BEWARD
IP-ВИДЕОНАБЛЮДЕНИЕ

Руководство по подключению

www.beward.ru

IP-видеокамера N520



Разрешение Full HD
WI-FI 802.11 b/g/n, поддержка WPS
Запись на внешний файловый сервер
Поддержка карт памяти microSDHC

Оглавление

ГЛАВА 1. МЕРЫ ПРЕДОСТОРОЖНОСТИ 3
ГЛАВА 2. ОБЩИЕ СВЕДЕНИЯ 5
2.1. Особенности IP-видеокамеры BEWARD N520 6
2.2. Основные характеристики 7
2.3. Комплект поставки 7
ГЛАВА 3. ВНЕШНИЙ ВИД 8
3.1. Вид спереди 8
3.2. Вид сзади 9
ГЛАВА 4. УСТАНОВКА И ПОДКЛЮЧЕНИЕ IP-КАМЕРЫ 11
4.1. Общие сведения о подключении IP-камеры N520 к сети 11
4.2. Рекомендации по установке 11
4.3. Монтаж устройства 13
4.4. Проводное подключение камеры к сети 13
4.5. Подключение тревожных контактов 14
ГЛАВА 5. НАСТРОЙКА ПРОВОДНОГО СОЕДИНЕНИЯ ДЛЯ WINDOWS 7 15
5.1. Определение параметров локальной сети для проводного подключения 15
5.1.1. Определение параметров сети при динамическом IP-адресе 19
5.2. Изменение параметров локальной сети для проводного подключения IP-камер 22
5.3. Получение доступа к IP-камере 26
5.3.1. Установка «BEWARD IP Installer» 26
5.3.2. Получение доступа к IP-камере с помощью ПО «BEWARD IP Installer» 26
5.3.3. Получение доступа к IP-камере с помощью меню [Сеть] ОС Windows 7 28
5.3.4. Получение доступа к IP-камере с помощью браузера Internet Explorer 29
5.4. Получение доступа к веб-интерфейсу IP-камеры 29
5.5. Изменение настроек подключения IP-камеры через веб-интерфейс 32
5.6. Возврат сетевых настроек ПК к первоначальным значениям 34
5.7. Проверка правильности настроек подключения IP-камеры к локальной сети 37
ГЛАВА 6. НАСТРОЙКА WI-FI-СОЕДИНЕНИЯ 39
6.1. Общие сведения о беспроводном Wi-Fi подключении IP-камеры N520 39
6.2. Подключение к беспроводной Wi-Fi сети с помощью WPS 39
6.2.1 Подключение с использованием веб-интерфейса IP-камеры 39
6.2.2 Подключение без использования веб-интерфейса IP-камеры 44
6.2.3. Проверка доступности IP-камеры 45
6.3. Подключение к беспроводной Wi-Fi сети без использования WPS 46
6.3.1. Определение текущих настроек Wi-Fi сети для ОС Windows 7 46
6.3.2. Изменение настроек Wi-Fi соединения IP-камеры через веб-интерфейс 50
6.3.3. Проверка правильности настроек Wi-Fi соединения IP-камеры 54
ГЛАВА 7. ПОДКЛЮЧЕНИЕ IP-КАМЕРЫ К СЕТИ ИНТЕРНЕТ 56
7.1. Общие сведения о подключении IP-камеры к сети Интернет 56
7.2. Подключение при статическом внешнем IP-адресе или PPPoE-соединении 57
7.2.1. Использование статического IP-адреса 57
7.2.2. Использование PPPoE-соединения 58
7.3. Подключение через сеть Интернет к IP-камерам, находящимся в локальной сети 60
7.3.1. Использование технологии UPnP 61
7.3.2. Настройка ручной переадресации портов маршрутизатора 62
7.4. Пример подключения через сеть Интернет с использованием DDNS 68
7.4.1. Общие сведения о подключении через Интернет с использованием DDNS 68
7.4.2. Регистрация на сервере DynDNS 68
7.4.3. Создание доменного имени на сервере DynDNS 72
7.4.4. Настройка оборудования для работы с сервисом DynDNS 76
ПРИЛОЖЕНИЯ 80
Приложение А. Значения используемых портов 80

ПРИЛОЖЕНИЕ B. ЗАВОДСКИЕ УСТАНОВКИ 81
ПРИЛОЖЕНИЕ C. ОБЩИЕ СВЕДЕНИЯ О БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СОЕДИНЕНИЙ 82
ПРИЛОЖЕНИЕ D. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА 84
ПРИЛОЖЕНИЕ E. ПРАВА И ПОДДЕРЖКА 87
ПРИЛОЖЕНИЕ F. ГЛОССАРИЙ 89

BEWARD

Глава 1. Меры предосторожности

Перед использованием необходимо помнить нижеследующее.

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

ВНИМАНИЕ!

Используйте при эксплуатации только совместимые устройства. Использование устройств, не одобренных производителем, недопустимо.

Соблюдайте инструкцию по эксплуатации!

Избегайте длительного использования или хранения камеры в неблагоприятных условиях:

- При слишком высоких или низких температурах (рабочая температура устройств от 0°C до +50°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:

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

Транспортировка

При транспортировке камеры положите камеру 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 удаления 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.

BEWARD

Глава 2. Общие сведения

BEWARD N520 – это компактная двухмегапиксельная IP-видеокамера с мультипотоковым видеоизображением в форматах H.264/MPEG-4/MJPEG, оснащенная встроенным Wi-Fi модулем стандарта IEEE 802.11 b/g/n, высокочувствительным КМОП-сенсором нового поколения с поддержкой функции WDR (расширенный динамический диапазон), встроенным инфракрасным датчиком движения (PIR-сенсор), встроенным микрофоном и слотом для установки карты памяти стандарта MicroSD.



Рис. 2.1

IP-камера BEWARD N520 позволяет просматривать видео в реальном времени через стандартный Интернет-браузер. Камера выдает видеопоток в различных форматах сжатия: H.264, MPEG4, MJPEG. Формат H.264 является идеально подходит в условиях ограниченной полосы пропускания. При его использовании достигается наименьший трафик и хорошее качество изображения. Формат MJPEG предназначен для записи и просмотра видеоизображения в наилучшем качестве, но требует больших сетевых ресурсов и места на жестком диске (для записи).

Камера N520 может быть подключена к сети при помощи проводного интерфейса 10/100BASE-TX Ethernet или с использованием беспроводного соединения стандарта Wi-Fi IEEE 802.11 b/g/n. Для удобства и быстроты подключения к беспроводной сети камера оснащена функцией WPS.

Высокое качество изображения двухмегапиксельного разрешения реального времени обеспечивается современным сенсором высокой чувствительности с прогрессивным сканированием, а также благодаря применению эффективных методов сжатия видео.

В процессе управления крупными системами видеонаблюдения оператор не всегда сможет оперативно среагировать, если обзор одной из камер будет закрыт злоумышленниками. В подобных ситуациях будет полезна функция *детектора саботажа*, которая позволяет своевременно информировать оператора и делает процесс видеонаблюдение более удобным.

При работе камеры в условиях недостаточного освещения возможны ложные срабатывания детектора движения либо наоборот отсутствие срабатываний. Для исключения подобных ситуаций служит встроенный инфракрасный датчик движения – PIR-сенсор. Работа PIR-сенсора основана на свойстве материала, из которого он изготовлен, генерировать определенное электрическое поле при облучении инфракрасными (тепловыми) лучами. Так как тело человека излучает тепло, PIR-сенсор обнаруживает движение в контролируемой зоне независимо от уровня внешнего освещения.

Поддержка карт памяти типа MicroSD позволяет сделать систему видеонаблюдения еще более надежной: важная информация не пропадет при потере соединения, в полном объеме она будет сохранена на карте памяти. В дальнейшем, ее можно будет воспроизвести как непосредственно с карты, так и удаленно после устранения технических неполадок сети.

2.1. Особенности IP-видеокамеры BEWARD N520

- Оптимальное соотношение цена/качество для IP-видеокамеры
- 1/2.7" КМОП-сенсор с прогрессивным сканированием и поддержкой WDR
- Поддержка карт памяти типа MicroSD/SDHC
- Встроенный Wi-Fi модуль 802.11b/g/n с поддержкой WPS
- Профессиональное программное обеспечение (16 каналов) в комплекте
- Одновременное многоформатное кодирование данных (H.264/MPEG4/MJPEG) для обеспечения оптимального отображения видео и записи файлов
- Возможность просмотра записанных файлов непосредственно из веб-интерфейса с помощью встроенного плеера
- Встроенный микрофон
- Встроенный динамик
- Встроенный инфракрасный датчик движения (PIR-сенсор)
- Встроенные детектор саботажа, детектор движения и детектор звука
- Отправка кадров и видеороликов по электронной почте и на FTP
- Запись на внешний файловый сервер (в том числе и в папку с открытым доступом на ПК с установленной ОС Windows или Linux)
- Поддержка ONVIF

2.2. Основные характеристики

- Светочувствительный элемент: двухмегапиксельный КМОП-сенсор с прогрессивным сканированием и поддержкой WDR
- Объектив: сменный M12, f4.0 мм, F1.8, угол обзора 72° (по горизонтали)
- Разрешение: 1920x1080, 1280x720, 640x480, 320x240
- Чувствительность: 0.05 лк при F1.8
- Затвор: электронный от 1/2 до 1/10000 сек
- Усиление видеосигнала: от 1x до 64x
- Частота кадров: до 30 кадров в секунду для всех разрешений
- Одновременное кодирование в форматах: H.264, MPEG-4, MJPEG
- Двустороннее аудио, компрессия: G.711 μ-law, α-law, AMR
- Поддерживаемые протоколы: Bonjour, TCP/IP, DHCP, PPPoE, ARP, ICMP, FTP, SSL, SMTP, DDNS, NTP, UPnP, RTSP, RTP, RTCP, HTTP, TCP, UDP, 3GPP/ISMA RTSP
- Питание: 5В, 0.75А (постоянный ток)
- Рабочая температура: от 0 до +50°С
- Влажность окружающей среды: 20-80% (без образования конденсата)
- Поддержка отраслевого стандарта ONVIF

2.3. Комплект поставки

- IP-видеокамера с установленным объективом
- Кабель патч-корд (длина 1 м)
- Источник питания постоянного тока 5В, 1А
- Терминальный блок (4 контакта, тревожные вход, выход)
- Антенна для подключения к беспроводной сети
- Кронштейн с комплектом крепежа
- CD-диск с программным обеспечением и документацией
- Руководство пользователя по быстрой установке

ВНИМАНИЕ!

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

Глава 3. Внешний вид

3.1. Вид спереди

На лицевой части камеры расположены следующие элементы *(Рис 3.1)*:



Рис. 3.1

Объектив: при размытом изображении необходимо настроить фокус камеры, для этого вращайте кольцо настройки фокуса, пока не добьетесь необходимой фокусировки (изначально объектив камеры уже сфокусирован и не требует дополнительной настройки).

Индикатор питания: загорается после подключения камеры к источнику питания.

- **Индикатор питания горит красным**: к IP-камере подключено питание, идет загрузка системы.
- **Индикатор питания горит синим**: загрузка IP-камеры завершена, камера готова к работе.
- **Индикатор питания мигает фиолетовым цветом**: идет процесс обновления прошивки камеры, не отключайте питание и не закрывайте окно браузера до завершения прошивки и полной загрузки камеры.
- **Индикатор питания не горит**: к IP-камере не подключено питание либо отключена индикация в настройках камеры.

Индикатор соединения: индикатор загорается при подключении камеры к сети и показывает текущую сетевую активность.

- **Индикатор соединения мигает синим цветом**: IP-камера подключена к сети с помощью проводного соединения.
- **Индикатор соединения не горит (не мигает)**: IP-камера отключена от проводной сети, либо отключена индикация в настройках камеры.

Встроенный микрофон: позволяет пользователю слышать то, что происходит в зоне наблюдения камеры.

Встроенный динамик: в совокупности со встроенным микрофоном камеры данная опция дает возможность организовать двусторонний аудиоканал между оператором, управляющим камерой через веб-интерфейс, и человеком, находящимся в зоне наблюдения.

PIR сенсор: позволяет обнаруживать движение в контролируемой зоне независимо от уровня внешнего освещения, так как реагирует на инфракрасное (тепловое) излучение.

3.2. Вид сзади

На задней панели корпуса *(Рис 3.2)* камеры расположены следующие элементы:

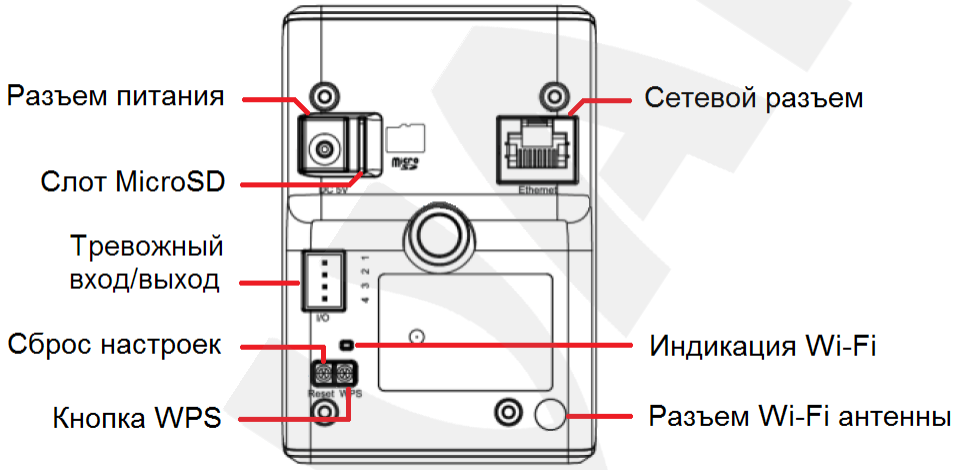

Рис. 3.2

Разъем питания (DC5V): предназначен для подключения блока питания 5В, 1А.

Для корректной работы камеры рекомендуется использовать только источник питания входящий в комплект поставки.

Слот MicroSD: слот для карты памяти формата MicroSD/SDHC.

Позволяет использовать карты памяти для записи информации как в режиме тревоги, так и в режиме постоянной записи. Также предусмотрена возможность автоматической резервной записи на карту во время отсутствия сети.

Сетевой разъем (Ethernet): разъем для подключения камеры к сети Интернет, роутеру или коммутатору при помощи стандартного RJ-45 штекера.

Тревожные вход/выход: возможна настройка активации различных событий при определенных состояниях тревожного входа, и настройка событий при активации которых, тревожный выход изменит состояние (более подробно см. в пункте 4.5 данного Руководства).

Сброс настроек [Reset]: кнопка предназначена для сброса настроек камеры в заводские установки.

Для возврата параметров устройства к значениям по умолчанию удерживайте данную кнопку нажатой в течение 10-15 секунд. Если удерживать кнопку нажатой менее 10 секунд, камера перезагрузится без сброса параметров в заводские установки.

Кнопка WPS (полуавтоматическое подключение по Wi-Fi): при нажатии данной кнопки происходит получение сетевых настроек по протоколу WPS. Для подключения камеры к беспроводной сети с помощью WPS необходимо нажать данную кнопку на IP-камере и на том устройстве, к которому требуется подключиться (более подробную информацию см. в пункте 6.2 данного Руководства).

Индикация Wi-Fi (беспроводного подключения): индикатор подключения загорается при подключении камеры к сети и показывает текущую сетевую активность.

- **Индикатор подключения мигает синим**: IP-камера подключена к сети с помощью беспроводного соединения.
- **Индикатор подключения не горит (не мигает)**: IP-камера отключена от беспроводной сети, либо отключена индикация в настройках камеры.

Разъем Wi-Fi антенны: RP-SMA коннектор для подключения входящей в комплект антенны для беспроводного подключения.

Стикер, наклеенный на задней панели камеры, содержит следующую информацию:

- **SN**: серийный номер IP-камеры;
- **MAC**: MAC-адрес IP-камеры в сети LAN (MAC-адрес устройства при проводном подключении);
- **WMAC**: MAC-адрес IP-камеры в сети WLAN (MAC-адрес устройства при беспроводном подключении).

Глава 4. Установка и подключение IP-камеры

4.1. Общие сведения о подключении IP-камеры N520 к сети

IP-камера N520 может подключаться к локальной сети либо сети Интернет как при помощи проводного соединения (Ethernet), так и по беспроводному (Wi-Fi) соединению. Подключение может осуществляться как напрямую к ПК, так и при помощи вспомогательного сетевого оборудования (маршрутизаторы, коммутаторы, точки доступа).



Рис. 4.1

Как правило, в домашних маршрутизаторах предусмотрен один WAN-порт для подключения к сети Интернет и четыре внутренних LAN-порта для подключения компьютеров, IP-камер и других устройств домашней сети. Кроме этого, для подключения IP-камер N520 при помощи Wi-Fi соединения маршрутизатор должен иметь Wi-Fi интерфейс.

4.2. Рекомендации по установке

В данном разделе приведен краткий список рекомендаций, которые необходимо учитывать при монтаже оборудования IP-видеонаблюдения.

Рекомендации по прокладке кабеля типа «витая пара»:

- В коридорах пучки электрических и слаботочных кабелей желательно прокладывать по разным кабель-каналам, проходящим по разным стенам.
- В одном кабель-канале допускается прокладывать витопарные и электрические кабели только в разных отсеках или секциях, имеющих сплошные продольные перегородки из несгораемого материала с пределом огнестойкости не менее 0,25 ч, и только в рабочих зонах на расстоянии не более 15-ти метров, если электрическая мощность будет не более 5 кВА.

- Электрические и слаботочные кабельные трассы допускается прокладывать параллельно на расстоянии не менее 50 мм друг от друга в разных кабель-каналах или секциях кабель-каналов. Если напряженность электрического поля, образующегося от электрического кабеля, будет более 3 В/м, то необходимо увеличить расстояние между электрическими и слаботочными кабелями или снизить уровень электромагнитных помех.
- Витопарные и электрические кабели должны пересекаться только под прямым углом.
- Неэкранированные витопарные кабельные трассы должны проходить на расстоянии не менее 125 мм от газоразрядных ламп дневного света (люминесцентных ламп) и других высоковольтных устройств, содержащих разрядники.
- Неэкранированные витопарные кабели должны прокладываться на расстоянии не менее 1.5 метров от источников сильных электромагнитных помех, образующих напряженность электрического поля свыше 3 В/м.
- Распределительные устройства с заделанными неэкранированными витопарными кабелями должны располагаться на расстоянии не менее 3-х метров от источников сильных электромагнитных помех, образующих напряженность электрического поля свыше 3 В/м.
- Прокладка витой пары между точками подключения должна производиться целыми кусками, при этом направление трассы следует заранее продумать так, чтобы её протяжённость была как можно меньше.
- Минимальный радиус изгиба для кабеля – четыре диаметра кабеля (или 1 дюйм=2,5 см), но существуют рекомендации размещать кабель таким образом, чтобы обеспечивать изгиб радиусом 2 дюйма (5 сантиметров).
- Максимальная длина сегмента должна быть не более 100 метров.
- При использовании беспроводного Wi-Fi соединения следует учитывать, что уровень/качество сигнала сильно зависит от множества факторов: удаленности от точки доступа, от электромагнитной обстановки, конфигурации помещения и т.д.

4.3. Монтаж устройства

Шаг 1: прикрепите кронштейн к поверхности, используя отверстия в основании.

Шаг 2: ослабьте винтовое соединение фиксатора кронштейна, чтобы иметь возможность поворачивать камеру для выбора необходимой зоны наблюдения.

Шаг 3: закрепите камеру на кронштейне, настройте угол наклона камеры и зафиксируйте её *(Рис. 4.2).*

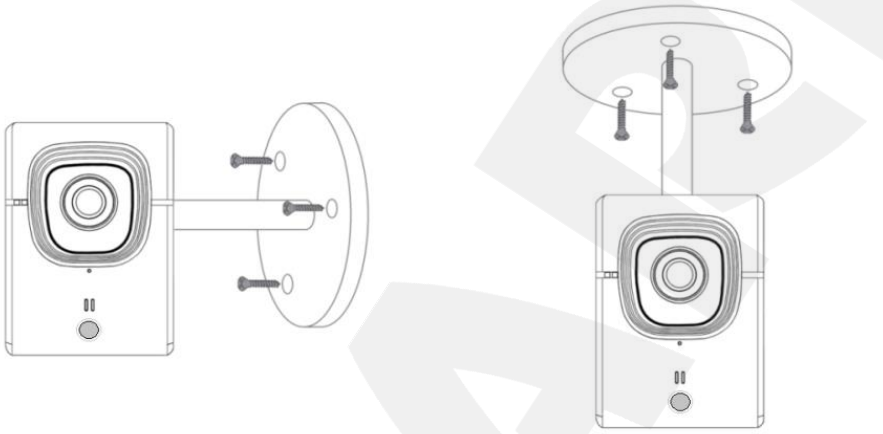

Рис. 4.2

4.4. Проводное подключение камеры к сети

Используя соединительный кабель с разъемом RJ-45, подключите IP-камеру к локальной сети (к LAN-интерфейсу маршрутизатора).

В случае необходимости соединительный кабель можно приобрести отдельно или, при наличии необходимых материалов, инструментов и опыта, изготовить самостоятельно.

Вариант «прямого» кабеля (UTP категории 5e) с разъемом RJ-45

С одного конца		С другого конца	
	1: Бело-оранжевый		1: Бело-оранжевый
	2: Оранжевый		2: Оранжевый
	3: Бело-зелёный		3: Бело-зеленый
	4: Синий		4: Синий
	5: Бело-синий		5: Бело-синий
	6: Зелёный		6: Зелёный
	7: Бело-коричневый		7: Бело-коричневый
	8: Коричневый		8: Коричневый

Для изготовления «прямого» кабеля необходимы: кабель UTP (витая пара категории 5e или лучше), два разъема RJ-45 и устройство для обжима разъемов RJ-45 (кримпер).

При таком порядке подключения пар (указанном в таблице) обеспечиваются гарантированные производителем величина и распределение задержек распространения сигнала, а соответственно, и заявленная скорость передачи данных 100 Мбит/с.

4.5. Подключение тревожных контактов

IP-камера BEWARD N520 снабжена тревожным входом и тревожным выходом для подключения внешних датчиков и тревожных устройств.

- **Тревожный вход**: служит для подключения внешних датчиков (например, датчик объема). Возникновение тревожного события обусловлено замыканием либо размыканием (задается настройками камеры) контактов 3 (тревожный вход) и 2 (GND) (*Рис. 4.3*).
- **Тревожный выход**: служит для подключения тревожных устройств (например, извещатель) через ретрансляторы (например, реле). В случае наступления тревожного события контакт 4 (тревожный выход) замыкается либо размыкается (задается настройками камеры) с контактом 2 (GND). Это приводит к изменению напряжения между контактами 1 (5V DC) и 4 (тревожный выход), что вызывает изменение состояния реле, подключенного к этим контактам (*Рис. 4.3*).

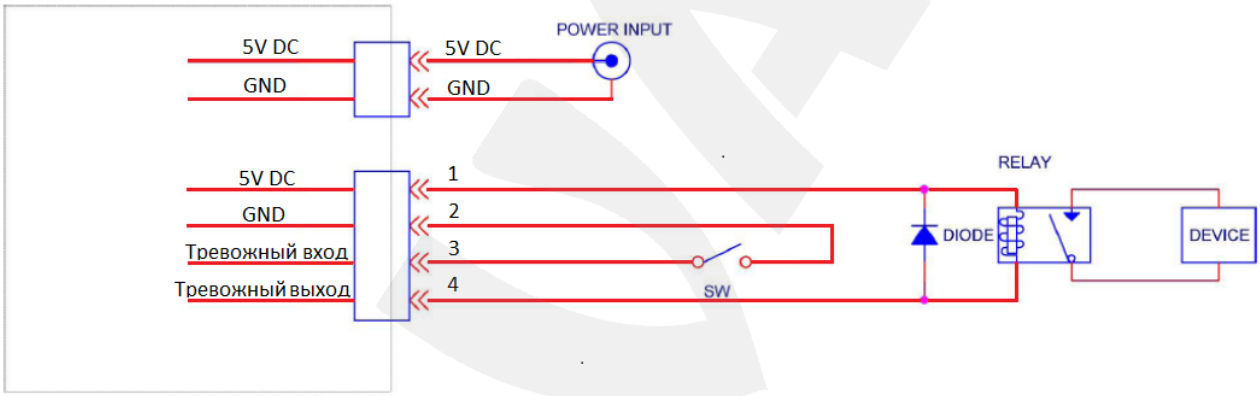

Рис. 4.3

ПРИМЕЧАНИЕ!

При использовании внешнего ретранслятора необходимо подключать диод параллельно нагрузке для защиты электроники камеры от скачков напряжения во время переходных процессов (*Рис. 4.3*).

При использовании внешних датчиков следует помнить о том, что тревожные вход, выход камеры – логические, и допускать превышение предельно допустимых значений напряжения/тока (5В/100мА) ЗАПРЕЩЕНО!

ВНИМАНИЕ!

Не рекомендуется выполнять подключение устройств при включенном питании камеры.

Глава 5. Настройка проводного соединения для Windows 7

Для того чтобы IP-камера N520 работала в Вашей локальной сети совместно с Вашими компьютерами, ноутбуками и другим оборудованием, необходимо включить IP-камеру в сеть в соответствии с настройками данной сети, для чего необходимо определить текущие настройки.

ПРИМЕЧАНИЕ!

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

5.1. Определение параметров локальной сети для проводного подключения

При подключении с помощью кабеля пачт-корд необходимо определить текущие настройки кабельной сети. При подключении по Wi-Fi (без использования WPS) необходимо определить настройки как беспроводной сети, так и проводной сети.

Для определения текущих настроек компьютера в локальной проводной сети нажмите ***Пуск – Панель управления*** (*Рис. 5.1*).

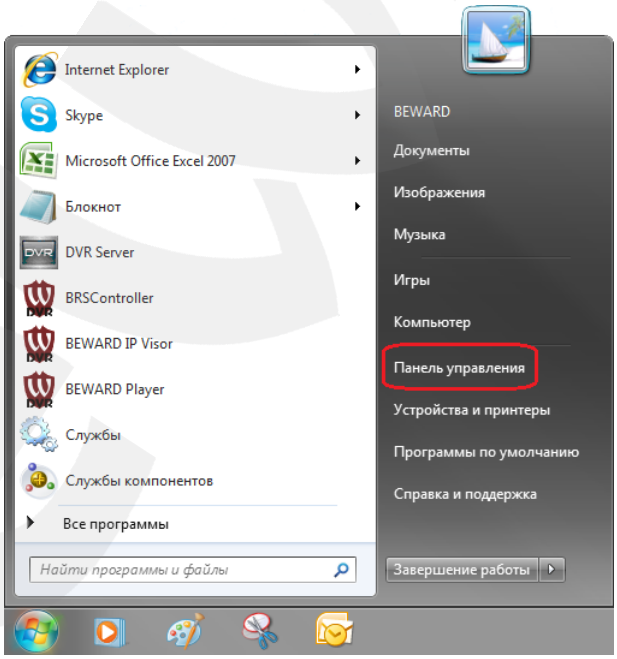

Рис. 5.1

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

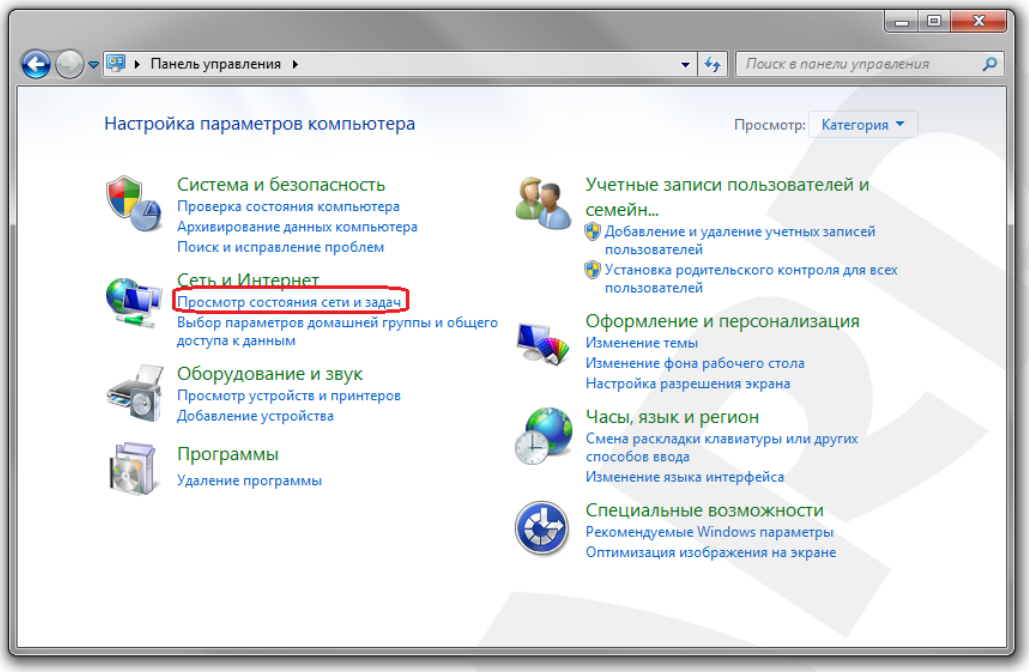

Рис. 5.2

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

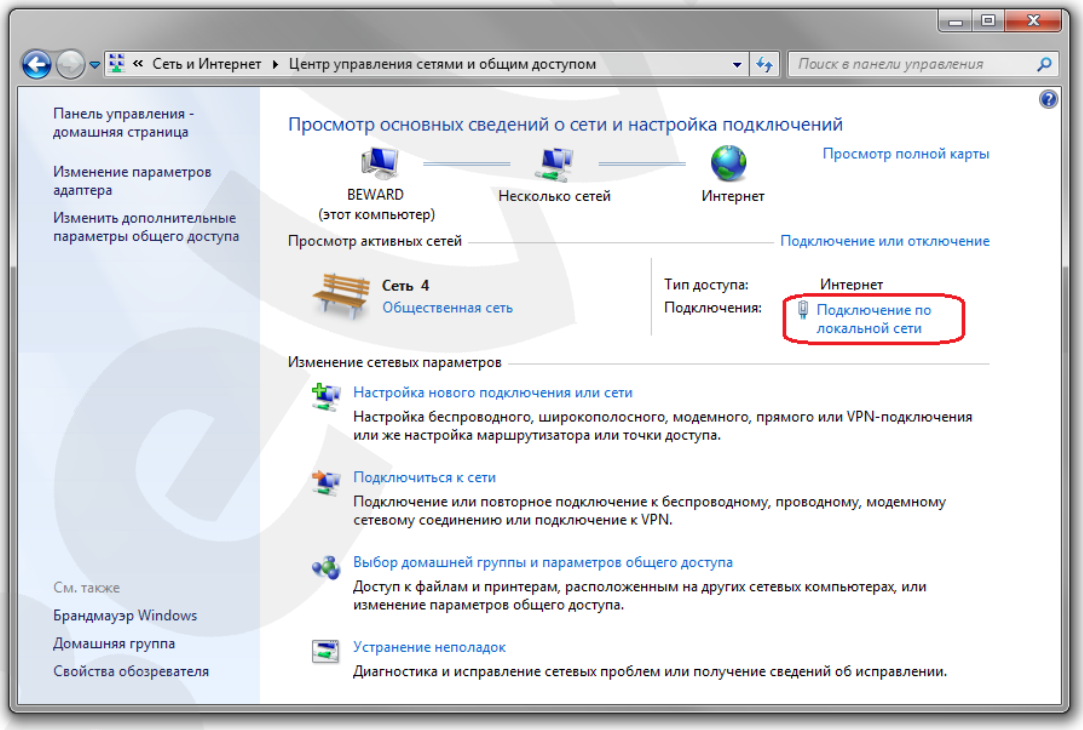

Рис. 5.3

ПРИМЕЧАНИЕ!

