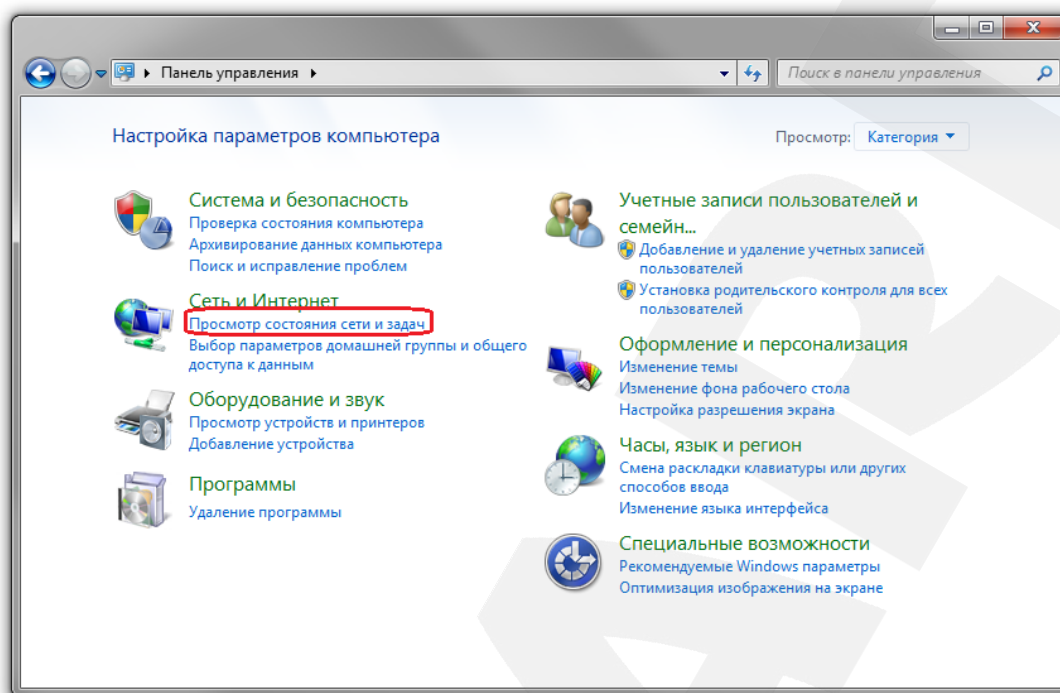


Рис. 5.2

В открывшемся диалоговом окне нажмите **[Подключение по локальной сети]** (Рис. 5.3).

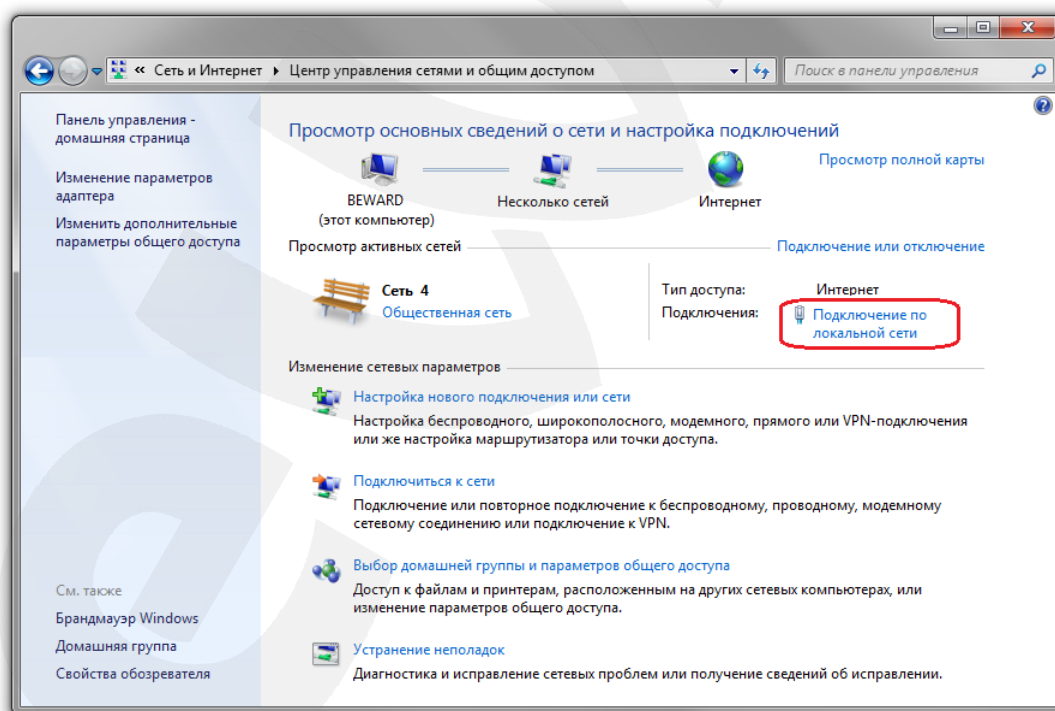


Рис. 5.3

ПРИМЕЧАНИЕ!

При наличии нескольких подключений выберите то, к которому планируется подключить IP-камеру.

В открывшемся окне нажмите кнопку **[Свойства]** (Рис. 5.4).

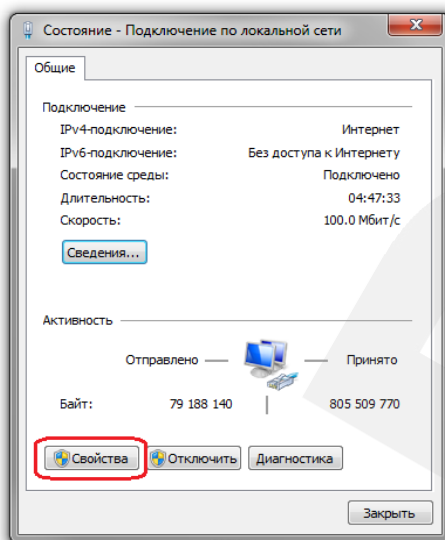


Рис. 5.4

В диалоговом окне свойств сетевого подключения необходимо выбрать пункт [Протокол Интернета версия 4 (TCP/IPv4)] и нажать кнопку [Свойства] (Рис. 5.5).

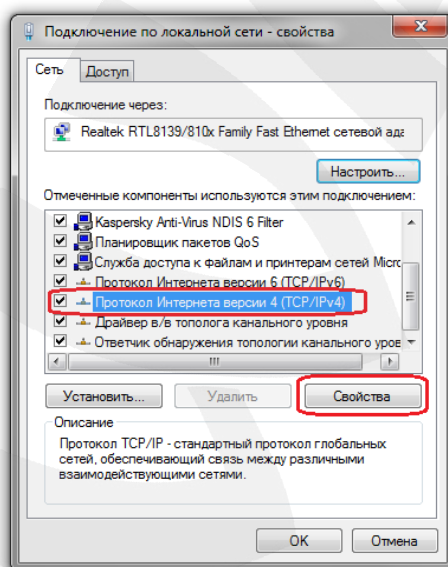


Рис. 5.5

Откроется окно, в котором отображается информация о настройках сетевого подключения. Возможны два варианта настройки IP-адреса сетевого подключения Вашего ПК:

1. Получить IP-адрес автоматически: IP-адрес назначается автоматически DHCP-сервером (Рис. 5.6). Если IP-адрес Вашему ПК выдается автоматически, тогда для определения параметров локальной сети перейдите к пункту [5.1.1](#) данного Руководства.

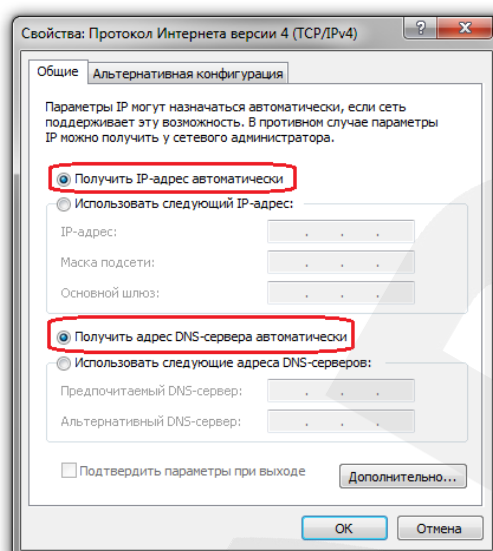


Рис. 5.6

2. Использовать следующий IP-адрес: IP-адрес задается пользователем вручную (Рис. 5.7):

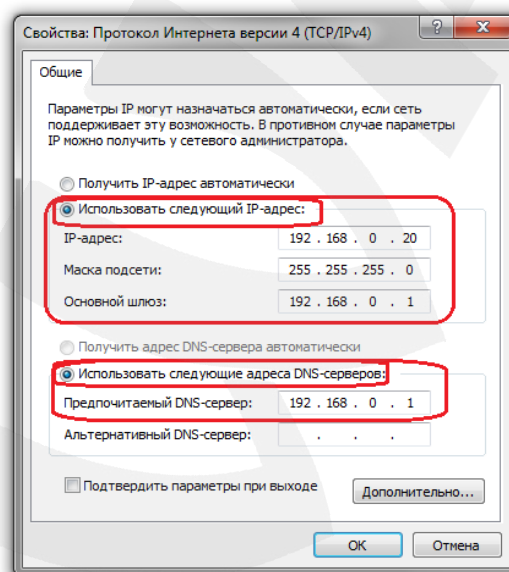


Рис. 5.7

Запишите, либо запомните параметры сетевого адаптера Вашего ПК (IP-адрес, Маска подсети, Основной шлюз, DNS-сервер).

ВНИМАНИЕ!

Если Вы не записали сетевые параметры компьютера, то после настройки камеры будет невозможно вернуть их в первоначальное состояние для восстановления подключения к локальной сети и/или сети Интернет.

5.1.1. Определение параметров сети при динамическом IP-адресе

ПРИМЕЧАНИЕ!

Данный пункт Руководства предназначен для определения параметров локальной сети при назначении IP-адреса Вашему ПК автоматически (DHCP-сервером).

Для определения текущих настроек компьютера в локальной проводной сети нажмите **Пуск – Панель управления** (Рис. 5.8).

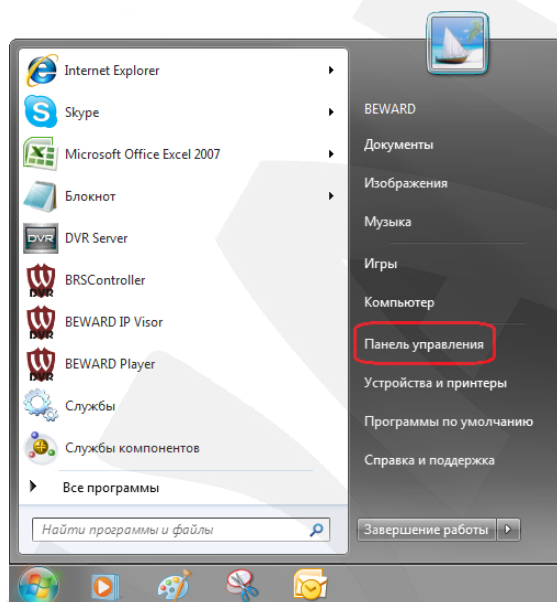


Рис. 5.8

В открывшемся диалоговом окне выберите пункт **[Просмотр состояния сети и задач]** в разделе **[Сеть и Интернет]** (Рис. 5.9).

