

Руководство по подключению

www.beward.ru

IP-видеокамера N630

Встроенная ИК-подсветка
Мегапиксельное разрешение
Степень пыле- и влагозащиты: IP66
Поддержка карт памяти microSDHC



Оглавление

ГЛАВА 1. МЕРЫ ПРЕДОСТОРОЖНОСТИ	2
ГЛАВА 2. ОБЩИЕ СВЕДЕНИЯ	4
2.1. ОСОБЕННОСТИ IP-ВИДЕОКАМЕРЫ BEWARD N630	5
2.2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ	6
2.3. КОМПЛЕКТ ПОСТАВКИ	6
ГЛАВА 3. ВНЕШНИЙ ВИД	7
3.1. Вид СПЕРЕДИ	7
ГЛАВА 4. УСТАНОВКА И ПОДКЛЮЧЕНИЕ IP- КАМЕРЫ	10
4.1. ОБЩИЕ СВЕДЕНИЯ О ПОДКЛЮЧЕНИИ IP-КАМЕРЫ N630	10
4.3. МОНТАЖ УСТРОЙСТВА	12
4.4. ПРОВОДНОЕ ПОДКЛЮЧЕНИЕ КАМЕРЫ К СЕТИ	13
ГЛАВА 5. НАСТРОЙКА ПРОВОДНОГО СОЕДИНЕНИЯ	15
5.1. ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ ЛОКАЛЬНОЙ СЕТИ ДЛЯ ПРОВОДНОГО ПОДКЛЮЧЕНИЯ	15
5.1.1. <i>Определение параметров сети при динамическом IP-адресе</i>	19
5.2. ИЗМЕНЕНИЕ ПАРАМЕТРОВ ЛОКАЛЬНОЙ СЕТИ ДЛЯ ПРОВОДНОГО ПОДКЛЮЧЕНИЯ IP-КАМЕР	22
5.3. ПОЛУЧЕНИЕ ДОСТУПА К IP-КАМЕРАМ	26
5.3.1. <i>Установка «BEWARD IP Installer»</i>	26
5.3.2. <i>Получение доступа к IP-камере с помощью «BEWARD IP Installer»</i>	26
5.3.3. <i>Получение доступа к IP-камере с помощью [Сеть] ОС Windows 7</i>	28
5.3.4. <i>Получение доступа к IP-камере с помощью браузера Internet Explorer</i>	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 НАСТРОЕК ПОДКЛЮЧЕНИЯ К ЗАВОДСКИМ НАСТРОЙКАМ	34
5.7. ПРОВЕРКА ПРАВИЛЬНОСТИ НАСТРОЕК ПОДКЛЮЧЕНИЯ IP-КАМЕРЫ К ЛОКАЛЬНОЙ СЕТИ	37
ГЛАВА 6. ПОДКЛЮЧЕНИЕ IP-КАМЕРЫ К СЕТИ ИНТЕРНЕТ	39
6.1. ОБЩИЕ СВЕДЕНИЯ О ПОДКЛЮЧЕНИИ IP-КАМЕРЫ К СЕТИ ИНТЕРНЕТ	39
6.2. ПОДКЛЮЧЕНИЕ ПРИ СВОБОДНОМ ВНЕШНЕМ IP-АДРЕСЕ ИЛИ PPPoE-СОЕДИНЕНИИ	40
6.2.1. <i>Использование статического IP-адреса</i>	40
6.2.2. <i>Использование PPPoE-соединения</i>	41
6.3. ПОДКЛЮЧЕНИЕ ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ К IP-КАМЕРАМ, НАХОДЯЩИМСЯ В ЛОКАЛЬНОЙ СЕТИ	43
6.3.1. <i>Использование опции UPnP</i>	44
6.3.2. <i>Настройка перенаправления портов маршрутизатора</i>	45
6.4. ПРИМЕР ПОДКЛЮЧЕНИЯ К СЕТИ ИНТЕРНЕТ С ИСПОЛЬЗОВАНИЕМ DDNS	51
6.4.1. <i>Общие сведения о DDNS</i>	51
6.4.2. <i>Регистрация на сервере DynDNS</i>	52
6.4.3. <i>Настройка публичного имени на сервере DynDNS</i>	55
6.4.4. <i>Программное обеспечение для работы с сервисом DynDNS</i>	59
ПРИЛОЖЕНИЕ А	63
Приложение А. НАСТРОЙКИ ПОЛЬЗУЕМЫХ ПОРТОВ	63
Приложение В. ЗАВОДСКИЕ НАСТРОЙКИ	64
Приложение Г. ОБЯЗАТЕЛЬСТВА	65
Приложение Д. ПОДДЕРЖКА	68
Приложение Е. НЕИЗВЕСТНОЕ POE ОБОРУДОВАНИЕ	70
Приложение F. ГЛОССАРИЙ	71

Глава 1. Меры предосторожности

Перед использованием необходимо помнить нижеследующее:

Данный продукт удовлетворяет всем требованиям безопасности. Однако 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 камеры в неблагоприятных условиях:

- При слишком высоких или низких температурах. Рабочая температура устройств от -40°C до +50°C).
- Избегайте попадания прямых солнечных лучей на течение длительного времени, а также нахождения поблизости отопительных и обогревательных приборов.
- Избегайте близости устройствами, создающими большим электромагнитным эффектом.
- Недопустима установка камер в местах с сильной вибрацией.

ВНИМАНИЕ!

В случае неисправности камеры обратитесь в сервисный центр ООО «НПП «Бевард».

В случае остановки работы камеры:

- При обнаружении дыма или необычного запаха.
- При попадании воды или других инородных объектов внутрь.
- При обнаружении повреждения 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 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.

Глава 2. Общие сведения

BEWARD N630 – уличная, мегапиксельная, высококачественная IP-камера с мультипотоковым видеоизображением в форматах H.264/MPEG-4, для установки карты памяти стандарта MicroSD, высокочувствительный CMOS-сенсор нового поколения с функцией WDR (расширенный динамический диапазон).



Рис. 2.1

IP-камера BEWARD N630 позволяет передавать видео в реальном времени через стандартный Интернет-браузер. Особностью камеры является возможность использования профилей видеоизображения (функция X-Panner), которые вы можете сконфигурировать. Для каждого профиля можно задать индивидуальные параметры: тип сжатия, разрешение и зону просмотра. Пользователь, задавая для каждого профиля свой формат и скорость передачи данных, достигает оптимального соотношения между качеством изображения и использованием полосы пропускания. Таким образом, возможно выбрать нужный профиль и использовать его, когда это необходимо.

Камера может передавать видеопоток в различных форматах сжатия: H.264/MPEG-4. Формат кодирования H.264 является идеальным для использования в условиях ограниченной полосы пропускания, при его использовании достигается меньший размер файла и лучшее качество изображения, MJPEG предназначен для записи и хранения видеоизображения в наилучшем качестве, но при этом требует больших сетевых ресурсов и места на жестком диске при записи.

Камера N630 подключается к сети при помощи проводного интерфейса 10/100BASE-TX Ethernet, и имеет поддержку PoE.

Высокое качество изображения мегапиксельного разрешения реального времени обеспечивается за счет применения современного сенсора высокой чувствительности с прогрессивным сканированием, а также благодаря применению эффективных методов сжатия видеопотоков.

При использовании крупных систем видеонаблюдения с камерами всегда может сразу заметить закрытие камеры. Для предупреждения подобных действий со стороны третьих лиц, служит встроенный детектор саботажа, который позволяет информировать оператора о подобных несанкционированных действиях. Видеонаблюдение более интеллектуальным.

Поддержка карт памяти типа MicroSD, позволяет сделать видеонаблюдение еще более надежной: важная информация не пропадет при отключении. Весь объем информации будет сохранен в самой камере на карте памяти, который можно будет воспроизвести как непосредственно с карты, так и после устранения технических проблем сети.

2.1. Особенности IP-видеокамеры Beward N630

- Оптимальное соотношение цены и качества видеокамеры
- 1/4" КМОП-сенсор с прогрессивным сканированием и поддержкой WDR
- Электромеханический ИК-фильтр
- ИК-подсветка
- Соответствие стандарту пыле- и влагозащиты IP66
- Поддержка функции X-Panner
- Поддержка карт памяти типа MicroSD
- Профессиональное звуковое сопровождение (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
- Аналоговый вход
- Встроенный детектор саботажа и детектор движения
- Возможность скачивания кадров и видеороликов по электронной почте и на FTP
- Возможность подключения к внешнему файловому серверу (в том числе и в папку с открытым доступом на ПК с установленной ОС Windows или Linux)
- Поддержка протокола ONVIF

2.2. Основные характеристики

- Светочувствительный элемент: мегапиксельный КМОП-сенсор с активным сканированием и поддержкой WDR
- Объектив (опционально): f4.0 мм F1.8 (угол обзора 52° по горизонтали)
- Разрешение: 1280x800, 1280x720, 640x480, 320x240, 160x120
- Чувствительность: 0.2 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 разрешения 1280x800
- Форматы кодирования: H.264, MPEG-4, MJPEG
- Одновременное кодирование в форматах: H.264, MPEG-4, MJPEG
- Поддерживаемые протоколы: Bonjour, TCP/IP, DHCP, PPPoE, ARP, ICMP, FTP, SMTP, DDNS, NTP, UPnP, RTSP, RTSP over HTTP, HTTP, HTTPS, TCP, UDP, 3GPP/ISMA RTSP
- Питание: 12В, 0.5А (постоянный ток по стандарту IEEE 802.3af)
- Рабочая температура: от -40 до +50°C
- Поддержка отраслевого стандарта ONVIF

2.3. Комплект поставки

- IP-видеокамера с угловым объективом M12, f4.0 мм, F1.8
- Солнцезащитный козырек
- Источник питания постоянного тока
- Переходник
- Комплект крепежа
- CD-диск с программным обеспечением и документацией
- Руководство пользователя по быстрой установке

Глава 3. Внешний вид

3.1. Вид спереди

На лицевой части камеры расположены следующие элементы (Рис.3.1).

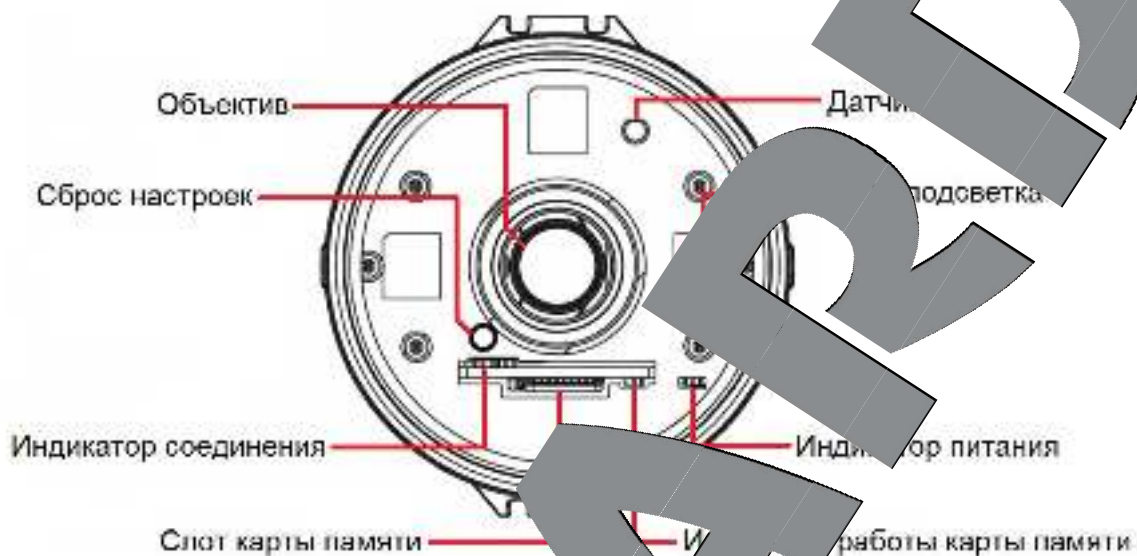


Рис.3.1.

Объектив: при размытом изображении необходимо настроить фокус камеры, для этого открутите переднюю крышку корпуса, добейтесь необходимой фокусировки путем вращения кольца настройки фокуса, когда Вы добьетесь необходимой фокусировки, закрутите переднюю крышку корпуса обратно (изначально камера уже сфокусирован и не требует дополнительной настройки).

Сброс настроек [Reset]: кнопка предназначена для сброса настроек камеры и возврата их в заводские.

Для сброса параметров в значениям по умолчанию удерживайте данную кнопку нажатой в течение 10-15 секунд. Если пользователь будет удерживать кнопку нажатой до 1 минуты, камера перезагрузится без сброса параметров в заводские установки.

Датчик освещенности: фотодатчик предназначенный для автоматического перехода камеры из режима «День» в режим «Ночь» и обратно.

ИК-подсветка: в любое время суток, при недостаточной освещенности камера переходит в режим «Ночь» (черно-белое изображение) и включается ИК-подсветка, которая позволяет вести видеонаблюдение даже в полной темноте. ИК-подсветка является альтернативой освещению стандартным лампам, но при этом она мало заметна для человеческого глаза.

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

- **Индикатор соединения мигает желтым 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.

Слот карты памяти: слот для карты памяти Micro SD/SDHC.

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

Индикация работы карты памяти: индикатор загорается при подключении карты памяти желтым цветом. При обращении к карте памяти для чтения/записи индикатор мигает.

Индикатор питания: индикатор питания загорается при подключении камеры к источнику питания.

- **Индикатор питания горит красным:** камере подключено питание, идет загрузка системы.
- **Индикатор питания горит синим:** загрузка IP-камеры завершена, камера готова к работе.
- **Индикатор питания мигает синим и красным одновременно:** идет обновление программного обеспечения камеры, отключите питание и не закрывайте окно браузера до завершения прошивки и полной загрузки камеры.
- **Индикатор питания не горит:** IP-камере не подключено питание либо отключена индикация в настройках камеры.

В задней части камеры при помощи специального крепления зафиксирован соединительный порт (рис. 3.2) на конце которого расположены следующие разъемы:

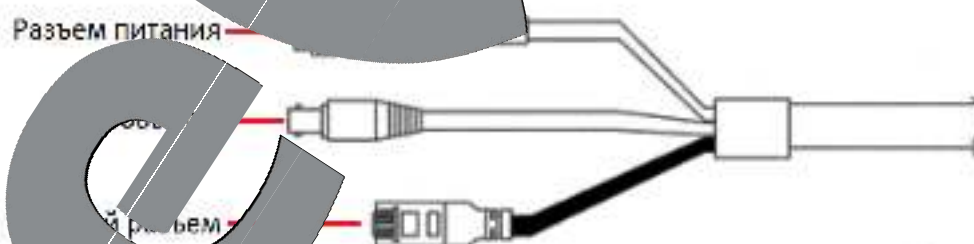


Рис. 3.2

Разъем питания: предназначен для подключения блока питания 12В, 1А.

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

Видео разъем: служит для вывода аналогового видеосигнала с камеры.

Сетевой разъем (Ethernet): разъем для подключения к сети при помощи стандартного RJ-45 штекера. Так же предусмотрена возможность получения питания через кабель витая пара (технология PoE).

Сбоку на корпусе наклеен стикер, содержащий информацию о продукте:

SN: серийный номер IP-камеры

MAC: MAC-адрес IP-камеры в сети LAN (при проводном подклю

Глава 4. Установка и подключение IP- камеры

4.1. Общие сведения о подключении IP-камеры N630 к сети

IP-камера N630 может подключаться к локальной сети либо к Интернету при помощи проводного соединения (Ethernet). Подключение можно осуществлять как напрямую к ПК, так и при помощи вспомогательного сетевого оборудования (маршрутизаторы, коммутаторы).



Обычно в домашних маршрутизаторах предусмотрены один WAN-порт для подключения сети Интернет и несколько внутренних LAN-портов для подключения компьютеров, IP-камер и других устройств домашней сети.

4.2. Рекомендации по установке

В данном разделе приведены список рекомендаций, которые необходимо учитывать при монтаже оборудования для видеонаблюдения.

Рекомендации по размещению камеры:

- IP-камера BEWARD N630 предназначена для осуществления видеонаблюдения в помещениях с предельной температурой эксплуатации от -40 до +50°C. Единительные части провода необходимо размещать в месте, не подверженном воздействию атмосферных осадков окружающей среды.
- Избегать попадания на камеру прямых солнечных лучей в течение длительного времени, а также нахождения поблизости отопительных и обогревательных приборов.

- Неправильная расстановка камер видеонаблюдения приведёт к появлению нежелательных «слепых» зон, которые будут оставаться вне поля зрения оператора.
- Избегайте близости с устройствами-генераторами мощных электромагнитных волн.
- Убедитесь в возможности размещения устройства в месте прохода соединительных кабелей.
- Избегайте способа крепления камеры, допускающего сильную вибрацию. Данное воздействие снизит эффективность детектора движения и четкость изображения в целом.
- Камеры видеонаблюдения необходимо держать в надёжности так, чтобы как случайное, так и специальное повреждение или изменение направления обзора было невозможно.
- Направление обзора (зона видеонаблюдения) должно быть твёрдо определено на момент установки.

Рекомендации по прокладке кабеля «камеры»:

- В коридорах желательно прокладывать пучки электрических и слаботочных кабелей по разным кабель-каналам, проходящим по разным стенам.
- Допускается в одном кабель-канале прокладывать витопарные и электрические кабели в разных отсеках, имеющих сплошные продольные перегородки с пределом огнестойкости не менее 0,25 ч. из негорючего материала. Рабочих зон на расстоянии не более 15-ти метров, если электрическая мощность 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, образуемая 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.
- Экранированные 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 1.5 метров от источников сильных электромагнитных помех, образующих напряженность электрического поля свыше 3 В/м.
- Прокладка витой пары между точками подключения производится целыми кусками, при этом направление трассы следует выбирать заранее таким, чтобы её протяжённость была как можно меньше.
- Минимальный радиус изгиба для кабеля – радиус изгиба кабеля (или 1 дюйм=2,5 см), но существуют рекомендации размещать кабель таким образом, чтобы обеспечивать изгиб радиусом не менее 10 сантиметров).
- Максимальная длина сегмента должна быть не более 100 метров.