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

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

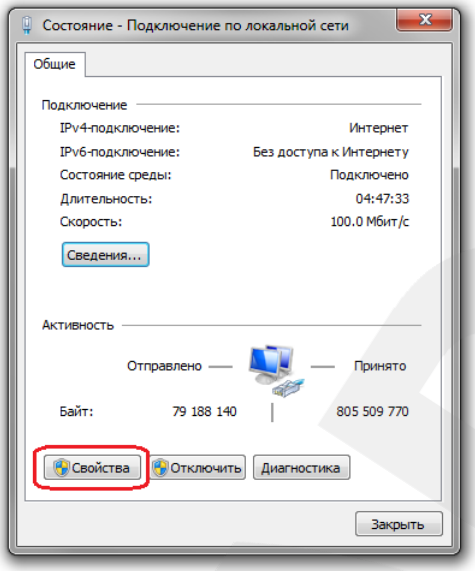

Рис. 5.4

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

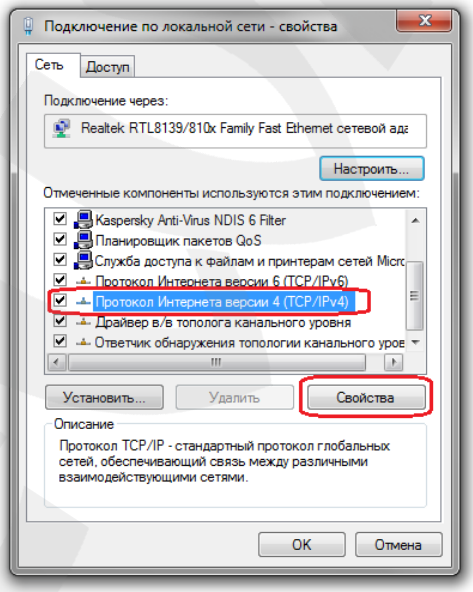

Рис. 5.5

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.

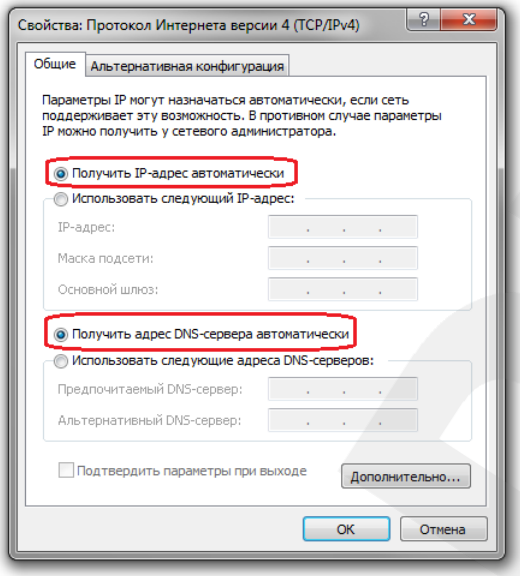

Рис. 5.6

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

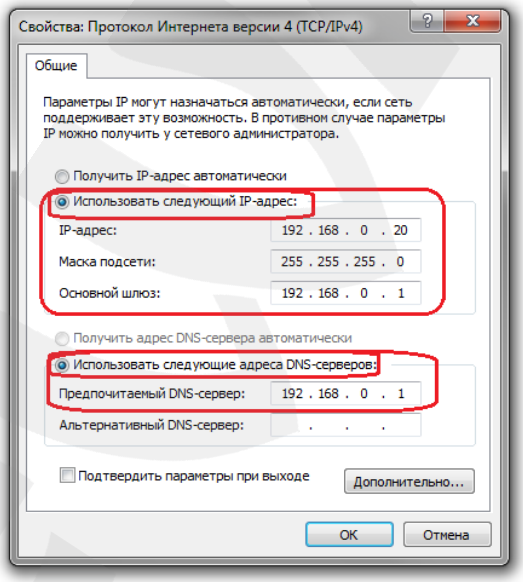

Рис. 5.7

Запомните либо запишите конфигурацию сетевых настроек адаптера Вашего ПК (IP-адрес, маска подсети, сетевой шлюз, DNS-сервер).

ВНИМАНИЕ!

Если Вы не записали данные текущего сетевого подключения, то после настройки камеры будет невозможно вернуть сетевые настройки компьютера в первоначальное состояние для 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).

Подключите компьютер (ноутбук) с помощью кабеля к Вашей локальной сети и дождитесь окончания процесса подключения.

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

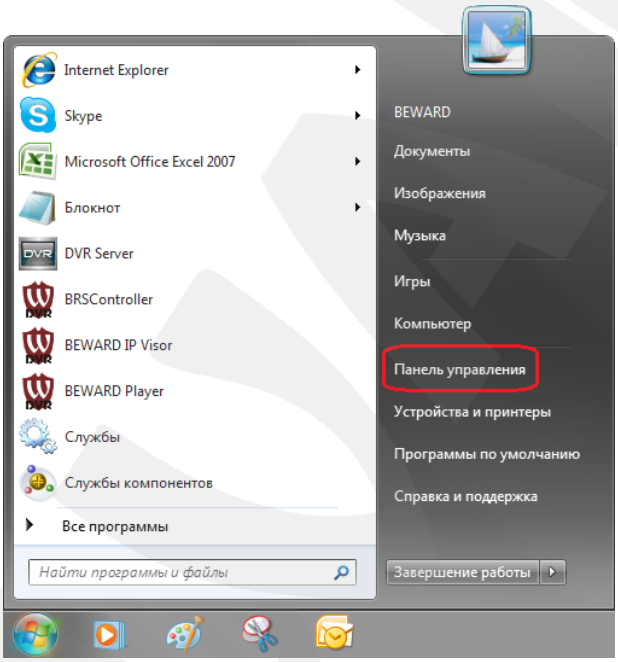

Рис. 5.8

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

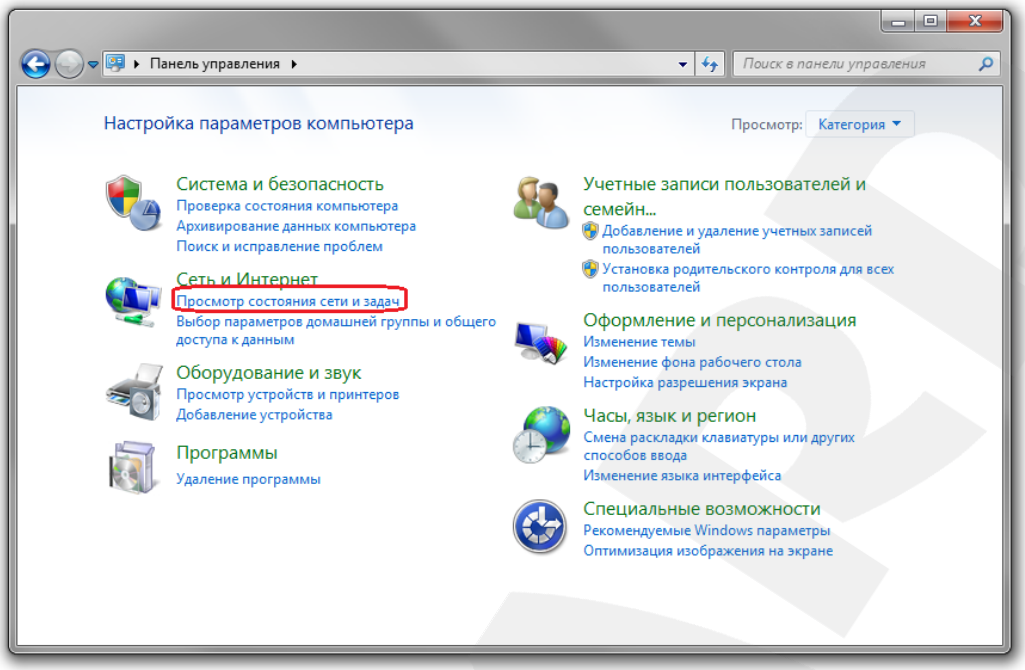

Рис. 5.9

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

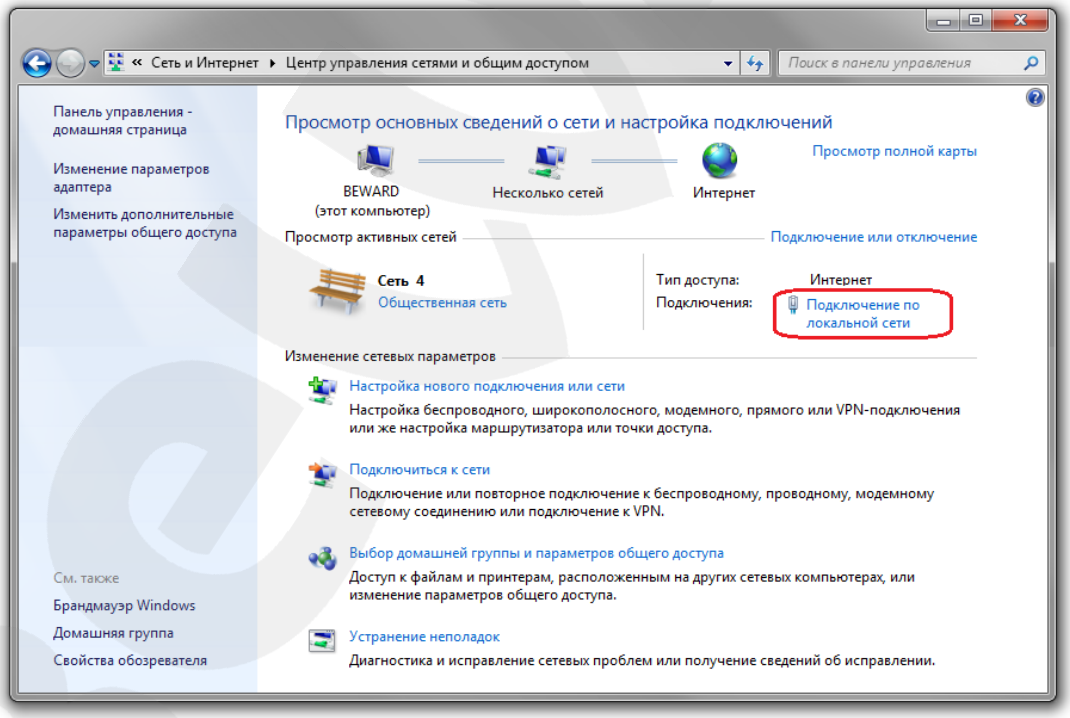

Рис. 5.10

ПРИМЕЧАНИЕ!

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

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

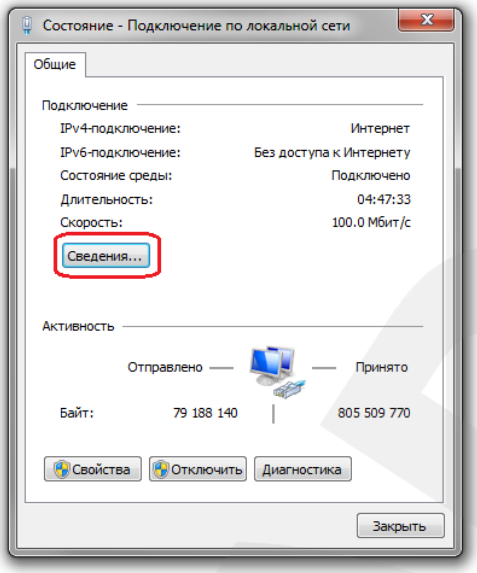

Рис. 5.11

В открывшемся окне можно увидеть информацию о текущем сетевом подключении (*Рис. 5.12*).

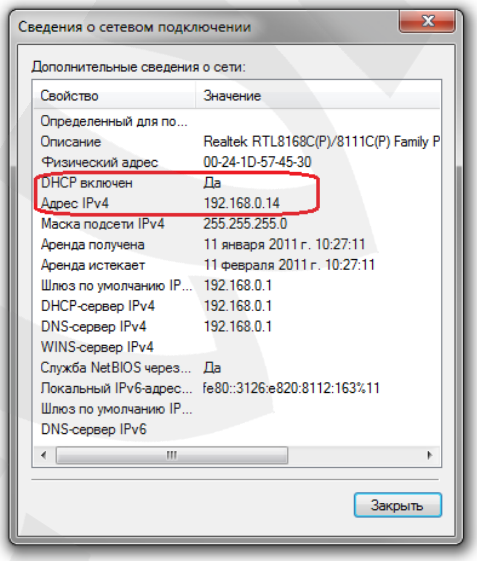

Рис. 5.12

Если в открывшемся окне Вы увидели следующие строки: **[DHCP включен]** – Да, **[Адрес IPv4– xxx.xxx.xxx.xxx]** (где xxx.xxx.xxx.xxx – значение IP-адреса), значит Вашему ПК для проводного соединения был назначен IP-адрес, значение которого указано в строке **[Адрес IPv4]**, маска подсети указана в строке **[Маска подсети IPv4]**, адрес сетевого шлюза - в строке **[Шлюз по умолчанию IPv4]**, адрес DNS-сервера - в строке **[DNS-сервер]**. Запомните либо запишите конфигурацию сетевых настроек адаптера Вашего ПК (IP-адрес, Маска подсети, Сетевой шлюз, DNS-сервер).

ВНИМАНИЕ!

Если Вы не записали данные текущего сетевого подключения, то после настройки камеры будет невозможно вернуть сетевые настройки компьютера в первоначальное состояние для подключения к локальной сети и/или сети Интернет!

ВНИМАНИЕ!

Если в открывшемся диалоговом окне **[Сведения о сетевом подключении]** Вы увидели следующие 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 сети по кабельному соединению (DHCP-сервер не присвоил IP-адрес Вашему ПК). Проверьте правильность подключения к проводной сети и в случае необходимости обратитесь к системному администратору Вашей сети.

5.2. Изменение параметров локальной сети для проводного подключения IP-камер

По умолчанию IP-камера N520 имеет IP-адрес 192.168.0.99. Для того 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 сетевых устройств в сети не должны совпадать.

ВНИМАНИЕ!

IP-камеры BEWARD N520 по умолчанию имеют IP-адрес 192.168.0.99! Если Вы планируете подключать несколько IP-камер, то для исключения конфликта IP-адресов подключайте камеры по одной и изменяйте их IP-адреса на любые свободные из Вашей локальной сети!

ВНИМАНИЕ!

Если Вы уверены, что сетевой адаптер Вашего ПК, подключенный в проводную сеть с IP-камерой либо напрямую к IP-камере, находится в одной подсети с IP-камерой, тогда Вы можете перейти к пункту 5.3 данного Руководства.

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

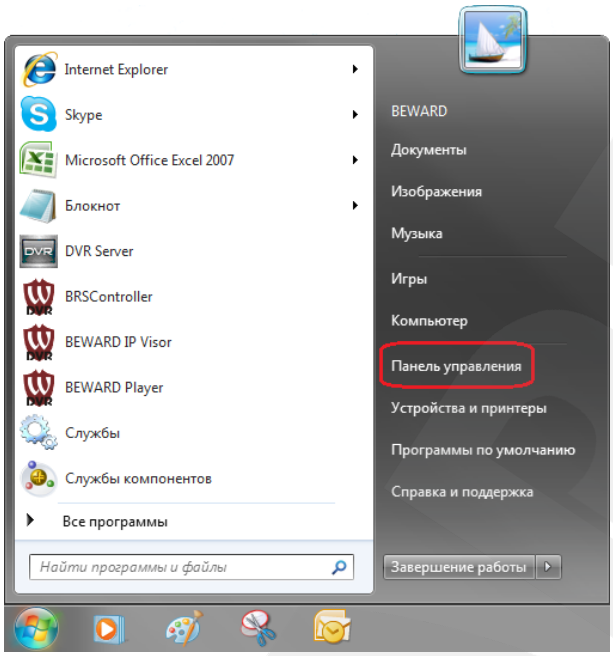

Рис. 5.13

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

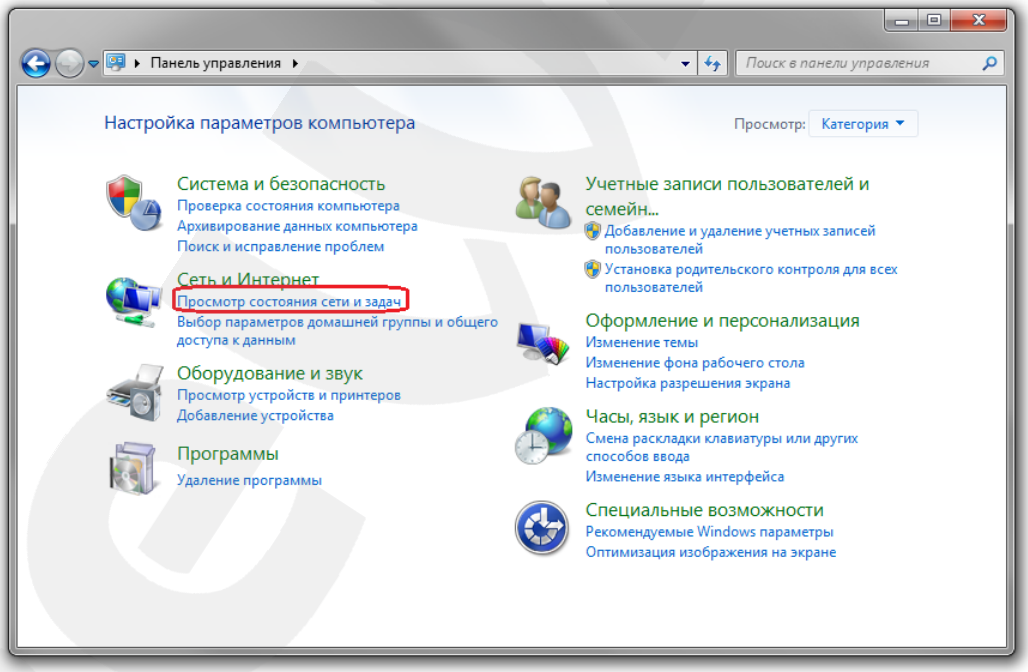

Рис. 5.14

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

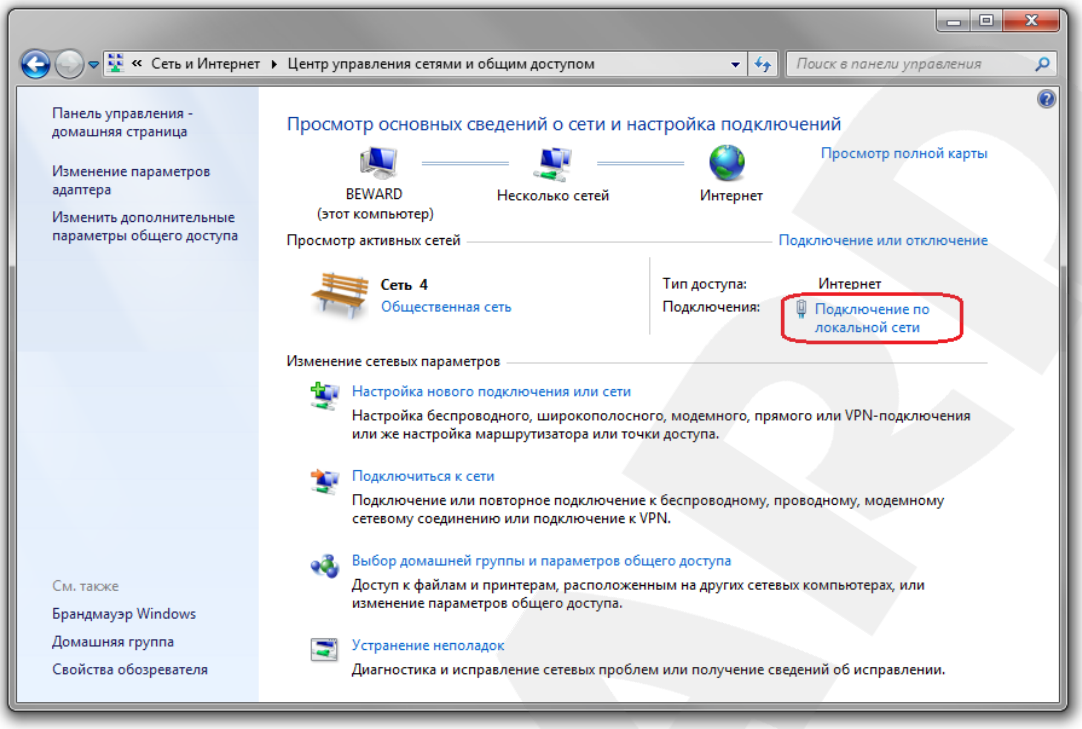

Рис. 5.15

ПРИМЕЧАНИЕ!

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

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

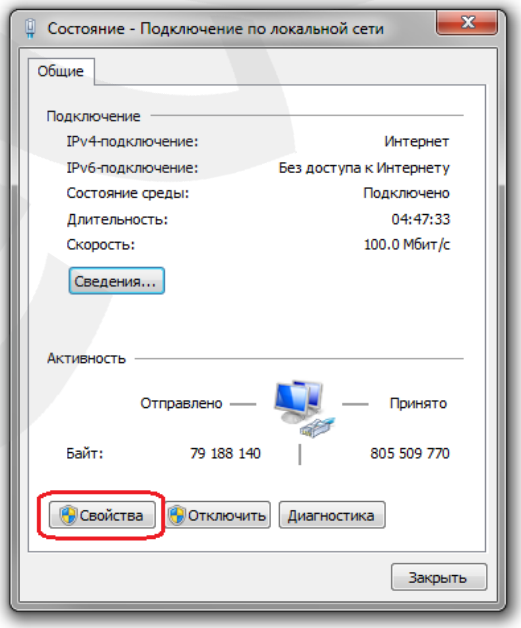

Рис. 5.16

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

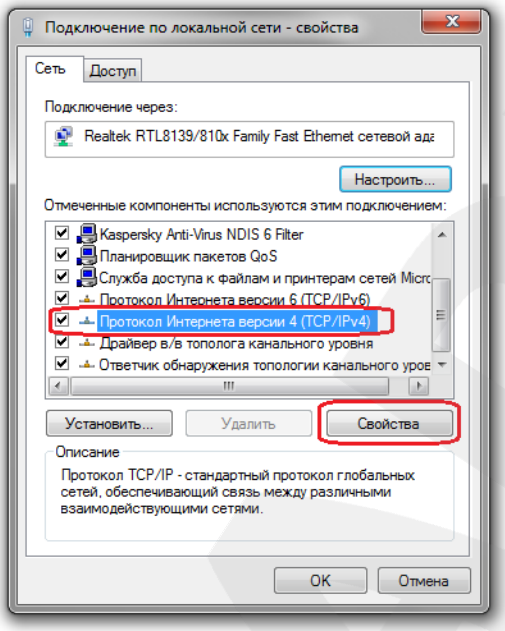

Рис. 5.17

Откроется меню, в котором 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, **[Маску подсети]** 255.255.255.0, остальные значения вводить нет необходимости (*Рис. 5.18*).

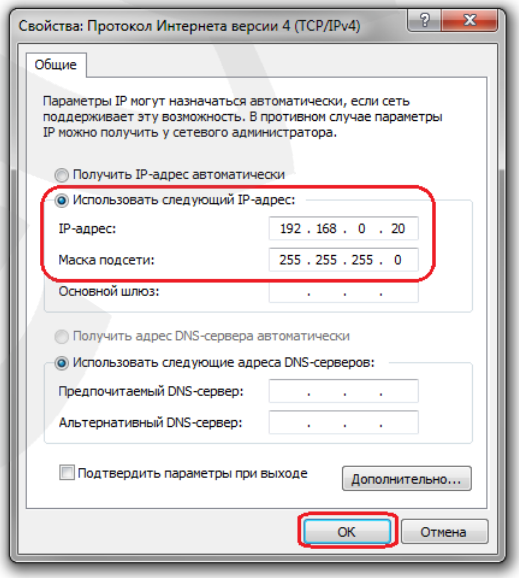

Рис. 5.18

Для применения изменений настроек нажмите кнопку **[OK]** для всех открытых окон.

5.3. Получение доступа к IP-камере

Получить доступ к IP-камере Вы можете следующими способами:

- с помощью ПО **«BEWARD IP Installer»**.
- с помощью меню **[Сеть]** ОС Windows 7.
- с помощью браузера Internet Explorer.

ВНИМАНИЕ!

При подключении IP-камеры к локальной сети необходимо учитывать, что по умолчанию IP-камера имеет сетевой адрес: 192.168.0.99.

5.3.1. Установка «BEWARD IP Installer»

Вставьте диск с программным обеспечением в привод CD-ROM. На экране появится меню установки (*Рис.5.19*).

Для установки программного обеспечения выберите **[BEWARD IP Installer]** и выполните процесс установки (подробно процесс установки описан в **«Руководстве по эксплуатации ПО BEWARD IP Installer»**).

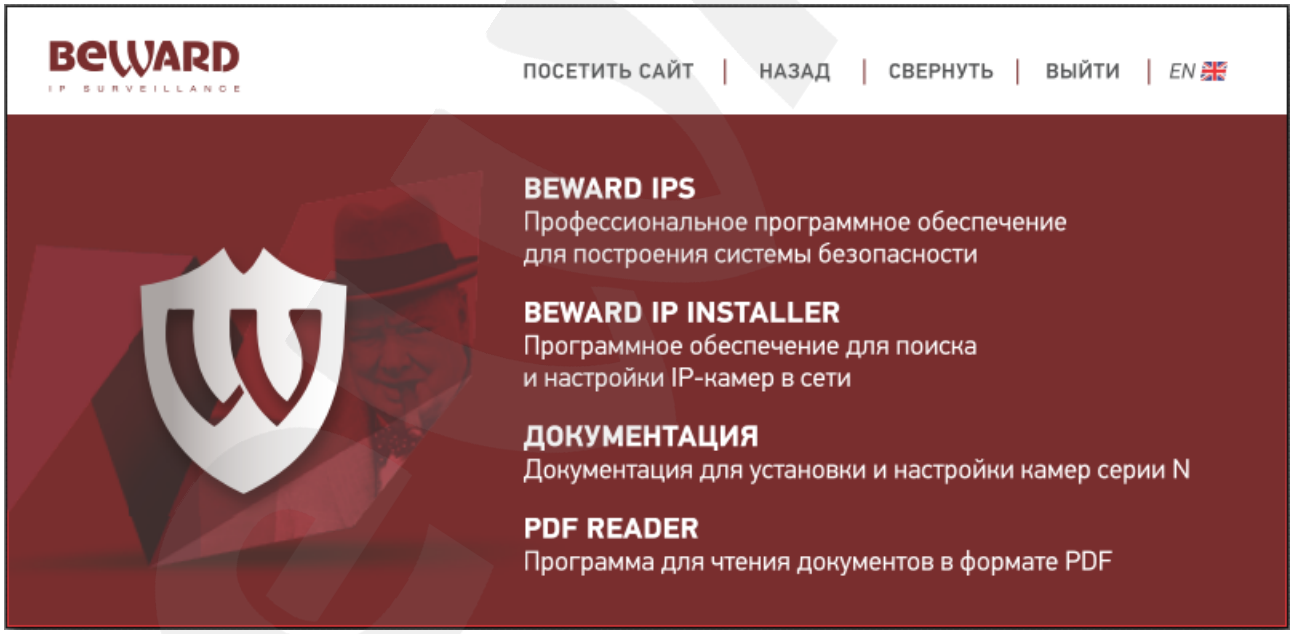

Рис. 5.19

5.3.2. Получение доступа к IP-камере с помощью ПО «BEWARD IP Installer»

ВНИМАНИЕ!

Для поиска IP-камер с помощью ПО **«BEWARD IP Installer»** должна быть включена поддержка технологии UPnP для Вашего ПК и для IP-камеры. Для ОС Windows 7 поддержка UPnP включена по умолчанию.

ПРИМЕЧАНИЕ!

Для IP-камер BEWARD N520 использование поддержки технологии UPnP включено по умолчанию.

Для поиска камеры с помощью ПО **«BEWARD IP Installer»** запустите программу при помощи ярлыка на рабочем столе. В открывшемся окне появится список всех активных камер и видеосерверов. Выберите требуемую IP-камеру и нажмите **[Открыть в IE]** (*Рис. 5.20*).

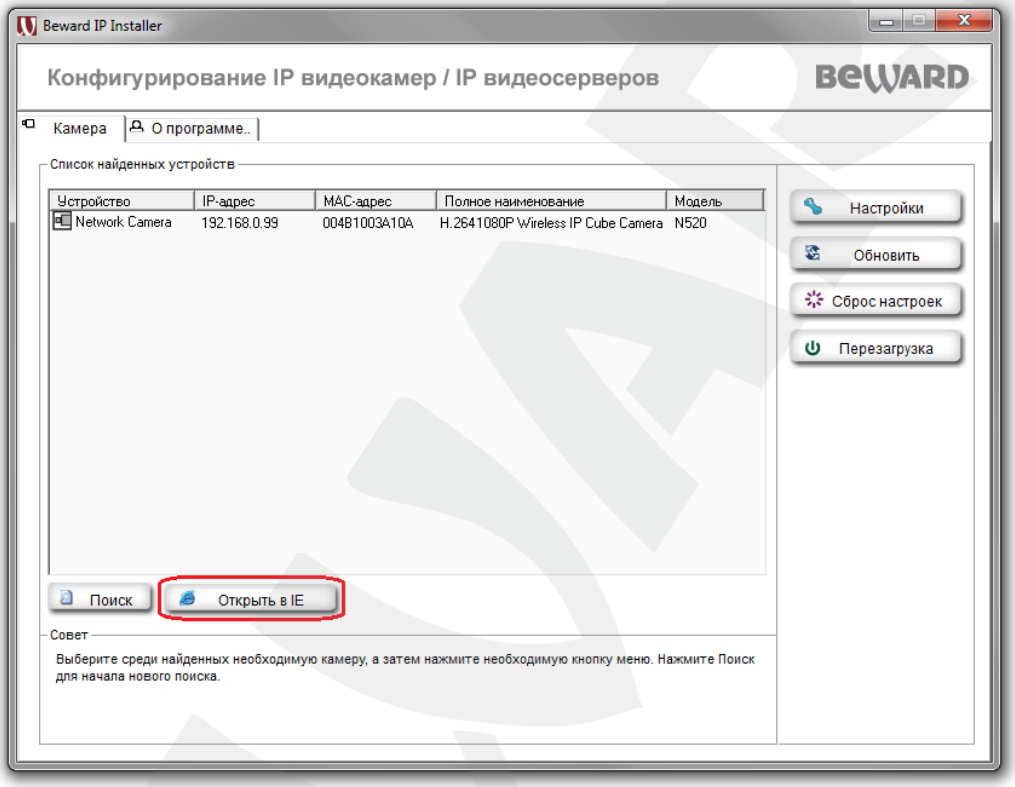

Рис. 5.20

ВНИМАНИЕ!