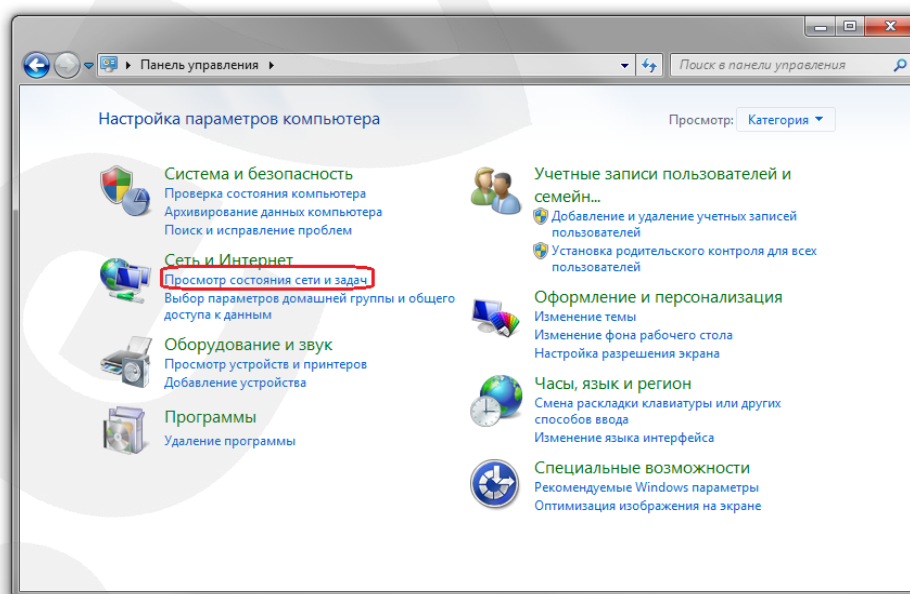


Рис. 5.9

В открывшемся диалоговом окне нажмите **[Подключение по локальной сети]** (Рис. 5.10).

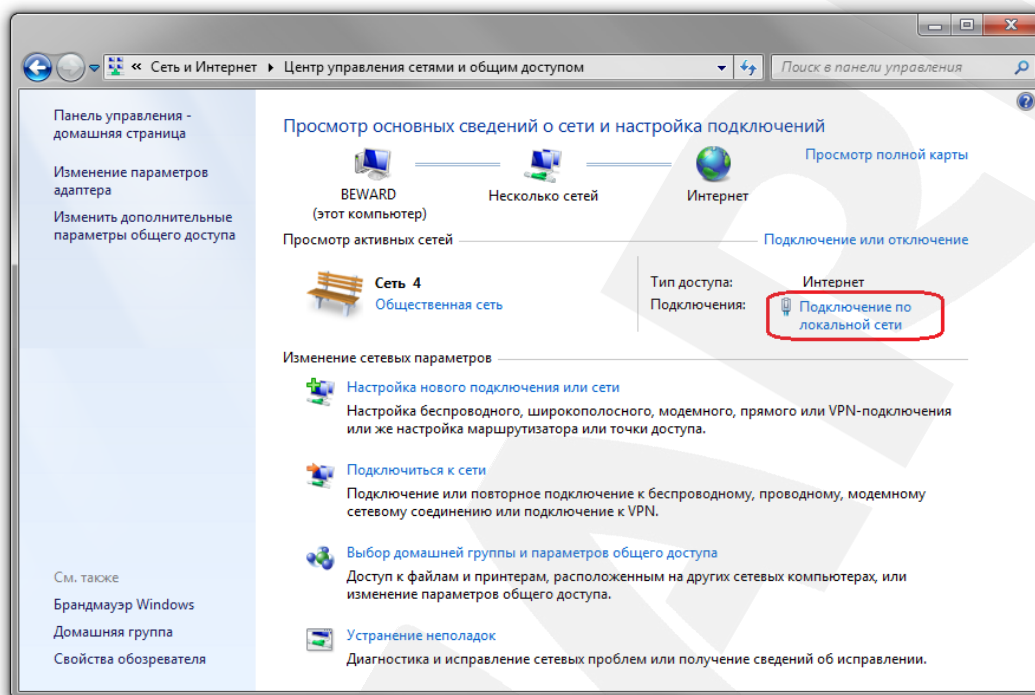


Рис. 5.10

ПРИМЕЧАНИЕ!

При наличии нескольких сетевых подключений выберите то, к которому планируется подключить IP-камеру.

В открывшемся окне нажмите кнопку **[Сведения]** (Рис. 5.11).

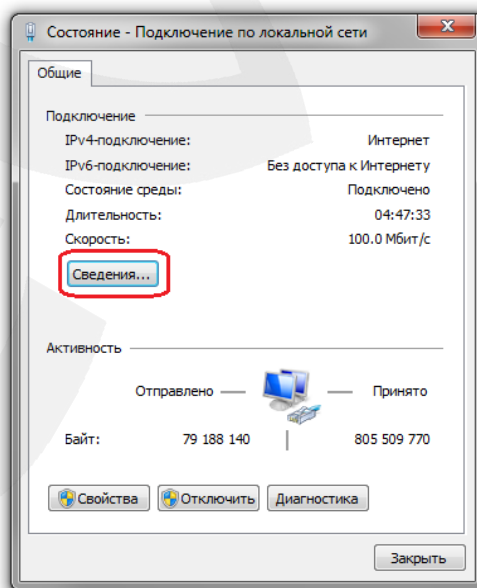


Рис. 5.11

В окне «Сведения о сетевом подключении» представлена следующая информация (Рис. 5.12):

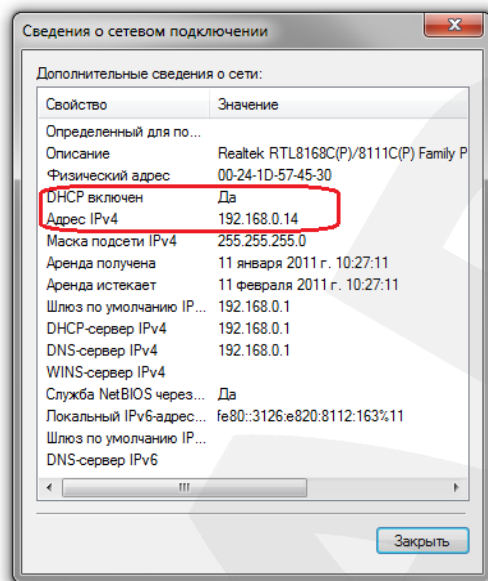


Рис. 5.12

Если в этом окне Вы увидели строки – **«DHCP включен - Да»**, **«Адрес IPv4 - xxx.xxx.xxx.xxx»** (где «xxx.xxx.xxx.xxx» – значение IP-адреса), – значит IP-адрес Вашему ПК назначен автоматически. Маска подсети указана в строке **[Маска подсети IPv4]**, адрес сетевого шлюза – в строке **[Шлюз по умолчанию IPv4]**, адрес DNS-сервера – в строке **[DNS-сервер IPv4]**. Запишите, либо запомните данные параметры (IP-адрес, Маска подсети, Сетевой шлюз, DNS-сервер).

ВНИМАНИЕ!

Если Вы не записали сетевые параметры компьютера, то после настройки камеры будет невозможно вернуть их в первоначальное состояние для восстановления подключения к локальной сети и/или сети Интернет.

ВНИМАНИЕ!

Если в окне **«Сведения о сетевом подключении»** Вы увидели строки:

«DHCP включен - Да»; «IPv4-адрес автонастройки - xxx.xxx.xxx.xxx», (где xxx.xxx.xxx.xxx – значение IP-адреса), – значит Вам не удалось подключиться к проводной сети (DHCP-сервер не присвоил IP-адрес Вашему ПК). Проверьте правильность подключения к проводной сети. В случае необходимости, обратитесь к Вашему системному администратору.

5.2. Изменение параметров локальной сети для подключения к IP-камере

По умолчанию IP-камера BFM2530-LP(E) имеет IP-адрес 192.168.0.99. Чтобы подключиться к камере для первоначальной настройки необходимо, чтобы Ваш компьютер находился в той же подсети, что и камера. При этом IP-адреса камер, компьютеров и любых других устройств в сети не должны совпадать между собой.

ВНИМАНИЕ!

Если Вы планируете подключить несколько IP-камер в сети без DHCP сервера, то для исключения конфликта IP-адресов подключайте камеры по одной и изменяйте их IP-адреса на любые свободные в Вашей локальной сети.

ВНИМАНИЕ!

Если Вы уверены, что Ваш ПК, подключенный к проводной сети, и IP-камера, физически подключенная к той же сети, либо напрямую к Вашему ПК, находятся в одной подсети, Вы можете сразу перейти к пункту [5.3](#) данного Руководства.

Для изменения текущих настроек компьютера в локальной проводной сети нажмите **Пуск – Панель управления** (Рис. 5.13).

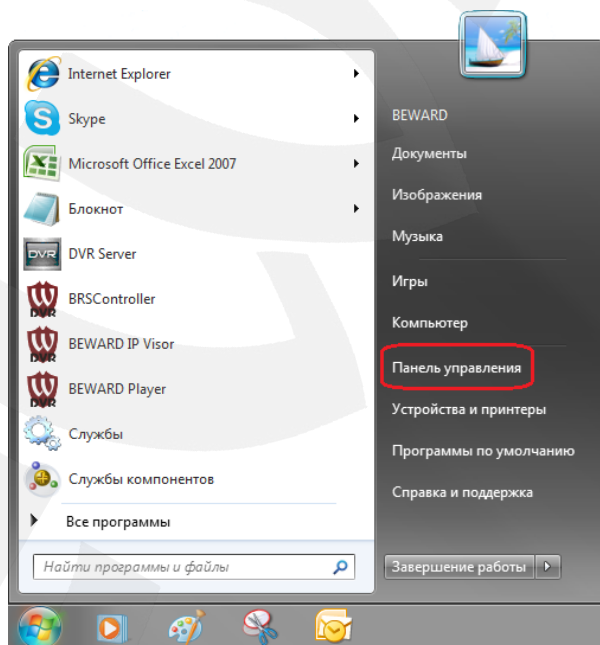


Рис. 5.13

В открывшемся диалоговом окне выберите пункт **[Просмотр состояния сети и задач]** в разделе **[Сеть и Интернет]** (Рис. 5.14).

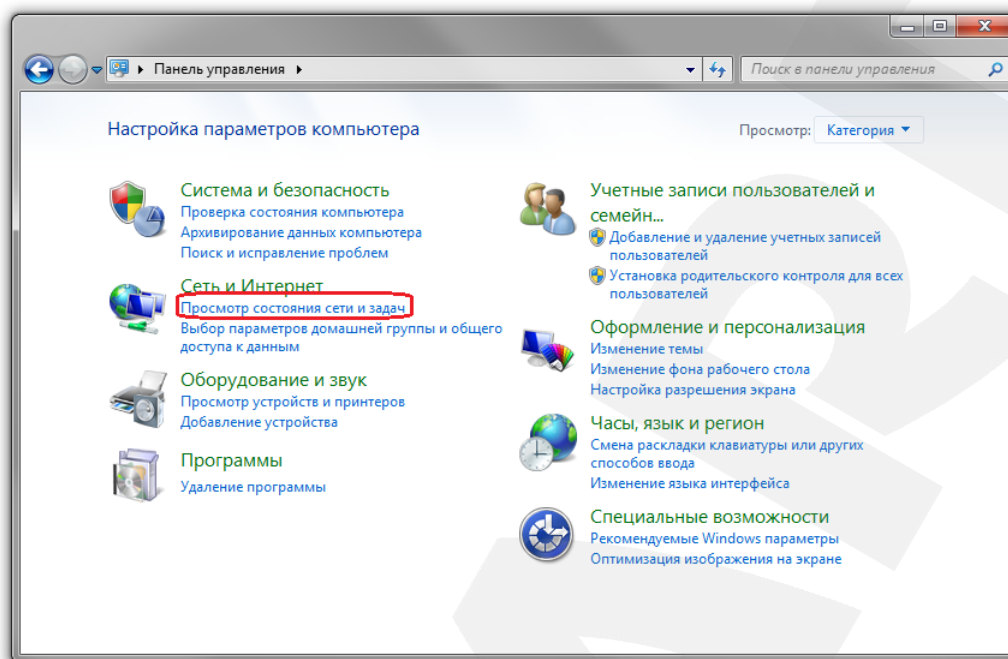


Рис. 5.14

В открывшемся окне нажмите «Подключение по локальной сети» (Рис. 5.15).