4.3. Монтаж устройства

Если необходимо – установите камеру сверху защитный козырек. Его крепление осуществляется с помощью двух винтов, идущих в комплекте.

Шаг 1: закрепите козырек с помощью 2-х шурупов, но не фиксируйте его, козырек должен свободно перемещаться вперед и назад.

Шаг 2: определите, на какую глубину нужно продвинуть козырек.

Шаг 3: зафиксируйте положение козырька.

Камера крепится к поверхности с помощью 2-х шурупов (размер дюбеля 25x6 мм)

Шаг 1: обозначьте место крепления, затем просверлите отверстия под шурупы для крепления камеры.

Шаг 2: просверлите два отверстия глубиной 25 мм, если Вы планируете использовать шурупы из комплекта.

Шаг 3: закрепите крепление кронштейна к поверхности с помощью двух шурупов, используя отверстия в кронштейне.

Шаг 4: ослабьте винтовые соединения фиксатора кронштейна, чтобы иметь возможность поворачивать камеру для выбора необходимой зоны наблюдения.

Шаг 5: выберите угол наклона камеры и зафиксируйте её, используя винтовые соединения фиксатора кронштейна (Рис. 4.2).

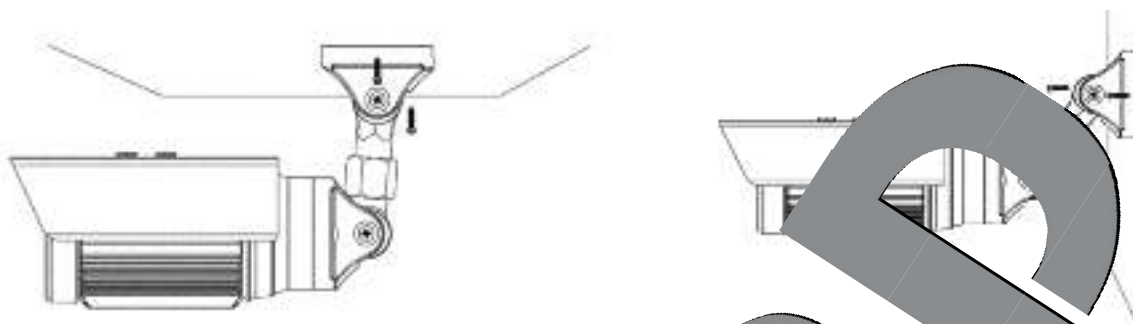


Рис. 4.2

После установки камеры на несущую поверхность, необходимо поместить соединительные провода в недоступное для попадания влаги место или в монтажную коробку со степенью влагозащиты не менее IP54. Например, модель 67051, с размерами 120x80x50 мм.

4.4. Проводное подключение камеры к сети

Шаг 1: подключите IP-камеру к источнику питания из комплекта поставки.

Шаг 2: используя соединительный кабель с разъемом RJ-45 (входит в комплект поставки), подключите IP-камеру к локальной сети (раوترу, LAN-маршрутизатору).

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

С одной стороны		С другой стороны	
	1: Бело-оранжевый		1: Бело-оранжевый
	2: Оранжевый		2: Оранжевый
	3: Бело-зелёный		3: Бело-зелёный
	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 «прямой» кабеля необходимы: кабель UTP (витая пара категории 5е или лучше) и устройство для обжима разъемов RJ-45 (кремпер).

При подключении пар, указанном в таблице, обеспечиваются гарантированные производителем величина и распределение задержек распространения сигнала, и заявленная скорость передачи данных 100 Мбит/сек.

Камера Beward N630 имеет возможность передачи питания по кабелю «витая пара» одновременно с данными (поддержка технологии **PoE**).

Технология предназначена для IP-телефонии, точек доступа беспроводных сетей, IP-камер, сетевых концентраторов и других устройств, к которым нежелательно или невозможно проводить отдельный электрический кабель.



Рис. 4.3

Для подключения камеры при использовании технологии PoE достаточно только подключить камеру при помощи патч-корда, при этом использовать дополнительный источник питания не нужно.

ВНИМАНИЕ!

Одновременная подача питания от электросети и от источника питания при помощи технологии PoE – ЗАПРЕЩЕНА!

Глава 5. Настройка проводного соединения для Windows 7

Для того чтобы IP-камера N630 работала в Вашей локальной сети совместно с Вашими компьютерами, ноутбуками и другим оборудованием, необходимо подключить IP-камеру в сеть в соответствии с настройками данной сети, для чего необходимо изменить текущие настройки.

ПРИМЕЧАНИЕ!

Описание установки и настройки соединения для Windows 7 приведено 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 необходимо определить текущие настройки проводной сети.

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

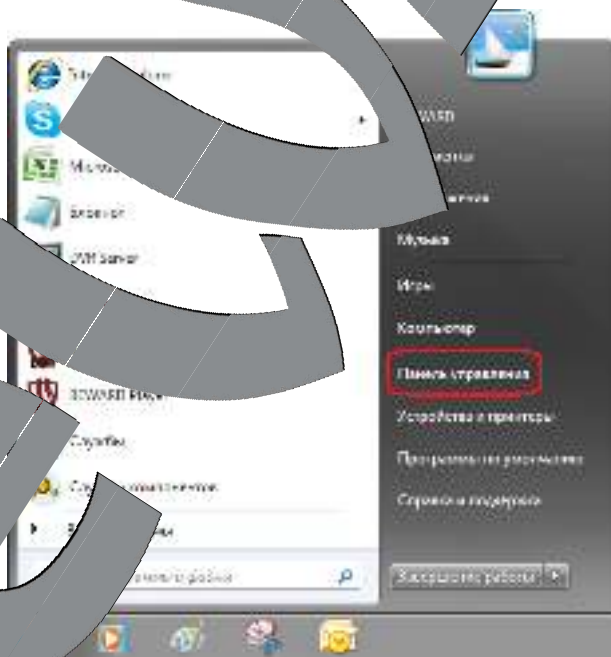


Рис. 5.1

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

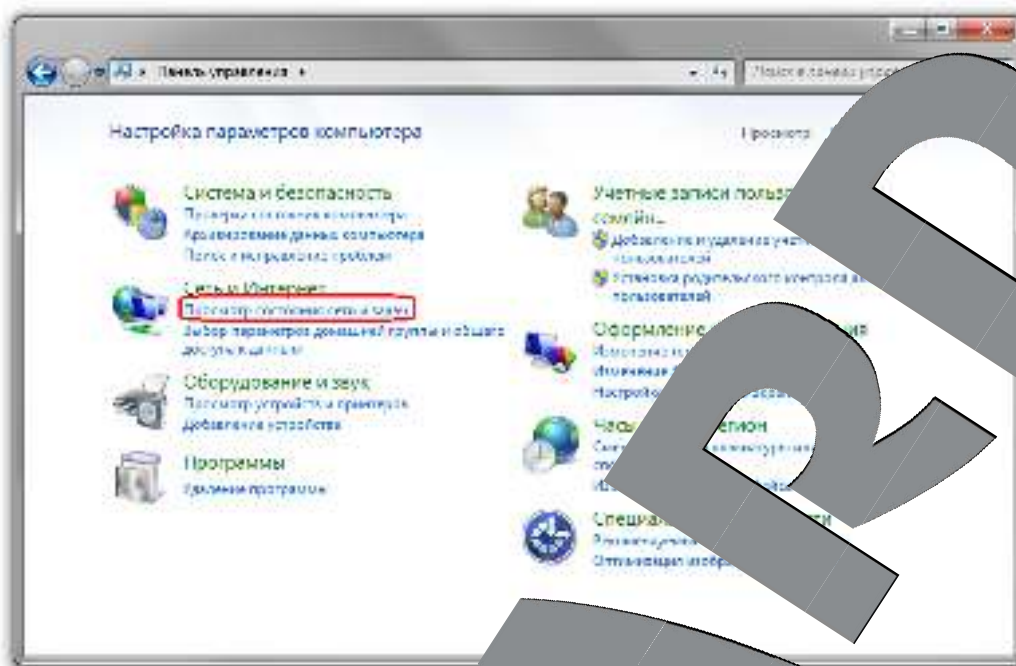


Рис.

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

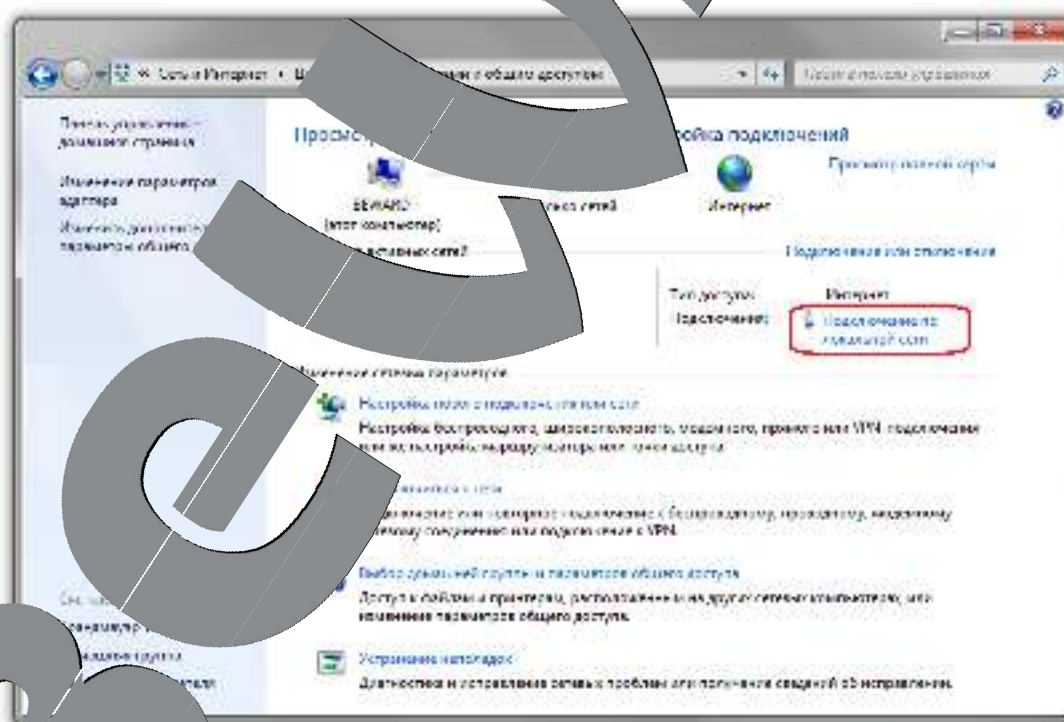
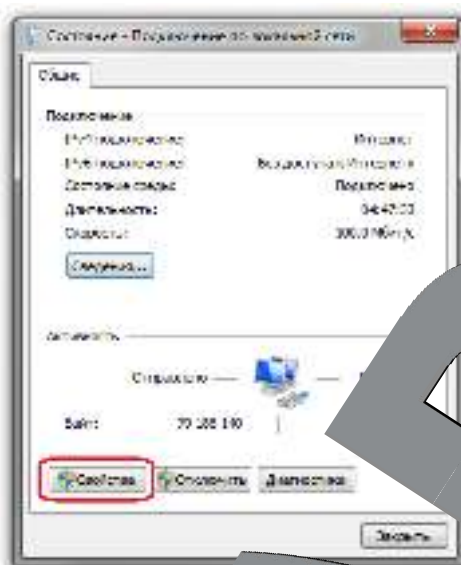


Рис. 5.3

ПРИМ.

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

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



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

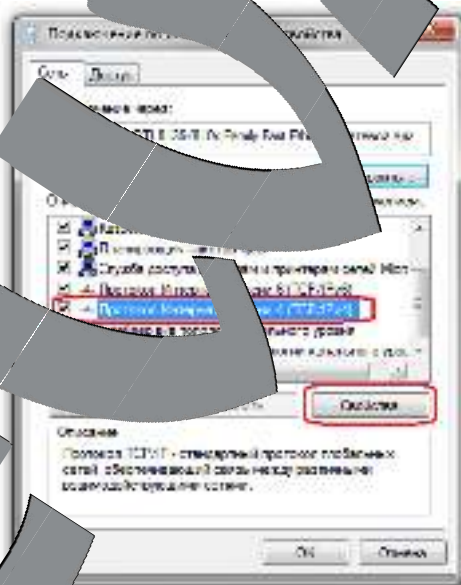


Рис. 5.5

Откроется окно, в котором отображается информация о настройках сетевого подключения. Включены две варианты настройки IP-адреса сетевого подключения Вашего ПК:

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.

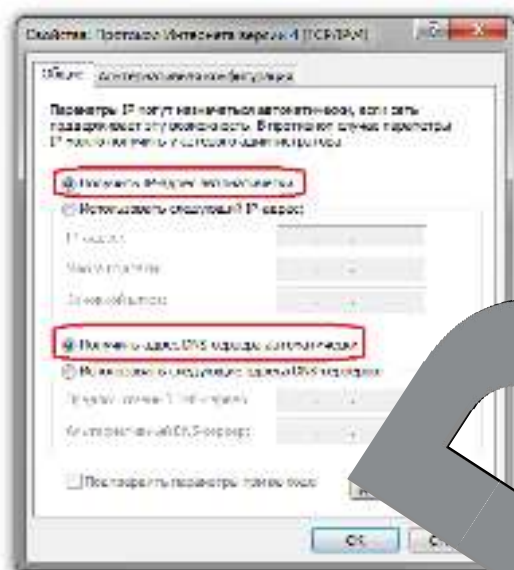


Рис. 5.6

2. Использовать следующий IP-адрес и адрес DNS сервера пользователем вручную (Рис. 5.7):

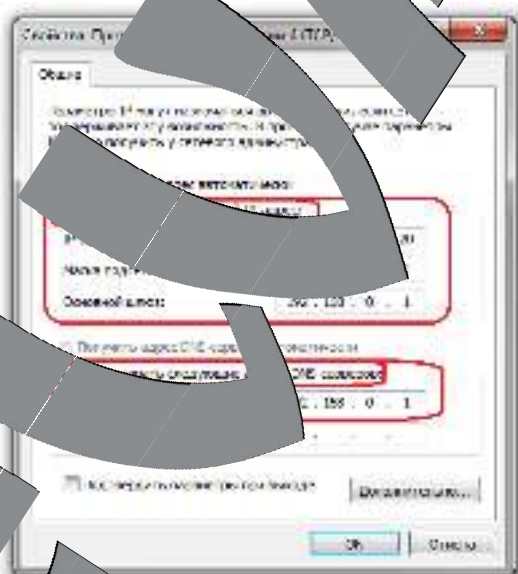


Рис. 5.7

Запомним конфигурацию сетевых настроек адаптера Вашего ПК (IP-адреса подсети, сетевой шлюз, DNS-сервер).

Важно! Если не запомнить данные текущего сетевого подключения, то после настройки камеры N630 придется 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 локальной проводной сети нажмите **Пуск – Панель управления** (Рис. 5.8).



Рис. 5.8

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

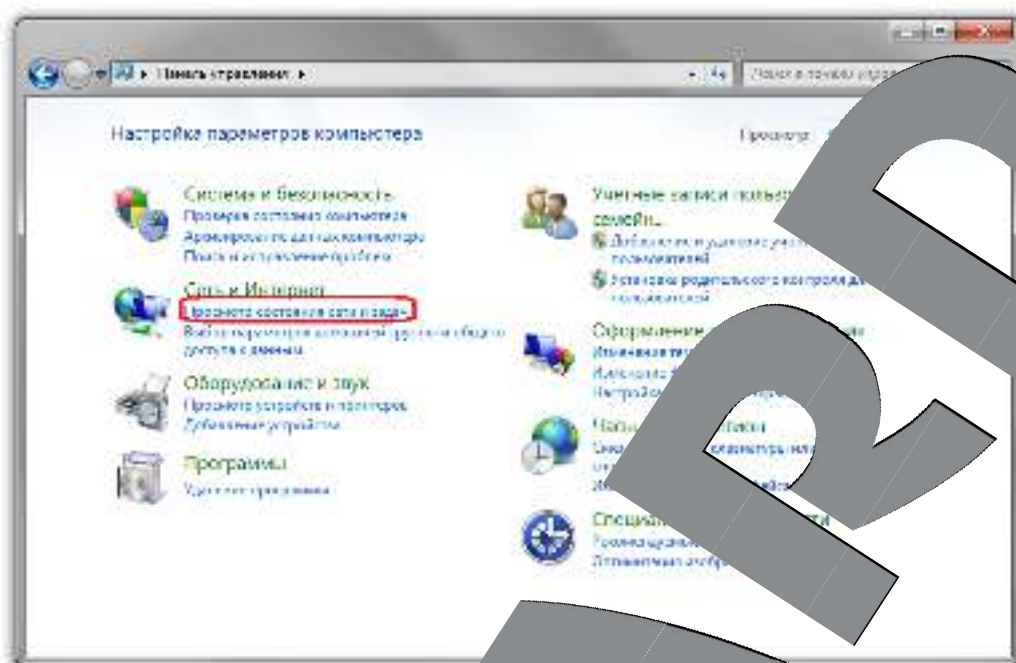


Рис.