Для корректной работы BEWARD IP Installer необходимо добавить его в список доверенных приложений Вашего антивируса и сетевого экрана.

ПРИМЕЧАНИЕ!

В Windows 7 для корректной работы программы может потребоваться запуск BEWARD IP Installer от имени администратора. Для этого нажмите на ярлыке программы правой клавишей мыши и в появившемся контекстном меню выберите пункт **[Запуск от имени администратора]**.

ПРИМЕЧАНИЕ!

Если IP-устройство (или устройства) не появились в окне поиска, то нажмите кнопку **[Поиск]** для обновления списка (*Рис. 5.20*).

5.3.3. Получение доступа к IP-камере с помощью меню [Сеть] ОС Windows 7

ПРИМЕЧАНИЕ!
Для IP-камер BEWARD N520 использование поддержки технологии UPnP включено по умолчанию.

Для поиска камеры с помощью меню **[Сеть]** ОС Windows 7 откройте окно **[Мой компьютер]** и выберите пункт **[Сеть]** (*Рис. 5.21*).

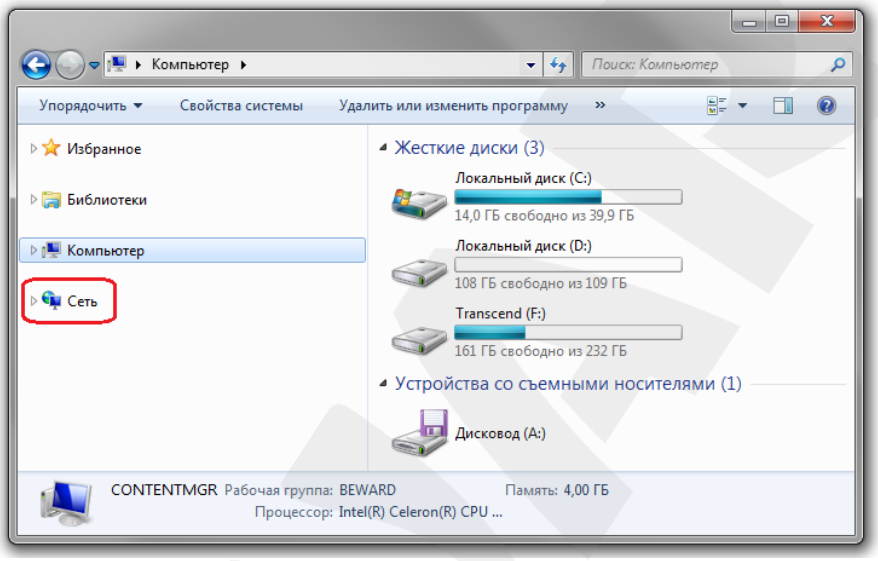

Рис 5.21

В появившемся меню найдите интересующее Вас устройство и нажмите на нем два раза левой кнопкой мыши (*Рис. 5.22*).

После этого IP-камера N520 откроется в браузере, который установлен по умолчанию.

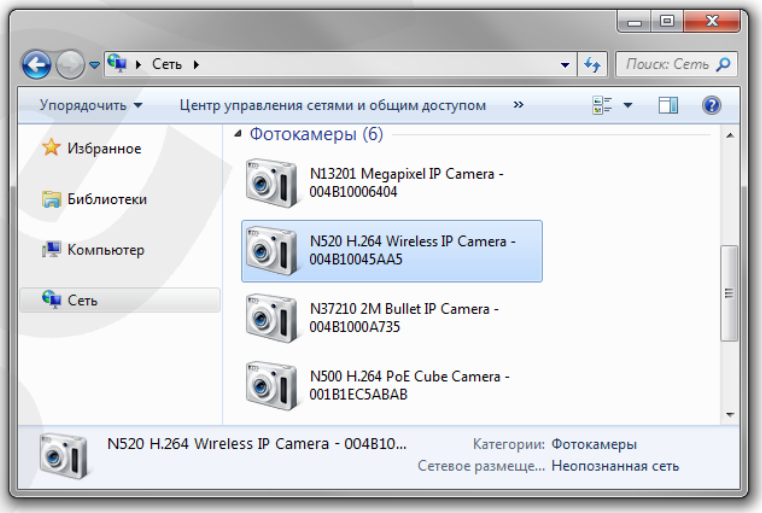

Рис 5.22

5.3.4. Получение доступа к IP-камере с помощью браузера Internet Explorer

Для доступа к камере с помощью браузера Internet Explorer необходимо запустить браузер и в адресной строке ввести запрос: **http://<IP>:<port>/**;, где **<IP>** – IP-адрес камеры, а **<port>** – значение http-порта), после чего нажать **[Перейти]** либо **[Ввод]** (*Рис. 5.23*).

ВНИМАНИЕ!

IP-камера BEWARD N520 по умолчанию имеет сетевой адрес 192.168.0.99, http-порт 80.

ПРИМЕЧАНИЕ!

Если для http-порта используется значение 80, тогда для доступа к камере в браузере достаточно ввести строку http://<IP>/, где <IP> – IP-адрес камеры.

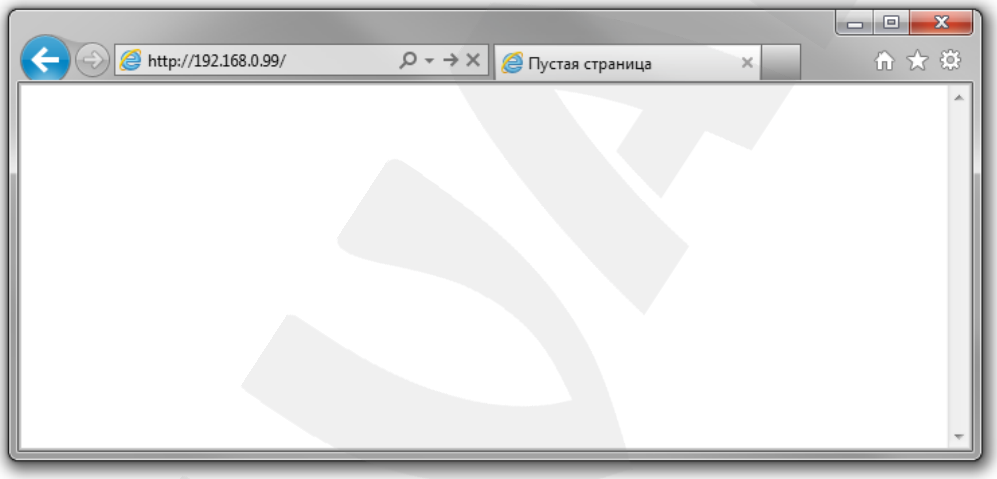

Рис. 5.23

5.4. Получение доступа к веб-интерфейсу IP-камеры

После того как Вы получили доступ к IP-камере любым из способов, рассмотренных в пунктах 5.3.2, 5.3.3, 5.3.4 данного Руководства, будет запущен браузер Internet Explorer, где откроется окно авторизации для получения доступа к веб-интерфейсу устройства.

ПРИМЕЧАНИЕ!

Для корректной работы веб-интерфейса IP-камеры необходима версия браузера Internet Explorer не ниже 9.0.

Введите имя пользователя и пароль, после чего нажмите **[OK]** (*Рис. 5.24*).

ВНИМАНИЕ!

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

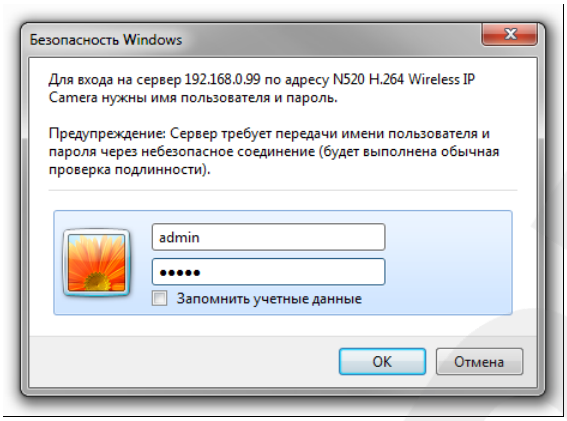

Рис. 5.24

После удачной авторизации при первом подключении ОС Windows 7 будет блокировать установку приложения ActiveX (необходимо для просмотра изображения с камеры), о чем будет свидетельствовать системное уведомление в нижней части окна Internet Explorer: **«Этот веб-сайт пытается установить следующую надстройку: «AxMediaControl.cab» от «BEWARD Co., Ltd»**. Нажмите на кнопку **[Установить]** для продолжения установки (*Рис. 5.25*).

ВНИМАНИЕ!

Установка компонентов ActiveX возможна только на 32-битную версию браузера Internet Explorer.

ПРИМЕЧАНИЕ!

В операционной системе, отличной от Windows 7, или в браузере, отличном от Internet Explorer 9.0, названия меню или системные сообщения могут отличаться от названий меню и системных сообщений в других ОС семейства Windows или в других браузерах.

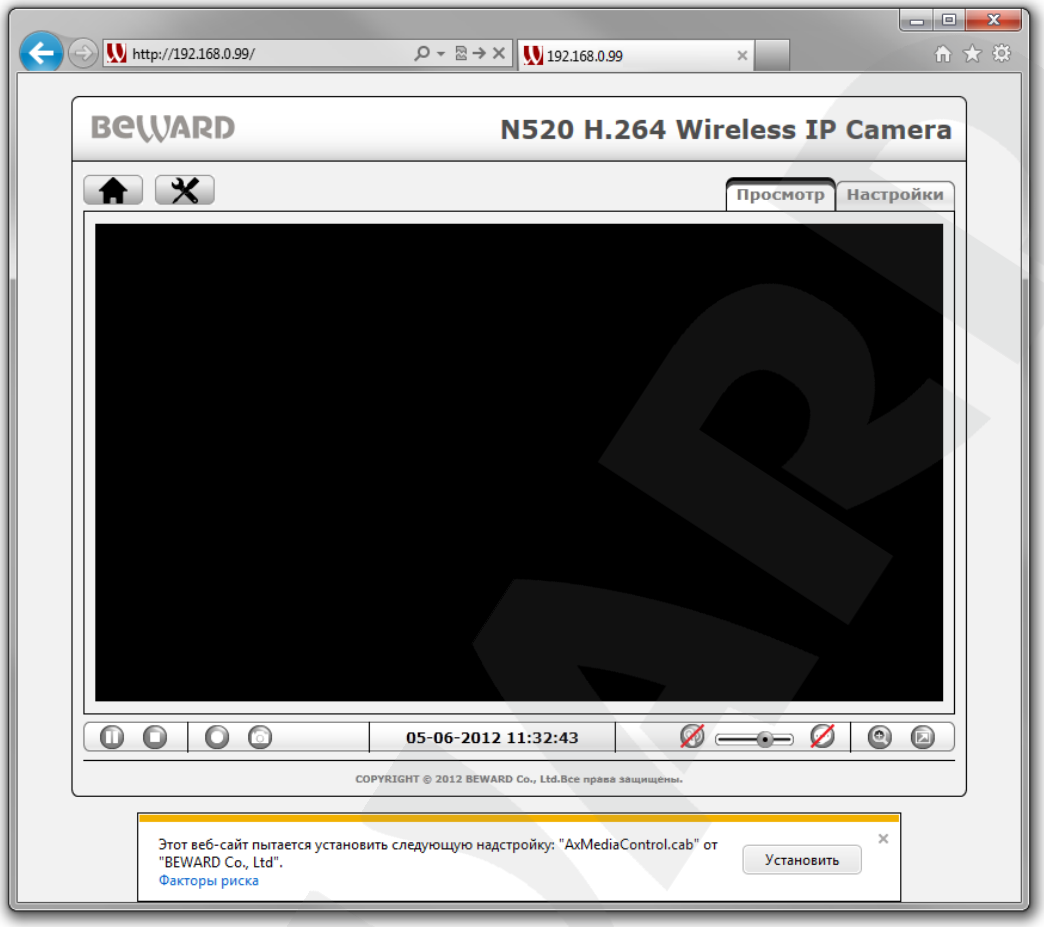

Рис. 5.25

Система безопасности браузера Internet Explorer также будет автоматически блокировать установку ActiveX. Для продолжения установки нажмите кнопку **[Установить]** в окне подтверждения установки (*Рис. 5.26*).

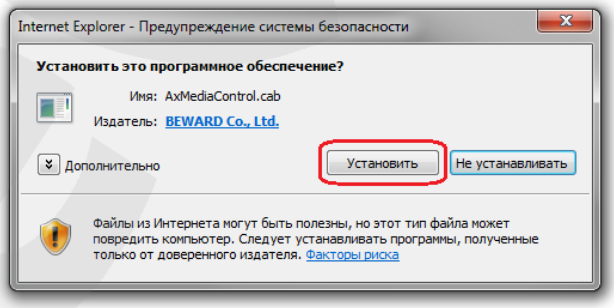

Рис. 5.26

ПРИМЕЧАНИЕ!

При установке ActiveX для ОС Windows 7 при включенном контроле учетных записей будет дополнительно производиться блокировка установки, о чем пользователю будет выдаваться дополнительное оповещение. Для разрешения установки необходимо положительно ответить в появившемся диалоговом окне.

При правильно выполненных действиях Вы сможете увидеть изображение с Вашей IP-камеры через веб-браузер *(Рис. 5.27)*.

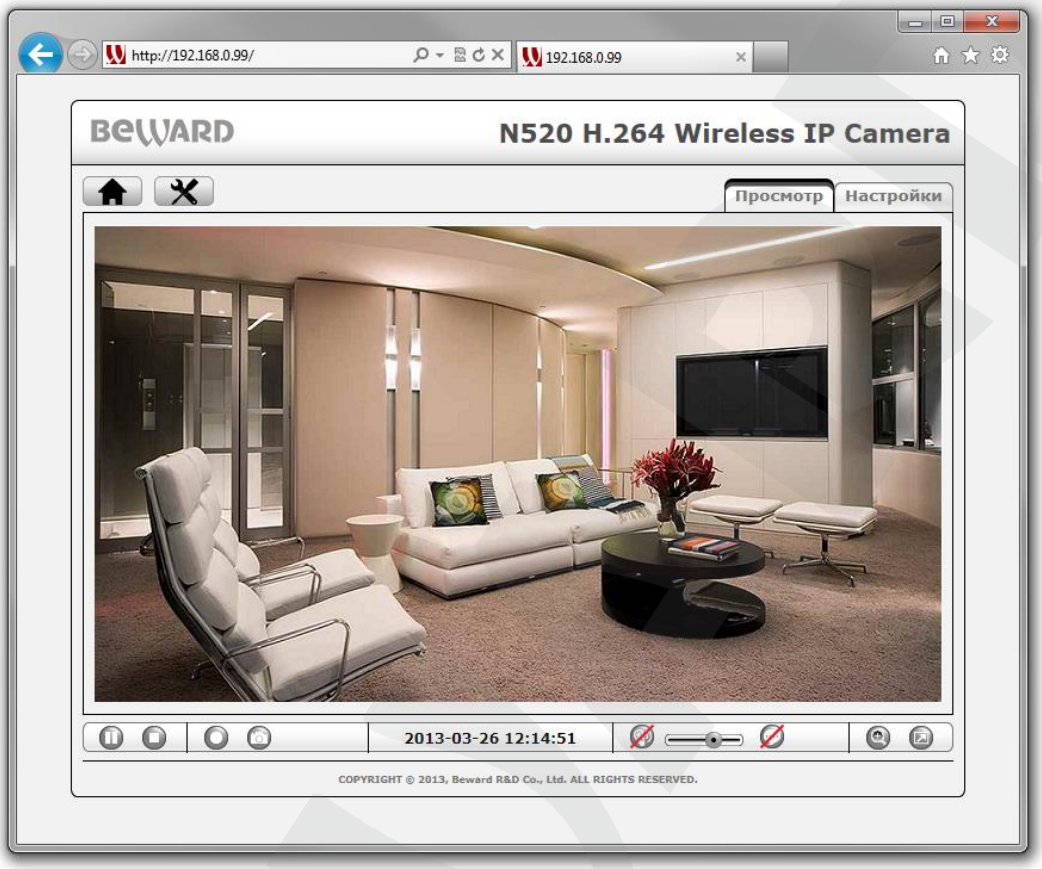

Рис. 5.27

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

После подключения к IP-камере N520 по проводной сети необходимо изменить настройки камеры таким образом, чтобы она находилась в одной подсети с остальным оборудованием (например, Вашим ПК).

ВНИМАНИЕ!

Для работы IP-камеры и Вашего ПК необходимо, чтобы совпадали три части IP-адреса, за исключением четвертой части, и чтобы полностью совпадала маска подсети.

Например, IP-адрес Вашего ПК: 192.168.50.40. IP-адрес разделен точками на четыре октета. В данном примере: 1 октет – 192, 2 октет – 168, 3 октет – 50, 4 октет – 40. Вам необходимо изменить IP-адрес камеры так, чтобы их первые три октета совпадали, то есть, чтобы IP-адреса имели вид 192.168.50.XX. Четвертый октет обязательно должен быть отличным от значения IP-адреса Вашего ПК, а также любого другого оборудования в Вашей сети (если таковое имеется).

Для изменения сетевых настроек в веб-интерфейсе нажмите в главном меню камеры кнопку **[Настройки]** и перейдите в меню ***Сеть – Основные*** (*Рис. 5.28*).

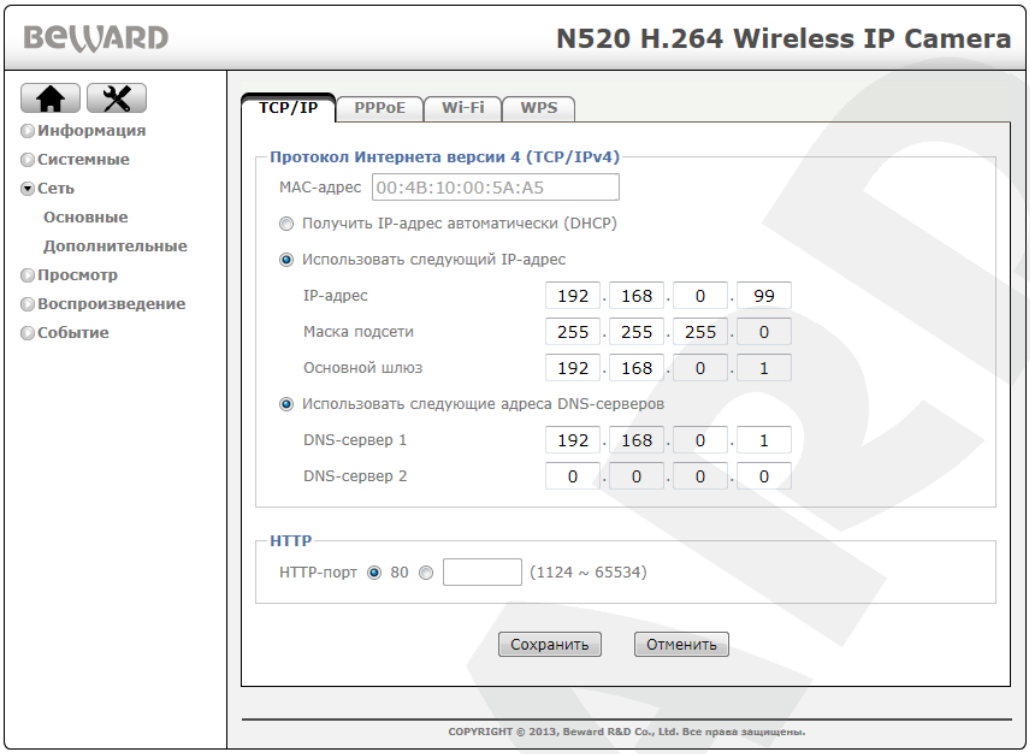

Рис. 5.28

Во вкладке **[TCP/IP]** нужно ввести такие значения IP-адреса и других сетевых параметров для IP-камеры, чтобы она находилась в одной подсети с остальным оборудованием.

ПРИМЕЧАНИЕ!

В случае необходимости для назначения сетевых настроек устройствам обратитесь к Вашему сетевому администратору.

Для сохранения изменений сетевых настроек проводного соединения нажмите кнопку **[Сохранить]**, после чего в появившихся окнах необходимо нажать кнопку **[OK]**.

На этом настройка проводного соединения для IP-камеры завершена.

5.6. Возврат сетевых настроек ПК к первоначальным значениям

Чтобы вернуть настройки сетевого подключения к прежним значениям, выполните следующие действия.

Нажмите ***Пуск – Панель управления*** (*Рис. 5.29*).

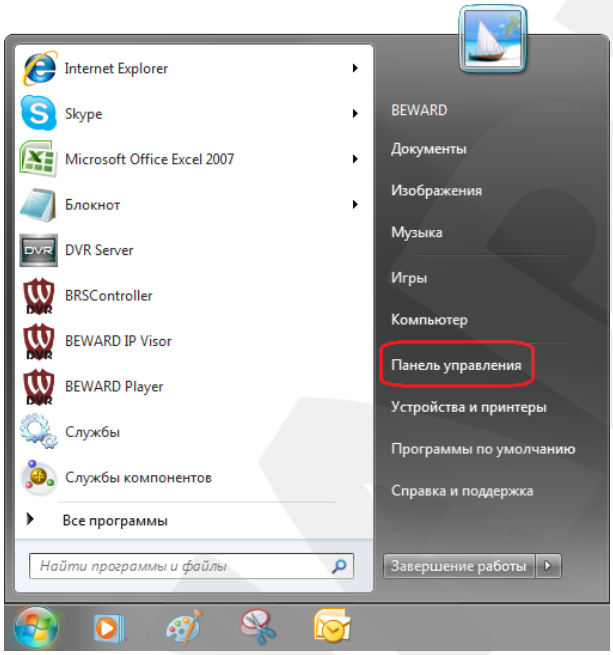

Рис. 5.29

В открывшемся диалоговом окне выберите пункт **[Просмотр состояния сети и задач]** в разделе **[Сеть и Интернет]** (*Рис. 5.30*).

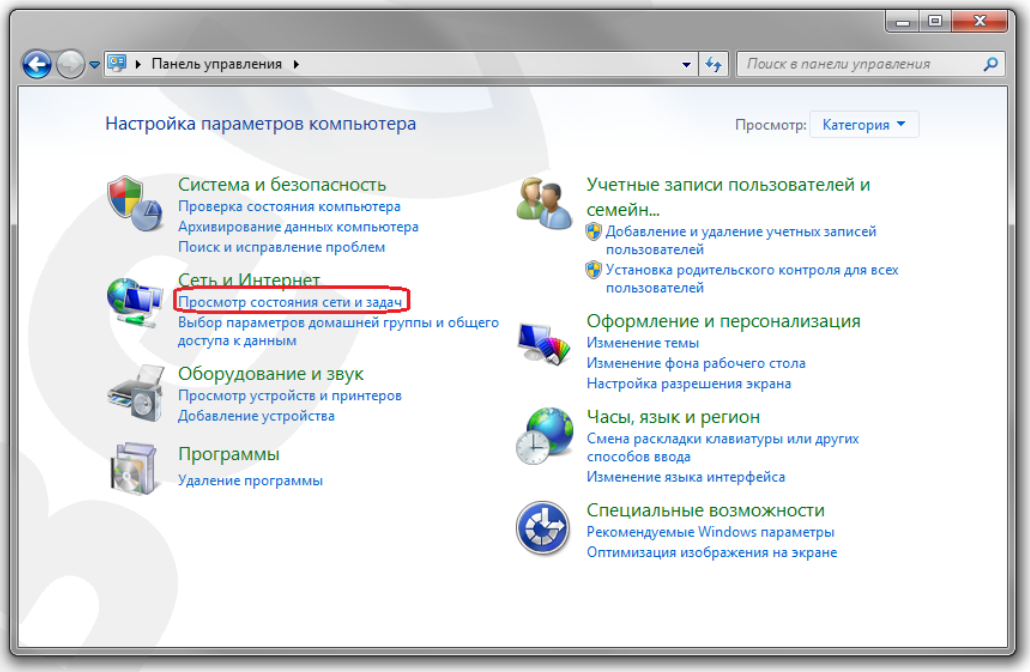

Рис. 5.30

В открывшемся окне нажмите **[Подключение по локальной сети]** (*Рис. 5.31*).

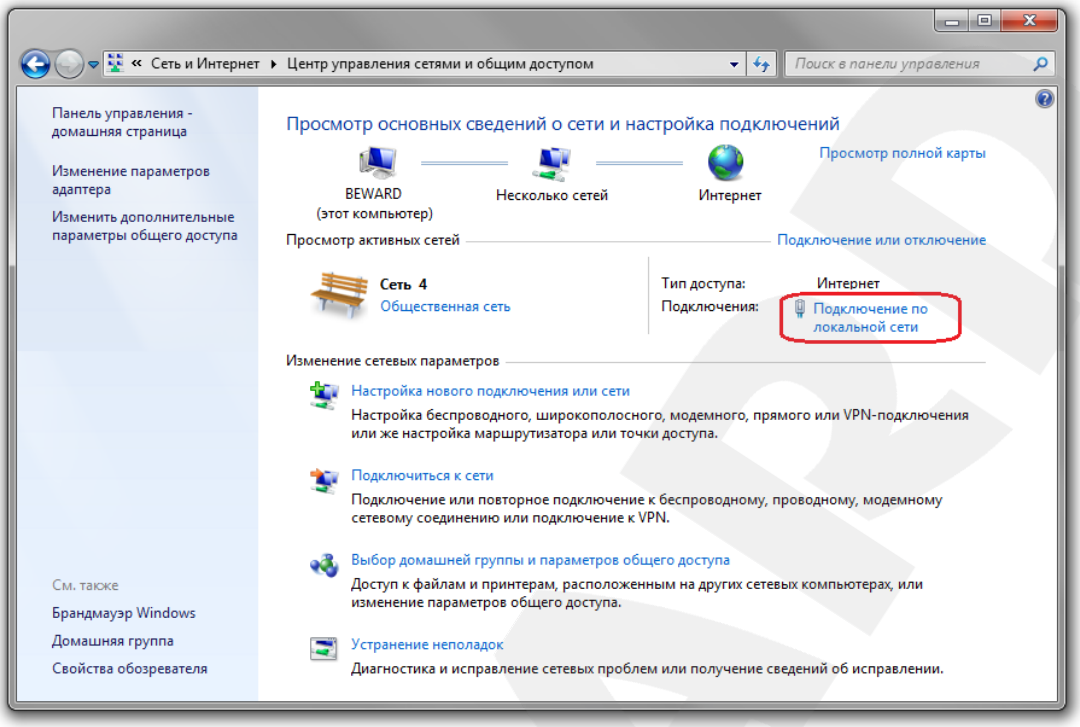

Рис. 5.31

В открывшемся окне нажмите кнопку **[Свойства]** (*Рис.5.32*).

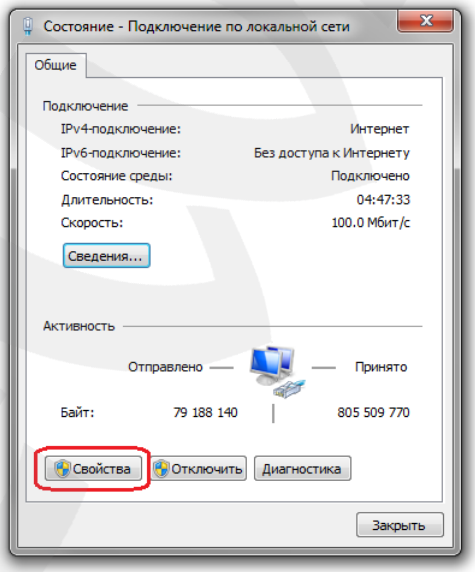

Рис. 5.32

В открывшемся окне свойств сетевого подключения необходимо выбрать пункт **[Протокол Интернета версия 4 (TCP/IPv4)]** и нажать кнопку **[Свойства]** (*Рис. 5.33*).

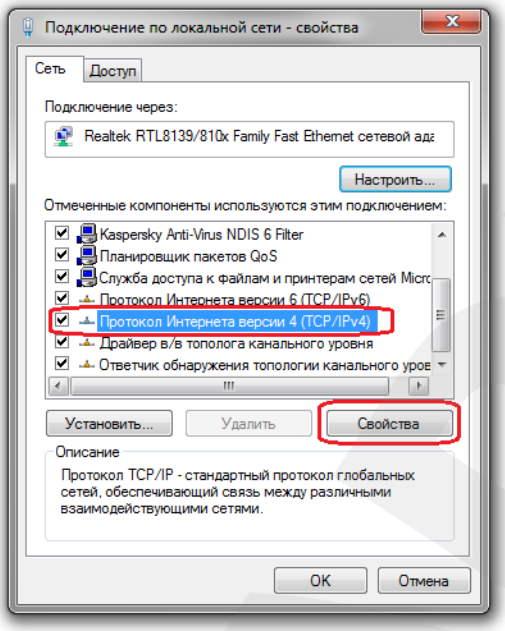

Рис. 5.33

Откроется меню, в котором необходимо задать значения сетевых настроек, установленных изначально (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 **[OK]** для всех открытых окон (*Рис. 5.34*).