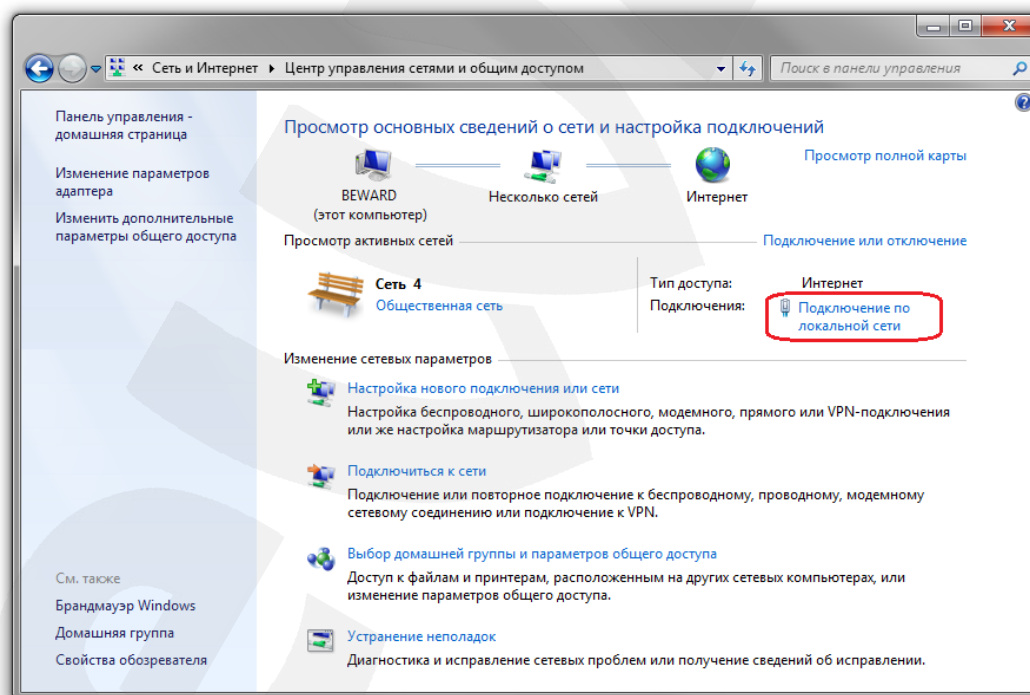


Рис. 5.15

ПРИМЕЧАНИЕ!

При наличии нескольких сетевых подключений выберите то, к которому планируется подключить IP-камеру.

В открывшемся окне нажмите кнопку **[Свойства]** (Рис. 5.16).

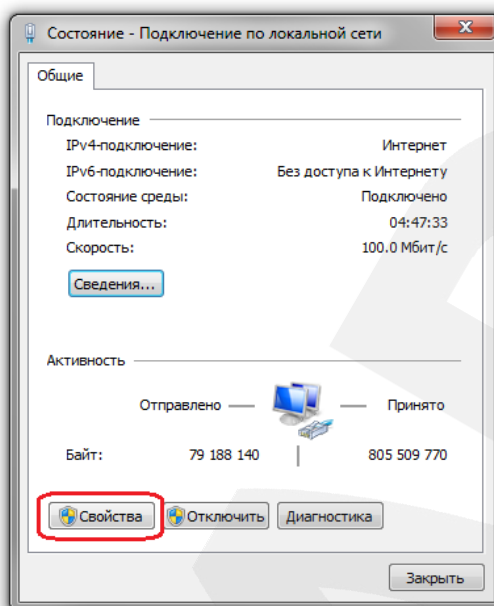


Рис. 5.16

В открывшемся окне свойств сетевого подключения необходимо выбрать пункт **[Протокол Интернета версия 4 (TCP/IPv4)]** и нажать кнопку **[Свойства]** (Рис. 5.17).

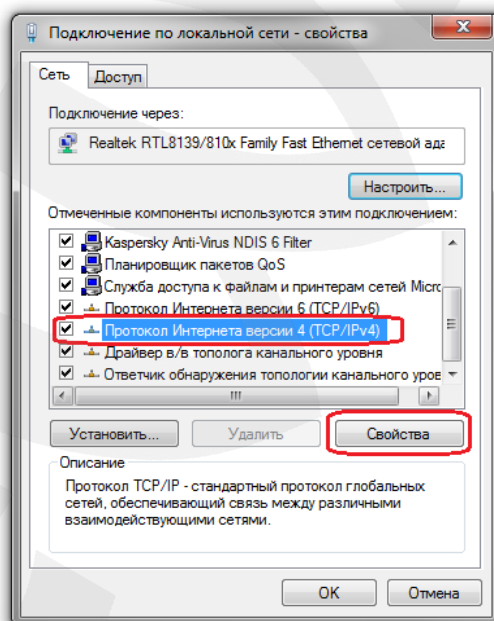


Рис. 5.17

В появившемся окне необходимо установить значения IP-адреса и маски подсети. Выберите пункт **[Использовать следующий IP-адрес]** и введите свободный **IP-адрес** из подсети камеры, например **192.168.0.20**, и **Маску подсети** – **255.255.255.0**. Остальные значения вводить нет необходимости (Рис. 5.18).

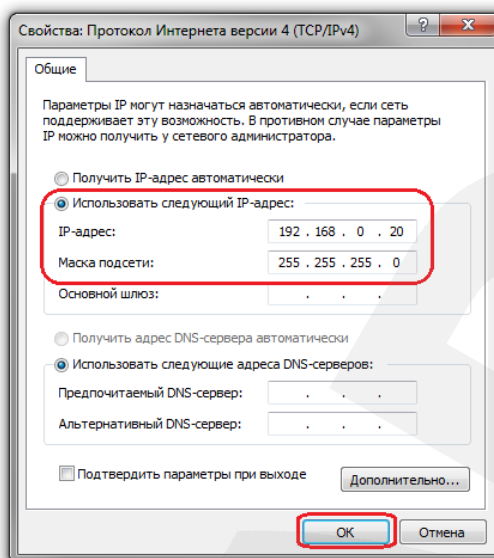


Рис. 5.18

Для применения изменений настроек нажмите кнопку **[OK]** во всех открытых окнах.

5.3. Получение доступа к IP-камере с помощью браузера

ВНИМАНИЕ!

IP-адрес видеокamеры по умолчанию присваивается по DHCP. Адрес автонастройки в сети без DHCP сервера – 192.168.0.99, HTTP-порт по умолчанию – 80 и в запросе не указывается.

Текущий адрес IP-видеокamеры вы можете определить с помощью функции сетевого обнаружения Windows (Рис. 5.19). Альтернативным способом является использование ПО Beward IP Searcher.

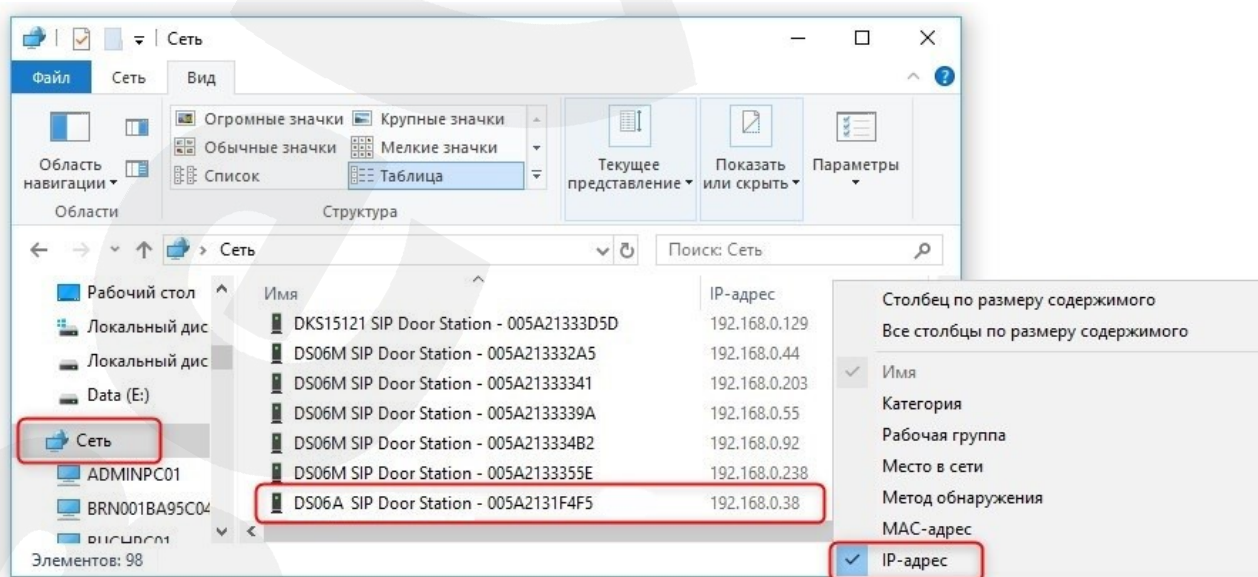


Рис. 5.19

Запустите браузер Google Chrome, в адресной строке введите запрос вида: **http://<IP>:<PORT>**, где **<IP>** - IP-адрес устройства, **<PORT>** - HTTP-порт устройства (Рис. 5.20).

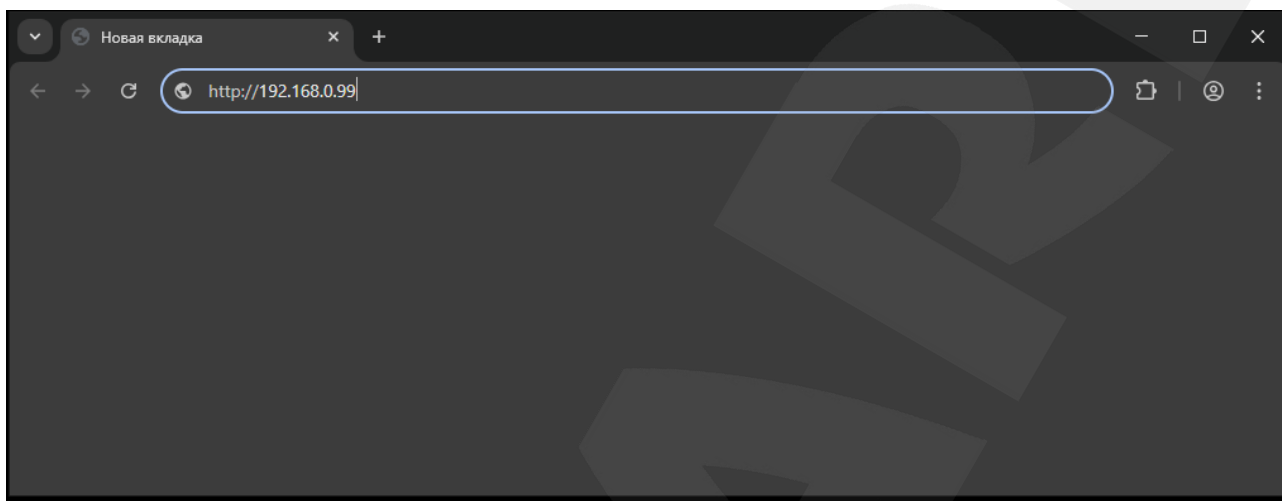


Рис. 5.20

5.4. Получение доступа к веб-интерфейсу IP-камеры

После загрузки страницы веб-интерфейса камеры при помощи браузера Google Chrome Вы увидите окно авторизации. Введите имя пользователя и пароль. По умолчанию используется имя пользователя – **admin**, пароль по умолчанию – **admin** (Рис. 5.21).