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

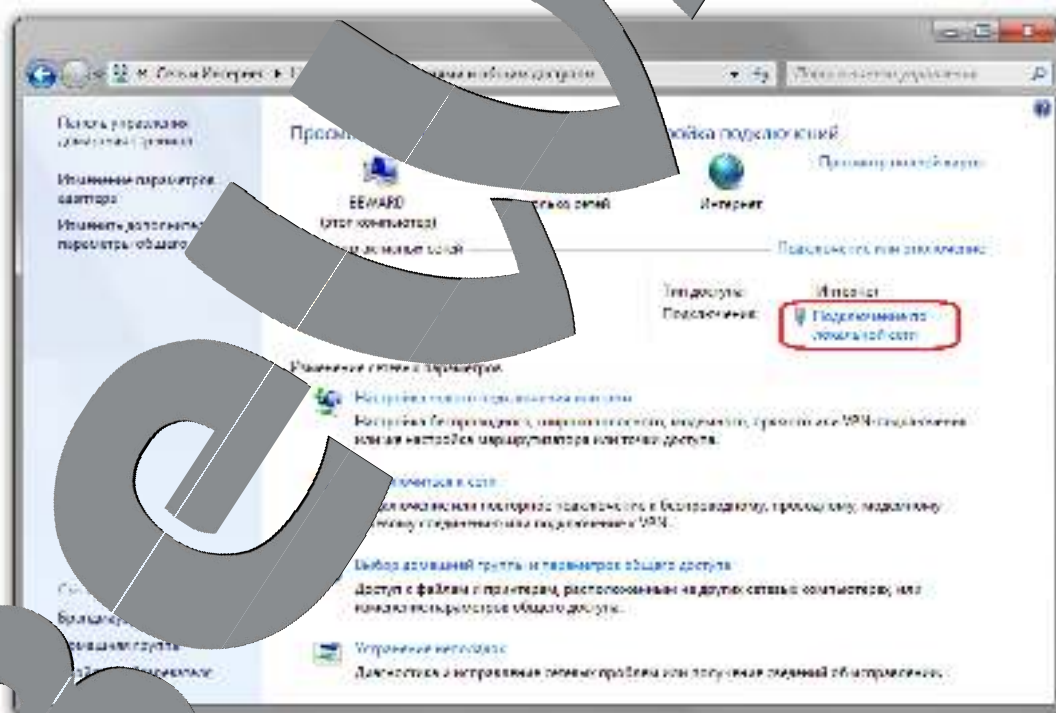


Рис. 5.10

ПРИ

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

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

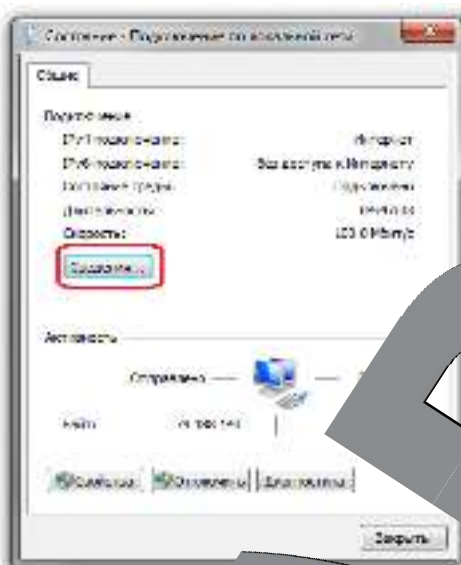


Рис. 5.11

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



Рис. 5.12

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 был назначен IP-адрес, значение которого указано в строке **[Адрес IPv4]**, маска подсети указана в строке **[Маска подсети IPv4]**, адрес сетевого шлюза – в строке **[Адрес шлюза IPv4]**, адрес DNS-сервера – в строке **[DNS-сервер]**. Запомните и 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 N630 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]** увидели следующие строки: **[DHCP включен]** – Да, **[IPv4-адрес автоматически]** – **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 Вашей ПК). Проверьте правильность подключения к проводной сети и в случае необходимости обратитесь к системному администратору Вашей сети.

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

По умолчанию IP-камера N630 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. Поэтому IP-адреса камер, компьютеров и любых сетевых устройств в сети не должны совпадать.

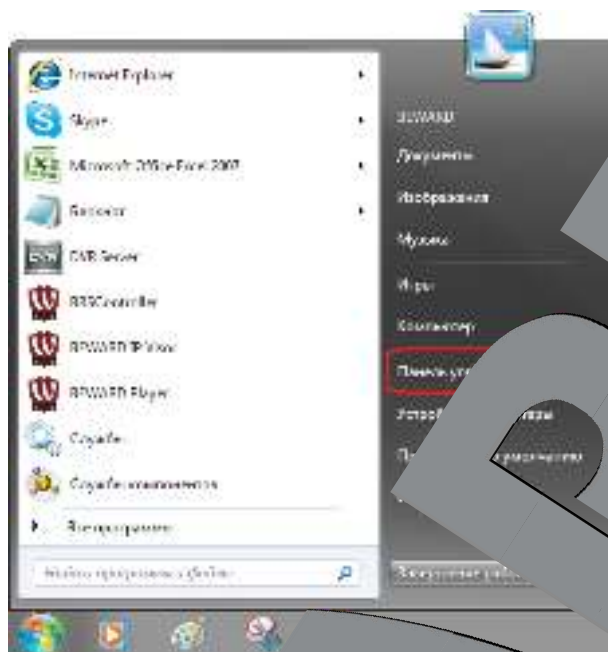
ВНИМАНИЕ!

IP-камеры BEWARD N630 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 камере, находится в одной подсети с IP-камерой, тогда Вы можете перейти к пункту [5.3](#) для настройки Ручного подключения.

Для изменения настроек компьютера в локальной проводной сети нажмите **Пуск** → **Панель задач** → **Сетевые ресурсы** (Рис. 5.13).



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

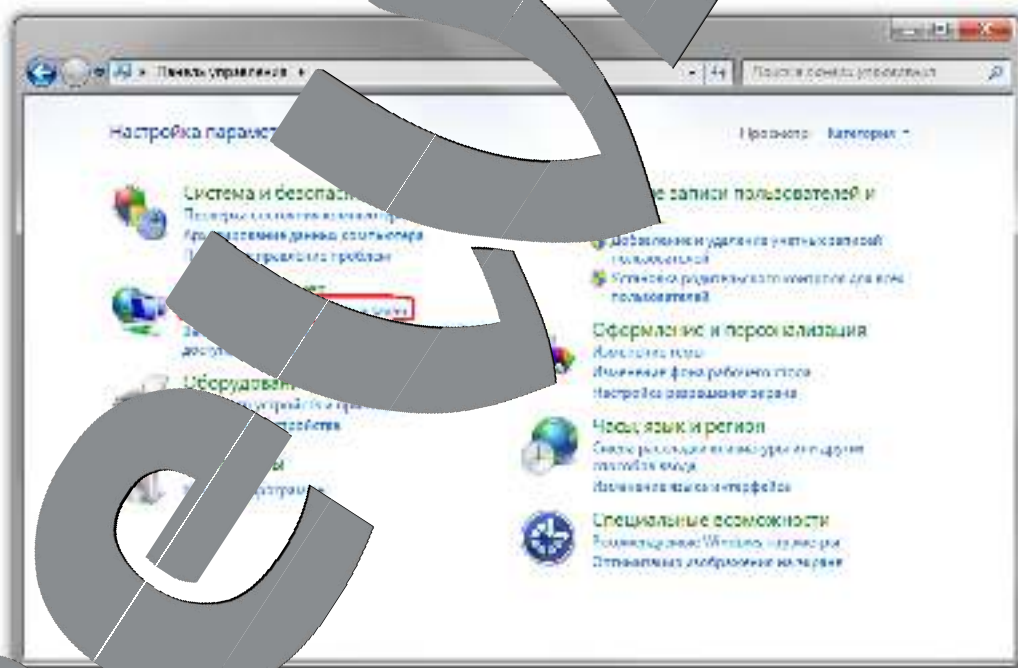


Рис. 5.14

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

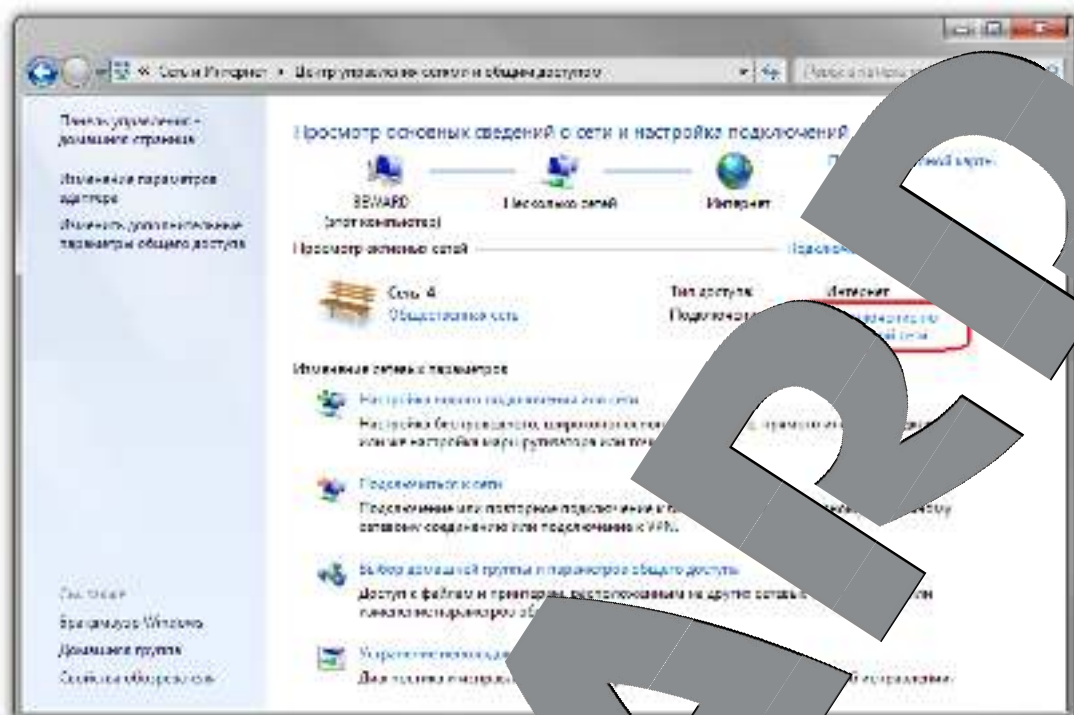


Рис. 5.

ПРИМЕЧАНИЕ!

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

В открывшемся окне нажмите **Свойства** (Рис. 5.16).

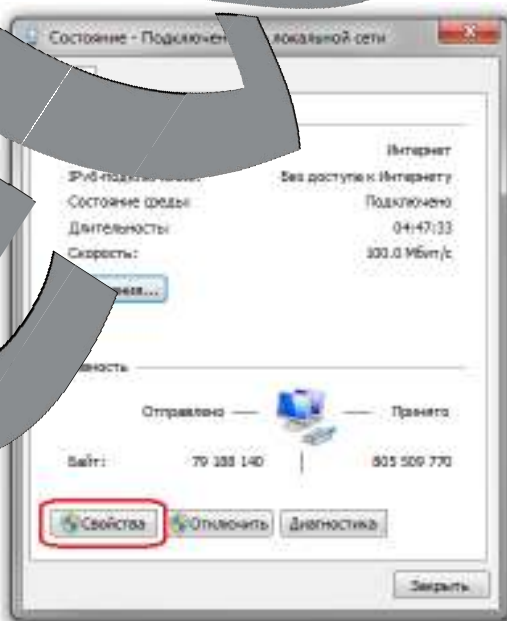


Рис. 5.16

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

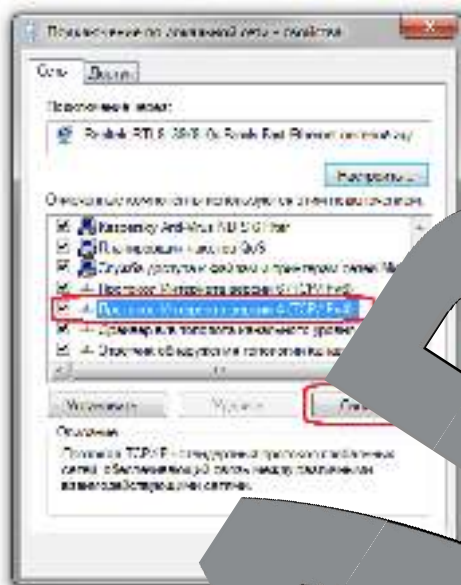


Рис. 5.17

Откроется меню, в котором необходимо указать значения IP-адреса и маски подсети. Выберите пункт **[Использовать следующий IP-адрес]** и введите свободный **[IP-адрес]** из подсети камеры, например 192.168.1.20, **[Маску подсети]** 255.255.255.0, остальные значения вводить не требуется (Рис. 5.18).

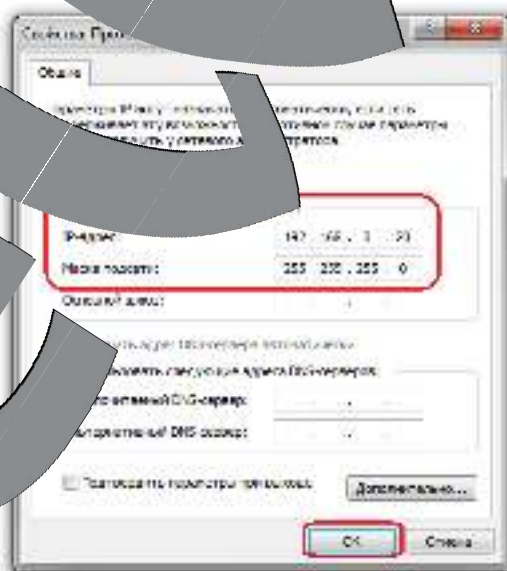


Рис. 5.18

После внесения изменений настроек нажмите кнопку **[ОК]** для всех открытых окон.

5.3. Получение доступа к IP-камерам

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 учесть, 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 автоматически появится меню установки (*Рис. 5.19*).

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

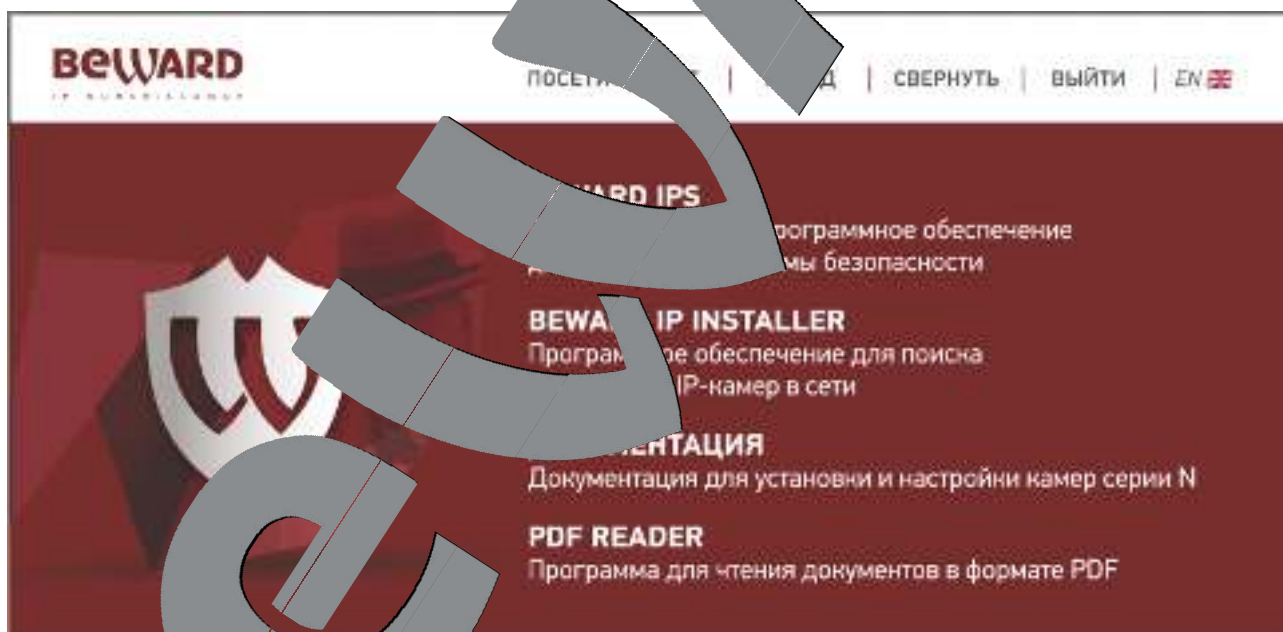


Рис. 5.19

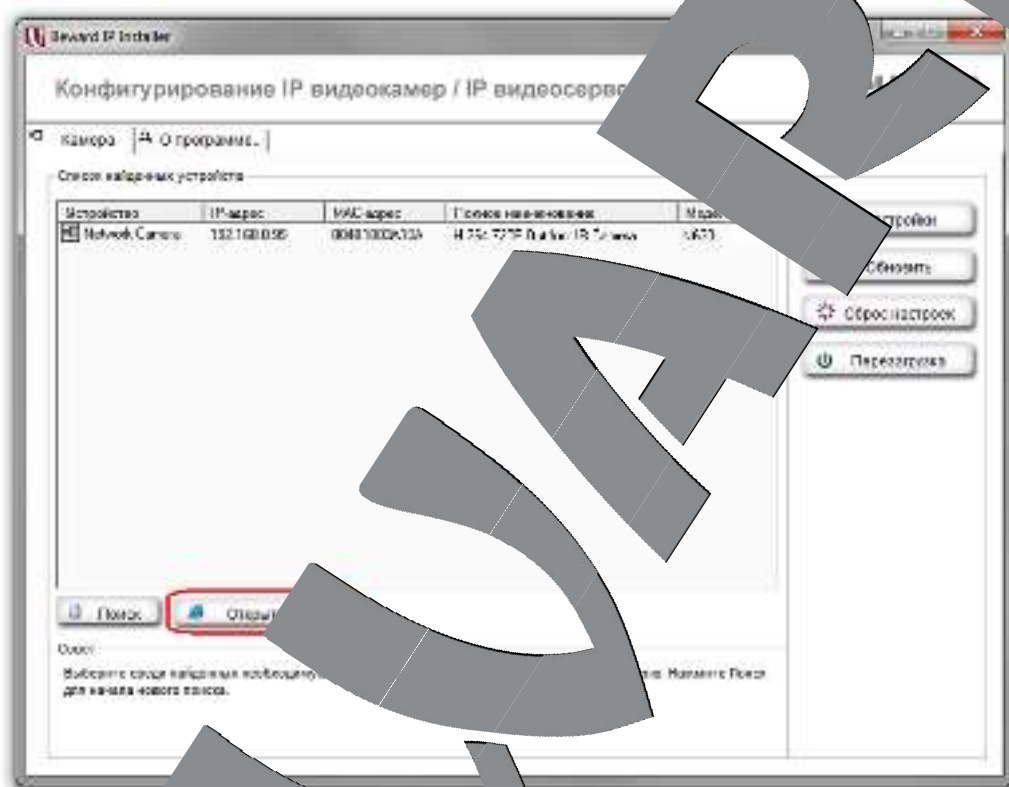
Получение доступа к IP-камерам с помощью ПО «BEWARD IP Installer»

Для получения доступа к IP-камере 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 N630 использование поддержки технологии UPnP включено по умолчанию.