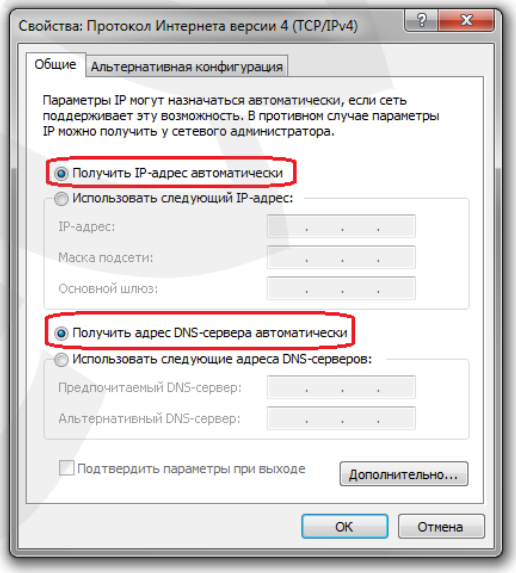

Рис. 5.34

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 **[OK]** для всех открытых окон (*Рис. 5.35*).

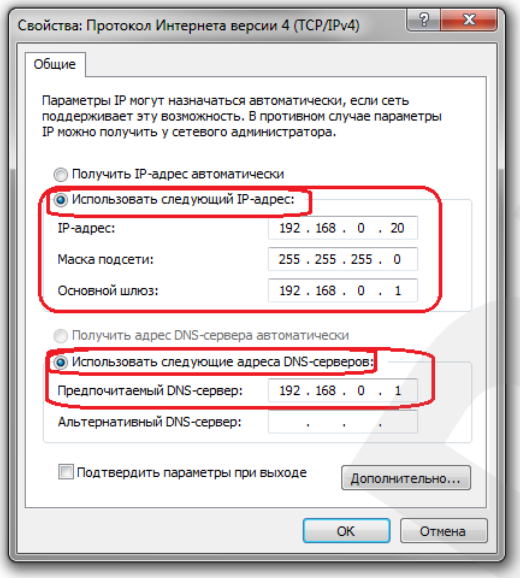

Рис. 5.35

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 Internet Explorer.

Запустите браузер Internet Explorer. Для этого нажмите ***Пуск – Все Программы*** и выберите строку **[Internet Explorer]**.

Введите в адресной строке IP-адрес, присвоенный камере (например: http://192.168.0.99) (*Рис. 5.36*).

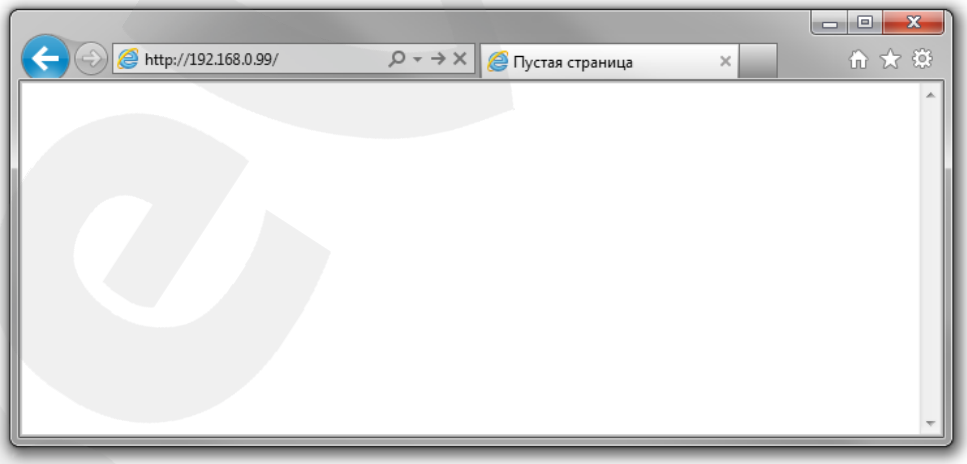

Рис. 5.36

При правильных настройках откроется меню авторизации. Для авторизации введите имя пользователя и пароль, после чего нажмите **[OK]** (*Рис. 5.37*).

ВНИМАНИЕ!

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

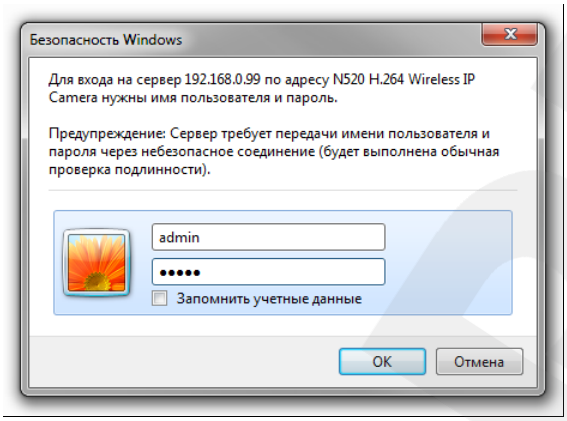

Рис. 5.37

При правильно выполненных действиях Вы сможете зайти в веб-интерфейс через браузер и увидеть изображение с Вашей IP-камеры (*Рис. 5.38*).

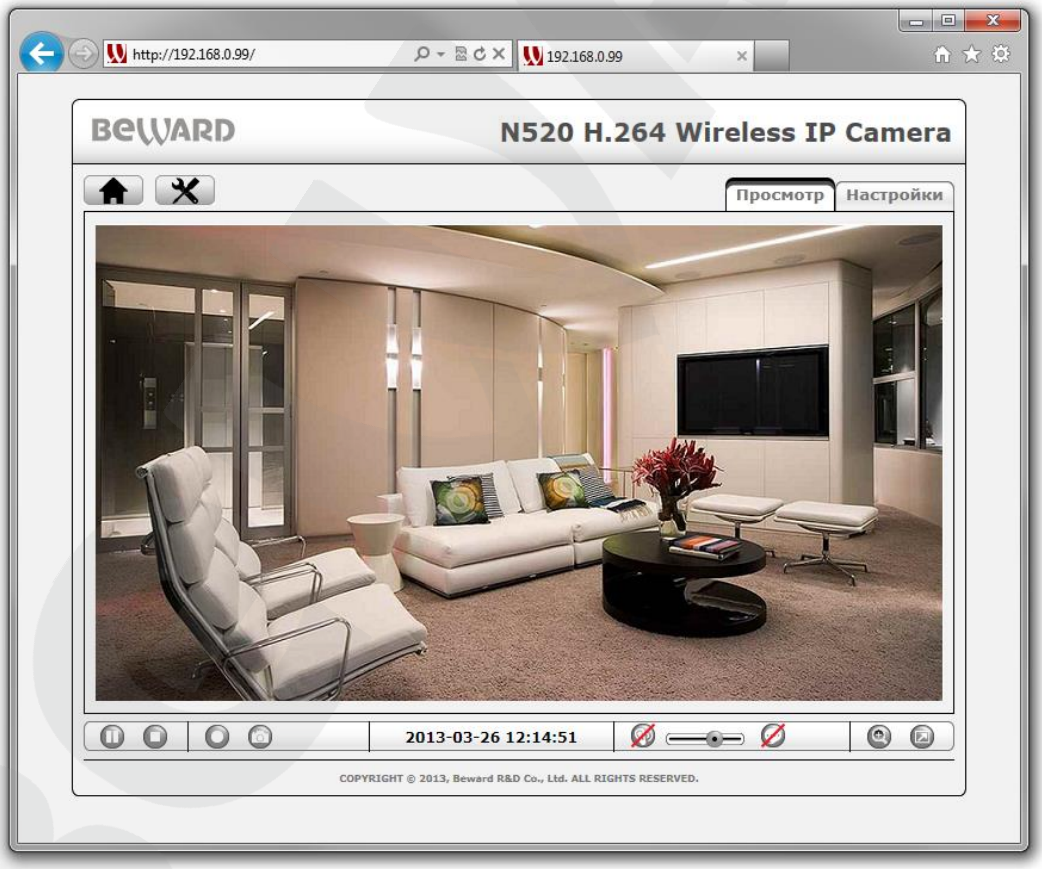

Рис. 5.38

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 системному администратору Вашей сети.

Глава 6. Настройка Wi-Fi-соединения

6.1. Общие сведения о беспроводном Wi-Fi подключении IP-камеры N520

Для того чтобы IP-камера BEWARD N520 работала в Вашей беспроводной Wi-Fi сети совместно с Вашими компьютерами, ноутбуками и другим оборудованием, необходимо включить IP-камеру в сеть в соответствии с текущими настройками данной беспроводной сети. Подключение можно выполнить следующими способами:

- Подключить IP-камеру, используя технологию WPS, которая позволяет автоматически получить данные, требуемые системой защиты беспроводной сети (при условии, что сеть является защищенной).

ВНИМАНИЕ!
Настройка IP-камеры с помощью функции WPS возможна только при условии, что маршрутизатор, к которому Вы хотите подключиться по Wi-Fi, поддерживает данную функцию.

- Подключится к камере без использования технологии WPS. Для этого необходимо сначала определить настройки требуемого Wi-Fi соединения при помощи:
  меню настроек Вашего маршрутизатора (см. инструкцию по эксплуатации Вашего маршрутизатора) или при помощи другого оборудования, подключенного к нему (например, ноутбука).

6.2. Подключение к беспроводной Wi-Fi сети с помощью WPS

Способы подключения к беспроводной Wi-Fi сети с помощью WPS можно условно разделить на два типа:

- Способ настройки, при котором необходимо сделать соответствующие изменения в веб-интерфейсе IP-камеры, а также в веб-интерфейсе того Wi-Fi маршрутизатора, к которому Вы собираетесь подключиться.
- Способ настройки беспроводного соединения, при котором нет необходимости заходить в веб-интерфейс Wi-Fi устройств, а достаточно лишь поочередно нажать кнопки WPS на корпусах Wi-Fi устройств.

Оба способа подключения более подробно описаны ниже.

6.2.1 Подключение с использованием веб-интерфейса IP-камеры

Получите доступ к веб-интерфейсу IP-камеры любым из способов проводного соединения, описанных в пункте 5.3 данного Руководства.

В открывшемся окне введите имя пользователя и пароль (*Рис. 6.1*).

ВНИМАНИЕ!

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

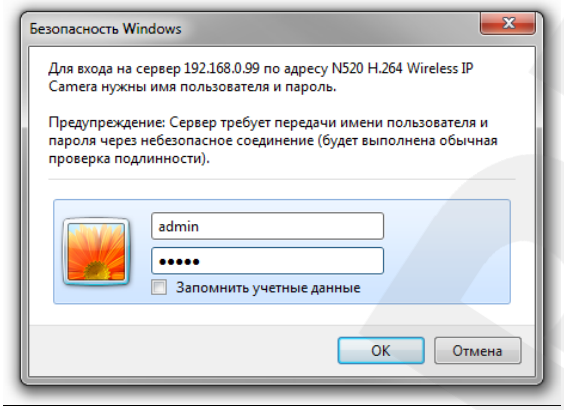

Рис. 6.1

После успешной авторизации в браузере появится главное меню веб-интерфейса IP-камеры. Нажмите в этом меню кнопку **[Настройки]** (*Рис. 6.2*).

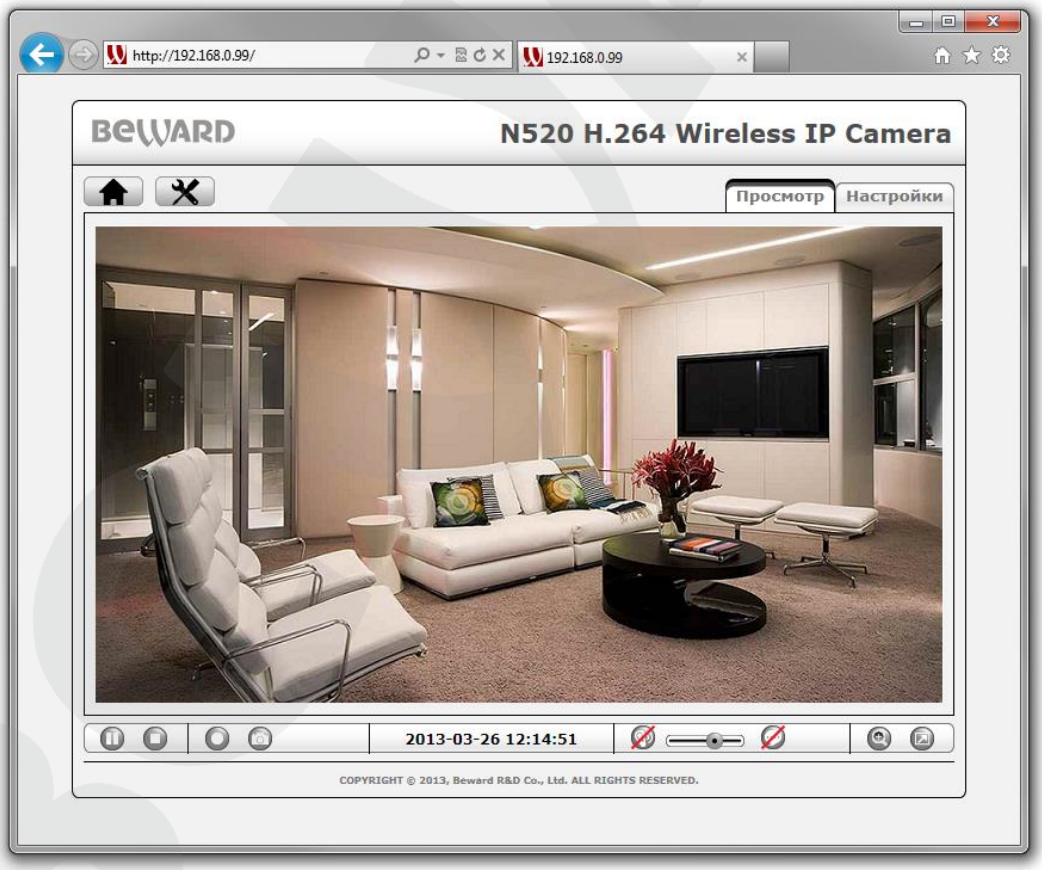

Рис. 6.2

Затем перейдите в меню ***Сеть – Основные – WPS***. Для включения функции **WPS** в данном меню выберите опцию **«Включено»**, после чего станут доступны пункты, показанные на *Рисунке 6.3*.

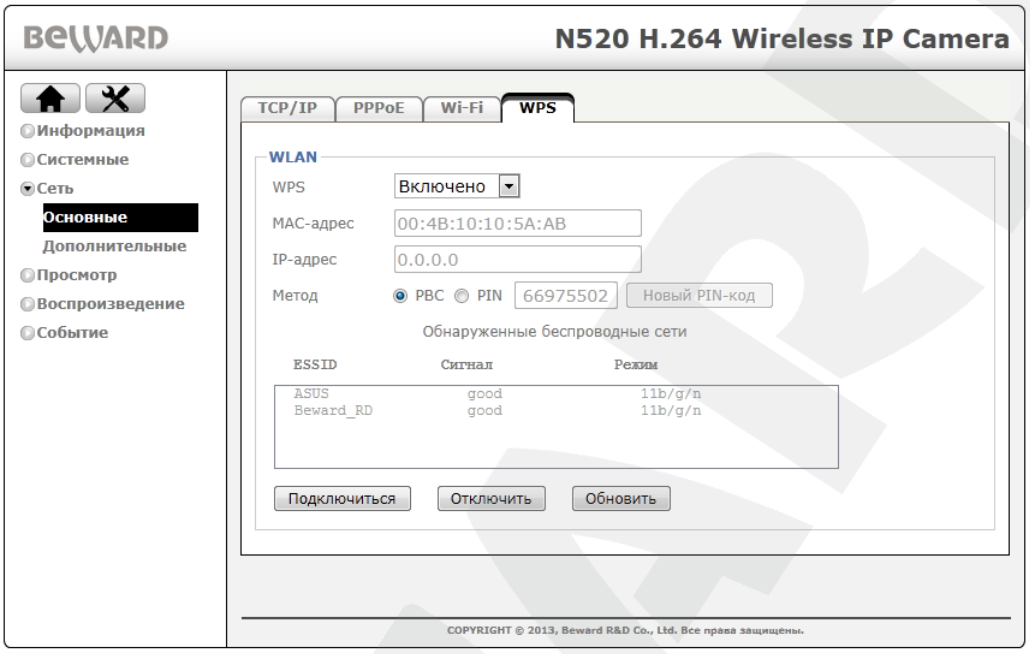

Рис. 6.3

Поле **[Обнаруженные беспроводные сети]** предназначено для отображения доступных к подключению беспроводных сетей с помощью функции WPS.

ВНИМАНИЕ!

Беспроводные сети с функцией WPS отображаются в данном поле только тогда, когда данная функция включена на маршрутизаторе и находится в данный момент в активном состоянии. На некоторых моделях маршрутизаторов активное состояние WPS длится 2 минуты. Подробное описание работы функции WPS для Вашего маршрутизатора должно находиться в прилагаемой к нему инструкции.

В пункте меню **[Метод]** для выбора доступны два метода настройки:

- **[PBC]**: это способ настройки беспроводного соединения через WPS путем поочередного нажатия кнопки WPS на обоих устройствах. После нажатия кнопки необходимо подождать некоторое время, пока завершится процесс передачи настроек между маршрутизатором и IP-камерой. Как правило, у большинства Wi-Fi устройств с поддержкой технологии WPS процедура передачи и применения сетевых настроек длится примерно 2 минуты.
- **[PIN]**: данный способ отличается от способа **[PBC]** тем, что для настройки беспроводного соединения необходимо ввести PIN-код, сгенерированный IP-камерой, в соответствующие настройки WPS на маршрутизаторе, после чего

настройки беспроводного соединения будут переданы не любому Wi-Fi устройству с поддержкой WPS, а только Вашей IP-камере, на которой был сгенерирован PIN-код. PIN-код отображается в небольшом поле рядом с положением переключателя **[PIN]**. Для создания нового PIN-кода используйте кнопку **[Новый PIN-код]** (*Рис 6.3*).

ПРИМЕЧАНИЕ!

При запуске процесса поиска и настройки подключения IP-камеры индикатор питания камеры мигает розовым цветом.

ВНИМАНИЕ!

Подробное описание ввода PIN-кода для конкретной модели маршрутизатора в рамках данного Руководства не рассматривается, так как предполагается, что оно описано в инструкции к маршрутизатору. Такая инструкция может находиться на сайте производителя Вашего маршрутизатора или идти в его комплектации.

Если выбран метод настройки **[PBC]**, то для установки соединения следует выполнить следующие шаги:

Шаг 1: включите функцию WPS на Вашем маршрутизаторе. Для этого есть два способа:

- физически нажать кнопку WPS на корпусе Вашего маршрутизатора.
- нажать кнопку в настройках веб-интерфейса Вашего маршрутизатора.

Выбор способа включения активного состояния WPS не имеет значения. После выполнения данного шага длительность активного состояния WPS будет продолжаться ограниченный промежуток времени, и Вам будет необходимо за это время выполнить остальные шаги (обычно на это отводится достаточно времени – около 2-х минут).

Шаг 2: нажмите кнопку **[Обновить]** в меню настроек камеры ***Сеть – Основные – WPS***, затем дождитесь появления в списке Вашей беспроводной сети (*Рис. 6.4*).

Шаг 3: выберите в списке Вашу беспроводную сеть, в данном примере это **BEWARD**.

Шаг 4: нажмите кнопку **[Подключиться]**, после чего на экране появится окно ожидания настройки подключения (*Рис.6.4*).

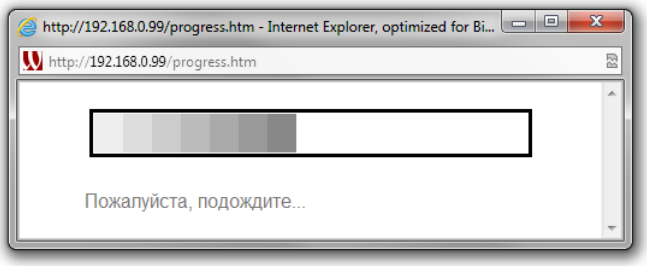

Рис 6.4

Шаг 5: подождите около двух минут для завершения операции настройки.

После выполнения **Шага 4** появится окно, отображающее ход подключения (*Рис 6.4*). Пока данное окно открыто, между маршрутизатором и IP-камерой происходит установка беспроводного соединения. В случае успешного завершения настройки соединения в окне появится надпись вида: **«Connecting to AP(BEWARD)...success!»** (*Рис 6.5*). В скобках указано имя маршрутизатора (точки доступа), к которому произошло подключение, в данном примере это **BEWARD**.

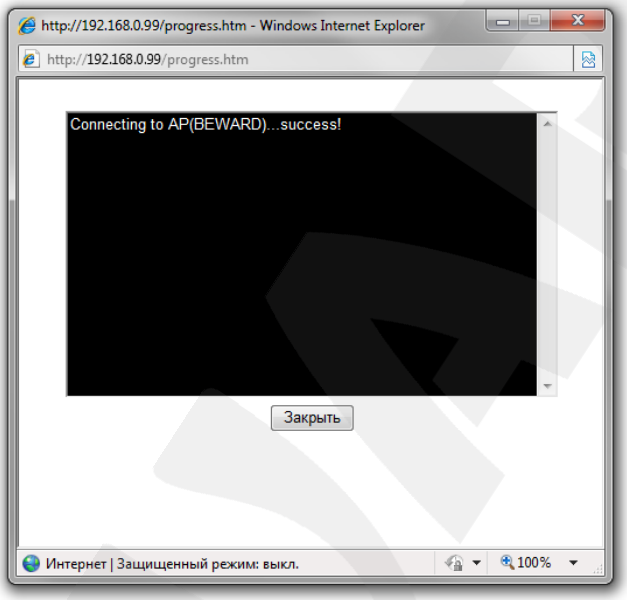

Рис 6.5

Если подключение прошло неудачно, то по окончании операции в данном окне появится надпись: **«Fail!»** (*Рис 6.6*). В этом случае попробуйте повторно провести настройку, предварительно закрыв окно об ошибке.

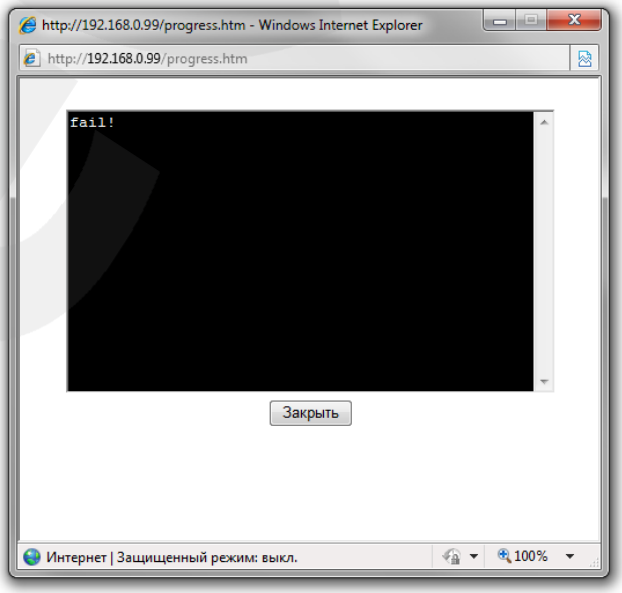

Рис 6.6

Для повторной настройки повторите шаги для подключения методом **[PBC]** (с 1 по 5). Если по каким-то причинам Вам не удается настроить беспроводное соединение, обратитесь за помощью к Вашему системному администратору.

Если выбран метод настройки **[PIN]**, то для установки соединения следует выполнить следующие шаги:

Шаг 1: сгенерируйте и запомните PIN-код с IP-камеры, при необходимости запишите его или скопируйте.

Шаг 2: зайдите в веб-интерфейс маршрутизатора (точки доступа) и на соответствующей странице настроек (WPS) введите PIN-код IP-камеры в поле **PIN-код клиента** (см. руководство пользователя для маршрутизатора).

Шаг 3: нажмите в этом же меню маршрутизатора соответствующую кнопку для запуска настройки **WPS** (см. руководство пользователя для маршрутизатора).

Шаг 4: нажмите кнопку **[Обновить]** в меню настроек камеры ***Сеть – Основные – WPS*** и дождитесь появления в списке Вашей беспроводной сети (*Рис. 6.3*).

Шаг 5: выберите в списке Вашу беспроводную сеть, в данном примере это **BEWARD** (*Рис. 6.3*).

Шаг 6: нажмите кнопку **[Подключиться]**, после чего на экране появится окно с ожиданием настройки подключения.

Шаг 7: ожидайте завершения операции настройки приблизительно в течение двух минут.

Если Вы правильно ввели PIN-код, операция подключения пройдет успешно, и в окне ожидания подключения IP-камеры появится надпись вида: **«Connecting to AP(BEWARD)...success!»** (*Рис 6.5*). Если камере не удастся установить соединение с точкой доступа, то в данном окне появится надпись: **«Fail!»** (*Рис 6.6*). В этом случае попробуйте повторить шаги (с 1 по 7) для подключения методом **[PIN]**. Если Вам не удается настроить беспроводное соединение, то обратитесь за помощью к Вашему системному администратору.

ВНИМАНИЕ!
Подробная настройка функции WPS для конкретной модели маршрутизатора в рамках данного Руководства не рассматривается и должна быть описана в инструкции к маршрутизатору.

6.2.2 Подключение без использования веб-интерфейса IP-камеры

Технология WPS позволяет также осуществить подключение к беспроводной сети без дополнительной настройки IP-камеры или маршрутизатора через веб-интерфейс. Пользователю необходимо нажать кнопки WPS поочередно на маршрутизаторе и на IP-

камере в течение отведенного для этого временного интервала, который составляет, примерно, 2 минуты.

Для осуществления настройки беспроводного соединения без использования веб-интерфейса выполните следующие шаги:

Шаг 1: нажмите кнопку **[WPS]** на IP-камере (кнопка находится на задней стороне корпуса).

Шаг 2: в течение двух минут нажмите кнопку **[WPS]** на маршрутизаторе.

Шаг 3: ожидайте завершения настройки приблизительно в течение двух минут.

ПРИМЕЧАНИЕ!
При запуске процесса поиска и настройки подключения IP-камеры индикатор питания камеры мигает фиолетовым цветом.

Шаг 4: проверьте доступность камеры по беспроводному соединению.

6.2.3. Проверка доступности IP-камеры

После завершения процедуры подключения IP-камеры к беспроводной сети необходимо определить корректность подключения. При правильно выполненных шагах и поддержки технологии UPnP камера должна быть доступна в «Сетевом окружении» в ОС Windows или с помощью ПО «BEWARD IP Installer» (см. пункт 5.3 данного Руководства).

Если же поддержка технологии UPnP на IP-камере отключена, то необходимо узнать IP-адрес камеры, который ей назначил маршрутизатор по беспроводному сетевому подключению. Для этого подключите камеру при помощи проводного соединения LAN и посмотрите IP-адрес камеры для беспроводного соединения в меню: ***Сеть – Основные – Wi-Fi*** (*Рис 6.7*). Далее необходимо зайти на камеру по указанному IP-адресу. Процедура получения доступа к веб-интерфейсу камеры подробно расписана в пункте 5.3 данного Руководства.

Если все настройки сделаны верно, то Вы сможете получить доступ к веб-интерфейсу IP-камеры по IP-адресу беспроводного соединения.

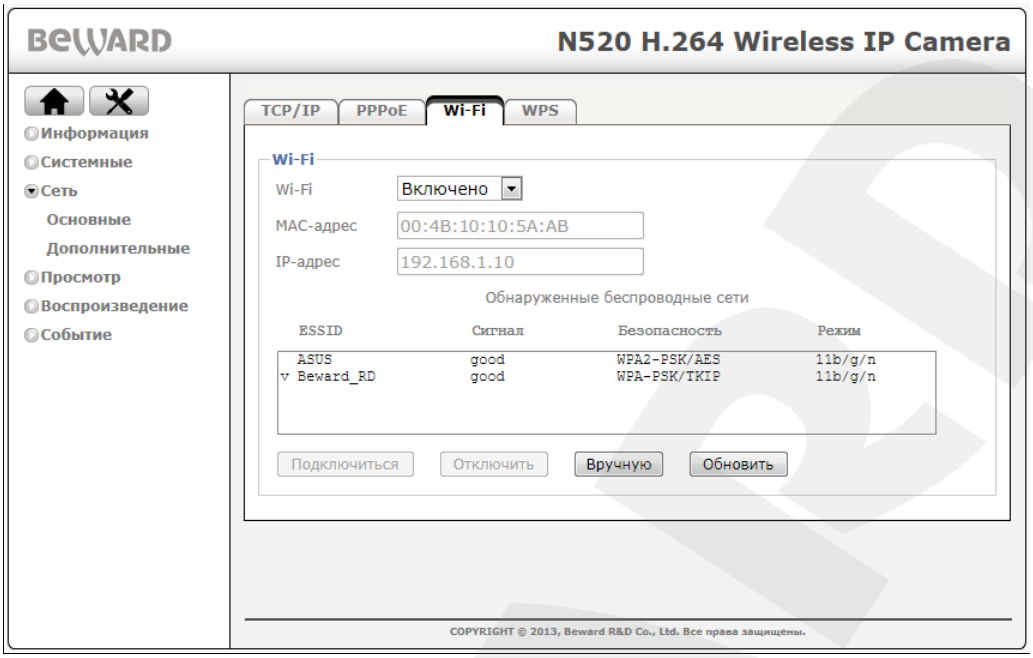

Рис 6.7

На этом настройка беспроводного Wi-Fi соединения через WPS для IP-камеры завершена.

6.3. Подключение к беспроводной Wi-Fi сети без использования WPS

На сегодняшний день большинство маршрутизаторов с поддержкой Wi-Fi также поддерживают и технологию WPS, но, несмотря на это, многие маршрутизаторы не имеют данной функции. В этом случае необходимо сначала определить настройки беспроводной сети. Определить настройки беспроводного Wi-Fi подключения можно двумя способами:

- Зайти через веб-интерфейс в меню настроек Вашего маршрутизатора и определить настройки сетевого подключения маршрутизатора (см. инструкцию по эксплуатации Вашего маршрутизатора).
- Определить настройки Wi-Fi подключения при помощи другого оборудования, подключенного к маршрутизатору (например, ноутбука).

Ниже приведен пример определения настроек требуемой беспроводной сети, а также рассмотрен метод настройки беспроводного подключения Вашей IP-камеры.

6.3.1. Определение текущих настроек Wi-Fi сети для ОС Windows 7

ПРИМЕЧАНИЕ!

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

ПРИМЕЧАНИЕ!

Если настройки беспроводной сети Вам известны, тогда Вы можете пропустить данный пункт инструкции и перейди к пункту 6.3.2 данного Руководства.

Рассмотрим процесс определения настроек беспроводной Wi-Fi сети с помощью подключенного к ней ноутбука.

Для определения текущих настроек беспроводной Wi-Fi сети ноутбука отключите от него кабель Ethernet и подключитесь к Вашей беспроводной Wi-Fi сети.

После подключения к Wi-Fi сети нажмите ***Пуск – Панель управления*** (*Рис. 6.8*).