ВНИМАНИЕ!

Вы можете изменить имя пользователя и пароль в меню **Настройки – Системные – Пользователи**. В случае утери пароля или имени пользователя устройство можно вернуть к заводским установкам. Этого необходимо нажать кнопку сброса в течении 10 секунд.

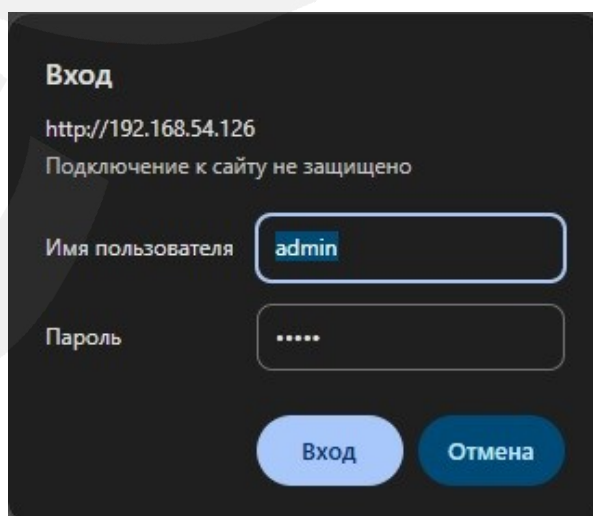


Рис. 5.21

После успешной авторизации Вы получите доступ к веб-интерфейсу IP-камеры (Рис. 5.22).

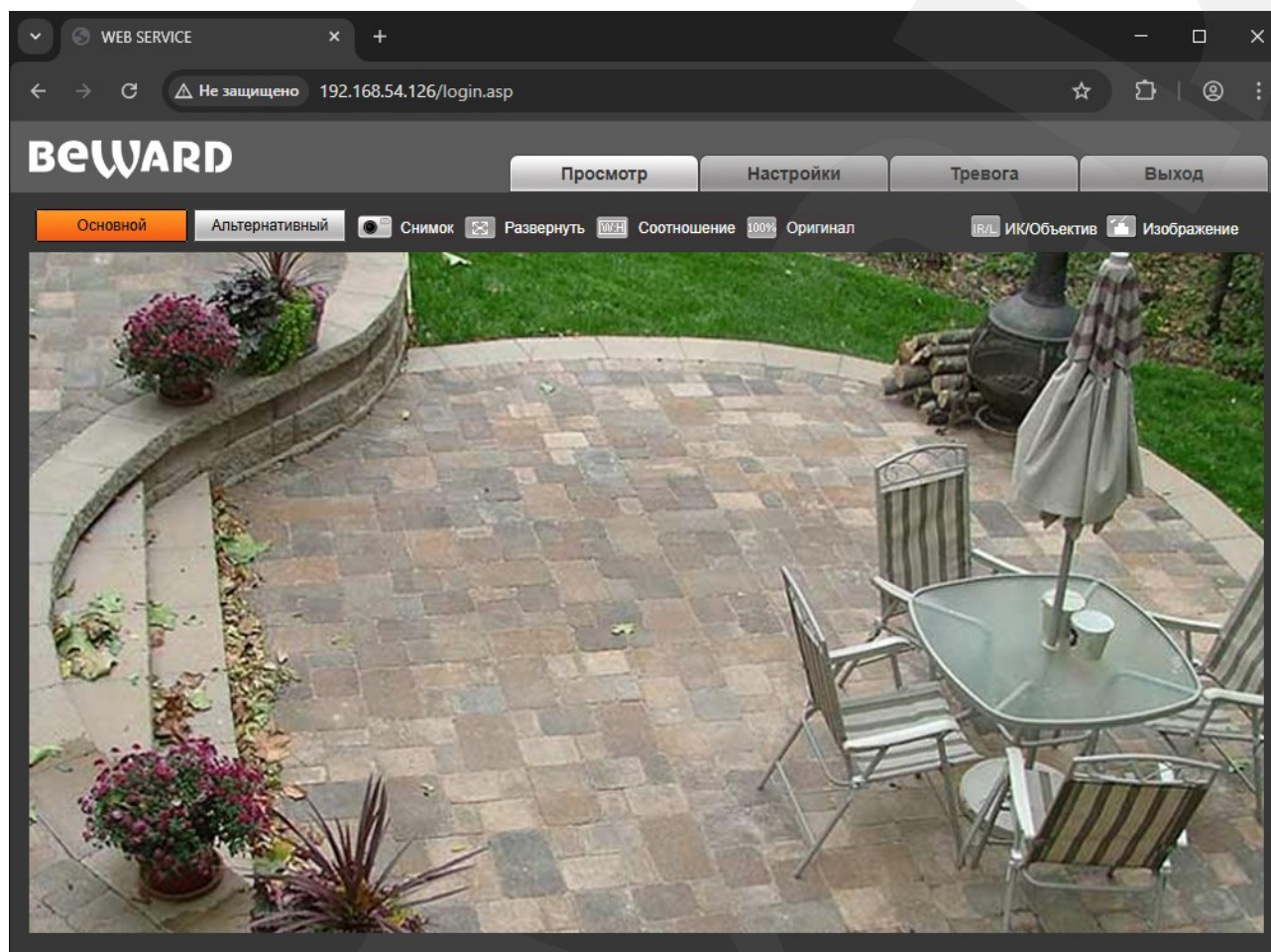


Рис. 5.22

5.5. Изменение настроек подключения IP-камеры через веб-интерфейс

После подключения к IP-камере необходимо изменить ее настройки таким образом, чтобы она находилась в одной подсети с остальным оборудованием.

ВНИМАНИЕ!

Для совместной работы нескольких устройств в одной подсети необходимо, чтобы у них совпадали **первые три** части (октета) IP-адреса, и полностью совпадала маска подсети.

Например, IP-адрес Вашего ПК: 192.168.1.100. IP-адрес разделен точками на четыре октета. В данном примере: 1 октет – 192, 2 октет – 168, 3 октет – 1, 4 октет – 100. Вам необходимо изменить IP-адрес камеры так, чтобы их первые три октета совпадали, то есть IP-адрес камеры должен иметь вид: 192.168.1.XX. Четвертый октет IP-адреса каждого устройства обязательно должен быть индивидуальным.

Для изменения сетевых настроек в веб-интерфейсе нажмите в главном меню камеры кнопку **[Настройка]** и перейдите в меню **Сеть – LAN** (Рис. 5.23).

BEWARD

Просмотр Настройки Тревога Выход

Видео

Сеть

- Основные
- LAN**
- WatchDog IP
- PPPoE
- UPnP
- Bonjour
- E-mail
- FTP
- NAS
- DDNS
- PPTP
- RTSP
- HTTPS
- Cloud
- Уведомление

Запись

Тревога

Системные

База номеров

Настройка LAN

Использовать IPv6 ☐

Версия IP IPv4

Получить автоматически ☒

DHCP Release ☐

IP-адрес 192.168.54.126

Маска подсети 255.255.254.0

Основной шлюз 192.168.55.1

Получить автоматически ☒

Предпочитаемый DNS 192.168.55.1

Альтернативный DNS 0.0.0.0

MAC-адрес 18-68-82-33-84-F3

Проверка сети

Проверить адрес Ping

Сохранить

Рис. 5.23

В полях **[IP-адрес]**, **[Маска подсети]**, **[Основной шлюз]**, **[Предпочитаемый DNS]**, **[Альтернативный DNS]** нужно ввести такие значения, чтобы камера попала в одну подсеть с остальным оборудованием (Рис. 5.29). Для этого обратитесь к ранее записанным, текущим настройкам проводной локальной сети (см. пункты [5.1](#) или [5.1.1](#)) и, в соответствии с ними, установите вышеуказанные параметры.

ПРИМЕЧАНИЕ!

В случае необходимости, для настройки сетевых параметров устройств обратитесь к Вашему сетевому администратору.

Для применения изменений сетевых настроек камеры нажмите кнопку **[Сохранить]**, после чего появится уведомление о перезагрузке устройства.

После перезагрузки, IP-камера будет доступна по заданному Вами IP-адресу. На этом настройка проводного подключения IP-камеры завершена.

5.6. Возврат настроек подключения ПК в первоначальные значения

Чтобы вернуть значения проводного сетевого подключения к установленным ранее значениям, выполните следующие действия.

Нажмите **Пуск – Панель управления** (Рис. 5.24).

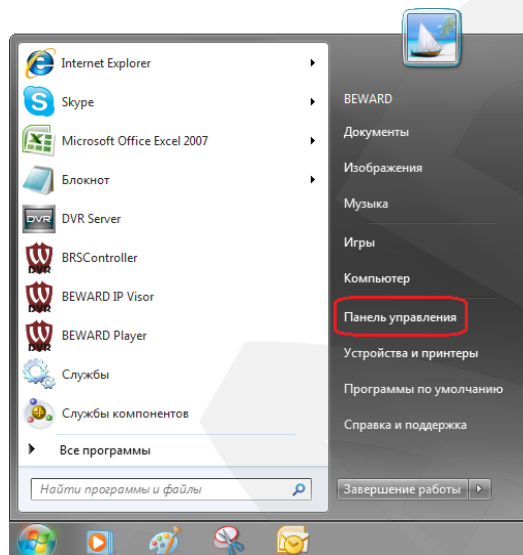


Рис. 5.24

В открывшемся диалоговом окне выберите пункт **[Просмотр состояния сети и задач]** в разделе **[Сеть и Интернет]** (Рис. 5.25).

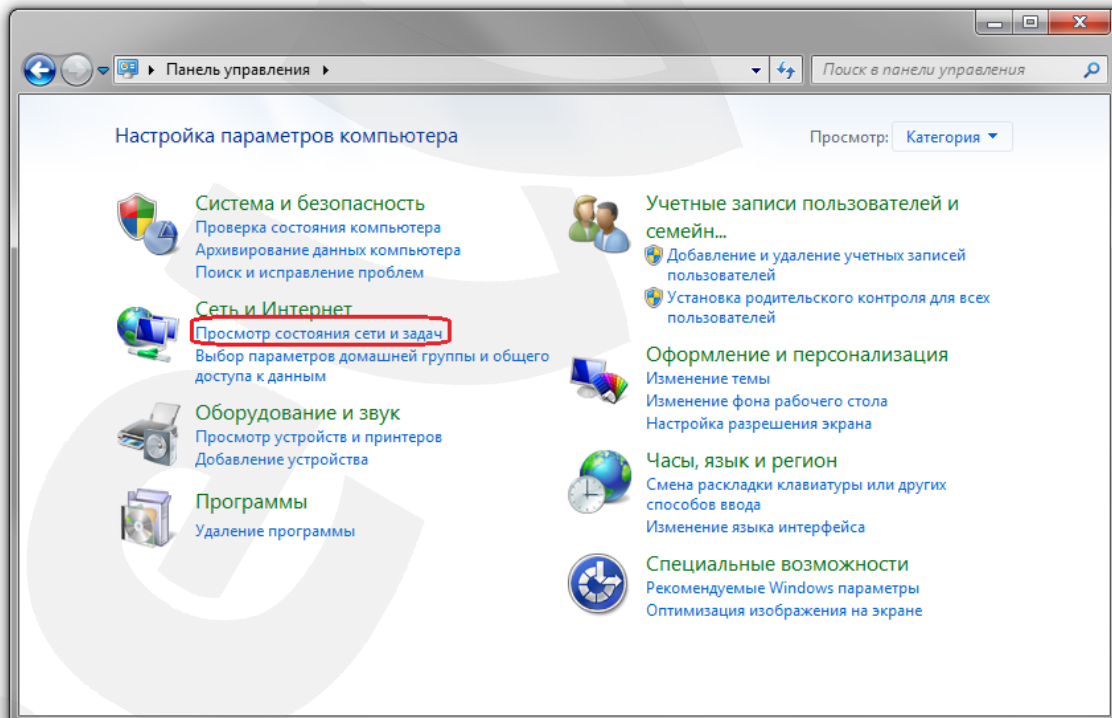


Рис. 5.25

В открывшемся окне нажмите **[Подключение по локальной сети]** (Рис. 5.26).