Для поиска камеры с помощью ПО «**BEWARD IP Installer**» нажмите программу при помощи ярлыка на рабочем столе. В открывшемся окне появятся список всех найденных камер и видеосерверов. Выберите требуемую IP-камеру и нажмите кнопку **В** (Рис. 5.20).

**ВНИМАНИЕ!**

Для корректной работы **BEWARD IP Installer** необходимо добавить его в список доверенных приложений и его авторизовать в меню экрана.

ПРИМЕЧАНИЕ!

В Windows 7 для нормальной 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]**.

ВНИМАНИЕ!

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

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

ПРИМЕЧАНИЕ!

Для IP-камер BEWARD N630 использование поддержки технологии UPnP включено по умолчанию.

Для поиска камеры с помощью меню **[Сеть]** ОС Windows 7 выполните следующие действия: **[Панель задач] > [Мой компьютер]** и выберите пункт **[Сеть]** (Рис. 5.21).

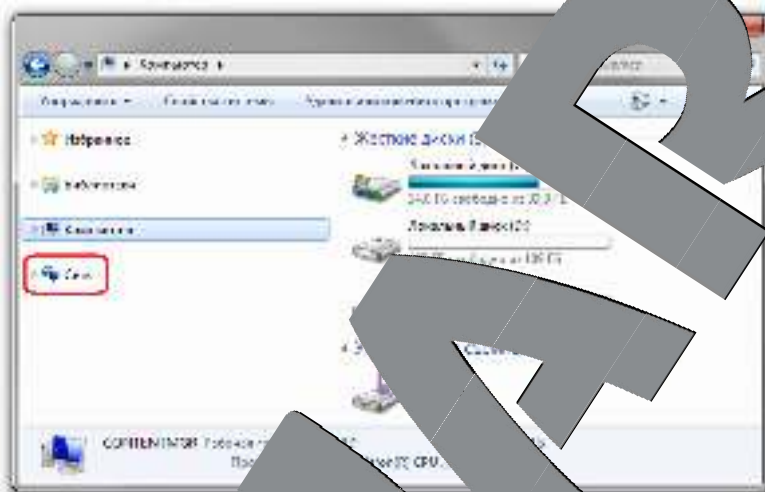


Рис. 5.21

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

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



Рис. 5.22

Если по умолчанию выбран браузер, отличный от Internet Explorer, то для того чтобы открыть камеру в Internet Explorer, перейдите в пункт [5.3.4](#).

5.3.4. Получение доступа к IP-камерам 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 **[F5]** (Рис. 5.23).

ВНИМАНИЕ!

IP-камера BEWARD N630 по умолчанию имеет сетевой адрес 192.168.1.99, `http – 80`.

ПРИМЕЧАНИЕ!

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



5.4. Получение доступа к веб-интерфейсу IP-камеры

После того как Вы получили доступ к камере любым из способов, рассмотренных в пунктах [5.3.2](#), [5.3.3](#) и [5.3.4](#) настоящего руководства, будет запущен браузер Internet Explorer, где откроется окно для получения доступа к веб-интерфейсу устройства.

ПРИМЕЧАНИЕ!

Для корректного доступа к веб-интерфейсу 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**.

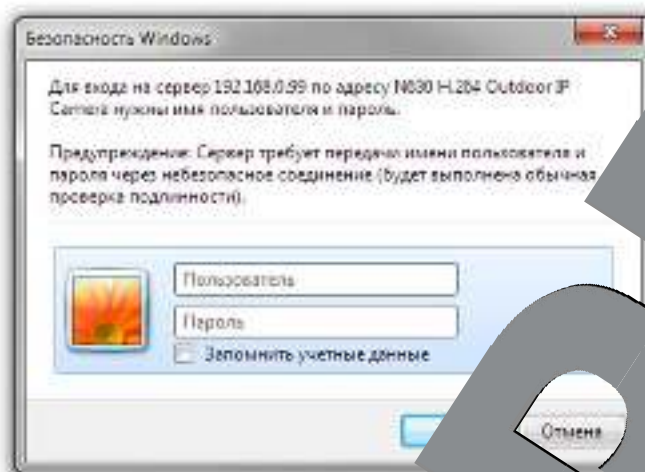


Рис. 5.24

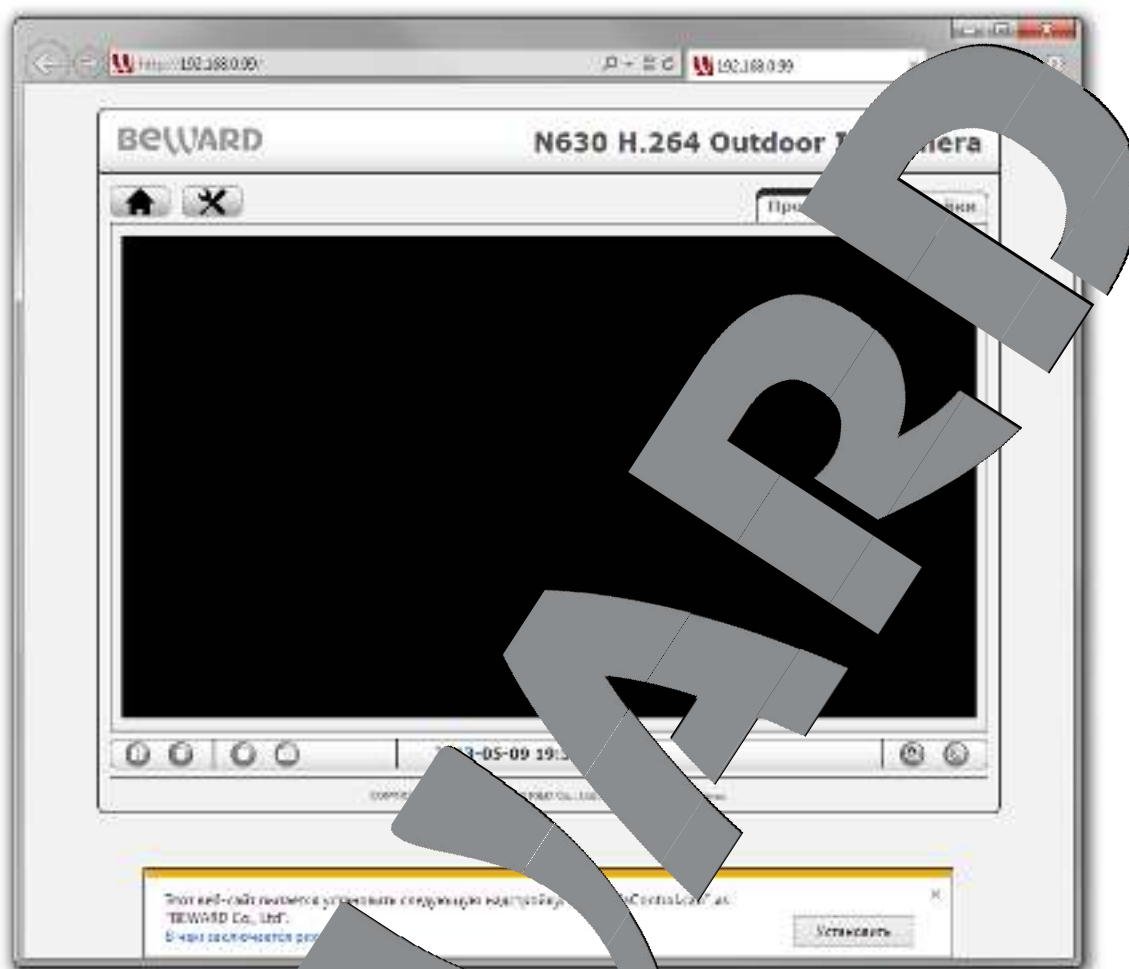
После удачной авторизации при подключении к Windows 7 будет блокировать установку приложения ActiveX (о просмотре изображения с камеры), о чем будет свидетельствовать сообщение в нижней части окна Internet Explorer: **«Этот веб-сайт пытается установить следующую надстройку: «AxMediaControl.cab» от «BEWARD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

ВНИМАНИЕ!

Установка компонентов ActiveX возможна только в браузере Internet Explorer.

ПРИМЕЧАНИЕ!

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



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



Рис. 5.26

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

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



Рис. 5.27

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

После подключения IP-камеры N630 по проводной сети необходимо изменить настройки камеры так, чтобы она находилась в одной подсети с остальным оборудованием (например, Ваш ПК).

ВНИМАНИЕ

Для работы камеры с Вашим ПК необходимо, чтобы совпадали три части IP-адреса, за исключением последней. Необходимо, чтобы полностью совпадала маска подсети.

Например, IP-адрес 192.168.50.40. IP-адрес разделен точками на четыре октета. В данном примере: 192 – 1 октет, 168 – 2 октет – 168, 3 октет – 50, 4 октет – 40. Вам необходимо изменить

IP-адрес, чтобы у него первые три октета совпадали, то есть чтобы было значение вида 192.168.50.X, где X – любой октет обязательно должен быть отличным от значения на Вашем ПК, а также отличным от IP-адреса любого другого оборудования Вашей сети (если такое имеется).

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

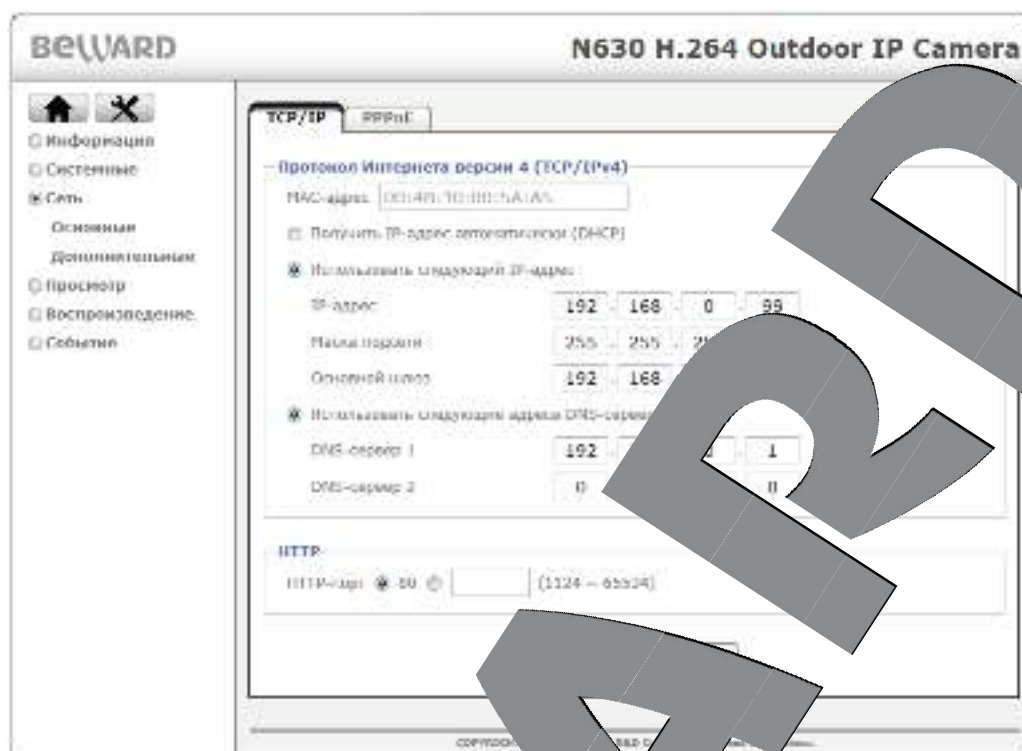


Рис. 5.28

Во вкладке **[TCP/IP]** нужно ввести значение IP-адреса и других сетевых параметров для IP-камеры, чтобы она находилась в одной подсети с остальным оборудованием (Рис. 5.28).

ПРИМЕЧАНИЕ!

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

Для сохранения изменений сетевых настроек проводного соединения нажмите кнопку **[Сохранить]**. В появившихся окнах необходимо нажать кнопку **[ОК]**.

На этом настройка проводного соединения для IP-камеры завершена.

5.6. Возврат настроек подключения ПК в первоначальные значения

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

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

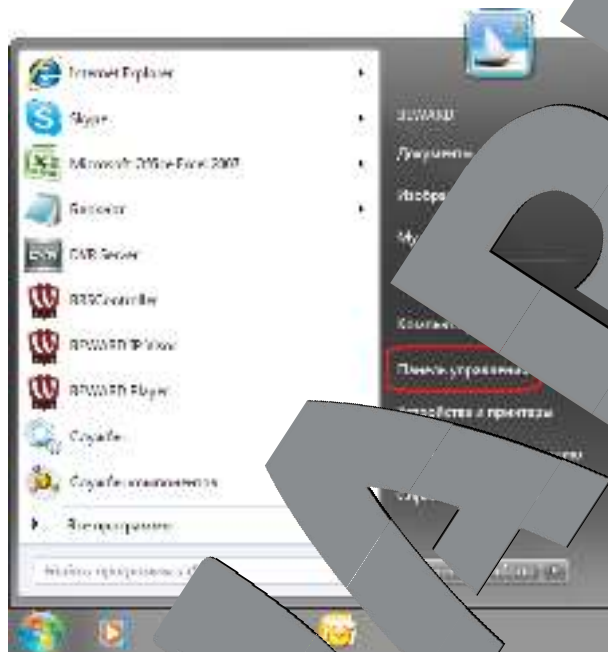


Рис. 5.29

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

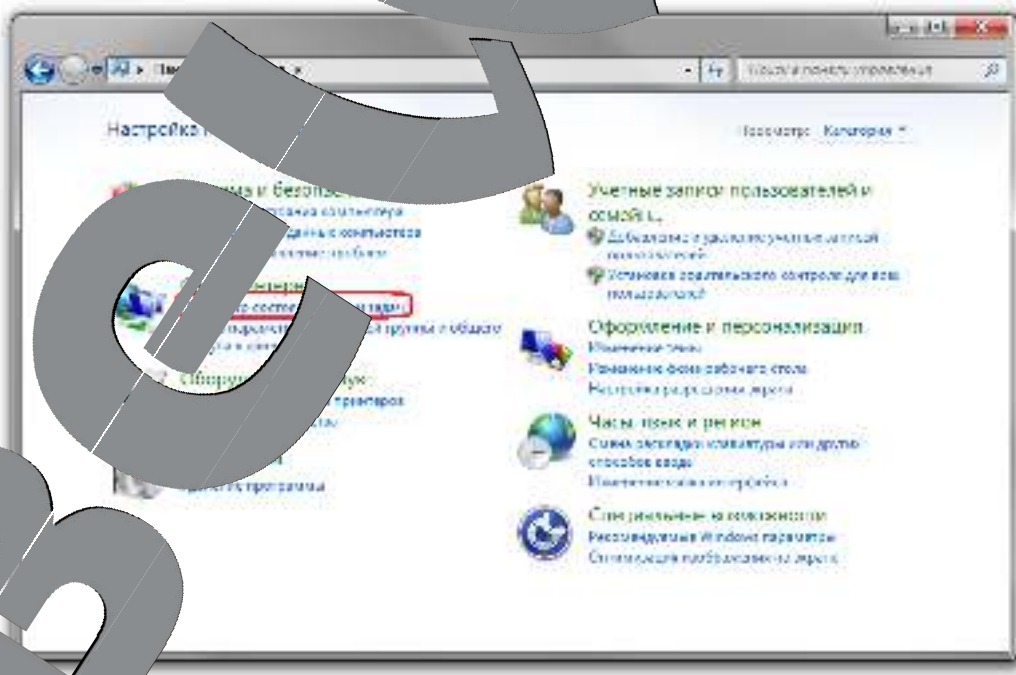


Рис. 5.30

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

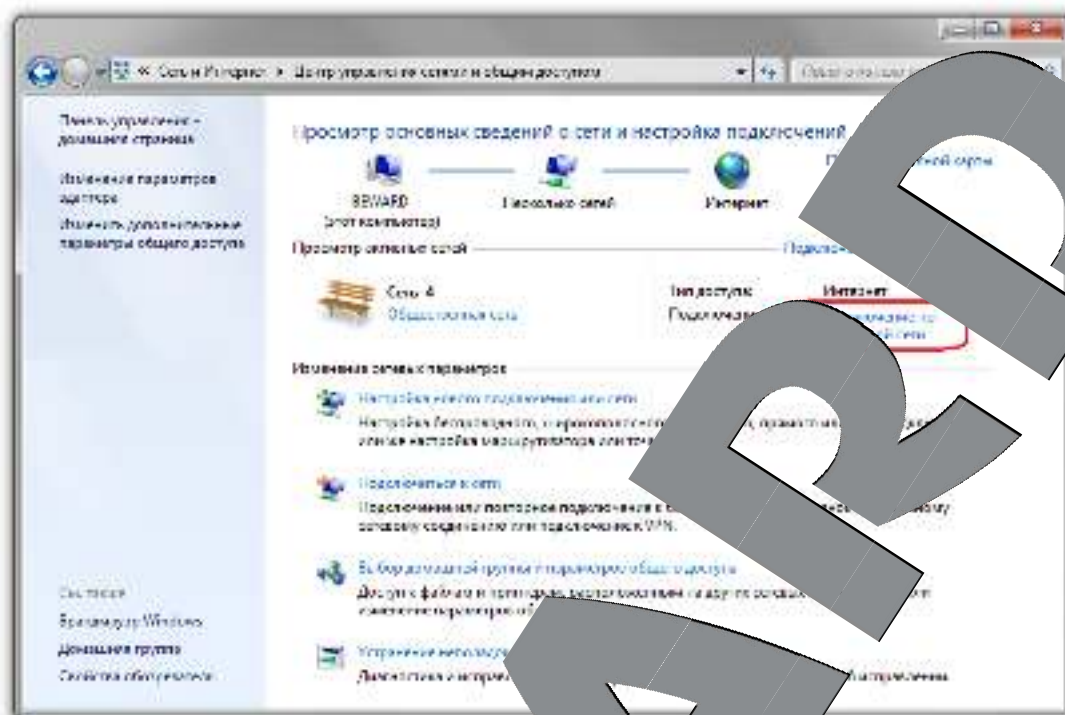


Рис. 5.31

В открывшемся окне нажмите кнопку **Изменить сетевые параметры** (Рис. 5.32).