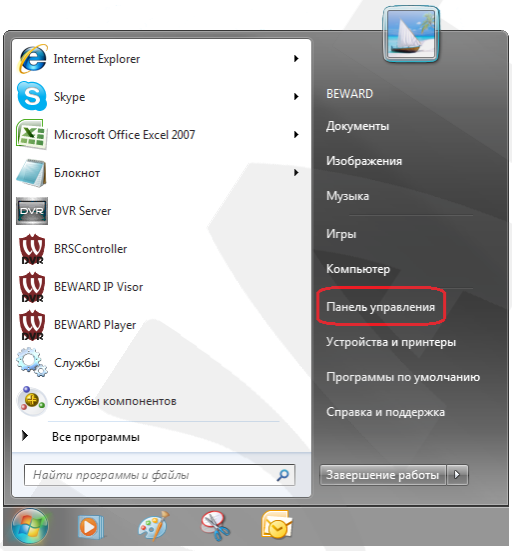

Рис. 6.8

В открывшемся диалоговом окне выберите пункт **[Просмотр состояния сети и задач]** в разделе **[Сеть и Интернет]** (*Рис. 6.9*).

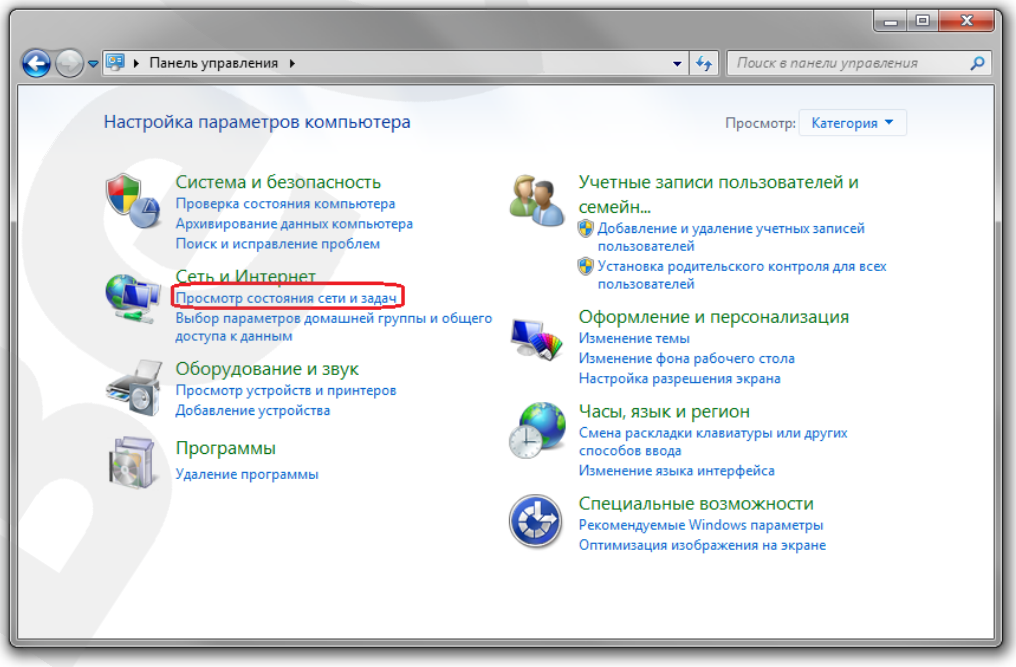

Рис. 6.9

В открывшемся окне нажмите **[Беспроводное сетевое соединение]** (*Рис. 6.10*).

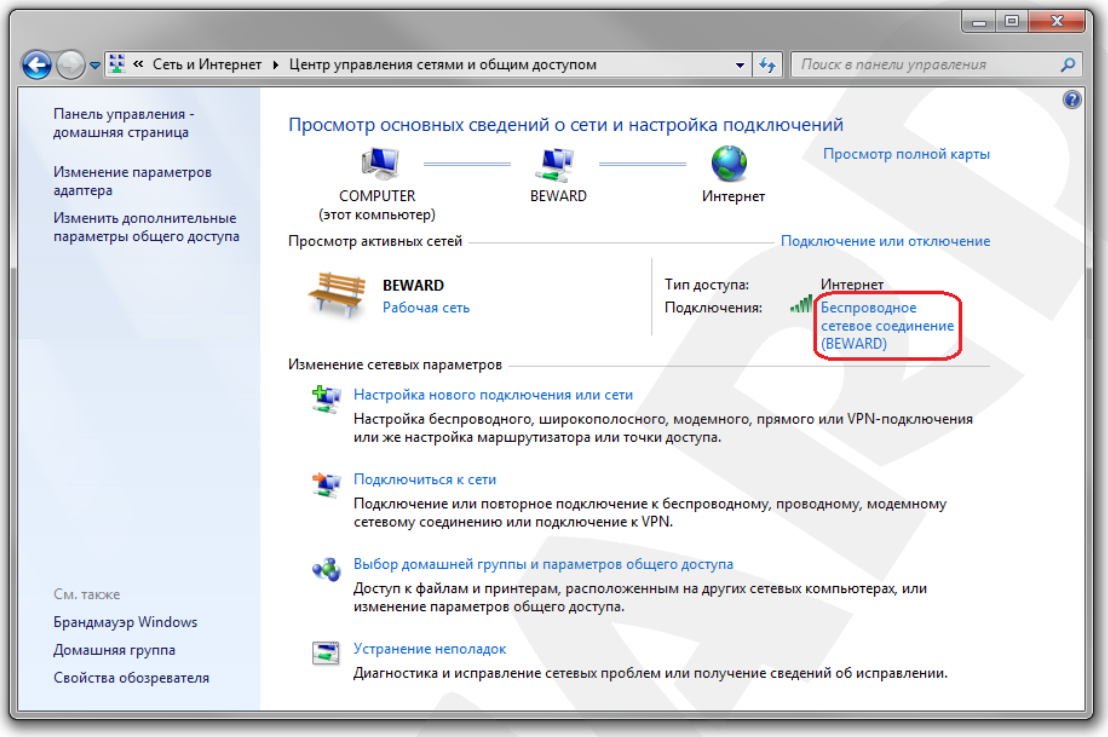

Рис. 6.10

ПРИМЕЧАНИЕ!

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

ВНИМАНИЕ!

Если у Вас нет такого пункта меню, убедитесь, что Ваш ноутбук подключен к сети Wi-Fi: отключите сетевой кабель от ноутбука, включите адаптер Wi-Fi, после чего данный пункт меню должен появиться.

В открывшемся окне указано имя Вашей беспроводной сети **[SSID]**. Запомните либо запишите название сети, оно понадобится при подключении камеры к Wi-Fi сети. Нажмите кнопку **[Сведения]** (*Рис. 6.11*).

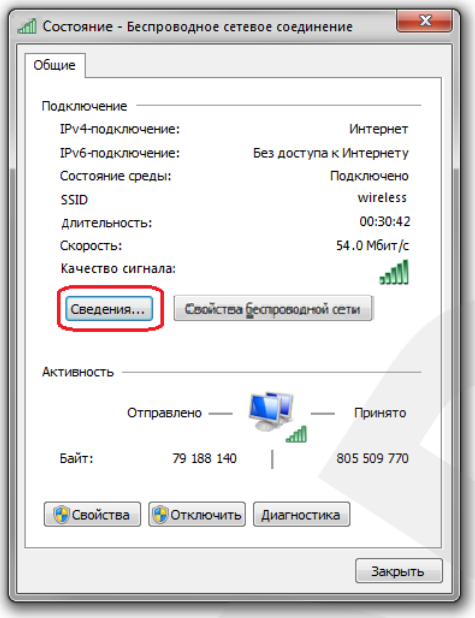

Рис. 6.11

В открывшемся окне можно увидеть информацию о текущем беспроводном сетевом подключении (*Рис. 6.12*).

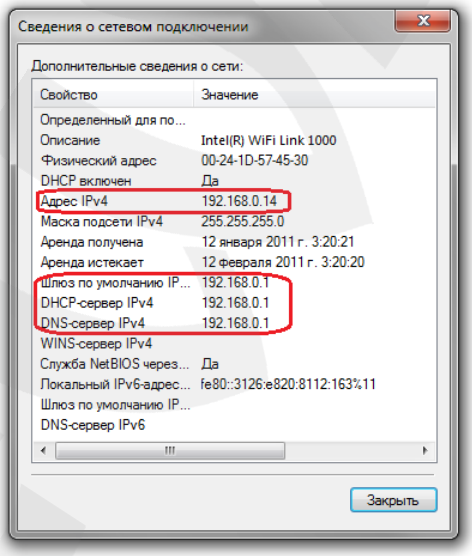

Рис. 6.12

Запишите отмеченные на *Рисунке 6.12* данные: **[Адрес IPv4]**, **[Маска подсети IPv4]**, **[DNS-сервер IPv4]**, **[Шлюз по умолчанию]**.

Теперь необходимо подключить IP-камеру N520 к Вашей беспроводной сети. При этом камера N520 должна быть включена в Вашу проводную локальную сеть для первоначальной настройки.

6.3.2. Изменение настроек Wi-Fi соединения IP-камеры через веб-интерфейс

Получите доступ к веб-интерфейсу IP-камеры любым из способов, описанных в пункте 5.3 для проводного соединения в ОС Windows 7.

В открывшемся окне введите имя пользователя и пароль (*Рис. 6.13*).

ВНИМАНИЕ!

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

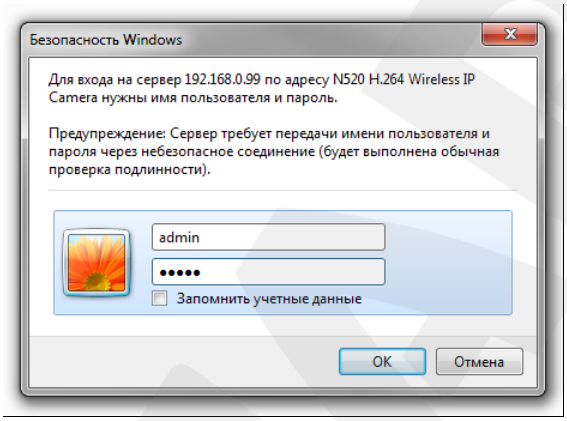

Рис. 6.13

После успешной авторизации Вы сможете увидеть через веб-браузер изображение с Вашей IP-камеры.

В веб-интерфейсе камеры нажмите кнопку **[Настройки]** , перейдите в меню ***Сеть – Основные*** и выберите вкладку **[Wi-Fi]**, предназначенную для настройки основных параметров беспроводного соединения (*Рис. 6.14*).

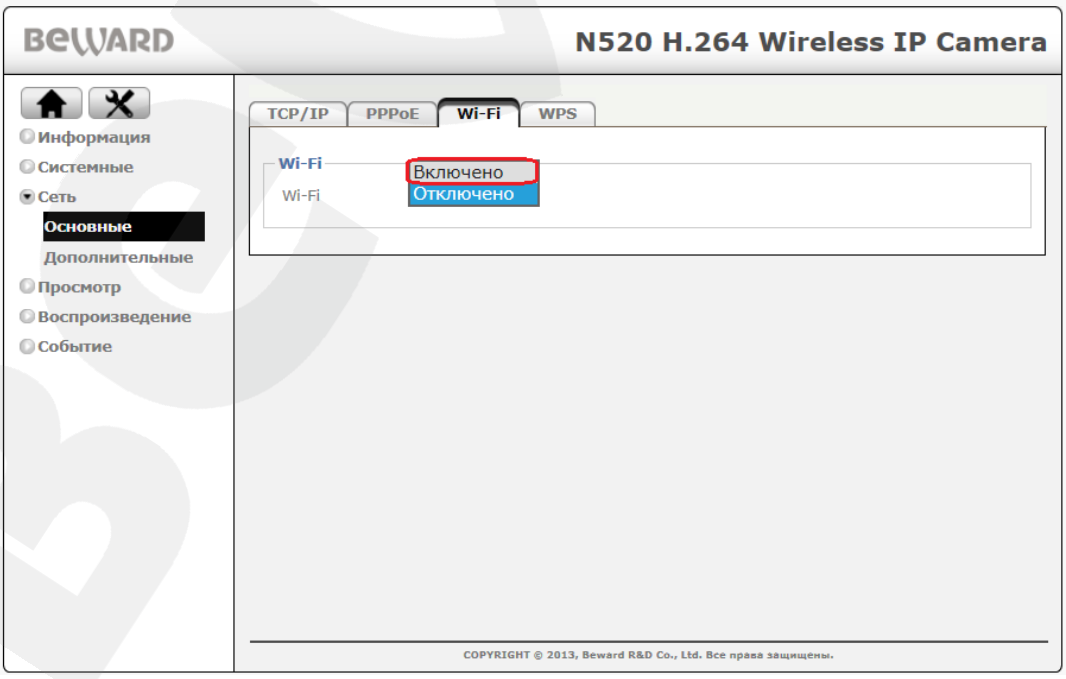

Рис. 6.14

На данной странице в строке **[Wi-Fi]** выберите положение **[Включить]**. Через некоторое время (несколько минут) камера выведет список доступных беспроводных сетей.

Выберите среди найденных беспроводных сетей Вашу, щелкнув по ней левой кнопкой мыши (*Рис. 6.15*).

ПРИМЕЧАНИЕ!

Чтобы найти Вашу сеть в таблице **[Обнаруженные беспроводные сети]**, найдите строку, для которой значение столбца **[ESSID]** совпадает с записанным Вами значением **[ESSID]** (см. пункт 6.3.1 данного Руководства).

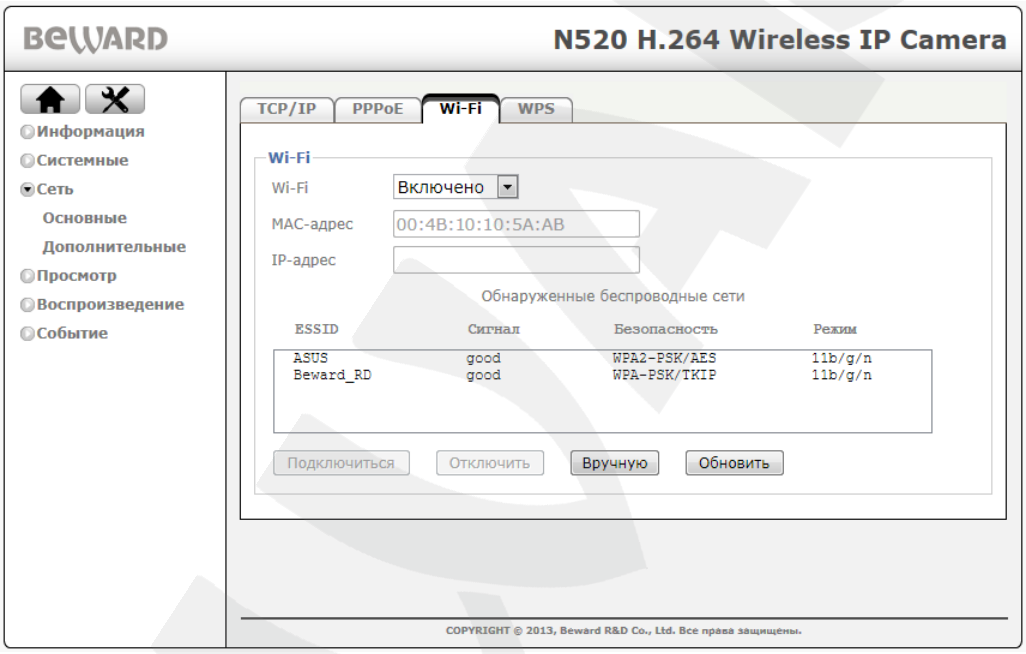

Рис. 6.15

После этого выберите способ настройки соединения с сетью. Существует два варианта настройки сети:

- **автоматический** – кнопка **[Подключиться]**
- **ручная настройка** – кнопка **[Вручную]**

Если в Вашей беспроводной сети есть DHCP-сервер, который назначает динамические IP-адреса устройствам в сети, то Вы можете выбрать вариант автоматической настройки Wi-Fi подключения. Для этого нажмите кнопку **[Подключиться]**. В открывшемся диалоговом окне, если сеть защищена от несанкционированного подключения, потребуется ввести пароль для подключения к данной сети. Введите пароль в поле **[Пароль]**, затем повторно введите тот же пароль в поле **[Повторно]** (*Рис. 6.16*). Значения настроек в полях **[Аутентификация]** и **[Шифрование]** определяются автоматически.

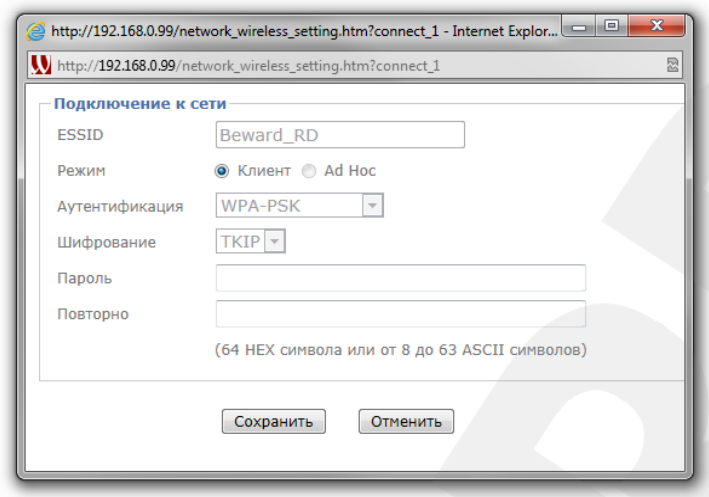

Рис. 6.16

Для сохранения изменений сетевых настроек беспроводного соединения нажмите кнопку **[Сохранить]**. Если пароль указан правильно, то подключение пройдет успешно, после чего появится окно, приведенное на *Рисунке 6.17*.

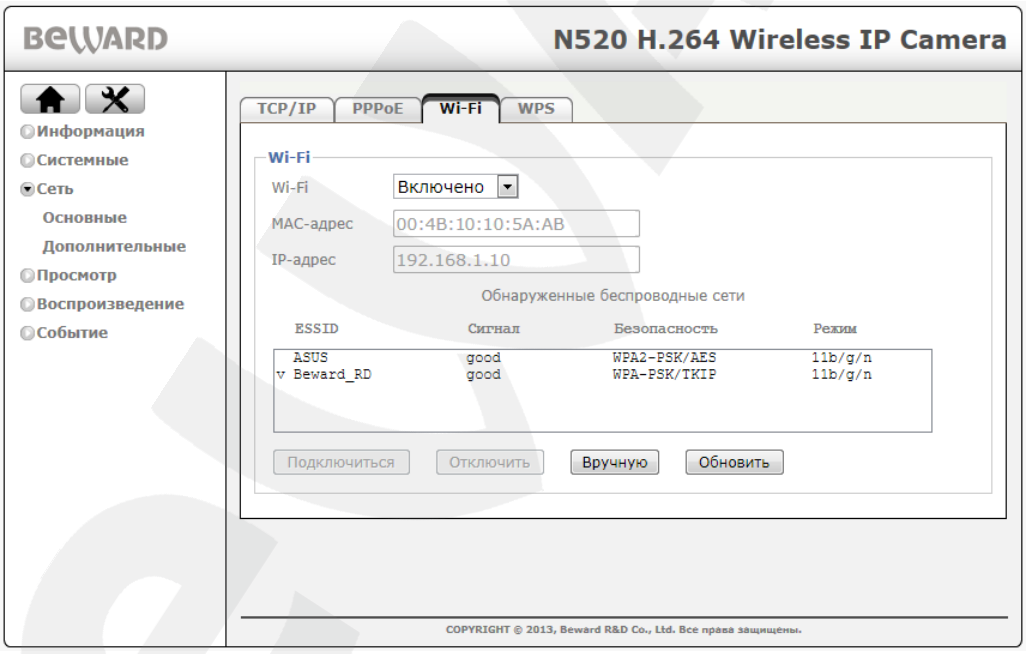

Рис. 6.17

В данном окне, в строке **[IP-адрес]** указан IP-адрес, присвоенный камере DHCP-сервером для беспроводного соединения. Используя данный IP-адрес, Вы сможете зайти на камеру через беспроводное соединение.

Если в Вашей беспроводной сети нет DHCP-сервера либо по каким-то причинам не удается установить соединение автоматическим способом, описанным выше, то Вы можете использовать ручную настройку беспроводного подключения. Для настройки подключения вручную нажмите кнопку **[Вручную]**. Появится окно, приведенное на *Рисунке 6.18*.

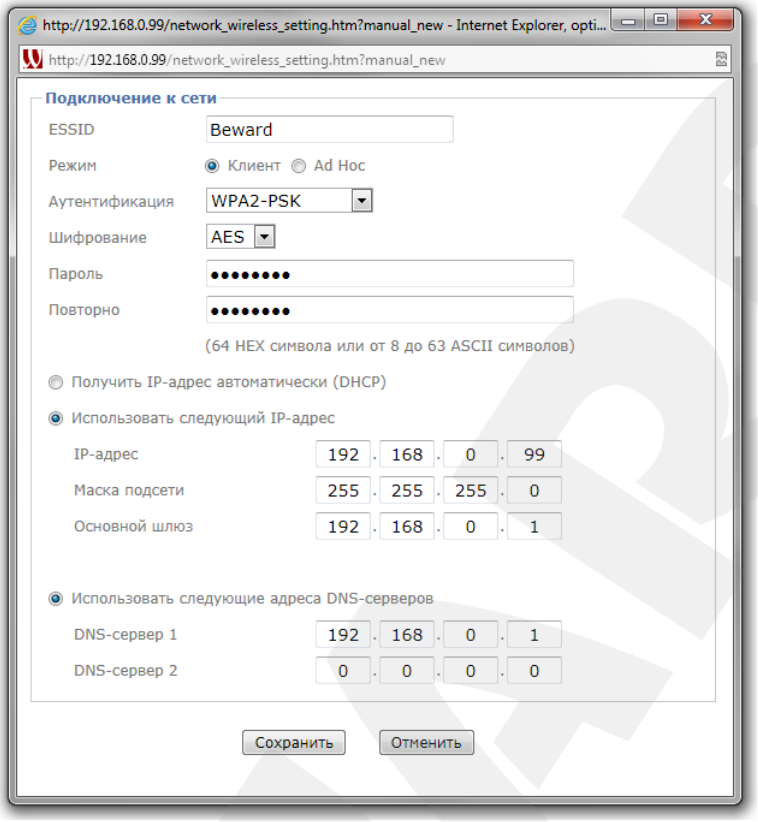

Рис. 6.18

На *Рисунке 6.18* показаны поля, которые будет необходимо заполнить вручную. Введите в данные поля значения, соответствующие параметрам Вашей беспроводной сети, которые были определены с помощью ноутбука (см. пункт 6.3.1 данного Руководства).

ESSID: введите имя Вашей беспроводной сети.

[Аутентификация]: выберите тип аутентификации в Вашей сети.

Для большей безопасности рекомендуется выбирать тип аутентификации WPA2 при условии поддержки со стороны маршрутизатора.

[Шифрование]: выберите тип шифрования, который используется в Вашей сети. Определяется автоматически, но доступен для изменения и при необходимости может быть изменен пользователем на другое значение.

Пароль: Если сеть защищена от несанкционированного подключения, то потребуется ввести ключ шифрования (пароль) данной сети. Введите ключ шифрования в поле **[Пароль]**, затем повторно введите тот же ключ шифрования в поле **[Повторно]** (*Рис. 6.18*).

IP-адрес: введите значение из той же подсети, что и значение IP-адреса, записанное Вами в пункте 6.3.1 данного Руководства, но отличающейся от него и других адресов в сети.

Маска подсети: введите значение маски подсети.

Основной шлюз: введите значение основного шлюза.

Предпочитаемый DNS-сервер: введите значение DNS-сервера.

Для сохранения изменений сетевых настроек беспроводного соединения нажмите кнопку **[Сохранить]**.

В появившемся окне необходимо нажать кнопку **[ОК]** (*Рис. 6.19*).

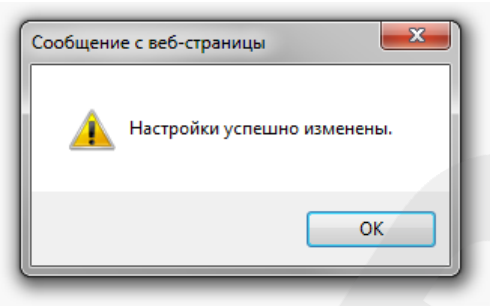

Рис. 6.19

Подождите некоторое время (около 30 секунд) для применения новых настроек камеры и завершения процесса подключения по беспроводному соединению. После завершения настройки беспроводного соединения в строке **[IP-адрес]**, на *Рисунке 6.17*, должен появиться тот IP-адрес, который Вы назначили камере для беспроводного соединения.

6.3.3. Проверка правильности настроек Wi-Fi соединения IP-камеры

Для контроля правильности сетевых настроек беспроводного Wi-Fi подключения камеры и компьютера нужно подключиться к камере через браузер Internet Explorer. Для этого нажмите ***Пуск – Все Программы*** и нажмите строку **[Internet Explorer]**. Введите в адресной строке IP-адрес, присвоенный камере для беспроводного Wi-Fi соединения (*Рис. 6.20*).

ВНИМАНИЕ!

Для проверки беспроводного Wi-Fi соединения введите в браузере IP-адрес, присвоенный камере в пункте 6.3.2 данного Руководства.

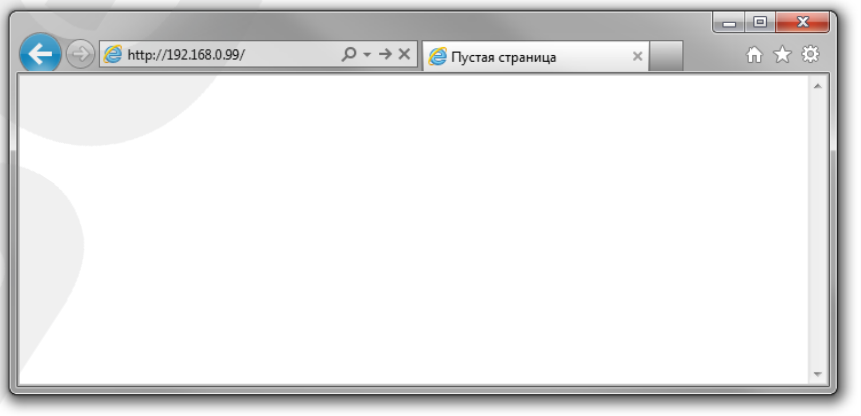

Рис. 6.20

Введите имя пользователя и пароль, после чего нажмите **[OK]** (*Рис. 6.21*).

ВНИМАНИЕ!

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

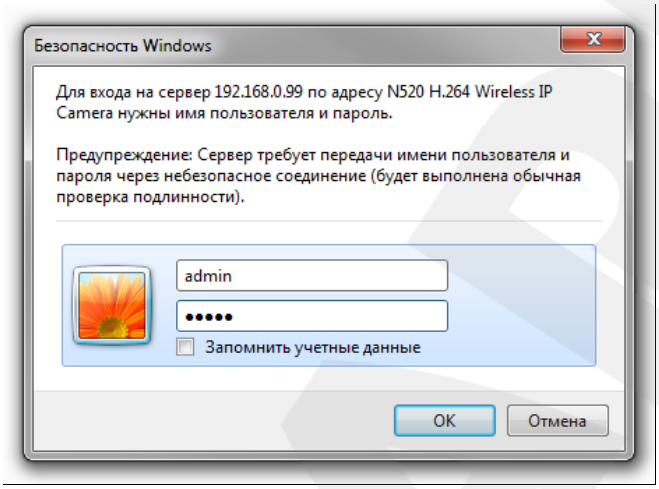

Рис. 6.21

При правильно выполненных действиях Вы сможете увидеть через веб-браузер изображение с Вашей IP-камеры (*Рис. 6.22*).



Рис. 6.22

На этом настройка сетевого подключения камеры к беспроводной сети Wi-Fi завершена.

Глава 7. Подключение IP-камеры к сети Интернет

7.1. Общие сведения о подключении IP-камеры к сети Интернет

При установке IP-камеры N520 в квартире, коттедже или офисе, удобно иметь к ней доступ не только из локальной сети того или иного помещения, но и из сети Интернет.

В этом случае для одновременной работы компьютеров, ноутбуков, IP-камер и другого оборудования в сети Интернет, чаще всего, используется маршрутизатор. При этом для подключения по Wi-Fi требуется, чтобы маршрутизатор имел поддержку беспроводного интерфейса.

При организации доступа к IP-видеокамерам из сети Интернет, как правило, используются следующие три варианта:

- Имеется выделенный провайдером внешний статический IP-адрес или PPPoE-соединение. При этом данный IP-адрес (или PPPoE-соединение) используется для подключения только одной IP-камеры и не может быть назначен еще какому-либо устройству.
- Имеется выделенный провайдером внешний статический IP-адрес, который используется для подключения к сети Интернет офисной или домашней локальной сети, к которой, в свою очередь, планируется подключить одну или несколько IP-камер. При таком подключении используется маршрутизатор. При этом число подключаемых камер зависит, в основном, от количества переназначаемых маршрутизатором портов.
- Провайдер не выделяет внешний статический IP-адрес. IP-адрес назначается провайдером динамически, то есть так, что при каждом новом подключении этот адрес присваивается заново и изменяется в процессе работы (такая ситуация особенно характерна при работе через ADSL и GPRS). В этом случае, чтобы обеспечить возможность подключения одной или нескольких камер к сети Интернет, вне зависимости от того, какой IP-адрес выделен провайдером в данный момент, необходимо задействовать интернет-службы, работающие с динамическими адресами.

Далее, эти варианты организации доступа к IP-камерам из сети Интернет будут рассмотрены подробнее.

7.2. Подключение при статическом внешнем IP-адресе или PPPoE-соединении

7.2.1. Использование статического IP-адреса

Для подключения IP-камеры к сети Интернет необходимо изменить ее сетевые параметры в соответствии с данными, полученными от провайдера. Как правило, провайдер предоставляет следующие сетевые настройки: IP-адрес (в данном случае, статический), Маска подсети, Сетевой шлюз и адрес DNS-сервера.

Для получения доступа к IP-камере через сеть Интернет по статическому IP-адресу необходимо выполнить следующие шаги:

Шаг 1: подключите IP-камеру напрямую к Вашему ПК.

Шаг 2: измените сетевые настройки проводного соединения IP-камеры (см. пункт 5.5 данного Руководства) в соответствии с настройками, предоставленными Вашим Интернет-провайдером (*Рис. 7.1*).