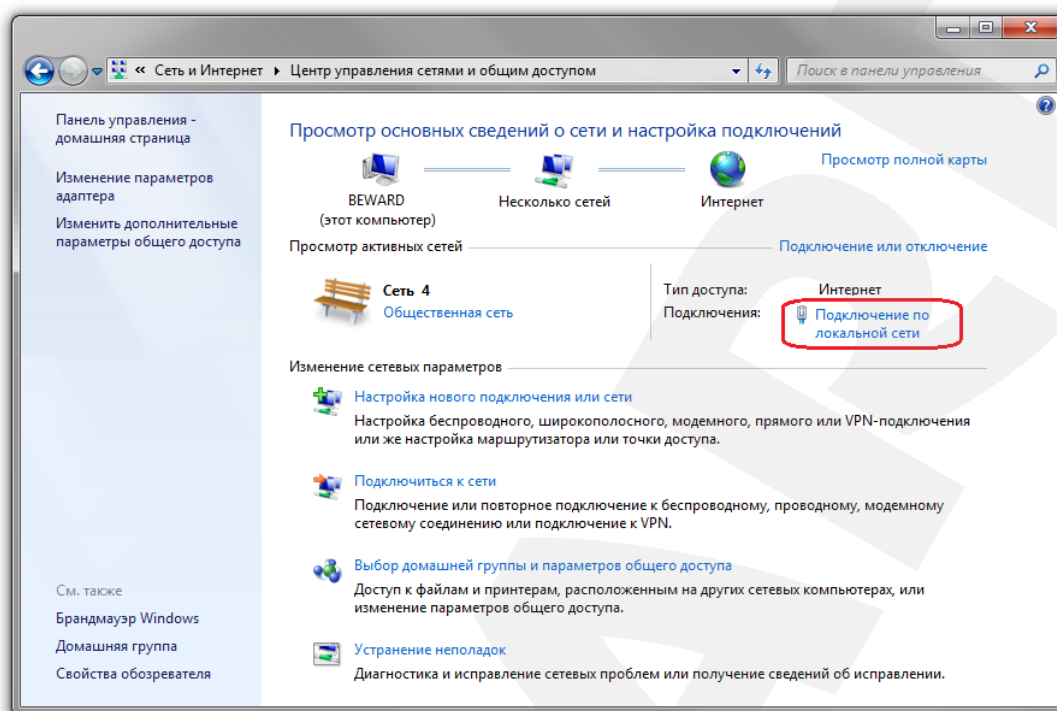


Рис. 5.26

В открывшемся окне нажмите кнопку **[Свойства]** (Рис.5.27).

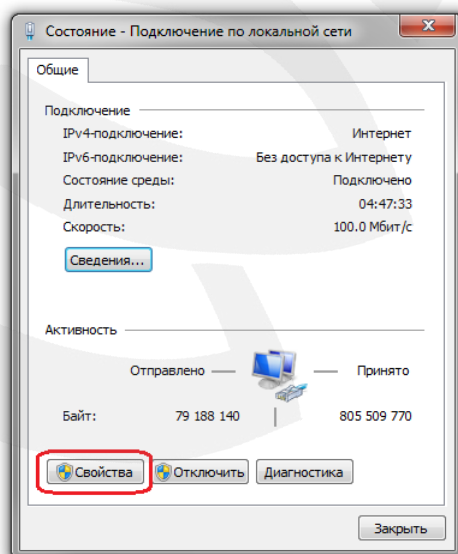


Рис. 5.27

В открывшемся окне свойств сетевого подключения необходимо выбрать пункт **[Протокол Интернета версия 4 (TCP/IPv4)]** и нажать кнопку **[Свойства]** (Рис. 5.28).

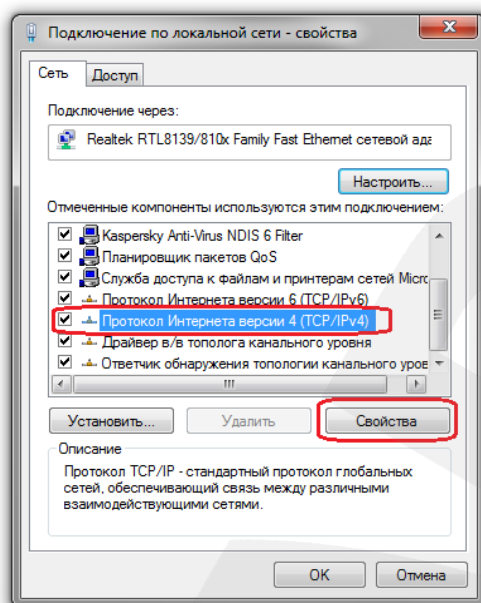


Рис. 5.28

Откроется меню, в котором необходимо установить значения начальных настроек, записанных вами ранее (см. пункты [5.1](#), [5.1.1](#) данного Руководства).

Если изначально IP-адрес Вашему ПК назначался автоматически, тогда выберите пункты **[Получить IP-адрес автоматически]** и **[Получить адрес DNS-сервера автоматически]**, после чего нажмите кнопку **[ОК]** для всех открытых окон (Рис. 5.29).

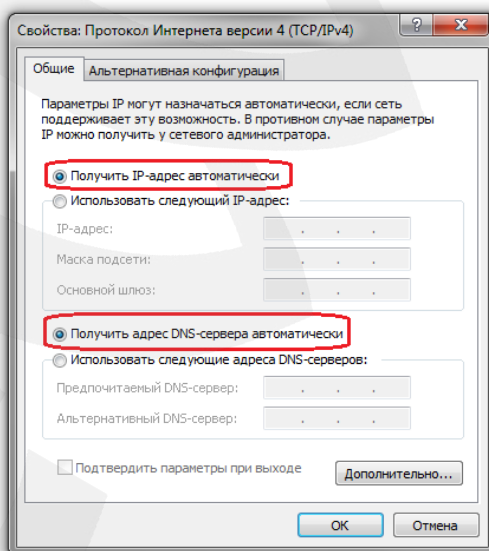


Рис. 5.29

Если изначально IP-адрес Вашему ПК был задан вручную, тогда выберите пункт **[Использовать следующий IP-адрес]** и заполните необходимые поля (см. пункт [5.1](#) данного Руководства), после чего нажмите кнопку **[ОК]** для всех открытых окон (Рис. 5.30).

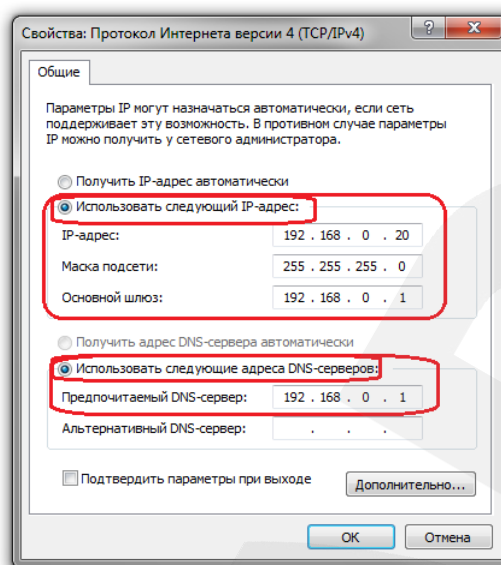


Рис. 5.30

5.7. Проверка правильности настроек подключения IP-камеры к локальной сети

Для контроля правильности сетевых настроек камеры и компьютера нужно подключиться к камере через браузер Google Chrome.

Запустите браузер Google Chrome. Для этого нажмите **Пуск** и выберите строку **[Google Chrome]**.

Введите в адресной строке IP-адрес, присвоенный камере (например: `http://192.168.0.99`) (Рис. 5.31).

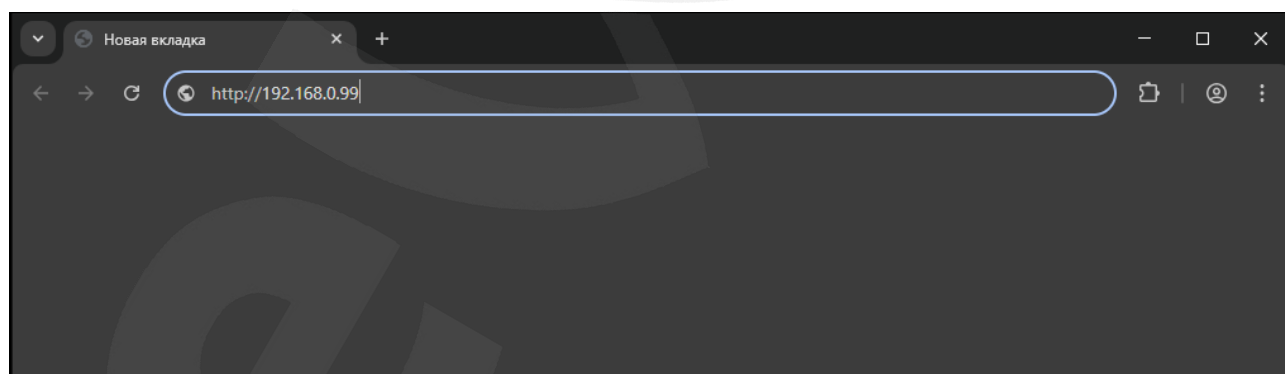


Рис. 5.31

При правильных настройках откроется окно авторизации. Для авторизации введите имя пользователя и пароль, после чего нажмите **[OK]** (Рис. 5.32).

ВНИМАНИЕ!

Имя пользователя по умолчанию: **admin**. Пароль по умолчанию: **admin**.

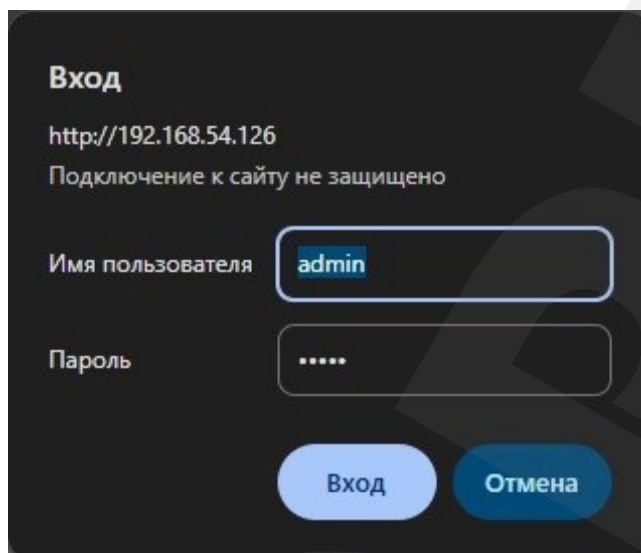


Рис. 5.32

При правильно выполненных действиях Вы сможете зайти в веб-интерфейс через браузер и увидеть изображение с Вашей IP-камеры (Рис. 5.33).