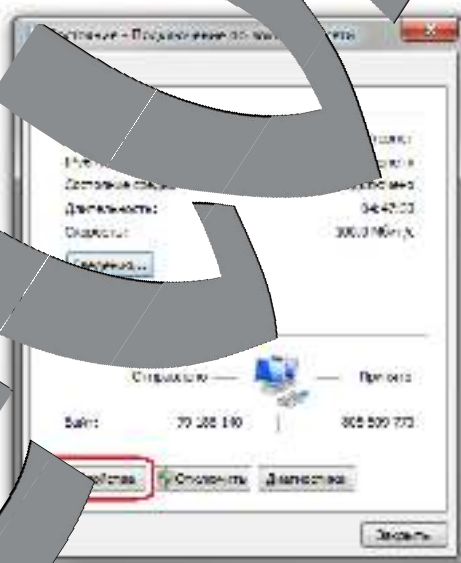


Рис. 5.32

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

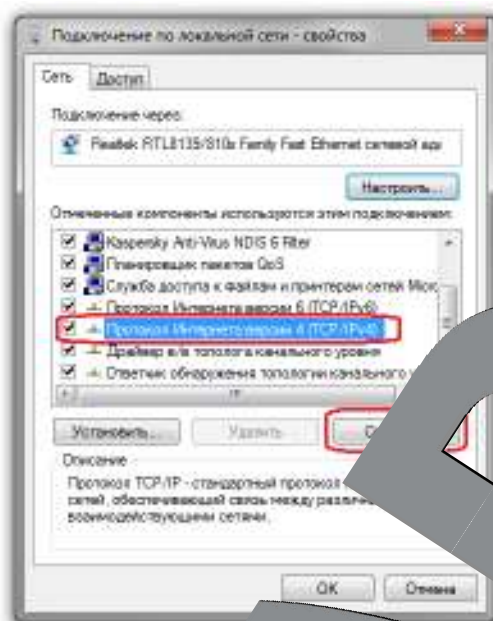


Рис. 5.33

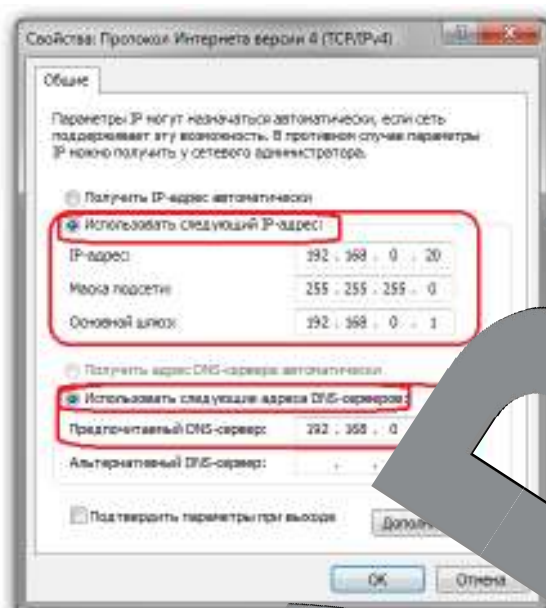
Откроется меню, в котором необходимо задать значения сетевых настроек, установленных изначально (см. пункт [5.1.1](#) данного Руководства).

Если изначально IP-адрес Вашему ПК назначен автоматически, тогда выберите пункты **[Получить IP-адрес автоматически]** и **[Получить адрес DNS-сервера автоматически]**, после чего нажмите кнопку **[ОК]** для всех открытых окон (Рис. 5.34).



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



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

Для контроля правильности настройки подключения 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).

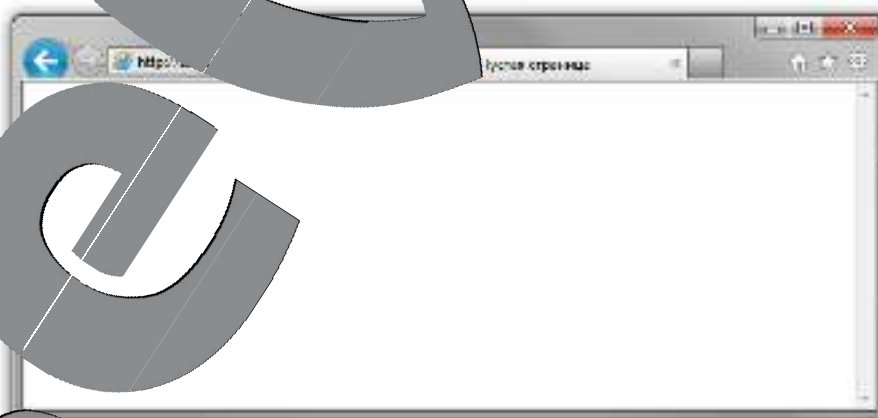
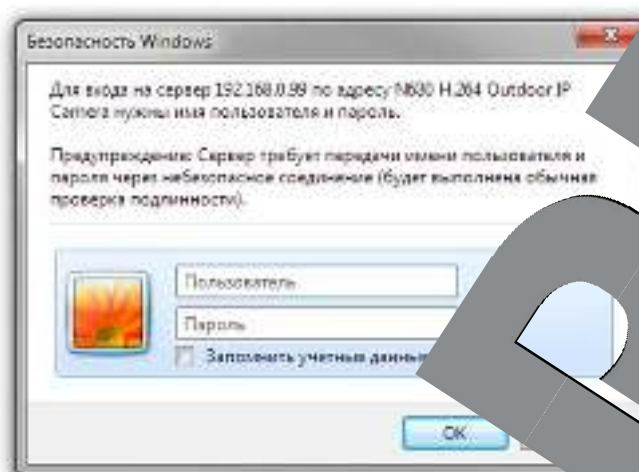


Рис. 5.36

В появившемся меню настроек откроется меню авторизации. Для авторизации введите имя пользователя и пароль, после чего нажмите **[ОК]** (Рис. 5.37).

ВНИМАНИЕ!

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



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

В случае неудачного соединения с камерой проверьте правильность подключения к проводной сети. В начале данной главы и повторите настройку. В случае необходимости обратитесь к системному администратору Вашей сети.

Глава 6. Подключение IP-камеры к сети Интернет

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

При установке IP-камеры N630 в квартире, коттедже или офисе требуется, чтобы у нее имелся доступ не только из локальной сети того или иного помещения, но и к сети Интернет.

В этом случае для одновременной работы компьютеров, ноутбуков, IP-камер и другого оборудования в сети Интернет, чаще всего, используется маршрутизатор.

При организации доступа к IP-видеокамерам к 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 домашней 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 статический IP-адрес. IP-адрес назначается провайдером динамически, и при каждом новом подключении этот адрес присваивается заново и изменяется в процессе работы (такая ситуация особенно характерна для работы через ADSL и GPRS). В этом случае, чтобы обеспечить возможность доступа одной или нескольких камер к сети Интернет, независимо от того, какой IP-адрес выделен провайдером в данный момент, необходимо задействовать интернет-службы, работающие с динамическими IP-адресами.

Далее в вариантах организации доступа к IP-камерам из сети Интернет будут рассмотрены.

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

6.2.1. Использование статического IP-адреса

Для подключения IP-камеры к сети Интернет необходимо изменить ее сетевые параметры в соответствии с данными, полученными от провайдера. 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 к статическому IP-адресу необходимо выполнить следующие шаги:

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

Шаг 2: измените сетевые настройки проводного сетевого интерфейса IP-камеры (см. пункт 5.5 данного Руководства) в соответствии с настройками, предоставленными Вашим Интернет-провайдером (Рис. 6.1).

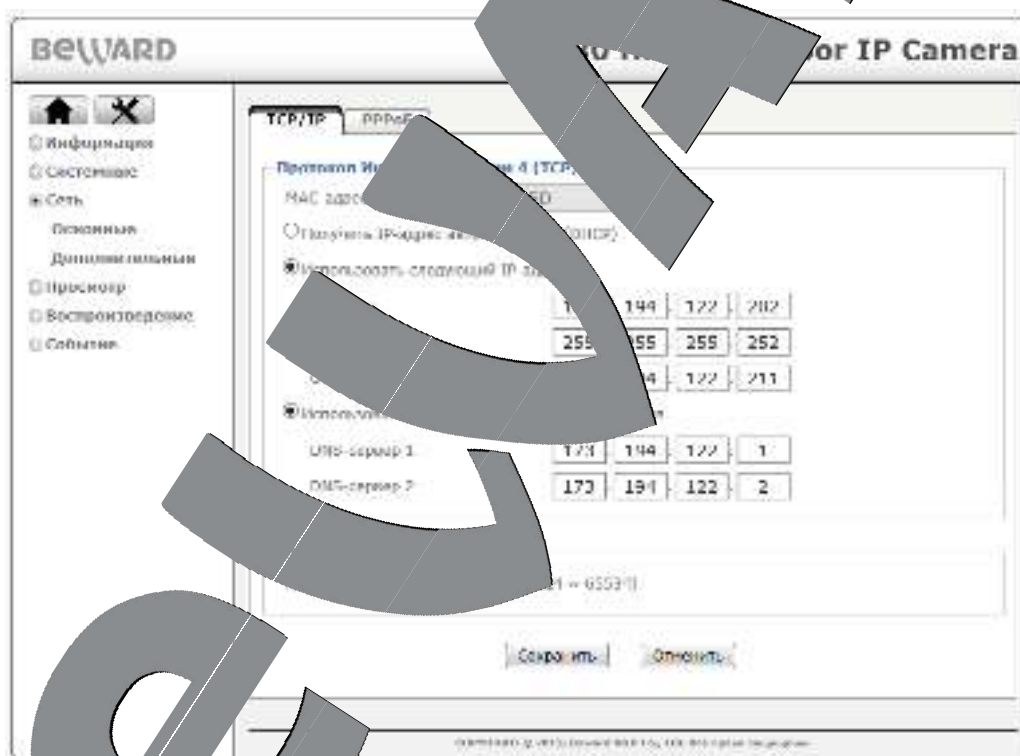


Рис. 6.1

Шаг 3: подключите камеру к выделенной сети Ethernet.

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

В данном примере провайдер предоставил следующие данные:

- IP-адрес: 173.194.122.202
- Маска подсети: 255.255.255.252
- Сетевой 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 HTTP-порт, заданное по умолчанию («80»), то, чтобы обратиться к камере через сеть Интернет, необходимо набрать запрос «http://173.194.122.202».

ПРИМЕЧАНИЕ!

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

6.2.2. 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 **имя пользователя и пароль**.

IP-камера N630 поддерживает PPPoE. Для использования необходимо выполнить следующие шаги:

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

Шаг 2: войдите в меню PPPoE через меню IP-камеры: **НАСТРОЙКИ**  – **Сеть** – **Основные** – **PPPoE**.

Шаг 3: в текстовых полях **[Пользователь]** и **[Пароль]** введите значения, полученные от Интернет-провайдера (Рис. 6.2).



Рис. 6.2

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 Интернете по IP-адресу, присвоенным ей Вашим провайдером и отображаемым в поле «IP-адрес» (рис. 6.2).

ПРИМЕЧАНИЕ!

Для удобства, IP-адрес камеры, под которым она доступна в Интернете, 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 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 равно «80»).

ПРИМЕЧАНИЕ!

При подключении к камере по умолчанию задан порт, заданный по умолчанию (значение равно «80»), запрос в адресной строке браузера должен быть **http://<IP>**, где **<IP>** – IP-адрес камеры.

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

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

ВНИМАНИЕ!

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

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

ВНИМАНИЕ!

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

Для этого требуется выполнить следующие действия:

- Изменить сетевые параметры маршрутизатора 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 внутренний LAN-интерфейс и обеспечивается практически любым современным маршрутизатором.

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

- Использование технологии UPnP на маршрутизаторе и камере.

- Ручная установка параметров перенаправления портов на маршрутизаторе и камере.

6.3.1. Использование для подключения опции UPnP

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

Для организации доступа к IP-камере из сети Интернет остается сделать следующее:

- Разрешить использование и настроить функцию UPnP своего маршрутизатора.

ПРИМЕЧАНИЕ!

Настройка функции UPnP маршрутизатора должна быть описана в прилагаемой инструкции.

ВНИМАНИЕ!

Не все модели маршрутизаторов поддерживают функцию UPnP для переназначения портов LAN- и WAN-интерфейсов. Если Ваш маршрутизатор не поддерживает данную функцию, то он требует дополнительной настройки (см. пункт [6.3.2](#)).

- Разрешить использование и настроить функцию UPnP IP-камеры.

Чтобы настроить функцию UPnP камеры, необходимо выполнить следующие действия:

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

Шаг 2: установите галочку напротив строки **[Разрешить переадресацию портов]**

(Рис. 6.3).

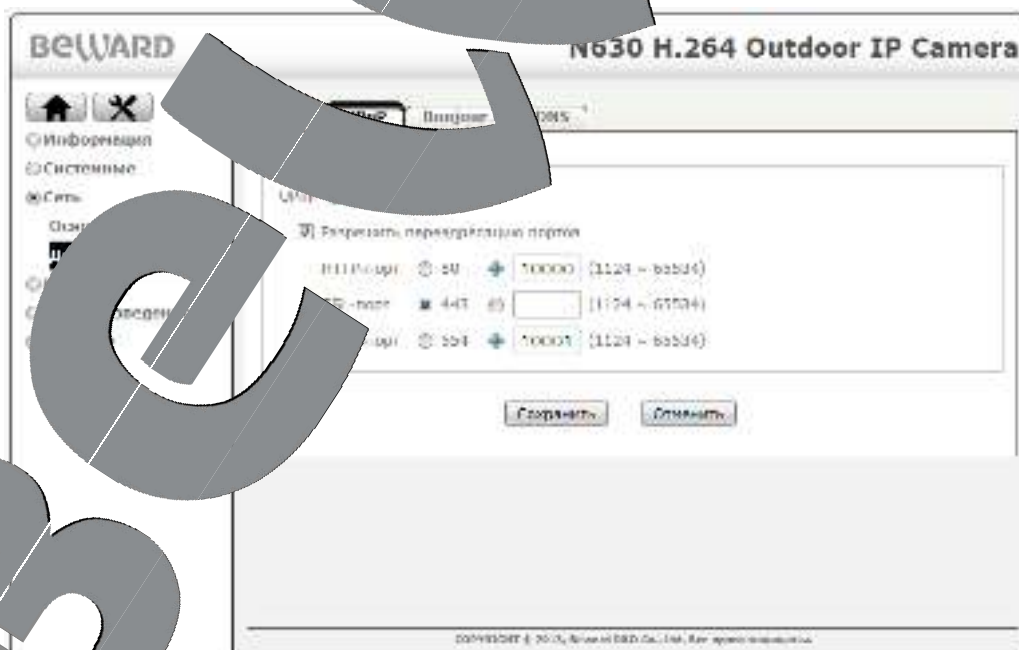


Рис. 6.3

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 данной камеры при доступе к ней из сети Интернет.

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

ВНИМАНИЕ!

Для применения сетевых параметров требуется перезагрузить устройство.

ВНИМАНИЕ!

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

Теперь, чтобы получить доступ к камере из сети Интернет, надо обратиться к ней по IP-адресу, выданному провайдером («внешний» порт 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 и несколько камер, надо лишь для каждой из них задать свои, уникальные значения портов.

6.3.2. Настройка ручного перенаправления портов маршрутизатора.

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

Рассмотрим процесс подключения IP-камеры к сети Интернет с помощью маршрутизатора TP-Link TL-WR543ND (настройка большинства функций маршрутизаторов различных моделей осуществляется схожим образом).

Начиная с того момента, как мы подключаем маршрутизатор к локальной сети и сети Интернет уже не будем возвращаться к настройкам. 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 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 на «реальный порт»! Соответственно, для всех камер необходимо задать различные значения RTSP-портов.