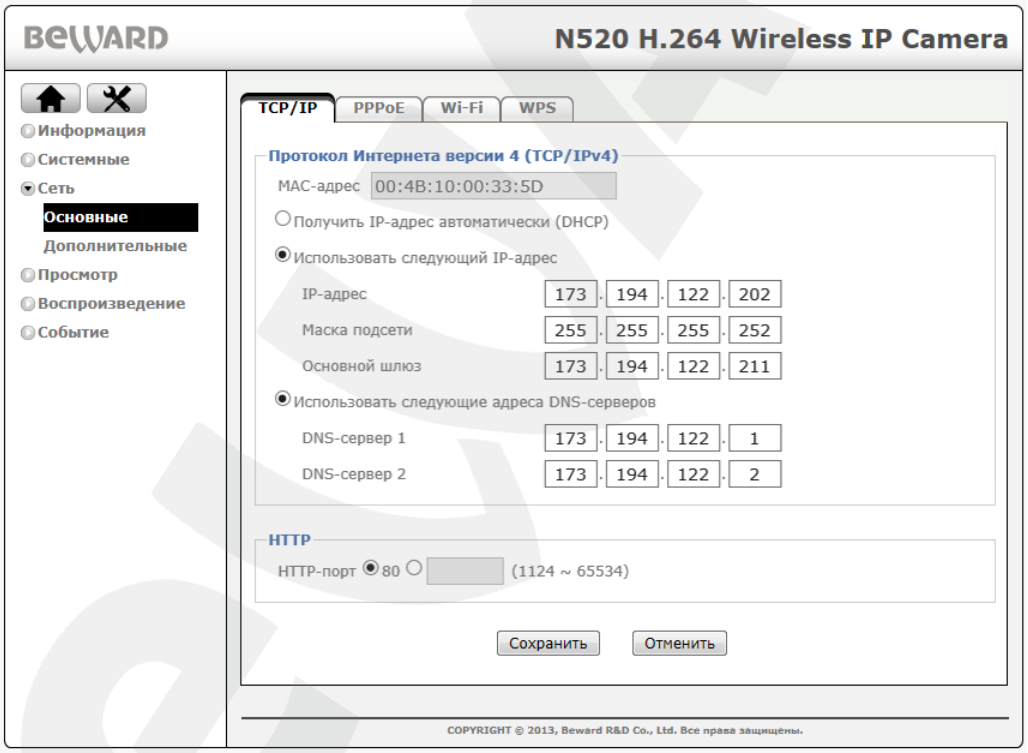

Рис. 7.1

Шаг 3: подключите IP-камеру к выделенной сети Ethernet.

Если все параметры указаны верно, камера должна быть доступна в сети Интернет.

В приведенном примере провайдер предоставил следующие данные:

- **IP-адрес:** 173.194.122.202
- **Маска подсети:** 255.255.255.252
- **Основной шлюз:** 173.194.122.211
- **DNS-сервер 1:** 173.194.122.1
- **DNS-сервер 2:** 173.194.122.2

В общем случае, для обращения к IP-камере через сеть Интернет в адресной строке браузера вводится следующий запрос: **http://<IP>:<Port>**, где **<IP>** – IP-адрес камеры, **<Port>** – значение HTTP-порта. Так как в данном примере используется значение HTTP-порта, заданное по умолчанию («80»), то, чтобы обратиться к IP-камере через сеть Интернет, необходимо набрать запрос «http://173.194.122.202».

ПРИМЕЧАНИЕ!
При подключении к камере через HTTP-порт, заданный по умолчанию (значение равно 80), запрос в адресной строке браузера имеет вид: **http://<IP>**, где **<IP>** – IP-адрес камеры.

7.2.2. Использование PPPoE-соединения

Интернет-провайдер не всегда может обеспечить подключение по статическому IP-адресу. Чаще всего, провайдер организует доступ к сети Интернет через PPPoE-соединение. В этом случае, он предоставляет абоненту **имя пользователя** и **пароль**.

IP-камера N520 поддерживает PPPoE, и для его использования необходимо выполнить следующие шаги:

Шаг 1: подключите IP-камеру к Вашей локальной сети или напрямую к ПК (см. Главу 5).

Шаг 2: войдите в меню PPPoE-настроек IP-камеры: ***Настройки*** – ***Сеть – Основные – PPPoE***.

Шаг 3: в текстовых полях **[Пользователь]**, **[Пароль]** введите значения, полученные от Интернет-провайдера (*Рис. 7.2*). Тип аутентификации выберите в зависимости от типа, используемого Вашим провайдером.



Рис. 7.2

Шаг 4: для принятия изменений нажмите кнопку **[Сохранить]**.

ВНИМАНИЕ!
Для применения сетевых параметров требуется перезагрузка устройства.

Шаг 5: подключите IP-камеру к выделенной сети Ethernet.

ВНИМАНИЕ!
После подключения IP-камеры к выделенной сети Ethernet она будет доступна в сети Интернет под IP-адресом, присвоенным ей Вашим провайдером и отображаемым в поле **[IP-адрес]** (см. *Рис. 7.2*).

ПРИМЕЧАНИЕ!
Для удобства, IP-адрес камеры, под которым она доступна в сети Интернет, может быть сообщен на указанный Вами адрес электронной почты (функция «IP-уведомление»). Для настройки данной опции, пожалуйста, обратитесь к Руководству по эксплуатации.

Для обращения к IP-камере через сеть Интернет, в адресной строке браузера вводится следующий запрос: **http://<IP>:<Port>/**,– где **<IP>** – IP-адрес камеры, назначенный Вашим провайдером при установлении PPPoE-соединения, **<Port>** – значение HTTP-порта (по умолчанию равное «80»).

ПРИМЕЧАНИЕ!
При подключении к камере через HTTP-порт, заданный по умолчанию (значение равно 80), запрос в адресной строке браузера имеет вид: **http://<IP>**, где **<IP>** – IP-адрес камеры.

7.3. Подключение через сеть Интернет к IP-камерам, находящимся в локальной сети

Если доступ в сеть Интернет осуществляется по выделенной линии Ethernet или по ADSL, для подключения локальной сети используется маршрутизатор.

ВНИМАНИЕ!
Для использования данного метода подключения необходимо заранее приобрести у Вашего провайдера ПУБЛИЧНЫЙ СТАТИЧЕСКИЙ IP-адрес. Провайдер предоставляет, как правило, ДИНАМИЧЕСКИЙ ВНУТРЕННИЙ IP-адрес, который доступен только в подсети провайдера. Поэтому уточните тип используемого Вами IP-адреса заранее.

Для того чтобы подключиться к IP-камере из сети Интернет, надо обратиться по IP-адресу, выданному провайдером («внешний» IP-адрес маршрутизатора), и к определенному HTTP-порту.

ВНИМАНИЕ!
При обращении из сети Интернет для всех камер, находящихся в одной локальной сети, существует только один IP-адрес (выданный провайдером). Поэтому для доступа к этим камерам необходимо назначить каждой свое значение HTTP-порта.

Для этого требуется выполнить следующие действия:

- Изменить сетевые параметры IP-камер в соответствии с настройками, принятыми в Вашей локальной сети (см. пункт 5.5 для проводного подключения камер к локальной сети).
- Настроить функцию перенаправления портов. Данная функция позволяет перенаправлять обращения из сети Интернет к какому-либо устройству, подключенному к локальной сети, с внешнего WAN-интерфейса маршрутизатора на его внутренний LAN-интерфейс и обеспечивается практически любым современным маршрутизатором.

При этом существует два способа настройки маршрутизации (перенаправления портов):

- Использование технологии UPnP на маршрутизаторе и камере.
- Ручная установка параметров перенаправления портов на маршрутизаторе и камере.

7.3.1. Использование технологии UPnP

Пусть требуется обеспечить доступ из сети Интернет к одной IP-камере. Считаем, что подключение маршрутизатора к локальной сети и сети Интернет уже установлено. Маршрутизатор имеет следующий публичный статический IP-адрес, выданный провайдером для подключения к сети Интернет: 173.194.122.201:

- Разрешить использование и настроить функции UPnP Вашего маршрутизатора.

ВНИМАНИЕ!

Не все модели маршрутизаторов поддерживают функцию UPnP для переадресации портов LAN- и WAN-интерфейсов. Если Ваш маршрутизатор не поддерживает данную функцию, то он требует дополнительной настройки (см. пункт 7.3.2).

- Разрешить использование и настроить функцию UPnP IP-камеры.

Чтобы настроить функцию UPnP IP-камеры выполните следующие действия:

Шаг 1: пройдите в меню ***Настройки*** – ***Сеть – Дополнительные – UPnP***.

Шаг 2: поставьте галочку напротив строки **[Разрешить переадресацию портов]** (*Рис. 7.3*).

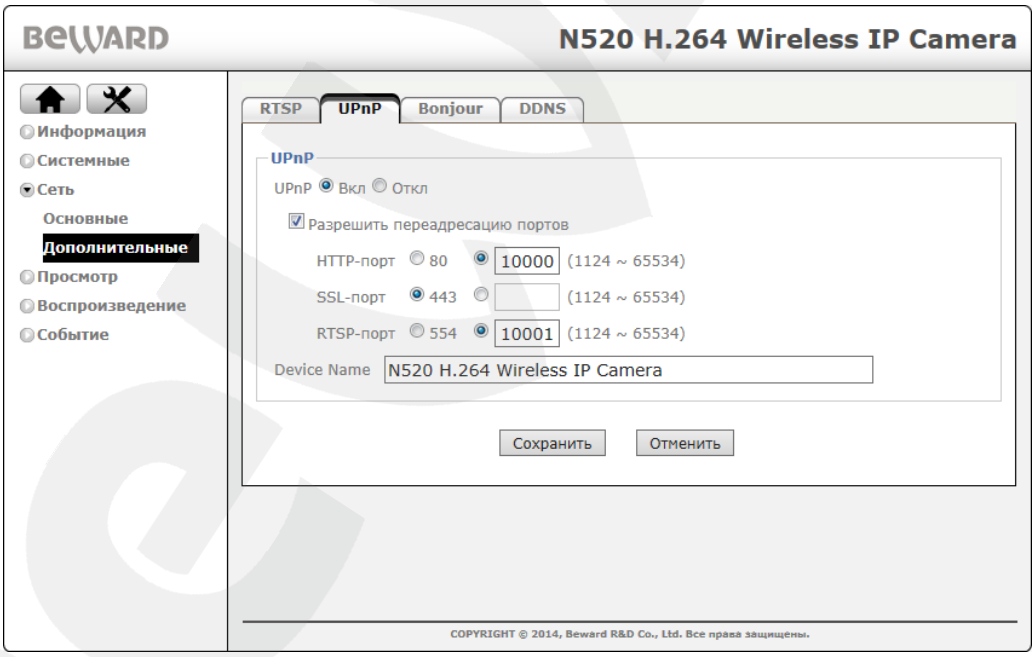

Рис. 7.3

Шаг 3: введите в поле **[HTTP-порт]** значение порта HTTP для данной камеры при доступе к ней из сети Интернет. Например, пусть в качестве HTTP-порта для доступа из сети Интернет используется порт 10000. При таких настройках, чтобы обратиться к IP-камере в локальной сети, используется порт 80, а при запросе потока через сеть Интернет будет использоваться порт 10000.

Шаг 4: введите в поле **[RTSP-порт]** значение порта RTSP для данной камеры при доступе к ней из сети Интернет.

Шаг 5: для применения настроек нажмите кнопку **[Сохранить]**.

ВНИМАНИЕ!
Для применения сетевых параметров требуется перезагрузка устройства.

ВНИМАНИЕ!
Значения при переадресации соответствующих портов на IP-камере и на маршрутизаторе должны быть одинаковыми.

Теперь, чтобы получить доступ к камере из сети Интернет, надо обратиться к ней по IP-адресу, выданному провайдером («внешний» IP-адрес маршрутизатора), и назначенному ей порту HTTP.

В рассмотренном примере IP-адрес маршрутизатора – 173.194.122.201. HTTP-порт, назначенный камере для переадресации, – 10000. Значит, для обращения к камере из сети Интернет необходимо в адресной строке браузера набрать запрос: **http://173.194.122.201:10000/**.

Таким же образом может быть настроено несколько камер, надо лишь для каждой из них задать свои, уникальные значения портов.

7.3.2. Настройка ручной переадресации портов маршрутизатора.

Если Ваш маршрутизатор не поддерживает технологию UPnP, либо данная опция работает некорректно, тогда необходимо настроить переадресацию портов вручную.

Рассмотрим задачу подключения IP-камеры к сети Интернет с помощью маршрутизатора TP-Link TL-WR2543ND (настройка большинства функций маршрутизаторов различных моделей выполняется схожим образом).

Считаем, что подключение маршрутизатора к локальной сети и сети Интернет уже настроено. Маршрутизатор имеет следующий публичный статический IP-адрес, выданный Интернет-провайдером (IP-адрес WAN-интерфейса маршрутизатора): 173.194.122.201.

Локальная сеть имеет IP-адреса в диапазоне «192.168.1.1 – 192.168.1.255», причем «192.168.1.1» – «внутренний» IP-адрес маршрутизатора (IP-адрес LAN-интерфейса маршрутизатора), «192.168.1.199» – IP-адрес камеры. Для настройки используем компьютер, подключенный к этой локальной сети.

Для подключения IP-камеры к сети Интернет требуется назначить порты, через которые будет осуществляться внешний доступ к ее настройкам и видеопотоку. В локальной

сети эти порты по умолчанию имеют следующие значения: HTTP-порт – «80», RTSP-порт – 554.

ВНИМАНИЕ!

При обращении из сети Интернет для всех камер, находящихся в одной локальной сети, существует только один IP-адрес (выданный провайдером). Поэтому для доступа к этим камерам необходимо каждой назначить свои группы портов.

Для изменения портов IP-камеры выполните следующие действия:

ВНИМАНИЕ!

HTTP-порты камер можно перенаправлять с помощью виртуального сервера, однако RTSP-порты должны быть разными у всех камер и транслироваться «порт в порт»! Соответственно, для всех камер необходимо задать различные значения RTSP-порта.

Шаг 1: откройте раздел меню ***Настройки*** – ***Сеть – Дополнительные – RTSP***.

Шаг 2: введите в поле **[RTSP-порт]** новое значение порта RTSP, отличное от значения по умолчанию. Например, пусть в качестве RTSP-порта используется порт 3001 (*Рис. 7.4*).

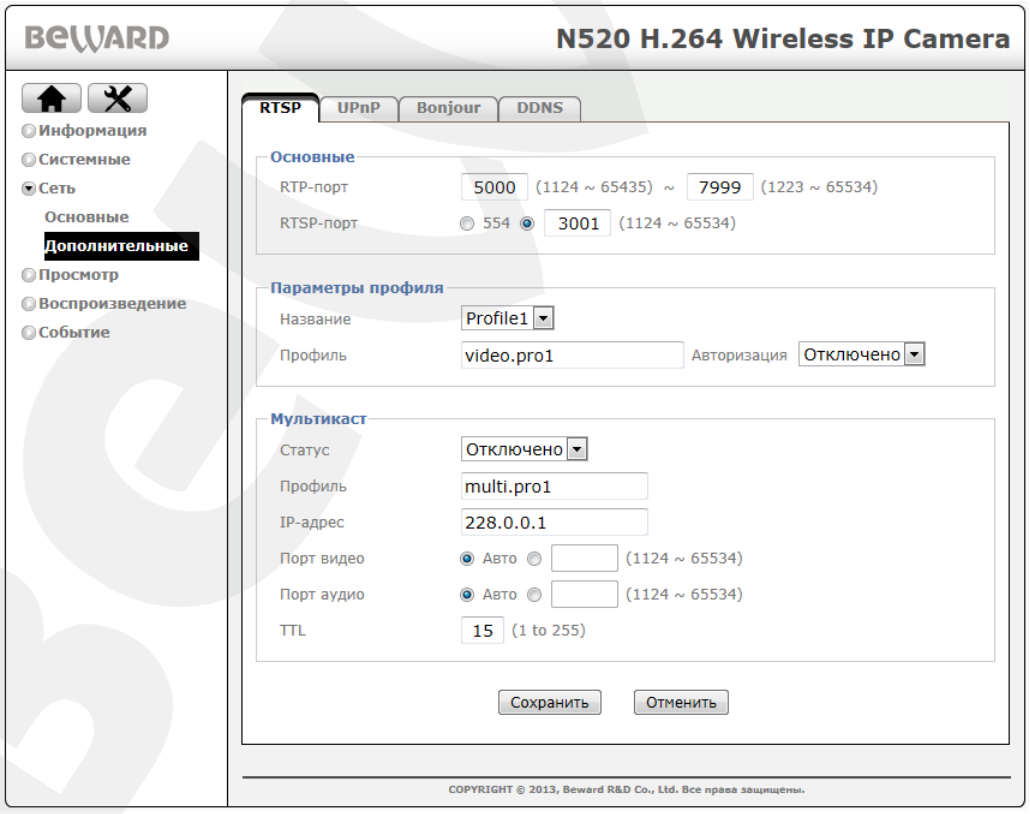

Рис. 7.4

Шаг 3: для применения настроек нажмите кнопку **[Сохранить]**.

Таким образом, порты для доступа к данной камере внутри локальной сети будут: HTTP-порт – «80», RTSP-порт – «3001».

Для второй камеры можно выбрать порт HTTP – «80» и порт RTSP – 3002.

Камера настроена. Осталось правильно настроить маршрутизатор.

Для настройки маршрутизатора выполните следующие действия:

Шаг 1: введите в адресной строке браузера IP-адрес маршрутизатора (в нашем примере – «192.168.1.1»). В появившемся окне авторизации введите логин и пароль. После удачной авторизации откроется основная страница настроек маршрутизатора (*Рис. 7.5*).

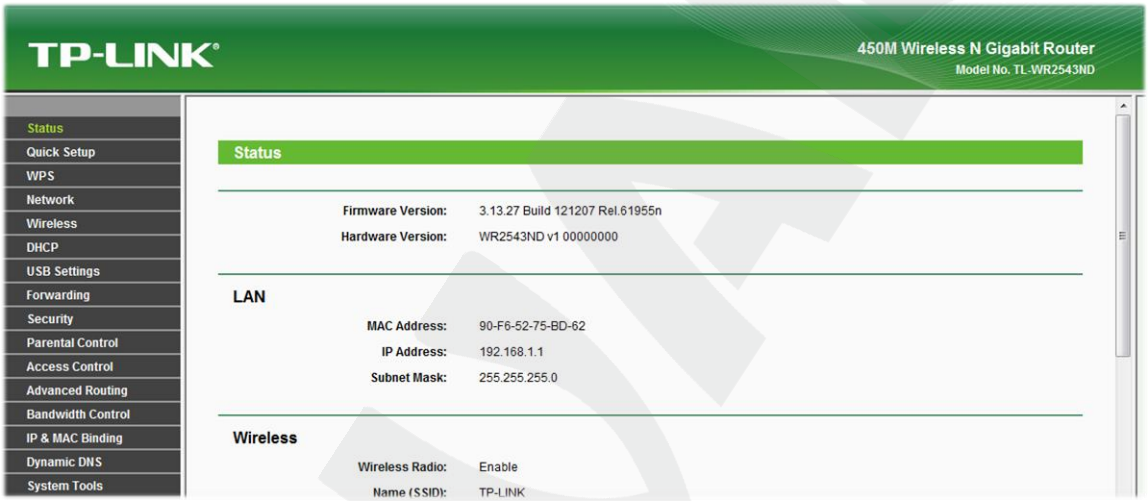

Рис. 7.5

Шаг 2: выберите пункт меню ***Forwarding – Virtual Servers***. В появившемся меню нажмите кнопку **[Add New]** (*Рис.7.6*).

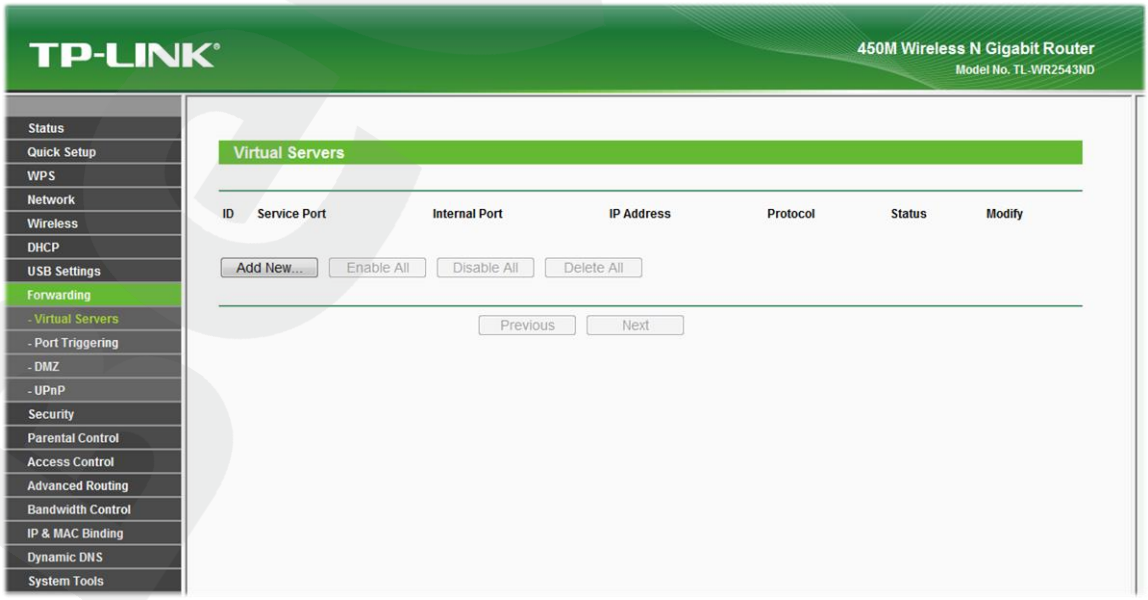

Рис. 7.6

Шаг 3: добавьте правила перенаправления портов для IP-камеры (*Рис. 7.7*). Задайте следующие параметры:

[Service Port]: укажите порт, который будет использоваться для доступа к камере из сети Интернет.

ПРИМЕЧАНИЕ!

Во избежание конфликтов не используйте для перенаправления портов зарегистрированные значения. Рекомендуется использование портов диапазона 1124-7999. (Значения портов от 0 до 1123 официально зарегистрированы под различные протоколы, службы, приложения.)

[Internal Port]: укажите порт, используемый в данный момент для доступа к камере из локальной сети.

[IP Address]: укажите IP-адрес камеры, для которой настраивается перенаправление.

Остальные пункты не требуют настройки.

Добавьте правило для порта HTTP (*Рис. 7.7*).

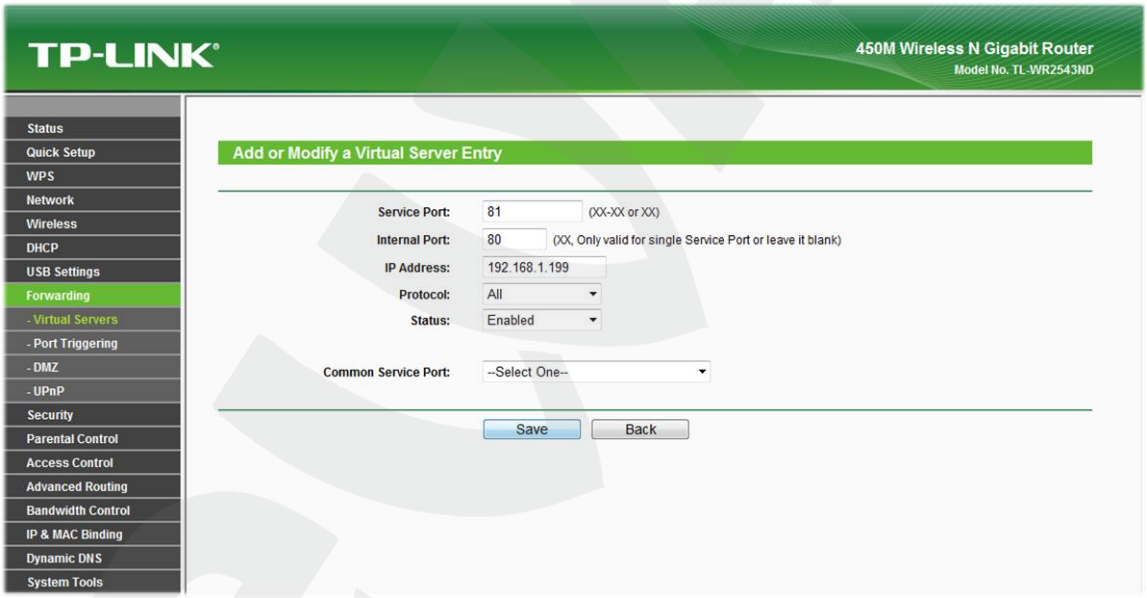

Рис. 7.7

Шаг 4: нажмите кнопку **[Save]**, чтобы сохранить правило. Правило добавлено (*Рис. 7.8*):

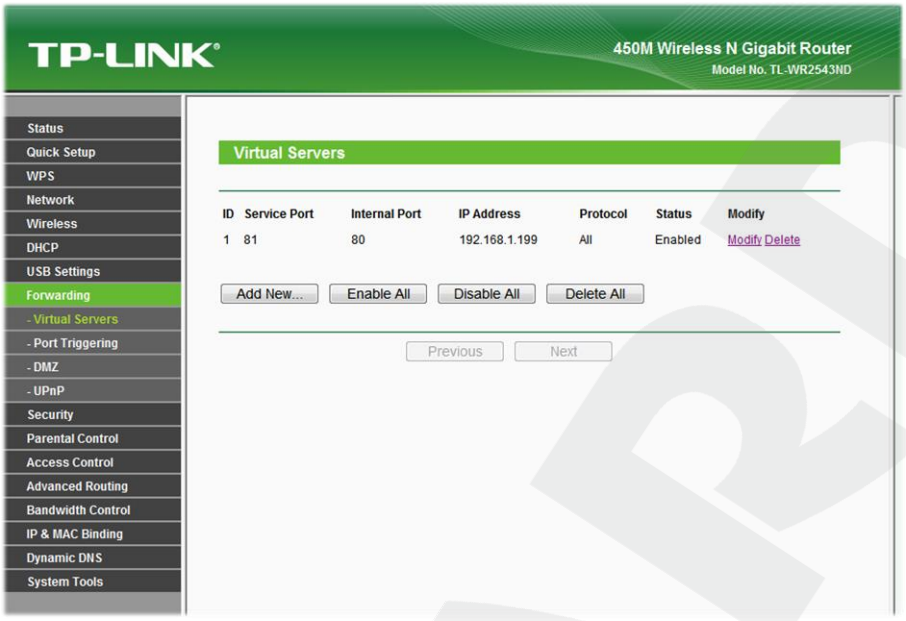

Рис. 7.8

Шаг 5: тем же способом добавьте правило для порта RTSP (*Рис. 7.9*):

ВНИМАНИЕ!

HTTP-порты камер можно перенаправлять с помощью виртуального сервера, однако RTSP-порты должны быть разными у всех камер и транслироваться «порт в порт»! Например, порт 3001 камеры №1 транслируется в порт 3001 маршрутизатора, порт 3002 камеры №2 – в порт 3002 маршрутизатора и т.д.

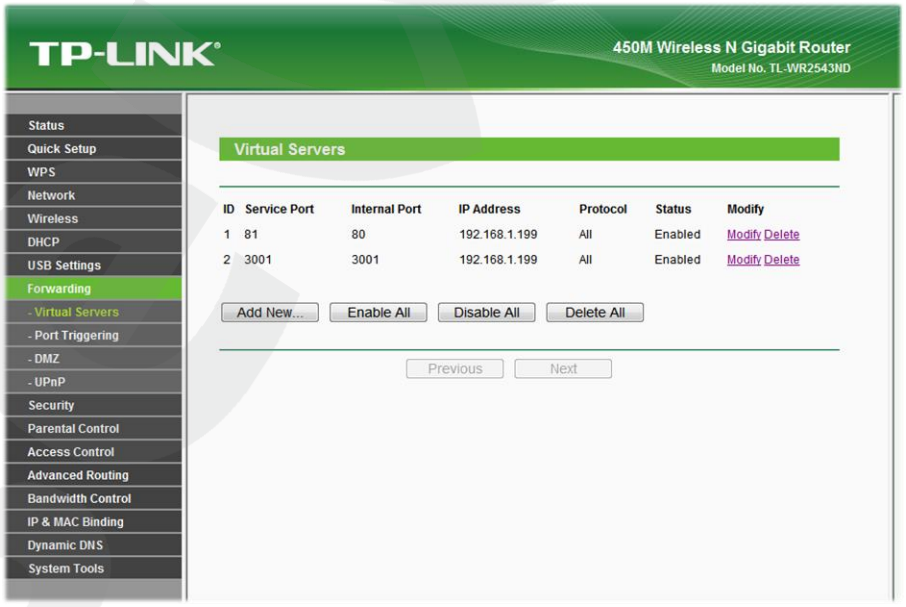

Рис. 7.9

Шаг 6: если Вы используете несколько камер, то Вам необходимо повторить **шаги 2-5** для остальных камер (*Рис.7.10*).

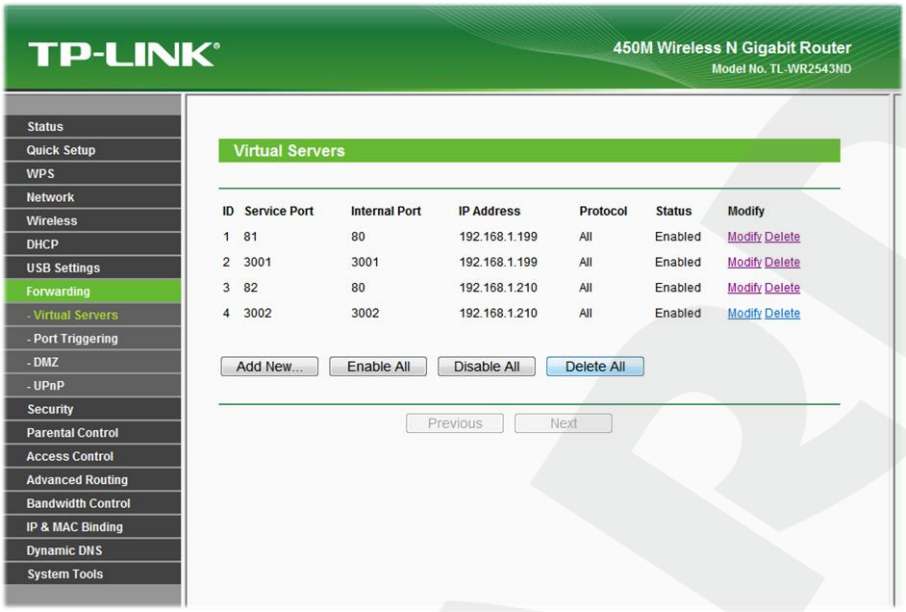

Рис.7.10

Настройка маршрутизатора завершена.

Теперь, чтобы получить доступ к камере из сети Интернет, надо обратиться к ней по IP-адресу, выданному провайдером («внешний» IP-адрес маршрутизатора), и назначенному ей порту HTTP.