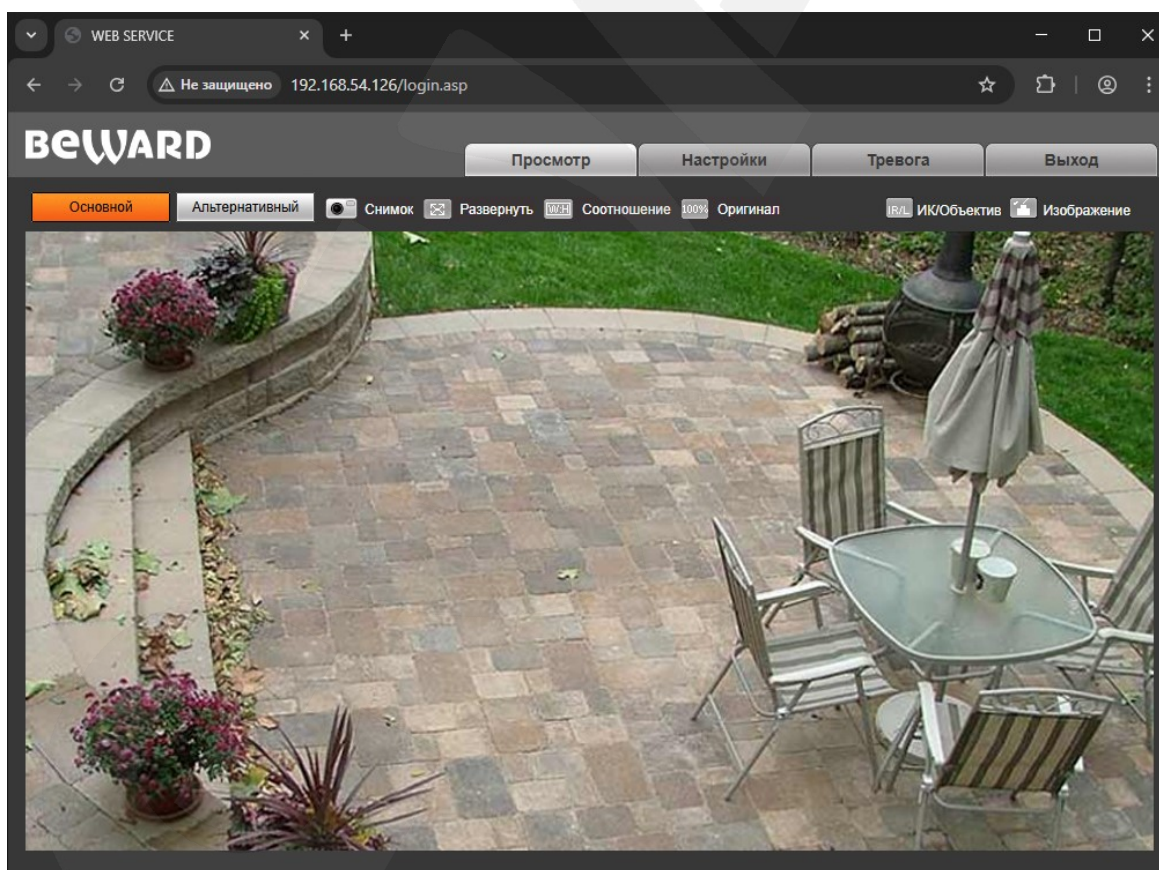


Рис. 5.33

ПРИМЕЧАНИЕ!

В случае неудачного соединения с камерой, проверьте правильность подключения к проводной сети, вернитесь в [начало](#) данной главы и повторите настройку. В случае необходимости обратитесь к Вашему системному администратору.

Приложения

Приложение А. Заводские установки

Ниже приведены некоторые значения заводских установок.

Наименование	Значение
DHCP	Включено
IP-адрес	192.168.0.99
Маска подсети	255.255.255.0
Шлюз	192.168.0.1
Имя пользователя (администратора)	admin
Пароль (администратора)	admin
HTTP-порт	80
Порт данных	5000
RTSP-порт	554
SMTP-порт	25
ONVIF-порт	80
NTP-сервер	time.nist.gov time.windows.com time-nw.nist.gov time-a.nist.gov time-b.nist.gov

Приложение В. Гарантийные обязательства

В1. Общие сведения

а) Перед подключением оборудования необходимо ознакомиться с Руководством по эксплуатации.

б) Для повышения надежности работы оборудования, защиты от бросков в питающей сети и обеспечения бесперебойного питания следует использовать сетевые фильтры и устройства бесперебойного питания.

В2. Электромагнитная совместимость

Это оборудование соответствует требованиям электромагнитной совместимости EN 55022, EN 50082-1. Напряжение радиопомех, создаваемых аппаратурой, соответствует ГОСТ 30428-96.

В3. Электропитание

Должно соответствовать параметрам, указанным в Руководстве по эксплуатации для конкретного устройства. Для устройств со встроенным источником питания – это переменное напряжение 220 В $\pm 10\%$, частотой 50 Гц $\pm 3\%$. Для устройств с внешним адаптером питания – стабилизированный источник питания 5 В $\pm 5\%$ или 12 В $\pm 10\%$ для устройств с 12-вольтовым питанием. Напряжение пульсаций – не более 0.1 В.

В4. Заземление

Все устройства, имеющие встроенный блок питания, должны быть заземлены путем подключения к специальным розеткам электропитания с заземлением или путем непосредственного заземления корпуса, если на нем предусмотрены специальные крепежные элементы. Заземление электропроводки здания должно быть выполнено в соответствии с требованиями ПУЭ (Правила Устройства Электроустановок). Оборудование с выносными блоками питания и адаптерами также должно быть заземлено, если это предусмотрено конструкцией корпуса или вилки на шнуре питания. Монтаж воздушных линий электропередачи и линий, прокладываемых по наружным стенам зданий и на чердаках, должен быть выполнен экранированным кабелем (или в металлорукаве), и линии должны быть заземлены с двух концов. Причем, если один конец экрана подключается непосредственно к шине заземления, то второй – подключается к заземлению через разрядник.

В5. Молниезащита

Молниезащита должна соответствовать РД 34.21.122-87 "Инструкция по устройству молниезащиты зданий и сооружений" и ГОСТ Р 50571.18-2000, ГОСТ Р 50571.19-2000, ГОСТ Р 50571.20-2000. При прокладке воздушных линий и линий, идущих по наружной стене зданий и по чердачным помещениям, на входах оборудования должны быть установлены устройства молниезащиты.

В6. Температура и влажность

Максимальные и минимальные значения температуры эксплуатации и хранения, а также влажности, Вы можете посмотреть в техническом описании конкретного оборудования. Максимальная рабочая температура – это температура, выше которой не должен нагреваться корпус устройства в процессе длительной работы.

В7. Размещение

Для вентиляции устройства необходимо оставить как минимум по 5 см свободного пространства по бокам и со стороны задней панели устройства. При установке в телекоммуникационный шкаф или стойку должна быть обеспечена необходимая вентиляция. Для этого рекомендуется устанавливать в шкафу специальный блок вентиляторов. Температура окружающего воздуха и вентиляция должны обеспечивать необходимый температурный режим оборудования (в соответствии с техническими характеристиками конкретного оборудования).

Место для размещения оборудования должно отвечать следующим требованиям:

- а) Отсутствие запыленности помещения.
- б) Отсутствие в воздухе паров влаги, агрессивных сред.
- в) В помещении, где устанавливается оборудование, не должно быть бытовых насекомых.
- г) Запрещается размещать на оборудовании посторонние предметы и перекрывать вентиляционные отверстия.

В8. Обслуживание

Оборудование необходимо обслуживать с периодичностью не менее одного раза в год с целью удаления из него пыли. Это позволит оборудованию работать без сбоев в течение продолжительного времени.

В9. Подключение интерфейсов

Оборудование должно подключаться в строгом соответствии с назначением и типом установленных интерфейсов.

В10. Гарантийные обязательства

ООО «НПП «Бевард» не гарантирует, что оборудование будет работать должным образом в различных конфигурациях и областях применения, и не дает никакой гарантии, что оборудование обязательно будет работать в соответствии с ожиданиями клиента при его применении в специфических целях.

ООО «НПП «Бевард» не несет ответственности по гарантийным обязательствам при повреждении внешних интерфейсов оборудования (сетевых, телефонных, консольных и т.п.) и самого оборудования, возникшем в результате:

- а) несоблюдения правил транспортировки и условий хранения;
- б) форс-мажорных обстоятельств (таких как пожар, наводнение, землетрясение и др.);
- в) нарушения технических требований по размещению, подключению и эксплуатации;
- г) неправильных действий при перепрошивке;
- д) использования не по назначению;
- е) механических, термических, химических и иных видов воздействий, если их параметры выходят за рамки допустимых эксплуатационных характеристик, либо не предусмотрены технической спецификацией на данное оборудование;
- ж) воздействия высокого напряжения (удар молнии, статическое электричество и т.п.).

Приложение С. Права и поддержка

С1. Торговая марка

Copyright © BEWARD 2025.

Некоторые пункты настоящего Руководства, а также разделы меню управления оборудования могут быть изменены без предварительного уведомления.

BEWARD является зарегистрированной торговой маркой ООО «НПП «Бевард». Все остальные торговые марки принадлежат их владельцам.

С2. Ограничение ответственности

ООО «НПП «Бевард» не гарантирует, что аппаратные средства будут работать должным образом во всех средах и приложениях, и не дает гарантий и представлений, подразумеваемых или выраженных относительно качества, рабочих характеристик, или работоспособности при использовании в специфических целях. ООО «НПП «Бевард» приложило все усилия, чтобы сделать это Руководство по эксплуатации наиболее точным и полным. ООО «НПП «Бевард» отказывается от ответственности за любые опечатки или пропуски, которые, возможно, произошли при написании данного Руководства.

Информация в любой части Руководства по эксплуатации изменяется и дополняется ООО «НПП «Бевард» без предварительного уведомления. ООО «НПП «Бевард» не берет на себя никакой ответственности за любые погрешности, которые могут содержаться в этом Руководстве. ООО «НПП «Бевард» не берет на себя ответственности и не дает гарантий в выпуске обновлений или сохранении неизменной какой-либо информации в настоящем Руководстве по эксплуатации, и оставляет за собой право вносить изменения в данное Руководство и/или в изделия, описанные в нем, в любое время без предварительного уведомления. Если Вы обнаружите в этом Руководстве информацию, которая является неправильной или неполной, или вводит в заблуждение, мы будем Вам крайне признательны за Ваши комментарии и предложения.

С3. Предупреждения FCC

Это оборудование было протестировано и признано удовлетворяющим требованиям положения о цифровых устройствах, принадлежащих к классу А, части 15 Правил Федеральной комиссии по связи (FCC). Эти ограничения были разработаны в целях обеспечения защиты от вредных помех, которые могут возникать при использовании оборудования в коммерческих целях. Это оборудование может излучать, генерировать и использовать энергию в радиочастотном диапазоне. Если данное оборудование будет установлено и/или будет использоваться с отклонениями от настоящего Руководства, оно может оказывать вредное воздействие на качество радиосвязи, а при установке в жилой

зоне, возможно, – на здоровье людей. В этом случае владелец будет обязан исправлять последствия вредного воздействия за свой счет.