Шаг 1: откройте раздел меню **Настройка сети – 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. 6.4).

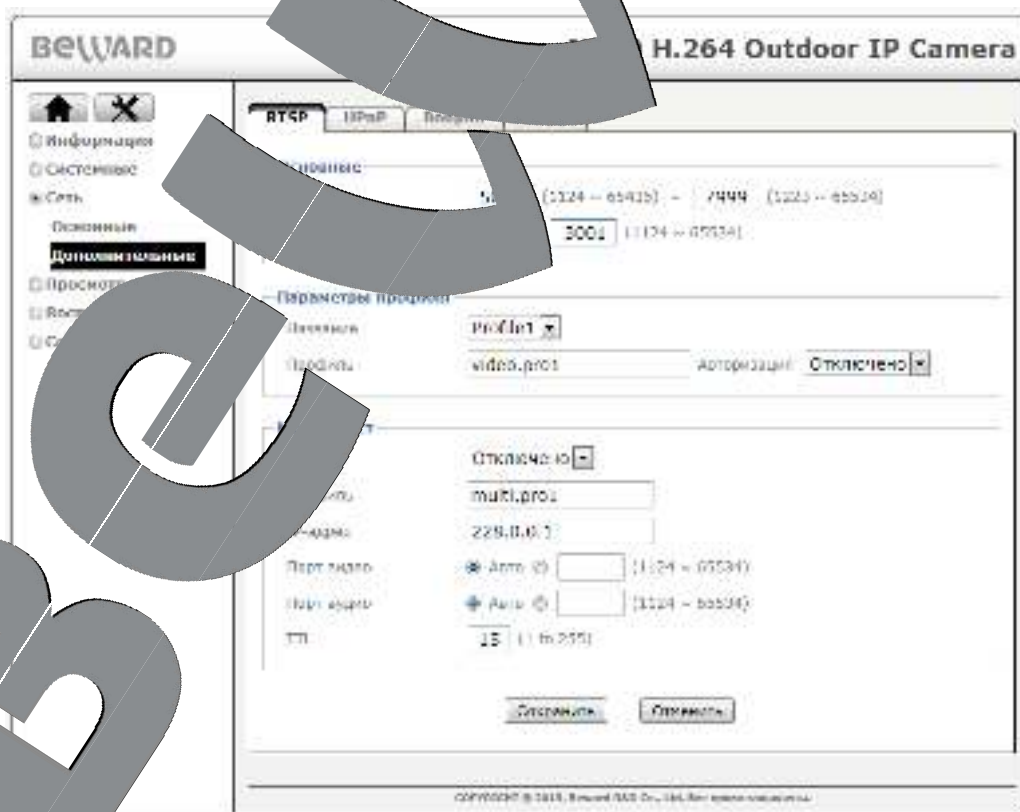


Рис. 6.4

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. 6.5).



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

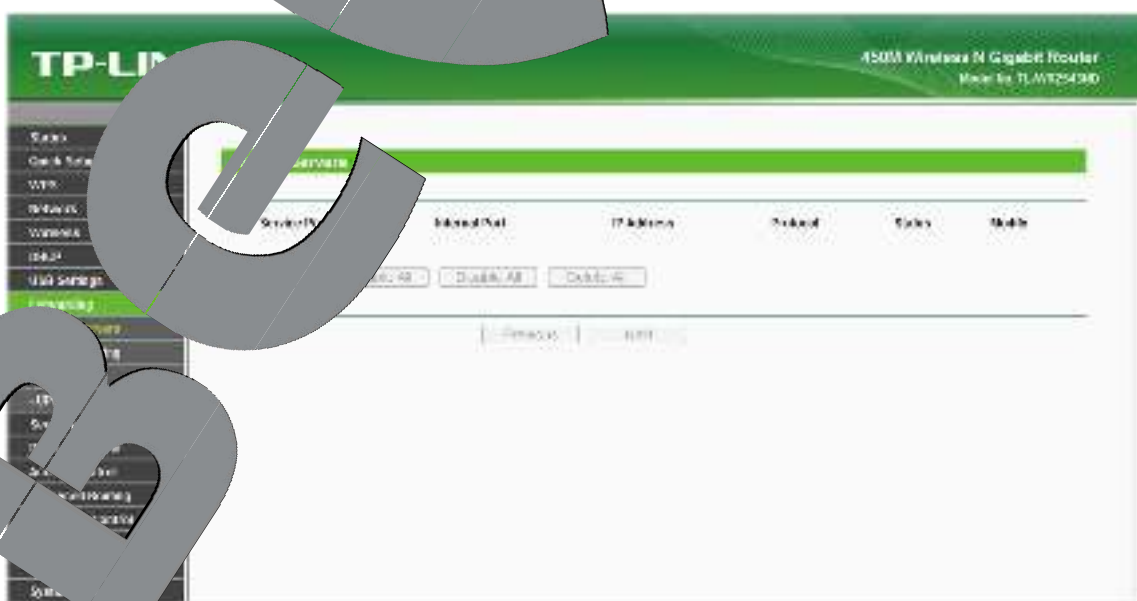


Рис. 6.6

Шаг 3: добавьте правила перенаправления портов для IP-камеры (Рис. 6.7). 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 зарезервированные значения. Рекомендуется использование портов диапазона 1024-65535. Значения портов от 0 до 1123 официально зарегистрированы под различные протоколы (службы, приложения.)

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

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

Остальные пункты не требуют настройки.

Добавьте правило для порта HTTP (Рис. 6.7).

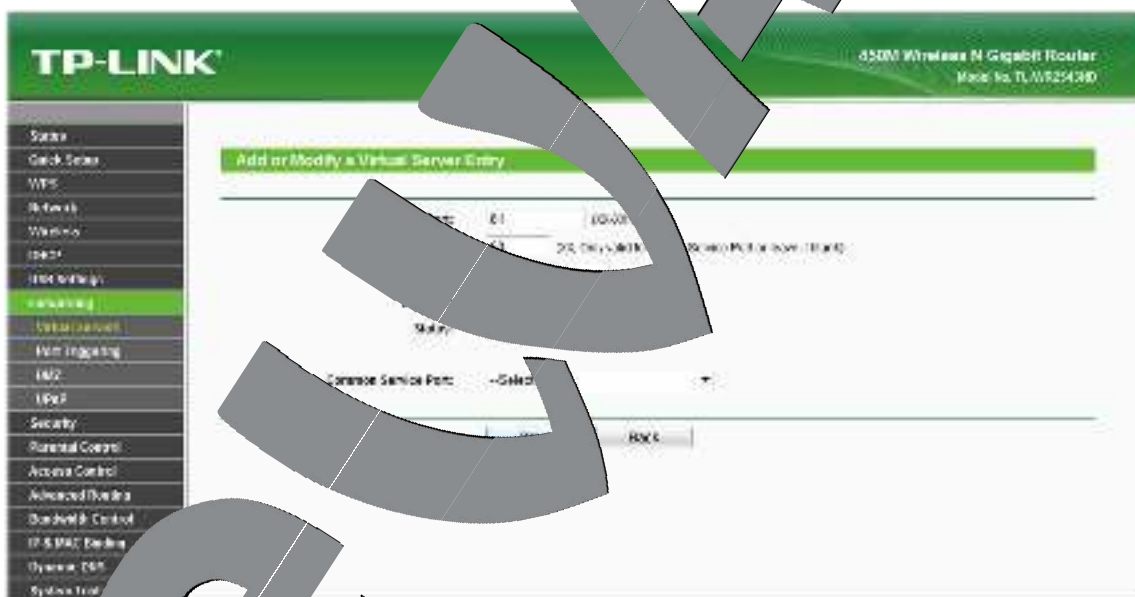


Рис. 6.7

Шаг 4: нажмите кнопку **[Save]**, чтобы сохранить правило. Правило добавлено (Рис. 6.8):



Шаг 5: тем же способом добавьте правило для порта 80 (Рис. 6.9):

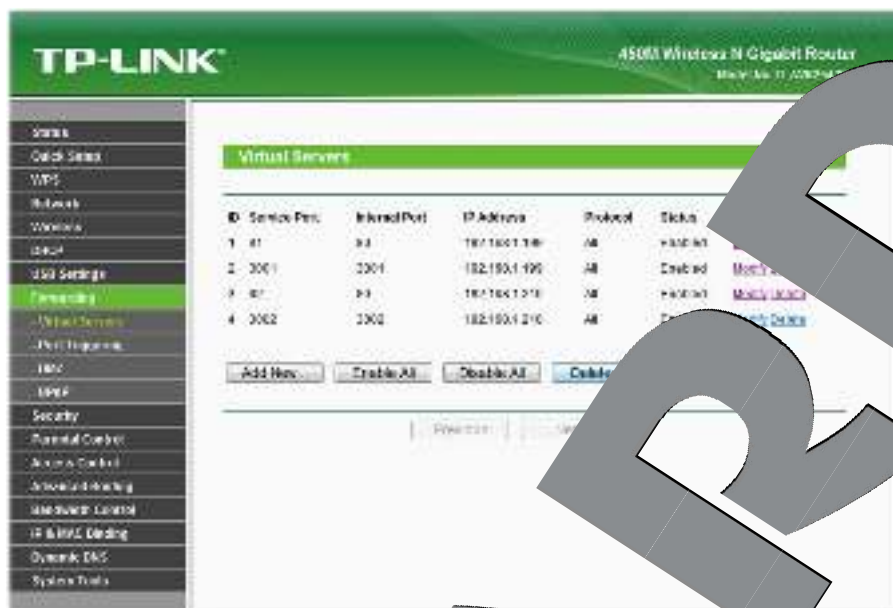
ВНИМАНИЕ!

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. 6.9

Если Вы используете несколько камер, то Вам необходимо повторить **шаги 2-5** для остальных камер (Рис.6.10).



Настройка маршрутизатора завершена.

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

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

6.4. Пример подключения через сеть Интернет с использованием DDNS

6.4.1. Общие сведения о подключении через Интернет с использованием DDNS

В случае если IP-адрес выдается компьютеру на определенное время (всего лишь на один сеанс связи), такой адрес называют динамическим. Большинство Интернет-провайдеры предоставляют пользователям динамический IP-адреса. Однако для того, чтобы можно было обратиться к оборудованию из сети Интернет, оно должно иметь постоянный или фиксированный адрес. С этой целью создается служба Dynamic DNS (DDNS).

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

В этом случае вместо того, чтобы обратиться к оборудованию по IP-адресу, Вы обращаетесь к нему по доменному имени вида camera184.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 будете 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 сервера DDNS для того, чтобы сообщить значение текущего IP-адреса. DDNS-провайдер в соответствии этому IP-адресу зарегистрированное Вами ранее доменное имя.

Рассмотрим процесс работы с DDNS-провайдером <http://www.dyndns.com>, методика регистрации и работы с DDNS аналогична данной. Для доступа к сетевому ресурсу с использованием доменного имени выполните следующие действия:

- Завести учетную запись (Account) на сайте www.dyndns.com для дальнейшей регистрации на сервере.
- Создать 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](http://camera184.dyndns.org). Соответственно получите домен третьего уровня для своего оборудования www.camera184.dyndns.org.
- Настроить соответствующим образом оборудование.

6.4.2. 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 Account]** (Рис. 6.11).



Рис. 6.11

Далее Вы автоматически попадете на страницу создания учетной записи (Рис. 6.12).

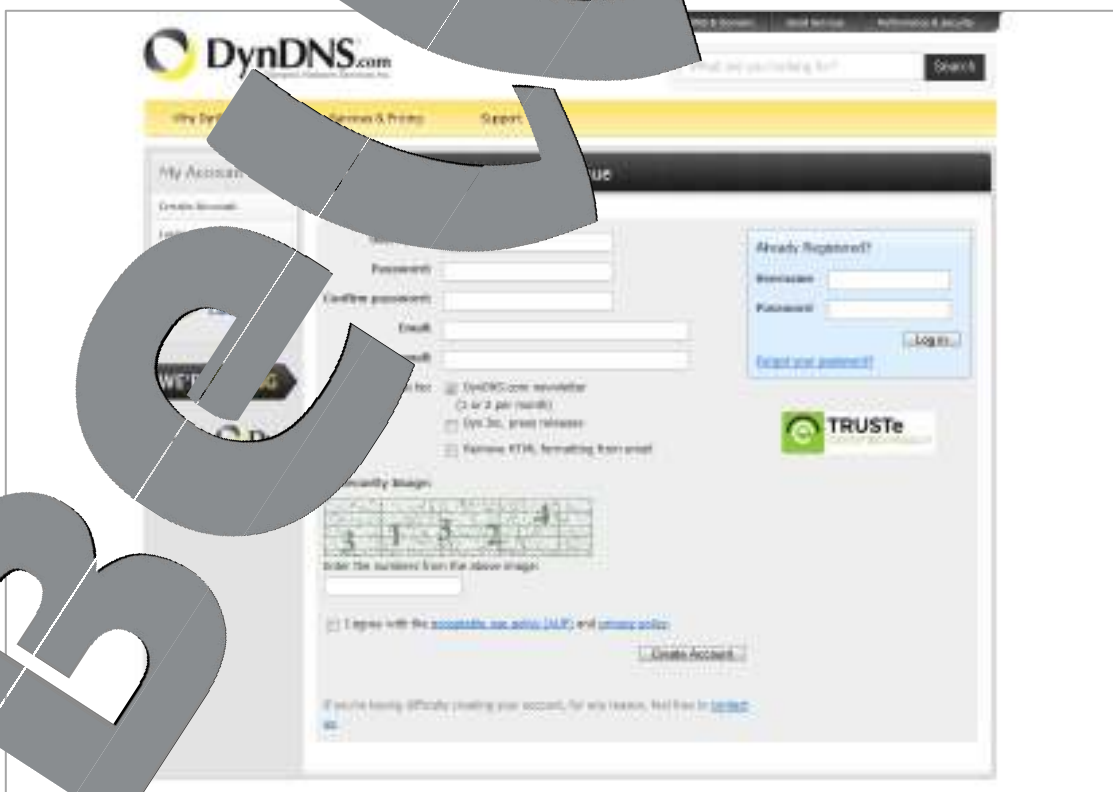


Рис. 6.12

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 выслан письмо со ссылкой на сайт, причем на один электронный адрес может быть зарегистрировано только одно 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 Beward в случае сбоев в обслуживании сервиса или каких-либо нововведений. Для отказа от новостной рассылки не выделяйте этот пункт.

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 на получение одного бесплатного аккаунта.

В качестве имени пользователя **[Username]** – camera184, адрес электронной почты **[Email]** – camera184@yandex.ru, вводим произвольный пароль (например, 123456).

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

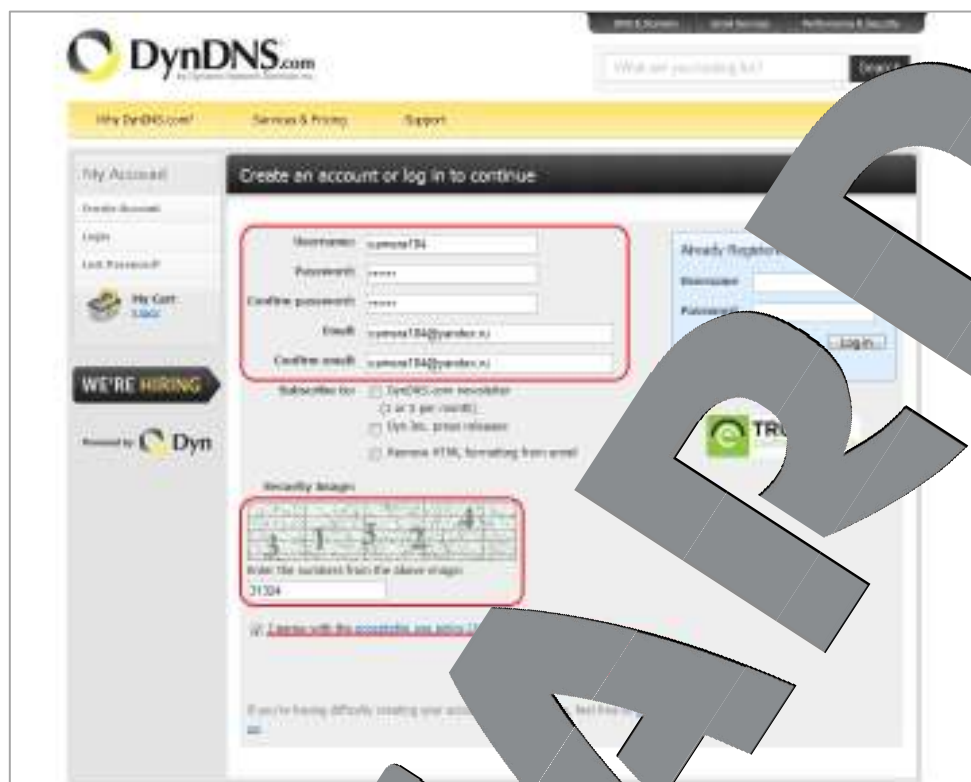


Рис. 6.13

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. 6.14).



Рис. 6.14

Шаг 4: в течение нескольких 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]**.