В рассмотренном примере IP-адрес маршрутизатора – «173.194.122.201». HTTP-порт, назначенный камере для переадресации, – «81». Значит, для обращения к камере из сети Интернет необходимо в адресной строке браузера набрать запрос: http://173.194.122.201:81/.

7.4. Пример подключения через сеть Интернет с использованием DDNS

7.4.1. Общие сведения о подключении через Интернет с использованием DDNS

В случае если IP-адрес выдается компьютеру на определенное время (чаще всего лишь на один сеанс связи), такой адрес называют динамическим. В большинстве случаев Интернет-провайдеры предоставляют пользователям динамические IP-адреса. Однако для того, чтобы можно было обратиться к оборудованию из сети Интернет в любой момент, оно должно иметь постоянный или фиксированный адрес. С этой проблемой легко справляется служба Dynamic DNS (DDNS).

Сервис Dynamic DNS предоставляет Вам возможность сделать IP-камеры легкодоступными из сети Интернет, даже если в Вашем распоряжении постоянно меняющийся, динамический IP-адрес. Внешние пользователи всегда будут иметь доступ к оборудованию, обращаясь к нему по его доменному имени.

В этом случае вместо того, чтобы обращаться к оборудованию по IP-адресу, Вы обращаетесь к нему по доменному имени вида: www.camera1.dyndns.org.

Для этого надо зарегистрироваться на сайте провайдера сервиса DDNS (например, www.dyndns.com), сообщить один раз текущий IP-адрес оборудования и выбрать доменное имя, по которому в дальнейшем Вы будите обращаться к оборудованию.

Тогда при смене IP-адреса или при новом подключении к сети Интернет устройство получает от интернет провайдера новый IP-адрес. Он обрабатывается встроенным в камеру ПО, которое обращается на сайт провайдера DDNS для того, чтобы сообщить значение текущего IP-адреса. DDNS-провайдер ставит в соответствие этому IP-адресу зарегистрированное Вами ранее доменное имя.

Рассмотрим пример работы с DDNS-провайдером http://www.dyndns.com. Методика регистрации и работы с другими поставщиками DDNS аналогична данной. Для доступа к сетевому ресурсу с использованием доменного имени выполните следующие шаги:

- Заведите себе учетную запись (Account) на сайте www.dyndns.com для дальнейшей регистрации на сервере.
- Создайте на сайте www.dyndns.com доменное имя (Hostname) для своего сервера. Вы можете выбрать любое незанятое в этом домене имя для своего оборудования, например, camera184. Соответственно получите домен третьего уровня для своего оборудования www.camera184.dyndns.org.
- Настройте соответствующим образом оборудование.

7.4.2. Регистрация на сервере DynDNS

Шаг 1: зайдите на сайт www.dyndns.com, для создания учетной записи нажмите справа вверху **[Sign In]** и в выпавшем списке выберите строку **[Create an Account]** (*Рис. 7.11*).

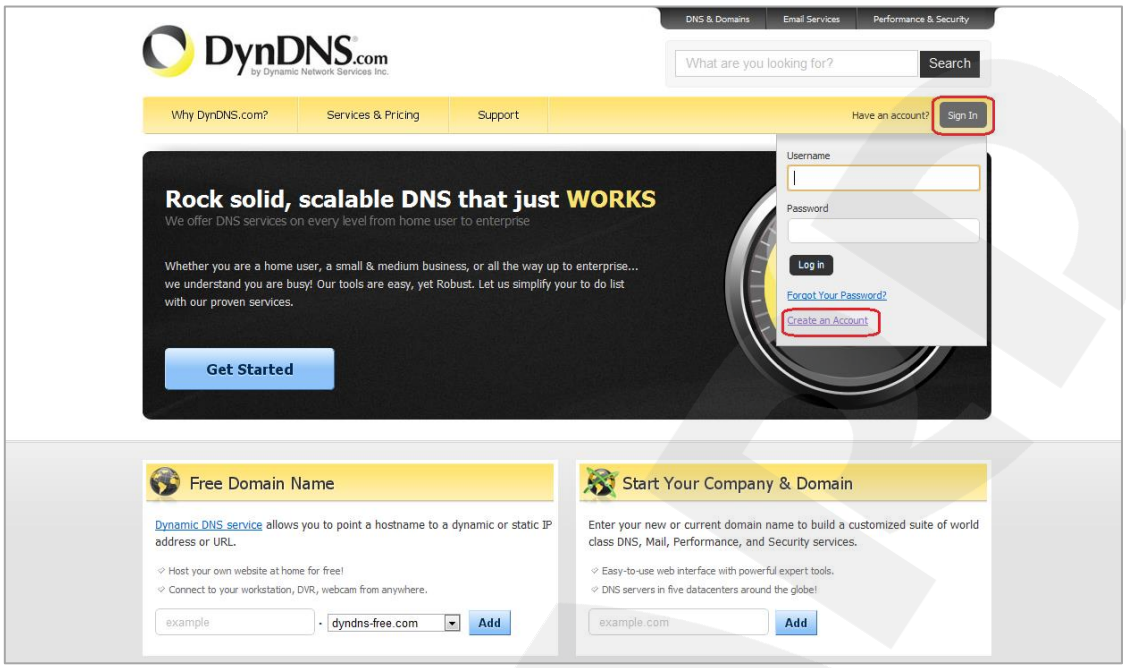

Рис. 7.11

Далее Вы автоматически перейдете на страницу создания учетной записи (*Рис. 7.12*).

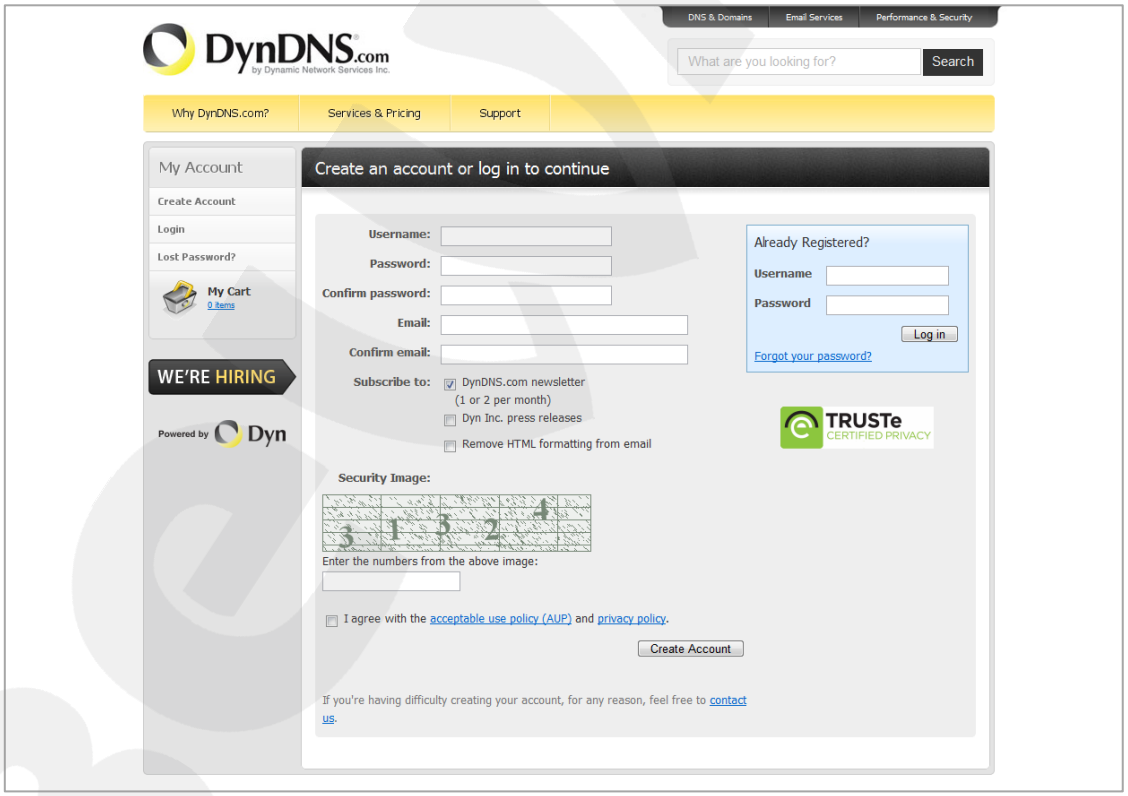

Рис. 7.12

Шаг 2: введите любое желаемое и незанятое имя пользователя (поле: **[Username]**), пароль (поля: **[Password]** и **[Confirm password]**).

ПРИМЕЧАНИЕ!
Для защиты от возможных ошибок при введении пароля, он указывается дважды. Обязательно следите за тем, чтобы значение пароля в обоих полях было одинаковым.

Укажите Ваш адрес электронной почты в обоих полях: **[Email]** и **[Confirm email]**. На адрес, указанный Вами в данных полях, будет выслано письмо с данного сайта, причем на один электронный адрес может быть зарегистрировано только одно доменное имя.

ПРИМЕЧАНИЕ!
Регистрация более одного доменного имени на один электронный адрес является платной.

ПРИМЕЧАНИЕ!
Для защиты от возможных ошибок при введении адреса электронной почты он указывается два раза. Обязательно следите за тем, чтобы значение адреса электронной почты для обоих полей было одинаковым.

Пункт **[DynDNS.com newsletter]** предназначен для почтового оповещения пользователя системой DynDNS в случае обновления сервиса или каких-либо нововведений. Для отказа от новостной рассылки уберите выделение этого пункта.

Введите код, который видите на картинке, и поставьте флажок для пункта **[I agree with the acceptable use policy (AUP) and privacy policy]**. Это означает согласие с условиями лицензионного соглашения для создания одного бесплатного аккаунта.

В качестве примера используется: имя пользователя **[Username]** – camera184, адрес электронной почты **[E-mail]** – camera184@yandex.ru, произвольный пароль (например, 123456).

Для завершения регистрации и окончания создания аккаунта нажмите на кнопку **[Create Account]** (*Рис. 7.13*).

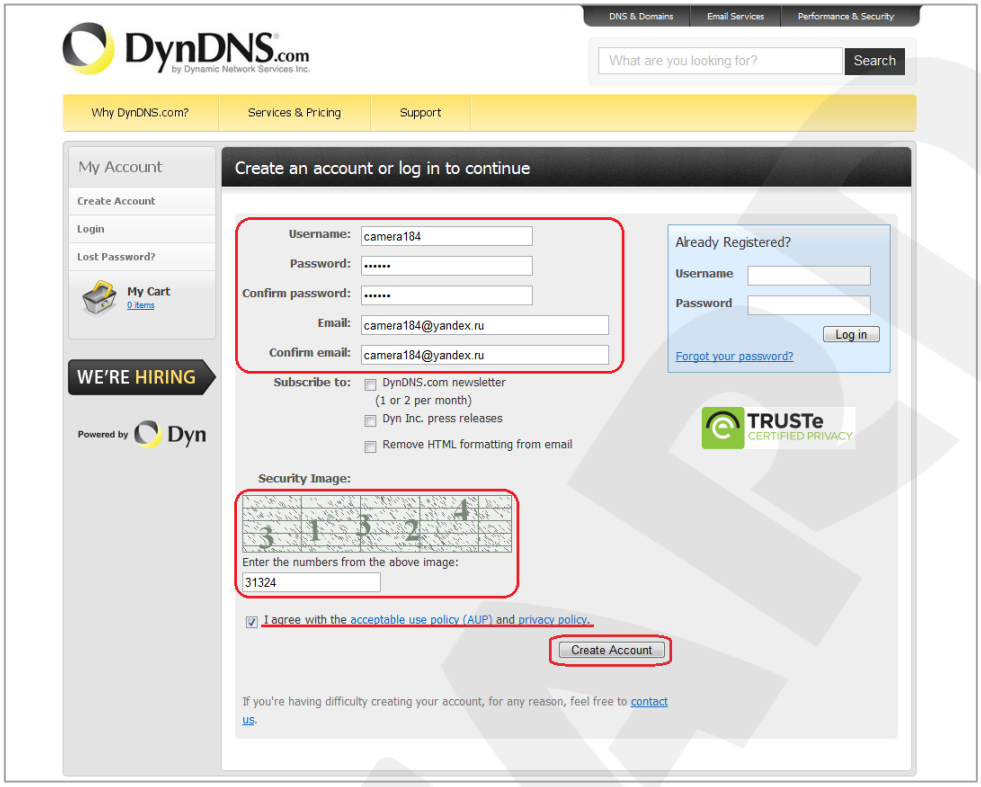

Рис. 7.13

Шаг 3: при правильном заполнении формы Вы получите сообщение о том, что остался один шаг до создания учетной записи: **[One more step to go...]** (*Рис. 7.14*).

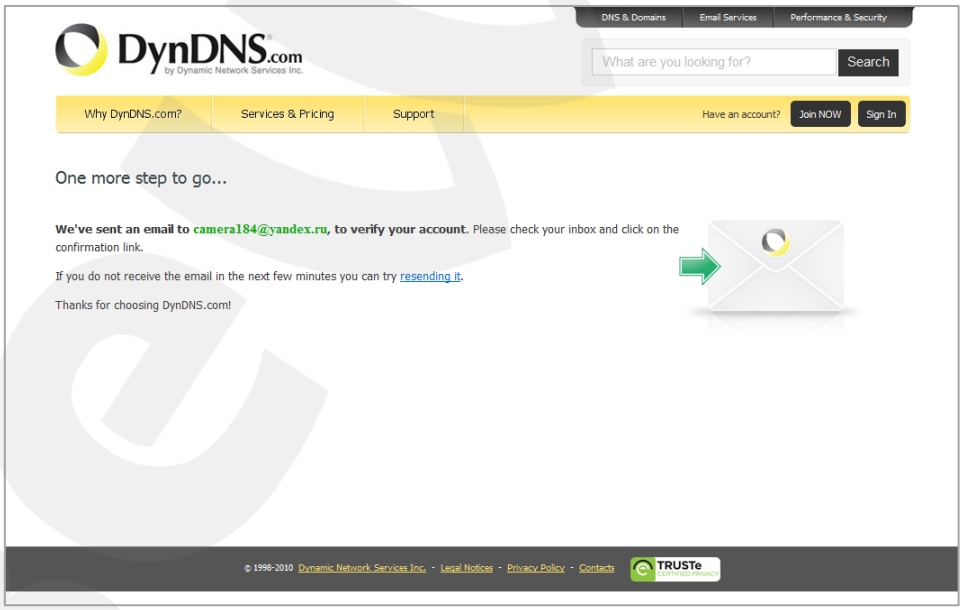

Рис. 7.14

Шаг 4: через несколько минут на электронный почтовый ящик, указанный при регистрации, придет письмо от службы «DynDNS Support» (почтовый адрес: support@dyndns.com). Для подтверждения регистрации учетной записи необходимо перейти по указанной в нем ссылке.

После перехода по адресу, указанному в теле письма, откроется страница с подтверждением создания и активации Вашей учетной записи. Для входа на сайт под созданной учетной записью введите пароль и нажмите **[Confirm Account]** (*Рис. 7.15*).

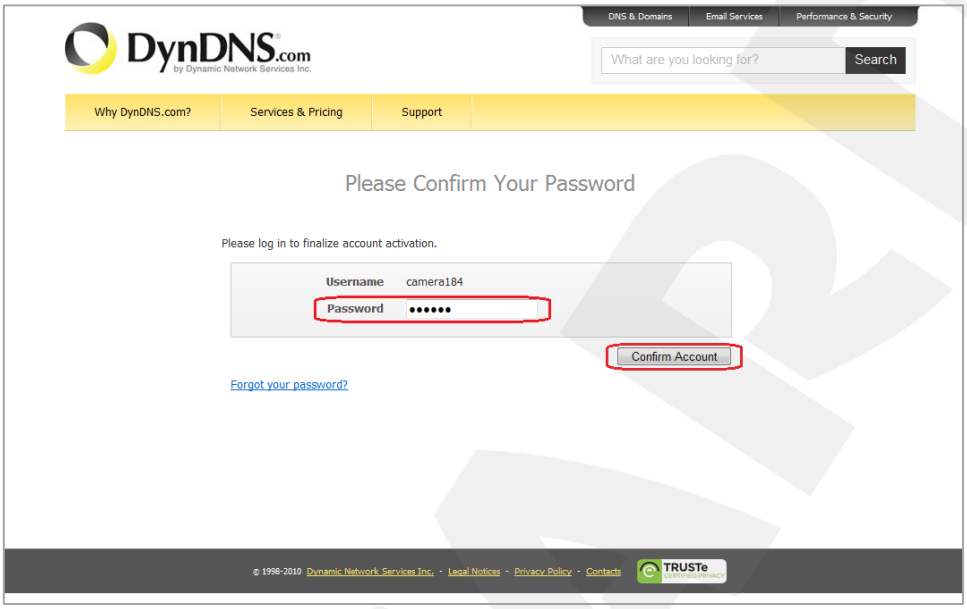

Рис. 7.15

Шаг 5: создание учетной записи для сервиса DynDNS завершено (*Рис. 7.16*).

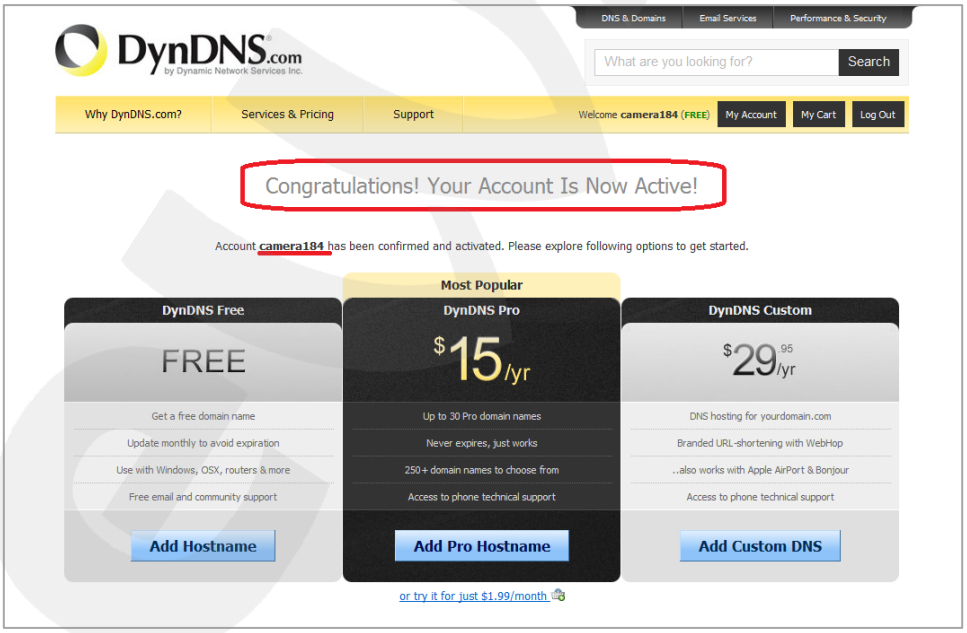

Рис. 7.16

7.4.3. Создание доменного имени на сервере DynDNS

Шаг 1: для настройки учетной записи на сервере DynDNS зайдите на сайт www.dyndns.com и авторизуйтесь под своей учетной записью, для чего укажите (в правом верхнем углу) созданные и зарегистрированные имя пользователя **[Username]** и пароль **[Password]**, после чего нажмите кнопку **[Login]** (*Рис. 7.17*).

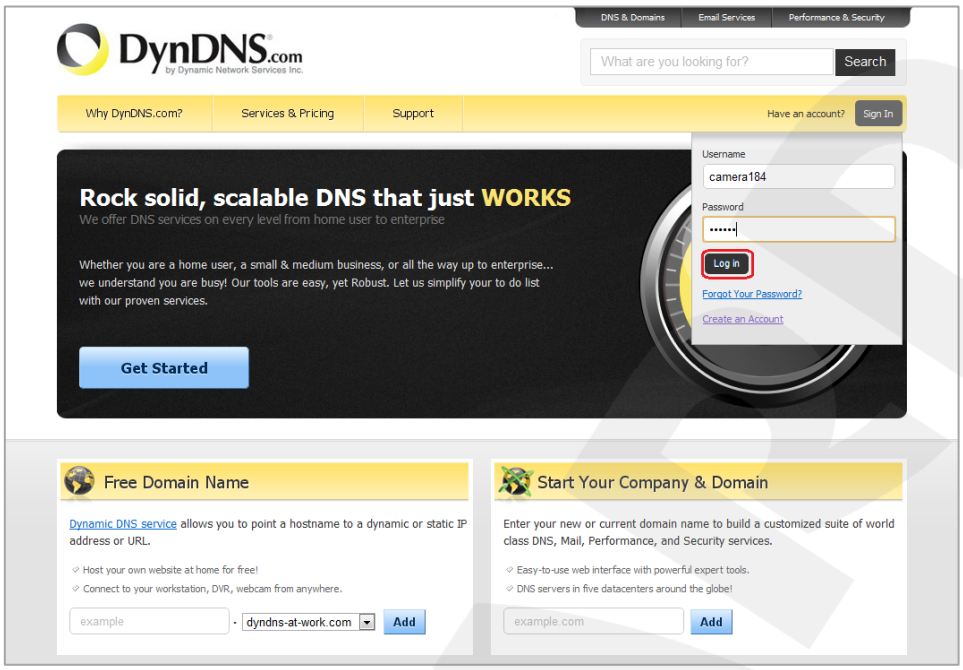

Рис. 7.17

Шаг 2: если все данные указаны правильно, Вы попадете на персональную страницу настроек. Для продолжения настройки выберите пункт **[Add Host Services]** (*Рис. 7.18*).

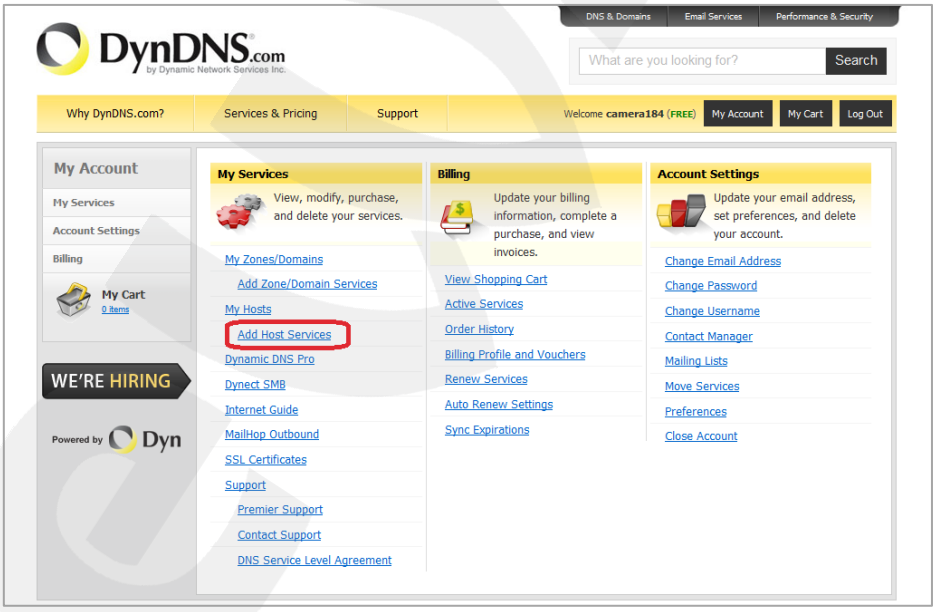

Рис. 7.18

Шаг 3: на открывшейся странице необходимо настроить параметры соединения с устройством. Выберите желаемый домен. Например, dyndns.org.

Далее в поле **[Hostname]** укажите доменное имя, для данного примера это – camera184. Если данное имя для выбранного домена свободно, то мы получим конечное доменное имя, в нашем примере это «camera184.dyndns.org» (*Рис. 7.19*).

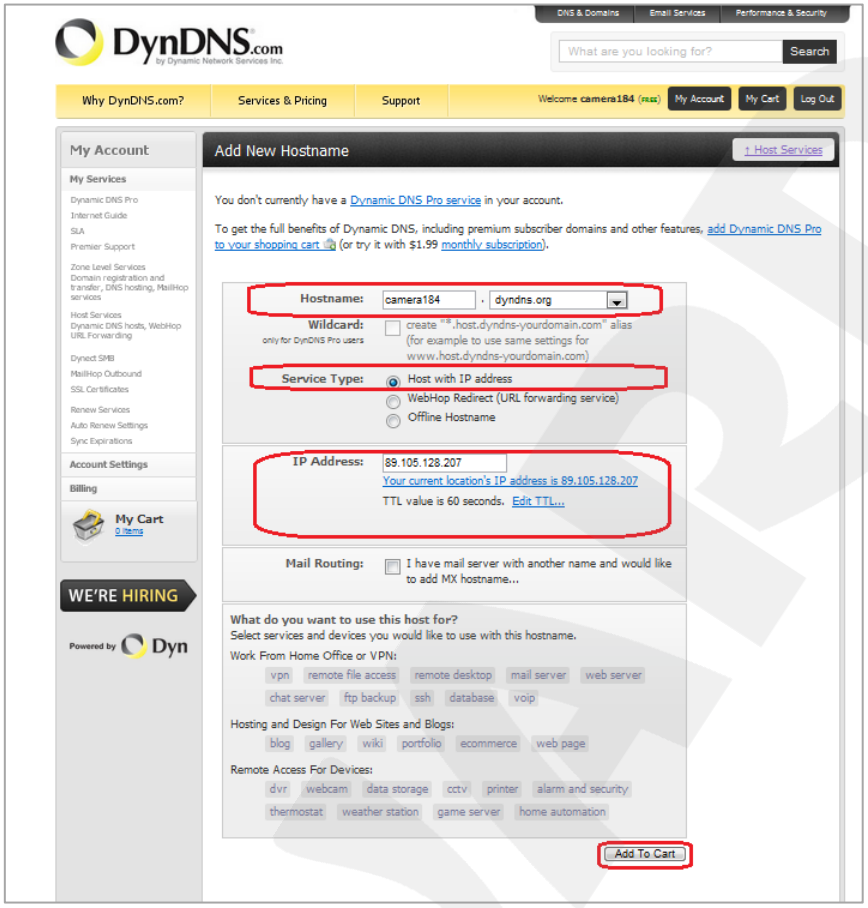

Рис. 7.19

Для сопоставления текущего динамического IP-адреса камеры с доменным именем необходимо указать IP-адрес того устройства, которое мы настраиваем для работы через DDNS. По умолчанию сервис определяет тот IP-адрес, с которого на данный момент времени происходит подключение (*Рис. 7.20*).

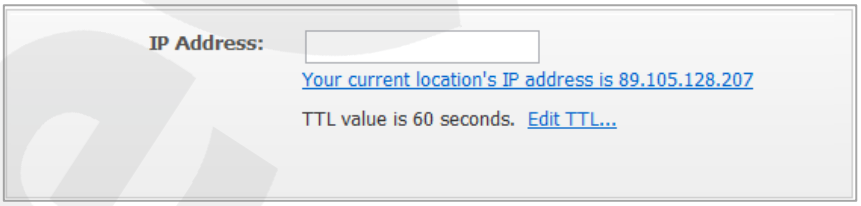

Рис. 7.20

Введите текущий IP-адрес, выданный Вашим провайдером в настоящий момент, и нажмите кнопку **[Add To Cart]**.

Шаг 4: при успешном создании доменного имени откроется страница с подтверждением этого. Так, для примера, описанного выше, будет указан созданный аккаунт camera184.dyndns.org. Для активации доменного имени нажмите кнопку **[Next]** (*Рис. 7.21*).

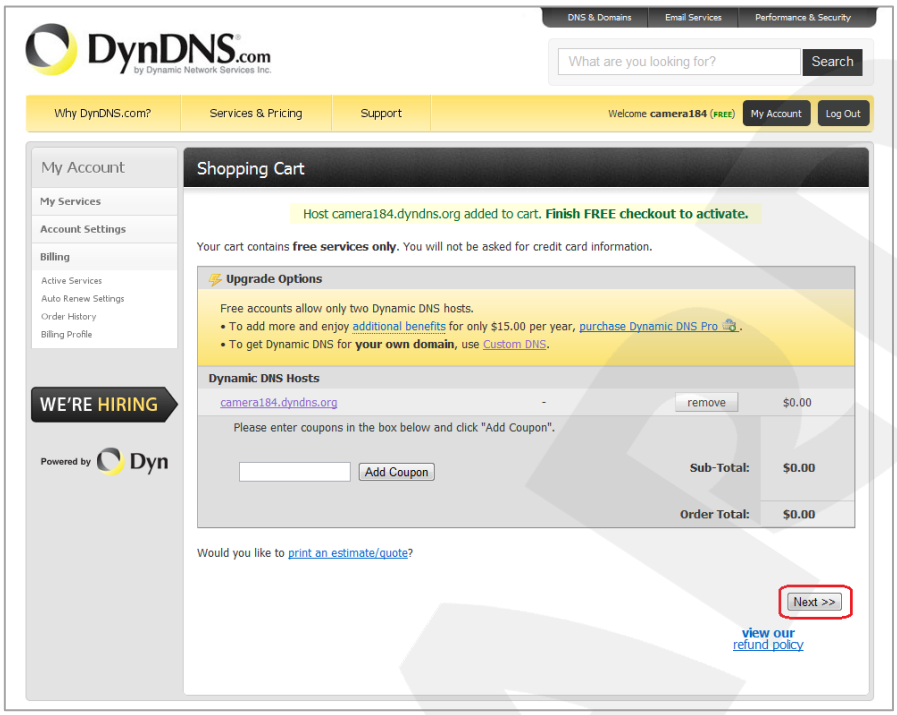

Рис. 7.21

На открывшейся странице активации нажмите кнопку **[Activate Service]** (*Рис. 7.22*).

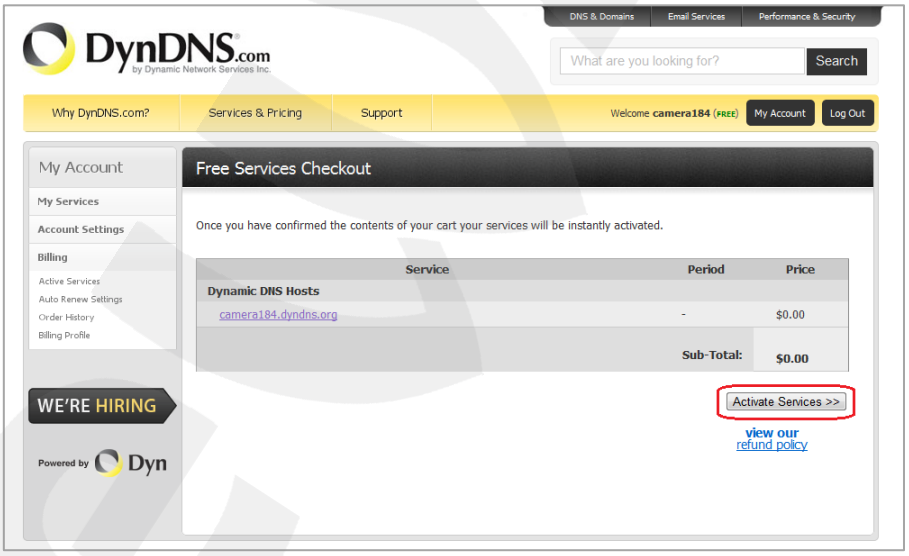

Рис. 7.22

Шаг 5: далее при успешной активации доменного имени откроется страница, подтверждающая это (*Рис. 7.23*).