C4. Предупреждение CE

Это устройство может вызывать радиопомехи во внешнем окружении. В этом случае пользователь может быть обязан принять соответствующие меры.

C5. Поддержка

Для информации относительно сервиса и поддержки, пожалуйста, свяжитесь с сервисным центром ООО «НПП «Бевард». Контактные данные Вы можете найти на сайте <http://www.beward.ru/>.

Перед обращением в службу технической поддержки, пожалуйста, подготовьте следующую информацию:

- Точное наименование и IP-адрес Вашего оборудования (в случае приобретения IP-оборудования), дата покупки.
- Сообщения об ошибках, которые появлялись с момента возникновения проблемы.
- Версия прошивки и через какое оборудование работало устройство, когда возникла проблема.
- Произведенные Вами действия (по шагам), предпринятые для самостоятельного решения проблемы.
- Скриншоты настроек и параметры подключения.

Чем полнее будет представленная Вами информация, тем быстрее специалисты сервисного центра смогут помочь Вам решить проблему.

Приложение D. Глоссарий

Angle / Угол обзора – это угол, который образуют лучи, соединяющие заднюю точку объектива и диагональ кадра. Угол зрения показывает съёмочное расстояние и чаще всего выражается в градусах. Обычно угол зрения измеряется на линзе, фокус которой установлен в бесконечность. В зависимости от угла зрения, объективы делят на три типа: широкоугольные, нормальные и длиннофокусные. В широкоугольных объективах, которые чаще всего используются для панорамного наблюдения, угол зрения составляет 75 градусов и больше. Нормальные объективы имеют угол зрения от 45 до 65 градусов. Угол зрения длиннофокусного объектива составляет 30 градусов.

Authentication / Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Один из способов аутентификации в компьютерной системе состоит во вводе вашего пользовательского идентификатора, в просторечии называемого «логином» (login — регистрационное имя пользователя) и пароля — некой конфиденциальной информации, знание которой обеспечивает владение определенным ресурсом. Получив введенный пользователем логин и пароль, компьютер сравнивает их со значением, которое хранится в специальной базе данных, и, в случае совпадения, пропускает пользователя в систему.

Bitrate / Битрейт (Скорость передачи данных) – буквально, скорость прохождения битов информации. Битрейт принято использовать при измерении эффективной скорости передачи информации по каналу, то есть скорости передачи «полезной информации» (помимо таковой, по каналу может передаваться служебная информация).

BLC (Back Light Compensation / Компенсация фоновой засветки, компенсация заднего света). Типичный пример необходимости использования: человек на фоне окна. Электронный затвор камеры обрабатывает интегральную, т.е. общую освещенность сцены, «видимой» камерой через объектив. Соответственно, малая фигура человека на большом светлом фоне окна выльется в итоге "засветкой" всей картинке. Включение функции «BLC» может в подобных случаях исправить работу автоматики камеры.

Bonjour – протокол автоматического обнаружения сервисов (служб), используемый в операционной системе Mac OS X, начиная с версии 10.2. Служба Bonjour предназначена для использования в локальных сетях и использует сведения (записи) в службе доменных имён (DNS) для обнаружения других компьютеров, равно как и иных сетевых устройств (например, принтеров) в ближайшем сетевом окружении.

CMOS / КМОП (Complementary Metal Oxide Semiconductor / Комплементарный металлооксидный полупроводник) – это широко используемый тип полупроводника,

который использует как отрицательную, так и положительную электрическую цепь. Поскольку только одна из этих типов цепей может быть включена в любое данное время, то микросхемы КМОПа потребляют меньше электроэнергии, чем микросхемы, использующие только один тип транзистора. Также датчики изображения КМОП в некоторых микросхемах содержат схемы обработки, однако это преимущество невозможно использовать с ПЗС-датчиками, которые являются также более дорогими в производстве.

DDNS (Dynamic Domain Name System, DynDNS) – технология, применяемая для назначения постоянного доменного имени устройству (компьютеру, сетевому накопителю) с динамическим IP-адресом. Это может быть IP-адрес, полученный по DHCP или по IPCP в PPP-соединениях (например, при удалённом доступе через модем). Другие машины в Интернете могут устанавливать соединение с этой машиной по доменному имени.

DHCP (Dynamic Host Configuration Protocol / Протокол динамической конфигурации узла) – это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры.

DHCP-сервер – это программа, которая назначает клиентам IP-адреса внутри заданного диапазона на определенный период времени. Данную функцию поддерживают практически все современные маршрутизаторы.

Domain Server / Сервер доменных имен – также домены могут быть использованы организациями, которые хотят централизованно управлять своими компьютерами (на которых установлены операционные системы Windows). Каждый пользователь в рамках домена получает учетную запись, которая обычно разрешает зарегистрироваться и использовать любой компьютер в домене, хотя одновременно на компьютер могут быть наложены ограничения. Сервером доменных имен является сервер, который аутентифицирует пользователей в сети.

Ethernet – пакетная технология передачи данных преимущественно в локальных компьютерных сетях. Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде – на канальном уровне модели OSI.

Factory default settings / Заводские установки по умолчанию – это установки, которые изначально использованы для устройства, когда оно отгружается с завода в первый раз. Если возникнет необходимость переустановить устройство до его заводских установок

по умолчанию, то эта функция применима для большинства устройств, и она полностью переустанавливает любые установки, которые были изменены пользователем.

Fps / Кадровая частота – количество кадров, которое видеосистема (компьютерная игра, телевизор, DVD-плеер, видеофайл) выдаёт в секунду.

Frame / Кадр – кадром является полное видеоизображение. В формате 2:1 чересстрочной развёртки интерфейса RS-170 и в форматах Международного консультативного комитета по радиовещанию, кадр создается из двух отдельных областей линий чересстрочной развёртки 262.5 или 312.5 на частоте 60 или 50 Гц для того, чтобы сформировать полный кадр, который отобразится на экране на частоте 30 или 25 Гц. В видеокамерах с прогрессивной разверткой каждый кадр сканируется построчно и не является чересстрочным; большинство из них отображается на частоте 30 и 25 Гц.

FTP (File Transfer Protocol / Протокол передачи файлов) – это протокол приложения, который использует набор протоколов TCP / IP. Он используется, чтобы обменивается файлами между компьютерами/устройствами в сети. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер. Протокол FTP относится к протоколам прикладного уровня и для передачи данных использует транспортный протокол TCP. Команды и данные, в отличие от большинства других протоколов передаются по разным портам. Порт 20, открываемый на стороне сервера, используется для передачи данных, порт 21 - для передачи команд. Порт для приема данных клиентом определяется в диалоге согласования.

Gain / Коэффициент усиления – коэффициентом усиления является коэффициент усиления и экстента, в котором аналоговый усилитель усиливает силу сигнала. Коэффициенты усиления обычно выражаются в единицах мощности. Децибел (дБ) является наиболее употребительным способом для измерения усиления усилителя.

Gateway / Межсетевой шлюз – межсетевым шлюзом является сеть, которая действует в качестве точки входа в другую сеть. Например, в корпоративной сети, сервер компьютера, действующий в качестве межсетевого шлюза, зачастую также действует и в качестве прокси-сервера и сервера сетевой защиты. Межсетевой шлюз часто связан как с маршрутизатором, который распознает, куда направлять пакет данных, который приходит в межсетевой шлюз, так и коммутатором, который предоставляет истинный маршрут в и из межсетевого шлюза для данного пакета.

H.264 – это международный стандарт кодирования аудио и видео, (другое название 'MPEG-4 part 10' или AVC (Advanced Video Coding)). Данный стандарт содержит ряд новых возможностей, позволяющих значительно повысить эффективность сжатия видео по сравнению с более ранними стандартами (MPEG-1, MPEG-2 и MPEG-4), обеспечивая также

большую гибкость применения в разнообразных сетевых средах. Используется в цифровом телевидении высокого разрешения (HDTV) и во многих других областях цифрового видео.

HTTP (Hypertext Transfer Protocol / Протокол передачи гипертекста) – это набор правил по обмену файлами (текстовыми, графическими, звуковыми, видео- и другими мультимедиа файлами) в сети. Протокол HTTP является протоколом высшего уровня в семействе протоколов TCP/IP. В данном протоколе любой пакет передается до получения подтверждения о его правильном приеме.

HTTPS (Hypertext Transfer Protocol Secure / Защищённый протокол передачи гипертекста) – расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTP, «упаковываются» в криптографический протокол SSL или TLS, тем самым обеспечивается защита этих данных. В отличие от HTTP, для HTTPS по умолчанию используется TCP-порт 443.

IP 66 (Ingress Protection) – это стандарт защиты оборудования, который описывает пыле- и влаго- защиту камеры видеонаблюдения. Первая цифра обозначает уровень защиты от попадания твёрдых частиц (например, цифра 6 обозначает полное исключение попадания пыли). Вторая цифра обозначает уровень защиты от попадания жидкостей (например, цифра 6 обозначает безупречную работу камеры при воздействии массивных водяных потоков воды или временном обливании.)

IP-камера – цифровая видеокамера, особенностью которой является передача видеопотока в цифровом формате по сети Ethernet, использующей протокол IP.

JPEG (Joint Photographic Experts Group / Стандарт Объединенной группы экспертов в области фотографии) – один из популярных графических форматов, применяемый для хранения фотоизображений и подобных им изображений. При создании изображения JPEG имеется возможность настройки используемого коэффициента сжатия. Так как при более низком коэффициенте сжатия (т.е. самом высоком качестве) увеличивается объем файла, существует выбор между качеством изображения и объемом файла.

Kbit/s (Kilobits per second / Кбит/сек) – это мера измерения скорости потока данных, т.е. это скорость, на которой определенное количество битов проходят заданную точку.

LAN (Local Area Network / Локальная вычислительная сеть) – компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт), то есть определенную географическую зону.

MAC-адрес (Media Access Control address / Аппаратный адрес устройства) – это уникальный идентификатор присоединенного к сети устройства или, точнее, его интерфейс для подключения к сети.

Mbit/s (Megabits per second / Мбит/сек) – это мера измерения скорости потока данных, т.е. это скорость, на которой биты проходят заданную точку. Этот параметр обычно используется, чтобы представить «скорость» сети. Локальная сеть должна работать на скорости 10 или 100 Мбит/сек.

MJPEG (Motion JPEG) – покадровый метод видеосжатия, основной особенностью которого является сжатие каждого отдельного кадра видеопотока с помощью алгоритма сжатия изображений JPEG. При сжатии методом MJPEG межкадровая разница не учитывается.

MPEG-4 – это международный стандарт, используемый преимущественно для сжатия цифрового аудио и видео. Стандарт MPEG-4 в основном используется для вещания (потокное видео), записи фильмов на компакт-диски, видеотелефонии (видеотелефон) и широко вещания, в которых активно используется сжатие цифровых видео и звука.

NTP (Network Time Protocol / Протокол синхронизации времени) – сетевой протокол для синхронизации времени с использованием сетей. NTP использует для своей работы протокол UDP.

ONVIF (Open Network Video Interface Forum) – отраслевой стандарт, определяющий протоколы взаимодействия таких устройств, как IP-камеры, видеорегистраторы и системы управления видео. Международный форум, создавший данный стандарт, основан компаниями Axis Communications, Bosch Security Systems и Sony в 2008 году с целью разработки и распространения открытого стандарта для систем сетевого видеонаблюдения.