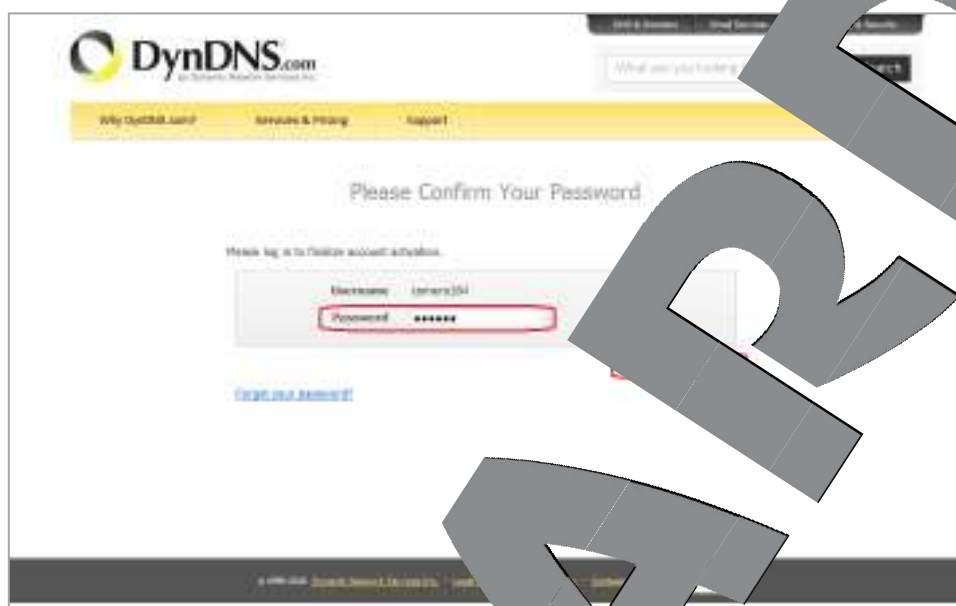


Рис. 6.15

Шаг 5: создание учетной записи для сервиса DynDNS завершено (Рис. 6.16).

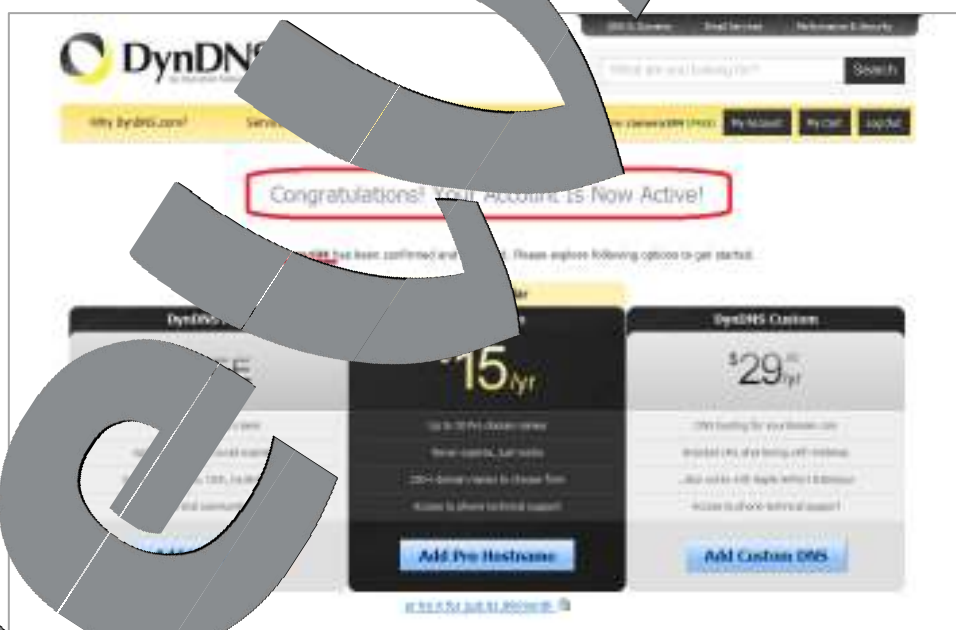


Рис. 6.16

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. 6.17).



Рис. 6.17

Шаг 2: если все данные указаны правильно, вы попадете на персональную страницу настроек. Для продолжения настройки нажмите пункт **[Host Services]** (Рис. 6.18).

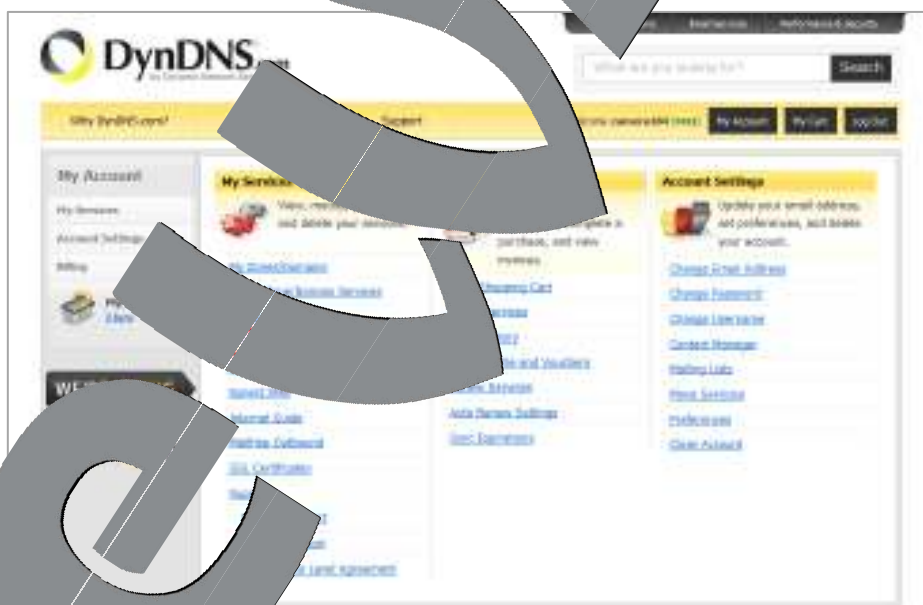
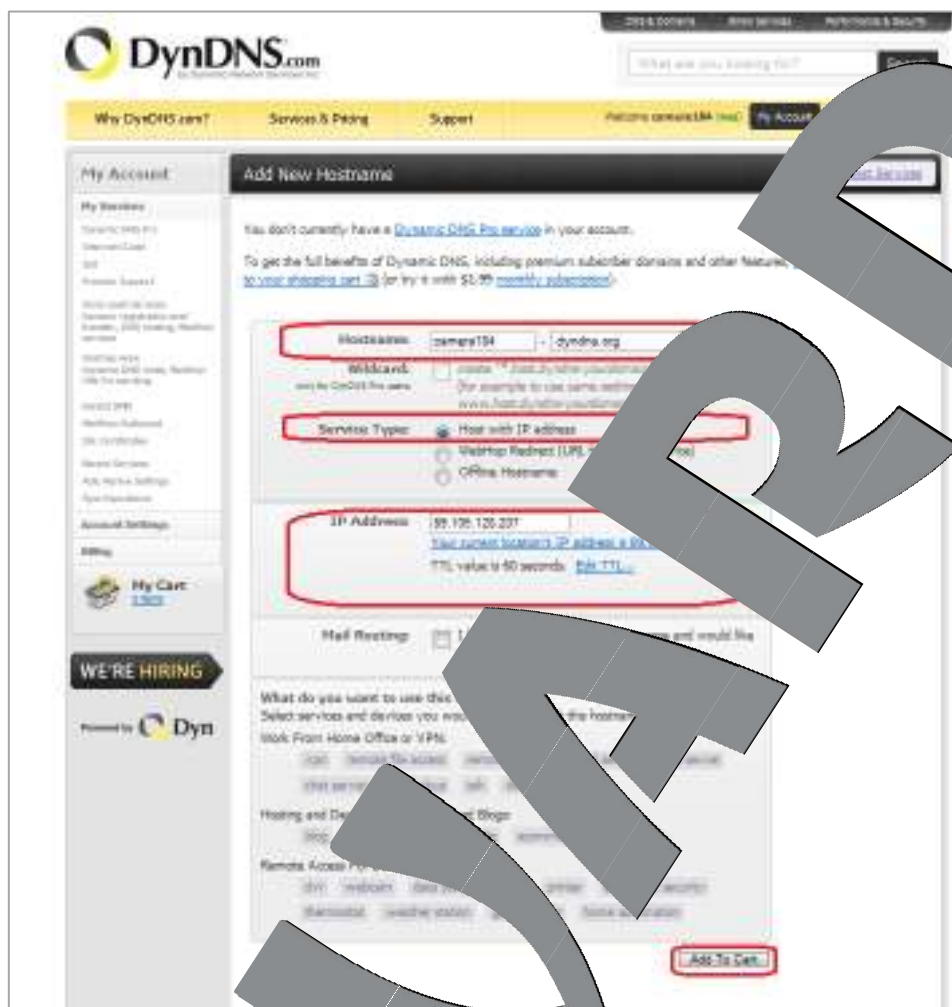


Рис. 6.18

На открывшейся странице необходимо настроить параметры соединения с сервером. В поле **[Host Services]** укажите желаемый домен. Например, dyndns.org.

Далее в поле **[Hostname]** укажите доменное имя, для данного примера это – camera184.dyndns.org. Если данное имя для выбранного домена свободно, то для выше указанного примера можно использовать любое другое доменное имя - camera184.dyndns.org (Рис. 6.19).



Для сопоставления текущего динамического IP-адреса камеры с доменным именем необходимо указать IP-адрес, который мы настраиваем для работы через DDNS. По умолчанию сервис использует IP-адрес, с которого на данный момент времени происходит соединение (Рис. 6.20).



Рис. 6.20

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

После успешного создания доменного имени откроется страница с подтверждением этого. Так для примера, описанного выше, будет указан созданный аккаунт camera184.dyns.org. Для активации доменного имени нажмите кнопку **[Next]** (Рис. 6.21).

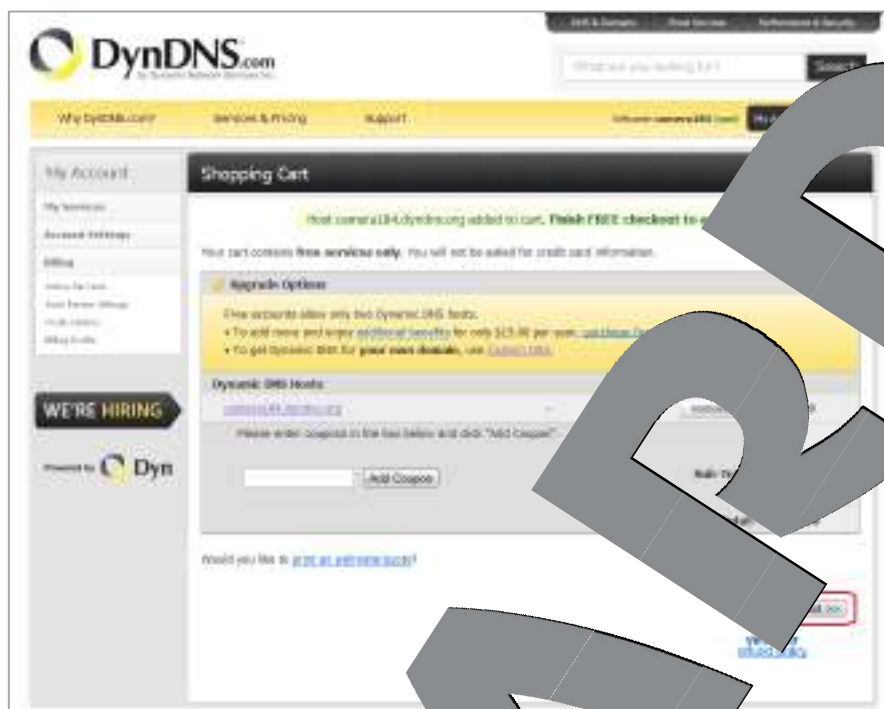


Рис.

На открывшейся странице аккаунта нажать кнопку **[Activate Service]** (Рис. 6.22).



Рис. 6.22

5: После успешной активации доменного имени откроется страница, подтверждающая это (Рис. 6.23).



Рис. 6.23

Шаг 6: создание доменного имени на сервисе DynDNS завершено.

6.4.4. Настройка оборудования для работы с сервисом DynDNS

Теперь требуется настроить оборудование в соответствии с данными, полученными при регистрации на сервисе DynDNS (пункты 6.4.1 и 6.4.3 данного Руководства).

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

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

ВНИМАНИЕ!

IP-камера должна быть подключена к Интернету напрямую.

Шаг 1: выберите опцию **[DDNS]** в настройках IP-камеры: **НАСТРОЙКИ – Сеть – Дополнительно – DDNS**.

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

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

Введите пароль, полученный при регистрации на сайте провайдера DDNS в поле **[Пароль]**.

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

Введите доменное имя, полученное при регистрации на сайте провайдера DDNS в поле **[Имя домена]**.

ВНИМАНИЕ!

Более подробно настройка камеры через веб-интерфейс рассмотрена в [Руководстве по эксплуатации](#).

В соответствии с данными, полученными при регистрации в сервисе DDNS (пункты [6.4.2](#), [6.4.3](#) данного Руководства), в поле **[Сервер]** выберите `dyndns.org`, поля **[Пользователь]** и **[Пароль]** введите соответственно `camera184` и `123456`. В поле **[Имя домена]** необходимо указать `camera184.dyndns.org` (Рис. 6.4.4).

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



24

ВНИМАНИЕ!

Для применения параметров требуется перезагрузка устройства.

ВНИМАНИЕ!

Если обновление 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-100. Маршрутизаторы 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 аутентификации откроется основная страница настроек маршрутизатора. Выберите пункт **[General Setup]** (рис. 6.25).



Рис. 6.25

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 6.4.2, 6.4.3 данного Руководства), в поле **[Provider]** выберите **www.dyndns.org**, в поле **[Domain name]** укажите **camera184.dyndns.org**, в поля **[Account]** и **[Password]** введите соответствующие данные (например, 123456). (Рис. 6.26).



Рис. 6.26

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.

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

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

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
Переадресация HTTPS с помощью UPnP	443	1124..65534
RTSP	554	1124..65534
Переадресация RTSP с помощью UPnP	554	1124..65534
Начальный порт диапазона RTP	1024	1124..65435
Конечный порт диапазона RTP	7999	1223..65534
Порт видео для Мультикаст	1024	1124..65534
Порт аудио для Мультикаст	-	1124..65534
SMTP	25	1..65535
Порт удаленного сервера журнала событий	1024	1124..65534
Порт сервера событий	1024	1..65535
Порт прокси	1024	1..65535
Детектор движения	1999	-
Поток MPEG-4 (H.264)	80	1124..65534
Поток MJPEG (H.264)	80	1124..65534

Приложение В. Заводские установки

Ниже приведены некоторые значения заводских установок

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	

Приложение С. Гарантийные обязательства

С1. Общие сведения

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

б) Условия эксплуатации всего оборудования должны соответствовать ГОСТ 150-69, ГОСТ В20.39.304-76 (в зависимости от исполнения устройства).

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

С2. Электромагнитная совместимость

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

С3. Электропитание

Должно соответствовать параметрам, указанным в Руководстве по эксплуатации для конкретного устройства. Для устройств с внутренним источником питания – это переменное напряжение 220 В $\pm 10\%$, частотой 50 Гц $\pm 3\%$. Для устройств с внешним стабилизированным адаптером – источник питания 5 В $\pm 5\%$ или 12 В $\pm 10\%$ (напряжение пульсаций – не более 10%).

С4. Заземление

Все устройства, имеющие блок питания, должны быть заземлены путем подключения к специальному контакту 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 опорах, должен быть выполнен экранированным кабелем (или в металлорукаве), и линии экранирования должны быть заземлены с двух концов. Причем, если один конец экрана подключается к заземлению непосредственно на шине заземления, то второй – подключается к заземлению через разрыв.

С5. Молниезащита

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

С6. Температура и влажность

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

С7. Размещение

Для вентиляции устройства необходимо оставить 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 установить 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 сырости помещения.
- б) Отсутствие в воздухе агрессивных сред.
- в) В помещении, где установлено оборудование, не должно быть бытовых насекомых.
- г) Запрещается размещать на оборудовании посторонние предметы и перекрывать вентиляционные отверстия.

С8. Обслуживание

Оборудование необходимо обслуживать с периодичностью не менее одного раза в год. При очистке необходимо удалять пыль из него. Это позволит оборудованию работать без сбоев в течение длительного времени.

С9. Подключение интерфейсов

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

С10. Гарантийные обязательства

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

ООО «НПП «Бевард» не несет ответственности по гарантийным обязательствам при повреждении внешних интерфейсов оборудования (сетевых, телефонных, видеовыходных 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 других воздействий, если их параметры выходят за рамки допустимых значений, указанных в технических характеристиках, либо не предусмотрены технической спецификацией на данное оборудование;
- ж) воздействия высокого напряжения (ударные токи, статическое электричество и т.п.).

Приложение D. Права и поддержка

D1. Торговая марка

Copyright © BEWARD 2016.

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

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

D2. Ограничение ответственности

ООО «НПП «Бевард» не гарантирует, что продукты будут работать должным образом во всех средах и приложениях, и не дает гарантий и представлений, подразумеваемых или выраженных относительно качества, характеристик, или работоспособности при использовании в других целях. ООО «НПП «Бевард» приложило все усилия, чтобы сделать это Руководство наиболее точным и полным. ООО «НПП «Бевард» отказывается нести ответственность 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» берет на себя ответственности и не дает гарантий в выпуске обновлений или сохранении какой-либо информации в настоящем Руководстве по эксплуатации, и оставляет за собой право вносить изменения в данное Руководство и/или в описанные в нем, в любое время без предварительного уведомления. Если Вы используете в Руководстве информацию, которая является неправильной или неполной, что может ввести в заблуждение, мы будем Вам крайне признательны за комментарии и предложения.

D3. Интерференция

Это оборудование протестировано и признано удовлетворяющим требованиям положения о радиопомехах, принадлежащих к классу А, части 15 Правил Федеральной комиссии по связи (FCC). Эти ограничения были разработаны в целях защиты от вредных помех, которые могут возникать при использовании оборудования в коммерческих целях. Это оборудование может излучать, генерировать и распространять энергию в радиочастотном диапазоне. Если данное оборудование будет установлено и использоваться с отклонениями от настоящего Руководства, оно может оказать 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.