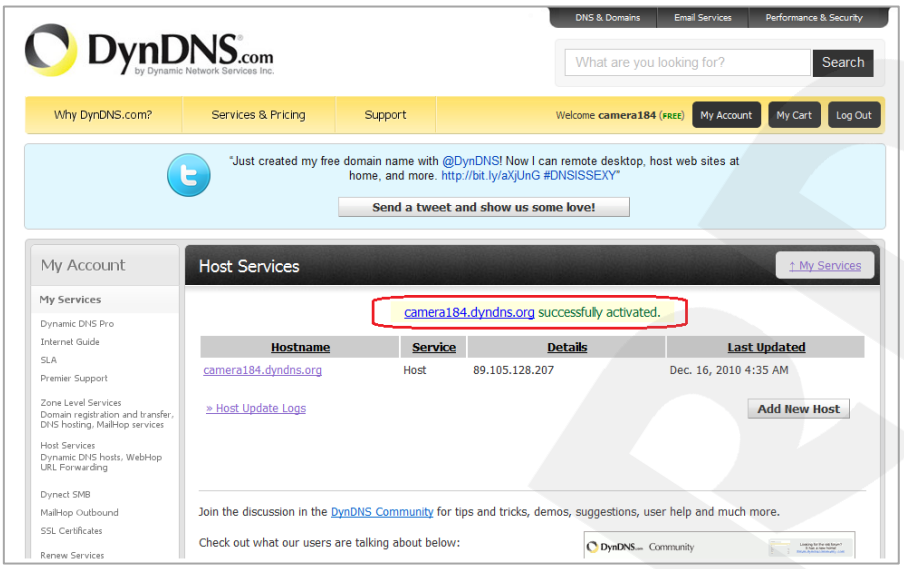

Рис. 7.23

Шаг 6: создание доменного имени на сервере DynDNS завершено.

7.4.4. Настройка оборудования для работы с сервисом DynDNS

Теперь требуется настроить IP-камеру в соответствии с данными, полученными при регистрации на сервисе DynDNS (пункты 7.4.2, 7.4.3 данного Руководства).

Обновлять IP-адрес на сервере DynDNS может как IP-камера, так и маршрутизатор (в случае если IP-камера подключена к сети Интернет через маршрутизатор).

Чтобы настроить IP-камеру для работы с сервисом DynDNS выполните следующие действия:

ВНИМАНИЕ!

IP-камера должна быть подключена к сети Интернет напрямую.

Шаг 1: разрешите опцию **[DDNS]** в настройках IP-камеры: ***Настройки – Сеть – Дополнительные – DDNS***.

Шаг 2: укажите поставщика сервиса DDNS в поле **[Сервер]**.

Шаг 3: введите имя пользователя, полученное при регистрации на сайте провайдера DDNS в поле **[Пользователь]**.

Шаг 4: введите пароль, полученный при регистрации на сайте провайдера DDNS в поле **[Пароль]**.

Шаг 5: повторно укажите пароль в поле **[Повторите пароль]**.

Шаг 6: введите доменное имя, полученное при регистрации на сайте провайдера DDNS в поле **[Название домена]**.

ВНИМАНИЕ!

Более подробно настройка камеры через веб-интерфейс рассмотрена в Руководстве по эксплуатации.

В соответствии с данными, полученными при регистрации на сервисе DynDNS (пункты 7.4.2, 7.4.3 данного Руководства), в поле **[Сервер]** выберите www.dyndns.org, в поля **[Пользователь]** и **[Пароль]** введите соответственно «camera184» и «123456». В поле **[Название домена]** необходимо указать: camera184.dyndns.org (*Рис. 7.24*).

Шаг 7: для применения настроек нажмите кнопку **[Сохранить]**.

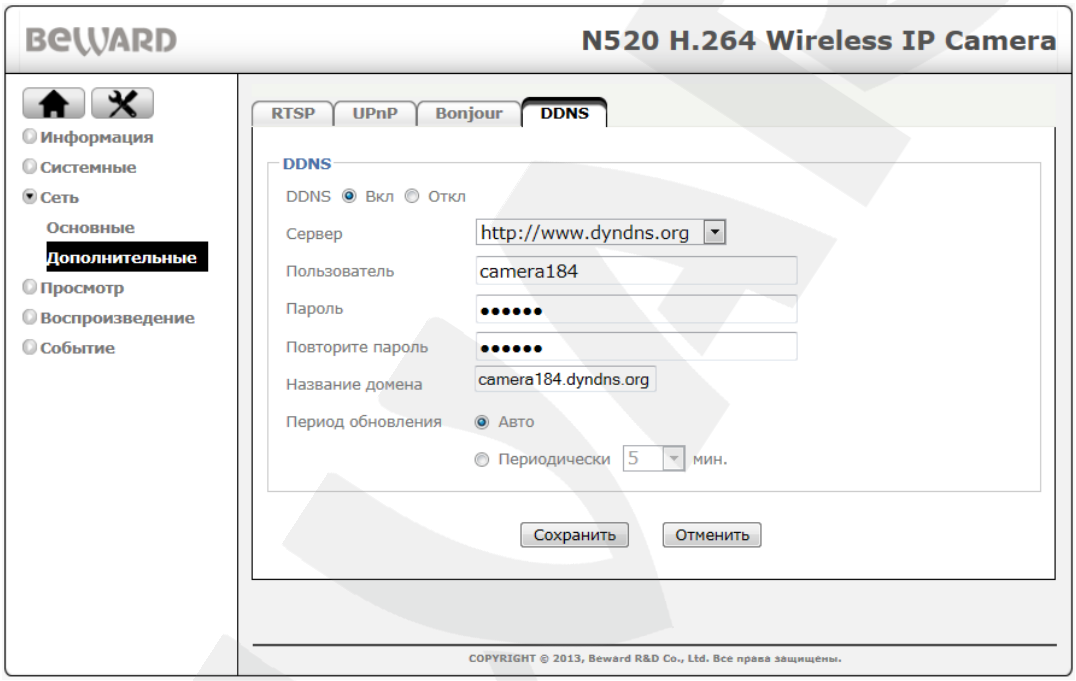

Рис. 7.24

ВНИМАНИЕ!

Для применения сетевых параметров требуется перезагрузка устройства.

ВНИМАНИЕ!

Если обновление IP-адреса для Вашего доменного имени не будет производиться в течение 35 дней, это доменное имя будет освобождено.

Шаг 8: настройка IP-камеры для работы с сервисом DynDNS завершена.

Рассмотрим пример настройки DDNS для маршрутизатора на примере Planet XRT-412. Оборудование других марок настраивается аналогично, в соответствии с инструкцией по эксплуатации к применяемому оборудованию. Чтобы настроить маршрутизатор для работы с сервисом DynDNS выполните следующие действия:

ВНИМАНИЕ!

Маршрутизатор должен поддерживать функцию работы с DDNS, должен быть подключен к сети Интернет и иметь соответствующие сетевые настройки.

Шаг 1: введите в адресной строке браузера IP-адрес маршрутизатора. В появившемся окне запроса введите логин и пароль. После удачной авторизации откроется основная страница настроек маршрутизатора. Выберите пункт **[General Setup]** (*Рис. 7.25*).

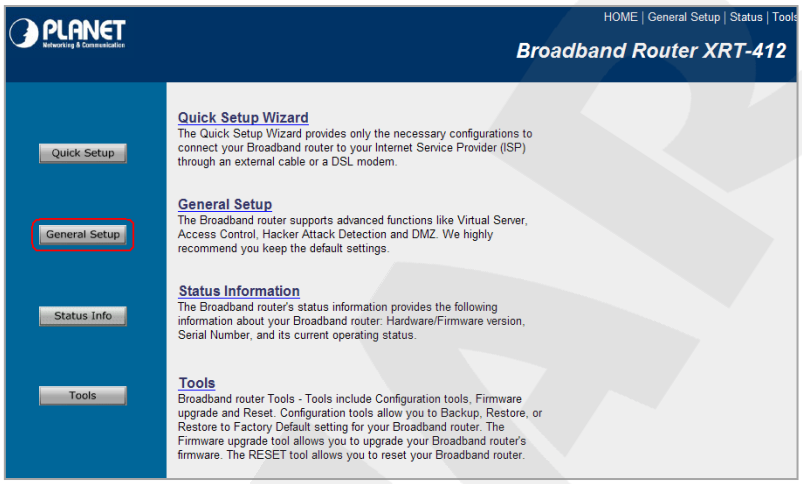

Рис. 7.25

Шаг 2: в появившемся меню выберите пункт **[DDNS]**. Активизируйте DDNS-клиент, поставив флажок **[Enable]**.

Шаг 3: в соответствии с данными, полученными при регистрации на сервисе DynDNS (пункты 7.4.2, 7.4.3 данного Руководства), в поле **[Provider]** выберите www.dyndns.org, в поле **[Domain name]** необходимо указать camera184.dyndns.org, в поля **[Account]** и **[Password]** введите соответственно «camera184» и «123456». (*Рис. 7.26*).

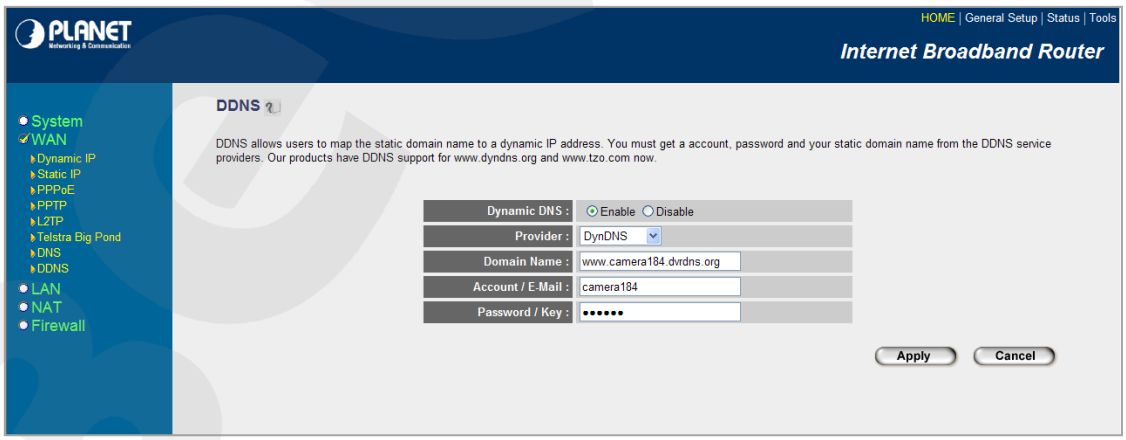

Рис. 7.26

ВНИМАНИЕ!

Будьте внимательны: при некорректном заполнении маршрутизатор не сможет подключиться к серверу DDNS.

Шаг 4: для сохранения изменений нажмите **[Apply]**.

Шаг 5: настройка маршрутизатора для работы с сервисом DynDNS завершена.

Если все настройки выполнены верно, то теперь Ваш собственный ресурс сети открыт для доступа из любой точки земного шара под своим уникальным именем, понятным и удобным для запоминания.

Теперь для обращения к камере достаточно в браузере ввести запрос http://camera184.dyndns.org, и, если все настройки выполнены корректно, то Вы попадете на главную страницу камеры.

BEWARD

Приложения

Приложение А. Значения используемых портов

Назначение порта	Значение по умолчанию	Диапазон значений
HTTP	80	1124..65534
Переадресация HTTP с помощью UPnP	80	1124..65534
HTTPS	443	1124..65534
Переадресация HTTPS с помощью UPnP	443	1124..65534
RTSP	554	1124..65534
Переадресация RTSP с помощью UPnP	554	1124..65534
Начальный порт диапазона RTP	5000	1124..65435
Конечный порт диапазона RTP	7999	1223..65534
Порт видео для Мультикаст	-	1124..65534
Порт аудио для Мультикаст	-	1124..65534
SMTP	25	1..65535
Порт удаленного сервера журнала событий	514	1124..65534
Порт сервера событий	80	1..65535
Порт прокси	-	1..65535
Детектор движения	1999	-
Поток MPEG4 (HTTP)	80	1124..65534
Поток MJPEG (HTTP)	80	1124..65534

Приложение В. Заводские установки

Наименование	Значение
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**
RTSP-порт	**554**
SMTP-порт	**25**

BEWARD

Приложение C. Общие сведения о безопасности беспроводных соединений

Для предотвращения несанкционированного доступа к беспроводному соединению необходимо особое внимание к вопросам безопасности.

Беспроводная точка доступа поддерживает несколько видов защиты Wi-Fi сети с использованием различных методов и алгоритмов шифрования и идентификации (WEP, 802.1x, 802.1x с WEP, WPA-PSK, WPA-AES и WPA RADIUS).

Использование того или иного вида шифрования позволит значительно снизить риск перехвата информации и несанкционированного подключения к Вашей беспроводной сети. Наиболее простой и одновременно наименее защищенный протокол шифрования это WEP с длиной ключа 64 бит. Его следует использовать только в том случае, если подключаемое оборудование не поддерживает других алгоритмов шифрования.

Протоколы защиты WEP (Wired Equivalent Privacy), WPA и WPA2 обеспечивают единую инфраструктуру для управления доступом, защиты и шифрования данных, пересылаемых между беспроводной точкой доступа и беспроводным клиентом. Для защиты подключения на точке доступа необходимо активизировать WEP или WPA.

В основе протокола WPA, который пришел на смену WEP, лежит подмножество стандарта IEEE 802.11i, а WPA2 основан на окончательной редакции стандарта IEEE 802.11i. В WPA применяется несколько способов и алгоритмов, в частности TKIP (Temporal Key Integrity Protocol) и AES (Advanced Encryption Standard) для повышения надежности методов управления ключами и шифрования. Большинство современных беспроводных устройств совместимы с WPA.

WEP и WPA шифруют данные, пересылаемые между Точкой доступа и удаленными клиентами. То есть, ключ (набор символов), известный как беспроводной Точке доступа, так и клиенту, используется для шифрования и восстановления данных, пересылаемых между этими устройствами. Взломщик, завладевший ключом, может расшифровать данные, пересылаемые между беспроводными AP и клиентом или установить соединение с беспроводной Точкой доступа.

Существенный недостаток WEP – это необходимость вручную вводить ключ, используемый для шифрования, как на беспроводной точке, так и на клиенте.

Для устранения недостатков WEP-шифрования протокол WPA дополнен функциями управления ключом. Как и в WEP, ключ здесь используется для шифрования данных. Однако он вводится один раз, а впоследствии с помощью этого ключа WPA генерирует настоящий ключ для шифрования данных. WPA периодически меняет ключ. Следовательно, в случае взлома ключа шифрования, тот будет полезен только до тех пор, пока беспроводная Точка доступа и клиент автоматически не изменят его.

Оптимальным режимом является WPA Pre-Shared Key (WPA-PSK), который обеспечивает достаточно надежную защиту и прост в настройке.

Для настройки использования режима WPA-PSK нужно выбрать параметр WPA Pre-Shared Key. В точке доступа реализованы три алгоритма WPA: TKIP, AES и совмещенный. TKIP – это устаревший протокол, предназначенный для того, чтобы устранить многочисленные проблемы WEP до широкого распространения протокола следующего поколения WPA (WPA2). В TKIP используется тот же алгоритм шифрования, что и в WEP, но многие изъяны WEP устранены благодаря динамической смене ключа шифрования данных, шифрованию данных настройки, представленных обычным текстом в WEP, и проверке целостности сообщений. AES – это новый, исключительно надежный алгоритм шифрования, базируемый на стандарте 802.11i и WPA2. Однако он пока не реализован во всех аппаратных средствах и программном обеспечении. По возможности следует выбирать AES.

После выбора режима работы вводится ключ WPA Shared Key. Необходимо ввести один и тот же ключ на всех клиентах, которые устанавливают связь с точкой доступа. Следует выбирать длинный, трудно разгадываемый ключ. Длина ключа не менее 8 символов, но не более 63 символов ASCII. Рекомендуемая длина ключа не более 20 символов.

ПРИМЕЧАНИЕ!
Не рекомендуется вводить ключ длиной больше 20 ASCII символов, так как длинный ключ может существенно замедлить работу беспроводной сети.

Если клиенты несовместимы с WPA, лучше использовать WEP, чем вовсе отказаться от защиты. Для настройки WEP в следует указать режим безопасности Shared Key (Меню Advanced Setting), выбрать ключ для использования в качестве стандартного ключа передачи (ключ с номером от 1 до 4) и длину WEP ключа (64 или 128) с представлением в шестнадцатеричном или ASCII-формате. Ключ следует ввести в поле Key, которое соответствует выбранному стандартному ключу передачи. Например, если выбран 64-х разрядный шестнадцатеричный ключ, то можно ввести строку из десяти шестнадцатеричных цифр. Эту конфигурацию WEP-ключа необходимо повторить во всех клиентах, поэтому следует выбирать вариант настройки, приемлемый для всех устройств.

ПРИМЕЧАНИЕ!
Процедура настройки WEP-шифрования может различаться для различного оборудования в большей степени, чем настройка WPA, поэтому рекомендации по WEP труднее адаптировать к конкретной ситуации.

Приложение D. Гарантийные обязательства

D1. Общие сведения

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

б) Условия эксплуатации всего оборудования должны соответствовать ГОСТ 15150-69, ГОСТ В20.39.304-76 (в зависимости от исполнения устройства).

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

D2. Электромагнитная совместимость

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

D3. Электропитание

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

D4. 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.

D5. 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.

D6. 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.

D7. 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.

D8. 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.

D9. Подключение интерфейсов

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

D10. 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 E. Права и поддержка

E1. Торговая марка

Copyright © BEWARD 2016.

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.

E2. 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.

E3. Предупреждения FCC

Это оборудование было протестировано и признано удовлетворяющим требованиям положения о цифровых устройствах, принадлежащих к классу A, 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.

E4. Предупреждение CE

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

E5. 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 F. Глоссарий

3GP – мультимедийный контейнер, определяемый Партнёрским Проектом Третьего поколения (Third Generation Partnership Project (3GPP) для мультимедийных служб 3G UMTS. Многие современные мобильные телефоны имеют функции записи и просмотра аудио и видео в формате 3GP.

ActiveX – это стандарт, который разрешает компонентам программного обеспечения взаимодействовать в сетевой среде независимо от языка(-ов), используемого для их создания. Веб-браузеры могут управлять элементами управления ActiveX, документами ActiveX и сценариями ActiveX. Элементы управления ActiveX часто загружаются и инсталлируются автоматически, как запрашиваемы. Сама по себе данная технология не является кроссплатформенной и поддерживается в полном объеме только в среде Windows в браузере Internet Explorer 9.0.

ADSL (Asymmetric Digital Subscriber Line / Асимметричная цифровая абонентская линия) – модемная технология, превращающая аналоговые сигналы, передаваемые посредством стандартной телефонной линии, в цифровые сигналы (пакеты данных), позволяя во время работы совершать звонки.

Angle / Угол обзора – это угол, который образуют лучи, соединяющие заднюю точку объектива и диагональ кадра. Угол зрения показывает съемочное 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.

ARP (Address Resolution Protocol / Протокол определения адреса) – использующийся в компьютерных сетях протокол низкого уровня, предназначенный для определения адреса канального уровня по известному адресу сетевого уровня. Наибольшее распространение этот протокол получил благодаря повсеместности сетей IP, построенных поверх Ethernet. Этот протокол используется для связи IP-адреса с MAC-адресом устройства. По локальной сети транслируется запрос для поиска узла с MAC-адресом, соответствующим IP-адресу.

Aspect ratio / Формат экрана – это форматное отношение ширины к высоте кадров. Общий формат кадра, используемый для телевизионных экранов и компьютерных мониторов, составляет 4:3. Телевидение высокой четкости (HDTV) использует формат кадра 9:16.

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.

Auto Iris / АРД (Авторегулируемая диафрагма) – это автоматическое регулирование величины диафрагмы для контроля количества света, попадающего на матрицу. Существует два варианта автоматической регулировки диафрагмы: Direct Drive и Video Drive.

Biterate / 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 отрабатывает интегральную, т.е. общую освещенность сцены, «видимой» камерой через объектив. Соответственно, малая фигура человека на большом светлом фоне окна выльется в итоге "засветкой" всей картинки. 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 предназначается 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.

CIDR / Бесклассовая адресация (англ. *Classless Inter-Domain Routing*, англ. *CIDR*) – метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации. Использование этого метода позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку возможно применение различных масок подсетей к различным подсетям.

CCD / ПЗС-матрица – это светочувствительный элемент, использующийся во многих цифровых камерах и представляющий собой крупную интегральную схему, состоящую из сотен тысяч зарядов (пикселей), которые преобразуют световую энергию в электронные

сигналы. Размер матрицы изменяется по диагонали и может составлять 1/4", 1/3", 1/2" или 2/3".

CGI (Единый шлюзовый интерфейс) – спецификация, определяющая взаимодействие web-сервера с другими CGI-программами. Например, HTML-страница, содержащая форму, может использовать CGI-программу для обработки данных формы.

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.

Digital Zoom / Цифровое увеличение – это увеличение размера кадра не за счет оптики, а с помощью кадрирования полученного с матрицы изображения. Камера ничего не увеличивает, а только вырезает нужную часть изображения и растягивает ее до первоначального разрешения.

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.

Firewall / Брандмауэр – брандмауэр (межсетевой экран) работает как барьер между сетями, например, между локальной сетью и Интернетом. Брандмауэр гарантирует, что только зарегистрированным пользователям будет разрешен доступ из одной сети в другую сеть. Брандмауэром может быть программное обеспечение, работающее на компьютере, или брандмауэром может быть автономное аппаратное устройство.

Focal length / Фокусное расстояние – измеряемое в миллиметрах фокусное расстояние объектива камеры, определяющее ширину горизонтальной зоны обзора, которое в свою очередь измеряется в градусах. Определяется как расстояние от передней главной точки до переднего фокуса (для переднего фокусного расстояния) и как расстояние от задней главной точки до заднего фокуса (для заднего фокусного расстояния). При этом, под главными точками подразумеваются точки пересечения передней (задней) главной плоскости с оптической осью.

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 развѐртки 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.

Full-duplex / Полный дуплекс – полный дуплекс представляет собой передачу данных одновременно в двух направлениях. В системе звуковоспроизведения это можно описать, например, телефонными системами. Также полудуплексная связь обеспечивает двухстороннюю связь, но только в одном направлении за один раз.

G.711 – стандарт для представления 8-битной компрессии PCM (ИКМ) сигнала с частотой дискретизации 8000 кадров/секунду и 8 бит/кадр. Таким образом, G.711 кодек создаёт поток 64 Кбит/с.

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.

Hub / Сетевой концентратор - сетевой концентратор используется для подключения многочисленных устройств к сети. Сетевой концентратор передает все данные в устройства, подключенные к нему, тогда как коммутатор только передает данные в устройство, которое специально предназначено для него.

ICMP (Internet Control Message Protocol / Межсетевой протокол управляющих сообщений) – сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна или хост или маршрутизатор не отвечают.

IEEE 802.11 / Стандарт IEEE 802.11 – это семейство стандартов для беспроводных локальных сетей. Стандарт 802.11 поддерживает передачу данных на скорости 1 или 2 Мбит/сек на полосе 2.4 ГГц. Стандарт же 802.11b задает скорость передачи данных 11 Мбит/сек на полосе 2.4 ГГц, в то время как стандарт 802.11a позволяет задать скорость до 54 Мбит/сек. на полосе 5 ГГц.

Interlaced video / Чересстрочная развертка – это видеозапись со скоростью 50 изображений (называемых полями) в секунду, из которых каждые 2 последовательных поля (полукадра) затем объединяются в 1 кадр. Чересстрочная развертка была разработана много лет назад для аналогового телевидения и до сих пор широко применяется. Она дает хорошие результаты при просмотре движения в стандартном изображении, хотя всегда существует некоторое искажение изображения.

Internet Explorer (IE) – серия браузеров, разрабатываемая корпорацией Microsoft с 1995 года. Входит в комплект операционных систем семейства Windows. Является наиболее широко используемым веб-браузером.

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.

Lux / Люкс – единица измерения освещенности. Определяется как освещенность поверхности площадью 1 кв.м. световым потоком 1 люмен. Используется для обозначения чувствительности камер.

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 (потоковое видео), записи фильмов на компакт-диски, видеотелефонии (видеотелефон) и широковещания, в которых активно используется сжатие цифровых видео и звука.

Multicast / Групповая передача – специальная форма широковещания, при которой копии пакетов направляются определённому подмножеству адресатов. Наряду с приложениями, устанавливающими связь между источником и одним получателем, существуют такие приложения, где требуется, чтобы источник посылал информацию сразу группе получателей. При традиционной технологии IP-адресации требуется каждому получателю информации послать свой пакет данных, то есть одна и та же информация передается много раз. Технология групповой адресации представляет собой расширение IP-адресации, позволяющее направить одну копию пакета сразу всем получателям. Множество получателей определяется принадлежностью каждого из них к конкретной группе. Рассылку для конкретной группы получают только члены этой группы.

Технология IP Multicast предоставляет ряд существенных преимуществ по сравнению с традиционным подходом. Например, добавление новых пользователей не влечет за собой необходимое увеличение пропускной способности сети. Значительно сокращается нагрузка на посылающий сервер, который больше не должен поддерживать множество двухсторонних соединений.

Для реализации групповой адресации в локальной сети необходимы: поддержка групповой адресации стеком протокола TCP/IP, программная поддержка протокола IGMP для отправки запроса о присоединении к группе и получении группового трафика, поддержка групповой адресации сетевой картой, приложение, использующее групповую адресацию, например, видеоконференция. Технология «мультикаст» использует адреса с 224.0.0.0 до 239.255.255.255. Поддерживается статическая и динамическая адресация. Примером статических адресов являются 224.0.0.1 – адрес группы, включающей в себя все узлы локальной сети, 224.0.0.2 – все маршрутизаторы локальной сети. Диапазон адресов с 224.0.0.0 по 224.0.0.255 зарезервирован для протоколов маршрутизации и других низкоуровневых протоколов поддержки групповой адресации. Остальные адреса динамически используются приложениями. На сегодняшний день большинство маршрутизаторов поддерживают эту опцию (в меню обычно есть опция, разрешающая IGMP протокол или мультикаст).

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

NTSC (National Television System Committee / Стандарт NTSC) – стандарт NTSC является телевизионным и видеостандартом в США. Стандарт NTSC доставляет 525 строк в кадре на 30 к/сек.

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 номером 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/TLS (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 защищённой 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).

TTL (Time to live) – предельный период времени или число итераций или переходов, за который набор данных (пакет) может существовать до своего исчезновения. Значение TTL может рассматриваться как верхняя граница времени существования IP-дейтаграммы в сети. Поле TTL устанавливается отправителем дейтаграммы и уменьшается каждым узлом (например, маршрутизатором) на пути его следования, в соответствии со временем пребывания в данном устройстве или согласно протоколу обработки. Если поле TTL становится равным нулю до того, как дейтаграмма прибудет в пункт назначения, то такая дейтаграмма отбрасывается и отправителю отсылается ICMP-пакет с кодом 11 – «Превышение временного интервала».

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.

WAP (Wireless Application Protocol / Беспроводной протокол передачи данных) – протокол, созданный специально для GSM-сетей, где нужно устанавливать связь портативных устройств с сетью Интернет. С помощью WAP пользователь мобильного устройства может загружать из сети Интернет любые цифровые данные.

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-потоком или другими данными.

Wi-Fi (Wireless Fidelity, дословно – «беспроводная точность») – торговая марка промышленной группы «Wi-Fi Alliance» для беспроводных сетей на базе стандарта IEEE 802.11. Любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance для получения соответствующего сертификата и права нанесения логотипа Wi-Fi.

W-LAN / Беспроводная LAN – это беспроводная локальная сеть, использующая в качестве носителя радиоволны: беспроводное подключение к сети конечного пользователя. Для основной сетевой структуры обычно используется кабельное соединение.

WPS (Wi-Fi Protected Setup) – стандарт, предназначенный для полуавтоматического создания беспроводной домашней сети. Протокол призван оказать помощь пользователям, которые не обладают широкими знаниями о безопасности в беспроводных сетях, и как следствие, имеют сложности при осуществлении настроек. WPS автоматически обозначает имя сети и задает шифрование, для защиты от несанкционированного доступа в сеть, при этом нет необходимости вручную задавать все параметры.

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.

Детектор саботажа – это программный модуль, который позволяет обнаруживать такие ситуации, как: расфокусировка, перекрытие или засвечивание изображения, отворот камеры, частичная потеря сигнала. Принцип действия основан на анализе в режиме реального времени изменения контраста локальных областей кадров из видеопотока, получаемого с телекамеры-детектора. Детектор саботажа автоматически выбирает области кадров, по которым необходимо оценивать изменение контрастности во времени и, если изменение контрастности в этих областях превышает некоторый относительный порог, принимает решение о потере «полезного» видеосигнала.

Диафрагма (от греч. diáphragma – перегородка) – это отверстие в объективе камеры, которое регулирует количество света, попадающего на матрицу. Изменение размера диафрагмы позволяет контролировать целый ряд показателей, важных для получения качественного изображения.

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.

Отношение сигнал/шум – численно определяет содержание паразитных шумов в сигнале. Измеряется в децибелах (дБ). Чем больше значение отношения сигнал/шум для видеосигнала, тем меньше помех и искажений имеет изображение.

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

Прокси-сервер (Proxy – представитель, уполномоченный) – служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс, расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного

кэша. Прокси-сервер позволяет защищать клиентский компьютер от некоторых сетевых атак и помогает сохранять анонимность клиента.

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.

Ручная диафрагма – противоположность автоматической диафрагмы, т.е. настройка диафрагмы камеры должна выполняться вручную для регулировки количества света, достигающего чувствительного элемента.

Светосила объектива – это характеристика, показывающая, какое количество света способен пропускать данный объектив. Чем больше максимальный диаметр открытой диафрагмы (или, соответственно, чем меньше F-число), тем большее количество света может попасть сквозь объектив на фокальную плоскость, и тем выше светосила объектива.

Симплекс – при симплексной связи сетевой кабель или канал связи может использоваться для передачи информации только в одном направлении.

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 светоизлучения.