PAL (Phase Alternating Line / Телевизионный стандарт PAL) – телевизионный стандарт PAL является преобладающим телевизионным стандартом в странах Европы. Телевизионный стандарт PAL доставляет 625 строк в кадре на 25 к/сек.

PoE (Power over Ethernet / Питание через Ethernet) – технология, позволяющая передавать удалённому устройству вместе с данными электрическую энергию через стандартную витую пару в сети Ethernet.

Port / Порт – идентифицируемый номер системный ресурс, выделяемый приложению, выполняемому на некотором сетевом хосте, для связи с приложениями, выполняемыми на других сетевых хостах (в том числе с другими приложениями на этом же хосте). В обычной клиент-серверной модели приложение либо ожидает входящих данных или запроса на соединение («слушает порт»), либо посылает данные или запрос на соединение на известный порт, открытый приложением-сервером.

PPP (Протокол двухточечного соединения) – протокол, позволяющий использовать интерфейс последовательной передачи для связи между двумя сетевыми устройствами. Например, подключение ПК к серверу посредством телефонной линии.

PPPoE (Point-to-Point Protocol / Протокол соединения «точка - точка») – протокол для подключения пользователей сети стандарта Ethernet к Интернету через широкополосное соединение, такое как линия DSL, беспроводное устройство или кабельный модем. С помощью PPPoE и широкополосного модема пользователи локальной сети могут получать доступ с индивидуальной проверкой подлинности к высокоскоростным сетям данных. Объединяя Ethernet и протокол PPP (Point-to-Point Protocol), протокол PPPoE обеспечивает эффективный способ создания отдельных соединений с удаленным сервером для каждого пользователя.

Progressive scan / Прогрессивное сканирование – это технология представления кадров в видеонаблюдении, при которой каждый кадр воспроизводится по одной линии в порядке их размещения каждую шестнадцатую долю секунды. То есть сначала показывается линия 1, затем 2, затем 3 и так далее. Таким образом, изображение не бьется на отдельные полукадры. В этом случае полностью исчезает эффект мерцания, поэтому качество отснятого видео получается более высоким.

RJ45 – унифицированный разъём, используемый в телекоммуникациях, имеет 8 контактов. Используется для создания ЛВС с использованием 4-парных кабелей витой пары.

Router / Маршрутизатор – это устройство, которое определяет точку ближайшей сети, в которую пакет данных должен быть направлен как в свой окончательный пункт назначения. Маршрутизатор создает и/или поддерживает специальную таблицу маршрутизации, которая сохраняет информацию, как только она достигает определенных пунктов назначения. Иногда маршрутизатор включен в качестве части сетевого коммутатора.

RTP (Real-Time Transport Protocol / Транспортный протокол в режиме реального времени) – это протокол IP для передачи данных (например, аудио или видео) в режиме реального времени. Протокол RTP переносит в своём заголовке данные, необходимые для восстановления голоса или видеоизображения в приёмном узле, а также данные о типе кодирования информации (JPEG, MPEG и т. п.). В заголовке данного протокола, в частности, передаются временная метка и номер пакета. Эти параметры позволяют при минимальных задержках определить порядок и момент декодирования каждого пакета, а также интерполировать потерянные пакеты. В качестве нижележащего протокола транспортного уровня, как правило, используется протокол UDP.

RTSP (Real Time Streaming Protocol / Протокол передачи потоков в режиме реального времени) – это протокол управления, который служит основой для согласования транспортных протоколов, таких как RTP, многоадресной или одноадресной передачи и для согласования используемых кодеков. RTSP можно рассматривать как пульт дистанционного управления потоками данных, предоставляемыми сервером мультимедиа. Серверы RTSP

обычно используют RTP в качестве стандартного протокола для передачи аудио- и видеоданных.

SD (Secure Digital Memory Card/ карта памяти типа SD) – формат карты флэш-памяти, разработанный для использования в основном в портативных устройствах. На сегодняшний день широко используется в цифровых устройствах, например: в фотоаппаратах, мобильных телефонах, КПК, коммуникаторах и смартфонах, GPS-навигаторах, видеокамерах и в некоторых игровых приставках.

Shutter / Электронный затвор – это элемент матрицы, который позволяет регулировать время накопления электрического заряда. Эта деталь отвечает за длительность выдержки и количество света, попавшего на матрицу перед формированием изображения.

SMTP (Simple Mail Transfer Protocol / Простой протокол передачи почты) – протокол SMTP используется для отсылки и получения электронной почты. Однако поскольку он является «простым» по своей структуре, то он ограничен в своей возможности по вместимости сообщений на получающем конце, и он обычно используется с одним из двух других протоколов, POP3 или протоколом интерактивного доступа к электронной почте (протокол IMAP). Эти протоколы позволяют пользователю сохранять сообщения в почтовом ящике сервера и периодически загружать их из сервера.

SSL/TSL (Secure Socket Layer / Transport Layer Security / Протокол защищенных сокетов / Протокол транспортного уровня) – эти два протокола (протокол SSL является приемником протокола TSL) являются криптографическими протоколами, которые обеспечивают безопасную связь в сети. В большинстве случаев протокол SSL используется через протокол HTTP, чтобы сформировать протокол защищенной передачи гипертекста (протокол HTTPS) в качестве использованного, например, в Интернете для осуществления финансовых транзакций в электронном виде. Протокол SSL использует сертификаты открытого криптографического ключа, чтобы подтверждать идентичность сервера.

Subnet mask / Маска подсети – битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая – к адресу самого узла в этой сети. Например, узел с IP-адресом 192.168.0.99 и маской подсети 255.255.255.0 находится в сети 192.168.0.0.

Switch / Коммутатор – коммутатором является сетевое устройство, которое соединяет сегменты сети вместе и которое выбирает маршрут для пересылки устройством данных к его ближайшему получателю. Обычно коммутатор является более простым и более быстрым механизмом, чем сетевой маршрутизатор. Некоторые коммутаторы имеют функцию маршрутизатора.

TCP (Transmission Control Protocol / Протокол управления передачей) – один из основных сетевых протоколов Интернета, предназначенный для управления передачей данных в сетях и подсетях TCP/IP. TCP — это транспортный механизм, предоставляющий поток данных с предварительной установкой соединения, за счёт этого дающий уверенность в достоверности получаемых данных, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета (см. также T/TCP).

UDP (User Datagram Protocol / Протокол дейтаграмм пользователя) – это протокол обмена данными с ограничениями на пересылаемые данные по сети, использующей протокол IP. Протокол UDP является альтернативой протоколу TCP. Преимущество протокола UDP состоит в том, что для него необязательна доставка всех данных и некоторые пакеты могут быть пропущены, если сеть перегружена. Это особенно удобно при передаче видеоматериалов в режиме реального времени, поскольку не имеет смысла повторно передавать устаревшую информацию, которая все равно не будет отображена.

UPnP (Universal Plug and Play) – технология, позволяющая персональным компьютерам и интеллектуальным сетевым системам (например, охранному оборудованию, развлекательным устройствам или интернет-шлюзам) соединяться между собой автоматически и работать совместно через единую сеть. Платформа UPnP строится на основе таких интернет-стандартов, как TCP/IP, HTTP и XML. Технология UPnP поддерживает сетевые инфраструктуры практически любого типа - как проводные, так и беспроводные. В их число, в частности, входят кабельный Ethernet, беспроводные сети Wi-Fi, сети на основе телефонных линий, линий электропитания и пр. Поддержка UPnP реализована в операционных системах Windows.

URL (Uniform Resource Locator / Единый указатель ресурсов) – это стандартизированный способ записи адреса ресурса в сети Интернет.

Web-server / Веб-сервер – это сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, обычно вместе с HTML-страницей, изображением, файлом, медиа-поток или другими данными.

Алгоритм сжатия видео – это методика уменьшения размера файла цифровой видеозаписи посредством удаления графических элементов, не воспринимаемых человеческим глазом.

Варифокальный объектив – объектив, позволяющий использовать различные фокусные расстояния в противоположность объективу с фиксированным фокусным расстоянием, который использует лишь одно расстояние.

Витая пара – вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных между собой, покрытых пластиковой оболочкой. Свивание проводников производится с целью повышения степени связи между собой проводников одной пары (электромагнитная помеха одинаково влияет на оба провода пары) и последующего уменьшения электромагнитных помех от внешних источников, а также взаимных наводок при передаче дифференциальных сигналов.

Выдержка – интервал времени, в течение которого свет воздействует на участок светочувствительного материала или светочувствительной матрицы для сообщения ему определённой экспозиции.

Детектор движения – это аппаратный либо программный модуль, основной задачей которого является обнаружение перемещающихся в поле зрения камеры объектов.

Доменное имя – это определенная буквенная последовательность, обозначающая имя сайта или используемая в именах электронных почтовых ящиков. Доменные имена дают возможность адресации интернет-узлов и расположенных на них сетевых ресурсов (веб-сайтов, серверов электронной почты, других служб) в удобной для человека форме.

ИК-подсветка (ИК-прожектор) – устройство, обеспечивающее подсветку объекта наблюдения с излучением в инфракрасном диапазоне.

Камера «день/ночь» – это видеокамера, предназначенная для работы круглосуточно в разных условиях освещенности. В условиях яркой освещенности изображение цветное. В темное время суток, когда яркий свет пропадает, и начинаются сумерки, изображение становится черно-белое, в результате чего повышается чувствительность.

Кодек – в системах связи кодек — это обычно кодер/декодер. Кодеки используются в интегрированных цепях или микросхемах для преобразования аналоговых видео- и аудиосигналов в цифровой формат для последующей передачи. Кодек также преобразует принимаемые цифровые сигналы в аналоговый формат. В кодеке одна микросхема используется для преобразования аналогового сигнала в цифровой и цифрового сигнала – в аналоговый. Термин «Кодек» также может относиться к компрессии/декомпрессии, и в этом случае он обычно означает алгоритм или компьютерную программу для уменьшения объема файлов и программ.

Нормально замкнутые контакты – такая конструкция датчика, которая в пассивном состоянии имеет замкнутые контакты, а в активном — разомкнутые.

Нормально разомкнутые контакты – такая конструкция датчика, которая в пассивном состоянии имеет разомкнутые контакты, а в активном – замкнутые.

Объектив – это часть оптической системы видеонаблюдения, предназначенная для фокусировки потока света на матрице видеокамеры.

Пиксель – это одна из множества точек, составляющих цифровое изображение. Цвет и интенсивность каждого пикселя составляет крошечную область изображения.

Протокол – стандарт, определяющий поведение функциональных блоков при передаче данных. Формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах.

Разрешение изображения – это количество пикселей (точек) на единицу площади изображения. Измеряется в мегапикселях или отображается в виде двух величин – высоты и ширины изображения. Высота и ширина также в данном случае измеряются в пикселях.

Уличная видеокамера – это камера видеонаблюдения, которая обладает всеми необходимыми характеристиками защиты от влияния внешней среды для работы на улице.

Цветная видеокамера – это камера, которая дает цветное изображение. По определению матрицы видеокамер черно-белые, а для получения цветного изображения возле каждой ячейки матрицы формируются цветные фильтры. Первый фильтр привносит красную составляющую цвета, второй зеленую, а третий синюю. Таким образом, три ячейки становятся одной точкой в цветовом формате RGB. Следовательно, вместо трех пикселей на результирующем изображении мы получаем только один.

Электромеханический ИК-фильтр – представляет собой устройство, которое способно в одном режиме подавлять инфракрасный диапазон при помощи инфракрасного ИК-фильтра, а в другом режиме ИК-фильтр убирается электромеханически, таким образом, делая доступным весь спектр светового излучения.