D4. Предупреждение CE

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

D5. Поддержка

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

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

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

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

Приложение Е. Совместимое PoE оборудование

Ревизия / SN	Модель	CD600	N630	N37210	N500	N300	B1210R	B2710R	B1210DM	B1710DM	0DM	B1210	B2720	B1720	B2720	B1710DV	B2720DV(Z)	B1710DR	B2710DR	DS03M	B5650	B2250
B2	D-Link DWL-P200	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
V4	TP-Link TL-SF1008P	-	-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
V2.5	TP-Link TL-SG3424P	-	-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
V3 / 2148895002278	TP-Link TL-PoE150S	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
AF00453500979	Planet POE-173	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
V2 / AF00094100032	Planet POE-2400	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
V3 / A310114400490	Planet FSD-804P	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
A310124200070	Planet FSD-804PS	+	+	-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
V2	Planet FNSW-1608PS	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
A920431700088	Planet FGSW-2612PVM	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
A920424400021	Planet FGSW-2620PVM	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
N13196541103443	Beward PD9501G	-	-	-	-	-	+	+	+	+	+	+	+	+	+	+	+	+	+	-	+	+
2415000211	Beward STL-11XP	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
1500100213	Beward STL-11HP	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
1500100066	Beward STL-01P	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
1400102594	Beward ST-8HP	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
1100103439	Beward ST-5HP4	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
1400101877	Beward ST-810HP	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
1500100027	Beward STP-811HP	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
1400100675	Beward STW-1622HP	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
1400100200	Beward STW-0240HP	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
1400100141	Beward STW-0240HP	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Приложение F. Глоссарий

3GP – мультимедийный контейнер, определяемый Партнёрским Проектом Третьего поколения (Third Generation Partnership Project (3GPP) для мультимедиа (3GPP Multimedia) (3GPP MM). Многие современные мобильные телефоны имеют функции загрузки, просмотра аудио и видео в формате 3GP.

ActiveX – это стандарт, который разрешает компонентам программ взаимодействие в сетевой среде независимо от языка, используемого для их создания. Веб-браузеры могут управлять элементами ActiveX, документами ActiveX и сценариями ActiveX. Элементы управления ActiveX загружаются и устанавливаются автоматически, как запрашиваемые. Эта технология не является кроссплатформенной и поддерживается в полном объеме только в среде Windows в браузере Internet Explorer 8.0.

ADSL (Asymmetric Digital Subscriber Line / Асимметричная цифровая абонентская линия) – модемная технология преобразования аналоговых сигналов, передаваемых посредством стандартной телефонной линии, в цифровые сигналы (пакеты данных), позволяющая во время работы получать 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. Съемочная зона зрения измеряется на линзе, фокус которой установлен в бесконечность. В зависимости от назначения, объективы делят на три типа: широкоугольные, нормальные и длиннофокусные. В широкоугольных объективах, которые чаще всего используют 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 15-30 градусов.

ARP (Address Resolution Protocol / Протокол определения адреса) – использующийся в компьютерных сетях протокол низкого уровня, предназначенный для определения физического уровня по известному адресу сетевого уровня. Наибольшее распространение 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 адресу.

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

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

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

Biterate / Битрейт (Скорость передачи информации) – обычно, скорость прохождения битов информации. Битрейт принято использовать при описании 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 фиксирует интегральную, т.е. общую освещенность сцены, «видимой» камерой через объектив. Малая фигура человека на большом светлом фоне окна вылетает в итоге "засветкой" всей картинкой. Включение функции «BLC» может в подобных случаях исправить работу автоматики камеры.

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

CIDR – Классовая адресация (англ. *Classless Inter-Domain Routing*, англ. *CIDR*) – метод адресации, позволяющий гибко управлять пространством IP-адресов, не используя жесткую классическую адресацию. Использование этого метода позволяет экономно использовать дефицитный ресурс IP-адресов, поскольку возможно применение различных масок подсетей для различных подсетей.

CMOS-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 может составлять 1/4", 1/3", 1/2" или 2/3".

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

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 время, то микросхемы КМОПа потребляют меньше электроэнергии. Микросхемы, использующие только один тип транзистора. Также датчики изображения КМОП, в которых микросхемах содержат схемы обработки, однако это преимущество невозможно использовать с ПЗС-датчиками, которые являются также более дорогими.

DDNS (Dynamic Domain Name System / DDNS / Динамическая технология, применяемая для назначения постоянного доменного имени устройству (компьютеру, сетевому накопителю) с динамическим IP-адресом. Это может быть IP-адрес, назначенный по DHCP или по IPCP в PPP-соединениях (например, при удаленном 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 принципу «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе инициализации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры.

DHCP Relay (Сервер DHCP-реле) – программа, которая назначает клиентам IP-адреса внутри заданного диапазона в определенный период времени. Данную функцию поддерживают практически все современные маршрутизаторы.

Digital Zoom (Цифровое увеличение) – это увеличение размера кадра не за счет оптического увеличения, а за счет цифрового. Камера ничего не увеличивает, а только вырезает нужную часть изображения и растягивает ее до заданного 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 компьютер, который аутентифицирует пользователей в сети.

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

Factory default settings / Заводские установки – по умолчанию это установки, которые изначально использованы для устройства, которое отгружается от завода в первый раз. Если возникнет необходимость переустановить устройство по заводским установкам по умолчанию, то эта функция применима для большинства устройств, и она полностью переустанавливает любые установки, которые были изменены пользователем.

Firewall / Брандмауэр – брандмауэр работает как барьер между сетями, например, между локальной сетью и интернетом. Брандмауэр гарантирует, что только зарегистрированным пользователям будет предоставлен доступ из одной сети в другую сеть. Брандмауэром может быть программа, работающая на компьютере, или брандмауэром может быть автономное аппаратное устройство.

Focal length / Фокусное расстояние – измеряемое в миллиметрах фокусное расстояние объектива камеры. Чем больше ширина горизонтальной зоны обзора, которое в свою очередь измеряется в градусах, тем больше 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 пересечения передней (задней) главной плоскости с оптической осью.

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

Frame / Кадр – кадр является полное видеоизображение. В формате 2:1 чересстрочной развертки интерфейса RS-170 и в форматах Международного консорциума по радиовещанию, кадр создается из двух отдельных областей. Для чересстрочной развертки 262.5 или 312.5 на частоте 60 или 50 Гц для того, чтобы сформировать кадр, который отобразится на экране на частоте 30 или 25 Гц. В прогрессивной развертке каждый кадр сканируется построчно и не является половинным; 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

обмениваются файлами между компьютерами/устройствами в сети. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загрузить файлы с сервера или на сервер. Протокол FTP относится к протоколам прикладного уровня. Для передачи данных использует транспортный протокол TCP. Команды и данные, в отличие от большинства других протоколов передаются по разным портам. Порт 20 используется на стороне сервера, используется для передачи данных, порт 21 - для передачи команд. Порт для приема данных клиентом определяется в диалоге согласования портов.

Full-duplex / Полный дуплекс – полный дуплекс представляет собой передачу данных одновременно в двух направлениях. В системах звуковоспроизведения это можно описать, например, телефонными системами. Также дуплекс 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. Таким образом, G.711 кодек создаёт поток 64 Кбит/с.

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

Gateway / Межсетевое шлюзовое устройство – межсетевым шлюзом является сеть, которая действует в качестве точки входа и выхода для трафика. Например, в корпоративной сети, сервер компьютера, действующий в качестве межсетевого шлюза, зачастую также действует и в качестве прокси-сервера сетевой защиты. Межсетевого шлюза часто связан как с маршрутизатором, который управляет пакетом данных, который приходит в межсетевого шлюза, так и с коммутатором, который предоставляет истинный маршрут в и из межсетевого шлюза для каждого пакета.

H.264 – это международный стандарт кодирования аудио и видео, (другое название 'MPEG-4 расширенный AVC (Advanced Video Coding)'). Данный стандарт содержит ряд новых возможностей, которые значительно повышают эффективность сжатия видео по сравнению с более старыми стандартами (MPEG-1, MPEG-2 и MPEG-4), обеспечивая также более высокое качество изображения в разнообразных сетевых средах. Используется в цифровом видео высокого разрешения (HDTV) и во многих других областях цифрового видео.

HTTP (Hypertext Transfer Protocol / Протокол передачи гипертекста) – это набор правил для передачи файлов (текстовыми, графическими, звуковыми, видео- и другими мультимедийными 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 / Защищенный 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, HTTPS по умолчанию используется TCP-порт 443.

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

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

IEEE 802.11 / Стандарт IEEE 802.11 – 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 802.11a 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 кадрами) в секунду, в которых каждые 2 последовательных поля (полукадра) записываются 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 риск искажения изображения.

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

IP67 (Ingress Protection) – это стандарт защиты оборудования, который описывает уровень защиты от попадания пыли и влаги. Первая цифра обозначает уровень защиты от попадания твердых 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 сжатия данных группы экспертов в области фотографии) – один из популярных графических форматов, применяемый для хранения фотоизображений и подобных изображений. При создании изображения JPEG имеется возможность настройки используемого коэффициента сжатия. Так как при более низком коэффициенте сжатия (т.е. с меньшим качеством) увеличивается объем файла, существует выбор между качеством изображения и объемом файла.

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

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

Lux / Люкс – единица измерения освещенности. Определяется как освещенность поверхности площадью 1 кв. метр световым потоком в 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 для обозначения «скорости» сети. Локальная сеть должна работать на скорости 100 или 1000 Мбит/сек.

MJPEG – 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 – международный стандарт, используемый преимущественно для сжатия цифрового аудио и видео. Стандарт MPEG-4 в основном используется для вещания (потокосжатия), записи фильмов на компакт-диски, видеотелефонии (видеотелефон) и широковеб-вещания, 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 получателем, существуют такие приложения, где требуется, чтобы источник послал информацию сразу группе получателей. При традиционной технологии IP-адресации требуется каждому получателю информации послать свой пакет данных, то есть одна информация передается много раз. Технология групповой адресации представляет собой расширение IP-адресации, позволяющее направить одну копию пакета сразу к множеству получателей. Множество получателей определяется принадлежностью каждого 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. 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 протоколов TCP/IP, полная 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. «Мультимедиа» 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 – адрес маршрутизаторов 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 назначаются 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.

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 2001 году с целью разработки и распространения открытого стандарта для систем сетевой 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 сетевой ресурс, выделяемый приложению, выполняемому на некотором сетевом хосте, для взаимодействия с приложениями, выполняемыми на других сетевых хостах (в том числе и другими приложениями на этом же хосте). В обычной клиент-серверной модели сервер ожидает входящих данных или запроса на соединение («слушает порт»). Клиент отправляет данные или запрос на соединение на известный порт, открытый приложением на сервере.

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 over Ethernet / Протокол «точка - точка» по Ethernet) – протокол для подключения пользователей локальной сети Ethernet к Интернету через широкополосное соединение, такое как линия DSL, беспроводное устройство или кабельный модем. С помощью PPPoE широкополосного модема пользователи локальной сети могут получать доступ с индивидуальной идентификацией подлинности к высокоскоростным сетям данных. Объединяет 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 видео, при которой каждый кадр воспроизводится по одной линии в полном размере, начиная с первой, затем 2, затем 3 и так далее. Таким образом, изображение не бьется по частям. В этом случае полностью исчезает эффект мерцания, поэтому снятое видео получается более высоким.

RJ-45 – стандартизированный 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 таблицу маршрутизации, которая сохраняет информацию, как только она помогает определить конечных пунктов назначения. Иногда маршрутизатор включен в состав части другого 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 приемнике. Кроме того, в заголовке протокола, в частности, передаются временная метка и номер пакета. Эти параметры позволяют при минимальных задержках определить порядок и момент приема каждого пакета, а также интерполировать потерянные пакеты. В качестве нижнего 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, передаваемых по сети. Серверы RTSP обычно используют RTP в качестве транспортного протокола для передачи аудио- и видеоданных.

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

Shutter / Затвор – это элемент матрицы, который позволяет регулировать время 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 SMTP является «простым» по своей структуре, то он ограничен в своей возможности по вместимости сообщений на получающем конце, и он обычно используется с одним из двух других протоколов, POP3 или протоколом интерактивного доступа к электронной почте.

(протокол IMAP). Эти протоколы позволяют пользователю сохранять сообщения в почтовом ящике сервера и периодически загружать их из сервера.

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

Subnet mask / Маска подсети – битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая – к адресу конкретного узла в этой сети. Например, узел с IP-адресом 192.168.0.99 и маской 255.255.0 находится в сети 192.168.0.0.

Switch / Коммутатор – коммутатором называется сетевое устройство, которое соединяет сегменты сети вместе и выбирает маршрут для пересылки устройством данных к его ближайшему получателю. Сетевой 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 по протоколу IP. TCP – транспортный механизм, предоставляющий поток данных с предварительным установлением соединения, за счёт этого дающий уверенность в достоверности передаваемых данных, осуществляет повторный запрос данных в случае потери данных и дублирование при получении двух копий одного пакета (см. также T/TCP).

TTL (Time To Live / Время жизни) – максимальный период времени или число итераций или переходов, за который пакет (пакет) может существовать до своего исчезновения. Значение TTL рассматривается как верхняя граница времени существования IP-дейтаграммы в сети. TTL устанавливается отправителем дейтаграммы и уменьшается каждым узлом (маршрутизатором) на пути его следования, в соответствии со временем пребывания в этом 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 пакеты по сети, использующей протокол IP. Протокол UDP является альтернативой протоколу TCP. Преимущество протокола UDP состоит в том, что для него не обязательна доставка всех данных и некоторые пакеты могут быть пропущены, если сеть перегружена. Это особенно удобно при передаче видеоматериалов в режиме реального времени, так как не имеет смысла повторно передавать устаревшую информацию. В этом случае все равно будет отображена.

UPnP (Universal Plug and Play) – технология, позволяющая персональным компьютерам и интеллектуальным сетевым системам, периферийному оборудованию, развлекательным устройствам или интернет-шлюзам взаимодействовать между собой автоматически и работать совместно через единую сеть. Платформа UPnP строится на основе таких интернет-стандартов, как SOAP и XML. Технология UPnP поддерживает сетевые инфраструктуры проводных и беспроводных сетей – как проводные, так и беспроводные. В их число, в частности, входят Ethernet, беспроводные сети Wi-Fi, сети на основе телефонных линий, оптоволоконного кабеля и пр. Поддержка UPnP реализована в операционных системах Windows, Mac OS, Linux.

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

WAP (Wireless Application Protocol / Единый протокол передачи данных) – протокол, созданный специально для беспроводных сетей, где нужно устанавливать связь портативных устройств с Интернетом. С помощью WAP пользователь мобильного устройства может загружать различные цифровые данные.

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

Wi-Fi (Wireless Fidelity, условно – «беспроводная точность») – торговая марка промышленной организации Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Любое устройство, соответствующее стандарту IEEE 802.11, может быть помечено как Wi-Fi Alliance для получения соответствующего сертификата и права использования Wi-Fi.

WLAN / Беспроводная LAN – это беспроводная локальная сеть, использующая в качестве 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 сохраняет 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 положение.

Витая пара – вид кабеля связи, состоящий из одной или нескольких пар изолированных проводников, скрученных между собой и заключенных в пластиковую оболочку. Свивание проводников производится с целью уменьшения степени связи между собой проводников одной пары (электромагнитная помеха негативно влияет на оба провода пары) и последующего уменьшения электромагнитных помех от внешних источников, а также взаимных наводок при передаче дифференциальных сигналов.

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

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

Детектор саботажа – это программный модуль, который позволяет обнаруживать такие ситуации, как: разфокусировка, перекрытие или засвечивание изображения, отворот камеры, частичная потеря сигнала. Принцип действия основан на анализе в режиме реального времени изменений контраста локальных областей кадров из видеопотока, получаемого с камеры. Детектор саботажа автоматически выбирает области кадров, которым необходимо оценивать изменение контрастности во времени и, если изменение контрастности в этих областях превышает некоторый относительный порог, инициирует сигнал тревоги 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. Такие имена дают возможность адресации интернет-узлов и расположенных на них 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, изображение становится черно-белое, в результате чего повышается контрастность.

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 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 относится к сжатию/распаковке, и в этом случае он обычно означает алгоритм или компьютерную программу для уменьшения объема файлов и программ.

Нормально замкнутый контакт – 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 системы видеонаблюдения, предназначенная для фокусировки изображения на матрице видеокамеры.

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

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

Прокси-сервер (Proxu – представитель, уполномоченный) – служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым ресурсам. 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 функций при передаче данных. Формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты на одном уровне, но в разных узлах.

Разрешение изображения – это количество пикселей на единицу площади изображения. Измеряется в мегапикселях или отображаемых 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 диаметр открытой диафрагмы (или, соответственно, чем меньше число f), тем большее количество света может попасть сквозь объектив на фоточувствительную поверхность, тем выше светосила объектива.

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

Уличная видеочамера – камера видеонаблюдения, которая обладает всеми необходимыми характеристиками для работы в окружающей среде для работы на улице.

Цветная видеочамера – это камера, которая дает цветное изображение. По определению матрица камер черно-белые, а для получения цветного изображения возле каждой ячейки матрицы устанавливаются цветные фильтры. Первый фильтр привносит красную составляющую цвета, второй – зеленую, а третий синюю. Таким образом, три ячейки становятся одним цветом в формате RGB. Следовательно, вместо трех пикселей на результате одним изображением мы получаем только один.

Электромеханический ИК-фильтр – представляет собой устройство, которое способно в любой момент времени включать инфракрасный диапазон при помощи инфракрасного ИК-фильтра, а в другое время ИК-фильтр убирается электромеханически, таким образом, делая видимым весь спектр светоизлучения.